KATHOLIEKE UNIVERSITEIT TE LEUVEN

FACULTEIT DER WETENSCHAPPEN

RADIKALEN VAN MULTIPLIKATIEVE GROEPEN IN DE ALGEBRAÏSCHE GETALTHEORIE

Thesis, voorgedragen tot het bekomen van de graad van Doctor in de Wetenschappen door

E. VAN TIEGHEM

Promotor: Prof. L. Bouckaert
Copromotor: Prof. W. Kuyk

1975

KATHOLIEKE UNIVERSITEIT TE LEUVEN

FACULTEIT DER WETENSCHAPPEN

RADIKALEN VAN MULTIPLIKATIEVE GROEPEN IN DE ALGEBRAÏSCHE GETALTHEORIE

Thesis, voorgedragen tot het bekomen van de graad van Doctor in de Wetenschappen door

E. VAN TIEGHEM

Promotor: Prof. L. Bouckaert
Copromotor: Prof. W. Kuyk

1975

Aan mijn ouders,
aan Greetje
aan Katrientje, Leentje
en Geertje.

VOORWOORD

Waarde Lezer,

Hier wil ik op de eerste plaats mijn dank betuigen aan mijn co-promotor, Professor W. Kuyk. Het feit dat hij zich ooit eens aan de Wiskunde wijdde, en daardoor —volgens mijn persoonlijke ervaring met hem— aan de mensen die dat ook willen doen, is voor het tot stand komen van deze thesis van veel groter belang dan hij zelf wellicht vermoedt. Mijn dankbaarheid tegenover hem is dan ook veel groter dan datgene wat deze regels kunnen laten uitschijnen.

Ook voor mijn promotor, Professor L. Bouckaert wil ik mijn waardering laten blijken. Zijn nooit-aflatend geloof in de realisatie van een dergelijk werk is voor mij een belangrijke stimulans geweest.

Nog velen ben ik dank verschuldigd, en ik kan ze allen in één keer vernoemen door te zeggen dat het diegenen zijn die steeds met hoop en/of geloof en/of liefde mijn verrichtingen van de vele voorbije jaren gevolgd hebben.

Speciaal wil ik hier Greetje, mijn vrouw bedanken, want zij heeft én de hoop, én het geloof, én de liefde omtrent dit werk ten toon gespreid en dit ondanks het "leed" dat ook wel eens om het hoekje komt kijken bij het verrichten van een dergelijke arbeid.

Ik hoop nu echter dat u allen ook zult mogen delen in de vreugde die ik bij dit schrijven ervaar. Dat u daar iets van zoudt gewaar worden is het beste bewijs dat deze dankwoorden oprecht gemeend zijn.

Op een bijzonder plaatsje komt het dankwoordje voor Nina De Maesschalck-Vleugels die met veel zorg het tikwerk voor haar rekening genomen heeft. Mocht u vreugde beleven aan dit werk, dan bent u, waarde lezer, haar eveneens dank verschuldigd.

Heverlee, 27 januari, 1975.

INLEIDING

In de algebraïsche Getallentheorie wordt een belangrijke plaats ingenomen door de studie van een aantal multiplikatieve, oneindige abelse groepen die op een of andere wijze aan een getallenveld geassocieerd zijn, zoals de eenhedengroep, de idealengroep e.a.. In sommige gevallen kan het ook nuttig zijn aandacht te besteden aan quotiënten van dergelijke groepen. Bijvoorbeeld, is L een totaalkompleks getallenveld van graad 2 over een totaal-reëel deelveld K, dan is het quotiënt van de eenhedengroep van L over die van K een eindige groep, wat aanleiding geeft tot resultaten in verband met klassegetal-problemen (zie [11], [12] en [26]). De orde van deze quotiëntgroep is, in het geval dat L abels is over $\mathbb{Q}$, uitvoerig door Hasse bestudeerd, en blijkt een belangrijke rol te spelen in de analytische uitdrukking voor het klassegetal van L (zie [14],[27] en [28]). Andere situaties, waarin bijvoorbeeld de eindigheid van het quotiënt van de eenhedengroep van een getallenveld modulo de deelgroep voortgebracht door eenhedengroepen van meerdere deelvelden van grote betekenis is voor de aritmetica van deze velden, treft men ondermeer aan in [1] en [23].

De gevallen waarin dergelijke quotiënten oneindig zijn hebben echter weinig de aandacht getrokken; we kunnen hier slechts het werk van Liang citeren ([20]), waarin de orde van de torsie-deelgroepen van een dergelijke quotiëntgroep (in een normale uitbreiding van $\mathbb{Q}$) onderzocht wordt.

Dit deed ons echter opmerken dat, wegens Dirichlet's eenhedenstelling, de torsie-deelgroep van elk quotiënt van eenhedengroepen steeds eindig is. Men kan bijgevolg steeds aan een willekeurige uitbreiding L van een getallenveld K (met eenhedengroepen respektievelijk U_L en U_K) een soort "eenheden-index" koppelen, namelijk : de orde van de torsie-deelgroep van de quotiëntgroep U_L/U_K of, wat op hetzelfde neerkomt : de index van U_K in zijn radikaal in U_L. Aangezien het precies deze index is die in de eerste van de hierbovengenoemde gevallen een zo belangrijke rol speelt, leek het ons opportuun hem in het meest algemene geval te onderzoeken en te

proberen iets van zijn aritmetische betekenis te achterhalen.

Spoedig hebben we dan kunnen vaststellen dat ook andere multiplikatieve groepen van getallenvelden bij dit onderzoek konden betrokken worden. Meer bepaald bleken een aantal groepen, geassocieerd aan een getallenveld K, eveneens van eindige index te zijn in een radikaal (dat met een eindige uitbreiding van K kon gedefinieerd worden), en konden de aldus bekomen invarianten met andere aritmetische grootheden in verband gebracht worden. Het zijn nu precies deze bevindingen die het onderwerp van deze thesis uitmaken.

In een eerste hoofdstuk geven we een overzicht van klassieke resultaten uit de algebraïsche getallentheorie. We zagen ons daartoe genoodzaakt wegens de afwezigheid van een "gangbare" terminologie in de nederlandse taal voor een groot aantal begrippen uit die tak van de Wiskunde. We hebben echter geen plaats voorzien voor een overzicht van resultaten uit de "elementaire" getallentheorie en de Algebra, omdat we veronderstellen dat de lezer vertrouwd is met hetgeen op dit gebied verderop gebruikt wordt. We verwijzen hier enkel naar de werken [18] en [29].

In hoofdstuk II zetten we de aritmetica van bikwadratische velden uiteen. De hierin voorkomende resultaten zijn niet nieuw; we hebben ze echter als dusdanig samengevat niet in de literatuur kunnen terugvinden, wat een eerste motief uitmaakte voor het neerschrijven van dit hoofdstuk. Anderzijds worden we hier gekonfronteerd met de belangrijkheid van de eenheden-index in de diepe formule voor het klassegetal, zodat het uiteenzetten ervan ons als een noodzaak voorkwam. Een gedetailleerde bespreking van de rol van deze index hebben we echter achterwege gelaten, aangezien deze in [14], §§20-26 voorkomt, en we voornamelijk oog gehad hebben voor de veralgemening ervan.

In hoofdstuk III verlaten we de getallentheorie en beschouwen we,

zuiver algebraïsch, de index van de multiplikatieve groep van een veld K in zijn radikaal in een uitbreidingsveld L. De motivering voor deze sprong is gelegen in het feit dat we bij een eerste onderzoek naar de mogelijke waarden van eenheden-indices tot het inzicht kwamen dat het probleem verband hield met radikaaluitbreidingen van een veld, zodat dit algebraïsch kon aangepakt worden.

De bedoeling van de uiteenzetting is te komen tot stelling III. 4.5. die we als nieuw aanzien. Het bewijs ervan dient in twee stappen te geschieden. Een eerste betreft het cyclische geval. We bereiken hier een veralgemening van het bewijs dat door Hasse en later door Uchida geleverd werd in het geval van totaal-komplekse getallenvelden van graad twee over een totaal-reëel veld (zie [14] en [27]; het bewijs via Cohomologie in [28] is een bijzonder geval van het hier voorgestelde, aangezien de in stelling III.3.2.2. voorkomende groep $(W_L)_N/(W_L)^\lambda$ niets anders is dan $H^1(G,W_L)$). Een tweede stap betreft uitbreidingen door toevoeging van n^{de} machtswortels. Over dergelijke uitbreidingen werd onlangs door Schinzel (cfr. [24]) informatie ingewonnen die de tekst van §4.2. aanzienlijk kan verkorten. We hebben echter gemeend er goed aan te doen onze oorspronkelijke tekst te behouden, enerzijds omdat Schinzel's resultaat (naar mondelinge mededeling) steunt op diepere resultaten van Kneser en er toch slechts een gedeelte van gebruikt wordt, anderzijds omdat we de uiteenzetting van §4.2. als noodzakelijk voor de continuïteit van het geheel aanzien.

In hoofdstuk IV keren we terug tot de Getallentheorie. Eerst gaat onze aandacht naar de S-eenhedengroep (waarvan de eenhedengroep een bijzonder geval is). Ons hoofdresultaat is vervat in stelling IV.1.2.2.. Het is een eenvoudige toepassing van de theorie der $\mathbb{Z}$-modulen en van het resultaat dat in vorig hoofdstuk bereikt werd. Als nevenresultaat bekomen we een karakterisering van abelse groepen die, modulo torsie, van eindige rang zijn (stelling IV.1.2.1.). Het is ons niet mogelijk deze resultaten in de literatuur te situeren.

Vervolgens onderzoeken we, met het oog op de aritmetische betekenis van de eenheden-indices, radikalen in idealengroepen. Dit

levert ons twee nieuwe invarianten, namelijk, de globale ramifikatie-index (waaraan in de literatuur blijkbaar geen aandacht geschonken wordt) en de index van de hoofdidealengroep in zijn radikaal t.o.v. een uitbreiding. Deze laatste is een invariant waarvan de betekenis vrij diep ligt, en die in het volgend hoofdstuk meer aan bod zal komen. Het onderzoek naar zijn priemdelers bracht ons tot het resultaat van stelling IV.2.4.2., dat tot nog toe slechts in bijzondere situaties werd toegepast (zie [30], voornamelijk de referentie naar [8] op blz. 16).

In het laatste hoofdstuk worden enige van de hoger ingevoerde invarianten in enige bijzondere gevallen besproken. De grootste aandacht gaat hier in de eerste plaats naar het radikaal van de hoofdidealengroep bij cyclische uitbreidingen. We worden hier via Herbrand's eenhedenstelling (stelling V.1.1.) tot de diepere "genustheorie" gebracht. De hierboven bekomen invarianten in verband met de idealengroepen kunnen inderdaad met behulp van norm-indices aan Chevalley's formule voor het inertie-klassegetal gekoppeld worden. Dat dit tot sterke resultaten uit de theorie der klassenvelden leidt illustreren we in §3, waar we de equivalentie kunnen aantonen tussen twee bekende stellingen, hetgeen blijkbaar totnutoe onopgemerkt is gebleven. Eveneens in §3, illustreren we de diepte van de index van de hoofdidealengroep in zijn radikaal aan de hand van kwadratische velden, door deze in verband te brengen met de oplosbaarheid van zekere vergelijkingen die in [1] "as deep as the problem of the solvability of $x^2-ny^2 = -1$" betiteld worden.

In §2 worden kwadratische uitbreidingen beschouwd. We vinden daar, door toepassing van stelling IV.1.2.2., een middel om het quotiënt van twee regulatoren te vervangen door een nieuwe soort regulator die men behoorlijk kan verwerken in de formule voor het relatieve klassegetal. We bekomen dan een uitdrukking waarin de eenheden-index als factor optreedt. Het was ons echter niet mogelijk te achterhalen of de aritmetische betekenis van deze index in deze richting moet gezocht worden.

In §3 vinden we, naast de reeds geciteerde toepassing, een stelling die het "eenheden-index 1 of 2-probleem" volledig oplost in

K. Omgekeerd, is p een priemideaal van K, dan bestaan er precies r priemidealen $P_1,\ldots,P_r$ van L waarvoor $P_i \cap \mathcal{O}_K = p$. Men zegt dat P_i boven p ligt, en we schrijven : $P_i|p$. Voor de kanonieke faktorisatie van het ideaal $p\mathcal{O}_L$ van L geldt :

$$p\mathcal{O}_L = P_1^{e_1}\ldots P_r^{e_r} ,$$

waarbij $e_1,\ldots,e_r \in \mathbb{N}_0$. We noemen $e_i = e(P_i|p)$ de ramifikatie-index van P_i t.o.v. p.

Verder kan het restklassenveld $\overline{L}_{P_i}$ als een uitbreiding van $\overline{K}_p$ aangezien worden, en er geldt :

$$[\overline{L}_{P_i} : \overline{K}_p] = f_i = f(P_i|p) < \infty.$$

Men noemt f_i de restklassengraad van P_i t.o.v. p. De getallen e_i en f_i voldoen verder nog aan de betrekking :

$$\sum_{i=1}^{r} e_i f_i = [L : K].$$

Ze zijn bovendien multiplikatief bij ketens. Dit betekent :

$$e(Q|P_i).e(P_i|p) = e(Q|p)$$

$$f(Q|P_i).f(P_i|p) = f(Q|p)$$

waarin Q een priemideaal is van een eindige uitbreiding F van L waarvoor $Q|P_i$.

De groep I_K kan als deelgroep van I_L aangezien worden wegens het feit dat de afbeelding

$$i_{L/K} : I_K \to I_L$$
$$: a \mapsto a.\mathcal{O}_L$$

een injektief homomorfisme is. Omgekeerd bestaat er een

homomorfisme $N_{L/K}$ van I_L naar I_K. Zijn waarde op een priemideaal P van L is gegeven door :

$$N_{L/K}(P) = p^{f(P|p)},$$

waarbij p niets anders is dan $P \cap \mathcal{O}_K$. Is β een element van L^*, dan geldt :

$$N_{L/K}(\beta.\mathcal{O}_L) = N_{L/K}(\beta).\mathcal{O}_L,$$

waarbij $N_{L/K}$ de gewone norm is van L tot K. We zullen $N_{L/K}$ eveneens de <u>norm van L tot K</u> noemen.

Is a een ideaal van K, dan heeft de ring $\mathcal{O}_K/a$ een eindig aantal elementen dat met $N_K(a)$ zal aangeduid worden. Er geldt verder :

$$N_{K/\mathbb{Q}}(a) = N_K(a).\mathbb{Z} .$$

Is $A \in I_L$, dan geldt eveneens :

$$N_L(A) = N_K(N_{L/K}(A))$$

Indien L/K een galois-uitbreiding is met galois-groep G, dan vormen de elementen σ van G waarvoor $\sigma P = P$ (P een priemdeler van L) een deelgroep G_P van G, <u>de dekompositiegroep van P</u> genoemd. Is

$$G = \bigcup_{j=1}^{r} \sigma_j G_P$$

een ontbinding van G in nevenklassen volgens G_P, dan is $\{\sigma_j P\}$ precies de verzameling van alle priemidealen van L die boven $p = P \cap \mathcal{O}_K$ liggen. Bovendien geldt :

$$e(\sigma_1 P|p) = \ldots = e(\sigma_r P|p) = e_p$$

$$f(\sigma_1 P|p) = \ldots = f(\sigma_r P|p) = f_p .$$

De getallen e_p en f_p noemt men de ramifikatie-index, respektievelijk de restklassengraad van p in L.

Wat betreft de norm van een ideaal A van L, geldt de relatie :

$$N_{L/K}(A)\mathcal{O}_L = \prod_{\sigma \in G} \sigma A.$$

1.3. De diskriminant.

Zij L een eindige uitbreiding van een getallenveld K, en zij $S_{L/K}$ het spoor van L tot K.

De elementen x van L waarvoor geldt : $S_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K$, vormen een ideaal van L. De norm $N_{L/K}$ van zijn inverse is een geheel ideaal van K en wordt de diskriminant van de uitbreiding L/K genoemd. Hij wordt met $D_{L/K}$ aangeduid.

Is p een priemideaal van K, dan geldt : $p \mid D_{L/K}$ dan en slechts dan als er een priemideaal P van L boven p bestaat waarvoor $e(P|p) > 1$. Dergelijke p noemen we vertakt (de andere heten onvertakt) in L.

Zij $\{\alpha_1,\ldots,\alpha_m\}$ $(m = [K : \mathbb{Q}])$ een integrale basis van K, en zij $\{\sigma_1,\ldots,\sigma_m\}$ de verzameling van alle inbeddingen van K in $\mathbb{C}$. Het getal :

$$D_K = (\det(\sigma_i(\alpha_j)))^2$$

behoort tot $\mathbb{Z}$, en wordt de diskriminant van K genoemd. Het verband met $D_{K/\mathbb{Q}}$ wordt gegeven door :

$$D_K.\mathbb{Z} = D_{K/\mathbb{Q}} .$$

1.4. Onvertakte en volledig splitsende priemidealen.

Zij K een getallenveld, L een eindige uitbreiding van K. Zij p een priemdeler van K. Er geldt :

(1). Is F een eindige uitbreiding van L, dan is p onvertakt in F enkel en alleen als p onvertakt is in L, en elke priemdeler van L boven p onvertakt is in F.

(2). Is E een andere eindige uitbreiding van K, en is p onvertakt in L, dan is elke priemdeler van E boven p onvertakt in het compositum LE.

(3). Zijn E_1 en E_2 twee eindige uitbreidingen van K, en is p onvertakt in E_1 en E_2, dan is p onvertakt in E_1E_2.

Een priemdeler p van K heet volledig gesplitst in L, als er precies $n = [L : K]$ verschillende priemdelers van L boven p liggen. De eigenschappen (1) (2) en (3) blijven geldig wanneer het woord "onvertakt" vervangen wordt door "volledig gesplitst".

§2. VALUATIES VAN GETALLENVELDEN

2.1. Algemeenheden over valuaties.

Een valuatie van een veld K is een funktie $v : K \to \mathbb{R}$ die voldoet aan :

(1) : $v(\alpha) \geqslant 0$ en $v(\alpha) = 0 \Leftrightarrow \alpha = 0$

(2) $v(\alpha\beta) = v(\alpha)v(\beta)$

(3) Er bestaat een $\mathfrak{C}$ $(\in \mathbb{R})$, $\geqslant 1$ zó dat

$$v(\alpha) \leqslant 1 \Rightarrow v(1 + \alpha) \leqslant \mathfrak{C}.$$

Een valuatie definieert een topologie op K. Twee valuaties die dezelfde topologie definiëren worden <u>equivalent</u> genoemd.

Een valuatie v heet <u>niet-archimedisch</u> als men $\mathfrak{C} = 1$ kan nemen in (3), zoniet heet v <u>archimedisch</u>.

Is v een niet-archimedische valuatie, dan vormen de elementen α van K waarvoor $v(\alpha) \leqslant 1$ een ring, $\mathcal{O}_K(v)$. De elementen α van K met $v(\alpha) < 1$ vormen een maximaal ideaal $P_K(v)$ in $\mathcal{O}_K(v)$.

Een veld k noemt men <u>volledig ten opzichte van een valuatie</u> als elke Cauchyrij konvergeert. Een veld K met valuatie v kan steeds aangezien worden als een deelveld van een volledig veld $\tilde{K}$ (met valuatie $\tilde{v}$ waarvoor $\tilde{v}|K = v$) waarin K overal dicht is. $\tilde{K}$ is enig (op isomorfisme na) en wordt de <u>vervolledigingvan K t.o.v. v</u> genoemd. Is v archimedisch dan is $\tilde{K}$ ofwel $\mathbb{R}$ ofwel $\mathbb{C}$; korresponderend hiermee wordt v dan <u>reëel</u> of <u>kompleks</u> genoemd.

2.2. <u>Valuaties van getallenvelden</u>.

Zij K een getallenveld, p een priemideaal van K.

Is α een element van K^* en $\alpha\mathcal{O}_K = \prod_p p^{m_p(\alpha)}$ de kanonieke faktorisatie van het ideaal $\alpha\mathcal{O}_K$, dan is, voor elke $c \in (0,1)$, de funktie $v_{p,c} : K \to \mathbb{R}$, gedefinieerd door :

$$v_{p,c} : \alpha \mapsto c^{m_p(\alpha)}$$

$$: 0 \mapsto 0,$$

een niet-archimedische valuatie van K. Is $c' \in (0,1)$ dan is $v_{p,c'}$ equivalent met $v_{p,c}$. Bovendien geldt : $p = \mathcal{O}_K \cap P_K(v_{p,c})$. Neemt men $c = N_K(p)^{-1}$, dan noemen we $v_{p,c}$ <u>de (genormeerde) valuatie geassocieerd aan p</u> of <u>de p-adieke valuatie</u>. Is v een

niet-archimedische valuatie van K, dan is $P_K(v) \cap \mathcal{O}_K$ een priemdeler van K waarvan de geassocieerde valuatie equivalent is met v; de priemdeler $P_K(v) \cap \mathcal{O}_K$ wordt <u>geassocieerd aan v</u> genoemd.

Zij $\{\sigma_1,\ldots,\sigma_n\}$ de verzameling van alle inbeddingen van K in $\mathbb{C}$. Voor elke $i \in \{1,2,\ldots,n\}$ is de funktie $|\ |_i : K \to \mathbb{R}$, gedefinieerd door :

$$|\ |_i : \alpha \mapsto |\sigma_i(\alpha)|$$

($|\ |$ is de gewone absolute waarde op $\mathbb{C}$), een archimedische valuatie van K. Omgekeerd, elke archimedische valuatie van K is equivalent met een van de $|\ |_i$ ($i = 1,2,\ldots,$of n). Bovendien zijn $|\ |_i$ en $|\ |_j$ dan en slechts dan equivalent als $i = j$ of $\sigma_i = \overline{\sigma}_j$, waarbij $\overline{\sigma}_j$ de kompleks-toegevoegde is van σ_j.

Zij L een eindige uitbreiding van K. Zij v een valuatie van K en w een valuatie van L die v uitbreidt (notatie : w|v). Is v niet-archimedisch, dan het v <u>vertakt</u> (resp. : <u>onvertakt</u>, <u>volledig gesplitst</u>) <u>in L</u> als de aan v geassocieerde priemdeler p de gelijkluidende eigenschap heeft. Is v archimedisch (en dus eveneens w), laat dan σ (resp. σ') de inbedding van K (resp. L) in $\mathbb{C}$ zijn die met v (resp. w) korrespondeert. We zeggen dan dat v <u>vertakt in L</u> als $\sigma(K) \subset \mathbb{R}$ en $\sigma'(L) \not\subset \mathbb{R}$. In alle andere gevallen heet v <u>onvertakt in L</u>, of zegt men dat w|v <u>onvertakt is</u>. De vervollediging van K t.o.v. v kan steeds aangezien worden als een deelveld van de vervollediging van L t.o.v. w. De graad van de uitbreiding is eindig, en wordt de <u>lokale graad van de uitbreiding L/K t.o.v. w|v</u> genoemd. Is p het priemideaal geassocieerd aan v, en P het priemideaal van L geassocieerd aan w, (in het niet-archimedisch geval) dan geldt steeds

dat de lokale graad gelijk is aan $e(P|p).f(P|p)$. In het archimedische geval is de lokale graad steeds 1 of 2, al naargelang $w|v$ onvertakt is of niet.

Indien de uitbreiding L/K galois is, dan is voor elke w die v uitbreidt de lokale graad dezelfde en wordt daarom de lokale graad van v in L genoemd.

Voor onvertakte valuaties gelden verder nog eigenschappen analoog als die in 1.4.

§3. HET KLASSEGETAL

In deze paragraaf is K een getallenveld van graad m over $\mathbb{Q}$.

3.1. De groep der S-eenheden.

Zij S een verzameling van onderling niet-equivalente valuaties van K.

Een S-eenheid is een element ε van K zodat $v(\varepsilon) = 1$ voor alle v die met geen enkel element van S equivalent zijn. De S-eenheden vormen een deelgroep van K^* die we met $U_K(S)$ zullen aanduiden.

Is $S = \phi$, dan is $U_K(S)$ de groep van alle eenheidswortels van K. Deze groep is steeds eindig cyclisch. We zullen verder steeds W_K schrijven in plaats van $U_K(\phi)$.

Veronderstel nu dat $\#S = d$, $1 \leq d < \infty$, en dat S alle inequivalente archimedische valuaties van K bevat. De groep $U_K(S)$ is dan het direkt produkt van W_K met $\mathbb{Z}^{d-1}$ (dit is de zogenaamde "stelling van Dirichlet voor S-eenheden"). Er bestaan dus S-eenheden

$\varepsilon_1,\ldots,\varepsilon_{d-1}$ zó dat elke S-eenheid ε kan geschreven worden als :

$$\varepsilon = \zeta.\varepsilon_1^{a_1}\ldots\varepsilon_{d-1}^{a_{d-1}} ,$$

waarbij $\zeta \in W_K$ en $a_i \in \mathbb{Z}$ eenduidig bepaald zijn door ε. Een dergelijk stel $\{\varepsilon_1,\ldots,\varepsilon_{d-1}\}$ wordt een <u>fundamenteel systeem van S-eenheden voor K</u> genoemd.

3.2. <u>De eenhedengroep en de regulator</u>.

Zij $S = \{v_1,\ldots,v_r\}$ de verzameling van alle niet-equivalente archimedische valuaties. In dit geval zal in alle voorgaande definities en notaties de letter "S" weggelaten worden.

