STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

Oriënteringscursus ALGEBRA

gehouden te Groningen 1962/63

door

Dr. J. Koksma

onder auspiciën van het Genootschap "Johann Bernoulli"

Samenvatting

van de oriënteringscursus Algebra te Groningen 1962/63, onder auspiciën van het Genootschap "Johann Bernoulli", te houden door

Dr. J. Koksma

I. Inleiding

1. Abstractie. Onze (denk-)begrippen zijn abstract, d.w.z. ze zijn ontstaan, doordat van een voorstelling enkele aspecten, of van een groep van voorstellingen de gemeenschappelijke aspecten in het oog werden gevat en van alle andere werd geabstraheerd, d.w.z. dat die buiten beschouwing werden gelaten. Kenmerkend voor de wiskunde is, dat ze daartoe de kwantitatieve en ruimtelijke aspecten van de dingen kiest en daarvan de logische relaties opspoort. Sinds de ontdekking van de analytische meetkunde is langzamerhand het ruimtelijke tot het kwantitatieve herleid en is men het "getal" als grondbegrip en de rekenkunde als fundament van de wiskunde gaan zien. De vruchtbaarheid van de wiskundige methode blijkt bij de toepassing, d.i. het bij het resultaat van de wiskundige werkzaamheid weer vullen van de daarin optredende begrippen met hun oorspronkelijke (of ook een geheel andere) inhoud.

Het eigenlijk typerende van de wiskunde is overigens, dat de beoefenaar die abstractie bewust zoekt en in stand tracht te houden en daarbij niet op de mogelijkheid van toepassing let, hij onderzoekt de abstracte begrippen en hun relaties zelf. Zijn werkzaamheid kan zich daarbij in één van twee richtingen bewegen: ze kan gericht zijn op uitbouw, of ze kan terug zoeken naar zo eenvoudig mogelijke "grondslagen". In beide richtingen zijn in de vorige eeuw grote resultaten bereikt, de abstracte algebra is een natuurlijke vrucht van de laatste. Het zoeken naar grond-

slagen zuivert de begrippen steeds meer van niet-logische bestanddelen, ze worden steeds abstracter, d.w.z. steeds leger. Het volmaakt abstracte begrip is ook volmaakt "zin"-loos. En hier zet dan een herhaling van de geschiedenis in, men kan de ontwikkeling van de algebra zien als analoog aan die van b.v. de analyse. De algebra trekt n.l. de consequenties en abstraheert bewust van het getalkarakter der wiskundige grondbegrippen. Daarmee zet dan een verdieping en verbreding van de wiskunde in, waarop het boven van de kwantitatieve wiskunde gezegde geheel van toepassing is.

Ook blijft waar, dat de algebra haar begrippen om henzelf onderzoekt. Dit heeft nog niet geleid tot een zo strenge scheiding van "zuivere" en "toegepaste" algebra als in de wiskunde in zwang is gekomen, noch worden de leerboeken zo angstvallig "zuiver" gehouden, als met de analyseboeken b.v. meestal nog steeds het geval is. Dat neemt niet weg, dat ook in deze cursus het zwaartepunt wel in de algebraïsche structuren zelf moet komen te liggen.

2. Getalbegrip.

2.1. We zullen trachten de overgang van rekenkunde naar algebra geleidelijk te maken. Uitgangspunt vormen enkele stadia van de "ontwikkeling van het getalbegrip", een vroeger (misschien nog) verplicht stuk leerstof, waarin, uitgaande van de natuurlijke getallen, door ingewikkelde logische constructies hogere getalsoorten worden ingevoerd. Het oorspronkelijke onderzoek hiernaar is uiteraard hoofdzakelijk andersom gericht geweest, men heeft van boven naar beneden grondslagen gezocht, of liever geconstrueerd, en zal daarbij geleid zijn door de getalnotie, m.a.w. men heeft bewust van een reële getalvoorstelling een abstract getalbegrip gemaakt.

De bekendste behandeling van de natuurlijke getallen is die van Peano.

2.2. Peano beschouwt een verzameling N, waarvan hij de elementen "natuurlijke getallen" noemt. Hij veronderstelt, dat ze aan de volgende eisen voldoen:

1. Er is een natuurlijk getal 1.
2. Bij elk element a hoort precies één element a^+ (zijn "opvolger").
3. Er is geen element a met $a^+ = 1$.
4. Uit $a^+ = b^+$ volgt $a = b$.
5. Is A een deelverzameling van N met de eigenschappen:

1^{o}. $1 \in A$,

2^{o}. als $a \in A$, dan $a^{+} \in A$,

dan is $A = N$.

Op deze postulatie is, door middel van geschikte definities, de gehele analyse op te bouwen.

2.3. Men kan het fundament ook minder diep leggen, b.v. in de verzameling der gehele getallen (voortaan aan te duiden als C). Men kan dan uitgaan van het volgende stel eigenschappen:

1. In C zijn twee bewerkingen gedefinieerd: optelling en vermenigvuldiging (een bewerking voegt aan twee elementen in gegeven volgorde een derde element toe).
2. Beide zijn associatief en commutatief, de vermenigvuldiging is distributief t.o.v. de optelling.
3. Er zijn twee verschillende elementen 0 en 1 met de eigenschap

$$a + 0 = a, \quad a \cdot 1 = a \qquad \text{voor elke } a \in C.$$

(Ze heten de "identiteitselementen" of "neutrale elementen" voor hun bewerkingen.)

4. Elk element a heeft een "tegengestelde" -a met

$$a + (-a) = 0$$

5. Uit $ab = 0$ volgt $a = 0$ of $b = 0$
(of omgekeerd: uit $a \neq 0$ en $b \neq 0$ volgt $ab \neq 0$).

2.4. Niet alle eigenschappen der gehele getallen zijn uit deze te halen, de orderelaties vallen er buiten. Maar het gewone rekenen zit er geheel in.
B.v. de mogelijkheid van de aftrekking, d.w.z. het oplossen van de vergelijking

$$a + x = b.$$

Tel beiderzijds -a op. Er volgt $x = -a+b$, deze wortel voldoet bij substitutie.

Er is maar één wortel, de aftrekking is ondubbelzinnig: stel $a+x=a+y$. Tel beiderzijds -a op. Er volgt $x = y$.

Er is maar één nul. Stel twee, 0 en 0'. Dan:

$$0 = 0 + 0' = 0'.$$

Per element ook maar één tegengestelde, wegens de ondubbelzinnigheid van de aftrekking (a+x=0).

Belangrijke eigenschap van de nul:

$$a \cdot 0 = 0.$$

Bewijs: enerzijds $a(b+0) = ab + a.0$

anderzijds $a(b+0) = ab = .ab + 0.$

Dus $ab + a.0 = ab + 0$. Tel beiderzijds $-(ab)$ op. Er volgt $a.0 = 0$.

2.5. Men kan de grondeigenschappen van de gehele getallen natuurlijk ook anders kiezen.

Bij voorbeeld: eig. 3 is symmetrisch voor optelling en vermenigvuldiging, eig. 4 stelt nog een extra-eis aan de optelling. In plaats van de existentie van de nul en de tegengestelde kan men ook de onbeperkte aftrekkingsmogelijkheid eisen. Dat wordt dan:

Bij elke a en b is er een x met $a + x = b$.

Te bewijzen: er is een nul.

Bewijs: Neem een a. Dan heeft $a + x = a$ een oplossing. Stel p.

Neem nu willekeurige b, en een y met $y + a = b$.

Dan is $b + p = y + a + p = y + a = b$.

Ander voorbeeld: eig.5 is te vervangen door de "vereenvoudigingswet":

uit $ab = ac$ volgt $a = 0$ of $b = c$ (dus $b = c$ als $a \neq 0$).

Bewijs van de gelijkwaardigheid:

1^o. Geg. eig.5.

Stel $ab = ac \rightarrow ab - ac = 0 \rightarrow a(b-c) = 0 \rightarrow a = 0$ of $b - c = 0$.

In het laatste geval is $b = c$.

2^o. Geg. de vereenvoudigingswet.

Stel $ab = 0 \rightarrow ab = a.0 \rightarrow a = 0$ of $b = 0$.

3. Overgang naar de algebra

3.1. De in de vorige paragraaf gegeven bewijsjes zijn in hoge mate formeel, van het intuïtieve getalbegrip is volledig geabstraheerd. Het zijn ketens van uitsluitend - logische conclusies met als uitgangspunt de eigenschappen van 2.3. Die zijn boven "grondeigenschappen" genoemd. Ziet men ze als zodanig dan heeft het geen zin naar hun "bewijs" te vragen, dat kan alleen gegeven worden, wanneer er een dieper gelegen fundament is, waarop het zou kunnen worden gebaseerd. Zo'n fundament wordt b.v. gevormd door de postulaten van Peano plus definities van het gehele getal en van de bewerkingen.

Het woord "bewijzen" kan hier trouwens misleidend zijn, het suggereert de betekenis "waar maken" en daarvan is hier geen sprake. De rekenkunde is er geen zier waarder of aannemelijker om, dat ze uit "Peano" wordt afgeleid, didactici mogen wel bedenken dat het voor de onrijpe leerling zelfs wel andersom zal zijn. De prestatie van Peano ligt niet zo zeer in het "bewijzen" van de stellingen der rekenkunde als wel in het uit die stellingen isoleren van zijn axioma's, minder in het stelsel van die axioma's als uitgangspunt dan als resultaat van wiskundige werkzaamheid. Het is vrucht van een analyse, van een retrograde bezinning dus. Die bezinning is duidelijk bewust abstraherend. Peano komt uit bij een verzameling van lege "dingen", waarvan het essentiële ligt in enkele relaties, eigenlijk slechts reeksen woorden, waarmee mechanisch - logisch moet worden geopereerd. En daarmee heeft hij dan de zelfgestelde taak volbracht: de volledige abstractie van het intuïtieve getalbegrip tot...vrijwel niets, maar niettemin (toen) de grondslag der rekenkunde.

Evenwel: ziet men wijder dan eng-wiskundig, dan blijkt het intuïtieve getalbegrip toch de eigenlijke basis gebleven te zijn, het is immers bij die analyse leidraad zowel als norm geweest, er is angstvallig voor gewaakt, dat er straks bij de opbouw niets uit kan komen dan het wèlbekende en wat daar wettig uit volgt.

Hier zet nu de algebra in, ze snijdt radicaal de band met de voorstelling door, waarvan geabstraheerd is. Als we toch doen alsòf, waarom zouden we het niet ècht maken? Voorwerp van onderzoek wordt een stel postulaten over dingen, waarbij men zich niets voorstelt; wat er uitkomt, zien we vanzelf.

3.2. We kiezen het stel van 2.3 om deze verandering van instelling nader toe te lichten; een verzameling, die er aan voldoet, heet een integriteitsgebied.

Er is een verzameling verondersteld en daarin twee bewerkingen; een bewerking (verbinding, operatie) is een voorschrift dat aan twee elementen in gegeven volgorde een derde toevoegt. Dat "voorschrift" moet men niet te letterlijk nemen, het wordt hier slechts verondersteld; het moet alleen zo zijn, dat het aan de postulaten voldoet. Die postulaten dragen nu in het geheel niet meer het karakter van "onbewezen stellingen", het zijn voorwaarden, die men aan de bewerkingen oplegt en welker keuze (formeel) zelfs geheel willekeurig is, als ze maar niet tot tegenspraken leiden. In het bijzonder is er in het geheel geen aanleiding meer onder de postulaten van het integriteitsgebied weer een basis te schuiven, door b.v. op Peano terug te gaan, ze staan daar "in their own right".

Zo gezien, ligt er een geheel veld van mogelijkheden open, men kan postulaten wijzigen, weglaten, toevoegen of zelfs geheel nieuwe stelsels ontwerpen en van de aldus "gestructureerde" verzameling de eigenschappen opsporen.

Het nader aangeven van de bewerkingsvoorschriften is zaak van toepassing. Voldoen ze aan een stel postulaten, dan bezit de onderzochte verzameling natuurlijk ook alle eigenschappen, die daar uit afgeleid zijn. Vaak blijken zo verzamelingen met bewerkingen, die op het oog niets met elkaar te maken hebben, toch dezelfde structuur te bezitten. Men ziet de analogie met de analyse, de algebra is even vruchtbaar gebleken.

Psychologisch is de ontwikkeling even anders, of misschien (gelukkig) nog zo ver niet gevorderd. In § 1 werd al opgemerkt dat er (nog) geen scherpe scheiding is tussen "zuivere" en "toegepaste" algebra, het is b.v. geen gewoonte om de rekenkunde van het gehele getal uit een algebraboek te weren, omdat ze slechts een toepassing van het integriteitsgebied zou zijn.

3.3. We geven nu eerst een voorbeeld van definitie van een bewerking. We bevinden ons dus in het gebied van de toepassing en gaan niet van een abstracte verzameling uit. Neem b.v. de verzameling der gehele getallen. Er zijn al twee bewerkingen in bekend, we kunnen echter willekeurig andere vaststellen, b.v. $a \circ b = a + b^2$. (Let op het nieuw ingevoerde teken.)

Deze bewerking is duidelijk niet-commutatief. Associatief?

$$\left.\begin{aligned}(a \circ b) \circ c &= (a+b^2) + c^2 = a + b^2 + c^2\\ a \circ (b \circ c) &= a + (b+c^2)^2 = a + b^2 + 2bc^2 + c^4\end{aligned}\right\}$$ antwoord: nee.

Is er een neutraal element? Wegens niet-commutativiteit moeten we links en rechts onderscheiden.

Stel $a \circ x = a \rightarrow a + x^2 = a \longrightarrow x = 0$.

Dus 0 is rechts-neutraal-element (rechtséénelement, als we de bewerking vermenigvuldiging noemen).

Stel $x \circ a = a \rightarrow x + a^2 = a \longrightarrow$ Geen links-neutraal-element.

Bij een bewerking kan wel meer dan één éénelement optreden. Een voorbeeld laat zich voor een eindige verzameling gemakkelijk construeren. Bij een eindige verzameling kunnen de uitkomsten van de bewerking worden verenigd in een tabel als de volgende. De betekenis daarvan zal wel duidelijk zijn, de kolom vóór de verticale streep geeft de linkerfactor, de rij boven de horizontale streep de rechter. De tabel kan ook dienen tot definitie van de bewerking, dat is in dit

	a	b	c	d	e
a	a	b	c	d	e
b	a	b	c	d	e
c					
d					
e					

geval gebeurd om twee linkeréénelementen te krijgen, twee rijen zijn daartoe gegeven, de rest kan willekeurig worden ingevuld. Uit de tabel blijkt, dat er nu geen rechteréénelement kan zijn. Dat is ook makkelijk te bewijzen:

Stel dat ε links- en ε' rechtséénelement is. Dan is $\varepsilon = \varepsilon\varepsilon' = \varepsilon'$. Dus alle eventuele éénelementen zijn gelijk, als er van beide soorten één is.

Bij zo'n tabel verraadt commutativiteit zich door symmetrie om de hoofddiagonaal, associativiteit is niet gemakkelijk te constateren.

Voorbeelden van andersoortige elementen zijn getallenparen en -tripels, matrices enz.

3.4. Voorbeelden van integriteitsgebieden

3.4.1. In 2.4 werd al gezegd, dat de gehele getallen door de postulaten van 2.3 niet volledig gekarakteriseerd zijn. Dat blijkt ook daaruit dat de verzamelingen der rationale, der reële en der complexe getallen er ook aan voldoen.

Bij een integriteitsgebied zijn optelling en vermenigvuldiging (bedoeld is: de bewerkingen, die zo heten) onbeperkt mogelijk en bovendien de omkering van de optelling, die we natuurlijk aftrekking noemen. Bij de genoemde verzamelingen is ook de omkering van de vermenigvuldiging, dus de deling, onbeperkt mogelijk, behalve door nul. Onder de postulaten van het integriteitsgebied kan deling door nul niet worden gedefinieerd: de vergelijking $x.0 = b$ is voor $b \neq 0$ onoplosbaar, voor $b = 0$ is elk element oplossing.

Is in een integriteitsgebied de deling (behalve door nul) onbeperkt uitvoerbaar, dan heet het een commutatief lichaam (het algemene begrip lichaam is ruimer en geen bijzonder geval van het integriteitsgebied), Stelt men de eis van de onbeperkte delingsmogelijkheid (dus de oplosbaarheid van de vergelijking $ax = b$, met $a \neq 0$), dan kan de eis, dat er een 1 is vervallen. Omgekeerd kan de eis van deelbaarheid vervangen worden door een éénelement te postuleren en voor elk element $\neq 0$ de existentie van een omgekeerde of inverse te eisen, dat is de wortel van de vergelijking $a.x = 1$ (alles analoog aan het in 2.5 van de aftrekking gezegde).

3.4.2. De getallen $a + b\sqrt{2}$ (a en b willekeurig geheel) vormen een integriteitsgebied. Daar 0 en 1 tot deze verzameling behoren en deze getallen reëel zijn, is contrôle der postulaten verder overbodig. Wel moet men nagaan of de verzameling "gesloten" is voor de beide bewerkingen, d.w.z. of som en product van twee zulke getallen weer van die vorm zijn.

Neemt men a en b rationaal, dan is de verzameling zelfs een commutatief lichaam. Immers is

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2+2b^2} = \frac{a}{a^2+2b^2} + - \frac{b}{a^2+2b^2}\sqrt{2}.$$

3.4.3. Een voorbeeld van een eindig integriteitsgebied (C_7) wordt gegeven door de getallen 0,1,2,3,4,5,6 met als rekenvoorschrift: gewoon optellen en vermenigvuldigen, maar de uitkomst "reduceren modulo 7", d.w.z. vervangen door de (positieve) rest bij deling door 7.
De contrôle van de postulaten is eenvoudig. Wat het laatste postulaat betreft: ab levert nul op, als het een 7-voud is. Voor $a \neq 0$ en $b \neq 0$ kan dat niet, omdat 7 priem is.

Voor $a \neq 0$ volgt dus uit $ab_1 = ab_2$, dat $b_1 = b_2$. Vermenigvuldigen we alle 7 elementen met a, dan krijgen we ze dus alle 7 als product terug. Dus: $ax = b$ is voor elke b oplosbaar. Dus: C_7 is een commutatief lichaam. Hetzelfde geldt voor C_p, p willekeurig priem.

3.4.4. Hoe zit het met C_m, als m niet priem is?
Voorbeeld C_{10} : 0,1,2,3,4,5,6,7,8,9.
Nu is $2 \times 5 = 4 \times 5 = 6 \times 5 = 8 \times 5 = 0$.
Geen integriteitsgebied, het laatste postulaat is niet vervuld. Nog wel een <u>ring</u> (definitie komt nog).
De elementen 2,4,6,8,5 heten <u>nuldelers</u>, het zijn elementen $\neq 0$, waarbij een tweede element $\neq 0$ te vinden is, zodanig dat hun product nul is. (Sommige auteurs rekenen 0 er ook toe.)

Postulaat 5 kan dus ook luiden: er zijn geen nuldelers.

3.4.5. Beschouw nader de deelverzameling (0,2,4,6,8) van C_{10}. Met de elementen gewoon rekenen, maar de uitkomsten modulo 10 reduceren. Men verifiëert gemakkelijk, dat deze verzameling voor beide bewerkingen gesloten is en dat nu geen der elementen nuldeler is. Aftrekking en deling (niet door 0) zijn onbeperkt mogelijk. De verzameling is dus een commutatief lichaam. Dat heeft een éénelement, op te lossen uit een vergelijking $ax = a$, met a willekeurig. Neem b.v. $2x = 2$. Volgt $x = 6$. (alles vgl. 3.4.1).

We gingen van 2 uit en namen daarvan de veelvouden; 5 doet het ook. De elementen 0 en 5 vormen een commutatief lichaam met éénelement 5.

Evenzo bij C_{15} : (0,3,6,9,12) is een commutatief lichaam met éénelement 6, (0,5,10) een commutatief lichaam met éénelement 10.

Algemeen: C_{pq} met p en q priem, $p \neq q$. De deelverzameling $(0,p,2p,\ldots,(q-1)p)$ is een commutatief lichaam. Het éénelement (stel het x) is op te lossen uit de vergelijking $px = p$, of (met een gelijkteken in de gewone betekenis) $px = pq\text{-voud} + p$. Dus $x = q\text{-voud} + 1$. Inderdaad was in onze voorbeelden $6 = 5 + 1$, $5 = 4 + 1$, $10 = 9 + 1$.

4. Verzamelingen

4.1. Begrippen

De verzameling A heet deelverzameling van de verzameling V ($A \subset V$ of $V \supset A$), als elk element van A element van V is.

De doorsnee $A \cap B$ van A en B bestaat uit de elementen, die tot A èn tot B behoren.

De vereniging $A \cup B$ van A en B bestaat uit de elementen, die tot A òf tot B behoren.

Twee verzamelingen A en B heten dan en alleen dan gelijk ($A = B$), als ze uit dezelfde elementen bestaan, dus als elk deelverzameling van de andere is.

Is A deelverzameling van V maar niet gelijk aan V, dan heet A een echte deelverzameling van V.

Men voert nog in één lege verzameling ϕ, d.w.z. een verzameling, die geen element bevat. Dat is een conventie om te kunnen spreken van de doorsnede van A en B, als die disjunct zijn, d.w.z. geen element gemeen hebben. Men stelt dan $A \cap B = \phi$. De lege verzameling wordt als deelverzameling van elke verzameling beschouwd.

4.2.

Als aanvulling van 3.3 volge hier een voorbeeld van bewerkingsdefinities, die van geheel andere aard zijn, dan de daar gegevene.

Neem een verzameling en vorm de verzameling V van de deelverzamelingen daarvan. Het nemen van de doorsnee van twee deelverzamelingen levert een nieuwe, dus weer een element van V. Dat doorsnee nemen is dus een (commutatieve) bewerking. Hetzelfde geldt voor het nemen der vereniging. We noemen het verenigen optellen en het doorsnee nemen vermenigvuldigen; we schrijven dus $A \cup B$ als $A+B$ en $A \cap B$ als AB. Deze bewerkingen zijn duidelijk commutatief en ook associatief. Het onderzoek naar de distributiviteit levert een verrassend resultaat, elk van de bewerkingen blijkt distributief t.o.v. de andere! Dat wil zeggen, dat

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad (\text{of } A(B+C) = AB+BC)$$

en $$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad (\text{of } A+BC = (A+B)(A+C)).$$

De lege verzameling ϕ fungeert als nulelement, immers

$$A + \phi = A \cup \phi = A.$$

V zelf is éénelement, want AV = A $\cap$ V = A.
De verzameling is geen integriteitsgebied, want aan A+X = ϕ is niet te voldoen voor A $\neq \phi$; ook volgt niet A of B = ϕ als AB = ϕ .

Een nieuwe eigenschap is:
Bij elk element A is een element $\overline{A}$ te vinden met

$$A \cup \overline{A} = V \text{ en } A \cap \overline{A} = \phi .$$

Abstraheren we van het "verzameling-zijn" der elementen, dan kunnen de genoemde eigenschappen gepostuleerd worden. Het is gebleken, dat daarbij de associativiteit der bewerkingen gemist kan worden, die kan uit de rest worden bewezen. Het resultaat ziet er zo uit:

Gegeven zij een verzameling van minstens twee elementen, waarin twee bewerkingen zijn gedefiniëerd ("optelling" en "vermenigvuldiging"), voldoend aan de volgende postulaten:

1. Ze zijn beide commutatief
2. Voor beide is er een neutraal element (0 en 1).
3. Elk van de twee is distributief t.o.v. de andere.
4. Bij elk element A is een element $\overline{A}$ te vinden, zodanig dat $A + \overline{A} = 1$ en $A.\overline{A} = 0$.

Het geheel van de eigenschappen dezer verzameling (dus van de conclusies uit deze postulaten) heet de algebra van Boole. Ze werd door de voorzitter van "Johann Bernoulli" in zijn voordracht van 11 maart 1961 uitvoerig ontwikkeld. Hij wees o.a. op de symmetrie tussen optelling en vermenigvuldiging, die maakt, dat alle stellingen in duale paren optreden, zodat men er telkens slechts één hoeft te bewijzen. Ook leverde hij het hier niet gegeven bewijs van de associativiteit.

Het interessantste was de algebra van Boole te voorschijn te zien komen bij de algebraïsering van een stuk logica, dat zo in toepassing kan worden gebracht bij de constructie van rekenmachines.

4.3. Relaties

Tussen twee elementen van een verzameling kan een gegeven relatie (al of niet) bestaan: getallen kunnen een gegeven verschil hebben, of het ene kan het dubbele zijn van het andere; mannen kunnen broers zijn of stoelen even duur.

Belangrijk zijn de equivalenties (aan te geven door $\sim$). Een in een verzameling gedefinieerde relatie heet een equivalentie als ze is:

1) reflexief, d.w.z. elk element is equivalent met zichzelf ($a \sim a$ voor elke a);
2) symmetrisch: uit $a \sim b$ volgt $b \sim a$;
3) transitief: uit $a \sim b$ en $b \sim c$ volgt $a \sim c$.

Deze eisen zijn onafhankelijk van elkaar, zoals uit de volgende voorbeelden blijkt:

1 van 2 en 3: $ab > 0$ (gehele getallen);
2 van 1 en 3: $a \geq b$ (gehele getallen);
3 van 1 en 2: $|a-b| < 2$ (reële getallen).

In een verzameling van mannen is het "dezelfde vader hebben" een equivalentie, het broerschap daarentegen niet (het is niet reflexief en zelfs niet transitief, want uit AbB en BbA zou toch volgen AbA). Men scherpe zijn vernuft aan het volgende (in sommige boeken opgegeven) vraagstukje: de reflexiviteit volgt uit de symmetrie en de transitiviteit, want is $b \sim a$ als $a \sim b$, dan volgt uit beide $a \sim a$. Waar zit de fout?

Is in een verzameling een equivalentie gedefinieerd, dan kan men elk element met alle er aan equivalente tot een deelverzameling samenvoegen. Elk element komt dan in precies één zo'n deelverzameling te liggen, m.a.w. de verzameling valt uiteen in disjuncte deelverzamelingen, de z.g. equivalentieklassen ("klasse" is synoniem met "verzameling").

Omgekeerd definiëert elke indeling in disjuncte deelverzamelingen een equivalentie, twee elementen heten equivalent, wanneer ze in dezelfde deelverzameling liggen.

Het vormen van de equivalentieklassen brengt equivalentie van elementen terug tot gelijkheid van equivalentieklassen.

Is in een verzameling een operatie gedefinieerd, dan is het van belang, als een eventuele equivalentie "bestand is tegen" die operatie, d.w.z. dat uit $a \sim a'$ en $b \sim b'$ volgt, dat $a \circ b \sim a' \circ b'$.

Bij ringen (twee operaties) en groepen (één operatie) noemen sommige auteurs een equivalentie in dat geval een "congruentie" en de klassen "restklassen naar die congruentie".

