Guido Fubini. Lezioni di Teoria dei numeri (1916-17)

CENTRO STUDI DI STORIA DELL'UNIVERSITÀ DI TORINO
Lezioni e Inediti di 'Maestri' dell'Ateneo Torinese

GUIDO FUBINI

LEZIONI DI TEORIA DEI NUMERI 1916-17

Università degli Studi di Torino

CENTRO STUDI DI STORIA DELL'UNIVERSITÀ DI TORINO

Lezioni e Inediti di 'Maestri' dell'Ateneo Torinese

4

1. Guido Fubini (1879-1943)

CENTRO STUDI DI STORIA DELL'UNIVERSITÀ DI TORINO

Lezioni e Inediti di 'Maestri' dell'Ateneo Torinese

4

Guido Fubini

Lezioni di Teoria dei numeri
1916-17

A cura di

Erika Luciano, Elena Scalambro, Lea Terracini

Università degli Studi di Torino

CENTRO STUDI DI STORIA DELL'UNIVERSITÀ DI TORINO

Lezioni e Inediti di 'Maestri' dell'Ateneo Torinese

ISBN: 978-88-909997-6-5

Questo volume è stato sottoposto a referaggio da parte di Aldo Brigaglia (Università di Palermo) e di Paolo Valabrega (Politecnico di Torino). Il Centro Studi di Storia dell'Università di Torino è responsabile del processo.

INDICE

Prefazione di Paolo Valabrega p. IX

Abbreviazioni e sigle p. XI

Introduzione. Le *Lezioni di Teoria dei numeri* di G. Fubini – a cura di Erika Luciano, Elena Scalambro, Lea Terracini p. 1

1. Fubini e la teoria dei numeri, fra ricerca e insegnamento p. 1
2. L'insegnamento della teoria dei numeri in Italia p. 2
3. Il corso di Fubini del 1916-17 p. 4
4. Temi e contenuti delle *Lezioni di Teoria dei numeri* p. 8
   4.1. Concetti preliminari p. 8
   4.2. Geometria dei numeri p. 11
   4.3. *'Completeremo aggiungendo nuovi enti che chiameremo ideali'*: forme quadratiche e ideali p. 14
   4.4. Cenni di aritmetica analitica, corpi quadratici e campi ciclotomici p. 19
5. Conclusioni p. 32

Appendice – I corsi di Teoria dei numeri in Italia dal 1910 al 1938 p. 35

Guido Fubini, *Lezioni di Teoria dei numeri*, a.a. 1916/1917 p. 39

Criteri dell'edizione critica p. 41

Capitolo I – Introduzione p. 43
1. L'algoritmo di Euclide per l'MCD p. 43
2. Campi oloidi p. 45
3. Moduli e ideali p. 48
4. Un primo esempio di aritmetica analitica p. 50
5. La funzione $\varphi(m)$ e sue prime proprietà p. 52

Capitolo II – Congruenze p. 55
1. Definizioni p. 55
2. Il teorema di Fermat p. 57
3. Congruenze di primo grado ed analisi indeterminata di primo grado p. 58
4. Sistemi di congruenze di primo grado p. 61
5. Congruenze di grado qualunque p. 63
6. Il teorema di Wilson p. 65
7. Radici primitive; indici p. 65
8. Congruenze binomie p. 67
9. Applicazioni ed esercizi p. 71

Capitolo III – Geometria dei numeri p. 75
1. Rete di punti p. 75
2. Gruppi di traslazioni e campi fondamentali p. 86
3. Il teorema fondamentale di Minkowski p. 81
4. Ricerca dei parallelogrammi ed esagoni limiti p. 83
5. I campi del tipo $|\alpha x + \beta y|^p + |\gamma x + \delta y|^p \leq 1$ p. 85
6. Studio più completo della precedente disuguaglianza p. 87
7. Risoluzione del problema nel caso *p=2* p. 90
8. Sistema di due reti una contenuta nell'altra p. 91

Capitolo IV – Applicazioni e illustrazioni aritmetiche p. 95
1. Analisi indeterminata di primo grado p. 95
2. Frazioni continue p. 95
3. Interpretazione geometrica p. 97
4. Considerazioni aritmetiche p. 100
5. Generalizzazione coi teoremi di Minkowski p. 101
6. Riduzione delle forme quadratiche binarie definite p. 103

Capitolo V – Analisi indeterminata di secondo grado e forme quadratiche p. 105
1. Considerazioni generali sulle trasformazioni modulari p. 105
2. Analisi indeterminata di secondo grado p. 106
3. Forme definite ridotte p. 108
4. Il campo fondamentale del gruppo modulare p. 113
5. Riduzione di una forma definita p. 117
6. Forme indefinite p. 121
7. Periodi di forme ridotte p. 123
8. Trasformazioni che portano una forma in una forma equivalente p. 125

Capitolo VI – Numeri interi algebrici p. 129
1. Una prima generalizzazione del numero intero p. 129
2. Alcune nuove difficoltà p. 133
3. Alcuni cenni di geometria dei numeri nello spazio a 3 dimensioni p. 134
4. Campi algebrici p. 136
5. Numeri interi algebrici p. 140
6. Unità di un corpo algebrico p. 144
7. Il gran teorema di Dirichlet p. 145
8. Il caso dei corpi quadratici p. 147

Capitolo VII – Teoria della divisibilità di un corpo algebrico p. 151
1. Un esempio preliminare p. 151
2. Prime definizioni della teoria degli ideali p. 152
3. Un lemma fondamentale p. 156
4. Prodotto di ideali p. 157
5. Teoria di Kronecker – Hilbert p. 160
6. Generalizzazioni aritmetiche varie p. 163
7. Generalizzazione della funzione φ e del teorema di Fermat. Ideali primi p. 167
8. Classi di ideali p. 169
9. Ideali primi p. 174
10. Applicazione dei precedenti risultati p. 178
11. Forme decomponibili del corpo p. 180

Capitolo VIII – Aritmetica analitica p. 181
1. Lemmi fondamentali p. 181
2. Alcune trasformazioni di serie p. 183
3. Volume di un corpo C in uno spazio a m dimensioni p. 185
4. Un limite fondamentale p. 186
5. Calcolo del volume di C_1 p. 188
6. Il grande teorema della progressione aritmetica p. 190

Capitolo IX – I corpi quadratici p. 193
1. Ideali primi p. 193
2. Ideali di un corpo quadratico p. 194

3. Ideali ambigui e applicazioni p. 195
4. Il teorema di reciprocità p. 198
5. L'ultimo problema di Fermat – Osservazioni preliminari p. 201
6. Forme quadratiche p. 204

Capitolo X – L'equazione dei poligoni regolari p. 211
1. Formule preliminari p. 211
2. I periodi di Gauss p. 213
3. Il teorema di reciprocità p. 218
4. Ideali primi nel corpo $K(z)$ p. 219

Bibliografia p. 225
Fonti iconografiche p. 235
Indice dei nomi e dei soggetti p. 237

Prefazione

PAOLO VALABREGA

Guido Fubini fu professore di Analisi matematica al Politecnico di Torino dal 1908 al 1938, anno in cui fu espulso in forza delle leggi per la difesa della razza e fu costretto a trasferirsi all'estero. A lui si devono importanti risultati in vari e diversi campi della matematica, a partire dal famoso e citatissimo Teorema di Fubini sull'inversione dell'ordine delle integrazioni. Sono anche ben note le sue grandi capacità didattiche, espletate nel corso tenuto per tanti anni al Politecnico ma anche in quello di Analisi superiore, da lui svolto presso l'Università di Torino dal 1910 al 1938, nel quale trattava ogni anno un nuovo argomento, dalle equazioni differenziali alle funzioni ellittiche, dalla geometria non euclidea alla geometria proiettiva differenziale.

Nel 1916-17 il corso di Analisi superiore riguardò la Teoria dei numeri, argomento per lui di notevole interesse culturale, pur senza aver mai costituito oggetto di ricerche originali. Non ci sono infatti nel corso risultati nuovi, ma la trattazione è certo di alto livello e affronta questioni anche molto difficili.

Il testo litografato delle sue lezioni manoscritte è stato ritrovato dalle autrici nella biblioteca di matematica dell'Università; si tratta in realtà di un manoscritto di non facilissima lettura che le autrici hanno ricostruito e riprodotto in una bella edizione critica, munita di centinaia di note, in parte esplicative del testo (talvolta non chiarissimo, anche a causa della calligrafia), in parte dedicate a riferimenti bibliografici e storici, nelle quali compaiono i numerosi scritti consultati da Fubini, dovuti ai pochi matematici italiani che si erano occupati di teoria dei numeri e ai non pochi matematici, soprattutto tedeschi, che vi avevano già dato contributi importanti.

La riproduzione del manoscritto è preceduta da una trentina di pagine di introduzione e commento. In esse si presenta brevemente lo stato degli studi (quasi inesistenti) di teoria dei numeri in Italia tra la fine dell'Ottocento e i primi due decenni del Novecento, a cui corrispondono ben pochi insegnamenti universitari (elencati dalle autrici dettagliatamente). Si esamina quindi l'architettura del corso, presentando e discutendo l'elenco dei testi (principalmente tedeschi) ai quali Fubini fa, implicitamente o anche esplicitamente, riferimento. Non viene dimenticata l'*audience* delle lezioni che, trattandosi di anni di guerra, era prevalentemente femminile.

Le autrici passano quindi a descrivere il contenuto del corso, capitolo per capitolo, mettendo in evidenza i temi che vengono affrontati, i concetti introdotti, le dimostrazioni proposte agli studenti, con particolare attenzione, in alcuni casi, alle ragioni, interne al corso stesso, della scelta di una fra varie dimostrazioni possibili. Si parte da questioni semplici sui numeri primi, le congruenze, l'insieme $\mathbb{Z}$ degli interi e quello dei polinomi in una variabile, per arrivare allo studio delle equazioni diofantee, della fattorizzazione negli anelli di interi (da Fubini chiamati 'campi oloidi'), degli interi algebrici di un campo, degli ideali di un anello, dei campi quadratici e ciclotomici, dei collegamenti fra teoria dei numeri e geometria, dell'ultimo teorema di Fermat. È continuo il riferimento alle opere dei matematici italiani, Bianchi (maestro di Fubini) e Gazzaniga, ma soprattutto dei principali studiosi stranieri di teoria dei numeri, conosciuti da Fubini grazie anche alla sua ottima conoscenza del tedesco (Euler e Gauss *in primis*, Kummer e Dedekind, Dirichlet, Klein, Minkowski, Hilbert, Chebyshev, ecc.).

In particolare le autrici mettono in evidenza l'introduzione e l'uso da parte di Fubini della teoria degli ideali, rilevandone pregi e difetti.

Occorre sottolineare che la presentazione di quanto fatto da Fubini è integrata e completata da considerazioni e commenti sugli sviluppi successivi della teoria dei numeri, riguardanti fra l'altro la funzione zeta, il teorema dei numeri primi, la funzione $\pi(x)$, le leggi di reciprocità dovute a Emil Artin, fino alla risoluzione della congettura di Fermat da parte di Andrew Wiles.

Nelle lezioni di Fubini non si tratta la teoria di Galois, oggetto di un corso successivo, nell'anno accademico 1931-32; purtroppo le autrici, nonostante gli sforzi, non hanno trovato il testo litografato, del quale è comunque attestata l'esistenza.

Fra l'introduzione e la riproduzione del manoscritto è inserita una interessante tabella con sedi, anni e argomenti dei corsi di Teoria dei numeri tenuti in Italia fra il 1910 e il 1938 (ultimo anno di Fubini in Italia, a causa delle leggi per la difesa della razza). Non ho informazioni su di essi, ma certo posso affermare che le lezioni di teoria dei numeri proposte da Fubini a Torino nel 1916-17 furono di livello ben alto, al punto che temo non sarebbero facilmente presentabili in un corso di laurea in matematica di quarto o quinto anno dei nostri giorni.

ABBREVIAZIONI E SIGLE

a.a.	anno accademico
art.	Articolo
ASUT	Archivio Storico dell'Università di Torino
AsTo Poli	Archivio storico del Politecnico di Torino
ASTo	Archivio di Stato di Torino
BAMS	Bulletin of the American Mathematical Society
BSM	Biblioteca Speciale di Matematica, Dipartimento di Matematica 'G. Peano', Università di Torino
c.d.d.	come dovevasi dimostrare
cap.	capitolo/i
cfr.	confronta
CNR	Consiglio Nazionale delle Ricerche
CSSUT	Centro Studi per la Storia dell'Università di Torino
DSSP	Deputazione Subalpina di Storia Patria, Torino
ed., eds.	Editore/i
es.	esempio/i
Euclide, *Elementi*	Euclide, *Elementi*, a cura di A. Frajese e M. Maccioni, Torino, UTET, 1977
fasc.	fascicolo/i
fr.	francese
IAS	Institute for Advanced Study, Princeton
ingl.	inglese
it.	italiana
Lib.	Libro
LRQ	Legge di Reciprocità Quadratica
M.C.D.	Massimo Comun Divisore
mod.	modulo
ms.	manoscritto
n.	numero
p.	pagina/e
p. es.	per esempio
prop.	proposizione
reg.	registro/i
s.	Serie
sez.	sezione
suppl.	supplemento
t.	Tomo
teor.	Teorema
UMI	Unione Matematica Italiana
UTF	Ultimo Teorema di Fermat

Introduzione: le Lezioni di Teoria dei numeri di G. Fubini (1916-17)

ERIKA LUCIANO - ELENA SCALAMBRO - LEA TERRACINI

1. *Fubini e la teoria dei numeri, fra ricerca e insegnamento*

Fubini non è un teorico dei numeri. Il 'little giant' della matematica italiana è un analista, un geometra proiettivo-differenziale, un matematico applicato, ma non un teorico dei numeri.[1] Lui, che si era formato alla Scuola di Luigi Bianchi a Pisa, seguendone i corsi del 1897 incentrati sulla teoria dei gruppi di sostituzioni e sulle equazioni algebriche secondo Galois[2], eredita tuttavia dal suo Maestro il gusto per questa disciplina, e soprattutto per alcune sue linee di sviluppo: poligoni e poliedri fondamentali di gruppi discontinui, forme aritmetiche e ideali, forme quadratiche ed Hermitiane.[3]

Il fatto che, nei ventotto anni in cui tiene per incarico l'insegnamento di Analisi superiore presso la facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università di Torino, scelga di dedicare due corsi monografici alla teoria dei numeri è indicativo del suo interesse non episodico per questo settore di studi. Dopo le lezioni nel 1916-17,[4] qui pubblicate, Fubini tornerà di fatto a occuparsi di numeri algebrici e della relazione tra le equazioni algebriche e i campi di Galois nel 1931-32,[5] e infine tratterà le reti modulari e i loro legami con l'analisi diofantea nell'ultimo corso tenuto a Torino nel 1937-38, prima di essere costretto a lasciare l'Italia e a riparare all'Institute for Advanced Study di Princeton, a causa delle leggi razziali.

Fubini non ha al suo attivo una produzione di ricerca di carattere originale in teoria dei numeri ma vanta una salda cultura in materia. Poliglotta (conosce perfettamente il francese e il tedesco), egli può del resto contare su una biblioteca, quale quella Speciale di Matematica, fra le più ricche e fornite a livello nazionale[6] e su una rete di contatti scientifici intrecciati da Corrado Segre, Gino Fano, Guido Castelnuovo e Federigo Enriques con i matematici tedeschi, *in primis* con quelli di Göttingen, fin dal 1883.[7]

Fubini è un didatta eccellente. Le sue lezioni, sia quelle di Analisi infinitesimale al Politecnico di Torino sia quelle di carattere monografico che tiene all'Università sono leggendarie per ampiezza di orizzonti culturali, rigore metodologico, precisione e chiarezza espositiva. Per Fubini, *"parlatore vivace e arguto, sovente paradossale"*, far lezione è *"gioia e piacere"*[8]. Capace di captare e di conservare l'attenzione dell'uditorio, egli prova autentica soddisfazione nel trasmettere il sapere, e i suoi allievi, a Catania come a Torino, a Princeton come a New York, lo considerano un idolo.[9]

---

[1] Sulla biografia scientifica di Fubini cfr. Severi 1943, *Guido Fubini's obituary*, New York Times, 10.6.1943, Terracini 1944, Picone 1946, Segre 1954, Tricomi 1957, Tricomi 1962, Terracini 1968, Nastasi 1993, Magenes 1998, Roero 1999. Nuovi elementi in merito alla traiettoria personale e professionale di Fubini sono emersi dallo studio delle fonti d'archivio custodite in AsTo Poli, fascicolo personale di G. Fubini; ASUT, fascicolo personale di G. Fubini; Archivio delle tradizioni e del costume ebraici B. e A. Terracini, Torino; Archivio dell'IAS, Princeton; Archivio personale di David Fubini e Laurie Fubini Jacobs.

[2] Cfr. Bianchi 1897, Bianchi 1899.

[3] Cfr. Fubini 1929b, p. XXXV; Fubini 1928, p. 96.

[4] Fubini potrebbe aver deciso di dedicare il corso di Analisi superiore dell'a.a. 1916/17 alla teoria dei numeri a guisa di omaggio alla memoria di R. Dedekind, scomparso nell'aprile del 1916.

[5] La biblioteca personale di Fubini, allo stato attuale delle nostre ricerche, risulta purtroppo perduta. Al momento non sono ancora stati ritrovati gli appunti di questo secondo corso di teoria dei numeri.

[6] Cfr. Giacardi, Roero 1999; Luciano 2018a.

[7] Cfr. Luciano, Roero 2012; Conte, Giacardi 2016.

[8] Segre 1954 p. 286.

[9] Sul talento didattico di Fubini cfr. anche Picone 1946, p. 57 e Scimone 1989, p. 174.

2. *L'insegnamento della teoria dei numeri in Italia*

Nonostante la presenza di alcuni ottimi cultori, fino alla fine dell'Ottocento la teoria dei numeri non vanta in Italia una tradizione di ricerca di rilievo. Questa "astrusa" disciplina esercita il suo "fascino irresistibile"[10] su Enrico Betti[11] a Pisa e su Angelo Genocchi a Torino che, avidi lettori delle *Disquisitiones Arithmeticae* di Gauss, acquisiscono autonomamente la padronanza di alcuni 'capitoli': equazioni algebriche, teoria di Galois, teoria delle congruenze, ecc.[12] I loro, però, sono casi sostanzialmente isolati.

L'attenzione verso questi studi inizia a crescere a seguito della pubblicazione delle traduzioni italiane di tre testi fondamentali: la terza edizione delle *Vorlesungen über Zahlentheorie* di J.P.L Dirichlet, con la celebre appendice di R. Dedekind, a cura di Aureliano Faifofer (1881), quella del volume di E. Netto sulla teoria di Galois[13], ad opera di Giuseppe Battaglini (1885)[14], e la versione del saggio di P.L. Chebyshev sulle congruenze, edito con appunti e note da Iginia Massarini nel 1895.

In questo momento storico, fra i cultori di teoria dei numeri si contano in verità più insegnanti che matematici di professione: oltre a Faifofer e Massarini, basti citare P.A. Fontebasso, G. Candido e G. Frattini, che affidano i loro contributi ai giornali di taglio didattico (*La Matematica elementare*, *Il Bollettino di Matematiche*, *Il Bollettino di Matematica*, ecc.)[15] e Umberto Scarpis, autore del primo manuale di teoria dei numeri (1897).[16]

A fronte della posizione marginale di questa disciplina, non stupisce che siano ben poche le Università che contemplano regolarmente nella propria offerta formativa corsi di teoria dei numeri. Paolo Gazzaniga[17], libero docente a Padova, è l'unico a tenerne uno in modo continuativo dal 1885 al 1921. Gli studenti interessati a perfezionarsi in questo ambito si vedono dunque costretti a farlo fuori dall'Italia: emblematico, in tal senso, è il caso di Ernesto Cesàro che si reca in Belgio per completare il proprio apprendistato scientifico sotto la guida di Eugène Catalan.[18]

La situazione muta a inizio Novecento, principalmente per merito di Bianchi che, nel *"tentativo di sopperire ad una precisa carenza nel campo della cultura matematica italiana"*,[19] promuove largamente lo studio della teoria dei numeri attraverso le sue lezioni a Pisa (1899, 1911-12), nelle quali introduce per la prima volta la teoria degli ideali secondo l'impostazione della scuola tedesca. Il magistero di Bianchi lascia un'impronta durevole. Fra i suoi allievi alla Normale che si occuperanno di teoria dei numeri – in termini più o meno consistenti – troviamo G. Fubini, O. Nicoletti, G. Sansone, P. Mazzoni, A.M. Bedarida,[20] L. Fantappiè, T. Chella e F. Cecioni.

---

[10] Peano, 1889-90, p. 196.

[11] Sul ruolo di Betti cfr. Bottazzini 1982 e Mammone 1989.

[12] Cfr. Viola 1991; Goldstein, Schappacher, Schwermer 2007. Le celebri *Disquisitiones Arithmeticae* di C.F. Gauss (1801) avevano avuto scarsa ricezione in Italia, salvo casi sporadici quali Giuseppe Malfatti, ormai a fine carriera, e Guglielmo Libri che aveva pubblicato nel 1820 un lavoro sulle congruenze.

[13] Sui contributi italiani nella prima metà del XX sec. alla teoria di Galois cfr. Toti Rigatelli 1992.

[14] Battaglini ebbe il merito di aver diffuso in Italia il trattato di C. Jordan *Traité des substitutions et des équations algébriques* (1870) che rappresenta il primo esempio di concezione strutturale dell'algebra moderna. Cfr. Brigaglia, Scimone 1998, p. 507; Goldstein 2005; Brigaglia 2017.

[15] Cfr. *inter alia* Sforza 1900; Bortolotti 1908; Bottari 1912; Composto 1912; Concina 1913; Cavallaro 1914a e 1914b.

[16] Scarpis 1897.

[17] Per approfondimenti su Gazzaniga cfr. Emaldi 1994.

[18] Sull'apprendistato scientifico di Cesàro alla Scuola di Catalan cfr. Goldstein 1989; Butzer, Carbone, Jongmans, Palladino 1999 e 2000.

[19] Brigaglia, Scimone 1998, p. 520. Sui corsi di teoria dei numeri di Bianchi alla Normale si veda anche Pepe 2011.

[20] Alberto Mario Bedarida (1890-1957), cultore di teoria dei numeri e di geometria differenziale e libero docente di Analisi algebrica presso l'Università di Genova, recensisce fra l'altro le *Lezioni di Teoria dei numeri* di Fubini per il Bollettino di Matematica (1922, vol. XVIII, p. XVIII). All'interno della sua produzione compaiono vari

A partire dagli anni Venti, Pisa cede a Catania il testimone, come principale polo di sviluppo degli studi algebrici a livello nazionale: qui operano G. Scorza e M. Cipolla,[21] entrambi ex-allievi di Bianchi e autori di volumi di ottimo livello: *Corpi Numerici ed Algebre* (1921), *Teoria dei Gruppi di Ordine Finito e sue Applicazioni* (1919-1923) e *Lezioni sulla Teoria dei Numeri Algebrici* (1923).[22] Con il trasferimento di Scorza a Napoli, anche in questa città verrà a crearsi un certo interesse per la teoria dei numeri, come dimostrano gli studi di N. Spampinato e di S. Cherubino.[23]

Gli anni fra il 1925 e il 1938 sono tra i più critici per l'algebra italiana[24]. In questo periodo il nostro paese accumula un ritardo tale da poter essere colmato (parzialmente) solo nel secondo dopoguerra. La comunità matematica, compresi parecchi nomi illustri come F. Severi, resta sostanzialmente estranea all'impetuoso sviluppo che gli studi algebrici stanno conoscendo all'estero e anzi rifiuta di dare loro adeguato riconoscimento a livello istituzionale.[25] Gli insegnamenti di carattere avanzato, come quelli di Bianchi a Pisa e di Scorza e Cipolla a Catania, sono spenti, fatte salve poche eccezioni: Giovanni Ricci, che continua a insegnare teoria dei numeri alla Normale di Pisa dal 1928 al 1936; Fubini a Torino, Giuseppe Belardinelli a Milano, Beppo Levi e Ettore Bortolotti a Bologna.[26]

I ricercatori più promettenti, come Bedarida e Chella, disincentivati a occuparsi di questi studi, dirigono i propri interessi verso l'analisi e la geometria algebrica[27] che, insieme alla fisica matematica, aprono migliori prospettive di carriera. Chi è particolarmente sensibile alle istanze dello "spirito aritmetico algebrico"[28], si reca in Germania. Fabio Conforto, ad esempio, vincitore di una borsa di studio del CNR nel 1931-32, sceglie Gottinga per avere l'opportunità di seguire i corsi di E. Landau (teoria dei numeri analitica con approfondimenti sulla funzione zeta di Riemann), H. Weyl (teoria dei gruppi), H. Weber (numeri algebrici) ed Emmy Noether (algebra non commutativa). Conscio del fatto che in Italia *"l'Algebra moderna non è per niente entrata nell'ambito scolastico"*[29], Conforto tenterà poi di importare l'indirizzo tedesco nelle sue lezioni di teoria dei numeri all'Università La Sapienza di Roma, fra il 1939 e il 1948. [30]

---

lavori che si collocano nell'alveo della tradizione italiana di teoria dei numeri e che coniugano lo studio delle forme e le ricerche sugli ideali. Fra questi si può citare la nota *Le classi di forme aritmetiche di Dirichlet appartenenti ai generi della classe principale* (Bedarida 1922a, 1922b), presentata ai Lincei proprio dal socio corrispondente Fubini, nella quale Bedarida riprende dal corso di Fubini del 1916-17 la notazione con $K(\sqrt{-1})$ per indicare il corpo che attualmente si indica con $\mathbb{Q}(\sqrt{-1})$ o $\mathbb{Q}(i)$. Su Bedarida cfr. Sbrana 1957; Rollandi 2002; Varnier 2003.

[21] Sui *Rendiconti del Circolo Matematico di Palermo*, diretti dal 1914 da Michele De Franchis, compaiono pregevoli lavori di Cipolla sulle equazioni algebriche le cui radici sono tutte radici dell'unità (1914), oltre a quelli di P. Nalli sulla serie di Dirichlet (1915-1917), di A. Maroni sulla teoria dei gruppi (1915) e di V. Amato sulla risoluzione 'apiristica' delle congruenze binomie. Cfr. Martini 2004.

[22] Cfr. Brigaglia 2007; Brigaglia, Scimone 1998; Scimone 1989.

[23] Per una panoramica sulla matematica in Italia negli anni Venti cfr. Corry 1996.

[24] Per una panoramica sull'Algebra astratta fra le due guerre cfr. Guerraggio, Nastasi 2006.

[25] Per quanto riguarda l'interesse di Severi per l'Algebra astratta cfr. Van der Waerden 1970; Slembek 2007; Koreuber 2015.

[26] Si veda la tavola *I corsi di Teoria dei numeri in Italia (1910-1938)*, p. 35, 36 di questo volume.

[27] Sulla geometria algebrica cfr. Bottazzini, Gray 2013.

[28] Conforto a Bompiani, Göttingen 18.2.32 in Nastasi 2016.

[29] Conforto a Bompiani, Göttingen 24.1.32 in Nastasi 2016.

[30] Benedicty 1954, p. 227.

3. *Il corso di Fubini del 1916-17*

Il semestre in cui Fubini tiene le sue lezioni di teoria dei numeri è un momento drammatico dal punto di vista storico e politico.[31] L'Italia è entrata in guerra da circa un anno, accanto alla Triplice Intesa, e le condizioni economiche e sociali della popolazione, sensibilmente peggiorate, hanno costretto molte famiglie a far interrompere gli studi ai propri figli. A ciò si aggiunga che il reclutamento militare - non solo quello obbligatorio, ma anche quello volontario, incentivato dalla propaganda[32] - svuota le aule universitarie. Anche molte giovani studentesse, chiamate a svolgere mansioni lavorative da sempre considerate appannaggio maschile, lasciano l'Università.

Questo stato di cose rende ragione del limitato pubblico di allievi che segue il corso di Analisi superiore del 1916-17: una quindicina di studenti, di cui quattro maschi: Salvatore Lupica, Ugo Cassina, Eugenio Poisetti ed Enrico Purgotti.[33] L'insegnamento di Fubini riscuote comunque successo e ben cinque studenti gli chiedono la tesi di laurea: Maria Mancinelli sul teorema di reciprocità per i corpi quadratici (1917), Maria Gandiglio sui corpi algebrici quadratici (1918), Cassina sul gruppo modulare di sostituzioni (1919), Maria Teresa Morra sui residui quadratici e il teorema di reciprocità e Poisetti sui gruppi abeliani di ordine finito (1921). Alcuni argomenti svolti da Fubini nella prima parte del corso forniranno poi lo spunto per due prove d'esame finali alla Scuola di Magistero: quelle di Annetta Segre (26 febbraio 1919, *Una lezione per la quarta classe ginnasiale sulla divisibilità dei numeri interi*) e di Luisa Ghigi (15 luglio 1919, *Una lezione per la terza classe della Scuola Normale sul metodo della riduzione all'unità nella regola del 3*).

Come la maggior parte dei corsi di livello superiore offerti negli atenei italiani, quelli di Fubini hanno taglio monografico. La scelta del tema, che generalmente variava di anno in anno, spettava al docente.[34] Questi aveva piena autonomia nella selezione degli argomenti da affrontare, oltre che nell'approccio metodologico e didattico con cui svilupparli. La costruzione di un corso quale quello di Analisi superiore comporta quindi uno sforzo creativo e non si riduce a una mera attività di tipo compilativo. Per questo ha senso e significato analizzare la struttura delle *Lezioni di Teoria dei numeri* di Fubini, vagliandone le radici culturali. Come ricorda Belhoste, i corsi magistrali costituiscono, del resto, un tipo di attività matematica che implica

> le travail de recherche. (…) le travail créatif consiste ici à mettre en ordre, à clarifier, à simplifier. Ce travail peut aboutir par fois à l'invention de nouveaux concepts, de nouvelles méthodes, de nouvelles théories, mais surtout il contribue puissamment à organiser le savoir mathématique en imposant des choix: quelles sont jugés essentiels, ceux qui sont accessoires, ceux qu'il suffit de renvoyer en exercices d'application? Ces choix impliquent en effet non seulement une opinion sur la valeur didactique de tel ou tel mode d'exposition mais aussi une vision de la nature et de la

[31] Nell'ampia bibliografia inerente l'università di Torino durante la Prima guerra mondiale basti citare la piattaforma *L'Università di Torino nella Grande Guerra* (https://www.grandeguerra.unito.it/).

[32] La propaganda fa presa anche nel mondo femminile. Quattro studentesse di Fubini (Adelaide Carozzi, Annetta Segre, Ester De Benedetti e Angiolina Piva) lavorano per esempio nel *Laboratorio Universitario per i combattenti*, realizzando indumenti in lana destinati ai soldati al fronte e ai profughi di guerra ospitati nei locali universitari.

[33] Cfr. ASUT: Carriere scolastiche, vol. 33, 34, 35, 37; Registro degli esami speciali di Analisi superiore 1916-20. Il numero di studenti di questo corso, sensibilmente diminuito rispetto all'anno accademico precedente, raddoppierà di nuovo al termine della Grande Guerra.

[34] Una sinossi dei corsi di carattere avanzato tenuti nelle università italiane è pubblicata annualmente in BAMS, XXIII, n. 1, *Notes,* p. 50. Relativamente all'a.a. 1916/1917 si legge: "University of Turin. By Professor T. Boggio: Potential; selected topics of analytical mechanics, three hours.— By Professor G. Fubini: Cantor's numbers; entire and algebraic entire numbers; theory of numbers and forms with algebraic applications; applications of analysis to the theory of numbers, three hours.—By Professor C. Segre: Higher views concerning elementary geometry, three hours.—By Professor C. Somigliana: Electromagnetism with special regard to propagation phenomena, three hours."

> structure du savoir mathématique. De manière générale, le cours magistral ouvre ainsi souvent la voie à la rédaction du traité de mathématiques.[35]

All'atto di iniziare il suo corso Fubini ha già acquisito una propria visione epistemologica di questa disciplina, sostanzialmente sintetizzabile in tre punti. In primo luogo egli concepisce la teoria dei numeri come un campo con *"scarse o nulle applicazioni pratiche"*.[36] Ciò non deve rappresentare, tuttavia, un impedimento alla sua inclusione nell'offerta formativa universitaria, almeno fin tanto che la matematica sarà studiata *"indipendentemente dalle applicazioni, per il solo orgoglio dello spirito umano"*.[37]

In seconda istanza la teoria dei numeri, caratterizzata da proprietà in apparenza semplici ma spesso molto difficili da dedurre, dimostra secondo Fubini che *"la matematica ha portato la semplicità dove era la complicazione*, *(...) la complicazione dove era la semplicità, una semplicità, a dir il vero, soltanto apparente"*.[38] Sotto questo profilo, essa partecipa a quella sorta di continua evoluzione che rende la matematica un *"grande paesaggio, in cui il ricercatore innalza edifici, costruisce e varia le strade che conducono l'uno all'altro: è un paesaggio strano, in cui si va talvolta nei posti più impensati*".[39] In questi percorsi minime discordanze possono portare a scoperte grandiose, le ipotesi da cui si era partiti possono essere modificate, persino stravolte. In teoria dei numeri, allora, come in ogni altra branca della matematica i vecchi edifici non "cadono" mai, ma essi vanno in disuso, perché sorgono nuove costruzioni richieste dal variare dei problemi da risolvere, dal mutare e dal perfezionarsi dei metodi di ricerca. E, talvolta, nei vecchi edifici abbandonati, ma non crollati, si trova un oggetto che inspira nuove idee, che indica nuove strade, che dà al vecchio palazzo vita nuova e feconda.[40]

In aula Fubini sceglierà perciò di partire da alcuni temi di algebra elementare classica ma al contempo, tessendo una trama di collegamenti e giocando abilmente su analogie e parallelismi, riuscirà a presentare ai suoi studenti una serie di risultati di carattere avanzato e affronterà alcuni fra i temi più promettenti del dibattito coevo a livello internazionale. La linearità ed essenzialità della sua esposizione, il fatto di non disperdersi nelle *"cosette graziose"*[41] ma di puntare a illustrare i tratti generali di quel grandioso 'paesaggio' che è la teoria dei numeri, renderanno suggestivo ed incisivo il suo insegnamento. La consapevolezza di non poter ignorare la fragile preparazione della scolaresca in materia di algebra astratta lo condurrà a limitare il più possibile le digressioni puramente analitiche e a puntare alla massima "leggerezza" della notazione.

Infine, in accordo con la visione di Felix Klein e Federigo Enriques, la teoria dei numeri è per Fubini una scienza squisitamente sperimentale, nella misura in cui, sorretta e guidata dall'intuizione, essa ha a che fare con congetture e problemi aperti, nella risoluzione dei quali procede per prove ed errori. Come un artista, il teorico dei numeri compie allora atti di audace intuizione, senza i quali molteplici metodi e fatti gli resterebbero ignoti.[42] Al rigore - argomenta Fubini - spetta una seconda parte del lavoro: *"chiarire i limiti di validità della scoperta, porre in luce i legami che intercedono tra essa e gli altri fatti già noti, bandire le eventuali oscurità, togliere ogni interpretazione troppo larga che possa indurre in errore, e condurre a risultati paradossali"*.[43]

---

[35] Belhoste 1998, p. 299, 300.
[36] Fubini 1935, p. 13. Fubini, molto probabilmente anche a causa della sua lunga esperienza di insegnamento presso il Politecnico di Torino, è fortemente coinvolto nei dibattiti sul rapporto tra matematica pura e applicata.
[37] Fubini 1930, p. 98.
[38] *Ibid.*, p. 103.
[39] Fubini 1935, p. 11.
[40] Cfr. Fubini 1929a, p. 46 e Fubini 1929b, p. XXXVII.
[41] Segre 1954, p. 282.
[42] Fubini 1936, p. 30, 31.
[43] Fubini 1930, p. 100, 101.

In un insegnamento superiore, il compito del docente non potrà dunque essere quello di passare dalla risoluzione di *"un problema a quella di un altro, che sembra completamente distinto"*, bensì quello di *"trovare impensati collegamenti tra fenomeni disparatissimi"*, per esempio fra teoria dei numeri, geometria e analisi, e trarne *"l'incitamento sia a nuove scoperte, sia a nuove teorie"*. Fubini deplora perciò la tendenza di chi dà troppo peso alla parte formale, algoritmica e deduttiva del proprio insegnamento, a discapito di quella induttiva, e di chi tace agli allievi i *"procedimenti euristici, che hanno creato la scienza"*.[44]

Pur avendo inesausta fiducia nei metodi e negli strumenti della matematica, Fubini è infine ben consapevole dei limiti e delle difficoltà che i matematici incontrano nel far ricerca, tant'è che *gran parte di loro si accontenta di aver creato e di perfezionare con studio assiduo e con diligenza perenni una macchina meravigliosa per mezzo della quale con grande economia di pensiero l'uomo può dedurre, può saggiare sulle conseguenze più remote la bontà delle premesse, talvolta trovando perfino le correzioni che a queste deve apportare. Peccato purtroppo che questa macchina non sia automatica, anzi sia talvolta assai faticosa, peccato che non sia così perfetta da saper sempre risolvere i problemi affrontati!*

Alla luce di questi assunti, ben si comprende che l'architettura espositiva del corso di Teoria dei numeri di Fubini sia tutto fuorché casuale. Essa scaturisce da un impegnativo lavoro di sintesi della letteratura avanzata in questo ramo di studi, un lavoro reso assai difficile dalla povertà del contesto culturale italiano. A differenza di un Corrado Segre, che poteva aprire le sue lezioni di Geometria superiore con una bibliografia di 24 trattati e articoli di 16 autori e in 4 lingue differenti[45], Fubini ha a disposizione un patrimonio di fonti limitato, tanto più che, *"i giovani delle nostre Università hanno scarsa famigliarità con la lingua* [il tedesco]*, nella quale è scritta la maggior parte dei lavori"*.[46]

Sul fronte italiano, i trattati di teoria dei numeri si contano sulle dita di una mano: le litografie dei corsi di Bianchi[47] sui gruppi di sostituzioni e le equazioni algebriche secondo Galois (1897), sui gruppi continui finiti di trasformazioni (1903) e sulla teoria aritmetica delle forme quadratiche binarie e ternarie (1911); gli *Elementi della teoria dei numeri* di Gazzaniga; le traduzioni dei due capolavori Dirichlet-Dedekind e di Chebyshev. Le riprese testuali, con la citazione fedele di interi passi di questi volumi sono assai consistenti, ad esempio nel caso dell'interpretazione geometrica delle frazioni continue e della teoria degli ideali.

Anche se la struttura dei loro corsi è molto differente, la trattazione che Fubini dà delle forme binarie, delle rappresentazioni proprie di un numero per una forma, delle forme ridotte[48] e della loro equivalenza è ad esempio quella di Bianchi.[49] Idem dicasi delle sue lezioni sul gruppo modulare, sui periodi di Gauss e sull'introduzione all'aritmetica analitica.[50]

All'atto di delineare un progetto di ampio respiro, che unifichi la teoria dei numeri e la geometria algebrica, Fubini mostra invece di seguire da vicino le *Vorlesungen über Zahlentheorie* di Dirichlet nella traduzione di Faifofer. Da questo *point de répère*, che restituisce con fedeltà "la perfetta esposizione orale di Dirichlet",[51] e in particolare dal celebre

[44] *Ibidem*, p. 104, 106.
[45] Cfr. Coolidge 1904, p. 13.
[46] Gazzaniga 1903, p. III.
[47] Queste lezioni litografate, nelle quali Bianchi aveva fatto tesoro della sua esperienza a Göttingen (1879-1881), erano fra l'altro state acquistate dalla BSM a pochissima distanza dalla pubblicazione. Cfr. Archivio BSM: Consorzio Universitario Piemontese. Prospetto delle variazioni in aumento o diminuzione degli oggetti esistenti nella Scuola di Magistero, dal 1903 al 1919; Fondo Universitario, dal 1907 al 1910 e ASUT, Recap. SC Biblioteca matematica.
[48] Bianchi introduce però il concetto di reticolo di punti in modo leggermente differente da Fubini, ossia come *"sistema dei nodi di una rete parallelogrammica"* associata ad una forma binaria definita, e accenna al concetto di 'reticoli nello spazio.
[49] Cfr. Fubini 1917, p. 161-179 e Bianchi 1911-12, p. 2-47, 125-191.
[50] Cfr. Fubini 1917, p. 305-321, 365-384 e Bianchi 1911-12, p. 229-278, 318-330.
[51] Dirichlet 1881 (trad. it.), p. VI.

supplemento di Dedekind, Fubini trae l'esposizione delle forme binarie quadratiche e della teoria degli ideali. Oltre ad adottare il medesimo impianto contenutistico delle *Vorlesungen*, in alcuni capitoli delle *Lezioni* del 1916-17 egli ne riporta anche integralmente parecchie dimostrazioni, come quelle del teorema di Wilson e della legge di reciprocità.

Per la trattazione sistematica delle congruenze, oltre che ai classici (Gauss, Legendre, Euler) Fubini si rifà invece alla versione italiana del testo di Chebyshev,[52] da cui desume fra l'altro l'applicazione delle congruenze alla risoluzione dei problemi di analisi indeterminata e il largo impiego del simbolo di Legendre-Jacobi.[53]

Un discorso a parte meritano i tedeschi. Da questo punto di vista Fubini è per certi versi avvantaggiato da due circostanze: il fatto che esistesse da fine Ottocento una rete di contatti epistolari e di scambi scientifici fra Torino e la Germania e il fatto che Segre e Fano, i quali si erano recati a Göttingen per due soggiorni di studio nel 1891 e nel 1893 rispettivamente, avessero portato in Italia e donato alla BSM numerosi testi di lezioni litografate di F. Klein, A. Hurwitz, H. Weber, E. Landau e altri ancora. Così ad esempio, Fubini ha l'opportunità di essere fra i primi lettori della *Geometrie der Zahlen* e della *Diophantische Approximationen* di H. Minkowski[54], dalle quali trae ispirazione per i capitoli III, IV e V delle *Lezioni di Teoria dei numeri*, laddove collega la teoria geometrica dei numeri all'analisi funzionale e all'approssimazione diofantea.[55] Analogamente recepisce e apprezza le *Vorlesungen über Zahlentheorie* (1907) di J. Sommer,[56] una copia delle quali è da lui donata alla BSM nello stesso anno della loro pubblicazione. È a queste *Vorlesungen* che Fubini rimanda gli studenti del suo corso per una prima introduzione alla teoria dei numeri algebrici, così come erano stati sviluppati da Kummer, Dedekind e Hilbert. Il fatto che assegnare un corpo algebrico equivalga a dare un'equazione algebrica $g(z) = 0$ a coefficienti interi rileva invece l'orma lasciata su di lui dal saggio di L. Kronecker *Über bilineare Formen mit vier Variabeln* (1883) e dallo *Zahlbericht* di D. Hilbert (1897).[57] Fubini si affida inoltre a P. Bachmann per affrontare la teoria dei polinomi ciclotomici (Bachmann 1872, 1892) e a H. Weber per il tema dell'estensione della teoria degli ideali alle funzioni algebriche di una variabile (Weber 1895, 1898). Infine le pubblicazioni di E. Landau[58] all'interno dei *Rendiconti del Circolo Matematico di Palermo* hanno certamente esercitato un certo fascino su Fubini, fornendogli un valido supporto per la 'costruzione' del VII capitolo delle sue *Lezioni*.

Oltre al patrimonio librario, la BSM possedeva un'immensa miscellanea, purtroppo andata quasi completamente distrutta nei bombardamenti della seconda guerra mondiale. Gli oltre sessantamila estratti di cui era composta, molti dei quali donati da Segre, Peano, Fano, Fubini, Somigliana e altri ancora, erano messi a disposizione degli studenti, nella sala di lettura della

[52] Chebyshev 1895 (trad. it.), p. III.

[53] Curiosamente, Fubini non mostra invece di cogliere l'originalità della parte dell'opera di Chebyshev concernente le proprietà delle funzioni che determinano quanti sono i numeri primi minori di un numero dato. Cfr. Viola 2019.

[54] Pubblicata nel 1896, la *Geometrie der Zahlen* è posseduta dalla BSM a partire dal 1898; la *Diophantische Approximationen* è invece acquistata dalla BSM nell'anno stesso della pubblicazione, il 1907. Le opere di Minkowski avevano del resto avuto risonanza internazionale, ed erano state positivamente recensite sul Bullettin dell'American Mathematical Society (cfr. Dickson 1909, p. 252 e Dickson 1914, p. 131, 132).

[55] Cfr. p. 81-134 in questo volume. Minkowski (e, sulla sua scia, Fubini) dimostra geometricamente l'esistenza di una base di ogni ideale nei campi di numeri interi algebrici. L'introduzione dei reticoli non solo assicura un'impostazione geometrica altamente funzionale per la teoria algebrica ma permette anche di stabilire alcuni teoremi fondamentali sui numeri algebrici che non si potrebbero altrimenti dimostrare.

[56] Sui pregi didattici dell'opera di Sommer si veda Skinner 1914, p. 202.

[57] La BSM possiede l'opuscolo di Kronecker sin dal 1891, mentre il volume di Hilbert, nell'edizione francese di Lévy (*Théorie des corps de nombres algébriques* 1910), è acquistato nel 1912.

[58] Tra il 1907 e il 1914 E. Landau pubblica nei *Rendiconti* ben 11 lavori, di cui 3 sulla serie di Dirichlet (1907, 1909, 1914), oltre al famoso *Beiträge* del 1908. L'interesse dei *Rendiconti* – cui Fubini era automaticamente abbonato in qualità di membro del Circolo – nei confronti della teoria dei numeri era verosimilmente dovuto proprio alla presenza assai attiva di Landau all'interno dell'*editorial board.*

biblioteca. Sul versante della teoria dei numeri il patrimonio documentario comprendeva opuscoli ricevuti da tutto il mondo: America[59] (L.E. Dickson, G.A. Miller, H.F. Blichfeldt, R.D. Carmichael e H.S. Vandiver), Russia (V.P. Velimin, A.P. Zilinskij, V.I. Romanovsky e J.V. Uspensky), Francia (H. Laurent e Châtelet), impero britannico (G.H. Hardy, L.G. Mordell, A. Cunningham e S. Ramanujan) e Giappone (M. Fujiwara e T. Suzuki).

2. Fubini (al centro) con Tonelli, Severi, Fano, Levi-Civita e consorti nel 1925

4. *Temi e contenuti delle Lezioni di Teoria dei numeri*

L'architettura delle *Lezioni di Teoria dei numeri* è decisamente complessa. Essa è il frutto di ampie letture e di un'impegnativa opera di mediazione epistemico-cognitiva posta in essere da Fubini via via che sviluppava il suo insegnamento. L'interesse intrinseco dell'impianto strutturale del corso e delle soluzioni metodologiche adottate da Fubini nella concatenazione dei singoli capitoli, nell'ordine espositivo e nella scelta delle varie dimostrazioni e notazioni giustifica la minuziosa disamina dei temi e dei contenuti delle dispense del 1916-17.

4.1. *Concetti preliminari*

Conscio della lacunosa preparazione dei suoi studenti in materia di algebra, Fubini dedica le prime lezioni del corso ad argomenti propedeutici, di carattere elementare ma funzionali alla comprensione dei successivi sviluppi teorici avanzati.

L'esordio è rappresentato da alcuni temi classici: divisibilità, numeri associati e algoritmo euclideo per determinare il massimo comun divisore tra due numeri interi (*Elementi*, Lib. VII, prop. 2), sufficienti però ad affrontare la risolubilità in numeri interi dell'equazione diofantea $ax + by = 1$ con a, b primi tra loro, a dimostrare il teorema, su cui si basa *"tutta la teoria dei numeri primi"*[60], secondo il quale se a, b, l sono numeri interi, a, b sono primi tra loro e al è divisibile per b, allora l è divisibile per b, asserto che permette di provare l'unicità della decomposizione degli interi in fattori primi, a meno di fattori associati.

Generalizzando le proprietà di $\mathbb{Z}$ e dei polinomi a coefficienti in $\mathbb{C}, \mathbb{R}$ e $\mathbb{Q}$, Fubini introduce i campi oloidi, ossia strutture algebriche chiuse rispetto alle operazioni di somma, differenza e prodotto, con una definizione che corrisponde abbastanza bene a quella attuale di anello algebrico. La decomposizione dei polinomi a coefficienti in $\mathbb{Q}$ in fattori primi fa emergere il problema dei cosiddetti polinomi irriducibili – ossia polinomi che non si possono scrivere sotto forma di prodotto $P_1(x)P_2(x)$ di due polinomi non costanti a coefficienti razionali – e prelude

[59] Per approfondimenti sui contributi dei matematici americani cfr. Fenster 2007.
[60] Fubini 1917, cap. I, §1, p. 6.

alla loro caratterizzazione. Tra numeri interi e polinomi a coefficienti interi sussiste un significativo parallelismo: i polinomi irriducibili corrispondono infatti, in quest'ottica, ai numeri primi. Definiti i polinomi primitivi – ossia aventi coefficienti interi primi tra loro – si può enunciare e dimostrare il lemma di Gauss, dal quale a sua volta discendono due corollari, anch'essi rigorosamente dimostrati da Fubini con metodi elementari.[61]

La teoria degli ideali è reputata da Fubini di fondamentale rilievo per il prosieguo del suo corso. Definito allora il modulo come *"un insieme M di enti tali che la somma o la differenza di due enti in M, distinti o no, è ancora un ente in M"*[62], sulla scorta di quanto fatto da Dedekind nei supplementi delle *Vorlesungen*, dimostra che M è un modulo di interi se e solo se è formato da tutti i multipli di un intero K. Il modulo M generato da K, minimo comune multiplo dei numeri interi $a_1, a_2, \dots, a_n$, è indicato con la notazione $[a_1, a_2, \dots, a_n]$, ripresa probabilmente da Bianchi. Ai concetti di ideale (ovvero un modulo M, contenuto in un campo oloide K, tale che il prodotto di un ente di K e di un ente di M sia ancora un ente di M), ideale prodotto, divisibilità tra ideali, inclusione tra ideali e base di un ideale Fubini dedica ampio spazio, a livello sia teorico che applicativo, proponendo anche alcuni esercizi.

Il primo esempio di aritmetica analitica sviluppato in aula da Fubini è la dimostrazione del teorema di infinità dei numeri primi, ottenuta utilizzando la divergenza della serie di Dirichlet $\sum_n \frac{1}{n^s}$ per $s = 1$.[63] La dimostrazione, che si deve a Euler, è ripresa dalle *Vorlesungen* di Dirichlet e dagli studi di Bianchi del 1911-12 ed è scelta da Fubini in quanto emblematica di un tipo approccio che coniuga tre discipline (algebra, aritmetica e analisi) e che, a differenza dei precedenti e più antichi procedimenti argomentativi, si presta a molteplici generalizzazioni. Ponendosi in controtendenza rispetto alla tradizione didattica coeva, che generalmente preferiva la dimostrazione euclidea classica (*Elementi*, Lib. IX, prop. 20), basata su un procedimento ricorsivo, Fubini adotta infatti un approccio ancorato al concetto di serie infinita e al passaggio al limite, ovvero – in termini aristotelici – ricorre a un infinito di tipo attuale.

Lo studio della funzione $\varphi(m)$, che rappresenta il numero degli interi positivi $n \leq m$ primi con m conclude questa sorta di 'introduzione' alla teoria dei numeri. Fubini osserva qui che la somma dei valori di φ relativi ai vari divisori δ di m (inclusi i divisori $1, m$) vale m; dimostra che se m è un intero e se $p_1, p_2, \dots, p_r$ sono i fattori primi distinti, allora

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

ed enuncia due ulteriori proposizioni su tale funzione, lasciando agli studenti la dimostrazione della seconda.[64]

All'aritmetica degli interi $(mod\ m)$, che è equivalente a quella dei campi pseudo-oloidi[65], è dedicato un secondo gruppo di lezioni.

I contenuti sono ancora, in larga parte, quelli tipici dei trattati di teoria dei numeri elementare contemporanei (Gazzaniga 1903; Bianchi 1911-12): proprietà algebriche delle congruenze,[66] piccolo teorema di Fermat,[67] equivalenza tra i due problemi fondamentali della teoria dei numeri, ovvero la risoluzione della congruenza di primo grado in un'incognita $ax \equiv b\ (mod\ c)$

[61] *Ibidem*, cap. I, §2, p. 11.
[62] *Ibidem*, cap. I, §3, p. 14.
[63] *Ibidem*, cap. I, §4, p. 19-21.
[64] *Ibidem*, cap. I, §5, p. 24.
[65] Si tratta delle strutture dette oggi anelli a caratteristica positiva, ossia quei campi dove tra i numeri $1, 1+1, 1+1+1$, ecc. ve n'è uno non distinto da (ossia congruo a) zero: precisamente il numero $1+1+\dots+1$, quando gli addendi siano m. In tal modo *"i numeri interi in tale campo pseudo-oloide possono pensarsi come le anomalie dei vertici di un poligono regolare di m lati, quando un vertice abbia per anomalia zero, e si assuma come unità di misura degli angoli (anomalia) la m^{esima} parte di 4 retti"* (*Ibidem*, cap. II, §1, p. 27) .
[66] *Ibidem*, cap. II, §1, p. 29.
[67] La dimostrazione per particolari valori di n, p è lasciata agli studenti.

e quella dell'equazione diofantea di primo grado a due incognite $ax + cy = b$.[68] Ad essi è fatta seguire la costruzione delle soluzioni di questo particolare problema di analisi indeterminata di primo grado e lo studio del numero di soluzioni distinte della congruenza $ax \equiv b\ (mod\ c)$.[69] A questo proposito appare interessante che Fubini sottolinei il parallelismo tra l'aritmetica delle congruenze e la prova del 9 e dell'11 in una moltiplicazione, rivolgendosi a un pubblico di studenti per lo più indirizzati all'insegnamento secondario e che, in contemporanea al suo corso, seguiva quello di Magistero tenuto da C. Segre.

Sulla scia di Gazzaniga, ai sistemi di congruenze di primo grado $(mod\ K)$, principalmente nel caso in cui K sia un intero primo, vengono estesi molti dei metodi utilizzati nella risoluzione dei sistemi di equazioni lineari, prima di affrontare lo studio del sistema di n congruenze in una sola incognita $a_i x \equiv c_i\ (mod\ b_i), i = 1, \dots, n$, in cui il modulo b_i può invece variare da una congruenza all'altra. Dimostrato il cosiddetto 'teorema cinese dei resti', si osserva che, aumentando il numero delle incognite, un qualunque sistema di congruenze lineari si può trasformare in un problema di analisi indeterminata. Meno approfondito è invece il tema della risoluzione delle congruenze di grado qualunque.

Partendo dalla constatazione che nella teoria delle congruenze non esiste l'analogo del 'teorema fondamentale di Gauss' per le equazioni algebriche, né è generalmente vero che se il prodotto $ab \equiv 0\ (mod\ c)$ almeno uno dei fattori a, b è congruo a zero (teorema invece valido se il modulo c è un numero primo), Fubini giunge infine a dimostrare che una congruenza $p(x) \equiv 0$ di grado n rispetto ad un modulo primo c ha al massimo n radici incongrue. Segue il cosiddetto teorema di Wilson, dimostrato con il ragionamento standard, che fa appello al piccolo teorema di Fermat.[70]

L'impronta lasciata su Fubini dal magistero di Bianchi si rileva nel paragrafo dedicato alle radici primitive e agli indici. Dagli scritti del suo 'maestro' Fubini trae in particolare il fatto che ad un divisore δ di $p - 1$, con p primo, "appartengono" esattamente $\varphi(\delta)$ numeri. Il termine "appartenenza", per indicare il fatto che ci sono $\varphi(\delta)$ elementi $(mod\ p - 1)$ di periodo δ, già presente in Dirichlet, è attualmente caduto in disuso. Definite le radici primitive di p come i $\varphi(p - 1)$ interi che appartengono all'esponente $p - 1$, Fubini introduce poi la nozione di indice[71] e, nella linea delle *Disquisitiones Arithmeticae*, illustra l'analogia tra questa e il logaritmo.[72]

La conclusione delle lezioni sulle congruenze è affidata al tema della risoluzione delle congruenze binomie, ossia quelle del tipo $x^n \equiv D\ (mod\ p)$, ottenuta con un procedimento che viene paragonato all'operazione di estrazione di radice. Nel caso $n = 2$ è introdotto il simbolo di Jacobi-Legendre e viene enunciato per la prima volta il teorema di reciprocità quadratica, ampiamente discusso nel seguito del corso.[73]

Indicative del talento didattico di Fubini sono infine le *Applicazioni ed esercizi* posti in calce alle lezioni teoriche. Agli studenti è chiesto, fra l'altro, di trovare i numeri primi con D di cui D è un residuo, riconducendo il problema alla ricerca dei primi p divisori di $x^2 - Dy^2$ con x, y primi tra loro. Questo equivale a cercare i numeri dispari n per cui il simbolo di Legendre

[68] Fubini dimostra che condizione necessaria e sufficiente per la loro risolubilità in numeri interi è che b sia divisibile per il $M.C.D.(a, c) = d$.

[69] Se è risolubile, essa possiede esattamente d radici incongrue $(mod\ c)$.

[70] Cfr. Bottari 1912; Cibrario 1929.

[71] Se γ è una radice primitiva di p, gli interi $\gamma, \gamma^2, \gamma^3, \dots, \gamma^{p-2}, \gamma^{p-1} \equiv 1$ sono un sistema di numeri incongrui $(mod\ p)$; ogni numero $r \not\equiv 0$ è congruo ad uno ed uno solo di essi. Se, ad esempio, $r \equiv \gamma^s$ s è detto indice di r.

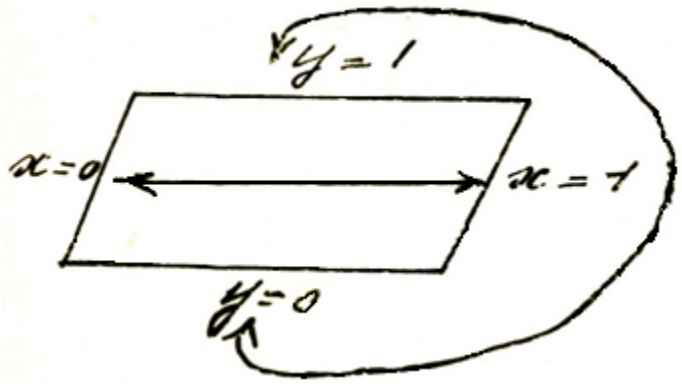
[72] Gauss 1801, sez. III, art. 57, 58, p. 47.

[73] Un caso particolare del teorema di reciprocità, ossia la relazione $\left(-\frac{1}{n}\right) = (-1)^{\frac{n-1}{2}}$ valida per ogni n dispari, è dimostrato nella sezione di *Applicazioni ed esercizi.*

$\left(\frac{D}{n}\right)$ è uguale a $+1$, questione affrontata da Fubini a lezione distinguendo i due casi $D \equiv 1\ (mod\ 4)$ e $D \equiv 3\ (mod\ 4)$.

4.2. *Geometria dei numeri*

Nei tre capitoli successivi delle lezioni del 1916-17 Fubini sviluppa alcuni collegamenti tra la teoria dei numeri e la geometria, collegamenti cui egli dà particolare rilievo, forse perché in contemporanea si sta preparando alla redazione dei suoi celebri testi di geometria differenziale (1918, 1919, 1920, 1922).



3. Parallelogramma fondamentale di una rete di punti

Il concetto di rete di punti[74] in $\mathbb{R}^2$, ossia il luogo di punti a coordinate intere in un sistema di riferimento cartesiano, definito come *"il piano della teoria dei numeri"* e che *"si presta bene allo studio dell'analisi indeterminata in due incognite"*[75], serve per introdurre quello di rete di parallelogrammi. Queste reti di punti, nel linguaggio moderno, sono dette reticoli (in inglese *lattices*) e, poiché *"in una regione finita del piano xy esiste un numero finito di punti della rete"*[76], esse costituiscono un sottogruppo discreto di $\mathbb{R}^n$.

Al fine di dimostrare per via puramente geometrica i risultati di analisi indeterminata di primo grado ottenuti precedentemente, Fubini si serve qui della nozione di gruppo[77], seguendo la linea tracciata da Klein nel programma di Erlangen e ancora prima da Lie[78]: i gruppi vengono infatti introdotti non come struttura algebrica astratta, ma piuttosto operativamente come gruppi di trasformazioni del piano, attraverso quella che attualmente prende il nome di *azione di un gruppo* su un insieme. Fubini, sulla scia di Minkowski, affronta poi alcune questioni di carattere geometrico strettamente connesse all'analisi indeterminata, quali i cosiddetti campi fondamentali, la ricerca di parallelogrammi ed esagoni limite, le disuguaglianze del tipo $(\alpha x + \beta y)^p + (\gamma x + \delta y)^p \leq 1$ ed i sistemi di due reti contenute l'una nell'altra. Al teorema fondamentale di Minkowski sui punti reticolari negli insiemi convessi è riservato ampio

---

[74] Fubini 1917, cap. III, §1, p. 66; la rete di punti è caratterizzata mediante le tre seguenti proprietà:
1. In una regione finita del piano xy esiste un numero finito di punti della rete (proprietà di discretezza).
2. Se A, B, C sono tre punti della rete, il punto D dedotto da C con la traslazione AB (tale cioè che AD sia la somma geometrica di AB, AC) appartiene ancora alla rete (proprietà di sottogruppo).
3. I punti della rete non sono in linea retta.

[75] *Ibidem*, cap. III, §1, p. 65.

[76] *Ibidem*, cap. III, §1, p. 66.

[77] *Ibidem*, cap. III, §2, pp. 75, 76: "Un gruppo G è una classe G di operazioni T che gode delle seguenti due proprietà:
i) Se G contiene un'operazione T, contiene anche l'inversa T^{-1}.
ii) Se G contiene due operazioni T, U, contiene anche il loro prodotto TU."

[78] Su questo approccio al concetto di gruppo cfr. Wussing 1969.

rilievo[79]. In ottica moderna, Fubini sostanzialmente cerca degli elementi della rete di punti che hanno, in un certo senso, 'norma piccola', ossia si propone di trovare gli elementi del reticolo per i quali una certa forma quadratica assume valore minimo. Questo problema si riduce a studiare i punti a coordinate intere contenuti all'interno di particolari figure, e ciò è strettamente collegato allo studio della riduzione delle forme quadratiche a coefficienti interi che verrà affrontato nelle successive lezioni.

Gli strumenti concettuali appena forniti portano alla dimostrazione del teorema fondamentale dell'analisi diofantea di primo grado. Fubini afferma infatti che condizione necessaria e sufficiente affinché il segmento OA che congiunge l'origine O al punto $A\ (x_1, y_1)$ della rete non contenga altri punti della rete, è che x_1, y_1 siano primi tra loro[80]. Solo in questo caso esisterà un altro punto $B\ (x, y)$ della rete tale che OA, OB siano lati di un parallelogramma fondamentale, cioè tale che $x_1 y - y_1 x = \pm 1$. Pertanto l'equazione nelle incognite intere x, y è risolubile solo se x_1, y_1 sono primi tra loro. Con le frazioni continue, Fubini dimostra poi alcuni risultati classici[81] riguardanti i convergenti (che egli chiama 'ridotte') dello sviluppo in frazione continua di un numero reale w. In particolare, dopo aver osservato che le ridotte sono alternativamente minori e maggiori di w, prova che esse forniscono le migliori approssimazioni del loro limite w in un senso ben preciso:

> […] perciò una ridotta $\frac{x_i}{y_i}$ è la frazione che meno dista da w di tutte le frazioni, i cui termini rispettivamente non superano $\frac{x_i}{y_i}$. [82]

Di fatto vale un risultato più forte, ovvero che la ridotta *i*-esima è la frazione che meno dista da w tra tutte le frazioni il cui denominatore non supera y_i .

L'interpretazione geometrica delle frazioni continue[83] è desunta testualmente delle lezioni di teoria dei numeri di Klein del 1896,[84] e prelude a una generalizzazione dei teoremi di Minkowski e alla riduzione delle forme quadratiche binarie definite.

I principali concetti e risultati della geometria dei numeri qui introdotti avranno la loro più importante applicazione più avanti, quando verranno utilizzati per dimostrare alcuni importanti teoremi sulla struttura degli interi in un campo di numeri, in particolare la finitezza del gruppo delle classi di ideali di un campo di numeri e il teorema di Dirichlet sulla struttura del gruppo delle unità. Nell'ottica moderna, questo risultato permette di "vedere" l'anello degli interi, gli ideali e il gruppo moltiplicativo delle unità come reticoli in uno spazio euclideo. Come si è detto in precedenza, un reticolo (o 'rete', secondo la terminologia di Fubini) è un sottogruppo discreto di $\mathbb{R}^n$. È possibile dimostrare che un reticolo in $\mathbb{R}^n$ è sempre liberamente generato, come gruppo abeliano, da una quantità $k \leq n$ di vettori linearmente indipendenti. Se si suppone $k = n$ (cosa sempre possibile, restringendo lo spazio euclideo ambiente), un reticolo si può rappresentare effettivamente come una rete nello spazio euclideo. Una base di un reticolo individua un parallelepipedo fondamentale e si dimostra che il volume di tale parallelepipedo dipende solo dal reticolo e non dalla base scelta; questa quantità viene detta 'volume' del reticolo. Ovviamente un sottogruppo di un reticolo è anch'esso un reticolo; il teorema dei divisori elementari asserisce che, dato un tale sottogruppo, è sempre possibile trovare una base del reticolo contenente un sottoinsieme di vettori i cui multipli sono una base del sottogruppo. I teoremi di Minkowski assicurano l'esistenza di un punto del reticolo in ogni regione

[79] Fubini 1917, cap. III, §3, p. 81-89. La nozione di convessità è introdotta come caso particolare della non concavità. Cfr. *Ibidem*, cap. III, §3, p. 82.
[80] *Ibidem*, cap. IV, §1, p. 116.
[81] *Ibidem*, cap. IV, §2, p. 118, 119; ad esempio Fubini prova per induzione la relazione ricorsiva $\frac{y_i}{x_i} = \frac{q_i y_{i-1} + y_{i-2}}{q_i x_{i-1} + x_{i-2}}$ e dimostra la proprietà dell'alternanza di segno delle ridotte: $y_i x_{i-1} - y_{i-1} x_i = (-1)^i$.
[82] *Ibidem*, cap. IV, §3, p. 125.
[83] *Ibidem*, cap. IV, §3, p. 124.
[84] Cfr. Klein 1896, p. 26, 27.

misurabile di $\mathbb{R}^n$, soddisfacente opportune condizioni di regolarità (convessità e simmetria rispetto all'origine), il cui volume sia sufficientemente grande rispetto al volume del reticolo. Nelle sue *Lezioni* Fubini dimostra il principale teorema di Minkowski – e, nel §8 del cap. III, il teorema dei divisori elementari – nel caso $n = 2$. Lavorando in modo molto concreto su segmenti del piano, si riduce dapprima a dimostrare l'esistenza di punti del reticolo all'interno di parallelogrammi e esagoni di area 4 centrati nell'origine; quindi conclude il ragionamento studiando la posizione dei punti del reticolo sul perimetro di queste regioni.

I teoremi di Minkowski sono stati utilizzati in molteplici ambiti della matematica, dall'analisi funzionale (Minkowski dimostrò che corpi convessi simmetrici inducono norme in spazi vettoriali di dimensione finita) al campo dell'ottimizzazione discreta, in particolare nella programmazione intera (lineare e non). Per quanto riguarda la programmazione intera, subito dopo la dimostrazione del teorema Fubini stesso fornisce ai suoi studenti un esempio di applicazione, trattando le funzioni del piano del tipo

$$f(x,y) = |\alpha x + \beta y|^p + |\gamma x + \delta y|^p,$$

dove $\Delta = det\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \neq 0$, e p è un numero reale > 1. Indicando con M il minimo di $f(x,y)$ al variare di x, y negli interi non entrambi nulli, Fubini mostra, utilizzando appunto il teorema di Minkowski, che $M < K_p\sqrt{|\Delta|}$, dove K_p è l'area della regione di equazione $|x|^p + |y|^p \leq 1$. Procede poi a studiare, fissato p, il valore massimo del rapporto $\frac{M}{K_p}$ al variare dei coefficienti $\alpha, \beta, \gamma, \delta$. Di particolare rilevanza è il caso $p = 2$, in quanto è noto che ogni forma quadratica definita positiva ha un'equazione della forma $f(x,y) = 0$, per opportuni coefficienti reali $\alpha, \beta, \gamma, \delta$. Un altro notevole campo di applicazione dei teoremi di Minkowski è quello dell'approssimazione diofantea, che studia la qualità dell'approssimazione di numeri reali mediante razionali.

Nello studio dell'aritmetica dei campi di numeri l'applicazione più interessante di questi risultati consiste nelle dimostrazioni della finitezza del gruppo delle classi di ideali e del teorema delle unità di Dirichlet. Sulla scia di Minkowski, Fubini dimostra prima il teorema delle unità, che chiama il 'gran teorema di Dirichlet' (§7 del cap. VI) e successivamente prova la finitezza del gruppo delle classi (§8 del cap. VII). Queste dimostrazioni si basano sulla possibilità di immergere oggetti algebrici (ideali, gruppi di unità, …) in un opportuno spazio euclideo in modo tale da rivederli come reticoli in tale spazio: nel caso degli ideali, l'immersione è semplicemente il prodotto delle diverse immersioni del campo nei numeri reali o nei numeri complessi; nel caso delle unità si utilizza invece l'immersione logaritmica, che permette il passaggio dalla struttura moltiplicativa a quella additiva. Il volume di questi reticoli è esprimibile in termini di discriminante del campo e norma dell'ideale in questione.

La trattazione di Fubini è suggestiva nella misura in cui precorre, per certi versi, l'indirizzo di Chevalley (1936) e Tate[85] (1950) che hanno creato un linguaggio estremamente ricco ed elegante, quello degli *adèles*, per sviluppare la teoria algebrica dei numeri. Dato un campo di numeri, le possibili norme definibili sul campo, per un teorema di Ostrowski, sono o quelle archimedee, corrispondenti ai diversi modi di immergere il campo nei numeri complessi, o quelle non archimedee, corrispondenti alle classi di coniugio degli ideali primi dell'anello degli interi del campo. Ogni norma induce un completamento topologico che nel caso archimedeo coincide con il campo dei numeri reali o dei complessi, mentre nel caso non archimedeo è un'estensione finita di qualche campo *p*-adico $\mathbb{Q}_p$. Inoltre, il completamento degli interi del campo rispetto alle metriche non archimedee definisce una struttura intera in ogni completamento non archimedeo. Gli *adèles* del campo sono il prodotto di tutti i possibili suoi completamenti, ristretto a tali strutture intere: si richiede cioè che le componenti corrispondenti

[85] Cfr. Cassels, Fröhlich 1967.

alle norme non archimedee siano tutte intere salvo al più un numero finito. Gli elementi invertibili dell'anello degli *adèles* formano il gruppo topologico degli *idèles*. *Adèles* e *idèles* si rivelano strumenti molto utili per studiare l'aritmetica dei campi di numeri: da una parte essi hanno componenti distinte associate ai diversi ideali primi del campo, e questo permette di studiare ogni primo separatamente, determinando proprietà locali del campo ad ogni singolo ideale primo. Dall'altra, hanno buone proprietà topologiche: essendo gruppi topologici localmente compatti, è definita su entrambi una misura di Haar, unica a meno di moltiplicazione per uno scalare, che permette di parlare di integrali e di volumi di sottoinsiemi; inoltre le proprietà topologiche dell'immersione "diagonale" del campo negli *adèles* riflettono proprietà locali che mettono in luce le relazioni che intercorrono tra i vari primi. In particolare, i teoremi di finitezza del gruppo delle classi e il teorema delle unità si dimostrano essere equivalenti al fatto che il quoziente $A_K^{(1)}/K^*$ del gruppo degli *idelès* di norma 1 per il sottogruppo degli elementi non nulli del campo è compatto. Questo discende a sua volta da un teorema di Minkowski adelico, che considera K^* come reticolo negli *idèles* e dimostra l'esistenza di elementi globali in sottoinsiemi degli *idèles* di volume sufficientemente grande.

4.3. *'Completeremo aggiungendo nuovi enti, che chiameremo ideali': forme quadratiche e ideali*

Le forme quadratiche a coefficienti interi o razionali occupano uno spazio estremamente rilevante nel corso di Fubini. Dopo alcuni cenni sulle trasformazioni modulari egli esordisce con quelle che noi chiameremmo 'equivalenze di strutture' – o, meglio ancora, 'equivalenze di categorie' – tra le coniche, che risultano essere equivalenti quando le loro equazioni si possono ridurre ad una forma canonica prestabilita, e le forme quadratiche, per le quali essere equivalenti significa trovare una trasformazione modulare che porta l'una nell'altra. Questo studio è particolarmente interessante, se interpretato in chiave moderna: le forme quadratiche a coefficienti reali, infatti, rappresentano coniche che sono classificate a partire da certi invarianti (segnatura, determinante, ecc.) e, a meno di equivalenza, quelle reali non degeneri sono tre a seconda della segnatura (ellisse, parabola, iperbole). Le coniche complesse non degeneri sono tutte equivalenti tra loro, a riprova del fatto che più un campo è grande, maggiore sarà il numero di isomorfismi al suo interno. Se invece "guardiamo" le forme quadratiche sui razionali o sugli interi lo studio diventa più complicato: infatti si scopre che esistono infinite classi di isomorfismi classificabili sulla base del discriminante di tali forme e tale classificazione è notevolmente più ricca di quella sui reali. Il risultato più importante, in questo campo, è costituito dal teorema di Hasse-Minkowski[86] che lega la rappresentabilità di un numero razionale tramite una forma quadratica a coefficienti razionali alla possibilità di rappresentare tale numero localmente, ovvero in ciascuno dei completamenti del corpo $\mathbb{Q}$. Questo risultato risale al 1921, motivo per cui Fubini non poteva esserne a conoscenza, tuttavia egli riserva a queste tematiche un'attenzione significativa, emblematica del suo 'fiuto' nel cogliere le linee di ricerca più promettenti a livello internazionale. Nell'ambito dello studio delle trasformazioni che portano una forma in una forma equivalente, Fubini arriva ad illustrare il metodo risolutivo per l'equazione di Pell[87] del tipo $T^2 - \Delta U^2 = 1$, rimandando alle *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie* di Bianchi per ulteriori approfondimenti.

Con il sesto e il settimo capitolo si torna propriamente nell'alveo della teoria dei numeri, pur senza rinunciare a qualche digressione di carattere geometrico. Fubini introduce il corpo $\mathbb{Q}(i)$, ovvero i *"numeri razionali di Gauss"*[88], facendo notare ai suoi studenti che questi costituiscono

[86] Il teorema di Hasse-Minkowski, in notazione moderna, afferma: sia $f(\boldsymbol{X}) \in \mathbb{Q}[X_1, \dots, X_n]$ una forma quadratica, f rappresenta lo zero in $\mathbb{Q}$ se e solo se f rappresenta lo zero su $\mathbb{Q}_v$, per ogni posto v di $\mathbb{Q}$.
[87] Fubini 1917, cap. V, §8, p. 181-183.
[88] *Ibidem*, cap. VI, §1, p. 184.

un corpo di Galois[89]. Definisce quindi gli interi di Gauss e le nozioni di divisibilità, numeri associati, unità e divisione con resto. *"Si ha così* – afferma Fubini – *con lieve variante per ciò che riguarda il resto, una completa analogia con la divisione degli interi nell'aritmetica elementare"*[90]. Portando avanti il parallelismo, si giunge infatti a definire il M.C.D. tra due o più interi di Gauss che, in questo caso, *"non risulta però completamente determinato; ma la sua indeterminazione si riduce a questo, che lo si può cambiare con uno dei numeri associati"*[91].

Considerando i numeri del tipo $x + y\theta$, con θ radice di un'equazione di secondo grado qualsiasi, non si può estendere l'algoritmo di Euclide a tutti i casi, in quanto può venire a mancare l'unicità della fattorizzazione in primi.[92] Fubini afferma che questo non deve però stupire perché *"altrettanto avviene in altri casi"*[93].

Ad esempio, considerando gli interi razionali congrui ad $1\,(mod\,4)$, si ha che $441 = 21 \cdot 21 = 9 \cdot 49$ e i numeri $21, 9, 49$ non sono a due a due associati né, nelle nostre ipotesi, decomponibili. Ciò avviene *"perché gli interi* $\equiv 1\,(mod\,4)$ *non formano un campo oloide completo; se noi lo completassimo con l'aggiunta degli altri interi razionali, ogni difficoltà svanirebbe"*.[94]

Allo stesso modo, sarà incompleto il campo dei numeri del tipo $x + y\sqrt{-5}$, con x, y interi razionali. L'intento di Fubini diventa quindi quello di *"aggiungergli nuovi enti, così da renderlo completo,* […] *così da ristabilire in esso le ordinarie leggi della divisibilità"*[95].

Nelle *Lezioni* del 1916-17 sono allora forniti alcuni cenni alla geometria dei numeri nello spazio a tre dimensioni[96], fra cui i classici teoremi di Minkowski in dimensione 3[97]. Notiamo inoltre come, pur avendo introdotto il concetto di corpo di numeri all'interno della trattazione dei corpi algebrici, Fubini lascia indefinito che cosa sia esattamente un numero, pur dando per scontato che in generale una "classe di numeri" sia un soprainsieme dei razionali. Strutture quali i campi finiti non vengono considerate.

Dopo aver trattato in modo approfondito i numeri interi algebrici – che costituiscono una *"generalizzazione del concetto abituale di numero intero"*[98] – Fubini affronta il cosiddetto 'gran teorema di Dirichlet'[99], attualmente noto come il 'teorema delle unità di Dirichlet'. Questo risultato fornisce la struttura del gruppo degli elementi invertibili degli anelli di interi, detto gruppo delle unità. Tali unità, siano esse in numero finito o infinito, costituiscono il gruppo moltiplicativo dell'anello. Il teorema delle unità afferma che questo gruppo è sempre finitamente generato, cioè ha una "parte libera" infinita, isomorfa a tante copie di $\mathbb{Z}$, e una parte di torsione finita. Tutto il gruppo è dunque costituito dal prodotto di gruppi ciclici infiniti per un gruppo finito che è formato dalle radici dell'unità. Fubini infatti afferma che gli elementi invertibili si possono sempre scrivere in modo unico come prodotto di un numero finito di elementi di ordine infinito, moltiplicati per una radice dell'unità. Questi generatori dei gruppi

[89] In quanto esso contiene il coniugato di ciascun intero di Gauss in esso contenuto. Cfr. Fubini 1917, cap. VI, §1, p. 185: "Un intero $x + iy$ di Gauss soddisfa l'equazione di secondo grado in $z - 2xz + (x^2 + y^2) = 0$, il cui primo coefficiente è 1, gli altri due sono interi razionali. L'altra radice $x - iy$ si dirà il numero coniugato".
[90] *Ibidem*, cap. VI, §1, p. 186.
[91] *Ibidem*, cap. VI, §1, p. 187.
[92] L'unicità della fattorizzazione in fattori primi, purché non si considerino come distinti due prodotti tali che i fattori del primo siano ordinatamente associati a quelli del secondo, è enunciata ma non dimostrata da Fubini.
[93] *Ibidem*, cap. VI, §1, p. 195.
[94] *Ibidem.*
[95] *Ibidem*, cap. VI, §2, p. 196.
[96] *Ibidem*, cap. VI, §3, p. 197; in particolare sono introdotti i concetti di parallelepipedo fondamentale (generalizzazione del parallelogramma fondamentale), trasformazioni modulari nello spazio e rete.
[97] La trattazione viene sviluppata senza dimostrazioni, per le quali lo studente viene rinviato alle lezioni di Minkowski.
[98] Fubini 1917, cap. VI, §5, p. 209.
[99] *Ibidem*, cap. VI, §7, p. 228.

ciclici infiniti sono detti, in linguaggio moderno, 'unità fondamentali'. I casi in cui la situazione può essere studiata molto facilmente sono due: i corpi quadratici e quelli ciclotomici. Qui si riescono a 'fare i conti' esplicitamente, ed è ciò che farà Fubini nel seguito del suo corso.

Riprendendo le precedenti osservazioni sulla mancata unicità della decomposizione in fattori primi all'interno di alcuni anelli di interi, egli si concentra su un *"esempio preliminare"*[100], quello della fattorizzazione del numero 21 in $K(\sqrt{-5})$, che non è unica. Fubini mostra quindi che nel caso di $\mathbb{Z}[\sqrt{-5}]$ non vale la decomposizione unica. La ragione di questo fenomeno è ascritta ad una sorta di "incompletezza" del campo oloide, cui si può ovviare "completandolo" mediante gli ideali, che vengono introdotti intuitivamente come i massimi comuni divisori "mancanti" degli elementi nell'anello degli interi del campo. Fubini scrive infatti, accogliendo l'impostazione di Dedekind: *"diremo ideale un ente che sia il M.C.D. di due interi α e β del corpo, e sia divisore di ogni numero, che sia somma di un multiplo di α e di un multiplo di β"*.[101]

Rimandando alle lezioni successive per una definizione rigorosa, sottolinea come questa forma intuitiva, anche se illogica, con la quale vengono introdotti gli ideali non deve destare stupore in quanto un espediente analogo è già stato utilizzato nella costruzione dei numeri complessi, per introdurre l'unità immaginaria i. Dimostra infine che, nel caso di $\mathbb{Z}[\sqrt{-5}]$, alla mancata decomposizione unica di 21 supplisce la fattorizzazione unica dell'ideale di tale numero in 'fattori ideali'.

Lo scopo diventa allora quello di *"porre in generale e giustificare le precedenti definizioni, o per meglio dire trasformarle in modo da renderle non assurde"*.[102] Fissati $\alpha_1, \alpha_2, \dots, \alpha_h$ interi del corpo, Fubini fornisce la costruzione degli ideali in senso moderno, definendo inoltre l'ideale principale (α) come quello formato dai multipli di un intero α del corpo. A questo punto, si può considerare al posto del corpo di numeri K l'insieme K' di tutti i suoi ideali, principali o meno.

Molto interessante, a nostro parere, è la motivazione con la quale Fubini introduce ai suoi studenti il concetto di ideale negli anelli di interi. Dopo aver dimostrato le consuete proprietà di divisibilità valide per gli interi, egli definisce i campi di numeri e, all'interno di questi, i loro anelli di interi algebrici. Il primo esempio è costituito dagli interi di Gauss; per questi è possibile definire una divisione con resto, a partire dalla quale tutta la teoria della divisibilità introdotta per gli interi è replicabile, cosicché vale il teorema di decomposizione unica di ogni elemento in un prodotto di elementi irriducibili. È però facile vedere come in altri casi la decomposizione unica non valga. L'esempio classico riportato da Fubini è quello dell'anello $\mathbb{Z}[\sqrt{-5}]$ in cui il numero 6 ha la doppia decomposizione in fattori irriducibili

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Significativa è la fortuna di questo esempio, che compare nelle opere di Dedekind e di Hilbert, fu ripreso in manuali posteriori alle *Lezioni* di Fubini ed è citato ancora oggi in vari corsi universitari di Teoria dei numeri.

Fubini fa poi notare agli studenti che sono noti in letteratura altri esempi: considerato l'insieme B dei numeri naturali congrui a 1 modulo 4, $B = \{1,5,9, \dots\}$, e detto 'irriducibile' un elemento in B se non è prodotto di due elementi in B, allora 9, 21 e 49 sono irriducibili, cosicché si ha la doppia decomposizione $441 = 21 \cdot 21 = 9 \cdot 49$. Nuovamente ciò avviene, secondo Fubini, perché l'insieme B è 'incompleto', nel senso che esso è immerso in una struttura più grande (l'insieme $\mathbb{N}$ dei numeri naturali), dove 9, 21 e 49 diventano decomponibili. In questo ambiente più grande, l'anomalia scompare in virtù del teorema fondamentale dell'aritmetica.

[100] *Ibidem*, cap. VII, §1, p. 233-236.
[101] *Ibidem*, cap. VII, §1, p. 234.
[102] *Ibidem*, cap. VII, §2, p. 236.

Sulla scia di Kummer e Dedekind, Fubini introduce quindi gli interi algebrici di un campo, procedendo per analogia con gli interi dei numeri razionali, e allo stesso modo vorrebbe studiarne l'aritmetica. In generale gli anelli di interi non sono tuttavia domini a ideali principali, dunque non hanno la fattorizzazione unica. Si pone allora il problema di come completare un anello di interi, ossia di quali elementi aggiungere per garantire la decomposizione unica. Essa è assicurata se ogni coppia di elementi ha un massimo comune divisore, per il quale valga l'identità di Bézout, cioè che si possa esprimere come combinazione lineare degli elementi in questione. Si tratta quindi di completare l'anello $\mathbb{Z}[\sqrt{-5}]$ aggiungendo i massimi comuni divisori mancanti: questi saranno appunto gli 'ideali', il cui termine viene in questo modo spiegato. L'ideale (α, β) in un anello di interi deve essere pensato come il massimo comun divisore – di fatto inesistente nel campo dato – degli elementi α, β dell'anello. Il completamento desiderato si ottiene considerando, oltre agli elementi dell'anello, anche i suoi ideali. Il fatto di educare i suoi studenti a 'vedere' gli ideali come numeri, come enti concreti piuttosto che astratti, ossia come massimi comuni divisori 'ideali' è un approccio, di impronta tedesca, interessante dal punto di vista didattico. Esso costituisce un ponte molto concreto, che nell'assiomatizzazione moderna si è perso, tra la teoria degli ideali e i numeri razionali.

Fubini vuole a questo punto cercare una condizione più debole, che renda i numeri algebrici 'simili' agli interi: definendo opportunamente il prodotto di ideali, si ha che ogni ideale si decompone in modo unico come prodotto di ideali primi. Non c'è la decomposizione unica a livello di numeri del campo, ma c'è a livello di ideali: i corpi che soddisfano tale proprietà vengono attualmente detti 'anelli di Dedekind'. Effettivamente il teorema fondamentale sui domini di Dedekind garantisce che negli anelli di interi valga sempre una forma 'debole' di decomposizione unica, ovvero la decomposizione unica di un ideale come prodotto di ideali primi.

Fubini passa a definire formalmente l'ideale $(\alpha_1, \dots, \alpha_k)$ in un anello come l'insieme delle combinazioni lineari a coefficienti nell'anello degli elementi $\alpha_1, \dots, \alpha_k$, così come siamo abituati a pensarlo modernamente.[103] È interessante come, con questo punto di vista, egli anticipi allo studente un argomento assai più avanzato (e non trattato esplicitamente nel corso del 1916-17) che è l'esistenza, per ogni campo di numeri *K*, del suo *corpo di classe di Hilbert*: un'estensione finita di *K* in cui tutti i suoi ideali diventano principali e sono quindi identificabili con un numero, il generatore. Il corpo di classe di Hilbert rappresenta allora, in un certo senso, il contesto in cui gli ideali diventano oggetti concreti.

Si noti inoltre che, mentre la definizione formale data da Fubini coincide di fatto con quella moderna di ideale in un anello noetheriano, la rappresentazione intuitiva di un ideale come un massimo comun divisore in un ambiente completato non è generalizzabile al di fuori del contesto degli anelli di interi di campi di numeri – per esempio nella geometria algebrica in dimensione superiore – proprio perché viene a mancare l'esistenza di un analogo del corpo di classe di Hilbert.[104] Un punto matematico fondamentale è che gli anelli di interi hanno, tra le altre proprietà, anche quella di avere dimensione 1; tutti gli ideali primi non nulli sono massimali e questo fatto è essenziale nella dimostrazione della decomposizione unica degli ideali.

Nelle sue *Lezioni*, Fubini inserisce a questo proposito un'interessante osservazione di geometria dei numeri: afferma infatti che i punti B immagine – mediante l'immersione canonica che manda l'ideale nella rete – degli interi di un dato ideale non nullo, formano una rete R contenuta nella rete r formata dai punti immagine degli interi del corpo. Fornisce quindi le definizioni di base e norma, mostrando che il discriminante di una base di un ideale è pari al prodotto del discriminante del corpo per il quadrato della norma e che la norma di un

[103] Cfr. Davenport 1952; Edwards 1980; Piazza 2000; Avigad 2004; Lemmermeyer 2011; Garret 2017.
[104] Cfr. Chevalley 1940.

ideale principale (α) vale $|Nm\ \alpha|$, ossia coincide con il valore assoluto del modulo dell'intero corrispondente α. Osserva che *"la norma di un ideale ha un notevole significato geometrico"*[105] e illustra come tale valore corrisponda al numero N degli interi del corpo che sono contenuti nel parallelepipedo fondamentale P di un ideale. Da ciò deduce che esistono nel corpo N interi tali che da ogni altro intero a del corpo si passa ad uno di essi in un unico modo, mediante l'aggiunta di un numero b dell'ideale. Dopo aver introdotto la congruenza rispetto ad un ideale, che generalizza la nozione di congruenza modulo un intero in $\mathbb{Z}$, ricava che il numero degli interi incongrui rispetto ad un ideale vale la norma di questo; in particolare, la norma di un ideale estende il concetto di valore assoluto di un intero nell'aritmetica elementare. Sono poi introdotti gli ideali primi[106], ossia ideali divisibili soltanto per se stessi e per l'ideale (1), con una definizione differente da quella attuale, ed è presentata la proprietà caratterizzante fondamentale: un ideale primo p che divide il prodotto ab di due ideali a, b divide almeno uno dei fattori. Da ciò discende l'unicità della scomposizione di ogni ideale nel prodotto di ideali primi, il che equivale ad affermare, in termini moderni, che ogni anello di interi è un dominio di Dedekind. Sulla teoria di Kronecker - Hilbert[107] e sulle generalizzazioni di alcuni concetti introdotti in precedenza (divisibilità di ideali, funzione di Euler, ideali primi, classi di ideali e forme decomponibili di un corpo algebrico) vertono le successive *Lezioni*. Kronecker, osserva Fubini, ha avuto il merito di sostituire i polinomi – da lui chiamati 'forme' – agli ideali, andando ad aggiungere agli interi del corpo degli altri enti, che sono appunto le forme, ossia polinomi i cui coefficienti sono interi del corpo. La teoria delle forme di Kronecker e delle loro norme è completamente equivalente a quella degli ideali e delle loro norme mediante la corrispondenza introdotta da Hilbert, che a una forma fa corrispondere il suo 'contenuto', ovvero l'ideale generato dai suoi coefficienti. Pertanto si raggiunge la completa analogia con l'aritmetica elementare aggiungendo al corpo indifferentemente gli ideali di Dedekind o le forme di Kronecker.

I teoremi di Minkowski e la geometria dei numeri permettono a Fubini di aprire la trattazione delle classi di ideali dimostrando che in ogni ideale j esiste almeno un intero non nullo ξ tale che $Nm\ \xi < \rho\sqrt{|d|}\ Nm\ j$, dove d è il discriminante del corpo e ρ è una costante che dipende soltanto dal corpo. Viene quindi introdotto il concetto di equivalenza tra ideali[108]: Fubini chiama 'equivalenti' due ideali J_1 e J_2 se sono ottenibili uno dall'altro moltiplicandoli per un elemento del campo K, ossia se esistono due interi $u, v \in K$ tali che $uJ_1 = vJ_2$. Dimostra che si tratta di una relazione di equivalenza e denota come 'classi di ideali' le classi di equivalenza. Inoltre definisce la 'classe principale' come quella costituita da ideali principali e indicata con $\mathbf{1}$, mostrando anche che l'operazione di prodotto tra ideali è compatibile con la relazione di equivalenza sopra citata. Il prodotto tra classi di ideali è quindi ben definito e tale prodotto ha elemento neutro $\mathbf{1}$. Dal lemma precedente e dalla considerazione che gli ideali di norma fissata sono in numero finito, segue che ogni classe di ideali contiene un ideale di norma $\leq \sqrt{|d|}$, dove d è il discriminante del campo. Di qui il fondamentale teorema di finitezza delle classi di ideali.

Nella trattazione moderna, si considera una generalizzazione del concetto di ideale, la nozione di 'ideale frazionario': sostanzialmente un ideale frazionario J di un campo K è un sottoinsieme di K tale che esiste $a \in K$ per cui aJ è un ideale di K. La definizione di classe di ideali si estende agli ideali frazionari, così come l'operatore di prodotto tra ideali, e si dimostra che le classi di ideali frazionari formano un gruppo finito, detto 'gruppo delle classi di ideali' del campo K. Questa costruzione non è esplicitamente presente nelle *Lezioni* di

[105] Fubini 1917, cap. VII, §2, p. 242.
[106] *Ibidem*, cap. VII, §4, p. 253.
[107] *Ibidem*, cap. VII, §5, p. 254: "dare un corpo equivale a dare un'equazione algebrica $g(z) = 0$ a coefficienti interi, il cui primo coefficiente si può supporre uguale ad 1".
[108] *Ibidem*, cap. VII, §8, p. 2

Fubini. Detto h il numero delle classi, si ha che $A^h = \mathbf{1}$ per ogni classe di ideali. Applicando questo risultato all'ideale generato da due elementi interi del campo si deduce che ogni coppia di elementi di un campo di numeri K ha un M.C.D., una cui potenza appartiene al campo dato. Ponendoci dal punto di vista della moderna teoria dei numeri, si può dire che tale M.C.D. si trova nell'*Hilbert classfield* di K, che è una estensione finita L di K tale che ogni ideale di K diventa principale in L.

La chiusa del VII capitolo è dedicata ad un ulteriore collegamento tra la teoria degli ideali e quella delle forme. Se $\alpha_1, \alpha_2, \dots, \alpha_n$ è una base di un ideale J in un corpo di grado n, ogni intero α di J può essere scritto come

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$$

con x_i interi razionali. La sua norma $Nm\ \alpha$ è un polinomio omogeneo nelle x a coefficienti interi razionali di grado n, decomponibile nel prodotto di n forme lineari. In particolare, *"una tale forma si dice corrispondere all'ideale J; cambiare la base dell'ideale, o cambiare un ideale in un ideale equivalente, fa passare dalla forma iniziale ad una forma equivalente"*[109]. Fubini dichiara poi, in modo in verità piuttosto oscuro, che la teoria degli ideali trova varie applicazioni a problemi nel campo assoluto di razionalità, in particolare concernenti le equazioni del tipo $F = m$, dove F è una delle forme citate e m un intero razionale. Probabilmente allude al fatto che la decomponibilità vale in un campo (la chiusura di Galois del campo dato) nel quale, quindi, "vivono" le radici dell'equazione sopra indicata.

4.4. *Cenni di aritmetica analitica, corpi quadratici e campi ciclotomici*

Nel capitolo intitolato *Aritmetica analitica*, il più breve della litografia e l'unico privo di esercizi e di riferimenti storici, Fubini sintetizza alcuni aspetti dell'analisi strettamente connessi alla teoria dei numeri. Egli parte dallo sviluppo di vari integrali per arrivare a calcolare i volumi di determinate zone dello spazio, che gli serviranno per concludere che ogni classe di ideali contiene un ideale che ha norma minore di una certa quantità, la quale dipende dalla radice quadrata del discriminante. Per fare ciò, utilizza i teoremi di Minkowski, immergendo l'anello degli interi in $\mathbb{R}^n$, come sottogruppo discreto per n opportuno. L'immagine dell'anello attraverso questo omomorfismo iniettivo è un reticolo; allo stesso modo gli ideali diventano reti all'interno di questo reticolo. Al calcolo del volume del parallelepipedo fondamentale di tale rete viene dedicato ampio spazio. Fubini affronta quindi lo studio dei corpi ciclotomici ovvero quelli generati da una radice ℓ-esima dell'unità, prestando particolare attenzione al caso in cui ℓ è primo. *Il grande teorema della progressione aritmetica*, ovvero il teorema di Dirichlet sulle progressioni aritmetiche, per il quale se n, ℓ sono coprimi esistono infiniti numeri primi razionali P tali che $P \equiv n\ (mod\ \ell)$, occupa da solo un'intera lezione.

Gli ultimi due capitoli delle *Lezioni di Teoria dei numeri* sono di notevole rilievo per la teoria dei numeri in quanto gettano un ponte verso sofisticati argomenti, di interesse ancora oggi assai vivo. Il IX, interamente incentrato sullo studio dei corpi quadratici, si apre con argomenti che fanno parte della trattazione standard della teoria dei numeri, quali la decomposizione degli ideali primi e le tre possibilità che si presentano per l'ideale generato da un numero primo nell'anello, il quale può essere il quadrato di un ideale primo, il prodotto di due ideali primi o esso stesso un ideale primo[110]. Il primo caso capita per un numero finito di

[109] *Ibidem*, cap. VII, §11, p. 304.

[110] Nella prima sez. del cap. IX Fubini studia come gli ideali primi (p) di $\mathbb{Z}$, estesi a K, si decompongono come prodotto di ideali primi di K. Se P è primo razionale, esso si decomporrà in ideali primi in K, ad esempio sarà $P = p_1 p_2 \dots p_r$. Proseguendo nella discussione, si individuano tre casi possibili:

i) P è primo anche in $K(\sqrt{m})$; $Nm\ P = P^2$. Il numero P si dice di secondo grado in K. Nel linguaggio corrente, tale P si chiama 'inerte'.

primi (detti primi che ramificano nel corpo), che sono i divisori del discriminante del campo; in alternativa, a seconda di certe congruenze si può sapere a priori se si ricade nel secondo o nel terzo caso. La semplicità di tali risultati è uno dei motivi per cui ancora oggi la decomposizione di ideali viene illustrata utilizzando i campi quadratici.[111] Questi paragrafi sono di per sé emblematici della cifra di concretezza che contraddistingue lo stile didattico di Fubini: egli espone infatti una determinazione esplicita dei generatori di un campo quadratico, individua la relazione di coniugio, definisce l'ideale coniugato e introduce infine il concetto di ideale ambiguo, attraverso il quale arriva a provare che, se il discriminante di un campo è un numero primo, allora il numero delle classi è dispari. Dopo aver introdotto il simbolo di Legendre-Jacobi[112], enuncia il 'teorema di reciprocità'. Noto anche come legge di reciprocità quadratica (LRQ), esso asserisce che

a) Se p, q sono primi dispari allora
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{2}} \left(\frac{q}{p}\right);$$
b) se p è un primo dispari allora
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$
c) se p è un primo dispari allora
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Tale relazione è abbastanza sorprendente, in quanto dà delle informazioni su una congruenza modulo q, a partire da una congruenza modulo p, elementi che a priori sembrerebbero indipendenti. Con gli strumenti concettuali trasmessi fino a questo punto, Fubini è già in grado di dimostrare la relazione in alcuni casi particolari, rimandando per quello generale all'ultimo capitolo delle *Lezioni*. La legge di reciprocità quadratica, congetturata da Euler e Legendre, è provata per la prima volta da Gauss nelle *Disquisitiones*. Nota anche come 'il gioiello della matematica', il 'teorema fondamentale" o, ancora, l'''*aureum theorema*' essa è importante sia intrinsecamente, in quanto fornisce indicazioni sulle profonde relazioni che intercorrono nelle congruenze tra i diversi numeri primi, sia in quanto costituisce il punto di partenza per generalizzazioni riguardanti l'aritmetica dei campi di numeri e la struttura dei loro gruppi di Galois, le quali si sono rivelate di grande fecondità e che sono ancora oggi oggetto di ricerca da parte della comunità matematica.[113] Nei teoremi elementari sulle congruenze modulo numeri primi, per esempio il piccolo teorema di Fermat, il teorema di Euler o quello di Wilson, entrano infatti di solito in gioco due numeri con due ruoli differenti: uno è il numero primo p che funge da modulo, l'altro è la base, ovvero la quantità di cui viene considerata la classe di resto $modulo\ p$. Al contrario, nell'enunciato della LRQ i ruoli di modulo e base si inter-scambiano: dati due primi dispari, il valere di una certa proprietà (l'essere un quadrato) di uno, modulo

---

ii) $P = p^2$, dove p è un ideale primo di K, tale che $pp' = Nm\ p = P$, cioè p coincide con l'ideale coniugato p'. Questo caso si ha se e solo se p è un divisore del discriminante d del corpo. Nel linguaggio moderno, P è detto 'primo che ramifica'.

iii) $P = pp'$ dove $p \neq p', Nm\ p = P$; in questo caso p è un ideale primo di K di primo grado. Oggi questi particolari P vengono detti 'primi che si decompongono'.

[111] Anche negli attuali corsi di teoria algebrica dei numeri spesso si studiano questi due casi: a posteriori, possiamo dire che questi corpi sono più facili da studiare, essendo noto il loro gruppo di Galois e avendo esso una struttura semplice (abeliano).

[112] Ricordiamo che se p è un numero primo e $a \in \mathbb{Z}$, il simbolo di Legendre $\left(\frac{a}{p}\right)$, da Fubini indicato con $\left(\frac{a}{p}\right)$, è definito da:
$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se } p|a \\ 1 \text{ se } p \nmid a \text{ e } a \text{ è un quadrato modulo } p \\ -1 \text{ se } p \nmid a \text{ e } a \text{ non è un quadrato modulo } p \end{cases}.$$

[113] Cfr. Lemmermeyer 1962.

l'altro, determina il valere della medesima proprietà del secondo, modulo il primo. I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della moderna teoria algebrica dei numeri. Uno dei suoi principali risultati è costituito dalle leggi di reciprocità stabilite da Emil Artin nel 1926 nell'ambito della teoria del corpo di classe, per qualunque estensione abeliana di corpi di numeri. Lo studio del caso non abeliano è attualmente al centro della ricerca in teoria dei numeri e ha portato a una rete di congetture e risultati parziali che formano il programma di Langlands[114]. Quando era stata scoperta nel Settecento la LRQ appariva probabilmente come una delle tante "curiose" proprietà della teoria dei numeri; negli anni delle *Lezioni* di Fubini, invece, si aveva già il sentore che essa fosse di speciale importanza.

Il capitolo prosegue con un paragrafo dedicato ad alcune osservazioni sull'ultimo teorema di Fermat, per il quale l'equazione diofantea $x^n + y^n = z^n$ non ammette soluzioni intere positive non banali per $n \geq 3$. Questo problema si riduce facilmente ai casi in cui $n = 4$ oppure $n = p$ è un primo dispari; inoltre è facile vedere che ogni eventuale soluzione può ricondursi ad una soluzione primitiva, in cui x, y, z non hanno un fattore comune. Fermat aveva provato l'impossibilità di una soluzione nel caso $n = 4$ utilizzando un procedimento induttivo detto "metodo della discesa"[115]. Era quindi sufficiente provare che l'equazione $x^p + y^p = z^p$ non ammette soluzioni primitive per ogni primo p dispari. Quando Fubini tiene il suo corso di teoria dei numeri, E. Kummer aveva già fornito una dimostrazione di questo risultato per tutti i primi p 'regolari', ossia quei primi dispari p che non dividono l'ordine h_p del gruppo delle classi di ideali del campo generato dalle radici p-esime dell'unità.

Come è noto, l'ultimo teorema di Fermat sarebbe stato dimostrato nella sua completa generalità da Andrew Wiles solo nel 1994, a coronamento di un intenso lavoro condotto da numerosi teorici dei numeri di fama mondiale. La dimostrazione è indiretta e richiede la traduzione del problema originario nel linguaggio della geometria algebrica, di cui utilizza strumenti assai sofisticati. In primo luogo è stato dimostrato che, a partire da un controesempio al teorema di Fermat, sarebbe stato possibile costruire un oggetto geometrico (una curva ellittica, detta *curva di Frey*) con proprietà aritmetiche molto particolari. Frey (1985), Serre (1987) e Ribet (1990) hanno poi provato che l'esistenza di una curva di Frey avrebbe fornito a sua volta un controesempio ad un'altra congettura, detta di Shimura-Taniyama-Weil, riguardante rappresentazioni di Galois che possono essere associate alle curve ellittiche razionali. Wiles ha infine fornito l'argomento conclusivo, dimostrando la congettura di Shimura-Taniyama-Weil in un caso particolare, sufficiente tuttavia a escludere l'esistenza di curve di Frey.[116] Sebbene la dimostrazione di Wiles sia stata oggetto di alcune semplificazioni dopo la sua pubblicazione, ad oggi non è stata trovata una dimostrazione più 'diretta' o 'naturale' dell'ultimo teorema di Fermat. A dire il vero, molti autorevoli matematici non ritengono che questo sia un obiettivo prioritario[117]: si sottolinea infatti come l'importanza di questo risultato risieda nella potenzialità e nella ricchezza delle teorie matematiche che sono state sviluppate a partire da esso, più che nell'enunciato in sé. Da questo punto di vista, la dimostrazione di Wiles rappresenta non una mèta bensì *"il punto di partenza di un dialogo aperto che è troppo inafferrabile e vivace per essere limitato da costrizioni fondazionali che sono estranee alla vera natura del soggetto"*[118].

[114] Il programma di Langlands è un'iniziativa di vasta portata, ancora in sviluppo, per la ricerca di connessioni tra la teoria dei numeri e la geometria. Fu proposto dal matematico R. Langlands quando cercò di relazionare i gruppi di Galois in teoria algebrica dei numeri con le forme automorfe e le rappresentazioni di gruppi algebrici su campi locali e anelli di adele. Ritenuto il più vasto singolo progetto della moderna ricerca matematica, è stato descritto da E. Frenkel come *"una sorta di grande teoria unificata della matematica"*. Cfr. Frenkel 2003, 2005 e 2007.
[115] Cfr. Ribenboim 1979. Si vedano anche Harris 2019 e Goldstein 1993, 1995a, 1995b, 1995c.
[116] Cfr. Frey 1986; Serre 1897; Ribet 1990.
[117] Cfr. Bertolini, Canuto 1996.
[118] Harris 2019.

Come accennato sopra, quando Fubini prepara le sue lezioni di teoria dei numeri Kummer aveva proposto un approccio alla dimostrazione dell'ultimo teorema di Fermat basato sull'aritmetica dei campi ciclotomici. Sebbene esso si fosse rivelato insufficiente a dimostrare il teorema nella sua generalità, esso aveva permesso di provarlo per una vasta classe di numeri primi (i cosiddetti primi 'regolari'). Come rileva Ribenboim, l'intuizione di Kummer si sarebbe rivelata corretta. L'aritmetica dei campi ciclotomici è infatti il contesto naturale in cui affrontare il problema.

Kummer aveva di fatto dimostrato un asserto più generale dell'ultimo teorema di Fermat e precisamente aveva provato che per ogni primo regolare p, l'equazione $x^p - y^p = z^p$ non ammette soluzioni non banali nell'anello degli interi del campo $\mathbb{Q}(\zeta_p)$ dove ζ_p è una radice primitiva p-esima dell'unità. Si ponga $\lambda = 1 - \zeta_p$; allora λ genera l'unico ideale primo che contiene p. Ogni soluzione primitiva x, y, z può essere ricondotta ad uno dei seguenti due casi:

I) xyz non è divisibile per λ;

II) xy non è divisibile per λ, e z è divisibile per λ.

Il caso II è il più complesso. La proprietà fondamentale utilizzata da Kummer per affrontarlo è nota come lemma di Kummer:

> Se p è un primo regolare e u è un'unità dell'anello $\mathbb{Z}[\zeta_p]$ tale che $u \equiv m\ (mod\ p)$ per qualche intero $m \in \mathbb{Z}$, allora u è la p-esima potenza di un'unità di $\mathbb{Z}[\zeta_p]$.

Nelle sue lezioni del 1916-17, Fubini non fa riferimento alla nozione di primo regolare, né al suo significato. Egli dimostra il risultato per $p = 3$, dichiarando di seguire l'argomentazione di Kummer, valida in particolare per tutti i primi dispari ≤ 100 (si tratta infatti di primi regolari, eccetto 37, 59 e 67). Certamente 3 è un primo regolare: infatti l'anello degli interi di $\mathbb{Q}[\zeta_3]$ è $\mathbb{Z}[\zeta_3]$, che si dimostra facilmente essere un dominio a fattorizzazione unica; quindi $h_3 = 1$.

Di fatto, il caso $p = 3$ presenta però delle semplificazioni rispetto a quello di un arbitrario primo regolare. In primo luogo, come spiegato da Fubini, il caso I non si pone. In secondo luogo, le unità dell'anello $\mathbb{Z}[\zeta_3]$ sono un insieme finito contenente 6 elementi, e il lemma di Kummer per questa specifica situazione è direttamente verificabile.

Le semplificazioni sono significative tant'è che il caso $p = 3$ era già noto precedentemente al lavoro di Kummer. La sua dimostrazione risale infatti a Euler[119], sebbene alcuni passaggi riguardati la fattorizzazione non fossero adeguatamente motivati; una seconda dimostrazione, pubblicata postuma, era stata data da Gauss. È a quest'ultima che si ispira Fubini. Seguiamone da vicino i passaggi.