De eenhedengroep U_K' valt samen met de groep der inverteerbare elementen van $\mathcal{O}_K$. Bovendien geldt :

$$\varepsilon \in U_K \Rightarrow |N_{K/\mathbb{Q}}(\varepsilon)| = 1.$$

Omgekeerd, is $\alpha \in \mathcal{O}_K$, en is $|N_{K/\mathbb{Q}}(\alpha)| = 1$, dan geldt : $\alpha \in U_K$. Een andere karakterisering van U_K is dat het de kern is van het homomorfisme :

$$\begin{aligned} \phi_K &: K^* \to I_K \\ &: \alpha \mapsto \alpha.\mathcal{O}_K \quad . \end{aligned}$$

Laat $\sigma_1,\ldots,\sigma_s$ de reële inbeddingen van K in $\mathbb{C}$ zijn (d.w.z. : $\sigma_i(K) \subset \mathbb{R}$ voor $i = 1,\ldots,s$), en laat $\sigma_{s+1},\overline{\sigma}_{s+1},\ldots,\sigma_{s+t},\overline{\sigma}_{s+t}$ de komplekse zijn ($\overline{\sigma}$ is hier : σ, gevolgd door komplekse toevoeging). We zullen verderop veronderstellen dat de elementen v_i van S gedefinieerd worden door :

$$v_i(\alpha) = \begin{cases} |\sigma_i(\alpha)| & \text{voor } 1 \leq i \leq s \\ |\sigma_j(\alpha)|^2 & \text{voor } s+1 \leq j \leq s+t \end{cases}$$

(Noteer dat #S = s+t). Zij $\{\varepsilon_1,\ldots,\varepsilon_{s+t-1}\}$ een fundamenteel systeem van eenheden. De <u>regulator van K</u> is de absolute waarde van een (willekeurige !) (s+t-1) × (s+t-1)-minor uit de matrix :

$$(\ln v_i(\varepsilon_j))_{i=1,\ldots,s+t;\ j=1,\ldots,s+t-1}$$

De regulator van K zal steeds met R_K aangeduid worden. De keuze van het fundamenteel systeem van eenheden heeft geen invloed op de waarde van R_K.

3.3. <u>Het klassegetal van een getallenveld</u>.

De <u>hoofdidealen</u> van K zijn de idealen van de vorm $\alpha.O_K$, $\alpha \in K^*$. Zij vormen een deelgroep van I_K die we met P_K zullen aanduiden. De faktorgroep I_K/P_K wordt de <u>ideaalklassengroep</u> van K genoemd. Een nevenklas van P_K wordt een <u>ideaalklas</u> genoemd. De orde van de ideaalklassengroep is altijd eindig en wordt <u>het klassegetal</u> van K genoemd. We duiden het aan met h_K.

Voor reële waarden van s, > 1, is de reeks :

$$\sum_{a} \frac{1}{N_K(a)^s}$$

waarbij a de gehele idealen van K doorloopt, konvergent. Zij stelt in het gebied $s \geqslant 1+\delta$, $\delta > 0$ een kontinue functie van s voor : de <u>Dedekind-zeta-funktie</u> van K. Deze funktie noteren we als $\zeta_K(s)$. Het verband met het klassegetal van K ligt in de betrekking :

$$\lim_{\substack{s\to 1 \\ >}} (s-1)\zeta_K(s) = h_K \frac{2^{s+t}\,\pi^t\,R_K}{(W_K:1)\sqrt{|D_K|}} .$$

In sommige gevallen (zoals : abelse uitbreidingen van $\mathbb{Q}$) kan de limiet nog verder omgewerkt worden (cfr. [18]). Hierop komen we terug in volgend hoofdstuk. Verder zal nog gebruik gemaakt worden van de identiteit van Euler, i.e. :

$$\zeta_K(s) = \prod_p (1 - N_K(p)^{-1})^{-1} \qquad \text{(voor } s > 1\text{)},$$

waarbij p de priemidealen van K doorloopt.

HOOFDSTUK II

BIKWADRATISCHE VELDEN

De bedoeling van dit hoofdstuk is, met een klassiek voorbeeld : aan te tonen hoe een bepaalde invariant, namelijk de index van de eenhedengroep van een getallenveld K in de eenhedengroep van een eindige uitbreiding L van K een belangrijke rol speelt bij de berekening van het klassegetal van L.

Volledigheidshalve, en tevens met de bedoeling de resultaten uit het voorgaande hoofdstuk te illustreren, geven we hier het gedeelte van de theorie der bikwadratische velden dat nodig is om het klassegetal uit zijn analytische uitdrukking te berekenen.

§1. OVERZICHT VAN DE THEORIE DER KWADRATISCHE VELDEN

1.1. De ring der gehelen.

Een kwadratisch veld is een uitbreiding van graad 2 van $\mathbb{Q}$. Dergelijke velden zijn van het type $\mathbb{Q}(\sqrt{d})$, waarbij $\sqrt{d}$ (*) een wortel is van de vergelijking :

$$\theta^2 - d = 0, \tag{1}$$

waarin voor d een kwadraatvrij geheel getal kan genomen worden. Verschillende dergelijke d geven verschillende kwadratische velden. Is $d < 0$ dan heet $\mathbb{Q}(\sqrt{d})$ imaginair of kompleks, anders heet het reëel.

(*) Met $\sqrt{d}$ bedoelen we hier het positieve getal θ waarvoor $\theta^2 = d$ indien d positief is en $i\sqrt{-d}$ indien d negatief is.

STELLING II.1.1. *Zij* $d \in \mathbb{Z}$, d *kwadraatvrij. Een integrale basis voor* $K = \mathbb{Q}(\sqrt{d})$ *is dan* $\{1, \omega_K\}$, *waarbij :*

$$\omega_K = \begin{cases} \dfrac{\sqrt{d}+1}{2} & \text{indien } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{indien } d \equiv 2 \text{ of } 3 \pmod 4 \end{cases}$$

BEWIJS. Zie [3], ch. II, 7.2.

Gevolg : Voor de diskriminant D_K van K geldt wegens I.1.4. :

$$D_K = \begin{cases} d & \text{indien } d \equiv 1 \pmod 4 \\ 4d & \text{indien } d \equiv 2 \text{ of } 3 \pmod 4 \end{cases}$$

1.2. Priemidealen in kwadratische velden.

Zij $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, d kwadraatvrij.

Zij p een priemideaal van $\mathbb{Q}$. Er zijn slechts drie soorten p te onderscheiden, namelijk :

(1). deze waarvoor $p\mathcal{O}_K = p_1 p_2$, p_1 en p_2 twee verschillende priemidealen van K waarvoor $f(p_i|p) = 1$ (deze p splitsen volledig in K);

(2). deze waarvoor $p\mathcal{O}_K = p$ een priemideaal is van K, en waarbij $f(p|p) = 2$. In dit geval zegt men dat p priem blijft in K.

(3). Deze waarvoor $p\mathcal{O}_K$ het kwadraat is van een priemideaal p van K waarvoor $f(p|p) = 1$ (deze p zijn vertakt in K).

Zij $(\frac{a}{b})$ het Jacobi-symbool. We definiëren de funktie $\chi_K : \mathbb{Z} \to \{0,1,-1\}$ als volgt :

- $\chi_K(x) = 0 \iff (x, D_K) \neq 1$

- voor $(x, D_K) = 1$ heeft men :

$$\chi_K(x) = \begin{cases} \left(\frac{x}{|d|}\right) \text{ indien } d \equiv 1 \pmod 4; \\ (-1)^{\frac{x-1}{2}} \left(\frac{x}{|d|}\right) \text{ indien } d \equiv 3 \pmod 4; \\ (-1)^{\frac{x^2-1}{8} + \frac{x-1}{2} \cdot \frac{d'-1}{2}} \left(\frac{x}{|d'|}\right), \text{ indien } d = 2d'. \end{cases}$$

DEFINITIE II.1.2. De funktie χ_K wordt het karakter van het veld K genoemd.

STELLING II.1.2. *Is p een priemideaal van* $\mathbb{Q}$ *dan geldt :*

(1) p *splitst volledig in* K $\iff \chi_K(p) = 1$

(2) p *blijft priem in* K $\iff \chi_K(p) = -1$

(3) p *is vertakt in* K $\iff \chi_K(p) = 0$

BEWIJS. Zie [3], ch. III., 8.2.

1.3. De eenhedengroep.

Voor een imaginair kwadratisch veld $K = \mathbb{Q}(\sqrt{d})$, d kwadraatvrij, $d < 0$ zijn de getallen s en t uit I.3.2. gelijk aan 0, respektievelijk 2. Dus, $U_K = W_K$. Verder is :

$$W_K = \begin{cases} \{\pm 1, \pm i\} \text{ voor } d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} \text{ voor } d = -3 \\ \{\pm 1\} \text{ en alle overige gevallen.} \end{cases}$$

Voor $d > 0$ heeft men : $s = 2$, $t = 0$. Alle eenheden van K zijn dus van de vorm $\pm\eta^n$, waarbij η een fundamentele eenheid is en $n \in \mathbb{Z}$. De eenheden $\eta^{-1}, -\eta$ en $-\eta^{-1}$ zijn echter, samen met η, eveneens fundamenteel. Een en slechts een onder hen is echter groter dan 1 : deze noemen we dan <u>de fundamentele eenheid van K</u>, en we noteren : η_K.

1.4. <u>Het klassegetal</u>.

Zij d een kwadraatvrij geheel getal. Zij $K = \mathbb{Q}(\sqrt{d})$, en zij χ het karakter van K (definitie II.1.2.).

Voor $s > 0$ konvergeert de reeks

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

naar een funktie van $L(s,\chi)$ die we <u>de L-funktie van het veld K</u> noemen.

<u>STELLING</u> II.1.4. *Zij h_K het klassegetal van het kwadratisch veld $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, d kwadraatvrij. Is $d > 0$, dan geldt :*

$$h_K = \frac{\sqrt{D_K}}{2 \ln \eta_K} L(1,\chi).$$

Is $d < 0$, dan geldt :

$$h_K = \frac{(W_K : 1)\sqrt{|D_K|}}{2\pi} L(1,\chi).$$

<u>BEWIJS</u>. Zie [3], ch.V, 4.

§2. ALGEMEENHEDEN OVER BIKWADRATISCHE VELDEN

1. Definitie en eerste eigenschappen.

Onder een bikwadratisch veld verstaan we hier : een Galois-uitbreiding van $\mathbb{Q}$ met als Galois-groep de Viergroep van Klein.

Het zij hier opgemerkt dat sommige auteurs andere benamingen gebruiken (zoals : "bicyclische bikwadratische getallenvelden") voor dit soort uitbreidingen.

Zij L een bikwadratisch veld, en $G = \{1,\sigma_1,\sigma_2,\sigma_3\}$ zijn Galois-groep over $\mathbb{Q}$. Er gelden dus volgende relaties :

(1) $\sigma_i^2 = 1$ voor alle $i \in \{1,2,3\}$

(2) $\sigma_{i_1}\sigma_{i_2} = \sigma_{i_3}$ voor elke permutatie (i_1,i_2,i_3) van $(1,2,3)$.

Zij K_i $(i = 1,2,3)$ het vast veld voor de deelgroep $\{1,\sigma_i\}$ van G. Klaarblijkelijk is $K_i/\mathbb{Q}$ kwadratisch, en dus :

$$K_i = \mathbb{Q}(\sqrt{d_i}),$$

waarbij d_i een kwadraatvrij geheel getal is. Bovendien geldt :

$$L = K_1K_2K_3 = \mathbb{Q}(\sqrt{d}_1,\sqrt{d}_2,\sqrt{d}_3).$$

Hieruit volgt onmiddellijk dat d_{i_1} het kwadraatvrij deel is van $d_{i_2}d_{i_3}$ voor elke permutatie (i_1,i_2,i_3) van $(1,2,3)$. Stel vervolgens :

(3) $$A_1 = \begin{cases} (d_2,d_3) \text{ indien minstens één van de getallen} \\ \qquad d_2,d_3 \text{ positief is} \\ -(d_2,d_3) \text{ in het ander geval.} \end{cases}$$

Men kan dus schrijven :

$$d_2 = A_3.A_1 \quad \text{en} \quad d_3 = A_2.A_1,$$

waarbij A_2 en $A_3 \in \mathbb{Z}$. Het is duidelijk dat A_1, A_2 en A_3 onderling verschillen, dat ze kwadraatvrij zijn, en dat ze twee aan twee relatief priem zijn. Bovendien zal hoogstens één onder deze getallen negatief zijn, en men heeft eveneens :

$$d_1 = A_2A_3.$$

Omgekeerd, zij $\{A_1, A_2, A_3\}$ een stel van drie verschillende kwadraatvrije gehele getallen, twee aan twee onderling ondeelbaar, en waarvan hoogstens één negatief is. Stel dan :

$$d_1 = A_2A_3; \quad d_2 = A_3A_1; \quad d_3 = A_1A_2,$$

en beschouw het veld

$$L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}).$$

Het is niet moeilijk na te gaan dat $[L : \mathbb{Q}] = 4$ (het stel $\{1, \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}\}$ is immers een basis voor $L/\mathbb{Q}$). Stelt men

$$\alpha = a_0 + a_1\sqrt{d_1} + a_2\sqrt{d_2} + a_3\sqrt{d_3} \quad (a_i \in \mathbb{Q}),$$

dan kan men onmiddellijk narekenen dat de funkties $\sigma_1, \sigma_2, \sigma_3$, gedefinieerd door :

$$\sigma_1(\alpha) = a_0 + a_1\sqrt{d_1} - a_2\sqrt{d_2} - a_3\sqrt{d_3}$$

$$\sigma_2(\alpha) = a_0 - a_1\sqrt{d_1} + a_2\sqrt{d_2} - a_3\sqrt{d_3}$$

$$\sigma_3(\alpha) = a_0 - a_1\sqrt{d_1} - a_2\sqrt{d_2} + a_3\sqrt{d_3}$$

drie verschillende automorfismen van L zijn waarvoor aan de

relaties (1) en (2) voldaan is. Dat tenslotte nog voldaan is aan (3) is eveneens eenvoudig na te gaan. Samenvattend geeft dit :

STELLING II.2.1. *Een bikwadratisch veld* L *wordt op één-éénduidige wijze bepaald door een stel van drie verschillende kwadraatvrije gehele getallen* $\{A_1,A_2,A_3\}$ *die twee aan twee onderling ondeelbaar zijn en waarvan hoogstens één negatief is. Het veld* L *is dan niets anders dan* $\mathbb{Q}(\sqrt{A_2A_3},\sqrt{A_3A_1},\sqrt{A_1A_2})$.

Tot slot merken we nog op dat

$$d_1d_2d_3 = (A_1A_2A_3)^2.$$

Hieruit volgt : $d_1d_2d_3 \equiv 0$ of $1 \pmod 4$. Dit resultaat zullen we verderop nog gebruiken.

2.2. Een kriterium voor bikwadraticiteit.

De volgende stelling leert ons wanneer een kwadratische uitbreiding van een kwadratisch veld bikwadratisch is.

STELLING II.2.2. *Zij* $K = \mathbb{Q}(\sqrt{d})$, d *een kwadraatvrij geheel getal. Zij* $L = K(\sqrt{\mu})$, $\mu \in K$, $\mu \notin K^2$, *een kwadratische uitbreiding van* K. *Zij* $N = N_{K/\mathbb{Q}}$ *de norm van* K *tot* $\mathbb{Q}$. *Dan geldt :*

(i) $L/\mathbb{Q}$ *is Galois* $\Leftrightarrow N(\mu) \in \mathbb{Q}^{*2} \cup \mathbb{Q}^{*2}.d$

(ii) $L/\mathbb{Q}$ *is bikwadratisch* $\Leftrightarrow N(\mu) \in \mathbb{Q}^{*2}$

(iii) $L/\mathbb{Q}$ *is cyclisch* $\Leftrightarrow N(\mu) \in \mathbb{Q}^{*2}.d$

BEWIJS. Zij σ het niet-identieke automorfisme van K (i.e. : $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$; $a,b \in \mathbb{Q}$).

Indien $L/\mathbb{Q}$ Galois is, dan is σ niets anders dan de beperking van een automorfisme $\bar{\sigma}$ van L. Stel : $\bar{\sigma}(\sqrt{\mu}) = \alpha + \beta\sqrt{\mu}$, waarbij $\alpha,\beta \in K$. Dan geldt :

$$(\alpha + \beta\sqrt{\mu})^2 = \alpha^2 + \beta^2\mu + 2\alpha\beta\sqrt{\mu} = (\bar{\sigma}(\sqrt{\mu}))^2 =$$

$$\bar{\sigma}(\mu) = \sigma(\mu) \in K,$$

waaruit volgt : $\alpha = 0$ of $\beta = 0$. De laatste gelijkheid kan niet opgaan wegens het feit dat $\mu \notin K^2$ (en dus ook : $\sigma(\mu) \notin K^2$). Dus, $\sigma(\mu) = \beta^2\mu$, zodat $\mu.\sigma(\mu) = N(\mu) = (\beta\mu)^2$. Er geldt bijgevolg : $N(\mu) \in K^{*2} \cap \mathbb{Q}$. Wegens $K^{*2} \cap \mathbb{Q} = \mathbb{Q}^* \cup \mathbb{Q}^{*2}d$, is het bewijs van "(i) $\Rightarrow$" geleverd.

Veronderstel nu : $N(\mu) = m^2$, $m \in \mathbb{Q}$. Laat σ_1,σ_2 en σ_3 funkties zijn (van L naar L) gedefinieerd door :

$$: \sigma_1(\alpha + \beta\sqrt{\mu}) = \alpha - \beta\sqrt{\mu}$$

$$: \sigma_2(\alpha + \beta\sqrt{\mu}) = \sigma(\alpha) + \sigma(\beta)m\frac{\sqrt{\mu}}{\mu}$$

$$: \sigma_3(\alpha + \beta\sqrt{\mu}) = \sigma(\alpha) - \sigma(\beta)m\frac{\sqrt{\mu}}{\mu},$$

waarbij $\alpha,\beta \in K$. Men kan zonder moeite narekenen dat σ_1,σ_2 en σ_3 drie verschillende, niet-identieke automorfismen zijn van L, en dat ze aan de relaties II.2.1. (1) en (2) voldoen. Hierdoor bewijst men "(ii) $\Leftarrow$".

Is $N(\mu) = m^2d$, $m \in \mathbb{Q}$, dan definiëren we de afbeelding $\tau : L \to L$ als volgt :

$$\tau(\alpha + \beta\sqrt{\mu}) = \sigma(\alpha) + \sigma(\beta)m\sqrt{d}.\frac{\sqrt{\mu}}{\mu}$$

en men rekent zonder moeite na dat τ, τ^2 en τ^3 drie verschillende niet-triviale automorfismen zijn van L, en dat $\tau^4 = id_L$. Dit bewijst "(iii) $\Leftarrow$".

Veronderstel nu dat L bikwadratisch is. Uit II.2.1. volgt dan dat L van de vorm $K(\sqrt{d'})$ is, waarbij $d' \in \mathbb{Q}^*$, $d' \neq d$. Dit betekent echter : $\mu = \alpha^2 d'$ voor een $\alpha \in K$, zodat :

$$N(\mu) = (N(\alpha))^2 d'^2 \in \mathbb{Q}^{*2},$$

zodat nu ook "(ii) $\Rightarrow$" bewezen is.

Het is nu duidelijk dat alle overige implikaties volgen uit het feit dat $\mathbb{Q}^{*2} \cap \mathbb{Q}^{*2}.d = \phi$ en het feit dat een vierdegraadsuitbreiding van $\mathbb{Q}$ die Galois is ofwel bikwadratisch, ofwel cyclisch moet zijn.

Gevolg : Is $d > 0$, en is $\mu = \eta_K$, de fundamentele eenheid van K (zie I.1.3.), dan ziet men dat het veld $L = K(\sqrt{\eta_K})$ dan en slechts dan bikwadratisch is, als $N(\eta_K) = 1$. Is daarentegen $N(\eta_K) = -1$, dan is $L/\mathbb{Q}$ zelfs geen Galois-uitbreiding.

Opmerking : Men kan zonder moeite nagaan dat de stelling ook volgt uit Seidelman's parametrische karakterisering van vierdegraadsuitbreidingen van een veld F. Een dergelijke uitbreiding L is namelijk dan en slechts dan cyclisch over F als L van de gedaante

$$F(f\sqrt{1+e^2}, \sqrt{g(1+e^2+\sqrt{1+e^2})})$$

is met $e,f,g \in F^*$ en $(1+e^2) \notin F^2$, of ook van de gedaante $F(\sqrt[4]{f})$ met $f \in F \setminus F^2$ indien $\sqrt{-1} \in F$. De velden L waarvan de galoisgroep over F de viergroep van Klein is zijn van de gedaante $F(\sqrt{f}+\sqrt{e}+\sqrt{ef})$ met $e,f,ef \in F \setminus F^2$ (zie [25]). Men bekomt het resultaat van stelling II.2.2. door $F = \mathbb{Q}$ te nemen, en voor K een behoorlijk kwadratische uitbreiding van $\mathbb{Q}$ te nemen die in L bevat is (nl. : $\mathbb{Q}\sqrt{1+e^2}$) in het cyclische geval, en $\mathbb{Q}(\sqrt{f})$ in het bikwadratische geval). Door de norm van L tot K te nemen van een element dat F voortbrengt over

L vindt men immers de voorwaarden van de stelling terug.

§3. DE RING DER GEHELEN VOOR BIKWADRATISCHE VELDEN

Doorheen deze paragraaf zal L het bikwadratisch veld

$$\mathbb{Q}(\sqrt{A_2A_3},\sqrt{A_3A_1},\sqrt{A_1A_2})$$

zijn, waarbij A_1,A_2 en A_3 getallen zijn zoals die in stelling II.2.1. Verder stellen we :

$$d_1 = A_2A_3;\quad d_2 = A_3A_1;\quad d_3 = A_1A_2,$$

en voor i = 1,2,3 :

$K_i = \mathbb{Q}(\sqrt{d_i})$

$O_i = O_{K_i} = \mathbb{Z} \oplus \mathbb{Z}\omega_i$, met $\omega_i = \omega_{K_i}$ zoals in stelling II.1.1.

σ_i = het automorfisme van L dat K_i als vast veld heeft.
D.w.z. : $\sigma_i(\sqrt{d_i}) = \sqrt{d_i}$ en $\sigma_i(\sqrt{d_j}) = -\sqrt{d_j}$ indien $j \neq i$.

N_i = de norm van L tot K_i

S_i = het spoor van L tot K_i .

3.1. De integrale basis.

Meestal vraagt het opzoeken van een integrale basis van een getallenveld zeer uitgebreide berekeningen (zie [2]). Voor bikwadratische velden kan men echter van de volgende eigenschap gebruik maken :

STELLING II.3.1.1. *Is* $\xi = \alpha_0 + \alpha_1\sqrt{d_1} + \alpha_2\sqrt{d_2} + \alpha_3\sqrt{d_3}$ $(\alpha_i \in \mathbb{Q})$ *een element van* $\mathcal{O}_L$, *dan geldt voor elke* $i \in \{1,2,3\}$:

$$N_i(\xi) \text{ en } S_i(\xi) \in \mathcal{O}_i.$$

Omgekeerd, is er een $i \in \{1,2,3\}$ *zo dat* $N_i(\xi)$ en $S_i(\xi) \in \mathcal{O}_i$, *dan geldt :* $\xi \in \mathcal{O}_K$.

BEWIJS. Het is bekend dat een element van een getallenveld L dan en slechts dan geheel is, als zijn karakteristieke polynoom ten opzichte van een deelveld K van L tot $\mathcal{O}_K[X]$ behoort. Voor een bikwadratisch veld betekent dit :

$$\xi \in \mathcal{O}_L \Leftrightarrow (X^2 - S_i(\xi)X + N_i(\xi)) \in \mathcal{O}_i[X],$$

waaruit het gestelde.

Ter illustratie berekenen we een integrale basis in een geval waarbij $\omega_i = \sqrt{d_i}$ voor alle $i \in \{1,2,3\}$, namelijk : het geval waarin d_1 en d_2 even zijn terwijl $d_3 \equiv 3 \pmod 4$. Hier heeft men dus : A_3 is even, A_1 en A_2 oneven en $A_1 + A_2 \equiv 0 \pmod 4$. De voorwaarden "$S_i(\xi) \in \mathcal{O}_i$" voor $i = 1,2,3$ geven dan :

$$2\alpha_0 + 2\alpha_i\sqrt{d_i} \in \mathcal{O}_i,$$

zodat : $\alpha_j = \frac{1}{2}a_j$, $a_j \in \mathbb{Z}$ voor alle $j \in \{0,1,2,3\}$. Klaarblijkelijk volstaat het hieraan nog slechts de voorwaarde "$N_3(\xi) \in \mathcal{O}_3$" toe te voegen, wat neerkomt op het oplossen van het stelsel :

$$\begin{cases} a_0^2 + a_3^2d_3 - a_1^2d_1 - a_3^2d_2 \equiv 0 \pmod 4 \\ a_0a_3 - a_1a_2A_3 \equiv 0 \pmod 2. \end{cases}$$

Men toont echter zonder moeite aan dat dit stelsel gelijkwaardig is met :

$$\begin{cases} a_0 \equiv a_3 \equiv 0 \pmod 2 \\ a_1 \equiv a_2 \pmod 2. \end{cases}$$

Op grond hiervan kunnen we schrijven :

$$a_0 = 2m_0; \quad a_2 = m_2; \quad a_1 = a_2 + 2m_1; \quad a_3 = 2m_3,$$

waarbij $m_0, m_1, m_2, m_3 \in \mathbb{Z}$. We bekomen aldus :

$$\xi = m_0 + m_1\sqrt{d_1} + m_2\left(\frac{\sqrt{d_1} + \sqrt{d_2}}{2}\right) + m_3\sqrt{d_3} \ ,$$

waaruit volgt :

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}.\sqrt{d_1} \oplus \mathbb{Z}.\left(\frac{\sqrt{d_1} + \sqrt{d_2}}{2}\right) \oplus \mathbb{Z}.\sqrt{d_3} \ .$$

De werkwijze voor de andere gevallen (die bepaald worden door de aard van de elementen ω_i) verloopt analoog en wordt aan de lezer overgelaten. We verwijzen hier eveneens naar [21], waar de integrale basis via een andere weg berekend wordt. De resultaten kunnen als volgt geresumeerd worden :

STELLING II.3.1.2. *Zij* L *het bikwadratisch veld, omschreven bij de aanvang van deze paragraaf.*

- *In de volgende twee gevallen :*

  (i) A_3 *even*

  (ii) Alle A_i *oneven en* $A_1 + A_3 \equiv A_3 + A_2 \equiv 0 \pmod 4$

geldt :

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}.\sqrt{d_1} \oplus \mathbb{Z}.\left(\frac{\sqrt{d_1} + \sqrt{d_2}}{2}\right) \oplus \mathbb{Z}.\omega_3$$

- *Is* $A_1 \equiv A_2 \equiv A_3 \equiv a \pmod 4$, *waarbij* $a = 1$ *of* 3, *dan geldt :*

$$\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}.\omega_1 \oplus \mathbb{Z}.\omega_2 \oplus \mathbb{Z}.\left(\frac{a + \sqrt{d_1} + \sqrt{d_2} + \sqrt{d_3}}{4}\right)$$

Elke geoorloofde keuze van de getallen A_1, A_2 *en* A_3 *kan na eventuele hernummering in een van de bovenstaande gevallen ondergebracht worden.*

Gevolg : De diskriminant D_L van L voldoet aan de betrekking :

$$D_L = D_{K_1} D_{K_2} D_{K_3}.$$

Dit bewijst men onmiddellijk door gebruik te maken van de definitie van D_L (zie I.1.4.) en de door II.1.1. geleverde waarde van D_{K_i}.