4.4. Als voorbeeld willen we het rekenen in C_n nu op de gebruikelijke basis zetten.

Twee gehele getallen a en b heten "congruent modulo n" ($a \equiv b \pmod{n}$), als ze bij deling door n dezelfde (positieve) rest geven, of, als hun verschil deelbaar is door n. Dit is een equivalentie, de klassen bestaan uit de gehele getallen, die dezelfde rest geven, de z.g. restklassen mod n. De relatie is bestand tegen optelling en vermenigvuldiging:

Uit $a \equiv a' \pmod{n}$ en $b \equiv b' \pmod{n}$ volgt

$a+b \equiv a'+b' \pmod{n}$ en $ab \equiv a'b' \pmod{n}$.

Het is nu gebruikelijk C_n op te vatten als de verzameling van de restklassen mod n. Som en product van twee restklassen bepaalt men door uit beide een willekeurig element (een "representant") te kiezen en deze elementen bij elkaar op te tellen resp. met elkaar te vermenigvuldigen. De restklasse waarvan de uitkomst element is, is de gezochte. Het bestand zijn van de relatie tegen de bewerkingen garandeert dat elke keuze van representanten tot dezelfde restklasse voert.

In het algemeen kan bij een congruentie in de zin van 4.3, slot, met de klassen gerekend worden door middel van representanten.

5. Afbeeldingen

5.1. Laat twee verzamelingen V en W gegeven zijn. Voegt men aan elk element v van V een element w van W toe, dan zegt men dat V in W wordt afgebeeld, w heet het "beeld" van v, v het "origineel" van w. De afbeelding kan door een letter worden voorgesteld, b.v. f. In het genoemde geval schrijft men $f(v) = w$, het symbool $f(v)$ stelt dan meteen het beeld voor.

Daar elke v slechts één beeld heeft, heet de afbeelding éénduidig. Is elk beeld w slechts beeld van éénelement van V, dan éénéénduidig.

De verzameling der beelden is een deelverzameling van W. Die kan met W samenvallen, dan is elk element van W beeld, men spreekt dan van een afbeelding van V <u>op</u> W.

Is V éénéénduidig op W afgebeeld, dan kan men de toevoeging ook opvatten als ene van het origineel v aan zijn beeld w, m.a.w. er is een <u>inverse</u> afbeelding. Men schrijft in dit geval als $w = f(v)$ ook $v = f^{-1}(w)$, voorts $W = f(V)$ en $V = f^{-1}(W)$.

Belangrijk is dit afbeeldingsbegrip als W met V samenvalt. (Is V de verzameling der reële getallen, dan komt het neer op het functiebegrip van de analyse.) Men noemt een éénéénduidige afbeelding van een verzameling op zichzelf een transformatie of permutatie van die verzameling. Op dit punt heerst wel enige spraakverwarring. Sommige boeken noemen elke afbeelding een transformatie of op zijn minst een afbeelding van een verzameling in zichzelf. Voorts moet vaak worden nagegaan of in een bepaald boek de woorden transformatie en permutatie nu synoniem zijn of niet.

Wij houden ons aan de boven gegeven definitie van de transformatie en zullen met "permutatie" steeds bedoelen een "transformatie van een eindige verzameling".

5.2. Laat een verzameling V gegeven zijn en laat f en g twee afbeeldingen van V in zichzelf voorstellen. Pas nu eerst f toe, daarna g op de beeldverzameling. Het uiteindelijk resultaat is een afbeelding van V in zichzelf, die het product g f van g en f heet. Daarmee is dus een bewerking (vermenigvuldiging) gedefinieerd in de verzameling van de afbeeldingen van V in zichzelf.

Die is niet commutatief. Neem als voorbeeld:

$$V = (1,2,3);\ f : \begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases} \qquad g : \begin{cases} 1 \to 3 \\ 2 \to 3 \\ 3 \to 3 \end{cases}$$

$$\text{Dan is } gf : \begin{cases} 1 \to 3 \\ 2 \to 3 \\ 3 \to 3 \end{cases} \qquad \text{en} \quad fg : \begin{cases} 1 \to 1 \\ 2 \to 1 \\ 3 \to 1 \end{cases}$$

Ze is wel associatief en dat zullen we voor transformaties vaak gebruiken. Bewijs:

$$\{f(gh)\}(v) = f\{(gh)(v)\} = f[g\{h(v)\}]$$
$$\{(fg)h\}(v) = (fg)\{h(v)\} = f[g\{h(v)\}].$$

Men lette er op, dat het product fg uitgevoerd wordt van rechts naar links. Sommige auteurs plaatsen het afbeeldingssymbool rechts van het element (dat dan niet tussen haakjes komt) : vf. De volgende afbeelding moet daar dan weer achter: vfg, zodat hier het product fg van links naar rechts moet worden uitgevoerd.

De verzameling der genoemde afbeeldingen heeft een éénelement, namelijk de identieke, waarbij elk element op zichzelf wordt afgebeeld.

5.3. Stel dat V éénéénduidig op W wordt afgebeeld en dat in beide een bewerking is gedefinieerd (beide aan te geven door een kringetje). Nu kan het zijn, dat de bewerking bij de afbeelding "behouden blijft", d.w.z., dat $f(v_1 \circ v_2) = f(v_1) \circ f(v_2)$; kort gezegd: "het beeld van het product is het product van de beelden".

In zo'n geval heet de afbeelding een <u>isomorfie</u> (teken $V \cong W$). Het begrip is nogal elastisch, zijn er meer bewerkingen, dan wordt het geacht op alle te slaan, eventueel kan het ook het behoud van orderelaties (b.v. "groter dan") inhouden.

Isomorfe verzamelingen zijn algebraïsch gezien <u>dezelfde</u>.

Is de afbeelding van V op W slechts éénduidig en blijft de bewerking behouden, dan spreekt men van een <u>homomorfie</u> (teken $V \sim W$); een isomorfie is dus een bijzonder geval van een homomorfie.

Een isomorfe afbeelding van een verzameling op zichzelf heet een <u>automorfie</u>.

Voorbeeld van een automorfie van een integriteitsgebied:

$$a + b\sqrt{2} \longrightarrow a - b\sqrt{2} \quad \text{(a en b gehele getallen)}.$$

Een voorbeeld van een isomorfe afbeelding (één bewerking) geeft de afbeelding van de positieve getallen op de reële door middel van het logaritme nemen. Immers $\log ab = \log a + \log b$.

Een voorbeeld van een homomorfie is de afbeelding van C op C_n, waarbij de gehele getallen worden afgebeeld op de restklasse, waartoe ze behoren.

6. <u>Karakterisering van de gehele getallen</u>

6.1. Zoals reeds gezegd worden de gehele getallen door de postulaten van het integriteitsgebied niet volledig gekarakteriseerd. Ter afronding van deze inleiding willen we ze nu nog in die zin aanvullen.

In de eerste plaats ontbreken de z.g. <u>ordeningsaxioma's</u>.

<u>Def.</u>: een verzameling heet <u>geordend</u>, wanneer daarin een relatie $\prec$ is gedefinieerd, voldoend aan:

1) voor elk paar elementen a en b is òf a = b, of $a \prec b$ (spreek uit "a voor b") òf $b \prec a$. Slechts één der uitspraken geldt.

2) de relatie is transitief, d.w.z. uit $a \prec b$ en $b \prec c$ volgt $a \prec c$.

Een integriteitsgebied noemt men geordend, als bovendien:

3) uit $a \prec b$ volgt $a + c \prec b + c$ (c willekeurig),

4) uit $a \prec b$ en $0 \prec c$ volgt $ac \prec bc$.

Is $a \prec b$, dan schrijft men ook $b \succ a$ (b na a). Bij de gehele getallen komt $\leq$ in de plaats van $\prec$.

6.2. Rationale en reële getallen vormen elk ook geordende integriteitsgebieden, er moet dus nog wat bij.

Def.: een geordende verzameling heet wèlgeordend, als elke niet-lege deelverzameling een "eerste" element heeft.

In een integriteitsgebied noemen we de elementen a met $0 \prec a$ positief. Stellen we nu nog de eis:

5) de positieve elementen vormen een wèlgeordende verzameling,

dan hebben we de gehele getallen gekarakteriseerd. Dat wil zeggen, we kunnen dan bewijzen de

Stelling: Elk geordend integriteitsgebied, waarvan de positieve elementen een welgeordende verzameling vormen is isomorf met het integriteitsgebied der gehele getallen (de isomorfie slaat hier zowel op de ordening als op de beide bewerkingen).

6.3. Voor het bewijs hebben we een paar stellingen over het integriteitsgebied meer nodig, dan in 2.4 zijn afgeleid. Ze mogen hier volgen.

In elk integriteitsgebied geldt:

I. $(-a)(-b) = ab$.

Bewijs: $ab + a(-b) + (-a)(-b) = a(b-b) + (-a)(-b) = (-a)(-b)$

$ab + a(-b) + (-a)(-b) = ab + (a-a)(-b) = ab$.

II. $(-a)^2 = a^2$.

Bijzonder geval van I.

In een geordend integriteitsgebied:

III. Uit $a \prec b$ volgt $-b \prec -a$.

Bewijs: $a \prec b \rightarrow 0 \prec b-a \rightarrow -b \prec -a$.

IV. Is $a \neq 0$, dan is $0 \prec a^2$.

Bewijs: Twee gevallen: $0 \prec a$ of $a \prec 0$.

In eerste geval: $0 = 0.a \prec a.a = a^2$.

In het tweede geval volgt uit III. $0 \prec -a$, dus volgens het eerste geval $0 \prec (-a)^2$ en volgens II. $0 \prec a^2$.

V. $0 \prec 1$.

Bewijs: $0 \prec 1^2 = 1$ (IV.)

In een geordend integriteitsgebied met wèlgeordende verzameling van positieve elementen:

VI. Voor geen element a geldt $0 \prec a \prec 1$.

Bewijs: Stel de verzameling van zulke elementen a is niet leeg. Ze zijn alle positief, dus is er een eerste, stel m. Uit $0 \prec m \prec 1$ volgt $0 \prec m^2 \prec m$. Dus m is de eerste niet.

VII. Er is geen element b met $a \prec b \prec a+1$.

Bewijs: Stel wel. Dan $0 \prec b-a \prec 1$. Tegenspraak met VI.

VIII. De volgende rij bevat alle positieve elementen:

$$1,\ 1+1,\ 1+1+1,\ldots\ldots\ldots$$

Bewijs: Stel de verzameling der ontbrekende positieve elementen is niet leeg. Dan is er een eerste m. Volgens VI is $1 \prec m$. Dan $0 \prec m-1$, dus m-1 is positief en die komt wel voor. Maar dan ook $(m-1)+1=m$.

IV. We krijgen het volledige integriteitsgebied als we de rij

$$-----,-(1+1+1),-(1+1),-1,0,1,1+1,1+1+1,---$$

naar beide zijden onbeperkt voortzetten.

Bewijs: volgt uit III.

Het bewijs van de stelling uit 6.2, slot, is nu eenvoudig. Hebben we twee geordende integriteitsgebieden C_1 en C_2, elk met een welgeordende verzameling van positieve elementen, dan geeft de afbeelding $0_1 \rightarrow 0_2$ en $1_1 \rightarrow 1_2$ een afbeelding van C_1 op C_2, waarvan zo te zien is, dat ze isomorf is.

II. Groepen

1. Definitie en eenvoudige eigenschappen

1.1. Een groep is een verzameling, waarin één bewerking gedefinieerd is. Onder de "orde" van de groep verstaat men het aantal elementen, als dat eindig is, anders heet de orde "oneindig".

De bewerking heet meestal "vermenigvuldiging", maar soms ook "optelling", in elk dezer gevallen sluiten terminologie en symboliek zich daarbij aan. Men spreekt ter onderscheiding wel van "multiplicatieve" en "additieve" groepen, maar kon ze meestal beter "multiplicatie" resp. "additief geschreven" groepen noemen.

In één geval is de eerste benaming geheel correct, namelijk wanneer in een verzameling een optelling en een vermenigvuldiging gedefinieerd zijn en die verzameling t.o.v. één dier bewerkingen een groep is. In die zin vormen de gehele getallen een additieve groep en de rationale getallen $\neq 0$ een multiplicatieve.

Wij kiezen, waar dit vrijstaat, de multiplicatieve schrijfwijze.

1.2. Postulaten:

1. de bewerking is associatief.
2. de bewerking is tweezijdig omkeerbaar, d.w.z. de vergelijkingen $ax = b$ en $xa = b$ zijn oplosbaar bij willekeurige keuze van a en b.

Is de bewerking bovendien commutatief, dan heet de groep commutatief of Abels.

1.3. Eenvoudige conclusies

1.3.1. De algemene associatieve eigenschap: men kan in het product $a_1 a_2 \ldots . a_n$ willekeurig opeenvolgende factoren tussen haakjes plaatsen. Is de groep commutatief, dan kan men ze eerst ook nog een willekeurige volgorde geven.

1.3.2. Er is precies één éénelement.

Bewijs: $ax = a$ is oplosbaar, stel de oplossing e_R.

$ya = b$ is oplosbaar, laat voor de oplossing y staan.

Dan is $be_R = yae_R = ya = b$. Dus e_R is een rechteréénelement. Evenzo is er een linkeréénelement. Voorts is $e_L = e_L e_R = e_R$. We noemen het éénelement e.

1.3.3. Elk element heeft precies één inverse.
Bewijs: $ax = e$ is oplosbaar, stel de wortel a^{-1}. Evenzo zij a_L^{-1} de oplossing van $xa = e$. Nu is $a_L^{-1} = a_L^{-1}e = a_L^{-1}a\ a_R^{-1} = ea_R^{-1} = a_R^{-1}$.
We noemen de inverse a^{-1}.

1.3.4. De inverse van a^{-1} is a, dus $(a^{-1})^{-1} = a$.
Duidelijk: $aa^{-1} = a^{-1}a = e$.

1.3.5. De wortels van $ax = b$ en $ya = b$ zijn opvolgend te schrijven als $x = a^{-1}b$ en $y = ba^{-1}$, zoals door voor - resp. navermenigvuldigen met a^{-1} blijkt. Tevens volgt dat de vergelijkingen elk slechts één oplossing hebben.

1.3.6. De vereenvoudigingswet geldt, d.w.z. uit $ab = ac$ volgt $b = c$ en uit $ba = ca$ eveneens. In te zien door voor- resp. navermenigvuldiging met a^{-1}.

1.4. Andere postulaten

1.4.1. Men kan de groepbewerking op verschillende manieren karakteriseren. Een zeer bruikbaar stel postulaten is het volgende:

1. de bewerking is associatief.
2. er is minstens één linkeréénelement e.
3. bij elk element a is er minstens één element a^{-1} met $a^{-1}a = e$ (a^{-1} is dus een linksinverse bij de e van postulaat 2).

Dat deze eigenschappen uit de postulaten 1.2 volgen is in 1.3 al bewezen. Om te laten zien dat ze gelijkwaardig zijn, bewijzen we nu nog het omgekeerde.

1^o. Die linksinverse is ook rechtsinverse, want $a^{-1}(aa^{-1}) = (a^{-1}a)a^{-1} = ea^{-1} = a^{-1}$, waaruit door voorvermenigvuldigen met $(a^{-1})^{-1}$ volgt $e(aa^{-1}) = e$ of $aa^{-1} = e$.

2^o. Dat linkséénelement e is ook rechtséénelement, want $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$.

3^o. De vergelijkingen $ax = b$ en $ya = b$ hebben nu resp. de oplossing $x = a^{-1}b$ en $y = ba^{-1}$.

2. Voorbeelden van groepen

2.1. De additieve groep der gehele getallen werd in 1.1. al genoemd. Men lette op de terminologie en de schrijfwijze. De vergelijkingen van postulaat 2 worden hier $a+x=b$ en $y+a=b$. Het éénelement wordt nulelement. De inverse heet nu tegengestelde en wordt geschreven $-a$.

2.2. De rationale getallen $\neq 0$ vormen een multiplicatieve groep, zoals ook reeds in 1.1 gezegd. De deling is namelijk in deze verzameling onbeperkt uitvoerbaar.

2.3. Dat C_m een groep is t.o.v. de optelling, is licht in te zien. Ten aanzien van de vermenigvuldiging dient dat nader te worden onderzocht. Natuurlijk moet de nul alvast worden uitgesloten. Verder moet elk element $a \neq 0$ een inverse x hebben met $ax = 1$, d.w.z. $ax \equiv 1 \pmod m$, d.w.z. er moet een geheel getal y zijn met $ax + my = 1$. Dat betekent dat de ggd (a,m) van a en m gelijk 1 is. Is omgekeerd die ggd = 1 dan zijn er gehele getallen x en y met $ax + my = 1$, zodat a dan de gewenste inverse heeft. Er volgt: de resten $a \neq 0$ van C_m, waarvoor (a,m) = 1, vormen een multiplicatieve groep. Is m priem, dan zijn dat alle resten $\neq 0$. Gebruikt zijn de postulaten 1.4.

Dat de zoeven genoemde gehele getallen x en y bestaan is een bekende stelling uit de rekenkunde. De waarheid daarvan ziet men het gemakkelijkst in door de ggd van a en m met de algorithme van Euclides te bepalen.

Luidt de eerste deling $a/\ m \setminus q$,
$\underline{q,a}$
r_1 , dan volgt $r_1 = m-q,a.$

Uit de tweede deling $r_1/\ a \setminus q_2$
$\underline{q_2 r_1}$
r_2 volgt dan weer $r_2 = a-q_2 r_1 =$

$a - q_2(m-q,a) = (1+q_2q_1)a - q_2m$. Elke volgende rest kan zo teruggebracht worden tot een uitdrukking xa + ym met gehele x en y, in het bijzonder de laatste, n.1. de ggd.

2.4. Als voorbeeld nemen we C_{12}, de multiplicatieve groep is (1,5,7,11). De groeptabel ziet er als volgt uit:

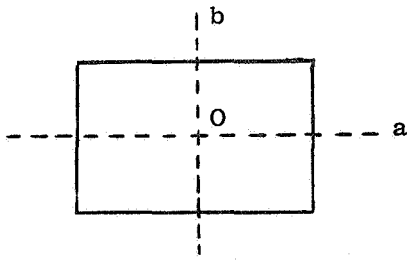
1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

Opmerkingen: 1) De "omranding" links en boven (verg.I,3.3) is hier weggelaten.

2) In een groeptabel komen noch in een kolom, noch in een rij ooit twee gelijke elementen voor.

3) De groep is commutatief, dus is de tabel symmetrisch om de hoofddiagonaal.

2.5. De "dekafbeeldingen" van een rechthoek vormen een groep. "Dekafbeeldingen" van een figuur zijn draaiïngen of wentelingen (we nemen ze in de ruimte), waardoor die figuur met zichzelf tot samenvallen wordt gebracht. Steeds wordt de "identieke" dekafbeelding meegerekend: we laten de figuur staan, zoals ze staat.



Voor de rechthoek komen daar nog bij: wentelingen over 180^o om de assen a en b en een draaiïng van 180^o om de as c door O loodrecht op het vlak van tekening. Het na elkaar uitvoeren van twee dekafbeeldingen betekent ook een dekafbeelding, het "product" van de eerste twee (van recht naar links uitvoeren). Daar we voor de rechthoek alle mogelijkheden hebben opgesomd, vormen de vier genoemde een groep. Noemen we ze in de volgorde van opsomming e,a,b,c, dan wordt de tabel:

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Uit de tabel blijkt, dat deze groep isomorf is met die van 2.4, we kunnen afbeelden: e $\longrightarrow$1, a $\longrightarrow$5, b $\longrightarrow$7, c $\longrightarrow$11. Ook had gekund: e $\longrightarrow$1, a $\longrightarrow$11, b $\longrightarrow$7, c $\longrightarrow$5.

Dat impliceert een <u>automorfie</u> van de eerste groep (ook van de tweede), nl. 1 $\longleftrightarrow$ 1, 5 $\longleftrightarrow$ 11, 7 $\longleftrightarrow$ 7, 11 $\longleftrightarrow$ 5.

In het geheel heeft die 6 van zulke automorfieën (de identieke meegeteld).

2.6. We kunnen de tabel van 2.5 opvatten als tabel van een abstracte groep. Die heet de "Vierergruppe" van Klein, in het Nederlands spreekt men tegenwoordig ook van "viergroep". Aanduiding V_4. De groepen van 2.4 en 2.5 zijn dus interpretaties van V_4 en daarmee isomorf. Een andere interpretatie krijgt men door voor de vierfuncties (b.v. gedefiniëerd gedacht op de verzameling der rationale getallen $\neq 0$) $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$ als product $(f_i f_k)(x)$ te beschouwen $f_i\{f_k(x)\}$.

Tabel (alleen in indices):

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

2.7. De transformaties van een verzameling vormen een groep. Het begrip werd ingevoerd in I 5.1, de associativiteit werd bewezen in I 5.2. De rest spreekt vanzelf. De identieke transformatie is éénelement en verder hoort bij elke transformatie een inverse.

3. Ondergroepen

3.1. Wanneer een deelverzameling van een groep t.o.v. de groepbewerking zelf een groep is, heet ze een ondergroep van die groep. Kenmerkend voor een ondergroep is:

a) de deelverzameling is gesloten voor de groepbewerking, d.w.z. ze bevat met twee elementen ook hun producten.
b) de deelverzameling bevat met elk element ook zijn inverse (dus ook het éénelement van de groep).

Toegepast zijn de groeppostulaten van 1.4.

3.4. Voorbeelden van ondergroepen:

De even getallen vormen een ondergroep van de additieve groep der gehele getallen. Evenzo de m-vouden (m willekeurig geheel).

C_m is niet een ondergroep van C, C_m heeft een andere bewerking. In de multiplicatieve groep (1,5,7,11) van C_{12} (zie 2.4) zijn (1.5), (1.7) en (1.11) ondergroepen.
Triviale ondergroepen zijn het éénelement en de groep zelf.

3.3. Nevenklassen

3.3.1. Gegeven zij de groep G met ondergroep H. Laat a een willekeurig element van G zijn. We vormen nu alle producten ha met $h \in H$, hun verzameling geven we aan met Ha. Ze heet een rechternevenklasse van H.

De elementen van Ha zijn alle verschillend. Is a geen element van H, dan zijn de elementen van Ha ook verschillend van elk element van H, want zou $h_1 a = h_2$ zijn, dan zou volgen $a = h_1^{-1} h_2 \in H$.

Als $a \in H$, dan is $Ha = H$. (Duidelijk geldt $Ha \subset H$. Daar elke vergelijking $xa = h$ binnen H op te lossen is, volgt ook $H \subset Ha$).

Als $b \in Ha$, is $Hb = Ha$. We kunnen immers stellen $b = ha$ met $h \in H$, dus $Hb = Hha = Ha$.

3.3.2. Neem a in G buiten H en vorm Ha. Is er nog een element b van G buiten H en buiten Ha, vorm dan Hb. Gaan we zo door, dan blijkt G uiteen te vallen in disjuncte rechternevenklassen van H (H zelf meegeteld). Elk element van G ligt in één dier nevenklassen, g in Hg, want $e \in H$ en $eg = g$.

Elke nevenklasse is éénéénduidig op elke andere af te beelden, Ha op Hb via $ha \longrightarrow he$, $h \in H$. Is H eindig dan hebben dus alle nevenklassen evenveel elementen als H.

Is G eindig, dan H ook en de orde van H is deelbaar op die van G. Hun quotiënt heet de <u>index</u> van H in G. Hij geeft blijkbaar het aantal nevenklassen aan.

Heeft H oneindig veel rechternevenklassen, dan geeft men H de index oneindig.

3.3.3. Al het bovenstaande kan worden herhaald voor de <u>linkernevenklassen</u> van H. In een Abelse groep is $Ha = aH$, elke rechternevenklasse is meteen linkernevenklasse en men kan het onderscheidend voorvoegsel laten vervallen. In het algemeen behoeft een linkernevenklasse niet ook tegelijk rechternevenklasse te zijn.

3.4. <u>Voorbeelden</u>

3.4.1. De even getallen vormen een ondergroep van de additieve groep der gehele getallen (3.2). De nevenklassen schrijven we hier als H+a; is a even, dan is dit H zelf, is a oneven, dan komt er de verzameling der oneven getallen. De index van H is dus 2.

3.4.2. De m-vouden vormden evenzo een ondergroep van de additieve groep der gehele getallen (m willekeurig natuurlijk). De nevenklassen zijn

$$H,\ H+1,\ H+2,\ldots\ldots,H+(m-1),$$

dat zijn dus de restklassen modulo m. De index is m.

3.4.3. Neem voor G de multiplicatieve groep der positieve rationale getallen, voor H de verzameling der getallen 2^m met willekeurige gehele m. Hier is de index oneindig. De restklassen krijgt men door H te vermenigvuldigen met een product van priemmachten $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, n natuurlijk, p's verschillend $\neq 2$, α's geheel. Verschillende producten leveren verschillende restklassen.

3.4.4. De viergroep (e,a,b,c) heeft de ondergroepen (e,a),(e,b) en (e,c). Nevenklasse van (e,a) is (b,c) enz.

3.5.5. De ondergroep (e) van G heeft de elementen van G tot nevenklassen. G heeft, als ondergroep beschouwd, alleen zichzelf tot nevenklasse.

4. Permutatiegroepen

4.1. Volgens de afspraak in I, 5.1 verstaan we onder een permutatie een transformatie van een eindige verzameling. Vroeger (misschien nog) bedoelde men er een volgorde mee, waarin de elementen van die verzameling zich lieten plaatsen. Waren er n elementen, dan bedroeg het aantal permutaties n!

Hier is dus de permutatie een afbeelding, het begrip is trouwens nauw aan het vroegere verwant.

Noemen we de x dingen 1,2,...,n dan kunnen we een permutatie voorstellen als

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$, de a's stellen de n elementen in

andere volgorde voor, b.v. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. Bedoeld wordt nu de afbeelding $1 \longrightarrow 2$, $2 \longrightarrow 4$, $3 \longrightarrow 1$, $4 \longrightarrow 3$.

De eerste regel kan ook anders geschreven worden:

$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ stelt uiteraard dezelfde permutatie voor.

Wil men alle permutaties opschrijven en houdt men bij alle de eerste regel gelijk, dan geven de tweede regels alle permutaties in de oude zin. Het aantal permutaties is dus ook hier n!

Dat de volgorde van de bovenste regel willekeurig is, is handig bij het vermenigvuldigen (d.w.z. na elkaar uitvoeren van rechts naar links).

Voorbeeld:

$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} =$$

$$\begin{pmatrix}1&2&4&3\\4&1&3&2\end{pmatrix}\begin{pmatrix}3&1&2&4\\1&2&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

De permutaties van een verzameling van n elementen vormen een groep (bewijs in 2.7). Die heet de symmetrische groep S_n. De naam is ontleend aan de symmetrische functies in n variabelen, die bij een permutatie der variabelen invariant is.

