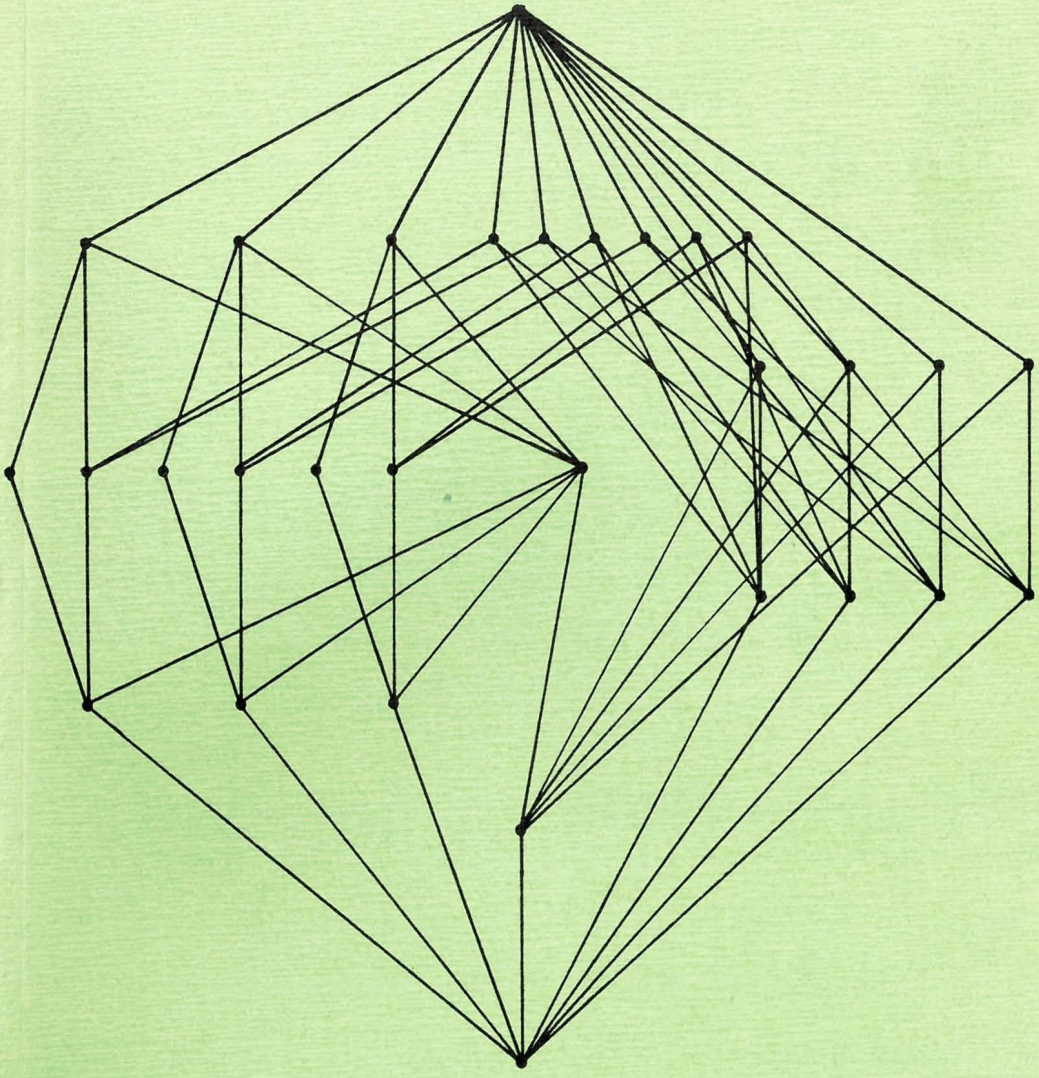
INTEGER VALUED POLYNOMIALS IN ALGEBRAIC NUMBER THEORY



H. ZANTEMA

INTEGER VALUED POLYNOMIALS IN ALGEBRAIC NUMBER THEORY

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR
IN DE WISKUNDE EN NATUURWETENSCHAPPEN
AAN DE UNIVERSITEIT VAN AMSTERDAM
OP GEZAG VAN DE RECTOR MAGNIFICUS DR D. W. BRESTERS
HOOGLERAAR IN DE FACULTEIT DER WISKUNDE EN NATUURWETENSCHAPPEN
IN HET OPENBAAR TE VERDEDIGEN IN DE AULA DER UNIVERSITEIT
(TIJDELIJK IN DE LUTHERSE KERK, INGANG SINGEL 411, HOEK SPUI)
OP WOENSDAG 16 NOVEMBER 1983 DES NAMIDDAGS TE 16.00 UUR

DOOR

HANTSJE ZANTEMA

GEBOREN TE GOINGARIJP, GEMEENTE DONIAWERSTAL

krips repro meppel

PROMOTOR: prof. dr. H. W. Lenstra Jr.

oan myn âlden,

aan Tineke.

VOORWOORD.

Dit proefschrift bestaat uit drie delen en een inleiding. Elk deel is geschreven als tijdschriftartikel; deel I en deel III zijn reeds als zodanig verschenen, en wel in "Manuscripta mathematica", respectievelijk 40 (1982), 155 -203, en 43 (1983), 87 - 106. Deel I, waarvan A. M. Cohen co-auteur is, verschijnt in "Journal für die Reine und Angewandte Mathematik". Deel I vormt de ruggegraat van het proefschrift, de delen II en III zijn er beide door gemotiveerd. In de inleiding wordt getracht het onderwerp van dit proefschrift voor een zo breed mogelijk publiek te belichten.

De afbeelding op het omslag geeft alle ondergroepen van S_4 aan: de punten stellen de ondergroepen voor (S_4 geheel onderaan) en de verbindingslijnen geven inclusies weer. In de laatste paragraaf van deel III speelt deze ondergroepenstructuur van S_4 een belangrijke rol.

Dank ben ik in de eerste plaats verschuldigd aan prof. dr. H. W. Lenstra Jr. voor het aangeven van het onderwerp, vele suggesties tijdens het gehele onderzoek, en het kritisch doornemen van vele voorlopige versies van de tekst. Voorts ben ik de Universiteit van Amsterdam erkentelijk voor het bieden van de nodige faciliteiten om dit onderzoek te verrichten. Tenslotte wil ik dr. A. M. Cohen van het Mathematisch Centrum danken voor zijn essentiële bijdrage aan deel II.

H. Zantema.

INHOUD.

GEHEELWAARDIGE VEELTERMEN IN DE ALGEBRAISCHE GETALTHEORIE.

INLEIDING.

Het is gebruikelijk proefschriften niet alleen te verspreiden onder vakgenoten, maar ook onder familie, vrienden en kennissen. Aangezien proefschriften in de regel nogal gespecialiseerd zijn, komen ze dan dikwijls in handen van mensen die deze specialisatie niet delen. Voor deze mensen kan het frustrerend zijn dat ze een boekwerkje in handen geduwd hebben gekregen waarvan ze - ook na ijverig doorbladeren - geen idee hebben waar het over gaat. De reactie blijft beperkt tot "knap hoor, zo helemaal in het Engels". Vervolgens bergt men het op een veilige plaats op, in de hoop het nooit weer in handen te krijgen.

Het spreekt vanzelf dat dit euvel niet helemaal te verhelpen is; de verdiensten van duizenden jaren beschaving maken het ondoenlijk te allen tijde op niveau nul te beginnen. Toch wil ik een bescheiden poging wagen om ook voor mensen die niet in de zuivere wiskunde gespecialiseerd zijn, het onderwerp van dit proefschrift te belichten. Niemand hoeft zich te schamen om het betoog niet tot het einde te kunnen volgen; tot eventuele toelichting ben ik altijd bereid.

Laten we eens kijken naar de uitdrukking

$$\frac{1}{6}X^3 + \frac{1}{2}X^2 + \frac{1}{3}X + 1.$$

Als we hierin voor X een geheel getal invullen, dat wil zeggen een van de getallen

$$\ldots\ldots -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots$$

dan blijkt de uitkomst steeds weer een geheel getal te zijn. Zo krijgen we bijvoorbeeld

$$\frac{1}{6}.1^3 + \frac{1}{2}.1^2 + \frac{1}{3}.1 + 1 = 2;$$

$$\frac{1}{6}.2^3 + \frac{1}{2}.2^2 + \frac{1}{3}.2 + 1 = 5;$$

$$\frac{1}{6}.3^3 + \frac{1}{2}.3^2 + \frac{1}{3}.3 + 1 = 11;$$

$$\frac{1}{6}.(-37)^3 + \frac{1}{2}.(-37)^2 + \frac{1}{3}.(-37) + 1 = -7769.$$

Een veelterm

$$a_n X^n + a_{n-1} X^{n-1} + \ldots\ldots + a_1 X + a_0$$

met deze eigenschap noemen we een *geheelwaardige veelterm* (Engels: integer valued polynomial).

De structuur van deze geheelwaardige veeltermen is als volgt te beschrijven. De volgende speciale veeltermen blijken alle geheelwaardig te zijn:

$$f_0 = 1,$$

$$f_1 = X,$$

$$f_2 = \frac{X(X-1)}{1.2} = \frac{1}{2}X^2 - \frac{1}{2}X,$$

$$f_3 = \frac{X(X-1)(X-2)}{1.2.3} = \frac{1}{6}X^3 - \frac{1}{2}X^2 + \frac{1}{3}X,$$

$$f_4 = \frac{X(X-1)(X-2)(X-3)}{1.2.3.4} = \frac{1}{24}X^4 - \frac{1}{4}X^3 + \frac{11}{24}X^2 - \frac{1}{4}X,$$

$$\vdots$$

$$f_i = \frac{X(X-1)(X-2)\ldots\ldots(X-i+1)}{1.2.3\ldots\ldots i}.$$

Nu is elke geheelwaardige veelterm hierin uit te drukken; precies gezegd: als

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots\ldots + a_1 X + a_0$$

een willekeurige geheelwaardige veelterm is, dan bestaan er gehele getallen $b_0, b_1, \ldots\ldots, b_n$ met

$$f = b_n f_n + b_{n-1} f_{n-1} + \ldots\ldots + b_1 f_1 + b_0 f_0.$$

Omgekeerd is duidelijk ook elke uitdrukking van deze vorm een geheelwaardige veelterm. Voor ons voorbeeld hebben we

$$\frac{1}{6}X^3 + \frac{1}{2}X^2 + \frac{1}{3}X + 1 = 1.f_3 + 2.f_2 + 1.f_1 + 1.f_0.$$

Het feit dat *alle* geheelwaardige veeltermen op deze manier in f_0, f_1, f_2,..... zijn uit te drukken is al heel lang bekend; het wordt in een paar regels aangetoond in het begin van §2 van deel I van dit proefschrift.

Tot nu toe hebben we stilzwijgend aangenomen dat de coëfficiënten $a_0, a_1, \ldots\ldots, a_n$ van zo'n veelterm f zelf gehele getallen of breuken van gehele getallen zijn. Dit proefschrift handelt over de vraag in hoeverre dit alles uit te breiden is naar grotere getal-

stelsels. Om het begrip geheelwaardige veelterm op een zinvolle manier uit te breiden, moeten we ook het begrip gehele getallen uitbreiden.

Voordat we een dergelijke uitbreiding naar grotere getalstelsels precies kunnen formuleren, moet er eerst wat terminologie ingevoerd worden. Breuken van gehele getallen, dus de getallen r/s waarbij r en s gehele getallen zijn (s niet nul), noemen we *rationale getallen*. De verzameling van alle rationale getallen geven we aan met $\mathbb{Q}$, dat is een verbasterde Q van "quotiënt". Lang niet alle getallen zijn rationaal; een voorbeeld van een niet-rationaal getal is $\sqrt{2}$.

We geven nu een aantal eigenschappen van de rationale getallen. De getallen 0 en 1 zijn rationale getallen. Als we een rationaal getal van een ander aftrekken, of ze optellen, of ze vermenigvuldigen, dan is de uitkomst altijd weer een rationaal getal. Ook als we een rationaal getal delen door een rationaal getal dat niet nul is, is de uitkomst een rationaal getal. Een verzameling met al deze eigenschappen noemen we een *lichaam* (Engels: field); in het bijzonder is $\mathbb{Q}$ dus een lichaam. Er zijn oneindig veel mogelijkheden voor een teller en ook oneindig veel mogelijkheden voor een noemer; zo op het eerste gezicht lijkt $\mathbb{Q}$ wel heel erg groot. Maar in termen van lichamen is $\mathbb{Q}$ juist heel erg klein, binnen de gewone getallen waar je mee rekent is $\mathbb{Q}$ zelfs het kleinste lichaam dat er bestaat.

Bij een *getallenlichaam* moeten we ons nu een lichaam voorstellen dat wel iets groter dan $\mathbb{Q}$ mag zijn, maar niet al te veel groter. Precies gezegd: een lichaam K heet een *getallenlichaam* (Engels: number field) als K tenminste alle rationale getallen bevat en er een *eindig* stel getallen $b_1, b_2, \ldots\ldots, b_n$ in K bestaat zodanig dat elke x uit K uit te drukken is als

$$x = q_1b_1 + q_2b_2 + \ldots\ldots + q_nb_n,$$

waarbij $q_1, q_2, \ldots\ldots, q_n$ rationale getallen zijn. De *graad* van K is het kleinste aantal n waarvoor passende $b_1, b_2, \ldots\ldots, b_n$ te vinden zijn. Zo vormen bijvoorbeeld de getallen van de vorm

$$q_1 + q_2\sqrt{2},$$

waarbij q_1 en q_2 rationale getallen zijn, een getallenlichaam van graad 2. Dit getallenlichaam geven we aan met $\mathbb{Q}(\sqrt{2})$. Verder is $\mathbb{Q}$ zelf ook een getallenlichaam, en wel van graad 1. Ons begrip van geheelwaardige veeltermen zullen we gaan beschouwen over getallenlichamen, dat wil zeggen dat de coëfficiënten $a_0, a_1, \ldots\ldots, a_n$ in een bepaald getallenlichaam bevat zijn.

In getallenlichamen bestaat er een zinvolle uitbreiding van de gehele getallen: een getal b heet *algebraïsch geheel* als er een n, en *gehele* getallen $r_0, r_1, \ldots\ldots, r_{n-1}$ bestaan waarvoor

$$b^n + r_{n-1}b^{n-1} + \ldots\ldots + r_1 b + r_0 = 0.$$

Gehele getallen hebben deze eigenschap: als b een geheel getal is, kies dan n = 1 en $r_0 = -b$. Dus elk geheel getal is algebraïsch geheel. Omgekeerd is elk rationaal getal dat algebraïsch geheel is een geheel getal; stel dat bijvoorbeeld b = 1/3 algebraïsch geheel zou zijn. Dan zou gelden

$$(\tfrac{1}{3})^n + r_{n-1}(\tfrac{1}{3})^{n-1} + \ldots\ldots + r_1.\tfrac{1}{3} + r_0 = 0,$$

oftewel

$$\tfrac{1}{3} = -r_{n-1} - 3.r_{n-2} - 3^2.r_{n-3} \ldots\ldots - 3^{n-1}.r_0.$$

Dit kan niet juist zijn, want rechts van het gelijkteken staat een geheel getal en links niet. Dus 1/3 is niet algebraïsch geheel. Op dezelfde manier kan voor elk rationaal getal dat niet geheel is, worden aangetoond dat het niet algebraïsch geheel is. Dus de algebraïsch gehele getallen in $\mathbb{Q}$ zijn precies de gehele getallen.

Als K een getallenlichaam is, geven we de verzameling van algebraïsch gehele getallen in K aan met $\mathcal{O}(K)$. Zo bestaat dus $\mathcal{O}(\mathbb{Q})$ precies uit de gehele getallen. Er kan bewezen worden dat van twee elementen van $\mathcal{O}(K)$ het verschil en het product ook in $\mathcal{O}(K)$ zit. Een verzameling waarvoor dat geldt wordt een *ring* genoemd. De verzameling $\mathcal{O}(K)$ heet de *ring van gehelen* van K. Als voorbeeld merken we op dat $\mathcal{O}(\mathbb{Q}(\sqrt{2}))$ precies bestaat uit de getallen

$$s + t\sqrt{2},$$

waarbij s en t gehele getallen zijn.

Als K een getallenlichaam is verstaan we onder een *veelterm over* K een uitdrukking

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots\ldots + a_1 X + a_0,$$

waarbij a_0, a_1, ..., a_n in K zitten. Als a_n niet nul is, noemen we n de *graad* van f. Zo hebben de veeltermen f_i over $\mathbb{Q}$ zoals die in het begin van deze inleiding naar voren kwamen, graad i. Een veelterm f over K met de eigenschap dat als men voor X een willekeurig element b van $\mathcal{O}(K)$ invult, de uitkomst f(b) ook weer in $\mathcal{O}(K)$ zit, noemen we een *geheelwaardige veelterm over* K.

Naar analogie van wat we al over geheelwaardige veeltermen over $\mathbb{Q}$ hebben opgemerkt, noemen we K een *Pólyalichaam* als er geheelwaardige veeltermen f_0, f_1, f_2, ... bestaan waarvoor f_i graad i heeft voor i = 0, 1, 2, ..., zodanig dat voor elke n, elke geheelwaardige veelterm f van graad n geschreven kan worden als

$$f = b_n f_n + b_{n-1} f_{n-1} + \ldots\ldots + b_1 f_1 + b_0 f_0,$$

waarbij b_0, b_1, ..., b_n elementen van $\mathcal{O}(K)$ zijn. Zo is $\mathbb{Q}$ dus een Pólyalichaam. Zulke Pólyalichamen zijn voor het eerst bestudeerd door G. Pólya in 1919. Dit proefschrift gaat over getaltheoretische eigenschappen van Pólyalichamen.

De *getaltheorie* bestudeert gehele en rationale getallen. Vele getaltheoretische problemen kunnen echter opgelost worden met behulp van getallenlichamen; dat is juist de reden dat getallenlichamen zijn ingevoerd en worden bestudeerd. Als we bijvoorbeeld willen weten welke getallen geschreven kunnen worden als

$$s^2 - 2t^2,$$

waarbij s en t gehele getallen zijn, kunnen we deze uitdrukking schrijven als

$$(s - t\sqrt{2})(s + t\sqrt{2}),$$

en dan verder binnen $\mathbb{Q}(\sqrt{2})$ rekenen. Hier komen we straks nog op terug. Het vakgebied dat zich bezighoudt met getallenlichamen en getaltheoretische problemen die daarmee samenhangen, heet *algebraische getaltheorie*.

Het lichaam $\mathbb{Q}$ en de bijbehorende ring van gehelen hebben een bijzondere eigenschap: elk geheel getal, behalve nul, is op precies één manier te schrijven als product van priemgetallen, met al of niet een minteken ervoor. Preciezer gezegd: als q een willekeurig geheel getal is, $q \neq 0$, dan is er precies één stel niet-negatieve gehele getallen k(2), k(3), k(5), k(7), k(11), ..., en één getal u met $u = 1$ of $u = -1$, zodanig dat

$$q = u.2^{k(2)}.3^{k(3)}.5^{k(5)}.7^{k(7)}.11^{k(11)} \ldots\ldots .$$

Als een priemgetal p geen deler is van q moeten we hierin $k(p) = 0$ nemen. Omdat $p^0 = 1$, kunnen we dan de factor $p^{k(p)}$ gewoon weglaten in bovenstaande ontbinding van q. Op die manier blijven er eindig veel factoren over, en is de uitdrukking zinvol.

Voor willekeurige *rationale* getallen q, $q \neq 0$, kunnen we precies hetzelfde opmerken, alleen vervalt dan de voorwaarde dat de gehele getallen k(2), k(3), k(5), k(7), k(11), ... niet negatief mogen zijn. Zo is bijvoorbeeld

$$-\frac{3}{4} = -1.2^{-2}.3^{1};$$

in dit geval is $u = -1$, $k(2) = -2$, $k(3) = 1$ en $k(p) = 0$ voor alle andere priemgetallen p. Omgekeerd levert elke keuze van $u = \pm 1$, en een stel gehele getallen k(2), k(3), k(5), k(7), k(11), ..., waarvan er slechts een eindig aantal ongelijk aan nul is, een rationaal getal.

In de algebraïsche getaltheorie wordt onderzocht in hoeverre getallenlichamen ook een dergelijke factorontbindingseigenschap hebben. Willen we zoiets vinden, dan moeten we beschikken over elementen van het getallenlichaam die de rol kunnen spelen van de priemgetallen en van de getallen u.

Wat is eigenlijk precies een priemgetal? Een positief geheel getal p heet een priemgetal als voor elke mogelijke schrijfwijze

$$p = s.t$$

met s en t gehele getallen, geldt dat òf $s = \pm 1$ òf $t = \pm 1$.

Deze getallen 1 en -1 zijn precies de gehele getallen u waarvoor 1/u ook geheel is. Zulke getallen noemen we *eenheden*. Dit begrip laat zich op een natuurlijke manier uitbreiden tot ge-

tallenlichamen K: een element u van $\mathcal{O}(K)$ heet een *eenheid van* $\mathcal{O}(K)$ als 1/u ook in $\mathcal{O}(K)$ bevat is. Zo is bijvoorbeeld $239 - 169\sqrt{2}$ een eenheid van $\mathcal{O}(\mathbb{Q}(\sqrt{2}))$, want

$$\frac{1}{239 - 169\sqrt{2}} = \frac{239 + 169\sqrt{2}}{239^2 - 2.169^2} = \frac{239 + 169\sqrt{2}}{-1} = -239 - 169\sqrt{2}.$$

Het kan worden bewezen dat de eenheden van $\mathcal{O}(\mathbb{Q}(\sqrt{2}))$ precies de getallen zijn van de vorm

$$\pm(1 + \sqrt{2})^k,$$

waarbij k een geheel getal is. Zo is

$$239 - 169\sqrt{2} = -(1 + \sqrt{2})^{-7}.$$

Naar analogie met priemgetallen definiëren we het volgende. Een element p van $\mathcal{O}(K)$ heet *irreducibel* in $\mathcal{O}(K)$ als voor elke schrijfwijze

$$p = a.b$$

met a en b in $\mathcal{O}(K)$, geldt dat òf a, òf b een eenheid van $\mathcal{O}(K)$ is. Zo zijn de irreducibele elementen van de gehele getallen precies de priemgetallen èn de priemgetallen voorzien van een minteken. Priemgetallen zijn niet altijd irreducibel in de ring van gehelen van een getallenlichaam. Zo is

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}),$$

terwijl $3 + \sqrt{2}$ en $3 - \sqrt{2}$ geen van beide eenheden van $\mathcal{O}(\mathbb{Q}(\sqrt{2}))$ zijn.

Nu hebben we voldoende begrippen ingevoerd om de vraag of getallenlichamen net zo'n factorontbindingseigenschap als $\mathbb{Q}$ hebben, precies te kunnen formuleren:

> *Bestaat er voor een getallenlichaam* K *een stel irreducibele elementen* $p_1, p_2, p_3, \ldots\ldots$ *van* $\mathcal{O}(K)$*, zodanig dat er voor elke* x *uit* $\mathcal{O}(K)$ *met* $x \neq 0$*, er precies één stel niet-negatieve gehele getallen* $k_1, k_2, k_3, \ldots\ldots$*, en precies één eenheid* u *van* $\mathcal{O}(K)$ *bestaat, waarvoor*
>
> $$x = u.p_1^{k_1}.p_2^{k_2}.p_3^{k_3} \ldots\ldots \quad ?$$

Opdat zo'n product zin heeft, mag voor slechts eindig veel i gel-

den dat $k_i \neq 0$. Als deze eigenschap geldt, is ook elk element van K zelf op precies één manier te ontbinden in een eenheid en p_1, p_2, p_3, ...; dan vervalt enkel de conditie dat k_1, k_2, k_3, ... niet negatief mogen zijn.

Het antwoord is: *soms, dat hangt van* K *af.* Als K deze factorontbindingseigenschap heeft, zeggen we dat het *klassengetal* van K gelijk is aan één. Anders is het klassengetal van K een geheel getal groter dan één; het voert te ver om het precies te definiëren. In ieder geval heeft $\mathbb{Q}$ klassengetal één; we kunnen dan kiezen $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ... Het klassengetal van een getallenlichaam K wordt kortweg aangegeven met h(K); het wordt en is zeer uitvoerig bestudeerd in de algebraïsche getaltheorie, en speelt ook een belangrijke rol in dit proefschrift en in de rest van deze inleiding.

Als voorbeeld merken we zonder bewijs op dat $h(\mathbb{Q}(\sqrt{2})) = 1$. Deze opmerking blijkt essentieel te zijn in het bewijs van de volgende bewering, die het antwoord geeft op de eerder gestelde getaltheoretische vraag. De getallen

$$s^2 - 2t^2$$

met s en t geheel, zijn precies de getallen die te schrijven zijn als

$$\pm v.w,$$

waarbij v het kwadraat van een geheel getal is en w het product is van priemgetallen p waarvoor $p = 2$ of waarvoor $p - 1$ of $p + 1$ een veelvoud van 8 is.

Stel nu eens dat ook de getallen

$$s^2 - 15t^2$$

te schrijven zouden zijn als $\pm v.w$, waarbij v een kwadraat is en w het product is van een stel priemgetallen van een bepaald type. Vanwege

$$5^2 - 15.1^2 = 2.5$$

moet dan 2 van dat bepaalde type zijn. Maar dan zouden er s en t moeten zijn met

$$s^2 - 15t^2 = \pm 2,$$

en die zijn niet te vinden. Dit alles hangt nauw samen met het feit dat $h(\mathbb{Q}(\sqrt{15})) \neq 1$. Zo zien we dat getallenlichamen en klassengetallen wel degelijk iets te maken hebben met puur getaltheoretische problemen.

Wat heeft het klassengetal nu met Pólyalichamen te maken? Ten eerste is een getallenlichaam met klassengetal één altijd een Pólyalichaam. We geven een ruwe schets van hoe dat bewezen kan worden. Laat K een getallenlichaam zijn met $h(K) = 1$, dus met de zojuist beschreven factorontbinding. Laat n een niet-negatief geheel getal zijn. Voor elke geheelwaardige veelterm

$$a_n X^n + a_{n-1} X^{n-1} + \ldots\ldots + a_1 X + a_0$$

over K van graad n ontbinden we a_n in irreducibele factoren:

$$a_n = u.p_1^{k_1}.p_2^{k_2}.p_3^{k_3}\ldots\ldots \ .$$

Voor f_n kiezen we nu een geheelwaardige veelterm over K van graad n waarbij elk van de getallen $k_1, k_2, k_3, \ldots\ldots$ minimaal is, dat wil zeggen dat voor elke i en voor elke geheelwaardige veelterm over K van graad n, de bijbehorende waarde van k_i tenminste zo groot is als bij f_n. Met enig gepuzzel kan worden aangetoond dat zo'n f_n inderdaad bestaat. Omdat $k_1, k_2, k_3, \ldots\ldots$ steeds zo klein mogelijk zijn, geldt voor elke andere geheelwaardige veelterm over K van dezelfde graad

$$b_n X^n + b_{n-1} X^{n-1} + \ldots\ldots + b_1 X + b_0,$$

dat er een c in $\mathcal{O}(K)$ bestaat met $b_n = c.a_n$. Uitgaande van deze eigenschap is het niet moeilijk te bewijzen dat $f_0, f_1, f_2, \ldots\ldots$ voldoen aan de voorwaarden uit de definitie van een Pólyalichaam. Dus als $h(K) = 1$, dan is K een Pólyalichaam.

Een voor de hand liggende vraag is nu: als K een Pólyalichaam is, is dan $h(K) = 1$? Antwoord: *niet altijd*. Zo is $\mathbb{Q}(\sqrt{34})$ een Pólyalichaam, terwijl $h(\mathbb{Q}(\sqrt{34})) \neq 1$. In dit proefschrift wordt echter aangetoond dat voor vele typen getallenlichamen K *wel* geldt dat $h(K) = 1$ als K een Pólyalichaam is. Voordat we een dergelijk resultaat precies formuleren, wordt nu eerst besproken hoe getallenlichamen daartoe in typen zijn in te delen.

Een goede gedachte is te kijken naar de graad van het lichaam; de definitie daarvan wordt zo meteen herhaald. Het zou leuk zijn om een stelling te hebben van het type: een Pólyalichaam van graad zus of zoveel heeft altijd klassengetal één. Een dergelijke stelling bestaat helaas niet; we moeten naar een fijnere indeling toe.

Laat K een getallenlichaam van graad n zijn. Dat hadden we gedefinieerd als een lichaam waarin n elementen b_1, b_2, ..., b_n bestaan, waarvoor elk element x van K te schrijven is als

$$x = q_1b_1 + q_2b_2 + \ldots\ldots + q_nb_n,$$

voor rationale getallen q_1, q_2, ..., q_n, terwijl hetzelfde niet mogelijk is met minder dan n elementen. Het is eenvoudig aan te tonen dat daaruit volgt dat voor elke x de bijbehorende rationale getallen q_1, q_2, ..., q_n helemaal vast liggen.

Er is een stelling, de stelling van het primitieve element, die zegt dat er in deze situatie een element a van K bestaat, zodanig dat we kunnen kiezen

$$b_1 = 1,\ b_2 = a,\ b_3 = a^2,\ \ldots\ldots,\ b_n = a^{n-1}.$$

Het lichaam K ligt helemaal vast door het ene element a; we schrijven ook wel $K = \mathbb{Q}(a)$. In het bijzonder zijn er rationale getallen q_1, q_2, ..., q_n waarvoor

$$a^n = q_1 + q_2a + q_3a^2 + \ldots\ldots + q_na^{n-1}.$$

Voor deze waarden van q_1, q_2, ..., q_n is a niet het enige getal dat aan deze betrekking voldoet. Als we schrijven $a = a_1$, dan zijn er nog n-1 andere getallen a_2, a_3, ..., a_n, zodanig dat

$$a_i^n = q_1 + q_2a_i + q_3a_i^2 + \ldots\ldots + q_na_i^{n-1}$$

voor i = 1, 2, ..., n. Deze getallen a_1, a_2, ..., a_n zijn namelijk precies de n zogenaamde complexe nulpunten van een veelterm van graad n. Het kan worden bewezen dat ze in dit géval alle n verschillend zijn.

Soms zitten deze a_2, a_3, ..., a_n ook in K, maar vaak ook niet, dat hangt van K af. De verzameling van alle getallen die op enigerlei wijze met sommen, verschillen, producten en quotiënten uit te drukken zijn in a_1, a_2, ..., a_n, geven we aan met L.

Het is duidelijk dat L een lichaam is; het is het kleinste lichaam waarin a_1, a_2, ..., a_n alle bevat zijn. We noemen L de *normale afsluiting* van K; het is zelf ook een getallenlichaam, en hangt alleen af van K en niet van de keuze van a. Voor het geval $K = \mathbb{Q}(\sqrt{2})$ kunnen we nemen $a = a_1 = \sqrt{2}$; dan is $a_2 = -\sqrt{2}$. Aangezien a_1 en a_2 beide in K zitten, is dan $L = K = \mathbb{Q}(\sqrt{2})$.

In het algemeen echter zitten a_2, ..., a_n niet allemaal in K, en is L groter dan K. De graad van L is ten hoogste gelijk aan

$n! = 1.2.3.....n;$

in de meeste gevallen is de graad van L zelfs precies gelijk aan n!.

Getallenlichamen K worden ingedeeld naar de Galoisgroep van L over $\mathbb{Q}$, opgevat als permutatiegroep op de elementen a_1, a_2, ..., a_n. Voor we verder kunnen moet eerst worden uitgelegd wat wordt verstaan onder een permutatiegroep en een Galoisgroep.