Si ponga $\omega = \zeta_3$. Innanzitutto Fubini scarta il caso I, infatti la struttura particolarmente semplice del gruppo delle unità permette di verificare che ogni intero di $\mathbb{Z}[\omega]$ non divisibile per λ ha cubo congruo a $\pm 1\ (mod\ \lambda^3) = 3\lambda$ e la somma di due tali cubi non può essere a sua volta congrua a $\pm 1\ (mod\ \lambda^3)$. Dopodiché, supponendo che x, y, z sia una soluzione rientrante nel caso II, pone $z = \lambda^n Z$, con Z non divisibile per λ. Si ha allora

$$x^3 - y^3 = \varepsilon \lambda^{3n} Z^3 \qquad \textbf{[a]}.$$

In questo primo passo della "discesa" si ha $\varepsilon = 1$, ma nei successivi potrà assumere come valore una generica unità del campo ciclotomico.

Si può decomporre il termine $x^3 - y^3$ nell'anello $\mathbb{Z}[\omega]$ ottenendo l'uguaglianza:

$$(x - y)(x - \omega y)(x - \omega^2 y) = \varepsilon \lambda^{3n} Z^3.$$

[119] Euler 1770, cap. 15, §423, p. 486-489.

Fubini dimostra che i tre fattori $x-y, x-\omega y$ e $x-\omega^2 y$ non hanno, oltre a λ, nessun fattore in comune, e che uno solo di essi (per esempio $x-y$) è divisibile per λ^2. Segue[120] che si può scrivere

$$x-y=\eta_1\lambda^{3n-2}\tau^3, \qquad x-\omega y=\eta_2\lambda\mu^3, \qquad x-\omega^2 y=\eta_3\lambda\nu^3,$$

dove η_1, η_2, η_3 sono unità e τ, μ, ν sono interi.

Sostituendo questi valori nell'equazione

$$\omega(x-y)+\omega^2(x-\omega y)+x-\omega^2 y=0$$

e, dividendo per $\lambda\omega^2\eta_2$, si trova (eventualmente scambiando ν con $-\nu$)

$$\mu^3-\nu^3=\varepsilon_1\lambda^{3(n-1)}\tau^3, \qquad [\mathbf{b}]$$

dove ε_1 è un'unità.

In questo modo si ottiene un'equazione del tipo [**a**] in cui l'esponente n è sceso di uno. Un argomento induttivo di discesa permette allora di affermare che, dopo un numero finito di passaggi, si giunge a un'equazione che rientra nel caso I, e ciò è già stato provato impossibile.

Questi metodi dimostrativi, tra cui quello adottato da Fubini, pur non essendo di carattere prettamente elementare, erano abbastanza noti all'epoca e si fondavano su concetti e risultati ormai consolidati di teoria algebrica dei numeri. Negli anni immediatamente precedenti alle *Lezioni* di Fubini, si erano registrati parecchi tentativi di dimostrare il teorema di Fermat nella sua generalità, quindi ci si aspettava che comparisse all'interno di un corso di teoria dei numeri. Gran parte degli argomenti affrontati nelle lezioni precedenti è funzionale proprio alla dimostrazione di questo teorema, grande classico della teoria dei numeri e problema, all'epoca, ancora 'aperto'.

Al termine del capitolo IX viene ripreso lo studio delle forme quadratiche. Osserviamo come, ancora una volta nello spirito della matematica italiana del tempo, Fubini si impegni a tradurre tutti i risultati precedentemente ottenuti nel linguaggio delle forme, oggi caduto in disuso. La trattazione delle forme permea le *Lezioni*, nelle sue varie accezioni. Già all'interno del cap. I, affrontando la trattazione dell'algoritmo di Euclide per il calcolo del M.C.D., è introdotto il concetto di forma lineare (in due variabili) a coefficienti interi e viene mostrato che il M.C.D. di due interi a, b è un valore – di fatto il minimo valore positivo – della forma lineare $ax+by$.

Il testo di Fubini ben riflette il fatto che nella storia della teoria dei numeri si sono sviluppate due teorie e due linguaggi: quello degli *ideali*, che si fa risalire a Dedekind, e quello delle forme, attribuito a Kronecker. Quest'ultimo e la sua relazione con la teoria degli ideali è stato illustrato da Hilbert[121], cui Fubini si ispira palesemente. Una forma di un corpo di numeri K è semplicemente un polinomio – non necessariamente omogeneo – a più variabili, a coefficienti negli interi di K. Una forma con un solo coefficiente si dice 'principale'. Le forme, afferma Fubini, *"sono da Kronecker sostituite agli ideali"*[122]. La relazione tra forme e ideali è messa in evidenza attraverso la nozione di 'contenuto': si tratta dell'ideale generato dai coefficienti di una forma. Ad ogni ideale (e anche ad ogni sistema di generatori di un ideale) corrispondono quindi più forme. Fubini enuncia poi il teorema fondamentale che asserisce che il contenuto di un prodotto di due forme è l'ideale prodotto dei due contenuti delle forme: oggi diremmo che il contenuto è un morfismo di monoidi. La dimostrazione si basa sulla fattorizzazione unica di un ideale in prodotto di potenze di primi, e quindi utilizza il fatto che l'anello di interi di un campo di numeri è un dominio di Dedekind. Moltiplicando una forma F per i suoi coniugati su $\mathbb{Q}$ si ottiene un polinomio f a coefficienti interi razionali; il M.C.D. di tali coefficienti è detto 'norma' della forma F.

---

[120] Questo passaggio non è del tutto chiaro nelle lezioni di Fubini. Egli utilizza qui il fatto, mai dichiarato esplicitamente, che l'anello degli interi nel quale si sta lavorando è un dominio a fattorizzazione unica.

[121] Cfr. Hilbert 1897 (trad. 1998), p. 13-20. Per quanto riguarda lo *Zalhbericht* cfr. Lemmermeyer, Schappacher 2003 e Schappacher 2005.

[122] Fubini 1917, cap. VII, §5, p. 255.

La norma è 1 se e solo se il contenuto di F è l'ideale generato da 1, l'anello degli interi di K. In tal caso si dice che la forma F è una 'forma unità'. Utilizzando il teorema fondamentale è possibile mostrare che due forme hanno lo stesso contenuto esattamente se il loro rapporto è uguale al rapporto di due forme unità: questa proprietà definisce la nozione di equivalenza di forme secondo Kronecker. Ne derivano due conseguenze notevoli: la prima è che due forme aventi gli stessi coefficienti hanno lo stesso contenuto e quindi sono equivalenti; la seconda è che forme equivalenti hanno uguali norme. Proseguendo nell'intento di illustrare il perfetto parallelismo tra l'approccio di Dedekind e quello di Kronecker, Fubini passa a mostrare la coincidenza dei concetti di norma per le forme e per gli ideali. La norma di una forma è uguale alla norma del suo contenuto. Per quanto già provato egli può semplificare l'argomento associando a un ideale J in un campo di numeri numeri K una forma di tipo lineare (ve ne è sempre almeno una in ogni classe di equivalenza): essa si può definire esplicitamente come $F = \alpha_1 x_1 + \cdots + \alpha_n x_n$, dove $\alpha_1, \dots, \alpha_n$ è una base di J come modulo libero su $\mathbb{Z}$. Considerando inoltre una base $\omega_1, \dots, \omega_n$ dell'anello degli interi di K su $\mathbb{Z}$ è possibile esprimere il prodotto della forma F per le sue coniugate mediante un prodotto di matrici; lo studio del loro determinante mostra l'uguaglianza desiderata.

Fubini conclude affermando che *"la teoria delle forme di Kronecker e delle loro norme è dunque completamente equivalente alla teoria degli ideali e loro norme"*[123]. In particolare, 'aggiungendo' al corpo o gli ideali di Dedekind o le forme di Kronecker – o, meglio, le loro classi di equivalenza – si raggiunge *"l'analogia con l'aritmetica elementare"*[124], ovvero la validità delle proprietà tipiche dei numeri interi e discendenti dalla fattorizzazione unica. Emerge nuovamente in questo contesto il punto di vista di Fubini, ossia il fatto che il fallimento della fattorizzazione unica nei campi di numeri sia attribuibile ad un fenomeno di incompletezza, cui l'introduzione degli ideali – o delle forme – pone rimedio. [125] Si è dunque provato che c'è una corrispondenza: fissate infatti una base dell'anello degli interi e una base dell'ideale – che sono tutte reti nella sua terminologia – ad ogni ideale si può associare una forma. Ideali che sono equivalenti, nel senso che danno origine alla stessa classe nel gruppo delle classi, danno origine a forme equivalenti, cioè che si possono ottenere l'una dall'altra applicando una trasformata lineare speciale. Fubini introduce poi la nozione più forte di 'ideali posequivalenti', ossia ottenibili l'uno dall'altro mediante una moltiplicazione per degli elementi del campo a norma positiva; mentre gli ideali equivalenti corrispondono a forme equivalenti, quelli posequivalenti corrispondono alle forme che lui chiama 'propriamente' equivalenti, ossia ottenibili mediante una trasformazione lineare a determinante positivo. Questo raffinamento – che porta alla definizione del cosiddetto *narrow class field* [126] – trova la sua principale ragion d'essere nella classificazione delle forme quadratiche, che sono il vero *leitmotiv* di queste *Lezioni*.

A distanza di un secolo, gli ideali hanno prevalso sulle forme. I manuali di teoria algebrica dei numeri descrivono l'aritmetica dei campi di numeri algebrici in termini di proprietà degli ideali ed è stato introdotto il concetto di dominio di Dedekind per caratterizzare gli anelli di interi di campi di numeri. A chi si è formato su queste nozioni, la teoria sembra in questo modo più pulita, non dovendo ricorrere a classi di equivalenza. Tuttavia la trattazione moderna perde in concretezza, e quest'ultima risulta necessaria in certi ambiti matematici, per esempio l'algebra computazionale, dove si rivelano di grande utilità il calcolo di generatori espliciti di un ideale (come le basi di Gröbner), le forme ad essi associate e le nozioni correlate a queste tematiche (come le sizigie) che si richiamano più da vicino al punto di vista di Kronecker.

[123] *Ibidem*, cap. VII, §5, p. 261.
[124] *Ibidem.*
[125] Cfr. Fantappiè 1927; Boniface, Schappacher 2002 e Goldstein 2007.
[126] Cfr. Cassels, Fröhlich 1967, p. 180.

Gettate le basi necessarie allo sviluppo della teoria successiva, Fubini dedica l'intero capitolo X ai temi a lui più cari, mettendo in luce alcuni collegamenti tra algebra astratta, analisi e geometria. L'ultima sezione delle *Lezioni* si apre con lo studio dell'equazione $x^\ell - 1 = 0$ da cui dipende il poligono regolare di ℓ lati, con ℓ primo dispari. In ottica moderna, quanto sviluppato da Fubini corrisponde allo studio delle funzioni polinomiali che sono invarianti per particolari permutazioni delle radici dell'unità, ossia invarianti per sottogruppi del gruppo di Galois del corpo $\mathbb{Q}(\zeta_\ell)$. Si tratta dunque di quella che potremmo chiamare una trattazione dei campi intermedi delle estensioni ciclotomiche. Tutto il discorso può essere facilmente reinterpretato in chiave di teoria di Galois, tema non affrontato tuttavia da Fubini che si prefigge di cercare dei generatori dei sottocampi dei campi ciclotomici ottenibili in modo sistematico. Per fare ciò egli introduce i periodi di Gauss che, di fatto, sono proprio tali generatori. Procede poi in modo molto concreto, volendo arrivare ad avere delle equazioni 'tangibili'. Anche F. Klein – una quindicina di anni prima di Fubini – aveva del resto adottato questo approccio nei suoi studi sulle cosiddette 'equazioni ciclotomiche', cioè le equazioni dei poligoni regolari che sono delle funzioni polinomiali le quali assumono lo stesso valore sui vertici e che sono perciò invarianti sotto l'azione di un certo gruppo. Questo indirizzo di ricerca sarebbe successivamente caduto in oblio in seguito alla formalizzazione e alla diffusione della teoria di Galois, e sarebbe stato soppiantato dallo studio dei campi ciclotomici.

L'obiettivo di Fubini, esposto sin dalla prima sezione del capitolo, è quello di risolvere l'equazione ciclotomica $x^n = 1$. È noto che le sue soluzioni, rappresentate nel piano di Argand-Gauss, sono i vertici di un *n*-agono regolare inscritto nella circonferenza di centro l'origine e raggio unitario e avente un vertice nel punto rappresentante l'unità. Per il teorema di Abel-Ruffini, l'equazione generale di grado *n* non è risolubile per radicali, perché il suo gruppo di Galois non è risolubile. Tuttavia le estensioni ciclotomiche sono abeliane, e quindi risolubili. Lo scopo diventa allora quello di individuare un procedimento che permetta di scrivere le radici dell'unità come espressioni coinvolgenti radici.

A questo fine Gauss aveva introdotto delle somme di radici dell'unità dette 'periodi', mediante i quali era stato in grado di ridurre le soluzioni dell'equazione ciclotomica a un sequenza di soluzioni di equazioni di grado più basso. La tecnica utilizzata da Gauss sfruttava la simmetria tra le varie radici dell'unità e si esprimeva molto agevolmente utilizzando la teoria di Galois. Tuttavia, la sua costruzione originaria diretta, utilizzata anche da Fubini, ne metteva in luce la concretezza e il carattere procedurale.

Ispirandosi a questa tradizione di pensiero, Fubini si limita a trattare il caso in cui $n = \ell$ è un primo dispari. Effettivamente la trattazione del problema generale non presenta grandi differenze rispetto ad esso.

Innanzitutto egli studia l'aritmetica del campo di spezzamento del polinomio $x^\ell - 1$. Detta Z una radice primitiva ℓ-esima dell'unità (concretamente, nelle *Lezioni* l'autore assume il numero complesso $Z = e^{\frac{2\pi i}{\ell}}$) e scelta *g* radice primitiva modulo ℓ, cioè un generatore del gruppo ciclico $\left(\frac{\mathbb{Z}}{\ell\mathbb{Z}}\right)^*$, le radici primitive ℓ-esime dell'unità possono essere indicizzate ponendo $\vartheta_i = Z^{g^i}$, in modo tale che valga la relazione ${\vartheta_i}^g = \vartheta_{i+1}$ (dove gli indici sono interpretati modulo $\ell - 1$). Questa simmetria è alla base dell'intero procedimento.

Se rivediamo la costruzione in termini di teoria di Galois, l'elevazione alla potenza *g*-esima delle radici ℓ-esime dell'unità corrisponde all'azione di un generatore del gruppo e l'azione del gruppo di Galois permuta ciclicamente la stringa $\vartheta_0, \vartheta_1, \dots, \vartheta_{l-2}$.

Si considera quindi un fattore e di $\ell - 1$ e si pone $\ell - 1 = ef$. Ciò corrisponde a scegliere un sottogruppo *H* del gruppo di Galois *G*, e quindi un sottocampo di $\mathbb{Q}(Z)$ di grado e. I periodi di Gauss associati a tale fattore sono gli e numeri complessi

$$\eta_{\mathbf{0}} = \vartheta_0 + \vartheta_e + \cdots + \vartheta_{(f-1)e}$$

$$\eta_{\mathbf{1}} = \vartheta_1 + \vartheta_{e+1} + \cdots + \vartheta_{(f-1)e+1}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\eta_{\boldsymbol{e-1}} = \vartheta_{e-1} + \vartheta_{2e-1} + \cdots + \vartheta_{fe-1}.$$

Osserviamo che la sostituzione $Z \mapsto Z^g$ trasforma ciclicamente $\eta_{\boldsymbol{i}}$ in η_{i+1}, cosicché i periodi sono lasciati invariati dalla sostituzione $Z \mapsto Z^{g^e}$ e dalle sue iterazioni (in termini galoisiani, i periodi stanno nel campo fissato dal sottogruppo di ordine *f* di *G*). Di fatto, i periodi costituiscono una base normale di tale campo. Tale è la parafrasi, in termini galoisiani dell'affermazione di Fubini: *"un polinomio in Z a coefficienti razionali, che non muta cambiando Z in Z^{g^e}, è combinazione lineare a coefficienti razionali dei periodi di Gauss"*.[127] Agli estremi, per $e = \ell - 1$ i periodi coincidono con i ϑ_i, mentre per per $e = 1$ c'è un unico periodo

$$\eta_0 = \vartheta_0 + \vartheta_1 + \cdots + \vartheta_{\ell-2} = -1.$$

Al crescere di *e* i periodi crescono quindi di complessità.
I periodi e le loro proprietà possono essere utilizzati per esprimere la radice primitiva ℓ-esima dell'unità *Z* mediante radicali. Il metodo di Gauss consiste in un vero e proprio algoritmo, che sfrutta i periodi per decomporre in sotto-problemi il problema di risolvere l'equazione ciclotomica. Di fatto, analizzandolo in dettaglio ci si rende conto che tale algoritmo lavora ricorsivamente sulla lunghezza dei periodi e pertanto sulla taglia del divisore *e*.

Gauss non dà un nome al campo generato dai periodi associati al divisore *e*; in questa sede, per comodità lo chiameremo K_f. Esso è il campo fissato dal sottogruppo di ordine *f* di $\left(\frac{\mathbb{Z}}{\ell\mathbb{Z}}\right)^*$, ha grado *e* su $\mathbb{Q}$ e ha come elementi le 'combinazioni lineari dei periodi di Gauss'; in altre parole i periodi di Gauss sono una base di K_f su $\mathbb{Q}$. D'altra parte, fissato un periodo, per esempio $\eta_{\mathbf{0}}$, è possibile provare (con un argomento galoisiano) che anche $1, \eta_0, {\eta_0}^2, {\eta_0}^3, \ldots, {\eta_0}^{e-1}$ sono una base di K_f e che ogni elemento di K_f si può quindi scrivere come polinomio in η_0 di grado minore o uguale a $e - 1$, ovvero, come diremmo in termini moderni, $K_f = \mathbb{Q}(\eta_0)$. In particolare, ogni periodo si può esprimere come un polinomio a coefficienti razionali in un qualsiasi altro periodo. Scrive Fubini: *"ed è questo il metodo dato da Gauss per risolvere il problema della ricerca dei poligoni regolari"* [128].

Segue, nelle lezioni del 1916-17, la descrizione dell'algoritmo; il testo in alcuni passi è piuttosto oscuro[129]. Sia $G_e(\eta) = (\eta - \eta_0)(\eta - \eta_1) \ldots (\eta - \eta_{e-1})$ il polinomio minimo annullato dai periodi associati alla decomposizione ef. Si tratta di un polinomio a coefficienti razionali. Fubini così esordisce: *"si cominci col risolvere l'equazione $G_e(\eta) = 0$; basterà trovarne una radice, perché siano note tutte"*[130]. Successivamente spiega come risolvere l'equazione: sia ε una radice primitiva e-esima dell'unità, e sia r un intero arbitrario, posto

$$Z_r = \eta_0 + \varepsilon^r \eta_1 + \cdots + \varepsilon^{(e-1)r} \eta_{e-1}$$

la quantità Z_r^e resta invariata applicando la sostituzione $Z \to Z^g$, e quindi è un elemento di $\mathbb{Q}(\varepsilon)$. Gli elementi Z_r possono quindi essere espressi come radicali di elementi di $\mathbb{Q}(\varepsilon)$, e i periodi $\eta_{\mathbf{0}}, \eta_{\mathbf{1}} \ldots, \eta_{e-1}$ si possono rappresentare come combinazioni $\mathbb{Q}(\varepsilon)$-lineari di tali radicali.

[127] Fubini 1917, cap. X, §2, p. 370.
[128] *Ibidem*, cap. X, §2, p. 372.
[129] Per una trattazione in termini moderni e corredata di esempi cfr. Spears 2016.
[130] Fubini 1917, cap. X, §2, p. 372

Il polinomio ciclotomico $F(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1$ si può decomporre come $F(x) = F_1(x)F_2(x) \ldots F_{e-1}(x)$, dove

$$F_i(x) = (x - \vartheta_i)(x - \vartheta_{i+e}) \ldots \left(x - \vartheta_{i+(f-1)e}\right).$$

Ogni polinomio $F_i(x)$ è un polinomio di grado f, invariante per la trasformazione $Z \to Z^{g^e}$ e quindi i suoi coefficienti stanno nel campo K_f generato dai periodi. Si tratta allora di risolvere i polinomi $F_i(x)$ rappresentandone le radici come radicali dei periodi $\eta_0, \eta_1, \ldots., \eta_{e-1}$. Se f ammette una decomposizione non banale, si può procedere iterativamente *"riducendo così il problema man mano ad equazioni di tipo più semplice"*[131]. L'unico esempio di applicazione fornito da Fubini è tuttavia quello relativo al caso $e = 2$. Qui la situazione è molto semplice in quanto ci sono due periodi:

$$\eta_0 = \sum_{i\ pari} \vartheta_i, \qquad \eta_1 = \sum_{i\ dispari} \vartheta_i\ ,$$

ed è facile calcolare l'equazione razionale di secondo grado di cui η_0 e η_1 sono radici. Da qui si ricava la loro espressione come radicali:

$$\eta_0, \eta_1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{(-1)^{\frac{\ell-1}{2}}\ell}.$$

Significativo è il fatto che Fubini riprenda, nel §3 del capitolo X, la LRQ. Di fatto egli ha già dimostrato precedentemente molti casi di questo teorema, utilizzando la decomposizione dei numeri primi nei campi quadratici e ha rimandato a Sommer per i rimanenti. Che ritenga opportuno ritornare sul tema all'interno della trattazione dei campi ciclotomici è segno che, nonostante non fosse uno specialista di teoria dei numeri, aveva tuttavia una profonda conoscenza di questa disciplina e nutriva per essa una forte sensibilità. Infatti, è proprio nel contesto della teoria di Galois dei campi ciclotomici che si rivela il significato profondo della LRQ e in cui si comprendono le diverse generalizzazioni che ne sono state proposte, e che costituiscono una parte fondamentale della moderna teoria algebrica dei numeri.

Come affermano F. Lemmermeyer ed E. Hecke *"la storia della legge di reciprocità è una storia della teoria algebrica dei numeri"*:

> La legge di reciprocità quadratica segna l'inizio della teoria dei numeri moderna. Per ciò che riguarda la sua forma, essa appartiene ancora alla teoria dei numeri razionali, in quanto essa si può formulare completamente in termini di relazioni tra numeri razionali; tuttavia il suo contenuto mira oltre al dominio dei numeri razionali.[…] Lo sviluppo della teoria algebrica dei numeri ha ora mostrato che il vero contenuto della legge di reciprocità quadratica diventa comprensibile soltanto se si considerano i numeri algebrici in generale e che una dimostrazione appropriata alla natura del problema può essere portata avanti soltanto con queste tecniche superiori.[132]

Ricordiamo che la legge di reciprocità quadratica afferma che dati due numeri primi dispari distinti p, q i due valori $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$ sono legati dalla relazione

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{2}\frac{}{2}}\left(\frac{q}{p}\right).$$

Tipicamente l'enunciato viene completato con le seguenti affermazioni che permettono di calcolare ogni simbolo di Legendre, sfruttandone la moltiplicatività e riducendosi a calcolare quadrati, modulo primi, sempre più piccoli:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}.$$

---

[131] *Ibidem.*

[132] Hecke 1923, p. 59; Lemmermeyer 1962, p. V.

Esistono più di 200 dimostrazioni della LRQ, alcune delle quali di tipo elementare (cioè che utilizzano solo i numeri interi e le loro proprietà aritmetiche). Il difetto di queste ultime è che non permettono di intuire le ragioni profonde e strutturali che implicano la validità del teorema. Per gettare luce su di esse è necessario affinare gli strumenti teorici e interpretare la legge nel contesto della teoria dei campi di numeri e della teoria di Galois.

L'argomento galoisiano utilizzato da Fubini – pur senza mai farne menzione esplicita – può essere schematizzato come segue: dati due numeri primi dispari distinti p, q si consideri il campo ciclotomico $\mathbb{Q}(\zeta_p)$ ottenuto aggiungendo a $\mathbb{Q}$ una radice primitiva p-esima dell'unità. Il gruppo degli automorfismi *G* di $\mathbb{Q}(\zeta_p)$ è isomorfo canonicamente a $(\mathbb{Z}/p\mathbb{Z})^*$; l'isomorfismo inverso associa alla classe di n in $(\mathbb{Z}/p\mathbb{Z})^*$ l'automorfismo indotto dalla sostituzione $\zeta_p \to {\zeta_p}^n$. Quindi, *G* è ciclico di ordine $p-1$ e possiede un unico sottogruppo *Q* di indice 2, che è il sottogruppo dei quadrati, il cui campo fissato è l'unico sottocampo quadratico K di $\mathbb{Q}(\zeta_p)$. Il periodo di Gauss corrispondente al divisore $e = 2$ di $p-1$ ne fornisce un generatore; precisamente risulta $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$. L'anello degli interi di $\mathbb{Q}(\zeta_p)$ è $\mathbb{Z}(\zeta_p)$; la sostituzione $\zeta_p \to {\zeta_p}^q$ induce un automorfismo σ_q di $\mathbb{Q}(\zeta_p)$ (l'automorfismo di Frobenius[133] a q), il quale si restringe ad un automorfismo $\sigma_q|_K$ di K. Ora, essendo K un campo quadratico, esso ha esattamente due automorfismi, uno banale e uno non banale. Il teorema fondamentale della teoria dei Galois assicura che $\sigma_q|_K$ è l'automorfismo non banale di K se e solo se σ_q è un quadrato nel gruppo degli automorfismi, ovvero se e solo se q è un quadrato in $(\mathbb{Z}/p\mathbb{Z})^*$. D'altra parte, per funtorialità $\sigma_q|_K$ è l'automorfismo di Frobenius a q dell'estensione $K/\mathbb{Q}$ e quindi è banale se e solo se il primo q si decompone completamente in K, cioè se e solo se $(-1)^{\frac{p-1}{2}}p$ è un quadrato modulo q. Si trovano quindi due condizioni che caratterizzano la non banalità di $\sigma_q|_K$, una espressa in termini di una congruenza di q modulo p e l'altra espressa in termini di una congruenza di p modulo q. Dal confronto delle due si ottiene la legge di reciprocità quadratica.

Nelle generalizzazioni della LRQ, il senso del termine 'reciproco' si perde. I vari 'simboli' che generalizzano quello di Legendre hanno argomenti appartenenti a domini differenti[134], e il carattere di simmetria attestato dalla LRQ non ha un analogo nelle formulazioni delle leggi di reciprocità successive. Ciò che sopravvive della reciprocità, almeno nel caso di un'estensione abeliana $K/\mathbb{Q}$ è il sussistere di una relazione di dipendenza tra due tipi di congruenze riguardanti un numero primo p che non ramifica nell'estensione[135] (questo accade per tutti i numeri primi, salvo un numero finito): un primo tipo che determina la completa riducibilità di uno o più polinomi modulo p (congruenze in cui p ha il ruolo di modulo) e un secondo tipo che considera le congruenze di p modulo un certo intero, detto conduttore dell'estensione, divisibile solo per i primi che ramificano nell'estensione; qui p ha il ruolo di base della congruenza. Si può dunque dire che ciò che caratterizza le varie leggi di reciprocità è l'affermazione di una interdipendenza tra congruenze rispetto a moduli diversi: un certo insieme di congruenze modulo un primo p vale se e solo se p soddisfa un altro insieme di congruenze modulo un altro intero, il conduttore dell'estensione.

Il gruppo di Galois assoluto $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ è il gruppo degli automorfismi dei numeri algebrici. Esso è un gruppo topologico profinito, agisce su ogni campo di numeri, su ogni anello di interi, e all'interno di essi permuta gli ideali primi di norma fissata.

[133] Su Frobenius cfr. Hawkins 2013.
[134] Per una panoramica su questi temi cfr. Lemmermeyer 1962, p. V-XV.
[135] Questo concetto è ben spiegato in Wyman 1972, p. 571-586.

La corrispondenza di Galois si estende garantendo una corrispondenza funtoriale tra i suoi sottogruppi chiusi e i sottocampi di numeri algebrici. Pertanto la sua struttura codifica le proprietà algebriche e aritmetiche di tutte le possibili estensioni algebriche dei razionali. Molti teorici dei numeri affermano che l'obiettivo della teoria algebrica dei numeri consiste nella comprensione della struttura del gruppo $G_{\mathbb{Q}}$. Un importante risultato in questa direzione è costituito dalla legge di reciprocità di Artin, che fornisce una descrizione dell'abelianizzazione di questo gruppo e che permette di associare ad ogni campo di numeri con gruppo di Galois abeliano un numero intero detto 'conduttore'. La legge di reciprocità di Artin implica un altro importante risultato, il teorema di Kronecker-Weber: ogni estensione abeliana dei razionali è contenuta in un'estensione ciclotomica e il suo conduttore è semplicemente l'ordine minimo della radice dell'unità che genera tale estensione. La legge di reciprocità di Artin permette di caratterizzare i primi che si decompongono completamente in un'estensione abeliana come quelli che soddisfano un certo insieme di congruenze modulo il conduttore. D'altra parte, tali primi sono quasi per definizione quelli modulo i quali un certo insieme di polinomi a coefficienti interi (i polinomi minimi di un insieme di generatori dell'anello degli interi dell'estensione) si riduce in fattori lineari. In questa relazione tra un insieme di congruenze modulo un primo p e un insieme di congruenze di p modulo il conduttore, consiste la generalizzazione della legge di reciprocità quadratica. La formulazione di una legge di reciprocità valida per campi di numeri con gruppo di Galois non abeliano è uno degli obiettivi prioritari della teoria dei numeri contemporanea, cui possono essere ricondotti filoni di ricerca di sicura importanza e profondità, come la teoria delle forme automorfe e il programma di Langlands.

Un ultimo cenno merita la trattazione della funzione ζ di Dedekind, che Fubini aveva introdotto all'interno del cap. VIII e cui dedica l'ultima parte del suo corso di teoria dei numeri del 1916-17. Tale funzione costituisce una generalizzazione della zeta di Riemann, funzione ben nota anche tra i non specialisti e con importanti applicazioni in teoria dei numeri, in fisica e teoria della probabilità[136]. Essa è solitamente definita mediante la serie di Dirichlet

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s}$$

convergente nel semipiano dei numeri complessi con parte reale > 1. È possibile estenderla, mediante un'equazione funzionale, ad una funzione meromorfa su $\mathbb{C}$ avente un unico polo semplice in $s = 1$ con residuo 1. Dal punto di vista della teoria dei numeri, le più importanti caratteristiche della funzione zeta sono le seguenti.

- *La sua rappresentazione come prodotto di Euler.* Il teorema fondamentale dell'aritmetica e i risultati di riordinamento dei termini di una serie permettono di riscrivere la funzione zeta come prodotto infinito

$$\sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}$$

dove *p* varia nell'insieme di tutti i numeri primi. Ogni fattore di tale prodotto infinito è detto *fattore euleriano a* p. Pur basandosi su un principio aritmetico elementare, la decomposizione euleriana riflette un principio molto profondo della prassi aritmetica moderna: ovvero quello di isolare, in un ente aritmetico, componenti *locali*, cioè dipendenti da un unico ideale o numero primo. I dati locali possono poi essere unificati per ottenere *risultati globali*. La decomposizione euleriana della funzione zeta ci dice che in essa concorrono fattori separati, ognuno dei quali dipende soltanto da un singolo numero primo; le informazioni aritmetiche globali che la funzione zeta codifica derivano dalla coesistenza e dall'interazione di tali fattori. Questo principio generale è detto *locale-globale.*

[136] Per ulteriori approfondimenti cfr. La Vallée Poussin 1896, Hadamard 1896, Viola 2019.

- *Il ruolo della funzione zeta nel teorema dei numeri primi.* Il teorema dei numeri primi (Hadamard, de La Vallée-Poussin, 1896) descrive il comportamento asintotico della funzione $\pi(x)$ che conta il numero di primi non superiori al numero reale x. Nella sua forma più debole, esso asserisce che $\pi(x)$ è asintoticamente equivalente a $\frac{x}{\ln(x)}$. La dimostrazione originaria utilizza l'analisi complessa e le proprietà della funzione zeta, in particolare il prodotto euleriano e il fatto che la funzione zeta non si annulli sulla retta verticale $Re(s) = 1$ del piano complesso. Alcuni matematici hanno deplorato l'uso dell'analisi complessa nella dimostrazione di un enunciato aritmetico, e nel 1948 Selberg e Erdos indipendentemente hanno presentato delle 'dimostrazioni elementari' del teorema. Il significato di 'elementare' è stato a sua volta contestato, in quanto le cosiddette dimostrazioni elementari sono molto più difficili di quelle che fanno ricorso all'analisi complessa. D'altra parte, nello stesso periodo Tate (1950) ha dimostrato proprietà analitico-complesse della funzione zeta e di alcune sue generalizzazioni utilizzando l'analisi di Fourier sul gruppo aritmetico degli *idèles.* Questo lavoro ha legato in un modo diverso aritmetica e analisi complessa, rivedendo entrambe in un ambiente più ricco e onnicomprensivo.

- La *congettura di Riemann.* La celebre congettura di Riemann afferma che la funzione zeta – o meglio il suo prolungamento analitico – non ha zeri sulla retta verticale $Re(s) = \frac{1}{2}$, che rappresenta in un certo senso l'asse di simmetria della funzione. A parte l'interesse intrinseco della congettura, essa è a sua volta alla base di molti risultati condizionali di estrema importanza per la teoria dei numeri riguardanti la distribuzione dei numeri primi, il tasso di crescita di funzioni aritmetiche e la complessità computazionale di algoritmi di primalità (ovvero test che stabiliscono se un numero dato è primo o meno) e di fattorizzazione.

- *I valori speciali*. I valori che la funzione zeta assume nei punti interi hanno un notevole significato aritmetico. Nel 1644 Pietro Mengoli aveva accennato alla determinazione della serie $\zeta(2) = \sum_{n=0}^{\infty} \frac{1}{n^2}$. Il risultato, successivamente noto in letteratura come *problema di Basel*, venne risolto nel 1734 da Euler, che provò che $\zeta(2) = \frac{\pi^2}{6}$. Più in generale, Euler fornì una formula per valutare la funzione zeta negli interi positivi pari

$$\zeta(2) = B_{2k} \frac{(-1)^{k+1}(2\pi)^{2k}}{2(2k)!}$$

dove B_k è il *k*-esimo numero di Bernoulli, definito da

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_k \frac{t^k}{k!}.$$

Meno noto ai non specialisti è il fatto che la funzione zeta di Riemann non è che un esempio, forse il più semplice, di una classe di funzioni complesse associate a diversi enti aritmetici e geometrici, di solito denotate con il nome di *funzioni L*, che codificano informazioni aritmetiche e geometriche. Le "buone" *funzioni L* hanno un prodotto euleriano che permette di separare fattori contenenti dati locali ai singoli primi, soddisfano equazioni funzionali e hanno valori speciali di significativo interesse. Queste particolari funzioni, attualmente associate a enti matematici di vario genere, hanno avuto una vitalità sorprendente: ad esempio, il già citato E. Artin formulò una congettura ancora oggi non dimostrata sulle *funzioni L* per una rappresentazione lineare di un gruppo di Galois. Inoltre, anche attualmente, tali funzioni sono ampiamente studiate in quanto è diffusa l'idea che esse portino in sé l'avatar dell'oggetto matematico cui sono associate, racchiudendone l'essenza.

È dunque significativo che Fubini includa nelle sue *Lezioni* la trattazione della funzione zeta di un campo di numeri. Oltre a costituire una generalizzazione della funzione zeta, che ammette un prodotto euleriano i cui fattori locali ai vari primi dipendono dal modo in cui i primi si decompongono, essa fornisce un interessante collegamento tra analisi e aritmetica, in quanto il numero di classe del campo è ricavabile come residuo della funzione zeta nella sua unica singolarità $s = 1$, coerentemente con il fatto che il campo razionale ha *class number* 1.

4. Guido Fubini negli anni Trenta

5. *Conclusioni*

Oltre a costituire un'importante traccia documentale di uno dei pochi corsi universitari di teoria dei numeri attivati in Italia nel primo Novecento, le *Lezioni* di Fubini consentono di documentare un aspetto assolutamente poco noto della sua biografia scientifica: la sua attività didattica in questo settore di studi.

Dalla loro analisi emerge con evidenza il talento di Fubini come docente e la "freschezza" del suo ingegno, ovvero la capacità di cogliere le linee di ricerca più promettenti coltivate dai colleghi stranieri,[137] di acquisirle molto rapidamente, anche a fronte di oggettive difficoltà di reperimento di testi e materiali bibliografici, e di saperle altrettanto prontamente integrare nel quadro degli insegnamenti superiori offerti agli studenti di Matematica dell'Università di Torino. Tenendo conto del fatto che questi ultimi, a differenza di quanto avviene oggigiorno, non possedevano quasi alcuna nozione sistematica di teoria algebrica dei numeri, la vastità degli argomenti affrontati da Fubini, la densità e la profondità dei concetti da lui introdotti risultano per certi versi sorprendenti.

Un ulteriore elemento di rilievo di queste *Lezioni* è rappresentato dal fatto che in esse Fubini approda a una sintesi armoniosa ed efficace di due tradizioni di pensiero distinte: quella italiana e quella tedesca. In tal senso, pur non avendo personalmente apportato contributi alla teoria dei numeri, a Fubini spetta il merito di aver coniugato - in modo originale - la teoria degli ideali e quella delle forme. Un filo conduttore di queste *Lezioni* può infatti essere individuato nello studio e nella classificazione delle forme quadratiche razionali a partire dalla teoria degli ideali. Più precisamente, nel suo insegnamento Fubini si propone di sviluppare in modo parallelo l'aritmetica dei campi di numeri e lo studio analitico-geometrico delle forme quadratiche fino a dimostrare, attraverso i risultati di Hilbert, la corrispondenza tra le due nozioni. È nel caso particolare dei campi quadratici che tale corrispondenza viene descritta in maggior dettaglio attraverso i noti risultati di riduzione. L'analisi interverrà per determinare il numero di forme equivalenti di discriminante dato, in quanto esso coincide con il *narrow class number*, che a sua volta è legato al residuo della funzione zeta del campo associato.

4. Guido Fubini con la moglie Anna Ghiron

[137] Quello che B. Segre definisce "il suo giudizio quasi infallibile su risultati futuri" (1954, p. 287).

Ringraziamenti

Siamo particolarmente grate al comitato scientifico del CSSUT che ha accolto questo volume nella collana *Lezioni e Inediti di "Maestri" dell'Ateneo Torinese*.

Un sentito grazie va alla direzione e al personale della Biblioteca Speciale di Matematica "G. Peano" dell'Università di Torino, a Paola Novaria (ASUT), Claudio Caschino (AsTo Poli), Franca Focacci (Biblioteca di Scienze matematiche, fisiche e geologiche dell'Università di Perugia) e Erica Mosner (Archive of Institute for Advanced Study, Princeton) che in vario modo hanno facilitato le nostre ricerche archivistiche e bibliografiche.

Esprimiamo la massima gratitudine a David Fubini e a Laurie Fubini Jacobs che ci hanno gentilmente messo a disposizione documenti inediti e che ci hanno concesso di riprodurre alcune fotografie di Guido Fubini custodite nel loro archivio famigliare.

Grazie ai *referees* per i loro preziosi suggerimenti e agli amici e colleghi Aldo Brigaglia, Livia Giacardi, Catherine Goldstein, Paolo Valabrega e Carlo Viola che ci hanno aiutato con indicazioni e scambi di opinione e che hanno accettato di leggere le versioni preliminari del lavoro.

Un grazie particolare a Clara Silvia Roero per l'attenta rilettura del manoscritto e per la preziosa collaborazione all'*editing* del volume.

R. UNIVERSITÀ DI TORINO

M. III. 76.

LEZIONI

DI

TEORIA DEI NUMERI

DEL PROF. FUBINI

Anno Accademico 1916-17

Dattilo - Litografia
A. VIRETTO
TORINO
Corso Valentino, 23

6. Esemplare delle Lezioni di Teoria dei numeri in BSM, Università di Torino

Appendice – I corsi di Teoria dei numeri in Italia[138]

a.a.	Argomenti del corso di Analisi superiore di Fubini	Altre Università italiane	Docente	Programma
1910/11	Mancante	Napoli	G. Torelli	Teoria analitica dei numeri
		Padova	P. Gazzaniga	Teoria dei numeri
1911/12	Teoria delle equazioni alle derivate parziali sia nel campo reale che in quello complesso; problemi al contorno di Cauchy	Bologna	U. Scarpis	Gruppi di operazioni e loro applicazione alla teoria dei numeri
		Napoli	G. Torelli	Teoria analitica dei numeri
		Padova	P. Gazzaniga	Teoria dei numeri
		Pisa	L. Bianchi	Teoria aritmetica delle forme quadratiche; aritmetica analitica
1912/13	Geometria euclidea e non euclidea; partizioni congruenti del piano e dello spazio; funzioni di variabile complessa; funzioni automorfe	Padova	P. Gazzaniga	Teoria dei numeri
1913/14	Equazioni differenziali ordinarie, risultati classici e recenti	Bologna	F. Enriques	Teoria delle funzioni algebriche
		Padova	P. Gazzaniga	Teoria dei numeri
1914/15	Calcolo delle variazioni; serie di Fourier	Padova	P. Gazzaniga	Teoria dei numeri
1915/16	I moderni avanzamenti del calcolo; applicazione all'espansione in serie, al calcolo delle variazioni	Padova	P. Gazzaniga	Teoria dei numeri
		Pavia	E. Bompiani	Geometria dei numeri; approssimazione diofantea
1916/17	Numeri di Cantor; numeri interi e algebrici; teoria dei numeri e delle forme con applicazioni algebriche; applicazioni dell'analisi alla teoria dei numeri	Catania	G. Scorza	Funzioni abeliane con applicazioni geometriche
		Padova	P. Gazzaniga	Teoria dei numeri
		Pavia	L. Berzolari	Teoria generale delle forme algebriche con applicazioni geometriche

[138] Questi dati sono stati desunti dal *Bulletin of the American Mathematical Society* e da *L'Enseignement mathématique*. In relazione all'a.a. 1922/23 non sono state reperite informazioni sui corsi di teoria dei numeri offerti nelle Università italiane.

a.a.	Argomenti del corso di Analisi superiore di Fubini	Altre Università italiane	Docente	Programma
1917/18	Funzioni abeliane, ellittiche e modulari	Catania	M. Cipolla	Teoria dei numeri nel campo razionale e in qualsiasi campo quadratico; argomenti classici dell'aritmetica asintotica
1918/19	Funzioni modulari, automorfe, fuchsiane; equazioni differenziali lineari a coefficienti razionali	Padova	P. Gazzaniga	Teoria dei numeri
		Roma	G. Castelnuovo	Equazioni algebriche e gruppi di sostituzioni
1919/20	Mancante	Padova	P. Gazzaniga	Teoria dei numeri
1920/21	Geometria differenziale e gruppi continui con particolare riferimento ai gruppi di moti e di trasformazioni proiettive e conformi	Catania	M. Cipolla	Teoria dei gruppi finiti ordinati con applicazioni
		Padova	P. Gazzaniga	Teoria dei numeri
		Pisa	L. Bianchi	Funzioni di variabile complessa; numeri algebrici e aritmetica analitica
1921/22	Le equazioni differenziali e i vari tipi di sviluppi in serie che si presentano nella fisica matematica	Catania	M. Cipolla	Sostituzioni lineari e gruppi
		Padova	P. Gazzaniga	Teoria dei numeri
		Roma	A. Perna	Equazioni algebriche
1923/24	Mancante	Catania	M. Cipolla	Applicazioni geometriche della teoria dei gruppi d'ordine finito
		Roma	A. Perna	Mancante
1924/25	Geometria proiettivo differenziale			
1925/26	Mancante	Catania	G. Andreoli	Teoria delle forme binarie: accenni alle forme ternarie

a.a.	**Argomenti del corso di Analisi superiore di Fubini**	**Altre Università italiane**	**Docente**	**Programma**
1926/27	Equazioni differenziali alle derivate ordinarie e parziali	Bologna	E. Bortolotti	Numeri reali, algebrici, trascendenti; aritmetica delle forme quadratiche
		Milano	O. Chisini	Teoria generale dei gruppi finiti di operazioni; equazioni algebriche e loro risoluzione
		Palermo	G. Mignosi	Elementi di teoria dei numeri con applicazioni
1927/28	Teoria dei gruppi con particolare riguardo alla teoria dei gruppi continui	Cagliari	G. Madia	Fondamenti di teoria dei numeri e di geometria
1928/29	Capitoli scelti di analisi con speciale riguardo alle applicazioni alla fisica	Palermo	G. Mignosi	La teoria di Galois e i problemi geometrici risolubili con riga e compasso
		Pavia	L. Berzolari	Forme algebriche e applicazioni alla geometria
1929/30	Equazioni differenziali; loro applicazioni alla geometria differenziale metrica e proiettiva	Milano	G. Belardinelli	La teoria di Galois e la risoluzione algebrica delle equazioni
1930/31	Funzioni analitiche con particolare riguardo alle funzioni fuchsiane e ipergeometriche	Bologna	B. Levi	Argomenti scelti di algebra e teoria dei numeri
		Genova	A.M. Bedarida	Aritmetica analitica
		Milano	G. Belardinelli	Teoria delle equazioni algebriche secondo Galois
		Roma	A. Perna	Teoria dei numeri
1931/32	Teoria dei numeri e dei numeri algebrici; relazione colla teoria di Galois delle equazioni algebriche	Catania	P. Nalli	Teoria dei numeri
		Milano	G. Belardinelli	Teoria dei numeri; risoluzione delle equazioni algebriche secondo Galois

a.a.	Argomenti del corso di Analisi superiore di Fubini	Altre Università italiane	Docente	Programma
1932/33	Funzioni analitiche: in particolare funzioni ipergeometriche; funzioni trigonometriche, sferiche, di Bessel, di Lamé, ellittiche	Milano	U. Cassina	Logica matematica; fondamenti dell'aritmetica e dell'analisi; introduzione alla teoria dei numeri
		Palermo	M. Cipolla	Calcolo delle variazioni; equazioni algebriche secondo Galois
1933/34	Equazioni a derivate parziali; teoria di S. Lie; invarianti integrali e problema di Pfaff	Palermo	M. Cipolla	Equazioni algebriche in un corpo finito
1934/35	Funzioni analitiche, abeliane, ellittiche, modulari, automorfe	Bologna	B. Levi	Algebra e teoria dei numeri
		Catania	G. Aprile	Corpi numerici e algebre
		Palermo	G. Mignosi	Corpi numerici e algebre
1935/36	Analisi complessa; funzioni analitiche, di Bessel, ellittiche; equazioni differenziali; serie	Bologna	E. Bortolotti	Teoria dei numeri; gruppi di sostituzioni ed equazioni algebriche
		Pisa	G. Ricci	Teoria dei numeri e degli insiemi; gruppi ed equazioni algebriche secondo Galois
		Palermo	M. Cipolla	Teoria analitica dei numeri
1936/37	Equazioni differenziali; serie e integrale di Fourier; applicazioni alla fisica			
1937/38	Analisi complessa; funzioni analitiche, ellittiche, di Jacobi; teoria algebrica delle forme; la rete modulare e l'analisi indeterminata			

Guido Fubini

Lezioni di Teoria dei numeri

1916-17

Infatti, se tale determinante fosse nullo, sarebbe, come si riconosce sviluppandolo:

$$\frac{\log|\varepsilon_1|}{\log|\varepsilon_2|} = \frac{\log|\varepsilon_1'|}{\log|\varepsilon_2'|}$$

Ora $\log|\varepsilon_i''| = -\log|\varepsilon_i| - \log|\varepsilon_i'|$ perchè $\mathrm{Nm}\,\varepsilon_i = 0$. Se ne deduce che, detto ρ il valore dei precedenti rapporti, sarebbe anche $\frac{\log|\varepsilon_1''|}{\log|\varepsilon_2''|} = \rho$, cosicchè sarebbe $|\varepsilon_1| = |\varepsilon_2|^\rho$, $|\varepsilon_1'| = |\varepsilon_2'|^\rho$, $|\varepsilon_1''| = |\varepsilon_2''|^\rho$. Essendo $|\varepsilon_1'| > 1$, $|\varepsilon_2'| < 1$, sarebbe pertanto $\rho < 0$, ciò che è assurdo perchè $|\varepsilon_1| < 1$, $|\varepsilon_2| < 1$.

Dunque le equazioni precedenti determinano le X, Y, e pertanto anche un punto nel piano π ove X, Y sono coordinate cartesiane. Io dico che questi punti formano una rete. Infatti, se X, Y, corrispondono all'unità σ, e ξ, η ad un'altra unità τ, la coppia $X+\xi, Y+\eta$ corrisponde al numero $\sigma\tau$, che è pure un'unità. Di più i punti (X, Y) non possono essere tutti sulla stessa retta; perchè tra essi vi sono i punti $(0,0), (0,1), (1,0)$. Infine, in una regione finita di π vi è un <u>numero finito</u> di tali punti, e ciò perchè, se sono dati limiti superiori delle X, Y, sono contemporaneamente dati li-

7. Guido Fubini, Lezioni di Teoria dei numeri 1916-17, p. 226

CRITERI DELL'EDIZIONE CRITICA

Il testo litografato *Lezioni di Teoria dei numeri* di Guido Fubini, risalente all'anno accademico 1916/1917, consta di 24 dispense per un totale di 397 pagine. Si tratta di un manoscritto non autografo in pulito, con Errata corrige di altra mano. La maggior parte delle correzioni segnalate nell'Errata corrige al termine del libro è anche sovrascritta a matita sul testo.

Al momento siamo al corrente dell'esistenza di tre esemplari di queste litografie: il primo è custodito presso la BSM (collocazione M.III.76) ed è la copia che, depositata il 24 giugno 1917, poco dopo la conclusione del corso di Fubini, fu messa a disposizione degli studenti.[1]

Il secondo esemplare, donato da Fubini al collega e amico A. Terracini, faceva parte della biblioteca personale di quest'ultimo; oggi è conservato presso la Biblioteca di Scienze matematiche, fisiche e geologiche (SMFG) dell'Università di Perugia (collocazione 11-XX/1917/1), che acquisì il patrimonio librario di Terracini dopo la sua scomparsa nel 1968. L'esemplare di Perugia è l'unico sul quale compare, in copertina, la dicitura dello studente Salvatore Lupica[2] che curò la compilazione degli appunti. La terza copia è depositata nella Biblioteca del Distretto tecnologico – sezione di Matematica e Informatica – dell'Università di Cagliari.

L'edizione critica è stata condotta sulla copia posseduta dalla BSM di Torino. Il testo originale è stato restituito con fedeltà, salvo una modifica a carico delle carte 3 e 4, che in fase di rilegatura erano state invertite.

L'ortografia, la terminologia e le notazioni sono state ovunque rispettate, con la sola eccezione del fattoriale, che Fubini indicava con la notazione  e che è stato invece qui reso con il segno moderno $p!$. Per ragioni di chiarezza, è inoltre parso opportuno normalizzare la punteggiatura in accordo al sistema di scrittura corrente, sia per quanto riguarda il testo sia per quanto attiene i segni di interpunzione nelle formule matematiche.

Le note contrassegnate con (*) sono dovute all'autore, che spesso le inserisce a piè di pagina con rinvio nel testo. Per una maggiore fruibilità da parte del lettore, tali note sono state da noi inserite al termine della sezione corrispondente e segnalate con (*) **Nota**.

Le parole sottolineate sono riportate come da originale, mentre le variabili nelle formule sono rese con il corsivo. Le parentesi all'interno del testo sono dovute all'autore.

Lo scioglimento delle abbreviazioni, segnalato tra partentesi quadre, è delle curatrici. La fine di pagina dell'originale è indicata con //.

---

[1] La copia presenta infatti segni di utilizzo di diverse mani. A titolo di curiosità si segnala che questa copia delle *Lezioni* di Fubini fu chiesta dal Liceo ginnasio governativo "M. Cutelli" di Catania nel luglio del 1948. L'esemplare rientrò in biblioteca a fine agosto dello stesso anno. Cfr. S. Chiarenza [preside] a F. Tricomi [direttore della BSM], Catania 22.7.1948, Registro della corrispondenza della Biblioteca Universitaria di Matematica (n° d'ordine 265).

[2] Nato a S. Agata di Militello (Messina) il 20 aprile 1891, Salvatore Lupica si immatricola a Torino il 30 novembre 1916, provenendo dall'Università di Palermo. A Torino segue il corso di Analisi superiore negli a.a. 1916-17 e 1917-18 con esiti non soddisfacenti, venendo due volte respinto all'esame (11 luglio e 20 novembre 1918). Si trasferisce infine all'università di Pavia nel settembre 1919. Cfr. ASUT, *Registri di carriera scolastica*, 45-278, n. 1978.

Abbreviazioni nelle note delle curatrici

a.m.	altra mano, *alia manu*
ad. post.	aggiunta posteriore
ad. sup.	aggiunta sovrascritta
cor. inf.	correzione infrascritta
cor. sup.	correzione sovrascritta
del.	cancellatura, *delevit*
e.c.	*errata corrige*
N.d.A.	*Nota dell'Autore*
N.d.C.	*Nota del Curatore*
p.d.p.	*piè di pagina*

Capitolo I - Introduzione

§.1 *L'algoritmo di Euclide per il massimo comun divisore (M.C.D.)*[1]

Dati due interi positivi o negativi a, b dividere a per b significa trovare due interi q (quoziente) e r (resto) tali che

$$a = bq + r$$

e che sia soddisfatta inoltre qualche ulteriore condizione che permetta di definire completamente q, r; quale ulteriore condizione nel caso di a, b interi positivi si assume di solito la seguente: "che q, r siano anch'essi interi positivi e che r sia inferiore a b". E con altre condizioni analoghe si potrebbero, volendo, determinare q, r anche quando a, b non sono entrambi positivi.[2]

Se r si può assumere nullo, dicesi che a è divisibile per b (è multiplo di b)[3]. Se a è divisibile per b, e anche b è divisibile per a, dicesi che a, b sono associati; in tal caso il loro quoziente $\varepsilon = \frac{b}{a}$ è[4] // intero insieme a $\frac{1}{\varepsilon}$. Un tal numero[5] r si chiama una unità. Di unità nel nostro caso vi sono soltanto i numeri ± 1.

Supponiamo a, b positivi; esiste un numero intero positivo c, che se ne chiama il M.C.D.[6] Esso gode di queste due proprietà:

α) Esso è divisore di a, b.

β) Ogni divisore comune di a, b è divisore anche di c.

Se prescindiamo dall'ipotesi restrittiva che a, b, c siano positivi, le proprietà α), β) definiscono c a meno del segno (e ciò perché nella teoria della divisibilità numeri associati debbansi considerare come equivalenti).

Supposti di nuovo a, b, c positivi, il M.C.D. c si determina, come è noto, con successive divisioni[7]. Posto:

$a = bq_1 + r_1$, (q_1 ed r_1 sono quoz. e resto ottenuti dividendo a per b)

$b = r_1 q_2 + r_2$, (q_2, r_2 sono quoz. e resto ottenuti dividendo b per r_1 , ecc.)

---

[1] Euclide, *Elementi*, Lib. VII, prop. 2. Cfr. anche Gauss 1801, sez. II, p. 14 Si tratta del celebre algoritmo di Euclide per determinare il massimo comun divisore tra due numeri interi, uno dei più antichi algoritmi conosciuti, risalente al III sec. a.C.; esso infatti è stato illustrato per la prima volta negli *Elementi* di Euclide anche se probabilmente era già conosciuto da circa 200 anni nell'ambito della matematica greca arcaica.

[2] Gazzaniga 1903, cap. I, p. 3. La notazione adottata da Gazzaniga è del tutto analoga a quella utilizzata da Fubini: $m = n.q + r, |r| < n$: 2. Paolo Gazzaniga (Soresina, 26 luglio 1853 – Venezia, 18 ottobre 1930), docente e matematico italiano che tenne un corso universitario interamente dedicato alla teoria dei numeri in maniera continuativa – dal 1885 al 1921 – presso l'Università di Padova.

[33] *Ibid.* A differenza di Fubini Gazzaniga definisce i multipli di n come i numeri della serie
$\ldots -3.n, -2.n, -n, 0, 2-n, 3.n, \ldots$

[4] Il testo è rilegato in modo scorretto: la p. 4 precede l'inizio dei primo capitolo.

[5] *e.c.*: invece di r leggasi ε.

[6] Gazzaniga 1903, cap. I, p. 5. Gazzaniga enuncia qui una serie di proprietà del M.C.D. (per lo più proposizioni tratte dagli *Elementi* di Euclide) senza esporre l'algoritmo per determinare il M.C.D.

[7] Dirichlet 1877 (trad. 1881), cap. II, §23, p. 43-47. È singolare il fatto che il matematico tedesco non tratti l'algoritmo di Euclide immediatamente dopo aver fornito la definizione di M.C.D. ma inserisca questo argomento successivamente, solo all'interno del secondo capitolo, quando è necessario per trovare le radici dell'equazione diofantea di primo grado. Cfr. anche Sommer 1907 (trad. 1911), cap. 1, §1, p. 2.

$r_1 = r_2 q_3 + r_3,$
… … … … … … …
$r_{m-1} = r_m q_{m+1} + r_{m+1}$

i resti successivi vanno decrescendo; se r_{m+1} è il primo // resto nullo, il precedente r_m (che coincide con[8] $r_0 =$, se $r_1 = 0$) è il M.C.D. c di a, b.
Si noti che

$$r_1 = ax_1 + by_1; \text{ dove } x_1 = 1, y_1 = -q_1$$
$$r_2 = b - r_1 q_2 = b - (ax_1 + by_1)q_2 = ax_2 + by_2 \text{ dove } x_2 = -x_1[9], y_2 = 1 - y_1 q_2$$

ecc.

$$c = r_m = ax_m + by_m$$

dove x_m e y_m sono numeri interi, positivi o negativi che è facile determinare successivamente nel modo qui esposto. Posto $x = x_m$ e $y = y_m$ è

$$c = ax + by \qquad (1).$$

Il M.C.D. di due interi a, b è uguale ad una forma lineare $ax + by$ dove x, y sono interi. Questo teorema, come è facile provare, vale anche se a, b, c sono di segno qualsiasi. (Il segno di c si può prefissare ad arbitrario, cambiando i segni di x, y in (1) dal numero c si passa al numero $-c$).

Se a, b sono primi tra di loro ($c = \pm 1$) è dunque risolubile in numeri interi x, y l'equazione

$$ax + by = 1 \qquad (2).$$

E viceversa, se la (2) è risolubile in numeri interi, i numeri a, b sono primi tra loro. [Infatti da (2) segue che un divisore comune di a, b divide anche 1, cioè // non può essere distinto da ± 1].

Esercizi

1) Risolvere la (1) dando ad a, b valori interi particolari anche negativi.
2) Qual è la soluzione più generale (x, y) di (2) in numeri interi?
   (se x_1, y_1 è una soluzione particolare, deve essere $a(x - x_1) + b(y - y_1) = 0$ e quindi
   $y - y_1 = -ha, x - x_1 = hb$ con h intero qualsiasi).

Tutta la teoria dei numeri primi si basa sul teorema: se a, b, l sono numeri interi, se a, b sono primi tra loro, se al è divisibile per b, allora l è divisibile per b. Infatti, moltiplicando (2) per l si trae:

$$alx + bly = l.$$

Poiché per ipotesi la è divisibile per b, il primo membro, e quindi anche il secondo l è divisibile per b.

c.d.d.

Se ne deduce poi: Ogni intero è decomponibile in uno e in un solo modo in fattori primi[10] [purché non si considerino come distinte due decomposizioni, se i fattori di una sono ordinatamente associati ai fattori dell'altra come p. es. $21 = 3 \cdot 7$ e $21 = (-3)(-7)$].

[8] *e.c.*: invece di $r_0 =$ leggasi $r_0 = b$.
[9] *e.c.*: invece di $x_2 = -x_1$ leggasi $x_2 = -x_1 q_2$.
[10] Dirichlet 1877 (trad. 1881), cap. I, §11, p. 12. Qui Dirichlet dimostra il 'teorema fondamentale' il cui enunciato è il seguente: "ogni numero composto può sempre ed in modo unico essere rappresentato quale prodotto di un

§.2 ***Campi oloidi***

I numeri interi formano un campo oloide: perché la somma, la differenza, il prodotto di due interi // è ancora un intero. Altri esempi di campi oloidi sono i campi formati dai polinomi[11] in una o più variabili, p. es.

1) il campo (la classe) dei polinomi $P(x)$ in una variabile x a coefficienti reali e complessi qualsiasi
2) il campo dei polinomi $P(x)$ a coefficienti reali qualsiasi
3) il campo dei polinomi $P(x)$ a coefficienti razionali.[12]

Anche in questi campi si può definire in modo univoco la divisione, imponendo al resto di essere di grado inferiore al divisore. E, come è noto dall'algebra, se ne deduce la validità dell'algoritmo di Euclide per la ricerca del M.C.D. di due polinomi $A(x), B(x)$, cioè di quel polinomio $C(x)$ che è divisore comune di $A(x), B(x)$ e che è divisibile per ogni divisore di[13] $A(x), B(x)$.

Senza generalizzare tutte le precedenti considerazioni, osserveremo soltanto che da definizioni analoghe a quelle del §1 si deduce:
Due polinomi sono associati[14] (ciascuno di essi è cioè divisibile per l'altro) soltanto se il loro quoziente è una costante (polinomio di grado zero) appartenente al campo considerato (cioè reale nel 2° caso, razionale nel 3° caso), cioè le unità dei nostri campi sono le costanti (qualsiasi) // dei campi stessi. Il M.C.D. di due polinomi è determinato appunto a meno di un fattore unità, ecc. Se io chiamo primo[15] un polinomio $P(x)$ di uno dei nostri campi che sia divisibile soltanto per se stesso (e per i polinomi associati) e per le unità, troviamo che anche nei nostri campi vale il teorema che ogni polinomio si può decomporre in uno e in un solo modo in polinomi primi (quando naturalmente non si considerino distinte due decomposizioni, se i fattori della prima sono ordinatamente associati ai fattori dell'altra). Quali sono tali fattori primi? Nel primo campo per il teorema (di D'Alembert[16] e Gauss) fondamentale dell'algebra[17] troviamo che sono primi i polinomi di primo grado a coefficienti qualsiasi. Nel secondo dei campi citati si ricordi che un'equazione $P(x) = 0$ a coefficienti reali, che abbia una radice complessa α, ha anche la radice α_0 complessa coniugata, cosicché i fattori $(x - \alpha)$ e $(x - \alpha_0)$ corrispondenti hanno un prodotto $x^2 + px + q$ a coefficienti p, q reali. (Ricordo che le radici α e α_0 hanno ugual

numero finito di primi". Si tratta della classica dimostrazione di Euclide. Cfr. anche Gauss 1801, sez. II, p. 14, 15 Cfr. infine Sommer 1907 (trad. 1911), cap. 1, §1, p. 3, *théorème fondamental*.

[11] Weber 1895, vol. I, p. 24; sono qui introdotte la moltiplicazione e la divisibilità tra polinomi.

[12] Bianchi 1920-21, cap. I, §8, p. 50, 51. A differenza di Bianchi, Fubini introduce il campo dei polinomi a coefficienti razionali all'interno della classe più generale dei campi oloidi.

[13] Ibidem. Qui Bianchi sviluppa in modo approfondito l'algoritmo di Euclide per i polinomi e le proprietà di divisibilità, cosa che Fubini invece ha già fatto per i numeri interi al §1.

[14] Nelle opere di Bianchi e di Gazzaniga non compare la definizione di polinomi associati.

[15] Bianchi 1920-21, cap. I, §8, p. 52: "Se il massimo comun divisore $d(x)$ di due polinomi $f(x), \varphi(x)$ è una costante (un numero razionale) i due polinomi $f(x), \varphi(x)$ diconsi primi tra loro".

[16] D'Alembert tentò per primo di dimostrare il teorema fondamentale dell'algebra nel 1746, utilizzando però una proprietà non ancora dimostrata; tale risultato fu poi pubblicato nell'opera *Traité de dynamique* (1758). Gauss fu il primo a dimostrare rigorosamente il teorema fondamentale dell'algebra nel 1799, nella sua tesi di dottorato *Una nuova dimostrazione del teorema per il quale ogni funzione algebrica integrale di una variabile può essere risolta in fattori di primo o secondo grado*. Sulle questioni di priorità relative a questo celebre risultato cfr. Dhombres, Alvarez 2011 e 2013.

[17] Il teorema fondamentale dell'algebra, enunciato da Albert Girard nell'opera *L'invention en algebre* (1629) afferma: "ogni polinomio a coefficienti reali o complessi, di grado maggiore o uguale a 1, ammette almeno una radice complessa".

ordine di molteplicità). Dunque, siccome nel secondo dei campi citati si devono escludere i polinomi a coefficienti complessi, i polinomi da considerarsi come primi saranno: //

a) i polinomi di primo grado a coefficienti reali,
b) i polinomi di secondo grado a coefficienti reali che uguagliati a zero danno un'equazione priva di radici reali.

Più complicato è lo studio del terzo caso. Un polinomio $P(x)$ a coefficienti razionali, che si debba riguardare come primo, è un polinomio che non si può scrivere sotto forma di prodotto $P_1(x)P_2(x)$ di due polinomi non costanti a coefficienti razionali. Tali polinomi (per la cui decomposizione in fattori si deve necessariamente ricorrere a quantità irrazionali e complesse) diconsi comunemente irriducibili[18]. Noi vogliamo dare un metodo per decomporre un polinomio $P(x)$ (a coefficienti razionali) in fattori a coefficienti razionali (se possibile) o per riconoscere quando ciò è impossibile, cioè quando $P(x)$ è irriducibile. Sono perfettamente equivalenti i problemi della decomposizione in fattori di un polinomio $P(x)$ a coefficienti razionali, o di un polinomio $KP(x)$ associato a coefficienti interi [si può p. es. porre K uguale al minimo multiplo comune dei denominatori dei coefficienti di $P(x)$].
Un polinomio $P(x)$ a coefficienti interi dicesi primitivo[19], se i suoi coefficienti sono primi tra loro. //

Lemma 1° (di Gauss[20]). Se $A(x), B(x), C(x)$ sono polinomi a coefficienti interi, se $A(x) = B(x)C(x)$, se $B(x), C(x)$ sono primitivi, anche $A(x)$ è primitivo.

Infatti sia

$$B(x) = b_0x^n + b_1x^{n-1} + b_2x^{n-2} + \cdots b_n,$$
$$C(x) = c_0x^m + c_1x^{m-1} + c_2x^{m-2} + \cdots c_m,$$

sarà

$$A(x) = a_0x^{m+n} + a_1x^{m+n-1} + a_2x^{m+n-2} + \cdots a_{m+n}$$

dove:

$a_0 = b_0c_0$ (1)
$a_1 = b_0c_1 + b_1c_0$ (2)
$a_2 = b_0c_2 + b_1c_1 + b_2c_0$ (3)
$a_3 = b_0c_3 + b_1c_2 + b_2c_1 + b_3c_0$ (4)
……

Se $A(x)$ non è primitivo, esiste almeno un numero primo p, per cui sono divisibili $a_0, a_1, a_2, a_3, \ldots$ Siccome $B(x)$ è primitivo, non tutte le $b_0, b_1, b_2, \ldots$ sono divisibili per p. Sia p. es. b_2 la prima di esse non divisibile per p. Essendo le a divisibili per p, e altrettanto avvenendo per b_0, b_1, dalla (3) si deduce che $b_2c_0 = a_2 - b_0c_2 - b_1c_1$ è divisibile per p; non essendo b_2 multiplo di p, sarà c_0 divisibile per p. Dalla (4) essendo a_3, b_0, b_1, c_0 multipli di p si deduce // che b_2c_1 è multiplo di p. Così continuando si trova che tutte le $c_0, c_1, c_2 \ldots$ sono divisibili per p, cosicchè $C(x)$ non sarebbe primitivo.

[18] Bianchi 1920-21, cap. I, §8, p. 52: "Un polinomio $f(x)$ si dice riducibile se può decomporsi nel prodotto di due effettivi polinomi $f_1(x), f_2(x)$ (non costanti) $f(x) = f_1(x)f_2(x)$; altrimenti si dirà irriducibile".
[19] *Idem*, cap. I, §8, p. 54.
[20] Gauss 1801, sez. I, p. 11, 12.

Cor.[ollario]) Se A, B, C sono polinomi a coefficienti interi tali che

$$A(x) = B(x)C(x)$$

se β è il M.C.D. dei coefficienti di B, se γ è il M.C.D. dei coefficienti di C, allora $\alpha = \beta\gamma$ è il M.C.D. dei coefficienti di A.

Infatti

$$\frac{B(x)}{\beta} \qquad \frac{C(x)}{\gamma}$$

sono primitivi; quindi $\frac{1}{\beta\gamma}B(x)C(x) = \frac{1}{\beta\gamma}A(x)$ è primitivo; perciò $\beta\gamma$ è il M.C.D. dei coefficienti di $A(x)$.

Cor.[ollario]) Se $A(x)$ è un polinomio riducibile a coefficienti interi, si può supporre che i suoi fattori siano a coefficienti interi (mutando caso mai tali fattori in polinomi associati). Cioè, se $A(x) = B(x)C(x)$, dove B, C sono a coefficienti razionali, si può trovare un numero razionale K tale che $KB(x)$, $\frac{1}{K}C(x)$ siano a coeffi//cienti interi, pur essendo naturalmente $A(x) = KB(x)\frac{1}{K}C(x)$. Sia β_1 il minimo comune multiplo dei denominatori dei coefficienti di $B(x)$; allora $\beta_1 B(x)$ avrà coefficienti interi, di cui sia β_2 il M.C.D. Allora $\frac{\beta_1}{\beta_2}B(x)$ sarà un polinomio primitivo a coefficienti interi.

Definiamo analogamente gli interi γ_1, γ_2 per $C(x)$. Sarà

$$A(x) = B(x)C(x)$$
$$\frac{\beta_1}{\beta_2}\frac{\gamma_1}{\gamma_2}A(x) = \left[\frac{\beta_1}{\beta_2}B(x)\right]\left[\frac{\gamma_1}{\gamma_2}C(x)\right].$$

Essendo $\frac{\beta_1}{\beta_2}B(x)$ e $\frac{\gamma_1}{\gamma_2}C(x)$ primitivi, anche $\frac{\beta_1}{\beta_2}\frac{\gamma_1}{\gamma_2}A(x)$ sarà un polinomio a coefficienti interi primitivi $M(x)$.
Dunque, essendo anche $A(x) = \frac{\beta_1}{\beta_2}\frac{\gamma_1}{\gamma_2}M(x)$ a coefficienti interi, il numero $\frac{\beta_1}{\beta_2}\frac{\gamma_1}{\gamma_2}$ sarà un intero K.
E quindi p. es.

$$A(x) = \left[K\frac{\beta_1}{\beta_2}B(x)\right]\left[\frac{\gamma_1}{\gamma_2}C(x)\right]$$, dove i fattori sono a coefficienti interi.

Dunque:
Per trovare gli eventuali fattori (a coefficienti razionali) di un polinomio $P(x)$ a coefficienti razionali, basta trovare i fattori a coefficienti interi di un polinomio $A(x)$ [associato a $P(x)$], i cui coefficienti siano pure interi. Troviamo i fattori di n-esimo grado di $A(x)$. Siano $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n, \alpha_{n+1}$ «$n+1$» numeri interi qualsiasi; se[21] (x) è un polinomio di grado n, esso // sarà determinato dai valori $\beta_1, \beta_2, \beta_3, \ldots, \beta_n, \beta_{n+1}$, che assume ordinatamente nei punti precedenti, cioè coinciderà (Lagrange[22]) col polinomio seguente, che per $x = \alpha_i$ assume proprio il valore β_i (*)

[21] *e.c.*: invece di (x) leggasi $B(x)$.
[22] Lagrange 1797, nota X *Sur la decomposition des polynomes d'un degré quelconque en facteurs réels*, p. 202-229.

$$\sum_{1}^{n+1} \beta_i \frac{(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_{n+1})}{(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_{n+1})}.$$

Fissiamo i punti $\underline{\alpha}$, e non cambiamoli più. Se $B(x)$ ha coefficienti interi, ed è un fattore di $A(x)$ allora β_i non si può scegliere a piacere ma bensì tra i divisori del valore $A(\alpha_i)$ che $A(x)$ ha per $x = \alpha_i$. Il polinomio (5) si può dunque scegliere soltanto in un numero finito di modi. Affinché uno dei polinomi, che così si determineranno, sia uno dei fattori cercati, bisognerà in più che esso sia a coefficienti interi e sia un fattore di $A(x)$. Se per nessuno di essi queste condizioni sono soddisfatte, allora ciò significa che $A(x)$ non possiede fattori di grado n.

Oss.[ervazione] Per trovare tutti i fattori di $A(x)$ si cominciano a cercare gli eventuali fattori di primo grado. Diviso $A(x)$ per tali fattori, si cercheranno gli eventuali fattori di secondo grado del quoziente $A_1(x)$. Diviso $A_1(x)$ per tali // fattori di secondo grado (se ce ne sono) si cercheranno i fattori di terzo grado del quoziente, e così via.

(*) **Nota**: Per $n = 2$, il polinomio sarebbe

$$\beta_1 \frac{(x-\alpha_2)(x-\alpha_3)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} + \beta_2 \frac{(x-\alpha_1)(x-\alpha_3)}{(\alpha_2-\alpha_1)(\alpha_1-\alpha_3)} + \beta_3 \frac{(x-\alpha_3)(x-\alpha_1)}{(\alpha_3-\alpha_2)(\alpha_3-\alpha_1)}.$$

§.3 ***Moduli e ideali***

Si dice modulo un insieme M di enti tali che la somma o la differenza di due enti in M, distinti o no, è ancora un ente in M.[23]
Sia M un modulo di numeri reali. Se in M esiste un numero K_0 che sia il più piccolo di tutti in valore assoluto, allora M è la classe formata dai multipli di K.

Insieme a K esistono in M per definizione di modulo anche i numeri $K, K+K = 2K, 2K+K = 3K$, ecc. cioè i multipli di K. Contenga M , se possibile, un altro numero H da quelli distinto. Allora H sarà compreso tra due multipli

$$nK, (n+1)K \qquad (n \text{ intero})$$

consecutivi di K. Dunque

$$L = H - nK$$

(in valore assoluto) è minore di K. Ma L , differenza di due numeri in M, è ancora un numero di M, che in valore assoluto è minore di K. Ciò contraddice alla ipotesi. Dunque M, come si d.d., contiene tutti e // soli i multipli di K.

Se M è un modulo di numeri interi, esso è formato da tutti e soli i multipli di un intero K (e ciò poiché in una classe M qualsiasi di numeri interi ve ne è certamente uno che ha il più piccolo valore assoluto).
Evidentemente se $a_1, a_2, \dots, a_n$ sono interi, i loro multipli comuni formano un modulo M (perché la somma o la differenza di due multipli di a_i è ancora multiplo di a_i). Dunque esiste

[23] Dirichlet 1877 (trad. 1881), suppl. XI, §165, p. 468. Dedekind, curatore delle *Vorlesungen* di Dirichlet e autore della loro appendice, parlando dei moduli all'interno dell'ultimo supplemento, scrive: "Un sistema α di numeri reali o complessi, algebrici o trascendenti, si dice un modulo, se essi si riproducono mediante addizione e sottrazione, cioè se le somme e le differenze di due qualsivogliano di codesti numeri appartengono al medesimo sistema α."

un intero K, i cui multipli sono tutti e soli i multipli comuni di $a_1, a_2, \dots, a_n$. Questo numero K è il minimo comune multiplo dei numeri dati.
Ecco dunque provato che: I multipli comuni di più numeri interi $a_1, a_2, \dots, a_n$ sono i multipli del loro minimo comune multiplo K.

Il modulo M che abbiamo testè definito si indica con $[a_1, a_2, \dots, a_n]$ (con parentesi quadre). Molte volte qui, come in altri casi, si considerano come equivalenti un tale modulo, e il numero K che coi suoi multipli lo genera completamente.
Siano $a_1, a_2, \dots, a_n$ interi dati. Siano $x_1, x_2, \dots, x_n$ // interi variabili. Al variare delle x, il numero

$$a = a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad (1)$$

genera un modulo m (perché la somma o differenza di due tali numeri a è ancora un numero dello stesso tipo). Questo modulo si indica con $(a_1, a_2, \dots, a_n)$ (con parentesi tonde). Al solito esiste un intero h, che coi suoi multipli genera tale modulo. Tutti i numeri interi di $(a_1, a_2, \dots, a_n)$ (in particolare a_i, che si ottiene ponendo $x_i = 1$ e le altre x uguali a zero) sono multipli di h. D'altra parte h è un numero del modulo, esistono cioè degli interi y tali che

$$h = a_1y_1 + a_2y_2 + \cdots + a_ny_n.$$

Dunque ogni divisore comune delle a è un divisore di h. Dunque h è il M.C.D. dei numeri $a_1, a_2, \dots, a_n$. Ecco così trovate in generale le proprietà del M.C.D. di più numeri, che per $n = 2$ danno proprietà già trovate per altra via al §1.
Ne deduciamo in particolare che l'equazione (1) nelle incognite x è risolubile con valori interi di tali incognite allora e allora soltanto che a è divisibile per il M.C.D. delle $a_1, a_2, \dots, a_n$.

Es.[ercizio] Dedurre, almeno per $n = 2$, questo risultato dai teoremi del §1. //

Se un modulo M è contenuto in un campo oloide K, esso di chiama un ideale[24] se il prodotto di ogni ente di K e di un ente di M,[25] è ancora un ente di M [26]. In particolare, essendo M contenuto in K, ciò avverrà anche del prodotto di due enti di M (cosicchè M sarà un campo oloide contenuto nel campo più ampio K).
Il precedente risultato si può enunciare così:
Un modulo M di numeri interi, contenuto cioè nel campo oloide K dei numeri interi, è un ideale.
(Invece in un campo oloide di polinomi il modulo formato dai polinomi di primo grado non è un ideale).
Molto spesso indicheremo con lo stesso simbolo un tale ideale, e l'intero, i cui multipli lo generano.
Con[27] (α) indicherò cioè sia l'ideale generato dai numeri $x\alpha$, dove α è un intero dato, x un intero variabile, sia il numero α.

[24] Bianchi 1920-21, cap. II, §23, p. 145.
[25] *e.c.*: si aggiunga "è ancora un ente di M". *a.m.* nel ms.: "è ancora un ente di M".
[26] Bianchi 1920-21, Introduzione, §7, p. 47, 48.
[27] *Idem*, cap. II, §23, p. 146. Bianchi indica però in questo modo solo l'ideale principale generato da α.

L'ideale $(a_1, a_2, \dots, a_n) = (\alpha)$, se α è il M.C.D. delle a_i. Se $(a_1, a_2, \dots, a_n)$ è un ideale [cioè la classe dei numeri $x_1a_1 + x_2a_2 + \cdots + x_na_n$] e $(b_1, b_2, \dots, b_m)$ un altro ideale, allora l'ideale $(a_1b_1, a_1b_2, \dots, a_1b_m, a_2b_1, \dots, a_nb_m)$ dicesi l'ideale[28] prodotto dei due ideali dati. // Se il primo coincide con (α), il secondo con (β), l'ideale prodotto vale $(\alpha\beta)$. Se un ideale C vale il prodotto degli ideali A, B, allora C dicesi divisibile[29] per A e per B.
Se l'ideale A è divisibile per B, allora i numeri di A sono parte dei numeri di B, cioè A è contenuto in B.
Un ideale (nel campo dei numeri interi) è sempre generabile coi multipli di un solo intero α che si dice base dell'ideale.

Esercizi

1) Condizione necessaria e sufficiente affinché A sia il minimo multiplo comune di p. es. tre interi a, b, c è che $\frac{A}{a}, \frac{A}{b}, \frac{A}{c}$ siano interi primi tra loro.
2) È $[a, b, c] = \frac{abc}{(ab, bc, ca)}$. Con $[a, b, c]$ indicasi, come dicemmo, l'ideale formato dai multipli comuni di a, b, c, od anche il loro minimo comune multiplo. Si dimostri che dividendo il secondo membro per a, o per b, o per c si hanno quozienti primi tra loro.
3) Si dimostri con la teoria dei moduli che, se a, b sono primi tra loro, allora il M.C.D. di an, b è uguale al M.C.D. di n, b, se a è primo con b. // Basta provare che $(an, b) = (n, b)$. Ora $(an, b) = (an, nb, b) = (c, b)$ se $c = (an, nb) = n(a, b) = n$ [perché per ipotesi $(a, b) = 1$].
4) Se a, b, c, d sono interi $[(a, d), (b, d), (c, d)] = ([a, b, c], d)$.
   Basta provare che, dividendo il 2° membro per $\alpha = (a, d)$ $\beta = (b, d)$ $\gamma = (c, d)$ si hanno quozienti primi tra loro (eserc. 1°). Ora[30]
   $$\frac{([a,b,c],d)}{\alpha} = \left(\frac{a}{\alpha}\frac{[a,b,c]}{\alpha}, \frac{d}{\alpha}\right) = \left(\frac{[a,b,c]}{\alpha}, \frac{d}{\alpha}\right) \qquad (1)$$
   Perché $\frac{a}{\alpha}, \frac{d}{\alpha}$ sono primi tra loro (eserc. 3°). Ora (1) e le quantità analoghe hanno per[31] M.C.D.
   $$\left(\left(\frac{[a,b,c]}{a}, \frac{[a,b,c]}{b}, \frac{[a,b,c]}{c}\right), \frac{d}{\alpha}\right) = \left(1, \frac{d}{\alpha}, \frac{d}{\beta}, \frac{d}{\gamma}\right) = (1).$$

c.d.d.

§.4 ***Un primo esempio di aritmetica analitica***[32]

Ricordiamo che la serie (armonica)

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$$

[28] *del.* e *corr. sup.*; Fubini segnala invece questa modifica come *e.c.*
[29] Bianchi 1920-21, cap. II, §28, p. 159, 160.
[30] *e.c.*: $\frac{([\ ])}{\alpha} = \left(\frac{a}{\alpha}\frac{[a,b,c]}{\alpha}, \frac{d}{\alpha}\right) = \left(\frac{[a,b,c]}{\alpha}, \frac{d}{\alpha}\right)$ (1).
[31] *e.c.*: $\left(\left(\frac{[a,b,c]}{a}, \frac{[a,b,c]}{b}, \frac{[a,b,c]}{c}\right), \frac{d}{\alpha}, \frac{d}{\beta}, \frac{d}{\gamma}\right) = \left(1, \frac{d}{\alpha}, \frac{d}{\beta}, \frac{d}{\gamma}\right) = (1)$.
[32] Bianchi 1911-12, cap. VI, §57, p. 253, 254.

ha per somma $+\infty$, ossia diverge. Ammettiamo il teorema, che se ne deduce facilmente: // la serie

$$\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots$$

(che, come vedremo anche ora, converge per $s>1$) tende per $s=1$ ad ∞.

Noi dimostreremo per via trascendente (Eulero[33]) il teorema ben noto che ci sono infiniti numeri interi primi[34]. Supponiamo che di numeri primi positivi ce ne sia un numero finito[35]; essi siano $p_1=2, p_2=3,\ p_3, p_4, \ldots$ disposti in ordine crescente. È per $s>1$

$$\frac{1}{1-\frac{1}{p_i^s}}=1+\frac{1}{p_i^s}+\frac{1}{p_i^{2s}}+\frac{1}{p_i^{3s}}+\frac{1}{p_i^{4s}}+\cdots \qquad (1)$$

per nota formula della teoria delle progressioni geometriche decrescenti. Se ne deduce, in virtù dei teoremi ben noti sul prodotto di più serie assolutamente convergenti che:

$$\prod_i \frac{1}{1-\frac{1}{p_i^s}}=S(s) \qquad (2)$$

dove $S(s)$ è la somma di tutti i prodotti ottenuti moltiplicando tra di loro in tutti i modi possibili un termine di ciascuna delle serie (1), cioè la somma di tutte le espressioni $\frac{1}{n^s}$, dove $\underline{n}$ è un prodotto di alcuni numeri primi considerati. Poiché ogni intero positivo si può decomporre in un solo modo nel prodotto di numeri primi // positivi, la $S(s)$ vale $\sum\frac{1}{n^s}$, dove n percorre tutti i valori interi positivi, così che la (2) diventa

$$\prod_i \frac{1}{1-\frac{1}{p_i^s}}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots.$$

---

[33] Euler all'interno delle *Variae observationes circa series infinitas* (1737), quasi nascosta tra 19 teoremi e 16 corollari, presenta tale dimostrazione dell'esistenza di infiniti numeri primi, che poi ripropone nel capitolo *De seriebus ex evolutione factorum ortis* della *Introductio in analysin infinitorum* (1748).

[34] Fino a questo momento la dimostrazione dell'infinità dei numeri primi maggiormente diffusa era quella tratta dagli *Elementi* di Euclide (Lib. IX, prop. 20), il cui enunciato afferma: "Esistono [sempre] numeri primi in numero maggiore di quanti numeri primi si voglia proporre". La dimostrazione euclidea, puramente algebrica, era la seguente: si suppone che dati due numeri primi a, b, il numero $c=a\cdot b+1$ non sia primo; allora deve necessariamente ammettere un divisore primo d. Tuttavia $d\neq a, b$ perché se d fosse uguale ad uno dei numeri a, b dividerebbe il loro prodotto $a\cdot b$, ma d divide anche $c=a\cdot b+1$, quindi d dovrebbe dividere la differenza tra $a\cdot b+1$ e $a\cdot b$ ossia l'unità: il che è assurdo. Ciò dimostra che esistono almeno tre numeri primi; procedendo in questo modo, ossia aggiungendo di volta in volta 1 al prodotto di una quantità fissata di due numeri primi e iterando il ragionamento, si prova dunque l'esistenza di infiniti numeri primi. Tale dimostrazione, nello spirito della matematica greca, sfruttava un infinito potenziale, che può essere ottenuto ricorsivamente; quella che Fubini inserisce nelle sue lezioni, basata sul concetto di serie infinita, necessita invece di un infinito attuale, bandito all'interno della matematica greca, in quanto sfrutta un passaggio al limite.

[35] Bianchi 1920-21, cap. III, §44, p. 305. La dimostrazione di Bianchi ripercorre, con alcuni dettagli aggiuntivi, quella di Fubini. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. VI, §137, p. 350-352. Nella *Dimostrazione del teorema che ogni progressione aritmetica indefinita, il cui primo termine e la cui differenza sono numeri interi senza fattore comune, contiene una infinità di numeri primi*, Dedekind affronta la questione in modo più dettagliato e generale rispetto a Fubini. Il risultato cui perviene è il seguente: "Ogni progressione aritmetica illimitata $kx+m$, nella quale il primo termine m e la differenza k sieno primi fra loro, contiene una infinità di numeri primi positivi q".

Dunque per $s = 1$ il secondo membro, e quindi anche il primo, deve tendere a $+\infty$. Ciò che sarebbe assurdo, se il 1° membro fosse prodotto di un numero finito di fattori $\frac{1}{1-\frac{1}{p_i^s}}$ (con $p_i \geq 2$), cioè se vi fosse soltanto un numero finito di numeri primi. L'assurdo trovato prova il teorema. Questo metodo è fecondo (Dirichlet[36]) delle più svariate generalizzazioni.

§.5 *La funzione* φ(m) *e sue prime proprietà*[37]

Sia $\varphi(m)$ il numero degli interi $n \leq m$ primi con m (cioè tali che n, m abbiano 1 per M.C.D.). Sarà per es.[38] $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2,$ ecc. …

Se vi è un divisore δ di m, i numeri δ, 2δ, 3δ, …, $\delta\frac{m}{\delta} = m$ sono tutti e soli i numeri non superiori ad m, che non sono divisibili per δ. Anzi, uno di essi, p. es., $x\delta$ $\left(1 \leq x \leq \frac{m}{\delta}\right)$ avrà con m proprio δ come M.C.D. se x è primo con $\frac{m}{\delta}$. Di tali numeri x ve ne sono $\varphi\left(\frac{m}{\delta}\right)$. Dunque vi sono $\varphi\left(\frac{m}{\delta}\right)$ interi // $p \leq m$, che con m hanno δ per M.C.D.

Ogni numero $K \leq m$ ha con m per M.C.D. un divisore δ di m. Di tali numeri K ce ne sono m.

Quindi, se $\delta_1, \delta_2, \ldots, \delta_r$ sono i divisori di m, allora $m = \varphi\left(\frac{m}{\delta_1}\right) + \varphi\left(\frac{m}{\delta_2}\right) + \cdots + \varphi\left(\frac{m}{\delta_r}\right)$. Ma i numeri[39] $\frac{m}{\delta_i}$ sono gli stessi numeri scritti in un altro ordine. Perciò

$$m = \varphi(\delta_1) + \varphi(\delta_2) + \cdots + \varphi(\delta_r)$$

La somma dei valori di φ relativi ai vari divisori δ di m (inclusi i divisori 1, m) vale m.[40]

Sia p un intero primo, i cui divisori sono $1, p$. Sarà

$$\varphi(1) + \varphi(p) = p \qquad \varphi(1) = 1$$
$$\varphi(p) = p - \varphi(1) = p - 1.$$ [41]

Calcoliamo $\varphi(p^n)$. I divisori di p^n sono $1, p, p^2, \ldots, p^n$. Perciò

$$\varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^n) = p^n.$$

Scambiando n in $n - 1$, [e] sottraendo, se ne deduce[42]

---

[36] Si fa qui riferimento al teorema di Dirichlet (1835) che afferma che dati due numeri interi coprimi a e b, esistono infiniti primi della forma $a + nb$, dove $b > 0$ ($n \in \mathbb{N}$), o, in altre parole, ogni progressione aritmetica siffatta contiene infiniti numeri primi (generalizzazione dell'esistenza di infiniti numeri primi, enunciata e dimostrata in Euclide, *Elementi*, Lib. VII).

[37] Bianchi 1920-21, Introduzione, §4, p. 23. Cfr. anche Dirichlet 1881, cap. I, §11, p. 17, 18. Cfr. infine Sommer 1907 (trad. 1911), cap. 1, §2, p. 3.

[38] Gazzaniga 1903, cap. I, p. 25. Gazzaniga chiama $\varphi(m)$ indicatore di Gauss, o di 1° ordine, o semplicemente indicatore.

[39] *e.c.* e *corr. sup.*: invece di "sono gli stessi numeri" leggasi "sono i numeri δ_i".

[40] Dirichlet 1877 (trad. 1881), cap. I, §13, p. 22-23. L'autore qui scrive: "Se n assume successivamente tutti i valori dei divisori di m, è $\sum\varphi(n) = m$" e fornisce una verifica esplicita di questo risultato per $m = 60$.

[41] Gazzaniga 1903, cap. I, p. 25, prop. 54 (prima parte). Cfr. anche Dirichlet 1881, c. I, §11, p. 17, 18. Qui l'autore scrive che "perché l'unità è prima con se stessa è anzitutto $\varphi(1) = 1$".

[42] Gazzaniga 1903, cap. I, p. 25, 26, prop. 54 (seconda parte). Cfr. anche Sommer 1907 (trad. 1911), cap. 1, §1, p. 4, formula (2).

$$\varphi(p^n) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$$

Sia q un altro intero primo. I divisori di $p^n q^m$ sono[43]

$$1, p, p^2, \dots p^n, q, qp, \dots, p^n, \dots, q^m, q^m p, \dots, q^m p^n$$

Dunque[44]

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\varphi(p^i q^j) = p^n q^m$$

// da cui si può dedurre il valore $\varphi(p^n q^m)$ quando si conoscano i valori di $\varphi(p^i q^j)$ con $p^i q^j < p^n q^m$. E si trova

$$\varphi(p^n q^m) = p^n q^m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Così in generale, se $\underline{m}$ è un intero, e se $p_1, p_2, \dots, p_r$ sono i fattori primi distinti, si prova che[45]

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right).$$

Ciò si può provare anche direttamente: proviamolo, per es. per $r = 2$ (Cfr. più avanti). Calcoliamo

$$\varphi\left(p_1^{n_1}\, p_2^{n_2}\right) \qquad (p_1 \neq p_2).$$

I numeri minori di $p_1^{n_1}\, p_2^{n_2}$ primi con $p_1^{n_1}\, p_2^{n_2}$ sono quelli tra i numeri

$$1, 2, 3, 4, \dots, p_1^{n_1}, p_2^{n_2-1},\ p_1^{n_1}\, p_2^{n_2} \tag{1}$$

che rimangono in tale successione, quando si sopprimono i multipli di p_1 cioè i numeri

$$p_1, 2p_1, 3p_1, \dots, \left(p_1^{n_1-1} p_2^{n_2}\right)p_1 \tag{2}$$

ed i multipli di p_2, cioè i numeri

$$p_2, 2p_2, 3p_2, \dots, \left(p_1^{n_1} p_2^{n_2-1}\right)p_2. \tag{3}$$

Quanti interi rimarranno in (1) dopo tali soppressioni? Si noti che le (2), (3) hanno alcuni numeri comuni, cioè i multipli di $p_1 q_1$[46] cioè i numeri [47]

$$1 \cdot p_1 q_1; 2 \cdot p_1 q_1; 3 \cdot p_1 q_1; \dots; \left(p_1^{n_1-1} p_2^{n_2-1}\right)p_1 q_1 \tag{4}$$

---

[43] *e.c.*: $1, p, p^2, \dots p^n;\ q, qp, \dots, qp^n; \dots; q^m, q^m p, \dots, q^m p^n$.

[44] *e.c.*: $\sum_{i=0}^{n}\sum_{j=0}^{m}\varphi(p^i q^j) = p^n q^m$.

[45] Dirichlet 1877 (trad. 1881), cap. I, §11, p. 20-21. Qui è enunciato e dimostrato il teorema: "Se $a, b, c, \dots, k, l$ sono i differenti divisori primi di m, $\varphi(m) = m\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\dots\left(1 - \frac{1}{k}\right)\left(1 - \frac{1}{l}\right)$ esprime quanti dei numeri $1,2,3, \dots, m$ sono primi coll'ultimo m". Cfr. anche Sommer 1907 (trad. 1911), cap. 1, §2, p. 4, formula (4).

[46] *e.c.* e *corr. sup.*: invece di $p_1 q_1$ leggasi $p_1 p_2$.

[47] *e.c.* e *corr. sup.*: $1. p_1 p_2; 2. p_1 p_2; 3. p_1 p_2; \dots; \left(p_1^{n_1-1} p_2^{n_2-1}\right)p_1 p_2$.

// Quindi, poiché in (2) vi sono $p_1^{n_1-1}p_2^{n_2} = \frac{m}{p_1}$ interi, poiché in (3) vi sono $p_1^{n_1}p_2^{n_2-1} = \frac{m}{p_2}$ interi, poiché in (4) vi sono $p_1^{n_1-1}p_2^{n_2-1} = \frac{m}{p_1p_2}$ interi, nelle due successioni (2) e (3) vi saranno in tutto $\frac{m}{p_1} + \frac{m}{p_2} - \frac{m}{p_1p_2}$ interi distinti. Sopprimendo questi tra gli m interi di (1) ne rimarranno

$$\varphi(m) = m - \frac{m}{p_1} - \frac{m}{p_2} + \frac{m}{p_1p_2} = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

c.d.d.

Col metodo dianzi accennato si prova però in primis che, se una funzione $\psi(m)$ è tale che $\sum \psi(\delta) = m$, essendo δ i divisori di m, allora[48] $\psi(m) = \varphi(m)$. E ciò perché questa sola proprietà bastava a calcolare la funzione φ. (Si noti che qui parliamo di funzioni aritmetiche, cioè definite soltanto per valori interi della corrispondente variabile).

Se m, m' sono interi primi tra loro, si dimostri che[49]

$$\varphi(m)\varphi(m') = \varphi(m\,m').$$

Basta ricorrere alla formula che dà il valore di $\varphi(m)$.

8. Fubini (al centro) con Fano, Tonelli, Levi-Civita e consorti

[48] Gazzaniga 1903, cap. I, p. 25, 26, prop. 55. La proposizione è enunciata in modo differente, ma del tutto equivalente. Cfr. anche Dirichlet 1877 (trad. 1881), cap. I, §13, p. 22. Qui il matematico tedesco scrive che "il problema, di determinare il valore della funzione $\varphi(m)$, non è infine che un caso speciale del seguente: Essendo δ un divisore qualunque del numero $m = n\delta$, determinare quanti dei numeri $1,2,3,\dots,m$ hanno con m il massimo comun divisore δ".

[49] Bianchi 1920-21, Introduzione, §4, p. 23-24. A differenza di Fubini, Bianchi, dimostra tale proprietà nella sua versione più generale, ossia prova che se m si scinde nel prodotto di r fattori primi fra loro due a due: $m = m_1m_2 \dots m_r$, allora $\varphi(m) = \varphi(m_1)\varphi(m_2) \dots \varphi(m_r)$. Cfr. anche Dirichlet 1877 (trad. 1881), cap. I, §12, p. 21-22 in cui egli prova il teorema in questa forma, lo applica per $m = 60$, scrivendo successivamente che tale risultato può essere "esteso ad un prodotto di quanti si vogliano numeri $m, m', m'' \dots$, i quali siano primi tra loro".

Capitolo II – Congruenze

§.1 ***Definizioni***[1]

Scriverò[2]

$$a \equiv b \ (mod\ n) \qquad (a, b, n\ interi)$$

e dirò che a è congruo a b rispetto al modulo n, se $a - b$ è multiplo di n, cioè se $a - b$ è un numero del modulo generato da n. Tale congruenza equivale alla esistenza di un intero x tale che[3]

$$a = b + nx.$$

Se $a - b$ non è multiplo di n, dirò che a è incongruo a b rispetto al modulo n e scriverò

$$a \not\equiv b \ (mod\ n).$$

Nella teoria delle congruenze, numeri congrui si considerano come equivalenti. La congruenza ha molte proprietà dell'uguaglianza[4]. È infatti sempre

$$a \equiv a \ (mod\ n).$$

Dalla $a \equiv b \ (mod\ n)$ si deduce $b \equiv a \ (mod\ n)$.
Dalla $a \equiv b, b \equiv c \ (mod\ n)$ si deduce[5] $a \equiv c \ (mod\ n)$.
E ciò perché se $a - b$ e $b - c$ sono multipli di n, anche $(a - b) + (b - c) = a - c$ è multiplo di n.
Se $a \equiv b \ (mod\ n), c \equiv d \ (mod\ n)$, // è anche

$$a + c \equiv b + d, \qquad a - c \equiv b - d, \qquad ac \equiv bd \ (mod\ n).$$

Per dimostrare, p. es., l'ultima di queste formule, si noti che l'ipotesi fatte equivalgono ad ammettere l'esistenza di due interi x, y così che

$$a = b + nx, \qquad c = d + ny.$$

Se ne deduce

$$ac = bd + n(dx + by + nxy)$$

cioè $ac - bd =$ multiplo di n, cioè $ac \equiv bd \ (mod\ n)$.
Scrivere la $a \equiv b \ (mod\ n)$ equivale ad ammettere l'esistenza di un intero x tale che

$$a = b + nx.$$

---

[1] Gauss 1801, sez. I, p. 9, 10.
[2] Bianchi 1920-21, Introduzione, §3, p. 19. Egli fornisce qui le stesse definizioni di Fubini ma le estende al campo degli interi di Gauss. Cfr. anche Dirichlet 1877 (trad. 1881), cap. II, §17, p. 29, 30. L'autore scrive che "si potrebbero definire i numeri congrui come quelli la cui differenza è divisibile per il modulo". Cfr. infine Sommer 1907 (trad. 1911), cap. 1, §3, p. 5, 6.
[3] Gazzaniga 1903, cap I, p. 15. Vi si trova la stessa definizione di congruenza $(mod\ n)$.
[4] Dirichlet 1877 (trad. 1881), cap. II, §17, p. 30, 31. Qui Dirichlet enuncia e dimostra 6 proprietà delle congruenze, le cui prime 4 e l'ultima coincidono con quelle di Fubini.
[5] Sommer 1907 (trad. 1911), cap. 1, §3, p. 6, prop. I.

Sia d un divisore comune di a, b. Allora anche nx sarà divisibile per d; e, se n è primo con d, allora x sarà divisibile per d. Cioè $\frac{x}{d} = y$ sarà un intero, cosicché

$$\frac{a}{d} = \frac{b}{d} + ny,$$

ossia

$$\frac{a}{d} \equiv \frac{b}{d} \ (mod\ n).$$

La congruenza $a \equiv b\ (mod\ n)$ si può dividere per ogni intero d, divisore comune di a, b, il quale sia primo con n.
Se a, b, n sono divisibili per uno stesso numero h, allora dalla $a \equiv b\ (mod\ n)$ si può dedurre la //

$$\frac{a}{h} \equiv \frac{b}{h} \ \left(mod \frac{n}{h}\right).$$

Infatti dalla $a = b + nx$ si può dedurre la $\frac{a}{h} = \frac{b}{h} + \frac{n}{h}x$, dove per ipotesi $\frac{a}{h}, \frac{b}{h}, \frac{n}{h}$ sono interi.
Nell'aritmetica delle congruenze $(mod\ m)$ si considerano come non distinti due numeri congrui $(mod\ m)$, precisamente come in goniometria, quando si misurino gli angoli in gradi, si considerano come equivalenti due numeri che differiscono di un multiplo di 360°. Da questo punto di vista l'aritmetica degli interi $(mod\ m)$ è l'aritmetica di un campo pseudo oloide; in esso, contrariamente a ciò che avviene nell'aritmetica ordinaria, tra i numeri $1, 1+1,$ $1+1+1,$ ecc. ve n'è uno non distinto da (congruo a) zero: precisamente il numero $1+1+\cdots+1,$ quando gli addendi siano m. I numeri interi in tale campo pseudo-oloide possono pensarsi come le anomalie dei vertici di un poligono regolare di m lati, quando un vertice abbia per anomalia zero, e si assuma come unità di misura degli angoli (anomalia) la m^{esima} parte di 4 retti.
Ogni intero K è congruo $(mod\ m)$ ad uno ed uno solo degli m interi $0, 1, 2, \ldots, m-1$; che[6] (p. es. per restare nell'ambito degli interi K positivi) è il resto ultimo // nella divisione di K per m. Numeri congrui danno resti uguali; numeri incongrui danno resti distinti.
Sia p un intero primo; siano a, b interi. Sarà[7]

$$(a+b)^p = a^p + b^p + \frac{p}{1}a^{p-1}b + \frac{p(p-1)}{1.2}a^{p-2}b^2 + \cdots \frac{p(p-1)\ldots 4.3}{1.2.3\ldots.(p-2)}a^2b^{p-2} + \frac{p(p-1)\ldots 4.3.2}{1.2.3\ldots.(p-1)}ab^{p-1}.$$

I coefficienti di $a^{p-1}b, a^{p-2}b^2, \ldots, a^2b^{p-2}, ab^{p-1}$ nel secondo membro sono dati dalla formula nota sotto il nome di binomio di Newton, e, nonostante che si presentino sotto la forma di frazioni, sono numeri interi.[8]
Nel ridurre una di tali frazioni ai minimi termini (cioè ad un numero intero) si devono dividere il suo numeratore e il suo denominatore per il loro M.C.D. Questo M.C.D. non è divisibile per

[6] *del.* e *cor. sup*. Fubini segnala invece la correzione nell'*e. c*.
[7] *del.* e *cor. sup*. Fubini segnala invece la correzione nell'*e. c*.
[8] Dirichlet 1877 (trad. 1881), cap. II, §20, p. 37. Fubini utilizza lo stesso procedimento e la stessa notazione del matematico tedesco.

l'intero primo p, perché i fattori del denominatore sono tutti minori di p. Quindi, poiché ogni numeratore contiene il fattore p, l'intero, a cui si riduce una qualsiasi di tali frazioni, è divisibile per p. Dunque, se a, b sono interi, è

$$(a+b)^p = a^p + b^p + px \; con \; x \; intero$$

cioè[9]

$$(a+b)^p = a^p + b^p \;\; (mod\ p).$$

Se a, b, c sono interi, [10]applicando due volte que//sto teorema, si deduce:

$$[a+b+c]^p = [(a+b)+c]^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \;\; (mod\ p).$$

In generale, se $a_1, a_2, \dots, a_n$ sono interi, e p è un intero primo, si ha[11]:

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \;\; (mod\ p).$$

§.2 ***Il teorema di Fermat***[12]

Ponendo in tale formula $a_1 = a_2 = \cdots = a_n = 1$ si deduce[13]

$$n^p \equiv n \; (mod\ p)$$

formola che vale per ogni intero n e per ogni intero primo p.[14]
Se n è un intero primo con l'intero primo p (cioè non divisibile per p) [15]

$$n^{p-1} \equiv 1 \; (mod\ p)$$

perché la congruenza precedente si può dividere per n, primo con p.
Questa congruenza costituisce il teorema di Fermat[16]. Essa si può scrivere:

$$n^{\varphi(p)} \equiv 1 \; (mod\ p).$$

Sotto questa forma, il risultato è più generale[17]. Cioè, se n è un intero primo con l'intero m, allora[18] //

$$\mathrm{n}^{\varphi(\mathrm{m})} \equiv 1 \; (\mathrm{mod\ m}) \qquad (*).$$

---

[9] Gazzaniga 1903, cap I, p. 22. Cfr. anche Dirichlet 1881, cap. II, §20, p. 37.
[10] Termine parzialmente cancellato sovrascritto poi a matita.
[11] Gazzaniga 1903, cap I, p. 21, prop. 45. Cfr. anche Dirichlet 1881, cap. II, §20, p. 37.
[12] Il cosiddetto piccolo teorema di Fermat cui è dedicato questo paragrafo è stato enunciato da Fermat in una lettera all'amico e matematico B. Frenicle nel 1640 senza dimostrazione. Il primo a dimostrare questo risultato fu il matematico tedesco G.W. Leibniz in un manoscritto inedito non datato, dove scrisse anche che conosceva una dimostrazione da prima del 1683.
[13] Dirichlet 1877 (trad. 1881), cap. II, §20, p. 37, 38. Fubini segue qui il procedimento delle *Vorlesungen* per arrivare alla dimostrazione del piccolo teorema di Fermat, pur provandolo solo per n positivo.
[14] Bianchi 1920-21, Introduzione, §3, p. 25. Bianchi, a differenza di Fubini, enuncia e dimostra il piccolo teorema di Fermat nel campo dei numeri complessi.
[15] Gazzaniga 1903, cap. I, p. 22, prop. 46. Cfr. anche Dirichlet 1881, cap. II, §20, p. 38.
[16] Gauss 1801, sez. III, art. 50, p. 41, 42. Cfr. anche Sommer 1907 (trad. 1911), cap. 1, §4, p. 7.
[17] Bianchi 1920-21, Introduzione, §3, p. 25, 26. Viene enunciato un analogo del teorema di Fermat generalizzato.
[18] Gazzaniga 1903, cap. I, p. 27, prop. 57. Gazzaniga enuncia tale risultato sotto il nome di "prima generalizzazione della propos. di Fermat".

Per dimostrarlo osserviamo che, se q è un intero primo con m, ogni numero $q_1 \equiv q \ (mod\ m)$ è del tipo $q + mx$ con x intero, ed è pure primo con m (perché, se un intero $\neq 1$ dividesse q_1 ed m, esso dividerebbe anche $q_1 - mx = q$).
Perciò ogni numero primo con m è congruo ad uno (ad uno solo) dei $\varphi(m)$ numeri minori di m e primi con m. Cioè i numeri primi con m si dividono in $\varphi(m)$ sistemi, tali che gli interi di uno stesso sistema sono congrui tra loro e sono incongrui coi numeri di un altro sistema. In altre parole, poiché nell'aritmetica delle congruenze $(mod\ m)$ numeri congrui $(mod\ m)$ si possono considerare come identici, si potrebbe (con un modo però forse troppo rapido) dire che $(mod\ m)$ vi sono soltanto $\varphi(m)$ interi primi con m.
Sia $a_1, a_2, a_3, \dots, a_{\varphi(m)}$ un tale sistema di $\varphi(m)$ interi incongrui primi con m; se n è un intero qualunque primo con m, anche $a_1 n, a_2 n, a_3 n, \dots, a_{\varphi(m)} n$ // sono primi con m. Due di questi numeri sono incongrui tra loro; perché da

$$a_i n \equiv a_j n \ (mod\ m)$$

si dedurrebbe, dividendo per n (ciò che è lecito, perché n è primo con m)

$$a_i \equiv a_j \ (mod\ m)$$

contro l'ipotesi. Dunque i numeri $a_i n \ (i = 1,2, \dots, \varphi(m))$ sono congrui ai numeri a disposti in ordine conveniente. Perciò il prodotto dei numeri na_i è congruo al prodotto dei numeri a_i. Cioè, se A è il prodotto dei numeri a_i, poiché gli interi a_i sono in numero di $\varphi(m)$:

$$n^{\varphi(m)} A \equiv A \ (mod\ m).$$

Ma A è prodotto di numeri primi con m ed è perciò primo con m. Si può pertanto dividere per A e si ottiene:

$$n^{\varphi(m)} \equiv 1 \ (mod\ m)$$

che è appunto il teorema enunciato.
Il lettore verifichi per qualche valore di n, m.

(*) **Nota**: Per $m = 1$, il teorema è banale, supporrò $m \neq 1$.