4.2. Van n=3 af zijn de symmetrische groepen niet-commutatief. Voor S_3 volgt dit uit het voorbeeld

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} .$$

Is $n > 3$, dan is S_3 isomorf met een ondergroep van S_n, neem daarvoor maar die permutaties van S_n, die de eerste n-3 elementen van de verzameling op zichzelf afbeelden. Maar als een ondergroep niet commutatief is, dan de groep zelf evenmin.

4.3. Stelling van Cayley: Een groep van orde n is isomorf met een ondergroep van S_n.

Het bewijs wordt geleverd door de beeldpermutaties aan te geven. Laat de groep G de elementen $a_1, a_2, \ldots, a_n$ hebben. Is b er één van dan vormen de producten $ba_1, ba_2, \ldots, ba_n$ de groep G weer. De afbeelding $a_i \longrightarrow ba_i$ is dus een permutatie B van G. Verschillende b's geven verschillende B's, want uit $ba_i = b'a_i$ volgt b=b'.

De gezochte afbeelding luidt nu $b \longrightarrow B$. Die is alvast éénéénduidig. Wat de isomorfie betreft, merken we op:

$$b \longrightarrow \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ba_1 & ba_2 & \cdots & ba_n \end{pmatrix}$$

$$c \longrightarrow \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ca_1 & ca_2 & \cdots & ca_n \end{pmatrix} \quad \text{en}$$

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ba_1 & ba_2 & & ba_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ca_1 & ca_2 & \cdots & ca_n \end{pmatrix} =$$

$$\begin{pmatrix} ca_1 & ca_2 & \cdots & ca_n \\ bca_1 & bca_2 & \cdots & bca_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ca_1 & ca_2 & \cdots & ca_n \end{pmatrix} =$$

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ bca_1 & bca_2 & \cdots & bca_n \end{pmatrix}$$, dat is het beeld van bc.

4.4. Voorbeeld:

Volgens de stelling van Cayley is V_4 isomorf met een ondergroep van S_4. De in het bewijs gebruikte afbeelding luidt:

$$e \longrightarrow \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} \qquad e \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$a \longrightarrow \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} \quad \text{of} \quad a \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$b \longrightarrow \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} \qquad b \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$c \longrightarrow \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} \qquad c \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

4.5. Meestal schrijft men permutaties als producten van "cykels". Met de "cykel" (2,7,5,4) wordt de permutatie bedoeld, die 2 op 7 afbeeldt, 7 op 5, 5 op 4 en 4 op 2. Hij is dus ook te schrijven als (7,5,4,2),(5,4,2,7) of (4,2,7,5). Gaat het over b.v. 8 elementen dan stellen ze alle de permutatie

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 3 & 2 & 4 & 6 & 5 & 8 \end{pmatrix}$$

voor. Omgekeerd merken we in de permutatie

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 5 & 6 & 7 & 2 & 3 \end{pmatrix}$$

de cykels (1,4,5,6,7,2) en (3,8) op. De gegeven permutatie wordt verkregen door de cykels los van elkaar uit te voeren, de permutatie is dus hun product en in dat product zijn ze verwisselbaar. Steeds

zijn cykels verwisselbaar als ze geen element gemeen hebben. Hebben ze dat wel, dan zal in het algemeen de volgorde verschil maken.

Ter oefening rekene men het volgende product na:

$$(1,3,5,6,8)(2,1,4,5)(7,3)(5,8,4,2) = (1,4,3,7,5)(2)(6,8).$$

Bij het vermenigvuldigen trad een cykel (2) op met één element. Blijkbaar verandert die niets en kon hij worden weggelaten. Elke cykel met één element stelt de identiteit voor, is het gewenst die te schrijven, omdat er anders niets zou blijven staan, dan kiest men meestal (1).

4.6. Men onderscheidt de elementen van S_n in <u>even</u> en <u>oneven</u> permutaties. Ter definitie beschouwen we het product

$$\prod_{\substack{i=1,2,\ldots,n-1 \\ j=1,2,\ldots,n \\ i<j}} (x_i - x_j)$$

We passen een zekere permutatie toe op de indices van de x-en, "afbeelden op" betekene hier "vervangen door". Het product kan daarbij gelijk blijven, het kan ook in zijn tegengestelde overgaan. Beide komt voor: de identieke permutatie laat het gelijk, de permutatie (1,2) maakt het tegengesteld. Blijft het gelijk, dan heet de permutatie even, wordt het tegengesteld, dan oneven. Voor het product van twee permutaties gelden kennelijk de regels:

even x even = oneven x oneven = even en
even x oneven = oneven x even = oneven.

Een ondergroep van S_n kan uit uitsluitend even permutaties bestaan. Voorbeelden zijn de identieke permutatie als ondergroep beschouwd en de deelverzameling van alle even permutaties in S_n (diet heet de alternerende groep A_n).

Bevat een ondergroep van S_n een oneven permutatie en vermenigvuldigen we alle elementen van die ondergroep daarmee, dan leveren alle oneven permutaties een even product en alle even permutaties een oneven product. Daar deverzameling der producten de ondergroep zelf is, bevat die evenveel even als oneven permutaties. Dit geldt in het bijzonder voor S_n zelf, de alternerende groep A_n heeft bijgevolg de orde $\frac{1}{2}n!$ en de index 2. De enige nevenklasse $\neq A_n$ bestaat uit de oneven permutaties.

5. Voortbrenging van groepen

5.1. Is a element van een groep, dan ligt het voor de hand het gedurig product a.a.....a (n factoren) voor te stellen door a^n. Natuurlijk sluiten daarbij aan de definities $a^1=a$ en $a^0=e$. (Voor additief geschreven groepen wordt dit resp. na, 1a, 0a).

De exponent -1 was al gebruikt om de inverse van een element aan te geven. Maar kennelijk is voor $n \geq 1$ $a^{-1}.a^n = a^n.a^{-1}=a^{n-1},a^{-1}$ gedraagt zich dus wel als een macht. Verder is $(a^n)^{-1} = (a^{-1})^n$, want $(a^{-1})^n.a^n = (a^{-1}.a)^n=e^n=e$. We definiëren daarom

$$a^{-n} = (a^n)^{-1} \text{ of } = (a^{-1})^n.$$

Daarmee zijn de gehele machten van a gedefinieerd. De bewijzen van de bekende eigenschappen zijn zo uit een schoolboek over te nemen.

5.2. Cyclische groepen

De machten van a vormen een (onder-)groep; daar ze verwisselbaar zijn, is die groep Abels. Zo'n groep heet cyclisch, men zegt, dat a de groep voortbrengt.

Zijn de machten van a alle verschillend, dan is de door a voortgebrachte groep oneindig. Het rekenen met de elementen gebeurt eigenlijk met de exponenten: $a^p.a^q = a^{p+q}$.

De afbeelding $a^p \longleftrightarrow p$ op de additieve groep der gehele getallen ligt voor de hand, ze is een isomorfie. Bijgevolg zijn alle oneindige cyclische groepen isomorf, abstract gezien is er dus maar één.

De additieve groep der gehele getallen wordt voortgebracht door het getal 1.

Stel nu, dat er onder de machten van a gelijke voorkomen, laat b.v. $a^p = a^q$ zijn, met $p \neq q$. Er volgt dat $a^{p-q} = e$. Er zijn dus gehele getallen n met $a^n = e$. Daar dan ook $a^{-n} = e$, kan men n positief veronderstellen. Bijgevolg is er een kleinste positief getal m, met de eigenschap dat $a^m = e$. Voor willekeurige gehele q volgt dat $a^{qm}=(a^m)^q=e$.

Omgekeerd: is $a^n = e$, dan is n deelbaar door m. Stel maar $n=qm+r$ met $0 \leq r < m$. Dan is $r = n-qm$ en $a^r = a^n.a^{-qm} = e.e = e$. Maar m was het kleinste positieve getal met die eigenschap, dus is r=0.

Blijkbaar bestaat de groep uit m verschillende elementen, waarvoor we $e,a,a^2,\ldots,a^{m-1}$ kunnen nemen, voortzetting naar beide kanten leidt tot cyclische herhaling. Ditmaal is de isomorfie met de additieve groep van C_m gemakkelijk vast te stellen, er volgt weer, dat er maar één cyclische groep is met orde m.

5.3. Is a element van een groep G, dan is a voortbrengende van een cyclische ondergroep. De orde van die ondergroep heet ook de orde van a. Heeft G eindige orde, dan a ook; de orde van a is een deler van de orde van G (3.3.2).

Is de orde van G een priemgetal, dan is G cyclisch en wordt voortgebracht door elk zijner elementen $\neq e$.

5.4. Zijn $a_1,a_2,\ldots,a_n$ elementen van een groep G en vormt men alle mogelijke gedurige producten van machten van deze elementen, dan is de verzameling van deze producten een ondergroep van G, de elementen $a_1,a_2,\ldots,a_n$ heten een "stel voortbrengenden" van die ondergroep. Die ondergroep kan G zelf zijn, voor elke groep is trouwens onder zijn elementen een stel voortbrengenden aan te geven, men kan er immers de groep zelf voor nemen.

Het kan echter vaak met minder. Zo vormt de rij getallen $1,\frac{1}{2!},\frac{1}{3!},\ldots,\frac{1}{n!},\ldots$ een stel voortbrengenden van de additieve groep der rationale getallen. Neem maar een breuk $\frac{t}{n}=\frac{(n-1)!t}{n!}$, hij kan door $\frac{1}{n!}$ alleen al worden voortgebracht. Blijkbaar kunnen we een willekeurig aantal getallen uit de rij weglaten, komt b.v. $\frac{1}{n!}$ niet voor, maar $\frac{1}{(n+p)!}$ wel, dan brengt die $\frac{t}{n}=\frac{(n-1)!(m+1)(n+2)\ldots(n+p)t}{(n+p)!}$ wel voort. Maar er moeten we oneindig veel blijven staan, anders is de breuk $\frac{1}{p}$ met p priem $>$ de grootste n niet te maken.

5.5. In het voorgaande werd steeds verondersteld, dat een voortbrengende a al element van een groep was. Dat is niet nodig, men kan van lege symbolen als a,b, enz. formeel de machten en daarvan formeel de gedurige producten opschrijven en construeert dan zo een abstracte groep. Worden geen beperkende voorwaarden gesteld, dan is dat uiteraard een oneindige.

Wij willen op die manier alle abstracte groepen opsporen van de orden 1 tot en met 6.

Voor 1 is dat gauw gebeurt, we vinden maar één groep, alleen bestaande uit een éénelement e.

De orden 2,3 en 5 zijn priem, de gezochte groepen zijn dus cyclisch en uniek. Ze kunnen resp. worden voorgesteld als (e,a)(met $a^2=e$); (e,a,a^2)(met $a^3=e$) en (e,a,a^2,a^3,a^4) (met $a^5=e$).

Blijven de orden 4 en 6.

Orde 4

Is er een element a van orde 4, dan is de groep cyclisch en heeft hij de elementen e,a,a^2,a^3. ($a^4 = e$ gesteld).

Zijn er geen elementen van orde 4, dan hebben ze alle (op e na) orde 2, stel de elementen e,a,b,c. Daar $ab \neq e, \neq a, \neq b$, is ab = c, evenzo ba = c. Evenzo volgt bc = cb = a, ac = ca = b. De structuur is die van de viergroep V_4 (2.6).

Er zijn dus maar twee groepen van orde 4.

Orde 6

Ten eerste is er de cyclische groep van orde 6. Is een groep van orde 6 niet cyclisch, dan is er geen element van orde 6 en dan hebben de elementen $\neq$ e orden 2 of 3.

Een element van orde 3 heeft een inverse van dezelfde orde en vormt daarmee een paar verschillende elementen. Het aantal elementen van orde 3 is dus even en daar er 5 elementen $\neq$ e zijn, volgt het bestaan van tenminste één element van orde 2.

Zouden alle vijf elementen de orde 2 hebben, kies er dan twee van, a en b, en stel ab=c. Dan is c^2 = abab = e = aabb, waaruit volgt ab=ba. Verder ac = aab = b en bc = bba = a.

Kennelijk vormen e,a,b,c een ondergroep ($\cong V_4$) en daar 4 geen deler is van 6, is dat onmogelijk. Er is dus ook minstens één element van orde 3.

We gaan nu uit van elementen e,a (orde 3) en p (orde 2). De verzameling (e,a,a^2) is een cyclische ondergroep, een linker- en rechternevenklasse daarvan zijn resp. (p,pa,pa^2) en (p,ap,a^2p). (3.3)

Daar (e,a,a^2) de index 2 heeft vallen die nevenklassen samen zodat pa = ap òf $pa = a^2p$. Stel dat pa = ap, schrijf dan de machten van ap op:

$$(ap)^1 = ap;\ (ap)^2 = a^2;\ (ap)^3 = p;\ (ap)^4 = a;\ (ap)^5 = a^2p;\ (ap)^6 = e.$$

De uitkomsten zijn alle verschillend en vormen dus de hele groep, voortgebracht door ap en dus cyclisch, in tegenspraak met de beginveronderstelling. Er volgt dat $pa = a^2p$ en $ap = pa^2$.

Stellen we ap = q en pa = r, dan wordt q^2 = apap = a^3p^2 = e en evenzo r^2=e. Stellen we nog a^2 = b, dan komen we tot de zes elementen e,a,b,p,q,r, alle dwingend geconstrueerd.

De tabel ziet er als volgt uit:

e	a	b	p	q	r
a	b	e	q	r	p
b	e	a	r	p	q
p	r	q	e	b	a
q	p	r	a	e	b
r	q	p	b	a	e

De groep S_3 heeft de orde 3! = 6 en is niet commutatief (4.2), dus niet cyclisch. Hij is dus isomorf met de pas geconstrueerde abstracte groep. Om bovenstaande tabel te doen gelden, kan men stellen (1,2,3) = a, (1,3,2) = b, (1,2) = p, (1,3) = q, (2,3) = r. Tenslotte: er zijn dus ook maar twee abstracte groepen van orde 6.

6. Normaaldelers

6.1. Een ondergroep van een groep heet een normaaldeler van die groep, wanneer elke linkernevenklasse ook rechternevenklasse is.

Noemen we de groep G, de ondergroep H en is g een willekeurig element van G, dan zal dus Hg moeten samenvallen met gH. Dat wil zeggen $g^{-1}Hg \subset H$ en $gHg^{-1} \subset H$ beide voor willekeurige g. Maar daar G met elk element ook de inverse daarvan bevat, komen deze twee eisen op hetzelfde neer en kunnen we met b.v. de eerste volstaan.

Die komt er op neer dat $g^{-1}hg \in H$, voor willekeurige $g \in G$ en willekeurige $h \in H$. Dat is een veelgebruikt kenmerk bij het bewijs, dat een ondergroep normaaldeler is.

Het spreekt overigens wel vanzelf, dat in een Abelse groep elke ondergroep normaaldeler is. Verder is een ondergroep met index 2 steeds normaaldeler, hij heeft immers slechts één (van hemzelf verschillende) nevenklasse, die dus tegelijk rechter-en linkernevenklasse is. Zo is A_n normaaldeler van S_n (4.6).

6.2. Het belang van de normaaldeler ligt daarin, dat men met de nevenklassen rekenen kan, door dat met representanten te doen.

In het algemeen verstaat men onder het product HK van twee deelverzamelingen H en K van een groep de verzameling van alle producten hk met $h \in H$ en $k \in K$. Is nu N een normaaldeler en zijn a en b twee willekeurige elementen van de groep, dan is de bewering:

$$Na \cdot Nb = Nab.$$

Dat wil dus zeggen: het product van een willekeurig element van Na en een willekeurig element van Nb ligt in Nab en omgekeerd is elk element van Nab als zo'n product te krijgen.

Het laatste is gemakkelijk in te zien, men schrijve b.v. nab=na.eb. Wat het eerste betreft: stel $a' \in Na$ en $b' \in Nb$, te bewijzen is dan, dat $a'b' \in Nab$.

Er zijn elementen n_1 en n_2 van N, zodanig dat $a'=n_1a$ en $b'=n_2b$, dus is $a'b' = n_1an_2b$.

Nu hoort an_2 tot aN, dus tot Na; er is dus een $n_3 \in N$ met $an_2=n_3a$. Daaruit volgt $a'b' = n_1n_3ab \in Nab$.

6.3. Men kan vragen of het <u>noodzakelijk</u> is dat de ondergroep H van de groep G normaaldeler is, opdat men met b.v. de rechternevenklassen zo kan rekenen. Het antwoord luidt bevestigend. Stel maar Ha.Hb=Hab. Dan is er bij elk element h van H een element h_1 te vinden met $ea.hb=h_1ab$, dus $ah=h_1a$. Daaruit volgt $aH \subset Ha$. Ga nu uit van $Ha^{-1}.Hab = Hb$, dan is er bij elk element h van H een element h_2 met $ea^{-1}.hab = h_2b_1$ dus $ha=ah_2$. Daaruit volgt $Ha \subset aH$. Combinatie levert aH = Ha en H is normaaldeler.

6.4. <u>Congruenties</u>

Het behoren tot b.v. dezelfde rechternevenklasse van een ondergroep H is een equivalentie in de groep, immers elke indeling in disjuncte nevenklassen creëert er een (I,4.3). Hier is $a \sim b$, als $ab^{-1} \in H$, want dan $a \in Hb$ (bij de additieve schrijfwijze luidt het kenmerk $a-b \in H$). In 6.2 en 6.3 hebben we bewezen: deze relatie is een <u>congruentie</u> (d.w.z., dat de relatie bestand is tegen de bewerking; zie I, 4.3) dan en alleen dan, als de ondergroep een normaaldeler is.

We bewijzen nog:

Bij elke congruentie in een groep is een normaaldeler aan te wijzen, zodanig, dat de nevenklassen van die normaaldeler samenvallen met de restklassen naar die congruentie.

Als dit waar is, dan moet de ndormaaldeler die restklasse zijn, die het éénelement e bevat, hij is dus de verzameling der groepelementen $\equiv e$. Noem die verzameling N. We bewijzen:

1^o. N is ondergroep (kenmerken in 3.1)

a) N is gesloten voor de bewerking, want uit $n_1 \equiv e$ en $n_2 \equiv e$ volgt $n_1 n_2 \equiv ee = e$, dus $n_1 n_2 \in N$.

b) Met n ligt ook n^{-1} in N, want uit $n \equiv e$ en $n^{-1} \equiv n^{-1}$ volgt $nn^{-1} \equiv en^{-1}$, dus $e \equiv n^{-1}$ of $n^{-1} \in N$.

2^o. N is normaaldeler (kenmerk in 6.1), want is g een willekeurig groepelement en n een willekeurig element van N, dan is $g^{-1}ng \equiv g^{-1}eg = g^{-1}g = e$, dus $g^{-1}ng \in N$.

3^o. Is nu $a \equiv b$, dan is $ab^{-1} \equiv bb^{-1} = e$, dus $ab^{-1} \in N$, of $a \in Nb$, a en b liggen dus in dezelfde nevenklasse van N. Omgekeerd volgt uit $ab^{-1} \in N$ dat $ab^{-1} \equiv e$, dus $ab^{-1}b \equiv eb$ of $a \equiv b$. Congruentieklassen en nevenklassen vallen dus samen.

6.5. Factorgroep

6.5.1. In 6.2 werd de bewerking van de groep G overgedragen op de verzameling van de nevenklassen van een normaaldeler N. Uit de betrekking Na.Nb = Nab bleek dat het product van twee nevenklassen weer een nevenklasse is, m.a.w., de verzameling is gesloten voor de bewerking. We bewijzen nu, dat de nevenklassen een groep vormen, deze groep heet de factorgroep van G naar N en wordt geschreven G/N. Bij het bewijs passen we het kenmerk van 1.4 toe.

1. De associativiteit geldt, omdat met representanten, dus met elementen van G gerekend wordt.
2. (Linker-)éénelement is N zelf, want N, Na=Ne.Na=N.ea=Na.
3. (Linker-)inverse van Na is Na^{-1}, want Na^{-1}, $Na=Na^{-1}a=Ne=N$.

6.5.2. Omdat met representanten gerekend wordt, ligt het voor de hand G op G/N af te beelden volgens $a \longrightarrow Na$. Bij die afbeelding blijft duidelijk de bewerking behouden, ze is dus een homomorfie (I, 5.3). N heet de kern van de homomorfie.

6.5.3. Omgekeerd hoort bij elke homomorfe afbeelding van G een normaaldeler. Preciezer:

Stelling: Is G homomorf af te beelden op G', dan vormen de elementen van G, die het éénelement e' van G' tot beeld hebben een normaaldeler N van G. De deelverzamelingen van G, waarvan de elementen eenzelfde beeld in G' hebben, zijn de nevenklassen van N en de factorgroep G/N is isomorf met G'. (Ook hier heet N de kern van de homomorfie $G \sim G'$).

Bewijs: De afbeelding $gG \longrightarrow G'$ brengt een klassenindeling van G mee, de klassen bestaan telkens uit de originelen in G van eenzelfde beeld in G'. Deze klassenindeling definiëert een equivalentie in G, die zelfs een congruentie is, omdat de afbeelding homomorf is, de bewerking dus behouden blijft. Maar dan komt de klassenindeling neer op de indeling in nevenklassen naar een normaaldeler N (6.4). N's nevenklassen zijn dus de verzamelingen van elementen van G met eenzelfde beeld in G', in het bijzonder worden de elementen van N zelf afgebeeld op e'.

De gestelde isomorfie volgt direct uit de afbeelding $Na \longrightarrow a'$ (als a' het beeld van a is).

Omdat elk element van Na het beeld a' heeft, is de afbeelding $Na \longrightarrow a'$ eenduidig. Omdat elk origineel van a' in Na ligt, is ze éénéénduidig. Elk element van G' is beeld in de homomorfie, dus ook in deze afbeelding, dus is die een afbeelding op G'. Tenslotte volgt uit Na.Nb= Nab, dat ze isomorf is.

Onze slotsom is, dat bij alle homomorfe afbeeldingen van een groep G, waarbij de kern N dezelfde is, de beeldgroepen isomorf zijn met de factorgroep G/N, en dus ook onderling.

6.5.4. Het bewijs van de stelling in 6.5.3. bestond (tot het bewijs der isomorfie) uit een gevolgtrekking uit de stelling van 6.4. Het verdient aanbeveling de stelling uit dat verband los te maken en dit deel ad hoc te bewijzen. Veel moeite zal dat niet kosten, het komt er op neer, dat men het bewijs van 6.4 overdoet, maar overal voor het congruent zijn van twee elementen van G het "het-zelfde-beeld-in G'-hebben" substitueert.

6.5.5. Als voorbeeld nemen we voor G de additieve groep der gehele getallen. De afbeelding op de groep (e,a) van orde 2 (zie 5.5), waarbij de even getallen op e worden afgebeeld en de oneven op a, is kennelijk een homomorfie. De even getallen vormen de kern N, de onevene de (enige) andere nevenklasse. Stel A. Dat de groep (N,A) isomorf is met de groep

(e,a) is zeer doorzichtig. De homomorfie is blijkbaar dáárdoor tot een isomorfie gereduceerd, dat alle originelen van hetzelfde beeld tot één origineel zijn samengevat. Dat kan, omdat men met de nieuwe originelen door middel van hun representanten rekenen kan.

Is m een willekeurig natuurlijk getal, dan is de (door m voortgebrachte) groep $\{m\}$ der m-vouden een normaaldeler van de additieve groep C der gehele getallen. De nevenklassen zijn de restklassen modulo m, dus is $C/\{m\} = C_m$ en $C \sim C_m$. Bij deze homomorfie wordt weer elk element van C afgebeeld op de restklasse, waartoe het behoort.

Analoog aan het eerste voorbeeld kan de groep S_n op de groep (e,a) worden afgebeeld door de even permutaties het beeld e te geven en de onevene het beeld a. Normaaldeler is hier de alternerende groep A_n. Er volgt $S_n/A_n \cong (e,a)$.

7. Automorfieën

7.1. Het centrum van een groep

Het niet-commutatief zijn van een groep G geeft aanleiding tot interessante onderzoekingen, naar de "mate van verwisselbaarheid", die althans nog aanwezig is. Zo kan men vragen: zijn er elementen a en b verwisselbaar, d.w.z. dat ab=ba? Of: zijn er elementen, die met een bepaald element verwisselbaar zijn? Hier willen we zoeken naar de elementen, die met alle elementen van de groep verwisselbaar zijn. Hun verzameling is niet leeg, want het éénelement behoort ertoe. Ze heet het centrum Z van de groep. Dit centrum is een normaaldeler.

Bewijs:

1^o. Z is ondergroep (kenmerken in 3.1).

a) Stel z_1 en $z_2 \in Z$. Neem een willekeurig element g van G. Dan is $z_1z_2g = z_1gz_2 = gz_1z_2$, dus $z_1z_2 \in Z$.

b) Uit $gz = zg$ volgt $z^{-1}g = gz^{-1}$, dus $z^{-1} \in Z$, als $z \in Z$.

2^o. Z is normaaldeler.

Duidelijk: $gZ = Zg$.

7.2. Transformatie van groepelementen

Als a en b niet verwisselbaar zijn, dan kunnen we vragen naar het element x met $ab = bx$. Het is $x = b^{-1}ab$. Men zegt: x is uit a ontstaan door "transformatie met b', a en x heten "geconjugeerd".

In het algemeen heten twee elementen p en q geconjugeerd als er een element g aan te wijzen is, zodanig dat $p = g^{-1}qg$.

Dit geconjugeerd zijn is een equivalentie want het is

1^o. reflexief, immers $p = e^{-1}pe$;

2^o. symmetrisch, want als $p = g^{-1}qg$, dan is $q = (g^{-1})^{-1}pg^{-1}$;

3^o. transitief, want uit $p = g^{-1}qg$ en $q = h^{-1}rh$ volgt $p = g^{-1}h^{-1}r\ hg = (hg)^{-1}r(hg)$.

De groep valt dus uiteen in disjuncte deelverzamelingen van geconjugeerde elementen, de "conjugatieklassen".

7.3. Verband met normaaldelers

Stel, N is normaaldeler van de groep G. Als $n \in N$, $g \in G$ en $ag = gx$, dan is ook x element van N. Want $gx = ng \in Ng = gN$. We kwamen in 6.1 trouwens $g^{-1}ng \in N$ al tegen als kenmerk van N als normaaldeler onder de ondergroepen.

Blijkbaar bevat N met elk zijner elementen ook alle geconjugeerden daarvan, m.a.w. N is de vereniging van een aantal conjugatieklassen.

7.4. Inwendige automorfieën

Transformeert men elk element van een groep G met hetzelfde groepelement g, dan wordt door $x \longrightarrow g^{-1}xg$ de groep uiteraard in zichzelf afgebeeld. We bewijzen dat deze afbeelding een transformatie is en wel een isomorfe dus een automorfie (zie I,5.3).