Een *permutatie* op a_1, a_2, ..., a_n kan als volgt worden beschreven: pak het rijtje a_1, a_2, ..., a_n op en zet het in een of andere volgorde weer terug. Zo is het verwisselen van a_1 en a_2 een permutatie. Het totale aantal permutaties op a_1, a_2, ..., a_n is gemakkelijk te tellen: voor a_1 zijn er n mogelijke plaatsen om op teruggezet te worden; als de keuze voor a_1 bepaald is, blijven er voor a_2 nog n - 1 plaatsen over om op teruggezet te worden, vervolgens n - 2 voor a_3, enzovoort. Dus het totale aantal permutaties op a_1, a_2, ..., a_n is

$$n.(n - 1).(n - 2).....2.1 = n!.$$

Voor het beschouwen van deze permutaties worden a_1, a_2, ..., a_n enkel als verschillende symbolen opgevat. Nu gaan we ze weer beschouwen als elementen van L, als getallen waarmee we kunnen rekenen.

Het kan gebeuren dat de som van een aantal uitdrukkingen van de vorm

$$q.a_1^{k_1}.a_2^{k_2}.....a_n^{k_n},$$

waarin q een rationaal getal is en k_1, k_2, ..., k_n niet-negatieve gehele getallen zijn, nul oplevert. Een voorbeeld hiervan is

$$(-1).a_1^n + q_1 + q_2.a_1 + q_3.a_1^2 + \ldots\ldots + q_n.a_1^{n-1} = 0;$$

in dit voorbeeld is steeds $k_i = 0$ voor $i > 1$.

Een permutatie kunnen we laten werken op een uitdrukking van dit type, door in zo'n uitdrukking a_i te vervangen door a_j, waarbij j het nummer van de plaats is waarop a_i door de permutatie wordt teruggezet, en dit voor i = 1, 2, ..., n. Als de oorspronkelijke uitdrukking nul was, hoeft in principe de uitdrukking verkregen door er een permutatie op te laten werken, niet nul te zijn. De *Galoisgroep* G *van* L *over* $\mathbb{Q}$ (genoemd naar de Franse wiskundige E. Galois, 1811 - 1832) wordt gedefinieerd als de verzameling van permutaties op a_1, a_2, ..., a_n die *elke* uitdrukking van bovenstaand type waar nul uit komt, overvoeren in een uitdrukking die weer nul is. Uit deze definitie is het duidelijk dat het na elkaar uitvoeren van twee permutaties die in G zitten, een permutatie oplevert die weer in G zit. Een verzameling permutaties met deze eigenschap heet een *permutatiegroep*.

Deze definitie van de Galoisgroep ziet er nogal technisch en niet voor de hand liggend uit, maar wordt gerechtvaardigd door de volgende twee eigenschappen (de hoofdstelling van de Galoistheorie):

- *het aantal elementen van* G *is precies de graad van* L;
- *de lichamen die bevat zijn in* L *corresponderen precies met de permutatiegroepen die bevat zijn in* G.

Aangezien permutatiegroepen in de regel veel gemakkelijker te onderzoeken zijn dan getallenlichamen, geeft deze laatste eigenschap een goed mechanisme om te onderzoeken welke lichamen er in bepaalde getallenlichamen bevat zijn. Dit kunnen we zelfs als een rechtvaardiging opvatten voor het invoeren van de normale afsluiting L van K.

Het kan worden bewezen dat er voor elke i en j een permutatie in G is waardoor a_i op de j-de plaats wordt teruggezet. Een permutatiegroep met deze eigenschap heet *transitief*. Er bestaat een vermoeden dat elke transitieve permutatiegroep optreedt als de Galoisgroep van de normale afsluiting van een getallenlichaam over $\mathbb{Q}$; in elk geval is van geen enkele transitieve permutatiegroep het tegendeel bewezen.

De verzameling van alle permutaties op a_1, a_2, ..., a_n

geven we aan met S_n. Het is duidelijk dat S_n een permutatiegroep is en ook dat S_n transitief is.

Een ander voorbeeld van een transitieve permutatiegroep is C_n. Deze bestaat uit alle permutaties die verkregen worden door een aantal keren de laatste van de a_i's vooraan te zetten en de overige een plaats op te schuiven. Voor $n > 2$ bestaat C_n niet uit alle permutaties; het aantal elementen van C_n is n, en van S_n zoals opgemerkt n!. Er geldt $C_2 = S_2$; dat is ook de enige transitieve permutatiegroep op twee elementen. Alle transitieve permutatiegroepen op 2, 3, 4, 5 of 7 elementen staan opgesomd in een tabel in §10 van deel I van dit proefschrift, compleet met de resultaten voor Pólyalichamen.

Een getallenlichaam K noemen we een G-*lichaam* als G de Galoisgroep is van de normale afsluiting L van K over $\mathbb{Q}$. We hadden al opgemerkt dat de graad van L meestal gelijk is aan n!. Maar de graad van L is het aantal elementen van G, en als G precies n! elementen heeft, dan bestaat G uit alle permutaties op $a_1, a_2, \ldots, a_n$, en is G gelijk aan S_n. Dus K is meestal een S_n-lichaam. Deze vage bewering is wiskundig helemaal precies te maken, dat laten we hier echter achterwege. Deze eigenschap motiveert de studie van S_n-lichamen in het bijzonder. Een van de belangrijkste resultaten van dit proefschrift is dan ook het volgende.

STELLING. Laat n *een geheel getal zijn,* $n \geq 3$, *en laat* K *een* S_n*-lichaam zijn. Dan is* K *een Pólyalichaam dan en slechts dan als* $h(K) = 1$.

Voor $n = 2$ geldt deze stelling niet. De Pólyalichamen van graad 2 worden op geheel andere wijze volledig beschreven in 3.3 in deel I. Maar nu terug naar de stelling zelf; de structuur van het bewijs is als volgt.

In §6 van deel I van dit proefschrift wordt het begrip *pre-Pólyalichaam* ingevoerd; een pre-Pólyalichaam voldoet aan iets zwakkere eisen dan een Pólyalichaam. Vervolgens wordt afgeleid dat elk pre-Pólyalichaam klassengetal één heeft als de permutatiegroep G aan bepaalde voorwaarden voldoet. Voor allerlei permutatiegroepen wordt onderzocht of hieraan voldaan is; deel II is er

zelfs helemaal aan gewijd. Deze voorwaarden blijken vervuld te zijn voor S_n voor $n = 3$ en voor $n \geq 5$. Er geldt dan dus

$$K \text{ is een Pólyalichaam} \Rightarrow K \text{ is een pre-Pólyalichaam}$$

$$\nwarrow \qquad \swarrow$$

$$h(K) = 1,$$

oftewel al deze drie beweringen zijn equivalent. Hiermee is de stelling bewezen voor $n \neq 4$.

Voor $n = 4$ is de situatie wezenlijk anders. Zo is het S_4-lichaam $\mathbb{Q}(a)$ gegeven door

$$a^4 = 11 + 24a - 14a^2 - 32a^3$$

wel een pre-Pólyalichaam, maar geen Pólyalichaam, en $h(\mathbb{Q}(a)) \neq 1$. Uiteindelijk wordt de stelling voor $n = 4$ bewezen in deel III van het proefschrift, als gevolg van bepaalde eigenschappen van getallenlichamen die daar worden afgeleid.

Hiermee is dan een overzicht gegeven van de belangrijkste begrippen en enkele resultaten van dit proefschrift. Wat betreft de gebruikte technieken zij enkel nog opgemerkt dat klassenlichamentheorie en cohomologie van groepen daarin een belangrijke rol spelen.

PART I

INTEGER VALUED POLYNOMIALS OVER A NUMBER FIELD.

by H. Zantema.

manuscripta
mathematica

Abstract.

A number field is called a Pólya field if the module of integer valued polynomials over that field is generated by $(f_i)_{i=0}^{\infty}$ over the ring of integers, with $\deg(f_i) = i$, $i = 0, 1, 2, \ldots$. In this paper bounds on the class numbers and on the number of ramified primes in Pólya fields are derived.

Key words:

number field, Pólya field, permutation group.

1980 Mathematical Subject Classification:

12A20, 12A35, 12A40, 12A50, 20B20.

INTEGER VALUED POLYNOMIALS OVER A NUMBER FIELD.

1. INTRODUCTION.

Let K be a number field and let $\mathcal{O} = \mathcal{O}(K)$ be its ring of integers. Define

$$R(K) = \{ f \in K[X] \mid f[\mathcal{O}] \subset \mathcal{O} \}.$$

In section 2 we shall see that R(K) is a free $\mathcal{O}$-module for each number field K. In this paper we are interested in those fields K for which R(K) has an $\mathcal{O}$-basis $(f_i)_{i=0}^{\infty}$ with the property that $\deg(f_i) = i$, $i = 0, 1, 2, \ldots$. Such fields we call Pólya fields, after G. Pólya, who obtained the first results in this subject in 1919, see [P]. He remarked that a number field is a Pólya field if and only if for each positive integer i the fractional ideal $\underline{a}_i$ consisting of the i-th degree coefficients of elements of degree $\leq i$ of R(K), is principal. Hence if the class number h(K) of K is one then K is a Pólya field. One of Pólya's main conclusions was that a quadratic field is a Pólya field if and only if all ramified prime ideals are principal. In a paper immediately following Pólya's paper, A. Ostrowski ([O]) proves that K is a Pólya field if and only if the ideal

$$\underline{b}(q) = \prod_{N(\underline{p})=q} \underline{p}$$

is principal for all prime powers q, where $\underline{p}$ ranges over the prime ideals of $\mathcal{O}$ and N denotes the absolute ideal norm. If $K/\mathbb{Q}$ is Galois and q is a power of an unramified prime, then $\underline{b}(q)$ is evidently principal. Ostrowski remarks:

> Für beliebige endliche Körper scheint die weitere Reduktion unseres Theorems sehr schwierig zu sein. Für kubische Körper erhalt man jedoch sehr leicht außer der leicht anzugebenden auf die Diskriminantenteiler bezüglichen Bedingungen noch die merkwürdige Forderung, daß alle Primideale 2-ten Grades Hauptideale sind.

For cyclic cubic fields prime ideals of degree 2 do not exist; for non-cyclic cubic fields we show that the curious condition

mentioned by Ostrowski implies that the class number is one. This depends on techniques from class field theory which were not accessible to Ostrowski at that time. More generally we have:

Theorem 1.1. Let K be an S_n-field, $n = 3$ or $n \geq 5$, or an A_n-field, $n = 4$ or $n \geq 6$. Then K is a Pólya field if and only if $h(K) = 1$.

Here S_n and A_n denote the symmetric and alternating group on n symbols respectively. For a transitive permutation group G on n symbols a G-field is defined to be a field K of degree n over $\mathbb{Q}$ for which G is the Galois group of the normal closure N of K over $\mathbb{Q}$, and the action of G on the n embeddings of K into N corresponds to the action on the n symbols. In fact we can prove the conclusion of 1.1 for G-fields for a wide range of permutation groups G.

For the proof of the following theorem we use a classification of transitive permutation groups of prime degree depending on the classification of finite simple groups.

Theorem 1.2. Let $K/\mathbb{Q}$ be non-cyclic of prime degree. Assume that K is a Pólya field with $h(K) \neq 1$. Then K is a G-field for

$$PSl(2,2^k) \subset G \subset P\Gamma l(2,2^k)$$

as a permutation group on $\mathbb{P}^1(\mathbb{F}_{2^k})$.

In particular $[K:\mathbb{Q}]$ is a Fermat prime. A special case is $A_5 \simeq PSl(2,4)$.

Cyclic fields are studied by entirely different means. Here we start from the following theorem.

Theorem 1.3. Let $K/\mathbb{Q}$ be Galois with $G = Gal(K/\mathbb{Q})$. Let U be the group of units in K, and let e_p be the ramification index of a prime number p in $K/\mathbb{Q}$. Then K is a Pólya field if and only if

$$H^1(G,U) \simeq \bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z}).$$

For each group G this leads to a bound on the number of ramified primes in Pólya fields K with $Gal(K/\mathbb{Q}) \simeq G$; for cyclic Pólya fields we get a complete description.

An outline of this paper is as follows. In section 2 we give a modernized version of the proof given by Pólya and Ostrowski, and derive some immediate consequences for cyclotomic fields. In section 3 we prove theorem 1.3; in 3.2 and 3.5 we give a complete description of cyclic Pólya fields in terms of ramification. Fields with Galois group $V_4 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are studied in section 4. In section 5 we derive upperbounds for $|H^1(G,U)|$; according to 1.3 this leads to a bound on the ramification in Pólya fields with Galois group G. In section 6 we derive a group theoretical description of pre-Pólya fields (6.2); here a number field is called a pre-Pólya field if $\underline{b}(q)$ is principal for all powers q of unramified primes. The proof of 6.2 makes use of Tschebotarev's density theorem and some class field theory. The proof of 1.1 is given by deriving $h(K) = 1$ for pre-Pólya fields K. An S_4-field K is a Pólya field if and only if $h(K) = 1$; the proof will be given in [Z]. Here the situation is different: we give an example of an S_4-field K with $h(K) = 2$ which is a pre-Pólya field. In section 7 we prove theorem 1.2. In [CZ], which can be seen as an appendix to this paper, A. M. Cohen and the author classify the doubly transitive groups G for which a G-field may be a pre-Pólya field with $h(K) \neq 1$ according to 6.2. In section 8 a group theoretical description of Pólya fields is given, and the equivalence of Pólya fields and pre-Pólya fields is shown for G-fields for G as in 1.2. In particular this holds for $G = A_5$; further an example of an A_5-field K is given with $h(K) = 3$ and K is a Pólya field. In section 9 dihedral fields are studied. Finally in section 10 the results of this paper for fields of degree ≤ 7 are listed.

2. PÓLYA FIELDS, CYCLOTOMIC FIELDS.

For a number field K with ring of integers $\mathcal{O} = \mathcal{O}(K)$ define

$$R(K) = \{ f \in K[X] \mid f[\mathcal{O}] \subset \mathcal{O} \}.$$

Clearly R(K) is an $\mathcal{O}$-algebra. If $f \in R(K)$, $f = \Sigma_{i=0}^{n} a_i X^i$, $a_n \neq 0$, then

$$f(X+1) - f(X) = n a_n X^{n-1} + \ldots\ldots$$

is contained in R(K). By induction it follows that

$$(n!)a_n \in \mathcal{O}.$$

Let us compute $R(\mathbb{Q})$. Define

$$\binom{X}{i} = \frac{X(X-1)\ldots(X-i+1)}{i!}, \quad i \in \mathbb{Z}, \ i \geq 0.$$

The polynomial $\binom{X}{i}$ is contained in $R(\mathbb{Q})$. Conversely if

$$f = \Sigma_{i=0}^{n} a_i X^i, \quad a_n \neq 0,$$

then we saw that $(n!)a_n \in \mathbb{Z}$, hence there exists $a \in \mathbb{Z}$ such that

$$\deg\left(f - a\binom{X}{\deg(f)}\right) < \deg(f).$$

By induction we have

Proposition 2.1. Let $f_i = \binom{X}{i}$, $i \geq 0$. Then

$$R(\mathbb{Q}) = \{ \Sigma_{i=0}^{\infty} a_i f_i \mid a_i \in \mathbb{Z}, \text{ almost all zero} \}.$$

Our goal is to determine for which fields K the $\mathcal{O}(K)$-module R(K) has a basis $(f_i)_{i=0}^{\infty}$ such that $\deg(f_i) = i$ for $i = 0, 1, \ldots$ as in the case $K = \mathbb{Q}$. Define

$$\underline{a}_i = \{ a \in K \mid a \text{ is the i-th degree coefficient of an element of } R(K) \text{ of degree} \leq i \}$$

for $i = 0, 1, 2, \ldots$. This is a fractional ideal because it is an $\mathcal{O}$-module and $\mathcal{O} \subset \underline{a}_i \subset (1/i!).\mathcal{O}$. In fact $\underline{a}_i^{-1}$ can be considered as a generalization to number fields of the concept i! of $\mathbb{Q}$. Since ideals are projective $\mathcal{O}$-modules we get

$$R(K) \simeq \oplus_{i=0}^{\infty} \underline{a}_i.$$

One can show that such "big" projective modules are free, see [Ba],

i.e. R(K) has a basis as an $\mathcal{O}$-module.

Lemma 2.2. In the notation above we have

$$\underline{a}_i = \prod_{\underline{p} \text{ prime ideal of } \mathcal{O}} \underline{p}^{-\sum_{k=1}^{\infty}[i/N(\underline{p})^k]} \quad , \; i = 0, 1, 2, \ldots ,$$

where N denotes the absolute ideal norm and $[x]$ the greatest integer not exceeding x.

Remark. This lemma generalizes the property

$$i! = \prod_{p \text{ prime}} p^{\sum_{k=1}^{\infty}[i/p^k]} \quad , \; i = 1, 2, \ldots .$$

Proof of 2.2. For a prime ideal $\underline{p}$ of $\mathcal{O}$ define

$$\mathcal{O}_{\underline{p}} = \{ a/b \in K \mid a,b \in \mathcal{O}, \; b \notin \underline{p} \}.$$

This is a discrete valuation ring; let $\underline{m}$ be its maximal ideal, $\underline{m} = \underline{p}\mathcal{O}_{\underline{p}}$. Define

$$\underline{a}_{i,\underline{p}} = \{ a \in K \mid a \text{ is the i-th degree coefficient of some } f \in K[X] \text{ with } \deg(f) \leq i, \; f[\mathcal{O}_{\underline{p}}] \subset \mathcal{O}_{\underline{p}} \},$$

for $i = 0, 1, 2, \ldots$. Using that $\mathcal{O}$ is dense in $\mathcal{O}_{\underline{p}}$ in the $\underline{p}$-adic topology, it is easy to show that $\underline{a}_i.\mathcal{O}_{\underline{p}} = \underline{a}_{i,\underline{p}}$; it remains to prove that

$$\underline{a}_{i,\underline{p}} = \underline{m}^{-\sum_{k=1}^{\infty}[i/N(\underline{p})^k]}.$$

Let $N = N(\underline{p})$ and choose a set $\{ \alpha_0, \alpha_1, \ldots, \alpha_{N-1} \}$ of representatives of $\mathcal{O}_{\underline{p}}$ modulo $\underline{m}$, with $\alpha_0 = 0$. Choose a generator π of $\underline{m}$. We extend the definition of α_s to the set of all non-negative integers s by putting

$$\alpha_s = \sum_{j=0}^{\infty} \alpha_{c(j)} \pi^j$$

if $s = \sum_{j=0}^{\infty} c(j)N^j$, $c(j) \in \{ 0, 1, \ldots, N-1 \}$, $c(j) = 0$ for almost all j. Remark that

$$N^k \mid (s-t) \Leftrightarrow \alpha_s \equiv \alpha_t \bmod \underline{m}^k \qquad (*)$$

for non-negative integers s, t, k. Define $f_i \in K[X]$ by

$$f_i(X) = \prod_{j=0}^{i-1} \frac{(X-\alpha_j)}{(\alpha_i-\alpha_j)} \quad , \; i = 1, 2, \ldots .$$

For each $\alpha \in \mathcal{O}_{\underline{p}}$ and for each $M = N^k$, $k > 0$, and each $a \in \mathbb{Z}$, $a \geq 0$, the set

$$\{ \alpha_{aM}, \alpha_{aM+1}, \dots, \alpha_{(a+1)M-1} \}$$

contains exactly one element congruent to α modulo $\underline{m}^k$. Using this for all k and all $a < [i/n^k]$ we get

$$\Pi_{j=0}^{i-1} (\alpha - \alpha_j) \in \underline{m}^{\sum_{k=1}^{\infty}[i/N^k]}$$

for all $\alpha \in \mathcal{O}_{\underline{p}}$. From the "$\Leftarrow$"-side of (*) it follows that $\Pi_{j=0}^{i-1}(\alpha_i - \alpha_j)$ contains <u>exactly</u> $\sum_{k=1}^{\infty} [i/N^k]$ factors $\underline{m}$. Hence

$$f_i[\mathcal{O}_{\underline{p}}] \subset \mathcal{O}_{\underline{p}} \text{ for } i = 1, 2, \dots .$$

Conversely, if $g[\mathcal{O}_{\underline{p}}] \subset \mathcal{O}_{\underline{p}}$ for $g \in K[X]$, $\deg(g) = i$, define $g_0, g_1, \dots, g_{i-1} \in K[X]$ by

$$g_0(X) = g(X) - g(\alpha_0),$$
$$g_k(X) = g_{k-1}(X) - f_k(X) g_{k-1}(\alpha_k), \quad k = 1, 2, \dots, i-1.$$

Then $f_i(\alpha_k) = 0 = g_{i-1}(\alpha_k)$ for $k = 0, 1, \dots, i-1$, and $\deg(f_i) = i = \deg(g_{i-1})$, hence $g_{i-1} = c.f_i$ for some $c \in K$. Since $f_i(\alpha_i) = 1$ and $g_{i-1}[\mathcal{O}_{\underline{p}}] \subset \mathcal{O}_{\underline{p}}$, we get $c \in \mathcal{O}_{\underline{p}}$. Hence the leading coefficient of g, which is equal to that of g_{i-1}, is a divisor of the leading coefficient of f_i. We conclude

$$\underline{a}_{i,\underline{p}} = \underline{m}^{-\sum_{k=1}^{\infty} [i/N^k]},$$

which completes the proof. □

<u>Theorem</u> 2.3. The following statements are equivalent:

(a) $R(K)$ has a basis $(f_i)_{i=0}^{\infty}$ over $\mathcal{O}(K)$ satisfying $\deg(f_i) = i$, $i = 0, 1, \dots$

(b) $\underline{a}_i$ is a principal ideal in K for $i = 0, 1, \dots$,

(c) For all prime powers q the ideal

$$\underline{b}(q) = \prod_{N(\underline{p})=q} \underline{p}$$

is principal, where $\underline{p}$ ranges over the prime ideals of $\mathcal{O}(K)$ and N denotes the absolute ideal norm.

Definition 2.4. A number field satisfying the three equivalent conditions of theorem 2.3 is called a Pólya field.

Proof of 2.3.

(a) ⇒ (b) If $f_i = a_i X^i + \ldots$, then $\underline{a}_i = a_i \mathcal{O}(K)$.

(b) ⇒ (a) Let $\underline{a}_i = a_i \mathcal{O}(K)$, $i = 0, 1, 2, \ldots$. Choose for each i an $f_i \in R(K)$ such that $f_i = a_i X^i + \ldots$. Then $(f_i)_{i=0}^{\infty}$ is a basis of R(K) by immediate verification.

(c) ⇒ (b) From 2.2 we know that

$$\underline{a}_i = \prod_q \underline{b}(q)^{-\sum_{k=1}^{\infty} [i/q^k]},$$

and this is a principal ideal.

(b) ⇒ (c) By induction on q: if the statement is valid for $q < q_0$ then by 1.2 the ideal

$$\underline{b}(q_0) = \underline{a}_{q_0}^{-1} \cdot \prod_{q<q_0} \underline{b}(q)^{-\sum_{k=1}^{\infty} [i/q^k]}$$

is principal. □

In the rest of this paper only condition (c) will be used. Trivially each number field of class number one is a Pólya field, but the converse is not true.

Let $K/\mathbb{Q}$ be Galois. Then all prime ideals lying above a prime in $\mathbb{Q}$ have the same norm and the same ramification index. Hence for each prime number p there is only one power q of p such that $\underline{b}(q) \neq \mathcal{O}(K)$. If p is unramified in $K/\mathbb{Q}$ then $\underline{b}(q) = p\mathcal{O}(K)$, hence in that case the condition on $\underline{b}(q)$ being a principal ideal is fulfilled automatically. This remark combined with a straightforward computation leads to the next two propositions. For $m \in \mathbb{Z}$, $m > 1$, let ζ_m denote a primitive m-th root of unity.

Proposition 2.5. If $K/\mathbb{Q}$ is an abelian extension ramifying at only one prime, then K is a Pólya field.

Proof. Let p^ν be the conductor of K and consider K as a subfield of $\mathbb{Q}(\zeta_{p^\nu})$. Let $\beta \in K$ be the norm from $\mathbb{Q}(\zeta_{p^\nu})$ to K of $1 - \zeta_p$. Then

$$p\mathcal{O}(K) = (\beta\mathcal{O}(K))^{[K:\mathbb{Q}]}.$$

Hence $\underline{b}(p) = \beta\mathcal{O}(K)$ is a principal ideal, and K is a Pólya field. □

Proposition 2.6. For $m \in \mathbb{Z}$, $m > 1$, the fields $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ are Pólya fields.

Proof. If $m \equiv 2 \bmod 4$, $m > 2$, then replace m by m/2. Let

$$m = \prod p^{\nu(p)}$$

be the factorization of m. Let p be a prime ramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, then $\nu(p) > 0$. We have

$$p\mathcal{O}(\mathbb{Q}(\zeta_{p^{\nu(p)}})) = ((1 - \zeta_{p^{\nu(p)}})\mathcal{O}(\mathbb{Q}(\zeta_{p^{\nu(p)}})))^{\phi(p^{\nu(p)})} \qquad (*)$$

and if q is the norm of a prime above p in $\mathbb{Q}(\zeta_m)$ we get

$$\underline{b}(q) = (1 - \zeta_{p^{\nu(p)}})\mathcal{O}(\mathbb{Q}(\zeta_m)).$$

Hence $\mathbb{Q}(\zeta_m)$ is a Pólya field.

Next let $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. If m is a prime power then K is a Pólya field by 2.5. Assume that m is not a prime power. Let $p|m$ be prime, $k = m.p^{-\nu(p)}$, and $\zeta_{p^{\nu(p)}} = \zeta_m^k$. Define

$$a_p = (1 - \zeta_{p^{\nu(p)}})(1 + \zeta_m)^{-(m/2)-k} \quad \text{if m is even, and}$$

$$a_p = (1 - \zeta_{p^{\nu(p)}})(1 - \zeta_m^{(m+1)/2})^{-m-2k} \quad \text{if m is odd.}$$

From $a_p = \bar{a}_p$ (complex conjugation) it follows that $a_p \in K$. Since $(1 + \zeta_m)$ is a unit if m is even, and $(1 - \zeta_m^{(m+1)/2}$ is a unit if m is odd, we obtain from (*) that

$$p\mathcal{O}(K) = (a_p\mathcal{O}(K))^{\phi(p^{\nu(p)})}.$$

Let q be the norm of a prime above p in K; we have $\underline{b}(q) = a_p\mathcal{O}(K)$. Since this is true for each p we conclude that K is a Pólya field. □

3. GALOIS FIELDS, COHOMOLOGY AND CYCLIC FIELDS.

For the case $K/\mathbb{Q}$ is Galois we now give a cohomological interpretation of the Pólya property. Denote $\mathrm{Gal}(K/\mathbb{Q})$ by G. The groups I(K) of fractional ideals in K and P(K) of principal ideals in K have a natural G-action. If $\underline{p}$ and $\underline{q}$ are prime ideals in K lying above the same prime in $\mathbb{Q}$, then there exists $\sigma \in G$ such that $\sigma(\underline{p}) = \underline{q}$. Hence $I(K)^G$ is generated by

$$\{ \ \underline{b}(q) \ \mid \ q \text{ is a prime power } \}.$$

Thus we see that K is a Pólya field if and only if $I(K)^G \subset P(K)$, and if and only if $I(K)^G = P(K)^G$.

Denote by e_p the ramification index of a prime p in $K/\mathbb{Q}$. Define

$$q_p = N_{K/\mathbb{Q}}(\underline{p}),$$

where $\underline{p}$ is a prime ideal of K lying above p. In this section and in sections 4 and 5 infinite primes and ramification at infinity are excluded from consideration. Define

$$\psi : I(K)^G \to \bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z})$$

by

$$(\psi(\Pi \underline{b}(q_p)^{\nu_p}))_p = \nu_p \bmod e_p.$$

Clearly ψ is surjective; since $p\mathcal{O}(K) = \underline{b}(q_p)^{e_p}$, the kernel of ψ consists of principal ideals with a generator in $\mathbb{Q}$, i.e. $\ker(\psi) \simeq \mathbb{Q}^*/\{\pm 1\}$. Hence we have a short exact sequence

$$0 \to \mathbb{Q}^*/\{\pm 1\} \to I(K)^G \to \bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z}) \to 0.$$

Let $U = \mathcal{O}(K)^*$. Taking the cohomology sequence of

$$0 \to U \to K^* \to P(K) \to 0,$$

and applying Hilbert 90, we obtain an exact sequence

$$0 \to \{\pm 1\} \to \mathbb{Q}^* \to P(K)^G \to H^1(G,U) \to 0.$$

Combining both sequences yields an exact sequence

$$0 \to H^1(G,U) \xrightarrow{\Theta} \bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z}) \to I(K)^G/P(K)^G \to 0.$$

Remark that $I(K)^G/P(K)^G$ can be considered as a subgroup of the class group $Cl(K)$ of K, because $P(K)^G = P(K) \cap I(K)^G$. As we saw the group $I(K)^G/P(K)^G$ is trivial if and only if K is a Pólya field, so we have proved:

Proposition 3.1. Let $K/\mathbb{Q}$ be Galois with group G. For a prime p let e_p be the ramification index of p in $K/\mathbb{Q}$. Then there exists a canonical embedding θ of $H^1(G,U)$ into $\bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z})$, and θ is surjective if and only if K is a Pólya field.

For $K/\mathbb{Q}$ cyclic of degree n the cardinality of the group $H^1(G,U)$ can be determined explicitly using the Herbrand quotient

$$Q = |\hat{H}^0(G,U)|/|\hat{H}^1(G,U)|,$$

where $\hat{H}$ denotes the Tate cohomology. From corollary 2 in section 4 of chapter IX of [L] it follows that $Q = 1/n$ if K is real and $Q = 2/n$ if K is complex. Further $\hat{H}^0(G,U) \simeq \mathbb{Z}^*/N[U]$, hence

$$|\hat{H}^0(G,U)| = 2 \quad \text{if } N[U] = \{1\},$$

$$|\hat{H}^0(G,U)| = 1 \quad \text{if } N[U] = \{\pm 1\};$$

the latter case can only occur if K is real. Hence

$$|H^1(G,U)| = |\hat{H}^1(G,U)| = 2n \quad \text{if } K \text{ is real and } N[U] = \{1\},$$

$$= n \quad \text{else.}$$

Proposition 3.2. Let r be a prime number and $K/\mathbb{Q}$ a cyclic extension of degree r^k, $k \geq 1$. Then K is a Pólya field if and only if (1) or (2) holds:

(1) $K/\mathbb{Q}$ is ramified at only one prime,

(2) $r = 2$, exactly two primes are ramified in $K/\mathbb{Q}$, one of which has ramification index 2, and K is real and $N[U] = \{1\}$.

Proof. The extension $K_1/\mathbb{Q}$ defined by $[K_1:\mathbb{Q}] = r$ and $K_1 \subset K$, has to be ramified at at least one prime p. This prime p is totally ramified in $K/\mathbb{Q}$, so $e_p = r^k$. The proposition now follows from 3.1 and the computation of $H^1(G,U)$.

Example 3.3. A quadratic extension of $\mathbb{Q}$ is a Pólya field if and only if either exactly two primes are ramified, the field is real and the fundamental unit has norm +1, or only one prime is ramified.

For example $\mathbb{Q}(\sqrt{\Delta})$ is a Pólya field if

$$\Delta = -4, \pm 8, -p, r, 4p, 8p, pq,$$

where p, q, r are primes, $p \equiv q \equiv 3 \bmod 4$, $r \equiv 1 \bmod 4$. The cases $\Delta = 4p, 8p, pq$ give rise to Pólya fields since

$$X^2 - pY^2 \equiv -1 \bmod p,$$

$$X^2 - 2pY^2 \equiv -1 \bmod p,$$

$$X^2 - pXY + (p(p-q)/4)Y^2 \equiv -1 \bmod p,$$

have no solutions.