Hierbij merken we op dat D_L steeds een kwadraat is, aangezien $D_L = \mu_1\mu_2\mu_3 (A_1A_2A_3)^2$ (hierin is $\mu_j = D_{K_j}.d_j^{-1}$ en dit is 1 of 4 wegens II.1.1.).

Wat betreft de diskriminant van de uitbreiding L/K_i zij eraan herinnerd dat voor drie getallenvelden F, E, M, met $F \subset E \subset M$ de volgende relatie geldt :

$$D_{M/F} = (D_{E/F})^{[M:E]} N_{E/F}(D_{M/E})$$

Stelt men hierin $F = \mathbb{Q}$, $E = K_i$, $M = L$, dan verkrijgen we :

$$(1) \qquad N_{K_i/\mathbb{Q}}(D_{L/K_i}) = \frac{\mu_1\mu_2\mu_3}{\mu_i^2} A_i^2.\mathbb{Z},$$

We vestigen hier de aandacht op het feit dat de faktor $\mu_1\mu_2\mu_3\mu_i^{-2}$ slechts de waarden 1,4 of 16 kan aannemen.

3.2. Priemidealen.

Voor i = 1,2,3, zij χ_i het karakter van K_i (zie II.1.2.).

STELLING II.3.2.1. *Is* p *een priemgetal, dan geldt :*

(i) $\prod_{i=1}^{3} \chi_i(p) \neq 0 \Rightarrow \prod_{i=1}^{3} \chi_i(p) = 1$

(ii) zo er een $i \in \{1,2,3\}$ *is waarvoor* $\chi_i(p) = 0$, *dan bestaat er nog een andere index* $j \in \{1,2,3\}$ *waarvoor* $\chi_j(p) = 0$.

BEWIJS. De eerste bewering volgt rechtstreeks uit de definitie van χ_i en uit de eigenschappen van het Jacobi-symbool.

Voor wat betreft (ii), stel $\chi_1(p) = 0$. Dit betekent dus : $p|D_{K_1} = \mu_1 A_2 A_3$ (μ_1 zoals in vorig punt). Indien $p|A_2$ of $p|A_3$, dan is het duidelijk dat $p|D_{K_2}$ of $p|D_{K_3}$, zodat $\chi_2(p)$ of $\chi_3(p)$ nul zal zijn. Is $p \nmid A_2A_3$, dan moet "$p|\mu_1$" opgaan, en dus zal $\mu_1 = 4$, en zal $p = 2$. Uit $\mu_1 = 4$ volgt echter : $d_1 = 2$ of $3 \pmod 4$. Dat de eerste van deze twee mogelijkheden vervalt volgt uit het feit dat $p = 2$ geen deler is van $A_2A_3 = d_1$. Uit $d_1d_2d_3 = (A_1A_2A_3)^2 \equiv 0$ of $1 \pmod 4$ volgt dan : d_2 of $d_3 \equiv 2$ of $3 \pmod 4$, zodat in elk geval, hetzij "$p|D_{K_2}$" hetzij "$p|D_{K_3}$", opgaat. M.a.w. : $\chi_2(p)$ of $\chi_3(p) = 0$, Q.E.D.

Gevolg : Het drietal $(\chi_1(p),\chi_2(p),\chi_3(p))$ kan slechts een permutatie zijn van een van de volgende vijf drietallen :

$$(1,1,1);\quad (1,-1,-1);\quad (0,0,1);\quad (0,0,-1);\quad (0,0,0).$$

STELLING II.3.2.2. *Zij* p *een priemgetal, en zij*

$$X_p = \{\chi_1(p),\chi_2(p),\chi_3(p)\}.$$

Dan geldt voor de kanonieke dekompositie van het ideaal pO_L :

(1) $\quad X_p = \{1\} :\Leftrightarrow : pO_L = P_1P_2P_3P_4;\ P_i \neq P_j$ *voor* $i \neq j$ *en*

$f(P_i|p\mathbb{Z}) = 1$ *voor* $i = 1,2,3,4$.

(2) $X_p = \{1,-1\} : \Leftrightarrow : p\mathcal{O}_L = P_1P_2;\ P_1 \neq P_2$ *en* $f(P_i|p\mathbb{Z}) = 2$ *voor* $i = 1,2$.

(3) $X_p = \{0,1\} : \Leftrightarrow : p\mathcal{O}_L = P_1^2P_2^2;\ P_1 \neq P_2$ *en* $f(P_i|p\mathbb{Z}) = 1$ *voor* $i = 1,2$.

(4) $X_p = \{0,-1\} : \Leftrightarrow : p\mathcal{O}_L = P^2;\ f(P|p\mathbb{Z}) = 2$

(5) $X_p = \{0\} : \Leftrightarrow : p = 2$ *en* $2\mathcal{O}_L = P^4;\ f(P|2\mathbb{Z}) = 1$.

BEWIJS. Voor wat betreft (1), (2), (3), dit volgt eenvoudig door toepassing van I.1.5. (voor splitsende priemidealen). Het geval (4) volgt uit de multiplikativiteit van de restklassengraad by ketens. (cfr. I.1.2.). In het vijfde geval is het duidelijk dat $p = 2$; aangezien $\chi_i(p) = 0$ voor alle i slechts optreedt wanneer p alle diskriminanten D_{K_i} deelt, en dat dit, wegens het feit dat de getallen A_i twee aan twee onderling ondeelbaar zijn, slechts voorkomt als $D_{K_i} = 4.A_kA_l$ (hier is $\{k,l\} = \{1,2,3\} \setminus \{i\}$). De formule II.3.1. (1) geeft ons dan :

$$N_{K_i/\mathbb{Q}}(D_{L/K_i}) = 4A_i^2\mathbb{Z}.$$

De aanwezigheid van de faktor 4 en het rechterlid impliceert echter dat het (unieke !) priemideaal van K_i dat boven $2.\mathbb{Z}$ ligt een deler moet zijn van D_{L/K_i}. Hieruit volgt : $p_i\mathcal{O}_L = P^2$, aangezien de priemdelers van D_{L/K_i} precies deze zijn die vertakken in L (cfr. I.1.4.). Uit $2.\mathcal{O}_i = p_i^2$ volgt dan : $2.\mathcal{O}_L = P^4$. Dat omgekeerd, $X_p = \{0\}$ volgt uit $2\mathcal{O}_L = P^4$, is eenvoudig af te leiden uit de multiplikativiteit van de ramifikatie-index by ketens.

Opmerking : De vijf geciteerde mogelijkheden voor X_p hoeven niet

alle aan bod te komen. Dit is bijvoorbeeld het geval voor het veld $L = \mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{10})$. Men ziet daar dat $0 \in X_p$ betekent : $p = 2$ of 5. Men kan echter gemakkelijk narekenen dat

$$\chi_1(2) = \chi_3(2) = 0; \quad \chi_2(2) = -1;$$

$$\chi_1(5) = -1; \quad \chi_2(5) = \chi_3(5) = 0,$$

zodat : $0 \in X_p \Rightarrow X_p = \{0,-1\}$. (Noteer dat we hier onderstellen dat $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{5})$, $K_3 = \mathbb{Q}(\sqrt{10})$.)
Anderzijds bestaan er bikwadratische velden waarin elk van de vijf mogelijkheden voor X_p voorkomt. Dit is het geval voor het veld $L = \mathbb{Q}(\sqrt{7},\sqrt{2.3.5},\sqrt{2.3.5.7})$. Men vindt hier :

$$X_2 = \{0\}; \; X_3 = \{0,1\}; \; X_5 = \{0,-1\}; \; X_{11} = \{1,-1\} \text{ en } X_{19} = \{1\}.$$

3.3. De eenhedengroep.

Voor $i = 1,2,3$, zijn U_i de groep der eenheden en W_i de groep der eenheidswortels van K_i. Indien K_i reëel is, zij dan η_i zijn fundamentele eenheid.

STELLING II.3.3.1. *Is* W_L *de groep der eenheidswortels van het veld* L, *dan geldt :*

$$(W_L : 1) = \begin{cases} 12 \text{ } \textit{indien } L = \mathbb{Q}(\sqrt{-1},\sqrt{-3},\sqrt{3}) \\ 8 \text{ } \textit{indien } L = \mathbb{Q}(\sqrt{-1},\sqrt{-2},\sqrt{2}) \\ 6 \text{ } \textit{indien } L = \mathbb{Q}(\sqrt{-3},\sqrt{-d},\sqrt{3d}),\ d \in \mathbb{N}_0,\ \textit{kwadraatvrij en} \neq 1,3 \\ 4 \text{ } \textit{indien } L = \mathbb{Q}(\sqrt{-1},\sqrt{-d},\sqrt{d}),\ d \in \mathbb{N}_0,\ \textit{kwadraatvrij en} \neq 1,2 \textit{ of } 3 \\ 2 \text{ } \textit{in alle andere gevallen.} \end{cases}$$

BEWIJS. Stel : $(W_L : 1) = m$, en zij $\zeta_m = \exp(2\pi i\, m^{-1})$. Het is bekend dat m steeds even zal zijn. Verder is eveneens bekend dat :

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m),$$

waarbij $\phi(m)$ de indikator van Euler is. De voorwaarde : $\phi(m) \mid 4$ impliceert echter onmiddellijk : $m = 12,10,8,6,4$ of 2. Aangezien de uitbreiding $\mathbb{Q}(\zeta_{10})/\mathbb{Q}$ cyclisch is moet men $m = 10$ uitsluiten. De stelling volgt dan aanstonds uit het feit dat :

$$\zeta_{12} = \tfrac{1}{2}(\sqrt{3} + i);\ \zeta_8 = \tfrac{\sqrt{2}}{2}(1 + i);\ \zeta_6 = \tfrac{1}{2}(1 + \sqrt{-3});\ \zeta_4 = i;\ \zeta_2 = -1.$$

STELLING. II.3.3.2. *De groep* $U_1U_2U_3$ *heeft eindige index in de groep der eenheden* U_L *van* L.

BEWIJS. We onderscheiden twee gevallen.

1. Zij één der getallen A_1, A_2, A_3 negatief (zegge : A_3). Het is dan duidelijk dat alle inbeddingen van L in $\mathbb{C}$ kompleks zijn. De rang van de vrije groep U_L/W_L is dus 1. Anderzijds is het veld K_3 reëel, terwijl K_1 en K_2 kompleks zijn. Dus, U_1 en U_2 zijn torsiegroepen, terwijl U_3/W_3 rang 1 heeft. De groep $U_1U_2U_3$ is dus modulo torsie van dezelfde rang als U_L/W_L, waaruit het gestelde volgt.

2. Laat alle getallen A_1, A_2, A_3 positief zijn. Alle inbeddingen van L in $\mathbb{C}$ zijn dan reëel, zodat U_L/W_L van rang 3 is. Om de stelling te bewijzen zal het dus volstaan aan te tonen dat η_1, η_2 en η_3 multiplikatief onafhankelijk zijn. Welnu, veronderstel :

$$\eta_1^{a_1}\eta_2^{a_2} = \xi\eta_3^{a_3}, \quad \text{met} \quad a_i \in \mathbb{Z}, \quad \xi \in \{+1,-1\}.$$

Stel : $\delta_i = \eta_i^{a_i} = u_i + v_i\sqrt{d_i}$ voor $i = 1$ en 2, en

$\delta_3 = \xi\eta_3^{a_3} = u_3 + v_3\sqrt{d_3}$. Uit $\delta_i \in U_i$ volgt :

(1) : $u_i^2 - v_i^2 d_i = +1$ of -1

(2) : $2u_i,\ 2v_i \in \mathbb{Z}$.

Uit $\delta_1\delta_2 = \delta_3$ volgt dan :

$$u_1u_2 = u_3;\quad u_1v_2 = u_2v_1 = 0;\quad A_3v_1v_2 = v_3.$$

Men leidt hier zonder moeite uit af dat :

$$v_1 = v_2 = v_3 = 0 \quad \text{en} \quad u_i^2 = 1.$$

Dit kan echter slechts opgaan indien $a_1 = a_2 = a_3 = 0$, waaruit het gestelde volgt.

Opmerking : In het eerste geval zien we dat $(U_L : U_3)$ eindig is. Deze situatie is echter vrij uitzonderlijk (zie verder, hoofdstuk V, §2.). In de volgende hoofdstukken zal aangetoond worden hoe in een volstrekt willekeurige situatie, men in de groep der eenheden van een getallenveld E een deelgroep kan bepalen waarin de eenhedengroep van een deelveld F van E een eindige index heeft. In het hierna volgend punt zullen we aantonen wat de rol van de index $(U_L : U_3)$ zal zijn in de berekening van het klassegetal h_L in funktie van de klassegetallen van de velden K_i.

3.4. Het klassegetal van L.

Voor i = 1,2,3, zij χ_i het karakter van het veld K_i (definitie II.1.2.). De funkties $L(s,\chi_i)$ werden in §1.3. geintroduceerd.

STELLING II.3.4.1. *Is* ζ_L *de Dedekind-zeta-funktie van het veld* L, *dan geldt voor* s > 1 :

$$\zeta_L(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_3)$$

waarin $\zeta(s)$ *de klassieke Riemann-zeta-funktie is.*

BEWIJS. Voor $s > 1$ geldt : (Euler's identiteit)

$$(1) \qquad \zeta_L(s) = \prod_p (1 - N_L(P)^{-1})^{-1}.$$

Voor elk priemideaal p van $\mathbb{Q}$ stellen we :

$$(2) \qquad C_p(s) = \prod_{P \mid p} (1 - N_L(P)^{-s}).$$

De absolute konvergentie van het produkt in (1) verzekert ons dat :

$$\zeta_L(s) = \prod_p C_p(s)^{-1},$$

waarbij p alle priemidealen van $\mathbb{Q}$ doorloopt.

Anderzijds geldt, als rechtstreekse toepassing van Stelling II.3.2.2. :

$$C_p(s) = (1 - \frac{1}{p^s})(1 - \frac{\chi_1(p)}{p^s})(1 - \frac{\chi_2(p)}{p^s})(1 - \frac{\chi_3(p)}{p^s}).$$

Substitueert men dit in (2), dan bekomt men na behoorlijke hergroepering :

$$\zeta_L(s) = \prod_p (1 - \frac{1}{p^s})^{-1} \cdot \prod_{i=1}^{3} (1 - \frac{\chi_i(p)}{p^s}) .$$

Het is echter bekend dat de eerste faktor in dit produkt niets anders is dan $\zeta(s)$, terwijl elk van de andere drie faktoren de funkties $L(s,\chi_i)$ opleveren. Q.E.D.

We kunnen thans het klassegetal h_L in funktie van de klassegetallen h_{K_i} berekenen door middel van I.3.3. en Stelling II.1.4. Er geldt immers :

$$\lim_{s \to 1 \atop >} (s-1)\zeta(s) = 1 \quad \text{en} \quad \lim_{s \to 1 \atop >} L(s,\chi_i) = L(1,\chi_i),$$

zodat :

$$(3) \qquad \lim_{s \to 1 \atop >} (s-1)\zeta_L(s) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_3)$$

We beschouwen eerst het geval waarin $A_1, A_2 > 0$ en $A_3 < 0$ (we noemen L in dit geval imaginair). De limiet aan de linkerkant van (3) is dan wegens I.3.3. gelijk aan :

$$h_L \cdot \frac{4\pi^2 |2\ln|\varepsilon||}{(W_L : 1)\sqrt{|D_L|}},$$

waarbij ε een fundamentele eenheid is van L. Anderzijds is het linkerlid van (3) wegens Stelling II.1.4. gelijk aan :

$$h_1 h_2 h_3 \frac{4\pi^2 \, 2\ln \eta_3}{(W_1 : 1)(W_2 : 2)\sqrt{D_1 D_2 D_3}},$$

waarin h_i staat voor het klassegetal en D_i voor de diskriminant van K_i $(i = 1,2,3)$. Aldus bekomt men (met behulp van Stelling II.3.1.2., gevolg) :

$$h_L = \frac{(W_L : 1)}{(W_1 : 1)(W_2 : 1)} \left(\frac{\ln \eta_3}{|\ln|\varepsilon||}\right) h_1 h_2 h_3 .$$

Hierin kan men nu, met behulp van Stelling II.3.3.1., gemakkelijk nagaan dat de faktor $(W_L : 1).(W_1 : 1)^{-1}(W_2 : 1)^{-1}$ gelijk is aan 1/2, behalve wanneer $L = \mathbb{Q}(\sqrt{-1},\sqrt{-2},\sqrt{2})$ waar men 1 bekomt. Wat nu betreft de faktor $(\ln \eta_3).|\ln|\varepsilon||^{-1}$, deze leidt men af uit het feit dat er steeds een relatie tussen η_3 en ε bestaat van de gedaante :

$$\eta_3 = \zeta . \varepsilon^q,$$

waarbij $\zeta \in W_L$ en $q \in \mathbb{Z}$. Het is klaar dat we $q > 0$ mogen onderstellen. De betekenis van q is dan dat het precies gelijk is

aan de index : $(U_L : W_L U_3)$, wat ons uiteindelijk geeft :

STELLING II.3.4.2. *(1^e deel) : Het klassegetal van een imaginair bikwadratisch veld wordt gegeven door de betrekking :*

$$h_L = \frac{(U_L : W_L U_3)}{2} h_1 h_2 h_3 ,$$

met uitzondering van het veld $L = \mathbb{Q}(\sqrt{-1},\sqrt{-2},\sqrt{2})$ *waarvoor geldt :*

$$h_L = (U_L : W_L U_3) h_1 h_2 h_3 .$$

Voor wat betreft de reëele bikwadratische velden (d.w.z. $A_i > 0$ voor alle i) zal men zonder moeite op analoge wijze de formule :

$$h_L = \frac{(\ln \eta_2)(\ln \eta_2)(\ln \eta_3)}{R_L} h_1 h_2 h_3$$

bekomen. Is $\{\varepsilon_1,\varepsilon_2,\varepsilon_3\}$ een fundamenteel systeem van eenheden voor L, dan gelden volgende relaties (voor i = 1,2,3) :

$$\eta_i = \zeta_i \prod_{j=1}^{3} \varepsilon^{a_{ij}}, \text{ met } \zeta_i \in \{+1,-1\} = W_i .$$

Is τ dan een willekeurig automorfisme van L, dan gelden volgende relaties (voor j = 1,2,3) :

$$|\varepsilon_j^\tau| = \prod_{k=1}^{3} |\eta_k^\tau|^{b_{jk}}$$

Hierbij is de matrix (b_{jk}) de inverse van de matrix (a_{ij}). Aangezien we voor de regulator R_L van L kunnen nemen :

$$R_L = |\det(\ln|\sigma_i(\varepsilon_j)|)|,$$

en aangezien $|\eta_k^\tau| = \begin{cases} |\eta_k| & \text{indien } \tau = \sigma_k \\ |\eta_k|^{-1} & \text{indien } \tau \neq \sigma_k, \end{cases}$

volgt onmiddellijk :

$$R_L = |\det((b_{ij}).A)|,$$

waarin A de volgende matrix is :

$$\begin{pmatrix} +\ln \eta_1 & -\ln \eta_1 & -\ln \eta_1 \\ -\ln \eta_2 & +\ln \eta_2 & -\ln \eta_2 \\ -\ln \eta_3 & -\ln \eta_3 & +\ln \eta_3 \end{pmatrix}.$$

Dus, $R_L = \frac{1}{4}(\det(a_{ij}))^{-1}$. Hier is $|\det(a_{ij})|$ niets anders dan de index $(U_L : U_1U_2U_3)$ (de lezer vindt een bewijs hiervan in hoofdstuk IV., §1. 2.). We bekomen dus :

STELLING II.3.4.2. *(2^e deel). Het klassegetal van een reëel bikwadratisch veld is gegeven door :*

$$h_L = \frac{(U_L : U_1U_2U_3)}{4} h_1h_2h_3.$$

Opmerking. In hoofdstuk IV, §1 zullen we aantonen dat $q = (U_L : W_LW_3)$ in een imaginair bikwadratisch veld slechts de waarde 1 of 2 kan aannemen. Voor reëele bikwadratische velden kan de faktor $(U_L : U_1U_2U_3)$ slechts de waarden 1, 2 of 4 aannemen : we verwijzen de lezer hiervoor naar [17] (en de aldaar geciteerde werken in verband met bikwadratische velden) waar de lezer een algebraïsch bewijs van het 2^e deel van Stelling II.3.4.2. zal aantreffen.

HOOFDSTUK III

RADIKALEN IN MULTIPLIKATIEVE GROEPEN VAN VELDEN

In dit hoofdstuk stellen we ons tot doel de multiplikatieve groep K^* van een willekeurig veld K, en deze van een uitbreiding L van K, nader te onderzoeken. Meer bepaald zullen we in L^* een deelgroep definiëren, het radikaal van K^* in L^*, en de voorwaarden nagaan waaronder K^* van eindige index is in dit radikaal.

§1. HET RADIKAAL

In deze paragraaf zullen abelse groepen doorgaans multiplikatief genoteerd worden. Van een abelse groep A zal de torsie-deelgroep (dit is de deelgroep van A bestaande uit alle elementen van A met eindige periode of orde) steeds met W_A aangeduid worden.

1.1. Definities en eerste eigenschappen.

Zij G een abelse groep en H een deelgroep van G.

DEFINITIE III.1.1.1. Het radikaal van H in G is de verzameling van alle elementen x uit G waarvan een van nul verschillende macht tot H behoort.

We zullen het radikaal van H in G met $R_G(H)$ aanduiden. Er geldt dus :

$$R_G(H) = \{x \mid x \in G \ \& \ \exists\ n \in \mathbb{N}_0 \text{ zó dat } x^n \in H\}.$$

Het is onmiddellijk duidelijk dat $R_G(H)$ een deelgroep van G is die H bevat; het heeft dus zin over het quotient $R_G(H)/H$ te spreken.

DEFINITIE III.1.1.2. De orde van de quotiëntgroep $R_G(H)/H$ wordt de R-index van H in G genoemd en wordt met $Q_G(H)$ aangeduid.

Een andere karakterisering van het radikaal is klaarblijkelijk de volgende : $R_G(H)$ is het inverse beeld van de torsie-deelgroep $W_{G/H}$ van G/H onder het natuurlijk homomorfisme : $G \to G/H$. Het is verder eveneens duidelijk dat $W_G = R_G(\{1\})$, en dat W_G bevat is in $R_G(H)$ voor elke deelgroep H van G. Het heeft dus zin te spreken over het quotiënt $R_G(H)/H.W_G$ dat, wegens het feit dat $R_G(H) = R_G(H.W_G)$, niets anders is dan de torsie-deelgroep van $G/H.W_G$.

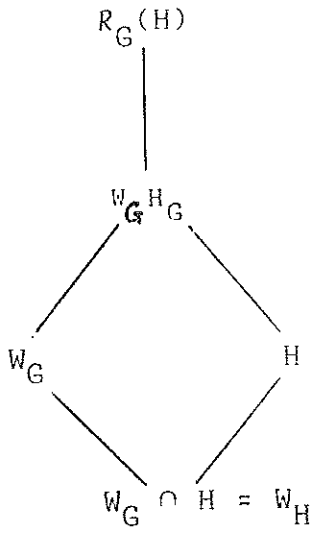
DEFINITIE III.1.1.3. De orde van de quotiëntgroep $R_G(H)/H.W_G$ wordt de RT-index van H in G genoemd en wordt met $q_G(H)$ aangeduid.

1.2. Stellingen.

STELLING III.1.2.1. *Zij* H *een deelgroep van een abelse groep* G. *Indien twee van de drie indices* $Q_G(H)$, $q_G(H)$, $(W_G : W_H)$ *eindig zijn, dan is de derde het eveneens en er geldt :*

$$Q_G(H) = (W_G : W_H).q_G(H).$$

BEWIJS. Beschouw het volgende diagram van inklusies :



De klassieke isomorfiestellingen uit de groepentheorie geven dan :

$$(R_G(H)/H)/(H.W_G/H) \cong R_G(H)/H.W_G$$

$$H.W_G/H \cong W_G/(W_G \cap H) \cong W_G/W_H \ ,$$

waaruit het gestelde volgt.

STELLING III.1.2.2. *Zijn* H,H', *deelgroepen van een abelse groep* G, *en is* $H \subset H'$ *dan geldt :* $R_G(H) \subset R_G(H')$. *Bovendien is het radikaal van* H *in* H' *gedefinieerd, en er geldt :*

$$R_{H'}(H) = R_G(H) \cap H'$$

BEWIJS. Triviaal.