1^o. Uit $g^{-1}ag = g^{-1}bg$ volgt $a = b$, de afbeelding g is dus éénéénduidig.

2^o. Is b een willekeurig element van G en stellen we $gbg^{-1} = a$, dan is $b = g^{-1}ag$, b is dus beeld en G is op zichzelf afgebeeld. De afbeelding is dus een transformatie van G.

3^o. $g^{-1}abg = g^{-1}ag.g^{-1}bg$, het beeld van het product is het product van de beelden, d.w.z. de transformatie is een automorfie. Men noemt ze een inwendige automorfie, er zijn ook nog andere. Die heten dan uitwendig..

7.5. Geconjugeerde ondergroepen

Een ondergroep van G wordt door een inwendige automorfie van G op een ondergroep afgebeeld. Zulke ondergroepen heten geconjugeerd, natuurlijk zijn ze isomorf.

Voor normaaldelers werd al in 7.3 opgemerkt, dat de beelden van de elementen weer tot de normaaldeler behoren. Omgekeerd is elk element van de normaaldeler beeld van zo'n element, want de inverse automorfie is ook inwendig en voegt het origineel aan het beeld toe. Er volgt dat een normaaldeler met al zijn geconjugeerden samenvalt, een normaaldeler is invariant voor een inwendige automorfie.

Dat is ook kenmerkend voor een normaaldeler, d.w.z. een ondergroep is normaaldeler, wanneer hij invariant is voor alle inwendige automorfieën van de groep. Voor zo'n ondergroep H zou immers volgen $g^{-1}Hg = H$ of $Hg = gH$ voor willekeurige g.

7.6. Als voorbeeld stellen we een tabel op van de inwendige automorfieën van S_3, men raadplege daarbij de in 5.5 gegeven groepstabel van S_3. Hij komt er zo uit te zien:

e	e	a	b	p	q	r	E
a	e	a	b	q	r	p	B
b	e	a	b	r	p	q	A
p	e	b	a	p	r	q	P
q	e	b	a	r	q	p	Q
r	e	b	a	q	p	r	R

De linkse afzonderlijke kolom geeft de elementen, waarmee getransformeerd wordt, de achter zo'n element staande rij van het middelste blok geeft de beelden van de er boven staande elementen van de eerste rij bij die transformatie. De automorfieën zijn permutaties van S_3, de n-de (n=1,2,...,6) wordt gegeven door de eerste en de n-de rij van het middenblok, b.v. de vierde (de transformatie met p) door

$$\begin{pmatrix} e & a & b & p & q & r \\ e & b & a & p & r & q \end{pmatrix} .$$

We geven deze permutaties namen in de vorm van hoofdletters, ze zijn in de rechtse kolom vermeld. We lezen af:
$B = (p,q,r)$; $A = (p,r,q)$; $P = (a,b)(q,r)$; $Q = (a,b)(p,r)$; $R = (a,b)(p,q)$.
A en B zijn van de derde orde, P,Q en R van de tweede. Er blijkt $A^2 = (p,r,q)(p,r,q) = (p,q,r) = B$ en evenzo $B^2 = A$; $AP = (p,r,q)(a,b)(q,r) = (a,b)(p,r) = Q$ enz. Stellen we van alle producten een tabel op, dan blijkt die dezelfde te zijn als die van S_3, als men daarin de kleine

letters door overeenkomstige hoofdletters vervangt. Blijkbaar vormen de inwendige automorfieën van S_3 een groep, die isomorf is met S_3.

7.7. De groep der inwendige automorfieën

We willen nu van een willekeurige groep G uitgaan en nagaan, welke resultaten van de vorige paragraaf algemene geldigheid bezitten. Allereerst bewijzen we: de inwendige automorfieën van G vormen een groep.

Automorfieën zijn transformaties, voor hun vermenigvuldiging nemen we dus het na-elkaar-uitvoeren (van rechts naar links) en deze vermenigvuldiging is associatief. Er moet nu worden nagegaan of het product van twee inwendige automorfieën wel weer een inwendige automorfie is. Neem er twee: $A_g : x \longrightarrow g^{-1}xg$ en $A_h : x \longrightarrow h^{-1}xh$, dan is $A_hA_g : x \longrightarrow h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$, dus $A_hA_g = A_{gh}$. De identieke automorfie is éénelement. De inverse $(A_g)^{-1}$ van A_g is $x \longrightarrow gxg^{-1}$, dus $(A_g)^{-1} = A_{g^{-1}}$. Volgens de postulaten van 1.4 vormen de inwendige automorfieën dus een groep.

De volgende vraag is, hoe het staat met eventuele isomorfie met G. Nemen we de afbeelding $g \longrightarrow A_{g^{-1}}$, dan volgt: $gh \longrightarrow A_{(gh)^{-1}} = (A_{gh})^{-1} = (A_hA_g)^{-1} = A_g^{-1}A_h^{-1} = A_{g^{-1}} \circ A_{h^{-1}}$. Bij de afbeelding blijft de bewerking dus behouden en dat betekent een homomorfie. Verder kunnen we ook niet komen, de afbeelding is namelijk zeker niet steeds een isomorfie, zoals blijkt, wanneer we een Abelse groep nemen. Die heeft immers maar één inwendige automorfie, de identieke, want steeds is $g^{-1}xg = g^{-1}gx = x$. Daar worden dus alle elementen van de groep op die ene automorfie afgebeeld.

In het voorbeeld van 7.6 waren er 6 inwendige automorfieën, daar treedt dus een isomorfie op.

Opmerking. De afbeelding $g \longrightarrow A_{g^{-1}}$ is lelijk, we hadden liever $g \longrightarrow A_g$ gezien. Net zoiets geldt voor de vermenigvuldigingsregel $A_gA_h = A_{hg}$. Zouden we gedefiniëerd hebben $A_g : x \longrightarrow gxg^{-1}$, dan zou de gewenste afbeelding het gedaan en de vermenigvuldigingsregel $A_gA_h = A_{gh}$ geluid hebben. Sommige auteurs kiezen inderdaad deze definitie, vermoedelijk treden daarbij dan weer andere antisymmetrieën op.

De hier gebruikte afbeelding verklaart de verwisseling van A en B, die in het voorbeeld van de vorige paragraaf opgevallen zal zijn. We beelden immers g af op de door g^{-1} verwekte automorfie en a en b zijn

elkaars inverse. Bij P,Q en R treedt geen verwisseling op, inderdaad zijn daar ook p,q en r elk hun eigen inverse.

7.8. We willen de homomorfe afbeelding van de vorige paragraaf nader onderzoeken en zoeken daartoe eerst de kern. Dat is de verzameling van die elementen van G, die afgebeeld worden op de identieke automorfie, immers het éénelement van de groep der inwendige automorfieën. De vraag is dus: voor welke g is $A_{g^{-1}}$ de identieke automorfie? Voor zo'n g geldt $g^{-1}xg = x$ of $xg = gx$ voor elke x van G. Maar dan is g element van het centrum Z (7.1). Het omgekeerde is evident, zodat volgt: de groep der inwendige automorfieën van G is isomorf met de factorgroep G/Z. Daarbij heeft de nevenklasse Zg het beeld $A_{g^{-1}}$ en in de homomorfie elk element van Zg eveneens het beeld $A_{g^{-1}}$.

In het voorbeeld van 7.6 was de homomorfie een isomorfie. Daaruit volgt, dat het centrum van S_3 uit alleen het éénelement e bestaat. Iets wat uit de tabel van S_3 gemakkelijk geverifiëerd kan worden.

7.9. Uitwendige automorfieën

7.9.1. Dat een groep ook andere automorfieën kan hebben dan inwendige moge blijken uit een voorbeeld. De groep S_3 heeft de normaaldeler (e,a,b). Een normaaldeler is invariant bij een inwendige automorfie, die bewerkt dus een automorfie van de normaaldeler als groep. Maar deze normaaldeler is commutatief en heeft dus maar één inwendige automorfie, de identieke. De tabel in 7.6 leert, dat die geleverd wordt door E,A en B. P,Q en R leveren een andere, namelijk $e \longrightarrow e$, $a \longrightarrow b$, $b \longrightarrow a$. Dat is dus geen inwendige.

Alle niet-inwendige automorfieën heten uitwendig.

7.9.2. Een goed voorbeeld is V_4, ook commutatief. De elementen noemen we ditmaal e,a_1,a_2,a_3. Voor ongelijke i,j,k geldt $a_i a_j = a_k$. Bij een automorfie wordt e op e afgebeeld, maar verder kunnen de indices 1,2 en 3 willekeurig worden gepermuteerd. Hieruit volgt dat de 6 automorfieën van V_4 een groep vormen, die isomorf is met S_3, 5 van de 6 zijn uitwendig.

Dat ook in het algemeen de automorfieën van een groep zelf een groep vormen, is gemakkelijk in te zien.

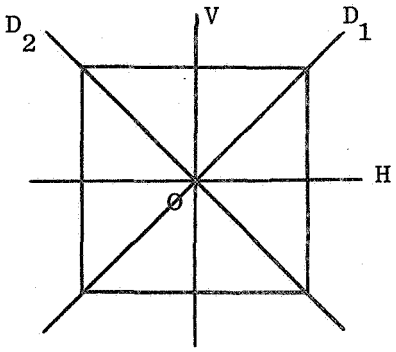
7.9.3. We willen nog even nagaan of S_3 zelf ook uitwendige automorfieën heeft, in 7.6 vonden we 6 inwendige. Bij een isomorfie is de orde van het beeld gelijk aan de orde van het origineel, bij een automorfie kan dus a alleen a of b tot beeld hebben (2 mogelijkheden) en p alleen p,q of r (3 mogelijkheden). Maar a en p brengen S_3 voort (5.5), hebben we dus de beelden voor a en p gekozen, dan ligt de afbeelding verder vast. Er zijn dus in totaal hoogstens $2 \times 3 = 6$ automorfieën, er zijn dus geen uitwendige.

7.9.4. Als sluitstuk bewijzen we de stelling:
Bij een willekeurige groep is de groep der inwendige automorfieën normaaldeler van de groep van alle automorfieën.

Natuurlijk is hij een ondergroep, we hoeven dus alleen het kenmerk voor een normaaldeler toe te passen (6.1). Neem daartoe een willekeurige automorfie ψ en een willekeurige inwendige automorfie φ van de gegeven groep. Dan is te bewijzen, dat $\psi^{-1}\varphi\psi$ inwendig is. Stel $\varphi : x \longrightarrow a^{-1}xa$. Dan is $(\psi^{-1}\varphi\psi)(x) = \psi^{-1}\left[\varphi\{\varphi(x)\}\right] =$
$= \psi^{-1}\{a^{-1}\varphi(x)a\} = \psi^{-1}(a^{-1}).\psi^{-1}\{\psi(x)\}.\psi^{-1}(a) = \psi^{-1}(a^{-1}).x.\psi^{-1}(a)$.
Dit is een inwendige automorfie als $\psi^{-1}(a^{-1})$ en $\psi^{-1}(a)$ elkaars inverse zijn. Dat is zo, want $\psi^{-1}(a^{-1}).\psi^{-1}(a) = \psi^{-1}(a^{-1}.a) = \psi^{-1}(e) = e$.

8. De groep D_4 van de dekafbeeldingen van het vierkant in de ruimte

8.1. Deze paragraaf geeft ter herhaling en ter illustratie een uitgebreid onderzoek van de groep D_4 der dekafbeeldingen (zie 2.5) van het vierkant. De identieke dekafbeeldingen noemen we E. De omklappingen



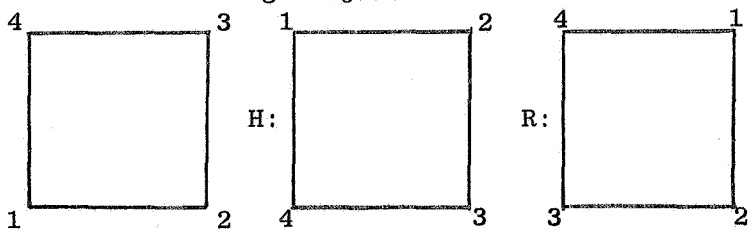
om de assen H,V,D_1 en D_2 noemen we naar die assen. Om O kunnen we 90°, 180° of 270° draaien, we denken ons de draaiïngen rechtsom en noemen ze resp. R,R^2 en R^3. Vermenigvuldiging van dekafbeeldingen worde van rechts naar links uitgevoerd.

Het maakt verschil of we ons voorstellen, dat de assen met het vierkant meedraaien, of dat we ze ons vast in de ruimte denken. In het eerste geval zou b.v. H in de stand van V komen door de draaiïng R en zou dus $HR = D_2$ zijn. In het tweede geval is $HR = D_1$. Daarom is het

nodig de draaiing om O op te vatten als te geschieden om een as door O loodrecht op het vlak van tekening. Draait hij mee, dan wordt R na H linksom (van boven gezien), blijft hij staan, dan blijft R rechtsom. Wij kiezen voor in de ruimte vaste assen.

8.2. Tabel

Uit onderstaande figuurtjes:



leidt men af, dat $RH = D_2$. Evenzo is te bewijzen:

$$V = R^2H,\ D_1 = R^3H \text{ en } HR = R^3H.$$

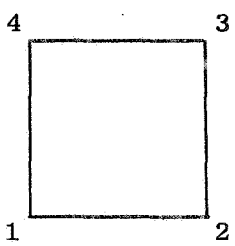
Blijkbaar brengen R en H de groep voort en kan men elk element schrijven als R^iH^j met i = 0,1,2,3 en j = 0,1.

Het samenstellen van de tabel is nu verder een formele aangelegenheid.

E	R	R^2	R^3	H	V	D_1	D_2
R	R^2	R^3	E	D_2	D_1	H	V
R^2	R^3	E	R	V	H	D_2	D_1
R^3	E	R	R^2	D_1	D_2	V	H
H	D_1	V	D_2	E	R^2	R	R^3
V	D_2	H	D_1	R^2	E	R^3	R
D_1	V	D_2	H	R^3	R	E	R^2
D_2	H	D_1	V	R	R^3	R^2	E

8.3. D_4 als permutatiegroep

Elke dekafbeelding permuteert de hoekpunten, D_4 is dus ook op te vatten als ondergroep van S_4. Gemakkelijk zien we: E = (1), H = (1,4)(2,3), V = (1,2)(3,4), D_1 = (2,4), D_2 = (1,3). Ten aanzien van R en zijn machten treedt echter een moeilijkheid op. Men zal neigen tot R = (1,2,3,4), men geeft dan aan de term "afbeelden op" de interpretatie van "vervangen door". Inderdaad is immers de term "afbeelden



op" algemeen en dus vaag, hij moet in elk bijzonder geval gepreciseerd worden. Wegens onze afspraak dat R een draaiïng van 90^o rechtsom zijn zou, moet 1⟶2 betekenen, dat 1 wordt vervangen door 2. De interpretatie "1 komt in de plaats van 2" zou daarentegen een draaiïng linksom inhouden.

De keuze is niet vrij, ze hangt samen met die in 8.1 tussen vaste en meedraaiende assen. We stellen dit even algemeen. Het product (-----,q,r,---)(-----,p,q,---) betekent: eerst p⟶q, dan q⟶r, samen p⟶r.

De eerste factor zegt, wat er met q in <u>beginstand</u> gebeurt, en dit moet een vervolgavontuur van p zijn. Zijn de assen vast, dan is die beginstand ruimtelijk absoluut, de tweede factor moet p brengen waar q stond, p⟶q betekent dus "p komt in de plaats van q". Draaien de assen mee, dan blijft het beginpunt in zijn stand t.o.v. de assen. De eerste factor zegt dus werkelijk wat er met q gebeurt en de tweede moet aangeven dat q komt, waar p was, m.a.w. "p wordt vervangen door q".

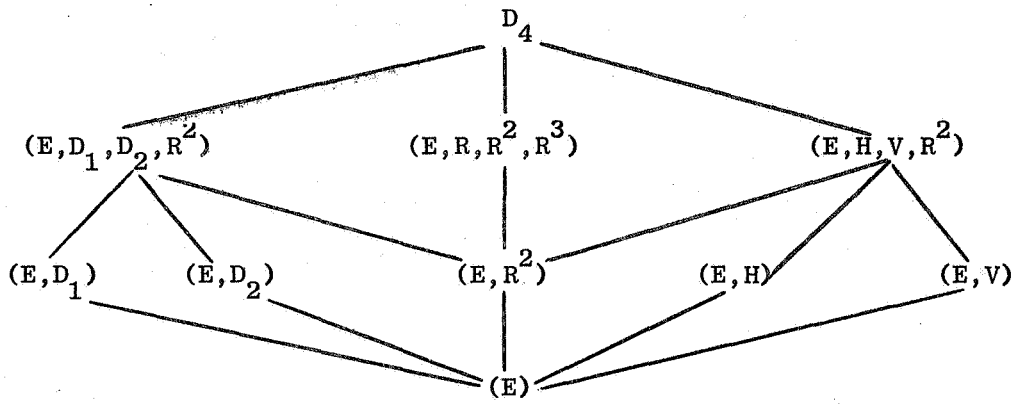
Nu wij de assen vast gekozen hebben moet ook de eerste interpretatie gelden. Er volgt

$$R = (1,4,3,2),\ R^2 = (1,3)(2,4),\ R^3 = (1,2,3,4).$$

Langs deze weg is het samenstellen van de tabel eenvoudiger dan in 8.2.

8.4. <u>Ondergroepen</u>

Ondergroepen van D_4 kunnen orde 1,2,4 en 8 hebben, het gaat natuurlijk om 2 en 4. We laten ze door elementen voortbrengen, eerst uitgaande van één, dan van twee. Daar H en R (ook V en R,D_1 en R, D_2 en R) al D_4 voortbrengen, is het onderzoek gauw klaar. Het volgende schema geeft alle ondergroepen, men kan er ook in zien, welke weer ondergroepen van welke zijn:



Alle echte ondergroepen blijken cyclisch, behalve (E,D_1,D_2,R^2) en (E,H,V,R^2); die zijn $\cong V_4$.

8.5. Centrum

Blijkens de tabel bestaat het centrum van D_4 uit de elementen E en R^2 (rij en kolom moeten voor zo'n element gelijk zijn). Het centrum is een normaaldeler (7.1). De factorgroep heeft de elementen (E,R^2), (R,R^3), (H,V), (D_1,D_2), de laatste drie hebben orde 2. De factorgroep is dus isomorf met V_4.

8.6. Automorfieën

Bij een automorfie hebben origineel en beeld dezelfde orde. Daar R en R^3 de enige elementen zijn van orde 4 zijn voor R de enige mogelijkheden $R \longrightarrow R$ en $R \longrightarrow R^3$, met resp. $R^3 \longrightarrow R^3$ en $R^3 \longrightarrow R$, in beide gevallen zou gelden $R^2 \longrightarrow R^2$.

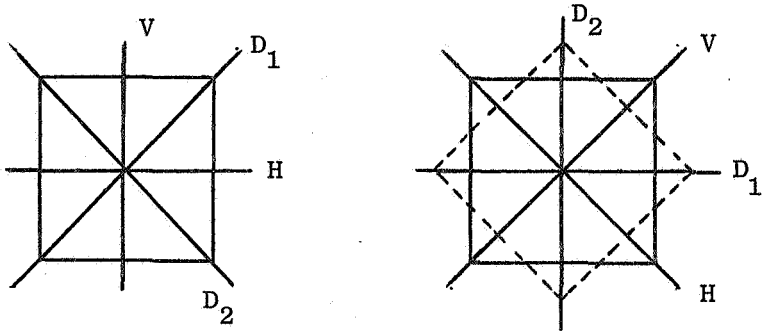
Als beeld van H zouden H,V,D_1,D_2 en R^2 kunnen fungeren, maar R^2 vervalt omdat R^2 zeker al beeld is.

R en H brengen de groep voort, de keuze van hun beeld is dus voor de hele automorfie dwingend. Blijkbaar zijn er hoogstens $2 \times 4 = 8$ automorfieën.

Nu zijn er zeker inwendige automorfieën, in 7.8 werd bewezen dat hun groep isomorf is met D_4/Z, als we het centrum weer Z noemen. Hier heeft Z index 4, er zijn dus 4 inwendige automorfieën, elementen uit dezelfde nevenklasse leveren dezelfde automorfie. In de volgende tabel vullen we die vier alvast in (de onderste rij daarvan blijft even buiten beschouwing):

Origineel	Inw.aut. geleverd door: E en R^2	R en R^3	H en V	D_1 en D_2	Eventuele uitw. aut.			
E ⟶	E	E	E	E	E	E	E	E
R ⟶	R	R	R^3	R^3	R	R	R^3	R^3
R^2 ⟶	R^2	R^2	R^2	R^2	R^2	R^2	R^2	R^2
R^3 ⟶	R^3	R^3	R	R	R^3	R^3	R	R
H ⟶	H	V	H	V	D_1	D_2	D_1	D_2
V ⟶	V	H	V	H	D_2	D_1	D_2	D_1
D_1 ⟶	D_1	D_2	D_2	D_1	V	H	H	V
D_2 ⟶	D_2	D_1	D_1	D_2	H	V	V	H
	E	R^2	H	V	R	R^3	D_2	D_1

De laatste vier kolommen vullen we in met wat er aan mogelijkheden overblijft, nl. R⟶R of ⟶ R^3 en H⟶ D_1 of ⟶ D_2. Er moet nog bewezen worden dat deze kolommen werkelijk automorfieën geven, maar het is genoeg dat voor één er van te bewijzen. De eerste vier vormen immers een ondergroep, is er een vijfde, dan weten we meteen, dat er acht zijn. We geven het bewijs van no 5 met behulp van twee figuurtjes:



Het getrokken vierkant in het tweede is hetzelfde als dat in het eerste, maar de letters bij de assen zijn volgens de afbeelding in kolom 5 vervangen. Het blijkt dat het stel assen daardoor als het ware 45^o rechtsom gedraaid is. Was het vierkant meegedraaid, dan was het in de gestippelde stand gekomen. Nu is het duidelijk, dat een dekafbeelding van het getrokken vierkant er ook een van het gestippelde is en omgekeerd. D_4 voor het gestippelde vierkant (dus de oorspronkelijke groep) is dus ook D_4 voor het getrokkene.

8.7. We bekijken de groep der 8 automorfieën nader. Het blijkt, dat no 5 de orde 4 heeft, pas ze maar 4 keer toe (bv. $H \longrightarrow D_1 \longrightarrow V \longrightarrow D_2 \longrightarrow H$). Evenzo heeft no 6 de orde 4, de andere, behalve no 1, de orde 2. Dit lijkt op D_4, we vermoeden daarom isomorfie en proberen de afbeelding no $5 \longrightarrow R$, waaruit zou volgen no $2 \longrightarrow R^2$, no $6 \longrightarrow R^3$, we noteren dat onder de betreffende kolommen. Als origineel van H kiezen we no 3. Door R en H werd D_4 voortgebracht, we gebruikten de betrekkingen $R^1H = V$, $R^3H = D_1$, $RH = D_2$, waaruit zou volgen no $4 \longrightarrow V$, no $8 \longrightarrow D_1$ en no $7 \longrightarrow D_2$. Het blijkt dan dat $HR = R^3H$ $(=D_1)$ geldt, wanneer we de automorfieën substitueren, zodat inderdaad door de automorfieën nos 5 en 3 een groep wordt voortgebracht $\cong D_4$. Natuurlijk zijn er weer 8 isomorfe afbeeldingen mogelijk.

8.8. Normaaldelers

Uit de tabel voor de inwendige automorfieën lezen we af, dat de conjugatieklassen zijn:

$$(E),\ (R,R^3),\ (R^2),\ (H,V) \text{ en } (D_1,D_2).$$

De normaaldelers vindt men door òf onder de ondergroepen de verenigingen van conjugatieklassen te zoeken òf in de tabel der inwendige automorfieën na te gaan, welke ondergroepen voor alle invariant zijn. Het blijken:

$$(E),\ (E,R^2),\ (E,R,R^2,R^3),\ (E,R^2,H,V),\ (E,R^2,D_1,D_2)$$

en D_4 zelf. Eigenlijk spreekt dat voor de eerste en de laatste vanzelf, van (E,R^2) wisten we het al en de andere drie hebben index 2.

8.9. Homomorfe beelden van D_4

1^o. Kern $(E) \longrightarrow D_4$ zelf.

2^o. Kern (E,R^2), homomorfie met V_4, al behandeld in 8.5.

3^o. Kern (E,R,R^2,R^3), (E,H,V,R^2) of (E,D_1,D_2,R^2): deze hebben alle een factorgroep van twee elementen, geven dus alle de homomorfie met de enige abstracte groep van twee elementen, b.v. te concretiseren in (E,R^2).

4^o. Kern D_4 geeft homomorfie met de groep van één element, bv. (E).

III. Ringen

1. Definitie en eenvoudige eigenschappen

1.1. Een ring is een verzameling, waarin twee bewerkingen zijn gedefinieerd; we noemen ze "optelling" en "vermenigvuldiging".

1. Ten aanzien van de optelling is de ring een commutatieve groep (de "additieve groep van de ring").
2. De vermenigvuldiging is
   a) associatief: a(bc) = (ab)c (dus te schrijven: abc).
   b) distributief t.o.v. de optelling: a(b+c) = ab+ac;
   (b+c)a = ba+ca.

Is de vermenigvuldiging bovendien commutatief, dan spreekt men van een commutatieve ring.

1.2. Uit de definitie volgt:

a) Ten aanzien van de optelling is er precies één neutraal element (het "nulelement" 0 van de ring).
b) Elk element a van de ring heeft precies één tegengestelde -a.
c) Voor elk paar elementen a en b is de aftrekking a-b mogelijk en ondubbelzinnig.
d) a.0 = 0 voor elke a, want ab=a(b+0) = ab+a.0.

Een ring behoeft geen éénelement te hebben. Er kunnen linkeréénelementen zijn of rechter. Bezit de ring van beide één, dan zijn ze gelijk en spreekt men van het éénelement ($e_L = e_L e_R = e_R$).

2. Voorbeelden

2.1. De bewerkingen in een integriteitsgebied (postulaten in I,2.3) voldoen aan de ringpostulaten, een integriteitsgebied is dus een ring.

We stellen in het vervolg de ring centraal en definiëren het integriteitsgebied als een commutatieve ring met een (van 0 verschillend) éénelement en zonder nuldelers (zie I, 3,4,4). (Door sommige schrijvers wordt het éénelement niet geëist.) Deze definitie stelt dus boven de ringpostulaten nog vier eisen. In de volgende voorbeelden blijkt, dat ze niet uit de postulaten volgen en onafhankelijk zijn van elkaar.

2.2. De eenvoudigste ring is de "nulring", hij bestaat uit één element O; bewerkingen: O+O = O, O.O = O. Uit de eerste betrekking blijkt, dat het enige element nulelement, uit de tweede, dat het éénelement is. Het is zijn eigen tegengestelde zowel als zijn eigen inverse. De nulring is geen integriteitsgebied, omdat nul en één samenvallen. Sommige auteurs eisen van een ring, dat hij minstens twee verschillende elementen bevat en sluiten dus de nulring uit.