We have considered cyclic extensions of $\mathbb{Q}$ of prime power degree. Cyclic extensions of $\mathbb{Q}$ of arbitrary degree will be dealt with in the corollary of the following theorem.

Theorem 3.4. Let K_1 and K_2 be finite Galois extensions of $\mathbb{Q}$, $L = K_1.K_2$, $K = K_1 \cap K_2$. For a prime p let $e_i(p)$ be the ramification index of p in K_i/K, $i = 1, 2$. Then

(a) If $\gcd(e_1(p),e_2(p)) = 1$ for all primes p and K_1 and K_2 are Pólya fields, then L is a Pólya field.

(b) If either $[K_1:K]$, $[K_2:K]$, $[K:\mathbb{Q}]$ are pairwise relatively prime, or K is a Pólya field and $\gcd([K_1:K],[K_2:K]) = 1$, then K_1 and K_2 are Pólya fields if L is a Pólya field.

Proof. Fix a prime p, let $e_i = e_i(p)$, $i = 1, 2$, and let e_0 be the ramification index of p in $K/\mathbb{Q}$. Since in all cases $\gcd(e_1,e_2) = 1$ is

assumed, the ramification index of p in L/K_1 is e_2, and the same for 1 and 2 interchanged. Define ideals $\underline{m}_0$, $\underline{m}_1$, $\underline{m}_2$, $\underline{m}$ of K, K_1, K_2, L respectively by

$$p\mathcal{O}(K) = \underline{m}_0^{e_0},\ p\mathcal{O}(K_i) = \underline{m}_i^{e_0 e_i},\ i = 1, 2,\ p\mathcal{O}(L) = \underline{m}^{e_0 e_1 e_2};$$

these are the ideals $\underline{b}(q_p)$ for the corresponding fields. We have

$$\underline{m}_1\mathcal{O}(L) = \underline{m}^{e_2} \text{ and } \underline{m}_2\mathcal{O}(L) = \underline{m}^{e_1}.$$

If K_1 and K_2 are Pólya fields, then $\underline{m}_i$ is a principal ideal in K_i, $i = 1, 2$. Hence $\underline{m}^{e_1}$ and $\underline{m}^{e_2}$ are principal ideals in L. Since $\gcd(e_1, e_2) = 1$ we may conclude that $\underline{m}$ is a principal ideal. This is valid for each prime p, so we are done with (a).

If L is a Pólya field then $\underline{m}$ is principal ideal, generated by α, say. Then

$$\underline{m}_1^{[K_2:K]} = \underline{m}_1^{[L:K_1]} = N_{L/K_1}(\underline{m}_1\mathcal{O}(L)) = N_{L/K_1}(\alpha^{e_2}\mathcal{O}(L)) =$$

$$= N_{L/K_1}(\alpha^{e_2}).\mathcal{O}(K_1)$$

is a principal ideal in K_1. On the first condition of (b) the ideal $\underline{m}_1$ is principal since $\underline{m}_1^{e_0 e_1} = p\mathcal{O}(K)$ and $\gcd([K_2:K], e_0 e_1) = 1$.

On the second condition $\underline{m}_1$ is principal since $\underline{m}_1^{e_1} = \underline{m}_0\mathcal{O}(K_1)$ is principal and $\gcd([K_2:K], e_1) = 1$. Hence $\underline{m}_1$ is a principal ideal for each prime p and K_1 is a Pólya field. By symmetry of the argument also K_2 is a Pólya field. □

Corollary 3.5. Let $L/\mathbb{Q}$ be cyclic of degree $n = \prod_{p \text{ prime}} p^{\nu(p)}$. Then L is a Pólya field if and only if for each prime p dividing n, the subfield L of degree $p^{\nu(p)}$ over $\mathbb{Q}$ is a Pólya field.

Proof. Immediate from 3.4 by induction on the number of prime factors of n. □

4. FIELDS WITH GALOIS GROUP V_4.

The simplest non-cyclic abelian group is $V_4 = C_2 \times C_2$, where $C_2 = \mathbb{Z}/2\mathbb{Z}$. In this section we make some remarks about the Pólya property of V_4-fields; a V_4-field is the compositum of two quadratic fields. Such V_4-fields can be real or complex.

Theorem 4.1. Let K be a complex V_4-field; let K^+ be the real quadratic subfield of K and $U^+ = \mathcal{O}(K^+)^* = \langle -1, u \rangle$. Let μ be the group of roots of unity in K, and let $U = \mathcal{O}(K)^*$. Then K is a Pólya field if and only if one of the following conditions holds:

(1) exactly two primes are ramified in $K/\mathbb{Q}$, and 2 is not totally ramified;

(2) exactly three primes are ramified in $K/\mathbb{Q}$, the prime 2 is not totally ramified, $N_{K^+/\mathbb{Q}}[U^+] = \{1\}$, and $U = \mu.U^+$;

(3) $K \simeq \mathbb{Q}(\zeta_8)$.

Remark 4.2. Suppose that $K^+ = \mathbb{Q}(\sqrt{\Delta})$ is a given real quadratic field whose fundamental unit u has norm 1; choose $u > 0$. There are at most two complex V_4-fields K with $K^+ \subset K$ and $U \neq \mu.U^+$. More precisely, if 2u is a square in K^+, then

$$U \neq \mu.U^+ \Leftrightarrow K = K^+(\sqrt{-u}) \text{ or } K = K^+(\sqrt{-1}),$$

and if 2u is not a square in K^+ then

$$U \neq \mu.U^+ \Leftrightarrow K = K^+(\sqrt{-u}).$$

In the case that u has norm -1 we always have $U = \mu.U^+$.

For the proof of 4.1 we need the following lemma.

Lemma 4.3. Let K be a complex V_4-field. Let $G \simeq V_4$ be its Galois group over $\mathbb{Q}$. Assume $K \neq \mathbb{Q}(\zeta_8)$. Then

$$H^1(G,U) \simeq C_2 \times C_2 \times C_2 \text{ if } N_{K^+/\mathbb{Q}}(u) = 1 \text{ and } U = \mu.U^+;$$

$$\simeq C_2 \times C_2 \text{ else.}$$

Proof. Abbreviate $N_{K^+/\mathbb{Q}}$ to N. We distinguish 7 cases:

(a) $i \notin K$, $N(u) = -1$;

(b) $i \notin K$, $N(u) = 1$, $U = \mu.U^+$;

(c) $i \notin K$, $N(u) = 1$, $U \neq \mu.U^+$;

(d) $i \in K$, $N(u) = -1$;

(e) $i \in K$, $N(u) = 1$, $U = \mu.U^+$;

(f) $i \in K$, $N(u) = 1$, $U \neq \mu.U^+$, $2u = \alpha^2$ for some $\alpha \in K^+$, $N(\alpha) = 2$;

(g) $i \in K$, $N(u) = 1$, $U \neq \mu.U^+$, $2u = \alpha^2$ for some $\alpha \in K^+$, $N(\alpha) = -2$.

We have $U \simeq \mu \times \mathbb{Z}$ as a group. As can be verified directly in each of the seven cases this group is uniquely determined as a G-module, up to possible 3-torsion caused by ζ_3. This 3-torsion may be neglected since it has no influence on the cohomology group we are interested in. In each of the seven cases it is possible to compute $H^1(G,U)$ directly as a group of cocycles modulo coboundaries, but it is not necessary to do so. From theorem 3.4 we derive that the fields $K = \mathbb{Q}(\sqrt{5},\sqrt{-2})$, $\mathbb{Q}(\sqrt{-2},\sqrt{-3})$, $\mathbb{Q}(\sqrt{5},\sqrt{-1})$, $\mathbb{Q}(\sqrt{7},\sqrt{-1})$ and $\mathbb{Q}(\sqrt{11},\sqrt{-1})$ are all Pólya fields. These are examples of the cases (a), (c), (d), (f) and (g) respectively. Hence by proposition 3.1 we have

$$H^1(G,U) \simeq C_2 \times C_2$$

in all of these five cases. In the same way we obtain

$$H^1(G,U) \simeq C_2 \times C_2 \times C_2$$

for the cases (b) and (e), e. g. by choosing $K = \mathbb{Q}(\sqrt{21},\sqrt{-2})$ and $\mathbb{Q}(\sqrt{21},\sqrt{-1})$ respectively. □

Proof of 4.1. The case $K \simeq \mathbb{Q}(\zeta_8)$ is covered by 2.5. If $K \neq \mathbb{Q}(\zeta_8)$ then 4.1 follows from 3.1, 4.3 and the remark that 2 is the only prime that can possibly be totally ramified in a V_4-extension. □

Next let K be a real V_4-field. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let $\mathbb{Q}(\sqrt{\Delta_i})$ be the quadratic subfields of K, i = 1, 2, 3. If the fundamental unit u_i of $\mathbb{Q}(\sqrt{\Delta_i})$ has norm 1, where $u_i > 0$, then choose $a_i \in \mathbb{Q}$ such that

$$\mathbb{Q}(\sqrt{\Delta_i},\sqrt{u_i}) = \mathbb{Q}(\sqrt{\Delta_i},\sqrt{a_i}), \text{ e. g. } a_i = N_{\mathbb{Q}(\sqrt{\Delta_i})/\mathbb{Q}}(u_i+1);$$

else choose $a_i = 1$, for $i = 1, 2, 3$. Define H to be the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^{*2})$ generated by the images of Δ_1, Δ_2, Δ_3, a_1, a_2, a_3. Then

$$H \simeq H^1(G,U),$$

except for the next two cases in which H is canonically isomorphic to a subgroup of index 2 of $H^1(G,U)$:

(1) the prime 2 is totally ramified in $K/\mathbb{Q}$ and there exists $x_1 \in \mathcal{O}(\mathbb{Q}(\sqrt{\Delta_i}))$ for $i = 1, 2, 3$, such that $N_{\mathbb{Q}(\sqrt{\Delta_1})/\mathbb{Q}}(x_1) = N_{\mathbb{Q}(\sqrt{\Delta_2})/\mathbb{Q}}(x_2) = N_{\mathbb{Q}(\sqrt{\Delta_3})/\mathbb{Q}}(x_3) = \pm 2$;

(2) all the fields $\mathbb{Q}(\sqrt{\Delta_i})$ contain units of norm -1 and $U = \mathcal{O}(\mathbb{Q}(\sqrt{\Delta_1}))^*.\ \mathcal{O}(\mathbb{Q}(\sqrt{\Delta_2}))^*.\ \mathcal{O}(\mathbb{Q}(\sqrt{\Delta_3}))^*$.

This theorem is due to C. Bennett Setzer; for the proof we refer to [BS], theorem 4.

If a real V_4-field is given, this theorem gives a way to determine if the field is a Pólya field or not, in terms of properties of the quadratic subfields, except for the case that all of these quadratic subfields have units of norm -1. In the proof of lemma 4.3 we saw that seven non-isomorphic V_4-modules can occur as the V_4-module of units in a complex V_4-field. In [BS] the same is done for real V_4-fields; her 22 non-isomorphic V_4-modules are found. In formulating a theorem similar to 4.1, classifying Pólya fields among real V_4-fields, many cases would be distinguished. To decide if a given V_4-field is a Pólya field or not, one computes H as defined above and applies 3.1. For example, in the field $K = \mathbb{Q}(\sqrt{35},\sqrt{381})$ we have

$$\Delta_1 = 35 = 5.7,\ \Delta_2 = 381 = 3.127,\ \Delta_3 = 13335 = 3.5.7.127.$$

Since the fundamental units are

$$6 + \sqrt{35},\ 1015 + 52\sqrt{381},\ 5081 + 44\sqrt{13335}$$

respectively, we get

$$a_1 = 2(6+1) = 2.7,\ a_2 = 2(1015+1) = 2^4.127,\ a_3 = 2(5081+1) = 2^2.3.7.11^2.$$

We see that all 5 prime numbers that are ramified in $K/\mathbb{Q}$ can be expressed in Δ_i, a_i, $i = 1, 2, 3$, modulo squares. All of these primes

have ramification index $e_p = 2$ in $K/\mathbb{Q}$. So

$$H^1(G,U) \simeq H \simeq \bigoplus_{p \text{ prime}} (\mathbb{Z}/e_p\mathbb{Z});$$

all isomorphisms are canonical. Hence K is a Pólya field.

5. BOUNDS ON RAMIFICATION.

For a given finite group G the number of ramified primes in Pólya fields K, normal over $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$, is bounded. One way to see this is the following. According to a theorem of Jordan and Zassenhaus, see [CR], section 79, each finitely generated free abelian group allows only finitely many non-isomorphic G-module structures. This assertion can easily be extended to finitely generated abelian groups. Further only finitely many isomorphism types of abelian groups occur as the group of units in a field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. Hence there are only finitely many possibilities for U as a G-module, up to G-isomorphism. Since in each of these cases $H^1(G,U)$ is finite, there is an upperbound on $|H^1(G,U)|$ only depending on G. By 3.1 this gives an upperbound for the number of ramifying primes in Pólya fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$.

The purpose of this section is making such bounds explicit for various groups G. By proposition 3.1 they can be deduced from upperbounds on $|H^1(G,U)|$. These are derived from the following four lemmas from cohomology theory.

Lemma 5.1. For each prime p dividing $|G|$ let G_p be a p-Sylow subgroup of G. Then for a G-module A there exists a natural injective map

$$H^1(G,A) \to \bigoplus_p H^1(G_p,A).$$

This lemma is an immediate consequence of corollary 3 of proposition 8 in chapter IV of [CF]; the map is the restriction map on each component.

Lemma 5.2. Let H be a normal subgroup of G, and A a G-module. Then there is an exact sequence

$$0 \to H^1(G/H,A^H) \xrightarrow{Inf} H^1(G,A) \xrightarrow{Res} H^1(H,A) \ .$$

This lemma is identical to proposition 4, chapter IV of [CF].

Lemma 5.3. Let G and H be two finite groups of relatively prime orders. Let A be a (G×H)-module. Then

$$H^1(G\times H,A) \simeq H^1(G,A^H) \times H^1(H,A^G).$$

Proof. For an abelian group X denote by $X_{|G|}$ the subgroup of X consisting of the elements which are annihilated by $|G|$, and similarly for H. We obtain from 5.2:

$$0 \to H^1(G,A^H) \to H^1(G\times H,A)_{|G|} \to H^1(H,A)_{|G|}$$

and

$$0 \to H^1(H,A^G) \to H^1(G\times H,A)_{|H|} \to H^1(G,A)_{|H|}.$$

Since $H^1(H,A)$ is annihilated by $|H|$ we get

$$H^1(H,A)_{|G|} \simeq \{1\},$$

and similarly

$$H^1(G,A)_{|H|} \simeq \{1\}.$$

Hence in both exact sequences the first two groups are isomorphic. We may conclude

$$H^1(G\times H,A) \simeq H^1(G\times H,A)_{|G|} \times H^1(G\times H,A)_{|H|} \simeq H^1(G,A^H) \times H^1(H,A^G). \ \square$$

Lemma 5.4. Let K/K_1 be a cyclic extension of number fields of degree m. Let $H = Gal(K/K_1)$ and $n = [K_1:\mathbb{Q}]$. Let U be the group of units in K. Then

$$|H^1(H,U)|$$

divides m^n if m is odd, and divides $m^n.2$ if m is even.

Proof. Since H is cyclic, we can use the Herbrand quotient, see [L], chapter IX, section 4. We obtain

$$|H^1(H,U)| = Q^{-1}.|H^0(H,U)|,$$

where $Q^{-1} = m.2^{-k}$ for some non-negative integer k. Let U_1 be the group of units in K_1. We get

$$H^0(H,U) \simeq U_1/N_{K/K_1}[U];$$

this group is a factor group of

$$U_1/(U_1^m).$$

By Dirichlet's unit theorem we know that $U_1 \simeq \mu_1 \times \mathbb{Z}^r$, where μ_1 is the group of roots of unity in K_1 and

$$r \leq n-1 \text{ if } \mu_1 = \{\pm 1\},$$

$$r < n-1 \text{ if } \mu_1 \neq \{\pm 1\}.$$

In both cases the lemma follows. □

Proposition 5.5. Let G be the Galois group of a finite field extension K/K_1, $n = [K_1:\mathbb{Q}] < \infty$. Assume G has a resolution

$$\{1\} = N_0 \subset N_1 \subset N_2 \subset \ldots \subset N_k = G,$$

such that for $i = 1, 2, \ldots, k$:

N_{i-1} is a normal subgroup of N_i and

N_i/N_{i-1} is cyclic of order m_i.

Let U be the group of units in K. Then $|H^1(G,U)|$ is a divisor of

$$m_1^{n\prod_{i=2}^{k} m_i} \cdot m_2^{n\prod_{i=3}^{k} m_i} \cdot \ldots \cdot m_{k-1}^{n.m_k} \cdot m_k^{n} \cdot 2^{|\{i \mid m_i \text{ is even}\}|}.$$

Proof. We keep the field K fixed and apply induction on the length of the resolution. Choose $H = N_{k-1}$ and $A = U$ in lemma 5.2. Since U^H is the group of units in the invariant field of H, we obtain from lemma 5.4 that

$$|H^1(G/H,U^H)|$$

divides m_k^n if m_k is odd, and divides $m_k^n.2$ if m_k is even. The induction hypothesis gives an upperbound for $|H^1(H,U)|$. Combining this and lemma 5.2 gives the required upperbound for $|H^1(G,U)|$. □

Corollary 5.6. Let $K/\mathbb{Q}$ be finite normal with Galois group G. Let

$$|H^1(G,U)| = \prod_{p \text{ prime}} p^{\beta(p)}.$$

Then

$\beta(p) = 0$ if p does not divide $|G|$;

$\beta(p) < |G|/(p-1)$ if p divides $|G|$, $p \neq 2$;

$\beta(2) \leq t(2^s-1+s)$, where $|G| = 2^s.t$, t odd.

Proof. Choose for each prime p dividing $|G|$ a p-Sylow subgroup G_p of G. From lemma 5.1 we see that the p-part of $|H^1(G,U)|$ does not exceed $H^1(G_p,U)$. As a p-group, G_p admits a resolution in which the factor group of each two successive groups is cyclic of degree p. Apply 5.5 to G_p and this resolution. Write

$$|G| = p^u.v,$$

with $\gcd(p,v) = 1$, for p odd. We see that

$$\beta(p) \leq v(p^{u-1} + p^{u-2} + \ldots + p + 1) < |G|/(p-1).$$

The result for $\beta(2)$ is found in the same way. □

In the theory of class field towers similar upperbounds on $|H^1(G,U)|$ are derived, see for example lemma 15 of chapter IX in [CF]. Our corollary 5.6 can be regarded as a consequence of this lemma. However, proposition 5.5 is slightly sharper than the bounds on $|H^1(G,U)|$ derived in [CF].

For normal finite extensions $K/\mathbb{Q}$ with solvable Galois group G which is not a p-group, the result from 5.5 with $K_0 = \mathbb{Q}$ is sharper than that from 5.6. For example for $G = S_3$ corollary 5.6 gives that $|H^1(G,U)|$ is a divisor of $2^6.3^2$; according to 5.5 it is even a divisor of $2^2.3^2$. The latter result is sharp as we shall see

by examples.

The next proposition deals with nilpotent Galois groups. If such a nilpotent group has at least two non-cyclic prime parts, then the result is sharper than that from 5.5.

Proposition 5.7. Let $K/\mathbb{Q}$ be finite and $G = \mathrm{Gal}(K/K_0) = \prod_{i=1}^{k} G_i$, where $|G_i|$, $i = 1, 2, \ldots, k$, are pairwise relatively prime. Let U, U_i be the unit groups in K, K_i, where K_i is the subfield of K, normal over K_0, such that $\mathrm{Gal}(K_i/K_0) \simeq G_i$, $i = 1, 2, \ldots, k$. Then

$$H^1(G,U) \simeq \prod_{i=1}^{k} H^1(G_i,U_i).$$

Proof. This follows by induction on k from lemma 5.3. □

We return to Pólya fields. Let e_p be the ramification index of a prime p in a finite normal extension $K/\mathbb{Q}$ with Galois group G. From proposition 3.1 we know that $|H^1(G,U)|$ is a divisor of

$$\prod_{p \text{ prime}} e_p$$

and that equality holds if and only if K is a Pólya field. Hence the results from 5.5, 5.6 and 5.7 all imply upperbounds for the amount of ramification in Pólya fields. For example, from 5.5 it follows that at most 5 primes ramify in a V_4-extension $K/\mathbb{Q}$, if K is a Pólya field. This bound is sharp, for in section 4 we saw that $\mathbb{Q}(\sqrt{5.7},\sqrt{3.127})$, in which 5 primes are ramified, is a Pólya field.

We conclude this section with two examples of normal extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$. The first one is the splitting field K of $f(X) = X^3 - 6X - 2$. The discriminant of f is $756 = 2^2.3^3.7$, that of $K/\mathbb{Q}$ is $108020304 = 2^4.3^9.7^3$, and we have

$$e_2 = 3, \quad e_3 = 6, \quad e_7 = 2.$$

Let α be a zero of f, then

$$\underline{b}(q_2) = (\alpha);$$

$$\underline{b}(q_3) = (\frac{3+\sqrt{21}}{2}.(1+\alpha)^{-1});$$

$$\underline{b}(q_7) = (\frac{7+\sqrt{21}}{2}).$$

All these ideals are principal, hence K is a Pólya field, and

$$|H^1(G,U)| = \prod_{p \text{ prime}} e_p = 36.$$

The second example is the splitting field of of $X^3 + 6X^2 - 36X - 2$. The discriminant of this polynomial is $242676 = 2^2.3^4.7.107$, that of the field is $44109839091024 = 2^4.3^8.7^3.107^3$. In this case we have

$$e_2 = 3, \quad e_3 = 3, \quad e_7 = 2, \quad e_{107} = 2.$$

In a similar way as above it can be shown that this field is a Pólya field.

6. NON-GALOIS FIELDS.

Definition 6.1 A number field K is called a pre-Pólya field if for each prime p which is unramified in $K/\mathbb{Q}$ and for each $f \in \mathbb{Z}$, $f > 0$, the ideal $\underline{b}(p^f)$ is principal in K.

Remark that each Galois extension of $\mathbb{Q}$ is a pre-Pólya field. However, as we shall see, in several non-Galois cases the pre-Pólya and the Pólya condition are equivalent.

The pre-Pólya condition can be described group theoretically as follows. Define $\tilde{K}$ to be the normal closure of the Hilbert class field H(K) of a number field K of degree n over $\mathbb{Q}$. Write

$$G = \mathrm{Gal}(\tilde{K}/\mathbb{Q}), \quad H = \mathrm{Gal}(\tilde{K}/K), \quad H_1 = \mathrm{Gal}(\tilde{K}/H(K)),$$

and let $\bar{\Omega}$ be the set of right cosets of H in G. Each element $g \in G$ defines an element

$$(Hs \mapsto Hsg^{-1})$$

of the group $S_{\bar{\Omega}}$ of bijections $\bar{\Omega} \to \bar{\Omega}$, which is isomorphic to S_n.

This is a homomorphism from G to $S_{\bar{\Omega}}$, and defines a transitive action of G on $\bar{\Omega}$. Let $g \in G$ be fixed. For this particular g write the corresponding permutation as a product of t disjoint cycles of orders $f_1, f_2, \ldots, f_t$. Let fixed points correspond to cycles of order one, so that

$$\Sigma_{i=1}^{t} f_i = n.$$

For $i = 1, \ldots, t$, choose $s_i \in G$ such that the element Hs_i of $\bar{\Omega}$ is permuted by the i-th cycle. From these definitions it follows that

$$s_i g^{f_i} s_i^{-1} \in H, \text{ for all } i = 1, \ldots, t.$$

If Hu_i is also permuted by the i-th cycle, then

$$Hs_i g^k = Hu_i$$

for some integer k, hence $h = s_i g^k u_i^{-1} \in H$. We obtain

$$s_i g^{f_i} s_i^{-1} = s_i g^k g^{f_i} g^{-k} s_i^{-1} = hu_i g^{f_i} u_i^{-1} h^{-1}.$$

Since $H/H_1 \simeq Cl(K)$ is abelian, this element is congruent to $u_i g^{f_i} u_i^{-1}$ modulo H_1. Hence modulo H_1 the element $s_i g^{f_i} s_i^{-1}$ does not depend on the choice of s_i.

Proposition 6.2. In the notation above, where f_i, s_i correspond to g, we have

$$\Pi_{i=1}^{t} (s_i g^{f_i} s_i^{-1}) \in H_1$$

for each number field K and each $g \in G$. The field K is a pre-Pólya field if and only if for each $g \in G$ and each $f \in \mathbb{Z}$, $f > 0$, we have

$$\prod_{i, f_i = f} (s_i g^{f_i} s_i^{-1}) \in H_1.$$

Remark. The map

$$g \mapsto \Pi_{i=1}^{t} (s_i g^{f_i} s_i^{-1})$$

is the transfer map Ver: $G/G' \to H/H_1$, see e. g. [Se], chapter VII, section 8.

Proof of 6.2. Let $\underline{p}$ be a prime of $\tilde{K}$ above p, unramified over $\mathfrak{P}$. Let $g = (\underline{p},\tilde{K}/\mathfrak{P})$ be the Frobenius element of $\underline{p}$ in G; each $g \in G$ occurs as the Frobenius element of an unramified prime ideal $\underline{p}$, according to Tschebotarev's density theorem. The decomposition group $Z_{\underline{p}}$ of $\underline{p}$ in $\tilde{K}/\mathfrak{P}$ is generated by g. The ideals

$$(s_i(\underline{p})) \cap K, \quad i = 1,\dots, t,$$

are precisely the prime ideals of K above p; the residue class degree of $(s_i(\underline{p})) \cap K$ in $K/\mathfrak{P}$ is f_i. This is proposition 2.8 of chapter III of [J]. We have for $f \in \mathbb{Z}$, $f > 0$:

$$\underline{b}(p^f) = \prod_{\underline{q} \text{ prime in } K,\ N(\underline{q})=p^f} \underline{q} \quad \text{is a principal ideal}$$

$$\Leftrightarrow \prod_{\underline{q} \text{ pr.in } K,\ N(\underline{q})=p^f} (\underline{q},H(K)/K) = 1$$

$$\Leftrightarrow \prod_{f_i=f} ((s_i(\underline{p}))\cap K,H(K)/K) = 1 \Leftrightarrow \prod_{f_i=f} (s_i(\underline{p}),\tilde{K}/K) \in H_1$$

$$\Leftrightarrow \prod_{f_i=f} (s_i g^{f_i} s_i^{-1}) \in H_1;$$

here the order of succession of the product is arbitarily chosen, and the last equivalence follows from

$$(s_i(\underline{p}),\tilde{K}/K) = (s_i(\underline{p}),\tilde{K}/\mathfrak{P})^{f_i} = s_i(\underline{p},\tilde{K}/\mathfrak{P})^{f_i}s_i^{-1} = s_i g^{f_i} s_i^{-1}.$$

In the same way we get

$$\prod_{i=1}^{t} (s_i g^{f_i} s_i^{-1}) \in H_1,$$

since the ideal

$$p\mathcal{O}(K) = \prod_f \underline{b}(p^f)$$

is principal. □

Lemma 6.3. Let Ω be a finite set and let H be a group acting transitively on Ω. Denote the number of fixed points of $h \in H$ by f(h) and define

$$T = \{ h \in H \mid f(h) = 0 \}.$$

Then the action of $\langle T \rangle$ on Ω is transitive and

$$\{ h \in H \mid f(h) \neq 1 \} \subset \langle T \rangle.$$

Proof. According to Burnside's formula we have

$$\sum_{h\in H} f(h) = |H|,$$

and

$$\sum_{h\in \langle T\rangle} f(h) = k.|\langle T\rangle|,$$

where k is the number of orbits of $\langle T\rangle$ on Ω. Hence

$$\sum_{h \in H\setminus\langle T\rangle} f(h) = |H| - k.|\langle T\rangle|.$$

Since $f(h) \geq 1$ for each $h \in H\setminus\langle T\rangle$, the only possibility is $f(h) = 1$ for each $h \in H\setminus\langle T\rangle$ and $k = 1$, which proves the lemma. □

For $H = \mathrm{Gal}(K/K)$, with the action on $\Omega = \bar{\Omega}\setminus\{H\}$ induced by the action of G on $\bar{\Omega}$, the definition of T is

$$T = \{ g \in H \mid Hsg^{-1} \neq Hs \text{ for all } s \in G,\ s \notin H \}.$$

Theorem 6.4. Let K be a number field of degree ≥ 3 over $\mathbb{Q}$, and let $\bar{\Omega}$, G, H and H_1 be defined as in the first part of this section, and T as above.

(1) Assume that $T \neq \emptyset$ and that K is a pre-Pólya field. Then $T \subset H_1$ and H(K) is contained in the normal closure of K.

(2) Assume that the action of G on $\bar{\Omega}$ is 2-transitive. Then $T \subset H_1$ if and only if K is a pre-Pólya field.

Remark 6.5. If the action of G on $\bar{\Omega}$ is 2-transitive, then the action of H on $\Omega = \bar{\Omega}\setminus\{H\}$ is transitive. Since $|\Omega| \geq 2$, from Burnside's formula it then follows that some element of H has no fixed point in Ω, hence $T \neq \emptyset$.

Proof of 6.4. Let $g \in T$ be arbitrarily chosen. According to 6.2 we have

$$\prod_{f_i=1} s_i g s_i^{-1} \in H_1.$$

Since $Hsg^{-1} \neq Hs$ for $s \notin H$ we have $f_i = 1$ only one time, while $s_i \in H$. We may choose $s_i = 1$ and we have $g \in H_1$. Hence $T \subset H_1$. Let

$$H_2 = \bigcap_{g \in G} gHg^{-1}.$$

Then for $h \in H_2$ we have $Hs(gh)^{-1} = Hs$ if and only if $Hsg^{-1} = Hs$, so $T.H_2 = T$. From $\emptyset \neq T \subset H_1$ it now follows that $H_2 \subset H_1$, i. e. $H(K)$ is contained in the normal closure of K, and we have proved (1).

The "if"-part of (2) is immediate from 6.5. For the "only if"-part we assume that the action of H on Ω is transitive and $T \subset H_1$. We have to prove that

$$\prod_{f_i=f} s_i g^{f_i} s_i^{-1} \in H_1$$

for each $g \in G$ and $f \in \mathbb{Z}$. Assume that $g \in G$ has no fixed point in $\bar{\Omega}$, i. e. all $f_i > 1$. Then for each $f > 2$ for which $f_i = f$ occurs, the element

$$s_i g^{f_i} s_i^{-1}$$

has at least 2 fixed points in $\bar{\Omega}$ and is contained in H. As an element of H acting on Ω it has at least 2 fixed points; according to lemma 6.3 it is contained in $\langle T \rangle \subset H_1$. Hence for $f > 2$ we have

$$\prod_{f_i=f} s_i g^{f_i} s_i^{-1} \in H_1.$$

The same statement for $f = 2$ holds since

$$\prod_f \Big(\prod_{f_i=f} s_i g^{f_i} s_i^{-1} \Big) = \prod_{i=1}^{t} (s_i g^{f_i} s_i^{-1}) \in H_1$$

according to proposition 6.2.