§.3 ***Congruenze di 1° grado ed analisi indeterminata di 1° grado***[19]

Sia data la congruenza

$$ax \equiv b \ (mod\ c) \qquad (1)$$

// dove a, b, c sono dati; si tratta di trovare l'incognita x in modo da soddisfare alla (1). Si noti che, se x è un intero che soddisfa ad (1), allora, $ax - b$ sarà un multiplo di c, poniamo $-cy$, dove y è un intero.
Sarà cioè [20]:

$$ax + cy = b. \qquad (2)$$

[19] Gauss 1801, sez. II, art. 29-37, p. 21-30.
[20] Gazzaniga 1903, cap. III, p. 48. Gazzaniga chiama questo tipo di congruenze 'lineari'.

Viceversa, se x, y sono interi soddisfacenti alla (2), la x soddisfa ad (1). Sono dunque equivalenti i problemi da risolvere[21].
α) una congruenza (1) di 1° grado in un'incognita
β) un problema (2) di analisi indeterminata di 1° grado in due incognite.
Cominciamo dalla (2). Essa è risolubile allora, e allora soltanto che b appartenga all'ideale (a, c), cioè soltanto se[22] c è multiplo del M.C.D.[23] di a, c.
Dunque:
Affinché la (1), o, ciò che è lo stesso, la (2) siano risolubili (in numeri interi) è necessario e sufficiente che b sia divisibile per il M.C.D. del coefficiente a e del modulo c.
Se questa condizione è soddisfatta, la (2) divisa per tale M.C.D., che chiameremo d diventa

$$\alpha x + \gamma y = \beta \quad (3)$$

// equivalente alla

$$\alpha x \equiv \beta \ (mod\ \gamma) \quad (4)$$

dove è posto $\alpha = \frac{a}{d}, \beta = \frac{b}{d}, \gamma = \frac{c}{d}$, e dove pertanto α e γ sono primi tra loro.
Supponiamo di conoscere una soluzione

$$x = x_0 \qquad y = y_0$$

della (3), cosicché $\alpha x_0 + \gamma y_0 = \beta$. Sottraendo questa uguaglianza da (3) si ha:

$$\alpha(x - x_0) = -\gamma(y - y_0).$$

Poiché α, γ sono primi tra loro, sarà $x - x_0$ multiplo di γ. Posto $x - x_0 = n\gamma$, si trova $y - y_0 = -n\alpha$.
E la soluzione più generale sarà data dalle:

$$x = x_0 + n\gamma \qquad y = y_0 - n\alpha \qquad (5)$$

con n intero qualsiasi.[24]
Tutto il problema è dunque ridotto a trovare una soluzione delle (3), (4). Una prima via ci è offerta dalla (4). Essendo α, γ primi tra loro, è per il teorema di Fermat

$$\alpha^{\varphi(\gamma)} \equiv 1 \ (mod\ \gamma)$$

cosicché

$$\beta\alpha \cdot \alpha^{\varphi(\gamma)-1} \equiv \beta \ (mod\ \gamma).$$

E si può porre [25] //

$$x_0 = \beta\alpha^{\varphi(\gamma)-1}. \qquad (*)$$

Un'altra via ci è offerta dalla (3). Essendo α, γ primi tra loro, noi sappiamo calcolare due interi ξ, η tali che $\alpha\xi + \gamma\eta = 1$. Basta porre

[21] Dirichlet 1877 (trad. 1881), cap. II, §23, p. 43.
[22] *e.c.*: invece di c leggasi b.
[23] Gazzaniga 1903, cap. I, p. 49, prop. 2. Cfr. anche Sommer 1907 (trad. 1911), cap. 1, §4, p. 9.
[24] Dirichlet 1877 (trad. 1881), cap. II, §24, p. 50.
[25] Fubini inserisce a p.d.p. il seguente rimando: *Teoria dei numeri disp. 3.*

$$x_0 = \beta\xi, \qquad y_0 = \beta\eta$$

per trovare una soluzione di (3).
Noi abbiamo dunque imparato a risolvere le (2), (3) quando ciò è possibile. Osserviamo la prima delle (5)

$$(6)\quad x = x_0 + n\gamma; \quad \gamma = \frac{c}{d}; \qquad n = intero\ arbitrario$$

che dà tutte le soluzioni di (1), quando se ne conosca una x_0. Osserviamo che due numeri congrui tra loro $(mod\ c)$ sono entrambi, o non sono né l'uno né l'altro soluzioni di (1); valori congrui della x non si debbono, nell'aritmetica delle congruenze, considerare come distinti. E noi, adottando questa convenzione, possiamo chiederci:
Quante soluzioni distinte ha la (1) (supposto naturalmente che sia risolubile)? Cioè [cfr. la (6)] quanti numeri incongrui $(mod\ c)$ sono dati dalla //

$$x = x_0 + n\gamma = x_0 + n\frac{c}{d}.$$

Se n, n' sono due valori di n i valori corrispondenti di x sono congrui allora allora soltanto che

$$\left(x_0 + n\frac{c}{d}\right) - \left(x_0 + n'\frac{c}{d}\right) = c\frac{n - n'}{d}$$

è multiplo di c, che cioè $\frac{n-n'}{d}$ è un intero che cioè

$$n \equiv n'\ (mod\ d).$$

Ora di numeri n incongrui $(mod\ d)$ ve ne sono precisamente d (p. es. i numeri $0, 1, 2, \dots, d-2, d-1$). Quindi[26]: Se la (1) è risolubile, essa possiede precisamente d radici incongrue, se d è il M.C.D. di a, c. Essa possiede una sola radice se $d = 1$.
Se il modulo c è un numero primo p, la (1) è risolubile, se $a \not\equiv 0\ (mod\ p)$ (cioè se a non è divisibile per p). E in tal caso ammette una sola soluzione. Se invece $a \equiv 0\ (mod\ p)$ la (1) è risolubile soltanto se anche $b \equiv 0\ (mod\ p)$, in tal caso la (1) è un'identità e ammette ogni numero per soluzione. (Si noti che $(mod\ p)$ vi sono soltanto p interi distinti).
Dunque se $c = p$ è primo, la teoria di (1) è perfettamente analoga a quella delle equazioni di primo grado.

Esercizi
Si studino le (1), (2) con valori particolari di a, b, c.

Alcune osservazioni
Per i calcoli numerici è utile osservare quanto segue; se si vuol verificare il teor.[ema] di Fermat per qualche intero particolare, o risolvere qualche congruenza di primo grado con le formole che abbiamo dedotto da tale teorema, si deve calcolare qualche potenza di un intero a, per es. $a^m\ (mod\ n)$. In tale calcolo si hanno notevoli semplificazioni, se si ricorda che a un numero K si può sempre sostituire un altro $h \equiv K\ (mod\ m)$.

[26] Dirichlet 1877 (trad. 1881), cap. II, §22, p. 42.

Per es. se studiando le congruenze $(mod\ 10)$ si volesse calcolare $7^{\varphi(10)} = 7^4$, si osserverebbe che $7^4 = (7^2)^2 = 49^2$. Ma non sarebbe necessario calcolare 49^2. Osservando che $49 \equiv 9 \equiv -1\ (mod\ 10)$, si trova che

$$7^4 = 49^2 = (9)^2 \equiv (-1)^2\ (mod\ 10),$$

cioè $7^4 \equiv 1\ (mod\ 10)$ senza alcun calcolo numerico fastidioso. In fondo in tale tipo di calcolo, quando si ha un'espressione $mx + K$ $(x, m, K$ interi$)$ e si studiano le congruenze $(mod\ m)$ l'espressione mx si trascura, si considera cioè come nulla. Simili procedimenti sono del resto noti nell'arit//metica elementare, quando si fa la prova del 9 (o dell'11) di una moltiplicazione, si fa in sostanza la stessa moltiplicazione nell'aritmetica delle congruenze $(mod\ 9$ o $mod\ 11)$, e si trascurano pertanto i multipli di 9 o di 11.

(*) **Nota**: Se è noto il valore x_0 di x, il valore corrispondente y_0 di y si deduce tosto dalla (3).

§.4 *Sistemi di congruenze di primo grado*

Si presentano talvolta sistemi di più congruenze di primo grado in parecchie incognite:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \equiv b_n \end{array}\right\} (mod\ K)$$

$(a_{ik}, b_i, K$ interi dati; x interi incogniti).

A questi sistemi di equazioni si possono estendere molti dei metodi che l'algebra applica ai sistemi di equazioni lineari; e ciò specialmente se K è un intero primo. Così, p. es., se $m = n$, se il determinante A delle a_{ik} è differente da zero, ed A_{rs} è il complemento algebrico di a_{rs} in A, si moltiplichi la r^{esima} delle precedenti congruenze per A_{rs} $(r = 1, 2, \ldots, m = n)$ e si sommi. Si troverà:

$$Ax_s = b_1A_{1s} + b_2A_{2s} + \cdots + b_nA_{ns}\ (mod\ K) \qquad (s = 1, 2, \ldots, n)$$

// che è un'equazione in un'incognita sola, la quale si può studiare coi metodi precedenti.
Senza qui più oltre occuparci di tale studio, studiamo invece il seguente sistema di $\underline{n}$ congruenze[27]

$$\begin{array}{c} a_1x \equiv c_1\ (mod\ b_1) \\ a_2x \equiv c_2\ (mod\ b_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_nx \equiv c_n\ (mod\ b_n) \end{array}$$

in una sola incognita $\underline{x}$ in cui però il modulo b può variare da una congruenza all'altra. Le eventuali soluzioni si troveranno risolvendo ciascuno dei sistemi di congruenze

$$x \equiv \beta_1\ (mod\ b_1);\ \ x \equiv \beta_2\ (mod\ b_2);\ \ x \equiv \beta_n\ (mod\ b_n)$$

che si ottengono scrivendo al posto di β_i una soluzione della $a_ix \equiv c_i\ (mod\ b_i)$ per $i = 1, 2, \ldots, n$.
Occupiamoci perciò di quest'ultimo sistema di congruenze. La prima si risolve ponendo

[27] Gazzaniga 1903, cap. III, p. 50, 51, prop. 3. Gazzaniga affronta però solamente il caso dei b_i primi tra loro a due a due (caso in cui il sistema di congruenze è sempre risolubile).

$$x = \beta_1 + b_1 y \quad con\ y\ intero.$$

Sostituendo nelle altre, si trova

$$b_1 y \equiv \beta_2 - \beta_1 \ (mod\ b_2)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$b_1 y \equiv \beta_n - \beta_1 \ (mod\ b_n)$$

che è un sistema di sole $n-1$ congruenze, che si // può studiare come il precedente, diminuendo successivamente di 1 il numero delle equazioni.
Se, p. es., $n = 2$, il nostro sistema di congruenze si riduce alla sola

$$b_1 y \equiv \beta_1 - \beta_2 \ (mod\ b_2)$$

che è risolubile, qualunque sieno β_1 e β_2, se b_1 e b_2 sono primi tra loro. E in tal caso $(mod\ b_2)$ vi è una sola soluzione y: vale a dire, se y_0 è una soluzione, le altre sono del tipo $y = y_0 + nb_2$ con n intero arbitrario. Cioè

$$x = \beta_1 + b_1 y = \beta_1 + b_1 y_0 + n b_1 b_2$$

cioè x resta determinato $(mod\ b_1 b_2)$.
Ne deduciamo dunque, p. es.: Se b_1, b_2 sono primi tra loro, per determinare un intero x rispetto al modulo $b_1 b_2$, basta dire a quali interi β_1, β_2 esso è congruo rispettivamente secondo i moduli b_1 e b_2. E viceversa.
Dunque, se x è determinato sia rispetto al modulo b_1, che b_2 (b_1, b_2 primi tra loro), x è determinato rispetto al modulo $b_1 b_2$. Se x è in più determinato rispetto al $mod\ b_3$, essendo b_3 primo con b_1 e con b_2, cioè primo con $b_1 b_2$, la x è determinata rispetto a $b_1 b_2 b_3$. E così via. Se x è deter//minato rispetto a più moduli $b_1, b_2, \dots, b_n$ primi tra loro, x è determinato rispetto al modulo $b_1 b_2 \dots b_n$ loro prodotto (e viceversa).
Ne vogliamo fare un'applicazione che completa un calcolo precedente. Il numero $\varphi(b_1 b_2)$ è il numero degli interi x primi con $b_1 b_2$ incongrui $(mod\ b_1 b_2)$. Dire che x è primo con $b_1\ b_2$ equivale (poiché b_1, b_2 sono primi tra loro) a dire che x è primo con b_1 ed è primo con b_2. E, per quanto si è ora dedotto, dire che due interi sono incongrui $(mod\ b_1 b_2)$ equivale a dire che essi sono incongrui almeno secondo uno dei due moduli b_1, b_2. Uno dei nostri interi x soddisfa dunque a due congruenze

$$x \equiv \beta_1 \ (mod\ b_1) \qquad x \equiv \beta_2 \ (mod\ b_2)$$

(β_1 primo con b_1; β_2 primo con b_2). E viceversa, se β_1 è dato $(mod\ b_1)$, e β_2 è dato $(mod\ b_2)$, allora x è determinato $(mod\ b_1 b_2)$.
Il numero $\varphi(b_1 b_2)$ degli interi studiati vale dunque il prodotto del numero $\varphi(b_1)$ degli interi β_1 per il numero $\varphi(b_2)$ degli interi β_2. Cioè: Se b_1, b_2 sono primi tra loro, allora:

$$\varphi(b_1 b_2) = \varphi(b_1)\varphi(b_2).$$

La proprietà si estende tosto ai prodotti di più fattori primi tra loro a due a due. Così se b_1, b_2, b_3 sono a due a due primi tra loro, è

$$\varphi(b_1 b_2 b_3) = \varphi[(b_1 b_2) b_3] = \varphi(b_1 b_2)\varphi(b_3) = \varphi(b_1)\varphi(b_2)\varphi(b_3) \ \ ecc\dots$$

Sia n un intero qualsiasi; siano $p_1, p_2, \dots p_r$ i suoi fattori primi distinti. E sia

$$n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}.$$

Sarà:

$$\varphi(n) = \varphi\left(p_1^{m_1}\right)\varphi\left(p_2^{m_2}\right) \dots \varphi\left(p_r^{m_r}\right) =$$
$$= p_1^{m_1}\left(1 - \frac{1}{p_1}\right) p_2^{m_2}\left(1 - \frac{1}{p_2}\right) \dots p_r^{m_r}\left(1 - \frac{1}{p_r}\right) =$$
$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Ecco così provata senz'altro una formola già scritta in un altro paragrafo.
Un'ultima osservazione: Un qualunque sistema di congruenze lineari si può, aumentando il numero delle incognite, trasformare in un problema di analisi indeterminata.
Così, p. es. un sistema di congruenze

$$\sum_k a_{ik} x_k \equiv \alpha_i \ (mod\ c_i) \ \ (k = 1, 2, \dots\ m; i = 1, 2, \dots n)$$

// equivale al sistema di equazioni

$$\sum_k a_{ik} x_k + c_i y_i = \alpha_i,$$

dove le y_i sono le nuove incognite. Rinvio per tale studio ai trattati già citati.

§.5 ***Congruenze di grado qualunque***[28]

Il teorema fondamentale di Gauss per le equazioni algebriche non ha l'analogo nella teoria delle congruenze; noi sappiamo, p. es., che anche una congruenza di primo grado $ax \equiv b\ (mod\ c)$ con $a \neq 0$ può non avere alcuna radice, e può anche averne più di una.
Così pure è generalmente (nella teoria delle congruenze) <u>falso</u> anche il teorema: <u>se il prodotto</u> $ab \equiv 0\ (mod\ c)$, <u>almeno uno dei fattori</u> a, b <u>è congruo a zero.</u> Il teorema è <u>vero</u> però, se il modulo c è un numero <u>primo</u>; perché se $ab \equiv 0$ cioè il prodotto ab è divisibile per il numero <u>primo</u> c, almeno uno dei fattori[29] b, c è divisibile per c.
Vale invece un teorema analogo a quello di Ruffini[30]. Se[31]

$$p(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n \equiv 0 \ \ (mod\ o)$$
$$(a_i, c = \text{numeri interi})$$

// possiede una radice α, cioè se $p(\alpha) \equiv 0\ (mod\ c)$, allora l'identità

$$p(x) = (x - \alpha) q(x) + p(\alpha),$$

[dove $q(x)$ è il polinomio (a coefficienti interi), che è quoziente della divisione di $p(x)$ per $x - \alpha$] diventa

$$\mathrm{p(x)} \equiv (\mathrm{x} - \alpha)\mathrm{q(x)} \ (\mathrm{mod\ c}). \qquad \text{(teor. di Ruffini)}$$

[28] Gazzaniga 1903, cap. III, p. 60. Gazzaniga dedica interamente a questo argomento il paragrafo *Delle congruenze di grado superiore al primo* (p. 60-63).
[29] *lapsus* del curatore: leggasi "almeno uno dei fattori a, b è divisibile per c.".
[30] Sommer 1907 (trad. 1911), cap. 1, §4, p. 11.
[31] *e.c.* e *cor. sup.*: invece di $(mod\ o)$ leggasi $(mod\ c)$.

Supponiamo che $p(x)$ possegga un'altra radice β, distinta dalla precedente $(mod\ c)$. Sarà:

$$p(\beta) \equiv (\beta - \alpha)q(\beta) \equiv 0 \ \ (mod\ c).$$

Dunque il prodotto $(\beta - \alpha)q(\beta)$ è congruo a zero; dal che non segue che almeno uno dei fattori sia congruo a zero; cosicché non si può ripetere il noto ragionamento algebrico per la decomposizione di un polinomio in fattori. Ma, se c è un numero primo allora possiamo dedurre che almeno uno dei fattori $\beta - \alpha$ e $q(\beta)$ è congruo a zero. E, poiché[32] $\beta \not\equiv d$, ne deduciamo che $q(\beta) \equiv 0$, cioè che $q(x) \equiv 0$ ha la radice β, e quindi come sopra, che

$$q(x) \equiv (x - \beta)q_1(x)$$
$$p(x) \equiv (x - \alpha)(x - \beta)q_1(x) \ \ (mod\ c)$$

// dove q_1 è un nuovo polinomio a coefficienti interi. Se $p(x)$ ha un'altra radice γ incongrua con le precedenti, si troverà similmente

$$p(x) \equiv (x - \alpha)(x - \beta)(x - \gamma)q_2(x) \ \ (mod\ c)$$

dove $q_2(x)$ è un nuovo polinomio a coefficienti interi. Questo calcolo si può ripetere al più n volte.
Dunque:
Una congruenza $p(x) \equiv 0$ di grado n rispetto ad un modulo primo c ha al massimo n radici incongrue[33]. Se essa possiede le n radici $\alpha_1, \alpha_2, \dots, \alpha_n$, il suo primo membro

$$p(x) \equiv (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)\alpha_0 \ \ (mod\ c)$$

[cioè la differenza dei due membri è un polinomio $\equiv 0\ (mod\ c)$, cioè un polinomio, i cui coefficienti sono divisibili per c].
Una radice della congruenza

$$p(x) \equiv 0 \ \ (mod\ K),$$

dove K è il prodotto di più interi $K_1, K_2, \dots, K_r$ è contemporaneamente radice delle congruenze

$$p(x) \equiv 0 \ \ (mod\ K_1)$$
$$p(x) \equiv 0\ (mod\ K_2)$$
$$\dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots$$
$$p(x) \equiv 0 \ \ (mod\ K_r).$$

// Questa osservazione è specialmente importante quando $K_1, K_2, \dots, K_r$ sono primi a due a due tra di loro (p. es. se $K = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, dove p_i sono primi distinti e $K_i = p_i^{n_i}$). In tal caso viceversa se x_i è una radice della $p(x) \equiv 0\ (mod\ K_i)$ si trova una radice della congruenza iniziale risolvendo il sistema delle

$$x \equiv x_i\ (mod\ K_i)\ (i = 1, 2, \dots, r)$$

dalle quali si ottiene x determinato $(mod\ K)$. E la congruenza data avrà pertanto $q_1, q_2, \dots, q_r$ soluzioni se la $p(x) \equiv 0\ \ (mod\ K_i)$ ne ha q_i.

[32] *e.c.* e *cor. sup.*: invece di $\beta \neq d$ leggasi $\beta \neq \alpha$.
[33] Dirichlet 1877 (trad. 1881), cap. II, §26, p. 56. L'enunciato di Fubini è identico a quello della traduzione italiana delle *Vorlesungen* a cura di Faifofer.

§.6 ***Il teorema di Wilson***[34]

La congruenza

$$x^{p-1} \equiv 1 \ (mod\ p)$$

dove p è un numero primo, ha per il teorema di Fermat proprio $p-1$ radici incongrue (i numeri primi con p; p. es. 1, 2, 3, … $p-1$). Dunque (cfr. §5)

$$x^{p-1} - 1 \equiv (x-1)(x-2) \dots [x-(p-1)] \ \ (mod\ p).$$

Confrontando i termini indipendenti da x si trova per $p > 2$, e quindi p dispari[35]:

$$-1 \equiv (p-1)! \ \ (mod\ p)$$

che è anche vera per $p = 2$. //

Viceversa, se vale questa congruenza, p è un numero primo. Sia infatti $a < p$ un divisore di p. Il numero a coinciderà con uno dei numeri $1, 2, 3, \dots, p-1$, e quindi sarà un divisore di $(p-1)!$. Ma esso deve essere pure un divisore di p, e quindi anche di $(p-1)!+1$, che per ipotesi è un multiplo di p. Dunque a è anche un divisore di 1. Cioè $a = 1$. Cioè l'unico divisore a di p, che sia minore di p, vale 1. Pertanto p è primo.

Dunque[36]:

Condizione necessaria e sufficiente, affinché un intero p sia primo, è che $(p-1)!+1$ sia multiplo di[37] p.

§.7 ***Radici primitive; indici*** [38]

[39]Se $p-1$ è divisibile per δ ed è $p-1 = \delta h$, allora posto $x^{\delta} = z$, è $x^{p-1} - 1 = z^h - 1$, che è divisibile per $z - 1 = x^{\delta} - 1$. Dunque

$$(x^{p-1} - 1) = \left(x^{\delta} - 1\right) q(x) \qquad (\alpha)$$

dove $q(x)$ è un polinomio a coefficienti interi di grado $p-1-\delta$. Dunque $q(x) \equiv 0\ (mod\ p)$ ha al più $p-1-\delta$ radici. Ora, per (α), ognuna delle $p-1$ radici di $x^{p-1} - 1 \equiv 0$ // $(mod\ p)$ è radice di $x^{\delta} - 1 \equiv 0$, oppure di $q(x) \equiv 0$.

Questa seconda congruenza ha, come dicemmo, al più $p-1-\delta$ radici; dunque la[40] $x - 1 \equiv 0$ ha almeno $p - 1 - [p-1-\delta] = \delta$ radici. Ma, essendo essa di grado δ, non può avere più di δ radici. Dunque essa ha proprio δ radici.

Dunque, se p è primo e δ è divisore di $p-1$, vi sono $(mod\ p)$ proprio δ numeri tali che[41]

---

[34] Gauss 1801, sez. III, art. 76-78, p. 60-62. Cfr. anche Cibrario 1929, p. 262-264.

[35] Per indicare il fattoriale di $p-1$ Fubini in questo paragrafo utilizza la notazione $\underline{\ p-1\ }$.

[36] Dirichlet 1877 (trad. 1881), cap. II, §27, p. 58.

[37] Gazzaniga 1903, cap. I, p. 21, prop. 44.

[38] Gazzaniga 1903, cap. IV, p. 72-75. Cfr. anche Gauss 1801, sez. III, art. 57, p. 46, 47. Qui Fubini riprende il titolo direttamente dall'art. 57 (*Radices primitivae, bases, indices*) delle *Disquisitiones*. Cfr. infine Weber 1895, vol. I, p. 585-594.

[39] Dirichlet 1877 (trad. 1881), cap. II, §27, p. 59. Fubini sviluppa la trattazione proprio come Dirichlet, pervenendo al medesimo risultato: "la congruenza $x^{\delta} \equiv 1\ (mod\ p)$, il cui grado δ è un divisore di $p-1$, ha sempre δ radici incongrue".

[40] *e.c.* e *cor. sup.*: $x^{\delta} - 1 \equiv 0$.

[41] *e.c.* e *cor. sup.*: $x^{\delta} - 1 \equiv 0$.

$$x^\delta - 1 \not\equiv 0 \ (mod\ p).$$

Viceversa sia a un qualsiasi numero[42] $\equiv 0 \ (mod\ p)$. Scriviamo le

$$a, a^2, a^3, a^4, \dots .$$

Per il teorema di Fermat è $a^{p-1} \equiv 1 \ (mod\ p)$. Sia $K \leq p-1$ il minimo intero tale che

$$a^K \equiv 1.$$

Se m, n sono $\leq K$, se $m \neq n$, sarà $a^m \not\equiv a^n$; perché, se fosse $a^m \equiv a^n$, e fosse, p. es., $m > n$, sarebbe $a^{m-n} \equiv 1 \ (mod\ p)$, mentre $m - n < K$; ciò che contraddice all'ipotesi fatta su K. Dunque i numeri

$$a, a^2, a^3, \dots, a^{K-1}, a^K \equiv 1$$

sono K numeri tra loro incongrui. I successivi[43]

$$a^{K+1}, a^{K+2}, a^{K+3}, \dots, 1a^{2K}$$

// sono ordinatamente congrui ai precedenti; altrettanto dicasi di

$$a^{2K+1},\ a^{2K+2}, \dots, a^{3K}$$

e così via. I soli numeri congrui ad $a^K \equiv 1$ sono a^{2K}, a^{3K}, a^{4K}, ecc. Poiché $a^{p-1} \equiv 1$, è dunque K un divisore di $p-1$. L'ipotesi fatta su K si enuncia dicendo che a appartiene all'esponente K. Dunque[44], se $a \not\equiv 0 \ (mod\ p)$ appartiene all'esponente K, allora K è un divisore di $p-1$.

Se δ è un divisore di $p-1$, tra i δ numeri che soddisfano alla $x^\delta - 1 \equiv 0$ quanti ve ne sono che appartengono all'esponente δ? Sia a un tal numero. Le sue potenze[45]

$$a, a^2, \dots,$$

a^δ sono δ numeri tra loro incongrui, che evidentemente soddisfano tutti alla

$$x^\delta - 1 \equiv 0.$$

Essi perciò, esauriscono le δ radici di tale congruenza. Uno di essi , p. es., a^r, appartiene all'esponente h, se h è il minimo intero tale che $(a^r)^h \equiv 1$, ossia tale che rh sia multiplo di δ. Dunque h è uguale al quoziente ottenuto divi//dendo δ per il M.C.D. di r, δ.

Dunque a^r appartiene all'esponente δ allora e allora soltanto che r è primo con δ . Dunque, poiché di interi $r \leq \delta$ primi con δ ce ne sono proprio $\varphi(\delta)$, vi sono nella nostra ipotesi $\varphi(\delta)$ numeri che appartengono all'esponente δ. La nostra ipotesi era che ci fosse almeno un numero a radice di $x^\delta - 1 \equiv 0$, che appartenesse all'esponente δ. Dunque[46]:

Se δ è un divisore di $p-1$, il numero $\psi(\delta)$ degli interi che appartengono all'esponente δ, o vale zero, o vale $\varphi(\delta)$. Ma ognuna delle $p-1$ radici di $x^{p-1} - 1 \equiv 0$ appartiene a

[42] *e.c.* e *cor. sup*: numero $\not\equiv 0 \ (mod\ p)$.
[43] *e.c.* e *cor. sup.*: invece di $1a^{2K}$ leggasi a^{2K}.
[44] Dirichlet 1877 (trad. 1881), cap. II, §28, p. 60. Fubini riprende chiaramente dalle *Vorlesungen* la definizione di appartenenza ad un dato esponente.
[45] *e.c.* e *cor. sup.*: $a, a^2, \dots, a^\delta$.
[46] Dirichlet 1877 (trad. 1881), cap. II, §29, p. 62, 63.

qualcuno di tali esponenti δ. Dunque $\sum \psi(\delta) = p - 1$. Ora $\psi(\delta) \leq \varphi(\delta)$, $\sum \varphi(\delta) = p - 1$. Dunque $\psi(\delta) = \varphi(\delta)$.
Cioè ad un divisore δ di $p - 1$ appartengono proprio $\varphi(\delta)$ numeri[47]. In particolare $\varphi(p - 1)$ interi appartengono all'esponente $p - 1$, e si dicono radici primitive[48] di p.
Per es. sia $p = 11, p - 1 = 10, \varphi(p - 1) = 4$. Il numero 2 e le sue successive potenze sono:[49]
//

$$2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5\ , 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1.$$

[50]Dunque 2 è una radice primitiva di 11. Le altre sono $2^3, 2^7, 2^9$, perché $1, 3, 7, 9$ sono i 4 interi ≤ 10 primi con 10, (cioè $2, 8, 7, 6$ sono le radici primitive di 11).
Se γ è una radice primitiva di p, gli interi

$$\gamma, \gamma^2, \gamma^3, \dots, \gamma^{p-2}, \gamma^{p-1} \equiv 1$$

Sono $(mod\ p)$ un sistema di numeri incongrui; ogni numero $r \not\equiv 0$ è congruo ad uno ed uno solo di essi. Se, p. es., $r \equiv \gamma^s$, dicesi $s = ind\ r$ (indice di r). L'indice[51] è l'analogo del logaritmo.[52]
Ci sono $\varphi(p - 1)$ sistemi di indici (tanti quante sono le radici primitive di p). Notiamo che $\gamma^s \equiv \gamma^\sigma\ (mod\ p)$ se $s \equiv \sigma\ (mod\ p - 1)$. Così, se un numero è determinato $(mod\ p)$, il suo indice è determinato $(mod\ p - 1)$. Solo i numeri $\equiv 0$ non hanno indice: altro punto di analogia con i logaritmi [così come $ind\ 1 \equiv 0\ (mod\ p - 1)$]. Così, se $p = 11$, posto[53] $\gamma = 1$ si ha la seguente tabella di indici[54]

Numeri	1	2	3	4	5	6	7	8	9	10
Indici	0	1	8	2	4	9	7	3	6	5

I numeri $2, 7, 8, 6$ che hanno gli indici $1, 7, 3, 9$ primi con 10 sono le altre radici primitive. Gli indici hanno ufficio analogo a quello dei logaritmi[55].

§.8 ***Congruenze binomie***[56]

In particolare essi possono servire a risolvere, quando possibile, la congruenza[57]

$$x^n \equiv D\ \ (mod\ p)$$

(che è l'operazione analoga a quella di estrazione di radice).

---

[47] Bianchi 1920-21, Introduzione, §4, p. 29.
[48] Dirichlet 1877 (trad. 1881), cap. II, §20, p. 63.
[49] *e.c.* e *cor. sup.*: $2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5$, ecc.
[50] Nota inserita da Fubini a p.d.p.: *Teoria dei numeri disp. 4*.
[51] Dirichlet 1877 (trad. 1881), cap. II, §30, p. 64.
[52] *Ibid.* L'autore scrive: "Manifestatamente tutto questo processo ha la più grande analogia con la costruzione delle tavole dei logaritmi, le quali sono basate sullo stesso concetto di rappresentare tutti i numeri positivi come potenze di un'unica base; anzi ora vedremo che nella teoria dei numeri gli indici seguono leggi analoghe, che i logaritmi, e che sono altrettanto opportuni per iscopi pratici".
[53] *e.c.* e *cor. sup.*: $\gamma = 2$.
[54] *Ibid.* Dirichlet fornisce qui un'analoga tabella per il primo $p = 13$.
[55] Gauss 1801, sez. III, art. 57, 58, p. 46-48. Palese è qui il riferimento a Gauss che per primo introduce la nozione di indice in analogia con le tavole dei logaritmi.
[56] Gazzaniga 1903, cap. IV, p. 68.
[57] Dirichlet 1877 (trad. 1881), cap. II, §31, p. 67. Cfr. anche Gauss 1801, sez. III, art. 60, *De radicibus congruentiae* $x^n \equiv A$, p. 48, 49. Cfr. infine Sommer 1907 (trad. 1911), cap. 1, §4, p. 11.

Se $D \equiv 0$, l'unica soluzione è $x \equiv 0$. Se $D \not\equiv 0$, prendendo gli indici dei due membri, si trova:

$$n\ ind\ x \equiv ind\ D \pmod{p-1}.$$

Se δ è il M.C.D. di n e di $p-1$, la congruenza è dunque risolubile soltanto quando $ind\ D$ è divisibile per δ. Ciò equivale a dire che[58] $D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$. Infatti $D^{\frac{p-1}{\delta}} \equiv \gamma^{\frac{p-1}{\delta} ind\ D}$. Poiché $\gamma^r \equiv 1$ soltanto quando r è multiplo di $p-1$, il numero $D^{\frac{p-1}{\delta}}$ sarà $\equiv 1$ soltanto se $\frac{p-1}{\delta}\ ind\ D$ è multiplo d i $p-1$, cioè $ind\ D$ multiplo di δ.
Se questa condizione è soddisfatta, la nostra congruenza è risolubile; D dicesi[59] residuo n^{esimo} (per $n=2$ residuo quadratico[60], o anche residuo // senz'altro).
Vi sono $\frac{p-1}{\delta}$ residui n^{esimi}; e $p-1-\frac{p-1}{\delta}$ non residui n^{esimi}.
[61]Per $n=2$ e p dispari vi sono $\frac{p-1}{2}$ residui,[62] $\frac{p-1}{z}$ non residui. I primi sono caratterizzati dalla $D^{\frac{p-1}{2}} \equiv 1$. Ora, per il teorema di Fermat[63]

$$0 \equiv D^{p-1} - 1 \equiv \left(D^{\frac{p-1}{2}} - 1\right)\left(D^{\frac{p-1}{z}} + 1\right) \quad (se\ p\ dispari).$$

Quindi per $n=2$ i residui sono caratterizzati dalla[64] $D^{\frac{p-1}{z}} \equiv 1$; i non residui dalla $D^{\frac{p-1}{2}} \equiv -1$ (se p primo dispari).
Per $p=2$, ogni numero $D \not\equiv 0$, cioè ogni D dispari è $\equiv 1^2$ ed è pertanto un residuo.
Supposto p primo e dispari, la congruenza

$$x^2 \equiv D \pmod{p^m} \quad [D \not\equiv 0 \pmod{p}]$$

è risolubile se è risolubile la $x^2 \equiv D \pmod{p}$, cioè se D è residuo (quadratico) di p. Ciò è evidente per $m=1$; e la condizione enunciata è evidentemente necessaria per ogni m. Basterà provare che, se essa è sufficiente per $m=h$, essa è anche sufficiente per $m=h+1$. Infatti se α è radice della nostra congruenza per $m=h$, cioè se $\alpha^2 - D \equiv 0 \pmod{p^h}$, si ponga $\beta = \alpha + p^h K$. Sarà

$$\beta^2 = \alpha^2 + 2p^h \alpha K + p^{2h} K^2 \equiv \alpha^2 + 2\alpha K p^h \pmod{p^{h+1}}. //$$

Sarà β radice della $x^2 \equiv D \pmod{p^{h+1}}$, se[65] $\alpha^2 + 2\alpha K p^h \equiv D \pmod{p^{h+1}}$.
Ora $\alpha^2 = D + lp^h$ dove l (come ogni altra lettera) indica un intero. La nostra congruenza diventa:

---

[58] *Idem*, cap. II, §31, p. 68, 69.
[59] *Idem*, cap. II, §31, p. 69, 70. Scrive l'autore: "Questi numeri D, che sono congrui ad una potenza ennesima di un numero, sono detti brevemente residui ennesimi […]. Quando è $n = 2,3,4$, questi numeri diconsi rispettivamente residui quadratici, cubici, biquadratici."
[60] Bianchi 1920-21, Introduzione, §4, p. 32. Bianchi fornisce qui la stessa spiegazione dei residui quadratici ma, al contrario di Fubini, prosegue la trattazione introducendo il simbolo $\left[\frac{D}{\pi}\right]$ di Dirichlet.
[61] Dirichlet 1877 (trad. 1881), cap. III, §32, p. 71-73.
[62] *e.c.* e *cor. sup.*: $\frac{p-1}{2}$.
[63] *e.c.* e *cor. sup.*: $0 \equiv D^{p-1} - 1 \equiv \left(D^{\frac{p-1}{2}} - 1\right)\left(D^{\frac{p-1}{2}} + 1\right)$.
[64] *e.c.* e *cor. sup.*: $\frac{p-1}{2}$.
[65] *e.c.* e *cor. sup.* che ha reso illeggibile il testo originale.

$$p^h(l + 2\alpha K) \equiv 0\ (mod\ p^{h+1}), \text{cioè}$$
$$l + 2\alpha K \equiv 0\ \ (mod\ p);$$

l'incognita K si può certo determinare, perché il suo coefficiente 2α è primo con p.
Quante radici ha la $x^2 \equiv D\ (mod\ p^m)$ (se risolubile)?
Se α, β sono due radici distinte sarà $\alpha^2 - \beta^2 \equiv 0$, cioè $(\alpha - \beta)(\alpha + \beta) \equiv 0$.
Ora $\alpha - \beta$ e $\alpha + \beta$ non possono entrambe essere divisibili per $\underline{p}$, perché altrettanto avverrebbe della loro somma 2α che per ipotesi è prima con p. Dunque o $\alpha - \beta$ oppure $\alpha + \beta$ sono divisibili per p^m. Ma, poiché $\alpha \not\equiv \beta$, sarà $\alpha + \beta \equiv 0$, cioè $\alpha \equiv -\beta$. E, viceversa, se $\underline{\alpha}$ è radice, anche $-\alpha$ (che è $\not\equiv \alpha$) sarà un'altra radice. Dunque la nostra congruenza avrà <u>zero</u> radici, se D è non residuo di p, mentre avrà <u>due</u> radici, se D è residuo.
Per $p = 2$ la $x^2 \equiv D\ (mod\ 2)$ con $D \not\equiv 0\ (mod\ p)$ è, come dicemmo, sempre risolubile in un solo modo; la // $x^2 \equiv D\ (mod\ 2^2)$ è risolubile soltanto se[66] $D \equiv 1\ (mod\ 4)$, perché essendo x dispari, cioè $x = 2y + 1$, sarà $x^2 \equiv 1\ \ (mod\ 4)$. E in tal caso ogni numero dispari risolve la congruenza, che perciò $(mod\ 4)$ avrà due radici distinte (p.es. ± 1) . La[67] $x^2 \equiv D\ (mod\ 8)$ sarà risolubile e avrà le quattro radici $1, 3, 5, 7$ incongrue $(mod\ 8)$ soltanto se $D \equiv 1\ (mod\ 8)$ perché il quadrato di ogni numero dispari $4n \pm 1$ è $\equiv 1\ \ (mod\ 8)$.
E, col metodo d'induzione completa, si prova facilmente (ciò che sarà utile esercizio al lettore) che la $x^2 \equiv D\ (mod\ 2^m)$ con $m \geq 3$ è risolubile, e in tal caso ammetterà 4 radici, soltanto se $D \equiv 1\ (mod\ 8)$.
In generale, per l'ultima osservazione del paragrafo 5, [68]indicando con P_i sono[69] gli eventuali fattori dispari primi distinti di K [70]la congruenza[71]

$$x^2 \equiv D\ (mod\ K);\quad se\ K = 2^\sigma p_2^{m_1} p_2^{m_2} \dots p_r^{m_r}$$

sarà risolubile allora e allora soltanto che sono risolubili le

$$x^2 \equiv D\ (mod\ 2^\sigma)$$
$$x^2 \equiv D\ \left(mod\ p_i^{m_i}\right)\ (i = 1, 2, \dots, r)$$

dove è da sopprimersi la prima congruenza se K è dispari, e mancano invece le altre se $K = 2^\sigma$ non ha fattori primi dispari. //
In virtù dell'osservazione citata, troviamo[72]:
1°) Se K è dispari $(\sigma = 0)$, la nostra congruenza è risolubile, soltanto quando D è residuo di tutti gli r fattori primi distinti di K, ed ha in tal caso 2^r radici.
2°) Se K è il doppio di un numero dispari, vale lo stesso teorema.
3°) Se K è il quadruplo di un numero dispari $(\sigma = 2)$, bisogna in più che $D \equiv 1\ (mod\ 4)$ e la congruenza ha 2^{r+1} radici.
4°) Se K è il prodotto di un numero dispari per 2^σ con $\sigma \geq 3$, la congruenza è risolubile soltanto quando $D \equiv 1\ (mod\ 8)$ ed ha in tal caso 2^{r+2} radici.
Sia <u>p primo dispari.</u>

---

[66] Dirichlet 1877 (trad. 1881), §36, p. 79.
[67] *Ibid.*
[68] *cor. sup.* e *a.m.* per "indicando con".
[69] *e.c.*: invece di "P_i sono" leggasi "p_i gli".
[70] *a.m.* e *ad. post.* per "la congruenza".
[71] *e.c.*: $x^2 \equiv D\ (mod\ K)$; se $K = 2^\sigma p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$.
[72] Gazzaniga 1903, cap. IV, p. 89. Fubini qui generalizza i risultati di Gazzaniga.

Se $D \equiv 0\ (mod\ p)$ e p è primo, si pone $\left(\frac{D}{p}\right) = 0$

Se $D \not\equiv 0$ e p è primo, si pone[73] con Legendre $\left(\frac{D}{p}\right) = 1$ se D è residuo di p; $\left(\frac{D}{p}\right) = -1$ se D è non residuo di p.

Evidentemente[74]

$$\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right).$$

Dunque $\left(\frac{m}{p}\right) = 1$ è la condizione necessaria e sufficiente affinchè m sia residuo (quadratico) di p. //

[75]Se P è positivo dispari non primo, e se m è primo con P, porremo con Jacobi $\left(\frac{m}{P}\right)$ uguale al prodotto[76]

$$\left(\frac{m}{p}\right)\left(\frac{m}{p_1}\right)\left(\frac{m}{p_{11}}\right) \ldots \text{ se } P = p\ p^I p^{II} \ldots \text{ con } p, p^I, p^{II} \text{ numeri primi.}$$

Dunque $\left(\frac{m}{P}\right) = +1$ equivale non al fatto che m sia residuo di P, ossia di tutti i fattori primi di P, ma soltanto a questo che m sia non-residuo di un numero pari (cioè $0, 2, 4, \ldots$) di fattori primi di P. Soltanto se P è primo, la $\left(\frac{m}{P}\right) = +1$ equivale all'essere m residuo di P.

In ogni caso il simbolo[77] $\left(\frac{m}{P}\right)$ è definito e vale ± 1, se P è dispari, ed m è primo con P.

Dimostrare[78]:

α) [79]Se $m \equiv n\ (mod\ P)$ allora $\left(\frac{m}{P}\right) = \left(\frac{n}{P}\right)$.

β) [80]Se m è primo coi dispari P, q allora $\left(\frac{m}{Pq}\right) = \left(\frac{m}{P}\right)\left(\frac{m}{q}\right)$.

γ) [81]Se m, n sono primi con P è $\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) = \left(\frac{mn}{P}\right)$. (Lo si è già osservato se P è primo e lo si può generalizzare; se P è primo, questa formola dice che: il prodotto di due residui o di due non residui è un residuo; il prodotto di un residuo per un non-residuo è un non-residuo). //

δ) $\left(-\frac{1}{P}\right) = (-1)^{\frac{P-1}{2}}$ (Lo si dimostri prima se P è primo e poi lo si dimostri in generale per P positivo).[82]

---

[73] Sommer 1907 (trad. 1911), cap. 1, §4, p. 11.

[74] *Idem*, cap. 1, §4, p. 12: "Cette dernière égalité nous donne la règle de la multiplication qui permet de ramener le calcul de ce symbole $\frac{p}{q}$ a u cas où q et p sont premiers".

[75] Dirichlet 1877 (trad. 1881), cap. III, §46, p. 99.

[76] *e.c.*: $\left(\frac{m}{p}\right)\left(\frac{m}{p^I}\right)\left(\frac{m}{p^{II}}\right)$.

[77] Gazzaniga 1903, cap. IV, p. 92.

[78] Dirichlet 1877 (trad. 1881), cap. III, §46, p. 99-105. Dirichlet dimostra tutte queste proprietà che invece Fubini lascia allo studente.

[79] *Idem*, cap. III, §46, p. 101, prop. 3.

[80] *Idem*, cap. III, §46, p. 100, prop. 1.

[81] *Ibid*., prop. 2. Dirichlet enuncia tale proprietà nel caso di un numero generico di fattori.

[82] *Idem*, cap. III, §46, p. 102, prop. 5. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §24, p. 122.

Nel seguito del corso proveremo in più il cosiddetto teorema di reciprocità[83] (che enunciato da Eulero[84] e Legendre fu dimostrato solo da Gauss[85]) e il suo complemento (intuito da Fermat, dimostrato da Lagrange):
$\left(\frac{P}{q}\right)\left(\frac{q}{P}\right) = (-1)^{\frac{P-1}{2}\,\frac{q-1}{2}}$ [86] se P, q sono positivi dispari primi tra loro[87]

$$\left(\frac{q}{P}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Queste formule servono a calcolare in ogni caso per numeri primi tra loro il valore del simbolo di Legendre-Jacobi[88]. Si calcoli[89] p. es. $\left(\frac{365}{1847}\right)$ dove 365 e 1847 sono primi tra loro. È[90]

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right) = \left(\frac{365\cdot 3+22}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right) = -\left(\frac{11}{365}\right) = -\left(\frac{365}{11}\right)$$
$$= -\left(\frac{11\cdot 33+2}{11}\right) = -\left(\frac{2}{11}\right) = +1.$$

§.9 ***Applicazioni ed esercizi***

Dato il modulo K, noi abbiamo già trovato come se ne trovano i residui D, cioè i numeri D primi con K, (*) per // cui è risolubile la $x^2 \equiv D\ (mod\ K)$. Il problema reciproco è il seguente: Dato D, come si trovano i numeri K primi con D, di cui D è residuo?[91]
Notiamo che le due congruenze[92]

$$x^2 \equiv D \qquad x^2 \equiv Dn^z \pmod K$$

sono risolubili contemporaneamente, perché se $\underline{\alpha}$ è radice della prima, αn è radice della seconda, e se β è radice della seconda, il numero α determinato dalla $n\alpha \equiv \beta$ è radice della

---

[83] Attualmente l'enunciato è noto come legge di reciprocità quadratica.
[84] Euler enunciò tale risultato nello scritto *Theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ *centorum* (1744-46). Cfr. *Opera Omnia*, I-2, p. 194-222.
[85] Gauss scoprì tale legge intorno al 1795 e fu il primo a darne una dimostrazione generale nelle *Disquisitiones Arithmeticae*; Gauss fu assai fiero di tale risultato, da lui chiamato *Aureum Theorema*, tanto che negli anni ne pubblicò svariate dimostrazioni. Cfr. Gauss 1801, sez. IV, p. 101-113.
[86] Gazzaniga 1903, cap. IV, p. 98. Cfr. anche Dirichlet 1877 (trad. 1881), cap. III, §46, p. 103, prop. 6. Cfr. infine Sommer 1907 (trad. 1911), cap. 1, §4, p. 13 e cap. 2, §25, p. 123.
[87] *Idem*, cap. V, p. 102. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §24, p. 122.
[88] Fubini qui si riferisce al simbolo, che oggi viene semplicemente chiamato 'simbolo di Jacobi', definito come segue. Sia $n > 2$ un numero naturale dispari e $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$; per ogni intero a, il simbolo di Jacobi è $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\dots\left(\frac{a}{p_k}\right)^{\alpha_k}$ dove $\left(\frac{a}{p}\right)$ con p primo è il cosiddetto simbolo di Legendre che, a sua volta, è uguale a
$$\begin{cases} 0 \text{ se } p \text{ divide } a \\ 1 \text{ se } a \text{ è un quadrato } (mod\ p) \\ -1 \text{ se } a \text{ non è un quadrato } (mod\ p) \end{cases}$$
Si pone $\left(\frac{a}{1}\right) = 1$ per convenzione.
[89] Dirichlet 1877 (trad. 1881), cap. III, §47, p. 105. Dirichlet fornisce qui lo stesso esempio, svolgendo i conti più nel dettaglio rispetto a Fubini.
[90] *e.c.* e *cor. sup.*: invece di $\left(\frac{365\cdot 3+22}{365}\right)$ leggasi $\left(\frac{365\cdot 5+22}{365}\right)$.
[91] Dirichlet 1877 (trad. 1881), cap. III, §32, p. 72. Il matematico tedesco si pone qui questo problema, che verrà risolto solo nei paragrafi successivi.
[92] *e.c.* e *cor. sup.*: invece di $x^2 \equiv Dn^z$ leggasi $x^2 \equiv Dn^2$.

prima. (Notisi che D, Dn^2 sono in questo studio supposti primi con K, dunque anche n è primo con K; e pertanto tale congruenza è risolubile).
Possiamo dunque limitarci al caso che D non sia divisibile per alcun quadrato, cioè sia prodotto di fattori primi distinti. I numeri K avranno per fattori primi solo dei numeri, per cui D è residuo. Noi dunque potremmo, come parte principale di tale studio, limitarci a cercare i primi dispari p, per cui D è residuo (Il caso $p = 2$ si esaurisce tosto senza alcuna difficoltà).[93]
Il problema così ridotto si può porre sotto altra forma equivalente. Trovare i p per cui è risolubile // la $x^2 - D \equiv 0$, equivale a cercare i p, che possono essere divisori del polinomio $x^2 - D$ per qualche valore di x. Ciò equivale a cercare i p che possono essere divisori di $x^2 - Dy^2$, quando ad x, y si dieno valori primi tra di loro.
Infatti un p divisore di $x^2 - D$ per $x = x_0$ è anche divisore di $x^2 - Dy^2$ per $x = x_0$, $y = 1$. E un divisore di $x^2 - Dy^2$ per $x = x_0, y = y_0$, (x_0, y_0 primi tra loro) è anche divisore di $x^2 - D$, quando x è $x_0 y_1$, essendo y_1 una radice di $y_0 y \equiv 1\ (mod\ p)$. Si osservi innanzitutto che questa congruenza è risolubile perché y_0 è primo con p [In caso opposto dalla $x^2 - Dy_0^2 \equiv 0\ (mod\ p)$ si dedurrebbe che anche x_0 è divisibile per p, cioè che x_0, y_0 non sarebbero, come supporremo, primi tra loro].
E ne segue

$$y_1^2(x_0^2 - Dy_0^2) \equiv (y_1 x_0)^2 - (y_1 y_0)^2 D \equiv (y_0 x_0)^2 - D\ \ (mod\ p).$$

Essendo $x_0^2 - Dy_0^2 \equiv 0\ \ (mod\ p)$, anche $(yy_0)^2 - D$ sarebbe divisibile per p.
La nostra ricerca equivale dunque a cercare i cosiddetti divisori p della forma

$$x^2 - Dy^2.$$

// Il numero D, privo di fattori quadratici, è del tipo $\pm P$, oppure $\pm 2P$, dove P è prodotto di fattori primi distinti.
I numeri p che noi cerchiamo sono quelli dei numeri dispari n per cui $\left(\frac{D}{n}\right) = +1$, che sono interi primi. E noi possiamo cercare senz'altro tutti questi numeri n anche non primi.
Bisogna distinguere i due casi[94]: $\pm P \equiv 1$ oppure $\pm P \equiv 3\ (mod\ 4)$. Noi qui studiamo solo il caso[95]
$D \equiv 1\ (mod\ 4)$, lasciando al lettore lo studio degli altri casi, che si trattano con metodo perfettamente analogo.
Sia $D \equiv 1\ (mod\ 4), D = \pm P$. Allora: $\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right)$.
Ciò è evidente se $D = P \equiv 1\ (mod\ 4)$ per il teorema di reciprocità.
Se invece
$D = -P$, è $\left(\frac{D}{n}\right) = \left(-\frac{1}{n}\right)\left(\frac{P}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{P}{n}\right) = (-1)^{\frac{n-1}{2}+\frac{n-1}{2}\frac{P-1}{2}}\left(\frac{n}{P}\right) = \left(\frac{n}{P}\right)$ perché dalla $D \equiv 1\ (mod\ 4)$ si trae che $\frac{P-1}{2}$ è dispari.

---

[93] Dirichlet 1877 (trad. 1881), cap. III, §39, p. 85.
[94] La distinzione di questi due casi effettuata da Fubini discende direttamente da quanto esposto da Gauss nelle *Disquisitiones* a proposito della teoria dei residui quadratici (sez. VI, art. 131). Infatti per il teorema fondamentale di tale teoria si ha che "se *p* è un numero primo della forma *4n+1*, allora *+p*, se *p* è della forma *4n+3*, allora *–p*, saranno residui [quadratici] (rispettivamente non residui) di ogni numero primo positivo che sia un residuo (rispettivamente un non residuo) di *p*".
[95] Dirichlet 1877 (trad. 1881), cap. III, §52, p. 117, 118. Dirichlet studia ampiamente questo caso; affronta poi (p. 119-121) nel dettaglio anche i casi $\pm P \equiv 3\ (mod\ 4)$, $\pm 2P \equiv 2\ (mod\ 8)$, $\pm 2P \equiv 6\ (mod\ 8)$.

Dunque si devono cercare i numeri n per cui $\left(\frac{n}{P}\right) = +1$. Dunque basterà esaminare i $\varphi(P)$ numeri positivi non maggiori di P e primi con P. Di questi almeno uno $\underline{h}$ soddisfa alla // $\left(\frac{h}{P}\right) = -1$. (Basta scegliere un $\underline{h}$ che sia residuo di tutti i fattori primi di P uno eccettuato).
Poiché se m', m sono due dei citati $\varphi(P)$ numeri è $\left(\frac{m\,m'}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{m'}{p}\right)$ ogni numero m per cui $\left(\frac{m}{p}\right) = 1$ ne individua uno $m' \equiv hm \ (mod\ P)$ tale che $\left(\frac{m'}{p}\right) = -1$.
Viceversa dato un tale m', la $m' \equiv hm\ (mod\ P)$ individua un $\underline{m}$ tale che $\left(\frac{m}{P}\right) = +1$.
Dunque i nostri $\varphi(P)$ numeri si dividono in due classi di $\frac{1}{2}\varphi(P)$ numeri ciascuna, tali che soltanto i numeri $\underline{n}$ della prima soddisfano alla $\left(\frac{n}{p}\right) = +1$.
I numeri $\underline{n}$ cercati sono perciò compresi in $\frac{1}{2}\varphi(P)$ progressioni aritmetiche di differenza P. Anzi, siccome dobbiamo trascurare i numeri di queste progressioni che sono pari, ci ridurremo a progressioni aritmetiche di differenza $2P$.
Che in tali progressioni vi siano proprio infiniti numeri primi è un teorema che soltanto l'aritmetica analitica è finora in grado di dimostrare. //

Osservazione
Ritorneremo più avanti sul teorema di reciprocità[96] e complementi. Qui ci accontentiamo di dimostrare che per ogni n dispari[97]

$$\left(-\frac{1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Se $\underline{n}$ fosse primo, ciò è evidente. Infatti -1 è residuo, o no di $\underline{n}$, cioè[98] $\left(-\frac{1}{p}\right)$ vale $+1$ oppure -1 secondo che $(-1)^{\frac{n-1}{2}} \equiv 1$ oppure $(-1)^{\frac{n-1}{2}} \equiv -1\ (mod\ n)$
cioè[99]

$$\left(-\frac{1}{p}\right) \equiv (-1)^{\frac{n-1}{2}}\ (mod\ n) \qquad (**)$$

Poiché i due membri valgono entrambi ± 1, se ne deduce l'asserto.
Sia $\underline{n}$ non primo, e sia $n = p_1 p_2 \dots p_r$ (p_i = numero primo dispari).
È per definizione e per quanto si è ora provato

$$\left(-\frac{1}{n}\right) = \left(-\frac{1}{p_1}\right)\left(-\frac{1}{p_2}\right)\dots\left(-\frac{1}{p_r}\right) = (-1)^{\left(\frac{p_1-1}{2}\right) + \frac{p_2-1}{2} + \dots + \frac{p_r-1}{2}}. \qquad (\alpha)$$

// Posto

$$\frac{p_i - 1}{2} = q_i \quad \text{è } n = (1+2q_1)(1+2q_2)\dots(1+2q_r)$$

---

[96] Bianchi 1920-21, Introduzione, §6, p. 38-41. Qui Bianchi tratta in modo più approfondito e più generale il teorema di reciprocità nel campo degli interi di Gauss.
[97] Gazzaniga 1903, cap. V, p. 102. Cfr. anche Dirichlet 1877 (trad. 1881), cap. III, §46, p. 102, prop. 5. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §25, p. 127.
[98] *e.c.*: $\left(-\frac{1}{n}\right)$.
[99] *e.c.*: $\left(-\frac{1}{n}\right) \equiv (-1)^{\frac{n-1}{2}}\ (mod\ n)$.

donde

$$\frac{n-1}{2} \equiv (q_1 + q_2 + \cdots + q_r) \pmod 2.$$

Ricordando il valore di q_r e la (α) se ne trae:

$$\left(-\frac{1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

c.d.d.

Esercizi

Sia K un intero dato non primo; se $K = 4$, oppure K è potenza [100]o due volte la potenza di un primo dispari; poniamo $\sigma = 1$; poniamo $\sigma = 0$ negli altri casi. Il prodotto dei $\varphi(K)$ numeri primi con K e non maggiori di K è $(mod\ K)$ congruo con $(-1)^\sigma$. Questo è il teorema di Wilson generalizzato.

Infatti ogni numero $r < K$ primo con K definisce un numero $s < K$ primo con K tale che $rs \equiv 1\ (mod\ K)$. Ed è $r \equiv s$, soltanto se r è radice della $x^2 \equiv 1\ (mod\ K)$. Di tali radici ve ne sono 2 se K è uguale a 4 od è potenza [101] o due volte la potenza di un primo dispari; negli altri casi il numeri di tali radici è multiplo di 4.

Poiché ogni radice ρ è accompagnata dalla $\rho' \equiv -\rho\ (mod\ K)$, cosicché $\rho\rho' \equiv -1\ (mod\ K)$, e gli altri numeri, che non sono radici, si distribuiscono // in coppie di numeri r, s, il cui prodotto è $\equiv 1$; risulta il teorema.

Si può costruire una teoria delle radici primitive e degli indici per i numeri primi con p^n (se $\underline{p}$ è primo dispari), in guisa che numeri congrui $(mod\ p^n)$ abbiano indici congrui $[mod \varphi(p^n)]$.

Basta dimostrare che: Se γ è radice primitiva di p, esiste un $g \equiv \gamma\ (mod\ p)$ tale che $g^{p-1} - 1$ è divisibile per p, ma non per p^2. Si dimostra per induzione completa che g è una radice primitiva di $p^2, p^3, \ldots$ Cioè $g^r \equiv 1\ (mod\ p^n)$ soltanto se $\underline{r}$ è multiplo di $\varphi(p^n)$. Si studino a parte i numeri 2, 4 e si provi per induzione completa che per $n \geq 3$ ogni dispari m è congruo con un numero $(-1)^{\alpha_\sigma \beta}\ (mod\ 2^n)$, dove $\alpha = 1$, oppure 2 e β non può superare $\frac{1}{2}\varphi(2^n)$. Dunque $(mod\ 2^n)$ un dispari ha per indice non un solo intero, ma una coppia di interi α, β. Per un modulo $K = 2^n p^\pi p_1^{\pi_1} \ldots$ (con $p, p_1, \ldots$ primi dispari) ogni numero h primo con K ha per indice un sistema di interi, costituito da vari indici di h rispetto ai moduli $2^n, p^\pi, p_1^{\pi_1}$, ecc. //

(*) **Nota**: Se D non[102] fosse primo con K, un primo p, fattore comune di D, K, sarebbe anche fattore di x. Si potrebbero dividere i due membri della congruenza (posto $x = py$) ed il modulo per tale p, ecc. ecc.

(**) **Nota**: Cioè -1 è residuo di quei numeri primi dispari che sono $\equiv 1\ (mod\ 4)$, è non residuo di quelli che sono $\equiv 3\ (mod\ 4)$

---

[100] *ad. post.* e *a.m.*: "o due volte la potenza".
[101] *ad. post.* e *a.m.*: "o due volte la potenza".
[102] *e.c.*: Se D fosse primo…

Capitolo III – Geometria dei numeri [1]

§.1 ***Rete di punti***[2]

Scegliamo due assi cartesiani qualsiasi, prefissando poi a piacere per ogni asse la corrispondente unità di misura (che può anche pertanto essere differente da un asse all'altro).
Indicheremo con O l'origine $x = y = 0$.
I punti $x = m, y = n$ (m, n) formano una cosiddetta rete di punti[3], che è il luogo dei punti a coordinate intere, è per così il dire il piano della teoria dei numeri, e si presta bene allo studio dell'analisi indeterminata in due incognite.
Le rette $x = m$ e le rette $y = n$ $(m, n$ interi), dividono il piano in infiniti parallelogrammi uguali e similmente orientati, che hanno per vertici tutti e soli i punti della rete citata. Noi diremo che essi formano una rete di parallelogrammi[4] dedotta dalla precedente rete[5] // di punti.
La rete di punti si presta bene ad interpretare qualche fatto geometrico. Così, per esempio, se A è un punto della rete di coordinate x, y il fatto che x, y siano primi tra loro si interpreta geometricamente dicendo che il segmento OA non contiene altri punti della rete.
La nostra rete di punti gode delle seguenti proprietà:
1°) In una regione finita del piano xy esiste un numero finito di punti della rete.
2°) Se A, B, C sono tre punti della rete, il punto[6] dedotto da C con la traslazione AB (tale cioè che AD sia la somma geometrica di AB, AC) appartiene ancora alla rete.
3°) I punti della rete non sono in linea retta. (Se i punti d'una figura godono delle proprietà 1, 2 e non della terza, essi sono punti di una retta, tali che ognuno di essi ha un precedente e un successivo e che la distanza di due punti consecutivi sia una costante).
Viceversa proveremo che, se una figura F di punti gode delle proprietà 1, 2, 3, essa è una // rete di punti, che in infiniti modi si può generare nel modo sopra definito. Ecco qui il metodo più generale che serve a tale scopo. Siano O, A due punti di F; sulla retta OA per la proprietà 1° di F esisteranno due punti di F che hanno da O la minima distanza possibile e che per 2° determineranno un segmento, di cui O è il punto di mezzo. Indichiamo senz'altro con A uno di questi punti. Per la proporzione[7] 2° è allora evidente che sulla retta OA cadono infiniti punti di F, che definiscono sulla retta una punteggiata tale che due punti consecutivi hanno una distanza costante uguale ad OA. Assumendo OA come asse delle x, O come origine, OA come unità di misura, tali punti sono quei punti di OA, la cui ascissa è un intero. Se B è un

[1] Gli argomenti illustrati da Fubini in questo capitolo non sono trattati né da Gazzaniga (*Gli elementi della teoria dei numeri*), né da Bianchi (*Lezioni sulla teoria dei numeri algebrici e di aritmetica analitica*) con l'unica eccezione della Nota III dove si forniscono alcuni cenni alle applicazioni geometriche. Alcuni di questi argomenti vengono invece trattati in un'altra opera di Bianchi, *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie*, anche se in modo parzialmente differente. Sottolineiamo, infine, come il tema della geometria dei numeri non compaia neppure nelle *Vorlesungen* di Dirichlet, motivo per il quale possiamo supporre che Fubini per la stesura di questo capitolo si sia basato quasi esclusivamente sulle opere di Klein, Sommer e Minkowski.
[2] Klein 1896, p. 2, 3. Qui Klein introduce i concetti di "punktgitter" e "parallelgitters" cui chiaramente Fubini si rifà nelle sue *Lezioni.* Cfr. anche Minkowski 1957, p. 20. Fubini riprende fedelmente la costruzione della griglia di punti fatta da Minkowski all'interno del paragrafo *Geometrische Darstellung des Zahlengitters.* Cfr. infine Sommer 1907 (trad. 1911), cap. 3, §38, p. 230: "La figure formée per l'ensamble de ces points […] s'appelle un *réseau régulier de points* (Punktgitter), et un de ces points est dit un *sommet* (ou un *point*) du réseaux".
[3] Bianchi 1911-12, cap. XIII, §132, p. 605. Qui si introduce il concetto di "reticolo di punti" in modo leggermente differente da Fubini, ossia come "sistema dei nodi di una rete parallelogrammica".
[4] *Idem*, cap. XIII, §131, p. 602. A differenza di Fubini, Bianchi introduce il concetto di rete di parallelogrammi associata ad una forma binaria definita. Cfr. anche Minkowski 1957, p. 24-28 e Klein 1896, p. 2, 3.
[5] Nota inserita da Fubini a p.d.p.: *Teoria dei Numeri Disp. 5.*
[6] *e.c.* e *cor. inf.* sul lato destro del foglio: il punto D.
[7] *e.c.* e *cor. sup.*: proposizione.

altro punto di F, i punti dedotti da B con una traslazione uguale o multipla di OA sono ancora (per 2) punti di F posti su una retta parallela ad OA; cioè i punti di F si distribuiscono su infinite parallele ad OA. Per la prima proprietà esisterà da ciascuna banda di OA // una di queste rette che da OA ha la minima distanza possibile. Sia MN una di tali due rette e siano B, C due punti di tale retta, appartenenti ad F, la cui distanza sia uguale ad OA. Se il verso BC è concorde ad OA, allora il parallelogrammo $OACB$ evidentemente contiene, oltre i vertici, nessun altro punto di F, ed altrettanto avverrà evidentemente dei parallelogrammi, che si deducono dal precedente applicando ad esso ripetutamente le traslazioni definite dai suoi lati. Tutti questi parallelogrammi ricoprono evidentemente tutto il piano una e una sola volta; i loro vertici sono pertanto tutti e soli i punti di F. Se assumiamo le rette OA, OB come assi delle x, y e i segmenti OA, OB come rispettive unità di lunghezza, i punti di F sono i punti a coordinate intere, cioè F è effettivamente una rete di punti. Come si vede, è rimasta arbitraria l'origine O, da scegliersi tra i punti da F, la retta OA purché contenente, oltre O, altri punti della rete, e infine il punto B da scegliersi tra quelli dei // punti di F, che hanno la minima distanza possibile dalla retta OA.
Corrispondentemente a questa generazione di F come rete di punti, abbiamo trovato una rete di parallelogrammi[8] dedotta da F. E risulta ben chiaro da quanto precede che da F si possono dedurre infinite reti di parallelogrammi, la cui indeterminazione si deduce pure tosto da quanto si è detto[9].
Per definire un'altra delle reti di parallelogrammi dedotta da F, basta dare un solo parallelogrammo della nuova rete (che evidentemente determina tutti gli altri) p. es. quel parallelogrammo della nuova rete che ha un vertice in O. Basterà dare i due lati OA', OB' di tale parallelogrammo. E, come sappiamo, il primo è posto su una retta qualsiasi uscente da O, che contenga oltre O altri punti della rete, A' è uno dei due punti di F, che giacciono su tale retta e che hanno da O la minima distanza possibile; B' è uno dei punti della rete che da OA' ha la minima distan//za possibile. (*)
Come si vede, le coordinate di A' nel primitivo sistema di assi OA, OB, possono essere due numeri x_0, y_0 qualsiasi primi tra di loro; e il punto B si può poi scegliere ad arbitrio tra quei punti (x, y) che rendono minimo $|x\, y_0 - y x_0|$ (che, a meno di un fattore, coincide con la distanza da (x, y) alla retta OA').
Ora, se x_0, y_0 sono primi tra di loro, tale espressione si può, come sappiamo, rendere uguale ad 1, e perciò, posto $B' = (x_1, y_1)$, gli interi x_1, y_1 si possono scegliere ad arbitrio tra quelli tali che $x_1 y_0 - x_0 y_1 = \pm 1$.
Ricordando il significato del primo membro se ne deduce un teorema notevole:
Comunque si vari la rete dei parallelogrammi dedotta da una rete di punti, l'area di un parallelogrammo generatore della rete è sempre la stessa; e noi la sceglieremo // come unità di misura delle aree (che è così definita dal parallelogrammo che ha due lati concorrenti sui due assi coordinati uguali alla corrispondente unità di misura delle lunghezze). [10]

[8] Sommer 1907 (trad. 1911), cap. 3, §38, p. 231: "Considérons un double système de parallèles, tel que tout sommet soit l'intersection de deux parallèles, et que deux parallèles voisines soient toutjours équidistantes, nous dirons que nous avons formé un *réseaux de parallèles*".
[9] *Idem*, cap. 3, §38, p. 232: "On voit de plus que ces parallélogrammes peuvent se déduire les uns des autres èar des translations parallèles aux axes, et mesurées par des nombres entiers".
[10] *Idem*, cap. 3, §38, p. 231: "Nous appellerons *parallélogramme élémentaire* ou *maille* du réseau, un parallélogramme qui ne contient aucun point à l'intériuer de son aire. Les mailles recouvrent totu le plan sans discontinuité. Un réseau est parfaitement determine par une maille donnée, en grandeur et en position".

Noi ci siamo qui serviti sia di considerazioni geometriche, sia del teorema aritmetico che l'equazione $xy_0 - x_0y = \pm 1$ è sempre risolubile in numeri interi, se x_0, y_0 sono primi tra di loro.
Noi vogliamo ritrovare questi risultati dapprima per via puramente aritmetica, poi per via puramente geometrica; dal che si potrebbe dedurre per via geometrica il teorema precedente relativo all'analisi indeterminata di primo grado.
Siano x, y ed X, Y due sistemi di coordinate cartesiane tali che in entrambi i punti di F siano i punti a coordinate intere. Con una traslazione potremo ridurci a due sistemi, con l'origine comune, senza che con ciò muti la enunciata proprietà dei punti di F e senza che cambino i parallelo//grammi relativi. Dalla geometria analitica sappiamo che sarà:

$$\begin{aligned} X &= ax + by \\ Y &= cx + dy \end{aligned} \qquad (ad - bc \neq 0)\ (a, b, c, d = \text{cost.}).$$

Poiché a valori interi di x, y devono corrispondere valori interi delle X, Y, le a, b, c, d saranno numeri interi.
Poiché viceversa a valori interi di X, Y devono corrispondere valori interi di x, y, le equazioni

$$\begin{aligned} x &= \frac{d}{ad - bc}X - \frac{b}{ad - bc}Y \\ y &= -\frac{c}{ad - bc}X + \frac{a}{ad - bc}Y \end{aligned}$$

ottenute risolvendo le precedenti rispetto alle x, y, dovranno pure essere a coefficienti interi. Sarà pertanto

$$\begin{aligned} a &= \alpha(ad - bc) \\ b &= \beta(ad - bc) \\ c &= \gamma(ad - bc) \\ d &= \delta(ad - bc) \end{aligned} \qquad (\alpha, \beta, \gamma, \delta \text{ interi})$$

donde //

$$ad - bc = (\alpha\delta - \beta\gamma)(ad - bc)^2.$$

Poiché $ad - bc \neq 0$ se ne deduce:

$$1 = (\alpha\delta - \beta\gamma)(ad - bc).$$

Poiché $a, b, c, d, \alpha, \beta, \gamma, \delta$ sono interi, sarà[11]

$$\alpha\delta - \beta\gamma = ad - bc = \pm 1.$$

Dunque a, b, c, d sono interi tali che

$$ad - bc = \pm 1.$$

Le due reti di parallelogrammi sono formate l'una da parallelogrammi P uguali a quello che ha per vertici i punti $(x = y = 0), (x = 1, y = 0), (x = y = 1), (x = 0, y = 1)$ e l'altra da

[11] Klein 1896, p. 29-33. Fubini adotta la stessa notazione utilizzata dal matematico tedesco all'interno del paragrafo *Diophantische Gleichung*.

parallelogrammi Π uguali a quello che ha per vertici i punti $(X = Y = 0), (X = 1, Y = 0), (X = Y = 1), (X = 0, Y = 1)$.
I vertici del primo P hanno per coordinate nel sistema delle X, Y precisamente[12]

$$X = Y = 0;\ X = a,\ Y = b\ ;\ X = a + b, Y = c + d;\ X = b, Y = d.$$

Poiché $ad - bc = \pm 1$, si riconosce tostocche P è equivalente a Π.

c.d.d.

Ogni parallelogrammo che ha per vertici punti di F e che ha per area 1 (nel nostro sistema di misurare le aree) genera pertanto una rete di parallelogrammi, che ha per verti//ci tutti e soli i punti di F.

(*) **Nota**: Se le rette OA', OB' sono scelte come nuovi assi e su esse i segmenti OA', OB' come corrispondenti unità di misura, i punti di F sono anche nel nuovo sistema di coordinate i punti a coordinate intere.

§.2 *Gruppi di traslazioni e campi fondamentali*[13]

Vogliamo ottenere con nuovo metodo il precedente risultato, a tale fine dovremo porre alcune definizioni tra le più importanti dell'intera matematica.
Sia T una corrispondenza biunivoca tra i punti, per esempio, del piano; la T farà corrispondere ad ogni punto A del piano un altro punto A', che varierà quando varia A. Noi porremo $A' = TA$. Per esempio, la T può essere una certa traslazione, oppure una certa proiettività, ecc. Sia U un'altra corrispondenza dello stesso tipo; sia A'' il punto che la U fa corrispondere ad A'; sia cioè $A'' = UA'$.
Noi scriveremo anche $A'' = UTA$, e diremo che la corrispondenza, che definisce A'' come corrispondente di A, è il prodotto UT delle corrispondenze considerate.
Essendo T una corrispondenza biunivoca, dato A', risulta determinato il punto A tale // che $A' = TA$.
Noi diremo che $A = T^{-1}A'$, indicando con T^{-1} la corrispondenza inversa della T. Viceversa T sarà l'inversa di T^{-1}. La corrispondenza prodotto TT^{-1}, come la $T^{-1}T$ coincidono con quella corrispondenza che si suol chiamare identica che fa corrispondere ad ogni punto se stesso, e che si indica con 1.
Si scrive cioè $TT^{-1} = T^{-1}T = 1$.
Evidentemente

$$1 \cdot T = T \cdot 1 = T,$$

ciò che giustifica il simbolismo adottato. In generale però il prodotto TU è distinto da UT. Se $TU = UT$, le U, T diconsi permutabili. Al posto della parola "corrispondenza" talvolta si usa la parola "funzione", talvolta la parola "operazione". Traslazioni, proiettività, ecc. saranno operazioni. Sia G una classe di operazioni T che gode di queste due proprietà. //
α) Se G contiene un'operazione T, contiene anche l'inversa T^{-1}.
β) Se G contiene due operazioni T, U, contiene anche il loro prodotto TU.

[12] *e.c.* e *cor. inf.*: invece di $Y = b$, leggasi $Y = c$.
[13] Klein 1896, p. 3-9. L'influenza di Klein su Fubini e, in generale, sulla matematica italiana per quanto concerne le trasformazioni è evidente.

In tal caso G si dirà essere un gruppo. Siano A, B due punti qualsiasi della nostra rete F; la traslazione che porta A in B trasforma, come è evidente, la F in se stessa. Tutte queste traslazioni generano evidentemente un gruppo G come si controlla anche dalla rappresentazione analitica di una qualsiasi di queste traslazioni

$$x' = x + m \qquad y' = y + n \quad (m, n \; interi).$$

Si otterranno tutte le traslazioni di G, facendo percorrere ad m, n tutti i valori interi possibili. Si diranno equivalenti rispetto a G due punti trasformati l'uno dell'altro con una operazione di G (nel nostro caso due punti (x_0, y_0) ed (x_1, y_1) tali che $x_1 - x_0$ ed $y_1 - y_0$ siano interi). // Due punti equivalenti ad un terzo sono equivalenti tra loro.
Se K è una classe di punti tale che ogni punto del piano sia equivalente ad uno ed un solo punto di K, allora K dicesi campo fondamentale[14] di G. Dato un punto (x, y) noi possiamo evidentemente trovare uno e un solo punto equivalente

$$x' = x + m, \quad y' = y + n$$

Dove n, m sono interi tali che le x', y' risultino né negativi, né maggiori di 1, tali cioè che[15]:

$$0 \leq x < 1 \qquad 0 \leq y < 1.$$

Ora queste disuguaglianze caratterizzano i punti del parallelogrammo P (cfr.§1) che individua la corrispondente rete di parallelogrammi. Poiché però è scritto[16]

$$0 \leq x' ed \; x < 1$$

(e non già[17] $x \leq 1$), e analogamente per[18] y, // dovremo più precisamente dire che le nostre disuguaglianze individuano il parallelogrammo P, a cui siano tolti due lati concorrenti $x = 1, y = 1$.
Tale parallelogrammo è così diventato un campo fondamentale per G. Se noi da P non sopprimessimo alcun lato, sarebbe ancora vero che ogni punto del primo è equivalente ad un punto di P, e in generale anche ad uno solo. L'eccezione proverebbe da ciò che un punto del piano equivalente ad un punto di un lato sarebbe anche equivalente ad un punto del lato opposto. In altre parole i punti interni a P non sono equivalenti ad alcun altro punto di P. Invece i punti del contorno di P sono a due a due equivalenti tra loro. (Le frecce della figura segnano le coppie di lati equivalenti).

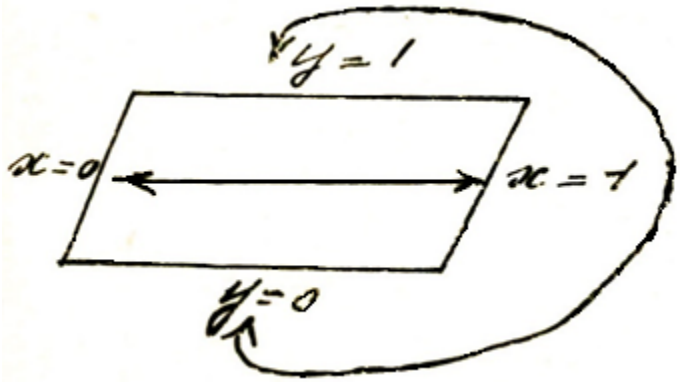


Fig. 1. Parallelogramma fondamentale

[14] Bianchi 1911-12, cap. IV, §26, p. 104.
[15] *e.c.* e *cor. sup.*: $0 \leq x' \leq 1, 0 \leq y' \leq 1$.
[16] *e.c.* e *cor. sup.*: leggasi x' al posto di x.
[17] *e.c.* e *cor. sup.*: leggasi x' al posto di x.
[18] *e.c.* e *cor. sup.*: leggasi y' al posto di y.

Le traslazioni
$S)\ x' = x + 1$
$T)\ y' = y + 1$

che portano un lato nell'equivalente bastano a definire l'intero gruppo; ogni traslazione del quale è del tipo $S^m T^n$, dove il significato degli esponenti è chiaro senza bisogno di spiegazioni. Si noti che le due traslazioni S, T generatrici del gruppo sono nel caso attuale permutabili. Sia K un campo fondamentale, ed H un suo pezzo; sia L il trasformato di H per una qualsiasi operazione di G. Allora

$$K - H + L$$

è ancora evidentemente un campo fondamentale. Infatti ogni punto del piano equivalente ad un punto di K, cioè ad un pun//to il quale o appartiene ad H, oppure appartiene a $K - H$. I punti di H sono ordinatamente equivalenti ai punti di L.
Dunque ogni punto del piano è equivalente ad uno ed a un solo punto scelto tra i punti che appartengono a $K - H$ oppure ad L, cioè ad un punto di

$$K - H + L.$$

Il campo fondamentale $K - H + L$ si dice dedotto da K con un cambiamento lecito. Con cambiamenti leciti si passa evidentemente da un campo ad un altro campo fondamentale qualsiasi. Ecco qui nella figura indicato a tratti il pezzo H che si sottrae dal parallelogrammo K, e in bianco il pezzo L che ad H si sostituisce. Sul contorno del nuovo campo si possono ripetere le considerazioni svolte dapprima per K. Circa L ed H sono nel caso nostro figure di area uguale, perché dedotte // l'una dall'altra con una traslazione. Dunque il nuovo campo fondamentale ha la stessa area dell'antico.

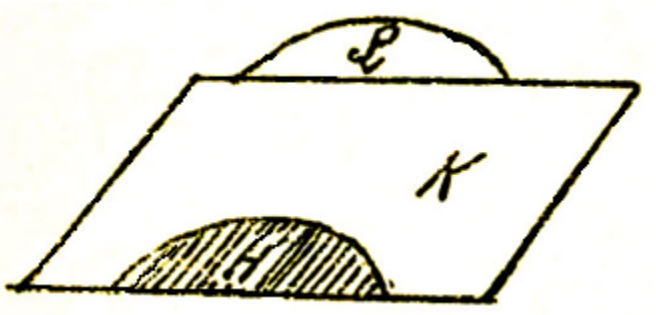


Fig. 2.. Campo fondamentale K-H+L

I campi fondamentali di un gruppo di traslazioni hanno aree uguali[19]. Se noi applichiamo questo teorema ai campi fondamentali formati dai parallelogrammi generatori delle reti di parallelogrammi considerate al §1, troviamo il teorema enunciato al §1; più generalmente ogni campo fondamentale ha per area 1 (ben inteso se tale campo è una figura, a cui si possono applicare i noti procedimenti per il calcolo dell'area).
Dunque: Una figura di area maggiore di 1 non è né un campo fondamentale, né parte di un tale campo; in essa esistono pertanto coppie di punti equivalenti.

[19] Bianchi 1911-12, cap. IV, §26, p. 105. Qui Bianchi enuncia una proprietà più generale rispetto a quella data da Fubini, ovvero: "applicando gli infiniti movimenti del gruppo T al campo fondamentale, si ricoprirà una ed una sola volta tutto il piano di una rete di campi tutti congruenti al fondamentale"; ciò implica che i campi fondamentali di un gruppo di traslazioni abbiano aree uguali.

§.3 ***Il teorema fondamentale di Minkowski***

Diremo che una figura (regione) piana F è non concava[20] se[21]: //
1°) Ogni segmento AB terminato a due punti della figura F o del suo contorno contiene soltanto punti di F, o del suo contorno.
2°) Per ogni punto C del contorno di F passa almeno una retta (retta d'appoggio) che non interseca F, cioè lascia tutto F dalla stessa parte.
Una tale retta sarà generalmente completamente determinata, e coinciderà con la tangente al contorno di F, che esce dal punto C. Questa seconda proprietà non è indipendente dalla precedente.
Se ogni corda di una figura non concava non contiene, oltre agli estremi, altri punti del contorno, la figura si dirà convessa[22]. Un cerchio e un quadrato sono non concavi, il cerchio è anche convesso.
Noi considereremo soltanto figure F non concave aventi un centro: cioè tali che entro F esista un punto O, che bisechi ogni corda di F passante per O.
Sia R una rete di punti; sia O un punto di R e sia O centro di una figura non concava $\mathfrak{f}$.[23] //
Consideriamo le figure ottenute da $\mathfrak{f}$ con omotetie di centro O, e che saranno ancora figure non concave di centro O. Tra esse ve ne sarà una φ ed una soltanto che all'interno non contiene, oltre O, alcun altro punto di R, mentre sul contorno contiene almeno un (altro) punto di R, e quindi anche il suo simmetrico rispetto ad O. Consideriamo, tra le figure $\mathfrak{f}$, quella F dedotta da φ con l'omotetia di centro O e rapporto $\frac{1}{2}$. Consideriamo, tra[24] le figure[25] F, con le solite traslazioni definite dalla nostra rete, cioè le figure uguali ed ugualmente orientate con F, le quali hanno per centro un punto di R. Indicheremo una di queste figure con F_A, se A è il punto di R, che ne è il centro.
Due di queste figure non hanno punti interni comuni.
Basta provare che la F iniziale, cioè la F_O non ha punti interni comuni con F_A, se A è punto della rete distinto da O. Tiriamo la retta OA; essa incontri il contorno di F_O nei due punti O_1 ed O_2, il contorno di F_A nei due punti A_1, A_2.
Sia r_1 una retta // d'appoggio di[26] F uscente da O_1; la retta r_2 parallela ad r_1, ottenuta da r_1 con la simmetria di centro O, ed uscente da O_2, sarà pure una retta d'appoggio per F_O (appunto perché F_O è una figura avente O per centro).
La traslazione che porta O in A porta F_O in F_A, i punti O_1, O_2 nei punti A_1, A_2; essa porterà pertanto le rette r_1, r_2 in altre due rette s_1, s_2 (parallele alle precedenti) che saranno rette di appoggio per F_A nei punti A_1, A_2. Dunque F_O è tutto interno alla striscia (r_1, r_2), e F_A è tutt'interno alla striscia (s_1, s_2); le due strisce essendo parallele tra loro.
Dunque F_O ed F_A potranno avere punti comuni, soltanto quando queste due strisce hanno punti comuni, cioè quando i segmenti O_1O_2 ed A_1A_2 hanno punti comuni.

---

[20] Minkowski 1896, §17, p. 35. Qui Minkowski introduce il concetto di non convessità, poi ripreso da Fubini.
[21] Nota inserita da Fubini a p.d.p.: *Disp.* 6^a *Teoria dei numeri*.
[22] Minkowski 1896, §18, p. 38, 39. Fubini si rifà chiaramente al matematico tedesco per introdurre la convessità.
[23] Bianchi 1920-21, Nota III, *Cenni sul significato geometrico dei teoremi di Minkowski*, p. 433-438. In questa nota Bianchi espone, nel caso tridimensionale, gli stessi ragionamenti geometrici qui svolti da Fubini nel caso bidimensionale.
[24] *e.c.*: sopprimere "tra".
[25] *cor. sup.*: "dedotte da".
[26] *e.c.* e *cor. inf.*: F_O.

Ciò può avvenire soltanto in due casi (si ricordi che $O_1O_2 = A_1A_2$, che O dimezza O_1O_2 e che A dimezza A_1A_2);
α) Il segmento OA è doppio di $OO_1 = OO_2 = AA_1 = AA_2$; in tal caso tanto uno dei due punti O_1, O_2 che uno dei punti A_1, A_2 coincidono col punto di // mezzo di OA.
Le due strisce citate hanno una delle due rette limiti comune. Ed F_O, F_A, oltre ad aver comune il punto medio di OA possono aver comune soltanto parte del loro contorno, posto su tale retta comune alle due strisce. In tal caso la φ contiene sul contorno il punto A.
β) Le due rette r_1, r_2 separano le rette s_1, s_2 e viceversa; in altre parole i segmenti $OO_1 = OO_2 = AA_1 = AA_2$ sono maggiori di $\frac{1}{2}OA$. Ma questo caso è escluso dalle nostre ipotesi.
In tal caso, infatti, essendo $OA < 2OO_1$, la figura φ dedotta da F con l'omotetia di centro O e rapporto 2 conterrebbe all'interno il punto A della rete, distinto da O. Ciò che è contrario all'ipotesi da noi fatta su φ. La figura F_O non contiene all'interno due punti tra loro equivalenti, perché altrimenti la traslazione che porta uno di essi nell'equivalente porterebbe F_O in un campo F_A, che con F_O ha punti interni comuni. Dunque F_O (e quindi anche una qualsiasi delle F) o è un // campo fondamentale, o è parte di tale campo. Quindi l'area di una F non supera 1; e l'area di φ non supera 4. L'area di F varrà 1, e l'area di φ varrà 4, soltanto se F è un campo fondamentale, cioè se F_O e le sue trasformate ricoprono tutto il piano senza lacune. Ma la F_O può avere punti comuni soltanto con quelle F_A in numero finito, i cui centri A sono sul contorno di φ; e i punti comuni ad F_O, F_A sono una parte rettilinea del contorno di F_O. Dunque:
Se una figura non concava col centro in un punto O della rete non contiene all'interno alcun altro punto della rete, la sua area è ≤4. Se l'area di una figura non concava col centro in un punto O della rete è >4, essa contiene all'interno oltre O qualche punto della rete (perché se non ne contenesse alcuno all'interno, l'area sarebbe ≤4). Se l'area di una figura non concava col centro nel punto O della rete vale proprio 4, allora la figura contiene all'interno o sul contorno qualche punto della rete [perché altrimenti // la figura dedotta coll'omotetia di centro O e rapporto $1 + \varepsilon$ con $\varepsilon > 0$ abbastanza piccolo avrebbe per area $4(1 + \varepsilon)^2 > 4$, mentre essa non conterrebbe né all'interno né al contorno alcun punto della rete distinto da O). Infine, sempre nell'ipotesi che l'area della nostra figura φ valga 4, e che essa contenga soltanto sul contorno punti della rete, si deduce che φ è un poligono rettilineo e che la figura F dedotta da φ con l'omotetia di centro O e rapporto $\frac{1}{2}$ ricopre, con le trasformate, tutto il piano una ed una sola volta.[27]
In quest'ultimo caso il contorno di F si può spezzare in segmenti (i cosiddetti lati di F, non escludendo che due lati consecutivi siano per diritto), ciascuno dei quali è parte del contorno di F e anche di una sua trasformata F_A. Se (p, q) sono le coordinate di A il punto $\left(\frac{p}{2}, \frac{q}{2}\right)$ è il punto medio di OA; e tale lato è anch'esso bisecato dal punto $\left(\frac{p}{2}, \frac{q}{2}\right)$. Insieme a tale lato vi sarà anche il lato simmetrico, che avrà per centro il punto $\left(-\frac{p}{2}, -\frac{q}{2}\right)$.
Sia $\left(\frac{p'}{2}, \frac{q'}{2}\right)$ il centro di un terzo lato; esso sarà // posto su una retta distinta da almeno una delle due rette su cui giacciono i due lati simmetrici considerati, p. es., distinto almeno dalla retta su cui giace il lato bisecato dal punto[28] (p, q). Allora $\left(\frac{p+p'}{2}, \frac{q+q'}{2}\right)$ è il punto M di mezzo del

[27] Minkowski 1957, p. 24-28.
[28] *e.c.* e *cor. sup.*: $\left(\frac{p}{2}, \frac{q}{2}\right)$.

segmento terminato ai punti (p,q) e (p',q'): i quali punti sono i punti di mezzo di due lati del poligono non concavo φ, posti su rette distinte.
Dunque il punto M è interno a φ, e poiché i punti (p,q) e $(-p',-q')$ sono distinti, esso non coincide con O. Il punto M, per la stessa definizione di φ, non può essere dunque un punto della rete.
Quindi $\frac{p+p'}{2}$ e $\frac{q+q'}{2}$ non possono essere entrambi interi (dal che segue che neanche $\frac{p-p'}{2}$ e $\frac{q-q'}{2}$ possono essere entrambi interi). Dunque ogni coppia di lati paralleli individua una coppia di interi (p,q) insieme all'opposta $(-p,-q)$, ed i due numeri di questa coppia non possono essere entrambi pari, perché altrimenti il punto $\left(\frac{p}{2},\frac{q}{2}\right)$ del contorno di F sarebbe un punto della rete distinto dal//l'origine O, interno a φ.
Se (p,q) e (p',q') sono coppie di interi corrispondenti a coppie distinte di lati paralleli, allora neanche $p+p', q+q'$ non[29] possono essere entrambi pari.
Poiché, rispetto al mod. 2, ogni coppia d'interi (p,q) non entrambi pari è congrua ad una delle coppie $(1,0),(0,1),(1,1)$ e lati non opposti danno origine a coppie di interi (p,q) tra loro incongrue, ne verrà che la nostra figura avrà al più sei lati, cioè sarà o un parallelogrammo, od un esagono coi lati opposti paralleli (perché deve avere il centro O).
Dunque, la ricerca delle figure non concave φ con il centro in O, non contenenti all'interno oltre O altri punti della rete, e di area 4, è ridotta alla ricerca di quei parallelogrammi od esagoni col centro in O di area 4, che, oltre O, contengono soltanto sul contorno punti della rete. Può avvenire che una φ, avente secondo la nostra definizione sei lati, si riduca ad un parallelogrammo, perché due coppie di lati siano coppie di lati posti su una // medesima retta.

§.4 ***Ricerca dei parallelogrammi ed esagoni limiti***

Ogni lato di uno dei parallelogrammi citati or ora deve contenere all'interno (e non eventualmente soltanto agli estremi) almeno un punto della rete; perché, se così non fosse, neanche il lato opposto conterrebbe punti della rete; e noi potremmo spostare tali lati parallelamente a se stessi, in modo di ingrandire il parallelogramma senza che questo contenesse all'interno punti della rete. Si giungerebbe così all'assurdo di un parallelogrammo col centro in O di area >4, che all'interno non contiene punti della rete.
Se un lato λ di un tale parallelogramma P contiene all'interno un solo punto A della rete, il lato opposto μ conterrebbe il solo punto B simmetrico di A. Io dico che A,B sono rispettivamente i punti medii di λ,μ. Infatti, se così non fosse, facendo rotare λ,μ attorno ad A,B in senso conveniente, dedurrei da P un nuovo parallelogrammo P' di area maggiore di quella di P (cioè maggiore di 4) che avrebbe il centro in O, e non conterrebbe all'interno punti della rete; ciò che è assurdo come sopra. La distanza di due punti della rete posti su uno stesso lato non può essere minore della metà del lato stesso. Se così non fosse, essi individuerebbero una traslazione che porta il punto O in un punto distinto O', interno a P, appartenente alla rete; ciò che è contrario all'ipotesi fatta su P.
Ne segue che un lato non può contenere all'interno tre punti della rete, perché altrimenti almeno due di questi avrebbero una distanza minore della metà del lato stesso né un lato terminato a vertici A,B che appartengono alla rete, può contenere all'interno altri due punti M,N della

[29] Sopprimere "non".

rete; perché altrimenti almeno uno dei quattro segmenti MA, MB, NA, NB è minore della metà del lato stesso.

Se l, λ sono due lati concorrenti di P, non può darsi che ciascuno di essi contenga all'interno due punti della rete. Infatti, se // A, B fossero i punti della rete posti su l, e se C, D quelli posti su λ, allora i due punti C', D' dedotti da C, D con la traslazione AB appartengono alla rete, e sono interni a P. Ma C', D' sono punti distinti; almeno uno è perciò distinto da O. Dunque P conterrebbe all'interno un punto della rete distinto da O; ciò che è assurdo. Possono in conclusione darsi due soli casi:

α) Ogni lato di P contiene all'interno un solo punto della rete che sarà necessariamente il suo punto di mezzo. Le due traslazioni che portano O nei punti di mezzo di due lati paralleli, portano i punti medi degli altri due lati nei vertici di P, che saranno pertanto anch'essi punti della rete.

β) Un lato di P contiene all'interno due punti della rete, la cui distanza vale la metà del lato stesso, altrettanto avviene del lato opposto, i quattro vertici di P non sono punti della rete; appartengono invece alla rete i punti medi degli altri due lati.

Oss.[ervazione]: i due punti della rete posti su uno stesso lato distano tra loro la metà di tale lato, perché la traslazione definita da essi deve portare il punto medio di un altro lato[30]. //

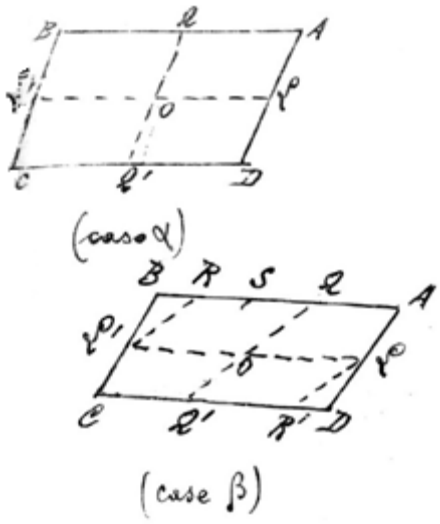


Fig. 3. Studio dei due casi di parallelogrammi limite

(caso α) (i punti L, Q, L', Q'; i vertici A, B, C, D; il centro O punti della rete).

(caso β) (i punti R, Q, L, R', Q', L'; il centro O appartengono alla rete; i vertici non appartengono alla rete).

I parallelogrammi $OLAQ$ nel caso α ed $OQRL'$ nel caso β sono la quarta parte di P ed hanno pertanto per area 1. Dette (p, q) le coordinate di Q ed (r, s) quelle di L si trova dunque

$$ps - qr = \pm 1,$$

dove, sostituendo casomai ad uno dei punti L, Q il suo simmetrico, possiamo ridurci ad avere sempre il segno $+$. Vedremo più avanti l'importante significato aritmetico di questi studi. Noi vogliamo qui prima di tutto studiare un caso particolare che ci darà occasione di fare cenno di una classe di problemi, che a buon diritto // si possono considerare tra i più difficili della teoria dei numeri.

Osservazione

Il caso α) si distingue dal caso β) anche per questa ragione. Consideriamo la figura F_O dedotta dal parallelogrammo $P = \varphi_O$ con l'omotetia di centro O e rapporto $\frac{1}{2}$, e, secondo le definizioni del §5, chiamiamo lato di F la parte di contorno che esso ha comune con uno dei campi equivalenti; chiamiamo lato di φ la parte corrispondente del contorno di φ. Allora:

1°) Nel caso α) $P = \varphi$ ha precisamente quattro lati: quelli che anche nella solita geometria elementare diconsi lati di P.

[30] La fine della frase risulta illeggibile.

2°) Nel caso β) $P = \varphi$ si deve considerare come un esagono; infatti, come segue dal §3, i punti (p, q) a coordinate intere posti sul contorno di φ sono o vertici, o punti di mezzo di un lato di φ.
Quindi, R, Q, L e i punti simmetrici, devonsi considerare come punti medi di lati di P; due coppie dei quali sono formati da lati // posti su una stessa retta; ciò avviene per i lati BS, SA ([31]dove S è il punto medio di RQ) e per i lati simmetrici. (Noto, infatti, che R e Q sono i punti medii dei segmenti BS ed SA).

Esagoni limiti

Per la ricerca generale degli esagoni limiti φ si può partire da ciò che i punti medii dei sei lati devono essere punti (p, q) a coordinate intere (punti della rete). Se (p_1, q_1) e (p_2, q_2) sono punti medii di due lati consecutivi, essi con O determinano un triangolo che all'interno non contiene punti della rete; essi con O sono pertanto vertici consecutivi di un parallelogrammo fondamentale. Noi potremo cambiare gli assi in modo che essi siano i punti $(1, 0)$ e $(0, 1)$. Le traslazioni che portano uno di questi nell'altro portano O nei punti $(1, -1)$ e $(-1, 1)$, che saranno i punti medii degli altri due lati.
Dunque, per costruire i nostri esagoni si scelga ad arbitrio un parallelogrammo fondamentale. Siano L, Q i vertici adiacenti ad O; // si trovi il punto R, in cui[32] Q è condotto dalla traslazione che porta L in Q [che sarà il punto di coordinate $(-1, 1)$, se gli assi sono scelti in guisa che $L = (1, 0)$ e $Q = (0,1)$]. Se[33] gli esagoni che hanno come punti medii dei loro lati un tale sistema di tre punti[34] A, B, C insieme ai loro simmetrici L', Q', R' sono gli esagoni cercati. Come dimostra la figura precedente, l'esagono si riduce ad un parallelogrammo, se un suo vertice S è scelto, p. es., sulla retta QR.

§.5 ***I campi del tipo***[35] $|\boldsymbol{\alpha x + \beta y}|^{\boldsymbol{p}} + |\boldsymbol{\gamma x + \delta y}|^{\boldsymbol{p}} \leq \mathbf{1}$ $(\boldsymbol{p > 1})$

Siano $\alpha, \beta, \gamma, \delta$ costanti con $\alpha\delta - \beta\gamma \neq 0$. Poniamo

$$X = \alpha x + \beta y \qquad Y = \gamma x + \delta y. \qquad (1)$$

La figura $|X|^p + |Y|^p \leq 1$ $(p = \text{costante})$ è nel piano XY una figura che il calcolo dimostra non concava. Altrettanto avverrà della figura C_p nel piano xy, che se ne deduce per (1), e che è definita da[36]

$$f(x, y) = |X|^p + |Y|^p = |\alpha x + \beta y|^p + |\gamma x + \delta y|^p \leq 1.$$

Se $p > 1$ tende ad 1, la nostra figura C_p tende alla figura C_1 definita dalla $|X| + |Y| \leq 1$, che è un // parallelogrammo π avente le rette $X = 0, Y = 0$ per diagonali (e per lati le rette $\pm X \pm Y = 1$). Ora, osserviamo che se due numeri positivi ξ, η soddisfano alla $\xi^p + \eta^p \leq 1$, essi soddisfano anche alla $\xi^q + \eta^q \leq 1$ se $q > p$ (perché dovendo essere $\xi \leq 1, \eta \leq 1$, è $\xi^q \leq \xi^p, \eta^q \leq \eta^p$). Quindi i punti di C_p appartengono anche a C_q, se $q > p$; cioè la figura

[31] *e.c.* e *del.*: "da sopprimere a cominciare da (dove S…" .
[32] *e.c.* e *cor. sup.*: O.
[33] *e.c.*: sopprimere "Se".
[34] *e.c.* e *cor. sup.*: L, Q, R.
[35] *e.c.*: "da qui a fine paragrafo si considerino sempre i valori assoluti delle quantità tra [ ]".
[36] Minkowski 1957, p. 53-55. Fubini utilizza all'interno di questo paragrafo la stessa notazione di Minkowski che però affronta solo il caso $|\alpha x + \beta y|^p + |\gamma x + \delta y|^p = 1$.

C_p ingrandisce al crescere di p; in altre parole, una figura C_p è contenuta in tutte le C_q corrispondenti a valori di $q > p$. Quando p tende a $+\infty$, la figura C_p tende alla figura C_∞ definita dalle:

$$|X| \leq 1 \quad |Y| \leq 1$$

(perché $\lim_{p=\infty} |X|^p = 0, \lim_{p=\infty} |Y|^p = 0$ se $|X| \leq 1 \quad |Y| \leq 1$).

Nel piano XY assumiamo come unità l'area del parallelogrammo $0 \leq X \leq 1, 0 \leq Y \leq 1$; nel piano xy l'area del parallelogrammo $0 \leq x \leq 1, 0 \leq y \leq 1$, conformemente a convenzioni già usate. L'area di C_∞ nel piano XY vale 4. Dunque, l'area di ogni altro C_p $(p > 1)$ nel piano XY è minore di 4.

Al parallelogrammo $0 \leq x \leq 1, 0 \leq y \leq 1$ corrispon//de[37] nel piano XY il parallelogrammo di vertici $(0,0), (\alpha, \gamma), (\beta, \delta), (\alpha + \beta, \gamma + \delta)$, la cui area vale $|\Delta|$, se $\Delta = \alpha\delta - \beta\gamma$.

Due figure nel piano xy hanno aree, il cui rapporto è identico a quello delle figure corrispondenti nel piano XY. Perciò, se α, A sono due figure corrispondenti nel piano xy e nel piano XY, sarà:

$$\frac{area\ \alpha}{area\ del\ parallelogr.\ 0 \leq x \leq 1, 0 \leq y \leq 1} = \\ = \frac{area\ A}{area\ del\ parallelogr.\ di\ vertici\ (0,0), (\alpha, \gamma), (\beta, \delta), (\alpha + \beta, \gamma + \delta)}$$

ossia

$$\frac{area\ \alpha}{1} = \frac{area\ A}{|\Delta|}.$$

Cioè l'area di una figura A nel piano XY si ottiene moltiplicando l'area della figura α corrispondente del piano xy per $|\Delta| (\Delta = \alpha\delta - \beta\gamma)$. Ora C_p nel piano XY è diviso dagli assi in 4 pezzi di uguale area che si calcola facilmente e con i soliti metodi di calcolo integrale (*). Indicheremo con $\frac{4}{K_p^2}$ l'area di C_p nel piano XY. (Sappiamo già che $K_p > 1$); l'area I di C_p nel piano xy varrà

$$I = 4 \frac{1}{K_p^2} \frac{1}{|\Delta|} = area\ di\ C_p\ nel\ piano\ xy.$$

Posto $p = 2$ si trova $\pi = \frac{4}{K_2^2}$.

Indichiamo con M^p il minimo valore assoluto di $f(x, y)$ per valori interi non entrambi nulli delle x, y. Il campo

$$f(x, y) \leq M^p \text{ nel piano } xy$$

dedotto da C_p con una omotetia di centro O e di rapporto M, è un campo φ_O^p convesso con centro nell'origine O, non contenente che sul contorno punti della solita rete del piano xy. La sua area è pertanto minore di 4, perché non può essere uguale a 4 (se $p > 1$) in quanto φ_O^p non è un poligono, come per il teorema di Minkowski sarebbe necessario. Ma tale area vale $M^2 I_p$; dunque, ricordando il valore di I_p si trova:

[37] Nota inserita da Fubini a p.d.p.: *Disp.* 7ª *Teoria dei numeri*.

$$M < K_p\sqrt{|\Delta|} \ \ ossia \ \ \frac{M}{\sqrt{|\Delta|}} < K_p.$$

Dunque, alle x, y si possono dare valori interi non nulli che alla $f(x,y)$ fanno assumere un valore minore di $K_p\sqrt{|\Delta|}$: teorema, che ha importantissime applicazioni[38]. //

(*) **Nota**: Per dimostrare che C_p per $p > 1$ è convesso, basta dimostrare che, p. es., nel 1° quadrante $\frac{d^2Y}{dX^2}$ è negativo. Ora si trova tosto che questa derivata vale $-\frac{(p-1)1}{Y^2p-1}X^{p-2}$. L'area del pezzo di C_p posto nel 1° quadrante vale $\iint dXdY$ esteso al campo $X > 0, Y > 0$, $X^p + Y^p \leq 1$. Ponendo $X^p = \rho,\ Y^p = \sigma,$ questo integrale si trova uguale a $\frac{1}{p^2}\iint \frac{1}{\rho p} - 1\frac{1}{\sigma p} - 1\ d\rho d\sigma$ esteso al campo $\rho \leq 1,\ \sigma \leq 1, \rho + \sigma \leq 1$ che vale $\frac{1}{K_p^2}$ quando si ponga $K_p = \left[\Gamma\left(1+\frac{2}{p}\right)\right]^{-\frac{1}{2}}\left[\Gamma\left(1+\frac{1}{p}\right)\right]^{-1}$ per $p = 2$ è $K_p^2 = \frac{4}{\pi^2}$.

§.6 ***Studio più completo della precedente disuguaglianza***

Fin qui noi abbiamo usato delle proprietà generali dei corpi convessi ma che cosa possiamo dedurre in più della forma speciale dei nostri campi C_p? Cioè, il rapporto $\frac{M}{\sqrt{|\Delta|}}$ non può superare K_p; al variare di $\alpha, \beta, \gamma, \delta$ raggiunge esso un valore massimo? e quale è questo valore massimo? (di cui, per ora, sappiamo soltanto che esso, se esiste, è minore di K_p). Proponiamoci dunque il problema: Trovare, se esiste, il valore massimo di $\frac{M}{\sqrt{|\Delta|}}$. Moltiplicando $\alpha, \beta, \gamma, \delta$ per una stessa costante K, tanto M che $\sqrt{|\Delta|}$ restano moltiplicati per K. Pertanto la frazione $\frac{M}{\sqrt{|\Delta|}}$ resta immutata; nel risolvere il nostro problema noi potremo scegliere tale costante in modo che $M = 1$, senza nulla togliere alla generalità.

L'area del campo φ_p nel piano x, y varrà $\frac{4}{K_p^2}\frac{1}{|\Delta|}$; il nostro problema della ricerca del massimo di $\frac{M}{\sqrt{|\Delta|}}$ diventa dunque (poiché $M = 1$) quello di rendere minimo il $|\Delta|$, cioè di // rendere minima nel piano XY l'area del parallelogrammo, immagine del parallelogrammo fondamentale $0 \leq x \leq 1, 0 \leq y \leq 1$ della nostra rete. Si ricordi che in questa ricerca il campo C_p del piano XY deve essere un campo il quale contiene all'interno il solo punto O tra i punti che sul piano XY formano la rete R' immagine della solita rete R di punti a coordinate intere del piano xy; invece di cercare nel piano xy il campo C_p, noi cerchiamo così la rete R' nel piano XY. Si noti che nel piano XY il campo C_p è fisso, mentre la rete R' varia con $\alpha, \beta, \gamma, \delta$ (contrariamente a ciò che avviene nel piano xy). Il valore massimo cercato di $\frac{M}{\sqrt{|\Delta|}}$ coincide col reciproco della radice quadrata dell'area minima del parallelogrammo fondamentale di R'. Siamo dunque ridotti a cercare nel campo[39] XY la rete R', di cui un punto è l'origine O, di cui nessun altro punto è interno a C_p; e il cui parallelogrammo fondamentale ha l'area minima.

[38] Minkowski 1957, p. 22, 23. Il matematico tedesco perviene alla stessa disuguaglianza qui riportata da Fubini, a meno della costante K_p, ossia ottiene il risultato $M < \sqrt{|\Delta|}$.

[39] *e.c.* e *cor. sup.*: piano.

Se noi nello stesso piano costruiamo il campo[40] C_p^n ottenuto da C_p con omotetia di centro O e rapporto $\frac{1}{2}$, ciò equivale a cercare // la rete R' tale che

1° Il campo $C_p{}'$ dato e quelli dedotti da esso con le traslazioni della rete R' non abbiano punti interni comuni.