STELLING III.1.2.3. *Zij* H *een deelgroep van een abelse groep* G, *en zij* F_H *de familie van alle deelgroepen van* G *die* H *bevatten en waarin* H *van eindige index is. Dan geldt :*

$$R_G(H) = \bigcup_{H' \in F_H} H' .$$

BEWIJS. Zij $H' \in \mathcal{F}_H$, en stel $m = (H' : H)$. Voor elke $x \in H'$ geldt dus : $x^m \in H$, zodat $x \in R_G(H)$. Hieruit volgt $H' \subset R_G(H)$, en dus :

$$\bigcup_{H' \in \mathcal{F}_H} H' \subset R_G(H).$$

Teneinde de omgekeerde inklusie te bewijzen, nemen we $x \in R_G(H)$, en noemen we m_x het kleinste onder alle van nul verschillende natuurlijke getallen n waarvoor $x^n \in H$. Is $H(x)$ de deelgroep van G voortgebracht door H en x, dan ziet men onmiddellijk dat de quotiëntgroep $H(x)/H$ cyclisch is van orde m_x. D.w.z. : $(H(x) : H) < \infty$, of : $H(x) \in \mathcal{F}_H$. Elk element van $R_G(H)$ is dus een element van een deelgroep H' uit $\mathcal{F}_H$, i.e. : het is een element van $\bigcup_{H' \in \mathcal{F}_H} H'$, Q.E.D.

Tot slot merken we nog op dat $R_G(R_G(H)) = R_G(H)$, zodat : $R_G(W_G) = R_G(R_G(\{1\})) = W_G$. Indien G een torsiegroep is (i.e. : $G = W_G$) dan geldt : $R_G(H) = G$ voor elke deelgroep H van G en omgekeerd. Is H een deelgroep van een abelse groep G, en is $W_G \subset H$, dan vallen de begrippen R-index en RT-index samen; dit is ondermeer steeds het geval als G torsievrij is (d.w.z. : $W_G = \{1\}$).

§2. DE R- EN RT-INDEX BIJ UITBREIDING VAN EEN VELD

2.1. Algemeenheden.

Zij K een willekeurig veld en L een willekeurige uitbreiding van K. We zullen thans onze aandacht laten uitgaan naar het radikaal van de multiplikatieve groep K^* in de multiplikatieve groep L^*. Hierbij zullen we – om typografische redenen – de volgende notaties voortaan in acht nemen : indien de multiplikatieve groep F^* van een veld F als index in sommige notaties voorkomt zullen we kortweg F schrijven. Aldus zullen we symbolen zoals $R_L(K^*)$, $Q_L(K^*)$, $q_L(K^*)$,

W_L, W_K ontmoeten in plaats van de overeenkomstige symbolen met L^* of K^* in de index. Hierbij zij opgemerkt dat W_L niets anders is dan de groep der eenheidswortels van L (zie ook : I.3.1.).

We stippen hier even het verband aan tussen de onderliggende verzameling van $R_L(K^*)/K^*$ en de verzameling F van alle uitbreidingen van de vorm $K(\sqrt[n]{a})$, $a \in K^*$, die in L bevat zijn. Is namelijk $\xi \in R_L(K^*)$, dan is het duidelijk dat het veld $K(\xi)$ tot F behoort. Dit geeft een afbeelding :

$$\phi : R_L(K^*) \to F$$
$$: \xi \mapsto K(\xi) ,$$

die duidelijk surjektief is. Is echter $\xi' \in R_L(K^*)$, en is $\xi'\xi^{-1} \in K^*$, dan is $K(\xi) = K(\xi')$, zodat ϕ faktoriseert door $R_L(K^*)/K^*$; met andere woorden : er bestaat een surjektieve afbeelding :

$$\tau : R_L(K^*)/K^* \to F.$$

Het is bovendien duidelijk dat F een singleton is dan en slechts dan als $R_L(K^*) = K^*$. Nochtans is τ meestal niet injektief, aangezien in vele gevallen $K(\xi)$ en $K(\xi^m)$ dezelfde velden zijn (voor $\xi \in R_L(K^*)$ en gepast gekozen m) zonder dat daarom ξ^{m-1} een element is van K^*. Een voorbeeld hiervan is : $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$.

2.2. Voorbeelden.

Hier zullen we aantonen dat de R-index van K^* in L^* oneindig kan zijn, alhoewel $\# F$ eindig is.

Voorbeeld 1. Zij $K = \mathbb{R}$ en $L = \mathbb{C}$. Vanzelfsprekend geldt hier : $F = \{\mathbb{R}, \mathbb{C}\}$.

Anderzijds heeft men wegens stelling III.1.2.1. :

$$Q_{\mathbb{C}}(\mathbb{R}^*) = (W_{\mathbb{C}} : W_{\mathbb{R}}).q_{\mathbb{C}}(\mathbb{R}^*).$$

Hierin is $W_{\mathbb{C}}$ een oneindige groep, terwijl $W_{\mathbb{R}}$ slechts de elementen +1 en -1 bevat. Derhalve is $Q_{\mathbb{C}}(\mathbb{R}^*)$ oneindig. Later zullen we aantonen dat dit uitsluitend te wijten is aan het oneindig zijn van de faktor $(W_{\mathbb{C}} : W_{\mathbb{R}})$.

Voorbeeld 2. Zij k_0 een veld van karakteristiek 2, en zij $K = k_0(t)$, t zijnde een transcendent element over k_0. Zij $L = K(\sqrt{t})$. Wegens $[L : K] = 2$ geldt hier eveneens : $\# F = 2$.
Een element $\alpha \in L$ is echter van de vorm :

$$\alpha = f + g\sqrt{t} \; ; \; f,g \in K,$$

en dus geldt : $\alpha^2 = f^2 + g^2.t \in K$. Dit impliceert dat $R_L(K^*)$ samenvalt met L^*. De groep L^*/K^* is echter van oneindige orde. Dit volgt uit het feit dat de elementen van de vorm $f + \sqrt{t}$ $(f \in K)$ alle in verschillende nevenklassen van L^* volgens K^* liggen, i.e. :

$$\frac{f + \sqrt{t}}{g + \sqrt{t}} \in K^* \Leftrightarrow f = g,$$

en er oneindig veel elementen $f + \sqrt{t}$ voorhanden zijn.
Het is verder duidelijk dat $W_L = W_K$ (zoniet was $L = K(\zeta)$, ζ een eenheidswortel; dergelijke uitbreidingen zijn echter steeds separabel, terwijl $K(\sqrt{t})/K$ inseparabel is). Het oneindig zijn van $Q_L(K^*)$ kan hier dus aan de inseparabiliteit van de beschouwde uitbreiding toegeschreven worden.

Het eerste voorbeeld toont aan dat het niet opportuun is de R-index van K^* en L^* te onderzoeken, daar deze oneindig wordt zodra $(W_L : W_K)$ oneindig is. Voor inseparabele uitbreidingen blijkt uit voorbeeld 2 dat een eenvoudig resultaat voor $q_L(K^*)$ niet kan

verwacht worden. In de volgende paragrafen zullen we echter zien dat de index $q_L(K^*)$ aan een zeer eenvoudige wet voldoet wanneer L/K eindig en separabel is.

§3. DE RT-INDEX BIJ CYCLISCHE UITBREIDINGEN

3.1. Een Lemma.

We geven hier een resultaat uit de theorie der abelse groepen dat in de loop van deze thesis nog meermaals zal gebruikt worden.

We behouden de multiplikatieve schrijfwijze voor abelse groepen. Is G een abelse groep, en h een homomorfisme van G (naar een niet nader vernoemde abelse groep), dan zal het beeld van h met G^h en de kern van h met G_h aangeduid worden. Is H een deelgroep van G, dan staan de notaties H^h en H_h respektievelijk voor het beeld en de kern van de beperking $h|H$ van h tot H.

LEMMA III.3.1. Zij A een abelse groep, f een homomorfisme van A (naar een niet nader vernoemde abelse groep), en zij B een deelgroep van A. Dan zijn de afbeeldingen $\bar{i} : A_f/B_f \to A/B$ en $\bar{f} : A/B \to A^f/B^f$, die gedefinieerd zijn door :

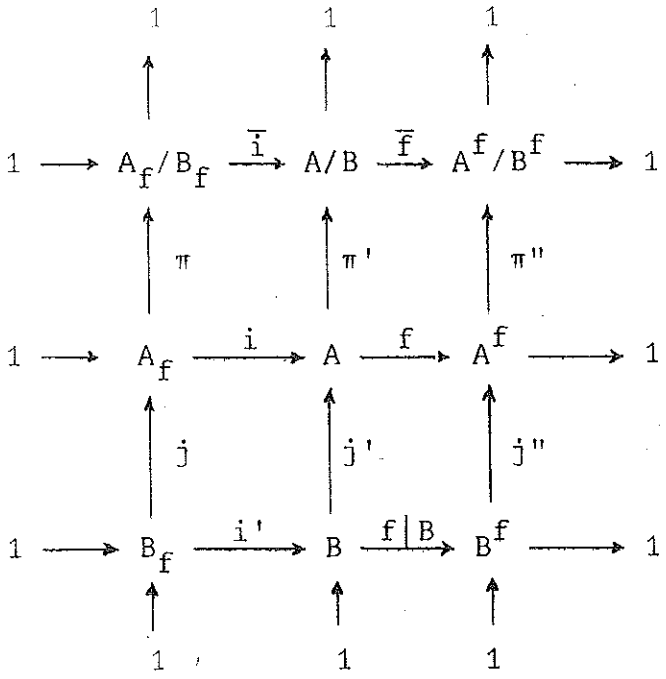
$$\bar{i}(a.B_f) = a.B \qquad (a \in A_f)$$

$$\bar{f}(c.B) = f(c).B^f \qquad (c \in A)$$

homomorfismen, en de volgende rij is exakt :

$$1 \to A_f/B_f \xrightarrow{\bar{i}} A/B \xrightarrow{\bar{f}} A^f/B^f \to 1.$$

BEWIJS. Dat $\bar{i}$ en $\bar{f}$ homomorfismen zijn is triviaal. Beschouw dan het volgende diagram :



Hierin zijn π, π', π" de natuurlijke homomorfismen, en i, i', j, j', j" de natuurlijke injekties. Het is niet moeilijk om na te gaan dat dit diagram kommutatief is (wegens de definitie van $\bar{i}$ en $\bar{f}$). Bovendien zijn de drie kolommen en de onderste twee rijen exakt. Men kan hier dus gebruik maken van het 3 × 3-lemma (cfr. bijvoorbeeld [7],) om tot het gewenste resultaat te komen.

Gevolg. Zijn twee van de drie indices $(A_f : B_f)$, $(A : B)$ en $(A^f : B^f)$ eindig, dan is de derde het eveneens, en er geldt :

$$(A : B) = (A^f : B^f)(A_f : B_f).$$

Dit volgt onmiddellijk uit het isomorfisme :

$$(A/B)/(A_f/b_f) \cong A^f/B^f,$$

dat door de exakte rij in de stelling geleverd wordt.

Cyclische uitbreidingen.

Zij L/K een cyclische uitbreiding met Galoisgroep G. Zij σ een generator van G, en stel : $n = [L : K]$. De aktie van G zal exponentieel genoteerd worden.

De norm van L tot K zullen we met N aanduiden. Het is dus de afbeelding bepaald door :

$$N : \alpha \to \alpha^{1+\sigma+\sigma^2+\ldots+\sigma^{n-1}} = N(\alpha).$$

We definiëren de afbeelding $\lambda : L^* \to L^*$ als volgt :

$$\lambda : \alpha \to \alpha^{\lambda} = \alpha^{1-\sigma} = \alpha(\sigma(\alpha))^{-1}.$$

Het is duidelijk dat λ en N homomorfismen zijn van L^* waarvoor geldt :

$$\lambda(N(\alpha)) = N(\lambda(\alpha)) = 1 \qquad \text{voor alle } \alpha \in L^*.$$

Bovendien geldt de volgende stelling, bekend onder de benaming "Hilbert's stelling 90" (cfr. [15], Satz 90).

STELLING III.3.2.1. *De kern van* N *is het beeld van* λ. *Met andere woorden :* $L_N^* = L^{*\lambda}$.

Het is verder duidelijk dat, voor elke deelgroep H van L^* geldt :

$$L_N^* \cap H = L^{*\lambda} \cap H = H_N.$$

Is $H \neq L^*$, dan is H_N ook meestal verschillend van H^{λ}. Het zij eveneens opgemerkt dat L_{λ}^* (= kern van λ) gelijk is aan K^*. Aangezien L^{*N} meestal een echte deelgroep is van K^*, zien we dat L_{λ}^* niet met L^{*N} mag geidentificeerd worden.

Teneinde de RT-index van K^* in L^* te berekenen vestigen we nu de aandacht op quotientgroep $R_L(K^*)/K^*W_L$.

STELLING III.3.2.2. *Er bestaat een isomorfisme :*

$$R_L(K^*)/W_L K^* \cong (W_L)_N/(W_L)^\lambda \ .$$

BEWIJS. Neem in Lemma III.3.1. : $A = R_L(K^*)$; $f = \lambda$ en $B = K^*W_L$. Wat betreft A_f, B^f en B^f hebben we onmiddellijk :

$$\begin{cases} A_f = (R_L(K^*))_\lambda = K^* \ , \\ B_f = (W_L K^*)_\lambda = K^* \ , \\ B^f = (W_L K^*)^\lambda = W_L^\lambda \ . \end{cases}$$

Wat betreft $A^f = (R_L(K^*))^\lambda$, zij $\alpha \in R_L(K^*)$, en zij m een element van $\mathbb{N}_0$ waarvoor $\alpha^m = a \in K^*$. Men heeft dus : $(\alpha^m)^\lambda = 1 = (\alpha^\lambda)^m$, d.w.z. : $\alpha^\lambda \in W_L$. Omgekeerd, zij $\beta \in L^*$ zó dat $\beta^\lambda \in W_L$. Er bestaat dus een $m \in \mathbb{N}_0$ zó dat $(\beta^\lambda)^m = 1$. Bijgevolg geldt : $(\beta^m)^\lambda = 1$, wat betekent : $\beta^m \in$ kern van $\lambda = K^*$, m.a.w. $\beta \in R_L(K^*)$. Er geldt dus : $(R_L(K^*))^\lambda = (L^*)^\lambda \cap W_L$, en dit is wegens de voorgaande stelling niets anders dan $(W_L)_N$. Het resultaat van Lemma III.3.1. opschrijven levert dan het gewenste isomorfisme op.

We onderzoeken thans de struktuur van $(W_L)_N/(W_L)^\lambda$.

STELLING III.3.2.3. *De graad* n *van de cyclische uitbreiding* L/K *is een exponent voor* $(W_L)_N/(W_L)^\lambda$. *Met andere woorden :* $\zeta \in (W_L)_N$ *impliceert* $\zeta^n \in (W_L)^\lambda$.

BEWIJS. Zij $g(\sigma)$ het element

$$\sigma^{n-2} + 2\sigma^{n-3} + \ldots + (n-2)\sigma + (n-1)$$

uit de groepring $\mathbb{Z}[G]$. Men kan dan eenvoudig narekenen dat :

$$\sigma^{n-1} + \sigma^{n-2} + \ldots + \sigma + 1 = (\sigma - 1)g(\sigma) + n.$$

Zij ζ een element van $(W_L)_N$. Er geldt dus :

$$N(\zeta) = \zeta^{\sigma^{n-1}+\sigma^{n-2}+\ldots+\sigma+1} = \zeta^{(\sigma-1)g(\sigma)+n} = 1.$$

Hieruit volgt :

$$\zeta^n = (\zeta^{g(\sigma)})^{1-\sigma} \in (W_L)^\lambda,$$

wat het gestelde bewijst.

Gevolg. Is ζ een p^ν-de eenheidswortel (p een priemgetal, $\nu \in \mathbb{N}_0$), dan zal zijn orde modulo $(W_L)^\lambda$ (die is de orde van het beeld van ζ onder het natuurlijk homomorfisme $(W_L)_N \to (W_L)_N/(W_L)^\lambda$) een deler zijn van n. Uit

$$\zeta^{p^\nu} = 1 \text{ (en } 1 \in (W_L)^\lambda)$$

volgt echter dat deze orde een deler is van p^ν. Dit betekent dat, indien de kanonieke ontbinding van n in priemfaktoren gegeven is door :

$$n = p_1^{a_1} \ldots p_r^{a_r},$$

de orde van ζ gelijk zal zijn aan p^κ, waarbij $\kappa = 0$ indien $p \neq p_i$ voor $i = 1,2,\ldots,r$, en $\kappa \leq a_i$, indien $p = p_i$ voor een

$$i \in \{1,2,\ldots,r\}.$$

Ter verkorting stellen we : $(W_L)_N = A$ en $(W_L)^\lambda = B$. Deze twee groepen zijn torsiegroepen.

We herinneren eraan dat de p-komponent (p een priemgetal) van

een abelse groep G de deelgroep van G is, bestaande uit alle elementen x van G waarvan de orde een macht van p is. De p-component van G noteren we verder met G_p. Van een torsiegroep is verder bekend dat hij direkte som is van zijn p-komponenten (cfr. FUCHS, [7]).

Voor de groepen A en B kunnen we dus schrijven :

$$A = \bigoplus_p A_p$$

$$B = \bigoplus_p B_p,$$

waaruit, wegens het feit dat $B_p \subset A_p$ en $B_p = B \cap A_p$:

$$A/B \cong \bigoplus_p (A_p/B_p).$$

Het gevolg van de voorgaande stelling leert ons dat voor $p \nmid n$ geldt :

$$A_p = B_p.$$

Er rest ons dus :

$$A/B \cong \bigoplus_{p|n} A_p/B_p.$$

Twee mogelijkheden kunnen zich voordoen :

(1). A_p is oneindig. We beweren dat A_p alle p^ν-de eenheidswortels bevat ($\nu \in \mathbb{N}_0$). Was dit niet het geval, dan bestond er een kleinste natuurlijk getal τ, verschillend van nul, zó dat een primitieve p^τ-de eenheidswortel ζ niet tot A_p behoorde. Is $\mu \in \mathbb{N}_0$, $\mu \geqslant \tau$, en is ζ' een primitieve p^μ-de eenheidswortel, dan bestaat er steeds een natuurlijk getal q zó dat $\zeta'^q = \zeta$. Uit het feit dat $N(\zeta) \neq 1$ volgt dan : $N(\zeta') \neq 1$, i.e. : $\zeta' \notin A_p$. Dit is duidelijk in strijd met het oneindig zijn van A_p.
Wat betreft B_p kunnen we een soortgelijk argument naar voor

brengen, d.w.z. : indien een primitieve p^τ-de eenheidswortel niet tot B_p behoort, dan zal geen enkele primitieve p^μ-de eenheidswortel tot B_p behoren zodra $\mu \geqslant \tau$. Uit het gevolg van de voorgaande stelling weten we echter dat er een $r \in \mathbb{N}$ bestaat zodanig dat voor alle ζ van A_p geldt : $\zeta p^r \in B_p$. Aangezien A_p alle p^ν-de eenheidswortels bevat volgt hier onmiddellijk uit dat $B_p = A_p$.

(2). A_p is een eindige groep. Aangezien elke eindige deelgroep van de multiplikatieve groep van een veld cyclisch is, en elk quotiënt van een cyclische groep door een deelgroep eveneens cyclisch is, vindt men :

A_p/B_p is cyclisch.

De orde van deze groep kan nu (met behulp van het gevolg van de voorgaande stelling) gevonden worden als zijnde van de gedaante p^κ, met $p^\kappa | n$.

Dit geeft uiteindelijk :

$$A/B \cong \bigoplus_{\substack{p|n \\ \#A_p \text{ eindig}}} (A_p/B_p),$$

waaruit volgt :

$$(A : B) = \prod_{\substack{p|n \\ \#A_p \text{ eindig}}} (A_p : B_p) = p_1^{b_1} \ldots p_r^{b_r}, \quad 0 \leqslant b_i \leqslant a_i$$

(a_i komende uit $n = p_1^{a_1} \ldots p_r^{a_r}$).

Verder zien we nog dat A/B direkte som is van cyclische groepen waarvan de ordes twee aan twee onderling ondeelbaar zijn. Het is welbekend dat dergelijke direkte sommen steeds cyclisch zijn. Met

behulp van stelling III.3.2.2. kunnen we onze resultaten als volgt samenvatten :

STELLING III.3.2.4. *De quotiëntgroep* $R_L(K^*)/W_L K^*$ *is een cyclische groep waarvan de orde een deler is van* $[L : K]$.

De RT-index van de multiplikatieve groep van een veld K in de multiplikatieve groep van een eindige cyclische uitbreiding van K is dus een deler van de uitbreidingsgraad.

3. Voorbeelden.

Hier tonen we aan dat de bekomen resultaten niet verscherpt kunnen worden. We doen dit door voorbeelden van kwadratische uitbreidingen met $q_L(K^*) = 1$ en andere met $q_L(K^*) = 2$ aan te geven.

Voorbeeld 1. Zij $K = \mathbb{R}$ en $L = \mathbb{C}$. Hier is $W_{\mathbb{C}}$ een oneindige groep. Het is duidelijk dat elke eenheidswortel norm 1 heeft, i.e. : $(W_{\mathbb{C}})_N = W_{\mathbb{C}}$. Derhalve is de groep A_p van daarnet een oneindige groep voor alle priemgetallen p. Hier geldt dus :

$$q_{\mathbb{C}}(\mathbb{R}^*) = 1$$

Deze situatie is niet uitsluitend te wijten aan de oneindigheid van de groep W_L : daarvan is volgend voorbeeld een illustratie.

Voorbeeld 2. Stel $K = \mathbb{Q}(\sqrt{-2})$; $L = \mathbb{Q}(\sqrt{-2},\sqrt{2},\sqrt{-1}) = K(\sqrt{2})$. Hier is (cfr. Stelling II.3.3.1.) :

$$W_L = \{\pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}\}.$$

Verder vindt men :

$$N(1) = N(-1) = N(i) = N(-i) = 1,$$

terwijl voor $\varepsilon,\delta \in \{+1,-1\}$:

$$N(\varepsilon \frac{\sqrt{2}}{2} + \delta \frac{\sqrt{-2}}{2}) = -1.$$

Dus : $(W_L)_N = \{\pm 1,\pm i\}$.

Verder geldt :

$$1^\lambda = (-1)^\lambda = 1; \quad i^\lambda = (-i)^\lambda = -1;$$

$$(\varepsilon \frac{\sqrt{2}}{2} + \delta \frac{\sqrt{-2}}{2})^\lambda = -2\varepsilon\delta\frac{i}{2},$$

waaruit volgt : $(W_L)^\lambda = \{\pm 1,\pm i\} = (W_L)_N$.

Derhalve verkrijgen we hier :

$$q_L(K^*) = \pm 1.$$

Dat ook $q_L(K^*) = 2$ kan optreden blijkt uit volgend voorbeeld :

Voorbeeld 3. Stel $K = \mathbb{Q}(\sqrt{2})$; $L = K(\sqrt{-2})$.

Hier kan men onmiddellijk narekenen dat :

$$W_L = (W_L)_N.$$

Daarenboven geldt :

$$W_L^\lambda = \{\pm 1,\pm i\}.$$

Hier is dus :

$$q_L(K^*) = 2$$

Voorbeeld 4. Zij L/K een cyclische uitbreiding waarbij $W_L = W_K$. Aangezien N, beperkt tot K, het effekt heeft van n^{de}-machtsverheffing is het duidelijk dat $(W_L)_N$ niets anders is dan de groep $W_{K,n}$ der n^{de} eenheidswortels van K. Anderzijds is $(W_L)^\lambda = \{1\}$, zodat :

$$q_L(K^*) = (W_{K,n} : 1).$$

Indien K alle n^{de} eenheidswortels bezit dan zal $q_L(K)$ precies gelijk zijn aan n, en omgekeerd. In dit geval volgt uit het cyclisch zijn van de groep $R_L(K^*)/W_L K^* = R_L(K^*)/K^*$ (stelling III.3.2.4.) dat de uitbreiding L/K van de gedaante $K(\sqrt[n]{a})$, $(a \in K^*)$ zal zijn. (Dit is een resultaat dat eveneens uit de Kummer-theorie volgt : cfr. [4] of [18]).

§4. DE RT-INDEX BIJ EINDIGE SEPARABELE UITBREIDINGEN

4.1. Uitbreidingen van de vorm $K(\sqrt[n]{a})/K$; $a \in K$.

Zij K een willekeurig veld. Van nu af aan zullen we zijn karakteristiek met ch(K) aanduiden.

STELLING III.4.1.1. *Zij* $n \geq 2$ *een geheel getal. Zij* $a \in K^*$. *Veronderstel dat* $a \notin K^{*p}$ *indien* p *een priemdeler is van* n, *en dat* $a \notin -4K^{*4}$ *in geval* $4|n$. *Dan is de polynoom* $X^n - a$ *irreduciebel in* K[X].

BEWIJS. Zie [18], ch. VIII, §9, th. 16.

Dus, is a een element van K dat aan de eisen van de stelling voldoet, dan geldt :

$$[K(\sqrt[n]{a}) : K] = n,$$

(1). K bezit alle p^{de} eenheidswortels. De vorige stelling leert ons dat L/K cyclisch is, en dat Gal(L/K) = G orde p heeft. Zij σ een generator voor G. In de notaties van voorgaande stelling nemen we : $r_\sigma = s$. Er geldt dus :

$$\sigma(\sqrt[p]{a}) = \zeta^s \sqrt[p]{a} \; ; \quad s \not\equiv 0 \pmod{p}.$$

Er geldt eveneens :

$$\sigma(\sqrt[p]{b}) = \zeta^t \sqrt[p]{b},$$

en het is duidelijk dat $t \not\equiv 0 \pmod{p}$.