It remains to prove the assertion for $g \in G$ having a fixed point in $\bar{\Omega}$. If $f = f_i > 1$, then the element

$$s_i g^{f} s_i^{-1}$$

has at least 3 fixed points in $\bar{\Omega}$ and is contained in H_1 for the same reason as above. And again the assertion holds for the remaining case $f = 1$ since

$$\prod_f \Big(\prod_{f_i=f} s_i g^{f_i} s_i^{-1} \Big) = \prod_{i=1}^{t} (s_i g^{f_i} s_i^{-1}) \in H_1. \qquad \square$$

Definition 6.6. For a transitive permutation group G on n symbols define

$$R(G) = H / \langle H', T, \mathrm{im}(\mathrm{Ver}) \rangle,$$

where H is the stabilizer of one fixed symbol,

T is the subset of H of elements with no further fixed symbol,

H' is the commutator subgroup of H, and

$\mathrm{im}(\mathrm{Ver}) = \{ h \in H \mid \mathrm{Ver}(g) = hH' \text{ for some } g \in G \}$.

The map Ver: $G \to H/H'$, the transfer map, was mentioned in 6.2. This map is induced by the restriction map

$$G/G' \simeq H_1(G,\mathbb{Z}) \xrightarrow{\mathrm{Res}} H_1(H,\mathbb{Z}) \simeq H/H',$$

where the actions of G and H on $\mathbb{Z}$ are trivial, see [Se], chapter VII, section 8.

Denote by a G-field a field K of degree n over $\mathbb{Q}$ for which G is the Galois group of the normal closure N of K over $\mathbb{Q}$ and the action of G on the n embeddings of K into N corresponds to the action on the n symbols.

Theorem 6.7. Let G be a transitive permutation group for which $T \neq \emptyset$, and let K be a G-field. Assume that K is a pre-Pólya field. Then the class group Cl(K) of K is a factor group of R(G).

Proof. Remark that $Cl(K) \simeq \mathrm{Gal}(H(K)/K) = H/H_1$. From 6.4(1) we know that

$$H(K) \subset N = \tilde{K} \quad \text{and} \quad T \subset H_1.$$

Since $H/H_1 \simeq Cl(K)$ is abelian we have $H' \subset H_1$. For $g \in G$ we already saw that

$$\mathrm{Ver}(g) = (\prod_{i=1}^{t} s_i g^{f_i} s_i^{-1}) H',$$

where t, s_i, f_i, $i = 1, \ldots, t$, correspond to g as before. It follows from 6.2 that

$$\mathrm{im}(\mathrm{Ver}) \subset H_1.$$

Combining these results gives

$$\langle H', T, \mathrm{im}(\mathrm{Ver}) \rangle \subset H_1,$$

which proves the theorem. □

Corollary 6.8. Let K be a G-field for a transitive permutation group G for which $T \neq 0$ and $R(G) \simeq \{1\}$. Then the following assertions are equivalent:

(i) K is a pre-Pólya field;

(ii) K is a Pólya field;

(iii) $h(K) = 1$.

Proof. (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) holds for each field. The implication (i) $\Rightarrow$ (iii) is immediate from 6.7. □

As a consequence we now obtain theorem 1.1 from the introduction:

Theorem 6.9. Let K be a G-field for one of the following groups G:

$G = S_n$, $n = 3$ or $n \geq 5$;

$G = A_n$, $n = 4$ or $n \geq 6$;

G is a Frobenius group, i. e. $T = H\backslash\{1\}$.

Then (i), (ii) and (iii) from 6.8 are equivalent.

For the two exceptions S_4 and A_5 we have

$$G = S_4,\ H = S_3,\ \langle H', T, \mathrm{im}(\mathrm{Ver})\rangle = A_3,$$

so $R(S_4) \simeq \mathbb{Z}/2\mathbb{Z}$, and

$$G = A_5,\ H = A_4,\ \langle H', T, \mathrm{im}(\mathrm{Ver})\rangle = V_4,$$

so $R(A_5) \simeq \mathbb{Z}/3\mathbb{Z}$. The groups $\langle H', T, \mathrm{im}(\mathrm{Ver})\rangle$ can be computed directly for S_4 and A_5, but we also can refer to the next section. In that section R(G) and $\langle H', T, \mathrm{im}(\mathrm{Ver})\rangle$ are computed for linear groups, in particular for $S_4 \simeq \mathrm{PGl}(2,3)$ and $A_5 \simeq \mathrm{PGl}(2,4)$.

In section 8 we prove that an A_5-field is a Pólya field if and only if it is a pre-Pólya field, and we give an example of such a Pólya field K with $\mathrm{Cl}(K) \simeq R(A_5) \simeq \mathbb{Z}/3\mathbb{Z}$.

For S_4-fields the situation is different. It can be shown that an S_4-field K is a Pólya field if and only if $h(K) = 1$, the proof will be published in [Z]. However, there exist S_4-fields K with the pre-Pólya property with $\mathrm{Cl}(K) \simeq R(S_4) \simeq \mathbb{Z}/2\mathbb{Z}$. An example of such a field is

$K = \mathbb{Q}(\alpha)$, where α is a zero of

$$f(X) = X^4 + 32X^3 + 14X^2 - 24X - 11.$$

The discriminant of f is $2^{14}.37^3$; the discriminant of $K/\mathbb{Q}$ is $2^8.37^3$. Both 2 and 37 are totally ramified in $K/\mathbb{Q}$. The prime ideal above 37 is principal; the one above 2 is not, so we see that K is not a Pólya field. We do not prove here that K is a pre-Pólya field and $h(K) = 2$.

7. NON-CYCLIC FIELDS OF PRIME DEGREE AND LINEAR GROUPS.

In section 6 we saw that if a G-field K is a pre-Pólya field and $T \neq \emptyset$, then the class group Cl(K) is a factor group of R(G). For the case that $K/\mathbb{Q}$ is non-cyclic of prime degree n we shall see in this section that $T \neq \emptyset$ is always fulfilled, and R(G) will be computed in all cases; cyclic fields have been considered in section 3. Most times we get $R(G) = \{1\}$, hence non-cyclic pre-Pólya fields of prime degree have trivial class numbers, with a few exceptions.

A theorem of Galois, theorem 3.6 of chapter II of [H], states that a solvable transitive permutation group of prime degree is a Frobenius group or is cyclic. As remarked in 6.9 for a Frobenius group G it is clear that $T \neq \emptyset$ and $R(G) = \{1\}$.

A theorem of Burnside, theorem 21.3 of chapter V of [H], states that an unsolvable transitive permutation group of prime degree is 2-transitive. Hence we may assume that G is 2-transitive. Then H acts transitively on $n - 1$ symbols, as the stabilizer of one symbol. Hence $T \neq \emptyset$; according to 6.3 the subgroup of H generated by T is even transitive.

The 2-transitive permutation groups G can be classified as is done as follows in [C]. The group G contains a minimal normal subgroup N with

$$N \subset G \subset \mathrm{Aut}(N).$$

This group N is simple, and finite simple groups have been classified recently. However, the proof of this classification is of an enormous size and may contain some errors. Wherever this classification is used in this paper, it is mentioned.

Assuming the classification of finite simple groups, the only possibilities for unsolvable transitive permutation groups of prime degree n (see [N]) are:

(1) A_n and S_n;
(2) groups G with $PSl(d,q) \subset G \subset P\Gamma l(d,q)$ acting on the $n = (q^d-1)/(q-1)$ points of the projective space $\mathbb{P}^{d-1}(\mathbb{F}_q)$;
(3) PSl(2,11) acting on 11 symbols;
(4) the Mathieu groups M_{11} and M_{23} acting on 11 and 23 symbols respectively.

Here the notation is as follows. For a prime power q and an integer $d > 1$ we denote by PGl(d,q) the group of invertible d×d-matrices over $\mathbb{F}_q$ modulo the normal subgroups of scalars. The group of d×d-matrices of determinant 1 modulo scalars is denoted by PSl(d,q). Both groups act on $\mathbb{P}^{d-1}(\mathbb{F}_q)$. Let A be the group of field automorphisms of $\mathbb{F}_q$; there is a natural action of A on $\mathbb{P}^{d-1}(\mathbb{F}_q)$. The permutation group on the points of $\mathbb{P}^{d-1}(\mathbb{F}_q)$ generated by A and PSl(d,q) is denoted by $P\Sigma l(d,q)$, the group generated by A and PGl(d,q) is denoted by $P\Gamma l(d,q)$.

Next we compute R(G) for all of these unsolvable transitive permutation groups G of prime degree.

The groups A_n and S_n have been discussed in 6.9. If G = PSl(2,11) then $H \simeq A_5$, see [H], chapter II, theorem 8.28(6). Hence H' = H, and R(G) = {1}. If $G = M_{23}$ then $H = M_{22}$ is simple, hence H' = H and R(G) = {1} If $G = M_{11}$ then H = PΣl(2,9) acting on 10 symbols transitively. We have H' = PSl(2,9). Let σ be the non-trivial automorphism of $\mathbb{F}_9$, then $f(\sigma) = 4$ in the notation of 6.3. According to 6.3 we have $\sigma \in \langle T \rangle$, hence $H = P\Sigma l(2,9) = \langle H', \sigma \rangle \subset \langle H', T \rangle$, and R(G) = {1}.

It remains to determine R(G) for

$$PSl(d,q) \subset G \subset P\Gamma l(d,q)$$

for the case that $n = (q^d-1)/(q-1)$ is a prime number. In this case d has to be prime, for if a is a divisor of d then

$$n = \left(\frac{q^d - 1}{q^a - 1}\right) \cdot \left(\frac{q^a - 1}{q - 1}\right).$$

If $q \equiv 1 \bmod d$ then

$$n = q^{d-1} + q^{d-2} + \ldots + q + 1 \equiv 0 \bmod d.$$

Hence if n is prime then d is a prime not dividing q - 1, so

$$PGl(d,q) = PSl(d,q) = Sl(d,q).$$

In the next theorem we do not require n to be prime. Let G satisfy

$$PSl(d,q) \subset G \subset P\Gamma l(d,q)$$

for arbitrary $d > 1$ and prime power $q = p^f$. Since $PSl(d,q)$ is a normal subgroup of $P\Gamma l(d,q)$, such groups G correspond to subgroups of $P\Gamma l(d,q)/PSl(d,q)$. The latter group is a semidirect product of

$$Gal(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/f\mathbb{Z} \text{ with } \mathbb{F}_q^*/(\mathbb{F}_q^*)^d \simeq \mathbb{Z}/\gcd(d,q-1)\mathbb{Z}$$

defined by the natural action of $Gal(\mathbb{F}_q/\mathbb{F}_p)$ on $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$.

Theorem 7.1. Let $d \geq 2$ and $q = p^f$ for a prime number p. Let G be a permutation group on the $(q^d-1)/(q-1)$ points of $\mathbb{P}^{d-1}(\mathbb{F}_q)$, with

$$PSl(d,q) \subset G \subset P\Gamma l(d,q).$$

Let $k = \text{index}(P\Gamma l(d,q) : G.PGl(d,q))$. Then

(a) $R(G) = \{1\}$ if $d > 2$;

(b) $R(G)$ is cyclic of degree $(p^k-1)/2$ if $d = 2$, p is odd and $G \subset P\Sigma l(2,q)$;

(c) $R(G)$ is cyclic of degree p^k-1 else.

Proof. We may identify H with the stabilizer G_α of one particular point $\alpha \in \mathbb{P}^{d-1}(\mathbb{F}_q)$. Choose coordinates on $\mathbb{P}^{d-1}(\mathbb{F}_q)$ such that

$$\alpha = [1,0,0,\ldots,0].$$

Elements of $(PGl(d,q))_\alpha$ can be identified with matrices

$$\begin{pmatrix} 1 & \cdot & \cdots & \cdot \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

where $B \in Gl(d-1,q)$.

First we prove (a). A matrix of the type

$$\begin{pmatrix} 1 & 0 & \cdot \\ 0 & 1 & \cdot \\ 0 & 0 & \cdot \end{pmatrix} \in PGl(3,q)$$

has at least 3 fixed points $\lceil 1,0,0\rceil$, $\lceil 0,1,0\rceil$, $\lceil 1,1,0\rceil$. More generally each element of $G \cap PGl(d,q)$ in which the first column and at least one other column coincide with the same columns in the unit matrix, has at least 3 fixed points. According to lemma 6.3, applied to $(G \cap PGl(d,q))_\alpha$ as a permutation group on $\Omega = \mathbb{P}^{d-1}(\mathbb{F}_q)\backslash\{\alpha\}$, all these matrices are contained in $<T>$. It is easy to see that for $d \geq 3$ every element of $(G \cap PGl(d,q))_\alpha$ can be expressed in such matrices, for instance by using the fact that elementary matrices generate all matrices with determinant 1. Hence

$$(G \cap PGl(d,q))_\alpha \subset <T>.$$

Choose σ to be a generator of $Gal(\mathbb{F}_q/\mathbb{F}_p)$. From the structure of $P\Gamma l(d,q)/PGl(d,q)$ we see that

$$G = <(G \cap PGl(d,q)),\ A\sigma^k>$$

for some $A \in PGl(d,q)$. Since

$$PSl(d,q) \subset G \cap PGl(d,q)$$

we may choose

$$A = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 1 & 0 \\ 0 & 0 & \dots & 0 & a \end{pmatrix}$$

for some $a \in \mathbb{F}_q^*$. If $d \geq 3$ then $A\sigma^k$ has at least 3 fixed points $\lceil 1,0,0,\dots,0\rceil$, $\lceil 0,1,0,\dots,0\rceil$, $\lceil 1,1,0,\dots,0\rceil$. According to lemma 6.3 we have $A\sigma^k \in <T>$, hence

$$H = G_\alpha = <(G \cap PGl(d,q))_\alpha,\ A\sigma^k> \subset <T>.$$

Hence H is generated by T, which proves (a).

From now on we take $d = 2$. We may identify $\mathbb{P}^{d-1}(\mathbb{F}_q)$ with $\mathbb{F}_q \cup \{\infty\}$, and let $\alpha = \infty$. Then we have

$$(PGl(2,q))_\alpha \simeq \{\ x \mapsto ax+b \mid a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\ \},$$

$$(PSl(2,q))_\alpha \simeq \{\ x \mapsto ax+b \mid a \in (\mathbb{F}_q^*)^2,\ b \in \mathbb{F}_q\ \},$$

as permutation groups on $\mathbb{F}_q$. These two coincide if and only if $p = 2$. An element of G_α can be written as

$$x \mapsto a\sigma^t(x) + b,$$

where $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q^*$, and t is a multiple of k. Define the map

$$\psi : G_\alpha \mapsto \mathbb{F}_{p^k}$$

by

$$\psi(x \mapsto a\sigma^t(x) + b) = N(a),$$

where N denotes the norm from $\mathbb{F}_q$ to $\mathbb{F}_{p^k}$. For every $a \in \mathbb{F}_q^*$ we have $N(\sigma^k(a)) = N(a)$, hence ψ is a homomorphism. We have

$$\psi[G_\alpha] = (\mathbb{F}_{p^k}^*)^2$$

if $G \subset P\Sigma l(2,q)$, and

$$\psi[G_\alpha] = \mathbb{F}_{p^k}^*$$

in any other case. It remains to prove that

$$\ker(\psi) = \langle G_\alpha', T, \mathrm{im}(Ver) \rangle.$$

Since $\psi[G_\alpha]$ is abelian we have $G_\alpha' \subset \ker(\psi)$. Let

$$(x \mapsto a\sigma^t(x) + b)$$

be an arbitrary element of T. Then there is no $x \in \mathbb{F}_q$ such that

$$x = a\sigma^t(x) + b,$$

so the additive homomorphism $f : \mathbb{F}_q \to \mathbb{F}_q$ defined by

$$f(x) = x - a\sigma^t(x)$$

is not surjective. Hence f is not injective and there exists $x \neq 0$ such that

$$x - a\sigma^t(x) = 0.$$

Then $a = x/\sigma^t(x)$, hence $N(a) = 1$ and $T \subset \ker(\psi)$.

Next we show that $\ker(\psi) \subset \langle T \rangle$. If $N(a) = 1$ then there exists $c \in \mathbb{F}_q^*$ such that

$$a^{-1} = \sigma^k(c)/c.$$

Hence if the permutation

$$(x \mapsto a\sigma^k(x))$$

is contained in G then it is contained in G_α and has at least two

fixed points 0 and c in Ω. According to 6.3 this permutation is contained in $\langle T \rangle$. Further, if $0 \neq b \in \mathbb{F}_q$ then

$$(x \mapsto x + b) \in T.$$

Every element of $\ker(\psi)$ is a product of elements of these two types, hence $\ker(\psi) \subset \langle T \rangle$. We conclude that $\langle T \rangle = \ker(\psi)$.

We still have to show that $\mathrm{im}(\mathrm{Ver}) \subset \langle T \rangle$. If $q = 2$ then $G_\alpha = \langle T \rangle$. If $q = 3$ then $\mathrm{Ver}[\mathrm{PSl}(2,q)] \subset \langle T \rangle$, because $\mathrm{PSl}(2,3) \simeq A_4$ and $G_\alpha/\langle T \rangle$ has order one or two. If $q \geq 4$ then $\mathrm{PSl}(2,q)$ is simple, so $\mathrm{Ver}[\mathrm{PSl}(2,q)]$ is trivial. In all cases we have

$$\mathrm{Ver}[\mathrm{PSl}(2,q)] \subset \langle T \rangle.$$

The group G is generated by $\mathrm{PSl}(2,q)$ and elements of G of the shape

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma^k,$$

for $a \in \mathbb{F}_q^*$. It remains to show that $\mathrm{Ver}(g) \subset \langle T \rangle$ for

$$g = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma^k \in G.$$

The fixed points of g are $[1,0]$ and points $[x,1]$ with $\sigma^k(x) = ax$.

If $N(a) = 1$ then there exists $x \in \mathbb{F}_q^*$ with $a = \sigma^k(x).x^{-1}$ by Hilbert 90, and g has at least 3 fixed points

$$[1,0],\ [0,1],\ [x,1].$$

From 6.3 we obtain

$$s\, g^f\, s^{-1} \in \langle T \rangle$$

for each $s \in G$, $f \in \mathbb{Z}$, $f > 0$, with $s\, g^f\, s^{-1} \in G_\alpha$. In particular we have in the notation of section 6:

$$\mathrm{Ver}(g) = \Pi_{i=1}^{t}\ s_i\, g^{f_i}\, s_i^{-1} \in \langle T \rangle.$$

If $N(a) \neq 1$, then $1 = N(\sigma^k(x).x^{-1}) \neq N(a)$ for each $x \in \mathbb{F}_q^*$, so the only fixed points of g are $[1,0]$ and $[0,1]$. The corresponding cosets of $H = G_\alpha$ are

$$H \quad \text{and} \quad H\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We have

$$\prod_{f_i=1} s_i g s_i^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma^k \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma^k \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} \sigma^k(a) & 0 \\ 0 & a \end{pmatrix} \sigma^{2k}.$$

The element $a\sigma^k(a)$ is a square in $\mathbb{F}_q^*$ since $N(a\sigma^k(a)) = (N(a))^2$ is a square in $\mathbb{F}_{p^k}^*$. Hence

$$\begin{pmatrix} \sigma^k(a) & 0 \\ 0 & a \end{pmatrix} \in PSl(2,q), \text{ so } Ver\begin{pmatrix} \sigma^k(a) & 0 \\ 0 & a \end{pmatrix}$$

is trivial. The element σ^{2k} has at least 3 fixed points $\lceil 1,0 \rceil$, $\lceil 0,1 \rceil$ and $\lceil 1,1 \rceil$, so $\sigma^{2k} \in \langle T \rangle$ by 6.3. If $f > 1$ is the length of an orbit of g and $s g^f s^{-1} \in G_\alpha$, then

$$s g^f s^{-1} \in \langle T \rangle$$

since it has at least $2 + f \geq 3$ fixed points. We obtain

$$Ver(g) = \prod_{i=1}^{t} s_i g^{f_i} s_i^{-1} = \begin{pmatrix} \sigma^k(a) & 0 \\ 0 & a \end{pmatrix} \sigma^{2k} \cdot \prod_{f_i>1} s_i g^{f_i} s_i^{-1} \in \langle T \rangle,$$

which concludes the proof. □

Examples.

G	n	$\lvert R(G) \rvert$
$A_4 \simeq PSl(2,3)$	4	1
$S_4 \simeq PGl(2,3)$	4	2
$A_5 \simeq PGl(2,4)$	5	3
$S_5 \simeq P\Gamma l(2,4)$	5	1
$A_5 \simeq PSl(2,5)$	6	2
$S_5 \simeq PGl(2,5)$	6	4

Corollary 7.2. Assume the classification of finite simple groups. Let $K/\mathbb{Q}$ be non-cyclic of prime degree n. Assume that K is a pre-Pólya field and $Cl(K)$ is non-trivial. Then $n = 2^{2^m} + 1$ is a Fermat prime, K is a G-field for a group G with

$$PSl(2,2^{2^m}) \subset G \subset P\Sigma l(2,2^{2^m}),$$

and $Cl(K)$ is cyclic of order a divisor of $n - 2 = 2^{2^m} - 1 = \prod_{i=0}^{m-1}(2^{2^i} + 1)$.

Proof. According to 6.7 the only possibilities are G-fields with R(G) non-trivial. In the first part of this section we saw that this condition is only satisfied if

$$PSl(d,q) \subset G \subset P\Gamma l(d,q);$$

remark that $PSl(d,q) = PGl(d,q)$ and $P\Sigma l(d,q) = P\Gamma l(d,q)$. According to 7.1(a) we have $d = 2$. Further $n = q + 1$ is prime, and q is a prime power. This is only possible if n is a Fermat prime. From 7.1(b,c) it follows that $R(G)$ is cyclic of order a divisor of $n - 2 = q - 1$, and we know from 6.7 that $Cl(K)$ is a factor group of $R(G)$. □

This classification of unsolvable permutation groups of prime degree with non-trivial $R(G)$ has been extended to all doubly transitive permutation groups by A. M. Cohen and H. Zantema, [CZ]. Besides the class of groups G with

$$PSl(2,q) \subset G \subset P\Gamma l(2,q),$$

four other classes of groups G have been found with $R(G)$ non-trivial. This classification has been executed by checking a list of doubly transitive permutation groups, which is assumed to be complete.

8. NON-CYCLIC POLYA FIELDS OF PRIME DEGREE; ICOSAHEDRAL FIELDS.

In section 7 we described all non-cyclic pre-Pólya fields of prime degree n, assuming the classification of finite simple groups. Now we shall derive that all such fields are Pólya fields. First we give a general group theoretical approach to Pólya fields like we did for pre-Pólya fields in section 6.

Let K be a field of degree n over $\mathbb{Q}$, let $H(K)$ be the Hilbert class field of K and let $\tilde{K}$ be a number field normal over $\mathbb{Q}$ with $H(K) \subset \tilde{K}$, e. g. the normal closure of $H(K)$. Let

$$G = Gal(\tilde{K}/\mathbb{Q}),\ H = Gal(\tilde{K}/K) \text{ and } H_1 = Gal(\tilde{K}/H(K)).$$

Let p be a prime of $\mathbb{Q}$ and let Z_p and I_p be the decomposition group and the inertia group in $\tilde{K}/\mathbb{Q}$ of one particular choice of a prime $\underline{p}$ of $\tilde{K}$

above p. As in section 6 the group G acts on the set of n cosets Hs by

$$g \circ (Hs) = Hsg^{-1}.$$

Let $g_1,\ldots,g_t$ be the lengths $|HsZ_p|/|Hs|$ of the orbits of Z_p. Since I_p is a normal subgroup of Z_p, each orbit of Z_p splits into orbits of I_p of equal length. Let us say that the i-th orbit of Z_p (of length g_i) splits into f_i orbits of length e_i of I_p. These e_i and f_i correspond to the usual definition of e_i and f_i for p in K, i. e. th prime decomposition of p in K is

$$p\mathcal{O}(K) = \prod_{i=1}^{t} \underline{p}_i^{e_i},$$

where $N_{K/\mathbb{Q}}(\underline{p}_i) = p^{f_i}$. Choose $s_i \in G$ such that Hs_i is in the i-th orbit of Z_p for $i = 1,\ldots, t$. Then

$$\underline{p}_i = s_i(\underline{p}) \cap K.$$

We can define maps

$$s_iZ_ps_i^{-1}/s_iI_ps_i^{-1} \xrightarrow{\phi_i} (s_iZ_ps_i^{-1}\ H)/(s_iI_ps_i^{-1}\ H) \xrightarrow{\psi_i} H/H_1,$$

where ϕ_i is defined by

$$\phi_i(x) = x^{f_i} \quad \text{for } x \in s_iZ_ps_i^{-1}/s_iI_ps_i^{-1},$$

and ψ_i is induced by the identity on H. Since

$$Hs_ig^{f_i}I_p = Hs_iI_p \text{ for } g \in Z_p,$$

the map ϕ_i is well-defined; since H(K)/K is unramified we have

$$s_iI_ps_i^{-1} \cap H \subset H_1,$$

hence ψ_i is well-defined.

Let g_p be the Frobenius symbol of $\underline{p}$ in the whole extension $\tilde{K}/\mathbb{Q}$, i. e. the canonical generator of Z_p/I_p. The element $\psi_i \circ \phi_i(g_p)$ is the Frobenius symbol of the prime $\underline{p}_i$ in the extension H(K)/K. A K-ideal is principal if and only if its Frobenius symbol in H/H_1 is trivial. Hence the field K is a Pólya field if and only if for all prime numbers p and for all $f \geq 1$:

$$\prod_{f_i=f} \psi_i \circ \phi_i(s_ig_ps_i^{-1}) = 1 \in H/H_1.$$

Since in any case the ideal generated by a prime number is principal,

we obtain for each field K:

$$\Pi_{i=1}^{t}(\psi_i\circ\phi_i(s_i g_p s_i^{-1}))^{e_i} = 1 \in H/H_1.$$

These statements can be reformulated as follows.

Proposition 8.1. For each pair (I,Z) which occurs as an inertia group and a decomposition group, respectively, of one prime in $K/\mathbb{Q}$, up to conjugacy in G, let t and f_i, s_i, i = 1,..., t, be defined as above. Choose $g \in Z$ which generates Z modulo I. Then for each i = 1,..., t, we can choose $a_i \in I$ such that

$$s_i g^{f_i} a_i s_i^{-1} \in H.$$

Further the field K is a Pólya field if and only if for each occurring pair (I,Z) and each $f \geq 1$ we have

$$\prod_{f_i=f} s_i g^{f} a_i s_i^{-1} \in H_1.$$

For each field K and each occurring (I,Z) we have

$$\Pi_{i=1}^{t}(s_i g^{f_i} a_i s_i^{-1})^{e_i} \in H_1.$$

(In both products the order of the factors is arbitrary.)

Remark 8.2. If we restrict to pairs (I,Z) with I is trivial, then each cyclic Z occurs by Tschebotarev's density theorem and we get proposition 6.2 back.

Theorem 8.3. Assume the classification of finite simple groups. Then a non-cyclic field K of prime degree over $\mathbb{Q}$ is a Pólya field if and only if it is a pre-Pólya field.

Proof. According to corollary 7.2 we may restrict to Fermat primes $n = q+1 = 2^{2^m}+1$, while K is a G-field for a group G with

$$PSl(2,q) \subset G \subset P\Sigma l(2,q).$$

Assume that K is a pre-Pólya field. Then $\tilde{K}$ may be chosen to be the

normal closure of K since H(K) is contained in that field. There exists $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)$ such that

$$G = \langle \mathrm{PSl}(2,q), \sigma \rangle .$$

We may choose coordinates such that

$$H = \left\langle \begin{pmatrix} \mathbb{F}_q^* & \mathbb{F}_q \\ 0 & 1 \end{pmatrix}, \sigma \right\rangle .$$

In the notation of the proof of 7.1 we have

$$\left\langle \begin{pmatrix} 1 & \mathbb{F}_q \\ 0 & 1 \end{pmatrix}, \sigma \right\rangle \subset \ker(\psi) \subset H_1 .$$

Hence we have

$$H_1 = \left\langle \begin{pmatrix} A & \mathbb{F}_q \\ 0 & 1 \end{pmatrix}, \sigma \right\rangle$$

for some subgroup $A \subset \mathbb{F}_q^*$.

We have to prove that K is a Pólya field, for which we shall use 8.1. The groups I and Z are solvable, while I is a normal subgroup of Z with a cyclic factor group. Since H(K)/K is unramified we have

$$xIx^{-1} \cap H \subset H_1$$

for all $x \in G$. If also

$$xZx^{-1} \cap H \subset H_1$$

for all $x \in G$ then we have for $i = 1, \ldots, t$:

$$s_i g^{f_i} a_i s_i^{-1} \in s_i Z s_i^{-1} \cap H \subset H_1 .$$

For this I and Z the assertion we have to prove follows immediately, hence we may restrict to those Z for which at least one conjugate, say Z itself, satisfies

$$Z \cap H \not\subset H_1 .$$

For each subgroup G_0 of G abbreviate $G_0 \cap \mathrm{PSl}(2,q)$ to $\tilde{G}_0$. We obtain

$$\tilde{x}\tilde{I}\tilde{x}^{-1} \cap \tilde{H} \subset \tilde{H}_1$$

for all $x \in \mathrm{PSl}(2,q)$, and

$$\tilde{Z} \cap \tilde{H} \not\subset \tilde{H}_1 ;$$

the latter because $\mathrm{index}(Z \cap H : Z \cap H_1)$ is odd and $\mathrm{index}(G : \mathrm{PSl}(2,q))$ is

a 2-power. Subgroups of PSl(2,q) have been classified completely by Dickson, see theorem 8.27 of chapter II of [H]. All solvable subgroups of PSl(2,q) are up to conjugacy equal to

$$\begin{pmatrix} \langle a \rangle & V \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

for some $a \in \mathbb{F}_q^*$ and some vector space V over $\mathbb{F}_2(a)$. If

$$\tilde{Z} = s\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right\rangle s^{-1}$$

for some $s \in PSl(2,q)$, then

$$\tilde{I} = s\begin{pmatrix} \langle a \rangle & 0 \\ 0 & 1 \end{pmatrix} s^{-1},$$

because this is the only non-trivial normal subgroup of $\tilde{Z}$ with $\tilde{Z}/\tilde{I}$ cyclic. An element x of $\tilde{H}$ is contained in $\tilde{H}_1$ if and only if the quotient of the two eigenvalues of x (defined up to taking the inverse) is contained in A. This quotient is equal to 1 for

$$x = s\begin{pmatrix} 0 & a^i \\ 1 & 0 \end{pmatrix} s^{-1},$$

and equal to a^i for

$$x = s\begin{pmatrix} a^i & 0 \\ 0 & 1 \end{pmatrix} s^{-1}.$$

From $\tilde{Z} \cap \tilde{H} \not\subset \tilde{H}_1$ we conclude that a is not contained in A. But then $s^{-1}\tilde{I}s \cap \tilde{H} \not\subset H_1$, contradiction.

Hence we may assume that

$$\tilde{Z} = s\begin{pmatrix} \langle a \rangle & V \\ 0 & 1 \end{pmatrix} s^{-1} \qquad \text{and} \qquad \tilde{I} = s\begin{pmatrix} \langle b \rangle & W \\ 0 & 1 \end{pmatrix} s^{-1}$$

for some $a, b \in \mathbb{F}_q^*$ and vector spaces V and W. Since $\tilde{Z} \cap \tilde{H} \not\subset \tilde{H}_1$, the group $\tilde{Z}$ contains an element for which the quotient of the two eigenvalues is not contained in A. Hence $a \notin A$. From $s^{-1}\tilde{I}s \cap \tilde{H} \subset \tilde{H}_1$ we similarly conclude that $b \in A$.

Let r_a be the order of a and let $v = |V|$. Then the orbits of $\tilde{Z}$ acting on the points of $\mathbb{P}^1(\mathbb{F}_q)$ are

$$s[1,0], \; s[V,1]$$

and sets of the type

$s\lceil c\langle a\rangle+V,1\rceil$ for $c \in \mathbb{F}_q$, $c \notin V$.