2° Il rapporto tra l'area di $C_p{}'$ e l'area di un parallelogrammo fondamentale di R' sia il massimo possibile; in altre parole (con un linguaggio un po' ardito, ma che si giustifica, come vedremo, con passaggi al limite) l'area racchiusa da tutti i $C_p{}'$ sia la massima possibile, cioè i $C_p{}'$ siano nel piano quanto più densi è possibile, cioè lascino vuota la minima parte possibile di piano. Ricordo che

$$\frac{area\ C_p{}'}{area\ paralleogr.\ fondam.\ di\ R'} = \frac{1}{K_p^2}\frac{1}{|\Delta|}.$$

Il valore massimo di tale rapporto vale dunque $\frac{1}{K_p^2}$ moltiplicato per l'inverso del valore minimo di $|\Delta|^p$.

Noi dunque nel piano XY possiamo enunciare geometricamente il nostro problema, o riferendoci al campo C_p, oppure al campo $C_p{}'$; per noi è più conveniente riferirci al campo C_p. Sappiamo già che il parallelogrammo fondamentale della rete cercata, R' ha un'area non maggiore[41] della quarta parte dell'area di C_p. Consideriamo dunque nel piano XY una rete di parallelogrammi, aven//te un vertice nell'origine O e tutti gli altri vertici esterni o sul contorno di C_p. Tale rete determina un sistema di assi cartesiani ξ, η tali che i punti

$$O\ (\xi = \eta = 0), A\ (\xi = 1, \eta = 0)\ e^{42}\ B\ (\xi = 0, \eta = 1)$$

siano vertici consecutivi di un parallelogrammo fondamentale della rete. Supponiamo che la rete non contenga punti sul contorno di C_p. Allora tenuto fisso il segmento OB, possiamo far muovere A verso O sul segmento OA (ciò che, modificando il parallelogrammo iniziale, modifica tutta la rete) fino a che almeno un punto della rete venga sul contorno di C_p. Ciò che avverrà certamente prima che l'area del parallelogrammo fondamentale della rete sia minore di $\frac{1}{4}$ dell'area di C_p. Con questa trasformazione la rete avrà almeno un punto D (e quindi anche il simmetrico) sul contorno di C_p, nessun punto interno a C_p, mentre l'area del suo parallelogrammo fondamentale è diminuita. Il segmento OD non contiene altri punti della rete (che sarebbero interni a C_p), dunque noi potremo cambiare il parallelogrammo fondamentale della rete in guisa che[43] // OD diventi un lato di esso. Corrispondentemente saranno cambiati gli assi coordinati ξ, η (con la stessa origine O).

Sia E il punto vertice opposto di D su tale parallelogrammo, noi, tenuti fissi i punti O, D della rete, potremmo far camminare il punto E sul segmento OE verso O [col che si muterà il parallelogrammo iniziale, e quindi tutta la rete] fino a che un altro punto della rete venga a cadere sul contorno di C_p; e varranno anche qui considerazioni analoghe a quelle fatte per la prima trasformazione della nostra rete. Verranno così a cadere sul contorno di C_p almeno due punti D, H della rete non simmetrici e quindi anche i loro simmetrici D', H' rispetto all'origine.

[40] *lapsus* del curatore: leggasi C_p'.
[41] *e.c.* e *cor. sup.*: minore.
[42] *e.c.* e *cor. sup.* di *a.m.*, che ha reso illeggibile il testo originale.
[43] *e.c., del.* e *cor. sup.* di *a.m.*, che ha reso illeggibile il testo originale.

Col variare della rete sono variati gli assi delle ξ, η e le corrispondenti unità di lunghezza, perché[44] si vuole che almeno[45] un parallelogrammo fondamentale abbia sempre per vertici consecutivi il punto O $(\xi = \eta = 0)$, e il punto $\xi = 1, \eta = 0$, e il punto $\xi = 0, \eta = 1$.
Il rapporto tra l'area di C_p e l'area di tale // parallelogrammo è sempre minore di 4 (perché C_p è anche per tale rete un campo φ convesso col centro nell'origine O che soltanto sul contorno contiene punti della rete distinti da O).
Siano H, K due punti non simmetrici della rete R' posti sul contorno di C_p e di coordinate ξ_0, η_0 e ξ_1, η_1. Siano H', K' i punti simmetrici. I quattro punti H, K, H', K' sono vertici di un parallelogrammo tale che

$$\frac{area\ parallelogr.HKH'K'}{area\ parallelogr.fondam.} = 2|\xi_1\eta_0 - \xi_0\eta_1|.$$

Ma il parallelogrammo $HKH'K'$ è un campo intorno[46] a C_p (coi soli i vertici sul contorno di C_p). Il precedente rapporto è dunque minore di $\frac{\text{area } C_p}{\text{area parallelogr.fond.}}$, che è minore di 4. Dunque

$$2|\xi_1\eta_0 - \xi_0\eta_1| < 4.$$

Ora, $\xi_0, \eta_0, \xi_1, \eta_1$ sono interi; la retta KO non passa per H, perché H non è simmetrico di K; cosicché $\xi_0\eta_1 - \xi_1\eta_0 \neq 0$; sarà dunque[47]

$$|\xi_1\eta_0 - \xi_0\eta_1| = numero\ intero < 2$$

e quindi $\xi_1\eta_0 - \xi_0\eta_1 = \pm 1$. //
Permutando caso mai i punti H, K possiamo dunque supporre

$$\xi_1\eta_0 - \xi_0\eta_1 = 1.$$

Cioè, K, O, H sono tre vertici consecutivi di un parallelogrammo, che possiamo assumere come parallelogrammo fondamentale[48]; resteranno così mutate le coordinate ξ, η in guisa che K diventi il punto $\xi = 1, \eta = 0$, mentre H diventa il punto $\xi = 0, \eta = 1$.
Ora, noi possiamo far muovere H sul contorno di C_p [col che si muta un parallelogrammo fondamentale di R' e la retta R' stessa] in guisa che H si avvicini alla retta OK. Il parallelogrammo fondamentale di R' andrà diminuendo di area, e prima che questi diventi la quarta parte dell'area di C_p, avverrà che almeno un ulteriore punto $L = (\xi', \eta')$ della rete, insieme al suo simmetrico, cadrà sul contorno di C_p: il quale contorno conterrà così almeno tre coppie di punti simmetrici della rete.
Ricordando che il determinante delle coordinate di due dei tre punti H, K, L deve valere ± 1, troviamo che //

$$\eta' = \pm 1, \quad \xi' = \pm 1.$$

E noi potremo, cambiando la direzione positiva degli assi, o sostituendo ad L il punto simmetrico, ottenere che L sia il punto $\xi = -1, \eta = 1$.

---

[44] *ad. post.* e *a.m.*
[45] *ad. post.* e *a.m.*
[46] *e.c.* e *cor. sup.*: interno.
[47] *e.c.* e *cor. sup.* che ha reso illeggibile il testo originale.
[48] Bianchi 1911-12, cap. XIII, §131, p. 602-603.

Né C_p può contenere sul contorno altre coppie di punti della rete; come è facile dedurre da ciò che le coordinate di un tal punto M insieme con le coordinate di ciascuno dei punti H, K, L dovrebbe dare origine a tre determinanti uguali a ± 1.
[Per tale proprietà delle coordinate di M, H e di M, K si dedurrebbe che le coordinate di M, supposto distinto da L e dal suo simmetrico, varrebbero $1,1$ oppure $-1,-1$; col che le coordinate di L, M darebbero un determinante uguale a ± 2, ciò che è assurdo].
La nostra rete R' sarebbe dunque una rete tale che è formata dai punti a coordinate ξ, η intere, i tre punti di essa di coordinate

$$(\xi = -1, \eta = 1), (\xi = 1, \eta = 0), (\xi = 0, \eta = 1)$$

apparterrebbero al contorno di C_p.
Ma la rete R' che noi otteniamo è l'immagine della rete R dei punti a coordinate x, y intere. //
Poiché dunque valori interi per le[49] $C\ x, y$ danno valori interi delle ξ, η e viceversa, le ξ, η ed x, y sono legate da una trasformazione[50] lineare intera omogenea a[51] α coefficienti interi e determinante ± 1. Se noi dunque, nelle formole che danno X, Y in funzione di x, y sostituiamo alle x, y i loro valori in funzioni delle ξ, η otterremo delle formole

$$X = \lambda\xi + \mu\eta \quad Y = \nu\xi + \rho\eta,$$

tali che il determinante $\lambda\rho - \mu\nu$ ha lo stesso valore assoluto $|\Delta|$ del determinante $\alpha\delta - \beta\gamma$. E in coordinate ξ, η il nostro problema diventa: Trovare i valori di λ, μ, ν, ρ in guisa che $|\Delta| = |\lambda\rho - \mu\nu| \neq 0$ abbia il minimo valore possibile, mentre i punti[52] $(0,0), (1,0), (0,1), (-1,1)$ soddisfano alla

$$|\lambda\xi + \mu\eta|^p + |\nu\xi + \rho\eta|^p = 1$$

[cioè mentre $|\lambda|^p + |\nu|^p = |\mu|^p + |\rho|^p = |\mu - \lambda|^p + |\rho - \nu|^p = 1$] e mentre i punti a coordinate intere ξ, η distinti dai precedenti e dai loro simmetrici sono esterni a C_p. //

§.7 ***Risoluzione del problema nel caso*** $\boldsymbol{p = 2}$

Nel caso $p = 2$ avremo dunque, posto

$$|\lambda\xi + \mu\eta|^p + |\nu\xi + \rho\eta|^p = a\xi^2 + 2b\xi\eta + c\eta^2$$

che:

$$a = 1, c = 1, a - 2b + c = 1$$

cosicché:

$$(\lambda\xi + \mu\eta)^2 + (\nu\xi + \rho\eta)^2 = \xi^2 + 2\xi\eta + \eta^2.$$

[49] *e.c.* e *del.*: x, y.
[50] Sommer 1907 (trad. 1911), cap. 3, §38, p. 233, 234: "Géométriquement, nous voyons que le passage d'un réseau à un autre s'obtient par une transformation homographique".
[51] *e.c.* e *del.*: sopprimere α.
[52] *e.c.* e *del.*: sopprimere $(0,0)$.

Poiché evidentemente $(ac - b^2) = (\lambda\rho - \mu\nu)^2$, è senz'altro $|\lambda\rho - \mu\nu| = |\Delta| = \frac{\sqrt{3}}{2}$. Il valore minimo di $|\Delta|$ è così completamente determinato senza bisogno di pensare agli altri punti della rete.

Enunciamo questo risultato sotto due forme.

Ecco la prima[53]:

Una forma quadratica[54] $ax^2 + 2bxy + cy^2$ definita positiva {che, com'è noto, si può sempre scrivere nella forma $(\alpha x + \beta y)^2 + (\gamma x + \delta y)^2$ dove in particolare è $D = ac - b^2 = (\alpha\delta - \beta\gamma)^2$} assume per valori interi convenienti non entrambi nulli delle variabili in[55] valore minimo M^2 tale che

$$\frac{M^2}{D} = \left(\frac{M}{\sqrt{|\Delta|}}\right)^2 \leq \frac{2}{\sqrt{3}}.$$

Vale il segno di uguaglianza soltanto quando con una trasformazione lineare a coefficienti interi di determinante ± 1 tale forma si può // trasformare in una forma proporzionale ad $x^2 + xy + y^2$.

Per il secondo enunciato si noti che, scegliendo convenientemente gli assi coordinati, e le corrispondenti unità di misura, un'equazione $ax^2 + 2bxy + cy^2 = 1$ è l'equazione di un cerchio. Un sistema di cerchi uguali coi centri nei punti di una rete di punti che a due a due non hanno punti interni comuni, ricoprono una regione del piano, il cui rapporto ω all'area del piano intero (*) non può mai superare $\frac{1}{x_2^2}$ moltiplicato per l'inverso del valore minimo $\frac{\sqrt{3}}{2}$ di $|\Delta|$, cioè non può superare $\frac{\pi}{2\sqrt{3}}$.

Si raggiunge questo valore massimo, se il cerchio col centro nell'origine tocca tre coppie di cerchi simmetrici, aventi anch'essi il centro in punti della rete; in tal caso si possono scegliere gli assi in guisa che i punti della rete // siano i punti a coordinate intere, e il cerchio col centro nell'origine abbia un'equazione $x^2 + xy + y^2 = \text{cost}$. In altre parole il valore massimo è raggiunto, quando uno dei cerchi ne tocchi altri sei i cui centri sono punti della rete, che siano vertici di un esagono regolare.

(*) **Nota**: Il numero ω più esattamente si definisce così: Se Q è un quadrato di lato l, il rapporto tra l'area di quella regione di Q che viene coperta dai nostri cerchi, e l'area totale di Q tende per $l = \infty$ al limite ω.

§.8 ***Sistema di due reti una contenuta nell'altra***

Sia data una rete R luogo dei punti a coordinate cartesiane X, Y intere; sia ρ una rete che contiene R (ogni punto di R appartiene a ρ, ma non è detto che viceversa ogni punto di ρ sia anche punto di R). L'origine O $(X = Y = 0)$ sarà anche punto di ρ; noi potremo scegliere altre coordinate cartesiane x, y con la stessa origine, in guisa che i punti di ρ siano i punti a coordinate x, y intere. Varranno delle formole[56]

---

[53] Minkowski 1957, p. 55. Il matematico tedesco prova che $f(x, y) \leq \frac{2}{\sqrt{3}}\sqrt{D}$.

[54] *e.c.* e *cor. sup.*: $ax^2 + \cdots$.

[55] *e.c.* e *cor. sup.*: un.

[56] Minkowski 1957, p. 194. Fubini adotta la stessa notazione qui utilizzata da Minkowski; le due equazioni sono identiche.

$$(1)\quad \begin{cases} x = pX + qY \\ y = rX + sY \end{cases} \qquad (ps - qr \neq 0).$$

Poiché a valori interi di X, Y corrispondono valori interi di x, y (essendo R contenuta in ρ) le costanti p, q, r, s saranno numeri interi.
Il gruppo G delle traslazioni corrispondenti ad R farà parte (sarà contenuto, sarà sottogrup//po) del gruppo g delle traslazioni corrispondenti a ρ; punti equivalenti rispetto a G saranno anche equivalenti secondo g, ma non viceversa. Se

$$D = |ps - rq|$$

vale 1, le due reti coincidono (perché ha valori interi di x, y le (1) fanno corrispondere valori interi di X, Y). Se assumiamo come unità di misura delle aree l'area del parallelogrammo fondamentale π per ρ

$$0 \leq x < 1, 0 \leq y < 1,$$

l'area del parallelogrammo fondamentale P per R

$$0 \leq X < 1, 0 \leq Y < 1,$$

varrà D; in P vi saranno D punti di ρ tra loro non equivalenti rispetto a G. Riassumendo: Se ρ contiene R, e quindi g contiene G, il parallelogrammo è[57] π ha per area la D^{esima} parte dell'area di P.
Il sistema dei punti equivalenti ad un punto A secondo g si divide in D sistemi di punti, tali che soltanto i punti di uno stesso sistema sono equivalenti secondo G.
Siano O, A, E, B i vertici del parallelogrammo fondamentale P di R. Vogliamo scegliere in mo//do <u>canonico</u> un corrispondente parallelogrammo per ρ.

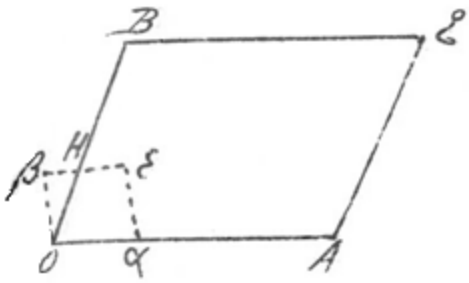


Fig. 5. Trasformazione di un parallelogramma fondamentale nel passaggio da una rete di punti ad un'altra

La retta OA contiene i punti O, A di R, che saranno anche punti di ρ; cerchiamo (secondo[58] i metodi generali per la costruzione di un parallelogramma fondamentale) quel punto α di ρ che giace su OA ed ha da O la minima distanza possibile. I punti di ρ, si distribuiscono su rette parallele ad $O\alpha$; e su ciascuna di queste rette due punti consecutivi di ρ determinano un segmento di lunghezza $O\alpha$. Prendiamo tra tali rette parallele ad $O\alpha$, quella δ che è più vicina ad $O\alpha$ e giace rispetto ad $O\alpha$ dalla stessa banda del punto B. Oltre ad O e α noi potremo scegliere come ulteriori vertici di π due punti consecutivi di r posti su tale retta δ. Scegliamo come terzo vertice β quello di questi punti che <u>non è a destra</u> di H (punto di intersezione di δ e di OB), ma che, o coincide con H, o giace alla sua sinistra, e che da H ha la minima distanza possibile (cosicché[59] // $0 \leq \beta H < O\alpha$). Se i segmenti $O\alpha, \beta\varepsilon$ sono uguali ed ugualmente orientati, $O\alpha\varepsilon\beta$ sarà un parallelogrammo π che è fondamentale per ρ. Scegliamo gli assi delle ξ, η in guisa che α sia il punto $(\xi = 1, \eta = 0)$, che β sia il punto $(0,1)$, che O sia l'origine (*), il punto A avrà le coordinate $\xi = h$ ed $\eta = 0$ con $h > 0$.

[57] *e.c.*: sopprimere "è".
[58] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale.
[59] Nota inserita da Fubini a p.d.p.: *Disp. 8 Teoria dei numeri.*

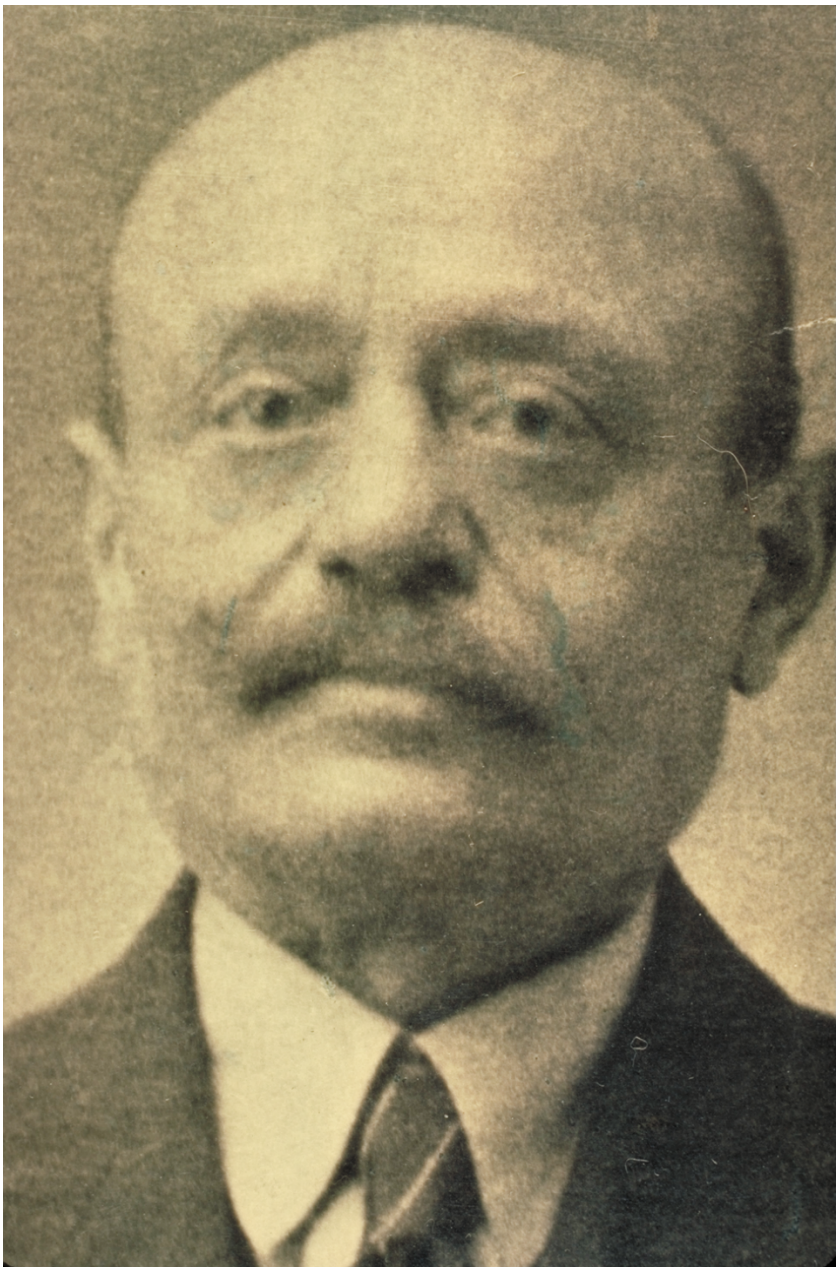
Se (l, m) è il punto B, il punto H sarà il punto $\left(\frac{l}{m}, 1\right)$. Poiché la sua ascissa $\frac{l}{m}$ vale βH, sarà $0 \leq \frac{l}{m} < 1$; pertanto sarà $0 \leq l < m$. D'altra parte i punti di ρ (e quindi anche i punti di R) avranno coordinate ξ, η intere; e viceversa i punti a coordinate ξ, η intere sono i punti di ρ. Quindi in particolare h, l, m sono interi.
Un punto (X, Y) di R si ottiene da O applicandogli X volte le traslazioni OA ed Y volte le OB. Pertanto le sue coordinate sono[60]:

$$(2)\quad \begin{cases} \xi = hX + lY \\ \eta = \quad mY \end{cases} \qquad (h, l, m\ interi; h \geq 1; 0 \leq l < m).$$

E sarà $|D| = hm$ (perché sia $|D|$ che hm valgono il rapporto di due parallelogrammi fondam. delle due reti). //
Poiché dire che ξ, η sono interi equivale a dire che x, y sono interi (perché entrambe queste frasi definiscono punti di ρ), le ξ, η sono legate alle x, y da una trasformazione modulare (cioè da una trasformazione lineare intera omogenea a coefficienti interi, ed a determinante ± 1). Quindi ogni trasformazione (1) che stabilisce il legame tra due reti una subordinata all'altra, si può concepire come prodotto di (2) e di una trasformazione unimodulare sulle ξ, η. La (1) e la (2) corrispondente hanno ugual determinante. Se è dato D, vi è un numero finito di reti ρ contenenti R, tali che $|D|$ sia il rapporto di due parallelogrammi fondamentali [perché è finito il numero delle (2)].
Di trasformazioni ridotte [cioè del tipo (2)] a coefficienti interi ce ne è un numero finito,[61] per ogni valore di D. //

(*) **Nota**: In conclusione l'asse delle ξ coincide con l'asse delle X, è cambiata soltanto la unità di misura corrispondente.

[60] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale.
[61] *ad. post.* e *a.m.*



9. Guido Fubini

Capitolo IV – Applicazioni e illustrazioni aritmetiche[1]

§.1 *Analisi indeterminata di primo grado*[2]

Questa applicazione è già stata sostanzialmente svolta nel Cap. III°. Affinché il segmento OA che congiunge l'origine O al punto[3] $A\,(x_2, y_2)$ della rete non contenga altri punti della rete, occorre e basta che x_1, y_1 siano primi tra loro.
Soltanto in tal caso esiste un punto $B\,(x, y)$ della rete tale che OA, OB sono lati di un parallelogrammo fondamentale, cioè tale che[4] $x_1 y - y_1 x = \pm 1$.
Dunque questa equazione nelle incognite intere x, y è risolubile soltanto quando x_1, y_1 sono primi tra loro[5]. Questo è il teorema fondamentale dell'analisi indeterminata di 1° grado.

§.2 *Frazioni continue*[6]

Sia w un numero positivo; sia q_1 il massimo intero che non supera w; se $w \neq q_1$, allora $\frac{1}{w-q_1}$ è maggiore di 1, sia q_2 il massimo intero che non lo supera; allora $\frac{1}{\left(\frac{1}{w-q_1}\right)-q_2}$, se il denominatore non è nullo, è maggiore di 1, sia q_3 il massimo intero che non lo su//pera. Allora

$$\frac{1}{\frac{1}{\left(\frac{1}{w-q_1}\right)-q_2}-q_3}$$

(se il denominatore non è nullo) è maggiore di 1, sia q_4 il massimo intero che non lo supera e così via. Si ha allora, come è ben noto,

$$w = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots}}}$$

dove la frazione continua del secondo membro è limitata, se in una delle successive espressioni sopra considerate avviene che il denominatore sia nullo. Se invece i successivi denominatori sono differenti da zero, tale frazione continua è illimitata. Il primo caso si presenta soltanto quando w è razionale, p. es., w uguale alla frazione $\frac{b}{a}$ (dove a, b sono interi). In tal caso

---

[1] Gli argomenti trattati da Fubini in questo capitolo non sono presenti nell'opera di Bianchi *Lezioni sulla teoria dei numeri algebrici e di aritmetica analitica,* mentre vengono trattati da Gazzaniga ne *Gli elementi della teoria dei numeri*, esclusivamente dal punto di vista algebrico, senza alcun cenno alle applicazioni geometriche. Alcune considerazioni geometriche si ritrovano invece nell'opera di Bianchi, *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie,* p. 598-666. Fubini si rifà invece agli *Ausgewählte Kapitel* di Klein.

[2] Gazzaniga 1903, cap. II, p. 36. Qui Gazzaniga spiega in dettaglio cos'è l'analisi indeterminata di primo grado ed evidenzia come essa sia stata trattata, per primo, da "Diofante alessandrino".

[3] *e.c.* e *cor. inf.*: $A(x_1, y_1)$.

[4] Sommer 1907 (trad. 1911), cap. 3, §38, p. 233.

[5] Gazzaniga 1903, cap. II, p. 37; prop. 1. Gazzaniga fornisce un enunciato equivalente a quello di Fubini: "Data l'equazione diofantea $ax + by = c$, se il M.C.D. di a e b non divide c, essa non ha soluzioni intere".

[6] Gazzaniga 1903, cap. VI, p. 108 e cap. VII, p. 123. Gazzaniga illustra qui il concetto di frazione continua, ma a differenza di Fubini, si colloca nell'ambito della scomposizione di un numero nella somma di due quadrati. Cfr. anche Klein 1896, p. 10-33; il matematico tedesco utilizza la notazione $\frac{p_i}{q_i}$ per indicare la ridotta *i-esima*, mentre Fubini nelle sue *Lezioni* la denota con $\frac{x_i}{y_i}$.

q_1 è uguale al quoziente ottenuto dividendo b per a; se il resto ottenuto è r, si ha che q_2 è la parte intera di

$$\frac{1}{\frac{b}{a}-q_1}=\frac{1}{\frac{r_1}{a}}=\frac{a}{r_1}.$$

// Dunque q_2 è il quoziente[7] dividendo a pe r_1; così via; questo algoritmo equivale, come è ben noto, all'algoritmo di Euclide per il M.C.D. di due interi.
Le frazioni

$$q_1, q_1+\frac{1}{q_2}, q_1+\frac{1}{q_2+\frac{1}{q_3}}, ecc.$$

si chiamano, per una ragione che vedremo, ridotte[8].
Porremo:

$$\frac{y_{-1}}{x_{-1}}=\frac{0}{1};\ \frac{y_0}{x_0}=\frac{1}{0};\ \frac{y_1}{x_1}=\frac{q_1}{1};\ \frac{y_2}{x_2}=q_1+\frac{1}{q_2};\ \frac{y_3}{x_3}=q_1+\frac{1}{q_2+\frac{1}{q_3}}. \qquad (*)$$

Per i=1, 2 si verifica tosto che

$$\frac{y_i}{x_i}=\frac{q_i y_{i-1}+y_{i-2}}{q_i x_{i-1}+x_{i-2}}. \qquad (1).$$

Ponendo $q_i+\frac{1}{q_i+1}$ al posto di q_i si passa alla ridotta successiva, che pertanto vale[9]: //

$$\frac{y_{i+1}}{x_{i+1}}=\frac{y_{i-1}\left[q_i+\frac{1}{q_{i+1}}\right]+y_{i-2}}{x_{i-1}\left[q_i+\frac{1}{q_{i+1}}\right]+x_{i-2}}=\frac{([y_{i-1}q_i+y_{i-2}]q_{i+1}+y_{i-1})}{([x_{i-1}q_i+x_{i-2}]q_{i+1}+x_{i-1})}=\frac{y_i q_{i+1}+y_{i-1}}{x_i q_{i+1}+x_{i-1}}.$$

Questa formola prova che se la formola (1) vale per un certo valore di i, allora la (1) vale anche per il valore successivo. Cioè la formola (1) vale in generale[10].
Poniamo:

$$\frac{1}{q_{i+1}+\frac{1}{q_{i+2}+\cdots}}=\varepsilon_i \quad (\varepsilon_i<1).$$

Sostituendo $q_i+\varepsilon_i$ alla q_i nel secondo membro di (1), si deve naturalmente trovare il valore di w.
Pertanto:

$$w=\frac{y_i+\varepsilon_i y_{i-1}}{x_i+\varepsilon_i x_{i-1}} \quad (\varepsilon_i<1). \qquad (2)$$

È per $i\geq 1$

$$y_{i+1}x_i-y_i x_{i+1}=[y_i q_{i+1}+y_{i-1}]x_i-[x_i q_{i+1}+x_{i-1}]y_i-[y_i x_{i-1}-y_{i-1}x_i].$$

[7] *e.c.* e *ad. sup.*: quoziente ottenuto dividendo.
[8] Gazzaniga 1903, cap. II, p. 44.
[9] *Idem*, cap. II, p. 41. Qui troviamo la stessa formula, ma con notazione differente: Gazzaniga usa N_{r-2} al posto di y_{i-1} e D_{r-2} al posto di x_{i-1}.
[10] *Ibid.* Dimostrazione del tutto analoga alla (1).

Cioè $y_i x_{i-1} - y_{i-1} x_i$ cambia soltanto di segno, aumentando i di una unità. Calcolata tale espressione per $i = 1$ e, se si vuole, anche per $i = 2$, se ne deduce che è sempre[11]

$$y_i x_{i-1} - y_{i-1} x_i = (-1)^i$$

// cosicché in particolare x_i, y_i sono primi tra loro, cioè $\frac{y_i}{x_i}$ è proprio ridotta ai minimi termini.

Ne segue anche il solito teorema per l'analisi indeterminata di primo grado. Se $w = \frac{b}{a}$ (con a, b primi tra loro), allora $\frac{b}{a}$ coincide proprio con l'ultima ridotta del suo sviluppo in frazione continua.

Se $\frac{\beta}{\alpha}$ è la penultima ridotta, allora

$$\beta a - \alpha b = \pm 1.$$

Ecco dunque trovato che se a, b sono primi tra loro, si può risolvere in numeri interi la

$$ax + by = \pm 1.$$

E si è anche dato un modo per risolverla: metodo che però non è differente da quello che abbiamo già (Cap. I°) esposto[12], perché ancora si fonda sull'algoritmo di Euclide.

D'altra parte per (2) è

$$w - \frac{y_i}{x_i} = \frac{\varepsilon_i [y_{i-1} x_i - y_i x_{i-1}]}{x_i [x_i + \varepsilon x_{i-1}]} = \varepsilon_i (-1)^{i+1} \frac{1}{x_i [x_i + \varepsilon x_{i-1}]}.$$

Le ridotte sono alternativamente minori e maggiori di w; il numero w differisce da una ridotta $\frac{y_i}{x_i}$ per un numero minore in valore assoluto di $\frac{1}{x_i^2}$ (perché ε sono numeri positivi minori di 1).

Se ne deduce // facilmente tra le frazioni con denominatore eguale o minore di x_i, la ridotta $\frac{y_i}{x_i}$ è quella che meno differisce da w.

(*) **Nota**: Intendo che le y e le x siano rispettivamente uguali al numeratore e denominatore della frazione, a cui si riducono i secondi membri, quando si facciano le operazioni indicate. Così $y_{-1} = 0;\ x_{-1} = 1;\ y_1 = q_1;\ x_1 = 1; y_2 = q_1 q_2 + 1;\ x_2 = q_2$ ecc. ecc. (È cioè sottointeso che nell'eseguire i calcoli non si introducano al numeratore e denominatore dei fattori estranei per il solo gusto di complicare i calcoli).

§.3 ***Interpretazione geometrica***[13]

La semiretta $\frac{y}{x} = w$ con x, y positivi divide il primo quadrante in due parti, che diremo rispettivamente sinistra e destra. Nella parte a destra di tale semiretta (compresa tra tale semiretta e il semiasse positivo delle x) giacciono le semirette $\frac{y}{x} = w'$ con $0 < w' < w$; le semirette $\frac{y}{x} = w''$ con $w'' > w$ giacciono a sinistra della semiretta iniziale (cioè fra questa e il semiasse positivo delle y).

[11] *Ibid.* Vi è qui una dimostrazione equivalente di tale risultato.

[12] Gazzaniga 1903, cap. II, p. 42. A differenza di Fubini, Gazzaniga fornisce un esempio di applicazione di tale metodo ($43x + 72y = 10000$ le cui soluzioni sono $x' = 184, y' = 29$).

[13] Klein 1896, p. 17, 18. Fubini riprende chiaramente da Klein questa interpretazione delle frazioni continue.

Supponiamo dapprima w irrazionale, e quindi differente da ogni sua ridotta. Allora, per quanto dicemmo, le semirette $\frac{y}{x} = \frac{y_i}{x_i}$ con i dispari giacciono a destra, quelle con i pari giacciono a sinistra della semiretta iniziale.

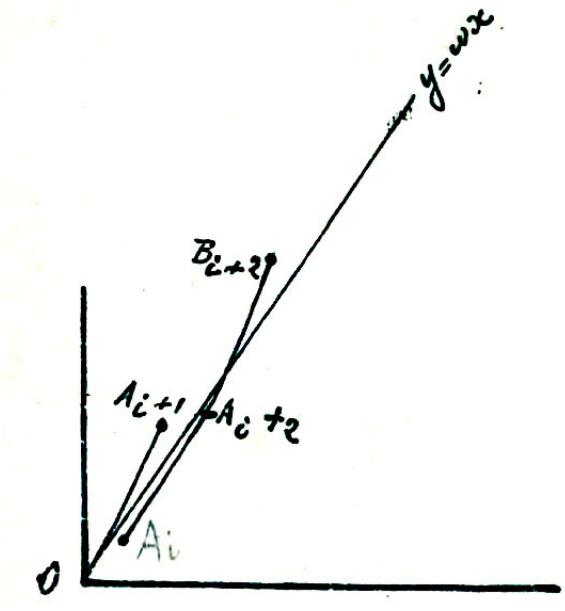


Fig. 5. Rappresentazione sul piano cartesiano delle ridotte di una frazione continua

(La $\frac{y}{x} = \frac{y_0}{x_0} = \frac{1}{0}$ si concepisce coincidente col semiasse positivo delle y). Di queste semirette consideriamo il segmento che dall'origine va al punto $A_i\ (x_i, y_i)$. Poiché $x_i y_{i+1} - y_i x_{i+1} = \pm 1$, due consecutivi di questi segmenti (da // bande opposte della $\frac{y}{x} = w$) sono lati di un parallelogrammo fondamentale. Pertanto, se noi da A_i tiriamo la parallela ad OA_{i+1}, nella striscia limitata da queste due rette (su cui giacciono lati opposti di un parallelogramma fondamentale) non cadono punti dalla rete (interni alla striscia). Come si trova A_{i+2}? È

$$\begin{aligned} y_{i+2} &= y_i + q_{i+2} y_{i+1} \\ x_{i+2} &= x_i + q_{i+2} x_{i+1}. \end{aligned} \qquad (1)$$

Pertanto il segmento[14] A_{i+2} si ottiene da A_i applicando q_{i+2} volte la traslazione OA_{i+1}. Pertanto esso si trova sulla parallela tirata da A_i alla OA_{i+1}, ad una distanza uguale a q_{i+2} volte il segmento OA_{i+1}. Cerchiamo il significato geometrico di q_{i+2}. Si noti che, per definizione di q_{i+2}, il numero w è compreso tra le frazioni $\frac{y_{i+2}}{x_{i+2}}$ e la frazione $\frac{Y_{i+2}}{X_{i+2}}$ i cui termini sono definiti dalle //

$$\begin{aligned} Y_{i+2} &= y_i + (q_{i+2} + 1) y_{i+1} \\ X_{i+2} &= x_i + (q_{i+2} + 1) y_{i+1} \end{aligned}$$

analoghe alle (1) (dedotte da (1) mutando q_{i+2} in $q_{i+2} + 1$).
La retta $\frac{y}{x} = w$ è perciò compresa tra le

$$\frac{y}{x} = \frac{y_{i+2}}{x_{i+2}}, \quad \frac{y}{x} = \frac{Y_{i+2}}{X_{i+2}}.$$

Vale a dire il punto B_{i+2} dedotto da A_i, facendo $q_{i+2} + 1$ volte la traslazione OA_{i+1} giace, rispetto ad A_i, dall'altra banda della semiretta $\frac{y}{x} = w$.
Pertanto q_{i+2} è il massimo numero di volte che si può applicare ad A_i la traslazione OA_{i+1} senza attraversare la $\frac{y}{x} = w$.
I punti[15] A_1, A_0 sono i punti unità dell'asse delle x e delle y; da due punti A_i, A_{i+1} si deduce il consecutivo A_{i+2} tirando da A_i una retta parallela ad OA_{i+1}, e prendendo su questa un segmento $A_i A_{i+2}$, che sia il massimo multiplo di OA_{i+1}, che non attraversi la semiretta $\frac{y}{x} = w$. Nella striscia limitata dalla retta $A_i A_{i+2}$ e dalla retta OA_{i+1}, quindi anche in quella

[14] *e.c.* e *cor. sup.*: punto.
[15] *e.c.* e *cor. inf.*: i punti A_{-1}, A_0.

parte di tale striscia che è limitata tra la retta A_iA_{i+2} e la retta $y - wx = 0$ non esistono punti della rete. //

Quindi non esistono punti della rete che siano compresi tra il segmento OA_{-1} sull'asse delle x, la semiretta $\frac{y}{x} = w$ e la spezzata $A_{-1}A_1A_3A_5$ ... (luogo dei punti A_i di indice dispari). Così non esistono punti della rete tra la semiretta $\frac{x}{y} = w$, il segmento OA_0 e la spezzata $A_0A_2A_4A_6$ ...

I vertici di tali spezzate, qualche punto dei loro lati, e l'origine sono poi tutti i punti del contorno di tali regioni che appartengono alla rete. Consideriamo un filo teso[16], di lunghezza infinita, che inizialmente abbia la posizione della semiretta $\frac{y}{x} = w$; l'estremo posto nell'origine possa scorrere soltanto sul semiasse positivo delle x (o delle y); ogni punto della rete porti uno spillo infisso nel piano xy che impedisca al filo di oltrepassarlo; il filo si contragga quanto gli è possibile, mentre il suo estremo si muove nel modo anzidetto. Il filo alla fine assumerà la forma di una spezzata terminata al punto A_{-1} (o al punto A_0), avente per vertici punti della rete, tale che tra i segmenti OA_{-1} (oppure OA_0), la semiretta $\frac{y}{x} = w$ e la nostra spezzata non vi siano punti della rete. Otterremo cioè le due spezzate[17] sopra citate. // I nostri ragionamenti di prima dimostrano che i lati di una di queste spezzate sono paralleli alle rette che congiungono l'origine O coi vertici dell'altra. Un lato A_iA_{i+2} di una spezzata incontra la $\frac{y}{x} = w$, quando venga prolungato dalla parte di A_{i+2}; l'angolo di un lato con la solita semiretta va diminuendo quando da un lato si passa al successivo. Le semirette OA_i, OA_{i+2}, OA_{i+4}, ... che vanno ai vertici successivi tendono alla semiretta $\frac{y}{x} = w$. Una retta OB che vada a un punto B della rete, che abbia le coordinate rispettivamente minori di quelle di A_i fa con la $\frac{y}{x} = w$ angolo maggiore della OA_i.

Perciò una ridotta $\frac{y_i}{x_i}$ è la frazione, che meno dista da w, di tutte le frazioni, i cui termini rispettivamente non superano y_i ed x_i.

Queste considerazioni si possono ripetere anche se w è razionale, però con qualche variante. In tal caso la semiretta $y = wx$ contiene, oltre l'origine, altri punti della rete; il primo punto che essa contiene della rete è il punto (x_n, y_n), se $\frac{y_n}{x_n}$ è l'ultima ridotta. (La $\frac{y_n}{x_n}$ è il numero[18] scritto sotto forma di frazione ridotta ai mini//mi termini). Questo punto si può considerare come appartenente alla parte del primo quadrante compreso tra la nostra semiretta e il semiasse positivo delle x, oppure all'altra parte di tale quadrante, cioè si può considerare $\frac{y_n}{x_n}$ come di posto pari o dispari (scrivendo, p. es., al posto di q_n la $(q_n - 1) + \frac{1}{q_{n+1}}$ con $q_{n+1} = 1$).

Una o l'altra delle spezzate finirà al punto $\frac{y_n}{x_n}$, e, se si vuole, si può considerare proseguita con la parte della solita semiretta, che comincia nel punto (x_n, y_n); l'altra spezzata finirà con un lato infinito parallelo alla semiretta.

Ciò che avviene per l'una e per l'altra spezzata, secondo la convenzione fatta per (x_n, y_n).

[16] Klein 1896, p. 26, 27. L'esempio del "filo teso" è una chiara citazione delle lezioni di Klein del 1896.

[17] *Ibid.* Il matematico tedesco correda il suo ragionamento, che ha evidentemente influenzato Fubini, con interessanti illustrazioni.

[18] *e.c.* e *cor. inf.* a lato del testo: *w* scritto.

§.4 ***Considerazioni aritmetiche***

Dalle proprietà delle ridotte segue che per ogni numero reale w si possono trovare due interi (x, y) tali che $\left|\frac{x}{y} - w\right| < \frac{1}{y^2}$ (Scambio il significato dato al §3 alle[19] x, y). E, se w è irrazionale, si può, pure supponendo x, y primi tra loro, scegliere la y grande a piacere. E questo risultato vale evidentemente anche per $w < 0$, purchè si supponga che x, y possano anche diventare negativi. // (Se w è razionale, si possono anzi scegliere x, y primi tra loro in guisa che $\left|\frac{x}{y} - w\right| = 0$).

Questo teorema può servire come tipo di una intiera classe di teoremi analoghi; e io ne enuncio qui qualcun altro.

Se w è un numero reale qualsiasi, $t > 1$ un intero positivo qualsiasi, si possono trovare due interi x, y tali che

$$1 \leq y \leq t \qquad \left|\frac{x}{y} - w\right| < \frac{1}{ty}$$

donde segue anche

$$\left|\frac{x}{y} - w\right| < \frac{1}{y^2} \qquad \left(perchè\ \frac{1}{t} \leq \frac{1}{y}\right)$$

e quindi anche

$$1 \leq y \leq t \quad |x - wy| < \frac{1}{y}.$$

Dimostriamolo senza usare l'algoritmo delle frazioni continue; ne dedurremo per nuova via il solito teorema per l'analisi indeterminata di primo grado. Il principio, da cui partiremo per la dimostrazione, è assai fecondo di applicazioni svariate.

I punti $\frac{1}{t}, \frac{2}{t}, \ldots, \frac{n-1}{t}$ dividono l'intervallo $(0,1)$ (l'estremo destro 1 escluso), in t intervallini parziali uguali, di cui lo i^{esimo} è il luogo dei numeri ξ tali che $(i-1)\frac{t}{n} \leq \xi < i\frac{t}{n}$. //

Diamo ad y successivamente i valori[20] $0, 1, 2, \ldots$ e corrispondentemente determiniamo l'intero x in guisa che

$$0 \leq x - wy < 1,$$

che cioè i $\langle\langle t+1 \rangle\rangle$ numeri $x - wy$ che così determineremo siano tutti compresi nell'intervallo $(0, 1)$, estremo destro escluso. Poiché gli intervallini parziali sono soltanto t, due almeno dei numer i $x - wy$ appartengono allo stesso intervallino; sieno essi $x' - wy'$ e $x'' - wy''$ e sia, p. es., $y' > y''$. Sarà $x = x' - x''$ intero; $y = y' - y''$ sarà un intero compreso tra 1 e t; e infine $x - wy$ sarà minore di $\frac{1}{t}$.

c.d.d.

Eserc.[izio] Il teorema che proveremo è evidente, se $s = 1$. Sia $s > 1$; sia r un intero primo con s; posto $w = \frac{r}{s}$, $t = s - 1$, esistono due interi x, y tali che $1 \leq y \leq s - 1$ e che

[19] Gazzaniga 1903, cap. VII, p. 126. In un'osservazione, Gazzaniga mette in luce come questo risultato segua direttamente dalle proprietà delle ridotte da lui poco prima illustrate.

[20] *e.c.* e *cor. sup.*: $0,1,2, \ldots, t$.

$\left|\frac{x}{y}-\frac{r}{s}\right|<\frac{1}{y(s-1)}$, che cioè $|xs-ry|<1+\frac{1}{s-1}$. Poiché $xs-ry\neq 0$ (in quanto che nel caso opposto sarebbe $\frac{r}{s}=\frac{x}{y}$ con $y\leq s-1$, cosicchè $\frac{r}{s}$ non sarebbe ridotto ai minimi termini), dovrà essere

$$xs-ry=\pm 1.$$

Questa equazione è dunque sempre risolubile // in numeri interi, se r,s sono primi tra loro.
Se noi, anziché studiare la divisione di un intervallo $(0,1)$ in t parti uguali, studiamo la divisione di un quadrato di lato 1 in t^2 parti uguali, possiamo dimostrare che:
Se w,w' sono numeri reali qualsiasi, $t>1$ un intero qualsiasi, potremmo trovare tre interi x,y,z tali che[21]

$$|x-wz|<\frac{1}{t}, \qquad |y-w'z|<\frac{1}{t} \qquad 1\leq z\leq t^2$$

donde segue anche

$$\left|\frac{x}{z}-w\right|<\frac{1}{tz}, \left|\frac{y}{z}-w'\right|<\frac{1}{tz}\leq\frac{1}{z\sqrt{z}}.$$

Abbiamo dunque approssimato contemporaneamente w,w' con frazioni di ugual denominatore.
Questi due teoremi si possono enunciare così:
Date le due forme $\frac{1}{t}y, tx-twy$ in due variabili x,y [Date le tre forme[22] $\frac{1}{t^2}z, tx-tw'z, ty-twz$ nelle tre variabili x,y,z] e determinante ± 1, si possono determinare valori interi delle variabili, in modo che esse in valore assoluto non superino l'unità, e al più una sola di esse valga ± 1 (mentre il valore assoluto dell'altra o delle altre è certo minore[23] // di 1).

§.5 ***Generalizzazione coi teoremi di Minkowski***

È quest'ultimo teorema valido soltanto per le forme del tipo particolare, che abbiamo considerato al precedente §4? Oppure è esso molto più generale?
Consideriamo senz'altro due forme qualsiasi

$$\xi=\alpha x+\beta y;\ \ \eta=\gamma x+\delta y \quad \text{con} \quad \alpha\delta-\beta\gamma=\pm 1.$$

Il parallelogrammo

$$-1\leq\xi\leq 1 \quad -1\leq\eta\leq 1$$

è un campo non concavo col centro nell'origine di area 4. Pertanto per il teorema di Minkowski esso contiene certamente all'interno o sul contorno punti della rete[24]; (i punti interni rendono le ξ,η entrambe minori di 1 in valore assoluto; e soltanto un punto della rete che coincida con un vertice le rende entrambe uguali ad 1; soltanto un punto della rete che coincida col punto di mezzo di uno dei lati può annullare una delle due forme, rendendo l'altra uguale a ± 1).

---

[21] *e.c.* e *cor. sup.*: invece di $|x-wz|<\frac{1}{t}$ leggasi $|x-wz|<\frac{1}{t}$, .
[22] *e.c.* e *cor. sup.*: invece di $ty-twz$, leggasi $ty-tw'z$.
[23] Nota inserita da Fubini a p.d.p.: *Disp. 9 Teoria dei numeri.*
[24] Bianchi 1920-21, Nota III, *Cenni sul significato geometrico dei teoremi di Minkowski*, p. 433-438.

Ricordando casi già da noi esaminati di parallelogrammi di area 4 col centro nell'origine non contenenti all'interno punti della rete, ne deduciamo: //
Se $\alpha\delta - \beta\gamma = \pm 1$, le due forme

$$\xi = \alpha x + \beta y \qquad \eta = \gamma x + \delta y$$

si possono rendere entrambe minori di 1 in valore assoluto con valori interi delle x, y non entrambi nulli.
Fanno eccezione i seguenti due casi:
1°) Esistono 8 coppie distinte di valori delle x, y (a due a due uguali e di segno opposto) quattro delle quali rendono uguali a ± 1 l[25] ξ, η, mentre le altre quattro annullano una delle ξ, η e rendono uguale a ± 1 l'altra.
2°) Esistono 6 coppie distinte di valori delle x, y (a due a due uguali e di segno contrario) due delle quali annullano una delle ξ, η e rendono l'altra uguale a ± 1 mentre le altre quattro rendono questa ultima minore di 1 in valore assoluto, e la prima uguale a ± 1.
In entrambi i casi tra le 6 od 8 coppie esistono due coppie (p, q) e (r, s) tali che

$$ps - qr = 1,$$

di cui la prima (p, q) annulla, p. es., $\xi = \alpha x + \beta y$ e rende $\eta = 1$, mentre (r, s) rende $\xi = \pm 1$, e rende η minore di 1 in valore assoluto. //
I punti $(p, q), (0,0)$ ed (r, s) sono vertici consecutivi di un parallelogrammo fondamentale. Se noi cambiamo assi in guisa che essi diventino i punti $(1,0), (0,0), (0,1)$, sarà (indicando con X, Y le nuove coordinate) in virtù delle nostre ipotesi sui valori assunti dalle ξ, η nei punti citati

$$\xi = \pm Y; \ \eta = X + wY \ con \ |w| < 1.$$

E in questo caso è ben evidente che per rendere ξ, η entrambe minori di 1 in valore assoluto, non v'è altro mezzo che porre $X = Y = 0$. Ora,

$$Y = 0 \text{ per } x = p, y = q,$$
$$Y = 1 \text{ per } x = r, y = s.$$

Quindi

$$\pm\xi = Y = py - qx.$$

Una delle forme date (la forma ξ) è dunque una forma $\alpha x + \beta y$ a coefficienti interi primi tra loro; questa condizione necessaria affinché si presenti il caso eccezionale è evidentemente anche sufficiente, perché, se essa è soddisfatta, si prova facilmente che, senza mutare la rete dei punti a coordinate intere, si possono introdurre nuove coordinate cartesiane X, Y, in guisa che le due forme diventino della forma $\pm Y, X + wY$ che noi abbiamo sopra considerato[26]. //

[25] *e.c.* e *cor. sup.*: le ξ, η.
[26] Bianchi 1911-12, cap. XIII, §131, p. 602-603.

§.6 ***Riduzione delle forme quadratiche binarie definite***[27]

Sia $ax^2 + 2bxy + cy^2$ una forma quadratica $f(x,y)$ definita positiva [cosicché $f = 1$ rappresenti un'ellisse reale; cioè $ac - b^2 > 0, a > 0, c > 0$]. Sia K_1 il minimo valore che assume la f nei punti della rete R distinti da O; sia tal valore assunto p. es., nel punto A_1 di R (e nel suo simmetrico A_1') di coordinate (l_1, m_1). Sia K_2 il minimo valore che $f(x,y)$ assume nei punti della rete non posti sulla retta OA_1A_1'. Sarà $K_2 \geq K_1$. Sia K_2 il valore assunto nel punto A_2 della rete (e nel suo simmetrico A_2') di coordinate (l_2, m_2). Sarà[28]

$$E = |l_1 m_2 - m_1 l_2| > 0.$$

Posto

$x = l_1 X + l_2 Y$ (1)
$y = m_1 X + m_2 Y$

avremo che $X = 1, Y = 0$ nel punto A_1, e che $X = 0, Y = 1$ nel punto A_2.
La $f(x,y)$ nelle nuove coordinate diverrà

$$AX^2 + 2BXY + CY^2.$$

Ricordando i valori assunti da $f(x,y)$ nei punti A_1, A_2, si trova che[29] $A = K_1, B = K_2$; cosicché //

$$f(x,y) = K_1X^2 + 2BXY + K_2Y^2 = \left(\sqrt{K_1}X + \frac{B}{\sqrt{K_1}}Y\right)^2 + \left(K_2 - \frac{B^2}{K_1}\right)Y^2.$$

Poniamo

$$h(x,y) = \left(\frac{\sqrt{K_1}X + \frac{B}{\sqrt{K_1}}Y}{\sqrt{K_1}}\right)^2 + \frac{\left(K_2 - \frac{B^2}{K_1}\right)}{K_2}Y^2.$$

Il secondo addendo[30] sarà, poiché $\frac{1}{K_2} \leq \frac{1}{K_1}$, maggiore uguale di[31] $\frac{1}{K_2}\left[\left(K_2 - \frac{B^2}{K_1}\right)Y^2\right]$; cioè

$$h(x,y) \geq \frac{1}{K_2}f(x,y).$$

Nel punto A_1 della rete e nel simmetrico è evidentemente $h = 1$; nei punti della rete posti sulla retta OA_1 sarà $h \geq 1$ (*) negli altri punti (distinti dalla origine) è $f \geq K_2$; e quindi $h \geq 1$. Dunque nel campo[32] $h \leq 1$ non esistono altri punti della rete. //
Cioè il minimo valore assunto da $h(x,y)$ in punti della rete distinti dalla origine vale proprio 1. Perciò

---

[27] Gazzaniga 1903, cap. VII, p. 162.
[28] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale.
[29] *lapsus* del curatore: leggasi $A = K_1, C = K_2$.
[30] *e.c.* e *cor. sup.*: invece di "membro", leggasi "addendo". L'*e.c.* è a sua volta errato: invece di "addendo", leggasi "membro".
[31] *e.c.* e *cor. inf.* a lato del testo: uguale ad $\frac{1}{K_2}\left[\left(K_2 - \frac{B^2}{K_1}\right)Y^2 + \left(\sqrt{K_1}X + \frac{B}{\sqrt{K_1}}Y\right)^2\right]$.
[32] *del.*: $h < 1$.

$$\frac{1}{\sqrt{D}} \leq \frac{2}{\sqrt{3}} \quad cio\text{è} \quad 1 \leq \frac{4}{3}D,$$

se D è il discriminante di $h(x,y)$, considerata come forma delle x, y, e quindi vale il prodotto di $\frac{1}{E^2}$ per il discriminante di h, pensato come forma delle X, Y. Calcolando quest'ultimo discriminante si trova pertanto:

$$1 \leq \frac{4}{3}\frac{1}{E^2}\left(1 - \frac{B^2}{K_1 K_2}\right).$$

Essendo $\underline{E}$ intero, K_1, K_2 positivi, sarà:

$$E = 1; \quad 3K_1K_2 \leq 4K_1K_2 - 4B^2$$

cioè[33] $4B^2 < K_1K_2$.

La (1) è dunque una delle solite trasformazioni, che trasformano la rete in se stessa (portano i punti a coordinate x, y intere in punti a coordinate X, Y intere, e viceversa). Con una tale trasformazione ogni forma quadratica si può trasformare in una forma

$$K_1X^2 + 2BXY + K_2Y^2$$

di ugual discriminante D. E sarà[34]: //

$4B^2 < K_1K_2 \qquad D = K_1K_2 - B^2$
$3B^2 < D$
$K_1K_2 < \frac{4}{3}D.$

Se si tratta di forme a coefficienti interi, queste disuguaglianze si possono, quando D sia prefissato, soddisfare soltanto in un numero <u>finito</u> di modi.[35]

(*) **Nota**: Infatti le coordinate di un punto della rete B posto sulla retta OA_1 sono proporzionali alle coordinate da A_1; in esso è perciò $X = \rho$; $Y = 0$; per tali punti è evidentemente $h = \frac{f}{K_1}$. Ora, poiché K_1 è il minimo valore differente da zero che l a f può assumere nella rete, il numero 1 sarà il minimo dei valori che f assume nei punti della rete, distinto da O, posti sulla retta OA_1; i quali valori sono, come osservammo, identici ai corrispondenti valori di h.

[33] *lapsus* del curatore: leggasi $4B^2 \leq K_1K_2$.
[34] Bianchi 1911-12, cap. XIII, §131, p. 123-126. Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §65, p. 150.
[35] Gauss 1801, sez. V, p. 120-221. Fubini riprende da Gauss l'utilizzo delle diseguaglianze sui coefficienti delle forme ridotte nella dimostrazione del fatto che il numero di forme ridotte di determinante fissato è finito.

Capitolo V – Analisi indeterminata di secondo grado e forme quadratiche[1]

§.1 *Considerazioni generali sulle trasformazioni modulari*[2]

Una trasformazione[3] $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ cioè una trasformazione

$$x = \alpha X + \beta Y$$
$$y = \gamma X + \delta Y$$

Dove $\alpha, \beta, \gamma, \delta$ sono numeri interi ed $\alpha\delta - \beta\gamma = \pm 1$ trasforma in se stessa la solita rete; fa cioè corrispondere a coppie di valori interi per x, y coppie di valori interi per X, Y; e viceversa. Una tale trasformazione si dirà modulare[4], propria se $\alpha\delta - \beta\gamma = 1$, impropria se $\alpha\delta - \beta\gamma = -1$. Salvo avvertenza contraria, noi parleremo soltanto di trasformazioni modulari proprie. // Sia $f(x, y)$ un polinomio in x, y. L'equazione

$$m = f(x, y)$$

sarà risolubile con valori interi di x, y soltanto quando sia risolubile con valori interi di X, Y la

$$m = f(\alpha X + \beta Y, \gamma X + \delta Y)$$

Dove $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ è una trasformazione modulare (anche impropria). Noi diremo che

$$f(\alpha X + \beta Y, \gamma X + \delta Y)$$

(che è un polinomio nelle X, Y) è equivalente ad $f(x, y)$ (propriamente od impropriamente[5] secondo che $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ è propria ed impropria[6]).

Salvo avvertenza contraria, parleremo soltanto di equivalenza propria.

Poiché il prodotto di due trasformazioni modulari proprie è ancora una trasformazione modulare propria, e l'inversa di una trasformazione modulare propria è ancora modulare propria, ne segue che tali trasformazioni modulari formano un gruppo[7], e che due polinomi equivalenti ad un terzo sono equivalenti tra loro.

Consideriamo, p. es., i polinomi $ax + by$ a coefficienti interi a, b. Se δ è il M.C.D. di a, b, allora $\frac{a}{\delta}$ e $\frac{b}{\delta}$ sono primi tra loro; esiste//ranno due numeri α, β tali che

---

[1] Gli argomenti trattati da Fubini in questo capitolo non sono presenti nell'opera di Bianchi *Lezioni sulla teoria dei numeri algebrici e di aritmetica analitica,* mentre vengono trattati da Gazzaniga ne *Gli elementi della teoria dei numeri* esclusivamente dal punto di vista algebrico e senza cenni alle applicazioni geometriche. Alcuni di questi argomenti, invece, sono presenti nell'opera di Bianchi *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie,* p. 1-58, 104-155 .

[2] Klein 1896, p. 3-9 e 34-38.

[3] Gazzaniga 1903, cap. VIII, p. 163.

[4] *Idem*, cap. VIII, p. 164. Gazzaniga scrive "diremo quindi sostituzioni modulari quelle in cui il determinante è uguale a +1".

[5] Gauss 1801, sez. V, art. 158, p. 125, 126. Fubini adotta la notazione e le definizioni fornite introdotte da Gauss nel paragrafo *Aequivalentia, propria et impropria*.

[6] Dirichlet 1877 (trad. 1881), cap. IV, §54, p. 126. Dirichlet introduce qui anche la nozione di "sostituzioni simili/dissimili", elemento cui Fubini invece non accenna.

[7] Gazzaniga 1903, cap. VIII, p. 165.

$$\frac{a}{\delta}\alpha + \frac{b}{\delta}\beta = 1 \text{ ossia } a\alpha + b\beta = \delta.$$

Posto

$$\left.\begin{aligned} x &= \alpha X - \frac{b}{\delta}Y \\ y &= \beta X + \frac{a}{\delta}Y \end{aligned}\right\} \qquad (1)$$

la trasformazione così definita è modulare (propria).
Ed è

$$ax + by = (a\alpha + b\beta)X = \delta X.$$

Cioè $ax + by$ è equivalente[8] a δX, se δ è il M.C.D. di a, b. Quindi sono perfettamente equivalenti le equazioni

$$m = ax + by \qquad (2)$$
$$m = \delta X. \qquad (3)$$

Dunque ne ricaviamo di nuovo che la (2) è risolubile con interi x, y soltanto quando m è multiplo di δ; e allora $X = \frac{m}{\delta}$, mentre Y è arbitrario. Le (1) ci danno tutti[9] le possibili soluzioni di x, y, ponendovi $X = \frac{m}{\delta}$ e lasciando Y arbitrario.

§.2 ***Analisi indeterminata di 2° grado***[10]

Sia $f(x, y)$ un polinomio di secondo grado; cerchiamo di vedere quando è risolubile in numeri interi l'equazione[11]

$$f(x, y) = ax^2 + 2bxy + cy^2 + dx + ey - m = 0.$$

// Si dimostra facilmente che la parte essenziale di tale studio è quello della risoluzione di una equazione[12]

$$m = ax^2 + 2bxy + cy^2 \qquad (1)$$

dove[13]

$$ac + b^2 \neq 0.$$

Porremo[14]

$$D = ac - b^2;\ \Delta = b^2 - ac.$$

---

[8] *Idem*, cap. VIII, p. 166.
[9] *lapsus* del curatore: leggasi "tutte".
[10] Gazzaniga 1903, cap. VIII, p. 150-153. Cfr. anche Gauss 1801, sez. V, art. 216, p. 215-218.
[11] Bianchi 1911-12, cap. II, §1, p. 1-3. Cfr. Anche Sommer 1907 (trad. 1911), cap. 3, §35, p. 202.
[12] Dirichlet 1877 (trad. 1881), cap. IV, §60, p. 135.
[13] *e.c.* e *cor. inf.* a lato: $ac - b^2 \neq 0$.
[14] Bianchi 1911-12, cap. I, §1, p. 2. Qui Bianchi utilizza una notazione differente da Fubini: infatti indica $D = b^2 - ac$. Cfr. anche Sommer 1907 (trad. 1911), cap. 3, §35, p. 203.

[15]Se a, b, c, m sono (come avviene nei casi più importanti) numeri interi, noi potremo limitarci a trovare le soluzioni proprie di (1), cioè quelle coppie di valori delle x, y primi tra di loro che soddisfano ad (1).
Infatti, se x, y è una soluzione di (1) ed h è il M.C.D. dei numeri x, y allora $\xi = \frac{x}{h}, \eta = \frac{y}{h}$ costituiscono una soluzione propria della

$$m' = \frac{m}{h^2} = a\xi^2 + 2b\xi\eta + c\eta^2. \qquad (2)$$

Dunque trovare le soluzioni improprie (non proprie) di (1) equivale a trovare le soluzioni proprie di tutte le equazioni (2) il cui primo membro è uguale ad un divisore m' di m tale che $\frac{m}{m'}$ sia un quadrato perfetto. Ora la (2) è un'equazione dello stesso tipo di (1). Tutto è dunque ridotto a // trovare le soluzioni proprie di un'equazione (1). Sia dunque $x = \alpha, y = \beta$ una soluzione propria di (1). Esisteranno due interi $\gamma_1\ \delta_1$ tali che $\alpha\delta_1 - \beta\gamma_1 = 1$. Gli interi γ, δ più generali, per cui avviene che

$$\alpha\delta - \beta\gamma = 1 \qquad (3)$$

saranno dati dalla

$$\left.\begin{aligned}\gamma &= \gamma_1 + h\alpha\\ \delta &= \delta_1 + h\beta.\end{aligned}\right\} \quad (h = \text{intero arbitrario})$$

La $x = \alpha X + \gamma Y$
$y = \beta X + \delta Y$
è una trasformazione modulare, che trasforma la forma

$$ax^2 + 2bxy + cy^2$$

nella forma equivalente[16]

$$(a\alpha^2 + 2b\alpha\beta + c\beta^2)X^2 + 2\{[a\alpha\gamma_1 + b(\alpha\delta_1 + \beta\gamma_1) + c\gamma\delta_1] + h[a\alpha^2 + 2b\alpha\beta + c\beta^2]\}Y + (a\gamma^2 + 2b\gamma\delta + c\delta^2)Y^2.$$

Il coefficiente di X^2 vale m, perché $x = \alpha, y = \beta$ costituiscono una soluzione di (1). Il coefficiente di $2XY$ vale

$$n = n_1 + hm \qquad (4)$$

(dove[17] $n_1 = a\alpha\gamma_1 + b(\alpha\delta_1 + \beta\gamma) + c\gamma\delta_1$). Il coefficiente di Y^2 sarà indicato con l. Dalla (3) // si deduce, come è ben noto, e come del resto si verifica col calcolo diretto che

$$n^2 - lm = (b^2 - ac)(\alpha\delta - \beta\gamma)^2 = \Delta. \qquad (5)$$

Dunque

$$n^2 \equiv \Delta\ (mod\ m). \qquad (5)bis$$

[15] Dirichlet 1877 (trad. 1881), cap. IV, §60, p. 136.
[16] *e.c.* e *cor. inf.*: $2\{[a\alpha\gamma_1 + b(\alpha\delta_1 + \beta\gamma_1) + c\beta\delta_1] + h[a\alpha^2 + 2b\alpha\beta + c\beta^2]\}XY + (a\gamma^2 + 2b\gamma\delta + c\delta^2)Y^2$.
[17] *e.c.* e *cor. sup.*: $n' = a\alpha\gamma_1 + b(\alpha\delta_1 + \beta\gamma_1) + c\beta\delta_1$).

Alla soluzione (α, β) di (1) corrisponde dunque una soluzione n di $(5\,bis)$. E questa soluzione è completamente determinata $(mod\ m)$, perché, come dimostra la (4), ove h è arbitrario, il numero n è proprio determinato a meno di un multiplo di m.
Prima condizione necessaria[18] per la risolubilità di (1) è dunque che Δ sia un residuo quadratico di[19] m.
Seconda condizione necessaria è che esista almeno una radice n della (5) tale che la forma

$$mX^2 + 2nXY + lY^2 \qquad (6)$$

(dove l è determinato dalla $lm = n^2 - \Delta$) sia equivalente alla forma $ax^2 + 2bxy + cy^2$. E si noti che, quando si considera una radice n di (5) per costruire la corrispondente forma (6), è inutile considerare le radici a quella congrue secondo il modulo m; ciò è evidente per la (4), // dove h è arbitrario, e del resto si può controllare anche così. Due forme

$$mX^2 + 2nXY + lY^2 \qquad m\xi^2 + 2n'\xi\eta + l'\eta^2$$

ove $n^2 - ml = n'^2 - ml'$
$n \equiv n'\ (mod\ m)$

sono sempre equivalenti tra loro. Infatti la trasformazione modulare

$$\left.\begin{aligned} X &= \xi + h\eta \\ Y &= \quad \eta \end{aligned}\right\} \ (h \text{ intero})$$

posta la prima in

$$m\xi^2 + 2(mh + n)\xi\eta + (mh^2 + 2nh + l)\eta^2.$$

Per ipotesi si può scegliere h così che $mh + n = n'$ (perché $n - n'$ è multiplo di m). Allora sarà anche $mh^2 + 2nh + l = l'$ (perché una trasformazione modulare non cambia il discriminante delle nostre forme). Ciò che, volendo, si può verificare, partendo dalle $h = \frac{n'-n}{m}, n'^2 - ml' = n^2 - ml$.
Viceversa le condizioni necessarie trovate sono anche sufficienti; perché, se $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ è una trasformazione modulare che trasforma il secondo membro d i (1) nella (6), allora $x = \alpha$, $y = \beta$ è una soluzione propria di (1). //
Dunque il problema proposto si riduce al seguente: Riconoscere quando due forme quadratiche binarie sono equivalenti; e in caso affermativo trovare le trasformazioni modulari che portano l'una nell'altra[20].

§.3 *Forme definite ridotte*

In geometria analitica, per riconoscere se due coniche sono uguali, si riducono le loro equazioni ad una forma canonica prestabilita (p. es., assumendo come assi coordinati gli assi della conica, oppure una direttrice e la perpendicolare calata su di essa dal fuoco corrispondente). E si guarda poi se le due equazioni canoniche trovate per le nostre due coniche coincidono, oppure no.

[18] Bianchi 1911-12, cap. I, §5, p. 21. Qui Bianchi evidenzia come questa condizione sia necessaria ma non sufficiente.
[19] Gazzaniga 1903, cap. VIII, p. 189, 190, prop. 2.
[20] Bianchi 1911-12, cap. I, §5, p. 22, 23.

E notiamo che la riduzione dell'equazione alla forma canonica (o forma ridotta) equivale ad una trasformazione di coordinate.
Così pure nel caso attuale per riconoscere se due forme quadratiche sono equivalenti, cercheremo anzitutto di dedurre da ciascuna di esse delle forme canoniche, o, come diremo con Gauss, delle forme ridotte[21], facendo opportune // trasformazioni modulari (queste sono appunto le trasformazioni, che corrispondono al cambiamento di assi coordinati della geom.[etria] analit.[ica])
Per le forme definite[22] positive $(\Delta < 0, a_1, c_1 > 0)$ potremmo servirci dei risultati ottenuti nell'ultimo paragrafo del capit.[olo] IV coi metodi di Minkowski[23]. Qui preferiamo affrontare la questione ex novo.
Dire che due forme

$$f = ax^2 + 2bxy + cy^2; \quad f_1 = a_1x^2 + 2b_1xy + c_1y^2$$

(in cui per semplicità diamo lo stesso nome x, y alle variabili) sono equivalenti[24] significa che esiste una trasformazione modulare

$$x' = \alpha x + \beta y \qquad (\alpha\delta - \beta\gamma = 1)$$
$$y' = \gamma x + \delta y$$

che porta l'una nell'altra[25]. Una trasformazione modulare è in sostanza una affinità (proiettività del piano in se stesso che lascia ferma la retta all' ∞) che lascia ferma l'origine, che trasforma in se stessa la solita rete R dei punti a coordinate intere, e che ha determinante positivo. Dunque il nostro problema acquista la seguente forma geometrica: //
Riconoscere se esiste un'affinità (a determinante positivo) che trasforma la figura F composta dalla conica

$$f = ax^2 + 2bxy + cy^2 = 1$$

e dalla rete R nella figura F_1 composta dalla conica

$$f_1 = a_1x^2 + 2b_1xy + c_1y^2$$

e dalla stessa rete R.
Osserviamo che non c'è bisogno di dire che l'origine deve restare trasformata in sé dalla nostra affinità; ciò segue dalle altre condizioni perché l'origine è centro di entrambe le coniche, cioè, è, rispetto ad entrambe le coniche, il polo della retta all'∞: retta che ogni affinità trasforma in sé stessa.
Osserviamo che, se noi non vogliamo introdurre coniche immaginarie, dovremo escludere che f, f_1 siano forme definite negative; in tal caso basterà sostituire alle forme f, f_1 le $-f, -f_1$.

---

[21] Gauss 1801, sez. V, p. 164-174. Fubini segue da vicino quanto fatto da Gauss per quanto riguarda l'equivalenza delle forme quadratiche.
[22] Bianchi 1911-12, cap. I, §6, p. 24. Qui Bianchi spiega perché tali forme si dicono "definite"; scrive infatti: "tale forma, non annullandosi mai, serba sempre lo stesso segno per valori qualunque (non interi) di x, y e dicesi perciò definita, positiva o negativa secondo che assume solo valori positivi o solo valori negativi".
[23] Minkowski 1910 è l'opera cui qui si allude.
[24] Gazzaniga 1903, cap. VIII, p. 166. Gazzaniga definisce "propriamente equivalenti" le forme che Fubini chiama "equivalenti". Cfr. anche Gauss 1801, sez. V, art. 158, p. 126-128, da cui Fubini riprende anche la notazione utilizzata.
[25] Dirichlet 1877 (trad. 1881), cap. IV, §59, p. 134.

Le figure F, F_1 sono composte di una stessa rete, e di due coniche distinte[26]; cerchiamo di ri//durci al caso di figure composte di una stessa conica e di due reti distinte.
Supponiamo f, f_1 definite positive; supponiamo cioè per ora che le $f = 1, f_1 = 1$ siano ellissi[27]: Posto

$$X = \sqrt{a}x + \frac{b}{\sqrt{a}}y \quad Y = \sqrt{c - \frac{b^2}{a}}y = \sqrt{\frac{D}{a}}y \tag{1}$$

la conica $f(x, y) = 1$ diventa definita dalla

$$X^2 + Y^2 = 1.$$

Le (1) definiscono pertanto un'affinità tra il piano xy ed un piano ove X, Y sono coordinate cartesiane ortogonali, cosicché alla nostra conica corrisponde sul piano XY il cerchio che ha per centro l'origine e raggio 1.
La (1) sarà a determinante positivo se i radicali sono presi col segno $+$.
Alla rete R determinata dal parallelogramma di vertici $(x = 0, y = 0), (x = 1, y = 0), (x = 1, y = 1), (x = 0, y = 1)$ corrisponderà sul piano XY una rete, che ancora indicherò con R, determinata dal parallelogrammo che ha per vertici i punti

$$\mathrm{O} = (\mathrm{X} = 0, \mathrm{Y} = 0);\ \mathrm{A} = \left(\mathrm{X} = \sqrt{\mathrm{a}}, \mathrm{Y} = 0\right);\ \mathrm{C} = \left(\mathrm{X} = \sqrt{\mathrm{a}} + \frac{\mathrm{b}}{\sqrt{\mathrm{a}}}, \mathrm{Y} = \sqrt{\frac{\mathrm{D}}{\mathrm{a}}}\right);$$

$$\mathrm{B} = \left(\mathrm{X} = \frac{\mathrm{b}}{\sqrt{\mathrm{a}}}, \mathrm{Y} = \sqrt{\frac{\mathrm{D}}{\mathrm{a}}}\right).$$

I lati di questo parallelogramma hanno per lun//ghezza $\sqrt{a}, \sqrt{\frac{b^2}{a} + \frac{D}{a}} = \sqrt{c};$ assunto al solito il semiasse positivo delle Y a sinistra del semiasse positivo delle x, il lato di lunghezza $\sqrt{c}$ che va dall'origine al vertice posto fuori dall'asse delle X giace nei primi due quadranti, e l'angolo[28] ω di cui deve rotare nel verso positivo l'asse delle x per portarsi su tale lato è minore di 2 retti, ed è definito completamente dalla[29]

$$cos\theta = \frac{b}{\sqrt{ac}}$$

(cosicché θ è acuto od ottuso, secondo che b è positivo o negativo).
La diagonale del parallelogrammo uscente dall'origine vale $\sqrt{a + c + 2b}$; l'altra vale $\sqrt{a + c - 2b}$.
Così pure con una affinità a determinante positivo potremo portare la figura F, in una figura formata dallo stesso cerchio $X^2 + Y^2 = 1$ e da un'altra rete R_1.
Così dunque il nostro problema diventa quello di riconoscere se con un'affinità a determinante positivo, che lascia fisso un cerchio col centro nell'origine, si può trasformare una rete R in un'altra rete R_1. Ma le affinità di determinante positivo che lasciano fisso tale cerchio si

[26] Nota inserita da Fubini a p.d.p.: *Disp. 10 teoria dei numeri*.
[27] Bianchi 1911-12, cap. IV, §36, p. 143-147. Qui Bianchi tratta in modo più approfondito rispetto a Fubini il caso ellittico e iperbolico, pur non soffermandosi sulle considerazioni geometriche.
[28] *e.c.* e *cor. sup.*: θ.
[29] Fubini qui cita palesemente il Gauss che, all'interno delle sue *Disquisitiones,* aveva introdotto la notazione $cos\alpha = \frac{b}{\sqrt{ac}}$.

riducono a rotazioni attorno all'origine. Bisognerà dunque vedere se con una tale rotazione si può portare R in R_1 (cioè in sostanza se le due reti sono uguali). [Se si // considerassero anche affinità a determinante negativo si dovrebbero anche considerare i prodotti di una tale rotazione per la simmetria rispetto ad un diametro del cerchio].
La equivalenza delle due forme equivale adunque alla sovrapponibilità delle due reti R, R_1 corrispondenti sul piano XY. Cioè due forme saranno equivalenti, allora e allora soltanto che le due reti corrispondenti si possono generare con quadrangoli uguali. Dunque per trovare tutte le forme equivalenti alla f basta cercare le reti R_1 generabili con un parallelogramma uguale ad un parallelogramma fondamentale di R. In altre parole ogni parallelogramma fondamentale di R individua una forma equivalente ad f. E le formole precedenti permettono di esplicitare tale forma. Se $\sqrt{a'}, \sqrt{c'}$ sono i lati di un tale parallelogramma fondamentale (dove le notazioni sono scelte in modo che rotando nel verso positivo di un angolo concavo[30] ω si passi dal primo al secondo lato) e se $cos\omega = \frac{b'}{\sqrt{a'c'}}$, allora la forma

$$a'x^2 + 2b'xy + c'y^2$$

è equivalente alla forma data; e in questo modo // si generano tutte le forme equivalenti alla f.
Ma ritorniamo al nostro problema iniziale:
Come si riconosce se f ed f' sono equivalenti? Ciò che equivale alla domanda: Dati i parallelogrammi fondamentali di due reti, come si riconosce se le reti sono uguali?
A tal fine cerchiamo di scegliere per una data rete in modo <u>canonico</u> (o ridotto) un parallelogrammo fondamentale $OA'C'B'$. Come vertice A' scegliamo un punto della rete che dista[31] da O il <u>meno</u> possibile; come sappiamo, gli altri punti della rete sono disposti su rette parallele ad OA'; sia r quella di queste parallele ad OA', che meno dista da OA', e che giace nel semipiano, a sinistra dell'osservatore che da O guardi verso A'; il vertice B' opposto ad A' si deve scegliere sulla retta r (o sulla simmetrica rispetto ad O). Noi determiniamo di sceglierle[32] sulla retta $\underline{r}$; e precisamente di scegliere come vertice B' quel punto della retta che giace su r, e che da O ha la <u>minima</u> distanza possibile.
Resta così in generale determinato in un solo modo il parallelogrammo $OA'C'B'$; e quindi <u>in</u> // <u>generale</u> due reti saranno sovrapponibili, soltanto se i corrispondenti parallelogrammi ridotti sono uguali tra loro.
Quando mai si presenta una eccezione? Quando mai cioè una rete può avere due parallelogrammi <u>ridotti</u> disuguali?
A tal fine è evidentemente necessario che, o vi sia arbitrarietà nella scelta del vertice A', o in quella del vertice B'. Notisi però che lo spostare A' nel punto simmetrico non cambia il parallelogramma, ma soltanto lo fa rotare di due retti attorno ad O. Non tenendo conto del punto simmetrico di A', vi può essere arbitrarietà nella scelta di A', soltanto quando <u>fuori</u> dalla retta OA' vi è un punto della rete, che ha anch'esso da O la stessa <u>minima</u> distanza OA'. Ma poiché OB' è la minima distanza da O ad un punto della rete esterno alla retta OA', dovrà in tal caso essere $OA' = OB'$. //
Indeterminazione sulla scelta di B' può soltanto avvenire quando due punti consecutivi della rete, posti su r, hanno ugual distanza da O; siano B_1', B_2' tali due punti $(OB_1' = OB_2')$. Se

[30] *e.c.* e *cor. sup.*: convesso.
[31] *e.c.* e *cor. sup.*: disti.
[32] *e.c.* e *cor. sup.*: sceglierlo.

B_1' è a sinistra di B_2', e si sceglie B_1' come vertice[33] B_{II}' la diagonale OB_2' del parallelogrammo sarà uguale al lato OB_1'; se si sceglie B_2' come vertice B_1' la diagonale $B_2'A'$ sarà uguale e parallela ad OB_1', e perciò uguale ad OB_2'.
$(B_1'B_2' = OA')$

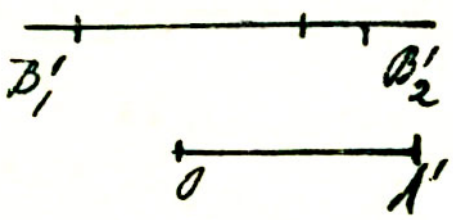


Fig. 6.. Caso di indeterminazione nella scelta del quarto vertice del parallelogramma fondamentale

I casi di eccezione si possono presentare soltanto quando un parallelogrammo ridotto ha due lati uguali oppure un lato uguale ed uno[34] diagonale.
Un parallelogrammo ridotto è caratterizzato da $OA' \leq OB'; OB' \leq OC'; OB' \leq A'B'$; vi può essere un altro parallelogrammo ridotto corrispondente alla stessa rete, e soltanto quando in una di queste disuguaglianze vale il segno di $=$.

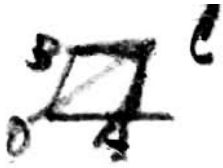


Fig. 7. Caso eccezionale

Come vedremo, non può avere più di due parallelogrammi ridotti disuguali. Dunque:
Due reti sono sovrapponibili soltanto quando il parallelogrammo fondamentale ridotto della pri//ma (o, in casi particolari, la coppia dei parallelogrammi ridotti della prima) è uguale al parallelogrammo ridotto della seconda.
Traduciamo ora in formule le condizioni di riduzione di un parallelogrammo, enunciamo questo risultato senz'altro per le forme quadratiche, anziché per i corrispondenti parallelogrammi, e infine, confrontiamo coi risultati ottenuti all'ultimo paragrafo del Cap. IV coi metodi di Minkowski.
I lati del parallelogrammo corrispondenti alla forma $ax^2 + 2bxy + cy^2$ [35]sono $\sqrt{a}, \sqrt{c}$, le diagonali $\sqrt{a + c \pm 2b}$. Dunque un parallelogrammo è ridotto, cioè la forma citata è ridotta quando

$$a \leq c \qquad c \leq a + c \pm 2b \qquad ossia \mp 2b \leq a$$

cioè, poiché a, c sono positivi quando[36]

$$2|b| \leq a \leq c$$

ogni forma definita positiva equivalente ad una, e in generale a una sola forma ridotta[37] (per la quale cioè valgono le precedenti disuguaglianze).
Vi può essere ambiguità, cioè due forme ridotte e distinte possono essere equivalenti tra loro soltan//to quando per ciascuna di esse in almeno una delle precedenti disuguaglianze vale proprio il segno di $=$.
Notiamo la identità dei risultati attuali con quelli ottenuti nell'ultimo paragrafo del Cap. IV coi metodi di Minkowski. Anzi le dimostrazioni date sono nel fondo equivalenti. Infatti trovare nella nostra rete il punto A, che meno dista da O, equivale a cercare il punto $(X\ Y)$ della rete per cui $X^2 + Y^2$ ha il minimo valore. Ora $X^2 + Y^2$ non è che la forma $f(x, y)$ scritta con le variabili X, Y. La nostra rete è l'immagine dei punti a coordinate x, y intere. Dunque in fondo,

[33] *lapsus* del curatore: invece di B_{II}' leggasi B_2'.
[34] *e.c.* e *cor. sup.*: uguale ad una.
[35] *ad. sup.* e *a.m.*: ridotta al cerchio.
[36] Bianchi 1911-12, cap. I, §6, p. 25. Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §67, p. 153.
[37] *Idem*, cap. I, §6, p. 26. Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §64, p. 147.

cercare A equivale a cercare il punto a coordinate x, y intere, ove $f(x,y)$ ha il minimo valore possibile.
Così analogamente la ricerca del punto B equivale a cercare un punto della rete esterno alla retta congiungente l'origine al punto già trovato, ove la $f(x,y)$ ha il minimo valore possibile tra quelli che assume nei punti della rete esterni a tale retta. //

(*) **Nota**: Veramente B' è un punto della rete, posto su r, che da O ha la minima distanza possibile. Se però ricordo che r è tra le rette parallele ad OA', che contengono punti della rete, una di quelle due che da OA' hanno la minima distanza possibile, se ne deduce tosto l'osservazione del testo. (Si ricordi che su r i punti della rete si seguono alla distanza OA' l'uno dal successivo, che OA' è la minima distanza di due punti della rete). La dimostrazione al lettore.

§.4 ***Il campo fondamentale del gruppo modulare***[38]

Diamo nuova veste geometrica ai precedenti risultati. Forme $ax^2 + 2bxy + cy^2$ tra loro equivalenti hanno lo stesso determinante; cosicché $D = ac - b^2$ ha uno stesso valore per tutte le forme considerate (positivo, se le forme sono definite). Dato il valore di $D > 0$, per determinare la forma, basterà dare i valori di $T = \frac{x}{y}$, che la rendono nulla. Infatti, nell'ipotesi $D > 0$, questi valori (che diremo gli <u>affissi</u> della forma) sono:

$$T = -\frac{b}{a} \pm i\frac{\sqrt{D}}{a}.$$

Cosicché dare T equivale a dare $\frac{b}{a}$ e $\frac{\sqrt{D}}{a}$; essendo noto D, ne risultano determinati, a meno del segno, le a, b, c. E ogni indeterminazione sparisce, se noi consideriamo il valore[39]

$$T = -\frac{b}{a} - i\frac{\sqrt{D}}{a},$$

che diremo l'<u>affisso principale</u> o anche soltanto l'<u>affisso</u> e ci limitiamo a forme positive $(a > 0)$. Tale affisso è un numero complesso $\xi + i\eta$, ove

$$\xi = -\frac{b}{a} \quad ed \quad \eta = \frac{\sqrt{D}}{a} > 0.$$

(Notisi che η risulta positivo).
Quale relazione passa tra gli affissi di due forme equi//valenti. Dall'una si passa all'altra con una trasformazione

$$x' = \alpha x + \beta y; \quad y' = \gamma x + \delta y. \quad (\alpha, \beta, \gamma, \delta, \text{interi})$$
$$(\alpha\delta - \beta\gamma = 1).$$

Basta ricordare la definizione di affissi, per dedurne che

$$T' = \frac{\alpha T + \beta}{\gamma T + \delta} = \frac{[(\alpha\xi + \beta)(\gamma\xi + \delta) + \alpha\gamma\eta^2]}{(\gamma\xi + \delta)^2 + \gamma^2\eta^2} + i\frac{\eta}{(\gamma\xi + \delta)^2 + \gamma^2\eta^2}$$

[38] Klein 1896, p. 34-38. Viene qui introdotto il gruppo modulare con la stessa simbologia poi adottata da Fubini.
[39] *e.c.* e *cor. sup.*: $T = -\frac{b}{a} + i\frac{\sqrt{D}}{a}$.

è la trasformazione corrispondente sugli affissi.
Si passa dal secondo al terzo membro, moltiplicando i due termini per la quantità immaginaria coniugata del denominatore, e ricordando che $\alpha\delta - \beta\gamma = 1$. Si noti anzi che questa trasformazione fa proprio corrispondere all'affisso principale di una forma l'affisso principale dell'altra.
Nel piano $\xi\eta$ l'asse delle ξ separa due semipiani: il semipiano $\eta > 0$ è il luogo degli affissi.
Dato D, vi è corrispondenza biunivoca tra le forme e i corrispondenti affissi.
Una forma ridotta è individuata dalle

$$2|b| \leq a \leq c$$

cioè[40] $|\xi| = \left|\frac{b}{a}\right| \leq \frac{1}{2} \qquad \xi^2 + \eta^2 = \frac{c}{a} \geq 1. \qquad (\alpha)$
// Gli affissi delle forme ridotte sono i punti del triangolo

$$-\frac{1}{2} \leq \xi \leq \frac{1}{2} \qquad \xi^2 + \eta^2 \geq 1$$

che ha due lati rettilinei paralleli all'asse delle ordinate e un lato circolare che noi chiameremo triangolo modulare[41].

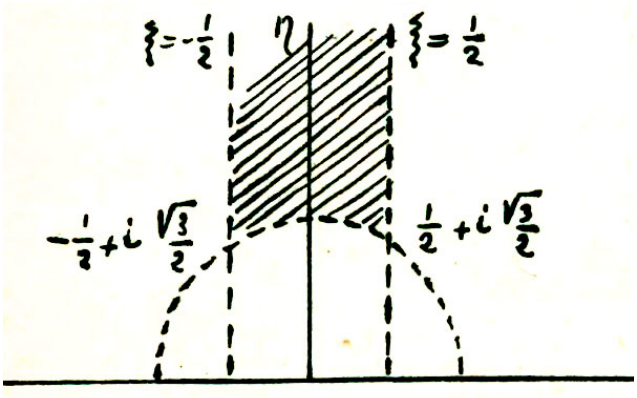


Fig. 8. Triangolo modulare

Questo triangolo nella figura è tratteggiato. I suoi vertici sono: il punto all'infinito dell'asse delle y e i punti[42] $-\frac{1}{2} \pm i\,\frac{\sqrt{3}}{2}$ (che sono le due radici cubiche complesse della unità[43]).
Tale triangolo si dice il triangolo modulare.
I nostri risultati si possono enunciare così:
Ogni punto del semipiano positivo O può con una trasformazione modulare

$$T' = \frac{\alpha T + \beta}{\gamma T + \delta} \qquad (\alpha, \beta, \gamma, \delta \; interi, \alpha\delta - \beta\gamma = 1)$$

essere portato entro il triangolo modulare.
Se due punti del triangolo modulare possono essere trasformati l'uno dell'altro mediante una trasformazione modulare (distinta dall'identità $T' = T$), allora per[44] le coordinate di entrambi devono soddisfare alle (α), in guisa che in almeno una di queste // valga il segno di

[40] Bianchi 1911-12, cap. I, §6, p. 25.
[41] *Idem*, cap. IV, §28, p. 114. Qui è inserita un'interessante figura rappresentante i triangoli modulari.
[42] *e.c.* e *cor. sup.*: $\pm\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
[43] *e.c.* e *del.*: "sopprimere (…)".
[44] Termine *del.* sul manoscritto originale ma che non viene segnalato nell'*e.c.*

uguaglianza; cioè entrambi i punti devono giacere sulla retta $\xi = \frac{1}{2}$, oppure nel cerchio[45] $\xi + \eta^2 = 1$; cioè i due punti appartengono entrambi al perimetro del triangolo fondamentale. È facile riconoscere che le trasformazioni $T' = \frac{\alpha T+\beta}{\gamma T+\delta}$ ($\alpha, \beta, \gamma, \delta$ interi; $\alpha\delta - \beta\gamma = 1$) formano un gruppo: il cosiddetto gruppo modulare[46].

I nostri risultati si possono enunciare dicendo che il precedente triangolo è un campo fondamentale del gruppo modulare nel nostro semipiano.

Tale triangolo, e i suoi trasformati per le trasformazioni del gruppo riempiono tutto il semipiano ed hanno a due a due comuni tutt'al più punti del contorno. Le trasformazioni $T' = T + 1$, $T' = -\frac{1}{T}, T' = T - 1$ del gruppo modulare portano il triangolo iniziale in tre triangoli adiacenti aventi un lato comune con esso; gli altri triangoli pertanto, o non avranno alcun punto comune col triangolo iniziale, oppure avranno comune al più un vertice: con S e con $\mathbb{T}$ indicheremo le trasformazioni $T' = T + 1$, $T' = -\frac{1}{T}$. È $\mathbb{T}^2 = 1$, cioè $\mathbb{T} = \mathbb{T}^{-1}$, mentre S^{-1} è definita dalla $T' = T - 1$.

Dunque le $S, S^{-1}, \mathbb{T}$ portano il triangolo iniziale // nei triangoli adiacenti; poiché si passa da un triangolo ad un altro qualsiasi con successivi passaggi da un triangolo ad un triangolo adiacente, si riconosce facilmente che ogni trasformazione modulare si può tenere come prodotto di potenze delle $S, \mathbb{T}$, ossia (poiché[47] $T^2 = 1$) come prodotto di[48] T e di potenze della S (cioè ogni trasformazione modulare è del tipo S^n, oppure $\mathbb{T}$, oppure $S^n\mathbb{T}, \mathbb{T}S^n, S^n\mathbb{T}S^m, S^n\mathbb{T}S^m\mathbb{T}$, ecc, ecc.).

La S ($T' = T + 1$) porta il lato $\xi = -\frac{1}{2}$ del primo triangolo nel lato $\xi = \frac{1}{2}$. La $T' = -\frac{1}{T}$ trasforma in sé stesso il lato $\xi^2 + \eta^2 = 1$, e precisamente porta ogni punto di questo cerchio nel simmetrico rispetto all'asse delle η; e lascia fisso soltanto il punto $T = i$, dove il cerchio incontra questo asse. Per questa ragione il punto $T = i$ si suole considerare come un nuovo vertice, e il nostro triangolo come un quadrangolo con un angolo piatto. Punti del contorno simmetrici rispetto all'asse delle y sono equivalenti[49] (*). Passando alle forme corrispondenti, troviamo: //

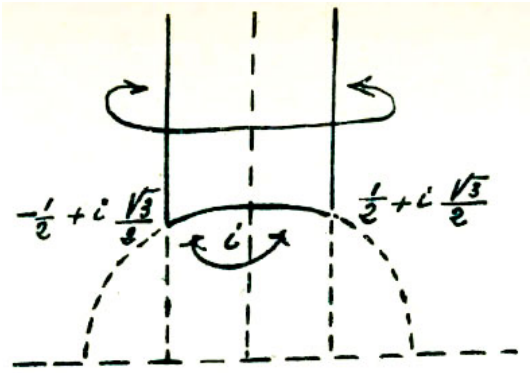


Fig. 9. Trasformazioni che agiscono sul triangolo modulare

Due forme ridotte sono equivalenti soltanto quando sono del tipo

$$ax^2 \pm axy + cy^2 \quad (a \leq c)$$

oppure del tipo

$$ax^2 \pm 2bxy + ay^2 \quad (2|b| \leq a).$$

Nel primo caso dall'una si passa all'altra con la trasformazione $x' = x + y, y' = y$; nel secondo caso con la[50] $x' = -y, y' = x$ (che sono le trasformazioni modulari a cui corrispondono le $S, \mathbb{T}$ sulla T).

[45] *e.c.* e *cor. sup.*: $\xi^2 + \eta^2 = 1$.
[46] Bianchi 1911-12, cap. IV, §29, p. 117.
[47] *lapsus* del curatore: leggasi $\mathbb{T}^2 = 1$
[48] *lapsus* del curatore: leggasi $\mathbb{T}$.
[49] Bianchi 1911-12, cap. IV, §29, p. 117, 118. Dimostrazione analoga a quella di Fubini.
[50] *e.c.* e *cor. sup.*: leggasi $x' = -y, y' = x$ o $x' = y, y' = x$.

Oss.[ervazione] Ricordo che[51] ogni trasformazione $T' = \frac{\alpha T+\beta}{\gamma T+\delta}$ sulla T corrispondono soltanto le due

$$x' = ax + \beta y, \qquad y' = \gamma x + \delta y \ \ ed \ \ x' = -(ax + \beta y), \qquad y' = -(\gamma x + \delta y)$$

sulle x, y.

Può una trasformazione modulare non identica trasformare in sé stesso un punto A interno al semipiano? Poiché ogni tale trasformazione scambia tra di loro i nostri triangoli, ciò potrà avvenire soltanto se A è un punto del contorno di un triangolo, il quale resti lasciato fisso da tale trasformazione.

Cominciamo dal triangolo iniziale; e sia A un punto del suo contorno lasciato fisso da qualche trasformazione del gruppo. Può darsi che tale trasfor//mazione porti il triangolo iniziale in un triangolo adiacente; ed in tal caso A sarà il punto $T = i$, unico punto lasciato fisso da una almeno delle S, T. Se invece la trasformazione, che lascia fisso A, porta il triangolo iniziale in un triangolo non adiacente, il punto A, dovendo essere comune a questi due triangoli, coinciderà con uno dei vertici $\pm\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Il punto $\underline{i}$ è lasciato fisso dalla $T' = -\frac{1}{T}$; il punto $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ dalla $T' = \frac{-T-1}{T}$, e dal suo quadrato; il punto $\frac{1}{2} + i\frac{\sqrt{3}}{2}$ dalla $T' = \frac{T-1}{T}$ e dal suo quadrato.

Gli altri punti del piano, che[52] sono lasciati fissi da una qualche trasformazione modulare, sono i punti equivalenti ad uno dei tre punti precedenti.

Se ne deduce: <u>Le forme quadratiche trasformate in se stesse da una trasformazione modulare distinta dalla</u> $x' = x, y' = y$ <u>e dalla</u> $x' = -x, y' = -y$ <u>sono le forme</u> $a(x^2 + y^2), a(x^2 \pm xy + y^2)$, <u>e le forme equivalenti ad una di queste</u>.

Vale infine il teorema:

<u>Dato</u> $D = ac - b^2$, <u>vi è un numero finito</u>[53] <u>di forme</u> $ax^2 + 2bxy + cy^2$ <u>ridotte a coefficienti interi</u>.

Infatti dalla $2|b| \leq a \leq c, D = ac - b^2$ si deduce: $4ac = 4D + 4b^2 \leq 4D + ac$, donde $3ac \leq 4D$. //

Questa disuguaglianza si può soddisfare in un numero finito di modi con valori interi di a, c con $a \leq c$. Le $2|b| \leq a \leq c, D = ac - b^2$ si possono, per ogni coppia di valori delle a, c, soddisfare con un intiero b in un numero <u>finito</u> di modi. Il numero delle forme ridotte di dato discriminante D si sa calcolare soltanto con la teoria delle serie.

(*) **Nota**: Le frecce della figura hanno un significato analogo a quello usato per i parallelogrammi fondamentali dei precedenti capitoli.

---

[51] *e.c.* e *cor. sup.*: a ogni.

[52] *ad. sup*.

[53] Gazzaniga 1903, cap VIII, p. 177. Gazzaniga afferma qui che ogni forma con determinante positivo è equivalente ad una forma ridotta e che il numero delle forme ridotte aventi determinante positivo è finito (enunciato equivalente a quello di Fubini). Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §75, p. 170. Scrive l'autore: "Dalla definizione di forma ridotta si ricava eziandio il seguente importante teorema. Per ogni determinante positivo esiste soltanto un numero finito di forme ridotte". Cfr. anche Bianchi 1911-12, cap. I, §6, p. 27. Cfr. inoltre Sommer 1907 (trad. 1911), cap. 3, §35, p. 203: "On démotre que toutes les formes de déterminant donné *D* peuvent être réparties en un nombre *fini* de classes". Cfr. infine Gauss 1801, sez. V, art. 223, p. 223, 224.

§.5 ***Riduzione di una forma definita***

Sia A un punto qualsiasi interno al semipiano: cerchiamo di trovare quella trasformazione modulare che porta A nel punto del triangolo iniziale (cioè nel punto ridotto) ad esso equivalente (punto che in generale è unico). Applicando ad A una conveniente potenza delle S $(T' = T + 1)$ porteremo A in un punto A' della striscia $-\frac{1}{2} \leq T \leq \frac{1}{2}$. Se A' è già ridotto, tutto è finito; se così non è, applichiamo ad A' la $\mathrm{T}\left(T' = -\frac{1}{T}\right)$. Il punto A' andrà in un punto equivalente B al quale applicheremo di nuovo una potenza di S, che lo porti in un punto B' della solita striscia; se B' non fosse ridotto, gli applicheremo la[54] T che lo porti in un punto C, sul quale di nuovo ripeteremo le solite operazioni[55]. // Notiamo che, se A' o B' ... non sono punti ridotti, allora essi sono interni al cerchio $\xi^2 + \eta^2 = 1$; se ne deduce facilmente che la T porta un tale punto in un altro che ha l'ordinata maggiore. Invece i punti A ed A' hanno uguale ordinata, i punti B, B' hanno uguale ordinata; cosicché

$$\text{ordinata } A = \text{ordinata } A' < \text{ordinata } B = \text{ordinata } B' < \text{ordinata } C \ldots .$$

È facile dimostrare che non si possono trovare infiniti punti equivalenti le cui ordinate vadano crescendo. Perciò (come nel caso più importante per noi verificheremo anche in altro modo) verrà un momento in cui il procedimento finisce perché si è arrivati a un punto ridotto equivalente ad A.

Interpretiamo questo procedimento col linguaggio della teoria delle forme quadratiche. Applichiamo alla forma $ax^2 + 2bxy + cy^2$ una tale potenza della $x' = x + y, y' = y$ cioè una tale trasformazione $x' = x + ny, y' = y$ (dove n è intero) che la forma così dedotta[56]

$$a(x' - ny')^2 + 2b(x' - ny')^2 y' + cy'^2 \quad 2(b - an)x'y' + c'y'^2$$
$$[c' = c - 2bn + an^2]$$

soddisfi alla

$$2|b - an| \leq a.$$

Se tale forma è ridotta, abbiamo trasformato la // forma data in una ridotta equivalente. Se invece

$c' < a$, applichiamo $x' = y'', y' = -x''$; col che la forma diventa

$$c'x''^2 - 2(b - an)x''y'' + ay''^2.$$

E, se la nuova forma non è ridotta, operiamo in questa come avevamo operato sulla forma iniziale. Notiamo che in queste trasformazioni il coefficiente di xy va diminuendo in valore assoluto; e altrettanto avviene del coefficiente di x^2, il quale resta inalterato quando si applica una potenza di S, e si muta nel coefficiente di y^2, quando si applica la T. Ora la T si applica soltanto, quando il coefficiente di y^2 è minore del coefficiente di x^2. Ora nel caso aritmetico il coefficiente di x^2 e il valore assoluto del coefficiente di xy sono numeri interi positivi che vanno sempre diminuendo. Il procedimento avrà dunque un termine; e pertanto arriveremo a una forma ridotta.

---

[54] *lapsus* del curatore: leggasi T.

[55] Nota inserita da Fubini a p.d.p.: *Disp. 11 Teoria dei numeri*.

[56] *e.c.* e *cor. sup.*: $a(x' - ny')^2 + 2b(x' - ny')y' + cy'^2 = ax'^2 + 2(b - an)x'y' + c'y'^2$ $[c' = c - 2bn + an^2]$.

Esempio

1) Trovare le forme aritmetiche ridotte di determinante 1.
Se $ax^2+2bxy+cy^2$ è una tale forma, allora $ac-b^2=1$ $2|b|\le a\le c$; donde $3ac\le 4$; poiché // $a>0, c>0$, sarà $a=c=1$; e poiché $2|b|\le a$, sarà $b=0$. Vi è la sola forma ridotta x^2+y^2.
Perciò tutte le forme positive $ax^2+2bxy+cy^2$ a coefficienti interi con $ac-b^2=1$ sono equivalenti alla $x^2+y^2=1$, e perciò sono equivalenti tra loro.
2) Trovare la trasformazione che riduce la $f=5x^2+6xy+2y^2$.
Applichiamo la $x=x'+ny, y'=y$. Avremo:

$$f=5(x'+ny')^2+6(x'+ny')^2y'+2y'^2=5x'^2+2(5n+3)x'y'+(5n^2+6n+2)y'^2$$

Vogliamo che $2|5n+3|\le 5$; ne verrà $n=-1$.

(1) $\qquad x=x'-y'; y'=y \qquad f=5x'^2-4x'y'+y'^2.$

Siamo nel caso in cui si deve applicare la[57]

(2) $\qquad x'=y''; y'=-x''$ cosicché $f=x''^2+4x''y''+5y''^2$.

Poniamo
(3) $\qquad x''=x'''+my'''; y''=y'''$ con m intero. Sarà[58]:

$$f=(x'''+my''')^2+4(x'''+my''')y'''+5y'''^2=x'''^2+2(m+2)x'''y'''+(\dots)y'''^2.$$

E si vede che si dovrà porre $m=-2$, col che la forma (il cui discriminante è rimasto immutato) diventa appunto $x'''^2+y'''^2$. Dunque la f iniziale diventa ridotta con la trasformazione prodotto delle $(1),(2),(3)$, cioè //

$$\begin{array}{l|l} x=y'''+(x'''-2y''') & y=-(x'''-2y''') \\ \quad =x'''-y''' & \quad =-x'''+2y'''. \end{array}$$

Scritto per semplicità X,Y al posto di x''', y''' vediamo che con la[59] $x=X-Y, y=-X-2Y$ la f diventa appunto:

$$5(X-Y)^2+6(X-Y)(-X+2Y)+2(-X+2Y)^2=X^2+Y^2.$$

3) Risolvere l'equazione[60]

(4) $\qquad m=ax^2+2bxy+cy^2$ *(a,b,c,m* interi*) ($a>0$)*

Con a,b,c interi ed $ac-b^2=1$. Bisogna a tal fine che sia risolubile la

$$n^2\equiv -1\ (mod\ m),$$

che cioè -1 sia residuo di m. Se così è, e $\frac{n^2+1}{m}=l$ (intero) bisogna che, almeno per una delle radici n di questa congruenza, la
(5) $\qquad mX^2+2nXY+lY^2$

[57] *e.c.* e *cor. sup.*: invece di $-5y''^2$ leggasi $+5y''^2$.
[58] *e.c.* e *cor. sup.*: invece di $-5y'''^2$ leggasi $+5y'''^2$.
[59] *e.c.* e *cor. sup.*: invece di $y=-X-2Y$ leggasi $y=-X+2Y$.
[60] Bianchi 1911-12, cap. IV, §37 p. 152-155. Qui Bianchi fa un esempio numerico analogo quello di Fubini.

sia equivalente al secondo membro dell'equazione data. Quest'ultima condizione è nel nostro caso sempre soddisfatta se $\underline{m}$ è positivo; perché due forme definite positive a coefficienti interi con $D = 1$ sono sempre equivalenti alla $x^2 + y^2$ e quindi equivalenti tra loro. Allora se

$$\begin{cases} x = \alpha X + \beta Y \\ y = \gamma X + \delta Y \end{cases} \tag{6}$$

// porta $ax^2 + 2bxy + cy^2$ nella (5), la $x = \alpha, y = \gamma$ è una soluzione di (4).
Si potrebbe continuare da questo punto di vista; ma, siccome noi abbiamo sempre fatto ricorso (per trovare tali trasformazioni (6)) alla teoria delle forme ridotte, si potrà anche cominciare il calcolo in altro modo.
Noi possiamo trovare una trasformazione

$$x = \alpha X + \beta Y; y = \gamma X + \delta Y;\ (\alpha, \beta, \gamma, \delta\ interi)\ (\alpha\delta - \beta\gamma = 1) \tag{7}$$

che porti $ax^2 + 2bxy + cy^2$ nella $X^2 + Y^2$ ridotta. Risolvere la (4) equivale a risolvere la

$$m = X^2 + Y^2 \tag{8}$$

perché, per mezzo delle (7), si può da ogni soluzione di (4) dedurne una della (8), e viceversa.
Studiamo la (8). Dovremo trovare una radice n della

$$n^2 \equiv -1\ (mod\ m) \tag{9}$$

e trovare le trasformazioni

$$\begin{cases} X = \alpha X' + \beta Y' \\ Y = \gamma X' + \delta Y' \end{cases} \tag{10}$$

che trasformano la $X^2 + Y^2$ nella

$$mX'^2 + 2nX'Y' + lY'^2. \tag{11}$$

Ogni tale trasformazione dà una soluzione $X = \alpha, Y = \gamma$ della (8); e viceversa. Alla (10) corrisponde la //

$$T = \frac{\alpha T' + \beta}{\gamma T' + \delta} \text{ [che indicheremo con } T = VT'] \tag{10}bis$$

che porta il punto A', affisso di (11) nel punto A $(T = i)$ affisso di $X^2 + Y^2$. Se è data tale $(10)bis$, ad essa corrispondono la trasformazione (10) sulle X, Y, e quella che se ne ottiene cambiando i segni di $\alpha, \beta, \gamma, \delta$.
È la $(10)bis$ determinata dalla condizione enunciata?
Siano U, V due trasformazioni tali che

$$A = UA' \qquad A = VA'.$$

Sarà $A' = V^{-1}A$, cioè

$$A = UV^{-1}A.$$

Dunque UV^{-1} trasformerà il punto $T = i$ in sé stesso. Ci troviamo di fronte ad un caso eccezionale perché $T = i$ è trasformato in sé stesso non soltanto dalla trasformazione identica $T' = T$, ma anche dalla $\mathrm{T}\left(T' = -\frac{1}{T}\right)$. Quindi

$$UV^{-1} = 1 \text{ oppure } UV^{-1} = \mathrm{T}, \text{ cioè}$$
$$U = V \text{ oppure } U = \mathrm{T}V.$$

Quindi, nota la V, ogni altra U, che goda della stessa proprietà, coincide con V e con $\mathrm{T}V$; si hanno pertanto due trasformazioni $(10)bis$ e corrispondentemente quattro trasformazioni (10).
Come esempio, troviamole supposto $m = 2$. Allora è $n = 1$; la (11) diventa //

$$2X'^2 + 2X'Y' + Y'^2.$$

Troviamo una (10) che porti questa forma nella $X^2 + Y^2$; ciò equivale a trovare una trasformazione che riduce la[61] $2X'^2 + 2XY' + Y'^2$. Si trova, con metodi sopra svolti,

$$X = X' \qquad X = -X'$$
$$Y = X' + Y' \text{ con la } Y = -X' - Y'$$

insieme alle

$$X = X' + Y' \qquad X = -X' - Y'$$
$$Y = -X' \qquad Y = -Y'.$$

Si deduce che $2 = X^2 + Y^2$ ha 4 soluzioni[62]

$$\begin{cases} X = 1 \\ Y = 1' \end{cases} \quad \begin{cases} X = -1 \\ Y = -1' \end{cases} \quad \begin{cases} X = 1 \\ Y = -1' \end{cases} \quad \begin{cases} X = -1 \\ Y = -1 \end{cases}$$

(che erano evidenti a priori). Le soluzioni della[63]

$$2 = 5x^2 + bxy + 2y^2$$

se ne deducono tosto con le

$$x = X - Y \qquad y = -X + 2Y$$

trovate all'esercizio precedente.