Anderzijds kan $\sqrt[p]{a}$ ook als volgt geschreven worden :

$$\sqrt[p]{a} = \sum_{i=0}^{p-1} k_i (\sqrt[p]{b})^i \qquad (k_i \in K),$$

zodat, na inwerking van σ op beide leden :

$$\zeta^s \sqrt[p]{a} = \sum_{i=0}^{p-1} k_i \zeta^{ti} (\sqrt[p]{b})^i = \sum_{i=0}^{p-1} k_i \zeta^s (\sqrt[p]{b})^i.$$

Hieruit volgt :

$$k_i \zeta^{ti} = k_i \zeta^s \qquad \text{voor alle } i = 0,1,2,\ldots,p-1.$$

Aangezien er slechts één i uit 0,1,2,...,p-1 kan gevonden worden waarvoor $\zeta^{ti} = \zeta^s$, zegge r, vindt men :

$$k_i = 0 \quad \text{voor alle } i \in \{0,1,2,\ldots,p-1\} \setminus \{r\}.$$

Dit geeft : $\sqrt[p]{a} = k_r (\sqrt[p]{b})^r$, waaruit na p^{de} machtsverheffing het gestelde volgt.

(2). K bezit geen p^{de} eenheidswortels. Het is duidelijk dat $p \neq 2$. Zij ζ een primitieve p^{de} eenheidswortel. Het is welbekend dat :

$$[F : K] \leq p-1,$$

waaruit volgt dat de uitbreidingsgraad van F/L onderling ondeelbaar is met die van L/K. Dit impliceert dat F en L lineair disjunkt zijn over K, zodat geldt :

$$[FL : F] = p.$$

Nu is FL echter niet anders dan het veld $F(\sqrt[p]{a})$. Uit (1) volgt dus : $a = b^r.\gamma^p$, waarbij $\gamma \in F$ en $r \in \mathbb{N}$, $1 \leq r < p$. Stel : $a.b^{-r} \notin K^{*p}$. Wegens Stelling III.4.1.1. heeft men dan :

$$[K(\sqrt[p]{ab^{-r}}) : K] = [K(\gamma) : K] = p.$$

Dit is echter duidelijk in tegenspraak met $[F : K] \leq p-1$ en het feit dat $K(\gamma) \subset F$. Bijgevolg zal ab^{-r} een element zijn van K^{*p}, waaruit het gestelde volgt.

Opmerking. Indien p geen priemgetal is, dan is de stelling niet langer geldig. Men heeft immers :

$$\mathbb{Q}(\sqrt[4]{-4}) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\sqrt[4]{1}),$$

(dit volgt uit : $\sqrt[4]{-4} = \sqrt[4]{(2i)^2} = \pm\sqrt{2i} = \pm\sqrt{(1+i)^2} = \pm(1+i)$) alhoewel $-4 \neq 1.m^4$ voor alle $m \in \mathbb{Q}$.

4.2. Uitbreidingen van de vorm $K(\sqrt[p^{n_1}]{a_1},\ldots,\sqrt[p^{n_d}]{a_d})/K$.

We behandelen hier een eenvoudige voldoende voorwaarde opdat een uitbreiding van de gedaante vermeld in de titel (met p een priemgetal en $a_1,\ldots,a_d \in K^*$) van graad $p^{n_1+\ldots+n_d}$ over K zou zijn.

DEFINITIE. Zij p een priemgetal. We noemen elementen $a_1,\ldots,a_d$ ($\neq 0$) van een veld K p-fundamenteel onafhankelijk in K en we schrijven :

"$a_1,\ldots,a_d$ zijn p-FO in K",

indien

$$a_1^{c_1}\ldots a_d^{c_d} \in K^{*p} \cup(-K^{*p}) \quad (c_1,\ldots,c_d \in \mathbb{Z})$$

impliceert :

$$c_1 \equiv c_2 \equiv\ldots\equiv c_d \equiv 0 \pmod{p}.$$

Het zij opgemerkt dat voor oneven p de gelijkheid $K^{*p} = -K^{*p}$ geldt, zodat enkel voor $p = 2$ er eventueel een verschil tussen K^{*2} en $(-K^{*2})$ kan optreden.

LEMMA III.4.2. Zijn $a_1,\ldots,a_d$ p-FO in K, en is $p \neq ch(K)$, dan zijn $\sqrt[p]{a_1},a_2,\ldots,a_d$ p-FO in $K(\sqrt[p]{a_1})$.

BEWIJS. Stel $L = K(\sqrt[p]{a_1})$. Het is duidelijk dat men heeft :

$$a_1,\ldots,a_d \text{ zijn p-FO in } K \Rightarrow a_1 \notin K^{*p}.$$

Wegens stelling III.4.1.1. geldt dus : $[L : K] = p$. Veronderstel dat er getallen $c_1,\ldots,c_d \in \mathbb{Z}$ bestaan zó dat :

$$(1) \qquad (\sqrt[p]{a_1})^{c_1}a_2^{c_2}\ldots a_d^{c_d} = \varepsilon.\alpha^p,$$

waarbij $\varepsilon \in \{+1,-1\}$ en $\alpha \in L$.
De p^{de} macht van (1) geeft :

$$a_1^{c_1}a_2^{pc_2}\ldots a_d^{pc_d} = \varepsilon^p.\alpha^{p^2}.$$

Stel : $a = \varepsilon^{-p}a_1^{c_1}a_2^{pc_2}\ldots a_d^{pc_d}$, en $m = p^2$.
Er geldt dus : $\alpha^m = a$, m.a.w. : α is wortel van de polynoom $X^m - a$.
Is c_1 niet deelbaar door p, dan zal (wegens het p-FO zijn van de elementen $a_1,\ldots,a_d$) a geen element zijn van K^{*p}, en indien $p = 2$,

dan zal (om dezelfde reden) a geen element zijn van $-4K^{*4}$ aangezien het geen element kan zijn van $-K^{*2} \supset -4K^{*4}$. Volgens stelling III.4.1.1. is de polynoom $X^m - a$ irreducibel. Maar dan is $[K(\alpha) : K] = m = p^2$, wat in strijd is met het feit dat $K(\alpha) \subset L$ en $[L : K] = p$. Derhalve geldt : $c_1 \equiv 0 \pmod p$, zegge : $c_1 \equiv pk_1$. De vergelijking (1) wordt dus :

$$a_1^{k_1} a_2^{c_2} \ldots a_d^{c_d} = \varepsilon.\alpha^p.$$

We stellen thans : $b = \varepsilon^{-1} a_1^{k_1} a_2^{c_2} \ldots a_d^{c_d}$, en weerom zien we dat α een wortel is van de polynoom $X^p - b$. Is een van de getallen $c_2,\ldots,c_d$ niet deelbaar door p, dan volgt weer uit het p-FO zijn van $a_1,\ldots,a_d$ dat $b \notin K^{*p}$ en dat $X^p - b$ irreduciebel is. Dit betekent echter :

$$K(\sqrt[p]{b}) = K(\sqrt[p]{a_1}).$$

Uit stelling III.4.1.3. volgt dan :

$$b_1 = a_1^r.c^p,$$

waarbij $c \in K^*$ en $r \in \mathbb{N}$, $1 \leqslant r < p$. Dit geeft :

$$\varepsilon^{-1} a_1^{k_1 - r}.a_2^{c_2} \ldots a_d^{c_d} = c^p \in K^{*p},$$

wat wegens het p-FO zijn van $a_1,\ldots,a_d$ onmogelijk is indien een van de getallen $c_2,\ldots,c_d$ niet deelbaar is door p.
Uit (1) volgt dus : $c_1 \equiv c_2 \equiv \ldots \equiv c_d \equiv 0 \pmod p$, wat neerkomt op het p-FO zijn van $\sqrt[p]{a_1}, a_2, \ldots, a_d$ in $K(\sqrt[p]{a_1})$, Q.E.D.

Opmerking. Is $p = ch(K)$, dan is de stelling niet langer geldig. Immers, zij $K = k_0(t)$ met k_0 zoals in III.2.2., voorbeeld 2. In dit veld zijn de elementen t en $t + 1$ 2-FO. Inderdaad, stel dan

$$t^{c_1}.(t+1)^{c_2} = \phi(t)^2,$$

met $\phi(t) \in k_0(t)$ en $c_1, c_2 \in \mathbb{Z}$. Door van beide leden de formele afgeleide te nemen bekomt men :

$$t^{c_1-1}.(t+1)^{c_2-1}(c_1 + (c_1 + c_2)t) = 0,$$

waaruit : $c_1 \equiv c_2 \equiv 0 \pmod 2$. De elementen t en $t+1$ zijn dus 2-FO in K; dit is niet het geval voor de elementen $\sqrt{t}$ en $t+1$ in $K(\sqrt{t})$, aangezien :

$$(\sqrt{t})^0(1+t)^1 = (1+\sqrt{t})^2.$$

STELLING III.4.2. *Zijn de elementen* $a_1,\ldots,a_d$ p-FO *in het veld* K, *en is* $p \neq ch(K)$, *dán geldt voor elk stel getallen* $n_1,\ldots,n_d$:

$$[K(\sqrt[p^{n_1}]{a_1},\ldots,\sqrt[p^{n_d}]{a_d}) : K] = p^{n_1+\ldots+n_d}$$

BEWIJS. Aangezien a_1 geen element is van K^{*p} en ook geen element is van $-4K^{*4}$ indien $p = 2$ en $n_1 \geqslant 2$, geldt (wegens stelling III.4.1.1.) :

$$[K(\sqrt[p^{n_1}]{a_1}) : K] = p^{n_1}.$$

Door successieve toepassing van voorgaand lemma zien we dat de elementen $a_2,\ldots,a_d$, p-FO zijnde in K, eveneens p-FO zijn in het veld $K(\sqrt[q]{a_1})(q = p^{n_1})$. Men kan dan opnieuw stelling III.4.1.1. toepassen voor a_2, wat geeft :

$$[K(\sqrt[p^{n_1}]{a_1},\sqrt[p^{n_2}]{a_2}) : K(\sqrt[p^{n_1}]{a_1})] = p^{n_2}.$$

Zo doorgaande komt men dan tot het gestelde.

Opmerking. De eisen van de stelling zijn tamelijk streng. Het is mogelijk dat er twee elementen bestaan die niet p-FO zijn in K,

maar waarvoor de stelling toch geldig is. Bijvoorbeeld, de elementen 2 en -1 zijn niet 2-FO in $\mathbb{Q}$ aangezien $2^{\circ}.(-1)^{1} = -1 \in -K^{*2}$. Nochthans is de uitbreiding $\mathbb{Q}(\sqrt{-1},\sqrt{2})$ van graad 4 over $\mathbb{Q}$. Een nodige en voldoende voorwaarde opdat een uitbreiding van de gedaante $K(\sqrt[n_1]{a_1},\ldots,\sqrt[n_d]{a_d})/K$ van graad $n_1 \ldots n_d$ zou zijn over K werd onlangs door A. Schinzel bepaald (cfr. [24]).

4.3. De RT-index bij uitbreidingen met konstante torsie.

DEFINITIE. Een uitbreiding L/K wordt een uitbreiding met konstante torsie genoemd indien $W_L = W_K$.

Zij K een willekeurig veld, L een uitbreiding van K. De quotiëntgroep $R_L(K^*)/K^*$ is steeds een torsiegroep daar hij het torsiedeel is van L^*/K^* (cfr. III.1.1.). Zoals we reeds eerder opmerkten is $R_L(K^*)/K^*$ dus direkte som van zijn p-komponenten (p een priemgetal) die we verderop met G_p zullen aanduiden. Het is duidelijk dat G_p steeds een eindige deelgroep bevat (het volstaat een element te kiezen in G_p en de groep voortgebracht door het element te bekijken). Voor een dergelijk deelgroep H_p van G_p schrijven we zijn kanonieke ontbinding in cyclische deelgroepen van orde p^{n_i} ($n_i \in \mathbb{N}_0$), nl. :

$$H_p = \bigoplus_{i=1}^{d} A_i \; ; \quad A_i \text{ cyclisch van orde } p^{n_i}.$$

Voor $i = 1,2,\ldots,d$, zij ξ_i een element van $R_L(K^*)$ wiens beeld onder het natuurlijk homomorfisme $R_L(K^*) \to R_L(K^*)/K^*$ een generator is voor A_i. Er zal dus gelden (voor getallen $v_i \in \mathbb{Z}$) :

$$(1) \qquad \xi_1^{v_1} \ldots \xi_d^{v_d} \in K^* \Leftrightarrow v_i \equiv 0 \pmod{p^{n_i}} \text{ voor alle } i = 1,2,\ldots,d$$

We stellen thans voor $i = 1,2,\ldots,d$:

$$(2) \qquad a_i = \xi^{p^{n_i}}.$$

Het is duidelijk dat $a_i \in K^*$.

STELLING III.4.3.1. *Is* L/K *een uitbreiding met konstante torsie, dan zijn de door (2) gedefinieerde elementen* $a_1,\ldots,a_d$ *p-FO in* K.

BEWIJS. Veronderstel dat de volgende relatie geldt :

$$a_1^{c_1}\ldots a_d^{c_d} = \varepsilon\, b^p,$$

waarbij $\varepsilon \in \{+1,-1\}$, $c_1,\ldots,c_d \in \mathbb{Z}$, en $b \in K^*$. Gebruiken we (2) hierin, dan wordt dat :

$$\xi_1^{c_1 p^{n_1}}\ldots\xi_d^{c_d p^{n_d}} = \varepsilon.b^p.$$

Hieruit volgt onmiddellijk dat het element

$$b^{-1}\xi_1^{c_1 p^{n_1-1}}\ldots\xi_d^{c_d p^{n_d-1}} = \phi$$

een (2p)-de eenheidswortel is van L. Wegens $W_L = W_K$ vindt men dat ϕ, en dus ook $b\phi$, tot K^* behoort. Uit (1) volgt dan onmiddellijk :

$$p^{n_i} | c_i p^{n_i-1} \quad \text{voor alle } i = 1,2,\ldots,d.$$

Dit betekent : $c_i \equiv 0 \pmod p$ voor alle $i = 1,2,\ldots,d$, wat precies de voorwaarde voor het p-FO zijn van $a_1,\ldots,a_d$ is.

Een uitbreiding met konstante torsie bevat dus steeds de tussenuitbreiding $K(\sqrt[p^{n_1}]{a_1},\ldots,\sqrt[p^{n_d}]{a_d})$, ongeacht de waarde van [L : K] of het feit of p al of niet gelijk is aan ch(K). We kunnen echter door bijkomende voorwaarden op te leggen aan p en aan L/K sterkere resultaten bekomen. Is bijvoorbeeld $p \neq ch(K)$, dan kan stelling III.4.2. toegepast worden, wat betekent dat L/K een tussenuitbreiding van graad $p^{n_1+\ldots+n_d}$ zal bevatten. Is bovendien [L : K]

eindig, dan moet $p^{n_1+\ldots+n_d}$ een deler zijn van [L : K]. Men weet echter dat $p^{n_1+\ldots+n_d}$ de orde is van een eindige deelgroep van de p-komponenten van $R_L(K^*)/K^*$, zodat men aanstonds kan opmerken dat G_p geen oneindige orde kan hebben. Integendeel, de orde van G_p is een deler van [L : K]. We resumeren dit als volgt :

STELLING III.4.3.2. *Zij* L/K *een eindige uitbreiding met konstante torsie. Is* p *een priemgetal,* $p \neq ch(K)$, *dan is de* p*-komponent van* $R_L(K^*)/K^*$ *een eindige groep waarvan de orde een deler is van* [L : K].

Onder de hypothesen van deze stelling kunnen we dus aan elke p-komponent G_p van $R_L(K^*)/K^*$ een tussenuitbreiding van graad $p^\nu = \sharp G_p$ over K associëren ($p \neq ch\ K$). Voor verschillende p zijn die tussenuitbreidingen lineair disjunkt over K, zodat K een tussenuitbreiding van graad $\prod_{p\neq ch(K)} p^\nu$ zal bevatten. We zien dus dat de deelgroep $\prod_{p\neq ch(K)} G_p$ van $R_L(K^*)/K^*$ een eindige groep is waarvan de orde een deler is van K.

Indien $p = ch(K)$, en indien $G_p \neq \{1\}$, dan kan men zoals hoger steeds een tussenuitbreiding van de vorm $K(\sqrt[p]{a})$ vinden. Deze uitbreiding is echter zuiver inseparabel over K. Bijgevolg zal $G_p = \{1\}$, zodra L/K separabel is. We resumeren als volgt :

STELLING III.4.3.3. *Is* L/K *een separabele uitbreiding met konstante torsie, dan is de* R*-index van* K^* *in* L^* *een deler van de uitbreidingsgraad.*

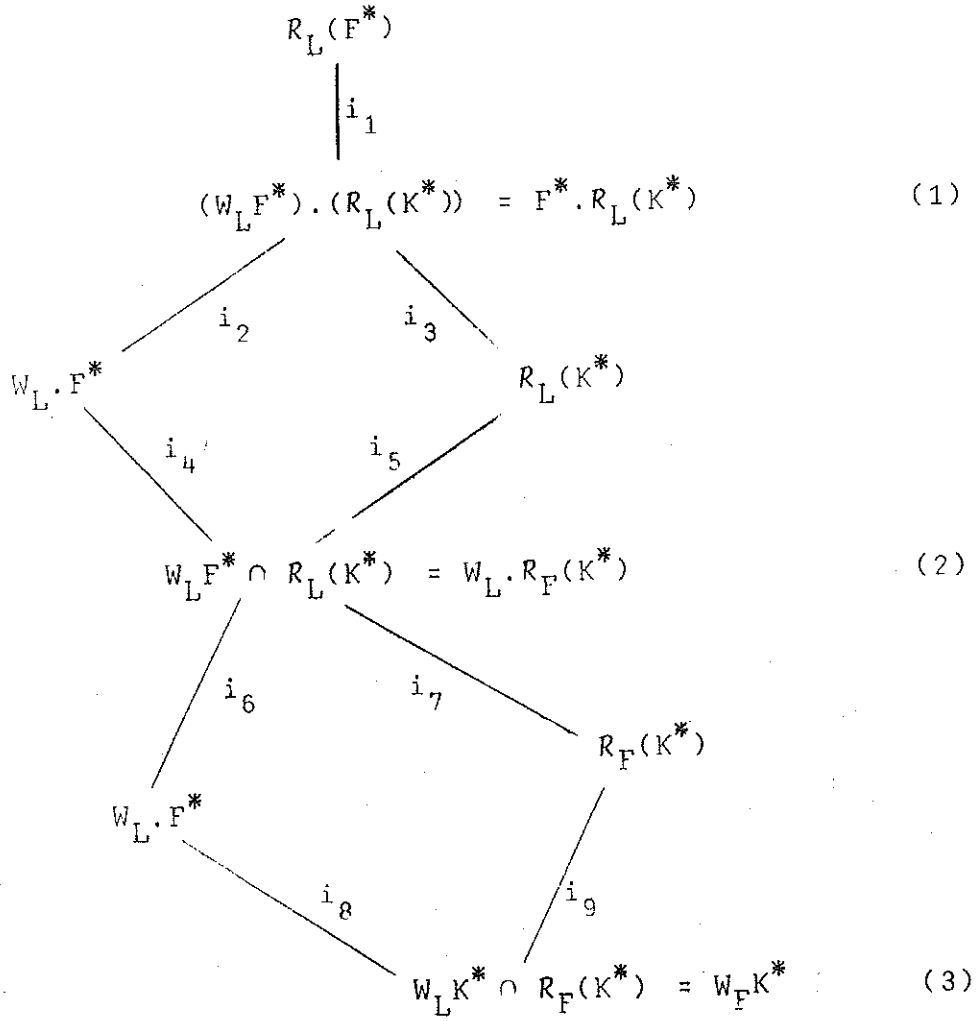
4.4. De RT-index by ketens.

STELLING III.4.4. *Zij* $K \subset F \subset L$ *een keten van (willekeurige) uitbreidingen. Zijn de indices* $q_F(K^*)$ *en* $q_L(F^*)$ *eindig, dan is de*

index $q_L(K^*)$ *het eveneens en er geldt :*

$$q_L(K^*) \mid q_F(K^*).q_L(F^*).$$

BEWIJS. Beschouw het volgende diagram van inklusies :



(Hierin stelt i_m (m = 1,2,...,9) de index voor van de groep onderaan het streepje in de groep bovenaan het streepje). We bewijzen eerst de drie voorkomende gelijkheden in dit diagram.

(1). $W_LF^*).(R_L(K^*)) = F^*R_L(K^*)$.

Dit is triviaal, aangezien $W_L \subset R_L(K^*)$.

(2). $W_LF^* \cap R_L(K^*) = W_L.R_F(K^*)$

Stel $\alpha \in W_L.R_F(K^*)$. Er bestaat dus een element $\zeta \in W_L$ en een

element $\xi \in R_F(K^*)$ zo dat $\alpha = \zeta.\xi$. Er bestaat dus steeds een natuurlijk getal $m(\neq 0)$ waarvoor $\alpha^m \in K^*$, i.e. : $\alpha \in R_L(K^*)$. Het is triviaal om aan te tonen dat $\alpha \in W_L F^*$, aangezien $R_F(K^*) \subset F^*$. Dus geldt : $W_L.R_F(K^*) \subset W_L F^* \cap R_L(K^*)$. Teneinde de omgekeerde inklusie te bewijzen, zij

$$\beta \in W_L F^* \cap R_L(K^*).$$

Uit $\beta \in W_L F^*$ volgt : $\beta = \eta.\tau$, met $\eta \in W_L$ en $\tau \in F^*$. Aangezien β ook behoort tot $R_L(K^*)$ heeft men : $\beta^m = \eta^m \tau^m \in K^*$ voor een gepast natuurlijk getal $m(\neq 0)$. Is $m' \in \mathbb{N}_0$ dan zó dat $\eta^{m'} = 1$, dan zien we dat $\tau^{mm'} \in K^*$, zodat $\beta \in W_L.R_F(K^*)$, Q.E.D.

(3). $K^* W_L \cap R_F(K^*) = W_F.K^*$.

Zij $\alpha \in K^* W_L \cap R_F(K^*)$. Dit betekent : $\alpha = \zeta.\kappa$ met $\zeta \in W_L$ en $\kappa \in K^*$. Uit $\zeta.\kappa \in R_F(K^*)$ volgt echter : $\zeta.\kappa \in F^*$, en dus : $\zeta \in F^*$ of beter : $\zeta \in W_F$. Dus : $\alpha \in W_F.K^*$. Omgekeerd, uit $\beta \in W_F K^*$ volgt : $\beta \in W_L K^*$ (want $W_F \subset W_L$). Aangezien $W_F K^*$ deel is van $R_F(K^*)$ volgt ook : $\beta \in R_F(K^*)$. Dit levert het gestelde.

Kijken we dan naar de definities van de getallen i_m, $q_F(K^*)$, $q_L(F^*)$ en $q_L(K^*)$, dan zien we :

$$i_1.i_2 = q_L(F^*)$$

$$i_5.i_6 = q_L(K^*)$$

$$i_9 = q_F(K^*)$$

Bij onderstelling zijn $i_1.i_2$ (en dus i_1 en i_2) en i_9 eindig. Wegens de klassieke isomorfiestellingen uit de groepentheorie heeft men verder :

$$i_2 = i_5 \quad \text{en} \quad i_6 = i_9.$$

De eindigheid van $q_L(K^*)$ is dus een feit, en bovendien vinden we :

$$q_L(K^*) = i_2.i_9 = \frac{q_L(F^*)}{i_1} \cdot q_F(K^*),$$

wat tot de gewenste konklusie leidt.

Gevolg. Is $F_0 \subset F_1 \subset \ldots \subset F_m$ een keten van uitbreidingen waarvoor geldt dat $q_{F_i}(F^*_{i-1})$ eindig is voor alle $i = 1,2,\ldots,m$, dan is $q_{F_m}(F^*_0)$ eveneens eindig en het is een deler van

$$q_{F_1}(F^*_0).q_{F_2}(F^*_1)\ldots q_{F_m}(F^*_{m-1}).$$

BEWIJS. Herhaalde toepassing van de stelling.

.5. De hoofdstelling over de RT-index.

STELLING III.4.5. *Is* L/K *een eindige separabele uitbreiding, dan is de RT-index van* K^* *in* L^* *een deler van de uitbreidingsgraad.*

BEWIJS. Men kan de uitbreiding L/K als volgt opbreken in een keten van uitbreidingen :

$$K \subset F \subset L, \text{ waarbij } F = K(W_L).$$

Men ziet aanstonds dat $W_F = W_L$, i.e. L/F is een separabele uitbreiding met konstante torsie. Stelling III.4.3.3. is dus toepasbaar, i.e. :

$$q_L(F^*) \mid [L : F].$$

Wat betreft F/K zij het opgemerkt dat F van de gedaante $K(\zeta)$ is, waarbij ζ een eenheidswortel is (ζ is niet noodzakelijk generator

voor W_L, aangezien W_L een oneindige groep mag zijn). Dergelijke uitbreidingen zijn echter oplosbaar, d.w.z. : F/K kan opgebroken worden in een keten

$$K = F_0 \subset F_1 \subset \ldots \subset F_m = F$$

waarin elke tussenstap F_i/F_{i-1} cyclisch is. Voor elk van die tussenstappen geldt stelling III.3.2.4., i.e. : $q_{F_i}(F^*_{i-1}) | [F_i : F_{i-1}]$. Wegens het gevolg van stelling III.4.4. geldt :

$$q_F(K^*) \Big| \prod_{i=1}^{m} q_{F_i}(F^*_{i-1}) \Big| \prod_{i=1}^{m} [F_i : F_{i-1}] = [F : K]$$

Opnieuw stelling III.4.4. toepassen levert dan uiteindelijk :

$$q_F(K^*) | q_L(F^*) . q_F(K^*) | [L : F].[F : K] = [L : K],$$

wat het gestelde is.