The lengths of these orbits are

$$1,\ v,\ r_a v,\ r_a v,\ \ldots\ ,\ r_a v.$$

The orbits of Z are possibly larger, but each orbit of Z splits into orbits of $\tilde{Z}$ of equal length because $\tilde{Z}$ is normal in Z. The number of orbits of $\tilde{Z}$ in which an orbit of Z splits is a divisor of index$(Z : \tilde{Z})$, which is a 2-power. Using $r_a \neq 1$ there is one orbit of Z of length 1, and one of length v, and further orbits of which the length is a 2-power times $r_a v$. However, if $v = 1$ then possibly the two orbits of $\tilde{Z}$ of length one combine to one orbit of Z of length two. This case we refer to as the exceptional case.

Since $\langle a\rangle \neq \langle b\rangle$ and $\tilde{I}$ is a normal subgroup of $\tilde{Z}$ with a cyclic factor group, we have $V = W$. Let r_b be the order of b, then the orbits of $\tilde{I}$ have lengths

$$1,\ v,\ r_b v,\ r_b v,\ \ldots\ ,\ r_b v.$$

In the same way as above I has orbits of lengths 1, v, and orbits whose lengths are 2-powers times $r_b v$. In the exceptional case the first two orbits may or may not combine. It is possible that $r_b = 1$, but the orbits of lengths $r_b v$ and v of $\tilde{I}$ do not combine because each orbit of I is contained in an orbit of Z.

We obtain

$$e_1 = 1,\ e_2 = v,\ e_i \text{ is a 2-power times } r_b \text{ for } i \geq 3;$$

$$f_1 = 1,\ f_2 = 1,\ f_i \text{ is a 2-power times } r_a/r_b \text{ for } i \geq 3.$$

In the exceptional case either $e_1 = 1$ and $f_1 = 2$, or $e_1 = 2$ and $f_1 = 1$, while the index 2 is not used.

We can write

$$\text{index}(Z : I) = w.r_a/r_b$$

for some 2-power w. For $i \geq 3$ let

$$w_i = \text{index}(Z : I)/f_i,$$

which is also a 2-power. In the notation of 8.1 we have

$$s_i g^{f_i a_i} s_i^{-1} \in H, \text{ and } (g^{f_i a_i})^{w_i} \in I,$$

the latter because $g^{(f_i w_i)} \in I$, $a_i \in I$ and Z/I is abelian. Hence

$$(s_i g^{f_i} a_i s_i^{-1})^{w_i} \in s_i I s_i^{-1} \cap H \subset H_1.$$

Since $\gcd(w_i, \text{index}(H : H_1)) = 1$, we conclude that for $i \geq 3$:

$$s_i g^{f_i} a_i s_i^{-1} \in H_1.$$

We still have to prove that

$$\prod_{i=1,2} s_i g a_i s_i^{-1} \in H_1.$$

In the exceptional case this product only runs over $i = 1$. Using the above result for $i \geq 3$ and

$$\prod_{i=1}^{t} (s_i g^{f_i} a_i s_i^{-1})^{e_i} \in H_1$$

it remains to prove in the non-exceptional case that

$$(s_2 g a_2 s_2^{-1})^{v-1} \in H_1.$$

Since $v = |V|$ and V is a vectorspace over $\mathbb{F}_2(a)$ we know that r_a is a divisor of $v - 1$. Remark that $\text{index}(Z : I) = w.r_a/r_b$; we get

$$(s_2 g a_2 s_2^{-1})^{(v-1)w} \in s_2 I s_2^{-1} \cap H \subset H_1.$$

Since $\gcd(w, \text{index}(H : H_1)) = 1$ we obtain

$$(s_2 g a_2 s_2^{-1})^{v-1} \in H_1,$$

which we had to prove. In the exceptional case we see that

$$(s_1 g^{f_1} a_1 s_1^{-1})^{e_1} \in H_1.$$

Since $\gcd(e_1, \text{index}(H : H_1)) = 1$ we get

$$s_1 g^{f_1} a_1 s_1^{-1} \in H_1,$$

which concludes the proof. □

The simplest example of a non-cyclic transitive permutation group G on n symbols, n prime, and non-trivial R(G) is $G = PSl(2,4) \simeq A_5$. From 8.3 we know that an A_5-field is a Pólya field if and only if it is a pre-Pólya field. We can wonder if there exists an A_5-field K which is a Pólya field with non-trivial class number h(K). For such a field we have $h(K) = 3$; more precisely we know from 7.1 that K is a Pólya field with $h(K) \neq 1$ if and only if the Hilbert class field H(K) of K is equal to F, the unique cubic extension of K inside its normal closure over $\mathbb{Q}$.

A table of A_5-fields with small conductors is given by Buhler, [Bu]. The first field in this table satisfying the condition that F/K is totally unramified, is $K = \mathbb{Q}(\alpha)$, where α is a zero of

$$f(X) = X^5 + 2X^3 + 4X^2 - 2X - 4.$$

The discriminant of $K/\mathbb{Q}$ is $2^6.73^2$.

Let d be the discriminant of some number field of degree n over $\mathbb{Q}$, with r_1 embeddings in $\mathbb{R}$. Then

$$\frac{1}{n}\log|d| \geq \gamma + \log(4\pi) + \frac{r_1}{n} - \frac{3}{5}(12\pi)^{2/3}(\lambda(3) + \frac{r_1}{n}\eta(2))^{1/3}n^{-2/3},$$

with

$$\gamma = .57722,\ \lambda(3) = 1.05180,\ \eta(2) = .88247,$$

see [D], formula (1). If we apply this formula to H(K), then $n = 5h(K)$, $r_1 = h(K)$ and $d = (2^6.73^2)^{h(K)}$, and we get

$$h(K) \leq \frac{36\pi\sqrt{3}}{5}(\lambda(3) + \frac{1}{5}\eta(2))^{1/2}(5\gamma + 5\log(4\pi) + 1 - \log(2^6.73^2))^{-3/2}$$

$$= 5.8297 < 6.$$

Since F/K is totally unramified and abelian, we see that $F \subset H(K)$ and 3 is a divisor of h(K). Hence $h(K) = 3$ and $F = H(K)$, and we may conclude that K is a Pólya field.

9. DIHEDRAL FIELDS.

Let D_n be the dihedral group of 2n elements acting on n symbols. If n is odd then D_n is a Frobenius group, so from 6.9 we know that for n odd a D_n-field is a pre-Pólya field if and only if the class number is one. For the case n even we first need a lemma.

Lemma 9.1. Let K be a D_n-field for n even. Let F be the unique subfield of K of degree n/2 over $\mathbb{Q}$. Then K/F is not totally unramified.

Proof. Identify the Galois group of the normal closure of K over $\mathbb{Q}$ with

$$D_n = \langle \sigma, \rho;\ \rho^n = \sigma^2 = (\rho\sigma)^2 = 1 \rangle .$$

The choice of this identification can be done in such a way that K corresponds to $\langle\sigma\rangle$. Then the field F corresponds to

$$\langle \sigma,\ \rho^{n/2} \rangle .$$

For a prime ideal $\underline{p}$ of K let $I_{\underline{p}}$ denote the inertia group of $\underline{p}$ in D_n. Since every number field is ramified over $\mathbb{Q}$, the groups $I_{\underline{p}}$ generate D_n. We have

$$D_n/\langle\rho^2\rangle \simeq V_4.$$

A set of generators of V_4 always contains an element of a given pair of non-zero elements of V_4. Hence at least one of the following two assertions holds:

(1) there exists a prime $\underline{p}$ and a $\in \mathbb{Z}$, a odd, such that $\rho^a \in I_{\underline{p}}$;

(2) there exists a prime $\underline{p}$ and a $\in \mathbb{Z}$, $a \equiv n/2 \bmod 2$, such that $\sigma\rho^a \in I_{\underline{p}}$.

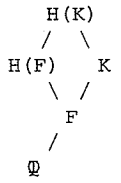
If (1) holds, then $(\rho^a)^{n/2} = \rho^{n/2} \in I_{\underline{p}}$, and $\underline{p}$ is ramified in K/F.
If (2) holds, then for $b = (2a - n)/4$ we have

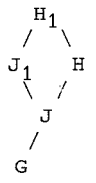
$$\rho^b(\sigma\rho^a)\rho^{-b} = \sigma\rho^{n/2}.$$

Hence the prime ideal $\rho^b(\underline{p})$ is ramified in K/F.

Proposition 9.2. Let K be a D_n-field for n even. Let F be the unique subfield of K of degree n/2 over $\mathbb{Q}$. Then K is a pre-Pólya field if and only if each ideal of K generated by an ideal of F is principal.

Proof. Let G denote the Galois group of some normal $\mathbb{Q}$-extension containing the Hilbert class field H(K) of K. Let H, H_1, J, J_1 be the subgroups of G corresponding to the fields K, H(K), F, H(F), respectively.





The group G acts on the right cosets of H as dicussed in section 6. The only orbit structure with different orbit lengths is

$$1,\ 1,\ 2,\ 2,\ldots\ ,\ 2.$$

According to 6.2 the field K is a pre-Pólya field if and only if

$$\prod_{i=1}^{f} s_i\, g\, s_i^{-1} \in H_1$$

for all $g \in G$ with this orbit structure, in the notation of 6.2. If we replace g by a conjugate of g which is contained in H, then

$$J = \{\ s \in G \mid sgs^{-1} \in H\ \}.$$

Hence K is a pre-Pólya field if and only if

$$gsgs^{-1} \in H_1$$

for all $g \in H$ with orbit structure 1, 1, 2, 2,... , 2, and with $s \in J\backslash H$. The map

$$g \mapsto gsgs^{-1}$$

as a map from H/H_1 to itself is exactly the composition of the following maps

$$H/H_1 \xrightarrow{i} J/J_1 \xrightarrow{Ver} H/H_1,$$

where i is induced by the inclusion map and Ver is the transfer map. From lemma 9.1 it follows that J is generated by H and J_1, hence i is surjective. Since H is generated by elements of H with orbit structure 1, 1, 2, 2,... , 2, we see that K is a pre-Pólya field if and only if the map

$$\mathrm{Ver}: J/J_1 \to H/H_1$$

is trivial. We have the following commutative diagram:

$$\begin{array}{ccc} Cl(F) & \to & Cl(K) \\ \downarrow & & \downarrow \\ J/J_1 & \xrightarrow{Ver} & H/H_1 \end{array}$$

where the vertical arrows are isomorphisms induced by the Artin map, and the upper arrow is induced by mapping an ideal of F to the ideal of K generated by that ideal of F. This proves the proposition. □

Proposition 9.3. Let K be a D_n-field for n even and let F be the subfield of K of degree n/2 over $\mathbb{Q}$. Assume that K is a pre-Pólya field. Then

$$Cl(F) \simeq (\mathbb{Z}/2\mathbb{Z})^m$$

for some $m \leq (n/2) + 1$.

Proof. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & P(F) & \to & I(F) & \to & Cl(F) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & P(K)^G & \to & I(K)^G & \to & Cl(K) & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & H^1(G,U(K)) & \to & (\mathbb{Z}/2\mathbb{Z})^k & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

where I = group of ideals,

P = group of principal ideals,

G = Gal(K/F),

U = group of units,

k = number of prime ideals ramified in K/F.

The first column is the cohomology sequence of

$$0 \to U(K)^* \to K^* \to P(K) \to 0,$$

by Hilbert 90; compare the exact sequences of section 3. Since

$$P(K) \cap I(K)^G = P(K)^G,$$

the group $I(K)^G/P(K)^G$ is a subgroup of Cl(K). From 9.2 we conclude that the right vertical arrow is the zero map. Then the snake lemma produces an exact sequence

$$0 \to Cl(F) \to H^1(G,U(K)) \to (\mathbb{Z}/2\mathbb{Z})^k.$$

The group $H^1(G,U(K))$ is an elementary abelian 2-group since $|G| = 2$. According to 5.4 the number of elements of $H^1(G,U(K))$ is a divisor of $2^{(n/2)+1}$. As a subgroup of $H^1(G,U(K))$ the same can be said for Cl(F). □

Proposition 9.4. If a D_4-field K is a Pólya field, then at most 5 primes of $\mathbb{Q}$ are ramified in $K/\mathbb{Q}$.

Proof. We use the same notation and exact sequences as in the proof of 9.3. Let j be the number of primes p of $\mathbb{Q}$ that are split in $F/\mathbb{Q}$ and for which both primes of F above p are ramified in K/F. Considering all ramification types and using the Pólya property we conclude that $I(K)^G/P(K)^G$ is an elementary abelian 2-group of rank at most j. Remark that k - j is the number of primes of $\mathbb{Q}$ that are ramified in K/F. Let i be the number of primes of $\mathbb{Q}$ that are ramified in $F/\mathbb{Q}$ and write $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$. In section 3 we found an exact sequence

$$0 \to H^1(\Gamma, U(F)) \to (\mathbb{Z}/2\mathbb{Z})^i \to Cl(F),$$

where the order of $H^1(\Gamma, U(F))$ is at most 4. Hence the order of Cl(F) is at least 2^{i-2}. Further the order of $H^1(G, U(K))$ is at most 8.

Combining these results in the exact sequence

$$0 \to Cl(F) \to H^1(G, U(K)) \to (\mathbb{Z}/2\mathbb{Z})^k \to I(K)^G/P(K)^G$$

we obtain

$$(k - j) + (i - 2) \leq 3,$$

from which the proposition follows. □

It is not clear if the bound in 9.4 is sharp; attempts to find an example with 5 ramified primes have not been successful.

Until now we found bounds on the number of ramified primes in Galois fields with the Pólya property in sections 3, 4 and 5. We found bounds on class numbers of non-Galois fields with the pre-Pólya property and the condition $T \neq \emptyset$ in section 6. In some sense D_n-fields for n even are of an intermediate type: proposition 9.4 is of the first type and 9.3 and the proof of 9.2 are of the second type. Finally the intermediate character is illustrated by the existence of the following D_4-fields K:

(1) h(K) = 1, e. g. $K = \mathbb{Q}(\sqrt[4]{2})$;

(2) h(K) = 2 and K is a Pólya field, e. g. $K = \mathbb{Q}(\sqrt{(22 + 2\sqrt{221})})$;

(3) K is a pre-Pólya field but not a Pólya field, e. g. $K = \mathbb{Q}(\sqrt[4]{-6})$;

(4) K is not a pre-Pólya field, e. g. $K = \mathbb{Q}(\sqrt{(23 + 2\sqrt{-15})})$.

10. SURVEY OF FIELDS OF DEGREE AT MOST SEVEN.

In a table we list all transitive permutation groups G on n symbols for n = 2, 3, 4, 5, 7, and list our results on the Pólya property of corresponding G-fields K. For a prime power q the group L_q is defined to be the following permutation group on $\mathbb{F}_q$:

$$L_q = \{ x \mapsto ax + b \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \}.$$

This group is a Frobenius group, and its order is the maximal order $q(q-1)$ that a Frobenius group on q symbols can have.

On 6 symbols there are 16 transitive permutation groups G up to conjugacy in S_6. We consider the following cases:

- G is cyclic of order 6, see 3.2 and 3.5;
- $G \simeq S_3$, see 5.5 and the examples concluding section 5;
- $G \simeq S_6$ or $G \simeq A_6$, see 6.9;
- $G \simeq PSl(2,5)$ or $G \simeq PGl(2,5)$, then R(G) is cyclic of order 2, 4, respectively, see 7.1;
- G is the maximal group imprimitive on two sets of three symbols. One easily verifies $T \neq \emptyset$ and R(G) is trivial. In this case we have

  $$\langle H', T \rangle \neq \langle H', T, \mathrm{im}(\mathrm{Ver}) \rangle;$$

  in fact it is the smallest example of this possibility;
- $G \simeq D_6$, see 9.2 and 9.3.

The remaining 8 permutation groups on 6 symbols are all imprimitive and all satisfy $T = \emptyset$. They cannot be dealt with by the methods discussed in this paper.

The information about Galois types of fields of degrees at most 7 over $\mathbb{Q}$ has been taken from [St].

Table accompanying section 10.

$n = [K : \mathbb{Q}]$	G	discussed in	K is a Pólya field if and only if
2	C_2	section 3	see 3.3
3	C_3	section 3	(i)
	S_3	6.9	$h(K) = 1$
4	C_4	section 3	see 3.2
	V_4	section 4	(ii)
	D_4	section 9	(ii)
	A_4	6.9	$h(K) = 1$
	S_4	(iii)	$h(K) = 1$
5	C_5	section 3	(i)
	D_5	6.9	$h(K) = 1$
	L_5	6.9	$h(K) = 1$
	A_5	section 8	(iv)
	S_5	6.9	$h(K) = 1$
7	C_7	section 3	(i)
	D_7	6.9	$h(K) = 1$
	$L_7 \cap A_7$	6.9	$h(K) = 1$
	L_7	6.9	$h(K) = 1$
	PGl(3,2)	7.1	$h(K) = 1$
	A_7	6.9	$h(K) = 1$
	S_7	6.9	$h(K) = 1$

(i) only one prime is ramified;

(ii) cannot be formulated as a simple restriction on ramification or on the class number;

(iii) will be published in [Z];

(iv) the Hilbert class field of K is contained in the normal closure of K.

REFERENCES.

[Ba] Bass, H., "Big projective modules are free", Illinois J. Math. 7 (1963), 24 - 31.

[Bu] Buhler, J. P., "Icosahedral Galois representations", Lecture Notes in Mathematics 654, Springer, 1978.

[BS] Bennett Setzer, C., "Units over totally real $C_2 \times C_2$-fields", J. Number Theory 12 (1980), 160 - 175.

[C] Cameron, P. J., "Finite permutation groups and finite simple groups", Bull. London Math. Soc. 13 (1981), 1 - 22.

[CF] Cassels, J. W. S., and Fröhlich, A. (eds), "Algebraic number theory", Academic Press, 1967.

[CR] Curtis, C. W., and Reiner, I., "Representation theory of finite groups and associative algebras", John Wiley & Sons, 1962.

[CZ] Cohen, A. M., and Zantema, H., "A computation concerning doubly transitive permutation groups", part II of this thesis.

[D] Diaz y Diaz, F., "Tables minorant la racine n-ième du discriminant d'un corps de degré n", Publ. Math. Orsay 80.06 (1980).

[H] Huppert, B., "Endliche Gruppen I", Springer, 1967.

[J] Janusz, G. J., "Algebraic number fields", Academic Press, 1973.

[L] Lang, S., "Algebraic number theory", Addison-Wesley, 1970.

[N] Neumann, P. M., "Transitive permutation groups of prime degree", Proc. of the 2nd Intern. Conf. on the Theory of Groups, Canberra 1973, Lecture Notes in Mathematics 372 (1974), Springer, 520 - 535.

[O] Ostrowski, A., "Über ganzwertigen Polynome in algebraischen Zahlkörpern", J. Reine Angew. Math. 149 (1919), 117 - 124.

[P] Pólya, G., "Über ganzwertigen Polynome in algebraischen Zahlkörpern", J. Reine Angew. Math. 149 (1919), 97 - 116.

[Se] Serre, J.-P., "Corps locaux", Hermann, 1962.

[St] Stauduhar, R. P., "The determination of Galois groups", Math. Comput. 27 (1973), 981 - 996.

[Z] Zantema, H., "Global restrictions on ramification in number fields", part III of this thesis.

PART II

A COMPUTATION CONCERNING DOUBLY TRANSITIVE PERMUTATION GROUPS

by A. M. Cohen and H. Zantema.

Abstract.

For a transitive permutation group G on a finite set containing the point α, consider the quotient group R(G) of the stabilizer G_α of α in G by the group

$$\langle G'_\alpha, T, \mathrm{im}(\mathrm{Ver})\rangle,$$

where G'_α is the commutator subgroup of G_α, the set T consists of the elements of G_α fixing no other point but α, and Ver is the transfer map from G to G_α/G'_α. The group R(G) is of interest in a problem from algebraic number theory studied by one of the authors. In this paper the group R(G) is computed for all known doubly transitive permutation groups G; in view of the classification of finite simple groups and recent work of Hering, all doubly transitive permutation groups are known.

Key word:

doubly transitive permutation group.

1980 Mathematical Subject Classification:

20B20.

II-1

1. INTRODUCTION.

Let G be a transitive permutation group on a finite set Ω. Fix an element α of Ω. We introduce the following notations:

G_α is the stabilizer of α in G;
G'_α is the commutator subgroup of G_α;
T is the subset of G_α consisting of all elements of which α is the only fixed point in Ω;
$\mathrm{Ver}: G \to G_\alpha/G'_\alpha$ is the transfer map, cf. [Hu], IV, §1;
$\mathrm{im}(\mathrm{Ver}) = \{ h \in G_\alpha \mid \mathrm{Ver}(g) = hG'_\alpha \text{ for some } g \in G \}$;
J is the (normal) subgroup of G_α generated by G'_α, T and im(Ver);
$R(G) = G_\alpha/J$.

Since G is transitive, the isomorphism class of the group R(G) does not depend on the choice of α. The reason for studying R(G) is given at the end of this introduction.

Due to the classification of finite simple groups, cf. [A], all doubly transitive permutation groups can be classified, see [Cm]. In fact, in [N] this work is announced to be completed by Hering, cf. [H1], [H2]. Although this classification seems to be complete, we safely speak about the *known* doubly transitive permutation groups. For all of these groups we compute R(G) in this paper. The result is stated in the following theorem. *Throughout the paper,* p *denotes a prime number, and* $q = p^f$ *for a positive integer* f.

THEOREM 1.1. *Let* G *be a known doubly transitive permutation group on a finite set. Then* R(G) *is cyclic. Moreover,* R(G) *is trivial except for the following cases:*

(a) $G = \{ x \mapsto a\sigma^i(x) + b \mid a, b \in \mathbb{F}_{2^f}, a \neq 0, i \in \mathbb{Z} \}$, *on the elements of* $\mathbb{F}_{2^f}$, *where* f *is a 2-power and* σ *is a generator of* $\mathrm{Aut}(\mathbb{F}_{2^f})$; *in this case we have* $|R(G)| = 2$;

(b) $\mathrm{PSl}(2,q) \leq G \leq \mathrm{P\Gamma l}(2,q)$, *on the points of* $\mathbb{P}^1(\mathbb{F}_q)$; *let* $k = [\mathrm{P\Gamma l}(2,q) : G.\mathrm{PGl}(2,q)]$; *in this case we have*

$$|R(G)| = \begin{cases} (p^k-1)/2 & \text{if } p \text{ is odd and } G \leq \mathrm{P\Sigma l}(2,q), \\ p^k-1 & \text{otherwise;} \end{cases}$$

(c) $PSU(3,q) \leq G \leq P\Gamma U(3,q)$ *on the points of a unital; let* $k = [P\Gamma U(3,q) : G.PGU(3,q)]$, *and*

$$\varepsilon = \begin{cases} 1 & \text{if } 2f/k \text{ is even,} \\ \frac{1}{2} & \text{if } 2f/k \text{ is odd;} \end{cases}$$

in this case we have $|R(G)| = \begin{cases} (p^{k\varepsilon}-1)/2\varepsilon & \text{if } p \text{ is odd,} \\ p^{k\varepsilon}-1 & \text{if } p \text{ is even;} \end{cases}$

(d) ${}^2G_2(q) \leq G \leq \mathrm{Aut}({}^2G_2(q))$ *on the points of a unital, for* $q = 3^{2m+1}$, $m \geq 1$; *let* $k = [\mathrm{Aut}({}^2G_2(q)) : G]$; *in this case we have* $|R(G)| = (3^k-1)/2$;

(e) ${}^2B_2(q) \leq G \leq \mathrm{Aut}({}^2B_2(q))$ *on the points of an ovoid, for* $q = 2^{2m+1}$, $m \geq 1$; *let* $k = [\mathrm{Aut}({}^2B_2(q)) : G]$; *in this case we have* $|R(G)| = 2^k-1$.

Thus, surprisingly, it turns out that the only known doubly transitive permutation groups G for which R(G) is non-trivial, occur among the groups of Lie type of rank one, and their doubly transitive parabolic subgroups, cf. [Ct].

We conclude this introduction by motivating the study of R(G). Let G be a transitive permutation group on the finite set Ω. Define a G-field to be a number field K of degree $|\Omega|$ over $\mathbb{Q}$ for which G is the Galois group of the normal closure N of K over $\mathbb{Q}$, and the action of G on the $|\Omega|$ embeddings of K into N corresponds to the action on Ω. Let $\mathcal{O}$ be the ring of integers of K. As in [Z] the field K is defined to be a Pólya field if the free $\mathcal{O}$-module

$$\{ f \in K[X] \mid f[\mathcal{O}] \subset \mathcal{O} \}$$

admits an $\mathcal{O}$-basis $\{f_i\}_{i=0}^{\infty}$ such that $\deg(f_i) = i$ for $i = 0, 1, 2, \ldots$. The group R(G) arises naturally in this context, as is shown by the following result, cf. [Z], theorem 6.7:

THEOREM 1.2. *Let* K *be a* G*-field. Assume that* $T \neq \emptyset$ *and assume that* K *is a Pólya field. Then the class group of* K *is isomorphic to a factor group of* R(G).

Remark that for G doubly transitive the condition $T \neq \emptyset$ is always fulfilled. An immediate consequence of 1.1 and 1.2 is the following corollary.

COROLLARY 1.3. *Let* G *be a known doubly transitive permutation group, not of one of the types (a), (b), (c), (d), (e) of 1.1. Let* K *be a* G*-field which is a Pólya field. Then the class group of* K *is trivial.*

2. THE DOUBLY TRANSITIVE GROUPS.

The table below comprises all known finite doubly transitive permutation groups. For the groups without a regular normal subgroup we refer to [Cm] and [K]; for groups having a regular normal subgroup we refer to [H1]. The groups of the types (1) to (12) are of the former type, the groups of the types (13) to (21) are of the latter type. As stated before this list is expected to contain all finite doubly transitive permutation groups.

TABLE. *The known doubly transitive permutation groups* G *on a finite set* Ω.

	G	Ω	restrictions
(1)	S_n, A_n	n symbols	$n \geq 2$, $n \geq 4$
(2)	$PSl(n,q) \leq G \leq P\Gamma l(n,q)$	$(q^n-1)/(q-1)$ points of $\mathbb{P}^{n-1}(\mathbb{F}_q)$	$n \geq 2$
(3)	$PSU(3,q) \leq G \leq P\Gamma U(3,q)$	q^3+1 points of a unital	
(4)	${}^2G_2(q) \leq G \leq Aut({}^2G_2(q))$	q^3+1 points of a unital	$q = 3^{2m+1}, m \geq 1$
(5)	${}^2B_2(q) \leq G \leq Aut({}^2B_2(q))$	q^2+1 points of an ovoid	$q = 2^{2m+1}, m \geq 1$
(6)	$Sp(2m,2)$	$2^{m-1}(2^m \pm 1)$ non-degenerate quadrics	$m \geq 3$
(7)	$PSl(2,11)$	11 points of a block design	
(8)	A_7	15 points of $\mathbb{P}^3(\mathbb{F}_2)$	
(9)	M_{11}, M_{12}, M_{22}, $Aut(M_{22})$, M_{23}, M_{24}	11, 12, 22, 22, 23, 24 points of a Steiner system	
(10)	M_{11}	12 points of a 3-design	
(11)	HS	176 points of a design	
(12)	Co.3	276 points in the Leech lattice	
(13) (*)	$Sl(d,q) \leq G_0 \leq \Gamma l(d,q)$	$(\mathbb{F}_q)^d$	$d \geq 1$
(14) (*)	$Sp(2d,q) \lhd G_0$	$(\mathbb{F}_q)^{2d}$	$d \geq 2$
(15) (*)	$G_2(q) \lhd G_0$	$(\mathbb{F}_q)^6$	$q = 2^f$
(16) (*)	$E \lhd G_o$ (**)	$(\mathbb{F}_3)^4$, $(\mathbb{F}_q)^2$	$q = 3,5,7,11,23$
(17) (*)	$G_0^{(\infty)} \simeq Sl(2,5)$ (***)	$(\mathbb{F}_q)^2$	$q=9,11,19,29,59$
(18) (*)	$G_0 \simeq A_6$	$(\mathbb{F}_2)^4$	
(19) (*)	$G_0 \simeq A_7$	$(\mathbb{F}_2)^4$	
(20) (*)	$G_0 \simeq Sl(2,13)$	$(\mathbb{F}_3)^6$	
(21) (*)	$G_0 \simeq PSU(3,3)$	$(\mathbb{F}_2)^6$	

(*) G is generated by G_0 and Ω; as an elementary abelian (additive) group, Ω is considered here as a permutation group on itself.

(**) E is an extraspecial group of order 2^{n+1}, where n is defined by $|\Omega| = p^n$.

(***) $G_0^{(\infty)}$ is the last term of the commutator series of G_0.

3. THE PROOF OF THE THEOREM.

For the proof of theorem 1.1 we need two lemmas.

LEMMA 3.1. *Let* $h \in G_\alpha$ *have at least three fixed points in* Ω *(i. e., α and at least two other points). Then* h *is contained in the subgroup of* G_α *generated by* T.

This lemma is an immediate consequence of lemma 6.3 in [Z].

LEMMA 3.2. *Let* $g \in G$ *have at least three fixed points in* Ω. *Then* Ver(g) *is contained in the subgroup of* G_α/G'_α *generated by* T *modulo* G'_α.

PROOF. We may identify Ω with the set of right cosets of G_α in G, while the action of G on Ω is:

$$g \circ (G_\alpha s) = (G_\alpha s g^{-1}),\ g \in G.$$

As mentioned in [Z], section 6, we have

$$\mathrm{Ver}(g) = (\Pi_{i=1}^{t} s_i g^{f_i} s_i^{-1}) G'_\alpha.$$

Here $g \in G$ decomposes into t disjoint cycles of lengths $f_1, f_2, \ldots, f_t$, while a fixed point is considered as a cycle of length one, and $G_\alpha s_i$ is an element of the i-th cycle of g, i = 1,..., t. Each element

$$s_i g^{f_i} s_i^{-1}$$

is contained in G_α. Furthermore, $s_i g^{f_i} s_i^{-1}$ has at least 3 fixed points; according to 3.1 it is contained in the group generated by T. Hence

$$\Pi_{i=1}^{t} s_i g^{f_i} s_i^{-1} \in \langle T \rangle,$$

so

$$\mathrm{Ver}(g) \in \langle T \rangle G'_\alpha / G'_\alpha,$$

which concludes the proof of lemma 3.2.

We shall give the proof of theorem 1.1 by computing R(G) for each of the doubly transitive groups listed in the table. If F is a field and σ is a field automorphism of F, we denote by F^{σ} the field of all elements of F fixed by σ. If

$$g \in PGl(n,q),$$

we shall sometimes sloppily present g as a matrix while in fact this matrix is determined by g only up to a scalar factor.

The cases (1), (2) and (7) have been dealt with in [Z]; case (2) corresponds to part (b) of theorem 1.1. In case (1) the group R(G) is trivial except for

$$G = S_4 \simeq PGl(2,3) \text{ and } G = A_5 \simeq PGl(2,4),$$

which are included in case (2). In case (7) the group R(G) is also trivial.

We now compute R(G) for the other cases; cases (3), (4), (5), (13) correspond to the parts (c), (d), (e), (a) of theorem 1.1 respectively.

(3) Denote the involutory automorphism of $\mathbb{F}_{q^2}$ (whose fixed field is $\mathbb{F}_q$) by

$$x \mapsto \bar{x},$$

and let $Q: \mathbb{F}_{q^2}^3 \to \mathbb{F}_{q^2}$ be the hermitian form given by

$$Q(\underline{x}) = x_1\bar{x}_2 + x_2\bar{x}_1 + x_3\bar{x}_3$$

where $\underline{x} = (x_1,x_2,x_3) \in \mathbb{F}_{q^2}^3$.