Si supponga, invece, $m = p$ (e primo dispari). La

$$n^2 \equiv -1 \ (mod\ p)$$

è risolubile[64] soltanto se -1 è residuo $(mod\ p)$, cioè se p è $\equiv 1\ (mod\ 4)$. E in tal caso ha due soluzioni $\pm\alpha$; si dovranno considerare le quattro trasfor//mazioni che portano $X^2 + Y^2$ in ciascuna delle $px^2 + 2\alpha xy + c'y^2$ (essendo $\frac{\alpha^2+1}{p} = c'$): in tutto ne dedurremo otto soluzioni della $p = X^2 + Y^2$. Ma, poiché da una soluzione se ne possono dedurre altre sette (in fondo

---

[61] *e.c.* e *cor. sup.*: $2X'^2 + 2X'Y' + Y'^2$.
[62] *e.c.* e *cor. sup.*: invece della seconda $\{$ leggasi $\begin{cases} X = -1 \\ Y = 1 \end{cases}$.
[63] *e.c.* e *cor. sup.*: $2 = 5x^2 + 6xy + 2y^2$.
[64] Bianchi 1911-12, cap. I, §11, p. 46

non distinte da quella) cambiando i segni di una o di entrambe le X, Y, oppure permutando le X, Y, avremo che: Se $p \equiv 1\ (mod\ 4)$ e soltanto in tal caso, il primo dispari p è somma dei quadrati di due interi x, y (completamente determinati, a meno dell'ordine e del segno) (Teorema di Fermat[65], dimostrato per la 1^a volta da Eulero[66]). E questo teorema si può generalizzare ad ogni equazione aritmetica $p = ax^2 + 2bxy + cy^2$ con a, b, c interi ed $ac - b^2 = 1$.

Osserv.[azione] Con questo metodo si trovano le soluzioni proprie; le improprie si determinano, come sappiamo, per via analoga; esse si presentano soltanto se m è divisibile per qualche quadrato.

§.6 ***Forme indefinite***[67]

Una trasformazione[68]

$x' = lx + my$

$y' = nx + py \qquad ep - mn = 1$

applicata a una forma //

$$ax^2 + 2bxy + cy^2 \tag{1}$$

la trasforma in un'altra di uguale discriminante. Applichiamo questo teorema a una forma del fascio determinato dalla (1) e dalla

$$rx^2 + 2sxy + ty^2 \tag{2}$$

cioè alla[69]:

$$(a + \lambda r)z^2 + 2(b + \lambda s)xy + (c + \lambda t)y^2.$$

Il valore di

$$(a + \lambda r)(c + \lambda t) - (b + \lambda s)^2 = ac - b^2 + \lambda(rc + at - 2bs) + \lambda^2(2t - s^2)$$

non varia, applicando contemporaneamente alle nostre forme una stessa delle citate trasformazioni. Ciò in particolare avverrà per $ac - b^2$ ed $rt - s^2$ [come sapevamo, trattandosi di espressioni uguali ai discriminanti di (1) (2)]; altrettanto avverrà per

$$I = rc + at - 2bs,$$

---

[65] Si fa qui riferimento all'ultimo teorema di Fermat che afferma che non esistono soluzioni intere positive dell'equazione $a^n + b^n = c^n$ se $n > 2$. Fermat enunciò tale risultato nel 1637, ma non rese nota la dimostrazione che affermò di aver trovato. Scrisse in proposito, ai margini di una copia dell'*Arithmetica* di Diofanto di Alessandria: "Dispongo di una meravigliosa dimostrazione di questo teorema, che non può essere contenuta nel margine troppo stretto della pagina". Tale teorema fu dimostrato rigorosamente solo nel 1994 da Andrew John Wiles (Cambridge, 11 aprile 1953); la dimostrazione è stata pubblicata nel 1995 all'interno dell'articolo *Modular elliptic curves and Fermat's Last theorem*.

[66] Euler formulò una dimostrazione dell'ultimo teorema di Fermat per $n = 3$. Tale dimostrazione è effettuata con il metodo della discesa infinita e in essa si fa uso dei numeri complessi. Il 4 agosto 1753 il matematico tedesco annunciò all'amico Goldbach, in una lettera, di essere riuscito a dimostrare che "un cubo in numeri interi non può essere la somma di due cubi"; la dimostrazione fu pubblicata solo successivamente all'interno della sua celebre *Algebra* (1770). cap. 15, §423, p. 486-489.

[67] Gazzaniga 1903, cap. VIII, p. 194 e Bianchi 1911-12, cap. I, §8, p. 33. Fubini, come Bianchi, definisce "forme indefinite" le forme aventi determinante positivo; Gazzaniga invece le chiama "forme di segno indeterminato".

[68] *e.c.* e *cor. sup.*: invece di $ep - mn = 1$ leggasi $lp - mn = 1$.

[69] *e.c.* e *cor. sup.*: $(a + \lambda r)x^2 + 2(b + \lambda s)xy + (c + \lambda t)y^2$.

che pertanto è un invariante comune delle forme $(1), (2)$.
Se $I = 0$, le forme diconsi coniugate[70]; se due forme sono coniugate, anche le forme che se ne deducono, applicando una qualsiasi delle nostre trasformazioni, sono coniugate. Sarà utile esercizio l'interpretare geometricamente il coniugio // di due forme.
Sia (2) definita positiva; e ne sia

$$\xi + i\eta = -\frac{s}{r} \pm i\sqrt{\frac{tr - s^2}{r^2}} \qquad \left[\xi = -\frac{s}{r};\ \xi^2 + \eta^2 = \frac{t}{r}\right]$$

l'affisso. La relazione di coniugio diventa:

$$c + 2b\xi + a(\xi^2 + \eta^2) = 0. \tag{3}$$

Se la forma (1) è indefinita $(b^2 - ac = \Delta > 0)$, la (3) definisce un cerchio reale, luogo degli affissi delle forme definite coniugate con (1).
Questo cerchio ha il centro sull'asse delle ξ; incontra questo asse nei punti, le cui ascisse soddisfano alla:

$$a\xi^2 + 2b\xi + c = 0 \qquad \left(\xi = -\frac{b}{a} \pm \frac{\sqrt{b^2 - ac}}{a}\right)$$

cioè nei punti, che si potrebbero chiamare gli affissi della (1) [affissi che ora sono entrambi reali].
Conosciuto Δ, la forma è determinata dal cerchio, a meno del segno. Infatti, dato il cerchio, restano determinati i rapporti delle a, b, c; e, se in più è noto Δ, le a, b, c sono determinate a meno del segno. Per non avere ambiguità di segno si chiami $-\frac{b}{a} + \frac{1}{2}\sqrt{b^2 - ac}$ il primo affisso, l'altro il secondo affisso. E si ponga sul cerchio una freccia che fissi il verso dal primo al secondo affisso. Dato il cerchio, e tale verso la forma è com//pletamente determinata. Se con una delle solite trasformazioni la (1) è portata in un'altra forma

$$a'x'^2 + 2b'x'y' + c'y'^2 \tag{1}'$$

è facile riconoscere col calcolo effettivo che la trasformazione corrispondente sulla $T = \xi + i\eta$ porta non solo il cerchio, ma anche il verso corrispondenti ad (1) nel cerchio e nel verso corrispondenti ad $(1)'$ (cioè porta il primo affisso di (1) proprio nel primo affisso di $(1)'$, il secondo affisso di (1) nel secondo affisso di $(1)'$).
Noi diremo che una forma (1) è ridotta se il cerchio immagine incontra il triangolo fondamentale della rete modulare. Esso in tal caso conterrà all'interno o sulla periferia almeno uno dei punti $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$; i punti (ξ, η) all'interno di (3) soddisfano alla

$$a\{a(\xi^2 + \eta^2) + 2b\xi + c\} < 0.$$

Quindi dovrà essere almeno con uno dei segni $\pm$,

$$a^2 \pm ab + ac \leq 0 \quad \text{ossia} \quad a(a + c \pm b) \leq 0.$$

[70] Gazzaniga 1903, cap. VIII, p. 162. Gazzaniga dà qui una definizione di forme coniugate differente ma equivalente a quella di Fubini, , ossia "le due forme: (a, b, c) e $(-a, -b, -c)$ dicesi coniugate fra di loro". Cfr. anche Kronecker 1882, cap. II, §18.

Cioè a deve avere segno opposto di almeno una delle[71] $a + c \pm b$ (o una delle $a, a + c \pm b$ deve essere nulla). Ogni forma F è equivalente almeno ad una ridotta[72] R. Infatti, scelto un punto generico A del semicerchio immagine di F nel solito semipiano, noi possiamo con // una trasformazione modulare portare A in un punto A' del nostro triangolo fondamentale per il gruppo modulare. Allora il semicerchio corrispondente ad F viene mutato in un semicerchio che incontra tale triangolo.
La trasformazione corrispondente sulle x, y porterà pertanto F in una forma ridotta. Per ogni valore (positivo) intero di Δ esiste un numero finito di forme ridotte a coefficienti interi[73].
Infatti dalle

$$a^2 + ac \pm ab \leq 0 \quad \Delta = b^2 - ac$$

si deduce

$$a^2 + b^2 \pm ab \leq +\Delta \ cio\grave{e}\ 3a^2 + (2b \pm a)^2 \leq 4\Delta,$$

che si può scrivere anche nella forma[74]

$$3b^2 + (2a \pm b)^2 \leq 4\Delta.$$

Questa disuguaglianza limita, dato Δ, il numero dei valori (interi) che si possono dare ad a, b, e quindi anche dei valori che si possono dare alla $c = \frac{b^2 - \Delta}{a}$, che deve d'altra parte essere ancora intera; ciò che porta una nuova restrizione ai possibili valori delle a, c.

c.d.d.

Osserv.[azione] Come segue dalla dim. del penultimo teorema, per ridurre una forma indefinita basta // trovare una trasformazione modulare che riduca una delle forme definite coniugate: cioè lo stesso algoritmo di riduzione delle forme definite si può applicare alle indefinite.

§.7 ***Periodi di forme ridotte***[75]

Possono due forme ridotte essere equivalenti tra loro?
Abbiamo visto che vi è grande indeterminazione nel modo di ridurre una data forma indefinita (secondo la forma definita coniugata che si riduce). Riesce dunque probabile che una forma si possa ridurre in più di un modo, e che una forma ridotta possa essere equivalente ad altre forme ridotte distinte (caso che era da riguardarsi come eccezionale per le forme definite). Noi ci proponiamo dunque il problema:
Quando due forme ridotte indefinite sono equivalenti?
Risposto a questa domanda, sarà risoluto il problema analogo anche per forme non ridotte: due tali forme saranno equivalenti quando, trasformatele coi metodi noti, in forme ridotte, queste risulteranno equivalenti. //

---

[71] *Idem*, cap. VIII, p. 177. Gazzaniga osserva che i coefficienti *a* e *b* devono essere necessariamente di segno opposto (caso meno generale rispetto a quello trattato da Fubini).
[72] *Ibid.* Gazzaniga scrive "Ogni forma con determinante positivo è equivalente ad una forma ridotta". Cfr. anche Bianchi 1911-12, cap. I, §8, p. 35.
[73] *Ibid.* Gazzaniga scrive "Il numero delle forma ridotte aventi lo stesso determinante è finito". Cfr. anche Bianchi 1911-12, cap. I, §8, p. 35.
[74] Bianchi 1911-12, cap. IV, §31, p. 125.
[75] *Idem*, cap. IV, §31, p. 127-130. Bianchi dedica a tale studio l'intero paragrafo *Periodi delle forme ridotte – Risoluzione del problema dell'equivalenza*.

Se F, F' sono forme ridotte equivalenti, vi sarà una trasformazione modulare che porta il semicerchio C orientato, immagine di F nel semicerchio C' orientato immagine di F'. [Dico orientato un semicerchio di cui sia fissato il verso].
Una tale trasformazione porterà ogni triangolo della rete attraversato da C in un triangolo attraversato da C'. Poiché C' e C incontrano entrambi il triangolo fondamentale, ne segue che una tale trasformazione porta almeno[76] uno dei triangoli incontrati da C nel triangolo fondamentale.
E viceversa, se una trasformazione modulare porta uno dei triangoli attraversato da C nel triangolo fondamentale esso porta la F in una forma ridotta equivalente. Premettiamo, ora, un'osservazione:
Ogni triangolo della rete modulare si ottiene applicando una trasformazione modulare U al triangolo fondamentale limitato dalle rette $\xi = \frac{1}{2}, \xi = -\frac{1}{2}$ e dal cerchio $\xi^2 + \eta^2 = 1$. Ogni trasformazione modulare, come è noto, trasforma in sé stesso il sistema delle rette dei cerchi normali all'asse delle ξ. Perciò ogni triangolo della rete // è, come il triangolo modulare, limitato da rette e cerchi normali all'asse delle ξ. I suoi vertici sono i punti ove la trasformazione U porta i vertici del triangolo fondamentale. I vertici trasformati di $\mp\frac{1}{2} + i\frac{\sqrt{3}}{2}$ sono <u>interni</u> al semipiano; il terzo vertice è il punto, dove la U porta il vertice $T = i_\infty$ del triangolo fondamentale; cioè (se U è definita da[77] $T' = \frac{\alpha T + \beta}{\gamma T + \delta}$) il terzo vertice è il punto $T = \frac{\alpha}{\gamma}$; esso è pertanto ancora all' ∞, se $\gamma = 0$, ed è invece il punto ($\xi = \frac{\alpha}{\gamma} =$ numero razionale; $\eta = 0$) dell'asse delle ξ, se $\gamma \neq 0$.
Invece il cerchio immagine di una forma indefinita incontra l'asse delle ξ in un punto irrazionale, che è perciò distinto da ogni vertice della rete modulare. Ne segue facilmente che ogni tale cerchio interseca infiniti triangoli della rete.
Sia C un cerchio immagine di una forma ridotta F. Esso incontrerà il triangolo t iniziale; appena uscito da t, incontrerà uno dei triangoli adiacenti a t; se invece[78] C passa proprio per uno dei punti $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, appena oltrepassato questo punto, attraverserà un triangolo che con $\underline{t}$ ha un vertice comune. //
Sia t' un tale triangolo (adiacente a $\underline{t}$, o che con $\underline{t}$ ha almeno un vertice comune) attraversato da C.
La trasformazione che porta t' in t porta C in un nuovo cerchio C' che incontra t, porta la forma F, di cui C è l'immagine, in un'altra forma F' ridotta che diremo <u>contigua</u> di F. Se noi consideriamo invece il triangolo t'', adiacente a t o che ha almeno un punto comune con t, che il cerchio C incontra prima di arrivare a t, otterremo corrispondentemente un'altra forma F'', che pure diremo <u>contigua</u> di F.
Se F' si chiama la forma contigua a destra di F, la F'' si chiama la forma contigua a sinistra. Evidentemente la contigua a destra di F'' è la stessa F.
Ora, se t_1 è uno qualsiasi dei triangoli attraversati da C, la trasformazione che porta t_1 in t, porta la F in una nuova ridotta F_1. E, come i triangoli incontrati da C si susseguono su C

[76] *ad. post.* e *a.m.*
[77] *e.c.* e *cor. sup.*: $T' = \frac{\alpha T + \beta}{\gamma T + \delta}$.
[78] *ad. post.* e *a.m.*

in un certo ordine, così ne viene che tali forme F_1 ridotte si potranno disporre nell'ordine dei corrispondenti triangoli[79]. Due forme ridotte consecutive saranno // contigue.[80]
Ma, poiché le ridotte di dato discriminante a coefficienti interi sono in numero finito, tali forme F_1 sono in numero finito. Vale a dire nella successione di tali forme F_1 ve ne saranno due uguali tra loro.
Siano, per esempio, $\varphi_r, \varphi_{r+1}, \dots, \varphi_{r+s}$ forme a due a due contigue tali che $\varphi_r = \varphi_{r+s}$; e supponiamo che le forme intermedie siano distinte tra loro e dalle φ_r, φ_{r+s}. Nella successione di forme ridotte, che contiene le forme precedenti, la forma φ_{r+s+1} contigua, per esempio, a destra di φ_{r+s} cioè di φ_r, sarà identica a φ_{r+1}; la φ_{r+s+2} a φ_2, ecc. Così, la φ_{r-1} contigua a sinistra di $\varphi_r = \varphi_{r+s}$ coinciderà con[81] φ_{r+2-1}, ecc, ecc.
Vale a dire la nostra successione consta delle forme $\varphi_r, \varphi_{r+1}, \dots, \varphi_{r+s-1}$ ripetute infinite volte nell'ordine stesso in cui sono qui scritte.
Tali forme si dicono costituire un periodo[82] di forme ridotte (che si potrebbe provare intimamente connesso al periodo dei quoti incompleti nello sviluppo in frazione continua degli affissi di tali forme). //
Ogni forma indefinita a coefficienti interi è equivalente a tutte e sole le forme ridotte di ugual discriminante e di uno stesso periodo.[83]

Oss.[ervazione] Le trasformazioni che portano una ridotta nelle due contigue sono generalmente due delle S, S^{-1}, T che portano t in un triangolo adiacente; soltanto eccezionalmente una di esse può invece coincidere con una delle trasformazioni che porta t in un triangolo che con t ha comune uno dei vertici[84] $\pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$.
Il lettore può facilmente riconoscere se e quando si presenta questo caso eccezionale.

§.8 *Trasformazioni che portano una forma in una forma equivalente*

Sia F una forma ridotta, e sia $\dots, F_{-2}, F_{-1}, F, F_1, F_2 \dots$ la successione di forme ridotte, a due a due contigue, che ne possiamo dedurre. Sia i, p. es., il minimo valore positivo tale che $F = F_i$. Ora ognuna delle precedenti forme F_k definisce una trasformazione modulare che porta F in F_k. Le forme uguali alla F sono soltanto le

$$\dots, F_{-3i}, F_{-2i}, F_{-i}, F, F_i, F_{2i}, F_{3i}, \dots$$

// Ognuna di queste definirà una trasformazione modulare che porta F in sé stessa. Se U è la trasformazione che porta F in F_i (cioè in sé stessa), tutte queste altre trasformazioni saranno le potenze della U. Se φ è una forma qualsiasi equivalente alla ridotta F, e se V porta la φ

[79] Nota inserita da Fubini a p.d.p.: *Disp. 12 Teoria dei numeri*.
[80] Dirichlet 1877 (trad. 1881), cap. IV, §63, p. 146: "Il caratteristico della relazione fra due così fatte forme contigue φ e φ' consiste primamente in ciò, che esse hanno lo stesso determinante, in secondo luogo, che l'ultimo coefficiente a dell'una forma, della φ, è ad un tempo il primo coefficiente dell'altra forma φ', ed in terzo luogo, che la somma $b + b'$ dei loro coefficienti medi è divisibile per questo comun coefficiente a'".
[81] *e.c.* e *cor. sup.*: φ_{r+s-1}.
[82] Dirichlet 1877 (trad. 1881), cap. IV, §78, p. 177, 178: "Dai teoremi or ora dimostrati sulle forme ridotte contigue a destra e sinistra si deduce che tutte le forme ridotte di un determinante positivo D si possono distribuire in periodi".
[83] Bianchi 1911-12, cap. I, §29, p. 129. Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §82, p. 191.
[84] *e.c.* e *cor. sup.*: $\pm\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

nella F_1 allora la $V^{-1}UV$ trasforma la φ in sé stessa; ed evidentemente tutte e sole le potenze di $V^{-1}UV$ portano φ in sé stessa.
Per ogni forma indefinita a coefficienti interi esiste una ed una sola trasformazione modulare, che con le sue potenze esaurisce tutte le trasformazioni modulari, che trasformano la forma in sé stessa[85].
Sia data la forma

$$ax^2 + 2bxy + cy^2.$$

La $\left.\begin{array}{l}\lambda x' + \mu y' = x \\ \nu x' + \rho y' = y\end{array}\right\}$ $(\lambda\rho - \mu\nu = 1)$

trasformi tale forma in $ax'^2 + 2bx'y' + cy'^2$, cioè trasformi la forma in sé stessa. Cioè equivale ad imporre alle λ, μ, ν, ρ (oltre alla $\lambda\rho - \mu\nu = 1$) le condizioni

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a \qquad (1)$$
$$a\lambda\mu + b(\lambda\rho + \mu\nu) + c\nu\rho = b. \qquad (2)$$

// Se $b^2 - ac$ non è un quadrato perfetto, e quindi $a \neq 0$, si ponga

$$u = \frac{\nu}{a} \quad (\nu = au).$$

Si deduce facilmente, ponendo in (2) $\mu - \nu + 1$ al posto di $\lambda\rho$, e quindi eliminando tra l'equazione così ottenuta e la (1) una volta $2b$, una seconda volta c:

$$\mu = -cu \qquad \lambda - \rho = -2bu.$$

Ora

$$(\lambda + \rho)^2 = (\lambda - \rho)^2 + 4\lambda\rho = 4b^2u^2 + 4(\mu\nu + 1) = 4(b^2 - ac)u^2 + 4.$$

Posto

$$\frac{\lambda + \rho}{2} = t$$

si avrà pertanto

$$t^2 - \Delta u^2 = 1 \qquad (3)$$
$$\nu = au; \ \ \mu = -cu; \ \ \lambda = t - bu; \ \ \rho = t + bu. \qquad (4)$$

Se λ, μ, ν, ρ sono interi, e se δ è il M.C.D. di $a, 2b, c$ (che potremo sempre supporre uguale ad 1 oppure a 2) allora

$$au\ (= \nu), \qquad cu\ (= -\mu), \qquad 2bu\ (= \rho - \lambda)$$

sono interi. Cioè

$$U = \frac{u}{\sigma} \text{ è intero.}$$

Pertanto è intero anche $\mathbb{T} = \frac{t}{\sigma}$, perché da (3) si deduce[86]

[85] Bianchi 1911-12, cap. IV, §33, p. 131.
[86] *Idem*, cap. IV, §33, p. 133. Cfr. anche Dirichlet 1877 (trad. 1881), cap. IV, §83, p. 192, 193.

$$\mathrm{T}^2 - \Delta U^2 = \sigma^2.$$

// Per semplicità continuiamo il calcolo, supponendo $\sigma = 1$.
[87]La ricerca delle nostre trasformazioni equivale pertanto in tal caso alla ricerca delle soluzioni[88] intere della precedente equazione di Pell[89] con $\sigma = 1$. Se $\mathrm{T} = \mathrm{T}_0, U = U_0$ è una tale soluzione, allora la trasformazione modulare

$$\left.\begin{aligned} x &= \mathrm{T}_0 x' + \Delta U_0 y' \\ y &= U_0 x' + \mathrm{T}_0 y' \end{aligned}\right\} \qquad (5)$$

trasforma la forma $x^2 - \Delta y^2$ in se stessa. Noi dunque siamo ridotti a studiare questa unica forma. Noi sappiamo che basta trovare una di tali trasformazioni (la cosiddetta trasformazione minima) per poter trovare tutte le altre con innalzamento a potenza. E noi abbiamo insegnato a calcolare tale trasformazione minima.[90]
Si noti che il quadrato di (5) è definito dalle

$$\begin{aligned} x &= (\mathrm{T}_0^2 + \Delta U_0^2)x' + \Delta(2U_0\mathrm{T}_0)y' \\ y &= 2U_0\mathrm{T}_0 x' + (\mathrm{T}_0^2 + \Delta U_0^2)y' \end{aligned}$$

a cui corrisponde la nuova soluzione

$$\mathrm{T}_1 = T_0^2 + \Delta U_0^2 \qquad U_1 = 2U_0\mathrm{T}_0$$

della equazione di Pell; notiamo che

$$\mathrm{T}_1 + U_1\sqrt{\Delta} = \left(\mathrm{T}_0 + U_0\sqrt{\Delta}\right)^2.$$

// Così, in generale, si dimostra facilmente che se T_0, U_0 è la soluzione è minima, le altre soluzioni T, U si ottengono dalla

$$\mathrm{T} + U\sqrt{\Delta} = (\mathrm{T}_0 + U_0\sqrt{\Delta})^n \text{ (per } \underline{n} \text{ intero).}$$

Vedremo più avanti l'intima ragione di questo fatto.
Per risolvere un'equazione Diofantea

$$m = ax^2 + 2bxy + cy^2$$

anche nel caso attuale è necessario trovare tutte le trasformazioni che portano $ax^2 + 2bxy + cy^2$ in una delle forme equivalenti $mx^2 + 2nxy + ly^2$ di uguale discriminante, corrispondenti alle soluzioni della $n^2 \equiv \Delta\ (mod\ m)$.
Ora, con l'algoritmo delle forme ridotte, noi sappiamo calcolare una di queste trasformazioni (prodotto di una trasformazione che porta $ax^2 + 2bxy + cy^2$ in una forma ridotta e dell'inversa della trasformazione che porta la $mx^2 + 2nxy + ly^2$ nella stessa ridotta). Se U è una delle trasformazioni cercate, tutte le altre si ottengono moltiplicando U per tutte le

[87] Gazzaniga 1903, cap. VIII, p. 193, 194.
[88] Bianchi 1911-12, cap. IV, §34, p. 136. A differenza di Fubini, Bianchi dedica un intero paragrafo, intitolato *Algoritmo per la formazione dei periodi e per la risoluzione dell'equazione di Pell*, ai metodi computazionali per risolvere tali problemi.
[89] Minkowski 1910, §45, p. 147-171. La notazione utilizzata dal matematico tedesco differisce solo nel termine noto da quella adottata da Fubini; scrive infatti $\mathrm{T}^2 - \Delta U^2 = \varepsilon^2$. Cfr. anche Weber 1895, p. 395-399.
[90] Dirichlet 1877 (trad. 1881), cap. IV, §84, p. 199-204. La trattazione di Fubini è del tutto analoga a quella sviluppata da Dirichlet in questa sezione.

trasformazioni che portano $ax^2 + 2bxy + cy^2$ in sé stessa, che noi abbiamo imparato a calcolare.
Cfr. il libro citato di Dirichlet-Dedekind per esercizi: // il metodo ivi seguito è però differente dal nostro. A lezione abbiamo esposto come si interpretino in geometria non euclidea le teorie qui svolte. Ma noi, ora, senz'altro passiamo ad un altro campo di studi, in cui sono incluse, come caso particolarissimo, le precedenti ricerche. Per più ampi sviluppi Cfr. le Lezioni del Prof. Bianchi sulla teoria aritmetica delle forme quadratiche (binarie e ternarie)[91]

10. Guido Fubini

[91] Fubini qui fa riferimento all'opera di Bianchi, *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie* (1911-12) già citata in numerose note precedenti.

Capitolo VI – Numeri interi algebrici

§.1 *Una prima generalizzazione del numero intero*[1]

Chiamiamo numeri razionali (di Gauss[2]) i numeri $x + iy$, con x, y numeri razionali ordinari; il loro insieme che indicheremo con $K(i)$ si chiamerà il corpo generato da i, perché contiene tutti e soli i numeri che si ottengono da i in un numero finito di operazioni aritmetiche (somme, sottrazioni, prodotti, divisioni).

Quelli, tra i numeri precedenti, per cui x, y sono interi ordinari, si dicono interi di Gauss. E, per evitare equivoci, gli ordinari numeri interi si di//ranno interi razionali. Un intero $x + iy$ di Gauss soddisfa l'equazione di secondo grado in z

$$z^2 - 2xz + (x^2 + y^2) = 0,$$

il cui primo coefficiente è 1, gli altri due sono interi razionali. L'altra radice $x - iy$ si dirà il numero coniugato[3]. Poiché anch'essa è un numero di $K(i)$, cioè, poiché $K(i)$ insieme ad ogni intero di Gauss contiene anche il coniugato, tale corpo $K(i)$ si dice essere un corpo di Galois. Un intero di Gauss coincide col coniugato soltanto quando è un intero razionale.

Norma[4] di un intero $x + iy$ dicesi il prodotto $x^2 + y^2$ di esso per il coniugato.

L'intero z dicesi divisibile[5] per t, se $\frac{z}{t}$ è intero. Due interi z, t diconsi associati[6], se ciascuno di essi è divisibile per l'altro. In tal caso il loro quoziente è un numero u tale che u e il reciproco $\frac{1}{u}$ sono entrambi interi. Altrettanto avverrà dei numeri coniugati $u', \frac{1}{u'}$. Quindi uu' ed $\frac{1}{uu'}$ sono numeri razionali interi.

Pertanto $uu' = \pm 1$ (anzi nel caso attuale $uu' = 1$). Cioè la norma di u vale ± 1. E viceversa, se la norma di $\frac{z}{t}$ vale ± 1, i numeri z, t sono associati[7]. //

Un numero, la cui norma vale ± 1, dicesi un'unità[8]. (Le unità sono i numeri $\pm 1, \pm i$, cioè le potenze di i). Due numeri sono associati, se il loro quoziente è un'unità.

Se $\alpha + i\beta$ è un qualsiasi numero complesso, si trovino gli interi razionali x, y tali che $|\alpha - x| \leq \frac{1}{2}$, $|\beta - y| \leq \frac{1}{2}$.

Sarà (indicando con $Nm\, z$ la norma di z):

---

[1] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 424-442. Dedekind, autore di questo supplemento, esordisce scrivendo "Il concetto di numero intero in questo secolo ha ricevuto un'estensione, per mezzo della quale alla teoria dei numeri furono aperte strade sostanzialmente nuove; il primo e il più notevole passo in questo campo lo ha fatto Gauss, e noi esporremo innanzi tutto la teoria da lui fondata dei numeri interi complessi".

[2] Weber 1895, p. 585-594. L'autore parla qui di "numeri di Gauss". Cfr. inoltre Sommer 1907 (trad. 1911), cap. 1, §4, p. 13: "Gauss avec l'heureuse intuition du génie a ouvert de nouveaux et riches domaines à la science".

[3] Gazzaniga 1903, cap. IX, p. 223. Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 425.

[4] *Idem*, cap. IX, p. 223. Gazzaniga scrive "dicesi […], il prodotto N di (a, b) pel suo coniugato, norma". Cfr. anche Bianchi 1920-21, Introduzione, §1, p. 4, 5. A differenza di Fubini, Bianchi introduce per prima cosa il campo degli interi di Gauss. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 426; Fubini utilizza qui la stessa notazione di Dedekind. Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §6, p. 23.

[5] Bianchi 1920-21, Introduzione, §1, p. 6. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 426; qui Dedekind scrive "L'analogia con la teoria dei numeri razionali ci consiglia così ad introdurre il concetto di divisibilità".

[6] Gazzaniga 1903, cap. IX, p. 227: "Due interi (a, b) e (c, d) diversi da zero, divisibili l'uno per l'altro si dicono tra loro associati". Cfr. anche Bianchi 1920-21, Introduzione, §1, p. 6.

[7] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 428.

[8] Gazzaniga 1903, cap. IX, p. 224; Bianchi 1920-21, Introduzione, §1, p. 6. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 427: "Per unità s'intende ogni numero intero ε, che sia divisore del numero 1 e per conseguenza anche di tutti i numeri interi".

$$Nm\ [(\alpha + i\beta) - (x + iy)] \leq \frac{1}{2}.$$

Siano $u + iv, h + ik$ due interi di Gauss. Potrò trovare un intero $x + iy$ di Gauss tale che

$$Nm\left\{\frac{u + iv}{h + ik} - (x + iy)\right\} \leq \frac{1}{2}$$

cosicché

$$Nm\,\{(u + iv) - (h + ik)(x + iy)\} \leq \frac{1}{2} Nm\,(h + ik).$$

Il numero $x + iy$ si potrà chiamare il quoziente della divisione di $u + iv$ (dividendo) per $h + ik$ (divisore). Si dirà resto il numero $(u + iv) - (h + ik)(x + iy)$, la cui norma non supera la metà della norma del divisore.
Si ha così, con lieve variante per ciò che riguarda il resto, una completa analogia con la divisione degli interi nell'aritmetica elementare. E l'analogia // si potrebbe rendere più completa se nella divisione di due interi razionali positivi o negativi, noi imponessimo al resto di non superare in valore assoluto la metà del divisore[9].
Partendo da questa definizione, noi potremmo costruire un algoritmo affatto analogo a quello di Euclide per la ricerca del M.C.D.[10] di due o più interi in $K(i)$, definendo come M.C.D. di più interi un intero di Gauss che sia loro divisore comune e che sia a sua volta divisibile per ogni altro loro divisore comune[11].
Il M.C.D. così definito non risulta però completamente determinato; ma la sua indeterminazione si riduce a questo che lo si può cambiare con uno dei numeri associati.
Poiché se z, t sono interi di Gauss, e z è un divisore di t, la $Nm\,z$ non può superare $Nm\,t$, se ne conclude che un numero può avere al più un numero intero[12] z finito di divisori.
Se z_1 è quello di norma minima, che è distinto da un'unità, se z_2 è il divisore di norma minima di $\frac{z}{z_1}$ e se z_2 non è un'unità, se z_3 è il divisore (che non sia un'unità) di norma minima del//l'intero $\frac{z}{z_1 z_2}$ ecc. se ne conclude facilmente che ogni intero z è associato a un prodotto

$$z_1 z_2 \ldots z_n \qquad (n = \text{ intero razionale finito}),$$

dove un intero z_i è divisibile soltanto per le unità o per i numeri ad esso associati. Tali numeri si diranno primi[13].
Perciò ogni intero di Gauss è decomponibile nel prodotto di un numero finito di fattori primi[14]. E, come nell'aritmetica ordinaria, si dimostra che tale decomposizione è unica[15], purché non si riguardino come distinti due prodotti, quando i fattori del primo sono ordinatamente associati ai fattori del secondo [così come nell'aritmetica solita non si riguardano distinte le decomposizioni $15 = 3 \cdot 5 = (-3)(-5)$].
Cerchiamo gli interi $\pi = x + iy$ primi in $K(i)$. Sia π' il coniugato di π, evidentemente primo anch'esso. I multipli razionali interi di $Nm\,\pi = \pi\pi' = x^2 + y^2$ sono interi razionali

[9] Bianchi 1920-21, Introduzione, §1, p. 9, 10; §2, p. 11, 12.
[10] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 428, 429.
[11] Gazzaniga 1903, cap. IX, p. 227-232. Qui Gazzaniga illustra approfonditamente il "procedimento delle successive divisioni".
[12] *ad. sup.*
[13] Bianchi 1920-21, Introduzione, §1, p. 7.
[14] *Idem*, Introduzione, §2, p. 13, 14.
[15] Gazzaniga 1903, cap. IX, p. 240. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 432.

divisibili per π. Sia $\underline{p}$ il minimo intero razionale positivo divisibile per π. Se fosse $p = 1$, sarebbe $Nm\,\pi = 1$, cioè π sarebbe un'unità e non sarebbe primo. Dunque $p > 1$. Se p non fosse un primo razionale, // e fosse $p = qr$ con $1 < q < p, 1 < r < p$, allora π, dividendo il prodotto qr, dividerebbe uno dei fattori q, r. Cioè p non sarebbe il minimo intero razionale positivo divisibile per[16] p. Dunque $\underline{p}$ è <u>primo</u>[17]. Ora, $Nm(p) = p^2$. Quindi $Nm(\pi)$ è un intero positivo razionale divisore di p^2.
Cioè[18] $Nm\,\pi = p^2$ oppure $Nm\,\pi = p$.
Caso 1°. $Nm\,\pi = p^2$. Il numero π dicesi primo di secondo grado; $\pi\pi' = p^2$. Allora $\frac{p}{\pi}$ è un intero di norma 1, cioè è un'unità. Dunque π è associato a p; e perciò il numero π non si deve considerare, in questo studio, come distinto da p. Cioè, $\underline{p}$ è un primo razionale, che è primo (di 2° grado) anche in $K(i)$.
Caso 2°. $Nm\,\pi = x^2 + y^2 = p$. In tal caso π si dice numero primo di primo grado; la sua norma è un primo razionale.
Dunque il problema di trovare gli interi primi in $K(i)$ si riduce all'altro:
<u>Quali sono gli interi primi razionali p che sono somma di due quadrati?</u>[19]
Questi primi razionali saranno norma di un primo di primo grado; gli altri saranno // primi anche in $K(i)$ (di secondo grado).
La teoria delle forme da noi svolta ci dice che i primi $\underline{p}$ per cui è risolubile l'equazione Diofantea $p = x^2 + y^2$ sono <u>il numero primo $p = 2$, e i numeri primi dispari che divisi per 4 danno per resto 1</u>.
<u>Dunque questi ultimi numeri non sono primi in $K(i)$, ma sono norma di un primo in $K(i)$; invece i primi razionali $p \equiv 3\ (mod\ 4)$ sono primi anche in $K(i)$</u>.
Vediamo già qui una prima relazione tra la teoria di alcune forme quadratiche, e i nostri studii. Ma si può viceversa, partendo dagli studii attuali, dedurre per nuova via il teorema sulle forme quadratiche, che abbiamo precedentemente invocato.
Intanto che per i numeri $p \equiv 3\ (mod\ 4)$ la $p = x^2 + y^2$ non sia risolubile con interi razionali è ben evidente, perché la somma dei quadrati di due interi x, y è congrua $(mod\ 4)$ ad uno dei numeri $0, 1, 2$ (secondo la parità dei numeri x, y). Basterà provare che un dispari $p \equiv 1\ (mod\ 4)$ è prodotto di due primi di Gauss. Infatti in tal caso -1 è // residuo di $\underline{p}$. Cioè esiste un intero x tale che $x^2 + 1 = (x + i)(x - i)$ è divisibile per p. Ora, se uno dei due numeri $x \pm i$ fosse divisibile per $\underline{p}$, altrettanto avverrebbe anche dell'altro e quindi anche della somma $2x$, e della differenza $2i$ (ciò che è assurdo). Quindi $\underline{p}$ non divide né l'intero di Gauss $x + i$, né l'intero $x - i$, pur dividendo il loro prodotto. Quindi $\underline{p}$ non può essere un <u>primo</u> di Gauss.

c.d.d.

[20]Ma si può dimostrare tale teorema, anche senza ricorrere alla teoria dei residui. È facile estendere agli interi di Gauss la definizione di congruenza, e il teorema che una congruenza di grado $\underline{n}$ rispetto a un modulo primo non ha più di $\underline{n}$ radici. Ora la congruenza

[16] *lapsus* del curatore: leggasi π.
[17] Bianchi 1920-21, Introduzione, §2, p. 14.
[18] *Idem*, Introduzione, §2, p. 15. Qui Bianchi tratta i due casi in modo del tutto analogo a Fubini. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 432, 433.
[19] Gazzaniga 1903, cap. IX, p. 233.
[20] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 434.

$$z^{p-1} \equiv 1 \ (mod\ p)$$

ha se $p \equiv 1 \ (mod\ 4)$ la soluzione $z = i$, oltre le soluzioni $1, 2, 3, \dots, p-1$, che essa possiede per il teorema di Fermat, cioè ha p soluzioni distinte. Dunque p non può essere primo.

c.d.d.

Quanto al numero primo 2, si noti che dalla $2 = 1^2 + 1^2$, si deduce $2 = (1+i)(1-i)$. I due fattori $1+i, 1-i$ sono però associati, perché $\frac{i-1}{i+1} = -\frac{2i}{2} = -i$ è un' // unità; perciò $2 = -i(1+i)^2$. Cioè 2 è associato[21] al quadrato del numero primo $1+i$.
Invece i fattori di un dispari primo $p \equiv 1 \ (mod\ 4)$ non sono mai associati tra loro. In tal caso sarebbe infatti $p = x^2 + y^2 = i^n(x+iy)^2 =$ (n intero razionale)
$= i^n\{(x^2 - y^2) + 2ixy\}$.

Per n pari i^n è reale, e se ne dedurrebbe $xy = 0$, ciò che è assurdo. Per n dispari i^{n+1} è reale, e se ne dedurrebbe $x^2 - y^2 = 0$, cioè $x^2 = y^2$, da cui seguirebbe che p è dispari contro l'ipotesi fatta.
Si dimostra, come nel caso ordinario, che un'espressione

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

dove le α sono interi di Gauss prefissati, le x interi di Gauss variabili, assume tutti e soli i valori interi che sono multipli del M.C.D. m di $\alpha_1, \alpha_2, \dots, \alpha_n$. L'insieme di questi numeri si chiamerà l'ideale[22] $(\alpha_1, \alpha_2, \dots, \alpha_n)$. Se $m = a + ib$, questo ideale è la classe dei numeri

$$(x+iy)(a+ib) = (xa - yb) + i(bx + ay) = x[a+ib] + y[-b+ia]$$

dove x, y sono interi razionali variabili. //
Pertanto $a_1 = a + ib, a_2 = -b + ia$ diconsi costituire una base dell'ideale. Se b_1, b_2 sono due altri numeri tali che al variare degli interi razionali ξ, η i numeri $\xi b_1 + \eta b_2$ descrivano lo stesso ideale, anche b_1, b_2 diconsi una base dell'ideale. Esisteranno degli interi $\xi_1, \xi_2, \eta_1, \eta_2$ razionali tali che

$$(1) \qquad \begin{cases} \xi_1 b_1 + \eta_1 b_2 = a_1 \\ \xi_2 b_1 + \eta_2 b_2 = a_2 \end{cases}$$

cosicché

$$a_1 x + a_2 y = b_1(\xi_1 x + \xi_2 y) + b_2(\eta_1 x + \eta_2 y).$$

Sarà dunque $\xi b_1 + \eta b_2 = x a_1 + y a_2$, se

$$(2) \qquad \begin{cases} \xi = \xi_1 \mathrm{x} + \zeta_2 \mathrm{y} \\ \eta = \eta_1 \mathrm{x} + \eta_2 \mathrm{y} \end{cases} \qquad (\xi_1, \xi_2, \eta_1, \eta_2 \text{ interi razionali}).$$

Poiché a valori interi razionali delle ξ, η corrispondono valori interi razionali delle x, y sarà

$$\xi_1\eta_2 - \eta_1\xi_2 = \pm 1.$$

[21] *Idem*, suppl. XI, §159, p. 433; Dedekind scrive, analogamente a come farà poi Fubini, che "il numero 2 è associato col quadrato del numero primo di primo grado $1 - i$".
[22] Bianchi 1920-21, cap II, §23, p. 146.

Cioè le $(1), (2)$ sono trasformazioni modulari proprie o improprie. Troviamo così un nuovo ufficio delle trasformazioni modulari: quello cioè di trasformare l'una nell'altra le basi di un ideale[23]. //

La norma di un numero[24] $\xi_1 b_1 + \eta b_2$ di un ideale è la forma

$$\xi^2 b_1 b_1' + (b_1 b_2' + b_1' b_2)\xi\eta + \eta^2 b_2 b_2'$$

(dove con b' ho indicato il numero coniugato di b).

Vediamo già in questo caso che a un ideale corrisponde una forma a coefficienti interi razionali (nel caso dell'aritmetica ordinaria si presentava pure un fatto analogo: soltanto che la forma corrispondente ad un ideale era di primo grado). E non sarebbe facile[25] convincersi che alle differenti basi di uno stesso ideale corrispondono forme propriamente o impropriamente equivalenti tra loro.

Presentiamo già da questi pochi cenni quanto possa essere fecondo lo studio delle possibili generalizzazioni dei numeri interi. Per gli interi di Gauss confronta il Trattato di Dirichlet-Dedekind tradotto da A. Faifofer[26] pag. 424-440.

§.2 ***Alcune nuove difficoltà***[27]

Se noi chiamassimo interi algebrici[28] i numeri del tipo $x + y\theta$, dove θ è radice di una delle equazioni $\theta^2 \pm 2 = 0, \theta^2 - 3 = 0, \theta^2 + \theta + 3 = 0,\ ecc.$, noi potremmo ripetere sostanzialmente analoghe considerazioni. // Ma, se noi indicassimo con θ una radice della $\theta^2 + 5 = 0$, vedremmo che non potremmo più dare una definizione della divisione di due interi analoga alla precedente, e non potremmo più estendere l'algoritmo di Euclide[29]. Né la difficoltà si potrebbe superare per altra via; si trova infatti che[30] per $\theta = \sqrt{-5}$, è:

$$6 = 2 \cdot 3 = (1 + \theta)(1 - \theta)$$

dove i numeri $2, 3, 1 + \theta, 1 - \theta$ non sono a due a due associati e non sono ulteriormente decomponibili in fattori.[31]

Altrettanto avviene in altri casi. Osserviamo, anzi, che se noi ci limitassimo a studiare gli interi razionali congrui ad $1\ (mod\ 4)$ e i loro prodotti (ancora congrui ad 1 rispetto al modulo 4), e abbandonassimo gli altri interi, si presenterebbe un fatto analogo. Così, per esempio[32]

---

[23] Nota inserita da Fubini a p.d.p.: *Disp. 13 Teoria dei numeri*.

[24] *e.c.* e *del.*: $\xi b_1 + \eta b_2$.

[25] *e.c.* e *cor. sup.*: difficile.

[26] Aureliano Faifofer, matematico e accademico austriaco, traduttore delle *Vorlesungen* di Dirichlet-Dedekind.

[27] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 440-442.

[28] Bianchi 1920-21, cap. I, §9, p. 55. Cfr. anche Hilbert 1897 (trad. 1911), cap. I, §2, p. 10.

[29] Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 441; Dedekind qui scrive che "il processo di divisione […] non riesce più, e nel tempo stesso qui per la prima volta si presenta il fenomeno singolare, che i numeri, che non possono venir ulteriormente decomposti in fattori di norma minore, pure non possiedono il carattere di veri numeri primi, o piuttosto che spesso uno stesso numero può venire rappresentato in più modi essenzialmente differenti come prodotto di cotali numeri indecomponibili".

[30] *Ibid.* Fubini riprende palesemente l'esempio del corpo $K(\sqrt{-5})$ dal supplemento di Dedekind. Anche in Sommer 1907 (trad. 1911), cap. 2, §7, 1° esempio, p. 29-32, viene affrontato lo studio di tale corpo.

[31] *Ibid.* Fubini riprende palesemente questa decomposizione dal supplemento di Dedekind. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §7, p. 31; qui l'autore fornisce gli esempi delle "doppie" decomposizioni di $6, 9, 21$ in $K(\sqrt{-5})$.

[32] Sommer 1907 (trad. 1911), cap. 2, §8, p. 35.

$$21 \cdot 21 = 9 \cdot 49.$$

I numeri $21, 9, 49$ non sono a due[33] associati, e non sono nelle nostre ipotesi decomponibili. Questo fatto nel caso attuale si presenta perché gli interi $\equiv 1\ (mod\ 4)$ non formano un campo oloide completo; se noi lo completassimo con l'aggiunta degli altri interi razionali, ogni difficoltà svanirebbe. Così il // campo dei numeri $x + y\sqrt{-5}$, dove x, y sono interi razionali, si riguarderà come incompleto. Si cercherà di aggiungergli nuovi enti, così da renderlo completo, vale a dire, così da ristabilire in esso le ordinarie leggi della divisibilità[34]. Ecco il problema che noi risolveremo in forma assai generale seguendo i metodi di Kummer[35], Dedekind, Kronecker[36], Hilbert[37].

§.3 *Alcuni cenni di geometria dei numeri nello spazio a tre dimensioni*

In questo paragrafo diamo alcuni teoremi di geometria dei numeri per spazio a tre dimensioni. Si tratta di generalizzazioni di risultati da noi già conseguiti nel caso del piano. E perciò ci accontenteremo dei soli enunciati senza dimostrazioni; per le quali rinviamo alle citate lezioni del Minkowski.

Assunto un sistema di coordinate cartesiane $x, y, z,$ i punti a coordinate intere si diranno costituire una rete di punti, la quale in fondo costituisce lo spazio della teoria dei numeri. Questa rete R definisce un gruppo G di traslazioni, per cui le

$$0 \leq x < 1; 0 \leq y < 1;\ 0 \leq z < 1$$

// determinano un parallelepipedo fondamentale[38].

Una rete è una classe di punti, che gode delle seguenti proprietà:

α) I suoi punti non giacciono in uno stesso piano.

β) Se O, A, B sono tre dei suoi punti, la traslazione, che porta O in A, porta B in un quarto punto della rete.

γ) In una sfera di raggio finito cade un numero finito di punti della rete.

---

[33] *e.c.* e *cor. sup.*: sono a due a due.

[34] Gazzaniga 1903, cap IX, p. 251-254. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 441; qui Dedekind scrive "sembra impresa del tutto priva di speranza, quella di ricondurre a leggi semplici la composizione e divisibilità dei numeri. Però, come in simile stato delle cose già sovente è accaduto nello sviluppo delle scienze matematiche, anche qui codesta difficoltà apparentemente insuperabile divenne la fonte di una scoperta veramente grande e gravida di conseguenze; infatti Kummer nell'investigare quei campi di numeri, sui quali conduce il problema della divisione del cerchio, trovò che le antiche leggi euclidiane della divisibilità mantengono anche in questi campi il loro pieno valore, purché essi vengano resi compiuti mediante l'introduzione di nuovi numeri, che esso chiamò numeri ideali".

[35] Fubini allude ai corsi di teoria dei numeri che Kummer tenne all'Università di Breslavia (oggi Wroclaw in Polonia) a partire dal 1843 e che ebbero notevole influenza sul collega e suo parente Dirichlet. Fubini probabilmente si riferisce ai lavori di Kummer *Zur Theorie der complexen Zahlen* (Journal für Math., XXXV, 1847) e *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist* (Abh. der K. Akad. der Wiss. zu Berlin, 1856).

[36] Kronecker si laureò nel 1845 discutendo una dissertazione preparata con la supervisione di Dirichlet sulla teoria dei numeri algebrici nella quale probabilmente è contenuto il metodo qui citato da Fubini, poi inserito nell'opera *Grundzilge einer arithmetischen Theorie der algebraischen Grössen* (Journal für Math., XCXII, 1882).

[37] Fubini probabilmente allude alla traduzione francese (*Théorie des corps de nombres algébriques*, 1911) dell'opera di Hilbert nota come *Zahlbericht* (1897) che egli aveva sicuramente a disposizione quando 'costruì' il suo corso di teoria dei numeri, in quanto rientrava nel posseduto della BSM.

[38] Bianchi 1911-12, cap. XIII, §133, p. 612-613. Cfr. anche Minkowski 1910, §27, p. 63-69 e Minkowski 1957, p. 67-75.

Data una tale classe di punti, essa si può in infiniti modi pensare come luogo dei punti a coordinate cartesiane x, y, z intere, e[39] infiniti modi si può definire un corrispondente parallelepipedo fondamentale.
Da un tale sistema di coordinate x, y, z si deducono infiniti sistemi analoghi per mezzo delle trasformazioni lineari intere omogenee a coefficienti interi e determinante ± 1 applicate alle x, y, z (trasformazioni modulari nello spazio).
Se una rete R è contenuta in una rete r, si può trovare un tale sistema di coordinate cartesiane ξ, η, ζ che valgano equazioni del tipo se//guente[40]:

$$\begin{aligned} \xi &= l_1 X + l_2 Y + l_3 Z \\ \eta &= \quad m_2 Y + m_3 Z \\ \zeta &= \quad\quad n_3 Z \end{aligned}$$

(l, m, n interi; $0 < l_1; 0 \leq l_2 < m_2; 0 \leq m_3 < n_3$) in guisa che i punti di R siano i punti per cui X, Y, Z sono interi e i punti di r i punti per cui sono intere le ξ, η, ζ.
I parallelepipedi fondamentali della rete dei punti a coordinate x, y, z intere sono tutti equivalenti; se noi li assumiamo come unità di volume si dimostra:
Un corpo φ non concavo col centro in un punto O della rete, che contenga all'interno il solo punto O della rete, ha un volume ≤ 8; e, se φ avesse proprio per volume 8, allora esso contiene certamente sul contorno qualche punto della rete.
In quest'ultimo caso il corpo F dedotto da φ con l'omotetia di centro O e rapporto $\frac{1}{2}$ ricopre, insieme ai campi equivalenti (cioè ai campi che se ne deducono con le traslazioni di G) tutto lo spazio senza lacune[41].
Il contorno di F è diviso in parti (che chiameremo // facce) piane, ciascuna delle quali è comune al contorno di F e di un campo F' ad esso equivalente, ed ha per centro un punto $\frac{p}{2}, \frac{q}{2}, \frac{r}{2}$, se p, q, r sono le coordinate (intere) del centro di F'.
Dunque nel caso qui studiato anche φ sarà un poliedro, che si dimostra avere al massimo $2(2^3 - 1) = 14$ facce e contenere sul contorno al più $(3^3 - 1) = 26$ punti della rete.
Se ne deduce:
Se ξ, η, ζ sono polinomi reali omogenei di 1° grado nelle x, y, z con determinante Δ, allora esistono valori non tutti nulli delle x, y, z che soddisfano alle disuguaglianze[42]:

$$|\xi| \leq \sqrt[3]{\Delta};\ |\eta| \leq \sqrt[3]{\Delta};\ |\zeta| \leq \sqrt[3]{\Delta}.$$

E, in generale si potrà ottenere che in queste disuguaglianze valga contemporaneamente il segno di $<$; nei casi eccezionali in cui almeno in una deve valere il segno di $=$, le ξ, η, ζ, con un cambiamento di coordinate x, y, z si possono ridurre alla forma

$$\xi = a_1 x + a_2 y + a_3 z;\ \eta = b_2 y + b_3 z;\ \zeta = c_3 z.$$

Si dimostra pure che con valori interi non tutti nulli delle x, y, z si può soddisfare alla //

$$|\xi| + |\eta| + |\zeta| < \sqrt[3]{6|\Delta|},$$

[39] *e.c.* e *cor. sup.*: e in infiniti.
[40] Minkowski 1957, p. 176. Fubini adotta qui la stessa notazione del matematico tedesco, con l'unica eccezione dell'utilizzo di ξ, η, ζ al posto di x, y, z sopralineati.
[41] Bianchi 1920-21, Nota III, *Cenni sul significato geometrico dei teoremi di Minkowski*, p. 436-438.
[42] Minkowski 1957, §6, p. 9. Il matematico tedesco perviene a queste disuguaglianze all'interno del paragrafo *Satz über drei ternäre lineare Formen*.

cosicché

$$|\xi\eta\zeta| \leq \left(\frac{|\xi| + |\eta| + |\zeta|}{3}\right)^3 < \frac{2}{9}|\Delta|.$$

Anzi, se noi volessimo proprio trovare il minimo valore assunto da $|\xi| + |\eta| + |\zeta|$ per valori interi non tutti nulli delle $x, y, z,$ troviamo che possiamo addirittura scrivere[43]

$$|\xi| + |\eta| + |\zeta| \leq \sqrt{6 \cdot \frac{18}{19}|\Delta|}\,.$$

Se fosse[44]

$$\xi = \frac{\varphi + i\psi}{\sqrt{2}}, \qquad \eta = \frac{\varphi - i\psi}{\sqrt{2}}$$

Dove φ, ψ, ζ sono polinomi a coefficienti reali, si troverebbe che si possono trovare valori interi di x, y, z non tutti nulli così che:

$$|\xi| < \sqrt[3]{2\,\frac{|\Delta|}{\pi}}, \qquad |\eta| < \sqrt[3]{2\,\frac{|\Delta|}{\pi}}, \qquad |\zeta| < \sqrt[3]{2\,\frac{|\Delta|}{\pi}}$$

oppure che

$$|\xi\eta\zeta| < \frac{8|\Delta|}{9\pi}.$$

§.4 ***Campi algebrici***

Definizioni preliminari. Chiameremo corpo[45] di numeri ogni classe K di numeri che gode della seguente proprietà: la somma, la differenza, il prodotto, il quoziente di due numeri distinti o coincidenti di K è ancora un numero di K. È sottin//teso che in K esista almeno un numero α differente da zero. In ogni K esisteranno pertanto il numero [46] $\frac{\alpha}{\alpha} = 1,$ e quindi anche i numeri $1, 1+1, 1+1+1, ecc.$; cioè in K esisterà ogni intero positivo $n;$ esisterà in K pertanto ogni razionale $\frac{n}{m},$ quoziente di due tali interi, ed anche ogni razionale negativo, che si può sempre ottenere come differenza di due razionali positivi.
La classe R di tutti i razionali (che è anche essa un corpo) è pertanto contenuta in ogni corpo K.
Dati più numeri $\alpha_1, \alpha_2, \ldots, \alpha_n$ essi determinano un corpo $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ formato dai numeri che si ottengono dagli α_i con somme, sottrazioni, prodotti, quozienti.[47]
In altre parole $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è formato da tutti i numeri che si possono scrivere come quozienti di due polinomi nelle $\alpha_1, \alpha_2, \ldots, \alpha_n$ a coefficienti razionali.
Un tale corpo si dice algebrico, se ciascuno dei numeri α_i è radice di una equazione algebrica a coefficienti razionali. L'algebra dimostra che non si diminuisce per nulla la generalità, //

[43] *e.c.* e *cor. sup.*: invece di $\sqrt{\ }$ leggasi $\sqrt[3]{\ }$.
[44] Minkowski 1957, p. 128, formula (11). Fubini trae palesemente da questo paragrafo (p. 127-130) la notazione adottata nel resto del capitolo.
[45] Bianchi 1920-21, cap. I, §11, p. 65, 66. Cfr. anche Hilbert 1897 (trad. 1911), cap. I, §1, p. 9.
[46] *Idem*, cap. I, §11, p. 66.
[47] Dirichlet 1877 (trad. 1881), suppl. XI, §162, p. 453, 454.

supponendo $n = 1$, cioè considerando i campi algebrici $K(\theta)$, individuati da un solo numero θ soddisfacente a un'equazione algebrica[48]

$$\varphi(\theta) = \theta^m + a_1\theta^{m-1} + a_2\theta^{m-2} + \cdots + a_{m-1}\theta + a_m = 0 \qquad (1)$$

a coefficienti $a_1, a_2, \ldots, a_m$ razionali.
Notiamo che il numero θ può soddisfare a parecchie equazioni di tale tipo.
Supporremo che la (1) sia tra esse quella di minimo grado m. Di equazioni (1) di minimo grado m non ve ne possono essere 2; perché altrimenti θ, soddisfacendo ad entrambe, annullerebbe la loro differenza, che è un'equazione di grado inferiore.
La (1) è irriducibile[49]; perché se il primo membro $\varphi(\theta)$ fosse prodotto di due polinomi $\psi(\theta), \lambda(\theta)$ a coefficienti razionali di grado minore di m, allora θ, annullando il prodotto, annullerebbe uno dei due fattori $\psi(\theta), \lambda(\theta)$; e perciò esso sarebbe radice di almeno una equazione $\psi(\theta) = 0, \lambda(\theta) = 0$ di grado minore di m.
Se $m = 1$, allora θ è razionale; e $K(\theta) = R$.
Noi escluderemo questo caso elementare. //
L'algebra dimostra: Se un polinomio $f(\theta)$ è nullo anche per una sola radice θ di un'equazione irriducibile $\varphi(\theta) = 0$ e se f ha come φ, i coefficienti razionali, allora $f(\theta)$ è divisibile per $\varphi(\theta)$, ed è perciò nullo anche per tutte le altre radici di $\varphi(\theta) = 0$.
Perciò le altre equazioni $f(\theta) = 0$ a coefficienti razionali, a cui soddisfa θ si ottengono tutte, moltiplicando la (1) per un polinomio in θ a coefficienti razionali.
Ogni numero α di $K(\theta)$ è il quoziente dei due polinomi in θ a coefficienti razionali

$$\alpha = \frac{b_0 + b_1\theta + b_2\theta^2 + \cdots + b_r\theta^r}{c_0 + c_1\theta + c_2\theta^2 + \cdots + c_s\theta^s} = \frac{P(\theta)}{Q(\theta)}$$

il cui denominatore $Q(\theta) \neq 0$.
Ora $Q(\theta)$ essendo $\neq 0$ per almeno una radice θ dell'equazione irriducibile $\varphi(\theta) = 0$, esso sarà differente da zero anche per tutte le altre radici di $\varphi(\theta) = 0$. Cioè $Q(\theta)$ e $\varphi(\theta)$ saranno primi tra loro; e pertanto potremo trovare due altri polinomi $S(\theta), T(\theta)$ a coefficienti razionali in guisa che sia identicamente in θ

$$Q(\theta)S(\theta) + \varphi(\theta)T(\theta) = 1.$$

// Posto in questa identità θ uguale alla radice considerata della $\varphi(\theta) = 0$, se ne deduce che per tale valore di θ è

$$S(\theta) = \frac{1}{Q(\theta)}$$

Cosicché $\alpha = P(\theta)S(\theta)$; cioè ogni numero α di $K(\theta)$ è eguale ad un polinomio in θ a coefficienti razionali.
Ma la (1) [la $\varphi(\theta) = 0$], e le equazioni che se ne deducono moltiplicando per $\theta, \theta^2, \theta^3, \ldots$ dimostrano facilmente che le $\theta^m, \theta^{m+1}, \theta^{m+2}, \ldots$ si possono esprimere come polinomi di grado $m - 1$ e a coefficienti razionali nella θ. Potremo pertanto nel prodotto $P(\theta)S(\theta)$ eliminare le potenze di θ con esponente maggiore di $m - 1$ (*). E ne dedurremo:

[48] *Idem*, suppl. XI, §162, p. 453.
[49] *Idem*, suppl. XI, §162, p. 454; Dedekind qui fornisce anche la definizione di "sistema irreducibile" di n numeri.

Ogni numero α di $K(\theta)$ è uguale ad un polinomio[50]

$$\alpha = p_0 + p_1\theta + p_2\theta^2 + \cdots + p_{m-1}\theta^{m-1} \tag{2}$$

di grado $m-1$ a coefficienti razionali nella θ. //
Dato α, questo polinomio è completamente determinato[51]; se infatti due di questi polinomi rappresentassero lo stesso numero α, la loro differenza (che è un polinomio di grado minore di m) sarebbe nulla; e pertanto θ soddisferebbe, contro l'ipotesi, a un'equazione di grado minore di m a coefficienti razionali.
Studiare i numeri α di $K(\theta)$ equivale a studiare i polinomi (2).
A questa osservazione possiamo dare forma più generale così. Noi ci siamo ridotti ai polinomi (2) di grado $m-1$, perché un polinomio qualsiasi $f(\theta)$ di grado qualsiasi si può scrivere nella forma:

$$f(\theta) = \varphi(\theta)q(\theta) + r(\theta)$$

dove q ed r sono quoziente e resto ottenuti dividendo $f(\theta)$ per $\varphi(\theta)$. Ed $r(\theta)$ è un polinomio di grado $\leq m-1$.
Ora per il numero θ da noi considerato è $\varphi(\theta) = 0$; e perciò, anziché considerare il polinomio $f(\theta)$ ci siamo limitati a considerare i polinomi $r(\theta)$; nel nostro studio i polinomi $f(\theta)$ ed $r(\theta)$ sono equivalenti. Due polinomi sono dun//que nel nostro studio equivalenti, cioè definiscono lo stesso numero in $K(\theta)$, quando, divisi per $\varphi(\theta)$, danno resti uguali, in altre parole quando essi sono congrui tra loro $(mod\ \varphi(\theta))$.
Lo studio del campo algebrico $K(\theta)$ equivale pertanto allo studio dei polinomii a coefficienti razionali, quando si considerino come equivalenti (uguali) due polinomi congrui rispetto al polinomio irriducibile a coefficienti razionali $\varphi(\theta)$. (Kronecker[52]).
Il nostro studio è dunque la generalizzazione all'algebra dei polinomi dell'aritmetica delle congruenze rispetto ad un modulo primo.
I numeri $\alpha_1, \alpha_2, \ldots, \alpha_{m-1}$, che si ottengono da (2) sostituendo a θ le altre $m-1$ radici di (1), diconsi i numeri coniugati[53] di α. Il loro prodotto dicesi $Nm\,\alpha$ (norma[54] di α); la loro somma dicesi traccia[55] di α. Entrambe sono polinomi simmetrici nelle radici di (1) a coefficienti razionali, essi sono pertanto numeri razionali.
Se, comunque, è scelto α in $K(\theta)$, i numeri coniu//gati appartengono a $K(\theta)$, il corpo dicesi normale o di Galois[56].

---

[50] Bianchi, 1920-21, cap. I, §11, p. 69. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §162, p. 458.
[51] *Idem*,cap. I, §11, p. 70, 71. Qui Bianchi ripercorre esattamente lo stesso ragionamento di Fubini.
[52] Cfr. Kronecker 1882, cap. II, §19; dopo aver introdotto l'equivalenza tra forme e ideali, all'interno del paragrafo intitolato *Die ganzen algebraischen Zahlen und ihre Divisoren. Das Kummer'schen Princip der Aequivalentz*, il matematico tedesco scrive: "Diese methode beruht einzig und allein auf der kenntnis der anzahl der elemente eines vollstandigen restsystems fuor einen complexen modul, ob dieser nun eine wirkliche gebrochene complexe zahl, ob er ein modulsymbol und zwar nach der Kummer'schen theorie eine 'ideale Zahl' oder nach der Dedekind'schen eine 'ideal' sei".
[53] Dirichlet 1877 (trad. 1881), suppl. XI, §163, p. 461; Dedekind fornisce qui anche la definizione di numeri coniugati come conseguenza di quella di "corpi coniugati". Cfr. anche Hilbert 1897 (trad. 1911), cap. I, §1, p. 10.
[54] Bianchi 1920-21, cap. I, §12, p. 74. Bianchi dà qui la stessa definizione di norma. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §164, p. 464. Cfr. infine Hilbert 1897 (trad. 1911), cap. I, §3, p. 13.
[55] *Idem*, cap. I, §12, p. 74. Bianchi dà la stessa definizione di traccia.
[56] Dirichlet 1877 (trad. 1881), suppl. XI, §163, p. 463, 464. Dedekind qui introduce questa definizione in modo leggermente diverso da Fubini: scrive infatti che "se gli n corpi $\Omega^{(r)}$ coniugati con Ω sono tutti identici fra loro, epperò con Ω, diremo Ω un corpo normale od anche un corpo di Galois, perché l'essenza dei principi algebrici introdotti da Galois consiste nel ricondurre la ricerca di qualsivoglia corpo finito a quella di un corpo normale".

Poiché θ è pure un numero di $K(\theta)$, e i numeri coniugati di θ sono le altre radici di (1), bisogna a tal fine che $K(\theta)$ contenga anche tutte queste altre $m-1$ radici, cioè che queste radici sieno uguali a polinomii nella θ a coefficienti razionali. E questa condizione è anche sufficiente. In tal caso $K(\theta)$, contenendo tutte le radici di (1), conterrà tutti i numeri che se ne ottengono con addizioni e moltiplicazione, cioè conterrà sia i polinomi (2), sia quelli che se ne deducono sostituendo a θ le altre radici di (1).
Ogni numero α di $K(\theta)$ soddisfa almeno ad un'equazione a coefficienti razionali $g(\alpha)=0$: p. esempio a quella che si ottiene eliminando θ tra le (1) e (2). Sarà[57]:

$$g(p_0+p_1\theta+\cdots+p_{m-1}0^{m-1})=0.$$

Questa equazione nella θ, avendo una radice comune con l'equazione irriducibile (1), sarà soddisfatta anche da tutte le altre radici di (1). Ma, sostituendo a θ queste altre radici // il polinomio $p_0+p_1\theta+\cdots+p_{m-1}\theta^{m-1}$ diventa uguale ai numeri coniugati di α. E perciò $g(\alpha)=0$ avrà per radici anche i numeri coniugati di α.
Il numero α e i coniugati siano a due a due differenti tra di loro. Dato α, le (1), (2), saranno due equazioni in θ con una sola radice comune; perché, se esse avessero due radici θ, θ_i comuni, il numero α sarebbe uguale al coniugato α_i; che si deduce da α, scrivendo appunto θ_i al posto di θ nella (2).
Come insegna l'algebra, l'unica radice θ comune alle (1) e (2) se ne deduce con procedimenti razionali, cioè con sole somme, sottrazioni, prodotti, quozienti. Perciò θ si dedurrà da α con tali operazioni; così come α si deduce da θ con operazioni dello stesso tipo, cioè, se un numero α è differente dai coniugati, esso definisce un campo $K(\alpha)$, che coincide con $K(\theta)$.
L'equazione irriducibile a cui soddisfa α è la trasformata della (1) corrispondentemente alla (2), ed è pure di grado m. //
Se immaginiamo il nostro corpo definito da α anziché da θ, se β è un numero del corpo, e se β_i è un numero coniugato di β secondo la definizione da noi data, è facile riconoscere che β_i si conserva ancora coniugato di β, quando si pensi il corpo definito da α.
Notiamo che anche θ è un numero differente dai coniugati; perché, se così non fosse, la (1) ammetterebbe radici multiple, e sarebbe pertanto riducibile.

(*) **Nota**: In altre parole si può dire così: Dividendo $P(\theta)S(\theta)$ per $\varphi(\theta)$ si ha un quoziente $Q(\theta)$ e un resto $R(\theta)$ di grado minore di m; perciò vale l'identità in θ

$$P(\theta)S(\theta)=Q(\theta)\varphi(\theta)+R(\theta).$$

Sostituendo a θ la radice considerata di $\varphi(\theta)=0$, il secondo membro si riduce al polinomio $R(\theta)$, che al massimo è di grado $m-1$, e che ha i coefficienti razionali.

[57] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale: invece di $p_{m-1}0^{m-1}$ leggasi $p_{m-1}\theta^{m-1}$.

§.5 ***Numeri interi algebrici***

Chiamiamo intero algebrico[58] un numero x, che soddisfi un'equazione algebrica

$$x^m + a_1 x^{m-1} + \cdots + a_m = 0 \qquad (1)$$

a coefficienti $a_1, a_2, \ldots, a_m$ interi razionali, e col primo coefficiente uguale ad 1.
Che questa definizione sia una generalizzazione del concetto abituale di numero intero, e che non sia mai in contraddizione con questo, si riconosce da ciò, che, se un intero algebrico è razionale, allora esso è un intero ordinario. Infatti, l'algebra dimostra che le radici[59] // razionali di (1) sono numeri interi. Gli interi ordinari si diranno interi razionali.
I numeri radici di (1), i cui coefficienti fossero razionali, anche non interi, diconsi algebrici[60], come è noto.
Teor.[ema] Ogni numero algebrico x moltiplicato per un conveniente intero razionale K, diventa un intero algebrico[61] y.
Infatti, se $y = Kx$, se x soddisfa alla (1) con coefficienti razionali, la y soddisfa alla[62]

$$y^m + a_1 K x^{m-1} + a_2 K^2 x^{m-2} + \cdots + a_{m-1} K^{m-1} x + a_m K^m = 0.$$

Se per esempio K è il minimo comune multiplo dei denominatori di $a_1, a_2, \ldots, a_m$, questa equazione, il cui primo coefficiente vale 1, ha per coefficienti interi razionali; e quindi y è un intero algebrico.
Sarà utile esercizio al lettore dimostrare che:
Somma, prodotto, differenza[63] di due o più interi algebrici sono pure interi algebrici[64]. Ogni numero[65] sia radice di un'equazione algebrica, il cui primo coefficiente è 1, e gli altri coefficienti sono interi algebrici, è ancora un intero algebrico[66]. //
Se x è un intero algebrico, anche $\sqrt[n]{x}$ un intero algebrico[67], sarà $x = \left[\sqrt[n]{x}\right]^n$, qualunque sia l'intero razionale positivo n. Perciò ogni intero algebrico si può decomporre nel prodotto di quanti si vogliano interi algebrici. Cessa perciò ogni possibilità di estendere l'ordinaria teoria dei numeri primi alla classe formata da tutti i numeri algebrici.
Noi perciò ci limiteremo a considerare gli interi algebrici contenuti in un dato corpo algebrico $K(\theta)$. Evidentemente, se un numero di $K(\theta)$ è intero, anche i coniugati sono interi[68]. Noi, potremo, moltiplicando, casomai, θ per un conveniente intero razionale K, supporre θ intero. Per fissar le idee supporremo che il minimo grado di un'equazione algebrica a coefficienti

[58] Bianchi 1920-21, cap. I, §9, p. 55. Qui Bianchi dà la stessa definizione di intero algebrico. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §160, p. 442. Cfr. infine Hilbert 1897 (trad. 1911), cap. I, §2, p. 11.
[59] Nota inserita da Fubini a p.d.p.: *Disp. 14 Teoria dei numeri*.
[60] Dirichlet 1877 (trad. 1881), suppl. XI, §160, p. 442. Fubini probabilmente riprende da Dedekind la distinzione tra numeri algebrici e numeri interi algebrici. La stessa distinzione si trova inoltre all'interno dello *Zahlbericht* di Hilbert.
[61] Bianchi 1920-21, cap. I, §9, p. 57, teorema b). Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §166, p. 482.
[62] *e.c.* e *cor. inf.*: invece di x leggasi y.
[63] Hilbert 1897 (trad. 1911), cap. I, §3, p. 12.
[64] Bianchi 1920-21, cap. I, §9, p. 59, teorema d). Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §160, p. 443, 444, prop. 1; qui Dedekind dimostra nel dettaglio tale proprietà.
[65] *e.c.* e *cor. sup.*: numero che sia.
[66] Bianchi 1920-21, cap. I, §10, p. 61, teorema α). Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §160, p. 445, 446, prop. 2; qui Dedekind dimostra nel dettaglio tale proprietà.
[67] Dirichlet 1877 (trad. 1881), suppl. XI, §160, p. 443-446; Dedekind enuncia tale risultato nella seguente forma generale: "se α è un numero intero, ed r, s sono numeri interi positivi razionali, anche $\sqrt[r]{\alpha^s}$ è un numero intero".
[68] Bianchi 1920-21, cap. I, §9, p. 57, teorema a).

razionali, a cui soddisfi θ, sia il terzo. I nostri risultati valgono però in generale. Allora ogni numero di $K(\theta)$ si può scrivere nella forma

$$x + y\theta + z\theta^2$$
$$(x, y, z \text{ razionali}).$$

Vale a dire i numeri di $K(\theta)$ si possono rappresentare coi punti di uno spazio S a tre dimensioni // dove x, y, z sono coordinate cartesiane.
Ai numeri interi algebrici di $K(\theta)$ corrispondono in S dei punti formanti una classe di punti, che dimostreremo essere una rete ρ.
Infatti, poiché la somma o la differenza di due o più interi di K è ancora un intero di K, è ben evidente che ρ gode della proprietà: Se $A_1\ (x_1, y_1, z_1), A_2\ (x_2, y_2, z_2)$ ed $A_3\ (x_3, y_3, z_3)$ sono tre punti di ρ, anche il punto di coordinate $x_3 + (x_2 - x_1), y_3 + (y_2 - y_1), z_3 + (z_2 - z_1)$, che si deduce applicando ad A_3 la traslazione A_1A_2, è un punto di ρ.
D'altra parte i punti di ρ non giacciono in uno stesso piano, perché a ρ appartengono i 4 punti non complanari $(0,0,0), (1,0,0), (0,1,0), (0,0,1)$.
In una regione finita di S cadono al più punti di ρ in numero finito, come dimostreremo subito. Queste tre proprietà sono le proprietà caratteristiche di una rete di punti nello spazio. E pertanto ρ è una rete; cioè esistono, oltre all'origine, altri tre punti B_1, B_2, B_3 che bastano ad individuarla.
Detti $\omega_1, \omega_2, \omega_3$ i tre punti corrispondenti, ogni altro intero λ di $K(\theta)$ è rappresentato dun//que dalla

$$x_1\omega_1 + x_2\omega_2 + x_3\omega_3 = \lambda \qquad (2)$$
$$(x_1, x_2, x_3 \text{ interi razionali}).$$

Per dimostrare la proposizione ammessa poche righe più sopra, basta evidentemente provare che:
Se H è un'arbitraria costante positiva, esiste in $K(\theta)$ al più un numero finito di interi α_1 tali che α_1 ed i coniugati non superino mai H in modulo.
Se α_2, α_3 sono i coniugati di α_1 allora

$$|\alpha_1 + \alpha_2 + \alpha_3| \leq 3H, \qquad |\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1| \leq 3H^2, \qquad |\alpha_1\alpha_2\alpha_3| \leq H^3$$

cioè $\alpha_1, \alpha_2, \alpha_3$ sono le radici di un'equazione

$$\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0 \qquad (3)$$

i cui coefficienti c_i sono limitati in valore assoluto.
Ma le c_i, funzioni simmetriche intere a coefficienti razionali delle α, sono numeri razionali; anzi sono interi, perché le α sono interi. Ma numeri interi razionali limitati in valore assoluto possono al più avere un numero finito di valori. Di equazioni (3) ve ne è un numero finito; vi è pertanto un numero finito di interi // α_1.

c.d.d.

Con ragionamenti identici a quelli fatti per le c_i si prova che:
Norma e traccia di ogni intero (2) di $K(\theta)$ sono interi razionali[69].

[69] *Idem*, cap. I, §12, p. 75. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §164, p. 467, 468; qui Dedekind enuncia e prova tale proprietà solo per il discriminante. Cfr. infine Hilbert 1897 (trad. 1911), cap. I., §3, p. 12.

Se $\lambda_1, \lambda_2, \lambda_3$ sono 3 interi di $K(\theta)$ e λ_i', λ_i'' ne sono i coniugati, in modo simile si prova che il quadrato D di[70]

$$\Delta = \begin{bmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_1' & \lambda_2' & \lambda_3' \\ \lambda_1'' & \lambda_2'' & \lambda_3'' \end{bmatrix} \qquad (D = \Delta^2)$$

è un intero razionale, che noi chiameremo il discriminante[71] $D(\lambda_1\lambda_2\lambda_3)$ dei numeri λ_i.
Se $\lambda_1 = 1 = \lambda^0;\ \lambda_2 = \lambda,\ \lambda_3 = \lambda^2,$ noi lo chiameremo il discriminante $D(\lambda)$ di λ.
Così $D(\theta)$ è il discriminante dell'equazione che definisce θ.
Se i numeri $\lambda_1, \lambda_2, \lambda_3$ sono a due a due distinti, il loro discriminante è diverso da zero. I numeri $\omega_1, \omega_2, \omega_3$ che compaiono in (2) diconsi una base[72] del corpo; come ci è noto dai nostri studi generali sulle reti di punti, la base è determinata a meno di una trasformazione // modulare (lineare intera omogenea a coefficienti interi razionali a determinante ± 1).
Applicando una tale trasformazione modulare alle $\omega_1, \omega_2, \omega_3,$ si ricava una nuova base $\delta_1, \delta_2, \delta_3,$ il cui discriminante è uguale a $D(\omega_1\omega_2\omega_3)$ moltiplicato per il quadrato del determinante ± 1 della trasformazione modulare considerata, cioè è uguale a $D(\omega_1\omega_2\omega_3)$. Questo numero non dipende perciò dalla base considerata, e si chiama il discriminante D del corpo. Se

$$\begin{aligned} \lambda_1 &= x_{11}\omega_1 + x_{12}\omega_2 + x_{13}\omega_3 \\ \lambda_2 &= x_{21}\omega_1 + x_{22}\omega_2 + x_{23}\omega_3 \\ \lambda_3 &= x_{31}\omega_1 + x_{32}\omega_2 + x_{33}\omega_3 \end{aligned} \qquad (x_{ik} \text{ interi razionali})$$

sono tre interi del corpo, allora

$$D(\lambda_1\lambda_2\lambda_3) = D\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix}^2.$$

Dunque D è il minimo valore non nullo che possa avere il discriminante di tre numeri del corpo.
Anzi D divide il discriminante $D(\lambda_1\lambda_2\lambda_3)$ di tre numeri qualsiasi del corpo, ed il quoziente //

$$\frac{D(\lambda_1\lambda_2\lambda_3)}{D}$$

è un quadrato perfetto.
Poniamo in particolare $\lambda_1 = 1, \lambda_2 = \theta, \lambda_3 = \theta^2$. Avremo che D è un divisore di $D(\theta)$ e che, se

$$\theta^i = x_{i1}\omega_1 + x_{i2}\omega_2 + x_{i3}\omega_3 \quad (i = 0,1,2), \tag{4}$$

allora $\frac{D(\theta)}{D}$ è uguale al quadrato X^2 del determinante X delle x. Dalle (4) abbiamo che le ω si possono scrivere nella forma:

[70] *e.c.* e *cor. sup.*: invece di $|\lambda_1\ \lambda_2\ \lambda_3|$ leggasi $|\lambda_1\ \lambda_2\ \lambda_3|^2$.
[71] Bianchi 1920-21, cap. I, §12, p. 75. Bianchi dà però la definizione più generale di discriminante nel caso n-dimensionale.
[72] Dirichlet 1877 (trad. 1881), suppl. XI, §162, p. 458; §165, p. 468, 469. Fubini introduce il concetto di base del corpo mediante la teoria delle reti di punti e delle trasformazioni modulari; Dedekind invece lo fa, in modo equivalente, all'interno della teoria dei moduli.

$$\omega_i = \frac{y_{i1}+y_{i2}\theta+y_{i3}\theta^2}{X} \ (y_{ik} \text{ interi razionali}).$$

Dunque per (2), ogni intero del corpo si può scrivere nella forma:

$$\lambda = \frac{a+b\theta+c\theta^2}{X} \ (a, b, c \text{ interi razionali})$$

Ove X è un intero razionale, il cui quadrato X^2 divide $D(\theta)$ [così che $\frac{D(\theta)}{X^2}$ è uguale al discriminante del corpo].
Indicheremo costantemente con ω_i' ed ω_i'' i numeri coniugati di ω_i. Poniamo[73]:

$$\xi = x_1\omega_1 + x_2\omega_2 + x_3\omega_3$$
$$\eta = x_1\omega_1' + x_2\omega_2' + x_3\omega_3'$$
$$\zeta = x_1\omega_1'' + x_2\omega_2'' + x_3\omega_3''.$$

Le ξ, η, ζ sono tre forme lineari nelle x, con determinante $\sqrt{D}$. //
Supposto θ reale coi coniugati queste forme sono a coefficienti reali; e dai teoremi di Minkowski segue che si possono scegliere per le x valori interi razionali non tutti nulli, tali che[74]:

$$|\xi| < \left|\sqrt[6]{D}\right|; \quad |\eta| < \left|\sqrt[6]{D}\right|; \quad |\zeta| < \left|\sqrt[6]{D}\right|$$

cosicché[75]

$$|\xi\eta\zeta| < \sqrt{|D|}.$$

Ma $\xi\eta\zeta$ è norma dell'intero algebrico non nullo ξ; perciò $|\xi\eta\zeta| \geq 1$; donde $|D| > 1$. Un metodo analogo si applica negli altri casi. E si ha:
Un corpo algebrico distinto da R ha sempre un discriminante maggiore di 1 in valore assoluto.
Teor.[ema] Esiste un numero finito di corpi algebrici di grado n e discriminante D assegnati.
Supponiamo, per esempio, $n = 3$, e cerchiamo quelli dei nostri corpi che sono reali insieme ai coniugati. In modo simile si tratta il caso generale.
Dai teoremi di Minkowski segue che si può trovare un intero ξ in guisa che esso ed i coniugati η, ζ, soddisfino alle: $|\xi| < 1, |\eta| < 1, |\zeta| \leq \sqrt{D}$. //
Poiché $|Nm\,\xi| \geq 1$, sarà $|\xi\eta\zeta| \geq 1$; e perciò $|\zeta| > 1$, cioè $\zeta \neq \xi, \zeta \neq \eta$.
Ora, se $\xi = \eta$, l'equazione di terzo grado a cui soddisfa la ξ avrebbe almeno una radice doppia; e perciò ξ sarebbe razionale. Cioè ξ coinciderebbe coi coniugati, mentre invece $\zeta \neq \xi$.
Dunque ξ, η, ζ sono differenti tra loro e perciò ξ definisce il corpo algebrico, a cui appartiene. Ma le radici ξ, η, ζ dell'equazione, a cui soddisfa ξ, sono limitate in valore assoluto, come dicemmo più sopra. I coefficienti di tale equazione sono perciò anch'essi limitati in valore assoluto. Ma, poiché essi sono interi razionali, di tali equazioni non ve ne potrà essere che un numero finito.
I ragionamenti qui fatti sono analoghi per dimostrare che:
Gli interi α di un corpo $K(\theta)$ minori insieme ai coniugati di una stessa costante H in valore assoluto, sono in numero finito. //

[73] Minkowski 1957, p. 128, formula (8).
[74] *Ibid.*, formula (9).
[75] *Ibid.*, formula (10).

Per più ampi sviluppi cfr. le citate lezioni di Dirichlet-Dedekind, e le Dioplantische[76] approximationen del Minkowski.

§.6 ***Unità di un corpo algebrico***[77]

Premettiamo un'osservazione:

La $Nm\,\alpha$, se α è un intero di un corpo $K(\theta)$, è un intero razionale[78]. La $\frac{Nm\,\alpha}{\alpha}$ è perciò numero del corpo $K(\theta)$, che è anch'esso intero, perché è uguale al prodotto dei numeri coniugati di α.

Diremo che un intero α di $K(\theta)$ è un'<u>unità</u>[79], se anche $\frac{1}{\alpha}$ è intero. In tal caso $Nm\,\alpha$ e $\frac{1}{Nm\,\alpha}$ sono interi razionali reciproci. E pertanto dovrà essere $Nm\,\alpha = \pm 1$. Viceversa, se $Nm\,\alpha = \pm 1$, per l'osservazione precedente $\frac{1}{\alpha} = \pm\frac{Nm\,\alpha}{\alpha}$ sarà pure intero[80]. Dunque l'intero α è un'unità se $\frac{1}{\alpha}$ è intero, ossia se $Nm\,\alpha = \pm 1$.

Supposto al solito $K(\theta)$ di 3° grado, reale coi coniugati, sia α un'unità, di cui α', α'' sono le unità coniugate. Sarà $Nm\,\alpha = \alpha\alpha'\alpha'' = \pm 1$.

Studiamo dapprima il caso che $|\alpha| = |\alpha'| = |\alpha''| = 1$. // Detta $\omega_1, \omega_2, \omega_3$ una base di $K(\theta)$, detti ω_i' ed ω_i'' i coniugati di ω_i, sarà, essendo α intero

$$\left.\begin{aligned} \alpha &= x_1\omega_1 + x_2\omega_2 + x_3\omega_3 \\ \alpha' &= x_1\omega_1' + x_2\omega_2' + x_3\omega_3' \\ \alpha'' &= x_1\omega_1'' + x_2\omega_2'' + x_3\omega_3'' \end{aligned}\right\} \quad (x_1, x_2, x_3 \text{ interi razionali})$$

Le x non possono essere tutte e tre pari. Altrimenti $\frac{\alpha}{2}$ sarebbe intero, mentre la sua norma[81] $\frac{\alpha'}{2}, \frac{\alpha'}{2}, \frac{\alpha''}{2}$ varrebbe il fratto $\pm\frac{1}{8}$: ciò che è assurdo.

Sia β un'altra unità $y_1\omega_1 + y_2\omega_2 + y_3\omega_3$ (dove le y sono interi razionali), e sia pure $|\beta| = |\beta'| = |\beta''| = 1$. Se $\alpha \neq \beta, \alpha \neq -\beta$, si ha: $\frac{|\beta-\alpha|}{2} < \frac{|\beta|+|\alpha|}{2} = 1$.

E similmente $\frac{|\beta'-\alpha'|}{2} < 1, \frac{|\beta''-\alpha''|}{2} < 1$.

Perciò $Nm\frac{\beta-\alpha}{2} < 1$. Essendo $\frac{\beta-\alpha}{2} \neq 0$, il numero $\frac{\beta-\alpha}{2}$ non può essere intero. E perciò i numeri $x_1 - y_1, x_2 - y_2, x_3 - y_3$ non possono essere <u>tutti</u> pari. Cioè i numeri x_1, x_2, x_3 non possono avere rispettivamente la stessa parità di y_1, y_2, y_3.

Ma ora tre numeri non tutti e tre pari possono avere la parità di una delle seguenti // $2^3 - 1$ terne $(1,0,0), (1,0,1), (1,1,0), (1,1,1), (0,0,1), (0,1,0), (0,1,1)$.

---

[76] *e.c.* e *cor. sup.*: Diophantische.

[77] Hilbert 1897 (trad. 1911), cap. VI, p. 40-51; la sez. VI, intitolata *Les unités du corps*, è interamente dedicata a tale argomento.

[78] Bianchi 1920-21, cap. I, §13, p. 82.

[79] Hilbert 1897 (trad. 1911), cap. VI, §19, p. 44; l'autore inizia la trattazione scrivendo "nous appellerons unité du corps k tout nombre entier ε dont la valeur inverse $\frac{1}{\varepsilon}$ est encore un nombre entier. La norme d'une unité $= \pm 1$, et, réciproquement, si la norme d'un entier du corps $= \pm 1$, ce nombre est une unité du corps".

[80] Bianchi 1920-21, cap. I, §13, p. 82, 83.

[81] *e.c.* e *del.*: $\frac{\alpha}{2}, \frac{\alpha'}{2}, \frac{\alpha''}{2}$.

Ad ognuna di queste terne possono corrispondere al più due unità uguali e di segno opposto. Perciò di unità che, insieme alle coniugate, sono uguali ad 1 in valore assoluto ce ne sono al più $2(2^3-1)=14$. Per un corpo di grado n ce ne sono al più $2(2^n-1)$.
Ora, se α è una cosiffatta unità, anche $\alpha^2, \alpha^3, \alpha^4$ ... sono unità dello stesso tipo. Ma poiché al massimo vi sono al più $2(2^n-1)$ unità cosiffatte, esisteranno due interi p, q che al più differiscono di $2(2^n-1)$ tali che $\alpha^p = \alpha^q$, ossia che $\alpha^{p-q}=1$.
Cioè α è radice dell'unità di indice massimo $2(2^n-1)$. Viceversa se $K(\theta)$ contiene una radice di 1, questa è un'unità del corpo.
Questo risultato dice:
Se le radici $\alpha, \alpha', \alpha'', \ldots$ di un'equazione algebrica a coefficienti intieri razionali, di cui il primo e l'ultimo valgono ± 1 sono in valore assoluto uguali ad 1, ciascuna di esse // soddisfa ad un'equazione $\alpha^h = 1$ con $h < 2(2^n-1)$ se h è il grado dell'equazione considerata.
Cerchiamo le altre unità ε, tali che almeno uno dei numeri $|\varepsilon|, |\varepsilon'|, |\varepsilon''|$ sia differente da 1.

§.7 ***Il gran teorema di Dirichlet***[82]

Poniamo

$$\xi = x\omega_1 + y\omega_2 + z\omega_3$$
$$\eta = x\omega_1' + y\omega_2' + z\omega_3'$$
$$\zeta = x\omega_1'' + y\omega_2'' + z\omega_3''.$$

Se x, y, z sono interi razionali, le ξ, η, ζ sono interi coniugati. Dato uno di essi, per esempio ξ, sono determinate η, ζ e quindi anche x, y, z. Cioè nello spazio, ove $x, y, z,$ sono coordinate cartesiane, un piano $\xi = cost.$ oppure un piano $\eta = cost.$, oppure un piano $\zeta = cost.$ contengono ciascuno al più un solo punto della rete R luogo dei punti a coordinate x, y, z intere razionali. Il determinante delle ξ, η, ζ vale $\sqrt{D}$; quindi il parallelepipedo P determinato dai piani $-1 \le \xi \le 1, -1 \le \eta \le 1, -1 \le \zeta \le 1$ ha il volume $\frac{8}{\sqrt{D}}$. Ognuna delle sue facce contiene uno // dei punti di R immagine di uno degli interi ± 1, e quindi non contiene altri punti di R. Né entro P vi sono altri punti di R distinti dall'origine O. Un tale punto corrisponderebbe a un intero di- $K(\theta)$ minore, insieme ai suoi coniugati, di 1 in valore assoluto. La sua norma sarebbe pertanto minore anch'essa di 1 in valore assoluto; ciò che è assurdo.
Ingrandiamo P sostituendo alle facce $\xi = \pm 1$ le $\xi = \pm m$ (con $|m| > 1$). Se $|m|$ è così grande che il volume del nuovo parallelepipedo sia > 8, allora per il teorema di Minkowski, esso conterrà all'interno almeno un nuovo punto A della rete, e il suo simmetrico A' esterni entrambi alle facce $\eta = \pm 1, \zeta = \pm 1$.
Sia h il minimo intero positivo > 1 tale che le facce $\xi = \pm h$ contengono questi due punti e che nessun altro punto della rete, oltre O, sia compreso nel parallelepipedo

$$-h \le \xi \le h, \qquad -1 \le \eta \le 1, \qquad -1 \le \zeta \le 1.$$

Se noi troviamo per A, A' i piani $\eta = \pm k, \zeta = \pm l$ con k, l costanti che contengono tali punti, // sarà $|k| < 1, |l| < 1$. Il parallelepipedo

$$-h \le \xi \le h, \qquad -k \le \eta \le k, \qquad -l \le \zeta \le l,$$

[82] Dirichlet 1877 (trad. 1881), suppl. XI, §177, p. 542-554.

che contiene nel contorno i soli punti A, A' di R, contiene all'interno il solo punto O di R. Il suo volume $8\frac{hkl}{\sqrt{D}}$ è per il teorema di Minkowski minore di 8. Cioè gli interi che corrispondono ai punti A, A' hanno per valore assoluto $|hkl|$ della loro norma un numero $< \sqrt{D}$.
Ripetendo su questo parallelepipedo il ragionamento fatto per P, è così continuando, si trova: Esistono nel nostro corpo infiniti interi ξ la cui norma in valore assoluto è minore di $\sqrt{D}$, che vanno crescendo in valore assoluto, mentre gli interi coniugati η, ζ, vanno diminuendo in valore assoluto.
Tra questi interi ξ ne esisteranno infiniti la cui norma ha uno stesso valore assoluto $N < \sqrt{D}$. Se $\xi_h = x_h\omega_1 + y_h\omega_2 + z_h\omega_3$ $(h = 1,2,3, \dots)$ sono tali interi, ne esisteranno almeno due ξ_n, ξ_m con $n > m$ tali che: //

$$\frac{x_n - x_m}{N}, \frac{y_n - y_m}{N}, \frac{z_n - z_m}{N} \text{ sono interi razionali.}$$

Pertanto $\frac{\xi_n}{\xi_m} = 1 + \frac{\xi_n - \xi_m}{N}\frac{N}{\xi_m}$ è intero, perché $\frac{N}{\xi_m} = \pm\frac{Nm\,\xi_m}{\xi_m}$ è intero. D'altra parte $\left|\frac{\xi_n}{\xi_m}\right| > 1$, perché $n > m$. E infine $Nm\frac{\xi_n}{\xi_m} = \pm 1$; perché $Nm\,\xi_n = \pm Nm\,\xi_m = \pm N$. Dunque: Esiste almeno una unità ε, che in valore assoluto supera 1, mentre le unità coniugate $\varepsilon', \varepsilon''$ sono in valore assoluto minori di 1. Similmente si prova l'esistenza di altre due unità $\varepsilon_1, \varepsilon_2$ tali che $|\varepsilon_1'| > 1, |\varepsilon_1| < 1, |\varepsilon_1''| < 1$; e che $|\varepsilon_2''| > 1, |\varepsilon_2| < 1, |\varepsilon_2'| < 1$.
Sia σ un'unità qualsiasi, e siano σ', σ'' le unità coniugate.
Poniamo:

$$\log|\sigma| = X\log|\varepsilon_1| + Y\log|\varepsilon_2| \quad \text{cioè} \quad |\sigma| = |\varepsilon_1^X\,\varepsilon_2^Y|$$
$$\log|\sigma'| = X\log|\varepsilon_1'| + Y\log|\varepsilon_2'| \qquad |\sigma'| = |\varepsilon'^X_1\,\varepsilon'^Y_2|$$

Si hanno due equazioni lineari nelle incognite X, Y, il cui determinante è differente da zero[83]. // Infatti, se tale determinante fosse nullo, sarebbe, come si riconosce sviluppandolo[84]:

$$\frac{log\,|\varepsilon_1|}{log\,|\varepsilon_2|} = \frac{log\,|\varepsilon_1'|}{log\,|\varepsilon_2''|}$$

Ora $\log|\varepsilon_i''| = -\log|\varepsilon_i| - \log|\varepsilon_i'|$ perché[85] $Nm\,\varepsilon_i = 0$. Se ne deduce che, detto ρ il valore dei precedenti rapporti, sarebbe anche $\frac{\log|\varepsilon_1''|}{\log|\varepsilon_2''|} = \rho$, cosicché sarebbe $|\varepsilon_1| = |\varepsilon_2|^\rho$, $|\varepsilon_1'| = |\varepsilon_2'|^\rho, |\varepsilon_1''| = |\varepsilon_2''|^\rho$. Essendo $|\varepsilon_1'| > 1, |\varepsilon_2'| < 1$, sarebbe pertanto $\rho < 0$, ciò che è assurdo perché $|\varepsilon_1| < 1, |\varepsilon_2| < 1$.
Dunque le equazioni precedenti determinano le X, Y, e pertanto anche un punto nel piano π ove X, Y sono coordinate cartesiane. Io dico che questi punti formano una rete. Infatti, se X, Y, corrispondono all'unità σ, e ξ, η ad un'altra unità τ, la coppia $X + \xi, Y + \eta$ corrisponde al numero $\sigma\tau$, che è pure un'unità. Di più i punti (X, Y) non possono essere tutti sulla stessa retta; perché tra essi vi sono i punti $(0,0), (0,1), (1,0)$. Infine, in una regione finita di π vi è un numero finito di tali punti; e ciò perché, se sono dati i limiti superiori delle X, Y, sono contemporaneamente dati li//miti superiori per $|\sigma|, |\sigma'|, |\sigma''|$; e di interi σ, limitati insieme ai

[83] Nota inserita da Fubini a p.d.p.: *Disp. 15 Teoria dei numeri*.
[84] *e.c.* e *del.*: $\frac{\log|\varepsilon_1|}{\log|\varepsilon_2|} = \frac{\log|\varepsilon_1'|}{\log|\varepsilon_2''|}$.
[85] *e.c.* e *cor. sup.*: $\log Nm\,\varepsilon_i = 0$.

coniugati in valore assoluto, ve ne è un numero finito. Pertanto i punti (X, Y) sono in numero finito.
Se ne potranno (in infiniti modi) scegliere due X_1, Y_1 ed X_2, Y_2 in guisa che ogni altro punto della rete sia dato dalle:

$$X = xX_1 + yX_2 \qquad Y = xY_1 + yY_2$$
con x, y interi razionali.

Sarà pertanto

$$|\sigma| = |\eta_1|^x |\eta_2|^y$$
$$|\sigma'| = |\eta_1'|^x |\eta_2'|^y$$
$$|\sigma''| = |\eta_1''|^x |\eta_2''|^y$$

dove η_1, η_2 sono le unità definite dalle:

$$\eta_1 = \varepsilon_1^{X_1} \varepsilon_2^{Y_1}; \qquad \eta_2 = \varepsilon_1^{X_2} \varepsilon_2^{Y_2}.$$

Quindi $\sigma \eta_1^{-x} \eta_2^{-y}$ è una unità, tale che il suo valore assoluto, e quello delle coniugate, valgano 1; essa è pertanto una unità η che è radice di 1. Pertanto ogni unità del nostro corpo è un intero del tipo

$$\eta_1^x \eta_2^y \eta \ (x, y \text{ interi razionali variabili}).$$

Con metodo analogo questo teorema si dimostra in ogni caso: //
Se tra il corpo dato ed i coniugati ve ne sono r reali, e $2s$ a due a due immaginarii coniugati, allora nel corpo dato si possono scegliere $\rho = r + s - 1$ unità $\eta_1, \eta_2, \dots, \eta_\rho$ tali che ogni altra unità del corpo si possa in uno e in un solo modo scrivere nella forma

$$\eta \eta_1^{x_1} \eta_2^{x_2} \dots \eta_\rho^{x_\rho} \ (x_1, x_2, \dots, x_\rho \text{ interi razionali})$$

dove η è una radice dell'unità[86] (Dirichlet).
Questo teorema perde ogni valore soltanto se $r + s = 1$, cioè se $r = 1, s = 0$ (nel qual caso il corpo coincide col caso elementare del corpo R dei razionali) oppure se $r = 0, s = 1$ (corpo quadratico immaginario insieme al coniugato).

§.8 ***Il caso dei corpi quadratici***[87]

Sia θ radice di un'equazione di secondo grado[88] $\theta^2 + p\theta + q = 0$ con p, q razionali. Essendo[89]

$\theta = -\frac{p}{2} \pm \sqrt{\frac{p^2}{2} - q}$, il corpo $K(\theta)$ coinciderà con $K\left(\sqrt{\frac{p^2}{4} - q}\right)$. Ora, se t razionale, è pure

$$K\left(\sqrt{\frac{p^2}{4} - q}\right) = K\left(t\sqrt{\frac{p^2}{4} - q}\right) = K\left(\sqrt{t^2\left(\frac{p^2}{4} - q\right)}\right).$$

[86] Bianchi 1920-21, cap. I, §22, p. 139. Cfr. anche Hilbert 1897 (trad. 1911), cap. VI, §19, p. 44, teor. 47.
[87] Dirichlet 1877 (trad. 1881), suppl. XI, §166, p. 485-488. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, p. 17-183: l'autore dedica l'intero cap. II – *Le corps quadratques* – allo studio approfondito del caso dei corpi quadratici.
[88] Bianchi, 1920-21, Cap. I, §14, p. 85.
[89] *e.c.* e *cor. sup.*: invece di $\pm\sqrt{\frac{p^2}{2} - q}$ leggasi $\pm\sqrt{\frac{p^2}{4} - q}$.

Potremo scegliere t in guisa che $t^2\left(\frac{p^2}{4}-q\right)$ sia un intero razionale $\underline{m}$ privo di fattori quadrati. Il nostro corpo si ridurrà a $K(\sqrt{m})$, dove $\sqrt{m}$ è // l'intero radice dell'equazione $\theta^2-m=0$. [Si suppone $m\neq 1$, perché altrimenti torneremmo al campo R assoluto di razionalità]. Il corpo è un corpo di Gailois[90] (coincide col coniugato). Il discriminante di $\sqrt{m}$ vale[91]

$$D(\sqrt{m})=\begin{pmatrix}1 & \sqrt{m}\\ 1 & -\sqrt{m}\end{pmatrix}^2=4m.$$

Pertanto gli interi del corpo sono numeri del tipo[92]

$$\frac{a+b\sqrt{m}}{X} \qquad (1)$$

essendo a,b,X interi razionali, tali[93] X^2 divide $4m$. È pertanto (per l'ipotesi fatta su m) $X=1$ oppure $X=2$. Nel primo caso possiamo moltiplicare i due termini di (1) in guisa che il denominatore venga uguale a 2. Supposto $X=2$, la (1) dà un intero, soltanto quando la sua traccia $\frac{2a}{X}=a$ e la sua norma $\left(\frac{a+b\sqrt{m}}{2}\right)\left(\frac{a-b\sqrt{m}}{2}\right)=\frac{a^2-b^2m}{4}$ sono interi razionali. La prima condizione è soddisfatta. Occupiamoci della seconda.

1° Caso) $\underline{a}$ pari; allora b^2m è divisibile per 4; ma $\underline{m}$ non è divisibile per 4 (che è il quadrato di[94]); dunque[95] b^2, e perciò anche $\underline{b}$ è pari; posto $\alpha=\frac{a}{2}$, $\beta=\frac{b}{2}$, la (1) diventa $\alpha+\beta\sqrt{m}$ con α,β interi razionali.

2° Caso) $\underline{a}$ dispari, cosicché $a^2\equiv 1\ (mod\ 4)$. Sarà pertan//to $b^2m\equiv 1\ (mod\ 4)$. Perciò $\underline{b}$ sarà dispari, e quindi $b^2\equiv 1\ (mod\ 4)$. E pertanto sarà anche $m\equiv 1\ (mod\ 4)$. Perciò:

Se $m\equiv 1\ (mod\ 4)$, gli interi del campo sono di uno dei tipi[96] $\alpha+\beta\sqrt{m}, \frac{(2\alpha+1)+(2\beta+1)\sqrt{m}}{2}$ con α,β interi razionali.

Se $m\not\equiv 1$, cioè $m\equiv 2$ oppure $m\equiv 3\ (mod\ 4)$ [perché non può essere $m\equiv 0\ (mod\ 4)$ non essendo $\underline{m}$ divisibile per alcun quadrato], gli interi del campo sono del tipo[97]

$$x+y\sqrt{m} \text{ con } x,y \text{ interi razionali.}$$

Nel primo caso si osservi che

$$\frac{(2\alpha+1)+(2\beta+1)\sqrt{m}}{2}=\frac{1+\sqrt{m}}{2}+\alpha+\beta\sqrt{m}.$$

Donde, posto $\alpha=\beta=0$, segue che $\omega=\frac{1+\sqrt{m}}{2}$ è pure un intero del corpo. Ed è $\sqrt{m}=2\omega-1$. Gli interi del corpo sono perciò $\alpha-\beta+2\beta\omega$ oppure $\alpha-\beta+(2\beta+1)\omega$; cioè sono tutti e soli i numeri del tipo

$$x+y\omega \text{ con } x,y \text{ interi razionali.}$$

[90] *e.c.* e *cor. sup.*: Galois.
[91] Dirichlet 1877 (trad. 1881), suppl. XI, §166, p. 486. Sommer 1907 (trad. 1911), cap. 2, §6, p. 24.
[92] Sommer 1907 (trad. 1911), cap. 2, §5, p. 17 e §6, p. 19.
[93] *e.c.* e *cor. sup.*: tali che X^2.
[94] *e.c.* e *cor. inf.* a lato del testo: quadrato di 2.
[95] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale.
[96] Sommer 1907 (trad. 1911), cap. 2, §6, p. 21.
[97] Bianchi 1920-21, cap. I, §14, p. 86, 87

Cioè, se $m \equiv 1\ (mod\ 4)$, una base del corpo è formata dai numeri $1, \omega = \frac{1+\sqrt{m}}{2}$; e il discriminante del corpo è $\begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = m$.
Se $m \equiv 2$ oppure $m \equiv 3\ (mod\ 4)$, una base del corpo è // invece formata dai numeri $1, \sqrt{m}$; cosicché $4m$ è il discriminante del corpo.

Oss.[ervazione] Notiamo qualche analogia con le forme $ax^2 + 2bxy + cy^2$. Se a, c sono pari, ma b è dispari, questa forma non è primitiva, ma non si può dividere per 2 senza abbandonare le notazioni di Gauss. Si noti che in tal caso $b^2 - ac$ è proprio $\equiv 1\ (mod\ 4)$.
Cerchiamo le unità[98], cioè gli interi a norma ± 1. Detto ω' il coniugato di ω, nel primo caso le unità sono caratterizzate dalla $(x + y\omega)(x + y\omega') = \pm 1$, cioè[99]

$$\left(x + \frac{y}{2}\right)^2 + \frac{my^2}{4} = x^2 + xy + \frac{1-m}{4}y^2 = \pm 1. \qquad (2)$$

Nel secondo caso le unità $x + y\sqrt{m}$ corrispondono alle soluzioni della

$$x^2 - my^2 = \pm 1. \qquad (3)$$

Se $m < 0$, e il corpo è complesso, la (2) ammette le soluzioni $x = \pm 1, y = 0$, e ne ammette altre soltanto se $m = -3$ (notisi che $m < 0, m \equiv 1\ (mod\ 4)$, cosicché m è uguale ad uno dei numeri $3, 7, 11$, ecc.). Infatti se $|y| \geq 1$, e $-m \geq 7$, il primo membro di (2) è maggiore di $\frac{7}{4} > 1$. Se $m = -3$, vi sono le ulteriori soluzioni //

$y = 1$ $\left(x + \frac{1}{2}\right)^2 = 1 - \frac{3}{4} = \frac{1}{4}$ cioè $x = 0$ oppure $x = -1$

$y = -1$ $\left(x - \frac{1}{2}\right)^2 = \frac{1}{4}$ cioè $x = 0$ oppure $x = 1$.