2.3. De even getallen vormen een ring. Die is commutatief, heeft geen nuldelers, maar ook geen éénelement. Hetzelfde geldt van de verzameling der k-vouden, $k \geq 2$, geheel.

2.4. C_m is een commutatieve ring met éénelement, echter alleen zonder nuldelers, als m priem is (zie I,3.4.4).

2.5. Een niet-commutatieve ring leveren de $n \times n$ matrices met b.v. gehele getallen als elementen. Nemen we n=2, dan zijn bedoeld de matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ met a,b,c,d geheel.

Optelling: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & g \end{pmatrix} = \begin{pmatrix} a+e, & b+f \\ c+g, & d+h \end{pmatrix}$.

Vermenigvuldiging: de gewone matrixvermenigvuldiging ("rij maal kolom"):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

Associativiteit en commutativiteit van de optelling zijn duidelijk, de vermenigvuldigingseigenschappen moeten nagerekend worden. Nulelement is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, éénelement: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

De niet-commutativiteit volgt uit het voorbeeld:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ en } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Er zijn nuldelers, zo is b.v. $\begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}\begin{pmatrix} -3 & 3 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Men doorziet wel, dat één der factoren willekeurig singulier en de andere bijpassend gekozen is.

2.6. Van twee ringen kan men een derde maken, die hem "direct product" heet (ook wel "directe som"). Heten de ringen R en R', dan is het directe product R ⨯ R' de verzameling van alle paren (a,a') met a ∈ R en a' ∈ R'. De optelling wordt gedefinieerd door: (a,a') + (b,b') = (a+b, a'+b'). De vermenigvuldiging door (a,a')(b,b') = (ab,a'b'). Daar de bewerkingen de elementen van de twee ringen gescheiden laten, spreekt de geldigheid der postulaten vanzelf.

Het nulelement is (0,0'), er zijn nuldelers, want (a,0')(0,a') = (0,0'). Een éénelement is er alleen, als beide ringen er een hebben, het is dan (e,e').

2.7. Van elke commutatieve groep kan men een ring maken door aan elk tweetal elementen het product nul toe te kennen. De elementen ≠ 0 worden daardoor alle nuldelers.

Sluiten we nuldelers uit, dan kan niet elke commutatieve additieve groep tot ring worden gemaakt, zoals blijkt uit de volgende

Stelling: In de additieve groep van een ring zonder nuldelers hebben alle elementen ≠ 0 dezelfde orde. Is die eindig, dan is ze priem.

Bewijs: Stel het element a ≠ 0 en ma = 0 (m is een natuurlijk getal en geen ringelement, ma is een "natuurlijk veelvoud" van a, nl. de som a+a+...+a met m termen). Neem nu een willekeurig element b ≠ 0, dan is (ma)b=0. Maar (ma)b = (a+a+...+a)b = ab+ab+...+ab = a(b+b+...+b) = a(mb), dus a(mb) = 0 en mb = 0. Blijkbaar is de orde k van b een deler van m. We kunnen voor m de orde van a nemen, maar uit kb = 0 volgt net als zoeven ka = 0, dus m is een deler van k. Bijgevolg is k=m.

Is m te ontbinden, b.v. m = jk (met j en k ≧ 2), dan is (jk)a = j(ka) = 0, dus het element ka (dat ≠ 0 is wegens k < m) heeft orde ≦ k < m, in tegenspraak met het resultaat, dat alle elementen ≠ 0 orde m hebben. Dus is m priem.

Is er geen natuurlijk getal m met de bedoelde eigenschap, dan hebben alle elementen ≠ 0 orde oneindig, in dat geval is o.a het enige "gehele" veelvoud van zo'n element a, dat = 0 is.

Men noemt de gemeenschappelijke orde van de groepelementen ≠ 0 de karakteristiek van de ring, als die orde eindig is. Is de orde oneindig, dan kent men de ring de karakteristiek nul toe, wegens bovengenoemd enige

nulveelvoud. In sommige boeken houdt men het echter op de gemeenschappelijke orde en spreekt men van de karakteristiek oneindig.

3. Homomorfie en isomorfie

3.1. De begrippen homomorfie en isomorfie zijn bekend uit I,5.3.

Een homomorfe afbeelding van een ring is eenduidig, een isomorfe éénéénduidig, bij beide blijven de bewerkingen behouden. Isomorfie is een bijzonder geval van homomorfie, bij een isomorfe afbeelding is een inverse afbeelding mogelijk en die is ook isomorf.

Het voorbeeld $C \longrightarrow C_n$ uit I,5.3 betrof de homomorfe afbeelding van een ring, elk geheel getal werd afgebeeld op de restklasse, waartoe het behoort. Als voorbeeld van een automorfie (d.w.z. isomorfe afbeelding op zichzelf) van een integriteitsgebied werd

$$a + b\sqrt{2} \longrightarrow a-b\sqrt{2} \quad \text{(a en b geheel)}$$

gegeven. Een voorbeeld van een homomorfie is nog de afbeelding $C \times C \longrightarrow C$ (dus van het directe product van de ring der gehele getallen C met zichzelf op C) volgens $(a,b) \longrightarrow a$. Of algemeen: van $R \times R'$ op R volgens $(a,a') \longrightarrow a$.

3.2. Zijn in een verzameling twee bewerkingen gedefiniëerd, en kan men een gegeven ring homomorf in die verzameling afbeelden door de ene bewerking met de optelling, de andere met de vermenigvuldiging te laten corresponderen, dan zal het duidelijk zijn, dat de beeldverzameling weer een ring is. Verder, dat het nulelement van de ring wordt afgebeeld op de nul van de beeldring, het éénelement op het éénelement, het tegengestelde van een element op het tegengestelde van het beeld van dat element en evenzo met een eventuele inverse. Is de ring commutatief, dan de beeldring ook.

3.3. Het voorbeeld $C \longrightarrow C_n$ bewijst, dat een integriteitsgebied niet een integriteitsgebied als homomorf beeld hoeft te hebben, als n niet priem is, heeft C_n nuldelers.

Wordt een integriteitsgebied isomorf afgebeeld, dan is de beeldring weer een integriteitsgebied, de nul in de beeldring heeft alleen de nul van de afgebeelde ring tot origineel, dus kan de nul van de beeldring

alleen dan uitkomst van een product zijn, als dat in de afgebeelde ring ook zo is. Bij een homomorfie, die geen isomorfie is, heeft de beeldnul ook andere originelen.

Het voorbeeld $C \times C \longrightarrow C$ volgens $(a,b) \longrightarrow a$ laat zien, dat een ring met nuldelers wel een integriteitsgebied als homomorf beeld kan hebben.

3.4. In 3.3 werd zonder bewijs opgemerkt, dat de nul van de beeldring slechts in geval van isomorfie precies één origineel heeft, bij andere homomorfieën daarentegen meer. Daarmee is dus gesteld: heeft bij de homomorfe afbeelding f van R op R' het nulelement O' alleen het nulelement O tot origineel, dan is de afbeelding een isomorfie, d.w.z. dan heeft elk element van R' slechts één origineel in R.

Bewijs: Laat het willekeurige element a' van R' de originelen a_1 en a_2 hebben. Dan is $f(a_1-a_2) = f(a_1)-f(a_2) = a'-a'=O'$, dus $a_1-a_2=O$ of $a_1=a_2$.

We hadden er ook van kunnen uitgaan, dat het willekeurige element a' alleen het origineel a had, ook dat is kenmerk voor isomorfie. Stel maar, O' heeft de originelen O en b, dan volgt $f(a+b) = f(a)+f(b) = a'+O' = a'$, dus $a+b = a$ en $b = O$.

Het vermoeden ligt voor de hand, dat bij de homomorfe afbeelding $R \longrightarrow R$ alle elementen van R' "evenveel" originelen in R hebben. Preciezer: zijn a' en b' twee elementen van R' dan is de verzameling van originelen van a' éénéénduidig af te beelden op de verzameling van originelen van b'. We zullen de verzameling van originelen van a' voortaan het "volledig origineel" van a' noemen. Voor het bewijs kunnen we b' = O' stellen, daar a' toch willekeurig is.

Bewijs: Stel het volledig origineel van O' I en laat a een origineel van a' zijn. Dan vormen we de verzameling I+a van alle sommen i+a met $i \in I$. Elk element van i+a heeft het beeld a': $f(i+a) = f(i) + f(a) = O' + a' = a'$. Is omgekeerd $f(c) = a'$, dan volgt $f(c-a) = f(c)-f(a) = a'-a'=O'$, dus $c-a \in I$ en $c \in I+a$.

I+a is dus het volledig origineel van a', het is éénéénduidig op I af te beelden volgens $i+a \longrightarrow i$. Een directe éénéénduidige afbeelding van I+a op I+b krijgen we door $i+a \longrightarrow i+b$.

3.5. Een aardige toepassing van de isomorfie levert het volgende voorbeeld. In de verzameling der gehele getallen scheppen we een nieuwe optelling (O) en een nieuwe vermenigvuldiging ($\triangle$) door de definities

$$a \circ b = a+b-3,\quad a \triangle b = ab-3a-2b+12.$$

Bij deze nieuwe bewerkingen vormen de gehele getallen een ring, men kan het narekenen. Nulelement is 3, want $a \circ 3 = a+3-3 = a$. Eénelement is 4, want $a \triangle 4 = 4a-3a-12+12 = a$.

Het bewijs van het ringschap is nu het gemakkelijkst te leveren door aan te tonen, dat de verzameling met de nieuwe bewerkingen isomorf is met de oorspronkelijke (we noemen dat geen automorfie, omdat het niet dezelfde bewerkingen zijn). Als afbeelding nemen we $a \rightarrow a+3$ (met nul en één klopt het dan).

Nu moet a+b het beeld a+b+3 hebben en inderdaad is
$(a+3) \circ (b+3) = a+3+b+3-3 = a+b+3$, dus $a+b \rightarrow (a+3) \circ (b+3)$.
Evenzo is $(a+3) \triangle (b+3) = (a+3)(b+3)-3(a+3)-3(b+3)+12 = ab+3a+3b+9-3a-9-3b-9+12 = ab+3$, zodat $ab \rightarrow (a+3) \triangle (b+3)$.

De bewerkingen blijven dus behouden, de afbeelding is isomorf en de beeldverzameling is een ring.

4. Deelbaarheid in ringen

4.1. In de rekenkunde van de gehele getallen is de deling vrijwel het belangrijkste onderwerp, juist omdat ze niet onbeperkt uitvoerbaar is. Men denke aan begrippen als deelbaarheid, priemgetal, ontbinding in priemfactoren, g.g.d. en k.g.v., congruenties. Weliswaar gaat het bij deze begrippen meestal om de natuurlijke getallen, maar een eventuele uitbreiding op de gehele getallen levert geen moeilijkheden op.

Het is duidelijk, dat de met deze begrippen samenhangende probleemstellingen ook in de theorie van de ringen een voorname plaats zullen innemen, ze zijn zelfs mede uitgangspunt geweest bij het ontstaan en de ontwikkeling van de abstracte algebra.

Nu is het geenszins zo, dat de resultaten van de rekenkunde maar direct op de ringen kunnen worden overgedragen, integendeel heeft die overdracht aanleiding gegeven tot de vorming van tal van nieuwe begrippen. Verwarrend is daarbij de grote verscheidenheid in definitie-eisen en in

de voorwaarden, waaronder stellingen worden bewezen (die zullen wel niet altijd noodzakelijk zijn). Verder treden bij verschillende schrijvers weer verschillende definities en verschillende stellingsvoorwaarden op.

In het volgende doen we hier en daar een greep uit deze stof:

4.2. Delen is het oplossen van de (of één der) vergelijkingen $ax = b$ en $xa = b$, het zal dus alvast verschil maken, of de ring commutatief is of niet.

Wegens $a.0 = 0$ voor elke a blijft het delen door 0 ongedefiniëerd, maar ook het delen door nuldelers stelt voor complicaties. Is a een nuldeler en a' een complementaire, dan zal uit $xa = b$ volgen $xaa' = ba' = 0$. Noodzakelijk voor de oplosbaarheid van de vergelijking $xa = b$ is dus alvast, dat ook b nuldeler is met a' als complementaire. Moet er nog onderscheid gemaakt worden tussen linker- en rechternuldelers, dan wordt de zaak nog ingewikkelder.

Is het element b te ontbinden als $b=ca$, dan ook als $b=(a'+c)a$, ook de ontbinding wordt dus gecompliceerd; dat komt, doordat de vereenvoudigingswet haar geldigheid verliest als er nuldelers optreden.

Het al of niet aanwezig zijn van een éénelement maakt groot verschil, zo is in de ring der even getallen geen getal door zichzelf deelbaar.

4.3. We geven nu enige definities en beperken ons daarbij tot <u>integriteitsgebieden</u>, al zouden sommige ook wel voor andere ringen zin hebben.

Een element $a \neq 0$ heet een deler van b, of deelbaar op b (notatie a/b, "niet deelbaar op b' schrijft men als $a \nmid b$), als de vergelijking $ax = b$ oplosbaar is, als er dus een element c is met $b = ac$; b heet een (ring-)veelvoud van a.

De afwezigheid van nuldelers maakt de deling eenduidig: uit $ac=ad$ volgt $a(c-d) = 0$, dus $c-d = 0$ of $c=d$.

Duidelijk is e/a voor elke a en a/a, $a/0$ voor elke $a \neq 0$. De deelbaarheid is transitief, d.w.z. uit a/b en b/c volgt a/c. Tenslotte volgt uit a/b en c/d, dat ac/bd.

Van belang zijn de z.g. "eenheden", dat zijn elementen, die op het éénelement e deelbaar zijn. Is ε/e, dan schrijft men $e = \varepsilon\varepsilon^{-1}$, het element ε^{-1} heeft de "inverse" van ε, eenheden zijn dus die elementen, die een inverse bezitten. Natuurlijk is $(\varepsilon^{-1})^{-1} = \varepsilon$, dus ε^{-1} is

ook een eenheid. Het product van twee eenheden is weer een eenheid, de inverse van $\varepsilon_1 \varepsilon_2$ is $\varepsilon_2^{-1} \varepsilon_1^{-1}$. Daar ook e een eenheid is, vormen de eenheden van een integriteitsgebied een groep.

In de ring der gehele getallen zijn 1 en -1 de eenheden, in de ring der gehele getallen van Gauss (de complexe getallen a+bi met gehele a en b) zijn het 1,-1, i en -i.

Het integriteitsgebied $C[\sqrt{5}]$ der getallen $a+b\sqrt{5}$ met gehele a en b heeft oneindig veel eenheden. Om er te vinden herleiden we $\frac{1}{a+b\sqrt{5}} = \frac{a+b\sqrt{5}}{a^2-5b^2}$, dus moet $a^2-5b^2 = \pm 1$ zijn. Een getal met die eigenschap is $2+\sqrt{5}$ en daarmee alle machten $(2+\sqrt{5})^n$, met willekeurige gehele n.

Het getal a^2-5b^2 heet de <u>norm</u> $N(a+b\sqrt{5})$ van $a+b\sqrt{5}$. Voor later gebruik rekenen we even na, dat $N(\alpha\beta) = N(\alpha).N(\beta)$. Stel maar $\alpha = a+b\sqrt{5}$ en $\beta = c+d\sqrt{5}$, dan is $\alpha\beta = (ac+5bd)+(bc+ad)\sqrt{5}$, dus $N(\alpha\beta) = (ac+5bd)^2 - 5(bc+ad)^2 = a^2c^2+10abcd+25b^2d^2-5b^2c^2-10abcd-5a^2d^2 = a^2c^2-5a^2d^2-5b^2c^2+25b^2d^2 = (a^2-5b^2)(c^2-5d^2) = N(\alpha).N(\beta)$.

Alle elementen van de ring zijn door een eenheid deelbaar, immers de vergelijking $\varepsilon x = a$ heeft de wortel $\varepsilon^{-1}a$.

Twee elementen van het integriteitsgebied heten <u>geassociëerd</u>, als het ene uit het andere kan worden verkregen door vermenigvuldiging met een eenheid, b.v. $a = b\varepsilon$. Het "geassociëerd-zijn" is een equivalentie, want $a = ae$ (reflexief), uit $a = b\varepsilon$ volgt $b = a\varepsilon^{-1}$ (symmetrisch) en uit $a = b\varepsilon_1$ en $b = c\varepsilon_2$ volgt $a = c\,\varepsilon_2\,\varepsilon_1$ (transitief). Uit $a = b\varepsilon$ volgt a/b en b/a, dat is kenmerkend voor het geassociëerd zijn. Stel maar $b = ac$ en $a = bd$, dan is $b = bdc$, dus $dc = e$ en d en c zijn eenheden.

Onder een grootste gemene deler d=(a,b) van a en b verstaat men een gemene deler van e en b, die deelbaar is door alle andere gemene delers. Men kan in het algemeen niet spreken van <u>de</u> g.g.d. omdat alle geassociëerden van d ook g.g.d.'s zijn. Omgekeerd zijn alle g.g.d.'s van a en b geassociëerd.

Een kleinste gemene veelvoud van a en b is een gemeenschappelijk (ring-) veelvoud, dat deelbaar is op alle gemene veelvouden. Ook alle geassociëerden zijn k.g.v. en omgekeerd.

Een deler van a heet een "echte deler", als hij geen eenheid is en ook niet met a geassociëerd. Is $a \neq 0$ en heeft a geen echte delers,

dan heet a onontbindbaar, irreducibel of ook een priemelement. In dat geval zijn ook alle met a geassocieerde elementen onontbindbaar.

In $C[\sqrt{5}]$ zijn de getallen 2 en $3 \pm \sqrt{5}$ onontbindbaar. De ontbinding $\gamma_1 \gamma_2$ van het element γ zou de ontbinding van de norm $N(\gamma) = N(\gamma_1).N(\gamma_2)$ (in C) meebrengen. Nu is $N(2) = N(3\pm\sqrt{5}) = 4$, we zoeken dus ontbindingen van 4. Dat zijn 1×4, -1×-4, 2×2 en -2×-2. Is $N(\gamma_1) = \pm 1$, dan is γ_1 een eenheid, de ontbinding dus triviaal. We zoeken dus een getal $a+b\sqrt{5}$ met norm ± 2.

Uit $a^2-5b^2=2$ volgt $a^2 \equiv 2 \pmod 5$, a^2 zou dus uitgaan op 2 of op 7. Uit $a^2-5b^2=-2$ volgt $a^2 \equiv 3 \pmod 5$ en a^2 zou uitgaan op 3 of 8. Geen van de vier is echter het laatste cijfer van een geheel kwadraat, dus zijn 2 en $3\pm\sqrt{5}$ onontbindbaar.

4.4. Al kunnen verschillende begrippen uit de rekenkunde der gehele getallen op andere ringen worden overgedragen, dan is daarmee nog niet gezegd, dat ze daar al hun eigenschappen behouden. Vandaar dat men ten aanzien van een belangrijke stelling wel zoekt naar de ringen, waarin ze geldt.

Een voorbeeld daarvan levert de z.g. hoofdeigenschap van de deelbaarheid (of zelfs van de rekenkunde), namelijk dat elk natuurlijk getal op precies één manier in eindig veel priemfactoren te ontbinden is (producten van één factor toegelaten). Voor de ring der gehele getallen geldt de stelling ook, alleen moet er dan bijgezegd worden, dat ontbindingen als $6=2 \times 3$ en $6=-2 \times -3$ of $6=-1 \times 2 \times -3$ voor dezelfde gerekend worden.

Het bewijs van de existentie der ontbinding verloopt zo: als het natuurlijke getal a priem is, vormt hetzelfd de gezochte ontbinding (in één factor). Kan men schrijven $a=bc$ dan volgt nader onderzoek van b en c enzovoort. Omdat de factoren telkens kleiner worden en toch minstens 2 moeten zijn, komt er na een eindig aantal stappen een eind.

Dat de zo gevonden ontbinding uniek is, is een conclusie uit de stelling: uit p/ab volgt p/a of p/b (p priem).

Bij twee ontbindingen

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \quad \text{(p's en q's priem)}$$

zou het rechterlid door p_1 deelbaar moeten zijn, dus één der q's, stel q_1. Maar daar die geen echte delers heeft moet hij met p_1 samenvallen

en kan dus weggestreept worden. Enzovoort.

Van geen der gestelde uitgangspunten kan men verwachten, dat het in een willekeurige ring of zelfs in een willekeurig integriteitsgebied zal gelden. Toch zijn er zulke integriteitsgebieden (we zullen ze te zijner tijd tegenkomen), men vat ze samen onder de naam factorontbindingsring.

Een factorontbindingsring is dus een integriteitsgebied, waarin van elk element $\neq 0$, dat geen eenheid is, precies één ontbinding in eindig veel priemfactoren bestaat. Natuurlijk komt het daarbij niet op de volgorde van de factoren aan en worden ontbindingen, die zich slechts in het optreden van eenheden en geassociëerde elementen onderscheiden, voor dezelfde gerekend.

Het integriteitsgebied $C[\sqrt{5}]$ is géén factorontbindingsring, want van het element 4 bestaan twee essentiëel verschillende ontbindingen in priemfactoren, namelijk 2×2 en $(3+\sqrt{5})(3-\sqrt{5})$.

In een factorontbindingsring heeft elk paar elementen een g.g.d. en een k.g.v.,op de bekende wijze uit de ontbindingen te bepalen.

4.5.1. Een ander voorbeeld van generalisatie als in 4.4 bedoeld levert de "deling-met-rest", die bij de natuurlijke getallen mogelijk is. Die komt er op neer, dat bij elk tweetal natuurlijke getallen a en b (met $b \neq 0$) twee natuurlijke getallen q en r (quotiënt en rest) te vinden zijn zodat $a = qb + r$, waarbij $0 \leqq r < b$. Is $r=0$, dan "gaat de deling op", d.w.z. b/a. Het essentiële van deze deling is de aan r gestelde voorwaarde $0 \leqq r < b$. Bij de natuurlijke getallen is de deling met rest eenduidig (d.w.z. er is maar één stel q en r, dat voldoet), want uit $q_1 b+r_1 = q_2 b+r_2$ zou volgen $(q_1-q_2)b = r_2-r_1$, waarin (als $q_1 > q_2$) het rechterlid $< b$ en het linkerlid $\geq b$ zou zijn.

Bij de gehele getallen bestaat de deling met rest ook, van r wordt dan geëist dat $0 \leqq |r| < |b|$. Ze is hier niet meer eenduidig zoals blijkt uit $7 = 2 \times 3+1$ en $7 = 3 \times 3-2$. Natuurlijk is de eenduidigheid gemakkelijk te redden door te eisen dat $0 \leqq r < |b|$, maar de bedoelde generalisatie ligt in de lijn van het eerstgenoemde.

Ook bij veeltermen kennen we deze deling, daar wordt van de rest geëist, dat hij nul is, dan wel een graad heeft kleiner dan die van de deler, de rol van $|b|$ wordt daar dus door die graad overgenomen.

Nu algemeen: men zegt, dat in een integriteitsgebied een deling met rest bestaat, als aan elk element $c \neq 0$ een niet-negatief geheel getal $g(c)$ kan worden toegevoegd, zodanig dat bij elk paar elementen a en b, met $b \neq 0$, twee elementen q en r bestaan met $a = qb+r$, waarin òf $r = 0$ is, òf $g(r) < g(b)$.

In C zijn de getallen $g(c) = c$ positief, bij veeltermen kan g ook nul zijn.

Een integriteitsgebied heet nu een Euclidische ring, als de deling met rest er in mogelijk is, terwijl bovendien voor elk paar elementen a en $b \neq 0$ voldaan is aan de voorwaarde

$$g(ab) \geqq g(a).$$

4.5.2. Niet alle schrijvers eisen, dat een integriteitsgebied een éénelement heeft, toch kan de definitie van een Euclidische ring dezelfde blijven. M.a.w.,als we uitgaan van een commutatieve ring met minstens twee elementen en zonder nuldelers, dan kan bewezen worden, dat er een éénelement is. Als volgt:

De getallen g(b) zijn nul of positief, er is dus een kleinste. Laat b zo gekozen zijn, dat g(b) minimaal is. Is a een willekeurig element en stellen we $a = qb+r$, dan is dus niet $g(r) < g(b)$, ergo r=0. Alle ringelementen zijn dus deelbaar door b, in het bijzonder b zelf. Stellen we b=eb, dan volgt ae=qbe=qb=a voor willekeurige a, d.w.z. e is éénelement.

4.5.3. De deling met rest wordt zowel bij de natuurlijke getallen als bij de veeltermen gebruikt om de g.g.d. van twee elementen op te sporen en dat gaat analoog bij Euclidische ringen (Euclidische algorithmus, daarnaar is de ring genoemd). Neem maar twee elementen a en b, $\neq 0$, en laat $g(a) \geqq g(b)$ zijn. Stel

$a = q_1 b + r_1$	$g(r_1) < g(b)$
$b = q_2 r_1 + r_2$	$g(r_2) < g(r_1)$
$r_1 = q_3 r_2 + r_3$	$g(r_3) < g(r_2)$
---	---

Daar de rij der g's daalt, komt er eenmaal een eind doordat de deling opgaat, stel bij $r_{n-2} = q_n r_{n-1}$ (eventueel $r_{-1} = a$ en $r_o = b$ gesteld). Dus is r_{n-1} deler van r_{n-2}, maar wegens $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$ ook van r_{n-3} en, zo teruggaande, tenslotte van b en van a. Net als eerder (in II,2.3) laat men zien, dat elke rest lineair in a en b is uit te drukken; er zijn dus elementen c en d met $r_{n-1} = ca+db$. Daaruit blijkt dat elke gemene deler van a en b ook deler van r_{n-1} is, r_{n-1} is dus een g.g.d.

4.5.4. De voorwaarde $g(ab) \geqq g(a)$ is in het voorgaande niet gebruikt. Hier volgen enkele conclusies er uit.

a) Alle eenheden hebben dezelfde g als e. Stel maar dat $\varepsilon\varepsilon' = e$, dan is $g(e) = g(\varepsilon\varepsilon') \geqq g(\varepsilon) = g(\varepsilon e) \geqq g(e)$, dus $g(\varepsilon) = g(e)$.

b) e heeft de kleinste g, want voor willekeurige $a \neq 0$ is $g(a) = g(ae) \geqq g(e)$.

c) Is $g(a) = g(e)$, dan is a een eenheid. Stel $e = qa + r$. Is dan $r \neq 0$, dan is tegelijk $g(r) < g(a) = g(e)$ en volgens b) $g(r) \geqq g(e)$. Dus is $r = 0$ en a/e of: a is een eenheid.

d) Geassocieerde elementen hebben dezelfde g, want $g(a\varepsilon) \geqq g(a) = g(a\varepsilon, \varepsilon') \geqq g(a\varepsilon)$, dus $g(a\varepsilon) = g(a)$.

e) Is $g(ab) = g(a)$, dan is b een eenheid.