By definition GU(3,q) is the subgroup of $Gl(3,q^2)$ consisting of the transformations stabilizing

$$U = \{ \underline{x} \in \mathbb{F}_{q^2}^3 \mid Q(\underline{x}) = 0 \},$$

and PGU(3,q) is its projective image. Now

$$P\Gamma U(3,q) = PGU(3,q).Aut(\mathbb{F}_{q^2})$$

is viewed as a permutation group on the set Ω of projective points

corresponding to elements of U, and

$$PSU(3,q) = P\Gamma U(3,q) \cap PSl(3,q^2).$$

Set $\alpha = [1,0,0]$. Then $\alpha \in \Omega$ and

$$PGU(3,q)_\alpha = \{ \begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & f & g \end{pmatrix} \mid a\bar{a} = g\bar{g} = 1,\ \bar{d}b + \bar{b}d + f\bar{f} = 0,\ c\bar{d} + \bar{f}g = 0 \ \} .$$

Note that the centre of $GU(3,q)$ is

$$\{ \lambda \in \mathbb{F}_{q^2}^* \mid \lambda\bar{\lambda} = 1 \}.$$

Put $k = [P\Gamma U(3,q) : G.PGU(3,q)]$ and choose a generator σ of $Aut(\mathbb{F}_{q^2})$. Then

$$G.PGU(3,q) = \langle PGU(3,q), \sigma^k \rangle.$$

Define r by

$$\mathbb{F}_r = \mathbb{F}_q \cap \mathbb{F}_{q^2}^{\sigma^k},$$

and let $N : \mathbb{F}_{q^2} \to \mathbb{F}_r$ be the norm map. Then either

$$r = p^k,\ 2f/k \text{ is even, and } \mathbb{F}_{q^2}^{\sigma^k} \subset \mathbb{F}_q,$$

or

$$r = p^{k/2},\ 2f/k \text{ is odd, and } \mathbb{F}_{q^2}^{\sigma^k} \not\subset \mathbb{F}_q.$$

Consider the map $P\Gamma U(3,q)_\alpha \to \mathbb{F}_r^*$ given by

$$A\sigma^t \mapsto N(a^2) \quad \text{if } 2f/k \text{ is even,}$$

$$A\sigma^t \mapsto N(a) \quad \text{if } 2f/k \text{ is odd,}$$

for $t \in \mathbb{Z}$,

$$A = \begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & f & g \end{pmatrix} \in PGU(3,q),$$

and denote by ϕ its restriction to G_α. Note that ϕ is well defined as $N(g) = 1$ whenever $g\bar{g} = 1$.

We claim that $J = \ker(\phi)$. This obviously proves that $R(G)$ is cyclic of order as mentioned in 1.1(c).

First we show that an element of the shape

$$\tau(h,t) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & h \end{pmatrix} \sigma^t \in P\Gamma U(3,q)_\alpha$$

has at least three fixed points in Ω. We distinguish three cases. Set $\tau = \tau(h,t)$.

Let $p = 2$. Then τ has at least three fixed points $[1,1,0]$, $[1,0,0]$, $[0,1,0]$ in Ω.

Let t be even. Then there are p elements y of $\mathbb{F}_{p^2}$ satisfying $y + \bar{y} = 0$, and τ has at least $p + 1$ fixed points $[1,y,0]$, $[0,1,0]$ in Ω.

Let t be odd and $p \neq 2$. Let $\mathbb{F}_s = \mathbb{F}_{q^2}^{\sigma^t}$. Then $\mathbb{F}_s$ is contained in $\mathbb{F}_q$, and

$$N_{\mathbb{F}_{q^2}/\mathbb{F}_s}(h) = 1 \text{ since } N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(h) = h\bar{h} = 1.$$

According to Hilbert 90 there exists $z \in \mathbb{F}_{q^2}^*$ with $h = z(\sigma^t(z))^{-1}$. Let $y = (-2)^{-1} z\bar{z}$, then τ has at least three fixed points

$$[1,0,0],\ [0,1,0],\ [1,y,z]$$

in Ω. Note that the last one is fixed by τ since

$$y = (-2)^{-1} z\bar{z} = (-2)^{-1} h\bar{h}\sigma^t(z\bar{z}) = (-2)^{-1}\sigma^t(z\bar{z}) = \sigma^t(y).$$

We conclude that in all cases τ has at least three fixed points in Ω.

In order to prove that $\ker(\phi) \subset J$, we remark that $\ker(\phi)$ is generated by elements of the types

$$\tau(h,t),\ \begin{pmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & f & g \end{pmatrix} \text{ with } f \neq 0, \text{ and } \begin{pmatrix} a & 0 & 0 \\ 0 & \bar{a}^{-1} & 0 \\ 0 & 0 & \bar{a}a^{-1} \end{pmatrix}.$$

Elements of the type $\tau(h,t)$ are contained in J by 3.1. Elements of the second type are contained in $T \subset J$ since their matrices have no eigenvectors but multiples of $(1,0,0)$.

In order to handle the third type, we distinguish three cases. Choose $h \in \mathbb{F}_{q^2}^*$ such that $\tau(h,k) \in G$. Let

$$A = \begin{pmatrix} a & 0 & 0 \\ 0 & \bar{a}^{-1} & 0 \\ 0 & 0 & \bar{a}a^{-1} \end{pmatrix} \in \ker(\phi).$$

If $2f/k$ is even, i. e. $\mathbb{F}_{q^2}^{\sigma^k} \subset \mathbb{F}_q$, and $N(a) = 1$, then choose

by Hilbert 90 an element $e \in \mathbb{F}_{q^2}^*$ with $a = e^{-1}\sigma^k(e)$. Now

$$A = \tau(h,k)\begin{pmatrix} e & 0 & 0 \\ 0 & \bar{e}^{-1} & 0 \\ 0 & 0 & \bar{e}e^{-1} \end{pmatrix}\tau(h,k)^{-1}\begin{pmatrix} e^{-1} & 0 & 0 \\ 0 & \bar{e} & 0 \\ 0 & 0 & e\bar{e}^{-1} \end{pmatrix}$$

is contained in $G'_\alpha \subset J$.

If $2f/k$ is even and $N(a) = -1$, then $N(a\bar{a}) = (N(a))^2 = 1$. By Hilbert 90 we can choose $e \in \mathbb{F}_{q^2}^*$ such that $a\bar{a} = e^{-1}\sigma^k(e)$. We have

$$e + \bar{e} = e + \sigma^f(e) = e(1 + \prod_{i=0}^{(f/k)-1} \sigma^{ik}(e^{-1}\sigma^k(e))) =$$

$$e(1 + \prod_{i=0}^{(f/k)-1} \sigma^{ik}(a\bar{a})) = e(1 + N(a)) = 0;$$

hence $[1,e,0] \in \Omega$. Now $A\tau(h,k)$ has at least three fixed points

$$[1,0,0],\ [0,1,0],\ [1,e,0]$$

in Ω, and is contained in $\langle T \rangle \subset J$ by 3.1. Since $\tau(h,k) \in J$ we get $A \subset J$.

If $2f/k$ is odd and $N(a) = 1$, then $a\bar{a} \in \mathbb{F}_q$ and $N_{\mathbb{F}_q/\mathbb{F}_r}(a) = 1$. By Hilbert 90 in the extension $\mathbb{F}_q/\mathbb{F}_r$ we can choose $e \in \mathbb{F}_q^*$ such that $a\bar{a} = e^{-1}\sigma^k(e)$. Choose

$$n \in (\mathbb{F}_{q^2}^{\sigma^k})^*$$

such that $n + \bar{n} = 0$. Since $e = \bar{e}$, we have $[1,ne,0] \in \Omega$. Now $A\tau(h,k)$ has at least three fixed points

$$[1,0,0],\ [0,1,0],\ [1,ne,0]$$

in Ω, and $A \in J$ as above.

In all three cases we have $A \in J$. We conclude that $\ker(\phi) \subset J$.

As for proving $J \subset \ker(\phi)$, note that it is immediate that $G'_\alpha \subset \ker(\phi)$. Furthermore, if $q > 2$, then $\mathrm{Ver}[PSU(3,q)]$ is trivial since $PSU(3,q)$ is simple; for $q = 2$ there is nothing to prove since $\ker(\phi) = G_\alpha$. By 3.2 we have $\mathrm{Ver}(\tau(h,t)) \in \langle T \rangle$ for all h, t for which $\tau(h,t) \in G$. Since G is generated by $PSU(3,q)$ and elements $\tau(h,t)$, we obtain $\mathrm{im}(\mathrm{Ver}) \subset \langle T \rangle$.

It remains to prove that $T \subset \ker(\phi)$. Let

$$B = \begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & f & g \end{pmatrix} \sigma^{kt}$$

be an arbitrary element of $G_\alpha \setminus \ker(\phi)$. If $2f/k$ is even then $N(a) \neq \pm 1$ and if $2f/k$ is odd then $N(a) \neq 1$.

A fixed point of B in $\Omega \setminus \{[1,0,0]\}$ must be of the form $[x,1,z]$ with

$$a\sigma^{kt}(x) + b + c\sigma^{kt}(z) = dx$$

and

$$f + g\sigma^{kt}(z) = dz.$$

Let $a\sigma^{kt}(x) - dx = 0$ for some $x \in \mathbb{F}_{q^2}^*$, then $x^{-1}\sigma^{kt}(x) = (a\bar{a})^{-1}$ and

$$1 = \Pi_{i=0}^{(2f/k)-1} \sigma^{ik}(x\sigma^{kt}(x)^{-1}) = \Pi_{i=0}^{(2f/k)-1} \sigma^{ik}(a\bar{a}).$$

If $2f/k$ is even, then the right hand term is equal to $N(a)^2$, if $2f/k$ is odd, then it is equal to $N(a)$; in both cases we have a contradiction. Hence the additive map

$$x \mapsto a\sigma^{kt}(x) - dx$$

on $\mathbb{F}_{q^2}$ is injective. The same can be said about the additive map

$$z \mapsto g\sigma^{kt}(z) - dz.$$

Consequently, there is precisely one point $[x,1,z]$ fixed by B. We do not yet know if it is contained in Ω; we see that at most one point in $\Omega \setminus \{[1,0,0]\}$ is fixed by B. But G_α and $\ker(\phi)$ are both transitive on $\Omega \setminus \{[1,0,0]\}$, so the average number of points in $\Omega \setminus \{[1,0,0]\}$ fixed by an element of $G_\alpha \setminus \ker(\phi)$ is one. Hence each $B \in G_\alpha \setminus \ker(\phi)$ has precisely one fixed point in $\Omega \setminus \{[1,0,0]\}$ and is therefore not contained in T. This establishes $T \subset \ker(\phi)$, so we are finished with (3).

(4) Let $q = 3^{2m+1}$, $m \geq 1$, and let σ be the field automorphism of $\mathbb{F}_q$ for which

$$\sigma^2(x) = x^3, \quad x \in \mathbb{F}_q.$$

Denote by $\omega(x,y,z)$ for $x, y, z \in \mathbb{F}_q$ the point $\lceil x,y,z,1,u,v,w \rceil \in \mathbb{P}^6(\mathbb{F}_q)$, where

$$u = x^2y + xz + \sigma(y) - x^3\sigma(x),$$
$$v = \sigma(xy) + \sigma(z) + xy^2 - yz - x^3\sigma(x^2)$$
$$w = -z^2 - xv - yu.$$

Put $\alpha = \lceil 0,0,0,0,0,0,1 \rceil$ and let Ω be the set consisting of α and all $\omega(x,y,z)$ for $x, y, z \in \mathbb{F}_q$.

By definition ${}^2G_2(q)$ is the subgroup of $PGl(7,q)$ stabilizing Ω setwise, see [T]. Furthermore, $Aut({}^2G_2(q))$ is the subgroup of $P\Gamma l(7,q)$ stabilizing Ω, i. e.,

$$Aut({}^2G_2(q)) = {}^2G_2(q).Aut(\mathbb{F}_q),$$

see [R]. For any $(a,b,c) \in \mathbb{F}_q^3$ there is a unique transformation $u_{a,b,c} \in PGl(7,q)$ such that ${u_{a,b,c}}^{\alpha} = \alpha$ and

$${u_{a,b,c}}^{\omega(x,y,z)} = \omega(x+a, \sigma(a)x+y+b, (a\sigma(a)-b)x+ay+z+c).$$

Thus

$$U = \{u_{a,b,c} \mid a, b, c \in \mathbb{F}_q\}$$

is a subgroup of ${}^2G_2(q)_{\alpha}$. Moreover, for $d \in \mathbb{F}_q^*$, the transformation $h_d \in PSl(7,q)$ corresponding to the diagonal matrix with entries

$$(d^{-1}\sigma(d^{-1}), d^{-1}, 1, d^{-2}\sigma(d^{-1}), d, d\sigma(d), d^2\sigma(d))$$

on the main diagonal belongs to ${}^2G_2(q)_{\alpha}$. We have

$${h_d}^{\omega(x,y,z)} = \omega(dx, d\sigma(d)y, d^2\sigma(d)z)$$

for $x, y, z \in \mathbb{F}_q$. Due to [T] we have

$${}^2G_2(q)_{\alpha} = U.\{h_d \mid d \in \mathbb{F}_q^*\}.$$

As a matter of fact, the group ${}^2G_2(q)$ is generated by ${}^2G_2(q)_{\alpha}$ and the element of $PGl(7,q)$ corresponding to the linear transformation of $\mathbb{F}_q^7$ permuting the basis vectors according to the permutation $(16)(25)(47)$.

Suppose ${}^2G_2(q) \leq G \leq Aut({}^2G_2(q))$. Write

$$k = [Aut({}^2G_2(q)) : G]$$

and choose $\tau \in Aut(\mathbb{F}_q)$ such that $G = {}^2G_2(q).\langle\tau\rangle$. Let $N : \mathbb{F}_q \to \mathbb{F}_q^{\tau}$

be the norm map and denote by ϕ the map from G_α to $(\mathbb{F}_q^\tau)^*$ given by

$$\phi(u_{a,b,c}h_d\tau^t) = N(d^2),$$

for $a, b, c, d \in \mathbb{F}_q$, $d \neq 0$, $t \in \mathbb{Z}$. We claim that $J = \ker(\phi)$. From this claim, part (d) of the theorem follows immediately.

First of all, U is regular on $\Omega \setminus \{\alpha\}$ and τ fixes at least three points of Ω, so that

$$U.\mathrm{Aut}(\mathbb{F}_q) \subset J \cap \ker(\phi).$$

next, suppose $h_d \in \ker(\phi)$ for some $d \in \mathbb{F}_q^*$. Since $N(d\sigma(d)) = 1$, there exists some $y \in \mathbb{F}_q^*$ with

$$y^{-1}\tau(y) = d^{-1}\sigma(d)^{-1}$$

by Hilbert 90. As α, $\omega(0,0,0)$ and $\omega(0,y,0)$ are three distinct points of Ω fixed by $h_d\tau$, we obtain from 3.1 that $h_d\tau$ and hence h_d is contained in J. This settles $\ker(\phi) \subset J$.

As for proving $J \subset \ker(\phi)$, it is clear that $G_\alpha' \subset \ker(\phi)$. Suppose

$$h = \tau^{-t}h_{d^{-1}}u_{a,b,c} \in G_\alpha \setminus \ker(\phi),$$

where $t \in \mathbb{Z}$ and $a, b, c, d \in \mathbb{F}_q$ with $d \neq 0$. If h fixes $\omega(x,y,z)$, then

$$x + a = d\tau^t(x),$$
$$\sigma(a)x + y + b = d\sigma(d)\tau^t(y),$$
$$(a\sigma(a) - b)x + ay + z + c = d^2\sigma(d)\tau^t(z).$$

Since $N(d)$, $N(d\sigma(d))$, $N(d^2\sigma(d)) \neq 1$ as $N(d^2) \neq 1$, we obtain similarly to the proof of (3) that there is a unique $\omega(x,y,z) \in \Omega \setminus \{\alpha\}$ fixed by h. This implies that

$$G_\alpha \setminus \ker(\phi) \subset G_\alpha \setminus T, \text{ whence } T \subset \ker(\phi).$$

It remains to prove that $\mathrm{im}(\mathrm{Ver}) \subset \ker(\phi)$. Since ${}^2G_2(q)$ is simple, the map Ver is trivial on ${}^2G_2(q)$. Further τ has at least $28 \geq 3$ fixed points

$$\alpha, \omega(x,y,z), x, y, z \in \mathbb{F}_3,$$

in Ω, so $\mathrm{Ver}(\tau) \in \langle T \rangle$ by 3.2. Hence

$$\mathrm{im}(\mathrm{Ver}) = \mathrm{Ver}[\langle {}^2G_2(q), \tau \rangle] \subset \langle T \rangle \subset \ker(\phi),$$

which concludes (4).

(5) Let $q = 2^{2m+1}$, $m \geq 1$, and let σ be the field automorphism of $\mathbb{F}_q$ for which

$$\sigma^2(x) = x^2, \quad x \in \mathbb{F}_q.$$

Denote by $\omega(x,y)$ for $x, y \in \mathbb{F}_q$ the point

$$\left[1, x, y, \sigma(y)+x^2\sigma(x)+xy\right] \in \mathbb{P}^3(\mathbb{F}_q).$$

Put $\alpha = [0,0,0,1]$ and let Ω be the set consisting of α and all $\omega(x,y)$ for $x, y \in \mathbb{F}_q$. Then ${}^2B_2(q)$ is by definition the subgroup of $PGl(4,q)$ stabilizing Ω setwise, see [L1]. Furthermore, we have

$$\mathrm{Aut}({}^2B_2(q)) = {}^2B_2(q).\mathrm{Aut}(\mathbb{F}_q),$$

see [S]. For any $(a,b) \in \mathbb{F}_q^2$ there is a unique transformation $u_{a,b} \in PGl(4,q)$ such that

$$u_{a,b}{}^{\alpha} = \alpha$$

and

$$u_{a,b}\omega(x,y) = \omega(x+a, y+\sigma(a)x+b), \quad x, y \in \mathbb{F}_q.$$

Thus

$$U = \{u_{a,b} \mid a, b \in \mathbb{F}_q\}$$

is a subgroup of ${}^2B_2(q)_{\alpha}$, regular on $\Omega\setminus\{\alpha\}$. Moreover, for $d \in \mathbb{F}_q^*$ the transformation $h_d \in PGl(4,q)$ corresponding to the diagonal matrix with main diagonal entries

$$(1,\ d,\ d\sigma(d),\ d^2\sigma(d))$$

belongs to ${}^2B_2(q)_{\alpha}$. We have

$$h_d\omega(x,y) = \omega(dx, d\sigma(d)y), \quad x, y \in \mathbb{F}_q.$$

Due to [L1], we have

$${}^2B_2(q)_{\alpha} = U.\{h_d \mid d \in \mathbb{F}_q^*\}.$$

As a matter of fact, ${}^2B_2(q)$ is generated by ${}^2B_2(q)_{\alpha}$ and the projective linear transformation permuting the basis vectors according to the permutation $(14)(23)$.

Suppose

$${}^2B_2(q) \leq G \leq \mathrm{Aut}({}^2B_2(q)).$$

Write $k = [\mathrm{Aut}({}^2B_2(q)) : {}^2B_2(q)]$ and choose $\tau \in \mathrm{Aut}(\mathbb{F}_q)$ such that

$$G = {}^2B_2(q).\langle\tau\rangle.$$

Let $N : \mathbb{F}_q \to \mathbb{F}_q^\tau$ be the norm map and denote by ϕ the map from G_α to $(\mathbb{F}_q^\tau)^*$ given by

$$\phi(u_{a,b}h_d\tau^t) = N(d),\ a, b, d \in \mathbb{F}_q,\ d \neq 0,\ t \in \mathbb{Z}.$$

We claim that $J = \ker(\phi)$. Obviously, part (e) of the theorem results from this claim.

As in the previous case, it is easily derived that

$$U.\mathrm{Aut}(\mathbb{F}_q) \subset J \cap \ker(\phi).$$

Suppose $h_d \in \ker(\phi)$ for some $d \in \mathbb{F}_q^*$. Since $N(d) = 1$, there is $x \in \mathbb{F}_q^*$ with $x^{-1}\tau(x) = d^{-1}$ by Hilbert 90. As α, $\omega(0,0)$ and $\omega(x,0)$ are distinct points of Ω fixed by $h_d\tau$, we obtain from 3.1 that $h_d\tau$ and hence h_d is contained in J. So far, we have shown that $\ker(\phi) \subset J$.

Conversely, suppose

$$h = \tau^{-t}h_{d^{-1}}u_{a,b} \in G_\alpha \setminus \ker(\phi),$$

where $a, b, d \in \mathbb{F}_q$, $d \neq 0$, $t \in \mathbb{Z}$. If h fixes $\omega(x,y) \in \Omega\setminus\{\alpha\}$, then

$$x + a = d\tau^t(x),$$
$$y + \sigma(a)x + b = d\sigma(d)\tau^t(y).$$

Since $N(d\sigma(d)) \neq 1$ whenever $N(d) \neq 1$ an argument similar to the one in the proof of (3) and (4) shows that h has a unique fixed point in $\Omega\setminus\{\alpha\}$. Therefore, we have $T \subset \ker(\phi)$. We have $G'_\alpha \subset \ker(\phi)$ obviously. The element τ has at least $5 \geq 3$ fixed points

$$\alpha,\ \omega(x,y),\ x, y \in \mathbb{F}_2,$$

in Ω, so

$$\mathrm{im}(\mathrm{Ver}) \subset \langle T\rangle \subset \ker(\phi)$$

as in the proof of (4). Hence $J \subset \ker(\phi)$. This ends the proof of (5), corresponding to part (e) of 1.1.

(6) Assume $m \geq 3$; if $m = 2$, then $Sp(2m,2) \simeq S_6 \simeq P\Sigma l(2,9)$ on 6 or 10 points; these cases occur in (1) and (2).

Consider the bilinear form $(.,.)$ on $\mathbb{F}_2^{2m}$ defined by

$$(x,y) = x_1y_2 + x_2y_1 + \dots + x_{2m-1}y_{2m} + x_{2m}y_{2m-1},$$

$$\text{for } x = (x_i),\ y = (y_i) \in \mathbb{F}_2^{2m}.$$

For $\varepsilon = \pm 1$, let G^{ε} be the subgroup of $PGl(2m,2)$ preserving $(.,.)$, viewed as a permutation group on the set of non-degenerate quadratic forms on $\mathbb{F}_2^{2m}$ of Witt index $m + \frac{1}{2}(\varepsilon - 1)$. Let α_ε for $\varepsilon = \pm 1$ be the quadratic form on $\mathbb{F}_2^{2m}$ given by

$$\alpha_1(x) = x_1x_2 + x_3x_4 + \dots + x_{2m-1}x_{2m}$$

and

$$\alpha_{-1}(x) = \alpha_1(x) + x_{2m-1}^2 + x_{2m}^2,$$

for $x = (x_i) \in \mathbb{F}_2^{2m}$. Then $G^{\varepsilon}_{\alpha_\varepsilon}$ is the full orthogonal group with respect to α_ε of order

$$2^{m^2-m+1}(2^m - \varepsilon)\prod_{i=1}^{m-1}(4^i - 1).$$

For $a \in \mathbb{F}_2^{2m}$, define $u_a \in Gl(2m,2)$ by

$$u_a(x) = x + (x,a)a,\ x \in \mathbb{F}_2^{2m}.$$

Any orthogonal transvection with respect to α_ε, see [D], is of the form u_a for some $a \in \mathbb{F}_2^{2m}$ with $\alpha_\varepsilon(a) = 1$. Since such u_a fix at least three non-degenerate quadratic forms of Witt index $m + \frac{1}{2}(\varepsilon - 1)$, they are elements of $\langle T \rangle$ by 3.1, and hence of J. Because $G^{\varepsilon}_{\alpha_\varepsilon}$ is generated by transvections, see [D], this yields $J = G^{\varepsilon}_{\alpha_\varepsilon}$.

Thus $R(G_\varepsilon)$ is trivial, which we had to prove for case (6).

(8) We have $G = A_7$ on the 15 points of $\mathbb{P}^3(\mathbb{F}_2)$. The stabilizer of a point is the simple group $Sl(3,2)$. Hence $R(G)$ is trivial.

(9) The cases $G = M_{11}$, M_{23} on 11, 23 points respectively have been dealt with in [Z], section 7. The groups M_{12}, M_{22}, M_{24} on 12, 22, 24 points respectively have stabilizers isomorphic to the simple groups M_{11}, PSl(3,4), M_{23}, so that R(G) is trivial in these cases too.

As for the remaining possibility, $G = \mathrm{Aut}(M_{22})$, the stabilizer of a point is equivalent to PΓl(3,4) on the 21 points of $\mathbb{P}^2(\mathbb{F}_4)$, as permutation group on the remaining points, see [L2]. Since the generator of $\mathrm{Aut}(\mathbb{F}_4)$ in this group fixes 7 points and the commutator subgroup of PΓl(3,4) is PSl(3,4), it follows that $J = G_\alpha$, so that R(G) is trivial.

(10) We have $G = M_{11}$ on the 12 points of a Hadamard 3-design. The stabilizer in G of one point is isomorphic to PSl(2,11). Since this group is simple, the group R(G) is trivial.

(11) The group G = HS is the simple group of D. G. Higman and C. C. Sims acting on the 176 points of a 2-design. The stabilizer of one point is isomorphic to PΣU(3,5) of order $2^5.3^2.5^3.7$. The simple group PSU(3,5) has index 2 in the stabilizer, while PΣU(3,5)\PSU(3,5) contains involutions that have 12 fixed points, see [Fr]. From 3.1 we obtain that R(G) is trivial.

(12) The group G = Co.3 is Conway's simple group .3 on a set of 276 points. The stabilizer of a point is isomorphic to Aut(Mc), where Mc stands for McLaughlin's simple group of order $2^7.3^6.5^3.7.11$. Since Mc has index 2 in Aut(Mc), and Aut(Mc)\Mc contains an involution with 12 fixed points, see [Fi], we obtain from 3.1 that R(G) is trivial.

The remaining part of the table (cases (13) to (21)) lists all subgroups G_0 of $\Gamma l(d,q)$ for which the action of G_0 on $(\mathbb{F}_q)^d \setminus \{0\}$ is transitive. The group G is generated by G_0 and $(\mathbb{F}_q)^d$, acting on $(\mathbb{F}_q)^d$. Let $\alpha = 0$, then $G_\alpha = G_0$. As always let $q = p^f$ for p prime.

Assume that $p > 2$; let $g \in G_0 \setminus T$. Then g has at least one fixed point $a \neq 0$ in $\Omega = (\mathbb{F}_q)^d$. But then λa is also a fixed point in Ω for each $\lambda \in \mathbb{F}_p^*$. From 3.1 we see that $g \in \langle T \rangle$, hence $\langle T \rangle = G_0$ and R(G) is trivial. Thus, for the cases (13) to (21) we may restrict to $p = 2$.

(13) $\quad Sl(d,2^f) \leq G_0 \leq \Gamma l(d,2^f)$.

Assume $d > 1$. The group G_0 is generated by $Sl(d,2^f)$ and elements of the type

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \vdots \\ \vdots & & & 1 \;\; 0 \\ 0 & \dots & 0 & a \end{pmatrix} \sigma$$

with $a \in \mathbb{F}_{2^f}^*$, $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^f})$. If $d > 2$ or $\langle \sigma \rangle \neq \mathrm{Aut}(\mathbb{F}_{2^f})$ then A has at least 4 fixed points

$$(b_1, b_2, \dots, b_{d-1}, 0)$$

for $b_i \in \mathbb{F}_{2^f}^{\sigma}$, $i = 1, \dots, d-1$, and we get $A \in \langle T \rangle$ by 3.1.

If $d = 2$ and $\langle \sigma \rangle = \mathrm{Aut}(\mathbb{F}_{2^f})$ then choose $b \in \mathbb{F}_{2^f}^*$ with $a = b\sigma(b^{-1})$. Then

$$(1,0),\ (1,b),\ (0,b),\ (0,0)$$

are all fixed points of A, so again $A \in \langle T \rangle$ by 3.1.

If $G_0 \neq Sl(2,2)$, then we have $Sl(d,2^f) \subset G_0' \subset J$. If $G_0 = Sl(2,2)$ then $G \simeq S_4 \simeq PGl(2,3)$, for which we found $R(G) \simeq \mathbb{Z}/2\mathbb{Z}$ in (2). This case is covered by part (b) of the theorem.

In all cases, except for $G_0 = Sl(2,2)$, we obtain $J = G_0$, and so R(G) is trivial.

It remains to consider $d = 1$, i. e., $G_0 \subset \langle \mathbb{F}_{2^f}^*, \mathrm{Aut}(\mathbb{F}_{2^f}) \rangle$, acting on $\Omega = \mathbb{F}_{2^f}$. Such a group can be written as

$$G_0 = \langle a, b\sigma \rangle,$$

with $G_0 \cap \mathbb{F}_{2^f}^* = \langle a \rangle$; $a, b \in \mathbb{F}_{2^f}^*$, $\sigma \in \mathrm{Aut}(\mathbb{F}_{2^f})$. Since G_0 is transitive

on $\Omega\setminus\{0\}$, we may assume that b generates $\mathbb{F}_{2^f}^*$ and $a \neq 1$. If σ does not generate $\mathrm{Aut}(\mathbb{F}_{2^f})$, then both a and $b\sigma$ have no fixed points in $\Omega\setminus\{0\}$, hence

$$G_0 \subset \langle T \rangle \subset J,$$

and R(G) is trivial. Next assume that σ generates $\mathrm{Aut}(\mathbb{F}_{2^f})$ and a does not generate $\mathbb{F}_{2^f}^*$. We may assume that $\sigma(b) = b^2$, then we have

$$a^k(b\sigma)^m(1) = a^k b^{2^m-1}$$

for integers k and m. For no values of k and m this expression equals b^{-1}; this contradicts the fact that G_0 is transitive on $\Omega\setminus\{0\}$. It remains to consider $G_0 = \langle \mathbb{F}_{2^f}^*, \mathrm{Aut}(\mathbb{F}_{2^f}) \rangle$; let σ generate $\mathrm{Aut}(\mathbb{F}_{2^f})$.

If f is not a prime power, then choose a generating set $\{\rho,\tau\}$ for $\mathrm{Aut}(\mathbb{F}_{2^f})$ such that none of its elements generates $\mathrm{Aut}(\mathbb{F}_{2^f})$; e.g., if m, n are non-trivial divisors of f with $\gcd(m,n) = 1$, then choose $\tau = \sigma^m$ and $\rho = \sigma^n$. Then both τ and ρ are contained in $\langle T \rangle$ since they have at least 4 fixed points, so

$$G_0 = \langle \mathbb{F}_{2^f}^*, \rho, \tau \rangle \subset \langle T \rangle \subset J,$$

and R(G) is trivial.