Dunque per $m \equiv 1\ (mod\ 4)$ ed $m < 0$, vi sono le sole unità ± 1, eccetto quando $m = -3$; nel qual caso vi sono inoltre le unità $\pm\frac{1+\sqrt{m}}{2}, \pm\frac{-1+\sqrt{m}}{2}$ (Si noti la coincidenza, tutt'altro che casuale con due vertici del triangolo modulare). Se invece $m < 0$, ma $m \not\equiv 1\ (mod\ 4)$ si trovano le unità ± 1, e nel solo caso $m = -1$ si trovano inoltre le unità $\pm i$ (si ricordi che anche il punto i si può considerare vertice di un triangolo modulare).
Passiamo al caso di $m > 0$, cioè di corpi reali. Si prova facilmente che di unità uguali ad 1 in valore assoluto vi sono soltanto le ± 1. Il gran teorema di Dirichlet assicura che esiste una unità ε, così che tutte le unità del corpo sono del tipo $\pm\varepsilon^n$ con[100] m intero razionale[101]. (Si noti che (3) è l'equazione di Pell; e si ricordino i risultati trovati per essa; essi appaiono casi particolari del gran teorema di Dirichlet).
Se $Nm\ \varepsilon = 1$, tutte le unità del corpo hanno per norma 1. Se $Nm\ \varepsilon = -1$, soltanto le potenze di $\eta = \varepsilon^2$ hanno per norma 1, le altre hanno per norma[102] -1. //

[98] Sommer 1907 (trad. 1911), cap. 2, §22, p. 103-113. La notazione di Fubini è del tutto analoga a quella adottata da Sommer nella sez. *Les unités du corps quadratiques*.
[99] *e.c.* e *cor. sup.*: invece di $\left(x + \frac{y}{2}\right)^2 + \frac{my^2}{4}$ leggasi $\left(x + \frac{y}{2}\right)^2 - \frac{my^2}{4}$.
[100] *e.c.* e *cor. sup.*: con n intero.
[101] Bianchi 1920-21, cap. I, §14, p. 89. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §22, p. 110.
[102] *Idem*, cap. I, §14, p. 89, 90. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §22, p. 111.

11. Guido Fubini nel 1939

Capitolo VII – Teoria della divisibilità in un corpo algebrico

§.1 *Un esempio preliminare*[1]

Approfondiamo in un esempio un fatto cui abbiamo già accennato.
Se noi chiamiamo indecomponibile un intero α che non si possa porre uguale al prodotto $\beta\gamma$ di due interi β, γ del corpo distinti da unità, non è vero che un intero si possa scrivere in un solo modo come prodotto di interi indecomponibili, anche quando non si considerino come distinti due prodotti, quando i fattori di uno sono associati ordinatamente ai fattori dell'altro. Così, p. es., in[2] $K(\sqrt{-5})$ vi sono le sole unità[3] ± -1. Ed è[4]

$$21 = 3 \cdot 7 = \left(4 + \sqrt{-5}\right)\left(4 - \sqrt{-5}\right) = \left(1 + 2\sqrt{-5}\right)\left(1 - 2\sqrt{-5}\right).$$

I numeri $3, 7, 4 \pm \sqrt{-5}, 1 \pm 2\sqrt{-5}$ sono indecomponibili, come il lettore può facilmente provare. E le tre decomposizioni precedenti sono distinte, perché le sole unità sono ± 1.
Noi completeremo (secondo una terminologia, a cui già abbiamo accennato) il corpo $K(\sqrt{-5})$, ag//giungendogli nuovi enti, che chiameremo <u>ideali</u>[5]. E, senza per ora a[6] badare a ragionamenti rigorosi, diremo <u>ideale</u> un ente che sia il M.C.D. di due interi α e β del corpo, e sia divisore di ogni numero, che sia somma di un multiplo di α e di un multiplo di β. Che un tal numero non esista sempre nel nostro corpo noi sappiamo già; la definizione precedente, che provvisoriamente accettiamo, è pertanto assurda come l'altra: <u>il numero -1 non possiede radice quadrata; noi chiameremo i la $\sqrt{-1}$</u>. Così come l'algebra dimostra accettabile la teoria dei numeri complessi, noi trasformeremo poi la precedente definizione in modo da renderla logicamente accettabile. Di ciò parleremo nel prossimo paragrafo. Per ora la useremo nella forma illogica, ma intuitiva, data più sopra.
Sia $\left[3, 4 + \sqrt{-5}\right]$ l'ideale M.C.D. di 3 e di $4 + \sqrt{-5}$.
Sia $[3, 4 — \sqrt{-5}]$ l'ideale M.C.D. di 3 e di $4 — \sqrt{-5}$.
Converremo di porre il loro prodotto uguale al M.C.D. dei numeri $3 \cdot 3, 3 \cdot (4 — 5)$, $\left(4 + \sqrt{-5}\right) \cdot 3, \left(4 + \sqrt{-5}\right) \cdot (4 - \sqrt{-5})$, così come se tali <u>ideali</u> godessero delle solite proprietà dei M.C.D. Tale prodotto è // dunque il M.C.D. di

$$3 \cdot 3,\ 3\left(4 - \sqrt{-5}\right),\ 3\left(4 + \sqrt{-5}\right),\ 3 \cdot 7 \qquad (\alpha)$$

e quindi è anche divisore di $3 \cdot 7 - 2(3 \cdot 3) = 3$. Ma ora, poiché 3 divide tutti i numeri (α), il prodotto dei nostri due ideali è 3. Cioè:

---

[1] Bianchi 1920-21, Introduzione, §7, p. 44-47. Bianchi tratta questo esempio in modo analogo a Fubini.
[2] Gazzaniga 1903, cap. IX, p. 250-254. Gazzaniga analizza questo esempio particolare in modo meno approfondito di Fubini, insieme ai corpi $K\left(\sqrt{-2}\right), K\left(\sqrt{-6}\right)$. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §159, p. 441; cfr. inoltre Minkowski 1957, p. 149-155. Qui Minkowski, per introdurre la teoria degli ideali, utilizza l'esempio di $\mathbb{Z}[\sqrt{-6}]$ al cui interno vale la seguente decomposizione $10 = 2 \cdot 5 = \left(2 + \sqrt{-6}\right)\left(2 - \sqrt{-6}\right)$. Fubini, pur conoscendo profondamente l'opera di Minkowski, riprende l'esempio della "mancata" fattorizzazione unica dal lavoro di Dedekind, dichiarando implicitamente di seguire quest'ultimo nella sua esposizione della teoria degli ideali.
[3] *e.c.* e *cor. sup.*: ± 1.
[4] Sommer 1907 (trad. 1911), cap. 2, §6, p. 30 e §8, p. 41.
[5] Dirichlet 1877 (trad. 1881), suppl. XI, §167, p. 497; Dedekind scrive che "il successo mostrerà che mediante la teoria degli ideali […] le leggi della divisibilità dei numeri vengono portate alla conclusione in modo esauriente".
[6] *lapsus* del curatore: leggasi "per ora badare".

$$3 = [3{,}4 + \sqrt{-5}][3{,}4 - \sqrt{-5}].$$

Così si prova

$$7 = [7{,}4 + \sqrt{-5}][7{,}4 - \sqrt{-5}].$$

Cosicché la $21 = 3 \cdot 7$ diventa[7]

$$21 = [3{,}4 + \sqrt{-5}][3{,}4 - \sqrt{-5}][7{,}4 + \sqrt{-5}][7{,}4 - \sqrt{-5}]. \qquad (\beta)$$

Il prodotto del primo per il terzo fattore sarà analogamente il M.C.D. di

$$3 \cdot 7, \qquad 3(4 + \sqrt{-5}), \qquad 7(4 + \sqrt{-5}), \qquad (4 + \sqrt{-5})^2 = 11 + 8\sqrt{-5}$$

che è divisore di //

$$7(4 + \sqrt{-5}) - 2[3(4 + \sqrt{-5})] = 4 + \sqrt{-5}.$$

Dunque tale prodotto vale proprio $4 + \sqrt{-5}$. Il prodotto del secondo e del quarto fattore di β si trova similmente uguale a[8] $4 + \sqrt{-5}$; e quindi nella (β) è inclusa la $21 = (4 + \sqrt{-5})(4 - \sqrt{-5})$. Il prodotto del primo per il quarto fattore di (β) è il M.C.D. di

$$3 \cdot 7,\ 3(4 - \sqrt{-5}),\ 7(4 + \sqrt{-5}),\ (4 + \sqrt{-5})(4 - \sqrt{-5}) = 21 \qquad (\gamma)$$

che è divisore di

$$-3 \cdot 3 \cdot 7 + 7(4 + \sqrt{-5}) + 3 \cdot 3(4 - \sqrt{-5}) = 1 - 2\sqrt{-5}.$$

Poiché, come è facile riconoscere, i numeri γ sono tutti i divisibili per $1 - 2\sqrt{-5}$, il prodotto del primo e quarto fattore di (β) vale $1 - 2\sqrt{-5}$; il prodotto degli altri due si prova similmente uguale a $1 + 2\sqrt{-5}$. Quindi nella (β) è anche inclusa la $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.
Dunque le nostre tre decomposizioni distinte sono tutte e tre comprese nell'unica decomposizione (β) in fattori ideali.

§.2 ***Prime definizioni della teoria degli ideali***[9]

Dobbiamo porre in generale e giustificare le precedenti definizioni, o per meglio dire trasformarle in modo da renderle non assurde.
A tal fine siano $\alpha_1, \alpha_2, \ldots, \alpha_h$ interi prefissati del corpo. Vogliamo definire un ente E che dovremo poi dimostrare poter sostituire il loro M.C.D., quando questo manchi. Osserviamo che un tale ente dovrebbe essere divisore anche di ogni intero $\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_h z_h$ che si ottenga dagli α_i, sommando i prodotti ottenuti moltiplicando le α per interi arbitrari z del corpo. Questo ente E dovrebbe essere pertanto il M.C.D. della classe // formata da tutti gli

[7] Sommer 1907 (trad. 1911), cap. 2, §8, p. 41.
[8] *e.c.* e *cor. sup.*: $4 - \sqrt{-5}$.
[9] Cfr. Hilbert 1897 (trad. 1911), cap. II, §4, p. 13-18. Il matematico tedesco introduce questa sezione scrivendo: "Le premier problème important de la théorie des corps algébriques est la recherche des lois de la décomposition (divisibilité) des nombres algébriques. Ces lois sont d'une admirable beauté et d'une grande simplicité. Elles présentent une analogie precise aver les lois élémentaires de la divisibilité pour les nombres entieres rationelles et elles ont la même signification fondamentale. Ces lois ont été découvertes d'abord par Kummer, mais mérite de les avoir établies pour le corps algébrique general revient à Dedekind et à Kronecker".

interi $\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_h z_h$, la quale classe C di numeri sarebbe a sua volta la classe formata dagli interi multipli di E.
L'ente E e la classe C sarebbero perciò determinati l'uno dall'altro. Noto E, la classe C sarebbe formata dai suoi multipli; data C, l'ente E sarebbe il M.C.D. di C.
E noi, perciò, non curiamoci di questa E; e chiamiamo ideale[10] la classe C precedentemente definita, che è determinata dagli α, e che perciò indicheremo col simbolo[11] $(\alpha_1, \alpha_2, \dots, \alpha_n)$.
Se i numeri α si riducono al solo α_1, se cioè $n = 1$, l'ideale (α_1) è la classe degli interi del corpo divisibile per α_1. Il numero α_1 individua l'ideale (α_1). Numeri associati con α_1 generano lo stesso ideale (α_1). Viceversa, se l'ideale (α_1) è dato, il numero intero α_1 è determinato a meno di un fattore, che è un'unità del corpo.
Se esiste un intero α del corpo, che si possa scrivere nella forma

$$\alpha = K_1\alpha_1 + K_2\alpha_2 + \cdots + K_n\alpha_n \quad (K_i = \text{ interi del corpo}),$$

e che sia un divisore di $\alpha_1, \alpha_2, \dots, \alpha_n$, un tale numero α è il M.C.D. di $\alpha_1, \alpha_2, \dots, \alpha_n$, perché ogni di//visore comune di $\alpha_1, \alpha_2, \dots, \alpha_n$ è anche un divisore di α. E l'ideale $(\alpha_1, \alpha_2, \dots, \alpha_n)$ coincide con (α). Un ideale (α) formato dai multipli di un intero α del corpo dicesi principale[12].
Noi alla considerazione del nostro corpo K di numeri sostituiamo la considerazione dell'insieme K' di tutti i suoi ideali, principali o no. Ad ogni numero del corpo K corrisponde un ideale (principale) di K'; ad ogni ideale (principale) di K' corrispondono un intero di K e gli interi associati; una K' può contenere degli ideali non principali, a cui in K non corrisponde alcun intero. Se noi consideriamo come enti equivalenti un intero e il corrispondente ideale principale, allora si può concepire K' come dedotto da K con l'aggiunta degli ideali non principali. Tra gli ideali vi è lo (0), formato dal solo numero zero[13], e lo[14] (1) formato da tutti gli interi del corpo. Ogni ideale contiene il numero zero.
Dovremo poi definire il prodotto di due o più ideali, la divisibilità di un ideale per un altro, ecc. ecc. Ma innanzi tutto vogliamo approfondire le proprietà degli ideali. //
Supponiamo, al solito, per fissare le idee, il corpo K di terzo grado. I punti B immagini degli interi di un ideale differente da (0) sono parte della rete di punti nello spazio a tre dimensioni, coi quali abbiamo rappresentato gli interi del corpo. Ad essi appartiene l'origine (perché ogni ideale contiene il numero zero). I punti B non giacciono tutti in uno stesso piano [perché, se

[10] Hilbert 1897 (trad. 1911), cap. II, §4, p. 14. Hilbert fornisce la seguente definizione di ideale: "Un système d'un nombre infini d'entieres algébriques $\alpha_1, \alpha_2, \dots$ du corps k, tel que toute combinaison linéaire $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ (où $\lambda_1, \lambda_2, \dots$ sont des nombres entiers du corps) appartienne encore au système est dit un idéal". Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §9, p. 36.
[11] Bianchi 1920-21, cap. II, §23, p. 146. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §9, p. 36, 37
[12] *Idem*, Introduzione, §7, p. 48; cap. II, §23, p. 146. Cfr. anche Gazzaniga 1903, cap. XII, p. 383. Cfr. inoltre Dirichlet 1877 (trad. 1881), suppl. XI, §168, p. 499; qui Dedekind scrive "un ideale […] che consta di tutti i numeri $\omega\eta$ divisibili per η, lo diremo ideale principale". Cfr. Hilbert 1897 (trad. 1911), cap. II, §4, p. 14; qui Hilbert afferma: "un idéal qui contient tous les nombres de la forme $\lambda\alpha$ et ne contient que ces nombres où λ désigne un nombre entier quelconque appartenant au corps et α un nombre entier déterminé du corps est dit un idéal principal; on le désigne part (α) ou plus brièvement par α, dans le cas où il ne peut être confondu aver le nombre α". Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §9, p. 37: "En particulier un idéal est dit un *idéal principal*, lorsque ses nombres sont des multiples d'un nombre entier du corps appartenant à l'ideal".
[13] Dirichlet 1877 (trad. 1881), suppl. XI, §168, p. 498; Dedekind afferma che "è poi chiaro che (0) stesso è un ideale, perché i numeri ω contenuti in (0) si riproducono mediante addizione, sottrazione e moltiplicazione; questo ideale […] rappresenta fra questi la parte stessa, che il numero 1 fra i numeri razionali interi positivi".
[14] Bianchi 1920-21, cap. II, §23, p.147. Bianchi definisce (1) "ideale unità". Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §9, p. 37.

un ideale contiene un numero α, esso contiene anche i prodotti di α per un intero qualsiasi del corpo; prodotti, a cui corrispondono punti non posti tutti su uno stesso piano passante per l'origine (*)]. Se B_1, B_2, B_3 sono tre dei punti B citati, anche il punto B_4 che si deduce da B_1 con la traslazione B_2B_3 è un punto B. //
Infatti, se $\beta_1, \beta_2, \beta_3$ sono gli interi del corpo che hanno per immagine i punti B_1, B_2, B_3, il punto B_4 ha per immagine l'intero[15] $\beta_1 + \beta_2 - \beta_3$. Ed evidentemente, se un ideale contiene più interi $\beta_1, \beta_2, \beta_3$ esso contiene anche $\beta_1 + \beta_3 - \beta_2$. Dunque:
i punti B immagine degli interi di un dato ideale, formano una rete R contenuta nella rete r formata dai punti immagine degli interi del corpo [[16]escluso naturalmente il solo ideale (0)]. Si potranno pertanto determinare tre interi $\gamma_1, \gamma_2, \gamma_3$ dell'ideale, tale che ogni altro numero di questo si può scrivere nella forma $x\gamma_1 + y\gamma_2 + z\gamma_3$ con x, y, z interi razionali. I numeri $\gamma_1, \gamma_2, \gamma_3$ si diranno una base del l'ideale. Da una base si deducono tutte le altre con le solite trasformazioni unimodulari. I numeri γ, essendo interi del corpo, saranno legati agli interi $\omega_1, \omega_2, \omega_3$ base del corpo da tre equazioni[17]

$$\left.\begin{aligned} \gamma_1 &= p_1\omega_1 + q_1\omega_2 + r_1\omega_3 \\ \gamma_2 &= p_2\omega_1 + q_2\omega_2 + r_2\omega_3 \\ \gamma_3 &= p_3\omega_1 + q_3\omega_2 + r_3\omega_3. \end{aligned}\right\} \qquad (1)$$

Con p, q, r interi razionali. Ma viceversa non si deve credere che, scelti a caso degli interi // razionali p_i, q_i, r_i, i numeri γ definiti da queste equazioni costituiscano la base di un ideale. Infatti, l'ideale $(\gamma_1, \gamma_2, \gamma_3)$ contiene ogni intero ottenuto moltiplicando γ_i per un intero qualsiasi $x\omega_1 + y\omega_2 + z\omega_3$ (x, y, z interi razionali) del corpo. E, se $\gamma_1, \gamma_2, \gamma_3$ è una base dell'ideale, tutti questi prodotti devono potersi scrivere nella forma $\xi\gamma_1 + \eta\gamma_2 + \zeta\gamma_3$ con ξ, η, ζ interi razionali. Si vede facilmente che a tal fine è necessario e sufficiente che sia

$$\gamma_i\omega_k = c_{ik_1}\gamma_1 + c_{ik_2}\gamma_2 + c_{ik_3}\gamma_3 \quad (i, k = 1,2,3)$$

dove le c_{ik_r} sono interi razionali.
L'ideale principale (α) ha una base costituita dai numeri $\alpha\omega_1, \alpha\omega_2, \alpha\omega_3$.
Il discriminante di una base di un dato ideale è indipendente dalla base scelta, e dipende esclusivamente dall'ideale considerato (come si riconosce facilmente coi soliti metodi).
Dalle (1) si deduce che tale discriminante vale[18]

$$D = \begin{pmatrix} p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \\ p_3 & q_3 & r_3 \end{pmatrix}^2.$$

// Il valore assoluto del determinante delle p, q, r che è dunque un intero razionale positivo si chiama la norma dell'ideale.
Il discriminante di una base di un ideale vale il prodotto del discriminante del corpo per il quadrato della norma.

[15] *e.c.* e *cor. sup.*: $\beta_1 - \beta_2 + \beta_3$.
[16] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale.
[17] *e.c.* e *cor. sup.*: $\gamma_2 = p_2\omega_1 + q_1\omega_2 + r_2\omega_3$.
[18] Nota inserita da Fubini a p.d.p.: *Disp. 16 Teoria dei numeri*.

Così la norma di un ideale principale (α) vale[19] $\sqrt{\frac{(\alpha\omega_1\alpha\omega_2\alpha\omega_3)}{D}}$ cioè $\sqrt{\frac{(Nm\,\alpha)^2 D}{D}} = |Nm\,\alpha|$: essa coincide perciò col valore assoluto[20] dell'intero corrispondente α.
La norma di un ideale ha un notevole significato geometrico.
Il parallelepipedo che ha un vertice nell'origine, e gli altri vertici nei punti immagine degli interi γ ha in virtù delle (1) un volume che è proprio uguale al prodotto del valore assoluto del determinante delle p, q, r per il volume del parallelepipedo, che ha un vertice nell'origine e gli altri vertici nei punti immagine degli interi $\omega_1, \omega_2, \omega_3$, che pertanto è proprio uguale alla norma dell'ideale. (Perché gli interi ω individuano i punti unità degli assi coordinati, e definiscono proprio il parallelepipedo, il cui volume è assunto// ad unità di misura dei volumi).
Dunque la norma N di un ideale dà il numero degli interi del corpo, che sono contenuti nel parallelepipedo P fondamentale di un ideale, o, in altre parole, che si possono rappresentare nella forma $X\gamma_1 + Y\gamma_2 + Z\gamma_3$ con $0 \leq X < 1, 0 \leq Y < 1, 0 \leq Z < 1$. Ora la rete di un ideale determina un gruppo di traslazioni; ogni punto dello spazio si può portare in uno e in un solo modo entro P con una traslazione di tale gruppo.
E ciò in particolare avverrà di un punto A che sia immagine di un intero a del corpo. Ora se tale traslazione porta l'origine nel punto che è immagine del numero b del nostro ideale, essa porta il punto A nel punto che è immagine del punto $a + b$, e che sarà dentro P.
Esistono pertanto nel corpo N interi (quelli rappresentati da punti interni a P) tali che da ogni altro intero a del corpo si passa in uno ed in un sol modo ad uno di essi con l'aggiunta di un numero b del nostro ideale.
Se noi indichiamo con j l'ideale, e diciamo che due interi a, b del corpo sono tra loro congrui[21] // rispetto ad j, se $a - b$ è un numero di j [ciò che indicheremo con $a \equiv b\ (j)$], ne deduciamo:
Il numero degli interi incongrui rispetto ad un ideale vale la norma di questo[22].
(La norma di un ideale generalizza pertanto il concetto di valore assoluto di un intero nell'aritmetica elementare).
Sia $a_1, a_2, a_3, \ldots, a_N$ un sistema completo di interi incongrui rispetto all'ideale j. Anche $1 + a_1, 1 + a_2, \ldots, 1 + a_N$ sarà un sistema completo di interi incongrui (perché, se $1 + a_n \equiv 1 + a_m$ l'intero $(1 + a_n) - (1 + a_m) = a_n - a_m$ sarebbe un intero di j, cosicchè si avrebbe anche $a_n \equiv a_m$).
Perciò ciascuno dei numeri $1 + \omega_n$ sarà congruo ad uno ed uno solo degli interi ω_m. E perciò

$$\omega_1 + \omega_2 + \cdots + \omega_N \equiv (1 + \omega_1) + (1 + \omega_2) + \cdots + (1 + \omega_N)\ (j).$$

La differenza N dei due membri è dunque un numero di j.
Ogni ideale contiene, tra i suoi numeri, la propria norma[23] (che è un intero razionale, positivo) e quindi anche tutti i multipli di questa. //

(*) **Nota**[24]: Infatti, se $\omega_1\ \omega_2\ \omega_3$ formano una base del corpo, i numeri $\alpha\omega_1\ \alpha\omega_2\ \alpha\omega_3$ fanno parte del l'ideale; e, se $\alpha \neq 0$, il loro discriminante, che evidentemente vale $D(Nm\,\alpha)^2$, è differente da zero. Ora è facile vedere che tra interi $\lambda_i = x_i\omega_1 + y_i\omega_2 + z_i\omega_3\ (i = 1,2,3)$

[19] Bianchi 1920-21, cap. II, §23, p. 151, 152.
[20] *ad. sup.* e *a.m.*: "il valore assoluto del modulo dell'intero".
[21] Bianchi 1920-21, cap. II, §24, p. 153.
[22] *Idem*, cap. II, §24, p. 157. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §169, p. 502.
[23] Sommer 1907 (trad. 1911), cap. 2, §9, p. 39.
[24] *e.c.* e *cor. sup.* che ha reso illeggibile il testo originale

sono rappresentati da punti (x_i, y_i, z_i) posti in uno stesso piano con l'origine soltanto quando è nullo il loro discriminante (che è uguale al prodotto di D per il quadrato del determinante delle $x_i y_i z_i$).

§.3 ***Un lemma fondamentale***[25]

Se A, B, C sono polinomii della x

$$A = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$$
$$B = \beta_0 x^m + \beta_1 x^{m-1} + \cdots + \beta_m$$
$$C = \gamma_0 x^r + \gamma_1 x^{r-1} + \cdots + \gamma_r$$

se $C = AB$, se i coefficienti γ di C sono interi algebrici, anche tutti i prodotti ottenuti moltiplicando un coefficiente α di A per un coefficiente β di B sono interi algebrici. Ciò è evidente per $\alpha_0\beta_0 = \gamma_0$.

Siano $x_1, x_2, \dots, x_n, x_{n+1}, x_{n+2}, \dots, x_r$ le radici di $C = 0$; le prime n siano le radici di $A = 0$, le altre di $B = 0$.

Sarà pertanto

$$(1) \qquad \frac{\alpha_i\beta_j}{\alpha_0\beta_0} = \frac{\alpha_i\beta_j}{\gamma_0} = \varphi_i(x_1, x_2, \dots, x_n)\psi_j(x_{n+1}, x_{n+2}, \dots, x_r) \qquad (*)$$

dove le φ_i e le ψ_j sono funzioni simmetriche delle variabili, da cui rispettivamente dipendono di grado i oppure j nel completo[26] di tutte queste variabili, ma di primo grado rispetto ad una sola di esse.

Se noi facciamo variare le $x_1, x_2, \dots, x_n$ tra le possibili $\binom{r}{n}$ combinazioni delle r radici della // $C = 0$ prese ad n ad n, il secondo membro di (1) riceve $N = \binom{r}{n}$ valori, i quali sono radici di un'equazione di grado $N = \binom{r}{n}$.

$$\zeta^N + l_1\zeta^{N-1} + l_2\zeta^{N-2} + \cdots + l_N = 0. \qquad (2)$$

A questa equazione soddisfa in particolare la $\zeta = \frac{\alpha_i\beta_j}{\gamma_0}$. Ed i suoi coefficienti l_s sono polinomi razionali simmetrici di tutte le x, cioè sono polinomi razionali nelle[27] $\frac{\gamma_1}{\gamma_2}, \frac{\gamma_2}{\gamma_0}, \dots, \frac{\gamma_r}{\gamma_0}$; anzi l_s è in ciascuna delle x un polinomio di s^{esimo} grado; e perciò l_s è un polinomio di grado s nelle $\frac{\gamma_1}{\gamma_0}, \frac{\gamma_2}{\gamma_0}, \dots, \frac{\gamma_r}{\gamma_0}$ (che sono tutti di primo grado nelle x). Cioè $l_s\gamma_0$ è un polinomio nelle γ, ed è perciò un intero algebrico . Ora, posto

$$z = \frac{\zeta}{\gamma_0}$$

La z soddisfa alla[28]

$$z^N + (l_1\gamma_0)z^{N-1} + (l_2\gamma_0)^2 z^{N-2} + \cdots + (l_N\gamma_0^N) = 0$$

equazione i cui coefficienti sono stati ora dimostrati interi (algebrici), mentre il primo coefficiente è 1.

---

[25] Bianchi 1920-21, cap. II, §25, p. 162-164. Bianchi enuncia e dimostra tale lemma all'interno della dimostrazione del teorema A) sul prodotto di ideali.

[26] *e.c.* e *cor. sup.*: complesso.

[27] *e.c.* e *cor. sup.*: invece di $\frac{\gamma_1}{\gamma_2}$ leggasi $\frac{\gamma_1}{\gamma_0}$.

[28] *e.c.* e *cor. sup.*: invece di $(l_2\gamma_0)^2 z^{N-2}$ leggasi $(l_2\gamma_0^2)z^{N-2}$.

Le ζ sono pertanto interi algebrici: cioè i prodotti di γ_0 per le varie radici z della (2) e in particolare $\alpha_i\beta_j$ sono interi algebrici. Cioè il prodotto di ogni // coefficiente α per ogni coefficiente β è intero algebrico.
[29]Se fosse $AB = C$ e i coefficienti di C fossero interi algebrici divisibili per un intero n, altrettanto avverrebbe del prodotto $\alpha_i\beta_j$ di un qualsiasi coefficiente α di A per un qualsiasi coefficiente β di B. Infatti il prodotto di A per $\frac{B}{n}$ sarebbe il polinomio $\frac{C}{n}$ a coefficienti interi; altrettanto avverrebbe del prodotto di ogni coefficiente α di A per ogni coefficiente $\frac{\beta}{n}$ di B. Perciò ogni tale prodotto $\alpha_i\beta_j$ sarebbe un intero divisibile per n.
Se A, B, C fossero a coefficienti interi razionali, e se i coefficienti α fossero primi tra loro, se i coefficienti β fossero primi tra loro, altrettanto avverrebbe dei γ. Perché se $n > 1$ fosse un intero primo divisore comune dei γ, allora n sarebbe divisore comune degli $\alpha_i\beta_j$; e un tale primo n, se anche non dividesse uno solo dei β, p. es. non dividesse β_γ, dovrebbe dividere tutti gli α; ciò che è assurdo.
Questo ragionamento vale soltanto per gli interi razionali, e per i corpi ove è valido l'algoritmo di Euclide. Per tali corpi il nostro attuale teore//ma è dunque la generalizzazione del teorema di Gauss da noi dato al §2 pag. 10.

(*) **Nota**: Se $i = 0$, allora $\varphi_i = 1$. Se $j = 0$, è[30] $\psi_i = 1$.

§.4 ***Prodotto di ideali***[31]

Se $(\alpha_1, \alpha_2, \dots, \alpha_n)$ e $(\beta_1, \beta_2, \dots, \beta_m)$ sono due ideali, l'ideale determinato da tutti i numeri $\alpha_i\beta_j$ $(i = 1,2, \dots, n), (j = 1,2, \dots, m)$, dicesi prodotto dei precedenti[32].
Il prodotto[33] di due ideali principali $(\alpha), (\beta)$ è l'ideale $(\alpha\beta)$ generato dal numero $\alpha\beta$, che è prodotto dei numeri α, β, che generano rispettivamente i due ideali fattori (α) e (β).
Sia $\alpha_1, \alpha_2, \alpha_3$ la base di un ideale j: Il prodotto Q del polinomio $p = \alpha_1 x + \alpha_2 y + \alpha_3 z$ per i polinomi coniugati $p' = \alpha_1' x + \alpha_2' y + \alpha_3' z$ e $p'' = \alpha_1'' x + \alpha_2'' y + \alpha_3'' z$ (cioè la norma di un numero generico di j) è un polinomio Q a coefficienti γ interi razionali. Ne sia n il M.C.D. Indichiamo con β i coefficienti di $p'p''$. Per il lemma precedente il prodotto di una delle α per una delle β è divisibile per n.
Ora osserviamo:
L'intero razionale n che è M.C.D. dei γ, si potrà ottenere come combinazione lineare di questi; ma ogni γ è combinazione lineare dei prodotti ottenuti moltiplicando una delle α per una delle β. Perciò // n è combinazione lineare a coefficienti interi razionali dei prodotti ottenuti moltiplicando una delle α per una delle β.
Ora i numeri β sono evidentemente interi (perché ottenuti con somme e moltiplicazioni dalle α', α'') ed appartengono al nostro corpo originario perché si esprimono razionalmente mediante le α. [Infatti i β sono i coefficienti di $\frac{Q}{\alpha_1 x + \alpha_2 y + \alpha_3 z}$, di cui il numeratore è un polinomio a coefficienti γ interi razionali].

---

[29] Gazzaniga 1903, cap. XII, p. 389. Gazzaniga riporta questo risultato sotto forma di lemma all'interno di una dimostrazione.
[30] *e.c.* e *cor. inf.*: $\psi_j = 1$.
[31] Dirichlet 1877 (trad. 1881), suppl. XI, §170, p. 503, 504. Cfr. anche Hilbert 1897 (trad. 1911), cap. II, §4, p. 15.
[32] Gazzaniga 1903, cap. XII, p. 389. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §9, p. 37.
[33] Bianchi 1920-21, cap. II, §25, p. 159.

Pertanto le β individuano un ideale J del nostro corpo; i prodotti di una delle α per una delle β l'individuano[34] l'ideale jJ.
Per le due proposizioni che abbiamo sopra osservato tutti i numeri di jJ sono divisibili per n; e il numero n stesso appartiene ad jJ. Quindi jJ è l'ideale formato nel corpo da noi studiato dai multipli di n, cioè coincide con n. Pertanto ogni ideale j si può moltiplicare per un altro ideale J così che il prodotto sia un ideale principale[35] (n).
Def.[inizione] Un ideale j_1 dicesi divisibile[36] per j_2 se esiste un ideale j_3 tale che $j_1 = j_2 j_3$.
// Se j_1 è divisibile per j_2 ed j_2 per j, allora j_1 è divisibile per j.
Un intero n si dice divisibile per un ideale j, se l'ideale principale (n) è divisibile per j.
Un ideale j si dice divisibile per l'intero n, se j è divisibile per (n).
Notiamo che l'intero n è divisibile per un altro intero m, soltanto quando (n) è divisibile per (m).
Le tre ideali j_1, j_2, j_3 sono legate dalla $j_1 j_2 = j_1 j_3$ (e se j_1 non coincide con l'ideale zero) allora[37] $j_2 = j_3$. Infatti, se J è un ideale è tale che j_1 sia un ideale principale (n), ne segue:

$$J j_1 j_2 = J j_1 j_3 \quad \text{cioè} \quad (n) j_2 = (n) j_3.$$

Ora $(n)j_2$ è l'ideale formato dai prodotti di n per un numero di j_2; i quali si potrebbero tutti ottenere anche moltiplicando n per un numero di j_3. Perciò ogni numero di j_2 è anche numero di j_3 e viceversa.

c.d.d.

Sia j_1 un ideale contenuto nell'ideale j_2. Sia J un ideale tale che $j_2 J$ ia principale; e sia $j_2 J = (n)$. Evidentemente $j_1 J$ sarà contenuto in $j_2 J = (n)$. Ogni numero di $j_1 J$, sarà pertanto divisibile per n; i quo//zienti ottenuti dividendo i numeri di $j_1 J$ per n formeranno un ideale j_3. E sarà:

$$j_1 J = (n) j_3 = j_2 J j_3;$$

donde per il teorema precedente:

$$j_1 = j_2 j_3.$$

L'ideale j_1 che è uguale al prodotto di j_2 per un altro ideale j_3, è pertanto divisibile per j_2. Perciò[38]: un ideale j_1, contenuto in un altro ideale j_2, è divisibile per j_2. Il teorema reciproco è evidente. Se j_1 ed j_2 sono ideali principali (n_1) ed (n_2), il primo è contenuto nel secondo soltanto se n_1 è multiplo di n_2; in questo caso il teorema precedente è dunque senz'altro evidente.
Dunque gli ideali principali (n) divisibili per j sono tutti e soli quelli generati dai numeri n, che appartengono ad (j). La norma di ogni intero n di j è un intero razionale divisibile per n, e quindi anche per j.

---

[34] *e.c.* e *cor. sup.*: individuano.
[35] *Idem*, cap. II, §25, p. 162, prop. A). Cfr. anche Gazzaniga, 1903, cap. XII, p. 389, prop. 19). Cfr. infine Hilbert 1897 (trad. 1911), cap. II, §5, p. 16, teor. 8.
[36] *Idem*, cap. II, §26, p. 168: "Diciamo che un ideale A è divisibile per l'ideale B, o che B è un divisore di A, quando A può risolversi nel prodotto di B per un terzo ideale C". Cfr. anche Gazzaniga 1903, cap. XII, p. 392: "A divisibile per B se esiste un ideale Q che moltiplicato per B dà un ideale uguale ad A". Cfr. inoltre Hilbert 1897 (trad. 1911), cap. II, §4, p. 15: "un idéal ***c*** est dit divisible par l'idéal ***a***, s'il existe un idéal ***b*** tel que ***c*** = ***ab***". Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §9, p. 38; qui l'autore aggiunge: "Les concepts de la multiplication et de la division des nombres entiers peuvent s'étendre aux idéaux, les corps d'addition et de soustraction ne peuvent être généralisés".
[37] *Idem*, cap. II, §25, p. 165, prop. a). Cfr. anche Hilbert 1911, cap. II, §5, p. 17, teor. 9.
[38] *Idem*, cap. II, §26, p. 168.

L'ideale (1) formato da tutti gli interi del corpo coincide coi suoi divisori. Infatti un divisore di (1), dovendo contenere (1), che coincide col corpo da noi studiato, non può che coincidere col corpo stesso. //

Un ideale j ha un numero finito di divisori[39] j'. Infatti, se a è un numero di j e ne è n la norma, allora $|n|$ è contenuto in (a), il quale è contenuto in (j), che è a sua volta contenuto in j'. Pertanto ogni j' contiene il numero n.

Se $\gamma_1, \gamma_2, \gamma_3$ è una base di[40] j, sarà[41]

$$\gamma_i = p_{i1}\omega_1 + p_{12}\omega_2 + p_{i3}\omega_3$$

Con p_{ik} interi razionali, se $\omega_1, \omega_2, \omega_3$ è una base del corpo.

L'ideale j' si potrà pensare definito dai numeri γ_i, e, a maggior ragione, dai quattro numeri $\gamma_1, \gamma_2, \gamma_3, |n|$.

Se q_{ik} ed r_{ik} sono quoziente e resto ottenuti dividendo p_{ik} per $|n|$ (cosicché $0 \leq r_{ik} < |n|$, è[42] $\gamma_i = n(q_{i1}\omega_1 + q_{i2}\omega_2 + q_{i3}\omega_3) + \delta_i$, ove

$\delta_i = r_{i1}\omega_1 + r_{i2}\omega_2 + r_{i3}\omega_3)$.

Per il solo fatto che j' contiene n e quindi anche i suoi multipli, si può affermare che j' contiene i numeri $n(q_{i1}\omega_1 + q_{i2}\omega_2 + q_{i3}\omega_3)$.

Dunque[43] j sarà definito, se inoltre si conoscono gli interi razionali r_{ik}; i quali non essendo negativi, e non potendo superare $|n|$, possono avere al più un numero finito di valori.

c.d.d.

// Un ideale divisibile soltanto per se stesso e per (1) dicesi primo[44]. Dai teoremi precedenti segue tosto l'esistenza di ideali primi.

L'ideale (1), che è l'unico avente per norma 1, e che coincide col corpo, tiene luogo delle unità nelle aritmetiche solite.

Teor.[ema] ***fondamentale***: Un ideale primo p che divida il prodotto ab di due ideali a, b divide almeno uno dei fattori[45].

[46]Sia a non divisibile per p. Sia q l'ideale definito dai numeri di a e da quelli di p, e dalle somme di un numero di a e di un numero di p. Questo ideale contiene sia a che p. Dunque a e p sono divisibili per q; ma poiché a non è divisibile per p, sarà $p \neq q$; poiché p è il[47] primo, sarà $q = (1)$. Cioè il numero 1 fa parte di q ed è perciò somma[48] di un numero α di a e di un numero π di p.

$$1 = \alpha + \pi.$$

Moltiplicando per un numero β di b, se ne trae:

---

[39] *Idem*, cap. II, §26, p. 171, prop. C). Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §169, p. 503, prop. 6. Cfr. infine Hilbert 1897 (trad. 1911), cap. II, §4, p. 15, lemma 1.

[40] *e.c.* e *cor. sup.*: j'.

[41] *e.c.* e *cor. sup.*: invece di $p_{12}\omega_2$ leggasi $p_{i2}\omega_2$.

[42] *e.c.* e *cor. sup.*: $\gamma_i = |n|(\dots)$,

[43] *e.c.* e *cor. sup.*: j'.

[44] Bianchi 1920-21, cap II, §26, p. 169, def. β). Cfr. anche Gazzaniga 1903, cap XII, p. 394. Cfr. inoltre Dirichlet 1877 (trad. 1881), suppl. XI, §171, p. 504. Cfr. infine Hilbert 1897 (trad. 1911), cap. II, §4, p. 15.

[45] *Idem*, cap II, §26, p. 173, prop. F). Cfr. anche Gazzaniga 1903, cap XII, p. 395, prop. 33) e Hilbert 1897 (trad. 1911), cap. II, §5, p. 17, teor. 11. Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §13, p. 57.

[46] *Idem*, cap. II, §26, p. 173-175. La dimostrazione di Bianchi è identica a quella qui svolta da Fubini sia per la notazione sia per il procedimento.

[47] *del.*: il.

[48] Dirichlet 1877 (trad. 1881), suppl. XI, §171, p. 505.

$$\beta = \alpha\beta + \pi\beta.$$

Poiché $\alpha\beta$ è divisibile per ab e quindi anche per p; e poiché π è divisibile per p, se ne trae che β // è divisibile per p. Cioè ogni numero di b è divisibile per p ossia è contenuto in p . Dunque b è contenuto in p, e quindi è divisibile per p.
Se ne deduce poi, come in aritmetica elementare:
Ogni ideale è decomponibile in uno e in un solo modo nel prodotto di ideali primi[49].

§.5 *Teoria di Kronecker – Hilbert*

Nella teoria di Kronecker[50] dare un corpo equivale a dare un'equazione algebrica $g(z) = 0$ a coefficienti interi, il cui primo coefficiente si può supporre uguale ad 1.
Gli interi del corpo non sono che i polinomi della z a coefficienti interi, quando si considerino uguali due tali polinomi congrui tra di loro $(mod\ g(z))$. Ad ogni polinomio P in z si può pertanto sostituire il polinomio di grado $n-1$, che si ottiene come resto quando si divida P per $g(z)$.
La perfetta identità coi nostri risultati segue da ciò che, se z_1 è quella radice della $g(z) = 0$ che individua il nostro corpo, ogni intero del corpo individua uno e un solo polinomio di grado $n-1$; il quale, quando a z si sostituisca // la radice z_1, diventa uguale al nostro intero. E viceversa. I polinomi di grado $> n-1$ danno gli stessi interi che i polinomi di grado $n-1$ ad essi congrui $[mod\ g(z)]$.
Siano $\omega_1, \omega_2, \dots, \omega_r$ r interi del corpo; consideriamo un qualsiasi polinomio F in una o più variabili $u, v, w, \dots$, di cui le ω siano i coefficienti. Tali polinomi (che Kronecker chiama forme[51], anche se non sono omogenei) sono da Kronecker sostituiti agli ideali. Vale a dire Kronecker aggiunge agli interi del corpo degli altri enti: le forme (polinomi i cui coefficienti sono interi del corpo). Una forma con un solo coefficiente dicesi principale.
Vediamo il legame tra il metodo di Kronecker, e i precedenti.
Diremo con Hilbert[52] contenuto di una forma l'ideale generato dai suoi coefficienti. Viceversa un ideale $(\alpha_1, \alpha_2, \dots, \alpha_r)$ è il contenuto di ogni forma, che abbia le α come coefficienti.
Teor.[ema] **fondamentale**[53]. Il contenuto del prodotto FF' di due forme F, F' è uguale al prodotto dei contenuti delle F, F'.

---

[49] Bianchi 1920-21, cap. II, §26, p. 176, Teorema principale. Cfr. anche Gazzaniga 1903, cap XII, p. 395, prop. 34). Cfr. inoltre Dirichlet 1877 (trad. 1881), suppl. XI, §173, p. 514 prop. 4; Dedekind qui scrive che "ogni ideale […] od è un ideale primo, oppure può essere rappresentato, e ciò in un modo soltanto, qual prodotto di ideali primi". Cfr. Hilbert 1897 (trad. 1911), cap. II, §5, p. 16, teor. 7; l'autore, dopo aver enunciato questo teorema nella forma "Tout idéal ***i*** peut être décomposé en un produit d'idéaux premieres et il ne peut l'être que d'une seule manière", afferma che "Dedekind a donné récentement une nouvelle exposition de sa démostration. La démonstration de Kronecker repose sur la théorie (créée par lui) des formes algébriques appartenant à un corps. La signification de cette théorie se comprend mieux, si l'on établit d'abord les théoremes de la théorie des idéaux". Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §13, p. 58.
[50] Tale teoria è esposta in modo organico dal matematico tedesco all'interno dei *Grundzilge einer arithmetischen Theorie der algebraischen Grössen* (1882).
[51] Dirichlet 1877 (trad. 1881), suppl. XI, §176, p. 531. Dedekind, a differenza di Fubini, non affronta nel dettaglio questi argomenti; scrive solamente che "la teoria degli ideali di un corpo Ω sta in immediata connessione con la teoria delle forme decomponibili, che corrispondono al medesimo corpo; noi ci ristringeremo in ciò ad accennare questa dipendenza nelle sue linee fondamentali".
[52] Hilbert 1897 (trad. 1911), cap. II, §6, p. 19: "chaque forme de coefficients $\alpha_1, \dots, \alpha_r$ fornit un idéal $\boldsymbol{a} = (\alpha_1, \dots, \alpha_r)$. C'est cet idéal que l'on nomme *contenu* de la forme F."
[53] *Ibid.*, teor. 13; l'enunciato coincide con quello di Fubini: "Le contenu du produit de deux formes est égal au produit de leurs contenus".

[54]Infatti sia p^a la massima potenza dell'ideale // primo p, che divide l'ideale contenuto di F, sia p^b la massima potenza di p che divide il contenuto di F'. Disponiamo le variabili $u, v, ...$, da cui dipendano F, F' in un certo ordine, e ordiniamo i termini di F. Di due termini scriviamo prima quello che contiene la massima potenza della prima variabile u; se i due termini contenessero la stessa potenza di u, scriviamo prima quello che contiene la massima potenza della seconda variabile v; se i due termini contenessero anche la stessa potenza di v, scriviamo prima quello che contiene la massima potenza di w; e così via.
Altrettanto facciamo per F'. Dei termini di F ve ne sarà uno almeno, il cui coefficiente è divisibile soltanto per[55] p non per una potenza superiore; sia T il primo di questi termini: sia T' il primo termine di F' divisibile per p^b, e non per una potenza superiore. Allora nel prodotto FF' i termini simili a TT' (cioè che ne differiscono al più per il coefficiente, e non per le potenze di $u, v, ...$, che vi figurano) si ottengono moltiplicando un termine // di F che precede T per un termine di F' che segue T', oppure un termine di F che segue T per un termine di F' che precede T'. Ora i coefficienti dei termini che precedono T o T' sono rispettivamente divisibili per una potenza di p di esponente superiore ad $\underline{a}$, oppure a $\underline{b}$; gli altri coefficienti di F (od F') sono <u>almeno</u> divisibili per p^a, o per p^b.
Quindi: Il coefficiente di TT' è divisibile per p^{a+b}; e non per una potenza di p ad esponente maggiore; i termini simili sono divisibili per una potenza superiore di p. Il termine di FF', che si ottiene riducendo ad un solo termine TT' e i termini simili, ha pertanto un coefficiente divisibile per p^{a+b}, e non per una potenza superiore. I coefficienti degli altri termini di FF' sono divisibili almeno per p^{a+b}. Dunque coefficienti di FF' danno un ideale divisibile proprio per p^{a+b}.
Ripetendo questo ragionamento per tutti gli ideali primi che sono fattori del contenuto di F o di F', si dimostra il teorema enunciato.
Se F è una <u>forma</u>, il prodotto di essa e delle coniugate sarà un polinomio f a coefficienti interi razionali[56]. //
Pertanto $\frac{f}{F} = \varphi$, prodotto delle forme <u>coniugate</u> di f, sarà una forma del nostro corpo algebrico (perché i coefficienti si ottengono da quelli di f, che sono interi razionali e da quelli di F, che sono interi del corpo con operazioni razionali). Il M.C.D. dei coefficienti di f è un <u>intero razionale</u> (che sceglieremo <u>positivo</u>), e che diremo <u>norma</u>[57] della F. (In tale intero, nel caso di una forma F di 1° grado, ci siamo già incontrati al §4). Se questa <u>norma</u> è 1, il contenuto di $F\varphi$ vale (1); perciò il contenuto di[58] F_1 che deve essere un divisore di (1) coincide con (1). La forma F si dice in tal caso [che cioè il suo contenuto è (1)] una forma unità.
<u>Una forma di norma 1 è pertanto una forma unità</u>[59].
Le forme F, G abbiano lo stesso contenuto j. Sia J un ideale tale che $jJ = (n)$, dove $\underline{n}$ è un intero razionale (cfr. §4). Sia H una forma, di cui J è il contenuto. Allora

---

[54] *Ibid.* La dimostrazione qui proposta da Fubini ripercorre abbastanza nel dettaglio quella di Hilbert; quest'ultimo utilizza però la forma G al posto della forma F' e pone $H=GF$.
[55] *e.c.* e *cor. sup.*: p^a.
[56] Nota inserita da Fubini a p.d.p.: *Disp. 17 Teoria dei numeri*.
[57] Hilbert 1897 (trad. 1911), cap. II, §6, p. 18: "prenons-la sous forme $nU(u, v, ...)$, où n est un entier rationnel et U une fonction entière rationelle, dont les coefficients sont des entiers rationnels sans diviseur commun, n s'appelle la *norme de la forme* F".
[58] *e.c.* e *cor. sup.*: F.
[59] *Ibid.* Hilbert scrive: "Lorsque la norme n est égale à 1, la forme se nomme une *forme unité*".

$$\frac{F}{G} = \frac{FH}{GH}.$$

Le forme FH, GH hanno entrambe per contenuto (n). Quindi $\frac{1}{n}FH, \frac{1}{n}GH$ sono due forme unità, // che indicheremo con L, M. E sarà $\frac{F}{G} = \frac{L}{M}$.
Viceversa, se L, M sono forme unità, e se vale questa uguaglianza, allora $FM = GL$. Il contenuto di F, che coincide con quello di FM [perché M ha il contenuto (1)], è uguale al contenuto di GL; il quale [poiché L ha per contenuto (1)] coincide con quello di G. Dunque due forme hanno lo stesso contenuto (e si riguardano nella teoria di Kronecker come equivalenti), soltanto quando il loro rapporto è uguale al rapporto di due forme unità. Esse in particolare avranno norme uguali[60].
Sia $\alpha_1, \alpha_2, \alpha_3$ una base di un ideale j; e sia $\omega_1, \omega_2, \omega_3$ una base del corpo. Sarà

$$\alpha_i \omega_r = \sum_s c_{irs} \alpha_s \qquad (i, r, s = 1,2,3)$$

con c_{irs} interi razionali.
Se λ è un intero

$$\lambda = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 \quad (x_i \text{ interi razionali})$$

dell'ideale j, sarà

$$\lambda \omega_r = \sum_{i,s} c_{irs} x_i \alpha_s.$$

Cioè, posto

$$\alpha_s = \textstyle\sum_t a_{st} \omega_t \qquad (a_{st} \text{ interi razionali})$$

Sarà //

$$\lambda \omega_r = \sum_t \omega_t \sum_s a_{st} \sum_i c_{irs} x_i = \sum_t \omega_t \sum_s a_{st} x_{rs},$$

ove è posto

$$x_{rs} = \sum_i c_{irs} x_i.$$

Eliminando le ω, se ne deduce un'equazione di terzo grado in λ, col coefficiente di λ^3 uguale a ± 1, e col termine noto (che varrà $\pm \lambda \lambda' \lambda''$) uguale, tutt'al più a meno del segno, al determinante delle $\sum_s a_{st} x_{rs}$ cioè al prodotto del determinante delle a_{st} per il determinante delle x_{rs}. Noi ammettiamo che quest'ultimo sia una forma primitiva (ciò che dimostriamo al venturo paragrafo). E ne deduciamo che il M.C.D. dei coefficienti di $\sum_s a_{st} x_{rs}$, cioè di $\lambda \lambda' \lambda''$ (prodotto della forma $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$ per le coniugate) vale precisamente $|a_{st}|$, che è la norma dell'ideale $(\alpha_1 \alpha_2 \alpha_3)$, contenuto della forma $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$. Ma tale M.C.D. è il contenuto di questa forma. Dunque:
La norma di una forma è uguale alla norma del suo contenuto (cioè dell'ideale corrispondente). Veramente noi lo abbiamo provato soltanto per la forma $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$; ma il risultato è ge//nerale, perché le forme di ugual contenuto hanno, come abbiamo dimostrato, uguali norme. La teoria delle forme di Kronecker[61] e delle loro norme è dunque completamente equivalente alla teoria degli ideali e loro norme.

[60] *Ibid.* L'autore scrive: "Deux forms sont dites *équivalentes* […] lorsque leur quotient est égal au quotient de deux forms unites" e, in nota, aggiunge "Kronecker emploie l'expression «équivalente au sens restreint»".
[61] Cfr. Kronecker 1882, cap. II, §17; il matematico tedesco introduce l'equivalenza tra forme all'interno della sezione intitolata *Die allgemeinen algebraischen Divisoren; ihre aequivalenz mit den besonderen, welche aus Linearformen gebildet sind*.

Si raggiunge cioè l'analogia con l'aritmetica elementare, aggiungendo al corpo o gli ideali di Dedekind, o le forme di Kronecker, e considerando equivalenti due forme, il cui rapporto sia uguale a quello di due forme unità.
Il teorema sul contenuto del prodotto di due forme diventa nell'aritmetica ordinaria equivalente al solito teorema di Gauss dato al §2 del Cap. I pag. 10 e già ricordato in fine del §3 di questo capitolo.
Oss.[ervazione] $\mathbf{1^a}$. Il teorema che ci siamo riservati di trovare al seg. §6, è:
Il quoziente ottenuto dividendo un intero generico di j per la norma di j la norma di un intero $\lambda = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$ è una forma primitiva delle x_1, x_2, x_3.
Oss.[ervazione] $\mathbf{2^a}$. Notiamo che nella teoria di Kronecker la norma di una forma si deduce dal prodotto della forma stessa e delle coniugate, così come // avviene per i numeri del corpo.
Oss.[ervazione] $\mathbf{3^a}$. Deduciamo anche il teorema, che dimostriamo nei seguenti paragrafi per via diretta. Poiché la norma del prodotto di due forme è evidentemente uguale al prodotto delle norme, poiché la norma di una forma è uguale alla norma dell'ideale suo contenuto, poiché infine il contenuto del prodotto di due forme è uguale al prodotto dei contenuti, segue che:
La norma del prodotto di due ideali è uguale al prodotto delle norme[62].

§.6 *Generalizzazioni aritmetiche varie (M.C.D. di più* N^i *od id; id primi tra loro)*

Dunque il M.C.D. di più interi $a_1, a_2, \dots, a_n$ è l'ideale $(a_1, a_2, \dots, a_n)$. Esso si può ottenere anche così.
Si decompongono nel prodotto di ideali primi gli ideali principali $(a_1), (a_2), \dots, (a_n)$.
Il M.C.D. [63] citato si ottiene moltiplicando tra di loro i fattori primi comuni a queste decomposizioni, ciascuna col minimo degli esponenti che esso ha in tali prodotti.
Questa regola non vale soltanto per il M.C.D. di // più interi, o dei corrispondenti ideali principali, ma anche per il M.C.D. di n ideali qualsiasi $j_i = (a_{i1}, a_{i2}, \dots, a_{ir_i})$ $(i = 1,2, \dots, n)$.
Tale M.C.D. è l'ideale minimo che contiene tutti gli ideali dati[64]: cioè è l'ideale determinato da tutti i numeri a_{ik} $(k = 1,2, \dots, t_i;\ i = 1,2, \dots, n)$; in altre parole è l'ideale luogo dei numeri che sono somma di un numero di j_1, di un numero di j_2, ecc., di un numero di j_n.
Il lettore definisca in modo simile il minimo comune multiplo.
Più ideali j_i $(i = 1, 2, \dots, n)$ sono primi tra di loro, quando il loro M.C.D. coincide con (1), cioè col corpo completo. In tal caso ogni intero del corpo, e in particolare il numero 1 è somma di un numero di j_1, di un numero di j_2, ..., di un numero di j_n. Viceversa, se 1 gode di questa proprietà, l'ideale M.C.D. degli j contiene 1, e quindi anche ogni altro intero, e perciò coincide con (1). Gli ideali sono primi tra di loro. Il lettore ricordi la proprietà corrispondente di più interi primi tra di loro.
Agli ideali si può estendere la teoria delle con//gruenze di primo grado[65]. Come primo esempio studiamo il sistema di congruenze

---

[62] Gazzaniga 1903, cap. XII, p. 393. Gazzaniga enuncia tale proprietà nel caso meno generale delle "norme assolute". Cfr. anche Hilbert 1897 (trad. 1911), cap. II, §7, p. 21, teor. 21. Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §11, p. 48: "La norme du produit de deux idéaux est égale au produit des normes".
[63] *Idem*, cap. XII, p. 387.
[64] Bianchi 1920-21, cap. II, §27, p. 178.
[65] Sommer 1907 (trad. 1911), cap. 2, §11, p. 45-48. Il matematico tedesco dedica l'intero paragrafo *Les congruences suivant les idéaux* a tale argomento.

(1) $$\begin{cases} x \equiv a_1 \ (mod\ j_1) \\ x \equiv a_2 \ (mod\ j_2) \ldots\ldots \\ x \equiv a_n \ (mod\ j_n) \end{cases}$$
(cioè $x - a_i$ è un intero di j_i)

essendo gli j_i primi tra di loro.
Posto

$$j = j_1 j_2 \ldots j_n$$
$$j = j_1 J_1;\ j = j_2 J_2\ ; \ldots;\ j = j_n J_n,$$

anche gli ideali $J_1, J_2, \ldots, J_n$ sono primi tra di loro. Potrò pertanto in J_i trovare un intero b_i, così che:

(2) $$b_1 + b_2 + \cdots + b_n = 1.$$

Poniamo

$$x = b_1 a_1 + b_2 a_2 + \cdots + b_n a_n.$$

Dico che questa x soddisfa alla (1).
Infatti b_i è contenuto in J_i, è pertanto divisibile per J_i; cosicché $b_2, b_3, \ldots, b_n$ sono divisibili tutti per j_1 (perché $J_2, J_3, \ldots J_n$ risultando dal prodotto di j_1 per altri ideali). Quindi dalla (2) segue $b_1 \equiv 1 \ (mod\ j_1)$ e quindi

$$x \equiv a_1 \ (mod\ j_1).$$

Nello stesso modo si prova che x soddisfa alle altre equazioni (1). //
Ogni altra soluzione y della (1) soddisfa alle

$$x \equiv y \ (mod\ j_i) \quad per \ \ i = 1, 2, \ldots, n.$$

Essendo gli j_i primi tra loro, sarà anche

$$x \equiv y \ (mod\ j_1 j_2 \ldots j_n).$$

Perciò la nostra soluzione è determinata, a meno di un addendo divisibile per[66] $j_1\, j_2 \ldots j_n$.
Il lettore noti la completa analogia col caso elementare.
Lemma. Se j è un ideale divisibile per un altro ideale J, esiste un intero η, tale che J sia M.C.D. di j e di (η).
Sia $J = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, dove i p sono ideali primi distinti.
Sia x_i un numero contenuto in $p_i^{e_i}$, e non in $p_i^{e_i+1}$.
Siano $k_1, k_2, \ldots, k_s$ gli ideali primi distinti tra loro e dai p, per cui j sia eventualmente divisibile.
Per il teorema precedente esiste un intero η tale che

$$\eta \equiv x_1 \left(mod\ p_1^{e_1+1}\right);\ \eta \equiv x_2 \left(mod\ p_2^{e_2+1}\right); \ldots;\ \eta \equiv x_r \left(mod\ p_r^{e_r+1}\right)$$

ed in più eventualmente[67] alle

$$\eta \equiv 1 \ (mod\ k_1);\ \eta \equiv 1 \ (mod\ k_2); \ldots;\ \eta \equiv 1 \ (mod\ k_s).$$

// Un tale η è divisibile per $p_i^{e_i}$ e non per $p_i^{e_i+1}$; e non è divisibile per gli eventuali k_l.
Dunque η soddisfa le condizioni volute.
Siano J, K due ideali qualsiasi; posto nel lemma precedente $j = JK$, ne deduciamo che esiste un numero η tale che J sia M.C.D. di j e di (η). Se $\eta = J J_1$, allora J_1 sarà primo con K.

[66] Bianchi 1920-21, cap. II, §28, p. 182, prop. A).
[67] *lapsus* del curatore: leggasi "soddisfa alle".

Dunque:
Dati due ideali qualsiasi J, K, si può trovare un ideale J_1 primo con K tale che il prodotto JJ_1 sia principale[68].
Sia J un ideale qualunque; sia n un numero di J. Allora (n) è divisibile per J. Dunque per il lemma si può trovare un intero η, tale che J sia M.C.D. di (n) e di (η). Dunque:
Ogni ideale J è M.C.D.[69] di due interi n, η.
Dunque l'aggiunta degli ideali equivale alla aggiunta di tali M.C.D., o, se si vuole usare la terminologia, a cui si giunge seguendo Kronecker[70] un corpo algebrico si completa (cioè diventa un corpo, per cui vale l'algoritmo del M.C.D.), aggiungendo le forme $nx + \eta y$, (essendo n, η interi qualsiasi del corpo). //
Insomma si tratta di aggiungere agli interi del corpo la coppia di interi (n, η) avvertendo che si scrive $(n, \eta) = (n_1, \eta_1)$ se n ed η sono somme di multipli di n_1 e di η_1 e viceversa se n_1 ed η_1 sono somme di multipli di n, η.
Quanta semplicità in questa concezione!
Vediamo dunque che si può anche enunciare così la differenza tra l'aritmetica elementare e quella di un campo algebrico.
Se $a_1, a_2, \dots, a_n$ sono n interi fissi , $x_1, x_2, \dots, x_n$ interi variabili, i numeri

$$(1) \qquad a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

sono nell'aritmetica elementare (e in ogni aritmetica in cui valga l'algoritmo del M.C.D.) tutti e soli i multipli

$$(2) \qquad pz$$

del M.C.D. p dei numeri $a_1, a_2, \dots, a_n$. Cosicché si può ridurre la forma (1) alla (2) dove p indica ancora un intero fisso (determinato a meno di un fattore unità) e la z un intero variabile nel modo più arbitrario entro il corpo studiato.
Invece in un corpo algebrico la (1) non si può sem//pre ridurre al tipo (2); e, quando non si può ridurre al tipo (2), essa si può ridurre alla forma

$$(2bis) \qquad p_1z_1 + p_2z_2,$$

dove p_1, p_2 sono interi fissi, z_1, z_2 interi del nostro corpo affatto arbitrari. I numeri p_1, p_2 sono due interi qualsiasi soddisfacenti alla sola condizione di avere l'ideale $(a_1, a_2, \dots, a_n)$ come M.C.D.; essi si possono scegliere in infiniti modi, perché p es. p_1 (sopra indicato con n) si può scegliere ad arbitrio tra gli interi dell'ideale $(a_1, a_2, \dots, a_n)$.
Siano b, c due ideali; sia a un ideale primo con c tale che ba sia un ideale principale (η). Se x descrive un sistema di $Nm\, b$ numeri incongrui $(mod\ b)$ ed y un sistema di $Nm\, c$ numeri incongrui $(mod\ c)$ allora

$$\eta y + x$$

descrive un sistema completo di numeri incongrui $(mod\ bc)$.
Infatti, se la coppia $x'\ y'$ è distinta dalla coppia $x\ y$ non può essere

[68] Bianchi 1920-21, cap. II, §28, p. 186, prop. C). Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §174, p. 523, prop. 6.
[69] Dirichlet 1877 (trad. 1881), suppl. XI, §173, p. 523, prop. 7; Dedekind enuncia qui la seguente proprietà più generale: "Ogni ideale può esser rappresentato in innumerevoli guise come massimo comun divisore di ideali principali".
[70] Kronecker 1882, cap. II.

$$\eta y + x = \eta y' + x' \pmod{bc}.$$

Infatti, essendo $\eta \equiv 0 \pmod{b}$ ne seguirebbe // $x \equiv x' \pmod{b}$ e pertanto $x = x'$.
Allora la

$$\eta y \equiv \eta y' \pmod{bc}$$

dà che $\eta(y - y')$ è divisibile per bc, e quindi $\frac{\eta}{b}(y - y')$ divisibile per c. Poiché $\frac{\eta}{b} = a$ è primo con c, ne seguirebbe $y \equiv y' \pmod{c}$ e perciò $y = y'$ contro l'ipotesi fatta.
D'altra parte un intero qualsiasi ω del corpo è congruo con uno e un solo degli $x \pmod{b}$; sia $\omega \equiv x_1 \pmod{b}$. Allora $\omega - x_1$ è un numero β di b. Essendo a, c primi tra loro posso trovare un numero α di a, un numero γ di c così che $\alpha + \gamma = 1$ e quindi che $\beta\alpha + \beta\gamma = \beta$. Poiché β è divisibile per b, γ per c, il numero $\beta\gamma$ è divisibile per bc; cioè $\beta \equiv \beta\alpha \pmod{bc}$. Ma per ragioni analoghe $\beta\alpha$ è divisibile per $ba = \eta$. E quindi esiste un intero n tale che $\beta\alpha = n\eta$. Se y_1 è quello degli y, che è $\pmod{c}$ congruo con $\underline{n}$, sarà

$$\beta \equiv \eta y_1 \pmod{bc}$$

cioè

$$\omega = x_1 + \beta \equiv x_1 + \eta y_1 \pmod{bc}.$$

E pertanto $\eta y + x$ descrive un sistema com//pleto di $Nm\, b\, Nm\, c$ numeri incongrui $\pmod{bc}$. Ma un tale sistema di numeri è formato di $Nm\,(bc)$ numeri. Ecco dunque dimostrato direttamente che:
La norma del prodotto di due o più ideali è uguale al prodotto delle norme[71].
Sia p un ideale primo; allora $Nm\, p$ è un intero razionale divisibile per p.
Sia P il minimo intero razionale positivo divisibile per P. Allora P è primo, perché se fosse $P = QR$ con Q, R interi razionali positivi minori di P, allora p dividerebbe uno almeno dei Q, R, entrambi i minori di P: ciò che è assurdo.
Sia $P = pp_1$. Prendendo le norme, supposto il corpo di grado $\underline{n}$, si trova $P^n = Nm\, p\, Nm\, p_1$. Dunque $Nm\, p$ divide P^n, dove P è primo. Perciò

$$Nm\, p = P^f \quad (\text{con } f \leq \underline{n}).$$

L'intero f si chiama il grado[72] di p.
La norma di p è la f^{esima} potenza di un primo razionale P, dove f (grado di p) non supera il grado del corpo.
Dimostriamo ora il teorema ammesso al §5. //
Se λ è un intero dell'ideale j, allora λ è divisibile per j; ed è pertanto $\lambda = jj_1$, dove j_1 è un altro ideale.
Dunque $Nm\, \lambda = Nm\, j\, Nm\, j_1$.
Ma j_1 è uno qualsiasi degli ideali che, moltiplicati per j, danno un prodotto che è un ideale principale (λ). Dunque per i risultati di questo paragrafo, si può scegliere j_1 primo con un ideale K prefissato a piacere.

[71] Bianchi 1920-21, cap. II, §28, p. 184; §29, p. 188. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §173, p. 504, prop. 7. Cfr. infine Hilbert 1897 (trad. 1911), cap. III, §7, p. 21, teor. 18 e Sommer 1907 (trad. 1911), cap. 2, §11, p. 48.
[72] Dirichlet 1877 (trad. 1881), suppl. XI, §171, p. 507, prop. 10.

Allora $\frac{Nm\,\lambda}{Nm\,j} = Nm\,j_1$ deve essere un polinomio primitivo nelle x (ricordo che si è posto al §5) $\lambda = x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3$). Perché, se così non fosse, i suoi coefficienti sarebbero tutti divisibili almeno per un intero primo razionale p. E ciò è assurdo. Infatti, in tal caso $Nm\,j$ sarebbe sempre divisibile per p. Ora j_1 si può scegliere primo con p. Basterà dunque provare: Se un ideale j_1 è primo con p (essendo p un primo razionale), allora $Nm\,j_1$ non è divisibile per p.
Infatti, se $j_1 = q_1 q_2 \dots q_r$ (dove i q sono ideali primi distinti o no), allora //

$$Nm\,j_1 = Nm\,q_1\,Nm\,q_2 \dots Nm\,q_r.$$

Ora

$$Nm\,q_i = Q_i^{f_i} \quad (i = 1,2,\dots,r)$$

dove Q_i è il minimo intero positivo primo razionale divisibile per q_i.
Se $Nm\,j_1$ fosse divisibile per p, almeno uno dei numeri Q_i coinciderebbe con p. Cioè p sarebbe divisibile per q_i (perché $p = Q_i$, e Q_i è divisibile per q_i); e quindi p ed j_1 non sarebbero primi tra loro, avendo essi il divisore comune q_i: ciò che è assurdo.
È così completamente dimostrato il nostro teorema.

§.7 *Generalizzazione della funzione* φ *e del teorema di Fermat*

Ideali primi

Ricordiamo dal §6 che, se le x descrivono un sistema completo di numeri incongrui $(mod\ b)$ e le y descrivono un sistema analogo $(mod\ c)$, si può determinare un intero η tale che i $Nm\,(bc)$ numeri

$$(1) \qquad \eta y + x \qquad [\eta \text{ divisibile per } b]$$

descrivano un sistema completo analogo[73] $(mod\ bc)$. // Solo quelli tra essi, per cui $x \equiv 0\ (mod\ b)$, sono divisibili per b. Cioè tra essi vi sono precisamente $Nm\,c = \frac{Nm\,(cb)}{Nm\,b}$ interi divisibili per b. Posto $bc = d$, ne deduciamo:
Se b è un divisore dell'ideale d, vi sono tra gli (1) $\frac{Nm\,d}{Nm\,b}$ interi divisibili per b; e perciò vi sono proprio $Nm\,d - \frac{Nm\,d}{Nm\,b} = Nm\,d\left(1 - \frac{1}{Nm\,b}\right)$ interi incongrui $(mod\ d)$ non divisibili per il divisore b di d.
Si possono ora generalizzare molti teoremi di aritmetica; diamo qui alcuni enunciati lasciando la dimostrazione al lettore.
Molti di essi riguardano la generalizzazione della funzione $\varphi(n)$, di cui ci siamo occupati nelle prime lezioni.
Se $p_1, p_2, \dots, p_r$ sono i fattori primi distinti di un ideale j allora[74]

$$\varphi(j) = Nm\,j\left(1 - \frac{1}{Nm\,p_1}\right)\left(1 - \frac{1}{Nm\,p_2}\right)\dots\left(1 - \frac{1}{Nm\,p_r}\right)$$

[73] Bianchi 1920-21, cap. II, §29, p. 188, 189.
[74] *Idem*, cap. II, §30, p. 197. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §174, p. 520, prop. 3. Cfr. infine Hilbert 1897 (trad. 1911), cap. III, §8, p. 23, teor. 23 e Sommer 1907 (trad. 1911), cap. 2, §17, p. 85.

è il numero degli interi di un sistema completo di numeri incongrui $(mod\ j)$ e primi con j. Se b divide a, allora $\varphi\left(\frac{a}{b}\right)$ è il numero degli interi di un sistema completo di numeri incongrui $(mod\ a)$ e che con a hanno b per M.C.D.[75] //

(Teor. [ema] ***di Fermat).*** Per ogni intero x primo con l'ideale a vale la $x^{\varphi(a)} \equiv 1\ (mod\ a)$. Una congruenza in una sola incognita x se di grado r rispetto a un ideale primo ha al più r radici[76].

Se p è un ideale primo di grado f (cioè se $Nm\ p = P^f$ dove P è primo razionale) allora $\varphi(p) = P^f - 1$; ogni intero x non divisibile per p soddisfa alla

$$x^{P^f-1} - 1 \equiv 0\ (mod\ p).$$

Degli interi primi con p ne esistono proprio $\varphi(P^f - 1)$ incongrui, che non soddisfano ad alcuna congruenza $x^t \equiv 1\ (mod\ p)$ con $t < P^f - 1$ (cfr. per le dimostrazioni di teoremi analoghi per gli interi razionali) e che si diranno primitivi[77] $(mod\ p)$. Se z è uno di essi, ogni intero n primo con p è $(mod\ p)$ congruo con una potenza z^m di z; l'esponente un intero razionale si dirà l'indice[78] di n e sarà completamente determinato $(mod\ P^f - 1)$ (cioè a meno di un multiplo di $P^f - 1$). Ecco così generalizzata la teoria degli indici, che può trarre con sé la generalizzazione, di cui non ci occupiamo, di altri teoremi. // Tale numero z non soddisfa ad alcuna congruenza del tipo $z^t - 1 \equiv 0\ (mod\ p)$ con $t < P^f - 1$, ma può bensì soddisfare ad altre congruenze $B(z) \equiv 0$ a coefficienti interi razionali $(mod\ p)$.

Sia f' il grado minimo di tali congruenze (È $f' \leq P^f - 1$, perché tra tali congruenze vi è la $z^{P^f-1} - 1 \equiv 0$). Il coefficiente di $z^{f'}$ in $B(z)$ è[79] $\equiv 0\ (mod\ P)$ perché altrimenti esso sarebbe $\equiv 0\ (mod\ p)$, e $B(z) \equiv 0\ (mod\ p)$ si ridurrebbe ad una congruenza di grado $\leq f' - 1$; ciò che è assurdo.

Potremo dunque moltiplicare $B(z)$ per un tale numero positivo che il coefficiente di $z^{f'}$ valga 1. Allora, scelto ad arbitrio l'intero $n \not\equiv 0\ (mod\ p)$, supposto m uguale al suo indice, si divida z^m per $B(z)$. Il quoziente $Q(z)$ e il resto $R(z)$ [di grado $\leq f' - 1$] avranno per coefficienti interi razionali; poiché $z^m = B(z)Q(z) + R(z)$, poiché $n \equiv z^m$ e $B(z) \equiv 0\ (mod\ p)$, sarà $n \equiv R(z)\ (mod\ p)$.

Cioè ogni intero n del corpo è congruo $(mod\ p)$ ad un polinomio a coefficienti interi razionali di grado $f' - 1$.

Veramente finora si era supposto n non divisibile per p; ma il teorema è vero anche se // $n \equiv 0\ (mod\ p)$. In tal caso basta scegliere il polinomio, i cui coefficienti sono tutti nulli.

Ma un polinomio di grado $f' - 1$ ha f' coefficienti interi razionali. Quanti interi razionali distinti vi sono, se consideriamo come identici due interi razionali c, d tali che $c \equiv d\ (mod\ p)$ ossia che $c - d$ sia divisibile per p? Se $c - d$ è divisibile per p, allora l'intero razionale $c - d$ è divisibile per P. (Infatti $c - d$ e P sono entrambi divisibili per p; altrettanto avviene del loro M.C.D., il quale deve essere un divisore di P, e perciò coincide con P, perché nessun intero minore di P è divisibile per p). Dunque vi sono tanti interi

[75] Nota inserita da Fubini a p.d.p.: *Disp. 18 Teoria dei numeri*.
[76] Bianchi 1920-21, cap. II, §30, p. 198. Dirichlet 1877 (trad. 1881), suppl. XI, §174, p. 524. Cfr. infine Hilbert, 1897 (trad. 1911) cap. III, §8, p. 23, teor. 24 e Sommer 1907 (trad. 1911), cap. 2, §18, p. 86.
[77] *Idem*, cap. II, §31, p. 202.
[78] *Ibid*. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. V, §129, p. 331.
[79] *e.c.* e *cor. sup.*: non è $\equiv 0$.

razionali incongrui $(mod\ p)$, quanti ve ne sono $(mod\ P)$; cioè ve ne sono proprio P. Ognuno degli f' coefficienti del nostro polinomio ha dunque $(mod\ p)$ proprio P valori distinti.
Se noi diamo certi valori interi razionali di coefficienti del polinomio $R(z)$ di grado $f'-1$ e poi diamo altri valori, che non siano $(mod\ p)$ ordinatamente congrui ai precedenti, il nostro polinomio avrà due valori R, R' che non // possono essere tra loro congrui $(mod\ p)$. Perché altrimenti la $R \equiv R'(mod\ p)$ sarebbe una congruenza di grado minore di f', a cui soddisfa la z. Dunque $R(z)$ assume $P^{f'}$ valori incongrui $(mod\ p)$; ma, poiché, come dicemmo, esso può assumere tutti i $Nm\ p = P^f$ valori possibili $(mod\ p)$, ne viene che $f = f'$. Dunque: Il grado f di un ideale primo è uguale al grado minimo di una congruenza a coefficienti razionali, a cui può soddisfare un numero primitivo z secondo p. Ogni intero del corpo è $(mod\ p)$ congruo a uno e un solo polinomio di grado $f-1$ in z a coefficienti razionali.
Qui ci accontentiamo di queste prime conseguenze del teorema di Fermat; nel paragrafo 9 ne dedurremo un metodo per la ricerca degli ideali primi.

§.8 ***Classi di ideali***[80]

Lemma[81]. In ogni ideale j esiste almeno un intero non nullo ξ tale che

$$Nm\ \xi < \rho\sqrt{|d|}\ Nm\ j,$$

dove d è il discriminante del corpo, ρ è un fatto//re numerico che dipende soltanto dal corpo (e che se si tratta per esempio di un corpo di 3° grado reale coi coniugati, vale[82] $\frac{2}{q}$).
Infatti, supposto per esempio il corpo di 3° grado reale coi coniugati, indicata con $\alpha_1, \alpha_2, \alpha_3$ una base di j, un intero ξ qualsiasi di j e gli interi coniugati ξ', ξ'' sono dati dalle:

$$\left.\begin{aligned} \xi &= \alpha_1 x + \alpha_2 y + \alpha_3 z \\ \xi' &= \alpha'_1 x + \alpha'_2 y + \alpha'_3 z \\ \xi'' &= \alpha''_1 x + \alpha''_2 y + \alpha''_3 z. \end{aligned}\right\} \quad (x, y, z \text{ interi razionali})$$

Il determinante di queste forme vale in valore assoluto $\sqrt{d}\ Nm\ j$; e pertanto, per i teoremi di Minkowsky[83], si possono trovare interi x, y, z non tutti nulli tali che[84]

$$|\xi\xi'\xi''| < \rho\sqrt{|d|}\ Nm\ j.$$

(Notiamo che per un corpo reale insieme ai coniugati si può porre in ogni caso $\rho = 1$, perché con valori interi razionali non tutti nulli delle x, y, z si possono rendere ξ, ξ', ξ'' non maggiori di 1 in valore assoluto, e una almeno minore di 1).
Vogliamo orientarci nell'insieme dei nuovi en//ti introdotti: gli ideali. Cominciamo ad osservare che se, moltiplicando gli interi di un ideale *j* per un fratto $\frac{\mu}{\nu}$, otteniamo numeri interi,

---

[80] Hilbert 1897 (trad. 1911), cap. VII, p. 51-62; l'intero capitolo VII, dal significativo titolo *Les classes d'idéaux des corps*, è dedicato a tale argomento.
[81] *Idem*, cap. VI, §18, teor. 46: "Soit $\boldsymbol{a}$ un idéal donné du corps k, il y a toujours un numbre x du corps différent de o divisible par $\boldsymbol{a}$ et tel que $|n(\alpha)| \leq |n(\boldsymbol{a})\sqrt{d}|$". Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §16, p. 77.
[82] *e.c.* e *cor. inf.*: $\frac{2}{9}$.
[83] *lapsus* del curatore: leggasi "Minkowski".
[84] Bianchi 1920-21, cap. II, §33, p. 218-220. Bianchi enuncia qui un lemma leggermente differente, ma equivalente a quello di Fubini.

questi formano a loro volta un altro ideale j_1, che naturalmente indicheremo col simbolo $j_1 = \frac{\mu}{\nu} j$, in quanto che è appunto $\nu j_1 = \mu j$.
E l'introduzione del solo ideale j porta con sé l'introduzione di j_1; cosicché, introdotto l'ente j, resta quasi introdotto nella teoria anche l'ente j_1 come prodotto di j per $\frac{\mu}{\nu}$ (così come nell'algebra l'introduzione di $i = \sqrt{-1}$ trae con sé l'introduzione di tutti i numeri complessi).
Noi diremo pertanto che $j \sim j_1$ (che leggiamo: j equivalente[85] ad j_1). È evidente che[86]:
Se $j \sim j_1$ ed $j_1 \sim j_2$, anche $j \sim j_2$.
Dalle ipotesi segue infatti l'esistenza di 4 interi λ, μ, l, m tali che:

$$lj = mj_1; \quad \lambda j_1 = \mu j_2;$$

donde:

$$(l\lambda)j = (m\mu)j_2$$

cioè

$$j \sim j_2.$$

Due ideali j, j_1 equivalenti hanno evidentemente // le basi proporzionali[87] (perché si passa da una base di j ad una base di j_1, moltiplicandole per $\frac{\mu}{\nu}$). E viceversa.
Se J è un ideale tale che jJ è principale, e se $j_1 \sim j$, anche $j_1 J$ è principale[88]. Infatti se $\mu j = \nu j$ e se $jJ = (l)$ con l'intero[89], sarà $\mu l = \nu j_1 J$.
Quindi $j_1 J$ sarà l'ideale principale $\left(\frac{\mu l}{\nu}\right)$.
Il teorema reciproco si prova nello stesso modo.
Dunque:
Se j_1 moltiplicato per j dà per prodotto un ideale principale, gli ideali equivalenti ad j sono tutti e solo quelli che moltiplicati per j_1, danno per prodotto un ideale principale. Gli ideali equivalenti ad (1) sono tutti e soli gli ideali principali.
Tutti gli ideali equivalenti ad un ideale j e quindi anche equivalenti tra loro si considereranno appartenenti ad una stessa classe[90] (contenente l'ideale j). Questa classe è completamente determinata da un suo ideale (per esempio da j).
Siano A, B due classi di ideali. Moltiplichiamo // un ideale qualsiasi j di A per un ideale qualsiasi k di B. Io dico che i prodotti k appartengono ad una stessa classe.
Infatti, se $j \sim j_1$ e se $k \sim k_1$, esistono 4 interi λ, μ, l, m tali che $\mu j = \nu j_1; mk = nk_1$. Sarà pertanto $(m\mu)jk = (n\nu)k_1 j_1$ cioè $jk \sim j_1 k_1$.

---

[85] *Idem*, cap. II, §33, p. 222. Bianchi definisce l'equivalenza tra ideali in modo del tutto equivalente a Fubini; scrive infatti "Due ideali A, B si dicono equivalenti quando hanno uno, e quindi tutti i moltiplicatori comuni". Cfr. anche Gazzaniga 1903, cap. XII, p. 396: "Due ideali non principali $A'\,A''$ si diranno equivalenti tra loro se esiste in $R(\theta)$ un ideale F tale che: $A'F$ ed $A''F$ siano ideali principali". Cfr. infine Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 525 e Sommer 1907 (trad. 1911), cap. 2, §16, p. 75.
[86] Sommer 1907 (trad. 1911), cap. 2, §16, p. 75, prop. 1.
[87] Bianchi 1920-21, cap. II, §33, p. 222. Bianchi scrive "Due ideali A, B sono equivalenti se hanno basi proporzionali".
[88] Sommer 1907 (trad. 1911), cap. 2, §16, p. 75, prop. 3.
[89] *e.c.* e *cor. sup.*: invece di "con l'intero" leggasi "con l intero".
[90] Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 525; qui Dedekind scrive "A è anche l'insieme di tutti gli ideali equivalenti ad A'. Un sistema così fatto A di ideali lo chiameremo una classe di ideali od anche più brevemente classe, chè già uno scambio con classi di numeri non è qui da temere; ogni classe A è compiutamente determinate mediante un ideale a qualunque contenuto in essa, epperciò codesto ideale lo si può guardare come rappresentante dell'intera classe A."

La classe dei prodotti jk si chiamerà la classe[91] $AB = BA$ prodotto delle classi A, B.
Se A è una classe di ideali, B un'altra classe, se un ideale di A moltiplicato per un ideale di B ha per prodotto un ideale principale, allora anche il prodotto di un qualsiasi ideale di A per un qualsiasi ideale di B è principale. La classe degli ideali principali si chiama la classe principale[92] e si indica con 1; e ciò perché ogni classe A moltiplicata per la principale dà A per prodotto.
Due classi A, B dotate della proprietà testé citata soddisfano dunque alla $AB = BA = 1$; perciò si pone $B = A^{-1}$ $(A = B^{-1})$; e le due classi A, B si dicono reciproche l'una dell'altra. Si pone per $AA = A^2, AAA = A^3$, ecc., $(A^{-1})^n = A^{-n}$; vale il teorema $A^n A^m = A^{m+n}$ per m, n interi ra//zionali.
***Teorema**:* In ogni classe A di ideali vi è un ideale di norma $< \sqrt{|d|}$, se d è il discriminante del corpo[93].
Infatti in un ideale j_1 della classe A^{-1} esiste un intero z la cui norma è in valore assoluto minore di $\rho\, Nm\, j_1 \sqrt{|d|}$. Perciò

$$\frac{|Nm\, z|}{Nm\, j_1} < \rho\sqrt{|d|}.$$

Ora z è contenuto in j_1 e quindi è divisibile per j_1. Dunque $z = jj_1$, dove j è un ideale di A. Ora $Nm\, j$ vale appunto

$$\frac{Nm\, |z|}{Nm\, j_1} < \rho\sqrt{d}.$$

Essendo ρ una costante, che in ogni caso si può assumere uguale ad 1, ma che si può anche scegliere minore di 1, segue l'asserto.
I numeri interi razionali positivi $n < \sqrt{|d|}$ sono in numero finito; un ideale che abbia per norma n contiene n, è perciò un divisore di n.
Ma gli ideali divisori di un intero n sono in numero finito. Pertanto gli ideali di norma // minore di $\sqrt{|d|}$ sono in numero finito; poiché ogni classe contiene almeno uno di questi ideali ed è da questo suo ideale completamente determinata, segue che:
Le classi di ideali di un corpo dato sono in numero finito[94] h.
Se $h = 1$, vi è una sola classe: la classe principale; e ogni ideale è principale (come nella aritmetica elementare).
Supponiamo $h \neq 1$; e sia A una classe qualsiasi.

---

[91] *Idem*, cap. II, §33, p. 224. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 526. Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §16, p. 76: "Tous les idéaux équivalents à un idéal donnée forment une classe d'idéaux":
[92] *Idem*, cap. II, §33, p. 224. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §16, p. 76: "Tous les idéaux principaux sont équivalents à l'idéal (1) et forment ensemble la *classe principale*".
[93] *Idem*, cap. II, §33, p. 224, 225. Le dimostrazioni di Fubini e di Bianchi sono analoghe. Negli *Elementi della teoria dei numeri*, 1903, Cap. XII, p. 397, Gazzaniga fornisce un enunciato più generale, ma equivalente. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 527; qui Dedekind enuncia e dimostra il "teorema fondamentale: In ogni classe di ideali M vi è almeno un ideale m, la cui norma non supera la costante s, e per conseguenza il numero delle classi di ideali è finito". Cfr. inoltre Hilbert 1897 (trad. 1911), cap. VII, §22, p. 52, teor. 50: "il y a dans tout classe d'idéaux un idéal dont la norme est inférieure à la valeur absolue de la racine carrée du discriminant du corps [Minkowski]". Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §16, p. 76.
[94] Bianchi 1920-21, cap. II, §33, p. 225, prop. A); Gazzaniga 1903, cap. XII, p. 397; l'autore afferma che questa proprietà segue direttamente dal fatto che è finito il numero dei rappresentanti di tali classi di ideali. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 526. Cfr. inoltre Hilbert 1897 (trad. 1911), cap. VII, §22, teor. 50: "Le nombres des classes d'idéaux du corps de nombres est fini [Dedekind, Kronecker]". Cfr. Infine Sommer 1907 (trad. 1911), cap. 2, §16, p. 76.

Le classi $A, A^2, A^3, A^4, \ldots$ non possono essere tutte distinte, perché le classi sono in numero finito.
Ve ne saranno pertanto due A^r, A^s con $s > r$ uguali; e sarà allora $A^{s-r} = 1$ con $s - r$ intero razionale positivo.
Sia g il minimo intero razionale positivo tale che $A^g = 1$.
Evidentemente le classi $A, A^2, \ldots, A^g$ sono tutte distinte; ed ogni potenza di A è uguale ad una ed una sola di esse.
Se non vi è alcun'altra classe, è $g = h$; se vi è // un'altra classe B, le classi

$$BA, BA^2, BA^3, \ldots, BA^g$$

sono distinte tra loro e dalle precedenti.
Infatti se $BA^r = A^s$ allora B sarebbe, contro l'ipotesi, una potenza di A; e d'altra parte, se fosse
$BA^r = BA^s$ con $0 < r < s \leq g$, sarebbe $A^r = A^s$ contro il supposto.
Se non vi sono altre classi, sarà $h = 2g$; se ve ne è una terza C, le classi $CA, CA^2, \ldots, CA^g$ sono distinte tra loro e dalle precedenti. E così via.
In ogni caso si trova che h è multiplo di g, cioè che $\frac{h}{g}$ è intero, cosicché

$$A^h = (A^g)^{\frac{h}{g}} = 1^{\frac{h}{g}} = 1.$$

Cioè ogni classe A è tale che A^h è principale[95]. In altre parole ogni ideale j è tale che j^h è principale; cioè j^h è formato dai multipli di un intero a.
La $\sqrt[h]{a}$ è pure un intero algebrico (perché le radici di un intero sono interi), ma non appartiene generalmente al corpo studiato, ma bensì a un corpo più ampio, entro cui il corpo iniziale è contenuto (è un sottocorpo). //
Io dico che:
I numeri di j non sono che quelli tra i numeri del nostro corpo, che sono multipli di $\sqrt[h]{a}$.
Infatti, se μ è un numero del corpo iniziale tale che $\frac{\mu}{\sqrt[h]{a}} =$ intero, anche $\frac{\mu^h}{a}$ è intero, cioè μ^h è multiplo di a, cioè μ^h è un numero di j^h, cioè è divisibile per j^h. Col metodo della decomposizione in fattori primi si dimostra allora che μ è divisibile per j, cioè è contenuto in j. Viceversa, se μ è contenuto in j, allora μ^h è contenuto in j^h, cioè è divisibile per j^h; pertanto μ^h è multiplo di a.
Dunque $\frac{\mu^h}{a}$ è intero; e quindi $\frac{\mu}{\sqrt[h]{a}}$ è intero.
Dunque la considerazione degli ideali di un corpo equivale a considerare alcuni interi di un certo corpo più ampio.
Siano γ, β due interi algebrici qualsiasi; sia K un corpo che li contiene entrambi; sia j lo ideale M.C.D. di[96] α, β in K. Sarà:

$$\gamma = jJ \qquad \beta = jJ'$$

Con J, J' ideali primi tra loro.
Sia h il numero delle classi in K.

[95] Dirichlet 1877 (trad. 1881), suppl. XI, §175, p. 528.
[96] *e.c.* e *cor. sup.*: γ, β.

Sarà $j^h = l,\ J^h = L, J'^h = L'$ con l, L, L' interi di K, ed // L, L' primi tra di loro. E dalle formole precedenti si trae

$$\gamma^h = lL, \qquad \beta^h = lL'.$$

Ora, essendo L, L' primi tra loro, esistono in K due interi x, y cosicché $Lx + L'y = 1$. E pertanto sarà

$$x\gamma^h + y\beta^h = l \text{ ove } l = j^h.$$

I numeri di j sono gli interi di K divisibili per $\sqrt[h]{l}$, dunque, essendo β, γ divisibili per j, gli interi β e γ sono divisibili per $\sqrt[h]{l}$, perciò

$$c = \frac{\gamma}{\sqrt[h]{l}} \text{ e } b = \frac{\beta}{\sqrt[h]{l}} \text{ sono interi.}$$

La nostra uguaglianza diventa

$$(xc^{h-1})\gamma + (yb^{h-1})\beta = \sqrt[h]{l}.$$

Essendo xc^{h-1} ed yb^{h-1} interi, segue che un <u>qualsiasi</u> intero, divisore comune di β e di γ, è anche divisore di $\sqrt[h]{l}$ [il quale è come sappiamo, divisore tanto di β che di γ]. Dunque $\sqrt[h]{l}$ (che è un intero in generale non appartenente a K) compie l'ufficio di M.C.D. degli interi β, γ. Dunque:

<u>Due interi algebrici qualsiasi β, γ hanno un</u> // M.C.D.; <u>il quale però in generale non appartiene al corpo definito dai numeri β, γ.</u>

Ogni ideale j di un corpo dato K è M.C.D. di due inter i α, β del corpo.

Se ad α, β sostituiamo numeri interi α', β' proporzionali (cosicché $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$), l'ideale j, viene mutato in un ideale j' equivalente. Dunque, se mutiamo la frazione $\frac{\alpha}{\beta}$ in una frazione uguale, l'ideale (α, β) viene mutato in un ideale equivalente; cioè <u>una frazione $\frac{\alpha}{\beta}$ individua una classe di ideali</u>.

<u>Quando mai due frazioni $\frac{\alpha}{\beta}$ ed $\frac{\alpha'}{\beta'}$ distinte individuano la stessa classe di ideali</u>?

Dovendo essere gli ideali (α, β) ed (α', β') equivalenti, esisteranno due interi ρ, σ tali che gli ideali $(\rho\alpha, \rho\beta)$ e $(\sigma\alpha', \sigma\beta')$ coincidano.

Si potranno pertanto trovare nel corpo degli interi x, y tali che

$$\rho\alpha = x(\sigma\alpha') + y(\sigma\beta') \qquad (1)$$

e degli interi u, v tali che

$$\rho\beta = u(\sigma\alpha') + v(\sigma\beta'). \qquad (2)$$

// Viceversa, poiché $\sigma\alpha'$ e $\sigma\beta'$ devono entrambi esser somma di un multiplo di $\rho\alpha$ e di un multiplo di $\rho\beta$, le equazioni

$$\sigma\alpha' = \frac{v(\rho\alpha) - y(\rho\beta)}{xv - yu} \qquad \sigma\beta' = \frac{-u(\rho\alpha) + x(\rho\beta)}{xv - yu}$$

devono essere a coefficienti interi; da cui segue facilmente che $xv - yu$ deve essere una unità. Dividendo (1) per (2) si ha dunque:

$$(3) \qquad \frac{\alpha}{\beta} = \frac{x\left(\frac{\alpha'}{\beta'}\right) + y}{u\left(\frac{\alpha'}{\beta'}\right) + v}$$

x, y, u, v interi tali che $xv - yu =$ una unità.
Viceversa, se vale la (3), esistono due interi ρ, σ tali che valgano le $(1), (2)$; e gli ideali (α, β) ed (α', β') sono equivalenti.
Ora la (3) è sulle frazioni del corpo una trasformazione, che a buon diritto potremo chiamare modulare, perché essa è la più naturale generalizzazione delle trasformazioni modulari dell'aritmetica nel campo assoluto di razionalità.
Studiare le classi di ideali equivale dunque a studiare le frazioni del corpo quando si considerino equivalenti due frazioni trasformate// l'una dell'altra con una trasformazione modulare.

§.9 ***Ideali primi***[97]

Sia p un ideale primo[98]

$$Nm\, p = P^f \quad (P \text{ intero primo razionale})^{99}.$$

Una radice primitiva λ soddisfa, come vedemmo al paragrafo 7, a una congruenza $g(\lambda) \equiv 0\ (mod\ p)$ a coefficienti interi razionali di grado minimo f. Gli interi razionali divisibili per p sono tutti e soli i multipli di P. Ogni intero del corpo è congruo ad uno ed un solo polinomio di grado $f - 1$ in λ a coefficienti interi razionali. Al numero λ si può sostituire un numero qualunque (del corpo) λ' tale che $\lambda' \equiv \lambda\ (mod\ p)$. Se π è divisibile per p, ma non per p^2, allora

$$g(\lambda + \pi) \equiv g(\lambda) + \pi g'(\lambda)\ (mod\ p^2).$$

Dunque o $g(\lambda)$ oppure $g(\lambda + \pi)$ non è divisibile per p^2, mentre entrambi sono divisibili per p. (Basta osservare che π è divisibile per p, ma non per p^2, e che $g'(\lambda) \not\equiv 0\ (mod\ p)$, perché altrimenti λ soddisferebbe alla congruenza[100] // $g'(\lambda) \equiv 0\ (mod\ p)$ di grado $f - 1 < f$)[101].
Indicheremo con λ quello dei numeri $\lambda, \lambda + \pi$ che soddisfa alle $g(\lambda) \equiv 0 (mod\ p)$, $g(\lambda) \not\equiv 0\ (mod\ p^2)$. P è divisibile per p. Poniamo[102] $P = p$ e j, dove j è primo con p. Sia a un numero di j primo con p. Sia $t = \varphi(p^2)$. Per il teorema di Fermat generalizzato

$$a^t \equiv 1\ (mod\ p^2), \qquad \lambda \equiv \lambda a^t\ (mod\ p^2).$$

Pongo $z = \lambda a^t$, e

$$g(\lambda) = a_0\lambda^f + a_1\lambda^{f-1} + a_2\lambda^{f-2} + \cdots . + a_{f-1}\lambda + a_f.$$

Il numero a_f è discongruo da zero $(mod\ p)$, perché altrimenti λ soddisferebbe alla $\frac{g(\lambda)}{\lambda} \equiv 0\ (mod\ p)$ di grado $f - 1 < f$. Il numero zero[103] è congruo a $\lambda\ (mod\ p^2)$ (cosicché anche $z \equiv \lambda\ [mod\ p]$); esso soddisfa pure pertanto alla $g(z) \equiv 0\ (mod\ p)$. Ma, poiché z e

[97] Gli argomenti trattati in questo paragrafo (come anche nei due successivi, che sono uno sviluppo di questo) non sono presenti, se non per brevi cenni, né nelle opere di Bianchi, *Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica* e *Lezioni sulla Teoria aritmetica delle forme quadratiche binarie e ternarie,* né in quella di Gazzaniga *Gli elementi della teoria dei numeri.* Si può quindi pensare che siano, almeno in parte, un contributo originale di Fubini, sviluppato proprio a partire dalle considerazioni "preliminari" di Bianchi e di Gazzaniga sugli ideali primi e dagli studi di matrice tedesca sulla teoria degli ideali e delle forme.
[98] Bianchi 1920-21, cap. II, §29, p. 193.
[99] Gazzaniga 1903, cap. XII, p. 395: "La norma di A è uguale a una potenza int. e pos. di p."
[100] Nota inserita da Fubini a p.d.p.: *Teoria dei numeri Disp. 19.*
[101] La parentesi tonda è stata da noi aggiunta.
[102] *e.c.* e *cor. sup.*: $P = p^e j$.
[103] *e.c.* e *cor. sup.*: zeta.

le sue potenze sono divisibili per j, tutti i termini, eccettuato l'ultimo, di $g(z)$ sono divisibili per j. L'ultimo termine a_f non può essere divisibile per alcun fattore primo q di j. Se così non fosse, essendo P divisibile per j e quindi anche per q, il M.C.D. di P e di a_f sarebbe divisibile per q.
Ora a_f e P sono interi razionali; e il loro M.C.D.// sarebbe un intero razionale. E, poiché P è primo, tale M.C.D. coincide con 1 o con P.
Nel secondo caso a sarebbe divisibile per P e quindi anche per p: ciò che abbiamo provato assurdo. Il M.C.D. di a_f e di P sarebbe pertanto 1. E quindi q sarebbe un divisore di 1, cioè $q = 1$, contro l'ipotesi.
Dunque

$$g(z) \equiv a_f \not\equiv 0 \ [mod\ q],$$

dove q è un qualsiasi divisore distinto da 1 dell'ideale j.
Inoltre è

$$g(z) \equiv 0\ (mod\ p), \qquad g(z) \not\equiv 0\ (mod\ p^2).$$

Dunque $g(z)$ e P hanno p per M.C.D. In altre parole l'ideale p è l'ideale $(g(z), P)$.
E sarebbe risoluto il problema di trovare gli ideali primi p divisori di un primo razionale P, se per ognuno di essi sapessimo trovare l'intero z, ed il polinomio $g(z)$. Noi supereremo questa difficoltà mediante alcuni artifici.
Lemma 1°: Una congruenza $g(x) \equiv 0\ (mod\ p)$ a coefficienti interi razionali, che ammetta // la radice z, ammette anche le radici[104]

$$z;\ \ z^P;\ \ (z^P)^P = z^{P^2};\ \ \left(z^{P^2}\right)^P = z^P; \ldots; z^{P^{f-1}}$$

[si ricordi che per il teorema di Fermat generalizzato è $z^{P^f} \equiv z\ (mod\ p)$].
Infatti[105] $[g(x)]$ è, per il teorema del binomio o polinomio di Newton, un polinomio che è formato
α) da termini ottenuti innalzando alla P^{esima} potenza i termini di $g(z)$;
β) da altri termini tutti i divisibili per P.
Se $a_s x^s$ è un termine di $g(x)$, allora $a_s^P x^{sP}$ è uno dei termini (α). Ora[106] $a_s^p \equiv \mathcal{A}_s\ (mod\ P)$ per l'ordinario teorema di Fermat.
Poiché i termini (β) sono nulli $(mod\ P)$, e poiché $a_s x^{sP}$ si deduce da $a_s x^s$, sostituendo x^P al posto di x, se ne deduce che identicamente

$$[g(x)]^P \equiv g(x^p)\ \ (mod\ P)$$

e quindi anche rispetto ad un qualsiasi multiplo che sia divisore di P. Dunque

$$g(z^P) \equiv [g(z)]^P \equiv 0\ \ (mod\ p).$$

La $g(x) \equiv 0\ (mod\ p)$, oltre ad una radice z, possiede la radice z^P. Insieme alla z^P possiede la $(z^P)^P = z^{P^2}$, ecc. ecc. //
Dunque la $g(x) \equiv 0$ di cui avevamo discorso poco sopra possiede le f radici

---

[104] *e.c.* e *cor. sup.*: invece di $\left(z^{P^2}\right)^P = z^P$ leggasi $\left(z^{P^2}\right)^P = z^{P^3}$.
[105] *e.c.* e *cor. sup.*: $[g(x)]^P$.
[106] *e.c.* e *cor. sup.*: $a_s^p \equiv a_s\ (mod\ P)$.

$$z, z^P, z^{P^2}, \dots, z^{P^{f-1}}.$$

Quindi, essendo $g(x)$ di grado f, e p un ideale primo

$$g(x) \equiv (x-z)(x-z^P)\left(x-z^{P^2}\right)\dots\left(x-z^{P^{f-1}}\right) \ (mod\ p).$$

Ogni intero del corpo θ_1 è $(mod\ p)$ congruo con un polinomio $\theta(z)$ di grado $f-1$ a coefficienti razionali.
Porremo

$$\theta_2 = \theta(z^P);\quad \theta_3 = \theta\left(z^{P^2}\right);\dots;\quad \theta_f = \theta\left(z^{P^{f-1}}\right).$$

Poiché le funzioni elementari simmetriche di tali potenze z, z^P, z^{P^2}, ecc. della z si possono esprimere $(mod\ p)$ razionalmente mediante i coefficienti di $g(z)$, che sono interi razionali, i numeri $\theta_1, \theta_2, \dots, \theta_f$ sono radici di una congruenza a coefficienti interi razionali di grado $f\ (mod\ p)$, che indicheremo con

$$\Pi(\bar{x}) \equiv 0\ (mod\ p).$$

Se poniamo $\theta_1 = u_1\omega_1 + u_2\omega_2 + \dots + u_n\omega_n$ dove le ω sono una base del corpo, supposto di grado n, e dove lasciamo <u>indeterminati</u> gli interi razionali <u>u</u>, allora Π sarà un polinomio // in x con coefficienti che sono polinomi a coefficienti interi razionali nelle u. Noi indicheremo tale polinomio col simbolo[107]

$$\Pi(x, u_1, u_2, \dots, u_n).$$

<u>Sia</u>[108] <u>$Q(x, u_1, u_2, \dots, u_n) \equiv 0\ (mod\ p)$ una congruenza coefficienti razionali soddisfatta da $x = \theta_1$</u>. Allora tale congruenza, essendo soddisfatta da $x = \theta(z)$, e pure soddisfatta da $x \equiv \theta(z^P), x \equiv \theta\left(z^{P^2}\right)$, ..., cioè ammette tutte le radici di $\Pi(x) \equiv 0\ (mod\ p)$.
Dividendo Q per Π avremo per resto un polinomio (a coefficienti interi razionali, come Q e π) di grado $f-1$, il quale pure uguagliato a zero $(mod\ p)$ dovrebbe avere le f radici $\theta_1, \theta_2, \dots, \theta_f$.
Poiché p è primo ed $f > f-1$, ciò può avvenire soltanto se tale resto è nullo.
Dunque Q è divisibile per Π.
Cioè: <u>Se $Q(z, u_1, \dots, u_n) \equiv 0\ (mod\ p)$ è una congruenza coefficienti interi razionali θ soddisfatta per $x = \theta_1$, allora Q è divisibile per Π</u>.
E potremo scrivere[109] //

$$Q = [\Pi(x, u_1, u_2, \dots, u_n)]^a H(x, u_1, u_2, \dots, u_n)$$

Dove Π^a è la massima potenza di Π, per cui Q è divisibile, e dove H definisce una congruenza a coefficienti interi razionali $H \equiv 0\ (mod\ p)$, che <u>non è più soddisfatta</u> per $x = \theta_1$.
La $H(\theta_1, u_1, \dots, u_n)$ è un polinomio delle u, i cui termini noi ordineremo nel modo già esposto a proposito della teoria di Kronecker; tali coefficienti non possono essere tutti divisibili per p (perché $H \equiv 0\ (mod\ p)$ non è soddisfatta da $x = \theta_1$). Sia T il primo termine di $H(\theta_1, u_1, \dots, u_n)$, il cui coefficiente <u>non</u> è divisibile per p. Ora $\Pi(\theta_1, u_1, u_2, \dots, u_n)$ non può

[107] Nell'originale leggasi $\Pi(x; u_1, u_2, \dots, u_n)$.
[108] Nell'originale leggasi $Q(x; u_1, u_2, \dots, u_n) \equiv 0\ (mod\ p)$.
[109] La parentesi tonda è stata da noi aggiunta.

essere sempre divisibile per p^2, perché quando le u sono scelte in modo che $\theta_1 = z$, allora la congruenza $\Pi(x) \equiv 0\ (mod\ p)$ si riduce alla congruenza $g(x) \equiv 0\ (mod\ p)$, che è soddisfatta per $x = z$, mentre la $g(x) \equiv 0\ (mod\ p^2)$ non è soddisfatta per $x = z$. I coefficienti di $\Pi(\theta_1, u_1, \dots, u_n)$ non possono pertanto essere tutti divisibili per p^2.
Sia T' il primo termine di Π, il cui coefficiente non è divisibile per p^2, ma è al più divisi//bile per p. Tra i termini di Q vi è il termine ottenuto riducendo TT' con gli eventuali termini simili ottenuti sviluppando il prodotto $\Pi^a H$. Come nel caso incontrato nella teoria di Kronecker, si vede che il coefficiente di TT' non è divisibile per una potenza di p superiore a p^a, mentre i termini simili sono divisibili per una potenza superiore.
Dunque $Q = \Pi^a H$ ha, quando si ponga $x = \theta_1$, i coefficienti divisibili al più per p^a.
Se dunque $Q(\theta_1, u_1, u_2, \dots, u_n)$ non solo è congruo a zero $(mod\ p)$, ma è congruo a zero $(mod\ p^e)$; allora Q è almeno $(mod\ p)$ divisibile per π^e (ammesso come sopra che Q sia a coefficienti interi razionali).
L'intero $\theta = \omega_1 u_1 + \dots + \omega_n u_n$ soddisfa ad una equazione algebrica di n^{esimo} grado a coefficienti interi razionali, col primo coefficiente uguale ad 1; equazione che possiamo scrivere

$$F(x) = (x - \theta)(x - \theta')(x - \theta'') \dots (x - \theta^{(n-1)})$$

se $\theta',\ \theta'', \dots, \theta^{n-1}$ sono gli interi coniugati di θ.
La $F(x) = 0$ include la $F(x) \equiv 0\ (mod\ P)$, e quindi // anche se p^e è la massima potenza di p che divide $P, F(x) \equiv 0\ (mod\ p^e)$. Pertanto dal teorema precedente si trae

$$F(x) \equiv [\Pi(x)]^e H(x)\ \ (mod\ p^e).$$

Siano $p_1, p_2, \dots, p_r$ gli ideali primi distinti fattori di P.
Sarà:

$$P = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}.$$

E se f_i è il grado di p_i, ne deduciamo, prendendo le norme:

$$n = e_1 f_1 + e_2 f_2 + \dots + e_r f_r.$$

Sarà[110]

$$F(x) \equiv [\Pi_1(x)]^{l_1} H_1\ \ (mod\ p_1^{e_1})$$

ove Π_1 è un polinomio a coefficienti interi razionali.
Ora $\Pi_1(x)$, quando x è un intero generico, è divisibile per p_1, ma non è divisibile né per p_2, né per p_3, ..., né per p_r (come risulta ponendo, per esempio, $x = z$, nel qual caso Π_1 si riduce a $g(z)$).
Ma, poiché in ogni caso $F(x) \equiv 0\ (mod\ p_2^{e_2})$ se ne deduce che H_1 sarà divisibile per un polinomio $\Pi_2(x, u_1, u_2, \dots, u_n)$ a coefficienti interi razionali, // ed anzi per[111] $\Pi_2^{e_2}\ (mod\ p_2)$.
Così continuando se ne trae:

$$F(x) \equiv [\Pi_1(x)]^{e_1} [\Pi_2(x)]^{e_2} \dots [\Pi_r(x)]^{e_r} h(x)\ \ (mod\ P)$$

[110] *e.c.* e *cor. sup.*: $F(x) \equiv [\pi_1(x)]^{e_1} H_1\ \left(mod\ p_1^{e_1}\right)$.
[111] *e.c.* e *cor. sup.*: invece di $(mod\ p_2)$ leggasi $\left(mod\ p_2^{e_2}\right)$.

dove Π_i è di grado f_i ed è a coefficienti interi razionali. Osservando che $F(x)$ è di grado n, e che $\Pi_1^{e_1}\Pi_2^{e_2}\ldots\Pi_r^{e_r}$ è di grado $e_1f_1+e_2f_2+\cdots+e_rf_r=n$, se ne deduce che $h(x)=cost.$, e che perciò

$$F(x)\equiv[\Pi_1(x)]^{e_1}[\Pi_2(x)]^{e_2}\ldots[\Pi_r(x)]^{e_r}\ (mod\ P).$$

Decomporre un primo razionale P in ideali primi equivale a decomporre in fattori il primo membro $F(x)$ dell'equazione fondamentale $F(x)=0$, a cui soddisfa l'intero generico $\theta=u_1\omega_1+u_2\omega_2+\cdots+u_n\omega_n$ del corpo (insieme agli interi coniugati).
L'ideale p_i appare poi come M.C.D. di P e di $\Pi_i(\theta)$.
Dunque al numero primitivo z incognito abbiamo sostituito l'intero generico θ; al polinomio $g(z)$ uno dei fattori Π a coefficienti interi razionali in cui si può $(mod\ P)$ decomporre $F(x)$. //

§.10 ***Applicazione dei precedenti risultati***

(Il primo teorema di questo paragrafo si può omettere).
Poniamo per un intero qualsiasi θ_1 del corpo[112]

$$\theta_1=u_{11}\omega_1+u_{12}\omega_{12}+\cdots+u_{1n}\omega_n$$

(u_{1i} interi razionali, che nel paragrafo 9 erano indicati con u_i).
Poiché θ_1^h per $h=0,1,2,\ldots,n-1$ sono pure interi del corpo, verranno uguaglianze analoghe

$$(1)\qquad \theta_1^h=u_{h1}\omega_1+u_{h2}\omega_2+\cdots+u_{hn}\omega_n \qquad (h=1,2,\ldots,n)$$

dove evidentemente le u_{hk} sono polinomi a coefficienti interi razionali nelle $u_{1i},u_{12},\ldots,u_{1n}$.
Il determinante u delle u_{ik} è $\not\equiv 0\ (mod\ P)$. Altrimenti i primi membri di (1) sarebbero $(mod\ P)$ legati da una relazione lineare; cioè esisterebbero degli interi razionali α, tali che

$$\alpha_0+\alpha_1\theta_1+\alpha_2\theta_1^2+\cdots+\alpha_{n-1}\theta_1^{n-1}\equiv 0\ (mod\ P).$$

Il primo membro, di grado $n-1$, sarebbe // divisibile per $\Pi^e\Pi_1^{e_1}$ ..., che è di grado n: ciò che è assurdo.
Dunque il determinante u delle u_{ik} non è divisibile per alcun numero primo razionale P, cioè è un polinomio nelle $u_{11},u_{12},\ldots,u_{1n}$ a coefficienti primi tra loro. E dalle (1) si trae

$$\Delta^2(1,\theta_1,\theta_1^2,\ldots,\theta_1^{n-1})=U^2d$$
($d=$ discriminante del corpo).