HOOFDSTUK IV

RADIKALEN IN GETALLENVELDEN

Doorheen dit hoofdstuk zal K een getallenveld zijn en L een eindige uitbreiding van K met $n = [L : K]$. Voor wat betreft de notaties verwijzen we naar hoofdstuk I.

Onze belangstelling zal hier voornamelijk uitgaan naar twee R-indices; die van de eenhedengroep U_K van K in L^* en die van de groep der idealen van K in de groep der idealen van L. We zullen beide indices dan in verband brengen met de R-index van $U_K K^*$ in L^*, die ons verdere informatie verstrekt in verband met de ideaalklassengroepen van K en van L.

§1. RADIKALEN IN S-EENHEDENGROEPEN

1.1 De RT-index van de S-eenhedengroep in L^*.

Zij S een eindige verzameling van onderling niet-equivalente valuaties van K. Veronderstel dat alle niet-equivalente archimedische valuaties van K tot S behoren. Zij $\tilde{S}$ de verzameling van alle (niet-equivalente) valuaties van L die de elementen van S uitbreiden.

Vooreerst wijzen we op een nuttige karakterizering van de groepen $U_K(S)$ en $U_L(\tilde{S})$. Namelijk, is η een element van K^*, zij dan

$$\eta.\mathcal{O}_K = \prod_p p^{m_p(\eta)}$$

de kanonieke faktorisatie van $\eta\mathcal{O}_K$. Uit de definitie van $U_K(S)$ (zie I.3.1.) volgt dan : $\eta \in U_K(S)$ dan en slechts dan als $m_p(\eta) = 0$ voor alle priemdelers p van K waarvan de geassocieerde valuatie v_p met geen enkele element van S equivalent is. De elementen ε van $U_L(\tilde{S})$ worden bijgevolg gekarakteriseerd door het feit dat in de kanonieke faktorisatie van $\varepsilon.\mathcal{O}_L$ slechts die priemdelers P zullen optreden die boven de priemdelers p van K liggen waarvoor v_p equivalent is met een element uit S.

Als eerste gevolg hiervan bewijzen we een eenvoudig lemma dat verderop nog dikwijls zal gebruikt worden.

LEMMA IV.1.1. Er geldt :

$$R_K(U_K(S)) = U_K(S).$$

BEWIJS. Het is duidelijk dat het volstaat de volgende implikatie aan te tonen :

$$\alpha \in K^* \ \& \ \alpha^m \in U_K(S) \text{ voor een } m \in \mathbb{N}_0 \Rightarrow \alpha \in U_K(S).$$

Door hetgeen voorafgaat weten we dat in de kanonieke faktorisatie van $(\alpha.\mathcal{O}_K)^m$ slechts priemdelers p zullen voorkomen waarvoor v_p equivalent is met een element in S. Hetzelfde geldt dus duidelijk voor $\alpha.\mathcal{O}_L$, aangezien de kanonieke faktorisatie uniek is. Dit is echter hetgeen te bewijzen was.

Een ander gevolg van de voorgaande karakterizering van $U_K(S)$ en $U_L(\tilde{S})$ is de volgende :

STELLING IV.1.1.1. *Er geldt :*

$$R_{U_L(\tilde{S})}(U_K(S)) = R_L(U_K(S)).$$

BEWIJS. De inklusie $U_L(\tilde{S}) \subset L^*$ geeft onmiddellijk :

$$R_{U_L(\tilde{S})}(U_K(S)) \subset R_{L^*}(U_K(S)) = R_L(U_K(S)).$$

Teneinde de omgekeerde inklusie te bekomen, neem $\varepsilon \in R_L(U_K(S))$, en laat $m \in \mathbb{N}_0$ zo zijn dat $\varepsilon^m \in U_K(S)$. Bekijkt men dan de kanonieke faktorisaties :

$$\varepsilon.\mathcal{O}_L = \prod_P P^{m_P(\varepsilon)}$$

en

$$\varepsilon^m \mathcal{O}_K = \prod_p p^{m_p(\varepsilon)} ,$$

dan is het duidelijk dat $m_p(\varepsilon) = 0$ impliceert : $m_P(\varepsilon) = 0$ voor alle priemdelers P van L boven p. Daaruit volgt meteen : $\varepsilon \in U_L(\tilde{S})$, Q.E.D.

We onderzoeken thans het verband tussen de RT-index van $U_K(S)$ in L^* en die van K^* in L^*. We hebben het volgende kommutatieve diagram van natuurlijke injekties :

$$\begin{array}{ccc} R_L(U_K(S)) & \longrightarrow & R_L(K^*) \\ \uparrow & & \uparrow \\ W_L.U_K(S) & \longrightarrow & W_L.K^* \end{array}$$

Dit geeft op een voor de hand liggende wijze aanleiding tot een homomorfisme :

$$\phi : R_L(U_K(S))/W_L.U_K(S) \longrightarrow R_L(K^*)/W_L.K^*$$

dat namelijk een element ε (van $R_L(U_K(S))$) modulo $W_L.U_K(S)$ stuurt naar ε modulo $W_L.K^*$. Dit homomorfisme is echter injektief. Hiertoe volstaat het aan te tonen dat

$$R_L(U_K(S)) \cap W_L.K^* = W_L.U_K(S)$$

Welnu, het is onmiddellijk duidelijk dat de groep aan de rechterkant van deze gelijkheid bevat is in de andere. Omgekeerd, zij ε een element van $R_L(U_K(S)) \cap W_L K^*$. Er geldt dus (wegens $\varepsilon \in W_L K^*$) : $\varepsilon = \zeta.a$, met $\zeta \in W_L$ en $a \in K^*$. Uit $\zeta a \in R_L(U_K(S))$ volgt anderzijds dat er een $m \in \mathbb{N}_0$ bestaat met de eigenschap : $a^m \in U_K(S)$. Wegens het lemma geldt daarom : $a \in U_K(S)$, en dus $\varepsilon \in W_L.U_K(S)$, Q.E.D.

De quotiëntgroep $R_L(U_K(S))/W_L.U_K(S)$ kan dus als een deelgroep van $R_L(K^*)/K^*$ aangezien worden. De orde van deze laatste groep is wegens stelling III.4.5. een deler van $n = [L : K]$. Dit geeft :

STELLING IV.1.1.2. *De RT-index van de groep der S-eenheden van K in L^* is een deler van de uitbreidingsgraad van L/K.*

Het zij hier opgemerkt dat de groep W_L van eindige orde is, zodat stelling III.1.2.1. kan toegepast worden, i.e. : de R-index van $U_K(S)$ in L^* is eveneens eindig en er geldt :

$$Q_L{}^*(U_K(S)) = (W_L : W_K).n', \text{ waarbij } n' | n.$$

Indien S precies de verzameling van alle niet-equivalent archimedische valuaties van K is, dan is $U_K(S) = U_K$, de groep der eenheden. Is bijvoorbeeld L een imaginair bikwadratisch veld, en K het reële kwadratische deelveld, dan ziet men wegens stelling II.3.3.2. en stelling III.1.2.3. dat $(U_L : W_L U_K)$ niets anders is dan de RT-index van U_K in L, en deze index kan dus wegens de voorgaande stelling slechts de waarde 1 of 2 aannemen.

Voor een andere toepassing verwijzen we naar volgend hoofdstuk,

Een andere karakterizering van $q_L(U_K(S))$.

We zullen hier gebruik maken van Dirichlet's stelling over de struktuur van $U_L(S)$, teneinde een praktische interpretatie van stelling IV.1.1.2. te bekomen.

DEFINITIE IV.1.2.1. Zij G een abelse groep en W_G zijn torsiedeelgroep. We noemen G regulier als de quotiëntgroep G/W_G een vrije groep is. Is de rang van G/W_G bovendien eindig, dan noemen we G eindig-regulier.

STELLING IV.1.2.1. *Een abelse groep is eindig-regulier dan en slechts dan als elke deelgroep* H *van* G *een eindige RT-index heeft in* G.

BEWIJS. (We schrijven G multiplikatief).
Zij G een eindig-reguliere groep. We kunnen G dus schrijven als direkt produkt :

$$G = W_G \times A$$

waarbij A een vrije abelse groep is, zegge met multiplikatieve $\mathbb{Z}$-basis $w_1,\ldots,w_n$. Elk element v van G kan dus geschreven worden als een produkt :

$$v = \zeta . w_1^{a_1} \ldots w_n^{a_n},$$

waarbij het element $\zeta \in W_G$ en de getallen $a_i \in \mathbb{Z}$ eenduidig bepaald zijn. Zij H een deelgroep van G. De quotiëntgroep H/W_H (met $W_H = W_G \cap H$) kan op natuurlijke wijze ingebed worden in de groep A, aangezien $H/W_H \cong HW_G/W_G$, en deze laatste een deelgroep is van G/W_G, die op zijn beurt isomorf is met A. Als deelgroep van een vrije abelse groep van eindige rang is H/W_H eveneens vrij en van rang

$r \leqslant n$. Hieruit volgt dat er r elementen, $v_1,\ldots,v_r$ van H bestaan zó dat elk element u van H eenduidig kan geschreven worden als :

$$u = \zeta' \, v_1^{b_1} \ldots v_r^{b_r} ,$$

waarbij $\zeta' \in W_H$ en $b_i \in \mathbb{Z}$. We kunnen de elementen v_i eveneens uitdrukken in funktie van de elementen w_j, i.e. :

$$v_i = \zeta_i \, w_1^{a_{i1}} \ldots w_n^{a_{in}} \qquad (i = 1,2,\ldots n).$$

Kiest men een andere multiplikatieve $\mathbb{Z}$-basis $w_1',\ldots,w_n'$ voor G/W_G en een andere (zegge $v_1',\ldots,v_r'$) voor H/W_H, dan zullen de relaties tussen de elementen v_i' en w_j' op analoge wijze een matrix (a_{ij}') definiëren die uit de matrix (a_{ij}) bekomen wordt door deze langs beide zijden te vermenigvuldigen met vierkante matrices waarvan de coëfficiënten in $\mathbb{Z}$ liggen en waarvan de determinant +1 of -1 is (dit zijn orthogonale matrices).

Zij D de grootste gemene deler van alle r × r-onderdeterminanten uit de matrix (a_{ij}). Het is bekend dat D ongewijzigd blijft zo men (a_{ij}) vermenigvuldigt (zowel links als rechts) met orthogonale matrices, en dat (a_{ij}) op die wijze kan herleid worden tot een matrix van de gedaante :

$$\begin{pmatrix} c_1 & 0\ldots 0 & 0\ldots 0 \\ 0 & c_2\ldots 0 & 0\ldots 0 \\ \ldots & \ldots \quad \ldots & \ldots \\ 0 & 0\ldots c_r & 0\ldots 0 \end{pmatrix}$$

waarbij $1 \leqslant c_1 \leqslant \ldots \leqslant c_r$ elementen zijn uit $\mathbb{N}$ waarvoor geldt :

$$c_i \mid c_{i+1} \quad \text{voor} \quad i = 1,2,\ldots,n-1.$$

We kunnen dus veronderstellen dat de elementen v_i en w_j zó gekozen

zijn dat ze voldoen aan de relaties :

$$v_1 = \zeta_1' w_1^{c_1}$$

(1)

$$v_r = \zeta_r' w_r^{c_r} .$$

Het is overduidelijk dat D hier niets anders is dan het produkt $c_1 \ldots c_r$. Nu zullen we bewijzen dat $D = q_G(H)$.
Zij B de deelgroep van G voortgebracht door W_G en door $w_1, \ldots, w_r$.
Uit (1) volgt onmiddellijk : $B \subset R_G(H)$. Omgekeerd, zij

$$\xi = \zeta'' w_1^{p_1} \ldots w_r^{p_r} w_{r+1}^{p_{r+1}} \ldots w_n^{p_n} \quad (p_1, \ldots, p_n \in \mathbb{Z};\ \zeta'' \in W_G)$$

een element van $R_G(H)$, en laat $n \in \mathbb{N}_0$ zodanig zijn dat $\xi^m \in H$.
Dit betekent :

$$(\zeta'')^m w_1^{mp_1} \ldots w_r^{mp_r} w_{r+1}^{mp_{r+1}} \ldots w_n^{mp_n} = \zeta''' v_1^{u_1} \ldots v_r^{u_r}$$

$$= \zeta'''' w_1^{u_1 c_1} \ldots w_r^{u_r c_r}$$

voor behoorlijke elementen $\zeta'''' \in W_G$ en $\zeta''' \in W_H$ en $u_1, \ldots, u_r \in \mathbb{Z}$.
Aangezien de elementen $w_1, \ldots, w_n$ multiplikatief onafhankelijk zijn volgt onmiddellijk :

$$p_{r+1} = \ldots = p_n = 0,$$

wat neerkomt op : $\xi \in B$. Dus geldt : $B = R_G(H)$. Men kan nu echter gemakkelijk representanten vinden in B voor de quotiëntgroep B/HW_G.
Hiertoe zullen de elementen :

$$w_1^{t_1} \ldots w_r^{t_r};\ 0 \leqslant t_i \leqslant e_i - 1 \text{ voor } 1 \leqslant i \leqslant r$$

gebruikt kunnen worden. Ze zijn immers wegens (1) twee aan twee incongruent modulo $W_G H$, en elk element uit B kan geschreven worden als het produkt van een dergelijk element met een element uit HW_G.
Aangezien er $c_1 \ldots c_r = D$ representanten zijn voor $B/W_G H = R_G(H)/W_G H$

verkrijgen we uiteindelijk :

$$q_G(H) = c_1 \ldots c_r = D, < \infty,$$

wat te bewijzen was.

Omgekeerd, laat G een abelse groep zijn waarin elke deelgroep een eindige RT-index heeft. Het is niet moeilijk in te zien dat dezelfde eigenschap geldig is voor de quotiëntgroep G/W_G, zodat we kunnen veronderstellen dat G torsievrij is.
Zij M een maximaal stel van $\mathbb{Z}$-onafhankelijke elementen v_i (waarvan de existentie verzekerd is door Zorn's lemma). Zij H de deelgroep van G voortgebracht door de elementen v_i. Uit de definitie van M volgt klaarblijkelijk dat H een vrije abelse groep is. Veronderstellen we even dat $\# M$ oneindig is. We kunnen dan gemakkelijk een deelgroep H' van H bepalen waarvoor $(H : H') = \# M$; men kan voor H' bijvoorbeeld de groep voortgebracht door de elementen v_i^2 nemen. Voor deze deelgroep H' geldt duidelijk : $H \subset R_G(H')$. Het is echter evident dat dit in tegenspraak is met het feit dat $(R_G(H') : H')$ eindig is voor elke deelgroep H' van G, en dus kunnen we veronderstellen dat $\# M = n < \infty$. Laten we thans $R_G(H)$ nader onderzoeken. Bij onderstelling is de quotiëntgroep $R_G(H)/H$ eindig, zodat uit het eindig-voortgebracht-zijn van H, het eindig-voortgebracht-zijn van $R_G(H)$ volgt. Bijgevolg is $R_G(H)$ zelf vrij, en zijn rang is $\geqslant n$ = rang van H. De maximaliteit van M verhindert echter de strikte ongelijkheid : $\text{rang}(R_G(H)) > \text{rang}(H)$. Daaruit volgt : $R_G(H) = G$, aangezien uit $w \in G$, $w \notin H$ volgt : $w^m \in H$ voor een $m \in \mathbb{N}_0$ (dit wordt door de maximaliteit van M verzekerd). Hiermee is het gestelde bewezen.

Keren we nu terug naar de groep $U_L(\tilde{S})$, dan zien we dat deze eindig-regulier is (dit is namelijk een zwakkere vorm van Dirichlet's

stelling). Voor de deelgroep $U_K(S)$ van $U_L(\tilde{S})$ kunnen we het volgende resultaat uit het bewijs van voorgaande stelling halen :

STELLING IV.1.2.2. *Er bestaat een fundamenteel systeem van* S-*eenheden* $\eta_1,\ldots,\eta_d$ *en een fundamenteel systeem van* $\tilde{S}$-*eenheden* $\varepsilon_1,\ldots,\varepsilon_h$ *die met elkaar verbonden zijn door de relaties :*

$$\eta_1 = \zeta_1\ \varepsilon_1^{a_1}$$

$$\ldots$$

$$\eta_d = \zeta_d\ \varepsilon_d^{a_d},$$

waarbij $\zeta_1,\ldots,\zeta_d \in W_L$; $a_1,\ldots,a_d \in \mathbb{Z}$ *en* $a_i | a_{i+1}$ *voor* $i = 1,2,\ldots,d$. *Bovendien is het produkt* $a_1\ldots a_d$ *een deler van de graad van de uitbreiding* L/K.

BEWIJS. Behoudens de laatste bewering volgt alles uit het bewijs van de voorgaande stelling. De laatste bewering volgt dan uit het feit dat $a_1\ldots a_d = q_{U_L(\tilde{S})}(U_K(S)) = q_L(U_K(S))$ en uit stelling IV. 1.1.2.

Deze stelling is de interpretatie waarvan we in het begin van dit punt gewag maakten. Het praktische ervan is gelegen in het feit dat, bij het opzoeken van de $\tilde{S}$-eenhedengroep van L, men reeds een deelgroep, namelijk $R_L(U_K(S))$, in een betrekkelijk gering aantal stappen kan vinden. Hiertoe volstaat het (in de veronderstelling dat W_L gekend is) inklusies zoals

$$K(\sqrt[m]{\zeta.\eta}) \subset L \quad (\zeta \in W_L)$$

voor een zekere $m \in \mathbb{N}_0$ en $\eta \in U_K(S)$ uit te testen.

Deze stelling leert ons eveneens dat $U_L(\tilde{S})$ direkt produkt is van $R_L(U_K(S))$ met de deelgroep van $U_L(\tilde{S})$ voortgebracht door de S-eenheden $\varepsilon_{d+1},\ldots,\varepsilon_h$, dit is een deelgroep die komplementair is aan $R_L(U_K(S))$.

DEFINITIE IV.1.2.2. Een multiplikatieve $\mathbb{Z}$-basis voor een deelgroep G van $U_L(\tilde{S})$ die komplementair is aan $R_L(U_K(S))$ noemt men een relatief fundamenteel systeem van $\tilde{S}$-eenheden voor de uitbreiding L/K.

Het is duidelijk dat twee relatief fundamentele systemen van $\tilde{S}$-eenheden $\varepsilon_{D+1},\ldots,\varepsilon_h$ en $\varepsilon'_{d+1},\ldots,\varepsilon'_h$ verbonden zullen zijn door betrekkingen van de vorm :

$$\varepsilon'_{d+j} = \eta'_j\ \varepsilon_{d+1}^{c_{j1}}\ldots\varepsilon_h^{c_{j,h-d}} \qquad (j = 1,2,\ldots,h-d)$$

waarbij $\eta'_1,\ldots,\eta'_{h-d} \in R_L(U_K(S))$; $c_{ij} \in \mathbb{Z}$ voor $1 \leq i,j \leq h-d$, en :

$$|\det(c_{ij})| = 1$$

Tenslotte zij het nog opgemerkt dat, indien S bestaat ui al de niet-equivalente archimedische valuaties van K, de verzameling $\tilde{S}$ eveneens slechts dit soort valuaties van L bevat, zodat $U_L(\tilde{S}) = U_L$. De stellingen en definities van deze paragraaf blijven dus van kracht zo men de prefixen "S-" en "$\tilde{S}$-" weglaat.

§2. RADIKALEN IN DE IDEALENGROEP

2.1. Het radikaal van I_K in I_L en globale ramifikatie.

Vooreerst zij eraan herinnerd dat de idealen van K geïdentificeerd kunnen worden met de idealen van L via de injektie $i_{L/K}$

(zie I.1.2.). Om precies te zijn, dit betekent dat we het ideaal a van K met het ideaal $a.\mathcal{O}_L$ van L zullen identificeren. Hierdoor wordt I_K beschouwd als een deelgroep van I_L, zodat het zin heeft over het radikaal van I_K in I_L te spreken. Het is verder duidelijk dat de groep der hoofdidealen P_K van K, door deze identifikatie, een deelgroep wordt van de groep der hoofdidealen P_L van L. Op te merken valt dat P_K meestal verschillend is van $P_L \cap I_K$. Voor een ideaal a van K zullen we verder ook nog gewag maken van zijn kanonieke faktorisatie in K, resp. in L al naargelang a als ideaal van K of als ideaal van L beschouwd wordt.

Aangezien I_L torsievrij is, zullen we geen onderscheid hoeven te maken tussen R-indices en RT-indices.

LEMMA IV.2.1. Zij V_K de deelgroep van I_K voortgebracht door alle priemdelers van K die vertakken in L, en zij V_L de deelgroep van I_L voortgebracht door alle priemdelers van L die boven de priemdelers van V_K liggen. Dan geldt :

$$R_{I_L}(I_K) = I_K.R_{V_L}(V_K).$$

BEWIJS. Zij A een ideaal van L dat tot $R_{I_L}(I_K)$ behoort. Veronderstel dat zijn kanonieke faktorisatie in L gegeven is door :

$$(1) \qquad A = \prod_{p}\Big(\prod_{P|p} P^{m_P}\Big),$$

waarbij p de priemdelers van K doorloopt en waarbij het tweede produkt zich uitstrekt over alle priemdelers P van L die boven dezelfde p liggen. Laat m een natuurlijk getal ($\neq 0$) zijn waarvoor $A^m \in I_K$, en zij

$$A^m = \prod_{p} p^{c_p}$$

de kanonieke faktorisatie van A^m in K. Is anderzijds

$$(2) \qquad p = \prod_{P|p} P^{e(P|p)}$$

de kanonieke faktorisatie van een priemideaal p van K in L, dan geeft de m^{de}-macht van (1) :

$$A^m = \prod_p \left(\prod_{P|p} P^{m.m_P} \right) = \prod_p p^{c_p} = \prod_p \left(\prod_{P|p} P^{c_p.e(P|p)} \right).$$

Uit de uniciteit van de kanonieke faktorisatie volgt dan :

$$(3) \qquad m.m_P = c_p.e(P|p).$$

Indien p onvertakt is in L, d.w.z. : $p \notin V_K$ en $e(P|p) = 1$ voor alle P boven p, dan volgt uit (3) dat de getallen m_P gelijk zijn aan elkaar, zegge aan d_p. Hieruit volgt :

$$\prod_{P|p} P^{m_P} = \left(\prod_{P|p} P \right)^{d_p}.$$

Dit laatste is echter wegens (2) (waarin $e(P|p) = 1$) niets anders dan p^{d_p}. Substitueert men dit in (1), en stelt men :

$$\prod_{p, p \notin V_K} p^{d_p} = a, \in I_K,$$

dan ziet men dat $A = a.*$, waarbij $* \in V_L$. Wegens het feit dat $A^m \in I_K$ heeft men eveneens : $*^m \in I_K$. Wegens de definitie van V_L zal $*^m \in V_K$, waarmee aangetoond is dat

$$R_{I_L}(I_K) \subset I_K.R_{V_L}(V_K).$$

De omgekeerde inklusie is vanzelfsprekend, zodat we tot de gewenste gelijkheid mogen besluiten.

STELLING IV.2.1.1. *Zijn* V_K *en* V_L *de deelgroepen van* I_K, *respektievelijk* I_L *bepaald in voorgaand lemma, dan bestaat er een isomorfisme :*

$$R_{I_L}(I_K)/I_K \cong R_{V_L}(V_K)/V_K \ .$$

BEWIJS. Uit het lemma volgt :

$$R_{I_L}(I_K)/I_K \cong I_K.R_{V_L}(V_K)/I_K.$$

Deze laatste quotiëntgroep is wegens de klassieke isomorfiestellingen uit de groepentheorie isomorf met de quotiëntgroep :

$$R_{V_L}(V_K)/I_K \cap R_{V_L}(V_K).$$

Aangezien de idealen van $R_{V_L}(V_K)$ in hun kanonieke faktorisatie in L slechts priemdelers zullen bevatten die in V_L zitten, zullen deze idealen, wanneer ze ook tot I_K behoren vanzelfsprekend elementen van V_K zijn. Er geldt dus : $I_K \cap R_{V_L}(V_K) \subset V_K$. De omgekeerde inklusie is triviaal, wat ons uiteindelijk toelaat tot het gewenste isomorfisme te besluiten.

Het zij hier opgemerkt dat V_K en V_L eindig voortgebrachte vrije abelse groepen zijn aangezien $p \in V_K$ equivalent is met $p|D_{L/K}$ (cfr. I.1.2.). We gebruiken dit in de volgende stelling.

STELLING IV.2.1.2. *Laat* $p_1,\ldots,p_k$ *de priemdelers zijn van de diskriminant* $D_{L/K}$ *van de uitbreiding* L/K. *Voor elke* i = 1,2,...,k, *zij*

$$p_i = P_{i1}^{e_{i1}} \ldots P_{is_i}^{e_{is_i}}$$

de kanonieke faktorisatie van p_i *in* L. *Dan is de R-index van* I_K *in* I_L *de grootste gemene deler van de getallen :*

$$e_{1,j_1} e_{2,j_2} \cdots e_{k,j_k}$$

(waarbij voor $1 \leqslant i \leqslant k$ *de getallen* j_i *voldoen aan :* $1 \leqslant j_i \leqslant s_i$*).*

BEWIJS. Er geldt dat $p_1,\ldots,p_k$ de generatoren zijn van V_K, terwijl V_L voortgebracht is door de priemidealen $P_{i,j}$ $(1 \leqslant i \leqslant k;\ 1 \leqslant j \leqslant s_i)$. Het bewijs van stelling IV.1.2.1. leert ons dat de R-index van V_K in V_L niet anders is dan de grootste gemene deler van alle $k \times k$-minoren uit de matrix :

$$\begin{pmatrix} e_{11}\cdots e_{1s_1} & 0 \ldots 0 & 0\ldots 0 & 0 \ldots 0 \\ 0 \ldots 0 & e_{21}\cdots e_{2s_2} & 0\ldots 0 & 0 \ldots 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 \ldots 0 & 0 \quad 0 & 0\ldots 0 & e_{k1}\cdots e_{ks_k} \end{pmatrix}$$

Een van nul verschillende $k \times k$-minor uit deze matrix is echter steeds van de vorm :

$$\pm\, e_{1j_1}\, e_{2j_2} \cdots e_{kj_k}\ ,$$

waarbij $i \leqslant j_i \leqslant s_i$ voor elke $i = 1,2,\ldots,k$. Hieruit volgt het gestelde.