For the remaining case let f be some power of a prime number r. As above, we have

$$\langle \mathbb{F}_{2^f}^*, \sigma^r \rangle \subset \langle T \rangle.$$

If $a\sigma^m \in G_0 \setminus \langle \mathbb{F}_{2^f}^*, \sigma^r \rangle$, then σ^m generates $\mathrm{Aut}(\mathbb{F}_{2^f})$, and by Hilbert 90 there exists $x \in \mathbb{F}_{2^f}^*$ with $a\sigma^m(x) = x$. Hence $a\sigma^m \notin T$, and we obtain

$$\langle \mathbb{F}_{2^f}^*, \sigma^r \rangle = \langle T \rangle = \langle T, G_0' \rangle.$$

We see that R(G) is cyclic of order r or 1; it remains to compute im(Ver). The group

$$G = \{x \mapsto a\sigma(x) + b \mid a, b \in \mathbb{F}_{2^f},\ a \neq 0\}$$

is generated by

$$g_b = (x \mapsto x + b),\ h_a = (x \mapsto ax),\ a, b \in \mathbb{F}_{2^f}^*, \text{ and } \sigma.$$

We use the notation from the proof of 3.2; elements of im(Ver) are considered modulo G_0'. For $b \in \mathbb{F}_{2^f}^*$, all of the orbits of g_b have length 2. So

$$\mathrm{Ver}(g_b) = \Pi_{i=1}^{t} s_i g_b^2 s_i^{-1} = 1,$$

since $g_b^2 = 1$. If $a \neq 1$ then 0 is the only fixed point of h_a. Moreover, $h_a^k = h_{a^k}$ for any positive integer k. Thus

$$\mathrm{Ver}(h_a) = \prod_{i=1}^{t} s_i h_a^{f_i} s_i^{-1} = h_a \cdot \prod_{f_i>1} s_i h_a^{f_i} s_i^{-1}.$$

We have $h_a \in T$ and $s_i h_a^{f_i} s_i^{-1} \in \langle T \rangle$ for $f_i \geq 2$; the latter since $h_a^{f_i} = h_{a^{f_i}}$ has at least $1 + f_i \geq 3$ fixed points. So

$$\mathrm{Ver}(h_a) \in \langle T \rangle.$$

The element σ has exactly 2 fixed points 0 and 1. For the s_i corresponding to these two points, we may choose the identity and

$$s = (x \mapsto x+1)$$

respectively. As for h_a, we get

$$\prod_{f_i>1} s_i \sigma^{f_i} s_i^{-1} \in \langle T \rangle.$$

Modulo $\langle T \rangle$ we have

$$\mathrm{Ver}(\sigma) \equiv \sigma s \sigma s^{-1} = \sigma^2.$$

Hence J is generated by T and σ^2. Since σ^2 is trivial in $G_0/\langle T \rangle$ if and only if $r = 2$, we conclude that

$$R(G) \simeq \mathbb{Z}/2\mathbb{Z}$$

for $r = 2$, and that R(G) is trivial for $r \neq 2$. This finishes case (13).

(14) The group G_0 contains $Sp(2d,2^f)$ as a normal subgroup. Let $q = 2^f$. First we show that the condition on G_0 is equivalent to

$$Sp(2d,q) \leq G_0 \leq (\mathbb{F}_q^* \times Sp(2d,q)).\mathrm{Aut}(\mathbb{F}_q).$$

According to [Ct] and [D] we have

$$\mathrm{Aut}(Sp(2d,q)) = Sp(2d,q).\mathrm{Aut}(\mathbb{F}_q)$$

for $d > 2$, and

$$\mathrm{Aut}(Sp(4,q)) = Sp(4,q).\mathrm{Aut}(\mathbb{F}_q).\langle \delta \rangle,$$

where δ is a "graph"-automorphism, interchanging transvections and (2,2)-involutions of Sp(4,q).

Let $g \in \Gamma l(2d,q)$ normalize $Sp(2d,q)$. Then g induces an automorphism $\bar{g}$ of $Sp(2d,q)$. If $d = 2$, and

$$\bar{g} \in Sp(4,q).Aut(\mathbb{F}_q).\delta,$$

then g would send the set of fixed points of a transvection into the set of fixed points of a (2,2)-involution, i. e., a 3-dimensional linear subspace into a 2-dimensional one, which is absurd. Hence

$$\bar{g} \in Sp(2d,q).Aut(\mathbb{F}_q),$$

for any $d > 1$. It follows that there exist $\lambda \in \Gamma l(2d,q)$ centralizing $Sp(2d,q)$ and $h \in Sp(2d,q).Aut(\mathbb{F}_q)$ such that $g = h\lambda$. By Schur's lemma and [H1], the element λ is a homothety by an element of $\mathbb{F}_q^*$. This shows

$$Sp(2d,q) \leq G_0 \leq (\mathbb{F}_q^* \times Sp(2d,q)).Aut(\mathbb{F}_q).$$

If $\tau \in \mathbb{F}_q^*.Aut(\mathbb{F}_q)$ has a fixed point in $(\mathbb{F}_q)^{2d}$ distinct from 0, then that fixed point has a coefficient $a \neq 0$. But then each element of $(\mathbb{F}_q)^{2d}$ with coefficients 0 and a is a fixed point, and since there are $2^{2d} \geq 3$ of them, we have $\tau \in \langle T \rangle$ by 3.1.

It remains to show that

$$Sp(2d,q) \subset J.$$

Since $Sp(2,q) = Sl(2,q)$ was considered in (13), we may restrict to $d \geq 2$. If d and q are not both equal to 2, the assertion is clear since then $Sp(2d,q)$ is equal to its commutator subgroup as a simple group. For d and q both equal to 2, we have

$$Sp(4,2) \simeq S_6,$$

where the action of $Sp(4,2)$ on $(\mathbb{F}_2)^4 \setminus \{0\}$ corresponds to the action of S_6 on the 15 2-cycles on 6 symbols. One 2-cycle in S_6 leaves $\binom{4}{2} = 6 \geq 2$ of these 2-cycles invariant, hence $\langle T \rangle$ contains a 2-cycle by 3.1. Since S_6 is generated by S_6' and a 2-cycle, this proves

$$Sp(4,2) \subset \langle T, G_0' \rangle \subset J.$$

This concludes (14).

(15) $G_2(2^f) \leq G_0 \leq (\mathbb{F}_{2^f}^* \times G_2(2^f)).\mathrm{Aut}(\mathbb{F}_{2^f})$.

We obtain $G_0 \cap (\mathbb{F}_{2^f}^*.\mathrm{Aut}(\mathbb{F}_{2^f})) \subset \langle T \rangle$ as in (14). It remains to show that $G_2(2^f) \subset J$. For $f > 1$ this is clear since $G_2(2^f)' = G_2(2^f)$ as a simple group.

Let $f = 1$. We have

$$G_2(2) = \langle G_2(2)', \sigma \rangle,$$

where $\sigma \in G_2(2)$ generates a root subgroup of $G_2(2)$ of order 2, in the terminology of [Ct]. Moreover, the action of $G_2(2)$ on the 63 nonzero vectors can be identified with the action of the group on the points of the classical generalized hexagon of order (2,2), in which σ is known to fix 7 points. So $\sigma \in J$ by 3.1, hence $G_2(2) \subset J$, thus finishing (15).

(16), (17), (20). The group R(G) is trivial since $p \neq 2$.

(18), (19), (21). The group R(G) is trivial since $G_0' = G_0$ as G_0 is a simple group.

This concludes the proof of theorem 1.1.

REFERENCES.

[A] M. Aschbacher, *The classification of the finite simple groups,* The Mathematical Intelligencer 3 (1981), 59-65.

[Cm] P. J. Cameron, *Finite permutation groups and finite simple groups,* Bull. London Math. Soc. 13 (1981), 1-22.

[Ct] R. W. Carter, *Simple groups of Lie type,* Wiley, New York, 1972.

[D] J. Dieudonné, *La géometrie des groupes classiques,* 2nd ed., Springer, Berlin, 1963.

[Fi] L. Finkelstein, *The maximal subgroups of Conway's group C_3 and McLaughlin's group,* J. Algebra 25 (1973), 58-89.

[Fr] J. S. Frame, *Computation of characters of the Higman-Sims group and its automorphism group,* J. Algebra 20 (1972), 320-349.

[H1] Ch. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order,* Geometriae Dedicata 2 (1974), 425-460.

[H2] Ch. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II,* preprint.

[Hu] B. Huppert, *Endliche Gruppen I,* Springer, Berlin, 1967.

[K] W. M. Kantor, *2-Transitive designs,* in *Combinatorics, Part 3: Combinatorial group theory,* M. Hall, Jr., and J. H. van Lint (eds.), M.C. Tract 57, Math. Centrum, Amsterdam, 1975.

[L1] H. Lüneburg, *Die Suzukigruppen und ihre Geometrieen,* Lecture Notes in Mathematics 10, Springer, Berlin, 1965.

[L2] H. Lüneburg, *Transitive Erweiterungen endlicher Permutationsgruppen,* Lecture Notes in Mathematics 84, Springer, Berlin, 1969.

[N] M. E. O'Nan, *Open problems in primitive permutation groups,* contribution to the Santa Cruz Conference on finite groups, 1979.

[R] R. Ree, *A family of simple groups associated with the simple Lie algebra of type (G_2),* American J. Math. 83 (1961), 432-462.

[S] M. Suzuki, *On a class of doubly transitive groups,* Annals of Math. (2) 75 (1962), 105-145.

[T] J. Tits, *Les groupes simples de Suzuki et de Ree,* Sém. Bourbaki 210 (1960/1961).

[Z] H. Zantema, *Integer valued polynomials over a number field,* part I of this thesis, also Manuscripta math. 40 (1982), 155-203.

PART III

GLOBAL RESTRICTIONS ON RAMIFICATION IN NUMBER FIELDS

by H. Zantema.

manuscripta
mathematica

ABSTRACT.

Let G be the Galois group of a number field extension. For each prime $\underline{p}$ a map

$$\varepsilon(\underline{p}): H^2(G,\{\pm 1\}) \to \{\pm 1\}$$

is defined. This local symbol has a global restriction: the product of $\varepsilon(\underline{p})$ over all primes is trivial. This paper discusses how to compute $\varepsilon(\underline{p})$ and gives an application to integer valued polynomials over certain quartic number fields.

KEY WORDS:

number field, ramification, Brauer group, Pólya field.

1980 MATHEMATICAL SUBJECT CLASSIFICATION:

12A40, 12A60.

III-1

GLOBAL RESTRICTIONS ON RAMIFICATION IN NUMBER FIELDS.

1. INTRODUCTION.

Let M/K be a normal extension of number fields with Galois group G. Let G act trivially on $\{\pm 1\}$. In this paper we define for each prime $\underline{p}$ of K a group homomorphism

$$\varepsilon(\underline{p}): H^2(G,\{\pm 1\}) \to \{\pm 1\},$$

which is trivial for $\underline{p}$ unramified in M/K. This map has the following property (proposition 2.1):

For all $\alpha \in H^2(G,\{\pm 1\})$ *we have*

$$\prod_{\underline{p}} \varepsilon(\underline{p})(\alpha) = 1,$$

where the product runs over all finite and infinite primes of K.

The proof makes use of the structure of Brauer groups of global fields.

For $\alpha \in H^2(G,\{\pm 1\})$ we can determine $\varepsilon(\underline{p})(\alpha)$ as follows. Let α correspond to the extension

$$0 \to \{\pm 1\} \to X \xrightarrow{\pi} G \to 0.$$

Let $\hat{G}_{\underline{p}}$ be the Galois group of the algebraic closure of $K_{\underline{p}}$ over $K_{\underline{p}}$; there is a natural map $\rho: \hat{G}_{\underline{p}} \to G$. Now $\varepsilon(\underline{p})(\alpha) = 1$ if and only if there exists a group homomorphism $\tilde{\rho}: \hat{G}_{\underline{p}} \to X$ for which $\pi \circ \tilde{\rho} = \rho$. For infinite primes $\underline{p}$ the group $\hat{G}_{\underline{p}}$ contains either one or two elements, and computing $\varepsilon(\underline{p})(\alpha)$ is easy.

For odd primes $\underline{p}$ we give a description how to compute $\varepsilon(\underline{p})(\alpha)$ in terms of α, the norm of $\underline{p}$, the decomposition group, the inertia group and the Frobenius element; see 3.1. Further we give in section 3 a relation to Stickelberger's congruence and to the quadratic reciprocity law.

For even primes $\underline{p}$ computing $\varepsilon(\underline{p})(\alpha)$ is more difficult; we only give results in the abelian case in 4.1 and 4.2.

Originally this paper was motivated by the result of section 5. In 5.1 a Pólya field is defined as a number field with a particular

condition on the module of integer valued polynomials, which was first investigated by G. Pólya, [P], in 1919. A number field with a trivial class group is always a Pólya field. In the study of Pólya fields in [Z] an exceptional role was played by quartic fields for which the Galois group of the normal closure over $\mathbb{Q}$ is isomorphic to S_4. Using the methods of [Z] it could only be proven that for such a Pólya field K the class number h(K) is either one or two. In section 5 we assume that h(K) = 2, and derive many restrictions on the ramification behaviour in K. Ultimately in 5.5 a contradiction to the product formula 2.1 is found, so that a quartic number field K of this type is a Pólya field if and only if h(K) = 1.

2. BASIC FACTS.

Let M/K be a normal extension of number fields, let G = Gal(M/K). Let $\bar{K}$ be an algebraic closure of K containing M. For each prime $\underline{p}$ of K choose a place of $\bar{K}$ above $\underline{p}$, which is also denoted by $\underline{p}$. Let $G_{\underline{p}}$ be the decomposition group of $\underline{p}$ in M/K. Write $\hat{G} = \mathrm{Gal}(\bar{K}/K)$ and $\hat{G}_{\underline{p}} = \mathrm{Gal}(\bar{K}_{\underline{p}}/K_{\underline{p}})$. The short exact sequence

$$0 \to \{\pm 1\} \to \bar{K}^*_{\underline{p}} \xrightarrow{\square} \bar{K}^*_{\underline{p}} \to 0,$$

where $\square$ denotes taking the square, gives rise to an exact sequence

$$H^1(\hat{G}_{\underline{p}}, \bar{K}^*_{\underline{p}}) \to H^2(\hat{G}_{\underline{p}}, \{\pm 1\}) \to \mathrm{Br}(K_{\underline{p}}) \xrightarrow{\square} \mathrm{Br}(K_{\underline{p}}),$$

where $\mathrm{Br}(K_{\underline{p}}) = H^2(\hat{G}_{\underline{p}}, \bar{K}^*_{\underline{p}})$ is the Brauer group of $K_{\underline{p}}$. This Brauer group is known to be isomorphic to $\mathbb{Q}/\mathbb{Z}$ for finite primes, cf. [S1], chapter XIII, prop. 6; it is cyclic of order 2 for $\underline{p}$ real in K, and trivial for $\underline{p}$ complex in K. The group

$$H^1(\hat{G}_{\underline{p}}, \bar{K}^*_{\underline{p}})$$

is trivial by Hilbert 90, hence we have

$$H^2(\hat{G}_{\underline{p}}, \{\pm 1\}) \simeq \{\pm 1\}$$

for finite and real primes.

Define

$$\varepsilon(\underline{p}): H^2(G,\{\pm 1\}) \to \{\pm 1\}$$

to be the composition of the maps in the commutative diagram

$$\begin{array}{ccc} H^2(G,\{\pm 1\}) & \overset{\text{Res}}{\to} & H^2(G_{\underline{p}},\{\pm 1\}) \\ \text{Inf}\downarrow & & \text{Inf}\downarrow \\ H^2(\hat{G},\{\pm 1\}) & \overset{\text{Res}}{\to} & H^2(\hat{G}_{\underline{p}},\{\pm 1\}) \simeq \{\pm 1\} \end{array}$$

for finite and real primes $\underline{p}$; define $\varepsilon(\underline{p})$ to be trivial for complex primes $\underline{p}$. Sometimes the map $\text{Inf}: H^2(G_{\underline{p}},\{\pm 1\}) \to H^2(\hat{G}_{\underline{p}},\{\pm 1\}) \simeq \{\pm 1\}$ is by abuse of language called $\varepsilon(\underline{p})$ too.

PROPOSITION 2.1. If $\underline{p}$ is unramified in M/K, then $\varepsilon(\underline{p})$ is trivial. If $\alpha \in H^2(G,\{\pm 1\})$, then

$$\prod_{\underline{p}} \varepsilon(\underline{p})(\alpha) = 1,$$

where the product runs over all finite and infinite primes of K.

PROOF. This is immediate from the structure of the Brauer group of K, as is used in deriving class field theory, cf. [CF], chapter VII, 10.2, theorem B. □

The next proposition is a tool for computing $\varepsilon(\underline{p})$ in concrete situations.

PROPOSITION 2.2. Let $\alpha \in H^2(G,\{\pm 1\})$ and let

$$0 \to \{\pm 1\} \to X \overset{\pi}{\to} G \to 0$$

be the group extension corresponding to α. Let $\underline{p}$ be a prime of K and let ρ be the composition of the natural maps

$$\hat{G}_{\underline{p}} \to G_{\underline{p}} \to G.$$

Then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if there is a homomorphism

$$\tilde{\rho}: \hat{G}_{\underline{p}} \to X$$

such that $\pi \circ \tilde{\rho} = \rho$.

Before proving 2.2 we make some remarks. In terms of fields this proposition means that $\varepsilon(\underline{p})(\alpha) = 1$ if and only if either the exact sequence

$$(*) \qquad 0 \to \{\pm 1\} \to \pi^{-1}(G_{\underline{p}}) \xrightarrow{\pi} G_{\underline{p}} \to 0$$

is split, or there exists a quadratic extension F of $M_{\underline{p}}$, normal over $K_{\underline{p}}$, and an isomorphism

$$\mu\colon \mathrm{Gal}(F/K_{\underline{p}}) \xrightarrow{\simeq} \pi^{-1}(G_{\underline{p}})$$

such that $\pi\circ\mu$ is the composition of the natural maps

$$\mathrm{Gal}(F/K_{\underline{p}}) \to \mathrm{Gal}(M_{\underline{p}}/K_{\underline{p}}) \xrightarrow{\simeq} G_{\underline{p}}.$$

Because $M_{\underline{p}}$ has only finitely many quadratic extensions, the problem of computing $\varepsilon(\underline{p})(\alpha)$ has become finite now. The sequence (*) is split if and only if $\mathrm{Res}(\alpha)$ is trivial in $H^2(G_{\underline{p}},\{\pm 1\})$.

Let $I_{\underline{p}}$ be the inertia group in $M_{\underline{p}}/K_{\underline{p}}$. The group $G_{\underline{p}}/I_{\underline{p}}$ is cyclic, so $H^2(G_{\underline{p}}/I_{\underline{p}},\{\pm 1\})$ contains at most one non-trivial element. If also

$$\mathrm{Inf}[H^2(G_{\underline{p}}/I_{\underline{p}},\{\pm 1\})] \subset H^2(G_{\underline{p}},\{\pm 1\})$$

contains a non-trivial element α', then for α' the unique unramified quadratic extension of $M_{\underline{p}}$ has the required property, so $\varepsilon(\underline{p})(\alpha') = 1$.

If $\underline{p}$ is infinite then clearly $\varepsilon(\underline{p})(\alpha) = 1$ if and only if the sequence (*) is split.

PROOF OF 2.2. The element $\varepsilon(\underline{p})(\alpha)$ of $H^2(\hat{G}_{\underline{p}},\{\pm 1\})$ corresponds to the group extension

$$0 \to \{\pm 1\} \to \{\ (x,g) \in X \times \hat{G}_{\underline{p}} \mid \pi(x) = \rho(g)\ \} \xrightarrow{\phi} \hat{G}_{\underline{p}} \to 0,$$

where ϕ is defined by $\phi(x,g) = g$.

If $\varepsilon(\underline{p})(\alpha) = 1$, then this sequence is split, i.e. there exists a homomorphism

$$\psi\colon \hat{G}_{\underline{p}} \to \{\ (x,g) \in X \times \hat{G}_{\underline{p}} \mid \pi(x) = \rho(g)\ \}$$

for which $\phi\circ\psi$ is the identity on $\hat{G}_{\underline{p}}$. Now choose $\tilde{\rho}$ to be the composition of ψ and the projection on the X-coordinate; clearly $\pi\circ\tilde{\rho} = \rho$ is satisfied.

Conversely, assume that there exists such a map $\tilde{\rho}$. Then the map

$$\psi: \hat{G}_{\underline{p}} \to \{ (x,g) \in X \times \hat{G}_{\underline{p}} \mid \pi(x) = \rho(g) \}$$

defined by $\psi(g) = (\tilde{\rho}(g),g)$ makes the sequence split, hence $\varepsilon(\underline{p})(\alpha) = 1$. □

3. ODD PRIMES.

Let $N(\underline{p})$ be the cardinality and p the characteristic of the residue class field of $K_{\underline{p}}$. Let $I_{\underline{p}}$ and $V_{\underline{p}}$ be the inertia group and the first ramification group in $M_{\underline{p}}/K_{\underline{p}}$, respectively. As in 2.2 let $\alpha \in H^2(G,\{\pm 1\})$ correspond to

$$0 \to \{\pm 1\} \to X \xrightarrow{\pi} G \to 0.$$

If $N(\underline{p})$ is odd then

$$\{ x \in \pi^{-1}(V_{\underline{p}}) \mid \text{order}(x) \text{ is a } p\text{-power} \}$$

is a normal subgroup of $\pi^{-1}(G_{\underline{p}})$, isomorphic to $V_{\underline{p}}$, which we also denote by $V_{\underline{p}}$.

PROPOSITION 3.1. Let $N(\underline{p})$ be odd. Choose $s \in \pi^{-1}(G_{\underline{p}})$ such that $\pi(s).I_{\underline{p}}$ is the Frobenius element of $G_{\underline{p}}/I_{\underline{p}}$. Choose $a \in \pi^{-1}(I_{\underline{p}})$ such that $\pi(a).V_{\underline{p}}$ is a generator of $I_{\underline{p}}/V_{\underline{p}}$. Then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if

$$s\, a^{-1}\, s^{-1}\, a^{N(\underline{p})} \in V_{\underline{p}}.$$

PROOF. First assume that $M_{\underline{p}}/K_{\underline{p}}$ is tamely ramified, i.e. $V_{\underline{p}}$ is trivial. Let $\hat{G}_{\underline{p},t}$ be the Galois group of the maximal tamely ramified extension of $K_{\underline{p}}$ over $K_{\underline{p}}$. Let

$$\rho: \hat{G}_{\underline{p},t} \to G_{\underline{p}}$$

be the natural projection. Now $\varepsilon(\underline{p})(\alpha) = 1$ if and only if there exists a homomorphism

$$\tilde{\rho}: \hat{G}_{\underline{p},t} \to \pi^{-1}(G_{\underline{p}})$$

with $\pi\circ\tilde{\rho} = \rho$. The group $\hat{G}_{\underline{p},t}$ is known; it is the profinite group on two generators $\hat{s}$ and $\hat{a}$, and one relation

$$\hat{s}\,\hat{a}^{-1}\,\hat{s}^{-1}\,\hat{a}^{N(\underline{p})} = 1,$$

compare [S2], II 5.6, exercise 1. Here $\hat{s}$ is a representative in $\hat{G}_{\underline{p},t}$ of the Frobenius automorphism of the maximal unramified extension of $K_{\underline{p}}$, and $\hat{a}$ is a generator of the inertia group in $\hat{G}_{\underline{p},t}$. The elements $\hat{s}$ and $\hat{a}$ may be chosen in such a way that

$$\rho(\hat{a}) = \pi(a) \text{ and } \rho(\hat{s}) = \pi(s).$$

If $\varepsilon(\underline{p})(\alpha) = 1$ then there is a homomorphism $\tilde{\rho}$ with $\pi\circ\tilde{\rho} = \rho$, so

$$\tilde{\rho}(\hat{a}) = \pm a \text{ and } \tilde{\rho}(\hat{s}) = \pm s.$$

Since $N(\underline{p})$ is odd and -1 is central in X, we then have

$$s\,a^{-1}\,s^{-1}\,a^{N(\underline{p})} = \tilde{\rho}(\hat{s}\,\hat{a}^{-1}\,\hat{s}^{-1}\,\hat{a}^{N(\underline{p})}) = 1.$$

Conversely if $s\,a^{-1}\,s^{-1}\,a^{N(\underline{p})} = 1$, then defining $\tilde{\rho}(\hat{s}) = s$ and $\tilde{\rho}(\hat{a}) = a$ gives rise to a homomorphism $\tilde{\rho}$ with $\pi\circ\tilde{\rho} = \rho$, so $\varepsilon(\underline{p})(\alpha) = 1$. This proves the proposition for the tamely ramified case.

For the wildly ramified case, i.e. $V_{\underline{p}}$ is not trivial, consider the following commutative diagram:

$$\begin{array}{ccc} H^2(G_{\underline{p}}/V_{\underline{p}},\{\pm1\}) & \xrightarrow{\text{Inf}} & H^2(G_{\underline{p}},\{\pm1\}) \\ & \searrow^{\text{Inf}} \quad \nearrow_{\text{Inf}} & \\ & H^2(\hat{G}_{\underline{p}},\{\pm1\}) \simeq \{\pm1\} & \end{array}$$

The groups $H^i(V_{\underline{p}},\{\pm1\})$ are trivial, $i = 1, 2$, since $|V_{\underline{p}}|$ is odd. Hence we see from the inflation-restriction sequence that the upper arrow is an isomorphism. This isomorphism evaluated in the element corresponding to

$$0 \to \{\pm1\} \to \pi^{-1}(G_{\underline{p}})/V_{\underline{p}} \to G_{\underline{p}}/V_{\underline{p}} \to 0$$

gives exactly $\text{Res}(\alpha) \in H^2(G_{\underline{p}},\{\pm1\})$, which can be verified directly. Remark that $G_{\underline{p}}/V_{\underline{p}}$ is the Galois group of the maximal tamely ramified subextension of $M_{\underline{p}}/K_{\underline{p}}$ over $K_{\underline{p}}$. Applying the above result for this tamely ramified extension completes the proof of 3.1. □

PROPOSITION 3.2. Let $N(\underline{p})$ be odd and assume that the Sylow 2-group of $G_{\underline{p}}$ is cyclic and non-trivial. Then $H^2(G_{\underline{p}},\{\pm 1\})$ contains only one non-trivial element α. Assume further that $G_{\underline{p}}/V_{\underline{p}}$ is abelian. Then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if $2[I_{\underline{p}}:V_{\underline{p}}]$ is a divisor of $N(\underline{p}) - 1$.

PROOF. Let S be a Sylow 2-group of $G_{\underline{p}}$. According to [H], IV, 2.8, there exists a normal subgroup N of $G_{\underline{p}}$ with $G_{\underline{p}}/N \simeq S$. Since $H^i(N,\{\pm 1\})$ is trivial for $i = 1, 2$, the inflation-restriction sequence gives an isomorphism

$$\text{Inf: } \{\pm 1\} \simeq H^2(G_{\underline{p}}/N,\{\pm 1\}) \xrightarrow{\simeq} H^2(G_{\underline{p}},\{\pm 1\}).$$

This proves the first part of the proposition. The map

$$\text{Res: } H^2(G_{\underline{p}},\{\pm 1\}) \to H^2(S,\{\pm 1\}) \simeq \{\pm 1\}$$

is injective because $\text{Cor}\circ\text{Res}$ is the same as multiplication by $[G_{\underline{p}}:S]$, which is odd. So $\text{Res}(\alpha)$ is non-trivial in $H^2(S,\{\pm 1\})$, hence $\pi^{-1}(S)$ is cyclic for π corresponding to α. Hence $\pi^{-1}(I_{\underline{p}})/V_{\underline{p}}$ is cyclic of order $2[I_{\underline{p}}:V_{\underline{p}}]$. Remark that $\pi^{-1}(G_{\underline{p}})/V_{\underline{p}}$ is abelian if $G_{\underline{p}}/V_{\underline{p}}$ is abelian. The second part of the proposition is now immediate from 3.1. □

As an example we consider fields M, cyclic of degree 4 over $\mathbb{Q}$, in which 2 is unramified. We obtain from 2.1 and 3.2 that for such fields the expression

$$\prod_{p,e_p=4} (-1)^{(p-1)/4} \cdot \prod_{p,e_p=2} (-1)^{(p-1)/2}$$

equals 1 if M is real and equals -1 if M is complex. Here the products run over the prime numbers p, and e_p denotes the ramification index of p in $M/\mathbb{Q}$.

REMARK 3.3. Let M/K be quadratic and let Δ be the discriminant of M/K. This is an ideal of K. For each odd prime $\underline{p}$ of K, ramified in M/K, we have $\underline{p}|\Delta$ and $\underline{p}^2 \nmid \Delta$. If a prime $\underline{p}$ above 2 is ramified in M/K then $\underline{p}^2|\Delta$. Let k be the number of infinite primes of K ramified

in M/K. From 2.1 and 3.2 we now get

$$(-1)^k N(\Delta) \equiv 0 \text{ or } 1 \bmod 4,$$

where N denotes the absolute ideal norm. This property can also be considered as a direct consequence of Stickelberger's congruence in terms of ideles, see [F], theorem 2.6.

In a table we list all pairs $(G_{\underline{p}}, I_{\underline{p}})$ which can occur as a decomposition group and an inertia group of a prime in the normal closure of a number field extension of degree at most 5. The following notation is used:

$C_n = \mathbb{Z}/n\mathbb{Z}$; $V_4 = C_2 \times C_2$;

$D_n = < \sigma, \rho \ ; \ \sigma^2 = \rho^n = (\sigma\rho)^2 = 1 >$;

$L_5 = < \tau, \rho \ ; \ \tau^4 = \rho^5 = 1, \ \tau\rho\tau^{-1} = \rho^2 >$;

S_n and A_n are the symmetric and alternating groups on n symbols. If there is no restriction, it is indicated in the table by - .

For the cases that $N(\underline{p})$ is odd and $G_{\underline{p}}$ has a non-trivial cyclic Sylow 2-group, the result of 3.2 is mentioned in the last column. Here α is the non-trivial element of $H^2(G_{\underline{p}}, \{\pm 1\})$. Next we discuss the cases in the table with $N(\underline{p})$ is odd and $G_{\underline{p}}$ has no cyclic Sylow 2-group; these are cases 6, 9, 21 and 22.

First case 6, let $G_{\underline{p}} = V_4 = < s, a; s^2 = a^2 = (sa)^2 = 1 >$, and $I_{\underline{p}} = C_2 = <a>$. We list all elements of $H^2(G_{\underline{p}}, \{\pm 1\})$; in all cases let $\pi^{-1}(G_{\underline{p}})$ be generated by elements -1, s and a, which map to 1, s, $a \in G_{\underline{p}}$, respectively, while -1 is central of order 2.

relations in $\pi^{-1}(G_{\underline{p}})$	notation	isomorphism type of $\pi^{-1}(G_{\underline{p}})$
$s^2 = 1, a^2 = 1, (sa)^2 = 1$	(0,0,0)	C_2^3
$s^2 = -1, a^2 = 1, (sa)^2 = 1$	(1,0,0)	D_4
$s^2 = 1, a^2 = -1, (sa)^2 = 1$	(0,1,0)	D_4
$s^2 = 1, a^2 = 1, (sa)^2 = -1$	(0,0,1)	D_4
$s^2 = -1, a^2 = -1, (sa)^2 = 1$	(1,1,0)	$C_2 \times C_4$
$s^2 = -1, a^2 = 1, (sa)^2 = -1$	(1,0,1)	$C_2 \times C_4$
$s^2 = 1, a^2 = -1, (sa)^2 = -1$	(0,1,1)	$C_2 \times C_4$
$s^2 = -1, a^2 = -1, (sa)^2 = -1$	(1,1,1)	Q

TABLE TO SECTION 3.

no.	$I_{\underline{p}}$	$G_{\underline{p}}$	$N(\underline{p})$	2-rank of $H^2(G_{\underline{p}},\{\pm 1\})$	if $N(\underline{p})$ odd then $\varepsilon(\underline{p})(\alpha) = 1 \Leftrightarrow N(\underline{p}) \equiv$
1	C_2	C_2	-	1	1 mod 4
2	C_3	C_3	0,1 mod 3	0	
3	C_3	S_3	0,2 mod 3	1	-
4	S_3	S_3	0 mod 3	1	1 mod 4
5	C_2	C_4	-	1	1 mod 4
6	C_2	V_4	-	3	
7	C_4	C_4	0,1,2 mod 4	1	1 mod 8
8	V_4	V_4	0 mod 2	3	
9	C_4	D_4	0,2,3 mod 4	3	
10	V_4	D_4	0 mod 2	3	
11	D_4	D_4	0 mod 2	3	
12	V_4	A_4	0 mod 2	1	
13	A_4	A_4	0 mod 4	1	
14	A_4	S_4	0 mod 2	2	
15	C_5	C_5	0,1 mod 5	0	
16	C_2	$C_2 \times C_3$	-	1	1 mod 4
17	C_3	$C_2 \times C_3$	0,1 mod 3	1	-
18	$C_2 \times C_3$	$C_2 \times C_3$	0,1 mod 3	1	1 mod 4
19	C_5	D_5	0,4 mod 5	1	-
20	D_5	D_5	0 mod 5	1	-
21	S_3	$C_2 \times S_3$	0 mod 3	3	
22	$C_2 \times C_3$	$C_2 \times S_3$	0,2 mod 3	3	
23	C_5	L_5	0,2,3 mod 5	1	-
24	D_5	L_5	0 mod 5	1	-
25	L_5	L_5	0 mod 5	1	1 mod 8

From 3.1 we get the following.