E perciò il discriminante d del corpo è il M.C.D. dei coefficienti del discriminante di un intero generico $u_1\omega_1+u_2\omega_2+\cdots+u_n\omega_n$ del corpo stesso.
Non se ne può concludere però che d è il M.C.D. di questi discriminanti; perché U, pure essendo un polinomio a coefficienti interi razionali primi tra loro, può per valori interi razionali qualsiasi dati alle u_i essere divisibile per P (ciò che avviene se, per esempio, U è del tipo $u_1^P-u_1$).

[112] *lapsus* del curatore: leggasi $\theta_1=u_{11}\omega_1+u_{12}\omega_2+\cdots+u_{1n}\omega_n$.

Se invece ciò non avviene, se cioè si possono dare alle u_i tali valori a_i che U assuma un valore A non divisibile per P, si può // provare che in tal caso nelle considerazioni del paragrafo 9 all'intero generico θ_1 del corpo si può sostituire l'intero

$$\lambda = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n. \qquad (*)$$

// Un intero generico del corpo soddisfa alla

$$F(x) = 0.$$

Se θ_1 è un tale intero, e se $\theta_1', \theta_1'', \ldots, \theta_1^{n-1}$ ne sono i coniugati, allora

$$F'(\theta_1) = (\theta_1 - \theta_1')(\theta_1 - \theta_1'') \ldots \left(\theta_1 - \theta_1^{(n-1)}\right).$$

I coefficienti di questo polinomio nelle $\underline{u}$ individuano un ideale δ, loro M.C.D.
Ed è facile a provare che $Nm\,\delta$ è il M.C.D. dei coeff.[icienti] di $Nm\,F'(\theta_1)$, cioè del discriminante della equazione fondamentale, cioè è il numero $\underline{d}$.
Dalla

$$F'(x) = e_1[\Pi_1(x)]^{e_1-1}[\Pi_2(x)]^{e_2} \ldots [\Pi_r(x)]^{e_r} + e_2[\Pi_1(x)]^{e_1}[\Pi_2(x)]^{e_2-1} \ldots [\Pi_r(x)]^{e_r} + \cdots$$

si deduce che $F'(\theta_1)$ è divisibile per $p_1^{e_1-1}$; altrettanto avviene pertanto della sua norma $\underline{d}$.
Poiché d è intero razionale, esso sarà divisibile per P.
Se ne deduce che://
Tutti e soli i primi P razionali che sono divisori del discriminante d del corpo, sono divisibili per il quadrato di un ideale primo (gli altri P non divisori di $\underline{d}$ sono scomponibili nel prodotto di ideali primi tutti distinti fra loro).

(*) **Nota**: Infatti, se B è l'intero razionale tale che $AB \equiv 1\ (mod\ P)$, dalle (1) si trae che le ω sono congrue a polinomi in λ con coefficienti interi razionali $(mod\ P)$ [coefficienti, tutti i divisibili per B]. Poiché $Nm\,P = P^n$, e $(mod\ P)$ vi sono perciò nel corpo P^n interi distinti, il numero λ soddisferà ad una congruenza di grado $\underline{n}$ $(mod\ P)$ ed a nessuna congruenza di grado minore (ciò che si prova in modo analogo a quello seguito per le congruenze, a cui soddisfa una radice primitiva); e tale congruenza non può essere che la $F(x) \equiv 0\ (mod\ P)$, se $F(x) = 0$ è l'equazione, cui soddisfano λ e gli interi coniugati.
Detti P_i i polinomi dedotti da Π_i ponendo $u_i = a_i$ se ne deduce

$$F(x) = [P_1(x)]^{e_1}[P_2(x)]^{e_2} \ldots [P_r(x)]^{e_r}\ (mod\ P).$$

Io dico che p_1 (invece che come M.C.D. di P e di Π_1) si può definire come M.C.D. di $P_1(\lambda)$ e di P. Infatti, se $P_1(\lambda)$ fosse divisibile per p_1^e o per p_1p_2 o ecc., λ soddisferebbe ad una congruenza di grado $n - 1 < n$, che si deduce dalla precedente dividendo per P_1 o per P_1P_2.

§.11 ***Forme decomponibili del corpo***[113]

Diamo qui soltanto un rapido cenno, riservandocene lo studio più ampio nel caso particolare dei corpi quadratici.

Se $\alpha_1, \alpha_2, \dots, \alpha_n$ è la base di un ideale J in un corpo di grado n, ogni intero α di J vale

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$$

(x_i interi razionali).

La sua norma $(Nm\,\alpha)$ è un polinomio omogeneo nelle x a coefficienti interi razionali di grado n, che è decomponibile nel prodotto di n forme lineari.

Tale forma è, come sappiamo, divisibile per $Nm\,J$, e, come abbiamo dimostrato a proposito della teoria di Kronecker[114], il polinomio $\frac{Nm\,\alpha}{Nm\,J}$ è un polinomio a coef//ficienti interi razionali primi tra loro di grado n, decomponibile nel prodotto di n polinomi lineari. Essa dunque per $n > 2$ non è una forma generale (che non sarebbe decomponibile). Una tale forma si dice corrispondere all'ideale J; cambiare la base dell'ideale, o cambiare un ideale in un ideale equivalente, fa passare dalla forma iniziale ad una forma equivalente.

Basti questo per provare quante applicazioni la teoria degli ideali può trovare nei problemi nel campo assoluto di razionalità, relativamente alle equazioni del tipo

$$F = m$$

dove F è una delle forme citate, m un intero razionale. //

[113] Dirichlet 1877 (trad. 1881), suppl. XI, §176, p. 531-542. Cfr. anche Hilbert 1897 (trad. 1911), cap. VII, §30, p. 62-64; Hilbert tratta in maniera approfondita tale argomento tant'è che il cap. VII è intitolato *Les formes décomposables du corps*.

[114] Kronecker 1882, cap. II; §14. Interessante è il fatto che Fubini riprenda da Kronecker, e non da Hilbert, la notazione per indicare la norma.

Capitolo VIII – Aritmetica analitica[1]

§.1 *Lemmi fondamentali*

[2]Se a, b, ρ sono numeri positivi, la serie

$$S(\rho) = \frac{1}{b^{1+\rho}} + \frac{1}{(a+b)^{1+\rho}} + \frac{1}{(2a+b)^{1+\rho}} + \frac{1}{(3a+b)^{1+\rho}} + \cdots$$

converge; ed è

$$\lim_{\rho=0} \rho\, S(\rho) = \frac{1}{a}.$$

Consideriamo la parte della figura limitata dalla curva

$$y = \frac{1}{x^{1+\rho}},$$

dall'asse delle x, che è posta a destra del punto $x = b$. Tale figura illimitata ha l'area finita[3]

$$A = \int_b^\infty \frac{dx}{x^{1+\rho}} = \left[\frac{-1}{\rho x^\rho}\right] = \frac{1}{\rho b^\rho}. \qquad (1)$$

Consideriamo le rette $x = b, x = b + a, x = b + 2a, x = b + 3a,$ ecc. Esse dividono l'area considerata in figure parziali; ciascuna di queste è compresa tra i rettangoli R, r di ugual base a, e la cui altezza è rispettivamente l'ordinata nell'estremo sinistro o destro. In particolare $A > \sum r$, cioè

$$A > a\left[\frac{1}{(b+a)^{1+\rho}} + \frac{1}{(b+2a)^{1+\rho}} + \frac{1}{(b+3a)^{1+\rho}} + \cdots\right],$$

e la serie del $2°$ membro converge. Converge pertanto[4] // anche

$$a\, S(\rho) = a\left[\frac{1}{b^{1+\rho}} + \frac{1}{(b+a)^{1+\rho}} + \frac{1}{(b+2a)^{1+\rho}} + \cdots\right],$$

(che differisce dalla precedente soltanto per l'aggiunta del primo termine). Ed è $aS > A$, perché[5] S rappresenta la somma delle aree dei rettangoli R. Perciò

$$a\, S(\rho) > A > a\, S(\rho) - a\frac{1}{b^{1+\rho}},$$

ossia

$$\frac{1}{\rho b^\rho} < aS(\rho) < \frac{1}{\rho b^\rho} + \frac{a}{b^{1+\rho}}.$$

Moltiplicando per ρ e passando al limite per $\rho = 0$, si trova

$$\lim_{\rho=0} \rho\, S(\rho) = \tfrac{1}{a} \quad .$$

c.d.d.

---

[1] Gli argomenti trattati in questo capitolo non sono presenti nell'opera di Gazzaniga *Gli elementi della teoria dei numeri.* Vengono invece trattati parzialmente nelle *Lezioni* di Bianchi: *Sulla teoria dei numeri algebrici e principi d'aritmetica analitica* e *Sulla Teoria aritmetica delle forme quadratiche binarie e ternarie.*

[2] Bianchi 1911-12, cap. VI, §52, p.228-230. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. II, §117, p. 300-302. La notazione utilizzata e la dimostrazione svolta da Fubini sono identiche a quelle di Bianchi e Dedekind.

[3] *e.c.*: invece di [ ] leggasi $[\ ]_b^\infty$.

[4] Nota inserita da Fubini a p.d.p.: *Teoria dei numeri Disp. 20.*

[5] *e.c.* e *cor. sup.*: aS.

[6]Siano $K_1, K_2, K_3, \ldots$ numeri (positivi) tali che

$$0 < K_1 \leq K_2 \leq K_3 \leq K_4 \leq \cdots \lim_{i=\infty} K_i = \infty.$$

sia $\mathrm{T}(t)$ il numero di quelle K_i che non superano t, cosicché $\mathrm{T}(t)$ è funzione discontinua non decrescente di t. Se

$$\lim_{i=\infty} \frac{\mathrm{T}(t)}{t} = \omega = \text{numero finito}$$

allora la serie

$$S(\rho) = \sum_n \frac{1}{K_n^{1+\rho}}$$

converge per $\rho > 0$ e per $\rho = 0$ vale la

$$lim\, \rho S(\rho) = \omega$$

(questo teorema vale anche ed è evidente se le K si suppongono invece in numero finito).
Se, per es., $K_n = b + (n-1)a$, allora T è il massimo // intero tale che $b + (T-1)a \leq t$; perciò $lim \frac{\mathrm{T}}{t} = \frac{1}{a}$; e si ritorna al teorema precedente.
Dimostriamo il teorema enunciato, e cominciamo ad osservare che, se si pone $l_n = \frac{n}{K_n}$, è $\lim_{n=\infty} l_n = \omega$. Ciò è evidente se le K_n sono tutte differenti tra loro. Infatti, se $t = K_n$, si ha $\mathrm{T} = n$; se dunque ci limitiamo a fare assumere alla t i valori K_n, il numero $\frac{\mathrm{T}(t)}{t}$ assume i valori l_n. Se poi vi sono dei K_n uguali tra di loro, si osservi che, se vi sono $h(n)$ numeri K uguali a K_n la differenza dei valori di T corrispondenti a $t = K_n$ ed a $t = K_n - \varepsilon$, (dove ε è scelto così piccolo che nessuno dei K sia compreso tra $K_n - \varepsilon$ e K_n) è precisamente h_n. Quindi nei due casi il rapporto $\frac{\mathrm{T}}{t}$ vale

$$\frac{\mathrm{T}(K_n)}{K_n} \quad \text{e} \quad \frac{\mathrm{T}(K_n) - h_n}{K_n - \varepsilon}.$$

Entrambi questi rapporti hanno il limite finito ω; prendendo $K_n - \varepsilon$ abbastanza grande, la loro differenza

$$\frac{-\varepsilon \mathrm{T}(K_n) + K_n h_n}{K_n(K_n - \varepsilon)}$$

si può rendere piccola a piacere in valore assoluto; e se ne deduce che $\lim_{n=\infty} \frac{h_n}{K_n} = 0$. //
Siano $m+1, m+2, \ldots, m+h(n)$ i valori di n, cui corrisponde un numero K uguale al considerato K_n. Per questi valori di n la frazione $\frac{n}{K_n}$ oscilla tra $\frac{m}{K_n}$ e $\frac{m}{K_n} + \frac{h(n)}{K_n}$; il secondo di questi vale $\frac{\mathrm{T}(t)}{t}$, quando $t = K_n$. Poiché $\lim \frac{h_n}{K_n} = 0$, e $\lim \frac{\mathrm{T}}{t} = \omega$, sarà anche in questo caso $\lim \frac{n}{K_n} = \omega$.
Ora

$$S(\rho) = \sum_n \frac{1}{K_n^{1+\rho}} = \sum_n \frac{l_n^{1+\rho}}{n^{1+\rho}}.$$

[6] Bianchi 1911-12, cap. VI, §52, p. 230-235. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. II, §118-119, p. 302-305. Anche in questo caso l'enunciato e la dimostrazione di tale lemma qui esposti da Fubini sono del tutto equivalenti a quelli di Bianchi e Dedekind.

La serie

$$\sigma(\rho) = \sum \frac{1}{n^{1+\rho}}$$

converge; le $l_n^{1+\rho}$ tendono ad $\omega^{1+\rho}$. Quindi anche $S(\rho)$ converge; ora $\rho\sigma(\rho)$ tende per $\rho = 0$ ad 1, in virtù del teorema precedente. Scelto dunque un $\varepsilon > 0$ piccolo ad arbitrio, ed un m così grande che per $n > m$ sia $|l_n^{1+\rho} - \omega^{1+\rho}| < \varepsilon$, sarà, indicando con θ un numero compreso tra -1 e $+1$:

$$\rho S(\rho) = \rho\left[\frac{1}{K_1^{1+\rho}} + \frac{1}{K_2^{1+\rho}} + \cdots + \frac{1}{K_m^{1+\rho}}\right] + \rho\left[\frac{1}{(m+1)^{1+\rho}} + \frac{1}{(m+2)^{1+\rho}} + \cdots\right](\omega^{1+\rho} + \theta\varepsilon)$$

$$= \rho\left[\frac{1}{K_1^{1+\rho}} + \cdots + \frac{1}{K_m^{1+\rho}}\right] - \rho\left[\frac{1}{1} + \frac{1}{2^{1+\rho}} + \cdots + \frac{1}{m^{\rho}}\right](\omega^{1+\rho} + \theta\varepsilon) + \rho\sigma(\rho)[\omega^{1+\rho} + \theta\varepsilon].$$

se ρ è abbastanza piccolo i primi due termini del // terzo membro sono minori di ε e $|\rho\sigma(\rho) - 1|$ è pure minore di ε.
Quindi per ρ abbastanza piccolo

$$|\rho S(\rho) - \omega^{1+\rho}|$$

è minore di $2\varepsilon + \varepsilon\omega^{1+\rho} + \varepsilon[\rho\sigma(\rho)] + \varepsilon^2$.
Cioè

$$\lim_{\rho=0} \rho S(\rho) = \omega.$$

§.2 ***Alcune trasformazioni di serie***

Ordiniamo gli ideali j di un corpo in modo che le loro norme $N(j)$ vadano crescendo[7], e studiamo la serie

$$Z(s) = \sum \frac{1}{[N(j)]^s} \; ove \; s = 1 + \rho.$$

Nel corpo R assoluto di razionalità tale serie è[8]

$$Z_R(s) = \sum \frac{1}{n^s} \; ;$$

essa converge per $s > 1$ e per $s = 1$ il prodotto $(s-1)\,Z_R(s)$ tende per limite[9] ad 1.
Se $j = p_1 p_2 \ldots p_r$ dove p sono i fattori primi di j, è

$$N(j) = N(p_1)N(p_2)\ldots N(p_r)$$

e perciò[10]

$$Z(s) = \sum \frac{1}{[N(p_1)]^s} \; \frac{1}{[N(p_2)]^s} \cdots \frac{}{[N(p_r)]^s}.$$

cioè $Z(s)$ è il prodotto di tutte le serie

---

[7] Bianchi 1911-12, cap. VI, §52, p.235-242. Bianchi tratta qui la serie di Dirichlet nel caso più generale: infatti afferma che deve essere soddisfatta semplicemente l'ipotesi che i numeri che compaiono a denominatore siano una successione decrescente.
[8] *Idem*, cap. III, §46, p. 315.
[9] Bianchi 1920-21, cap. III, §46, p. 317. Cfr. anche Bianchi 1911-12, cap. VI, §52, p.229.
[10] *e.c.* e *cor. sup.*: invece di $\frac{}{[N(p_r)]^s}$ leggasi $\frac{1}{[N(p_r)]^s}$.

$$1+\frac{1}{[N(p)]^s}+\frac{1}{[N(p)]^{2s}}+\frac{1}{[N(p)]^{3s}}+\cdots$$

// estese ai vari ideali primi P del corso[11]: queste serie sono progressioni geometriche decrescenti di somma $\frac{1}{1-[N(p)]^{-s}}$, cosicché[12]

$$Z(s)=\prod\frac{1}{1-[N(p)]^{-s}}.$$

E nel campo R

$$Z_R(s)=\prod\frac{1}{1-P^{-s}}$$

dove P percorre i vari primi razionali positivi.
Nel caso generale ordiniamo gli ideali primi p in modo da raggruppare quelli che sono divisori di uno stesso numero razionale positivo P; supponiamo

$$P=p_1^{e_1}\ p_2^{e_2}\ \dots\ p_r^{e_r}$$
$$Nm\ p_i=P^{f_i}\quad (e_1f_1+e_2f_2+\cdots+e_rf_r=n=\text{grado del corpo}).$$

I fattori che provengono dai divisori di P sono

$$\frac{1}{1-P^{-sf_1}}\ \ \frac{1}{1-P^{-sf_2}}\ \cdots\ \frac{1}{1-P^{-sf_r}}.$$

E perciò

$$Z(s)=\prod_P\left[\frac{1}{1-P^{-sf_1}}\ \ \frac{1}{1-P^{-sf_2}}\ \cdots\ \frac{1}{1-P^{-sf_r}}\right],$$

dove il prodotto è esteso a tutti i primi razionali P (e dove, si ricordi, $r, f_1, f_2, \dots, f_r$ possono variare con P).
Come vedremo più avanti per un corpo quadratico di discriminante d, se ne deduce che

$$Z(s)=\prod_P\frac{1}{1-P^{-s}}\prod_P\frac{1}{1-\left(\frac{d}{P}\right)P^{-s}}=Z_R(s)\prod_P\frac{1}{1-\left(\frac{d}{P}\right)P^{-s}}.$$

// Il secondo fattore, sviluppato in serie, diventa

$$\sum_n\left(\frac{d}{n}\right)\frac{1}{n^s}$$

dove n assume tutti i valori interi positivi, e $\left(\frac{d}{n}\right)$ è il simbolo di Jacobi.
Nel corpo $K\left(\sqrt[\ell]{1}\right)$, che proviene da una radice $\varepsilon=\sqrt[\ell]{1}$ ℓ^{esima} di 1, dove ℓ è un intero primo positivo, si trova che posto $\ell_\ell=0$, e posto $P_\ell=e^{\frac{2\pi i}{\ell-1}ind\ P}$ per ogni primo positivo $P\neq\ell$, è

$$Z(s)=Z_R(s)\prod_P\prod_{m=1}^{\ell-2}\frac{1}{\left[1-P_\ell^mP^{-s}\right]}$$

[11] *e.c.* e *cor. sup.*: corpo.
[12] Dirichlet 1877 (trad. 1881), suppl. IX, §178, p. 366.

come dimostreremo nell'ultimo capitolo dedicato ad esempi particolari. Si noti che dai teoremi del §1 si deduce che[13]

$$\lim_{s=1}(s-1)Z_R(s) = 1.$$

§.3 ***Volume di un corpo*** C ***in uno spazio ad*** m ***dimensioni***[14]

Supporremo $m = 2$; metodo e risultati si estendono facilmente al caso più generale.
Si divida il primo piano con le rette

$$x = n\varepsilon \qquad y = p\varepsilon$$

(n, p interi positivi; ε numero positivo arbitrario).
Otterremo una rete di quadrati Q, ciascuno dei quali ha per area ε^2. Tra essi vi siano q' quadrati[15] l' tutti interni a C, altri q'' quadrati[16] l'' che contengo//no almeno un punto del contorno di C, e infine altri q''' quadrati Q''' tutti esterni a C.
Se è noto ε, un quadrato Q è determinato da quel suo vertice, che ha la minima ascissa e la minima ordinata: noi diremo che il quadrato Q e quel suo vertice si corrispondono.
Il vertice corrispondente ad un Q' è un punto di C; se viceversa un nodo della nostra rete di quadrati è un punto di C, il quadrato corrispondente o è un quadrato Q', oppure un quadrato Q''. Il numero N dei nodi della nostra rete, che appartengono a C, è pertanto compreso tra q' e $q' + q''$. I quadrati Q' costituiscono un poligono P' tutto interno a C; i quadrati Q', Q'' costituiscono insieme un poligono P'', che contiene C all'interno. E, come è noto, l'area $q'\varepsilon^2$ di P' è[17] l'area $(q' + q'')\varepsilon^2$ di P'' hanno entrambe come limite per $\varepsilon = 0$ l'area di C. Poiché N è compreso tra q' e $q' + q''$, sarà anche

$$\lim_{\varepsilon=0} N\varepsilon^2 = \text{area di } C.$$

Facciamo subire a C e alla rete l'omotetia col centro nell'origine, e col rapporto $\sigma = \frac{1}{\varepsilon}$. La nostra rete si muterà nella rete R, i cui nodi sono i punti di coordinate intere. Il campo C si mu//terà in un campo omotetico C_σ; il numero N si potrà definire come il numero dei nodi della rete R appartenenti a C_σ. E sarà

$$\text{area } C = \lim_{\varepsilon=0} N\varepsilon^2 = \lim_{\sigma=\infty} \frac{N}{\sigma^2}.$$

Ci serviremo più avanti di questo nuovo modo di considerare l'area di un campo C.
Nel caso di spazii ad $\underline{m}$ dimensioni, basta scrivere $\frac{N}{\sigma^m}$, anziché $\frac{N}{\sigma^2}$.

---

[13] *Idem*, suppl. IX, §178, p. 566. Qui Dedekind enuncia e dimostra il risultato nella forma più generale per cui si ha che $\lim_{s=1}(s-1)Z_R(s) = gh$ con g costante e h numero delle classi.
[14] Bianchi 1911-12, cap. VI, §56, p. 249-253. Il procedimento qui illustrato da Bianchi è analogo a quello di Fubini, tenendo conto che utilizza la lettera ω per indicare l'area di C.
[15] *lapsus* del curatore: leggasi Q'.
[16] *lapsus* del curatore: leggasi Q''.
[17] *e.c.* e *cor. sup.*: e l'area.

§.4 ***Un limite fondamentale***[18]

Per fissare le idee, supponiamo di studiare un corpo K_1 di $7°$ grado, i cui coniugati K_2, K_3 sono reali, mentre i due K_4, K_5 sono complessi coniugati rispettivamente degli altri due K_6, K_7. Per il teorema di Dirichlet sulla unità di un corpo algebrico (pag. 228) il corpo K_1 avrà $3 + 2 - 1 = 4$ unità fondamentali[19] $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, ed un numero finito ω di altre unità η, radici di 1: ogni altra unità ε del corpo sarà della forma

$$\varepsilon = \varepsilon_1^{n_1}\, \varepsilon_2^{n_2}\, \varepsilon_3^{n_3}\, \varepsilon_4^{n_4}\, \eta.$$

Sia ξ_1 un intero di K_1 e siano $\xi_2, \dots, \xi_7$ i numeri coniugati. Poniamo

$l_1(\xi) = \log|\xi_1| \quad l_2(\xi) = \log|\xi_2| \quad l_3(\xi) = \log|\xi_3|$
$\log(\xi_4) = \frac{1}{2} l_4(\xi) + i l_6(\xi) \qquad \log(\xi_5) = \frac{1}{2} l_5(\xi) + i l_7(\xi)$
$\log(\xi_6) = \frac{1}{2} l_4(\xi) - i l_6(\xi)$ // $\qquad \log(\xi_7) = \frac{1}{2} l_5(\xi) - i l_7(\xi)$

con le condizioni $0 \leq \mathrm{l}_6 < 2\pi \quad 0 \leq \mathrm{l}_7 < 2\pi$.
Osservo che se $\xi_4 = \rho(cos\theta + isen\theta)$, quindi $\xi_6 = \rho\,(cos\theta - isen\theta)$

$$log(\xi_4) = log\,\rho + i\theta \quad log\,(\xi_6) = log\,\rho - i\theta$$

in cui possiamo supporre $0 \leq \theta < 2\pi$. Dunque più sopra si è indicato θ con $l_6(\xi)$.
Inoltre $\log \rho = \log|\xi_4| = \frac{1}{2}\log \rho^2 = \frac{1}{2}\log|\xi_4 \xi_6|$
perché ξ_4 e ξ_6 sono immaginari coniugati. Dunque[20]

$$log_4(\xi) = 2\, log\,|\xi_4| = log|\xi_4 \xi_6| = log\{|\xi_4|.\,|\xi_6|\} = log|\xi_4| + log|\xi_6|.$$

Analogamente $l_5(\xi) = \log|\xi_5 \xi_7|$.
Perciò

$l_1(\xi) + l_2(\xi) + \cdots + l_5(\xi) =$
$= \log|\xi_1| + \log|\xi_2| + \log|\xi_3| + 2\log|\xi_4| + 2\log|\xi_6| =$
$= \log|\xi_1| + \log|\xi_2| + \log|\xi_3| + \log|\xi_4| + \log|\xi_5| + \log|\xi_6|$ [21] $=$
$= \log|\xi_1 \dots \xi_7| = \log|Nm\ \xi|.$ (1)

Poniamo

$$\left.\begin{aligned} l_1(\xi) &= e_1 l_1(\varepsilon_1) + \cdots + e_4 l_1(\varepsilon_4) + \tfrac{1}{5} e_0 \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ l_4(\xi) &= e_1 l_4(\varepsilon_1) + \cdots + e_4 l_4(\varepsilon_4) + \tfrac{1}{5} e_0 \end{aligned}\right\} \quad (2)$$

$$l_5(\xi) = e_1 l_5(\varepsilon_1) + \cdots + e_4 l_5(\varepsilon_4) + \tfrac{1}{5} e_0. \quad (3)$$

[18] Bianchi 1920-21, cap. III, §48, p. 332-336. Bianchi affronta qui l'argomento dei numeri ridotti rispetto ad un sistema fondamentale di unità, senza però inserire, a differenza di Fubini, alcuna considerazione geometrica. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. XI, §178, p. 555-569. Fubini in questo paragrafo e nei seguenti sviluppa lo stesso ragionamento portato avanti da Dedekind in questa sezione. Cfr. infine Minkowski 1957, §4.9, p. 136-142.

[19] Hilbert 1897 (trad. 1911), cap. VI, §21, p. 50; l'autore fornisce qui la definizione di sistema di unità fondamentali.

[20] *e.c.* e *cor. sup.*: invece di $\log_4(\xi) =$ leggasi $l_4(\xi) =$.

[21] *e.c.* e *cor. sup.*: invece di $\dots + \log|\xi_6|$ leggasi $\dots + \log|\xi_6| + \log|\xi_7|$.

Ora $l_1(\varepsilon_1) + l_2(\varepsilon_1) + \cdots + l_5(\varepsilon_1) = \log|Nm\ \varepsilon_1| = \log 1 = 0.$

Quindi sommando membro a membro ottengo

$$e_0 = log|Nm\ \xi|. \tag{4}$$

Le (2) bastano a determinare le e_1, e_2, e_3, e_4: i cosiddetti esponenti di ξ. //
Moltiplicando ξ per $\varepsilon_1^{n_1}\varepsilon_2^{n_2}\varepsilon_3^{n_3}\varepsilon_4^{n_4}$ (n_i interi)[22] $l_1(e) = \log|\varepsilon_1|$ viene aumentato di

$$n_1 l_1(\varepsilon_1) + n_2 l_2(\varepsilon_2) + n_3 l_3(\varepsilon_3) + n_4 l_4(\varepsilon_4) \ldots\ldots\ldots\ldots\ldots$$

Così $l_4(\xi) = 2\log|\xi_4|$ viene aumentato di[23]

$$2n_1\ log|\varepsilon_1^{IV}| + \cdots + 2n_4\ log|\varepsilon_4^{IV}|_2 = n_1 l_4(\varepsilon_1) + n_2 l_4(\varepsilon_2) + \cdots + n_4 l_4(\varepsilon_4).$$

Genericamente $l_i(\xi)$ viene aumentato di $n_1 l_i(\varepsilon_1) + n_2 l_i(\varepsilon_2) + n_3 l_i(\varepsilon_3) + n_4 l_i(\varepsilon_4)$.
Cioè e_1, e_2, e_3, e_4 vengono aumentati rispettivamente degli interi n_1, n_2, n_3, n_4 (positivi o negativi).
Moltiplichiamo il numero ξ per una unità, cioè mutiamo ξ in un intero associato (con che resta invariato l'ideale è principale (ξ)). Ogni unità è della forma $\varepsilon = \varepsilon_1^{n_1}\varepsilon_2^{n_2}\varepsilon_3^{n_3}\varepsilon_4^{n_4}\eta$. Disponiamo delle η in guisa che risulti $0 \leq e_i < 1$. η può essere scelto in ω modi, quindi vi sono ω numeri associati che soddisfano a tale condizione.
Sia a_1 un ideale di K_1; e ne sia $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_7^{(1)}$ una base. Posto $\xi_1 = v_1\alpha_1^{(1)} + v_2\alpha_2^{(1)} + \cdots + v_7\alpha_7^{(1)}$ il numero ξ_1 dando alle v valori interi razionali, descrive gli interi di a_1; nello spazio V ove le v sono coordinate cartesiane ortogonali, ricaverò una retta[24] R, immagine degli interi di a.
Posto

$$|Nm\xi| \leq t \tag{5}$$

// sarà $e_0 \leq \log t$; tenuto conto delle $0 \leq e_i < 1\ (i = 1, \ldots, 4)$ dirette[25] le $e_i\ (i = 0, \ldots, 4)$ saranno limitate da queste uguaglianze[26]; perciò dalle $(2), (3)$ resteranno limitate le $l_1(\xi), \ldots, l_5(\xi)$, cioè

$$log|\xi_1| \ldots 2\ log|\xi_4|\ , 2\ log\ |\xi_5|$$

e quindi anche resteranno limitate i modulo[27] di ξ_1 e dei numeri coniugati (notando che[28] $|\xi_4| = |\xi_5|$ e $|\xi_5| = |\xi_4|$).
Essendo

$\xi_1 = v_1\alpha_1^{(1)} + v_2\alpha_2^{(1)} + \cdots + v_7\alpha_7^{(1)}$
$\xi_2 = v_1\alpha_1^{(2)} + v_2\alpha_2^{(2)} + \cdots + v_7\alpha_7^{(2)}$
……
……
$\xi_7 = v_1\alpha_1^{(7)} + \cdots + v_7\alpha_7^{(7)}$

[22] *e.c.* e *cor. sup.*: $l_1(e) = \log|\xi_1|$ viene aumentato di $n_1 l_1(\varepsilon_1) + n_2 l_1(\varepsilon_2) + n_3 l_1(\varepsilon_3) + n_4 l_1(\varepsilon_4)$.
[23] *e.c.* e *cor. sup.*: invece di $2n_4 \log|\varepsilon_4^{IV}|_2$ leggasi $2n_4 \log|\varepsilon_4^{IV}|$.
[24] *e.c.* e *cor. sup.*: rete R.
[25] *e.c.* e *del.*: sopprimere "dirette".
[26] *e.c.* e *cor. sup.*: disuguaglianze.
[27] *e.c.* e *cor. sup.*: limitati i moduli.
[28] *e.c.* e *cor. sup.*: invece di $|\xi_4| = |\xi_5|$ e $|\xi_5| = |\xi_4|$ leggasi $|\xi_4| = |\xi_6|$ e $|\xi_5| = |\xi_7|$.

ed essendo $\Delta(\alpha_1, \dots, \alpha_7) \neq 0$ perché discriminante della base di un ideale non nullo ricaviamo

$$v_i = \frac{\xi_1 \Delta_{1i} + \xi_2 \Delta_{2i} + \cdots + \xi_7 \Delta_{7i}}{\Delta}$$

[29]dove con Δ i intendo il suddetto complementare al termine[30] $\alpha_1^{(2)}$.
Dalle limitazioni precedenti segue che anche le v_i sono limitate in valore assoluto.
Quindi in V resterà determinata, in virtù di (5), una regione finita C_t; la quale dipenderà dal valore della costante $\underline{t}$.
Il campo C_t si ottiene dal campo C_1 con l'omotetia // che ha per centro l'origine, e rapporto $\sqrt[7]{t}$, perché, moltiplicando tutte le $\underline{v}$ per $\sqrt[7]{t}$, la $|Nm\,\xi|$ resta moltiplicata per t. Per il risultati del §3, sarà dunque

$$(6) \qquad \dots \; Volume\ di\ C_1 = \lim_{t=\infty} \frac{Numero\ dei\ punti\ di\ R\ non\ esterni\ a\ C_t}{\left(\sqrt[7]{t}\right)^7}$$

ove il denominatore $\left(\sqrt[7]{t}\right)^7 = t$.
Calcoliamo il numeratore del secondo membro di (6). E sia T il numero degli ideali principali divisibili per a_1, di norma $\leq t$. Ogni intero ξ_1 di a_1 tale che $|Nm\,\xi| \leq t$ genera un tale ideale; due interi siffatti generano lo stesso ideale soltanto quando sono associati; ognuno dei nostri ideali è generato da un tale intero di a_1 e dagli interi associati; ora due interi, per cui $0 \leq l_1 < 1; \dots; 0 \leq l_4 < 1$ sono associati soltanto quando il loro quoziente e una delle ω unità del corpo, che sono radici di 1; cioè gli interi ξ tali che $|Nm\,\xi| \leq t$ si distribuiscono in sistemi di ω interi ciascuno, che generano uno stesso dei T ideali citati. Perciò la (1) diventa

$$Volume\ di\ C_1 = \omega \lim_{t=\infty} \frac{\mathrm{T}}{t}$$

dove, ricordiamolo, T è il numero degli ideali divisibili per a_1, che hanno una norma non // maggiore di t.

§.5 ***Calcolo del volume di*** C_1[31]

Il campo C_1 è definito dalle[32]:

(1) $0 \leq e_1 < 1; \dots; 0 \leq e_4 < 1; 0 \leq l_6(\xi) < 1\pi; 0 \leq l_7(\xi) < 2\pi;\ 0 \leq e^{e_0} = |Nm\xi| \leq 1.$

Date le $e^{e_0}, e_1, e_2, e_3, e_4, l_6, l_7$, sono dati i

$$log|\xi_1|\,, log|\xi_2|\,, log|\xi_3|\,, log\,\xi_4, log\,\xi_5, log\,\xi_6, log\,\xi_7$$

cioè sono date tutte le ξ con la sola indeterminazione del segno per $\xi_1\,\xi_2\,\xi_3$. Date perciò le $e_0, \dots, e_4, l_6, l_7$ vi sono 2^3 numeri ξ, cioè 2^3 sistemi di valori per le v, cioè 2^3 punti di C_1. Perciò il volume di C_1 vale[33]

---

[29] *e.c.* e *cor. sup.*: dove con Δ_i intendo il suddeterminante complemento.
[30] *lapsus* del curatore: leggasi $\alpha_i^{(2)}$.
[31] Bianchi 1920-21, cap. II, §49, 50, p. 336-348. In questi due paragrafi Bianchi tratta in modo più approfondito rispetto a Fubini il calcolo del generico volume C nel caso n-dimensionale.
[32] *e.c.* e *cor. sup.*: invece di $0 \leq l_6(\xi) < 1\pi$ leggasi $0 \leq l_6(\xi) < 2\pi$.
[33] *e.c.* e *cor. sup.*: invece di $d(e_0\,, e_1, \dots, e_4, l_6, l_7)$ leggasi $d(e^{e_0}\,, e_1, \dots, e_4, l_6, l_7)$.

$$2^3 \int \iint \dots \int \frac{d(v_1,\ v_2, \dots v_7)}{d(e^{e_0}, e_1, \dots, e_4, l_6, l_7)} d(e^{e_0}) de_1 \ \dots de_4 dl_6 dl_7$$

dove le integrazioni si estendono al campo definito dalle (1). Il Jacobiano da integrare si calcola uguale a

$$\frac{1}{Nm\ a}\ \frac{1}{\sqrt{|d|}} L$$

ove

$$L = \begin{matrix} l_1(\varepsilon_1)\ l_1(\varepsilon_2)\ l_1(\varepsilon_3)\ l_1(\varepsilon_4) \\ l_2(\varepsilon_1)\ \dots\dots\dots\dots\dots\ l_2(\varepsilon_4) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ l_4(\varepsilon_1)\ \dots\dots\dots\dots\dots\ l_4(\varepsilon_4) \end{matrix}$$

// si chiama il <u>regolatore del corpo</u>[34]. Perciò il nostro volume vale[35]

$$2^3 \frac{1}{Nm\ a}\ \frac{1}{\sqrt{|d|}}\ L(2\pi)^2 = 2^{3+2}\pi^2 \frac{L}{Nm\sqrt{|d|}}.$$

Perciò[36]

$$\lim_{t=\infty} \frac{\mathrm{T}}{t} = \frac{x}{Nm} \quad \text{ove } x = \frac{1}{\omega} 2^{3+2}\pi^2 \frac{L}{\sqrt{|d|}}.$$

Nel caso generale si troverebbe[37] $x = \frac{1}{\omega} 2^{r_1+r_2}\pi^{r_2} \frac{L}{\sqrt{|d|}}$ ove r_1 ed r_2 sono rispettivamente il numero dei corpi reali e delle coppie dei corpi complessi coniugati che si trovano nell'insieme del corpo che si studia e dei corpi coniugati.
Gli ideali principali divisibili per a sono il prodotto di a per un ideale b appartenente alla classe B reciproca di quella, cui appartiene a. Ed è $Nm\ j = Nm\ a\ Nm\ b$. La $Nm\ j \leq t$ equivale alla

$$Nm\ b\ \leq \frac{t}{Nm\ a}.$$

Perciò T si può anche definire come il numero degli ideali della classe B, la cui norma non supera[38]
$T = \frac{t}{Nm\ r}$. E sarà[39]

$$\lim_{T=\infty} \frac{\mathrm{T}}{T} = lim\ Nm\ a \frac{\mathrm{T}}{t} = x.$$

Questa uguaglianza[40] //

$$\lim_{T=\infty} \frac{\mathrm{T}}{T} = x$$

---

[34] Hilbert 1897 (trad. 1911), cap. VI, §21, p. 50. A differenza Fubini, il concetto di 'regolatore del corpo', viene introdotto subito dopo la nozione di 'sistema di unità fondamentali', all'interno del paragrafo intitolato *Les unités fondamentales – Le régulateur du corps – Un systéme d'unités indépendantes*.

[35] *e.c.* e *cor. sup.*: invece di $L\frac{1}{Nm\sqrt{|d|}}$ leggasi $L\frac{1}{Nm\ a\sqrt{|d|}}$.

[36] *e.c.* e *cor. inf.*: invece di $\frac{x}{Nm}$ leggasi $\frac{x}{Nm\ a}$.

[37] Hilbert 1897 (trad. 1911), cap. VII, §25, p. 55, lemma 10.

[38] *e.c.* e *cor. sup.*: $T = \frac{t}{Nm\ a}$.

[39] Bianchi 1920-21, cap. III, §48, p. 330, prop. A).

[40] Hilbert 1897 (trad. 1911), cap. VII, §26, p. 57, teor. 54: "Si l'on désigne par T le nombre de tous les idéaux d'une classe A dont les normes sont $\leq t$, on a $\lim_{t=\infty} \frac{T}{t} = x$."

vale qualunque sia la classe B. Scriviamola perciò per tutte le h classi del nostro corpo: classi che supporremo essere in numero di h.
E sommiamo le h uguaglianze così ottenute. Il denominatore T che figura al 1° membro è lo stesso in tutte queste $\underline{h}$ formole; il numeratore della somma sarà perciò la somma dei vari numeratori T, cioè sarà la somma dei numeri T relativi alle varie classi (T è per una classe il numero dei suoi ideali, la cui somma non supera T).
La somma di questi T sarà perciò il numero N di tutti gli ideali del nostro corpo, la cui somma non supera T. Pertanto[41]

$$\lim_{T=\infty} \frac{N}{T} = xh.$$

Per i teoremi relativi[42] alla serie[43] $L(s)$ il primo membro vale[44]

$$\lim_{s=1}(s-1)L(s).$$

Perciò: <u>il numero h delle classi degli ideali di un corpo vale</u>[45]

$$\frac{1}{x}\lim_{s=1}(s-1)L(s). \ //$$

§.6 ***Il grande teorema della progressione aritmetica***[46]

Come vedremo, e abbiamo del resto già enunciato, per il corpo algebrico generato da $\sqrt[\ell]{1}$ (ℓ =primo razionale) si ha[47]

$$L(s) = L_R(s)\prod_P \prod_{m=1}^{\ell-2} \frac{1}{(1-P_\ell^m P^{-s})}$$

dove[48]:
$L_R(s)$ indica la serie $\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\dots$ cioè la funzione[49] $L(s)$ nel campo assoluto R di razionalità. Ed è[50]:

$$(1) \qquad \lim_{s=1}(s-1)L_R(s) = 1.$$

Il numero P descrive tutti i primi razionali positivi. Col simbolo P_l ho indicato l'espressione $\frac{2\pi i}{e^{\ell-1}} ind\ P$ per i primi $P \neq \ell$. Per $P = \ell$ col simbolo $P_\ell = \ell_\ell$ indico lo zero.

---

[41] *Idem*, cap. VII, §26, p. 58, teor. 55: "Si l'on désigne par T le nombre de tous les idéaux d'un corps k dont les normes sont $\leq t$, et si l'on désigne par h le nombre des classes d'idéaux, on a $\mathrm{L}_{t=\infty}\frac{T}{t} = hx$."
[42] *Idem*, cap. VII, §26, p. 58, teor. 56; prima di enunciare tale risultato, il matematico scrive "On peut, par des méthodes analytiques, déduire de cette formule une expression fondamentale pour h".
[43] *e.c.* e *cor. sup.*: $Z(s)$.
[44] *e.c.* e *cor. sup.*: invece di $L(s)$ leggasi $Z(s)$.
[45] *e.c.* e *cor. sup.*: invece di $L(s)$ leggasi $Z(s)$.
[46] Bianchi 1920-21, cap. III, §58, p. 394-401. Bianchi dedica l'intero paragrafo alla trattazione del caso l = numero primo, nel contesto più generale dei corpi circolari (che invece Fubini non ha ancora introdotto). In Bianchi 1911-12, cap. VI, §61, p. 273-276, l'intero paragrafo *Dimostrazione del teorema della progressione aritmetica e applicazione ai generi* è dedicato a tale argomento, anche se viene trattato in maniera leggermente differente rispetto a Fubini.
[47] *e.c.* e *cor. sup.*: invece di $L(s)$ leggasi $Z(s)$ e invece di $L_R(s)$ leggasi $Z_R(s)$.
[48] *e.c.* e *cor. sup.*: $Z_R(s)$.
[49] *e.c.* e *cor. sup.*: leggasi $Z(s)$.
[50] *e.c.* e *cor. sup.*: invece di $L(s)$ leggasi $Z(s)$.

Poiché $(s-1)Z_R(s)$ per $s=1$ tende ad 1, e $(s-1)Z(s)$ per $s=1$ tende a un limite finito diverso da zero (il numero $\underline{h}$ delle classi del corpo considerato[51]) si deduce che

$$\lim_{s=1} \prod_{m=1}^{\ell-2} \prod_{P} \frac{1}{\left[1-P_\ell^m P^{-s}\right]}$$

esiste, è finito e diverso da zero[52]. E se ne deduce fa//cilmente che ciascuno degli $\ell-2$ prodotti

$$\prod_{P} [1-P_\ell^m P^{-s}]$$

ha per $s=1$ limite finito e diverso da zero.
Prendendone il logaritmo si trova che

$$(2) \qquad \sum_P P_\ell^m P^{-s} + \sum_P \frac{\left[P_\ell^m P^{-s}\right]^2}{2} + \sum_P \frac{\left[P_\ell^m P^{-s}\right]^3}{3} + \cdots$$

tende per $s=1$ ad un limite finito. Ora il secondo, il terzo, il quarto, ecc. termine di questa serie sono ordinatamente in modulo non superiori ai termini di $\sum_P \frac{1}{2P^{2s}} + \sum_P \frac{1}{3P^{3s}} + \sum_P \frac{1}{4P^{4s}} + \ldots$, tutti insieme danno un contributo che non può superare in modulo il valore di questa serie; la quale evidentemente non supera[53]

$$\frac{1}{2}\sum_P (P^{-2s}+P^{-3s}+P^{+4s}+\cdots) = \frac{1}{2}\sum_P \frac{1}{P^{2s}}\frac{1}{1-P^{-s}} < \sum_P \frac{1}{P^{2s}} < \sum_P \frac{1}{P^2} < \sum \frac{1}{n^2}$$

dove l'ultima somma è estesa a tutti gli interi razionali $\underline{n}$. Dunque anche il solo primo termine

$$(A) \qquad \sum_P P_\ell^m P^{-s} \qquad (m=1,2,\ldots,\ell-2)$$

ha per $s=1$ un limite finito.
Invece

$$\lim_{s=1} Z_R(s) = \lim_{s=1} \prod_P (1-P^{-s})$$

è infinito, perché $(s-1)Z_R(s)$ tende ad 1. Studiando in modo simile lo sviluppo del suo logaritmo // si trova che il primo termine

$$(B) \qquad \sum_P P^{-s}$$

tende per $s=1$ ad ∞.
[54]Per un qualsiasi intero razionale $\underline{n}$ non divisibile per l porremo, come si è posta per i primi $P \neq \ell$,

$$n_\ell = \varepsilon^{ind\, P} \quad \text{ove} \quad \varepsilon = \ell^{\frac{2\pi i}{\ell-1}}.$$

Se g è un numero primitivo per $\underline{\ell}$ l'$ind\, n$ è un numero tale che $g^{ind\, n} \equiv n \pmod{\ell}$.
Se n, n' sono due interi razionali non divisibili per l, si ha

---

[51] *e.c.* e *cor. inf.* a lato: entro parentesi si aggiunga "moltiplicato per x".
[52] Nota inserita da Fubini a p.d.p.: *Disp. 21 Teoria dei numeri*.
[53] Invece di $\frac{1}{2}\sum_P(P^{-2s}+P^{-3s}+P^{+4s}+\cdots)$ leggasi $\frac{1}{2}\sum_P(P^{-2s}+P^{-3s}+P^{-4s}+\cdots)$.
[54] Bianchi 1911-12, cap. VIII, §71, p. 317-322. Bianchi introduce tale notazione e sviluppa questi argomenti nel paragrafo *Le somme di Gauss e le espressioni finite per numero h delle classi.*

$$n_l n'_l = (n\, n')_l.$$

Questa proprietà si conserva anche se conveniamo che $n_l = 0$, quando $\underline{n}$ è divisibile per ℓ. Supposto che n sia un intero primo con ℓ, aggiungiamo a B la quantità A moltiplicata per[55] $\frac{1}{n_e^m}$.

Si troverà

$$(C) \qquad \sum_P \left\{ P^{-s} \left[1 + \sum_{m=1}^{\ell-2} (P_\ell n_\ell^{-1})^m \right] \right\}.$$

La quantità tra [ ] è una progressione geometrica che vale $\ell - 1$ se $P_\ell n_\ell^{-1} = 1$, e vale negli altri casi[56]

$$\frac{1 - \left[P_\ell n_\ell^{-1}\right]^{\ell-1}}{1 - P_\ell n_\ell^{-2}}$$

che è nullo, perché P_ℓ ed n_ℓ sono radici $(\ell-1)^{esime}$ // dell'unità. Pertanto, siccome la C ha per $s = 1$ limite infinito, e quindi essa è una serie effettiva, e non una somma, devono esistere infiniti numeri primi razionali P tali che $P_\ell n_\ell^{-1} = 1$ ossia tali che

$$\varepsilon^{ind\, P - ind\, n} = 1$$

ossia tali che

$$ind\, P \equiv ind\, n\ (mod\ \ell - 1)$$

ossia che

$$P \equiv n\ (mod\ \ell).$$

In altre parole nella progressione

$$n_1 n + \ell_1 n + 2\ell_1 n + 3\ell \ldots\ldots\ldots$$

dove $\underline{n}$ è un numero razionale non divisibile per il numero primo ℓ_1 vi sono infiniti numeri primi.[57]

Studiando il corpo algebrico generato da $\sqrt[\ell]{1}$, quando $\underline{\ell}$ non è primo, si giunge allo stesso risultato con la sola ipotesi che n, ℓ siano primi tra di loro. In ciò appunto consiste il teorema di Dirichlet sulle progressioni aritmetiche (*). //

(*) **Nota**: Per completare la parte generale della teoria dei corpi algebrici si dovrebbe studiare la teoria di un corpo algebrico contenuto in un altro (la cosiddetta teoria del corpo relativo[58]). Non abbiamo qui il tempo di occuparcene.

[55] *e.c.* e *cor. inf.* sul lato destro della pagina: $\frac{1}{n_\ell^m}$.

[56] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale: $\frac{1-\left[P_\ell n_\ell^{-1}\right]^{\ell-1}}{1-P_\ell n_\ell^{-2}}$.

[57] Dirichlet 1877 (trad. 1881), suppl. VI, §137, p. 350-352.

[58] Tale teoria viene invece affrontata in Hilbert 1897 (trad. 1911), cap. V, §14-16, p. 34-40 e in Sommer 1907 (trad. 1911), cap. 5 – *Le corps relatif,* p. 303-350.

Capitolo IX – I corpi quadratici

Ci siamo già occupati di un tale corpo, e provato che esso si può sempre pensare generato da $\sqrt{m}$, dove $\underline{m}$ è un intero privo di fattori quadratici. Una base del corpo è[1]

$$\omega_1 = 1, \qquad \omega_2 = \sqrt{m} \qquad se\ m \not\equiv 1\ (mod\ 4)$$
$$\omega_1 = 1, \qquad \omega_2 = \frac{1}{2}\left[1 + \sqrt{m}\right] \quad se\ m \equiv 1\ (mod\ 4).$$

Nel primo caso il discriminante[2] d del corpo vale $4m$; nel secondo vale $\underline{m}$.
Un corpo $K(\sqrt{m})$ coincide col coniugato $K(-\sqrt{m})$.
Se j è un ideale di K, il coniugato j' appartiene pure a K. Si può parlare pertanto del prodotto jj', che sarà la norma di j.

§.1 *Ideali primi*

Sia P un primo razionale. Nel corpo K esso si decomporrà in ideali primi; sia per es.

$$P = p_1 p_2 \dots p_r.$$

P è coniugato a se stesso. Perciò $Nm\ P = P^2$. Ma

$$Nm\ P = Nm\ p_1\ Nm\ p_2 \dots Nm\ p_r.$$

Pertanto le $Nm\ p_1, Nm\ p_2, \dots, Nm\ p_r$ saranno tutte divi//sori di P^2; se una di esse coincide con P^2, sarà chiaramente $r = 1$; e perciò P è <u>primo</u> anche in $K(\sqrt{m})$. Se nessuna delle $Nm\ p$ coincide con P^2, allora tutte sono uguali a P; e sarà $r = 2$. In tal caso

$$P = p_1 p_2$$
$$P = Nm\ p_1 = Nm\ p_2 = p_1 p_1' = p_2 p_2'$$

dove p_i' è l'ideale coniugato[3] di p_i $(i = 1,2)$. Dalla $p_1 p_1' = p_2 p_2'$ segue che, o $p_2 = p_1$ oppure $p_2 = p_1'$.
In conclusione vi sono tre casi possibili[4]:
1°) P è primo anche in $K(\sqrt{m})$; $Nm\ P = P^2$. Il numero P è in K di secondo grado.
2°) $P = p^2$, dove p è un ideale primo di K, tale che $pp' = Nm\ p = P$. Cioè p coincide con l'ideale coniugato p'.
3°) $P = pp'$, dove $p \neq p', Nm\ p = P, p$ è un ideale primo di K di <u>primo</u> grado.
Il secondo caso si presenta, come sappiamo, allora e allora soltanto che p sia un divisore di d. Esclusi i divisori di $\underline{d}$, basta perciò saper distinguere il primo caso (dei primi razionali P indecomponibili in K) dal terzo (dei primi P decomponibili). //
Bisogna studiare le congruenze cui soddisfa un intero generico del corpo $(mod\ P)$. Poiché però ω_2 ha per discriminante proprio il discriminante $\underline{d}$ del corpo è facile riconoscere che basta al numero generico sostituire l'intero ω_2. Questo numero soddisfa alla:

---

[1] Gazzaniga 1903, cap. IX, p. 225. Gazzaniga esprime qui la proprietà enunciata da Fubini in modo diverso, ma del tutto equivalente: infatti egli non parla di base del corpo quadratico bensì della "forma" che gli elementi di tale corpo possono assumere. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §6, p. 21.
[2] Sommer 1907 (trad. 1911), cap. 2, §6, p. 24.
[3] Hilbert 1897 (trad. 1911), cap. III, §7, p. 22; viene qui fornita una definizione di ideale coniugato più generale di quella di Fubini.
[4] Dirichlet 1877 (trad. 1881), suppl. XI, §180, p. 595.

$$x^2 - m = 0 \qquad (se\ m \not\equiv 1\ [mod\ 4]) \quad (d = 4m)$$
$$(2x-1)^2 - m = 0\ (se\ m \equiv 1\ [mod\ 4]).$$

Studiamo il primo caso.
La congruenza $x^2 - m \equiv 0\ (mod\ P)$ è riducibile, e ammette radici se
α) m non è divisibile per P, ma è residuo di P; ed anzi in tal caso le due radici μ_1, μ_2 sono distinte $(mod\ P)$ se P è dispari; se invece $P = 2$, le due radici coincidono $(mod\ 2)$.
β) m è divisibile per P; la congruenza ammette una sola radice. Dunque[5]
1° Caso) $m \not\equiv 1\ (mod\ 4)$ $d = 4m$
Se P è un divisore di $\underline{d}$ (cioè se $P = 2$, oppure P è un divisore di m), allora la congruenza ammette due radici uguali. P è uguale al prodotto di due ideali primi uguali, cioè P è il quadrato p^2 di un ideale primo $\underline{p}$. //
Se μ è la radice, si ha $p = (P, \omega_2 - \mu) = \left(P, \sqrt{m} - \mu\right)$. È $\mu = 1$, se $P = 2$ ed m dispari. Negli altri casi $\mu = 0$. È facile riconoscere che p coincide col coniugato. Se P non divide $4m$, se m è residuo di P, e quindi anche d è residuo di P, allora $x^2 - m \equiv 0$ ha due radici <u>distinte</u> $\mu_1, \mu_2\ (mod\ P)$ e si ha $P = p_1 p_2$, ove $p_1 = \left(P, \sqrt{m} - \mu_1\right), p_2 = (P, \sqrt{m} - \mu_2)$ sono ideali primi distinti.
Infine se P non divide $4m$, ed m è <u>non residuo</u> di P, allora P è primo anche nel nostro corpo.
In modo affatto simile si studia il caso $m \equiv 1\ (mod\ 4)$. Resta da questi calcoli confermato anche che soltanto i P divisori di $\underline{d}$ sono il quadrato di un ideale primo. Noi porremo, estendendo il simbolo di Legendre
$\left(\frac{d}{P}\right) = 1$ se $\underline{d}$ non è divisibile per P, ed è residuo di P, e P è primo dispari,
$\left(\frac{d}{P}\right) = -1$ se $\underline{d}$ non è divisibile per P, é non residuo di P, e P è primo dispari,
$\left(\frac{d}{P}\right) = 0$ se d è divisibile per P (con P pari o dispari),
$\left(\frac{d}{2}\right) = 1$ se $d \equiv 1\ (mod\ 8)$, cioè $\underline{d}$ dispari e residuo di 8,
$\left(\frac{d}{2}\right) = -1$, se $\underline{d}$ è dispari e non residuo di 8.
Si trova in ogni caso che P è primo, o è il quadrato di un ideale primo, o è decomponibile // in fattori distinti secondo che $\left(\frac{d}{P}\right) = -1$, oppure $\left(\frac{d}{P}\right) = 0$, oppure $\left(\frac{d}{P}\right) = +1$.

§.2 *Ideali di un corpo quadratico*

Per trovare il tutti gli ideali di un corpo quadratico, o no si ricordi che in ogni classe di ideali vi è un ideale di norma $< \rho^{\sqrt{d}}$, dove ρ è un fattore numerico che dipende solo dal grado del corpo; si cerchino tutti gli ideali di norma $< \rho^{\sqrt{d}}$, che sono in numero finito, ecc. ecc.
Noi qui ci limitiamo ai corpi quadratici $K(\sqrt{m})$.
Ogni ideale j contiene le norme dei suoi numeri, cioè contiene degli interi razionali. Sia α_1, α_2 una base dell'ideale j e siano $x\alpha_1 + y\alpha_2$ (con x, y interi razionali) gli interi di j. Questi interi saran dunque rappresentati dalla rete dei punti a coordinate x, y intere razionali.
Sia $\lambda = x_1\alpha_1 + y_1\alpha_2$ un intero razionale di j, che sarà rappresentato dal punto A di coordinate x_1, y_1. Sul segmento OA che congiunge l'origine O ad A possono esistere altri punti della rete, i quali però saran tutti immagine di interi razionali di j. Quello di questi punti,

[5] Bianchi 1920-21, cap. II, §32, p. 208.

che è il più prossimo ad O, si può assumere come vertice di // un parallelogramma della rete. Ne segue dunque che si può sempre scegliere una base di j in modo che uno dei numeri base sia un intero razionale r_2. Sia (posto $\omega_2 = \omega$)

$$(r_2, r_1 + r\omega)$$

la base del nostro ideale. I numeri dell'ideale saranno i numeri $(xr_2 + yr_1) + yr\omega$ con x, y interi razionali.
Il numero $r_2\omega$ deve appartenere all'ideale; pertanto r_2 sarà un multiplo di r. Cioè[6] $r_2 = K'_r$ con r intero razionale.
D'altra parte se ω' è il coniugato di ω, anche $(r_1 + r\omega)\omega' = r\omega\omega' + r_1\omega'$ è un numero di j. Poiché $\omega\omega'$ è razionale, anche r_1 sarà un multiplo di r. E si potrà porre $r_1 = hr$ con h intero razionale. L'ideale j si può dunque sempre pensare del tipo

$$r(K, h + \omega)$$

con h, K, r interi razionali. Questi numeri devono soddisfare alla sola condizione che $(h + \omega)\omega$, o, ciò che è lo stesso, che $(h + \omega)\omega'$ sia una combinazione lineare a coefficienti interi razionali di K e di $h + \omega$. //

Se $m \not\equiv 1\ (mod\ 4)$, e quindi $\omega = \sqrt{m}$, ciò equivale a dire che $h\sqrt{m} + m = h(\omega + h) + m - h^2$ è una tale combinazione di K ed $h + \omega$. Dunque occorre e basta che $m - h^2$ sia multiplo di K. Se invece $m \equiv 1\ (mod\ 4)$ si prova in modo simile che occorre e basta che $h^2 + h + \frac{1-m}{4}$ sia multiplo di K.
[7]Se P primo razionale è primo anche nel corpo, allora P, come ideale primo del corpo, è l'ideale $(P, P\omega)$. Se P non è primo nel corpo, ognuno dei suoi fattori sarà un ideale del tipo $(P, h + \omega)$, dove h si deve determinare in modo da soddisfare alla precedente condizione. Si possono così ritrovare in modo diretto i risultati sopra enunciati per i numeri primi.[8]

§.3 *Ideali ambigui*[9] *e applicazioni*

Così si chiama un ideale, che coincide col coniugato, e che non è divisibile per alcun numero razionale.
Troviamo tali ideali, p. es. nell'ipotesi che m sia primo e che $m \equiv 1\ (mod\ 4)$. Un tale ideale avrà una base $(K, h + \omega)$ con h, K interi razionali soddisfacenti alla

$$(1) \qquad h^2 + h + \frac{1-m}{4} \equiv 0\ (mod\ K).$$

// Affinché tale ideale sia ambiguo, il numero $h + \omega'$ deve appartenere allo stesso ideale. Tale numero vale[10]

---

[6] *e.c.* e *del.*: $r_2 = K_r$.
[7] Bianchi 1920-21, cap. II, §32, p. 215.
[8] Sommer 1907 (trad. 1911), cap. 2, §14, p. 60-66; il matematico tedesco, all'interno della sezione *Les divideurs des nombres premiers rationnels dans le corps* $k(\sqrt{m})$, affronta proprio tale studio.
[9] Gazzaniga 1903, cap. IX, p. 195. Gazzaniga dà qui la definizione di "classe ambigua", introducendo poi nei capitoli successivi il concetto di ideale come modulo che soddisfa particolari proprietà. Cfr. anche Sommer 1907 (trad. 1911), cap. 2, §30, p. 158-167; il matematico tedesco tratta tale argomento all'interno di un discorso più ampio sulle *classes ambiges*.
[10] *e.c.* e *cor. sup.*: invece di $h + \frac{1\sqrt{m}}{2}$ leggasi $h + \frac{1-\sqrt{m}}{2}$.

$$h + \frac{1\sqrt{m}}{2} = h + 1 - \frac{1 + \sqrt{m}}{2} = h + 1 - \omega = 2h + 1 - (h + \omega).$$

Occorre dunque e basta che $2h + 1$ sia multiplo di K.
Per (1)

$$(2h + 1)^2 \equiv m \ (mod\ 4K).$$

Quindi m deve essere divisibile per K. Essendo per ipotesi $\underline{m}$ primo, dovrà essere $K = 1$, oppure
$K = m$. Se $K = 1$, l'ideale contenendo il numero 1, coincide con (1), cioè col corpo stesso. Nel secondo caso il nostro ideale è

$$(m, h + \omega).$$

Togliendo da $h + \omega$ un multiplo rm di m, si ottiene una nuova base

$$(m, h + \omega - rm)$$

dell'ideale. Possiamo scegliere l'intero razionale, r in modo che $0 \leq h - rm < m$. Chiamando h' l'intero $h - rm$, abbiamo che il nostro ideale è $(m, h' + \omega)$ con $0 \leq h' < m$, e con $2h' + 1$ multiplo di m. Dunque, essendo $h' < m$, dovrà essere $2h' + 1 = m$, cioè $h' = \frac{m-1}{2}$; e il nostro idea//le sarà

$$\left(m, \frac{m-1}{2} + \frac{1 + \sqrt{m}}{2}\right) = \left(m, \frac{m + \sqrt{m}}{2}\right)$$

Perché $\omega = \frac{1+\sqrt{m}}{2}$.
Questo ideale contiene il numero[11] $\sqrt{m} = 2\frac{(m+\sqrt{m})}{2}_{m}$.
E, poiché d'altra parte sia m che $\frac{m+\sqrt{m}}{2}$ sono due multipli di $\sqrt{m}$, tale ideale coincide con $\left(\sqrt{m}\right)^2$.
Dunque: <u>Se m è primo ed è congruo ad $1\ (mod\ 4)$ cioè se d è un numero primo, il corpo contiene i soli ideali ambigui</u> (1) e $(\sqrt{d})$.
Questo teorema vale anche se $m = 2$, e quindi $d = 8$. Il corpo[12] $K(\sqrt{4})$ contiene i soli ideali ambigui (1) e $(\sqrt{2})$.
Se d è primo e positivo l'unità fondamentale ε ha per norma -1. Infatti, se $Nm\ \varepsilon = \varepsilon\varepsilon' = 1$, sarebbe $\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}$. Gli ideali $(1 + \varepsilon)$ ed $(1 + \varepsilon')$ coinciderebbero. E perciò, se $\underline{r}$ è un intero razionale opportuno, sarebbe per quanto precede

$$(1 + \varepsilon) = (r\sqrt{m}) \text{ oppure } (1 + \varepsilon) = (r)$$

cosicché

$$1 + \varepsilon = r\eta\sqrt{m} \text{ oppure } 1 + \varepsilon = r\eta$$

[11] *e.c.* e *cor. sup.*: $\sqrt{m} = 2\frac{(m+\sqrt{m})}{2} - m$.
[12] *e.c.* e *cor. sup.*: $K(\sqrt{2})$.

dove η è un'unità.
Sarebbe dunque //

$$\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'} = -\frac{\eta}{\eta'} \text{ oppure } \varepsilon = \frac{1+\varepsilon}{1+\varepsilon'} = \frac{\eta}{\eta'}.$$

Ora η o è una potenza di ε, oppure $|\eta| = 1$, ed η è una radice dell'unità. Nel primo caso $Nm\,\eta$ sarebbe una potenza di $Nm\,\varepsilon = 1$; cioè $Nm\,\eta = 1, \eta = \frac{1}{\eta'}$ e quindi $\pm\varepsilon = \eta^2$. Dunque ε, che sarebbe una potenza dell'unità η, non sarebbe fondamentale. Ma non può neanche avvenire che η sia una radice dell'unità, altrimenti altrettanto avverrebbe di $\varepsilon = \pm\frac{\eta}{\eta'}$, che non sarebbe quindi l'unità fondamentale.
Se d è primo, il numero h delle classi è dispari.[13]
Ogni ideale j possiede un periodo r: il minimo intero positivo tale che j^r sia principale. E sappiamo che r è un divisore di h. Ne viene che, se h è dispari, tutti i periodi r sono dispari. È facile invertire il teorema, provando che, se i periodi sono dispari, anche h è dispari. Se dunque supponiamo h pari, esiste almeno un ideale j il cui periodo è un numero pari $2s$; cosicchè j^{2s} è principale, mentre j^s non lo è. Posto $\ell = j^s$, abbiamo dunque che ℓ non è principale, mentre è principale $\ell^2 = \ell\ell$. // Poiché anche $\ell\ell'$ è principale, ne segue che ℓ e ℓ' sono equivalenti, che cioè esistono due interi α, β tali che

$$\alpha\ell = \beta\ell'.$$

Poiché $Nm\,\ell = Nm\,\ell'$, ne segue che $|Nm\,\alpha| = |Nm\,\beta|$ cioè che $Nm\,\alpha = \pm Nm\,\beta$. Sostituendo casomai a β il numero $\varepsilon\beta$ (ricordo che $Nm\,\varepsilon = -1$) (col che non muta l'ideale $\beta\ell'$), ne segue che si può supporre $Nm\,\alpha = Nm\,\beta$ ossia $\alpha\alpha' = \beta\beta'$.
La $\alpha\ell = \beta\ell'$ diventa perciò

$$\alpha(\alpha' + \beta')\ell = \alpha'(\alpha + \beta)\ell'$$

perché

$$\frac{\alpha}{\beta} = \frac{\alpha(\alpha' + \beta')}{\alpha'(\alpha + \beta)}.$$

Dunque l'ideale $L = \alpha(\alpha' + \beta')l$, che non è principale, perché l non è principale, sarebbe uguale al suo coniugato; e perciò diviso per un intero razionale, diventerebbe ambiguo e quindi, come già vedemmo, principale: ciò che è assurdo.

c.d.d.

Osserv.[azione] Il teorema degli ideali ambigui vale se d è primo, anche negativo. Il teorema sulla norma dell'unità fondamentale non vale se $d < 0$, perché in tal caso manca l'unità fondamentale e del resto la norma di ogni numero è positiva. Il teorema sul numero delle classi vale se d è primo, anche quando d è negativo perché, se $\alpha\ell = \beta\ell'$, allora $Nm\,\alpha = \pm Nm\,\beta$. Poiché, se $d < 0$, le norme di tutti i numeri sono positive segue $Nm\,\alpha = Nm\,\beta$. E la dimostrazione continua come sopra. //

[13] Sommer 1907 (trad. 1911), cap. 2, §23, p. 117; l'autore dedica l'intero paragrafo *Les corps dont le nombre des classes est impair* alla dimostrazione di tale risultato.

§.4 ***Il teorema di reciprocità***[14]

Noi dimostreremo più avanti questo teorema in generale, ma per dare un esempio della fecondità dei nostri numeri, lo dimostriamo qui in qualche caso come conseguenza della teoria del corpo quadratico[15].

Caso 1°) Il corpo[16] $K(\sqrt{-1})$

Sappiamo già, ed è facile provare direttamente che ogni ideale è principale.
Se il primo razionale P è decomponibile, allora
1°) $P = (x + iy)(x - iy) = x^2 + y^2$ (*) con x, y interi razionali.
2°) la congruenza $x^2 + 1 \equiv 0\ (mod\ P)$ è risolubile, cioè -1 è residuo di P, come segue dai nostri studii generali.
3°) Se P è dispari, dalla $P = x^2 + y^2$ segue che uno ed uno solo degli interi x, y è dispari, ossia che $P \equiv 1\ (mod\ 4)$. //
Viceversa sia $P \equiv 1\ (mod\ 4)$. Allora in $K(\sqrt{P})$ per i teoremi del §3 esiste una unità

$$x + y\frac{1 + \sqrt{P}}{2}$$

di norma -1. Cosicché esistono due interi razionali x, y tali che

$$\left(x + \frac{y}{2}\right)^2 - \frac{P}{4}y^2 = -1,$$

ossia che

$$(2x + y)^2 + 4 \equiv 0\ (mod\ P).$$

Sia π un intero tale che $2\pi \equiv 1\ (mod\ P)$. Sarà:

$$\pi^2(2x + y)^2 + (2\pi)^2 \equiv 0\ (mod\ P).$$

Cioè il numero intero

$$X = \pi(2x + y)$$

soddisfa alla

$$X^2 + 1 \equiv 0\ (mod\ P).$$

Cioè -1 è residuo quadratico di P, e quindi P è decomponibile in $K(\sqrt{-1})$.

---

[14] Dirichlet 1877 (trad. 1881), cap. III, §42-52, p. 83-121; suppl. I, §115, p. 292-299; suppl. XI, §154, p. 403-406. Il teorema di reciprocità è dimostrato con ben 4 metodi differenti all'interno delle *Vorlesungen*. Cfr. anche Gauss 1801, sez. IV, art. 131, 132 p. 99-101 e sez. V, art. 261, 262, p. 291-294. Cfr. infine Sommer 1907 (trad. 1911), cap. 2, §24-25, p. 117-129.

[15] Gauss 1801, sez. IV, art. 131, p. 99, 100. Quanto affrontato da Fubini in questa sezione si riconduce facilmente al teorema fondamentale della teoria dei residui quadratici delle *Disquisitiones*, dal quale "omnia fere quae de residuis quadraticis dicis possunt, huic theoremati innituntur" e il cui enunciato è il seguente: "Si *p* est numerus primus formae *4n+1*, erit *+p*, si vero *p* formae *4n+3*, erit *–p* residuum vel non residuum cuiusuis numeri primi qui positive acceptus ipsius *p* est residuum vel non residuum". Il Nostro, tuttavia, dimostra la LRQ nel caso più generale all'interno dell'ultimo capitolo delle *Lezioni*, nel contesto più ampio dei campi ciclotomici.

[16] Gazzaniga 1903, cap. IX, p. 241-244. Gazzaniga esamina qui approfonditamente le proprietà del corpo $K(\sqrt{-1})$.

Corpo $K(\sqrt{2})$

Se $x^2 - 2 \equiv 0\ (mod\ P)$ è risolubile (P =primo dispari) cioè se 2 è residuo di P, allora P è decomponibile in $K(\sqrt{2})$; e, poiché ogni ideale di tal corpo è principale, il numero $\pm P$ sarà prodotto di due interi coniugat i $x \pm y\sqrt{2}$; cioè $\pm P = x^2 - 2y^2$. Poiché //

[17] P è dispari, x sarà un numero dispari del tipo $4n \pm 1$. D'altra parte y^2 diviso per 8 (essendo y intero razionale) dà per resto uno dei numeri $1, 4$. Quindi $x^2 - 2y^2$ è $(mod\ 8)$ congruo con ± 1, cioè $P \equiv \pm 1\ (mod\ 8)$.

Viceversa, sia $P \equiv \pm 1\ (mod\ 8)$. Poniamo $P_1 = \pm P \equiv 1\ (mod\ 8)$.

La congruenza $x^2 - P_1 \equiv 0\ (mod\ 2)$ ha la soluzione[18] $x \equiv 1$; e quindi 2 è decomponibile in $K\sqrt{P_1}$ nel prodotto di due ideali j, j'.

$$(2) = jj'.$$

Il numero delle classi essendo un numero dispari $2g + 1$, sarà

$$2^{2g+1} = j^{2g+1} j'^{(2g+1)}$$

dove le potenze del secondo membro indicano ideali principali generati da due interi coniugati

$$x + \frac{y}{2} \pm \frac{y}{2}\sqrt{P_1}.$$

Se $P_1 < 0$ questi interi hanno norma positiva; se $P_1 > 0$, li possiamo rendere a norma positiva, moltiplicandoli per l'unità fondamentale (la cui norma è -1) perché moltiplicando un intero per una unità, non si cambia l'ideale principale da esso definito. Ora poiché[19] //

$$2^{2g+1} = \left(x + \frac{y}{2} + \frac{y}{2}\sqrt{P_1}\right)\left(x + \frac{y}{2} - \frac{y}{2}\sqrt{P_4}\right) = \left(x + \frac{y}{2}\right)^2 - P_1\frac{y^2}{4} == \left(x + \frac{y}{2}\right)^2 \pm P\frac{y^2}{4}$$

cioè

$$(2x + y)^2 \equiv 2^{2g+1} 2\ (mod\ P).$$

Se π è un intero tale che $2^{g+1}\pi \equiv 1\ (mod\ \pi)$ allora $z = \pi(2x + y)$ soddisfa alla

$$z^2 \equiv 2\ (mod\ P)$$

cioè 2 è residuo di P. Dunque 2 è residuo di P soltanto se $P \equiv \pm 1\ (mod\ 8)$.

[20] **Teorema di reciprocità per P, Q primi e $P \equiv 1\ (mod\ 4)$.**

Se P è residuo di Q, cioè se

$$x^2 - P \equiv 0\ (mod\ Q)$$

è risolubile, allora Q è decomponibile in $K(\sqrt{P})$.

Cioè

---

[17] La pagina del ms. che inizia qui e termina con "Ora poiché" è del tutto illeggibile. Probabilmente in fase di litografazione, non era stata posizionata correttamente la carta copiativa, oppure essa risultata esausta. Conscio di questo disguido, Fubini riscrive completamente tale foglio nell'*e.c.*

[18] *lapsus* del curatore: leggasi $x = 1$.

[19] *e.c.* e *cor. inf.* sul lato destro della pagina: invece di $-\frac{y}{2}\sqrt{P_4}$ leggasi $-\frac{y}{2}\sqrt{P_1}$.

[20] Gazzaniga 1903, cap. V, p. 98, prop. 11).

$$Q = jj'$$

dove j, j' sono ideali di $K(\sqrt{Q})$. Poiché questo corpo ha un'unità di norma negativa ed ha un numero dispari $2g+1$ di classi, si trova, in modo analogo a quanto sopra che

$$Q^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{P}{4}y^2, \qquad ossia$$

$$(2Q)^2 Q \equiv (2x+y)^2 \ (mod\ P)$$

se π è un intero tale che $2Q\pi \equiv 1\ (mod\ P)$ allora // $z = \pi(2x+y)$ soddisfa alla[21]

$$z^z \equiv Q\ (mod\ P)$$

cioè Q è residuo di P.
In modo identico si prova, che, se Q è residuo di P anche P è residuo di Q almeno nel caso $Q \equiv 1\ (mod\ 4)$. Se invece $Q \equiv 3\ (mod\ 4)$ allo stesso risultato si perviene nel modo seguente. Dall'ipotesi che Q è residuo di P segue che, essendo -1 residuo di P perché $P \equiv 1\ (mod\ 4)$, che $-Q$ è pure residuo di P, che cioè è risolubile la congruenza[22] $z^z \equiv -Q\ (mod\ P)$, ossia che P è decomponibile nel corpo $K(\sqrt{-Q})$. La dim.[ostrazione] segue come sopra, osservando che $-Q \equiv 1\ (mod\ 4)$.

[23]**Teorema di reciprocità se $P \equiv Q \equiv 3\ (mod\ 4)$ e P, Q primi.**
Se P è non residuo di Q, allora, poiché -1 è non residuo di Q, il numero $-P$ sarà residuo di Q, cioè sarà risolubile la $z^2 \equiv -P\ (mod\ Q)$, cioè Q sarà decomponibile in $K\left(\sqrt{-P}\right)$. Se ne deduce, come sopra, la risolubilità di[24]

$$z^z \equiv Q\ (mod\ P)$$

e quindi che Q è residuo di P. Per dimostrare che viceversa, se Q è residuo di P, // allora P è non residuo di Q, si deve ricorrere al corpo $K(\sqrt{PQ})$, dove è $PQ \equiv 1\ (mod\ 4)$. Rinvio per tale dimostrazione al trattato del Sommer[25], perché noi nel prossimo capitolo daremo un'altra dimostrazione completa del teorema di reciprocità.

(*) **Nota**: I due fattori di sono principali, cioè sono interi coniugati del corpo.

[21] *e.c.* e *cor. sup.*: $z^2 \equiv Q\ (mod\ P)$.
[22] *e.c.* e *cor. sup.*: $z^2 \equiv -Q\ (mod\ P)$.
[23] *Ibid.*, prop. 12).
[24] *e.c.* e *cor. sup.*: $z^2 \equiv Q\ (mod\ P)$.
[25] Fubini allude qui a Sommer 1911.

§.5 ***L'ultimo problema di Fermat***[26]

Osservazioni preliminari.

È identicamente

$$x^3 - y^3 = (x-y)(x^2+xy+y^2) = (x-y)(x-\omega y)(x-\omega' y)$$

essendo ω, ω' le radici di $\omega^2 + \omega + 1 = 0$, e precisamente p. es.[27]

$$\omega = -\frac{1+\sqrt{-3}}{2};\ \omega' = -1-\omega = \frac{1}{\omega}.$$

Siamo indotti allo studio del corpo[28] $K\left(\sqrt{-3}\right)$, di cui una base è costituita dai numeri $1, \omega$. Cerchiamo le unità del corpo.

Se α, β sono interi razionali, un intero del corpo è del tipo $\alpha + \beta\omega$, la cui norma è $\left(\alpha - \frac{\beta}{2}\right)^2 + 3\frac{\beta^2}{4}$. L'intero $\alpha + \beta\omega$ è un'unità, se questa norma vale 1.

Allora β può essere nullo; se così è $\alpha = \pm 1$. Se β non è nullo, sarà $\beta = \pm 1$; $\left(\alpha - \frac{\beta}{2}\right)^2 = \frac{1}{4}; \alpha - \frac{\beta}{2} = \pm\frac{1}{2}; // \ \alpha = \frac{\beta}{2} \pm \frac{1}{2}$. Le unità del corpo sono pertanto

$$\pm 1;\ \pm(1+\omega) = \mp\omega';\ \pm\omega.$$

Osservo che[29]

$$\lambda = 1 - \omega = \frac{3+\sqrt{-3}}{2} = \sqrt{3}\frac{1+\sqrt{-3}}{2} = -\sqrt{-3}\omega.$$

Poiché ω è un'unità, $(\lambda) = \left(\sqrt{-3}\right), (\lambda)^2 = (3);\ \lambda^3 = (3\sqrt{-3})$. Un sistema completo di numeri incongrui $(mod\ \lambda)$ è composto di $3 = Nm\,\lambda$ numeri; perciò, essendo $0, 1, -1$ tra loro incongrui $(mod\ \lambda)$:

Ogni intero del corpo è $(mod\ \lambda)$ congruo con 0, o con ± 1.

Un sistema completo di numeri incongrui $(mod\ \lambda^2)$ è composto di $(Nm\,\lambda)^2 = 9$ numeri; tra essi ve ne sono perciò $6 = 9 - 3$ non divisibili per λ. Poiché le 6 unità $\pm 1, \pm\omega, \pm(1+\omega)$ sono incongrue $(mod\ \lambda^2)$ e non divisibili per λ, ogni intero del corpo è $(mod\ \lambda^2)$ congruo con una delle unità $\pm 1, \pm\omega, \pm(1+\omega)$. I cubi di queste sono sempre ± 1.

Ogni intero del corpo essendo $(mod\ \lambda)$ congruo con 0 o con ± 1, esso è del tipo λz oppure $\pm 1 + \lambda z$, ove z è un intero. Il suo cubo è perciò del tipo $\lambda^3 z^3$ oppure $\pm 1 \pm 3\lambda^2 z^2 + 3\lambda z + \lambda^3 z^3$; e, poiché $(3) = (\lambda^2)$, il cubo di ogni intero del corpo è $(mod\ \lambda^3)$ congruo con 0 oppure con ± 1. Ne segue che: //

Se la somma dei cubi di tre interi del corpo è congrua a zero $(mod\ \lambda^3)$, almeno uno dei tre numeri è congruo a zero $(mod\ \lambda)$, cioè è divisibile per λ.

L'equazione

---

[26] Fubini per la stesura di questo paragrafo fa riferimento principalmente a Kummer che attorno al 1850 trovò la sua famosa dimostrazione dell'UTF per quelli che chiamò 'primi regolari', includendo tutti i primi minori di 100 (eccetto 37, 59 e 67). Cfr. anche Gauss 1801, sez. V, art. 293, p. 348, 349: il matematico tedesco prova qui un enunciato equivalente ad un caso particolare dell'UTF, dimostrando che ogni intero $\equiv 3\ (mod\ 8)$ può essere scritto come somma di tre quadrati. Cfr. infine Sommer 1907 (trad. 1911), cap. 3, §34, p. 184-201.

[27] *e.c.* e *cor. inf.* nel lato destro della pagina: $\omega = -\frac{1+\sqrt{-3}}{2};\ \omega' = -1-\omega = -\frac{1-\sqrt{-3}}{2}$.

[28] Gazzaniga, 1903, Cap. IX, p. 245-248. Gazzaniga studia qui in modo approfondito il corpo $K\left(\sqrt{-3}\right)$.

[29] *e.c.* e *cor. sup.*: invece di $\sqrt{3}$ leggasi $\sqrt{-3}$.

$$x^n + y^n = z^n$$

è per n intero razionale maggiore di 2 irresolubile con valori interi razionali delle x, y, z. Questo celebre teorema di Fermat, prima sorgente della teoria dei numeri interi algebrici, non è dimostrato in generale, per quanto i risultati di Kummer[30] lo provino, tra l'altro, per tutti i valori di $n \leq 100$. Noi lo dimostreremo qui nel caso $n \equiv 0 \ (mod\ 3)$ con un metodo analogo a quello seguito da Kummer in casi più generali. Notiamo che, se $n = pq$, dove p è primo, dalla nostra equazione segue

$$X^p + Y^p = Z^p$$

Con $X = x^q, Y = y^q, Z = z^q$ interi razionali. Basterà dimostrare il teorema quando n vale 4 od è un primo dispari razionale per averlo // dimostrato in generale; p. es. basterà provarlo per $n = 3$, perché il teorema risulti provato anche quando n è multiplo di 3. Notiamo che, come si vede scambiando z in $-z$, nella $x^3 + y^3 = z^3$ le tre incognite hanno un ufficio affatto simmetrico. Noi la scriveremo nella forma $z^3 = x^3 - y^3$.
Dimostreremo[31] che in $K(\sqrt{-3})$ non esistono tre interi x, y, z tali che $x^3 - y^3 = z^3$; con ciò resterà provato anche un teorema più generale di quello di Fermat, che vogliamo dimostrare. Intanto, se due dei tre interi, x, y, z hanno un fattore intero n comune, anche il terzo intero è divisibile per n; e noi dividendo per n^3, potremmo ridurci all'equazione

$$x_1^3 - y_1^3 = z_1^3$$

con $x_1 = \frac{x}{n}, y_1 = \frac{y}{n}, z_1 = \frac{z}{n}$ interi. Così continuando, potremmo ridurci al caso che due degli interi x, y, z non abbiano fattori interi comuni.
Essendo in particolare $(x)^3 + (-y)^3 + (-z)^3 \equiv 0 \ (mod\ \lambda^3)$, per una delle osservazioni preliminari, segue che uno degli x, y, z e, per quanto si è detto ora, uno solo degli x, y, z è divisibile per λ. // Sia, p. es., z divisibile per λ; e sia precisamente $\lambda^n \ (n \geq 1)$ la massima potenza di λ che divide z. E sia $z = \lambda^n Z$ con Z intero non divisibile per λ. Sarà $x^3 - y^3 = \lambda^{3n} Z^3$ con $n \geq 1$ e con[32] x, y, z non divisibili per λ.
Io proverò senz'altro impossibile la

(1) $\qquad x^3 - y^3 = \varepsilon \lambda^{3n} Z^3$ dove ε è un'unità del corpo.

Infatti, non essendo x, y divisibili per λ^2, è per una delle osservazioni preliminari

$$x = \eta + \lambda^2 \alpha \qquad y = \eta_1 + \lambda^2 \beta$$

con η, η_1 unità, e con α, β interi.
Sarà perciò

$$x^3 - y^3 = \eta^3 - \eta_1^3 + 3(\eta^2 \lambda^2 \alpha - \eta_1^2 \lambda^2 \beta) + \cdots$$

E poiché $(3) = (\lambda^2)$

[30] Fubini probabilmente allude all'opera di Kummer *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen für den Fall, dass die Klassenanzahl durch* λ *teilbar ist nebst Anwendung derselben auf einen weiteren Beweis des lelzten Fermat'schen Lehrsatzes* (Abh. der K. Akad. der Wiss. zu Berlin, 1857).
[31] Sommer 1907 (trad. 1911), cap. 3, §34, p. 192-196; la dimostrazione riportata da Fubini segue da vicino quella qui proposta da Sommer all'interno del paragrafo *c) Méthodes de Kummer et de Hilber*.
[32] *e.c.* e *cor. sup.*: x, y, Z.

$$x^3 - y^3 \equiv \eta^3 - \eta_1^3 \ (mod\ \lambda^3).$$

Poiché $x^3 - y^3 = \varepsilon\lambda^{3n}Z^3$ con $n \geq 1$, sarà $\eta^3 - \eta_1^3$ divisibile per λ^3; ora $\eta^3 = \pm 1$; $\eta_1^3 = \pm 1$. Dovrà dunque essere $\eta^3 = \eta_1^3$. E se ne deduce che $x^3 - y^3$ deve essere divisibile per λ^4. Dunque $3n \geq 4$; e perciò $n \geq 2$. Ora

$$(x^3 - y^3) = (x - y)(x - \omega y)(x - \omega^2 y).$$

Poiché[33] $x \equiv \pm 1\ (mod\ \lambda); y \equiv \pm 1\ (mod\ \lambda); x^3 - y^3 = z^3 \equiv 0\ //\ (mod\ \lambda^3)$ si deduce che $x \equiv y \equiv \pm 1\ (mod\ \lambda)$. Cosicché

$$x - y \equiv x - \omega y \equiv x - \omega^2 y \equiv 0\ (mod\ \lambda).$$

Due di queste tre differenze hanno in comune il fattore λ, ma non possono entrambe essere divisibili per λ^2; perché, se p. es. λ^2 dividesse $x - y$ ed $x - \omega y$, allora λ^2 dividerebbe $(x - \omega y) - (x - y) = \lambda y$, ed y, contro l'ipotesi sarebbe divisibile per λ. Nello stesso modo si prova che $x - y, x - \omega y, x - \omega^2 y$ non hanno, oltre λ, alcun altro fattore comune.
Dunque la (1) si può soddisfare soltanto ponendo una delle $x - y, x - \omega y, x - \omega^2 y$ uguale ad $\eta_1\lambda^{3n-2}\tau^3$, p. es.

$$x - y = \eta_1\lambda^{3n-2}\tau^3$$

e poi

$$x - \omega y = \eta_2\lambda\mu^3$$
$$x - \omega^2 y = \eta_3\lambda\nu^3$$

dove η_1, η_2, η_3 sono unità, τ, μ, ν interi. Poiché

$$\omega(x - y) + \omega^2(x - \omega y) + x - \omega^2 y = 0$$

otterremo, dividendo per λ

$$\omega\eta_1\lambda^{3n-3}\tau^3 + \omega^2\eta_2\mu^3 + \eta_3\nu^3 = 0$$

cioè dividendo per $\omega^2\eta_2$ che è un'unità

$$\mu^3 - \varepsilon\nu^3 = \varepsilon_1\lambda^{3(n-1)}\tau^3$$

// dove ε ed ε_1 sono nuove unità. Essendo $n > 1$, il secondo membro è divisibile per λ^3; altrettanto avviene del primo. Poiché μ, ν non sono divisibili per λ, è $\mu^3 \equiv \pm 1\ (mod\ \lambda^3), \nu^3 \equiv \pm 1\ (mod\ \lambda^3)$. Scambiando dunque, caso mai, ν in $-\nu$ ed ε in $-\varepsilon$, potrò ottenere che $\mu^3 \equiv \nu^3\ (mod\ \lambda^3)$ e che perciò $\varepsilon \equiv 1\ (mod\ \lambda^3)$. Cioè, essendo ε una unità, sarà $\varepsilon = 1$. E la nostra equazione diventa

$$\mu^3 - \nu^3 = \varepsilon_1\lambda^{3(n-1)}\tau^3$$

che è dello stesso tipo della (1), salvo il nome dato alle incognite, e salvo che al posto di $\underline{n}$ è sostituito $n - 1$. Così continuando, potrei impicciolire l'esponente $\underline{n}$ fino a ridurlo uguale ad 1; ciò che abbiamo già provato impossibile. Dal che segue l'osservazione di Fermat.

[33] *e.c.* e *cor. sup.*: invece di $x^3 - y^3 = z^3 \equiv 0$ leggasi $x^3 - y^3 - z^3 \equiv 0$.

§.6 ***Forme quadratiche***[34]

Ci siamo già occupati, specialmente a proposito della teoria di Kronecker[35], di alcune forme, la cui teoria è intimamente connessa a quella degli ideali.

Riassumiamo tali risultati. Se $\omega_1, \omega_2, \dots, \omega_n$ è una base di un corpo di grado n, se $\alpha_1, \alpha_2, \dots, \alpha_n$ è una base di un suo ideale j il più generale intero // α di j è dato dalla

(1) $$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$
(x_i interi razionali).

Ed è

(2) $$\alpha_s = \sum_t a_{st}\omega_t \qquad \alpha_i\omega_r = \sum_s b_{irs}\alpha_s$$
(b_{irs}, α_{ir} interi razionali)

(3) $$\alpha\omega_r = \sum_i x_i \sum_s b_{irs}\alpha_s = \sum_i x_i \sum_s b_{irs} \sum_t \alpha_{st}\omega_t = \sum_t \omega_t \sum_s \alpha_{st}x_{rs}$$

ove le x_{rs} sono polinomi omogenei di 1° grado a coefficienti interi razionali nelle x. Il determinante[36] delle x_{rs} è una <u>forma a coefficienti interi razionali primi tra loro omogenea di grado n nelle x,</u> che vale

$$\varphi(x_1, x_2, \dots, x_n) = \pm\frac{Nm\,\alpha}{Nm\,j}.$$

Infatti, eliminando le ω dalle (3) si trova un'equazione di grado $\underline{n}$ in α. Se il coefficiente di α^n è 1, il termine noto (che sarà $(-1)^n Nm\,\alpha$) vale appunto $(-1)^n$ moltiplicato per il determinante delle $\sum a_{st}x_{rs}$; il quale a sua volta vale il prodotto del determinante delle a_{st} per il determinante delle x_{rs}. E il determinante delle a_{st} vale[37], in valore assoluto, $Nm\,j$.

Introduciamo una limitazione: che cioè il deter//minante delle a_{st} sia positivo: cioè supponiamo le α scritte in ordine opportuno. [Scambiando due delle α, tale determinante cambia di segno]. Allora il determinante delle x_{rs} varrà proprio

$$\varphi(x_1, \dots, x_n) = \frac{Nm\,\alpha}{Nm\,j}.$$

Essendo $Nm\,j$ costante, tale forma sarà, come $Nm\,\alpha$, decomponibile nel prodotto di n polinomi di primo grado.

Diremo <u>posequivalenti</u> (positivamente equivalenti) due ideali j, J se si possono trovare due interi a, b del corpo tali che $aj = bJ$, e che $Nm\,a > 0, Nm\,b > 0$.

Due ideali <u>equivalenti</u>[38] sono anche <u>posequivalenti</u> se ogni numero del corpo ha norma positiva, oppure se nel corpo esiste un'unità ε di norma -1, perché dalla $aj = bJ$ segue[39] $ai = (\alpha\varepsilon)j =$

[34] Gazzaniga 1903, cap. VIII, p. 150-208; cap. XII, p. 343-378; cap. XII, p. 378-408. Gazzaniga tratta gli argomenti di questo paragrafo in ordine differente rispetto a Fubini, pur giungendo entrambi a considerazioni equivalenti; infatti Gazzaniga introduce in primo luogo la nozione di equivalenza tra moduli con le relative proprietà; in seguito illustra i concetti di norma e di ideale e infine estende quanto dimostrato per i moduli agli ideali, mediante la teoria di Kummer. Cfr. anche Sommer 1907 (trad. 1911), cap. 3, §36, p. 205-222.

[35] Fubini probabilmente allude a Kronecker 1882.

[36] Kronecker 1882, cap. I, §8-10. Il matematico tedesco affronta in questi paragrafi la questione dei determinanti delle forme da lui precedentemente introdotte.

[37] La lettera "v" del termine "vale" risulta cancellata probabilmente a causa di un difetto in fase di litografazione, così come la lettera "I" di "Introduciamo" alla riga seguente del ms.

[38] Gazzaniga 1903, cap. VII, p. 166.

[39] *e.c.* e *cor. sup.*: invece di $(\alpha\varepsilon)j$ leggasi $(a\varepsilon)j$.

$bJ = (b\varepsilon)J$; ed almeno uno dei numeri[40] $\alpha, \alpha\varepsilon$ (come uno dei numeri $b, b\varepsilon$) è a norma positiva. Se invece vi sono dei numeri interi a norma negativa, tra cui nessuna unità, ogni classe di ideali si sdoppia in due sottoclassi: ciascuna delle quali è formata da ideali posequiva//lenti. Indicheremo con 1 la sottoclasse degli ideali posequivalenti ad (1) cioè degli ideali principali generati da un intero di norma positiva (ideali positivamente principali).
Se j, J sono due ideali, e se μ è un intero di j tale che $\frac{\mu}{j}$ sia primo con J, altrettanto avverrà di $\frac{\nu}{j}$, se ν è un intero tale che $\nu \equiv \mu\ (mod\ jJ)$. E, se z è un intero positivo razionale di jJ, se t è un intero razionale arbitrario, questa condizione è soddisfatta da $\nu = \mu + zt$.
E di più, se t è abbastanza grande, $Nm\,\nu$ è positiva. (*)
Quindi

$$\nu = j\frac{\nu}{j}.$$

Cioè j si può mutare in un ideale (ν) positivamente principale, moltiplicandolo per un ideale $\frac{\nu}{j}$ primo con un ideale J arbitrario prefissato.
Le sottoclassi, cui appartengono gli ideali j e $\frac{\nu}{j}$, si diranno pos-inverse; il loro prodotto va//le la sottoclasse (1) degli ideali positivamente principali.
Insomma per le sottoclassi si possono ripetere i ragionamenti già fatti per le classi.
Applichiamo questi principii a un corpo quadratico di base $\omega_1 = 1, \omega_2 = \omega$. Sia α_1, α_2 una base di un ideale j; e sia

$\alpha_1 = a_{11}\omega_1 + a_{12}\omega_2$
$\alpha_2 = a_{21}\omega_1 + a_{22}\omega_2$ (a_{rs} interi razionali)

ove le α_1, α_2 si segnano in ordine tale che sia positivo il determinante
$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$, che coinciderà pertanto con $Nm\,j$.

Sia
$\omega\alpha_1 = b_{11}\alpha_1 + b_{12}\alpha_2$
$\omega\alpha_2 = b_{21}\alpha_1 + b_{22}\alpha_2$ (b_{ik} interi razionali).

Poniamo

$$\alpha = x\alpha_1 + y\alpha_2.$$

Sarà

$\alpha\omega_1 = x\alpha_1 + y\alpha_2$ (perché $\omega_1 = 1$)
$\alpha\omega_2 = x(b_{11}\alpha_1 + b_{12}\alpha_2) + y(b_{21}\alpha_1 + b_{22}\alpha_2)$.

Il determinante dei coefficienti delle α_1, α_2 al // secondo membro

$$\varphi = \begin{vmatrix} x & y \\ b_{11}x + b_{21}y & b_{12}x + b_{22}y \end{vmatrix}$$

soddisfa alla

[40] *e.c.* e *cor. sup.*: $a, a\varepsilon$.

$$\begin{vmatrix} \alpha & \alpha' \\ \alpha\omega & \alpha'\omega' \end{vmatrix} = \varphi \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha_1' & \alpha_2' \end{vmatrix}$$

cioè

$$(Nm\,\alpha)\begin{vmatrix} 1 & 1 \\ \omega & \omega' \end{vmatrix} = \varphi \begin{vmatrix} 1 & 1 \\ \omega & \omega' \end{vmatrix} \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

ossia

$$\frac{Nm\,\alpha}{Nm\,j} = \varphi = b_{12}x^2 + (b_{22} - b_{11})xy - b_{21}y^2.$$

Potendosi scegliere l'intero α di j così che $\frac{\alpha}{j}$ sia primo con un qualsiasi ideale prefissato, gli interi[41] $b_{12}, b_{22} - b_{11}, b_{12}$, coefficienti di φ, sono primi tra loro.
Cioè la forma φ è primitiva[42].
Noto che φ ha il segno di $Nm\,\alpha$. Perciò φ potrà avere valori negativi soltanto se in j vi sono interi a norma negativa. Poiché però in ogni ideale j vi sono interi a norma positiva, si deduce // che la forma φ assume i valori di $\frac{Nm\,\alpha}{Nm\,j}$, dove α è un intero a norma positiva di j, cioè che φ assume per x, y interi razionali tutti i valori di cui è suscettibile la norma di un ideale appartenente alla classe positivamente reciproca della classe, cui appartiene j; e che queste norme sono i soli numeri positivi capaci di essere rappresentati con φ.
Le trasformazioni su α_1, α_2 che mutano α_1, α_2 in un'altra base β_1, β_2 soddisfacente alle stesse condizioni sono le trasformazioni propriamente modulari

$$\beta_1 = \lambda\alpha_1 + \mu\alpha_2$$
$$\beta_2 = \nu\alpha_1 + \rho\alpha_2$$

($\lambda, \mu, \nu, \rho,$ interi razionali tali che $\lambda\rho - \mu\nu = 1$). Sarà

$$x\alpha_1 + y\alpha_2 = x'\beta_1 + y'\beta_2$$

donde

$$x\alpha_1 + y\alpha_2 = x'(\lambda\alpha_1 + \mu\alpha_2) + y'(\nu\alpha_1 + \rho\alpha_2)$$

cosicché[43]

$$x = \lambda x' + \nu y'$$
$$y = \mu x' + \rho y'$$

cioè le x, y si deducono dalle x', y' con una trasfor//mazione[44] modulare propria. Cioè, cambiando la base di un ideale, la forma corrispondente viene mutata in un'altra ad essa propriamente equivalente. Viceversa se una forma Φ è propriamente equivalente alla forma φ ottenuta da un ideale j partendo da una certa base α_1, α_2, allora Φ si può pure dedurre dallo stesso ideale, considerandone un'altra base. A uno stesso ideale corrisponde pertanto una classe di forme propriamente equivalenti[45].

[41] *lapsus* del curatore: leggasi $b_{12}, b_{22} - b_{11}, b_{21}$.
[42] Gazzaniga 1903, cap. VIII, p. 162.
[43] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale: $y = \mu x' + \rho y'$.
[44] Nota inserita da Fubini a p.d.p.: *Disp. 23 Teoria dei numeri*.
[45] Gazzaniga 1903, cap. VIII, p. 166.

Sia j un ideale, di cui α_1, α_2 è una base, J un ideale, di cui β_1, β_2 è una base. Può avvenire che le forme

$$\frac{Nm(x\alpha_1 + y\alpha_2)}{Nm\, j}, \qquad \frac{Nm(x\beta_1 + y\beta_2)}{Nm\, J}$$

dedotte da tali ideali partendo dalle basi citate siano identiche. Sarà, poiché

$$Nm\, j = \frac{1}{\alpha}\begin{vmatrix}\alpha_1 & \alpha_1' \\ \alpha_2 & \alpha_2'\end{vmatrix} > 0, \qquad Nm\, J = \frac{1}{\alpha}\begin{vmatrix}\beta_1 & \beta_1' \\ \beta_2 & \beta_2'\end{vmatrix} > 0$$

$$(1) \qquad \frac{x^2\alpha_1\alpha_1' + xy(\alpha_1\alpha_2' + \alpha_2\alpha_1') + y^2\alpha_2\alpha_2'}{\alpha_1\alpha_2' - \alpha_2\alpha_1'} = \frac{x^2\beta_1\beta_1' + xy(\beta_1\beta_2' + \beta_1'\beta_2) + y^2\beta_2\beta_2'}{\beta_1\beta_2' - \beta_2\beta_1'}.$$

// I numeratori dei due membri devono essere tra loro proporzionali. Perciò:

$$\frac{\alpha_1\alpha_2' + \alpha_2\alpha_1'}{\alpha_1\alpha_1'} = \frac{\beta_1\beta_2' + \beta_1'\beta_2}{\beta_1\beta_1'}$$

cioè: $\left(\frac{\alpha_2}{\alpha_1}\right)' + \left(\frac{\alpha_2}{\alpha_1}\right) = \left(\frac{\beta_2}{\beta_1}\right)' + \left(\frac{\beta_2}{\beta_1}\right)$

$\frac{\alpha_2\alpha_2'}{\alpha_1\alpha_1'} = \frac{\beta_2}{\beta_1}\frac{\beta_2'}{\beta_1}$ [46]cioè $\left(\frac{\alpha_2}{\alpha_1}\right)\left(\frac{\alpha_2}{\alpha_1}\right)' = \left(\frac{\beta_2}{\beta_1}\right)\left(\frac{\beta_2}{\beta_1}\right)'$.

Da (1) si deduce ancora che:

$$\frac{\alpha_1\alpha_2' - \alpha_2\alpha_1'}{\alpha_1\alpha_1'} = \frac{\beta_1\beta_2' - \beta_2\beta_1'}{\beta_1\beta_1'}$$

ossia

$$\left(\frac{\alpha_2}{\alpha_1}\right)' - \frac{\alpha_2}{\alpha_1} = \left(\frac{\beta_2}{\beta_1}\right)' - \frac{\beta_2}{\beta_1}.$$

Queste equazioni dimostrano che $\frac{\alpha_2}{\alpha_1} = \frac{\beta_2}{\beta_1}$, ossia $\frac{\alpha_1}{\beta_1} = \frac{\alpha_2}{\beta_2}$.

Chiamando λ il valore di questi rapporti, se ne deduce

$$\alpha_1\alpha_2' - \alpha_1'\alpha_2 = \lambda\lambda'(\beta_1\beta_2' - \beta_1'\beta_2).$$

Poiché

$$\frac{(\alpha_1\alpha_2' - \alpha_1'\alpha_2)}{\beta_1\beta_2' - \beta_1'\beta_2} = \frac{Nm\, j}{Nm\, J} > 0,$$

sarà $\lambda\lambda' = Nm\, \lambda > 0$.

Quindi i due ideali j, J saranno <u>positivamente equivalenti</u>. //

È ben evidente che a due tali ideali corrispondono forme uguali (perché, moltiplicando la base di un ideale per un numero λ di norma positiva, per la stessa definizione la forma corrispondente non cambia). Ricordando poi quanto si è detto sul cambiamento di base di un ideale si deduce che: <u>a una classe di ideali pos-equivalenti corrisponde una classe di forme propriamente equivalenti</u>; a ideali non pos-equivalenti corrispondono forme non propriamente equivalenti[47].

---

[46] *e.c.* e *cor. sup.*: invece di $\frac{\beta_2}{\beta_1}\frac{\beta_2'}{\beta_1}$ leggasi $\frac{\beta_2}{\beta_1}\frac{\beta_2'}{\beta_1'}$.

[47] Gazzaniga 1903, cap. VIII, p. 166.

Se moltiplichiamo invece la base di un ideale per un intero di norma negativa, allora, secondo le nostre convenzioni sulla base di un ideale, la forma φ si muta in $-\varphi$. Moltiplicando la base di un ideale j per una unità ε tale che $Nm\,\varepsilon > 0$, si ottiene una nuova base, e quindi una trasformazione modulare propria T sulle x, y. La forma φ si è mutata nella forma che rappresenta $\frac{Nm\,(\alpha\varepsilon)}{Nm\,j}$, dove α è un intero qualunque del corpo[48]. Poiché $Nm\,(\alpha\varepsilon) = Nm\,\alpha$ alla unità ε con $Nm\,\varepsilon = 1$ corrisponde una trasformazione modulare propria T della // forma φ in se stessa.
Alle unità ε con $Nm\,\varepsilon = -1$ corrisponde invece una T che porti φ in $-\varphi$; e quindi φ e $-\varphi$ sono propriamente equivalenti, se esiste una tale unità ε. L'ideale[49] j coniugato di j appartiene alla classe reciproca della classe di j.