Stellen we $a = q.ab + r$, dan is a/r, dus $g(a) \leqq g(r)$, maar meteen $g(r) < g(ab) = g(a)$, een tegenspraak dus als $r \neq 0$. Dus is r=0 en $a = qab$ of $e=qb$ en b is een eenheid.

Wanneer dus b geen eenheid is, is $g(ab) > g(a)$, of ook: $g(a) > g(b)$, wanneer b een echte deler van a is.

4.5.5. Stelling: Een Euclidische ring is een factorontbindingsring.

Het bewijs loopt net als bij de natuurlijke getallen (zie 4.4). Eerst wordt bewezen, dat er voor het element $a \neq 0$ een ontbinding in priemfactoren bestaat. Is a priem, dan levert a zelf de ontbinding (in één factor), zo niet, dan zijn er echte delers b en c met a=bc. Volgens het slot van 4.5.4 zijn de g's van b en c kleiner dan die van a, het proces der successieve ontbinding loopt dus in een eindig aantal stappen af.

Het eenduidig zijn der ontbinding volgt weer uit de ook hier geldende stelling, dat uit $p \mid ab$ en $p \nmid a$ volgt $p \mid b$, als p een priemelement is. Uit $p \nmid a$ volgt dat p en a een g.g.d. e hebben en dat er dus elementen s en t zijn met $e = sa + tp$. Hieruit volgt $eb = sab + tpb$ en daaruit $p \mid b$.

Opmerking: In 10.4 zullen we deze stelling nog eens bewijzen, maar dan zonder van de voorwaarde $g(ab) \geqq g(a)$ gebruik te maken.

4.5.6. De gehele getallen van Gauss (d.w.z. de complexe getallen a+bi met gehele a en b) vormen een Euclidische ring. Dat ze een integriteitsgebied vormen is gemakkelijk in te zien.

Is $\alpha = a+bi$ een willekeurig complex getal, dan heet het getal a^2+b^2 zijn norm $N(\alpha)$. Men komt er net zo aan als in $C[\sqrt{5}]$ (zie 4.3), het is namelijk de komende noemer in de herleiding $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$. Ook hier geldt $N(\alpha\beta) = N(\alpha).N(\beta)$, maar verder is hier $N(\alpha) = 0$ dan en alleen dan als $\alpha=0$ en $N(\alpha) > 0$, als $\alpha \neq 0$.

Voor de gehele getallen van Gauss nemen we nu $g(\alpha) = N(\alpha)$, aan de voorwaarde $g(\alpha\beta) \geqq g(\alpha)$ is dus alvast voldaan. Blijft te bewijzen, dat bij elk tweetal gehele getallen van Gauss $\alpha = a+bi$ en $\beta = c+di \neq 0$ er nog twee, γ en ρ, te vinden zijn met

$$\alpha = \gamma\beta + \rho \text{ , waarin ôf } \rho = 0, \text{ ôf } N(\rho) < N(\beta).$$

Daartoe delen we α door β :

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{-ad+bc}{c^2+d^2}\,i, \text{ stel } p+qi.$$

Zijn p en q geheel, dan gaat de deling op, $\gamma = p+qi$ en $\rho=0$. Zijn p en q niet beide geheel, dan kiezen we de gehele getallen m en n zo dicht mogelijk bij p resp. q, er geldt dus $|m-p| \leqq \frac{1}{2}$ en $|n-q| \leqq \frac{1}{2}$.

We kiezen nu $\gamma = m+ni$, dan wordt $\rho = \alpha - \gamma\beta = (c+di)(p+qi) - (m+ni)(c+di)$

$= \{(p-m)+(q-n)i\}\,(c+di)$,

dus $N(\rho) = N\{(p-m) + (q-n)i\}\,.N(c+di)$

$= \{(p-m)^2 + (q-n)^2\}\,N(\beta)$

$\leqq \{(\frac{1}{2})^2 + (\frac{1}{2})^2\}\,N(\beta) = \frac{1}{2}N(\beta) < N(\beta)$.

Opmerkingen: 1) Het kan gebeuren, dat $|p-m|$ of $|q-n|$ precies $\frac{1}{2}$ is, er is dan voor m resp. n keuze uit twee waarden. De deling met rest is in dit integriteitsgebied dus niet eenduidig.

2) Uit het bewezene volgt, dat twee gehele getallen van Gauss (die $\neq 0$ zijn) een g.g.d. hebben, dat er priemelementen onder voorkomen en dat er voor elk geheel getal van Gauss $\neq 0$ precies één ontbinding in eindig veel priemfactoren bestaat.

5. Lichamen

5.1. De meeste in de vorige paragraaf ingevoerde begrippen verliezen hun zin, althans hun belang, als in de ring de deling (behalve door nul) onbeperkt uitvoerbaar is. In dat geval heet de ring een lichaam; is de vermenigvuldiging commutatief, dan een commutatief lichaam. Meestal wordt van een lichaam verondersteld dat het minstens één element $\neq 0$ bezit.

Voor de vermenigvuldiging gelden dus de postulaten:

1^{o}) ze is associatief,

2^{o}) de vergelijkingen $ax = b$ en $xa = b$ zijn oplosbaar, als $a \neq 0$.

Maar dat zijn de postulaten van een multiplicatieve groep. Er volgt:

a) een lichaam heeft een éénelement;

b) elk element $\neq 0$ heeft precies één inverse (al die elementen zijn dus eenheden);

c) de wortels der vergelijkingen $ax = b$ en $xa = b$ zijn resp. $a^{-1}b$ en ba^{-1}, ze zijn eenduidig bepaald en in geval van commutativiteit gelijk (ze kunnen dan als "quotiënt" $\frac{b}{a}$ worden geschreven);

d) is $b=0$, dan zijn die wortels 0, een lichaam heeft dus geen nuldelers; daaruit volgt weer de vereenvoudigingswet: uit $ab = ac$ volgt $b = c$, als $a \neq 0$;

e) een commutatief lichaam is een integriteitsgebied.

5.2. Voorbeelden van een commutatief lichaam zijn de verzamelingen van de rationale, de reële, en de complexe getallen. In I, 3.4 werden als verdere voorbeelden nog genoemd C_7 (in het algemeen C_p met p priem) en de verzameling der even elementen van C_{10}.

Een eindig lichaam met p elementen (p priem) is isomorf met C_p. De additieve groep is immers cyclisch en kan door het éénelement e worden voortgebracht, de elementen van het lichaam zijn dus O, e, 2e,...,(p-1)e. Beelden we af $qe \to q \in C_p$ (q=0,1,...,p-1) dan blijft de optelling uiteraard behouden, maar ook de vermenigvuldiging, want $q_1e.q_2e =$ ... $(e+e+...+e)(e+e+...+e) = q_1q_2e \to q_1q_2$. Beide worden analoog modulo p gereduceerd.

Op dezelfde wijze als in I, 3.4.3 met C_7 gebeurde, kan men bewijzen, dat elk eindig integriteitsgebied een lichaam is. Noem de elementen $a_1, a_2, \ldots, a_n$. Is $a \neq O$ er één van, dan zijn de producten $aa_1, aa_2, \ldots, aa_n$ alle verschillend, want uit $aa_i = aa_j$ zou volgen $a_i = a_j$. Het volle integriteitsgebied staat er dus weer. Kiezen we een willekeurig element b, dan is er dus een element a_i, dat wortel is van de vergelijking ax=b.

5.3. Wordt een lichaam K homomorf afgebeeld op een ring R', dan zoeken we het volledig origineel van het nulelement O' van R'. Bevat dat een element $a \neq O$ van K en is b een willekeurig element van K, dan bezit K een element c met b = ac, zodat f(b) = f(ac) = O'c' = O', m.a.w. elk element van K heeft het beeld O'.

Voor een lichaam zijn er dus maar twee algebraïsch verschillende homomorfe afbeeldingen mogelijk, namelijk de isomorfe (waarbij de kern alleen de nul van het lichaam bevat) en de afbeelding op de nulring.

6. Deelringen en deellichamen

6.1. Een deelverzameling van een ring heeft een deelring, als ze ten aanzien van de bewerkingen van de ring zelf een ring is.

Evenzo kan een lichaam een deellichaam hebben, een deelverzameling dus die bij dezelfde bewerkingen zelf een lichaam is.

Deelring en deellichaam zijn natuurlijk ondergroepen van de additieve groep, ze bevatten dus het nulelement van de omvattende ring.

Het deellichaam is ook ondergroep van de multiplicatieve groep van het omvattende lichaam, dat is de verzameling van de elementen $\neq O$. Een deellichaam bevat derhalve het éénelement van het omvattende lichaam. Voor een deelring van een ring behoeft dat niet te gelden, ook al heeft die ring een éénelement, zo is de ring der even getallen een deelring van de ring der gehele getallen.

6.2. Als kenmerk voor een ondergroep noemden we in II, 3.1:

a) de deelverzameling is gesloten voor de groepbewerking;

b) de deelverzameling bevat met elk element ook de inverse daarvan.

Deze twee voorwaarden zijn tot de volgende ene samen te vatten:

de deelverzameling bevat met de elementen a en b ook ab^{-1}. Immers: bevat de deelverzameling de elementen a en b, dan ook $aa^{-1} = e$, dus ook $ea^{-1} = a^{-1}$, en ook $a(b^{-1})^{-1} = ab$.

Voor een additief geschreven groep luidt de voorwaarde, dat de deelverzameling met a en b ook a-b bevat.

6.3. We willen hier nu het korte kenmerk gebruiken, het moet gelden voor de deelring ten aanzien van de additieve groep van de ring, voor het deellichaam ten aanzien van beide groepen van het lichaam. Voor de deelring moet nog gelden, dat hij voor de vermenigvuldiging gesloten is. Alzo: een deelverzameling van een ring is een deelring, als ze met de elementen a en b ook de elementen a-b en ab bevat; en: een deelverzameling van een lichaam is een deellichaam als ze met de elementen a en b ook de elementen a-b en ab^{-1} (als $b \neq 0$) bevat.

Een lichaam, dat geen niet-triviale deellichamen bezit, heet een priemlichaam.

6.4. Bezit een lichaam K een commutatieve deelring R, dan liggen de wortels $b^{-1}a$ en ab^{-1} van de vergelijkingen $bx = a$ resp. $xb = a$ (met a en $b \in R$ en $b \neq 0$) in K. Uit $ab = ba$ volgt (door voor- en navermenigvuldigigen met b^{-1}) dat deze wortels gelijk zijn en dus als eenduidig quotiënt $\frac{a}{b}$ geschreven kunnen worden. Voor zulke quotiënten geldt: $\frac{a}{b} = \frac{c}{d}$, dan en alleen dan, als $ad = bc$. Het "alleen dan" volgt uit de overlegging $\frac{a}{b} = \frac{c}{d} \rightarrow bd\frac{a}{b} = bd\frac{c}{d} \rightarrow da = bc$; het "dan" uit: $ad = bc \rightarrow ad(bd)^{-1} = (bd)^{-1}bc \rightarrow add^{-1}b^{-1} = d^{-1}b^{-1}bc \rightarrow ab^{-1} = d^{-1}c$.

We bekijken nu de deelverzameling Q van deze quotiënten nader. Ze blijkt voor de bewerkingen gesloten, want $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ en $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, beide te bewijzen door telkens linker- en rechterlid met bd te vermenigvuldigen en te bedenken, dat uit $bdx = bdy$ volgt $x = y$. De tegengestelde van

$\frac{a}{b}$ is $\frac{-a}{b}$, de inverse (als $a \neq 0$) $\frac{b}{a}$, beide behoren tot Q. Q is dus een commutatief deellichaam van K, men noemt het het quotiëntenlichaam van R. Q omvat R, want, zijn a en b ($b \neq 0$) elementen van R, dan volgt $a = \frac{ab}{b} \in Q$. Is R al een lichaam, dan valt Q met R samen.

6.5. R zij een ring zonder nuldelers en met éénelement, de karakteristiek (2.7) noemen we p.

Is $p \neq 0$, dan vormen de natuurlijke veelvouden $e, 2e, \ldots, (p-1)e$, $pe = 0$ van het éénelement e een deelring van R. Zijn immers me en ne er twee van, dan is $me-ne = (m-n)e$ en $me \cdot ne = (e+e+\ldots+e)(e+e+\ldots+e) = (mn)e$ en in deze uitkomsten kunnen de coëfficiënten modulo p worden gereduceerd, die uitkomsten behoren dus tot de neergeschreven veelvouden. Kennelijk is de deelring $\cong C_p$, hij is dus zelfs een lichaam.

Is p=0, dan kan men analoog de deelring

$$\ldots\ldots, -2e, -e, 0, e, 2e, \ldots\ldots$$

vormen, isomorf met C.

Was R een lichaam, dan kan men in het geval $p \neq 0$ de gevonden deelring een deellichaam noemen en in het geval $p = 0$ hem tot zijn quotiëntenlichaam aanvullen door toevoeging van de quotiënten $\frac{me}{ne}$ ($n \neq 0$). Dit quotiëntenlichaam is isomorf met het lichaam der rationale getallen (afbeelding $\frac{me}{ne} \rightarrow \frac{m}{n}$).

In beide gevallen is het gevonden deellichaam een priemlichaam. Elk lichaam dat het lichaam R omvat en ook elk deellichaam van R heeft dit priemlichaam tot deellichaam. Al die lichamen hebben dus ook dezelfde karakteristiek.

7. Quotiëntenlichaam

7.1. Als de commutatieve ring zonder nuldelers R niet al deelring is van een lichaam kan men zijn quotiëntenlichaam construeren als het "kleinste" lichaam, waarin hij als deelring kan worden "ingebed" en dat alle quotiënten van alle paren ringelementen (deler $\neq 0$) bevat.

Het te volgen procédé is hetzelfde dat bij de uitbreiding van het getalbegrip gebruikt wordt om van de gehele getallen tot de rationale te komen. Het zal dus bekend zijn en kan hier schetsmatig worden aangegeven.

Om te beginnen vormen we alle geordende paren (a,b) $(b \neq 0)$ van ringelementen ("geordend" wil zeggen, dat (a,b) een ander paar is dan (b,a) als $a \neq b$). Bij de volgende definities houde men in het oog, dat (a,b) straks het quotiënt $\frac{a}{b}$ zal moeten voorstellen, schrijft men dat er even voor, dan wordt alles vanzelfsprekend.

Allereerst betekene de relatie $(a,b) \sim (c,d)$, dat $ad = bc$. Ze is reflexief, symmetrisch en transitief (uit $(a,b) \sim (c,d)$ en $(c,d) \sim (e,f)$ volgt $ad = bc$ en $cf = de$, dus $adf = bcf = bde$, dan $d \neq 0$ wegstrepen!). Ze is dus een equivalentie.

We definiëren nu

$$(a,b) + (c,d) = (ad + bc, bd) \text{ en } (a,b)(c,d) = (ac,bd).$$

Wegens $bd \neq 0$ is de verzameling der paren voor deze bewerkingen gesloten. Verder kan men narekenen dat de equivalentie tegen de bewerkingen bestand is, ze is dus een congruentie (I, 4.3). De verzameling valt dus uiteen in de restklassen naar die congruentie en daarmee kan men rekenen door middel van representanten. Geven we de klasse waartoe een paar behoort even aan door daar een streep boven te zetten, dan betekent dat dat

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a,b) + (c,d)} \text{ en } \overline{(a,b)}\,\overline{(c,d)} = \overline{(a,b)(c,d)}.$$

De verzameling van deze klassen is nu het gezochte quotiëntenlichaam, we kunnen de elementen dus wel als quotiënten of breuken schrijven, d.w.z. $\overline{(a,b)}$ als $\frac{a}{b}$. Dan komen de bekende rekenregels

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{en} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Er moeten dus nog drie dingen bewezen worden, namelijk, dat de verzameling een commutatief lichaam is, dat R daarin kan worden ingebed en dat $\frac{a}{b}$ dan wortel is van de vergelijking $bx = a$.

7.2. Voor het eerste moet men narekenen, of optelling en vermenigvuldiging wel associatief en commutatief zijn en of de vermenigvuldiging wel distributief is ten opzichte van de optelling. We laten dat maar achterwege. Dan moeten er een nul- en éénelement zijn, elk element moet een tegengestelde hebben en elk element $\neq 0$ een inverse.

Nul is $\frac{0}{a}$ met willekeurige $a \neq 0$. De paren $(0,a)$ vormen inderdaad een klasse, want $(0,a) \sim (0,b)$ en als $(0,a) \sim (b,c)$ dan is $ab = 0.c = 0$, dus $b = 0$. Dat die klasse nulelement is volgt uit $\frac{b}{c} + \frac{0}{a} = \frac{ab}{ac} = \frac{b}{c}$ (want $(ab,ac) \sim (b,c)$).

Eénelement is $\frac{a}{a}$ met willekeurige $a \neq 0$. Ook de paren (a,a) vormen een klasse, want $(a,a) \sim (b,b)$ en als $(a,a) \sim (b,c)$ volgt, dat $ac = ab$ dus $c = b$. Dat die klasse éénelement is blijkt uit $\frac{b}{c} \cdot \frac{a}{a} = \frac{ba}{ca} = \frac{b}{c}$.

De tegengestelde $-\frac{a}{b}$ van $\frac{a}{b}$ is $\frac{-a}{b}$, want $\frac{a}{b} + \frac{-a}{b} = \frac{0}{b^2}$. De inverse van $\frac{a}{b}$ is $\frac{b}{a}$ (alleen als $\frac{a}{b} \neq \frac{0}{b}$, dus als $a \neq 0$, is er sprake van een inverse), want $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab}$.

7.3. Nu moet worden bewezen dat de oorspronkelijke ring R in het geconstrueerde lichaam (noem het Q') kan worden "ingebed". Daarmee wordt bedoeld dat Q' een deelring R' bevat, die isomorf is met R. Van algebraïsch standpunt zijn isomorfe ringen niet te onderscheiden, het "inbedden" kan dus met de vaststelling van de isomorfie afgelopen zijn. Men identificeert eenvoudig elk element van R met zijn beeld in R'. Wil men het onderscheid tussen R en R' handhaven, dan kan men elk element van R' door zijn origineel in R vervangen, Q' gaat daardoor over in de verzameling Q. Daarin worden de bewerkingen door de volgende afspraak vastgelegd: alle bewerkingen, waarbij geen element van R optreedt, worden uitgevoerd als in Q', treedt er wel een element van R op, dan wordt het eerst door zijn beeld in R' vervangen. De uitkomst wordt dus in Q' bepaald; komt hij niet in R' voor, dan blijft hij staan; is hij element van R', dan wordt hij vervangen door zijn origineel in R.

7.4. De in 7.3 bedoelde isomorfe afbeelding is $a \rightarrow \frac{ac}{c}$, c willekeurig $\neq 0$ (inderdaad is $(ac,c) \sim (ad,d)$, $\frac{ac}{c}$ geeft dus eenduidig een klasse aan; verder volgt uit $(ac,c) \sim (bc,c)$ dat $ac^2 = bc^2$ dus $a = b$, de afbeelding is dus éénéénduidig).

Dat deze afbeelding isomorf is, blijkt voor de optelling uit:

$$a+b \rightarrow \frac{(a+b)c}{c} \quad \text{en} \quad \frac{ac}{c} + \frac{bc}{c} = \frac{ac^2+bc^2}{c^2} = \frac{(a+b)c^2}{c^2} = \frac{(a+b)c}{c} .$$

Voor de vermenigvuldiging uit: $ab \rightarrow \frac{abc}{c}$ en $\frac{ac}{c} \cdot \frac{bc}{c} = \frac{abc^2}{c^2} = \frac{abc}{c}$.

Dat het nu te construeren lichaam Q inderdaad alle quotiënten van R-elementen bevat, blijkt daaruit, dat de vergelijking $bx = a$ $(b \neq 0)$ de oplossing $\frac{a}{b}$ heeft, immers $b \cdot \frac{a}{b}$ $(= \frac{bc}{c} \cdot \frac{a}{b} = \frac{abc}{bc})$ $= a$. Q is deellichaam van alle lichamen, die R en al die quotiënten bevatten (dus hun doorsnee), daarom heette het "het kleinste". Is R zelf al een lichaam, dan valt Q' samen met R', dus Q met R. Immers het willekeurige element $\frac{a}{b}$ van Q' heeft in R het origineel c met de eigenschap $bc = a$ $(c \rightarrow \frac{bc}{b} = \frac{a}{b})$.

8. Idealen

8.1. Bij de groepen is gebleken (II,b): bij elke congruentie in de groep is een normaaldeler te vinden, zodanig dat de indeling van de groep in nevenklassen samenvalt met de indeling in congruentieklassen en omgekeerd. Deze klassen vormen een groep, die homomorf beeld is van de oorspronkelijke en omgekeerd is bij elke homomorfe afbeelding van de groep een normaaldeler te vinden, zodanig dat de beeldgroep isomorf is met de factorgroep naar die normaaldeler.

We willen nu onderzoeken in hoeverre zo'n verband tussen congruenties, homomorfieën en zekere deelverzamelingen ook bij ringen bestaat.

8.2. Laat in de ring R een congruentie gegeven zijn, we kunnen dan door middel van representanten rekenen met de restklassen naar die congruentie. Beelden we nu een ringelement af op de klasse waartoe het behoort, dan is die afbeelding "eenduidig op" en de bewerkingen blijven duidelijk behouden, omdat we bij optelling of vermenigvuldiging van twee klassen juist de originelen als representanten kunnen kiezen. De afbeelding is dus homomorf.

Laat nu een homomorfe afbeelding van R op een ring R' gegeven zijn, we vormen dan de volledige originelen van de elementen van R' (zie 3.4). Daarmee is R in klassen ingedeeld, het tot dezelfde klasse behoren is een equivalentie in R. Die equivalentie is bestand tegen de bewerkingen, want, vervangen we in een som of product van elementen van R een element

door een equivalent element, dan verandert er aan som of product van de beelden in R' niets en de uitkomsten in R liggen dus in dezelfde klasse. De equivalentie is dus een congruentie, men kan met de klassen door middel van representanten rekenen, ze vormen een ring, die homomorf beeld is van R en isomorf beeld van R'. Van R worden daarbij de elementen afgebeeld op de klasse waartoe ze behoren, van R' op hun volledige originelen.

8.3. In 3.4 werd in het bijzonder het volledige origineel I beschouwd van het nulelement O' van R'. I heet de kern van de homomorfie. In de ring van klassen treedt I op als nulelement.

Gaan we van de congruentie uit, dan kunnen we I definiëren als de klasse, die het nulelement van R bevat. Er werd bewezen, dat de klasse waarin het element a van R ligt aan te duiden is als I+a, d.w.z. dat ze bestaat uit alle elementen i+a met $i \in I$, of ook, dat twee elementen a en b dan en alleen dan in dezelfde klasse liggen als $a-b \in I$. In het bijzonder volgt uit $a \in I$ en $b \in I$, dat $a-b \in I$. Verder geldt, als r een willekeurig element van R is, dat $ra \in I$ en $ar \in I$, als $a \in I$; het beeld van ra en ar in R' is immers O'.

Hieruit blijkt dat I een deelring van R is (kenmerk in 6.3).

8.4. Een deelverzameling I van de ring R die de laatst genoemde twee eigenschappen bezit, namelijk:

1^{o}. uit $a \in I$ en $b \in I$ volgt $a-b \in I$;

2^{o}. uit $a \in I$ en $r \in R$ volgt $ar \in I$ en $ra \in I$,

heet een ideaal van R.

In 8.3 werd dus bewezen, dat de kern van een homomorfie een ideaal is, wij willen nu omgekeerd aantonen, dat elk ideaal kern van een homomorfie is. Daartoe vormen we de nevenklassen I+r (r willekeurig $\in$ R) van I in de additieve groep van R. Het behoren tot dezelfde nevenklasse is in R een equivalentie en in de additieve groep van R zelfs een congruentie. Om te bewijzen dat het ook in R een congruentie is moet worden aangetoond dat het bestand is tegen de vermenigvuldiging. Laat daartoe $r' \in I+r$ en $s' \in I+s$, dan kunnen we stellen $r' = i_1+r$, $s'=i_2+s$, dus $r's' = i_1i_2 + i_1s + ri_2 + rs$. Van het rechterlid behoren de eerste drie termen,

dus ook hun som, tot I, zodat r's' $\in$ I+rs.

Daarmee is het bewijs geleverd, er volgt, dat de nevenklassen een ring vormen, homomorf met R en dat I de kern van de homomorfie is.

Het ideaalbegrip hoort dus in de ring op dezelfde wijze bij congruentie en homomorfie als in de groep de normaaldeler.

We noemen de klassen I+r de restklassen naar I, liggen twee elementen a en b in dezelfde restklasse, dan heten ze congruent modulo I, in teken a $\equiv$ b (mod.I). De door de restklassen gevormde ring heet de restklassenring R/I (van R naar I).

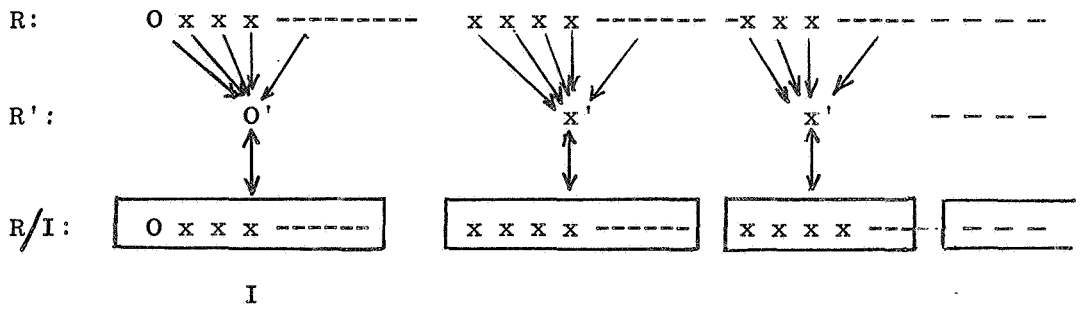
8.5. Samenvatting van het bewezene

I. Voor elk ideaal I van R vormen de restklassen een ring R/I, waarin I het nulelement is en die homomorf blijkt met R, als we de elementen van R afbeelden op de restklassen, waartoe ze behoren. Het tot dezelfde restklasse behoren is een congruentie in R, de restklassen naar die congruentie vallen uiteraard samen met de restklassen naar I.

II. Bij elke congruentie in R is de restklasse waarin het nulelement van R ligt een ideaal van R, de restklassen naar dat ideaal vallen samen met de restklassen naar die congruentie.

III. Bij elke homomorfe afbeelding van R op een ring R' is het volledige origineel van het nulelement van R' een ideaal I van R, de restklassen van I in R vallen samen met de volledige originelen van de elementen van R' en de restklassenring R/I blijkt isomorf met R' als de elementen van R' op hun volledige originelen worden afgebeeld.