If $N(\underline{p}) \equiv 1 \bmod 4$ then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if $\pi^{-1}(G_{\underline{p}})$ is abelian.

If $N(\underline{p}) \equiv 3 \bmod 4$ then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if

$$\alpha \in \{ (0,0,0), (1,0,1), (0,1,0), (1,1,1)\}.$$

As an example of this case 6 we consider fields M, normal over $\mathbb{Q}$ with $G = \mathrm{Gal}(M/\mathbb{Q}) \simeq V_4$, in which 2 is unramified. Applying 2.1 to the elements (1,1,0), (1,0,1) and (0,1,1) of $H^2(G,\{\pm 1\})$ gives nothing else than 2.1 applied to the quadratic subfields of M, i.e. Stickelberger's congruence in these subfields. If we apply 2.1 to (1,1,1) we get the following result. The expression

$$\prod_{p,e_p=2,f_p=1} (-1)^{(p-1)/2} \cdot \prod_{p,e_p=2,f_p=2} (-1)^{(p+1)/2}$$

equals 1 if M is real and equals -1 if M is complex. Here the products run over the prime numbers p, and e_p, f_p denote the ramification index and the residue class degree of p in $M/\mathbb{Q}$. Remark that an odd prime p is split in $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$, $\Delta \in \mathbb{Z}$, $p \nmid \Delta$, if and only if Legendre's symbol $(\frac{\Delta}{p})$ equals 1. For the particular field

$$M = \mathbb{Q}(\sqrt{((-1)^{(p-1)/2}.p)}, \sqrt{((-1)^{(q-1)/2}.q)}),$$

where p and q are odd prime numbers, the above result now turns out to be exactly equivalent to the quadratic reciprocity law.

The second case in the table for odd primes $\underline{p}$ for which $G_{\underline{p}}$ has no cyclic Sylow 2-group is case 9; here $N(\underline{p}) \equiv 3 \bmod 4$. Let $G_{\underline{p}} = D_4 = \langle s, a ; s^2 = a^4 = (sa)^2 = 1 \rangle$ and $I_{\underline{p}} = C_4 = \langle a \rangle$. As before we list the elements of $H^2(G_{\underline{p}},\{\pm 1\})$.

relations in $\pi^{-1}(G_{\underline{p}})$	notation	isomorphism type of $\pi^{-1}(G_{\underline{p}})$
$s^2 = 1,\ a^4 = 1,\ (sa)^2 = 1$	(0,0,0)	$\Gamma_2 a_1 \simeq D_4 \times C_2$
$s^2 = -1,\ a^4 = 1,\ (sa)^2 = 1$	(1,0,0)	$\Gamma_2 c_1$
$s^2 = 1,\ a^4 = -1,\ (sa)^2 = 1$	(0,1,0)	$\Gamma_3 a_1 \simeq D_8$
$s^2 = 1,\ a^4 = 1,\ (sa)^2 = -1$	(0,0,1)	$\Gamma_2 c_1$
$s^2 = -1,\ a^4 = -1,\ (sa)^2 = 1$	(1,1,0)	$\Gamma_3 a_2$
$s^2 = -1,\ a^4 = 1,\ (sa)^2 = -1$	(1,0,1)	$\Gamma_2 c_2$
$s^2 = 1,\ a^4 = -1,\ (sa)^2 = -1$	(0,1,1)	$\Gamma_3 a_2$
$s^2 = -1,\ a^4 = -1,\ (sa)^2 = -1$	(1,1,1)	$\Gamma_3 a_3 \simeq Q_8$

In the last column we use the notation of Hall and Senior, see [HS].

From 3.1 we get the following.

If $N(\underline{p}) \equiv 3 \bmod 8$ then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if

$$\alpha \in \{ (0,0,0), (1,0,1), (1,1,0), (0,1,1) \}.$$

If $N(\underline{p}) \equiv 7 \bmod 8$ then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if

$$\alpha \in \{ (0,0,0), (1,0,1), (0,1,0), (1,1,1) \}.$$

In this case, as well as in case 6, the element (1,0,1) is contained in $\mathrm{Inf}[H^2(G_{\underline{p}}/I_{\underline{p}}, \{\pm 1\})]$ on which $\varepsilon(\underline{p})$ is trivial in any case as we saw.

The remaining possibilities for odd primes in the table are cases 21 and 22. Here we have $G_{\underline{p}} = S_3 \times C_2$, and $I_{\underline{p}}$ is either $S_3 \times \{1\}$ or $C_3 \times C_2$. The map

$$\mathrm{Inf}: H^2(S_3 \times C_2/C_3 \times \{1\}, \{\pm 1\}) \to H^2(S_3 \times C_2, \{\pm 1\})$$

is an isomorphism, and $\varepsilon(\underline{p})$ factors over it. Hence $\varepsilon(\underline{p})(\alpha) = 1$ if and only if $\varepsilon(\underline{p})(\mathrm{Inf}^{-1}(\alpha)) = 1$, considered in the subextension of degree 4. In this subextension we have $G_{\underline{p}} = V_4$, $I_{\underline{p}} = C_2$, which we already discussed (case 6). In fields of degree at most 5 however not all elements of $H^2(S_3 \times C_2, \{\pm 1\})$ can occur. If $G_{\underline{p}} \simeq S_3 \times C_2$ then $G \simeq S_5$, since S_5 is the only transitive permutation group on ≥ 5 elements containing a subgroup isomorphic to $S_3 \times C_2$. Write

$$G_{\underline{p}} = \langle s, a \; ; \; s^2 = a^6 = (sa)^2 = 1 \rangle,$$

where s is even in S_5, e.g. $s = (12)(45)$ and $a = (123)(45)$. Then the image of

$$\mathrm{Res}: V_4 \simeq H^2(S_5, \{\pm 1\}) \to H^2(G_{\underline{p}}, \{\pm 1\})$$

consists of the four extension classes in which $a^6 = (sa)^2$. This can be derived directly from an explicit description of the extensions of the symmetric groups, as is given in [Sch].

4. EVEN PRIMES.

For primes above 2 the problem of computing $\varepsilon(\underline{p})$ is more difficult. The next proposition, which also holds for odd primes, gives a result for the abelian case.

PROPOSITION 4.1. Let $\underline{p}$ be a finite prime of K. Assume that $\pi^{-1}(G_{\underline{p}})$ is abelian, where π corresponds to $\alpha \in H^2(G,\{\pm 1\})$. Let $\theta\colon K^*_{\underline{p}} \to G_{\underline{p}}$ be the reciprocity map. Then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if

$$\pi^{-1}(<\theta(-1)>) \simeq \{\pm 1\} \times <\theta(-1)>.$$

PROOF. Since $\pi^{-1}(G_{\underline{p}})$ is abelian, the map $\rho\colon \hat{G}_{\underline{p}} \to G$ factors over $\hat{G}_{\underline{p}}/[\hat{G}_{\underline{p}},\hat{G}_{\underline{p}}]$ in the notation of 2.2, and the same for $\tilde{\rho}\colon \hat{G}_{\underline{p}} \to X$, if it exists. From local class field theory we know that $K^*_{\underline{p}}$ can be considered as a dense subgroup of $\hat{G}_{\underline{p}}/[\hat{G}_{\underline{p}},\hat{G}_{\underline{p}}]$, while the diagram

$$\begin{array}{ccc} \hat{G}_{\underline{p}}/[\hat{G}_{\underline{p}},\hat{G}_{\underline{p}}] & \leftarrow & \hat{G}_{\underline{p}} \\ \uparrow & \searrow & \downarrow \rho \\ K^*_{\underline{p}} & \xrightarrow{\theta} & G_{\underline{p}} \end{array}$$

is commutative. Hence according to 2.2 we have $\varepsilon(\underline{p})(\alpha) = 1$ if and only if there exists a homomorphism $\tilde{\theta}\colon K^*_{\underline{p}} \to \pi^{-1}(G_{\underline{p}})$ such that $\pi \circ \tilde{\theta} = \theta$. As a group we have

$$K^*_{\underline{p}} \simeq \mathbb{Z} \times \mu \times \mathbb{Z}_p^n,$$

where μ is the group of roots of unity in $K^*_{\underline{p}}$, the residue class characteristic is p, and $n = [K_{\underline{p}}:\mathbb{Q}_p]$. A map

$$\mathbb{Z} \times \mathbb{Z}_p^n \to G_{\underline{p}}$$

always lifts to a map $\mathbb{Z} \times \mathbb{Z}_p^n \to \pi^{-1}(G_{\underline{p}})$. Hence $\varepsilon(\underline{p})(\alpha) = 1$ if and only if $(\theta|\mu)\colon \mu \to G_{\underline{p}}$ lifts to a homomorphism $\mu \to \pi^{-1}(G_{\underline{p}})$. This is the case if and only if either $\theta(-1) = 1$ or

$$\pi^{-1}(\theta[\mu]) \simeq \{\pm 1\} \times \theta[\mu].$$

This equivalent to $\pi^{-1}(<\theta(-1)>) \simeq \{\pm 1\} \times <\theta(-1)>$. □

PROPOSITION 4.2. Let $K = \mathbb{Q}$ and $\underline{p} = (2)$. Assume that $\pi^{-1}(G_{\underline{p}})$ is abelian and $\pi^{-1}(I_{\underline{p}})$ is cyclic. Then $\varepsilon(\underline{p})(\alpha) = 1$ if and only if $M_{\underline{p}}$ is contained in an unramified extension of $\mathbb{Q}_2(\zeta + \zeta^{-1})$ for some 2-power root of unity ζ.

PROOF. The maximal abelian extension E of $\mathbb{Q}_2$ is obtained by adjoining all roots of unity to $\mathbb{Q}_2$, cf. [S1], XIV, section 7. This field E has degree 2 over the maximal unramified extension E' of the field obtained by adjoining $\zeta + \zeta^{-1}$ to $\mathbb{Q}_2$ for all 2-power roots of unity ζ. Since

$$\mathrm{Gal}(E/\mathbb{Q}_2) \simeq \hat{\mathbb{Z}} \times \{\pm 1\} \times \mathbb{Z}_2,$$

the field E' corresponds to the subgroup $\{\pm 1\}$. So $M_{\underline{p}}$ is contained in E' if and only if $\theta(-1) = 1$, where

$$\theta\colon \mathbb{Q}_2^* \to \mathrm{Gal}(M_{\underline{p}}/\mathbb{Q}_2) = G_{\underline{p}}$$

is the reciprocity map. From 4.1 and the restriction on $\pi^{-1}(I_{\underline{p}})$ to be cyclic, we see that $\theta(-1) = 1$ if and only if $\varepsilon(\underline{p})(\alpha) = 1$. □

It remains to consider $\varepsilon(\underline{p})(\alpha)$ for $\underline{p}$ above 2 and $G_{\underline{p}}$ not abelian. We should like to have a proposition similar to 3.1. However, in this case wild ramification may affect the behaviour of $\varepsilon(\underline{p})(\alpha)$. The maximal pro-2-group that occurs as a Galois group over $K_{\underline{p}}$ is described with generators and one relation in [S3], section 4. It is not clear, however, to which elements of $G_{\underline{p}}$ these generators map.

TABLE TO SECTION 5. RAMIFICATION BEHAVIOUR IN S_4-FIELDS.

no.	I_p	G_p	ramification in K	p	unramified in $K(\sqrt{\Delta})/K$?	$(\underline{b}(q), K(\sqrt{\Delta})/K)=1$ for all $q = p^f$?
1	$\langle(13)(24)\rangle$	$\langle(1234)\rangle$	2^2		yes	yes
2	$\langle(13)(24)\rangle$	$\langle(13),(24)\rangle$	$1^2 1^2$		yes	yes
3	$\langle(13)(24)\rangle$	V_4	2^2		yes	yes
4	$\langle(13)(24)\rangle$	$\langle(13)(24)\rangle$	$1^2 1^2$		yes	yes
5	$\langle(13)\rangle$	$\langle(13),(24)\rangle$	$1^2 2$		no	
6	$\langle(13)\rangle$	$\langle(13)\rangle$	$1^2 11$		no	
7	$\langle(123)\rangle$	S_3	$1^3 1$	0,2 mod 3	yes	yes
8	$\langle(123)\rangle$	$\langle(123)\rangle$	$1^3 1$	0,1 mod 3	yes	yes
9	$\langle(1234)\rangle$	D_4	1^4	2,3 mod 4	yes	no
10	$\langle(1234)\rangle$	$\langle(1234)\rangle$	1^4	1,2 mod 4	yes	yes
11	V_4	A_4	1^4	2	yes	yes
12	V_4	D_4	1^4	2	yes	no
13	V_4	V_4	1^4	2	yes	yes
14	$\langle(12),(34)\rangle$	D_4	2^2	2	no	
15	$\langle(12),(34)\rangle$	$\langle(12),(34)\rangle$	$1^2 1^2$	2	no	
16	S_3	S_3	$1^3 1$	3	no	
17	D_4	D_4	1^4	2	no	
18	A_4	S_4	1^4	2	yes	no

5. AN APPLICATION TO PÓLYA FIELDS.

DEFINITION 5.1. A number field K with ring of integers $\mathcal{O}$ is called a *Pólya field* if the free $\mathcal{O}$-module

$$\{ f \in K[X] \mid f[\mathcal{O}] \subset \mathcal{O} \}$$

admits a basis $(f_i)_{i=0}^{\infty}$ with $\deg(f_i) = i$, $i = 0, 1, 2, \ldots$.

In [Z] Pólya fields are studied extensively. An important characterization of Pólya fields given there is the following proposition due to A. Ostrowski, cf. [Z], 2.3.

PROPOSITION 5.2. A number field K is a Pólya field if and only if for all prime powers q the ideal

$$\underline{b}(q) = \prod_{N(\underline{p})=q} \underline{p}$$

is principal, where $\underline{p}$ ranges over the prime ideals of $\mathcal{O}$ and N denotes the absolute ideal norm.

Define an S_4-field to be a number field of degree 4 over $\mathbb{Q}$, for which the Galois group of the normal closure over $\mathbb{Q}$ is isomorphic to S_4. The following proposition has been derived in section 6 of [Z].

PROPOSITION 5.3. Let K be an S_4-field which is a Pólya field. Then the Hilbert class field H(K) of K is contained in $K(\sqrt{\Delta})$, where $\mathbb{Q}(\sqrt{\Delta})$ is the quadratic subfield of the normal closure of K.

The purpose of this section is to exclude the possibility $H(K) = K(\sqrt{\Delta})$. To achieve that we first need a lemma.

LEMMA 5.4. Let K be a number field and N its normal closure. Let P be a set of prime numbers p for which the decomposition group in $\mathrm{Gal}(N/\mathbb{Q})$ (defined up to conjugacy) is abelian, and for which N/K is unramified at all primes above p. Then there exists a number field E with the following properties:

(i) $E/\mathbb{Q}$ is abelian;

(ii) $E/\mathbb{Q}$ is unramified at finite primes not contained in P;

(iii) K.E/K is unramified at all finite primes;

(iv) $[E:\mathbb{Q}] = \prod_{p\in P} e_p$, where e_p is the ramification index of p in $N/\mathbb{Q}$.

REMARK. It is not difficult to see that the field E in 5.4 is unique. Since we shall not use it, we don't give the proof.

PROOF OF 5.4. For each $p \in P$ choose a place $\underline{p}$ of $\bar{\mathbb{Q}}$ above p. Since $K_{\underline{p}}/\mathbb{Q}_p$ is assumed to be abelian, we obtain from the local version of Kronecker-Weber ([S1], XIV, section 7) that there exists a field F_p with

$$\mathbb{Q}_p \subset F_p \subset \mathbb{Q}_p(\zeta_{p^\infty})$$

such that $K_{\underline{p}}.F_p/F_p$ and $K_{\underline{p}}.F_p/K_{\underline{p}}$ are unramified. Remark that

$$[F_p:\mathbb{Q}_p] = e_p.$$

For every p there is a natural isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p),$$

so there is a natural correspondence between subfields of $\mathbb{Q}(\zeta_{p^\infty})$ and fields between $\mathbb{Q}_p$ and $\mathbb{Q}_p(\zeta_{p^\infty})$, preserving degrees. Let E be the compositum over all $p \in P$ of the subfields of $\mathbb{Q}(\zeta_{p^\infty})$ corresponding to F_p. It is clear that E satisfies (i), (ii) and (iv).

Condition (iii) only has to be verified for $p \in P$. Fix such a $p \in P$. Since $K_{\underline{p}}.F_p/K_{\underline{p}}$ and $E_{\underline{p}}/F_p$ are unramified, we see that K.E/K is unramified at $\underline{p}$. The extensions N/K and N.E/K.E are unramified at all primes above p. Different primes above p have the same ramification indices in the normal extension $N/\mathbb{Q}$. The same can be said for $N.E/\mathbb{Q}$. We conclude that K.E/K is unramified at all primes above p. We see that E satisfies the required properties. □

THEOREM 5.5. Let K be an S_4-field. Then K is a Pólya field if and only if the class number h(K) of K is one.

PROOF. If h(K) = 1 then K is a Pólya field by 5.2. If K is a Pólya field then by 5.3 either h(K) = 1 or H(K) = $K(\sqrt{\Delta})$. From now on assume that K is a Pólya field with H(K) = $K(\sqrt{\Delta})$; it suffices to derive a contradiction from this assumption.

In order to decide which types of ramification are allowed, we need a more detailed table than in section 3, not only distinguishing G_p and I_p as groups, but also as subgroups of S_4 up to conjugacy. In the new table let

$$V_4 = \langle (13)(24),\ (12)(34) \rangle;$$
$$S_3 = \langle (12),\ (123) \rangle;$$
$$D_4 = \langle (1234),\ (12)(34) \rangle.$$

If $p\mathcal{O} = \prod_{i=1}^{k} \underline{p}_i^{e_i}$, then this decomposition in K is denoted as

$$f_1^{e_1} f_2^{e_2} \ldots f_k^{e_k},$$

where $N(\underline{p}_i) = p^{f_i}$ for i = 1, 2,... k.

Cases 5, 6, 14, 15, 16, 17 are excluded since then $K(\sqrt{\Delta})/K$ is ramified. In particular the infinite prime may not ramify as 6, so K is either totally real or totally complex.

Cases 9, 12, 18 are excluded since then the Artin symbol $(\underline{b}(p), K(\sqrt{\Delta})/K)$ is non-trivial. Since $K(\sqrt{\Delta})$ = H(K) this means that $\underline{b}(p)$ is non-principal, contradicting 5.2.

Let p_0 be a prime dividing Δ. Then I_{p_0} is not contained in A_4, which among the remaining cases only occurs at case 10. Let P be the set of prime numbers ramifying according to cases 1, 2, 3, 4, 10 or 13, i.e. not to cases 7, 8 or 11. From 5.4 we obtain a field E, abelian of degree

$$\prod_{p \in P} e_p$$

over $\mathbb{Q}$. If K is totally comlex then define

$$M = E.K, \text{ else } M = (E \cap \mathbb{R}).K.$$

Clearly M/K is abelian and totally unramified. Hence we have

$$2 = h(K) \geq [M:K] \geq \tfrac{1}{2}[E.K:K] = \tfrac{1}{2}[E:\mathbb{Q}] = \tfrac{1}{2}\prod_{p\in P} e_p.$$

Since $e_{p_0} = 4$ and $p_0 \in P$, this is only possible if $e_p = 1$ for all $p \in P\setminus\{p_0\}$ and both inequalities are sharp. So $M \neq E.K$, so E is not real and K is not totally complex. Since we saw that K is either totally complex or totally real, we conclude that K is totally real. Further we see that case 10 occurs exactly once (at p_0), and among the other cases only 7, 8 and 11 may occur. If p_0 is odd then E is the quartic subfield of $\mathbb{Q}(\zeta_{p_0})$. Since E is not real, we get

$$p_0 \equiv 5 \bmod 8 \quad \text{or} \quad p_0 = 2.$$

Assume that case 11 occurs at a prime p. Then $p = 2$, and since G_p is contained in A_4, the prime p is split in $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$. This contradicts

$$\Delta = p_0 \equiv 5 \bmod 8.$$

We conclude that except for p_0 only the cases 7 and 8 may occur.

Remark that $S_4 \simeq PGl(2,3)$. Let $\alpha \in H^2(S_4,\{\pm 1\})$ be the element corresponding to the extension

$$0 \to \{\pm 1\} \to Gl(2,3) \to PGl(2,3) \to 0.$$

Let p be a prime of ramification type 7 or 8. Then G_p is contained in a subgroup of PGl(2,3) isomorphic to S_3. Such a subgroup is conjugate to

$$\begin{pmatrix} \pm 1 & \mathbb{F}_3 \\ 0 & \pm 1 \end{pmatrix}/\{\pm 1\},$$

and since the sequence

$$0 \to \{\pm 1\} \to \begin{pmatrix} \pm 1 & \mathbb{F}_3 \\ 0 & \pm 1 \end{pmatrix} \to \begin{pmatrix} \pm 1 & \mathbb{F}_3 \\ 0 & \pm 1 \end{pmatrix}/\{\pm 1\} \to 0$$

is split, we have $\varepsilon(p)(\alpha) = 1$. Combining the results until now, we get $\varepsilon(p)(\alpha) = 1$ for all primes $p \neq p_0$, including infinity.

Next we compute $\varepsilon(p_0)(\alpha)$. An element of PGl(2,3) of order 4 is conjugate to

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

which can only lift to an element of order 8 in Gl(2,3). Hence $\mathrm{Res}(\alpha) \in H^2(G_{\mathfrak{p}_0}, \{\pm 1\})$ is non-trivial.

If $p_0 \neq 2$ then we saw that $p_0 \equiv 5 \bmod 8$. From 3.2 (or the table to section 3) we then get $\varepsilon(p_0)(\alpha) = -1$.

Let $p_0 = 2$ and assume that $\varepsilon(p_0)(\alpha) = 1$. Then we see from 4.2 that K_2 is contained in an unramified extension of $\mathbb{Q}_2(\zeta + \zeta^{-1})$ for some 2-power root of unity ζ. Since $K_2.E_2/K_2$ is unramified, the same is true for E_2. From the way of constructing E in the proof of 5.4 we see that

$$E \subset \mathbb{Q}(\zeta + \zeta^{-1}),$$

contradicting the fact that E is not real.

In all cases we have $\varepsilon(p_0) = -1$ and $\varepsilon(p) = 1$ for $p \neq p_0$, so

$$\prod_p \varepsilon(p)(\alpha) = -1.$$

This is a contradiction to 2.1. Hence an S_4-field K with $H(K) = K(\sqrt{\Delta})$ cannot be a Pólya field. □

REFERENCES.

[CF] Cassels, J. W. S., and Fröhlich, A. (eds), *Algebraic number theory*, Academic Press, 1967.

[F] Fröhlich, A., *Discriminants of algebraic number fields*, Math. Zeitschr. 74 (1960), 18 - 28.

[H] Huppert, B., *Endliche Gruppen I*, Springer, 1967.

[HS] Hall, M., and Senior, J. K., *The groups of order* $2^n (n \leq 6)$, Macmillan New York, 1964.

[P] Pólya, G., *Über ganzwertigen Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. 149 (1919), 97 - 116.

[S1] Serre, J.-P., *Corps locaux*, Hermann Paris, 1962.

[S2] Serre, J.-P., *Cohomologie galoisienne*, Lecture Notes in Mathematics 5, Springer, 1964.

[S3] Serre, J.-P., *Structure de certains pro-p-groupes*, Séminaire Bourbaki 252 (1963).

[Sch] Schur, I., *Über die Darstellungen der symmetrischen und alternierenden Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. 139 (1911), 155 - 250.

[Z] Zantema, H., *Integer valued polynomials over a number field*, part I of this thesis, also Manuscripta math. 40 (1982), 155 - 203.

GEHEELWAARDIGE VEELTERMEN IN DE ALGEBRAISCHE GETALTHEORIE.

SAMENVATTING.

Een getallenlichaam K met ring van gehelen $\mathcal{O}$ heet een Pólya-lichaam als het vrije $\mathcal{O}$-moduul

$$\{ f \in K[x] \mid f[\mathcal{O}] \subset \mathcal{O} \}$$

een basis $(f_i)_{i=0}^{\infty}$ bezit waarvoor f_i graad i heeft voor i = 0, 1, 2, ... In dit proefschrift worden getaltheoretische eigenschappen van Pólyalichamen bestudeerd, met name de klassengroep. Als de Galoisgroep G van de normale afsluiting van een Pólyalichaam, opgevat als permutatiegroep, een element bevat met precies één vast punt, blijkt de klassengroep een factorgroep te zijn van een eindige groep R(G), die alleen van G afhangt. Deze groep R(G) wordt voor verschillende permutatiegroepen G berekend, o. a. voor alle tweevoudig transitieve permutatiegroepen, en blijkt dikwijls triviaal te zijn. Zo zijn bijvoorbeeld $R(S_n)$ voor n = 3 en n ≥ 5, en $R(A_n)$ voor n = 4 en n ≥ 6, alle triviaal. Een bijzondere rol wordt gespeeld door de groep S_4, werkend op 4 symbolen. Hoewel $R(S_4)$ uit twee elementen bestaat, blijkt er toch geen vierdegraads Pólyalichaam van dit type te bestaan met een niet-triviale klassengroep. Dit laatste wordt bewezen met behulp van een globale beperking op het vertakkingsgedrag in getallenlichamen, die in dit proefschrift wordt afgeleid.

STELLINGEN.

1. Laat $\alpha(k)$ voor k geheel, $k \geq 2$, het grootste reële getal zijn zodanig dat er een eindige verzameling V bestaat met k deelverzamelingen $V_1, V_2, \ldots\ldots, V_k$ die voldoen aan:

(i) $|V_1| \leq |V_2| \leq \ldots\ldots \leq |V_k|$;

(ii) voor $1 \leq i < j \leq k$ geldt: $|V_j \setminus V_i| \geq \alpha(k)|V|$.

Dan geldt: $\alpha(2) = 1$, $\alpha(3) = \alpha(4) = 1/2$, $\alpha(5) = \alpha(6) = 2/5$, $\alpha(7) = 3/8$, $\alpha(8) = 4/11$, $\alpha(9) = 13/37$, $\alpha(10) = 9/26$, $\alpha(11) = 31/92$, $\alpha(12) = 1/3$, $\lim_{k\to\infty} \alpha(k) = 1/4$.

2. Als de punten (a,b), (c,d) en (a+c,b+d) in $\mathbb{R}^2$ alle drie liggen op de kromme

$$x^4 + x^3y + x^2y^2 + xy^3 + y^4 = 1,$$

dan geldt

$$1 \leq |ad - bc| < 1{,}0036.$$

Met behulp van de ongelijkheid $1 \leq |ad - bc|$ kan een door J. Browkin gestelde vraag worden beantwoord: de elementen van orde 5 in $K_2\mathbb{Q}$ worden voortgebracht door de symbolen van de vorm

$$\{a, a^4+a^3+a^2+a+1\},$$

waarbij $a \in \mathbb{Q}^*$.

Lit.: J. Browkin, *Elements of small order in* K_2F, Lecture Notes in Mathematics 966, 1-6, Springer, 1982.

3. Zij n een positief geheel getal. Het aantal 4×4-matrices $(a_{ij})_{i,j=1,2,3,4}$ met coëfficiënten in $\{1, 2, \ldots\ldots, n\}$ waarvoor

(*) $\quad \Sigma_{j=1}^4 a_{kj} = \Sigma_{i=1}^4 a_{ik} = \Sigma_{i=1}^4 a_{ii} = \Sigma_{i=1}^4 a_{i,5-i} = a_{11}+a_{12}+a_{21}+a_{22}$,

$k = 1, 2, 3, 4,$

is gelijk aan

$$\frac{4}{35}n^7 + \frac{2}{5}n^5 + \frac{4}{15}n^3 + \frac{23}{105}n.$$

4. Er zijn $3456 = 6\cdot(4!)^2$ matrices die voldoen aan (*) uit stelling 3 waarvan de coëfficiënten precies de gehele getallen 1 tot en met 16 zijn. Deze zijn op eenduidige wijze van de vorm

$$\begin{pmatrix} s_1+t_1 & s_2+t_2 & s_3+t_3 & s_4+t_4 \\ s_4+t_3 & s_3+t_4 & s_2+t_1 & s_1+t_2 \\ s_2+t_4 & s_1+t_3 & s_4+t_2 & s_3+t_1 \\ s_3+t_2 & s_4+t_1 & s_1+t_4 & s_2+t_3 \end{pmatrix}$$

met $\{s_1, s_2, s_3, s_4\} = V_k$, $\{t_1, t_2, t_3, t_4\} = V_{7-k}$, $k = 1, 2, 3, 4, 5, 6$, waarbij

$$V_1 = \{0, 1, 2, 3\},\ V_2 = \{0, 1, 4, 5\},\ V_3 = \{0, 1, 8, 9\},$$

$$V_4 = \{1, 3, 5, 7\},\ V_5 = \{1, 3, 9, 11\},\ V_6 = \{1, 5, 9, 13\}.$$

5. Voor een ring R is het mogelijk om expliciet afbeeldingen

$$K_0R \to \pi_1(BQR,0), \quad K_1R \to \pi_1(B(S^{-1}S),0)$$

aan te geven en daarvan rechtstreeks te bewijzen dat het groepsisomorfismen zijn.

Lit.: D. Quillen, *Higher algebraic K-theory I*, Lecture Notes in Mathematics 341, 85-147, Springer, 1973;
D. Grayson, *Higher algebraic K-theory II*, Lecture Notes in Mathematics 551, 217-240, Springer, 1976.

6. Uitgesproken opvattingen op het gebied van verkeersproblematiek, voedingsgewoonten, bewapening, alcoholgebruik, roken, kernenergie, onderwijs, culturele minderheden en het gebruik van de Friese taal hoeven geen aanleiding te geven tot stellingen bij een proefschrift.

7. Van de volgende vier beweringen zijn er precies drie juist:

- een rechthoek van 9 bij 1 past binnen een rechthoek van 6 bij 8;
- er zijn oneindig veel manieren om een kubus in zes congruente veelvlakken te verdelen, zodanig dat geen der snijvlakken evenwijdig is aan een zijde van de kubus;
- voor elk positief geheel getal n passen er meer dan twee keer zoveel bollen met middellijn 1 in een kubus met ribbe n dan kubussen met ribbe 1 in een bol met middellijn n;
- er zijn ten minste 100 gelijkbenige driehoeken in $\mathbb{R}^2$, elk met een oppervlakte van ten hoogste 20.000 waarvan de omtrek en de coördinaten van de hoekpunten gehele getallen zijn, en waarvan geen tweetal gelijkvormig is.