DEFINITIE IV.2.1. De R-index van I_K in I_L wordt de globale ramifikatie-index van de uitbreiding L/K genoemd en met $v_{L/K}$ aangeduid.

We bespreken thans het verband tussen $v_{L/K}$ en $[L : K]$. Vooreerst zij eraan herinnerd dat een eindige abelse groep kan geschreven worden als de direkte som van cyclische deelgroepen waarvan de orde een macht is van een priemgetal en dat een dergelijke cyclische

deelgroep een cyclische komponent van G genoemd wordt. De orde van een cyclische komponent noemt men dan een invariant van G.

STELLING IV.2.1.3. *De invarianten van* $R_{I_L}(I_K)/I_K$ *delen de graad van de uitbreiding* L/K.

BEWIJS. Zij H een cyclische komponent van $R_{I_L}(I_K)/I_K$, en stel dat $(H : 1) = p^\nu$, p een priemgetal. Er is dus te bewijzen : $p^\nu | n$. Zij $A \in R_{I_L}(I_K)$ een ideaal dat door het natuurlijk homomorfisme : $R_{I_L}(I_K) \to R_{I_L}(I_K)/I_K$ op een generator van H afgebeeld wordt. Het is duidelijk dat dit betekent :

$$A^{p^\nu} = a \in I_K \quad \text{en} \quad a \notin I_K^p ,$$

want was $a = b^p$ voor een ideaal b van K, dan was $A^{p^\nu - 1}$ reeds een element van I_K, wat uitgesloten is indien A modulo I_K een generator is voor H.

Zij de kanonieke faktorisatie van A in L gegeven door :

$$A = \prod_p \left(\prod_{P|p} P^{m_P} \right),$$

en zij de kanonieke faktorisatie van een priemideaal p van K in L gegeven door :

$$p = \prod_{P|p} P^{e(P|p)} .$$

Is dan

$$A^{p^\nu} = \prod_p p^{c_p}$$

de kanonieke faktorisatie van A^{p^ν} in K, dan vindt men analoog zoals in Lemma IV.2.1. :

$$m_P \, p^\nu = e(P|p) c_p, \text{ voor alle } P \text{ boven dezelfde } p.$$

Uit $a \notin I_K^p$ volgt dat er minstens een priemideaal p van K bestaat waarvoor $c_p \not\equiv 0 \pmod{p}$. Voor dit priemideaal geldt dus :

$$e(P|p) \equiv 0 \pmod{p^\lambda}, \text{ voor alle } P|p.$$

Uit de relatie :

$$\sum_{P|p} e(P|p)f(P|p) = n = [L : K]$$

(cfr. I.1.2.) volgt tenslotte het gestelde.

Opmerking 1. Het is duidelijk dat $v_{L/K}$ geen deler hoeft te zijn van n : dit ziet men gemakkelijkst bij kwadratische velden waar men onmiddellijk narekent dat $v_{L/K} = 2^t$, waarbij t het aantal priemdelers van de diskriminant van het kwadratisch veld is. Men kan dat aantal wegens stelling II.1.1., gevolg, willekeurig groot nemen.

Opmerking 2. Het is bekend dat $\mathbb{Q}$ geen onvertakte uitbreidingen kan bezitten. Nochtans bestaan er uitbreidingen K van $\mathbb{Q}$ die globaal onvertakt zijn (d.w.z. $v_{K/\mathbb{Q}} = 1$). Een voorbeeld hiervan is $K = Q(\theta)$, waarbij θ een wortel is van de polynoom X^3-X-1. De enige vertakte priemdeler van $\mathbb{Q}$ is $23.\mathbb{Z}$, en er geldt :

$$23.\mathcal{O}_K = p_1 p_2^2,$$

(p_1 en p_2 priemdelers van K). Hier heeft men dus wegens stelling IV.2.1.2. :

$$v_{K/\mathbb{Q}} = \text{G.g.d.}(1,2) = 1.$$

Opmerking 3. Is L/K een galoisuitbreiding dan is $v_{L/K}$ het produkt van alle ramifikatie-indices e_p van de priemdelers p van K. Dit komt doordat in stelling IV.2.1.2. :

$$e_{i1} = e_{i2} = \ldots = e_{is_i} = e_{p_i} \quad \text{voor} \quad i = 1,2,\ldots,k,$$

wat impliceert dat de getallen $e_{1j_1}\, e_{2j_2} \ldots e_{kj_k}$ dezelfde zijn voor elke geoorloofde keuze van $j_1,\ldots,j_k$.

2. Het radikaal van P_K in I_L en in P_L.

STELLING IV.2.2.1. *Er geldt :*

$$R_{I_L}(P_K) = R_{I_L}(I_K).$$

BEWIJS. Wegens stelling III.1.2.2. volgt uit $P_K \subset I_K$:

$$R_{I_L}(P_K) \subset R_{I_L}(I_K).$$

Omgekeerd, uit stelling III.1.2.3. volgt dat $H \subset R_{I_L}(P_K)$ voor elke deelgroep H van I_L waarin P_K bevat is en waarin P_K van eindige index is. Aangezien $(I_K : P_K) = h_K$ eindig is geldt : $I_K \subset R_{I_L}(P_K)$, waaruit :

$$R_{I_L}(I_K) \subset R_{I_L}(R_{I_L}(P_K)) = R_{I_L}(P_K) \quad \text{(cfr. III.1.1.)}.$$

Hiermee is het gestelde bewezen.

Gevolg. De R-index van P_K in I_L is gelijk aan het produkt

$$h_K \cdot v_{L/K} .$$

Dit volgt onmiddellijk uit de inklusies $P_K \subset I_K \subset R_{I_L}(I_K)$ en elementaire groepentheorie.

STELLING IV.2.2.2. *De R-index van* P_K *in* P_L *is een deler van het produkt* $h_K \cdot v_{L/K}$. *Bovendien is het geheel getal* $a_{L/K}$, *gedefinieerd door :*

$$a_{L/K} = \frac{h_K \cdot v_{L/K}}{Q_{P_L}(P_K)} ,$$

een deler is van het klassegetal h_L *van* L.

BEWIJS. De eerste bewering volgt onmiddellijk uit het diagram van inklusies :

$$\text{index} : h_K \cdot v_{L/K} \left\{ \begin{array}{l} R_{I_L}(P_K) \\ | \\ R_{I_L}(P_K) \cap P_L = R_{P_L}(P_K) \quad \text{(zie stelling III.1.2.2.)} \\ | \qquad \leftarrow \text{index} : Q_{P_L}(P_K) \\ P_K \end{array} \right.$$

De tweede bewering volgt onmiddellijk uit :

$$R_{I_L}(P_K)/(R_{I_L}(P_K) \cap P_L) \cong R_{I_L}(P_K).P_L/P_L \subset I_L/P_L$$

en uit het feit dat $h_L = (I_L : P_L)$.

Via het omgekeerde beeld van het homomorfisme $\phi_L : L^* \to P_L$ (dat een element α van L^* stuurt naar het hoofdideaal $\alpha.\mathcal{O}_L$) zullen we nu het radikaal van P_K in P_L interpreteren als het radikaal van een zekere deelgroep van L^* in L^*.

STELLING IV.2.2.3. *Er geldt :*

$$\phi_L^{-1}(R_{P_L}(P_K)) = R_L(U_L.K^*).$$

BEWIJS. Is α een element van $\phi_L^{-1}(R_{P_L}(P_K))$, dan geldt, voor een zeker getal $m \in \mathbb{N}_0$: $(\phi_L(\alpha))^m = (\alpha.\mathcal{O}_L)^m = \alpha^m.\mathcal{O}_L \in P_K$. Dit betekent : er bestaat een $a \in K^*$ zódanig dat $\alpha^m.\mathcal{O}_L = a.\mathcal{O}_L$. Dus

$$\mathcal{O}_L = \alpha^{-m}.a.\mathcal{O}_L,$$

zodat er een eenheid ε van L bestaat waarvoor $\alpha^m = \varepsilon.a$. Dus geldt :

$$(1) \qquad \phi_L^{-1}(R_{P_L}(P_K)) \subset R_L(U_L K^*).$$

Omgekeerd, is α een element van $R_L(U_L K^*)$, dan bestaat er een $m \in \mathbb{N}_0$, een $\varepsilon \in U_L$ en een element a van K^* zo dat $\alpha^m = \varepsilon.a$. Hieruit volgt :

$$\phi(\alpha^m) = (\phi(\alpha))^m = (\alpha.\mathcal{O}_L)^m = a.\mathcal{O}_L \in P_K,$$

wat de omgekeerde inklusie in (1) impliceert.

Wat betreft de R-index van $U_L K^*$ in L^* zij het opgemerkt dat deze samenvalt met de RT-index, aangezien $W_L \subset U_L$.

STELLING IV.2.2.4. *Er geldt :*

$$Q_L(U_L K^*) = Q_{P_L}(P_K).$$

BEWIJS. We passen lemma III.3.1. toe met $A = R_L(U_L K^*)$, $B = U_L K^*$ en f = de beperking van ϕ_L tot $R_L(U_L K^*)$. Men ziet onmiddellijk dat $A_f = B_f = U_L = \mathrm{Ker}(\phi_L)$ (cfr. I.3.2.) en dat

$$A^f = R_{P_L}(P_K)$$

(dit is nl. de voorgaande stelling). Verder is klaarblijkelijk $B^f = P_K$, zodat we volgend isomorfisme bekomen :

$$R_L(U_L K^*)/U_L K^* \cong R_{P_L}(P_K)/P_K.$$

De definitie van de R-index laat ons dan toe tot het gewenste resultaat te besluiten.

Een relatie tussen $Q_L(K^*)$, $Q_L(U_K)$ en $Q_{P_L}(P_K)$.

STELLING IV.2.3. *Het getal* $Q_L(K^*).Q_L(U_K)^{-1}$ *is geheel en deelt de index* $Q_{P_L}(P_K)$.

BEWIJS. Wegens de in IV.1.1. bekomen injektie (met $U_K(S) = U_K$) :

$$\phi : R_L(U_K)/W_L.U_K \to R_L(K^*)/W_L K^*$$

kan men besluiten tot :

$$\frac{q_L(K^*)}{q_L(U_K)} \in \mathbb{N}_0 .$$

Wegens stelling III.1.2.1. heeft men :

$$\frac{Q_L(K^*)}{Q_L(U_K)} = \frac{(W_L : W_K).q_L(K^*)}{(W_L : W_K).q_L(U_K)} = \frac{q_L(K^*)}{q_L(U_K)} \in \mathbb{N}_0 ,$$

wat het eerste deel van het gestelde bewijst. Wat betreft het tweede deel, beschouw het volgend diagram :

$$\begin{array}{ccccccccc}
 & & & & & & & & \\
1 & \longrightarrow & R_L(U_K) & \xrightarrow{i} & R_L(K^*) & \xrightarrow{\phi_L|R_L(K^*)} & \phi_L(R_L(K^*)) & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & U_K & \xrightarrow{i'} & K^* & \xrightarrow{\phi_L|K^*} & \phi_L(K^*) & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Hierin zijn i, i' en de vertikale pijlen natuurlijke injekties. De kommutativiteit van het diagram en de exaktheid van de kolommen erin zijn evident. De onderste rij is exakt wegens I.3.2. De exaktheid van de bovenste rij volgt uit de gelijkheden :

$$\mathrm{Ker}(\phi_L|R_L(K^*)) = (\mathrm{Ker}\ \phi_L) \cap R_L(K^*) = U_L \cap R_L(K^*) = R_{U_L}(U_K)$$

(wegens stelling III.1.2.2.)

en uit het feit dat $R_{U_L}(U_K) = R_L(U_K)$ (zie stelling IV.1.1.1., met $U_K(S) = U_K$ en $U_L(\tilde{S}) = U_S$.

Men kan thans het 3×3-lemma toepassen om tot het volgend isomorfisme te komen (waarbij gebruik gemaakt wordt van de gelijkheid $\phi_L(K^*) = P_K$) :

$$(1) \qquad (R_L(K^*)/K^*)/R_L(U_K)/U_K \cong \phi_L(R_L(K^*))/P_K.$$

Het is verder duidelijk dat $R_L(K^*) \subset R_L(U_K K^*)$, zodat :

$$\phi_L(R_L(K^*)) \subset \phi_L(R_L(U_L K^*)) = R_{P_L}(P_K) \text{ (stelling IV.2.2.3.).}$$

De rechtse quotiëntgroep in (1) is dus een deelgroep van de quotiëntgroep $R_{P_L}(P_K)/P_K$. Het gewenste resultaat volgt dan onmiddellijk uit de definitie van de R-index.

Opmerking. Het getal $Q_L(K^*).Q_L(U_K)^{-1} = q_L(K^*).q_L(U_K)^{-1}$ is wegens stelling III.4.5. en stelling IV.1.1.2. een deler van $n = [L : K]$. Wat de andere priemdelers van $Q_{P_L}(P_K)$ nog kunnen zijn wordt in het volgende punt onderzocht.

2.4. De priemdelers van $Q_L(U_L K^*)$.

In wat voorafging werd aangetoond dat $R_L(U_L K^*)/U_L K^*$ een eindige groep is. Hij is dus te schrijven als direkte som van cyclische komponenten. Voor de orde van een cyclische komponent (d.i. : een invariant voor $R_L(U_L K^*)/U_L K^*$) geldt dan volgende stelling :

STELLING IV.2.4.1. *De invarianten van de groep* $R_L(U_L K^*)/U_L K^*$ *zijn delers van de graad van de uitbreiding* L/K. □

BEWIJS. Zij H een cyclische komponent van $R_L(U_K K^*)/U_L K^*$, en stel : $(H : 1) = p^\nu = q$ (p een priemgetal). Zij α een element van

$R_L(U_L K^*)$ dat onder het natuurlijk homomorfisme :

$$R_L(U_L K^*) \to R_L(U_L K^*)/U_L K^*$$

afgebeeld wordt op een generator van H. Dit betekent dat het element α aan de volgende twee voorwaarden voldoet :

(1) : $\alpha^{p^\nu} = \alpha^q = \varepsilon.a$, met $\varepsilon \in U_L$ en $a \in K^*$;

(2) : Voor $\lambda \in \mathbb{N}_0$, $\lambda < \nu$ geldt : $\alpha^{p^\lambda} \notin U_L K^*$.

Zij bovendien :

$$a.\mathcal{O}_K = \prod_p p^{m_p}$$

de kanonieke faktorisatie van het ideaal $a.\mathcal{O}_K$ in K, en

$$p = \prod_{P|p} P^{e(P|p)}$$

de kanonieke faktorisatie van een priemideaal p van K in L. Hieruit vindt men onmiddellijk voor de kanonieke faktorisatie van het ideaal $a.\mathcal{O}_L$ in L :

$$a.\mathcal{O}_L = \prod_p \left(\prod_{P|p} P^{e(P|p)m_p} \right)$$

Uit (1) volgt dat dit ideaal de q^{de} macht moet zijn van een ideaal (nl. $\alpha.\mathcal{O}_L$) van L. Dit betekent :

(3) $\quad q = p^\nu | e(P|p)m_p$

voor alle priemdelers p van K en alle priemdelers P van L boven p. Zij w gedefinieerd als zijnde het grootste natuurlijk getal m met de eigenschap :

$$p^m | m_p \qquad \text{voor alle } p.$$

Dit komt hierop neer dat het ideaal $a.\mathcal{O}_K$ de p^w-de-macht is van een

ideaal a van K dat zelf geen p^{de}-macht meer is van een ander ideaal van K (het ideaal a kan eventueel een p^{de}-macht zijn van een ideaal uit L, wat geen afbreuk doet op onze beschouwingen).
Het kan voorkomen dat w nul is. In dit geval volgt uit (3) :

$$\exists\, p \text{ zo dat } p^{\nu} \mid e(P|p) \text{ voor alle } P \text{ er boven.}$$

Het priemideaal p is namelijk een van die waarvoor $p \nmid m_p$. Uit de betrekking :

$$\sum_{P|p} e(P|p)f(P|p) = n = [L : K]$$

volgt dan onmiddellijk : $p^{\nu} \mid n$, wat moest bewezen worden. Veronderstel dus : $w \neq 0$. We beweren dat p^w de orde is van a modulo P_K of, m.a.w. :

$$u \in \mathbb{N} \;\&\; 0 < u < w \Rightarrow a^{p^u} \notin P_K.$$

Welnu, veronderstel dat dit niet waar is. Zij b dan een element van K^* zodanig dat :

$$a^{p^u} = b.\mathcal{O}_K.$$

Er geldt dan :

$$a.\mathcal{O}_K = a^{p^w} = (b.\mathcal{O}_K)^{p^{w-u}} = b^{p^{w-u}}.\mathcal{O}_K.$$

Er bestaat dus een eenheid η van K zodanig dat :

$$a = \eta.b^{p^{w-u}}.$$

Wegens (1) bekomt men :

$$\alpha^{p^{\nu}} = \varepsilon.\eta.b^{p^{w-u}} = \varepsilon.\eta.c^p,$$

waarin $c = b^{p^{w-u-1}}$.

Hieruit volgt :

$$(\alpha^{p^{\nu-1}}.c^{-1})^p = \varepsilon' \in U_L.$$

Uit Lemma IV.1.1. volgt :

$$\alpha^{p^{\nu-1}}.c^{-1} \in U_L,$$

wat in strijd is met (2). Hiermee is onze bewering bewezen. Een onmiddellijk gevolg ervan is :

$$a^\nu \in P_K \Leftrightarrow p^w | \nu.$$

Nemen we nu in (1) de norm $N = N_{L/K}$ van beide leden, dan bekomen we :

$$(N(\alpha))^{p^\nu} = N(\varepsilon).N(a) = \eta'.a^n \quad (\eta' \in U_K).$$

Hieruit volgt :

$$(N(\alpha).\mathcal{O}_K)^{p^\nu} = a^{p^w}.n.$$

Is nu $w \geq \nu$, dan volgt hieruit :

$$N(\alpha).\mathcal{O}_K = a^{p^{w-\nu}}.n,$$

zodat, wegens (4) :

$$p^w | p^{w-\lambda}.n.$$

Klaarblijkelijk impliceert dit : $p^\nu | n$, hetgeen te bewijzen was.
Is anderzijds $w < \nu$, dan heeft men :

$$(N(\alpha).\mathcal{O}_K)^{p^{\nu-w}} = a^n.$$

Aangezien a geen p^{de}-macht meer is in I_K volgt hieruit :

$$n \equiv 0 (\text{mod } p^{\nu-w}), \text{ of : } n = t.p^{\nu-w} \text{ voor een } t \in \mathbb{N}_0.$$

Dit geeft :

$$N(\alpha).\mathcal{O}_K = a^t.$$

Uit (4) volgt dan : $p^w | t$. Het is dan eenvoudig na te gaan dat hieruit de relatie : $p^\nu | n$ volgt, hetgeen te bewijzen was.

Gevolg. Het getal $n = [L : K]$ is een exponent voor de groep $R_L(U_L K^*)/U_L K^*$, aangezien het een exponent is voor al zijn cyclische komponenten.

Deze stelling laat ons toe wat meer inzicht te verkrijgen in de onderlinge verhouding van de klassegetallen h_K en h_L als volgt :

STELLING IV.2.4.2. *Zij de kanonieke faktorisatie van het klassegetal* h_K *van* K *door :*

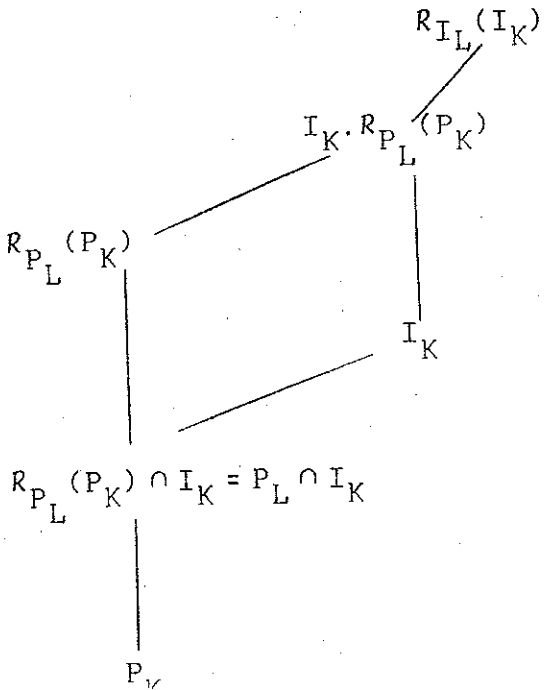
$$h_K = p_1^{a_1} \ldots p_r^{a_r} . q_1^{b_1} \ldots q_s^{b_s},$$

waarbij $p_i | n$ *voor* $i = 1,2,\ldots,r$ *en* $q_j \nmid n$ *voor* $j = 1,2,\ldots,s$. *Stelt men :*

$$h_{K,n} = q_1^{b_1} \ldots q_s^{b_s},$$

dan geldt : $h_{K,n} | h_L$.

BEWIJS. Beschouw het volgende diagram van inklusies :



De hierin voorkomende gelijkheid volgt uit :

$$R_{P_L}(P_K) \cap I_K = (P_L \cap R_{I_L}(P_K)) \cap I_K \quad \text{(stelling III.1.2.2.)}$$

$$= P_L \cap (R_{I_L}(P_K) \cap I_K)$$

en het feit dat $R_{I_L}(P_K) \cap I_K = I_K$.
De quotiëntgroep $(P_L \cap I_K)/P_K$ is dus een deelgroep van de quotiëntgroep $R_{P_L}(P_K)/P_K$ die wegens stellingen IV.2.2.3. en 4. isomorf is met de quotiëntgroep $R_L(U_L K^*)/U_L K^*$. Deze groep heeft –wegens voorgaande stelling– een orde die slechts door de priemgetallen $p_1,\ldots,p_r$ kan deelbaar zijn. Hieruit volgt dat de quotiëntgroep $I_K/P_L \cap I_K$ een orde zal hebben die deelbaar is door $h_{K,n}$, aangezien :

$$h_K = (I_K : P_L \cap I_K).(P_L \cap I_K : P_K).$$

In het diagram zien we echter duidelijk dat :

$$(I_K : P_L \cap I_K) = (I_K : R_{P_L}(P_K) \cap I_K) = (I_K.R_{P_L}(P_K) : R_{P_L}(P_K)).$$

Deze laatste index is echter een deler van $(R_{I_L}(I_K) : R_{P_L}(P_K)) = a_{L/K}$, waarvan in stelling IV.2.2.2. aangetoond werd dat het een deler is van h_L. Bijgevolg : $h_{K,n} | h_L$, Q.E.D.

Een welbekende toepassing van deze stelling luidt als volgt : "Is p een oneven priemgetal, $\zeta = \exp(2\pi i/p)$, en is het klassegetal van het veld $\mathbb{Q}(\zeta + \zeta^{-1})$ deelbaar door p, dan is het klassegetal van het p^{de} cyclotome veld $\mathbb{Q}(\zeta)$ eveneens deelbaar door p." (Kummer's stelling). De graad van de uitbreiding $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$ is immers gelijk aan 2, en aangezien $p \nmid 2$, kan de stelling toegepast worden.

Voor deelvelden van $\mathbb{Q}(\zeta)$ werd de stelling reeds bewezen door Fürtwängler (cfr. [8]).

Het zij verder opgemerkt dat de faktor $a_{L/K}$ die in de uitdrukking :

$$Q_L(U_L K^*) = \frac{h_K \cdot v_{L/K}}{a_{L/K}}$$

voorkomt meestal moeilijk te berekenen is. We beschikken dus niet over een "expliciete" formule voor $Q_L(U_L K^*)$. In het volgende hoofdstuk zal uiteengezet worden hoe dit verholpen kan worden wanneer de uitbreiding L/K cyclisch is.

HOOFDSTUK V

BIJZONDERE GETALLENVELDEN EN TOEPASSINGEN

In dit hoofdstuk zal onderzocht worden in welke mate het cyclisch zijn van de uitbreiding L/K (K een getallenveld) tot scherpere resultaten voert. Meer bepaald zullen we zien dat er dan een omrekening van $Q_L(U_L K^*)$ in termen van globale ramifikatie en normindex mogelijk is. De resultaten voeren ons tot Chevalley's formule voor het ~~inerte~~ inertie-klassegetal.

Vervolgens tonen we aan hoe in het bijzonder geval : $[L : K] = 2$, de index $Q_L(U_K)$ optreedt in de analytische uitdrukking voor het quotiënt van de klassegetallen van L en K.

In een laatste paragraaf worden dan nog enige toepassingen van de voorgaande resultaten gegeven.

§1. DE R- EN RT-INDICES IN CYCLISCHE UITBREIDINGEN

Doorheen deze paragraaf is K een getallenveld en L een cyclische uitbreiding van K. De galoisgroep van L/K zal met G aangeduid worden, en we veronderstellen : $[L : K] = (G : 1) = n$. Het symbool σ staat voor een van nu af aan vast gekozen generator voor G. Wat betreft de symbolen λ,N, verwijzen we naar hoofdstuk III, §3.2.; alle aldaar ingevoerde notaties blijven ook hier van kracht.

Het Herbrand quotiënt.