Het volgende schema kan punt III verduidelijken:



(Men kan ook R en R' als groepen en I als een normaaldeler opvatten).

8.6. Triviale idealen zijn de ring zelf en het nulelement, als deelring beschouwd. De ring, als ideaal opgevat, is het enige element in zijn restklassenring, die is dus isomorf met de nulring. De nul heeft als ideaal de ring zelf als restklassenring, elk element vormt op zichzelf een restklasse; het nulideaal is dus kern van een isomorfie.

In 5.3 werd bewezen, dat er voor een lichaam maar twee homomorfe afbeeldingen mogelijk zijn, namelijk de isomorfe en de afbeelding op de nulring. Een lichaam heeft dus ook geen andere idealen dan de twee genoemde triviale.

8.7. Een niet-lege deelverzameling I van de ring R met de eigenschappen

1^{o}) uit $a \in I$ en $b \in I$ volgt $a-b \in I$;

2^{o}) uit $a \in I$ en $r \in R$ volgt $ra \in I$,

heet een <u>linksideaal</u> van R; laat men bij 2^{o} volgen $ar \in I$, dan een <u>rechtsideaal</u>.

Een gewoon ideaal is dus zowel links- als rechtsideaal, het heet ter onderscheiding wel <u>tweezijdig ideaal</u>. In commutatieve ringen vervalt het onderscheid.

Links- en rechtsidealen zijn weer deelringen van R.

9. <u>Voortbrenging van idealen in commutatieve ringen</u>

9.1. Een ideaal van een commutatieve ring R bevat met het element a ook de elementen $a+a = 2a$, $a+a+a = 3a, \ldots$, de elementen $-a, -a-a = 2(-a)$, $-a-a-a = 3(-a), \ldots$, die we schrijven als $-1.a$, $-2a$, $-3a, \ldots$ en tenslotte het element $0.a = 0$. Met elkaar noemen we ze de "natuurlijke veelvouden van a en we vatten ze samen als na (n willekeurig getal).

Daarnaast bevat het ideaal de "ringveelvouden" ra van a (r is een willekeurig element van R) en verder nog de elementen na + ra; in deze uitdrukking zijn de twee soorten veelvouden (voor n=0, resp. r=0) ook vertegenwoordigd.

Omgekeerd vormen de elementen na + ra al een ideaal I van R. Men zegt dat I door a wordt "voortgebracht" en schrijft $I = (a)$. Het is het "kleinste" ideaal dat a bevat.

Heeft R een éénelement, dan kan de eerste term vervallen. We kunnen namelijk dan n(ea) schrijven in plaats van na. Is n positief, dan volgt n(ea) = ea+ea+...+ea = (e+e+...+e)a = (ne)a, hierin is ne een ringelement, zodat beide termen kunnen worden samengenomen. Voor n=O staat de eerste term er niet en het geval n < O kan gemakkelijk tot het positieve geval worden teruggebracht. Ook de elementen ra vormen al een ideaal. Heeft R een éénelement, dan valt het samen met het vorige, is dat niet het geval, dan bevat het eerste ideaal a als element, het tweede misschien niet. Een voorbeeld geeft de ring van de even getallen. Het door 2 voortgebrachte ideaal (2) bestaat uit de getallen n.2 + 2m.2 en is dus ring zelf (daar de ringelementen nu ook gehele getallen zijn, was de tweede term overbodig). Het tweede ideaal bestaat alleen uit de getallen 2m.2, dat zijn de viervouden.

Op het eerste gezicht lijkt de beperking tot commutatieve ringen onnodig, men kan licht denken dat in een willekeurige ring de elementen na + ra + as ook een ideaal vormen. Maar het rechtsproduct (na+ra+as)t = = nat+ rat + ast met een willekeurig element t is dan niet van de voorgeschreven vorm, de middelste term rat is niet (algemeen) tot één der drie voorgeschreven producttypen te herleiden.

Men kan ook door meer dan één element een ideaal van een commutatieve ring laten voortbrengen: onder het door de elementen $a_1, a_2, \ldots, a_m$ voortgebrachte ideaal $(a_1, a_2, \ldots, a_m)$ verstaat men dan de verzameling der elementen

$$n_1a_1 + n_2a_2 + \ldots + n_ma_m + r_1a_1 + r_2a_2 + \ldots + r_ma_m.$$

Een door één element voortgebracht ideaal heet een <u>hoofdideaal</u>. Het "nulideaal" is een hoofdideaal, het wordt door de nul voortgebracht, bestaat alleen uit de nul en kan als (O) geschreven worden. Heeft de ring een éénelement e, dan brengt dat de ring voort, men kan hem dus schrijven als (e).

9.2. In een integriteitsgebied bestaat het hoofdideaal (a) uit de elementen ra, dus uit de ringveelvouden van a. Vallen de hoofdidealen (a) en (b) $\neq$ O samen, dan zijn a en b geassociëerd en omgekeerd.

Bewijs: 1^{o}) Vallen (a) en (b) samen, dan zijn er elementen r en s met $b = ra$ en $a = sb$, dus $b = rsb$ of $rs = e$. Dus zijn r en s eenheden en a en b zijn geassocieerd.
2^{o}) Zijn a en b geassocieerd, dan is a veelvoud van b en b van a, dus $(a) \subset (b)$ en $(b) \subset (a)$, dus $(a) = (b)$. Is a een echte deler van b, dan is (b) een echte deelverzameling van (a) (en zelfs een ideaal van (a)).

9.3. Voorbeelden van idealen

9.3.1. In de ring der gehele getallen C bestaat het ideaal (m) uit de m-vouden. De restklassen naar dit ideaal zijn de restklassen modulo m (die we dus ook restklassen modulo (m) kunnen noemen) en $C/(m) = C_{|m|}$ ($C_o \cong C$ en $C_p = (0)$ gesteld).

9.3.2. Zouden we proberen een ideaal van C door twee elementen te doen voortbrengen, dan brengt dat niets nieuws. Immers geldt $a \in (d)$ en $b \in (d)$, als d de g.g.d. van a en b is (ze zijn er immers veelvouden van), dus $(a,b) \subset (d)$. Anderzijds zijn er gehele getallen m en n met $d = ma + nb$ (bewezen in II,2.3), zodat $d \in (a,b)$ en dus $(d) \subset (a,b)$. Er volgt $(a,b) = (d)$.

In feite zijn alle idealen van C hoofdidealen. Laat maar een ideaal I de elementen a en b bevatten en dus het door hun g.g.d. d voortgebrachte hoofdideaal (d). Bevat I een element c, dat geen veelvoud is van d, dus niet in (d) ligt, dan zoeken we de g.g.d. d_1 van d en c, en a,b en c liggen in het ideaal $(d_1) \subset I$.

Is er nog een element f in I, dat niet in (d_1) ligt, dan geeft dat aanleiding tot het meer omvattende ideaal (d_2), d_2 is de g.g.d. van d_1 en f. Daar deze d's voortdurend afnemen (we kiezen ze positief) komt er aan dit proces een eind; we stuiten op een d_i met $(d_i) = I$.

9.3.3. De restklassenring C_p (p priem) is een lichaam, heeft dus geen andere idealen dan de triviale. Is q in C_q niet priem, dan kunnen we om dezelfde reden als voor C geen andere dan hoofdidealen verwachten. Is voor de rest a de g.g.d. met q gelijk 1, dan zijn er gehele getallen m en n met $ma + nq = 1$ en dan geldt $(a) = C_q$. Voor C_6 krijgen we de idealen (0) en $(1) = (5) = C_6$ en verder $(2) = (4) = \{0,2,4\}$ (restklasse $\{1,3,5\}$) en $(3) = \{0,3\}$ (restklassen $\{1,4\}$ en $\{2,5\}$).

9.3.4. De getallen $\frac{m}{n}$ (m en n geheel en onderling ondeelbaar, $n \neq 0$ en onderling ondeelbaar met het priemgetal p) vormen een ring. Dat zou een deelring zijn van de ring der rationale getallen, we hoeven dus slechts het kenmerk daarvoor te controleren (6.3). Inderdaad kan in de uitkomsten van $\frac{m_1}{n_1} - \frac{m_2}{n_2}$ en $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}$ de p niet in de noemer komen.

Bij een niet-triviaal ideaal van deze ring bevatten de tellers der breuken minstens één factor p. Stel maar dat in $\frac{m}{n}$ m niet door p deelbaar is, dan hoort $\frac{n}{m}$ ook tot de ring en dus $\frac{n}{m} \cdot \frac{m}{n} = 1$ tot het ideaal. Maar dan valt dat met de ring samen.

Stel nu, dat k het kleinste aantal factoren p is, dat in de teller van enige breuk van het ideaal voorkomt en stel de betreffende breuk $\frac{p^k m}{n}$. Dan bevat het ideaal ook $\frac{n}{m} \cdot \frac{p^k m}{n} + p^k$ en daarmee het ideaal (p^k). Daarmee valt het ook samen, want is b.v. $\frac{p^l m}{n}$ een willekeurig element (m onderling ondeelbaar met p), dan is $l \geqq k$ en dus $\frac{p^l m}{n} = \frac{p^{l-k} m}{n} \cdot p^k$. Alle niet-triviale idealen van de ring zijn dus van de vorm (p^k) met $k \geqq 1$. Daar p element van de ring is, komen ook alle idealen van deze vorm voor.

10. Hoofdideaalringen.

10.1. Definitie. Een integriteitsgebied heet hoofdideaalring, als elk zijner idealen hoofdideaal is.

Daar een integriteitsgebied commutatief is en een éénelement bezit bestaat het ideaal (a) uit de ring-veelvouden van a.

In 9.3.2 werd bewezen, dat C hoofdideaalring is; ook de ring in 9.3.4 was er een. Een lichaam heeft slechts de idealen (o) en (e); dat zijn hoofdidealen, een lichaam is dus een hoofdideaalring.

10.2. Stelling. Een Euclidische ring is een hoofdideaalring.
Bewijs: Laat I een ideaal van de Euclidische ring R zijn (4.5.) Is I het nulideaal, dan is I hoofdideaal. Heeft I elementen $\neq 0$, dan kiezen we het element i zo, dat g(i) minimaal is. Is $k \neq 0$ een tweede element van I, dan bestaan er elementen q en r van R, zodanig dat $k=qi + r$, hierin is $r=0$ of $g(r) < g(i)$. Maar $r=k-qi$ en behoort dus tot I, dus is $r = 0$, omdat g(i) minimaal was. Er volgt $k = qi$; elk element van I is dus veelvoud van i en $I = (i)$, dus hoofdideaal.

10.3. Twee stellingen.

10.3.1. Elk paar elementen a en b $\neq 0$ van een hoofdideaalring heeft een grootste gemene deler d. De ring bevat elementen r en s, zodanig dat $d = ra + sb$.
Bewijs. Het ideaal (a,b) is hoofdideaal en dus te schrijven als (d), a en b zijn veelvouden van d, dus d is gemene deler van a en b. Daar $d \in (a,b)$ zijn er ringelementen r en s met $d = ra = sb$. Daaruit blijkt, dat elke gemene deler van a en b deler van d is, dus is d g.g.d.

10.3.2. Zijn a en b elementen en is p priemelement van een hoofdideaalring, dan volgt uit p/ab dat p/a of p/b.
Bewijs. Stel $p \nmid a$, dan is het éénelement e een g.g.d. van p en a. Er zijn dus elementen r en s met $e = rp + sa$, dus $b = rp\,b + sa\,b$. Hierin is het rechterlid deelbaar door p, dus ook het linkerlid.

10.4. Stelling; Een hoofdideaalring is een factorontbindingsring (4.4).

Bewijs. Uit 10.3.2. volgt al, dat, wanneer van een element een eindige priemfactorontbinding gevonden is, deze (op eenheden na) uniek is.

Blijft te bewijzen, dat voor een element $\neq 0$ een ontbinding in eindig veel priemfactoren mogelijk is. Zou dat voor het element a niet mogelijk zijn, dan zou a een echte deler a_1 hebben, die weer een echte deler a_2 had, enzovoort; er zou dus een oneindige rij elementen $a, a_1, a_2, \text{--------}$ bestaan, waarvan elke term echte deler van de vorige was. Dat betekent een oneindige rij idealen $(a), (a_1), (a_2), \text{--------}$, waarvan elk echt deel van alle volgende zou zijn (9.2, slot). Nu is de vereniging van al deze idealen zelf een ideaal en dus een hoofdideaal. Zijn namelijk p en q willekeurige elementen van die vereniging, dan liggen ze elk in één der (a)'s, b.v. $p \in a_i$ en $q \in a_j$ met $i \leqq j$. Maar dan geldt ook $p \in a_j$ en daarmee zijn ook p-q en rp (r is een willekeurig ringelement) elementen van a_j en dus van de vereniging . Is d het voortbrengend element van de vereniging, dan is d zelf daarvan element, er is dus een ideaal (a_n) in de rij met $d \in (a_n)$. Maar dat houdt in dat (a_n) al de vereniging zelf is, m.a.w. er is geen sprake van een oneindige rij idealen, waarvan elk echt deel van het volgende is.

Volgens 10.2 is dus in het bijzonder een Euclidische ring een factorontbindingsring. Dat was al in 4.9 bewezen, maar ditmaal is geen gebruik gemaakt van de voorwaarde $g(ab) \geqq g(a)$.

10.5. Stelling.

10.5.1. De te bewijzen stelling luidt:

Is p element van een hoofdideaalring R, dan is de restklassenring R/(p) dan en slechts dan een lichaam, als p een priemelement van R is.

Het bewijs valt uiteen in twee delen.

1°) Gegeven: p is priem. Te bewijzen: R/(p) is een lichaam.

Bewijs: We hebben slechts aan te tonen:

a) R/(p) heeft geen nuldelers.

b) elk element van R/(p), dat $\neq (p)$ is, heeft een inverse.

a) Stel dat a en $b \in R$ en dat a en b niet tot (p) behoren, dat wil dus zeggen $p \nmid a$ en $p \nmid b$.

Zouden de restklassen (p) + a en (p) + b complementaire nuldelers zijn, dan zou ab $\in$ (p) of p/ab, maar daaruit zou volgen p/a of p/b.
b) Neem de restklasse (p) + a met a $\notin$ (p), dus p$\not/$ a. De g.g.d. van a en p is e. Volgens 10.3.1. bevat R dan elementen r en s met ra + sp = e, waaruit volgt, dat ra in dezelfde restklasse ligt als e. Maar die is het éénelement van de restklassenring, dus is de restklasse (p) + r de inverse van (p) + a.
2^{o}) Gegeven: R/(p) is een lichaam. Te bewijzen: p is priem.
Bewijs: Er zijn geen nuldelers in R/(p). Dat houdt in: uit ab $\in$ (p) volgt a $\in$ (p) of b $\in$ (p). Of: uit p/ab volgt p/a of p/b.

Had p nu de niet-trivale ontbinding p_1p_2, dan zou wel gelden p/p_1p_2, maar niet p/p_1 of p/p_2. Dat is een tegenspraak, dus is p priemelement.
10.5.2. Uit deze stelling volgt nog eens, dat de restklassenring $C/(m) \cong C_m$ een lichaam is, dan en alleen dan als m een priemgetal is.
We ontlenen nog een voorbeeld aan de ring $C[i]$ van de gehele getallen van Gauss a + bi met gehele a en b. Daarin is 2 + i een priemelement, want de norm $2^2+1^2 = 5$ is niet anders dan trivaal te ontbinden. Dus is de ring $C[i]/(2+i)$ een lichaam.

Het is duidelijk, dat een getal a + bi tot het ideaal (2+i) behoort, als a en b vijfvouden zijn, want 2+i/5. Representanten van de restklassen hoeven we dus slechts te zoeken onder de getallen a+bi met a en b = 0,1,2,3,4. Is a + bi zo'n representant, dan is a + bi - b (2+i) = a-2b een representant van dezelfde restklasse en die kan weer modulo 5 worden gereduceerd tot één der getallen 0,1,2,3,4. Daaruit blijkt, dat 0,1,2,3 en 4 een volledig stel representanten vormen en dat $C[i]/(2+i) \cong C_5$.

11. Veeltermringen.

In de resterende paragrafen van dit hoofdstuk beperken we ons tot commutatieve ringen.

11.1. Zijn $a_o, a_1, \ldots, a_n$ elementen van een commutatieve ring R, dan heet de uitdrukking

$$f(x) = a_o x^o + a_1 x^1 + a_2 x^2 + \ldots\ldots + a_n x^n$$

een "veelterm" of "polynoom" "in x" "over R"; x heet een "onbepaalde" (in plaats van x^1 mag ook x geschreven worden).

De gewone veeltermterminologie geldt; we stippen alleen aan, dat we $a_n x^n$ de "hoogste term" en a_n de "hoogste coëfficiënt" noemen, verder dat n de graad van het polynoom heet ("echt", als $a_n \neq 0$), behalve in het geval van de veelterm $0.x^0$, waaraan geen graad wordt toegekend.

Twee polynomen heten dan en slechts dan gelijk als ze uit dezelfde termen bestaan, toevoeging of weglating van termen met coëfficiënt nul wordt verondersteld het polynoom ook gelijk te laten. Daarom geeft men een veelterm ook wel oneindig veel termen, slechts een eindig aantal daarvan heeft dan een coëfficiënt $\neq 0$.

11.2. De onbepaalde x is een leeg symbool. Ze stelt niets voor en is alleen gebonden aan zekere regels, die het mogelijk maken met x in verbinding met de elementen van R te rekenen. Behouden- in enkele later te noemen gevallen treedt x alleen in zijn (formeel op te vatten) machten met niet - negatieve exponent op en die komen alleen voor in de formele productverbinding ax^k met een coëfficiënt a uit R. De machten x^n en x^m worden als verschillend beschouwd als $n \neq m$.

Het is mogelijk nu de regels op te sommen, waaraan het rekenen met x gehoorzamen moet om de bekende bewerkingen met veeltermen:

$$\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k = \sum_{k=0}^{n} (a_k + b_k)\, x^k$$

en $$\sum_{k=0}^{m} a_k x^k \cdot \sum_{k=0}^{n} b_k x^k = \sum_{k=0}^{m+n} c_k x^k \quad \text{met } c_k = a_o b_k + a_1 b_{k-1} + \ldots$$

$$\ldots + a_k b_o$$

te kunnen bewijzen. (Bij de optelling hebben we de veeltermen gelijke graad gegeven door eventueel de veelterm met de laagste graad met nultermen aan te vullen; bij de vermenigvuldiging moeten in de uitdrukking voor c_k voor eventueel ontbrekende coëfficiënten a_i of b_j nullen gedacht worden).

Men kan ook deze bewerkingen met veeltermen per definitie stellen en daaruit de rekenregels voor x afleiden. Natuurlijk is dat slechts een

formele bezigheid, we noemen slechts, dat a en x^k in het product ax^k verwisselbaar zijn, dat $ax^k + bx^k = (a+b)x^k$ en dat $ax^m . bx^n = ab\,x^{m+n}$.

Ten slotte: hebben we twee veeltermen ongelijke ("echte") graad, dan is de graad van hun som gelijk aan de hoogste van die twee, zijn de graden gelijk, dan kan de graad van de som (als hij er is) wel lager zijn. De graad van een product is hoogstens gelijk aan de som van de graden der factoren, als de beide hoogste coëfficiënten complementaire nuldelers zijn is hij lager (als hij er is). Heeft R geen nuldelers, dan is die graad steeds gelijk aan die som. Ook hier zijn echte graden bedoeld.

11.3. Men wil wel zo geloven dat de polynomen in x over R een ring vormen; hij wordt aangeduid met $R[x]$. Uit de commutativiteit van R volgt die van $R[x]$.

Voor de veeltermen ax^o en bx^o geldt dat $ax^o + bx^o = (a+b)x^o$ en $ax^o.bx^o = abx^o$. De afbeelding $a \rightarrow ax^o$ is blijkbaar een isomorfe, m.a.w. R kan in $R[x]$ worden ingebed (zie 7.3). Veelal gaat men daarbij zo ver, dat men in $R[x]$ ax^o door a vervangt, R is dan werkelijk een deelring van $R[x]$. Daardoor geldt dan nu dat $0.x^k = 0$.

Bevat R nuldelers, dan dus $R[x]$ ook, heeft R geen nuldelers, dan $R[x]$ ook niet, want als de hoogste coëfficiënten van twee veeltermen $\neq 0$ zijn, is de hoogste coëfficiënt van hun product dat ook. Is tenslotte R een integriteitsgebied, dan $R[x]$ ook.

Heeft R een éénelement e,dan volgt $ex^k.ex^l = ex^{k+l}$, of in het bijzonder $(ex)^k = ex^k$. We maken geen fouten als we in zulke termen de coëfficiënt weglaten. Dat houdt in, dat we dan (en alleen dan) x en zijn machten als veeltermen en dus als elementen van $R[x]$ kunnen beschouwen. Het ligt voor de hand in dat geval ook $x^o = e$ te stellen.
$R[x]$ is nooit een lichaam, want geen enkele veelterm, die x werkelijk bevat, heeft een inverse, als R geen nuldelers bevat, x kan dan niet "wegvermenigvuldigd" worden. Eventuele eenheden van $R[x]$ zullen dus onder de elementen van R gezocht moeten worden. Heeft R geen nuldelers, dan kunnen we natuurlijk wel het quotiëntenlichaam van $R[x]$ vormen. Het bestaat uit de breuken met veeltermen als teller en noemer en wordt aangeduid met R(x).

11.4. Bij het rekenen met veeltermen komt het alleen op de coëfficiënten aan. Daarom kan men bij het vormen van de veeltermring over R het gebruik van de x wel vermijden en een veelterm opvatten als een geordend n-tal elementen van R: $(a_o,a_1,\ldots,a_n)$, men kan desgewenst a_n ook door een oneindig aantal nullen laten volgen. Som en product van twee zulke verzamelingen worden dan analoog aan zo even gedefinieërd. Heeft R een éénelement, dan kan men x ook opvatten als het paar (0,e), x^2 als (0,0,e) enz.

11.5. De polynoomring $R[x_1]$ kan door het invoeren van een tweede onbepaalde x_2 uitgebreid worden tot $R[x_1][x_2]$. We nemen aan, dat x_1 en x_2 met elkaar verwisseld mogen worden. Het is dan duidelijk dat $R[x_1][x_2] = R[x_2][x_1]$. We schrijven beide als $R[x_1,x_2]$.

Analoog krijgen we bij successieve invoering van de onbepaalden $x_1,x_2,\ldots,x_n$ de polynoomring $R[x_1,x_2,\ldots,x_n]$.

12. Deling en ontbinding in veeltermringen.

12.1.1. Is R een integriteitsgebied dan gaat veel van het bekende veeltermrekenen door in $R[x]$. We willen eerst eens de mogelijkheid nagaan van de z.g. "staartdeling". Is a_nx^n de hoogste term van f(x) en $_mx^m$ die van g(x), terwijl $n \geq m$, dan zal $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m}g(x)$ (de "eerste rest" van de deling) inderdaad een graad hebben $\leq n-1$ en de algoritme zal bij verdere voortzetting werkelijk uitlopen op de bepaling van quotiënt q(x) en de rest r(x) met $f(x) = q(x)g(x)+r(x)$, waarbij $r(x)=0$ is of een graad heeft, kleiner dan of gelijk aan die van g(x).
Slechts is te veronderstellen, dat het quotiënt $\frac{a_n}{b_m}$ en alle verdere analoog optredende quotiënten in R bestaan. Zal dus de staartdeling onbeperkt mogelijk zijn, dan is het nodig (en voldoende) dat R een lichaam is.

In dat geval is $R[x]$ een Euclidische ring, voor het getal g(f) nemen we de graad van f. Inderdaad is zo tevens voldaan aan de tweede voorwaarde, namelijk, dat $g(f_1f_2) \geq g(f_1)$.

$R[x]$ is als Euclidische ring tevens hoofdideaalring en factorontbindingsring.

12.1.2. Natuurlijk is het mogelijk, dat het quotiënt $\frac{a_n}{b_m}$ en de volgende bij de staartdeling optredende quotiënten in R bestaan, ook als R geen lichaam is. Dat dat zich voor kan doen is duidelijk, men kan immers van g(x), r(x) en q(x) uitgaan en f(x) bijpassend construeren. De staartdeling is steeds mogelijk, als de hoogste coëfficiënt van g(x) een eenheid is.

12.1.3. Is R een integriteitsgebied en geldt, dat $f(x)= q(x)g(x)+r(x)$, waarbij $r(x) = 0$, of een lager graad heeft dan g(x), dan zijn q(x) en r(x) door f(x) en g(x) eenduidig bepaald. Is immers

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

dan volgt $$(q_1 - q_2)\, g = r_2 - r_1.$$

Is $q_1 \neq q_2$, dan heeft het linkerlid minstens de graad van g, de graad van het rechterlid is minder dan die van g. Dus is $q_1 = q_2$ en dus $r_1=r_2$.

12.2.1. We willen het ontbinden van veeltermen nu nader onderzoeken en veronderstellen daarbij, dat R een factorontbindingsring is, elk paar elementen heeft dan een g.g.d. Er zijn zeker veeltermen, die onontbindbaar zijn, daartoe behoren alvast de lineaire ax + b met (a,b) = e.

We gaan bewijzen, dat $R[x]$ ook een factorontbindingsring is. Daartoe halen we het quotiëntenlichaam Q en R er bij, in 12.1.1 is bewezen, dat $Q[x]$ een factorontbindingsring is. Nu is een veelterm f(x) uit $R[x]$ er ook een in $Q[x]$ en daarin dus te ontbinden. Het zal blijken, dat daarmee meteen een ontbinding in $R[x]$ gevonden is.

12.2.2. Willen we een veelterm $f(x) = a_o + a_1 x + \ldots + a_n x^n$ uit $R[x]$ in factoren ontbinden, dan kunnen we beginnen met naar gemene delers van de coëfficiënten a_i te zoeken. Is a hun g.g.d., dan stellen we $f(x) = a f^*(x)$, de coëfficiënten van $f^*(x)$ hebben g.g.d. e. Zo'n veelterm heet primitief (t.o.v. R). Alle g.g.d.'s van de coëfficiënten a_i zijn geassocieerd, f^* is dus door f op een eenheidsfactor na bepaald.