Caso 1° $m \not\equiv 1\ (mod\ 4)$
In $K(\sqrt{m})\ \omega_1 = 1;\ \omega_2 = \omega = \sqrt{m}.$ Un ideale j ha per base

$$\alpha_1 = a > 0 \quad \alpha_2 = b + \sqrt{m} \quad (a, b \text{ interi razionali})$$

(si è ammesso un fattore razionale per noi inutile).
È[50]

$$\alpha_1\omega = -b\alpha_1 + a\alpha_2$$
$$\alpha_2\omega = -\frac{b^2 - m}{a}\alpha_1 + b\alpha_2.$$

L'ideale[51] j si ottiene cambiando b in $-b$. Deve essere $\frac{b^2-m}{a} =$ intero razionale, che indicheremo con h.

$$b^2 = m + ha.$$

Posto $\alpha = x\alpha_1 + y\alpha_2 = xa + y\left(b + \sqrt{m}\right)$
si ha

$$\alpha\omega = -(bx + hy)\alpha_1 + (ax + by)\alpha_2$$
$$\varphi = ax^2 + 2bxy + hy^2 \quad (a > 0)$$
$$(2b)^2 - 4ha = 4m = d.$$

L'ideale coniugato dà la forma //

$$\varphi' = ax^2 - 2bxy + hy^2 \quad (a > 0).$$

Caso 2° $m \equiv 1\ (mod\ 4)$

$$\omega_1 = 1;\ \omega_2 = \omega = \frac{1 + \sqrt{m}}{2};\ d = m$$
$$\alpha_1 = a > 0;\ \alpha_2 = b + \omega;\ (2b + 1)^2 - m = 4ha$$
$$a, b, h, m \text{ interi razionali.}$$

Si trova:

[48] *e.c.* e *cor. sup.*: dell'ideale.
[49] *e.c.* e *cor. sup.*: L'ideale j'.
[50] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale: $\alpha_1\omega = -b\alpha_1 + a\alpha_2$.
[51] *e.c.* e *cor. sup.*: ideale j'.

$$\varphi = ax^2 + (2b+1)xy + hy^2; a > 0; (2b+1)^2 - 4ha = m = d.$$

La forma φ' corrispondente all'ideale coniugato è

$$\varphi' = ax^2 - (2b+1)xy + hy^2.$$

In entrambi i casi si ottengono forme del tipo

$$\varphi, \varphi' = px^2 \pm qxy + ry^2 \qquad \{p, q, r \text{ interi razionali}\}$$
$$p > 0$$

Con $q^2 - 4pr = d =$ discriminante del corpo.
Poiché $p > 0$ noi abbiamo, tra le forme definite, trovate soltanto le positive. Vi sono forme definite soltanto se $q^2 - 4pr = d < 0$; cioè se il corpo è immaginario, non vi sono numeri di norma negativa, ed è perfettamente inutile distinguere l'equivalenza dalla posequivalenza.
Se la forma è indefinita, essa è sottoposta all'unica condizione di avere il primo coefficiente $p > 0$. Ogni forma indefinita soddisfa a questa condizione, oppure è equivalente ad una forma, che sod//disfa questa condizione.
Consideriamo la $q^2 - 4pr = d$. Questa forma dimostra che, data la forma, è determinato il corpo quadratico, perché ne è noto il discriminante d: se q è pari, la forma è del tipo di Gauss. E, posto, $m = \frac{d}{4} = \left(\frac{d}{2}\right)^2 - pr$, allora m è proprio il determinante secondo Gauss. Se q è dispari, a tale forma Gauss sostituisce la $2px^2 + 2qxy + 2ry^2$, il cui discriminante secondo Gauss è ancora il numero m, la cui radice quadrata $\sqrt{m}$ individua il corpo.
In ogni caso il solo discriminante della forma individua il corpo, in cui esistono ideali a cui corrisponde la forma data. Alla forma corrispondono soltanto l'ideale $\left(p, \frac{1}{2}\left[q + \sqrt{d}\right]\right)$, e quelli ad esso positivamente equivalenti.
Lo studio degli ideali di un corpo quadratico coincide pertanto con quello delle forme quadratiche. Al concetto di prodotto di due ideali corrisponde quello di composizione di due forme $\varphi(x_1, x_2)$ e $\Phi(y_1, y_2)$.
Anzitutto, affinché φ, Φ corrispondano ad ideali di uno stesso corpo bisogna e basta che entrambe // siano a coefficienti primi tra loro, che coefficienti di x_1, x_2 e di y_1, y_2 siano di ugual parità, e che le due forme abbiano ugual discriminante. Se α_1, α_2 sono una base dell'ideale j corrispondente a φ e A_1, A_2 una base per l'ideale J corrispondente a Φ, è

$$\varphi(x_1, x_2) = \frac{Nm(\alpha_1 x_1 + \alpha_2 x_2)}{Nm\, j}; \quad \Phi(y_1, y_2) = \frac{Nm(A_1 y_1 + A_2 y_2)}{Nm\, J}.$$

Se L è l'ideale jJ, se b_1 e b_2 ne sono una base, allora la forma ad esso corrispondente sarà

$$f(z_1, z_2) = \frac{Nm\,(b_1 z_1 + b_2 z_2)}{Nm\, j\, Nm\, J}.$$

Ora all'ideale jJ appartengono tutti i prodotti $(\alpha_1 x_1 + \alpha_2 x_2)(A_1 y_1 + A_2 y_2)$ di un numero di j per un numero di J; potremmo perciò trovare degli interi razionali c_{rst} tali che, posto $z_r = \sum_{s,t} c_{rst} y_s x_t$ $(r, s, t = 1{,}2)$ sia[52]

$$(\alpha_1 x_1 + \alpha_2 x_2)(A_1 y + A_2 y_2) = b_1 z_1 + b_2 z_2.$$

[52] Invece di $(\alpha_1 x_1 + \alpha_2 x_2)(A_1 y + A_2 y_2)$ leggasi $(\alpha_1 x_1 + \alpha_2 x_2)(A_1 y_1 + A_2 y_2)$.

[53]Perciò, date due forme $\varphi(x_1, x_2)$ e $\Phi(y_1, y_2)$ soddisfacenti alle precedenti ipotesi, si può trovare una forma $f(z_1, z_2)$, composta dalle due, tale che, poste le z_1, z_2 uguali ad opportune funzioni bilineari delle x, y sia //

$$f = \varphi\Phi.$$

Se φ_1 è equivalente a φ, e se Φ_1 è equivalente a Φ, e se f_1 è composta dalle φ_1, Φ_1, allora f_1 è equivalente ad f.
L'allievo illustri con casi particolari.

Un'osservazione preliminare[54]

(che si sarebbe dovuta premettere alla definizione di discriminante).

Sia $F(x) = 0$ un'equazione algebrica a coefficienti interi razionali e col primo coefficiente uguale ad 1. Ne siano $Z_1, Z_2, \dots, Z_n$ le radici. Sarà

$$F(x) = (x - Z_1)(x - Z_2) \dots (x - Z_n)$$

donde

$$F'(Z_1) = (Z_1 - Z_2)(Z_1 - Z_3) \dots (Z_1 - Z_n).$$

I numeri coniugati di $F'(Z_1)$ sono

$$\begin{gathered}(Z_2 - Z_1)\,(Z_2 - Z_3) \dots (Z_2 - Z_n)\\ \dots\ \dots\ \dots\ \dots\\ (Z_n - Z_1)\,(Z_n - Z_2) \dots (Z_n - Z_{n-1}).\end{gathered}$$

La $Nm\,F'(Z_1)$ vale il prodotto di $F'(Z_1)$ per i coniugati. Notando che in questo prodotto capitano come fattori tutte le differenze delle radici a due a due in tutti i modi possibili, o che ogni differenza compare pertanto due volte con segni opposti e che // di tali differenze ce ne sono $\binom{n}{2} = \frac{n(n-1)}{2}$, si deduce che

$$Nm\,F'(Z_1) = (-1)^{\frac{n(n-1)}{2}} P,$$

dove P è il prodotto dei quadrati delle

$$\begin{gathered}(Z_1 - Z_2), (Z_1 - Z_3), (Z_1 - Z_4), \dots, (Z_1 - Z_n)\\ (Z_2 - Z_3), (Z_2 - Z_4), \dots, (Z_2 - Z_n)\\ (Z_3 - Z_4), \dots, (Z_3 - Z_n)\\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\\ (Z_{n-1} - Z_n)\end{gathered}$$

cosicché P è il discriminante di Z. //

(*) **Nota**: Infatti $Nm\ v$ è un polinomio di n^{esimo} grado nella t, il cui primo termine è $z^n t^n$, e che perciò per t positivo abbastanza grande ha il segno (positivo) di z^n.

[53] Bianchi 1920-21, cap. II, §38, p. 260, 261. Bianchi generalizza qui tale concetto, arrivando ad affermare che "La forma decomponibile Z, corrispondente al prodotto di due ideali, si risolve, mediante la sostituzione lineare […], nel prodotto di due forme decomponibili corrispondenti agli ideali fattori".
[54] Gazzaniga 1903, cap. X, p. 305-309. Qui Gazzaniga fa un'osservazione analoga a quella di Fubini, pur non avendo ancora introdotto il concetto di norma.

Capitolo X – L'equazione dei poligoni regolari[1]
(Campi circolari)

§.1 *Formule preliminari*[2]

Ci limitiamo allo studio dell'equazione da cui dipende il poligono regolare di ℓ lati (ℓ primo dispari)[3].

$$x^{\ell} - 1 = 0.$$

Tolto il fattore $x - 1$, questa equazione[4] diventa[5]

$$F(x) = x^{\ell-1} + \quad ^{\ell-2} + \cdots + x + 1 = 0.$$

Ne è radice[6] $Z = e^{\frac{2\pi i}{\ell}}$; le altre radici sono $Z^2, Z^3, Z^4, \ldots, Z^{\ell-1}$. Il corpo $K(Z)$ è <u>al più</u> di grado[7] $\ell - 1$ (e proprio di tale grado, se $F(x)$ è irriducibile). Si noti ancora che dalla identità[8]

$$F(x) = x^{\ell-1} + \cdots + 1 = (x - Z)(x - Z^2) \ldots (x - Z^{\ell-1})$$

per $x = 1$ segue

$$\ell = (1 - Z)(1 - Z^2) \ldots \left(1 - Z^{\ell-1}\right). \qquad (1)$$

Per ogni intero g primo con ℓ (p. es. minore di ℓ) esiste un intero g' tale che $gg' \equiv 1(\ell)$. Allora dalle[9]

$$\frac{1 - Z^g}{1 - Z} = 1 + Z + Z^2 + \cdots + Z^{g-1};$$
$$\frac{1 - Z}{1Z^g} = \frac{1 - Z^{gg'}}{1 - Z^g} = 1 + Z^g + Z^{2g} + \cdots \,//\, Z^{(g'-1)g}$$

---

[1] Gauss 1801, sez. VII, p. 413-463; Fubini, per la stesura dell'ultimo capitolo delle sue *Lezioni*, si è probabilmente ispirato all'ultima sezione delle *Disquisitiones* all'interno della quale – pur senza far ricorso alla teoria degli ideali come fa invece il Nostro – viene ampiamente trattato il tema dei campi ciclotomici legato alla condizioni necessarie affinché un poligono regolare sia "costruibile" con riga e compasso.

[2] Dirichlet 1887 (trad. 1881), suppl. VII, §138-140, p. 353-363. All'interno del suppl. VII Dedekind affronta alcuni problemi analoghi a quelli trattati da Fubini in questo capitolo, anche se con alcune lievi differenze in quanto non parla dei periodi di Gauss né della teoria degli ideali connessa a tale argomento. Cfr. anche Dirichlet 1887 (trad. 1881), suppl. IX, §179, p. 569-592, al cui interno invece viene affrontato il problema della suddivisione del cerchio nell'ottica delle applicazioni della teoria degli ideali.

[3] Bianchi 1920-21, cap. II, §42, p. 282. Cfr. anche Dirichlet 1887 (trad. 1881), suppl. IX, §179, p. 569: "Affine di far apprezzare l'utilità ed il significato delle nostre ricerche fatte finora, i cui risultati non costituiscono che i primi elementi di una teoria generale dei numeri, ne faremo applicazione a due esempi determinati […]. Qual primo esempio prendiamo il caso classico della divisione del cerchio, sul quale Kummer ha sviluppata primamente e col più bel successo la sua creazione dei numeri ideali".

[4] Gazzaniga 1903, cap. XI, p. 250-254. Cfr. anche Gauss, 1801, sez. VII, art. 341, p. 417-419; come si deduce dal titolo del paragrafo – *Theoria radicum huius aequationis (ubi supponitur, n esse numerum primum). Omittendo radicem 1, reliquae* (Ω) *continentur in aequatione* $X = x^{n-1} + x^{n-2} + \text{etc} + x + 1 = 0$. *Functio X resolvit nequit in factores inferiores, in quibus omnes coefficientes sint rationales* – Fubini riprende dal matematico tedesco gran parte del procedimento qui esposto, con l'unica eccezione dell'aver introdotto la teoria degli ideali.

[5] *cor. sup.*: $F(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1 = 0$.

[6] Bianchi 1899, cap. VII, §91, p. 206. Cfr. anche Dirichlet 1887 (trad. 1881), suppl. VII, §139, p. 356.

[7] Bianchi 1920-21, cap. II, §42, p. 283.

[8] *Ibid.* Bianchi enuncia gli stessi risultati, ma con notazioni leggermente differenti: infatti usa m al posto di ℓ ed ε al posto di Z.

[9] *lapsus* del curatore: leggasi $\frac{1-Z}{1-Z^g}$.

si trae che

$$\varepsilon_g = \frac{1 - Z^g}{1 - Z} \qquad (g = 1,2,3, \dots, \ell - 1)$$

è intero come $\frac{1}{\varepsilon_g}$, cioè che ε_g è un'unità[10].
E la (1) dà, posto $\lambda = 1 - Z$

$$l = \varepsilon_2 \varepsilon_3 \dots \varepsilon_{l-1} \lambda^{\ell - 1} \tag{2}$$

cosicché gli ideali (ℓ) e $\lambda^{\ell-1}$ coincidono.
Ogni numero primo razionale in un corpo di grado n si decompone al più in n ideali primi. Perciò la (2) dimostra che il grado del nostro corpo vale almeno $\ell - 1$, e per quanto già vedemmo, tale grado è proprio $\ell - 1$. Cioè l'equazione $F(x) = 0$ è irriducibile[11].
Di più $(1 - Z) = \lambda$ è un ideale primo[12].
Ogni numero del corpo vale

$$a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{\ell-2} Z^{\ell-2}$$

con le a_i razionali; il discriminante di Z vale $(-1)^{\frac{(\ell-1)(\ell-2)}{2}}$ nella norma di $F'(Z)$ cioè di

$$\left[\frac{d\,\frac{x^\ell - 1}{x - 1}}{dx}\right]_{x=Z} = \left[\frac{\ell x^{\ell-1}(x-1) - \left(x^\ell - 1\right)}{(x-1)^2}\right]_{x=Z} = \left[\frac{\ell Z^{-1}}{Z - 1}\right].$$

Esso vale

$$\frac{\ell^{\ell-1}}{(Z-1)(Z^2-1)\dots(Z^{\ell-1}-1)}(-1)^{\frac{(\ell-1)(\ell-2)}{2}} = \ell^{\ell-2}(-1)^{\frac{\ell-1}{2}}$$

// [perché il denominatore vale $\ell(-1)^{\ell-1}$ ed ℓ è dispari].
Il discriminante di Z o di λ (che è lo stesso) vale

$$(-1)^{\frac{\ell-1}{2}} \ell^{\ell-2}.$$

Dunque i numeri α interi del corpo sono dati da una formola[13]

$$\alpha = \frac{a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_{\ell-2}\lambda^{\ell-2}}{\ell^{\ell-2}}$$

con le a_i interi razionali. Io dico che le a_i saranno anzi divisibili per ℓ. Se così non fosse, ed a_i fosse la prima delle a non divisibili per ℓ, allora[14] $a\lambda^i$ (*) sarebbe divisibile per λ^i e non per λ^{i+1}; i seguenti termini del numero sono divisibili per λ^{i+1}; e i precedenti pure, perché hanno coefficienti a divisibili per $\ell = \lambda^{l-1}\eta$ (dove η è un'unità). Il numeratore non sarebbe divisibile per λ^{i+1}, mentre lo è il denominatore. Ciò che è assurdo, perché α è intero. Dunque le a_i sono divisibili per ℓ. Soppresso un fattore ℓ al numeratore e al denominatore, ripetendo

[10] Dirichlet 1887 (trad. 1881), suppl. IX, §179, p. 570.
[11] Gauss 1801, sez. VII, art. 341, p. 419. Il termine 'irriducibile' venne però introdotto alcuni decenni più tardi.
[12] Dirichlet 1877 (trad. 1881), suppl. IX, §179, p. 571.
[13] *Ibid.* Qui Dedekind utilizza la notazione k al posto di $\ell^{\ell-2}$ a denominatore e θ al posto di λ a numeratore.
[14] *e.c.*: $a_i\lambda^i$.

lo stesso ragionamento si trova che le a_i sono divisibili per ℓ^2. E così con//tinuando si prova che le a_i sono divisibili per $\ell^{\ell-2}$. Cosicché infine si ha che tutti gli interi del corpo sono dati dalla formola

$$b_0 + b_1\lambda + b_2\lambda^2 + \cdots + b_{\ell-2}\lambda^{\ell-2}$$

dove le b sono interi razionali. Cioè i numeri

$$1, \lambda, \lambda^2, \dots, \lambda^{\ell-2}$$

o, ciò che è lo stesso, i numeri

$$1, Z, Z^2, \dots, Z^{\ell-2}$$

formano una base del corpo[15]; il quale avrà dunque per discriminante[16] il discriminante $(-1)^{\frac{\ell-1}{2}}\ell^{\ell-2}$ del numero Z. Unico fattore primo di esso è il numero ℓ; perciò ℓ è l'unico primo razionale, che nel corpo attuale si decompone in fattori non tutti distinti.

(*) **Nota**: Si ricordi che gli interi razionali divisibili per l'ideale primo λ sono tutti e soli quelli divisibili per l. Cosicché a_i non è divisibile per λ.

§.2 ***I periodi di Gauss***[17]

Sia g una radice primitiva[18] $(mod\ \ell)$.
I numeri

$$g^0 = 1, g, g^2, g^3, \dots, g^{\ell-2}$$

formano $(mod\ \ell)$ un sistema completo di resti[19].
È[20] $g^r \equiv g^s\ (mod\ \ell)$ se $r \equiv s\ (mod\ \ell - 1)$ e quindi $Z^{(g^r)} = Z^{(g^s)}$.
Le radici $Z, Z^2, Z^3, \dots, Z^{\ell-1}$ della nostra equa//zione coincidono perciò, salvo l'ordine, con

$$\theta_0 = Z, \theta_1 = Z^g, \theta_2 = Z^{(g^2)}, \dots, \theta_{\ell-2} = Z^{g^{\ell-2}}.$$

Posto $\theta_r = Z^{(g^r)}$ si trova $\theta_r = \theta_s$ se $r \equiv s\ (mod\ \ell - 1)$. È poi

$$\theta_{r-1}^g = \left[Z^{g^{r-1}}\right]^g = Z^{g^r} = \theta_r.$$

Una θ_r si ottiene dalla precedente θ_{r-1}, innalzandola alla g^{esima} potenza. Ripetendo $\ell - 1$ volte questa operazione, ogni radice ritorna in se stessa.
Quando mai un polinomio in Z, che (in virtù della equazione cui soddisfa Z) si può supporre di grado $\ell - 2$, non varia sostituendo a Z un'altra qualsiasi radice della nostra equazione? Sia

---

[15] Bianchi 1920-21, cap. II, §42, p. 287, prop. B). Bianchi dimostra anche tale proprietà (p. 287-289).
[16] *Idem*, cap. II, §42, p. 286, 287. Bianchi dimostra qui tale formula per il calcolo del determinante. Cfr. anche Gazzaniga 1903, cap. XI, p. 349. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. IX, §179, p. 572.
[17] Gauss 1801, sez. VIII, art. 343-351, p. 420-431. In particolare, i periodi successivamente chiamati 'di Gauss' vengono introdotti nell'art. 343 dal significativo titolo *Omens radices* Ω *in certas classes (periodos) distribuntur*.
[18] Dirichlet 1877 (trad. 1881), suppl. IX, §179, p. 572; Dedekind qui scrive: "prendiamo ad arbitrio una determinata radice primitiva e del numero primo m quale base di un sistema di indici".
[19] Bianchi 1920-21, cap. II, §43, p. 289.
[20] Gazzaniga 1903, cap. XI, p. 350, prop 2).

$$P(Z) = K_0 + K_1 Z + K_2 Z^2 + \cdots + K_{\ell-2} Z^{\ell-2}$$

un tale polinomio ed A il suo valore allora l'equazione $P(Z) - A = 0$ di grado $\ell - 2$ avrebbe le $\ell - 1$ radici dell'equazione data; dunque questa equazione è un'identità; e perciò $K_1 = K_2 = \cdots = K_{\ell-2} = 0$. Un polinomio in Z, che rimanga invariato sostituendo alla Z le altre radici della nostra equazione, si riduce ad una costante. Si noti che dire che il polinomio rimane invariato sostituendo // a Z un'altra radice qualunque della nostra equazione equivale a dire che esso rimane invariato sostituendo Z^g a Z. Infatti, applicando una o più volte questa trasformazione, si passa dalla Z ad una radice qualsiasi.
Sia e un divisore di $\ell - 1$; e sia[21] $\ell - 1 = ef$. Le radici della nostra equazione sono

$$\theta_0 = Z;\ \theta_1 = Z^g;\ \theta_2 = Z^{g^2};\ \ldots;\ \theta_{e-1} = Z^{g^{e-1}}$$
$$\theta_e = Z^{g^e};\ \theta_{e+1} = Z^{g^{e+1}};\ \theta_{e+2} = Z^{g^{e+2}};\ \ldots;\ \theta_{2e-1} = z^{g^{2e-1}}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\theta_{(f-1)e} = Z^{g^{(f-1)e}};\ \theta_{(f-1)e+1} = Z^{g^{(f-1)e+1}};\ \ldots;\ \theta_{l-2} = Z^{g^{ef-1}}.$$

Sostituendo Z^{g^e} alla Z, da una di queste righe si passa alla successiva e dall'ultima alla prima. Sia $P(Z)$ un polinomio in Z, che, come sappiamo, si può scrivere nella forma

$$K_0 + K_1 Z + K_2 Z^2 + \cdots + K_{\ell-2} Z^{\ell-2}.$$

Poiché

$$K_0 = K_0 Z^\ell = K_0 Z Z^{\ell-1} = -K_0 Z\left(Z^{\ell-2} + Z^{\ell-3} + \cdots + 1\right),$$

tale polinomio si potrà scrivere nella forma:

$$h_1 Z + h_2 Z^2 + h_3 Z^3 + \cdots + h_{\ell-1} Z^{\ell-1}.$$

E, sostituendo alle $Z, Z^2, \ldots$ le θ ad esse uguali, nell'altra:

$$m_0\theta_0 + m_1\theta_1 + \cdots + m_{\ell-2}\theta_{\ell-2}$$

// (le[22] m non sono che le θ disposte in altro ordine).
Se le K sono razionali, anche le m sono razionali.
Se le m, n sono razionali e se

$$m_0\theta_0 + m_1\theta_1 + \cdots + m_{\ell-2}\theta_{\ell-2} = n_0\theta_0 + n_1\theta_1 + \cdots + n_{\ell-2}\theta_{\ell-2}$$

allora ognuna delle m è uguale alla n corrispondente. Perché, se così non fosse, sostituendo alle θ quelle delle $Z, Z^2, \ldots, Z^{\ell-1}$ ad esse uguali, avremmo, dividendo per Z, un'equazione di grado $\ell - 2 < \ell - 1$ in Z a coefficienti razionali: ciò che è assurdo. Supponiamo che il polinomio iniziale non muti variando Z in Z^{g^e}, cioè ogni θ_r in θ_{r+e} (dove è inteso che al posto di θ_s con $s > l - 2$ si scrive θ_r se r è il resto ottenuto dividendo s per $\ell - 1$). Scambiando θ_r in θ_{r+e}, il polinomio

$$m_0\theta_0 + \cdots + m_{\ell-2}\theta_{\ell-2}$$

si muta in

[21] *Idem*, cap. XI, p. 352.
[22] *e.c.* e *cor. sup.*: Z.

$$m_0\theta_\ell + m_1\theta_{\ell+1} + \cdots$$

che deve essere identico al precedente. Perciò, per quanto si è detto,

$$m_0 = m_\ell = m_{2\ell} = \cdots$$
$$m_1 = m_{\ell+1} = m_{2\ell+1} = \cdots, ecc.$$

Se ne conclude che il nostro polinomio è del tipo:[23] //

$$r_0\eta_0 + r_1\eta_1 + \cdots + r_{e-1}\eta_{e-1}$$

ove le η indicano i periodi di Gauss[24].

$$\left.\begin{aligned}
&\eta_0 = \theta_0 + \theta_e + \cdots + \theta_{(f-1)e}\\
&\eta_1 = \theta_1 + \theta_{e+1} + \cdots + \theta_{(f-1)e+1}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\eta_{e-1} = \theta_{e-1} + \theta_{2e-1} + \cdots + \theta_{ef-1}
\end{aligned}\right\} \quad \left(\theta_i = Z^{g^i}\right)$$

Un polinomio in Z a coeff.[icienti] razion.[ali], che non muta cambiando Z in Z^{g^e}, è combinazione lineare a coeff.[icienti] razionali dei periodi di Gauss.
Posto $\eta_i = \eta_j$ se $i \equiv j\ (mod\ e)$, ne viene che ogni η va nella successiva, se si scambia Z in Z^g. Ripetendo e volte questa operazione, ogni η ritorna in sé stessa. Scriviamo l'equaz.[ione][25] (risolvente dell'equazione dei poligoni circolari[26]) a cui soddisfano i periodi di Gauss.

$$G_e(\eta) = (\eta - \eta_0)(\eta - \eta_1)\ldots(\eta - \eta_{e-1}) = 0.$$

I coeffic.[ienti] sono funzioni simmetriche delle η a coefficienti interi razionali, che sono perciò polinomi in Z a coeff.[icienti] interi razionali, che non mutano cambiando Z in Z^g. Essi sono perciò interi razionali. Ed è facile provare che tale equaz.[ione] è irriducibile. Costruiamo un qualsiasi polinomio a coeff.[icienti] interi razionali nelle $\eta_0, \eta_1, \ldots, \eta_{e-1}$. Un tale polinomio // resta evidentemente immutato se cambiamo Z in[27] perché con tale trasformazione ognuna delle η torna sé stessa. D'altra parte, ricordando la definizione delle η, si riconosce che tale polinomio si può scrivere nella forma di polinomio nella variabile Z, il quale, perciò[28] che si è dimostrato, sarà una funzione lineare nelle η stesse. Perciò ogni polinomio[29] a coeff.[icienti] razionali è uguale ad un polinomio di 1° grado a coefficienti razionali nelle η stesse[30].
Ciò in particolare avverrà di $\eta_0^2, \eta_0^3, \ldots, \eta_0^{e-1}$.

[23] Nota inserita da Fubini a p.d.p.: *Disp. 24 Teoria dei numeri*.
[24] Bianchi 1899, cap. VII, §95, p. 214. Cfr. anche Gazzaniga 1903, cap. XI, p. 352. Gazzaniga chiama però le η_i "periodi ad *f* termini del quadro".
[25] Bianchi 1899, cap. VII, §95, p. 214.
[26] *e.c.* e *cor. sup.*: regolari.
[27] *e.c.* e *cor. inf.* sul lato destro della pagina: Z in Z^{g^e}.
[28] *lapsus* del curatore: leggasi "per ciò".
[29] *ad. post.* e *a.m.*: nelle η.
[30] Gazzaniga 1903, cap. XI, p. 353, prop. 7.

Esistono perciò degli interi razionali b_{rs} tali che

$$\left.\begin{aligned}
&\eta_0^1 = b_{10}\eta_0 + b_{11}\eta_1 + \cdots + b_{1,e-1}\eta_{e-1}\\
&\eta_0^2 = b_{20}\eta_0 + b_{21}\eta_1 + \cdots + b_{2,e-1}\eta_{e-1}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\eta_0^{e-1} = b_{e-1,0}\eta_0 + b_{e-1,2}\eta_1 + \cdots + b_{e-1,e-1}\eta_{e-1}.
\end{aligned}\right\} \qquad (A)$$

D'altra parte[31]

$$\left.-1 = \eta_0 + \eta_1 + \cdots + \eta_{e-1}\right\} \qquad (B)$$

perché la somma delle η è uguale alla somma di $Z, Z^2, \ldots, Z^{\ell-1}$, cioè alla somma delle radici della

$$x^{\ell-1} + x^{\ell-2} + \cdots + 1 = 0.$$

Il determinante formato coi coeff.[icienti] delle η nei secondi membri delle $(A), (B)$ non può essere nullo; perché altrimenti le $\eta_0^2, \eta_0^3, \ldots, \eta_0^{e-1}, -1$ sarebbero legati da // una relazione lineare; e quindi η_0 soddisferebbe ad un'equaz.[ione] a coeff.[icienti] razionali di grado $e-1 < e$; ciò che è assurdo. Dunque dalle $(A), (B)$ si possono dedurre tutte le $\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$ appena si conosca una di esse, p. es., la η_0. Ed è questo appunto il metodo dato da Gauss per risolvere il problema della ricerca dei poligoni regolari.
Si cominci col risolvere l'equazione $G_e(\eta) = 0$; basterà trovarne una radice, perché siano note tutte. Allora l'equazione: $F(x) = \left(x^{\ell-1} + x^{\ell-2} + \cdots + 1\right) = 0$
si potrà scrivere

$$F(x) = F_0(x)F_1(x) \ldots F_{e-1}(x) = 0$$

ove

$$F_i(x) = (x - \theta_i)(x - \theta_{e+i}) \ldots \left[x - \theta_{i+e(f-1)}\right].$$

E basterà risolvere le $F_i(x) = 0$. I coeff.[icienti] di F_i sono polinomi in Z, che non cambiano, mutando Z in Z^{g^e}, e che hanno come loro proprii coeff.[icienti] interi razionali. Pertanto i coeff.[icienti] delle F_i sono uguali a polinomi nelle η a coeff.[icienti] interi razionali, e sono noti, appena siano note le η. Il grado delle F_i è f. Se f è decomponibile, ed $f = f'e'$ con f', e' interi razionali, di nuovo alle F_i si può applicare un metodo analogo[32] a quello che noi abbiamo applicato alla $F(x) = 0$. E così via. Si riduce così il problema man mano ad equazioni di tipo più semplice[33]. //
Oss.[ervazione] Per risolvere la $G(\eta) = 0$ si ponga ε uguale ad una radice e^{esima} dell'unità. Allora, posto

[31] *Ibid.*, prop. 5: "La somma dei periodi è uguale a: -1".
[32] Bianchi 1899, cap. VII, §97, p. 218. Bianchi tratta qui in modo approfondito anche il caso in cui il periodo f è riducibile.
[33] Gauss 1801, sez. VII, art. 342, p. 419, 420.; Fubini aderisce pienamente all'approccio di Gauss che scrive "Propositum disquisitionum sequentium […] eo tendit, ut *X* in factores continuo plures GRADATIM resolvatur, et quidem ita, ut horum coefficientes per aequationes ordinis quam infimi determinetur, usque dum hoc modo ad factores semplices sive ad radices Ω ipsas perveniatur", sottolineando come il suo scopo sia quello di decomporre l'equazione irriducibile di partenza in un numero sempre più grande di fattori in modo tale che i coefficienti di tali fattori possano essere determinati mediante equazioni di grado minore possibile.

$$Z_r = \left[\eta_0 + \varepsilon^r \eta_1 + \varepsilon^{2r}\eta_2 + \cdots + \varepsilon^{(e-1)r}\eta_{e-1}\right]$$
$$(r = \text{intero arbitrario})$$

Z_r^e resta invariato mutando Z in Z^g, ed è perciò un polinomio nella[34] ε. Conosciuto ε, sono conosciute tutte le Z_r^e e le Z_r. Ed è immediato dedurre il valore p. es. di η_0.

§.3 ***Un esempio*** $(\boldsymbol{e = 2})$

Consideriamo il divisore[35] $e = 2$ di $\ell - 1$, e i corrispondenti periodi

$$\eta_0 = Z + Z^{g^2} + Z^{g^4} + \cdots + Z^{g^{\ell-3}} = \sum Z^a$$
$$\eta_1 = Z^g + Z^{g^3} + \cdots + Z^{g^{\ell-2}} = \sum Z^b.$$

Nella 1^a somma $\underline{a}$ descrive un sistema completo di residui quadratici $(mod\ \ell)$; nella 2^a il numero $\underline{b}$ descrive un sistema completo di non-residui. È[36]

$$\eta_0 + \eta_1 = -1.$$

Per costruire l'equazione di 2° grado di cui η_0, η_1 sono radici, basterà calcolare $\Delta = S^2$ ove[37]

$$S = \eta_0 - \eta_1 = \sum Z^a - \sum Z^b = \sum (-1)^{ind\,\mu} Z^\mu$$

ove μ descrive un sistema completo di resti, zero escluso, rispetto al $mod.\,l$. Se ne deduce, innalzando al quadrato, che[38]:

$$\Delta = S^2 = (\eta_0 - \eta_1)^2 = (-1)^{\frac{\ell-1}{2}}\ell.$$

Infatti si trova[39] //

$$\Delta = \sum (-1)^{ind\,\mu + ind\,\nu} Z^{\mu+\nu}$$

Dove μ, ν descrivono un sistema completo di resti, zero escluso $(mod\ l)$. Posto $\mu \equiv m\nu\ (mod\ l)$, ogni valore di ν e di μ determina $\underline{m}$ [perché $\nu \not\equiv 0\ (mod\ l)$]. Basterà poi far percorrere alle m, ν il citato sistema di resti.
Sarà[40]

$$ind\,\mu + ind\,\nu = ind\,m + 2ind\,\nu = ind\,m + \text{numero pari}$$
$$\Delta = \sum_{m,\nu} (-1)^{ind\,m} Z^{(m+1)\nu}$$
$$= \sum_m \left[(-1)^{ind\,m}\left\{Z^{m+1} + Z^{(m+1)^2} + \cdots + Z^{(m+1)(\ell-1)}\right\}\right].$$

---

[34] *e.c.* e *cor. sup.*: nelle η.
[35] Gazzaniga 1903, cap. XI, p. 360, 361. In una nota a piè di pagina Gazzaniga tratta il caso particolare $e = 2$, $\ell = 5$.
[36] Bianchi 1899, cap. VII, §98, p. 222.
[37] Bianchi 1911-12, cap. VIII, §71, p. 318.
[38] *Idem*, cap. VIII, §71, p. 319. Cfr. anche Dirichlet 1877 (trad. 1881), suppl. IX, §179, p. 572.
[39] Bianchi 1899, cap. VII, §99, p. 222, 223.
[40] La parentesi è stata da noi aggiunta.

La quantità tra $\{...\}$ è una progressione geometrica, la cui somma vale $\ell - 1$ se $m + 1 \equiv 0\ (mod\ l)$ e quindi $Z^{m+1} = 1$. Negli altri casi vale, posto $\varepsilon = Z^{m+1}$

$$\varepsilon + \varepsilon^2 + \cdots + \varepsilon^{\ell-1} = -1$$

perché $\varepsilon = Z^{m+1}$ soddisfa, come Z, alla $X^{\ell-1} + X^{\ell-2} + \cdots + X + 1 = 0$. Dunque

$$\Delta = (-1)^{ind(\ell-1)}(\ell - 1) - \sum\nolimits_m{}' (-1)^{ind\, m}$$

dove in $\sum'$ percorre un sistema completo di resti $(mod\ \ell)$ escluso 0 ed ℓ1[41].
Ossia, facendo percorrere alle m anche il valore $\ell - 1$, si ha

$$\Delta = (-1)^{ind(-1)}\ell - \sum (-1)^{ind\, m}.$$

Poiché tra gli $ind\ m$ ce ne sono tanti pari quanto dispari (tra gli $\underline{m}$ ci sono tanti residui quanti non residui) è[42] $\sum(-)^{ind\, m} = 0$.
[43]E quindi $\Delta = (-1)^{ind(\ell-1)} l = (-1)^{\frac{\ell-1}{2}}\ell$.
L'equazione di $2°$ grado nelle η è nota; e si trova[44]

$$\eta_0, \eta_1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{(-1)^{\frac{\ell-1}{2}}\ell}.\ //$$

§.3 [45] ***Il teorema di reciprocità***[46]
Si ha col simbolo di Legendre

$$S = \eta_0 - \eta_1 = \sum_r \left(\frac{r}{\ell}\right) Z^r; \quad S^2 = (-1)^{\frac{\ell-1}{2}}\ell$$

dove r percorre un sistema completo di resti $(mod\ \ell)$ zero escluso. Se p è un altro primo dispari

$$S^p = S[S^2]^{\frac{p-1}{2}} = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\ell^{\frac{p-1}{2}}S$$
$$S^p - \left(\frac{p}{\ell}\right)S = S\left\{(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\ell^{\frac{p-1}{2}} - \left(\frac{p}{\ell}\right)\right\} \qquad (A)$$
$$\left(\frac{p}{\ell}\right)S = \sum_r \left(\frac{pr}{\ell}\right) Z^r = \sum_\rho \left(\frac{\rho}{\ell}\right) Z^{p\rho}$$

Dove ρ è il numero dato dalla $p\rho \equiv r\ (mod\ l)$, il quale percorre, al pari di r, un sistema completo di resti $(mod\ l)$, zero escluso. Si noti che

[41] *lapsus* del curatore: leggasi $\ell - 1$.
[42] *e.c.* e *cor. sup.*: $\sum(-1)^{ind\, m}$.
[43] *e.c.* e *cor. sup.*, che ha reso illeggibile il testo originale: E quindi $\Delta = (-1)^{ind(\ell-1)}\ell = (-1)^{\frac{\ell-1}{2}}\ell$.
[44] Bianchi 1899, cap. VII, §99, p. 224,
[45] Nel ms. la numerazione di questo paragrafo è errata.
[46] Bianchi 1899, cap. VII, §100, p. 225. Bianchi tratta qui il teorema di reciprocità all'interno della teoria dei residui quadratici. In Bianchi 1911-12, cap. VIII, §73, p. 328-330, si enuncia e dimostra il teorema di reciprocità in relazione al valore della funzione $\varphi(h, p)$ con p primo. In Gazzaniga 1903, cap. V, p. 98-102, si dimostra tale teorema in modo più elementare rispetto a Fubini e Bianchi, ma è corredato di numerosi esempi ed applicazioni. Tale argomento è ampiamente trattato in Sommer 1907 (trad. 1911), cap. 2, §24-25, p. 117-129.

$$\binom{pr}{\ell} = \binom{p^2\rho}{\ell} = \binom{p}{\ell}^2 \binom{\rho}{\ell} = \binom{\rho}{\ell}.$$

Cosicché (A) diventa:

$$\left[\sum_r \binom{r}{\ell} Z^r\right]^p - \sum_r \binom{r}{\ell} Z^{pr} = \sum_r \binom{r}{\ell} Z^2 \left\{(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \ell^{\frac{p-1}{2}} - \binom{p}{\ell}\right\}.$$

Nel primo membro le potenze p^{esime} dei termini tra [ ] sono distrutti dalla seconda sommatoria. Gli altri termini ottenuti dallo sviluppo di $[\dots]^p$ hanno coefficienti divisibili per p. Altrettanto deve avvenire pertanto del $2°$ membro. Cioè[47]

$$\ell^{\frac{p-1}{2}} (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \equiv \binom{p}{\ell} \ (mod\ p).$$

Ma[48] $\ell^{\frac{p-1}{2}} \equiv \binom{\ell}{p} \ (mod\ p)$, perciò $\binom{\ell}{p}\binom{p}{\ell} \equiv (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \ (mod\ p)$.

Cioè $\binom{\ell}{p}\binom{p}{\ell} \equiv (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$ se ℓ, p sono primi dispari.

c.d.d. //

§.4 ***Ideali primi[49] nel corpo*** K(Z)

Il nostro corpo coincide coi coniugati perché le altre radici dell'equazione irriducibile, a cui soddisfa Z, sono potenze di Z e quindi sono contenute nel corpo. Un ideale primo sarà divisore di uno e di un solo primo razionale. Basterà cercare i divisori dei primi razionali P, per trovare tutti gli ideali primi. Sia p. es. [50]

$$P = p_0 p_1 p_2 \dots p_{\ell-1}$$

Essendo p ideali primi. Passando dal corpo ai coniugati, il primo membro non cambia; e perciò gli ideali p, possono soltanto permutarsi tra loro. D'altra parte la norma p. es. di p_0 (prodotto di p_0 e dei coniugati) vale una potenza[51] P^f di P cioè

$$(p_0 p_1 \dots p_{\ell-1})^f.$$

Quindi p_0 e gli ideali coniugati di p_1, sono tutti e soli gli ideali[52] $p_0, p_1, \dots, p_{\ell-1}$ ciascuno ripetuto f volte. Pertanto

$$\ell - 1 = ef.$$

Si devono studiare le congruenze, a cui soddisfa l'intero generico del corpo. Ma poiché il discriminante di Z è uguale al discriminante del corpo, basta fare questo studio per il numero Z, il quale soddisfa all'equazione

---

[47] *Idem*, cap. VII, §100, p. 226.
[48] *Ibid.* Bianchi sottolinea che tale risultato è una conseguenza del teorema di Eulero.
[49] Gazzaniga 1903, cap. XI, p. 374-378. In queste pagine Gazzaniga affronta l'argomento in modo simile a Fubini, anche se meno specifico.
[50] *e.c.* e *cor. sup.*: invece di ... , $p_{\ell-1}$ leggasi ..., p_{e-1}.
[51] Bianchi 1920-21, cap. II, §43, p. 292.
[52] *e.c.* e *cor. sup.*: invece di ... , $p_{\ell-1}$ leggasi ..., p_{e-1}.

$$F(x) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1 = 0.$$

Dovrà essere //

$$F(x) = \Phi_0(x)\Phi_1(x) \ldots \Phi_{\ell-1}(x) \pmod P$$

essendo poi p_r il M.C.D. di P e di Φ_r (dove le Φ sono polinomi di grado f a coeff.[icienti] interi razionali). Se fosse $P = \ell$, dalla $F(x) \equiv (x-1)^{\ell-1} \pmod \ell$ si deduce che $\underline{\ell}$ è la potenza $(\ell-1)^{esima}$ del M.C.D. di $\underline{\ell}$ e di $(Z-1)$, ossia, poiché $\lambda = 1 - Z$ è divisore di ℓ, che[53] $(\ell) = (\lambda^{e-1})$. Ciò che già sapevamo.
Supponiamo $P \neq \ell$. Sia f' l'esponente cui appartiene $P \pmod \ell$. Cioè sia f' il minimo intero raz. posit. (divisore di $\ell - 1$) tale che[54]

$$P^{f'} \equiv 1 \pmod \ell.$$

Sarà $Z^{p^m} = Z^{p^n}$ per m, n razionali interi, soltanto se $m \equiv n \pmod{f'}$. Ora la

$$\Phi_r(x) \equiv 0 \pmod{p_r}$$

possiede la radice $x = Z$. D'altra parte, con artificio già usato, dal teor.[ema] di Fermat e dalla formola del polinomio di Newton si deduce che identicamente

$$[\Phi_r(x)]^\beta \equiv \Phi_r(x^P) \pmod P$$

e perciò, essendo p_r divisore di P

$$[\Phi_r(x)]^P \equiv \Phi_r(x^P) \pmod{p_r}.$$

Il primo membro si annulla $(mod\ p_r)$ per $x = Z$. Altrettanto avverrà del $2°$ membro. E pertanto Z^P sarà pure radice della $\Phi_r(x) \equiv 0 \pmod{p_r}$. Dunque il $1°$ membro è nullo per $x = Z^P$. E se ne deduce che $(Z^P)^P = Z^{P^2}$ è pure radice della $\Phi_r(x) \equiv 0 \pmod{p_r}$. Tale congruenza possiede per//ciò le radici

$$Z, Z^P, Z^{P^2}, Z^{P^3}, \ldots, Z^{P^m}, \ldots$$

Di queste le $Z, Z^P, Z^{P^2}, \ldots, Z^{P^{f'-1}}$ sono distinte; le seguenti riproducono queste. Perciò tale congruenza di grado f rispetto a un modulo primo ha <u>almeno</u> f' radici. Perciò $f' \leq f$. Consideriamo ora l'altra congruenza

$$x^{P^{f'}} - x \equiv 0 \pmod{p_r}. \quad (A)$$

Un qualsiasi intero $\alpha = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_{\ell-2} Z^{\ell-2}$ del corpo soddisfa per il teorema di Fermat alla

$$\alpha^P \equiv a_0 + a_1(Z^P) + a_2(Z^P)^2 + \cdots + a_{\ell-2}(Z^P)^{\ell-2} \pmod P.$$

Innalzando replicatamente alla P^{esima} potenza, se ne deduce infine

$$\alpha^{P^{f'}} \equiv \alpha \pmod P.$$

---

[53] *e.c.* e *cor. sup.*: $(\ell) = \left(\lambda^{\ell-1}\right)$.
[54] Bianchi 1920-21, cap. II, §43, p. 293.

Essendo p_r un divisore di P, se ne deduce che (A) possiede come radici tutti gli interi del corpo; i quali $(mod\ p_r)$ hanno $Nm\ p_r = P^f$ valori distinti. La (A) è una congruenza di grado $P^{f'}$ rispetto ad un modulo primo. Quindi $P^{f'} \geq P^f$, cioè[55] $f' \leq f$. Unendo questo alla $f' \leq f$ già dimostrata, si deduce che[56] $f = f'$.
[57]Dunque i fattori primi di P hanno per norma P^f, se f è il minimo esponente tale che

$$P^f \equiv 1\ (mod\ \ell).$$

La $\Phi_r(x) \equiv 0\ (mod\ p_r)$ ha per radici

$$Z, Z^P, Z^{P^2}, \dots, Z^{P^{f-1}}.$$

// Detto al solito g un numero primitivo $(mod\ \ell)$, sia π l'indice di P. Cioè sia

$$P \equiv g^\pi\ (mod\ \ell).$$

Allora f è il minimo intero tale che πf sia multiplo di $\ell - 1 = ef$; cioè $\frac{\pi}{e} = h$ è un intero; affinché f sia il minimo intero tale che $\pi f = hef$ sia multiplo di ef, dovrà essere h primo con f. Cioè

$$P \equiv g^{he}\ (mod\ \ell)$$

dove h è primo con f; le successive potenze

$$1, P, P^2, \dots, P^{f-1}$$

coincidono $(mod\ l)$ con

$$g^{0\cdot he} = 1, g^{he}, g^{2he}, \dots, g^{(f-1)he}.$$

Gli esponenti

$$0, he, 2he, \dots, (f-1)he$$

Coincidono $(mod\ l)$, salvo l'ordine, con

$$0, e, 2e, 3e, \dots, (f-1)e$$

perché essendo h primo con f, i numeri $0, h, 2h, \dots, (f-1)h$ descrivono un sistema completo di resti $(mod\ f)$. Pertanto Le radici della

$$\Phi_r(x) \equiv 0\ (mod\ p_r)$$

sono i numeri $Z, Z^{g^e}, Z^{g^{2e}}, \dots, Z^{g^{(f-1)e}}$. E, con le notazioni del §2, sarà

$$\Phi_r(x) \equiv F_0(x)\ (mod\ p_r).$$

// Cioè $F_0(x)$ è $(mod\ p_r)$ congruo ad un polinomio Φ_r a coefficienti interi razionali. Generalizziamo questa congruenza. Cominciamo col fissare l'ordine in cui si scrivono gli ideali

[55] *e.c.* e *cor. sup.*: cioè $f' \geq f$.
[56] *Ibid*. Bianchi dimostra tale risultato in modo analogo a Fubini e afferma che la prima dimostrazione di tale uguaglianza si deve a Kummer.
[57] Dirichlet 1877 (trad. 1881), suppl. IX, §179, p. 575.

$$p_0, p_1, \dots, p_{e-1}.$$

Cambiando Z in Z^g, od in Z^{g^2}, od in Z^{g^3}, ogni ideale va nei coniugati; indicheremo con p_r l'ideale in cui va p_0, quando a Z si sostituisca la Z^{g^r}. (Per $r = 0$, cioè mutando Z in $Z^{g^0} = Z$, l'ideale p_0 va appunto in p_0). Naturalmente mutando Z in Z^{g^r} per $r = 0,1,2, \dots, e-1$, si trovano i nostri ideali; per $r = e,\ e+1, \dots$ si ritorna agli ideali già determinati. Cosicché $p_r = p_s$ se $r \equiv s\ (mod\ e)$. La $\Phi_0(x) \equiv 0\ (mod\ p_0)$ con le radici $Z, Z^{g^e}, Z^{g^{2e}}, \dots, Z^{g^{(f-1)e}}$ diventa, trasformando Z in $Z^{g^r}\Phi_0(x) \equiv 0\ (mod\ p_r)$ con le radici

$$Z^{g^r}, Z^{g^{r+e}}, \dots, Z^{g^{r+(f-1)e}}.$$

Notiamo che, mutando Z in Z^{g^s}, l'ideale p_0 va in p_s; se poi si muta ancora Z in Z^{g^r}, l'ideale p_s va nell'ideale, cui si giunge[58], mutando Z in $(Z^{g^r})^{g^S} = Z^{g^{r+s}}$, cioè p_s va in p_{r+s}. Cioè, mutando Z in Z^{g^r}, ogni ideale p_s va in p_{r+s}. Perciò dalla:

$$\Phi_r(x) \equiv 0\ (mod\ p_r) \text{ con le radici } Z, Z^{g^e}, \dots, Z^{g^{(f-1)e}}$$

si deduce

$$\Phi_r(x) \equiv 0\ (mod\ p_{r+s}) \text{ con le radici } Z^{g^s}, Z^{g^{s+e}}, \text{ ecc.}$$

// cosicché

$$\Phi_s(x) \equiv F_r(x)\ \ (mod\ p_{r+s})$$

che pone in chiara luce le relazioni tra le Φ e le F.
Ora le F_r sono polinomii, i cui coeff.[icienti] sono polinomii nelle η_i a coeff.[icienti] interi razionali. Le η_i sono radici di una equazione

$$G_e(\eta) = 0$$

il cui 1° membro è un polinomio a coeff.[icienti] interi razionali, che noi sappiamo costruire. Ora per passare dalla F_r, i cui coeff.[icienti] dipendono dalle η, alla Φ_s, i cui coeff.[icienti] sono interi razionali, basterà sostituire a ciascuna delle η quei numeri interi razionali che sono loro rispettivamente congrui $(mod\ p_{r+s})$. Sarà così determinata la $\Phi_s\ (mod\ p_{r+s})$. Ecco dunque come si farà il calcolo:
I) Si calcolino le funzioni simmetriche delle η; esse saranno polinomi in Z a coeff.[icienti] interi razionali, che non mutano cambiando Z in Z^g e che perciò saranno addirittura interi razionali. Sarà così possibile costruire l'equazione (risolvente)

$$G_e(\eta) = 0$$

a coeff.[icienti] interi razionali, cui soddisfano le η.
Oss.[ervazione] La η_r, somma delle radici della $\Phi_s(x) \equiv 0\ (mod\ //\ p_{r+s})$ sarà $(mod\ p_{r+s})$ congrua al coeff.[iciente] intero razionale di x^{f-1} cambiato di segno del polinomio $\Phi_s(x) = x^f + K_s x^{f-1} + \cdots$. Dunque la congruenza

$$G_e(\eta) \equiv 0$$

[58] *ad. post.*: da p_s.

ammette le radici $-K_0, -K_1, \dots, -K_{e-1}$ intere razion.[ali] rispetto ad ognuno dei moduli primi p, e quindi anche rispetto al $mod\ P$ loro prodotto.
II) Per tentativi si cerchino tra i numeri $0, 1, 2, \dots, P-1$ le $\underline{e}$ radici della $G_e(\eta) \equiv 0\ (mod\ P)$. (È inutile provare altri interi razionali; ogni altro intero razionale è $(mod\ P)$ congruo ad uno dei precedenti). Siano esse gli interi razionali $K_0, K_1, \dots, K_{e-1}$. Una di queste radici, p. es., K_0 si assuma congrua ad $\eta_0\ (mod\ p_0)$. Ciò è lecito, perché si può indicare con p_0 uno qualsiasi dei fattori di P. Le relazioni già scritte al §2 tra i prodotti delle η a due a due e le η stesse, ci guideranno a trovare come si debbono ordinare le K in guisa che $\eta_i \equiv K_i\ (mod\ p_0)$.
III) Costruiamo il polinomio F_0, i cui coeff.[icienti] sono funzioni lineari delle η; sostituendovi a ciascuna delle η l'intero razionale corrispondente, troveremo $\Phi_0(x)$. L'ideale p_0 sarà il M.C.D. di P e di $\Phi_0(Z)$. Nelle lezioni di Dirichlet-Dedekind tradotte dal // Faifofer è dato l'esempio numerico corrispondente ad $\ell = 13, P = 3, f = 3, e = 4$; si è assunto ivi $g = 2$.
Oss.[ervazione] La funzione di Dirichlet[59] per il nostro corpo vale[60]

$$\prod \frac{1}{[1 - Nm\ p]^{-s}}\ ,$$

dove il prodotto infinito è esteso a tutti gli ideali primi del corpo. Ordiniamo questi ideali, aggruppando insieme quelli che dividono uno stesso intero primo razionale P. Se $P = \ell$, ad esso corrisponde un unico divisore, la cui norma è $\underline{\ell}$, e che nel prodotto infinito dà origine al fattore $\frac{1}{1-\ell^{-s}}$.
Se $P \neq \ell$, allora P è il prodotto di e ideali, ciascuno dei quali ha per norma P^f; essi danno (nel nostro prodotto infinito) complessivamente il fattore

$$\frac{1}{(1 - P^{-sf})^e}\ ,$$

se f è il minimo intero tale ch e $P^f \equiv 1\ (mod\ \underline{\ell})$ ed $\ell - 1 = ef$.
Posto $P^{-s} = x$, è

$$1 - P^{-sf} = 1 - x^f$$

che è un divisore di $1 - (x^f)^e = 1 - x^{\ell-1}$. L'equazione[61]

$$1 - x^f = 0$$

ha per radici (quando si ponga $\varepsilon = e^{\frac{2\pi i}{\ell-1}}$) quelle potenze ε^r di ε tali che rf sia multipla di $\ell - 1$, ossia che r sia multipla dell'indice π di P. Infatti i valori //

$$r = 0, \pi, 2\pi, \dots, (f-1)\pi$$

moltiplicati per f danno multipli di πf che è multiplo di $l - 1$; cosicché $(\varepsilon^r)^f = 1$ ed essi danno proprio f potenze ε^r distinte, perché la differenza di due di questi valori di r non è mai multipla di $\ell - 1$, essendo $f\pi$ il minimo comune multiplo di π e di $\ell - 1$. Facciamo

[59] Bianchi 1920-21, cap. III, §58, p. 394.
[60] *e.c.*: $\prod\left(\frac{1}{[1-Nm\ p]^{-s}}\right)$.
[61] Bianchi 1920-21, cap. III, §58, p. 396. Cfr. anche Bianchi 1899, cap. VII, §100, p. 206.

percorrere ad r i valori[62] $0, \pi, 2\pi, \dots, (f-1)\pi, f\pi, \dots, (\ell-1)\pi,$ otteniamo le stesse radici ciascuna ripetuta[63] $\frac{e-1}{f}$ e volte[64].
Pertanto[65] $(x^f - 1)^e = \prod_{m=0}^{\ell-1}(x - \varepsilon^{\pi m})$.
E, mutando π in $\frac{1}{\pi}$, si trova[66]:

$$\left(1 - x^f\right)^e = \prod_{m=0}^{\ell-1}(1 - \varepsilon^{\pi m} x).$$

Postovi $x = P^{-s}$, e separando il fattore corrispondente ad $m = 0$, dagli altri si ha infine

$$\left(1 - P^{-sf}\right)^e = (1 - P^{-s}) \prod_{1}^{\ell-1}[1 - P_\ell^m P^{-s}]$$

ove

$$P_\ell = \varepsilon^{ind\, P}, \qquad \varepsilon = e^{\frac{2\pi i}{\ell-1}}.$$

La stessa forma si può dare al fattore dipendente dal <u>primo</u> ℓ, purché si convenga che[67] $\binom{\ell}{\ell} = 0$.
Di questa forma della serie zeta di Dirichlet noi ci siamo serviti per provare il teorema della progressione aritmetica. //

[62] *e.c.:* i valori $0, \pi, 2\pi, \dots, \dots, (\ell-2)\pi$.
[63] *e.c.*: $\frac{\ell-1}{f} = e$.
[64] Bianchi 1920-21, cap. III, §48, p. 395.
[65] *e.c.*: invece di $\prod_{m=0}^{\ell-1}$ leggasi $\prod_{m=0}^{\ell-2}$.
[66] *e.c.*: invece d i $\prod_{m=0}^{\ell-1}$ leggasi $\prod_{m=0}^{\ell-2}$.
[67] La parentesi tonda è stata da noi aggiunta.

BIBLIOGRAFIA

ALBERS Donald J., ALEXANDERSON Gerald L., REID Constance 1987, *International mathematical congresses: an illustrated history: 1893-1986*, New York, Springer.

ALBERT Adrian A. 2012, *Leonard Eugene Dickson, January 22, 1874 – January 17, 1954*, «Celebratio Mathematica», p. 1-5.

ARGAND Jean R. 1814, *Réflexions sur la nouvelle théorie d'analyse*, «Annales de Mathématiques», V, p. 197-209.

AVIGAD Jeremy 2004, *Dedekind's 1871 version of the theory of ideals.* https://www.andrew.cmu.edu/user/avigad/Papers/ideals71.pdf

BACHMANN Paul G.H.

1872 *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie,* Leipzig, Teubner.

1892 *Die Elemente der Zahlentheorie*, Leipzig, Teubner.

BARBERIS Bruno G., GALLETTO Dionigi 2008, *Euler e Lagrange*, in *Leonhard Euler nel terzo centenario della nascita*, Quaderno n. 16, Torino, Accademia delle Scienze, p. 61-81.

BEDARIDA Alberto M.

1921 *Le classi di forme aritmetiche di Dirichlet appartenenti ai generi della classe principale* – Nota I, «Rend. Acc. Naz. Lincei, Cl. Sci. FMN», s. 5, XXX, p. 485-488.

1922a *Le classi di forme aritmetiche di Dirichlet appartenenti ai generi della classe principale* – Nota II, «Rend. Acc. Naz. Lincei, Cl. Sci. FMN», s. 5, XXXI, p. 5-8.

1922b *Guido Fubini – Lezioni di Teoria dei Numeri (litografie),* «Bollettino di Matematica», XVIII, p. XVII-XVIII.

BELHOSTE Bruno 1998, *Pour une réévaluation du rôle de l'enseignement dans l'histoire des mathématiques*, «Revue d'histoire des mathématiques», IV, p. 289-304.

BENEDICTY Mario 1954, *Necrologio di Fabio Conforto*, «Bollettino dell'UMI», s. 3, IX, 1, p. 227-228.

BERTOLINI Massimo, CANUTO Giuseppe 1996, *La congettura di Shimura-Taniyama-Weil*, «Bollettino dell'UMI», sez. A, 10, 2, p. 213-247.

BIANCHI Luigi

1897 *Teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois – Lezioni raccolte da V. Boccara*, Pisa, R. Lit. FF. Gozani.

1899 *Teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, Pisa, Spoerri Editore.

1903 *Lezioni sulla teoria dei gruppi continui finiti di trasformazioni – anno 1902-03,* Pisa, Spoerri Editore.

1911-12 *Lezioni sulla teoria aritmetica delle forme quadratiche binarie e ternarie*, Corso di matematiche superiori, Pisa, Spoerri Editore.

1920-21 *Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica*, Pisa, Spoerri Editore.

BINI Gilberto, CILIBERTO Ciro 2018, *Un errore, o meglio, un orrore di 80 anni fa*, «Matematica, Cultura e Società – Rivista dell'UMI», s. 1, III, 2, p. 85-92.

BONIFACE Jacqueline, SCHAPPACHER Norbert 2002, *'Sur le concept de nombre en mathématique'. Cours inédit de Leopold Kronecker à Berlin (1891)*, «Revue d'histoire des mathématiques», VII, p. 207-275.

BORTOLOTTI Ettore 1908, *Sulle equazioni irrazionali*, «Bollettino di Matematica», VII, p. 177-181.

BOTTARI Amerigo 1912, *Una dimostrazione del teorema di Wilson,* «Bollettino di Matematica», XI, p. 289.

BOTTAZZINI Umberto 1982, *Enrico Betti e la trasformazione della scuola matematica pisana*, in Montaldo, Grugnetti (eds.), *La storia delle matematiche in Itali*a, Cagliari, p. 229-237.

BOTTAZZINI Umberto, GRAY Jeremy 2013, *Hidden Harmony – Geometric Fantasies*, Berlin-New York, Springer.

BRIGAGLIA Aldo, SCIMONE Aldo 1998, *Algebra e Teoria dei numeri*, in Di Sieno, Guerraggio, Nastasi (eds.), *La matematica italiana dopo l'Unità: Gli anni tra le due guerre mondiali*, Milano, Marcos y Marcos, p. 505-568.

BRIGAGLIA Aldo 2017, *Es steht alles schon bei Dedekind: aspetti dell'influenza dell'opera di Dedekind sulla matematica italiana*, «Matematica, Cultura e Società – Rivista dell'UMI», s. 1, II, 1, p. 17-43.

BUTZER Paul L., CARBONE Luciano, JONGMANS François, PALLADINO Franco 1999 (éds.) *Les relations épistolaires entre Eugéne Catalan et Ernesto Cesàro*, «Bulletin de l'Acadèmie Royale de Belgique classe des Sciences», s. 6, X, p. 223-271.

BUTZER Paul L., CARBONE Luciano, JONGMANS François, PALLADINO Franco 2000 (éds.) *Les relations épistolaires entre Eugéne Catalan et Ernesto Cesàro*, «Bulletin de l'Acadèmie Royale de Belgique classe des Sciences», s. 6, X, p. 377-417.

CASSELS John W.S., FRÖHLICH Albrecht 1967, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Washington D.C., Thompson.

CAUCHY Augustin-Louis 1825, *Mémoire sur les intégrales définies, prises entre des limites imaginaires*, Parigi, Bure Frères.

CAVALLARO Vincenzo G.

1914a *Determinazioni grafiche del poligono di un numero primo p=257 di lati e digressione sul metodo dei segmenti alfa,* «Il Bollettino di Matematica», XV, 6, p. 132-137

1914b *Determinazione grafica di 13 poligoni regolari non euclidei di un numero primo p di lati*, «Il Bollettino di Matematica», XV, 7, p. 160-164.

CHEBYSHEV Pafnuti L. 1895, *Teoria delle congruenze,* Roma, Loescher (trad. it. a cura di I. Massarini)

CHEVALLEY Claude

1936 *L'Arithmétique dans les Algèbres de Matrices*, Parigi, Hermann.

1940 *La théorie du corps de classes*, «Annals of Mathematics», XLI, p. 394-418.

CIBRARIO Maria 1929, *Teorema di Leibniz-Wilson sui numeri primi*, «Periodico di Matematiche», s. 4, IX, p. 262-264.

COMPOSTO S. 1912, *Sulla funzione $\varphi(n)$ e sui numeri primi con un dato numero n,* «Il Bollettino di Matematica», XI, p. 12-33.

CONCINA Umberto 1913, *Di una estensione del teorema di Eulero relativo al numero $\varphi(n)$,* «Il Bollettino di Matematica», XII, p. 1-8.

CONTE Alberto, GIACARDI Livia 2016 *Segre's university courses and the blossoming of the italian school of algebraic geometry*, in Casnati, Conte, Gatto, Giacardi, Marchisio, Verra (eds.), *From classical to modern algebraic geometry Corrado Segre's mastership and legacy*, Basel, Birkhäuser, p. 3-91.

COOLIDGE Julian 1904, *The opportunities for mathematical study in Italy*, «Bulletin of the American Mathematical Society», s. 2, XII, p. 9-17.

CORRY Robert 1996, *Modern Algebra and the Rise of Mathematical Structures*, Basel-Boston-Berlin, Birkhäuser.

D'ALEMBERT Jean B. 1758, *Traité de dynamique*, Parigi, David.

DAVENPORT Harold 1952, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, Londra, Hutchinson.

DHOMBRES Jean, ALVAREZ Carlos

2011 *Une histoire de l'imaginaire mathématique: vers le théorème fondamentale de l'algèbre et sa démonstration par Laplace en 1795,* Parigi, Hermann.

2013 *Une histoire de l'invention mathématiques: les démonstrations du théorème fondamental de l'algèbre dans le cadre de l'analyse réelle et de l'analyse complexe de Gauss à Liouville*, Parigi, Hermann.

DICKSON Leonard E.

1909 *Review: Hermann Minkowski, Diophantische Approximationen. Eine Einführung in die Zahlentheorie,* «Bulletin of the American Mathematical Society», XV, 5, p. 251, 252.

1914 *Review: Hermann Minkowski, Geometrie der Zahlen,* «Bulletin of the American Mathematical Society», XXI, 3, p. 131, 132.

1919-23 *History of the theory of numbers*, Washington, Carnegie Institution.

DIRICHLET Peter G.L.

1877^2 *Vorlesungen über Zahlentheorie*, Braunshweig, F. Vieweg und Sohn (trad. it. a cura di A. Faifofer 1881, *Lezioni sulla Teoria dei numeri – pubblicate e corredate di appendici da R. Dedekind*, Venezia, Tip. Emiliana).

1894^3 *Vorlesungen über Zahlentheorie,* Braunshweig, F. Vieweg und Sohn.

1920-21 *Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica*, Pisa, Spoerri Editore.

EULER Leonhard

1744 *Variae observationes circa series infinitas,* «Commentarii academiae scientiarum Petropolitanae», IX, p. 160-188.

1744-46 *Theoremata circa divisores numerorum in hac forma* $pa^2 \pm qb^2$ *centorum*, «Comm. Acad. Sc. Petersburg», XIV, p. 151-181.

1748 *Introductio in analysin infinitorum,* Losanna, M.-M. Bousquet.

EDWARDS Harold M.

1984 *Galois theory,,* New York, Springer.

1980 *The Genesis of Ideal Theory*, «Archive for History of Exact Sciences», XXIII, 4, p. 321-378.

EMALDI Maurizio 1994, *Paolo Gazzaniga (1853-1930) e la teoria dei numeri algebrici*, in *Le scienze matematiche nel Veneto dell'Ottocento*, Venezia, p. 209-223.

ENRIQUES Federigo, CHISINI Oscar 1914, *Lezioni sulla teoria geometrica delle equazioni*, Bologna, Zanichelli.

FANTAPPIÈ Luigi 1927, *Le forme decomponibili coordinate alle classi di ideali nei corpi algebrici*, «Annali della Scuola Normale Superiore di Pisa, Classe di Scienze», s. 1, XV, p. 1-58.

FAVA Franco 1999, *Guido Fubini*, in Roero (ed.), *La facoltà di scienze MFN di Torino*, t. I, *I docenti*, p. 563-566.

FENSTER Della D.

1999 *Leonard Eugene Dickson and his work in the arithmetic of algebra,* «Archive for History of Exact Sciences», LII, p. 119-159.

2007 *Research in algebra at the university of Chicago,* in Gray, Parshall (eds.), *Episodes in the History of Modern Algebra,* American Mathematical Society and London Mathematical Society, p. 179-197.

FREY Gerhard 1986, *Links between stable elliptic curves and certain Diophantine equations*, «Annales Universitatis Saraviensis. Series Mathematicae», s. 1, I, p. 1-40.

FRENKEL Edward

2003 *Recent Advances in the Langlands Program*. https://arxiv.org/pdf/math/0303074.pdf

2005 *Lectures on the Langlands Program and Conformal Field Theory*, Les Houches. https://arxiv.org/pdf/hep-th/0512172.pdf

2007 *Langlands Correspondence for Loop Groups*, Cambridge Studies in Advanced Mathematics 103, Cambridge University Press.

FUBINI Guido

1917 *Lezioni di Teoria dei numeri – Anno Accademico 1916-1917*, Torino, Datt.-Lit. A. Viretto.

1928 *In memoria di Luigi Bianchi*, «Il Bollettino di Matematica», s. 2, VII, p. 59-97.

1929a *Luigi Bianchi e la sua opera scientifica*, «Annali di Matematica pura e applicata», s. 4, VI, p. 45-83.

1929b *Commemorazione del Socio Luigi Bianchi*, «Rend. Acc. Naz. Lincei, Cl. Sci. FMN», s. 6, X, p. XXXIV-XXXXIV.

1930 *La matematica come creazione del pensiero e come strumento tecnico*, «Giornale di Matematica Finanziaria», XII, p. 97-107.

1931 *La matematica come creazione del pensiero e come strumento tecnico*, «Annuario della scuola di Ingegneria di Torino», p. 3-12.

1935 *Luigi Lagrangia*, «Celebrazioni Piemontesi», parte 1, XIII, p. 3- 16.

1936 *Problemi tecnici e problemi matematici*, «Atti della Soc. It. per il Progresso delle Scienze», XXIV Riunione, III, p. 28-37.

FURINGHETTI Fulvia, SOMAGLIA Annamaria 1992, *Giornalismo matematico 'a carattere elementare' nella seconda metà dell'Ottocento*, «L'Insegnamento della Matematica e delle Scienze Integrate», XV, p. 815-852.

GARRET Reeve 2017, *The History of the Formulation of Ideal Theory.* https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/6/3494/files/2014/04/Grad-seminar-talk-112917-wzznvh.pdf

GAUSS Carl F.

1799 *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse,* Helmstadt, Fleckeisen.

1801 *Disquisitiones Arithmeticae*, Leipzig, Fleischer.

1808 *Theorematis arithmetici demonstratio nova,* «Commentarii Societatis Regiae Scientiarum Gottingensis», XVI, p. 457–462.

1811 *Summatio serierum quarundam singularium,* «Commentarii Societatis Regiae Scientiarum Gottingensis», p. 463–495.

1889 *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik. (Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarundam serierum singularium*, *ecc.)* hrsg. H. Maser, Berlin, Springer.

GAUSS Carl F., NETTO Eugen 1890, *Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischen Funktionen in reelle Faktoren ersten oder zweiten Grades (1799-1849),* Leipzig, Engelmann.

GAZZANIGA Paolo 1903, *Gli elementi della teoria dei numeri*, Verona-Padova, Druker.

GIACARDI Livia, VARETTO T. 1996, *Il Fondo Corrado Segre della Biblioteca "G. Peano" di Torino*, «Quaderni di Storia dell'Università di Torino», I, p. 207-246.

GIACARDI Livia, ROERO Clara S. 1999, *Biblioteca Speciale di Matematica "Peano"*, in Roero (ed.), *La facoltà di Scienze matematiche fisiche naturali di Torino 1848-1998*, t. 1, *Ricerca, Insegnamento, Collezioni scientifiche*, Torino, CSSUT-DSSP, p. 437-458.

GIACARDI Livia, LUCIANO Erika, PIZZARELLI Chiara, ROERO Clara S. 2015, *Gli Archivi di Corrado Segre presso l'Università di Torino,* «Rivista di Storia dell'Università di Torino», IV, 2, p. 49-57.

GIRARD Albert 1629, *L'invention en algèbre,* Amsterdam, Guillaime Ianffon Blaeuw.

GOLDSTEIN Catherine

1989 *Le métier des nombres au 17e et 19e siècles,* in Serres (éd.) *Éléments d'Histoire des Sciences*, Parigi, Bordas, p. 274-295.

1992 *On a Seventeenth-Century Version of the Fundamental Theorem of Arithmetic,* «Historia Mathematica», XIX, p. 177-187.

1993 *Descente infinie et analyse diophantienne: programmes de travail et mise en œuvre chez Fermat, Levi, Mordell et Weil,* «Cahier du Séminaire d'histoire et de philosophie des mathématiques», s. 2, III, p. 25-49.

1995a *Un théorème de Fermat et ses lecteurs,* Saint-Denis, PUV (Histoires de science).

1995b *La conjecture de Fermat est enfin un théorème,* «La Recherche» 277, XXVI, p. 678-

1995c 679.

Pierre de Fermat et le dernier théorème, «Quadrature», XXII, p. 3-6.

2005 *The Vorlesungen über die Zahlentheorie by p. G. Dirichlet,* in Grattan-Guinness (ed.) *Landmark Writings in Western Mathematics, 1640-1940*, Amsterdam, Elsevier, p. 480-490.

2009 *La théorie des nombres en France dans l'entre-deux-guerres: De quelques effets de la première guerre mondiale,* «Revue d'histoire des sciences», s. 1, LXII, p. 143-176.

2011 *Charles Hermite's Stroll through the Galois fields,* «Revue d'histoire des mathématiques», XVII, p. 211-270.

2016 *Découvrir des principes en classant: la classification des formes quadratiques selon Charles Hermite,* «Cahiers François Viète», s. 3, I, p. 103-135.

GOLDSTEIN Catherine, SCHAPPACHER Norbert, SCHWERMER Joachim 2007, *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, Heidelberg-Berlin, Springer.

GUERRAGGIO Angelo, NASTASI Pietro

2005 *Matematica in camicia nera: il regime e gli scienziati*, Milano, Mondadori.

2006 *Italian Mathematics between the Two World Wars*, Basel-Boston-Berlin, Birkhäuser.

2018a *Era l'estate del 1938…quella delle leggi antiebraiche*, «Lettera Matematica Pristem», 104, p. 31-34.

2018b *Un'amicizia beyond the life: Guido Fubini e Tullio Levi-Civita,* «Lettera Matematica Pristem», 104, p. 35-38.

HADAMARD Jacques 1896, *Sur la distribution des zéros de la fonction ζ(s) et ses conséquences arithmétiques*, «Bulletin de la Société Mathématique de France», XXIV, p. 199–220.

HARRIS Michael 2019, *Why the Proof of Fermat's Last Theorem Doesn't Need to Be Enhanced.* https://www.quantamagazine.org/why-the-proof-of-fermats-last-theorem-doesnt-need-to-be-enhanced-20190603/

HAWKINS Thomas 2013, *The Mathematics of Frobenius in Context*, Berlin-New York, Springer.

HECKE Erich 1923, *Vorlesung über die Theorie der algebraischen Zahlen*, Leipzig, Akadem. Verlagsges.

HILBERT David

1897 *Die Theorie der algebraischen Zahlkörper,* «Jahresbericht der Deutschen Mathematiker-Vereinigung», IV, p. 175–546.
(trad. fr. par A. Lévy 1911, *Théorie des corps de nombres algébriques,* Parigi, Hermann).
(trad. ing. by T. Adamson 1998, *The Theory of Algebraic Number Fields*, Berlin, Springer).
1910 *Théorie des corps de nombres algébriques,* «Annales de la Faculté des sciences de Toulouse: Mathématiques», s. 3, II, 3-4, p. 225-456.
1932 *Gesammelte Abhandlungen,* vol. 1, Berlin, Springer.

ISRAEL Giorgio, NASTASI Pietro 1998, *Scienza e Razza*, Bologna, Il Mulino.

KLEIN Felix 1896, *Ausgewählte Kapitel der Zahlentheorie*, Göttingen, lit.

KOREUBER Mechthild 2015, *Emmy Noether, die Noether–Schule und die modern Algebra*, Berlin-New York, Springer.

KRONECKER Leopold
1882 *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* Berlin, Reimer.
1883 *Über bilineare Formen mit vier Variablen,* «Abhandlungen der Königlich Preußischen Akademie der Wissenschaften», II, p. 1-60.
1895 *Werke: Hrsg. auf Veranlassung der Königlich Preußischen Akademie der Wissenschaften*, ed. K. Hensel, Leipzig, Teubner.
1978 *Vorlesungen über Zahlentheorie*, Berlin, Springer.

KUMMER Ernst E.
1844 *Kummers Briefe an Leopold Kronecker*, «Festschrift zur Feier des 100. Geburtstages Eduard Kummers mit Briefen an seine Mutter und an Leopold Kronecker», ed. Vorstand der Berliner Mathematischen Gesellschaft, p. 46–102.
1846 *Zur Theorie der komplexen Zahlen*, «Monatsberichte der Königlichen Akademie der Wissenschaften zu Berlin», p. 87–96.
1857 *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^{\lambda} = 1$ *gebildeten complexen Zahlen für den Fall, dass die Klassenanzahl durch* λ *teilbar ist nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, «Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin», p. 275–282.
1975 *Collected Papers*, ed. A. Weil, vol. 1, *Contributions to Number Theory*, Berlin-Heidelberg, Springer

LAGRANGE Giuseppe L. 1797, *Traitè de la résolution des équations numériques de tous les degrés*, Parigi, Lib. Sciences.

LANDAU Edmund
1907 *Über die Multiplikation Dirichletscher Reihen,* «Rend. del Circolo Matematico di Palermo», XXIV, p. 81-160.
1908 *Beiträge zur analytischen Zahlentheorie,* «Rend. del Circolo Matematico di Palermo», XXVI, p. 169-302.
1909 *Über das Konvergenzproblem der Dirichletsche Reihen*, «Rend. del Circolo Matematico di Palermo», XXVIII, p. 113-151.
1914 *Ein Satz über Dirichletsche Reihen mit Anwendung auf die zeta-Funktion und die L-Funktionen,* «Rend. del Circolo Matematico di Palermo», XXXVII, p. 269-272.

LAURENT Hermann
1902 *Sur les principes fondamentaux de la théorie des nombres et de la géométrie*, Évreux, Hérissey.
1904 *Théorie des nombres ordinaires et algébriques,* Parigi, Naud.

LA VALLÉE POUSSIN Charles-Jean 1896, *Sur la fonction de Riemann et le nombre de nombres premiers inférieurs à une limite donnée*, «Mémoires couronnés de l'Académie de Belgique», LIX, p. 1-74.

LEGENDRE Adrien-Marie
1798 *Essai sur la théorie des nombres,* Parigi, Duprat.
1808[2] *Essai sur la théorie des nombres,* Parigi, Courcier.

LEHTO Olli 1998, *Mathematics without borders: a history of the international mathematical union*, New York, Springer.

LEMMERMEYER Franz
1962 *Reciprocity Laws: from Euler to Eisenstein*, Berlin, Springer.
2011 *Jacobi and Kummer's Ideal Numbers*. https://www.researchgate.net/publication/51934423_Jacobi_and_Kummer's_Ideal_Numbers

LEMMERMEYER Franz SCHAPPACHER Norbert 2003, *Introduction to the English Edition of Hilbert's Zahlbericht*. http://www.fen.bilkent.edu.tr/~franz/publ/hil.pdf

LUCIANO Erika
2018a *Constructing an International Library: The Collections of Journals in Turin's Special Mathematics Library (1883-1964)*, «Historia Mathematica», XLV, 4, p. 433-449.
2018b *"Volgere i progressi della scienza a beneficio della scuola": Il Bollettino di Matematica di Alberto Conti*, «Mélanges de l'école française de Rome. Italie et Méditerranée», Dossier La fabrique transnationale de la «science nationale» en Italie (1839-fin des années 1920), 130, 1, p. 1-15.
2018c *From Emancipation to Persecution: Aspects and Moments of the Jewish Mathematical Milieu in Turin (1848-1938)*, «Bollettino di Storia delle Scienze Matematiche», XXXVIII, 1, p. 127-166.

LUCIANO Erika, ROERO Clara S. 2012, *From Turin to Göttingen: Dialogues and Correspondence (1879-1923)*, «Bollettino di Storia delle Scienze Matematiche», XXXII, 1, p. 7-232.

MAGENES Enrico, 1998, *Una testimonianza sul III Congresso dell'U.M.I.*, «Bollettino dell'UMI», s. 8, I-A, p. 1-6.

MAMMONE Pasquale 1989, *Sur l'apport d'Enrico Betti en théorie de Galois*, «Bollettino di Storia delle Scienze Matematiche», IX, p. 143-169.

MARTINI Laura 2004, *Algebraic research schools in Italy at the turn of the twentieth century: the cases of Rome, Palermo, and Pisa*, «Historia Mathematica», XXXI, p. 296-309.

MILLER George A.; BLICHFELDT Hans F.; DICKSON Leonard E. 1916, *Theory and applications of finite groups*, New York, J. Wiley & sons.

MINKWOSKI Hermann
1896 *Geometrie der Zahlen*, Leipzig, Teubner.
1910[2] *Geometrie der Zahlen*, Leipzig, Teubner.
1957[8] *Diophantische approximationen: Eine Einführung in die Zahlentheorie*, New York, Chelsea pub. co.

NASTASI Pietro
1993 *Guido Fubini a cinquant'anni dalla morte*, «Dossier Pristem», Lettera Pristem, X, p. I-XII.
2016 *La matematica in Italia XIX e XX secolo*, ipertesto tematico dell'Accademia Nazionale delle Scienze detta dei XL.

NASTASI Pietro; TAZZIOLI Rossana 2003, *Aspetti di meccanica e meccanica applicata nella corrispondenza di Tullio Levi-Civita (1873-1941)*, «Quaderni Pristem», XIV, Palermo, Bocconi.

NETTO Eugen 1885, *Teoria delle sostituzioni e sua applicazione all'algebra, versione dal tedesco con modificazioni ed aggiunte dell'autore per G. Battaglini*, Torino, Loescher.

PEANO Giuseppe 1889-90, *Angelo Genocchi*, «Annuario della R. Università degli Studi di Torino», p. 195-200.

PEPE Luigi 2011, *Matematica e matematici nella Scuola Normale Superiore di Pisa 1862-1918*, «Annali di storia delle Università italiane», 15, pp. 67-79.

PIAZZA Paola 2000, *I fondamenti di Zolotarev della teoria dei numeri algebrici*, «Bollettino dell'UMI», s. 8, III-A, p. 169–172.

PICONE Mauro 1946, *Necrologio di Guido Fubini*, «Bollettino dell'UMI», s. 3, I, 1, p. 56-58.

RICCI-CUBASTRO Gregorio 1900, *Lezioni di algebra complementare*, Verona-Padova, Druker.

RIBENBOIM Paul 1979, *13 Lectures on Fermat's Last Theorem*, New York, Springer-Verlag.

RIBET Kenneth A. 1990, *On modular representations of Gal(Q̄/Q) arising from modular forms*, «Inventiones Mathematicae», s. 2, C, p. 431–476.

RINALDELLI Lucia 1997-98, *In nome della razza, L'effetto delle leggi del 1938 sull'ambiente matematico torinese*, «QSU To», 2-3, p. 163-170.

ROLLANDI Maria S. 2002, *Le leggi razziali e l'Università di Genova: prime ricerche sui docenti*, «Atti della Società ligure di storia patria», XLII, p. 477-493.

ROTH Peter 1608, *Arithmetica philosophica, oder schöne neue wohlbegründete überaus künstliche Rechnung der Coss oder Algebrae*, Nürnberg, Lantzenberger.

SBRANA Francesco 1957, *Necrologio di Alberto Mario Bedarida,* «Bollettino dell'UMI», s. 3, XII, 4, p. 731.

SCARPIS Umberto 1897, *Primi elementi della teoria dei numeri,* Milano, Hoepli.

SCHAPPACHER Norbert

1991 *Edmund Landau's Göttingen - From the life and death of a great mathematical center,* «Mathematical Intelligence», XIII, p. 12-18.

1998 *"Wer war Diophant?",* «Mathematische Semesterberichte», 45/2, p. 141-156.

2005 *David Hilbert, report on algebraic number fields ("Zahlbericht"),* in Grattan-Guinness (ed.) *Landmark Writings in Western Mathematics,* Amsterdam-Boston, Elsevier; p. 700-709.

2007 *Der nahe und der ferne Euler*, «Elemente der Mathematik», LXII, p. 134-154.

SCIMONE Aldo 1989, *Il circolo matematico di Catania*, «Bollettino di Storia delle Scienze Matematiche», IX, p. 171-191.

SCORZA Gaetano 1930, *In Memoria di Luigi Bianchi*, «Annali della Scuola Normale Superiore di Pisa», XVI, p. 3-27.

SEGRE Beniamino 1954, *Commemorazione di Guido Fubini*, «Rend. Acc. Naz. Lincei, Cl. Sci. FMN», s. 8, XVII, p. 276-294.

SERRE Jean-Pierre 1987, *Sur les représentations modulaires de degré 2 de Gal(Q̄/Q)*, «Duke Mathematical Journal», s. 1, LIV, p. 179–23.

SEVERI Francesco 1943, *La Matematica Italiana nell'ultimo ventennio*, «Gli Annali della Università d'Italia», IV, p. 83-91.

SFORZA Guido 1900, *Sopra un problema di analisi indeterminata*, «Periodico di Matematica», s. 2, II, p. 252-255.

SKINNER Ernst B. 1914 *Review: Julius Sommer, Introduction a la Théorie des Nombres algébriques,* «Bulletin of the American Mathematical Society», XX, 4, p. 202-204.

SLEMBEK Silke 2007, *On the arithmetization of algebraic geometry,* in Gray, Parshall (eds.), *Episodes in the History of Modern Algebra,* American Mathematical Society and London Mathematical Society, p. 285-299.

SOMMER Julius 1907, *Vorlesungen über Zahlentheorie. Einführung in die theorie der algebraischen Zahl Körpern,* Leipzig-Berlin, Teubner (trad. fr. par A. Lévy 1911, *Introduction à la théorie des nombres algébriques*, Parigi, Hermann).

SPEARS Diana F. 2016, *Polygon constructibility, and Gauss's algorithm for solving cyclotomic equations*, 10.13140/RG.2.2.19898.39360.

TERRACINI Alessandro

1944 *Guido Fubini (1879-1943)*, «Revista de la Unión Matemática Argentina», s. 1, XX, p. 27-30.

1968 *Ricordi di un matematico, un sessantennio di vita universitaria*, Roma, Cremonese.

TODHUNTER Isaac 1875[2], *Complementi di algebra o teoria delle equazioni con una collezione di esempii tradotto dall'inglese, e corredato di aggiunte tratte dall'Algebra dello stesso autore da G. Battaglini*, Napoli, Pellerano.

TONELLI Leonida 1900, *Algebra*, lit.

TOTI RIGATELLI Laura 1992, *Contributi italiani della prima metà del XX secolo alla teoria di Galois*, «Amphora», p. 773-780.

TRICOMI Francesco G.

1957 *Matematici italiani del primo secolo dell'Italia unita*, «Bollettino dell'Unione Matematica Italiana», s. 3, XII, 4, p. 678-679.

1962 *Matematici italiani del primo secolo dello stato unitario*, «Memorie dell'Accademia delle Scienze di Torino. Cl. Sci. FMN», s. 4, I.

WEBER Heinrich

1893 *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*, «Mathematische Annalen», XLIII, p. 521-549.

1895 *Lehrbuch der Algebra*, Braunschweig, F. Vieweg und Sohn.

1898[2] *Traité d'Algèbre Supérieure, traduit de l'allemand sur la deuxième édition par J. Griess,* Parigi, Gauthier-Villars.

WHITEHEAD Alfred N. 1898, *A treatise on Universal Algebra with applications*, Cambridge, University Press.

WILES Andrew J. 1995, *Modular elliptic curves and Fermat's Last theorem*, «Annals of Mathematics», CXVI, p. 443-551.

WYMAN Bostwick F. 1972, *What is a reciprocity law?*, «The American Mathematical Monthly», LXXIX, 6, p. 571-586.

WUSSING Hans 1969, *Die Genesis des abstrakten Gruppenbegrieffes,* Berlin, Veb Verlag.

TATE John T. 1950, *Fourier analysis in number fields, and Hecke's zeta-functions*, in Cassels; Fröhlich (eds.) 1967, *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Washington D.C., Thompson, p. 305–347.

UMI 1959, *Carteggio Bianchi*, Roma, Cremonese.

VAN DER WAERDEN Bartel L. 1970, *The foundations of algebraic geometry from Severi to André Weil*, «Archive for History of Exact Sciences», VII, pp. 171-180.

VARNIER Giovanni B. 2003, *L'Accademia Ligure di Scienze e Lettere e le "leggi razziali" tra silenziose espulsioni e tarde reintegrazioni*, «Atti della Società ligure di storia patria», s. 42, p. 495-510.

VIOLA Carlo

1991 *Alcuni aspetti dell'opera di Angelo Genocchi riguardanti la teoria dei numeri*, in Conte; Giacardi (eds.), *Angelo Genocchi e i suoi interlocutori scientifici: contributi dall'epistolario*, Torino, DSSP, p. 11-29.

2019 *Il teorema dei numeri primi*, in Luciano, Oggero, Sabena (eds.), *Conferenze e Seminari dell'Associazione Subalpina Mathesis 2018-2019*, Torino, L'Artistica Savigliano, p. 155-170.

FONTI ICONOGRAFICHE

1. Guido Fubini (1879-1943)

2. Da sinistra L. Tonelli, Anna Fubini Ghiron, la moglie di F. Severi, G. Fano (alle spalle delle signore), G. Fubini (al centro), T. Levi-Civita, Libera Trevisani Levi-Civita, F. Severi (alla destra) ritratti in una sosta alla stazione di Varsavia durante il viaggio di piacere per alcune capitali europee nel 1925 (la foto proviene dall'archivio della famiglia di Vittorio Ceccherini, si riproduce per cortesia di P. Nastasi)

3. Parallelogramma fondamentale di una rete di punti (Fubini 1917, cap. 3, §2, p. 78)

4. Guido Fubini negli anni Trenta

5. Guido Fubini con la moglie Anna Ghiron

6. Esemplare delle *Lezioni di Teoria dei numeri* nella Biblioteca Speciale di Matematica, Università di Torino

7. Guido Fubini, *Lezioni di Teoria dei numeri 1916-17*, cap. 8, §7, p. 226

8. Da sinistra G. Fano (secondo da sinistra), G. Fubini, Libera Trevisani, Anna Fubini Ghiron, Levi-Civita, L. Tonelli, T. Levi-Civita

9. Guido Fubini

10. Guido Fubini

11. Guido Fubini nel 1939

Fig. 1. Parallelogramma fondamentale di una rete di punti (Fubini 1917, cap. 3, §2, p. 78)

Fig. 2. Campo fondamentale $K - H + L$ (Fubini 1917, cap. 3, §2, p. 80)

Fig. 3. Studio dei due casi di parallelogrammi limite (Fubini 1917, cap. 3, §4, p. 93)

Fig. 4. Trasformazione di un parallelogramma fondamentale nel passaggio da una rete di punti ad un'altra (Fubini 1917, cap. 3, §7, p. 113)

Fig. 5. Rappresentazione sul piano cartesiano delle ridotte di una frazione continua (Fubini 1917, cap. 4, §2, p. 122)

Fig. 6. Caso di indeterminazione nella scelta del quarto vertice del parallelogramma fondamentale (Fubini 1917, cap. 5, §3, p. 151)

Fig. 7. Rappresentazione posteriore, a matita, del caso eccezionale (Fubini 1917, cap. 5, §3, p. 151)

Fig. 8. Triangolo modulare (Fubini 1917, cap. 5, §4, p. 156)

Fig. 9. Trasformazioni che agiscono sul triangolo modulare (Fubini 1917, cap. 5, §4, p. 159)

INDICE DEI NOMI E DEI SOGGETTI

Abel Niels H. 25
Alvarez Carlos 45n
Amato Vincenzo 3n
Andreoli Giulio 36
Argand Jean-Robert 25
Artin Emil X, 21, 29, 30
Avigad Jeremy 17n
Bachmann Paul G.H. 7
Battaglini Giuseppe 2 e n
Bedarida Alberto Mario 2 e n, 3 e n, 37.
Belardinelli Giuseppe 3, 37
Belhoste Bruno 4 e n
Bernoulli Jakob 30
Bertolini Massimo 21n
Berzolari Luigi 35, 36
Betti Enrico 2 e n
Bianchi Luigi IX, 1 e n, 2 e n, 3, 6 e n, 9, 10, 14, 35, 36, 45n, 46n, 49n, 50n, 51n, 52n, 54n, 55n, 57n, 67n, 68n, 73n, 75n, 79n, 80n, 81n, 89n, 95n, 101n, 102n, 104n, 105n, 106n, 108n, 109n, 110n, 112n, 114n, 115n, 116n, 118n, 120n, 121n, 123n, 125n, 126n, 127n, 128 e n, 129n, 130n, 131n, 132n, 133n, 134n, 135n, 136n, 138n, 140n, 142n, 144n, 147n, 148n, 149n, 151n, 153n, 155n, 156n, 157n, 159n, 160n, 163n, 164n, 165n, 166n, 167n, 168n, 169n, 170n, 171n, 174n, 181n, 182n, 183n, 185n, 186n, 188n, 189n, 190n, 191n, 194n, 195n, 210n, 211n, 213n, 215n, 216n, 217n, 218n, 219n, 220n, 221n, 223n, 224n
Blichfeldt Hans F. 8
Boggio Tommaso 4n
Boniface Jacqueline 24n
Bortolotti Ettore 3, 37, 38
Bottari Amerigo 2n, 10n
Bottazzini Umberto 2n, 3n
Brigaglia Aldo 2n, 3n
Butzer Paul 2n
Campi IX, 1, 7n, 8, 9 e n, 11, 13, 14, 15, 16, 17, 19, 20, 21n, 22, 24, 25, 27, 28, 29, 32, 45 e n, 46, 78, 80 e n, 84, 85, 87, 134n, 135, 136, 137, 198n, 211 e n
Candido Giacomo 2
Cantor Georg F.L.P. 4n, 35
Canuto Giuseppe 21n
Carbone Luciano 2n
Carmichael Robert D. 8
Carozzi Adelaide 4n
Cassels John W.S. 13n, 24n
Cassina Ugo 4, 38
Castelnuovo Guido 1, 36
Catalan Eugène 2 e n
Cauchy Augustin-Louis 35
Cavallaro Vincenzo G. 2n
Cecioni Francesco 2
Cesàro Ernesto 2 e n
Châtelet Albert 8
Chebyshev Pafnuty IX, 2, 6, 7 e n
Chella Tito 2, 3
Cherubino Salvatore 3
Chevalley Claude 13, 17n
Chiarenza S. 41n
Chisini Oscar 37
Cibrario Maria 10n, 65n
Cipolla Michele 3 e n, 36, 38
Composto S. 2n
Concina Umberto 2n
Conforto Fabio 3 e n
Congruenze IX, 2 e n, 3n, 7, 9, 10, 18, 20, 28, 29, 55 e n, 56-74, 118, 131, 138, 163, 168, 169, 174-177, 179, 193, 194, 198-200, 219-222
Conte Alberto 1n
Coolidge Julian 6n
Corry Robert 3n
Cunningham Allan J.C. 8
D'Alembert Jean-Baptiste 45 e n
Davenport Harold 17n
De Benedetti Ester 4n
De Franchis Michele 3n
Dedekind Richard IX, 1n, 2, 6, 7, 9, 16, 17, 18, 23, 24, 29, 48n, 51n, 128, 129n, 133 e n, 134 e n, 137n, 138n, 140n, 141n, 142n, 144, 151n, 152n, 153n, 160n, 163, 165n, 170n, 171n, 181n, 182n, 185n, 186n, 211n, 212n, 213n, 223
Dhombres Jean 45n
Dickson Leonard E. 7n, 8

Diofanto di Alessandria 121n
Dirichlet Johann Peter Gustav Lejeune IX, 2, 3n, 6 e n, 7n, 9, 10, 12, 13, 15, 19, 29, 43n, 44n, 48n, 51n, 52 e n, 53n, 54n, 55n, 56n, 57n, 59n, 60n, 64n, 65n, 66n, 67n, 68n, 69n, 70n, 71n, 72n, 73n, 75n, 104n, 105n, 106n, 107n, 109n, 112n, 116n, 125n, 126n, 127n, 128, 129n, 130n, 131n, 133 e n, 134n, 136n, 138n, 140n, 141n, 142n, 144, 145 e n, 147 e n, 148n, 149, 151n, 153n, 155n, 157n, 159n, 160n, 165n, 166n, 167n, 168n, 170n, 171n, 172n, 180n, 181n, 182n, 183n, 184n, 186 e n, 192 e n, 193n, 198n, 211n, 212n, 213n, 217n, 221n, 223, 224
Edwards Harold M. 17n
Emaldi Maurizio 2n
Enriques Federigo 1, 5, 35
Euclide 15, 23, 43 e n, 45 e n, 51n, 52n, 96, 97, 130, 133, 157
Euler Leonhard IX, 7, 9, 18, 20, 22 e n, 29, 30, 51 e n, 71 e n, 121 e n, 219n
Faifofer Aureliano 2, 6, 64n, 133n, 223
Fano Gino 1, 7, 8f, 54f
Fantappiè Luigi 2, 24n
Fenster Della D. 8n
Fermat Pierre IX, X, 9, 10, 20-23, 57 e n, 59, 60, 65, 66, 68, 71, 121 e n, 132, 167-169, 174, 175, 201, 202 e n, 203, 220
Fontebasso Pier Andrea 2
Forme 1, 3n, 4n, 6, 7, 12-14, 18, 19, 21n, 23, 24, 29, 32, 35, 37, 44, 75n, 91, 95n, 101-103, 104 e n, 105 e n, 107, 108, 109 e n, 111-115, 116 e n, 117-120, 121 e n, 122 e n, 123 e n, 124, 125 e n, 126, 127, 128n, 131, 133, 135 e n, 138n, 143, 149, 154, 155, 160 e n, 161 e n, 162 e n, 163, 165, 169, 174n, 180 e n, 181n, 204 e n, 206-209, 210 e n
Frattini Giovanni 2
Frazioni continue 6, 12, 95 e n, 97 e n, 98f, 100, 125
Frenicle Bernard 57n
Frenkel Edward 21n
Frey Gerhard 21 e n
Frobenius Ferdinand G. 28 e n
Fröhlich Albrecht 13n, 24n
Fubini David 1n
Fubini Guido *passim.*
Fubini Jacobs Laurie 1n
Fujiwara Matsusaburo 8.
Funzione zeta X, 3, 29-32, 224
Funzione $\varphi(m)$ di Euler 9, 18, 52, 54 e n, 57, 167, 218n
Galois Évariste X, 1, 2 e n, 6, 15, 19, 20 e n, 21 e n, 25, 27-29, 31, 37, 38, 129, 138 e n, 148n
Gandiglio Maria 4
Garret Reeve 17n
Gauss Johann Friedrich Carl IX, 2 e n, 6, 7, 9, 10 e n, 14, 15 e n, 16, 20, 22, 25, 26, 28, 43n, 45 e n, 46 e n, 52n, 55n, 57n, 58n ,63, 65n, 67n, 71 e n, 72n, 73n, 104n, 105n, 106n, 109 e n, 110n, 116n, 129 e n, 130-133, 149, 157, 163, 191n, 198n, 201n, 209, 211n, 212n, 213 e n, 215, 216 e n
Gazzaniga Paolo IX, 2 e n, 6 e n , 9, 10, 35, 36, 43n, 45m, 52n, 54n, 55n, 57n, 58n, 59n, 61n, 63n, 65n, 67n, 69n, 70n, 71n, 73n, 75n, 95n, 96n, 97n, 100n, 103n, 105n, 106n, 108n, 109n, 116n, 121n, 122n, 123n, 127n, 129n, 130n, 131n, 134n, 151n, 153n, 157n, 158n, 159n, 160n, 163n, 170n, 171n, 174n, 181n, 193n, 195n, 198n, 199n, 201n, 204n, 206n, 207n, 210n, 211n, 213n, 215n, 217n, 218n, 219n.
Genocchi Angelo 2
Geometria dei numeri 11, 12, 15, 17, 18, 35, 75 e n, 76-93, 134-136
Ghigi Luisa Bettina 4
Ghiron Anna 32f
Giacardi Livia 1n
Girard Albert 45n
Goldbach Christian 121n
Goldstein Catherine 2n, 21n, 24n
Gray Jeremy 3n
Gröbner Wolfgang 24
Gruppi 1, 3, 4, 6, 11 e n, 12-15, 18, 20 e n, 21, 22, 24, 25, 28 e n, 29-31, 35-38, 78, 79, 80 e n, 92, 105, 113 e n, 115, 116, 123, 134, 155
Guerraggio Angelo 3n

Hadamard Jacques S. 29n, 30
Hardy Godfrey H. 8
Harris Michael 21n, 22n
Hasse Helmut 174 e n
Hawkins Thomas 28n
Hecke Erich 27 e n
Hilbert David IX, 7 e n, 16, 17, 18, 19, 23 e n, 32, 133n, 134 e n, 136n, 138n, 140n, 141n, 144n, 147n, 152n, 153n, 157n, 158n, 159n, 160 e n, 161n, 163n, 166n, 167n, 168n, 169n, 171n, 180n, 186n, 189n, 192n, 193n
Hurwitz Adolph 7
Ideali IX, X, 1, 2, 3n, 6, 7 e n, 9, 12-14, 16-18, 19 e n, 20 e n, 21-24, 29, 32, 48, 49 e n, 50, 59, 132, 133, 134n, 138n, 151 e n, 152, 153 e n, 154, 155, 156n, 157, 158 e n, 159, 160 e n, 161-164, 165 e n, 166-168, 169 e n, 170 e n, 171 e n, 172, 173, 174 e n, 175-180, 183, 184, 187-190, 193 e n, 194, 195 e n, 196-200, 204 e n, 205-207, 208 e n, 209, 210n, 211n, 212, 213, 219, 221-223
Indici 10 e n, 25, 28, 65 e n, 67 e n, 68, 74, 145, 168, 213n, 221, 223
Jacobi Carl 7, 10, 38, 70, 71n, 184
Jongmans François 2n
Jordan Camille 2n
Klein Felix IX, 5, 7, 11, 12 e n, 25, 75 e n, 77n, 78 n, 95n, 97n, 99n, 105n, 113n
Koreuber Mechthild 3n
Kronecker Leopold 7 e n, 18, 23-25, 29, 122n, 134 e n, 138 e n, 152n, 160 e n, 162 e n, 163, 165 e n, 171n, 176, 177, 180 e n, 204 e n
Kummer Ernst E. IX, 7, 17, 21, 22, 134 e n, 138n, 152n, 201n, 202 e n, 204n, 211n, 221n
La Vallée-Poussin 29n, 30
Lagrange Joseph-Louis 47n, 71
Landau Edmund 3, 7 e n
Langlands Robert 21 e n, 29
Laurent Hermann P.M. 8
Legendre Adrien-Marie 7, 10, 20 e n, 27, 28, 70, 71 e n, 194, 218
Legge di reciprocità quadratica X, 4, 7, 10 e n, 20, 21, 27-29, 71n, 72, 73n, 198n, 199, 200, 218n
Leibniz (von) Gottfried W. 57n
Lemmermeyer Franz 17n, 20n, 23n, 27 e n, 28n
Levi Beppo 3, 37, 38
Levi-Civita Tullio 8f, 54f
Lévy Paul P. 7n
Libri Guglielmo 2n
Lie Sophus M. 11, 38
Luciano Erika 1n
M.C.D. 15, 16, 19, 23, 43 e n, 44, 45, 47, 49, 50, 52, 56, 59, 60, 66, 68, 95n, 96, 105-107, 126, 130, 132, 151-153, 157, 161-165, 168, 172, 173, 175, 178, 179, 220, 223
Madia G. 37
Malfatti Gianfrancesco 2n
Mammone Pietro 2n
Mancinelli Maria 4
Maroni Arturo 3n
Martini Laura 3n
Massarini Iginia 2
Mazzoni Pacifico 2
Mignosi Gaspare 37, 38
Miller George A. 8
Minkowski Hermann IX, 7 e n, 11, 12, 13, 14 e n, 15 e n, 18, 19, 75n, 81 e n, 82n, 85n, 86n, 87n, 91n, 101 e n, 109 e n, 112, 127n, 134 e n, 135n, 136n, 143 e n, 144, 145, 146, 151n, 169n, 171n, 168n
Mordell Louis J. 8
Morra Maria Teresa 4
Nalli Pia M. 3n, 37
Nastasi Pietro 1n, 3n
Netto Eugen 2
Newton Isaac 56, 175, 220
Nicoletti Onorato 2
Noether Emmy 3
Numeri interi algebrici IX, 1, 3, 4, 7 e n, 15-17, 24, 27-29, 35-37, 48n, 75n, 95n, 105n, 129, 133, 134n, 140 e n, 141, 156, 157, 172, 173, 174n, 181n, 202
Ostrowski Alexander 13
Palladino Franco 2n
Peano Giuseppe 2n, 7

Pell John 14, 127 e n, 149
Pepe Luigi 2n
Periodi 6, 10, 25-28, 123 e n, 125 e n, 127n, 197, 211n, 213 e n, 215 e n, 216n, 217
Perna Alfredo 36, 27
Piazza Paola 17n
Picone Mauro 1n
Piva Angiolina 4n
Poisetti Eugenio 4
Ramanujan Srinivasa A. 8
Rete di punti/parallelogrammi 1, 6n, 7n, 11 e n e f, 12, 13, 14, 19, 21, 24, 75 e n, 76-79, 80n, 81-84, 88, 89, 91, 92f, 93, 103, 104, 110-112, 134, 141, 142 e n, 153, 155, 185
Ribenboim 21n, 22
Ribet Kenneth A. 21 e n
Ricci Giovanni 3, 38
Riemann G.F. Bernhard 3, 29, 30
Roero Silvia 1n
Rollandi Maria S. 3n
Romanovsky Vsevolod I. 8
Ruffini Paolo 25, 63
Sansone Giovanni 2
Scarpis Umberto 2 e n, 35
Schappacher Norbert 2n, 23n, 24n
Schwermer Joachim 2n
Scimone Aldo 1n, 2n, 3n
Scorza Gaetano 3, 35
Segre Annetta 4 e n
Segre Beniamino 1n, 5n, 32n
Segre Corrado 1, 4n, 6, 7, 10
Serre Jean-Pierre 21 e n
Severi Francesco 1n, 3 e n, 8f
Shimura Gorō 21
Skinner Ernst B. 7n
Slembek Silke 3n
Sommer Julius 7 e n, 27, 43n, 45n, 52n, 53n, 55n, 57n, 59n, 63n, 67n, 70n, 71n, 73n, 75n, 76n, 90n, 95n, 106n, 116n, 129n, 133n, 147n, 148m, 149n, 151n, 152n, 153n, 155n, 157n, 158n, 159n, 160n, 163n, 166n, 167n, 168n, 169n, 170n, 171n, 192n,193n, 195n, 197n, 198n, 200 e n, 201n, 202n, 204n, 218n
Spampinato Niccolò 3
Spears Diana 26
Suzuki Toshikazu 8
Taniyama Yutaka 21
Tate John T. 13, 30
Terracini Alessandro 1n, 41
Terracini Benvenuto 1n
Tonelli Leonida 8f, 54f
Torelli Gabriele 35
Toti Rigatelli Laura 2n
Tricomi Francesco 1n, 41n
Unità 3n, 4, 9n, 12-16, 19, 21-26, 28, 19, 43, 45, 51n, 52n, 86, 97, 101, 114, 129 e n, 130-132, 135, 144-147, 149, 151, 153 e n, 155, 159, 161-163, 165, 173, 174, 186n, 187, 188, 189n, 192, 196-205, 208, 212, 216
Uspensky James V. 8
Van der Waerden Bartel L. 3n
Vandiver Harry S. 8
Varnier Giovanni B. 3n
Velimin V.P. 8
Viola Carlo 2n, 7n, 29n
Weber Heinrich 3, 7, 29, 45n, 65n, 127n, 129n
Weyl Hermann 3
Wiles Andrew J. X, 21, 121n
Wilson John 7, 10, 20, 74
Wussing Hans 11n
Wyman Bostwick F. 28n
Zilinskij A.P. 8

Se esiste un testo didattico da cui emergano le doti di insegnante e di oratore di Guido Fubini e la 'freschezza' del suo ingegno, ovvero la capacità di cogliere le linee di ricerca più promettenti, di acquisirle rapidamente e di saperle trasmettere nei suoi corsi, questo è il manoscritto litografato di Lezioni di Teoria dei numeri. *Nel secondo semestre dell'a.a. 1916-17, in un'Università svuotata dalla guerra ed a poca distanza dalla scomparsa di R. Dedekind, Fubini sceglieva di presentare a un gruppo di allievi, quasi digiuni di algebra astratta, la teoria degli ideali, per poi avviarli allo studio delle forme quadratiche, degli interi algebrici di un campo, degli ideali di un anello, dei campi quadratici e ciclotomici, della geometria dei numeri. Allievo di Luigi Bianchi a Pisa, Fubini aveva forse ereditato dal suo maestro l'interesse per questi ambiti di ricerca e seppe costruire a Torino un corso di teoria dei numeri dall'architettura tanto originale quanto complessa, approdando a una sintesi armonica di due tradizioni di pensiero distinte: quella italiana e quella tedesca. Lezioni ricche, suggestive, quelle di Fubini, che dimostrano l'ampiezza di orizzonti culturali, il rigore metodologico, la precisione e chiarezza espositiva di questo illustre matematico e che costituiscono un documento di notevole valore nel quadro della storia degli insegnamenti scientifici offerti dall'Ateneo torinese nel primo Novecento.*

Guido Fubini (1879-1943) professore di Analisi algebrica e infinitesimale al Politecnico, tenne per incarico all'Università di Torino il corso di Analisi superiore dal 1910 al 1938, quando a causa delle leggi razziali fu costretto a emigrare negli Stati Uniti, a Princeton e a New York. Little giant *della matematica italiana, diede fondamentali contributi in diversi settori di studi, sia puri che applicati: analisi, teoria dei gruppi continui e discontinui, geometria non euclidea, geometria proiettivo-differenziale, fisica matematica, relatività, balistica e ingegneria. Autore di importanti testi, quali la* Geometria proiettiva differenziale, *l'*Introduction à la géométrie différentielle des surfaces *(1926-27 e 1931 con E. Čech) e* La matematica dell'ingegnere e le sue applicazioni *(1949 e 1954 con G. Albenga), fu un ricercatore di fama internazionale e un docente di grande talento didattico.*

€ 25,00

ISBN 978-88-909997-6-5