12.2.3. Voor twee (of meer) primitieve veeltermen geldt de stelling (van Gauss), dat hun product ook primitief is. Laat maar $f^*(x) = a_o + a_1 x + \ldots + a_n x^n$ en $g^*(x) = b_o + b_1 x + \ldots + b_m x^m$ twee primitieve veeltermen zijn. Zou nu het product $f^* g^*$ niet primitief zijn, dan zouden

zijn

coëfficiënten een priemfactor p (geen eenheid) gemeenschappelijk hebben, die niet in alle a's en evenmin in alle b's zat. Is, van a_o afgerekend, a_i de eerste coëfficiënt van f^* die niet deelbaar is door p en evenzo b_j de eerste in $g,^*$ dan bekijken we de (i+j) -de coëfficiënten in f^*g^*, namelijk

$$(a_o b_{i+j}+\ldots.+a_{i-1}b_{j+1}) + a_i b_j + (a_{i+1}b_{j-1}+\ldots.+a_{i+j}b_o).$$

De tussen haakjes geplaatste termen zijn alle door p deelbaar, de hele coëfficiënt ook, dus $a_i b_j$ eveneens. Maar uit $p/a_i b_j$ volgt (in een factorontbindingsring!) dat p/a_i of p/b_j, in tegenspraak met de veronderstelling.

12.2.4. Is nu Q het quotiëntenlichaam van R en is $\varphi(x) = \alpha_o + \alpha_1 x + \ldots + \alpha_n x^n$ een veelterm uit $Q[x]$, dan kan men de coëfficiënten α_i schrijven als breuken van elementen van R. Brengen we die alle onder dezelfde noemer b, dan is $\varphi(x)$ te schrijven als een breuk met noemer b, terwijl de teller een veelterm uit $R[x]$ is. Die is dan weer te herleiden tot de vorm $a\,F^*(x)$ met F^* primitief $\in R[x]$.
Er komt dan $\varphi(x) = \frac{a}{b}\ F^*(x)$.

Een met $\varphi(x)$ (in $Q[x]$) geassocieerde veelterm $\psi(x) = \frac{r}{s}\ \varphi(x)$ (r en $s \in R$) is evenzo te herleiden tot de vorm $\psi(x) = \frac{c}{d}\ G^*(x)$. Er volgt

$$\frac{c}{d}\ G^*(x) = \frac{r}{s}\,\frac{a}{b}\ F^*(x) \text{ of } s\,bc\,G^*(x) = r\,ad\,f^*(x).$$

We zijn nu weer geheel in $R[x]$, volgens 12.2.2 zijn de veeltermen F^* en G^* in $R[x]$ geassocieerd.
Saamgevat: In $Q[x]$ geassocieerde veeltermen zijn te schrijven als het product van een element van Q en een primitieve veelterm uit $R[x]$, die tot op een eenheidsfactor bepaald is.

12.2.5. Neem nu een primitieve veelterm $f^*(x)$ uit $R[x]$ met graad ≥ 1, hij is ook veelterm in $Q[x]$. Is $f^*(x)$ in $Q[x]$ onontbindbaar, dan ook in $R[x]$, zijn priemfactorontbinding is dan gevonden. Is $f^*(x)$ in $Q[x]$ ontbindbaar, is b.v. $f^*(x) = \varphi_1(x)\,\varphi_2(x)$, dan kunnen we stellen

$$\varphi_1 = \frac{a_1}{b_1}\ F_1^*, \quad \varphi_2 = \frac{a_2}{b_2}\ F_2^*,$$

hierin zijn de a's en b's elementen van R en F_1^* en F_2^* primitieve veel-

termen uit $R[x]$.

Er volgt $$f^* = \frac{a_1 a_2}{b_1 b_2} F_1^* F_2^* ,$$

dus $$b_1 b_2 f^* = a_1 a_2 F_1^* F_2^* ,$$

Het product $F_1^* F_2^*$ is primitief t.o.v. R, er is dus een eenheid ε in R, zodanig dat $f^* = F_1^* F_2^*$. Hadden we in plaats van φ_1 en φ_2 daarmee (in $Q[x]$ geassocieerde veeltermen genomen, dan had dat volgens 12.2.4 tot dezelfde ontbinding van G^* geleid. Dit resultaat is gemakkelijk uit te breiden tot n factoren $f^* = \varphi_1 \varphi_2 \ldots \varphi_n$, er zijn dan een eenheid ε en n primitieve veeltermen F_i^* in $R[x]$ met $f^* = \varepsilon F_1^* F_2^* \ldots F_n^*$.

Is in het bijzonder $\varphi_1 \varphi_2 \ldots \varphi_n$ de van f^* in $Q[x]$ bestaande ontbinding in priemfactoren, dan is $\varepsilon F_1^* F_2^* \ldots F_n^*$ er een van f^* in $R[x]$. Dat er geen tweede is, die zich essentieel hiervan onderscheidt, is duidelijk, het zou immers ook een tweede in $Q[x]$ zijn. Gaan we nu nog in $f(x) = af^*(x)$ de factor a in priemfactoren ontbinden, dan is van $f(x)$ in $R[x]$ de (op eenheden na) eenduidige priemfactorontbinding gevonden.

Dus: is R een factorontbindingsring, dan $R[x]$ ook. Volledige inductie levert het bewijs voor dezelfde eigenschap van $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

13. Gehele rationale functies.

13.1.1. Is $f(x) = a_o + a_1 x \ldots + a_n x^n$ een veelterm uit $R[x]$, dan kan men x door een element van R vervangen, dus α substitueren. De producten $a_i \alpha^i$ zijn elementen van R, evenals hun som, die we $f(\alpha)$ stellen.
Iets algemener gesteld: we kunnen α kiezen uit een ring S die R omvat (dus eventueel ook met R kan samenvallen), $f(\alpha)$ is dan een element van S.

Het polynoom $f(x)$ treedt in dit verband op als een voor elk element van S ("op S") gedefinieerde functie, d.w.z. een eenduidige afbeelding van S in zichzelf; x is nu een gewone variabele. Zo'n functie heet een gehele rationale functie.

13.1.2. In de analyse (waarin de veeltermen over het lichaam der reële getallen beschouwd worden) worden veelterm en functie vereenzelvigd, de algebra maakt onderscheidt en stelt daarbij de als formele rekengrootheid gedefiniëerde veelterm primair. De noodzaak van dit onderscheid zit in de verschillende gelijkheidsdefinities: twee veeltermen heten gelijk, als ze (afgezien van termen met coëfficiënt nul) term voor term overeenstemmen, twee functies, als ze voor elk element van S dezelfde waarde hebben. Het verschil van twee gelijke functies heeft voor elke $\alpha \in S$ de waarde nul en het komt in eindige ringen uiteraard voor, dat andere veeltermen dan de nulveelterm de "nulfunctie" voorstellen. Zo levert b.v. in $S = R = C_4$ de functie $x(x-1)(x-2)(x-3)$ bij elke mogelijke substitutie de uitkomst nul, toch is deze veelterm niet de nulveelterm.

Op C_2 zijn in totaal maar 4 functies te definiëren, er zijn immers maar 2 elementen als argumentwaarde en als functiewaarde beschikbaar. Men kan ze alle vier als gehele rationale functies opvatten, de veeltermen 0, 1, x en x+1 stellen die voor.

13.1.3. Zijn f(x) en g(x) twee veeltermen uit $R[x]$ en vat men die op als op S gedefiniëerde functies, dan is het duidelijk, dat het geen verschil maakt, of men een substitutie $x = \alpha$ uitvoert voordat of nadat men f en g bij elkaar heeft opgeteld of met elkaar heeft vermenigvuldigd. Het rekenen met $f(\alpha)$ en $g(\alpha)$ loopt dus geheel analoog met dat met f(x) en g(x), het doet er niet toe, of men f en g daarbij opvat als veeltermen dan wel als functies. De verzameling der gehele rationale functies is dus ook een ring en wel een ring, waarop de veeltermring $R[x]$ homomorf kan worden afgebeeld; telkens wordt daarbij een veelterm afgebeeld op de er door bepaalde functie. De kern van deze homomorfie wordt gevormd door de veeltermen, die de nulfunctie tot beeld hebben, dus de veeltermen f(x), waarvoor $f(\alpha) = 0$ voor elke $\alpha \in S$.

13.2.1. We nemen aan, dat R een integriteitsgebied is en f(x) een veelterm over R. Nu is volgens 12.1.2 de staartdeling mogelijk van f(x) door x-a (a willekeurig $\in R$), dat wil zeggen: er is een element r van R en een veelterm q(x) van $R[x]$, zodanig dat $f(x) = q(x)(x-a)+r$. Er volgt $f(a) = r$, de gewone reststelling dus. Ook het gevolg geldt: is $f(a) = 0$,

dan is f(x) deelbaar door x-a (en omgekeerd). Is f(a) = 0, dan zullen we a een "wortel" van f(x) noemen.

Verder geldt: zijn $a_1, a_2, \ldots, a_k$ verschillende wortels van f(x), dan is f(x) deelbaar door $(x-a_1)(x-a_2)\ldots(x-a_k)$, door volledige inductie gemakkelijk te bewijzen. Voor k=1 geldt de stelling, stel dus $f(x) = (x-a_1) \ldots (x-a_{k-1})\, g(x)$. Substitutie $x=a_k$ levert $0 = (a_k-a_1) \ldots (a_k-a_{k-1})\, g(a_k)$, waaruit volgt dat $g(a_k) = 0$ (geen nuldelers!), dus $x-a_k/g(x)$. Daaruit volgt nu weer, dat f(x) hoogstens n wortels heeft, als de graad n is. Bijgevolg zal in een oneindig integriteitsgebied R alleen de nulveelterm een nulfunctie leveren, in dat geval is dus de ring der veeltermen over R isomorf met de ring der op R gedefiniëerde gehele rationale functies en behoeven we tussen veeltermen en gehele rationale functies niet meer te onderscheiden.

13.2.2. Voor het bewijs van de reststelling behoefde R geen integriteitsgebied te zijn, de aanwezigheid van nuldelers verstoort het bewijs niet. Maar er moet een éénelement zijn, anders heeft x-a geen zin. Bij het bewijs van de tweede stelling in 13.2.1 is echter een beroep gedaan op de afwezigheid van nuldelers, die stelling geldt dan ook niet bij een ring met nuldelers. Zo heeft b.v. de veelterm 4x over C_8 de wortels 0,2,4 en 6. Inderdaad is $4x = 4(x-2) = 4(x-4) = 4(x-6)$, dus 4x is door elk der veeltermen x-2, x-4, x-6 deelbaar, echter niet door hun product.

13.3. We besluiten deze paragraaf met enkele voorbeelen betreffende de ringen C en C_n.

Allereerst merken we op, dat het voor het rekenen met veeltermen (of gehele rationale functies) in C_n niets uitmaakt, of men de coëfficiënten opvat als gehele getallen, dan wel als (representanten van) elementen van C_n. Is namelijk nx^k bedoeld als natuurlijk veelvoud van x^k (is dus n een natuurlijk getal), dan verandert er bij het rekenen (c.q. substitueren)niets, als men schrijft nex^k (waarin e het éénelement van C_n voorstelt). Maar ne = 0, bij het rekenen mogen dus alle coëfficiënten, hun sommen en producten modulo n gereduceerd worden.

Hieruit volgt dat de ontbinding in $C[x]$ van een veelterm over C meteen een ontbinding in $C_n[x]$ is van dezelfde veelterm over C_n, de

veelterm stelt voor elke n het product van de factoren voor. Is omgekeerd een veelterm voor enige n in $C_n[x]$ onontbindbaar, dan ook in $C[x]$.

Zo is de veelterm $x^3+6x^2+11x + 8$ in $C_2[x]$ te reduceren tot $x^3+x = x(x^2+1)$, dus ontbindbaar, in $C_3[x]$ is hij echter onontbindbaar. Hij zou immers een lineaire factor, dus een wortel moeten hebben en men overtuigt zich gemakkelijk (reduceer tot x^3+2x+2), dat dat niet het geval is. De veelterm is dus ook in $C[x]$ onontbindbaar.

De veelterm $x^4 + 8x^3 + x^2 + 2x + 5$ is in $C_2[x]$ gelijk aan $x^4 + x^2 + 1$. Hij heeft daar geen wortel, dus ook geen lineaire factor, die bezit hij dus evenmin in $C[x]$. Echter is in $C_2[x]$ $x^4 + x^2 + 1 = (x^2 + x + 1)^2$, kwadratische factoren zijn er dus wel.

In $C_3[x]$ is de veelterm te reduceren tot $x^4 + 2x^3 + x^2 +2x + 2$, hij blijkt daar de wortel 2 te hebben, de bijpassende ontbinding luidt $(x + 1)(x^3 + x^2 + 2)$. Voor verdere ontbindbaarheid zou $x^3 + x^2 + 2$ nu weer een lineaire factor, dus een wortel moeten hebben, die is echter niet aanwezig. De veel-term heeft dus in $C_3[x]$ geen kwadratische priemfactor, dus evenmin in $C[x]$. In $C[x]$ is hij bijgevolg onontbindbaar.

14. Idealen en veeltermringen.

14.1.1. We geven nog enkele voorbeelden van idealen in veeltermringen en kiezen hier die idealen uit $C[x]$, dus de ring der veeltermen met gehele getalcoëfficiënten.

Allereerst bewijzen we dat $C[x]$ geen hoofdideaalring is; het komt dus voor, dat een factorontbindingsring geen hoofdideaalring is.

Ten bewijze beschouwen we het ideaal (x,3). Was het hoofdideaal, dan zou $C[x]$ een veelterm φ bevatten, die deelbaar was op x en op 3. Uit het laatste volgt $\varphi = \pm 1$ of ± 3, we kunnen ons tot 1 en 3 beperken. Nu is $3 \nmid x$, dus zou $\varphi = 1$ zijn en er zouden veeltermen f en g in $C[x]$ zijn met $xf + 3g = 1$. De termen van xf zijn alle van minstens de eerste graad, de constante term van het linkerlid wordt dus geleverd door 3g. Dat zou inhouden 3/1, wat niet waar is. De veelterm φ bestaat dus niet en (x,3) is geen hoofdideaal.

14.1.2. De veeltermen van het ideaal (x,3) zijn de vorm xf + 3g, met f en g willekeurig uit C[x]. Van al die veeltermen is de constante term deelbaar door 3, omgekeerd zijn alle veeltermen met een drievoud tot constante term in deze vorm te schrijven. Dat is dus kenmerkend voor de veeltermen van dit ideaal. Dat twee veeltermen van C[x] in dezelfde restklasse liggen betekent blijkbaar, dat hun constante termen in dezelfde restklasse modulo 3 van C liggen en omgekeerd. Er volgt dus $C[x]/(x,3) \cong C_3$.

14.1.3. Bekijken we het ideaal $(x^2,3x)$ van C[x]. Het bestaat uit de veeltermen $x^2f + 3xg$ met willekeurige f en g uit C[x]. Die hebben alvast geen constante term en de coëfficiënt van de lineaire term is een drievoud. Ook dat is weer kenmerkend, veeltermen uit dezelfde restklasse naar $(x^2,3x)$ hebben dus dezelfde constante term en de coëfficiënten van de lineaire termen liggen in dezelfde restklasse modulo 3 van C. Als representanten van de restklassen kunnen we veeltermen ax + m kiezen, bij het rekenen er mee wordt een eventueel optredende kwadratische term weggelaten, de coëfficiënt van de lineaire term kan modulo 3 worden gereduceerd en de constante term moet blijven staan. Beelden we ax + m af op het paar (a,m) met $a \in C_3$ en $m \in C$, dan is dat een isomorfe afbeelding van $C[x]/(x^2,3x)$ op de verzameling dezer paren, wanneer we daarvoor de volgende bewerkingen vaststellen:
(a,m)+(b,n)=(a + b, m + n); (a,m)(b,n)=(na + mb,mn).
Op die manier kan men zeer gevariëerde ringen opbouwen uit paren (of n-tallen) elementen van verschillende ringen.

14.2.1. Laat R een integriteitsgebied zijn en $\varphi(x)$ een veelterm over R. Als R een lichaam is, wordt aan φ verder geen eis gesteld, is R geen lichaam, dan veronderstellen we dat de hoogste coëfficiënt van φ het éénelement e van R is. Op elk element van R[x] kan dan dus de staartdeling door φ worden toegepast (12.1).

Het ideaal (φ) van R[x] bestaat uit alle veeltermen $f\varphi$ met willekeurige $f \in R[x]$. Twee veeltermen f en g liggen in dezelfde restklasse van φ, als $\varphi/f-g$, dus als f en g bij deling door φ dezelfde rest geven. We kunnen deze resten als representanten van de restklassen

kiezen, heeft φ de graad n, dan zijn ze van de vorm

$$\rho(x) = a_o + a_1 x + \ldots\ldots + a_{n-1}x^{n-1} \quad (a's \in R).$$

Men kan deze vormen ook als nieuwe rekengrootheden opvatten, het rekenvoorschrift luidt dan: optellen en vermenigvuldigen als veeltermen, maar uitkomsten modulo φ tot deze vorm reduceren.

Om ons van de veeltermen te distanciëren, schrijven we ξ in plaats van x, onze rekenelementen zijn dus de uitdrukkingen $\rho(\xi) = a_o + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1}$, hun verzameling noemen we $R[\xi]$. Er geldt $R[x]/(\varphi) \cong R[\xi]$. De afbeelding $\xi \longrightarrow 0$ beeldt de uitdrukking af op a_o, blijkbaar is $R[\xi]$ en dus $R[x]/(\varphi)$ homomorf met R.

14.2.2. We nemen nu aan, dat R een factorontbindingsring is, dan is $R[x]$ het ook (12.2) en $\varphi(x)$ heeft een ontbinding in priemfactoren $\varphi_1 \varphi_2 \ldots \varphi_m$ (bedenk, dat R een lichaam zou zijn of dat $\varphi(x)$ de hoogste coëfficiënt e zou hebben, we hoeven voor dit product dus geen coëfficiënt uit R te zetten). Is m=1, dan is $\varphi = \varphi_1$ onontbindbaar.

Stel nu, dat φ ontbindbaar is, dus $m \geq 2$. Dan is het duidelijk, dat de uitdrukking $\rho(\xi)$ dan en alleen dan nuldeler is, als hij factoren $\varphi_i(\xi)$ bevat, echter niet alle. De complementaire nuldeler bevat de ontbrekende. In dit geval is dus $R[\xi]$ een ring met nuldelers.

Is daarentegen φ onontbindbaar, dus m=1, dan is $R[\xi]$ een integriteitsgebied, er zijn geen nuldelers. Was $\rho_1(\xi)$ er een, dan was b.v. $\rho_1 \rho_2 = 0$, dus $\varphi(x)/\rho_1(x)\ \rho_2(x)$. Maar in een factorontbindingsring volgt dan φ/ρ_1 of φ/φ_2, wat geen van beide het geval is.

Is R een lichaam en φ onontbindbaar, dan is $R[\xi]$ ook een lichaam. Bewijs: Laat $f(\xi)$ een element van $R[\xi]$ zijn ($\neq 0$), f(x) is dan niet door φ deelbaar. In 12.1.1. is bewezen, dat $R[x]$ hoofdideaalring is en uit 10.3.1 volgt dan dat f en φ een g.g.d. hebben en dat $R[x]$ veeltermen s(x) en t(x) bevat, zodanig dat die g.g.d. voor te stellen is als $s(x)\ f(n) + t(x)\ \varphi(x)$. Maar de g.g.d. is e, zodat $s(x)f(x) + t(x)\ \varphi(x) = e$. . Overgang op $R[\xi]$ betekent, dat het linkerlid modulo $\varphi(x)$ gereduceerd wordt, s(x) wordt vervangen door zijn rest r(x) en de tweede term valt weg. Er komt $r(\xi)\ f(\xi) = e$, m.a.w. $r(\xi)$ is de inverse van $f(\xi)$. Dus heeft elke uitdrukking $f(\xi) \neq 0$ een inverse in $R[\xi]$ en

$R[\xi]$ is een lichaam. We schrijven het $R(\xi)$ (haakjes).

14.2.3. R zij weer factorontbindingsring. Het is mogelijk dat in R of in een factorontbindingsring S, die R omvat (we houden het op S en laten S=R toe) een wortel α van $\varphi(x)$ ligt, waarvoor dus $\varphi(\alpha) = 0$. Met de uitdrukkingen $\rho(\alpha)$ wordt nu als het ware automatisch modulo $\varphi(\alpha)$ gerekend, want is b.v. $f(x) = q(x)\,\varphi(x) + \rho(x)$, dan is $f(\alpha) = \rho(\alpha)$.

Is $\varphi(x)$ irreducibel over R, dan is elke andere veelterm $\psi(x)$ over R met $\psi(\alpha) = 0$ deelbaar door $\varphi(x)$. Ze hebben immers in S een wortel α, dus een factor $x-\alpha$ gemeen en hebben dus in $S[x]$ een g.g.d. met graad ≥ 1. Maar die g.g.d. is door successieve delingen te bepalen en die verlopen geheel in $R[x]$, die g.g.d. hebben ze dus daar ook. (Mocht de algorithmus in $R[x]$ of $S[x]$ niet doorgaan, dan loopt de redenering na de veeltermringen over de quotiëntenlichamen van R en S; zie 12.2). Daar φ in $R[x]$ onontbindbaar is, is φ zelf de g.g.d. en φ/ψ. Is in het bijzonder ψ ook irreducibel dan zijn φ en ψ geassocieerd.

Onder $R[\alpha]$ zullen we nu uiteraard de verzameling der uitdrukkingen $\varphi(\alpha)$ verstaan. Er zijn geen gelijke onder, d.w.z. uit $\rho_1(\alpha) = \rho_2(\alpha)$ volgt $\rho_1(x) = \rho_2(x)$, anders was α wortel van een veelterm met lager graad dan φ. Het is duidelijk, dat $R[\alpha] \cong R[\xi]$, het maakt dus algebraisch niets uit, of α zo'n wortel is of niet.

Anders ligt het als φ ontbindbaar is, stel $\varphi = \varphi_1 \varphi_2 \ldots \varphi_m$. Nu volgt uit $\varphi(\alpha) = 0$, dat minstens één der uitdrukkingen $\varphi_i(\alpha) = 0$. De veeltermen $\varphi_i(x)$ zijn priem, is dus $\varphi_i(\alpha) = \varphi_j(\alpha) = 0$, dan zijn φ_i en φ_j volgens het bovenstaande geassociëerd. Is $\varphi_i(\alpha) = 0$, dan stellen we $\varphi_i = \psi$.

Het is duidelijk dat het nu weinig zin heeft het symbool $R[\alpha]$ te handhaven voor de verzameling der uitdrukkingen $\rho(\alpha)$, immers $\rho_1(\alpha) = \rho_2(\alpha)$ als $\rho_1(x) \equiv \rho_2(x) \pmod{\psi}$.

Het symbool $R[\alpha]$ is dan ook gereserveerd voor de opzet, waarbij van ψ uitgegaan wordt, zodat $R[\alpha] \cong R[x]/(\psi)$. In het bijzonder is $R[\alpha]$ een lichaam $R(\alpha)$, als R een lichaam is.

Het symbool $R[\xi]$ kan men bij ontbindbare φ (waarvan ψ een deler is) handhaven. De restveeltermen modulo ψ zijn uit de ρ's (dat zijn de restveeltermen modulo φ) te krijgen door ze verder modulo ψ te reduceren.

Daaruit volgt dat $R[\xi]$ homomorf is met $R[\alpha]$ bij de afbeelding $\xi \to \alpha$.

14.2.4. Voorbeelden.

14.2.4.1. We nemen R=C. Zoals men weet, bezit elke veelterm f(x) over C (met graad ≥ 1) in het lichaam der complete getallen minstens één wortel. Zo is x^2+1 over C irreducibel maar heeft de wortel i; dus is $C[x]/(x^2+1) \cong C[i]$, dat is het integriteitsgebied van de gehele getallen van Gauss a+bi met gehele a en b.

Evenzo is x^2-5 irreducibel en $C[x]/(x^2-5) \cong C[\sqrt{5}]$, het in 4.3 genoemde integriteitsgebied van de getallen $a+b\sqrt{5}$ met gehele a en b.

Ook de veeltermen x en x-3 zijn irreducibel, echter van de eerste graad. De resten $\rho(x)$ zijn dus van de nulde graad, d.w.z. elementen van C. Er volgt

$$C[x]/(x) \cong C[x]/(x-3) \cong C.$$

14.2.4.2. We nemen nu eens een ontbindbare veelterm, b.v. x^2-1. $C[\xi]$ bestaat nu niet uit de uitdrukkingen $\rho(\xi) = a+b\xi$ met gehele a en b, het reduceren van uitkomsten modulo ξ^2-1 kan eenvoudig door daarin $\xi^2=1$ te stellen (immers valt dan in $q(\xi)(\xi^2-1)+\rho(\xi)$ de eerste term weg). Nuldelers van $C[\xi]$ zijn die uitdrukkingen $a+b\xi$, die een factor $\xi-1$ of $\xi+1$ bevatten, dus die, waarin $a=\pm b$ is. De uitdrukking $c+d\xi$ is complementair met deze, dan en alleen dan als $c = \mp d$.

Voor α kunnen we 1 of -1 kiezen, elk is wortel van een lineaire vergelijking. $C[\alpha]$ is dus $C[1]$ of $C[-1]$, beide = C.

14.2.4.3. Als laatste voorbeeld bekijken we x^2+1 in C_7 en in C_5.

In C_7 is x^2+1 irreducibel, want C_7 bevat geen wortel. $C_7[x]/(x^2+1)$ is dus een lichaam, isomorf met het lichaam der uitdrukkingen $a+b\xi$ met $\xi^2+1 = 0$. Het bestaat uit 49 elementen. De inverse van $a+b\xi$ is $\frac{1}{a+b\xi} = \frac{a-b\xi}{a^2-b^2\xi^2} = \frac{a-b\xi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\xi$; de coëfficiënten $\frac{a}{a^2+b^2}$ en $\frac{-b}{a^2+b^2}$ zijn elementen van C_7.

In C_5 is $x^2+1 = (x-2)(x-3)$, $C_5[x]/(x^2+1)$ is een ring met 25 elementen, isomorf met de ring $C_5[\xi]$ der restvormen $a+b\xi$ met $\xi^2+1 = 0$.

Nuldelers in deze ring zijn de uitdrukkingen $a+b\xi$, die deelbaar

zijn door $\xi-2$ of door $\xi-3$, restvormen van tweeërlei soort zijn complementair. Deelbaarheid door $\xi-2$ treedt op voor a=-2b, dus a=3b, de nuldelers zijn

$$3+\xi,\ 1+2\xi,\ 4+3\xi,\ 2+4\xi.$$

Deelbaarheid door $\xi-3$ als a = 2b, dus bij

$$2+\xi,\ 4+2\xi,\ 1+3\xi,\ 3+4\xi.$$

Elke nuldeler van de eerste vier vormt met elke van het tweede viertal een complementair stel.

Voor α kunnen we kiezen tussen $\alpha = 2$ of $\alpha = 3$, in beide gevallen is $C_5[\alpha] = C_5$, omdat de veeltermen x-2 en x-3 lineair zijn.

De afbeeldingen $\xi \to 2$ en $\xi \to 3$ beelden $C_5[\xi]$ homomorf op C_5 af. In het eerste geval worden de eerste vier nuldelers van $C_5[\xi]$ op de nul van C_5 afgebeeld, in het tweede geval die van het tweede viertal.