We herinneren eraan dat, wanneer een cyclische groep G met generator σ, inwerkt op een abelse groep A (multiplikatief genoteerd), het Herbrand quotiënt van A als G-groep gedefinieerd is door :

$$h(G,A) = \frac{(A_\lambda : A^N)}{(A_N : A^\lambda)}$$

Hier zijn λ en N de endomorfismen van A gedefinieerd door :

$$\lambda : a \mapsto a^{1-\sigma} = a/\sigma a$$

$$N : a \mapsto a^{1+\sigma+\sigma^2+\ldots+\sigma^{n-1}} \quad (n = (G : 1)).$$

Vanzelfsprekend is deze definitie slechts van kracht indien de indices $(A_\lambda : A^N)$ en $(A_N : A^\lambda)$ eindig zijn.

STELLING V.1.1.1. *Is A een eindige groep waarop de cyclische groep G van orde n inwerkt, dan geldt :*

$$h(G,A) = 1.$$

BEWIJS. Zie [19], ch. IX, §1.

Keren we terug naar de uitbreiding L/K. Zij S_0 de verzameling van alle niet-equivalente archimedische valuaties van K. Voor $v \in S_0$, zij N_v de lokale graad van v in L (zie I.2.2.).

STELLING V.1.1.2. *Het Herbrand quotiënt van* U_L *als G-groep voldoet aan de betrekking :*

$$h(G,U_L) = \frac{1}{n} \prod_{v \in S_0} N_v.$$

BEWIJS. Zie [19], ch IX, §4, cor. 2.

.2. De index $q_L(K^*)$.

STELLING V.1.2. *Er geldt :*

$$q_L(K^*) = (W_K : N(W_L)).$$

BEWIJS. Wegens stelling III.3.2.2. geldt :

$$q_L(K^*) = ((W_L)_N : (W_L)^\lambda).$$

Deze laatste index is echter de noemer van het Herbrand quotiënt $h(G,W_L)$. Aangezien $(W_L : 1) < \infty$, kan stelling V.1.1.1. aangewend worden, i.e. : $h(G,W_L) = 1$. Hieruit volgt :

$$q_L(K^*) = ((W_L)_\lambda : (W_L)^N).$$

Uit : $(W_L)_\lambda = (\text{Ker } \lambda) \cap W_L = K^* \cap W_L = W_K$, volgt dan het gestelde.

Opmerking. Uit stelling III.3.2.4. volgt dat de index $(W_K : N(W_K))$ een deler is van n. Dit kan evenwel onmiddellijk aangetoond worden, wat dus een alternatief bewijs oplevert voor stelling III.3.2.4. Dit gebeurt als volgt :

- er geldt, gezien de eindigheid van $(W_L : 1)$:

$$(W_K : N(W_L)) = \frac{(W_K : N(W_K))}{(N(W_L) : N(W_K))}$$

- Verder is : $N(W_K) = W_K^n$, $(\text{Ker } N) \cap W_K = W_{K,n}$ (cfr. III.3., vb 4), en :

$$(W_K : N(W_K)) = \frac{(W_K : 1)}{(N(W_K) : 1)} .$$

- Uit de exaktheid van de rij :

$$1 \to W_{K,n} \to W_K \xrightarrow{N} N(W_K) \to 1$$

volgt verder :

$$(N(W_K) : 1) = (W_{K,n} : 1).$$

- Dit alles kombineren geeft uiteindelijk :

$$(W_K : N(W_L)) = \frac{(W_{K,n} : 1)}{(N(W_L) : N(W_K)} .$$

Hierin is de teller klaarblijkelijk een deler van n; de noemer deelt de teller (aangezien $(W_K : N(W_L)) \in \mathbb{N}$), i.e. : $(W_K : N(W_L))|n$.

.3. De index $q_L(U_L K^*)$.

Omtrent de notaties i.v.m. de kanonieke faktorisatie van een ideaal van L in L merken we het volgende op. Zij p een priemideaal van K en zij P een priemideaal van L boven p. De andere priemidealen van L boven p zijn dan :

$$P^{\sigma}, P^{\sigma^2}, \ldots, P^{\sigma^{r-1}},$$

waarbij $r = r_p$ het kleinste natuurlijk getal ($\neq 0$) is met de eigenschap :

$$P^{\sigma^r} = P.$$

Dit betekent dus dat σ^r een generator is voor de dekompositiegroep G_P van P (zie I.1.2.). Dat r enkel van p afhangt is dus duidelijk, evenals het feit dat $r_p|n$. De kanonieke faktorisatie van p in L kan nu als volgt geschreven worden :

$$(1) \qquad p\ (= p\mathcal{O}_L) = (P.P^{\sigma}.P^{\sigma^2}\ldots P^{\sigma^{r-1}})^{e_p} = (P^{1+\sigma+\sigma^2+\ldots+\sigma^{r-1}})^{e_p},$$

waarbij e_p de ramifikatie-index van p in L is (zie I.1.2.).

We veronderstellen voortaan dat boven elke priemdeler p van K

één priemdeler P_p van L geselekteerd werd. De kanonieke faktorisatie van een willekeurig ideaal A van L kan dan als volgt geschreven worden :

$$A = \prod_p P_p^{g_p(\sigma)},$$

waarbij het produkt zich uitstrekt over alle priemidealen p van K, en waarbij het element $g_p(\sigma)$ behoort tot de groepring $\mathbb{Z}[G]$ en van de volgende gedaante kan ondersteld worden :

$$g_p(\sigma) = a_{p,0} + a_{p,1}\sigma + \ldots + a_{p,r_p-1}\sigma^{r_p-1} \quad (a_{p,i} \in \mathbb{Z})$$

Daardoor zijn vanzelfsprekend de coëfficiënten $a_{p,i}$ eenduidig bepaald.

STELLING V.1.3.1. *Er bestaat een isomorfisme :*

$$R_L(U_L K^*)/U_L K^* \cong (U_L)_N/(U_L)^\lambda.$$

BEWIJS. Pas lemma III.3.1. toe, waarin $A = R_L(U_L K^*)$, $B = U_L K^*$ en $f = \lambda$. Er gelden volgende gelijkheden :

$$A_f = (R_L(U_L K^*))_\lambda = (\mathrm{Ker}\ \lambda) \cap R_L(U_L K^*) = K^* \cap R_L(U_L K^*) = K^*$$

$$B_f = (U_L K^*)_\lambda = (\mathrm{Ker}\ \lambda) \cap U_L K^* = K^* \cap U_L K^* = K^*$$

$$B^f = (U_L K^*)^\lambda = U_L^\lambda,$$

zodat wegens bovenvermeld lemma :

$$R_L(U_L K^*)/U_L K^* \cong (R_L(U_L K^*))^\lambda/(U_L)^\lambda$$

Er rest dus nog slechts te bewijzen dat

$$(R_L(U_L K^*))^\lambda = (U_L)_N.$$

Welnu, zij $\alpha \in R_L(U_L K^*)$. Er bestaat dus een $m \in \mathbb{N}_0$, een $\varepsilon \in U_L$

en een $a \in K^*$ zó dat :

$$\alpha^m = \varepsilon.a \quad .$$

Hieruit volgt :

$$(\alpha^m)^\lambda = (\alpha^\lambda)^m = \varepsilon^\lambda.a^\lambda = \varepsilon^\lambda \in U_L.$$

Wegens lemma IV.1.1. geldt : $\alpha^\lambda \in U_L$. Anderzijds geldt : $\alpha^\lambda \in \text{Ker } N$, wat impliceert : $\alpha^\lambda \in (U_L)_N$. Hiermee is de inklusie :

$$R_L(U_L K^*)^\lambda \subset (U_L)_N,$$

aangetoond.

Omgekeerd, zij $\varepsilon \in (U_L)_N$. Wegens stelling III.3.2.1. (Hilbert's stelling 90) geldt : er bestaat een $\alpha \in K^*$ zó dat $\varepsilon = \alpha^\lambda$. Laat de kanonieke faktorisatie van $\alpha \mathcal{O}_L$ gegeven zijn door :

$$\alpha.\mathcal{O}_L = \prod_p P_p^{g_p(\sigma)} \quad \text{(met } g_p(\sigma) \text{ zoals hoger).}$$

Uit "$\alpha^\lambda \in U_L$" volgt dan : $(\alpha\mathcal{O}_L)^\sigma = \alpha\mathcal{O}_L$, of :

$$\prod_p P_p^{g_p(\sigma)} = \left(\prod_p P_p^{g_p(\sigma)}\right)^\sigma = \prod_p P_p^{g_p(\sigma).\sigma} \quad .$$

Aangezien $P^{\sigma^{r_p}} = P$, heeft de exponent $g_p(\sigma).\sigma$, als element van $\mathbb{Z}[G]$, op P_p dezelfde werking als de exponent :

$$a_{p,0}\sigma + a_{p,1}\sigma^2 + \ldots + a_{p,r_p-2}\sigma^{r_p-1} + a_{p,r_p-1},$$

waaruit, wegens de uniciteit van de coëfficiënten $a_{p,i}$ volgt :

$$a_{p,0} = a_{p,1} = \ldots = a_{p,r_p-1} = a_p.$$

Dit betekent dat de kanonieke faktorisatie van $\alpha.\mathcal{O}_L$ in L van de volgende gedaante is :

$$\alpha.\mathcal{O}_L = \prod_p \left(P_p^{1+\sigma+\sigma^2+\ldots+\sigma^{r_p-1}}\right)^{a_p}.$$

Zij $v_{L/K}$ de globale ramifikatie-index van de uitbreiding L/K. Hier geldt (wegens IV.2.1., opmerking 3.) :

$$v_{L/K} = \prod_p e_p.$$

Er volgt dan :

$$(\alpha.\mathcal{O}_L)^{v_{L/K}} = \prod_p \left[\left(P_p^{1+\sigma+\ldots+\sigma^{r_p-1}}\right)^{e_p}\right]^{\frac{a_p v_{L/K}}{e_p}} ; \quad \frac{a_p.v_{L/K}}{e_p} \in \mathbb{Z}.$$

Uit (1) volgt dan (waarbij $b_p = a_p.v_{L/K}.e_p^{-1}$) :

$$(\alpha.\mathcal{O}_L)^{v_{L/K}} = \prod_p p^{b_p}, \in I_K.$$

Verder geldt :

$$I_K^{h_K} \subset P_K,$$

zodat uiteindelijk :

$$(\alpha.\mathcal{O}_L)^{h_K.v_{L/K}} \in P_K.$$

Er bestaat bijgevolg een element $a \in K^*$ zó dat :

$$(\alpha.\mathcal{O}_L)^{h_K.v_{L/K}} = a.\mathcal{O}_L = \alpha^{h_K.v_{L/K}}.\mathcal{O}_L,$$

waaruit

$$\alpha^{h_K v_{L/K}} = \varepsilon.a,$$

voor een $\varepsilon \in U_L$. Dus $\alpha \in R_L(U_L K^*)$, wat de omgekeerde inklusie bewijst.

<u>Gevolg</u>. Er geldt : $Q_L(U_L K^*) = ((U_L)_N : (U_L)^\lambda)$.

Men ziet dus dat $Q_L(U_L K^*)$ niet anders is dan de noemer van het Herbrand quotiënt van U_L als G-groep. Aangezien $(U_L)_\lambda = (\mathrm{Ker}\ \lambda) \cap U_L = K^* \cap U_L = U_K$ geeft dit met stelling V.1.1.2. :

STELLING V.1.3.2. *Er geldt :*

$$Q_L(U_L K^*) = \frac{n.(U_K : N(U_K))}{\prod\limits_{v \in S_0} N_v} .$$

Opmerking 1. In deze uitdrukking voor $Q_L(U_L K^*)$ kan het resultaat van stelling IV.2.4.1. gedeeltelijk teruggevonden worden in die zin, dat elke priemdeler p van $Q_L(U_L K^*)$ een deler is van n. Het is immers niet moeilijk in te zien dat de index $(U_K : N(U_L))$ een deler zal zijn van n^s, waarbij s het aantal elementen van S_0 voorstelt. Dit tonen we als volgt aan :

- de index $(U_K : N(U_L))$ is duidelijk een deler van $(U_K : N(U_K)) = (U_K : U_K^n)$.
- Anderzijds volgt uit Dirichlet's stelling :

  $$U_K = W_K \times F_K,$$

  waarbij F_K een vrije abelse groep is van rang s-1.
- Er geldt dus :

  $$U_K^n = W_K^n \times F_K^n,$$

  waaruit volgt :

  $$(U_K : U_K^n) = (W_K : W_K^n).(F_K : F_K^n).$$

- Het is duidelijk dat $(F_K : F_K^n) = n^{s-1}$. Verder volgt uit V.1.2. (zie de exakte rij op blz. 86) :

$$(W_K : W_K^n) = (W_K : N(W_K)) = (W_{K,n} : 1) \mid n,$$

wat uiteindelijk het gestelde bewijst.

Opmerking 2. De faktor $\prod_{v \in S_0} N_v$ is steeds een macht van twee, aangezien N_v voor elke $v \in S_0$ slechts de waarde 1 of 2 kan hebben (zie I.2.2.). Is dus n oneven, dan zal de teller in de uitdrukking voor $Q_L(U_L K^*)$ oneven zijn (voorgaande opmerking), zodat de noemer dan de waarde 1 zal hebben. Men kan dit echter ook onmiddellijk afleiden uit het volgende. Is $N_v = 2$ voor een $v \in S_0$, dan zal er een inbedding α van L in $\mathbb{C}$ bestaan waarvoor geldt : $\alpha(L) \not\subset \mathbb{R}$; $\alpha(K) \subset \mathbb{R}$. Daar L/K cyclisch is heeft men dat de uitbreiding $\alpha(L)/\alpha(K)$ de komplexe toevoeging J als automorfisme moet bezitten. Wegens $J^2 = id_{\mathbb{C}}$ heeft men : n even, Q.E.D..

STELLING V.1.3.3. *Is* L/K *een cyclische uitbreiding waarvan de graad deelbaar is door een oneven priemgetal, dan is* $Q_L(U_L K^*) \neq 1$. *Met andere woorden : er bestaat een eenheid van* L *wiens norm* 1 *is, en die niet van de vorm* $\varepsilon^{1-\sigma}$ *is, voor een* $\varepsilon \in U_L$.

BEWIJS. Is p een oneven priemgetal dat de graad n van de uitbreiding L/K deelt, dan ziet men dat in de teller van de uitdrukking voor $Q_L(U_L K^*)$ dit priemgetal voorkomt. Het kan, wegens voorgaande opmerking, niet door een faktor in de noemer weggedeeld worden.

Dit resultaat voor $n = p$, een oneven priemgetal is Hilbert's stelling 92 in [15]. Aangezien Hilbert's stelling 94 in [15] op deze stelling steunt kunnen we eveneens een veralgemening ervan als volgt formuleren :

STELLING V.1.3.4. *Is* L/K *een cyclische uitbreiding waarvan de*

graad deelbaar is door een oneven priemgetal, en is er geen enkel priemideaal van K dat vertakt in L, dan is er steeds een ideaal van K, dat geen hoofdideaal is van K, dat hoofdideaal wordt in L. Het klassegetal van K is dan deelbaar door dat oneven priemgetal.

BEWIJS. Wegens het feit dat L/K onvertakt is geldt : $v_{L/K} = 1$. Het diagram in stelling IV.2.4.2. leert ons dan :

$$Q_L(U_L K^*) = (P_L \cap I_K : P_K).$$

Wegens voorgaande stelling is deze index deelbaar door alle oneven priemfaktoren van n. Aangezien verder $(P_L \cap I_K : P_K)$ een deler is van h_K, is ook het laatste deel van de stelling bewezen.

Indien n = p, een oneven priemgetal is, kan men $Q_L(U_L K^*)$ eveneens interpreteren in termen van representatietheorie. We verwijzen de lezer hiervoor naar [22]

Is n niet deelbaar door een oneven priemgetal, dan is de voorgaande stelling niet geldig. Bijvoorbeeld, is $K = \mathbb{Q}(\sqrt{6})$ en $L = K(\sqrt{-3}) = \mathbb{Q}(\sqrt{6},\sqrt{-2},\sqrt{-3})$, dan kan men, met behulp van I.1.4. (2), onmiddellijk verifiëren dat alle priemdelers van K onvertakt zijn in L. Nochtans is $h_K = 1$. De reden zit hier in het vertakt zijn van de archimedische valuaties van K. Men heeft echter algemeen :

STELLING V.1.3.5. *Is* L *een cyclische uitbreiding van* K *met graad* n, *waarin elke valuatie van* K *onvertakt is, dan is er steeds een ideaal van* K *dat geen hoofdideaal is in* K *maar wel hoofdideaal in* L. *Het klassegetal van* K *is dan deelbaar door* n.

BEWIJS. De noemer in de uitdrukking voor $Q_L(U_L K^*)$ is dan 1, zodat

$Q_L(U_L K^*)$ deelbaar is door n. De rest volgt dan uit het diagram van stelling IV.2.4.2..

Opmerking. De veralgemening van Hilbert's stellingen 92 en 94 vindt men reeds in [5], chap. IV, (zie voornamelijk p. 402, voetnoot). De aldaar gevolgde weg is in wezen niet verschillend van de onze. Chevalley's resultaat steunt nl. op Herbrand's eenhedenstelling die we hier in beknopte vorm onder stelling V.1.1.2. weergegeven hebben. Essentieel is hier evenwel het gebruik van het radikaal van $U_L K^*$ in L^*, wat ons toelaat Chevalley's methode op bepaalde plaatsen wat eenvoudiger te formuleren. Ter illustratie daarvan tonen we in wat volgt de formule voor het inertie-klassegetal aan.

.4. De index $Q_L(U_L K^*)$ en de inerte ideaalklassen van L.

DEFINITIE V.1.4.1. Een ideaal A van L wordt inert *) genoemd als : $A^\sigma = A$.

Het aantal ideaalklassen van L die een inert ideaal bevatten zal thans berekend worden.

Het is duidelijk dat de inerte idealen een deelgroep van I_L vormen. Laten we deze deelgroep met $I_{L/K}$ aanduiden. Het aantal ideaalklassen van L die een inert ideaal bevatten is dus niets anders dan de index :

$$(I_{L/K} P_L : P_L).$$

Zij verder het getal $a_{L/K}$ zoals in stelling IV.2.2.2..

---

*) F : Ambige; E : Ambiguous.

STELLING V.1.4.1. *Het aantal ideaalklassen van* L *die een inert ideaal bevatten is gelijk aan* $a_{L/K}$.

BEWIJS. Zij A een ideaal van L, en veronderstel dat zijn kanonieke faktorisatie in L gegeven is door :

$$A = \prod_p P_p^{g_p(\sigma)}$$

(in de notatie van V.1.3.).

Indien $A^\sigma = A$, dan leert het bewijs van stelling V.1.3.1. ons dat $A \in R_{I_L}(I_K)$.

Omgekeerd, stel : $A \in R_{I_L}(I_K)$, en zij $m \in \mathbb{N}_0$ zó dat $A^m \in I_K$. Er geldt dus voor de kanonieke faktorisatie van A^m in K :

$$(\prod_p P_p^{g_p(\sigma)})^m = \prod_p p^{m_p},$$

waaruit volgt :

$$mg_p(\sigma) = m.a_{p,0} + m.a_{p,1}\sigma + \ldots + m.a_{p,r_p-1}\sigma^{r_p-1}$$

$$= m_p e_p + m_p e_p \sigma + \ldots + m_p e_p \sigma^{r_p-1}.$$

Dit impliceert klaarblijkelijk :

$$a_{p,0} = a_{p,1} = \ldots = a_{p,r_p-1} = \text{zegge : } a_p.$$

Dus;

$$A = \prod_p (P_p^{1+\sigma+\ldots+\sigma^{r_p-1}})^{a_p},$$

waaruit men zonder moeite de gelijkheid : $A^\sigma = A$ afleidt. Dit bewijst dus dat $I_{L/K}$ niets anders is dan $R_{I_L}(I_K)$, en uit de definitie van $a_{L/K}$ volgt dan het gestelde.

Gevolg. Er geldt :

$$a_{L/K} = \frac{h_K \cdot v_{L/K} \cdot \prod_{v \in S_0} N_v}{n.(U_K : N(U_L))} .$$

BEWIJS. Het volstaat stelling V.1.3.2. met stelling IV.2.2.2. te kombineren.

We merken thans op dat de groep G werkt op de ideaalklassengroep van L. Is namelijk A een representant voor een ideaalklasse, dan wordt de aktie van σ op de ideaalklasse $A.P_L$ gegeven door :

$$\sigma(A.P_L) = (A.P_L)^\sigma = A^\sigma.P_L.$$

Het is duidelijk dat de keuze van de representant A geen invloed heeft op de definitie van deze aktie.

DEFINITIE V.1.4.2. Een ideaalklasse A van L wordt inert genoemd als $A^\sigma = A$.

DEFINITIE V.1.4.3. Het aantal inerte ideaalklassen van L wordt het inertie-klassegetal van L genoemd en met $h_{L/K}$ aangeduid.

STELLING V.1.4.2. (Chevalley's formule). *Het inertie-klassegetal voldoet aan de betrekking :*

$$h_{L/K} = \frac{h_K \cdot v_{L/K} \cdot \prod_{v \in S_0} N_v}{n.(U_K : U_K \cap N(L^*))} .$$

BEWIJS. Zij $A_{L/K}$ de deelgroep van I_L bestaande uit alle idealen A van L met de eigenschap :

$$A^{1-\sigma} \in P_L.$$

Het is overduidelijk dat $P_L \subset A_{L/K}$ en dat $h_{L/K} = (A_{L/K} : P_L)$.

We passen thans Lemma III.3.1., gevolg, toe waarbij $A = A_{L/K}$, $B = P_L$ en $f = \lambda$ ($\lambda : I_L/P_L \to I_L/P_L$ met de betekenis van in V.1.1.). Met $(A_{L/K})_\lambda = I_{L/K}$ vindt men dan :

$$(1) \qquad (A_{L/K} : P_L) = (A_{L/K}^{\lambda} : P_L^{\lambda}).(I_{L/K} : P_L \cap I_{L/K}).$$

Uit voorgaande stelling halen we onmiddellijk :

$$(I_{L/K} : P_L \cap I_{L/K}) = (I_{L/K}.P_L : P_L) = a_{L/K}.$$

Wat betreft $A_{L/K}^{\lambda}$ zij opgemerkt dat $I_{L/K}$ niets anders is dan $\lambda^{-1}(P_L)$ (de λ die hier staat gaat van I_L naar I_L). Bijgevolg geldt :

$$I_{L/K}^{\lambda} = P_L \cap I_L^{\lambda}.$$

Beschouwen we thans de deelgroep $\Theta_{L/K}$ van L^* bestaande uit alle elementen van L^* wiens norm een eenheid is. Met andere woorden :

$$\Theta_{L/K} = N^{-1}(U_K).$$

Zij verder $\phi_L : L^* \to P_L$; $\phi_L(\alpha) = \alpha.\mathcal{O}_L$. We beweren thans :

$$\Theta_{L/K} = \phi_L^{-1} = (P_L \cap I_L^{\lambda}).$$

Inderdaad, zij $\alpha \in L^*$ zó dat $\phi_L(\alpha) = \alpha.\mathcal{O}_L = A^{1-\sigma}$ voor een ideaal A van L. Aangezien :

$$N(\alpha)\mathcal{O}_K = N_{L/K}(A^{1-\sigma}) = \mathcal{O}_K, \qquad \text{(zie I.1.2.)},$$

heeft men onmiddellijk : $N(\alpha) \in U_K$, i.e. : $\alpha \in \Theta_{L/K}$. Omgekeerd, zij $\alpha \in \Theta_{L/K}$, en zij

$$\alpha.\mathcal{O}_L = \prod_p P_p^{g_p(\sigma)}$$

de kanonieke faktorisatie van $\alpha.\mathcal{O}_L$ in L in de notatie van V.1.3.. Neemt men hier de norm van beide leden, rekening houdend met het feit dat $N(\alpha) \in U_K$, dan bekomt men :

(2) $$N_{L/K}(\alpha \mathcal{O}_L) = N(\alpha)\mathcal{O}_K = \mathcal{O}_K = \prod_p N_{L/K}(P_p^{g_p(\sigma)}).$$

Nu geldt (zie I.1.2.), voor elk priemideaal P' boven p :

$$N_{L/K}(P') = p^{f_p},$$

waarin f_p de restklassengraad van p in L is. Dus, indien $g_p(\sigma)$ is zoals in V.1.3., wordt (2) :

$$N_{L/K}(\alpha \mathcal{O}_L) = \mathcal{O}_K = \prod_p p^{(a_{p,0}+a_{p,1}+\ldots+a_{p,r_p-1})f_p}.$$

Hieruit volgt :

$$\sum_{i=0}^{r_p-1} a_{p,i} = 0.$$

Dit betekent echter dat het element $g_p(\sigma)$ van $\mathbb{Z}[G]$ kan geschreven worden als :

$$g_p(\sigma) = h_p(\sigma).(1-\sigma),$$

met $h_p(\sigma) \in \mathbb{Z}[G]$.
Voor het ideaal $\alpha.\mathcal{O}_L$ betekent dit :

$$\alpha.\mathcal{O}_L = (\prod_p P_p^{h_p(\sigma)})^{1-\sigma} \in I_L^{\lambda},$$

wat onze bewering bewijst.
We kunnen nu opnieuw lemma III.3.1. toepassen, met $A = \Theta_{L/K}$; $B = \phi_L^{-1}(P_L^{\lambda}) = U_L.L^{*\lambda}$, $f = \phi_L$. Dat levert ons volgende gelijkheid op :

$$(I_L^{\lambda} \cap P_L : P_L^{\lambda}) = (\Theta_{L/K} : U_L.L^{*\lambda}).$$

De laatste index kan men dan weerom met behulp van lemma III.3.1. (waarbij $A = \Theta_{L/K}$; $B = U_L.L^{*\lambda}$; $f = N$) omrekenen als volgt :

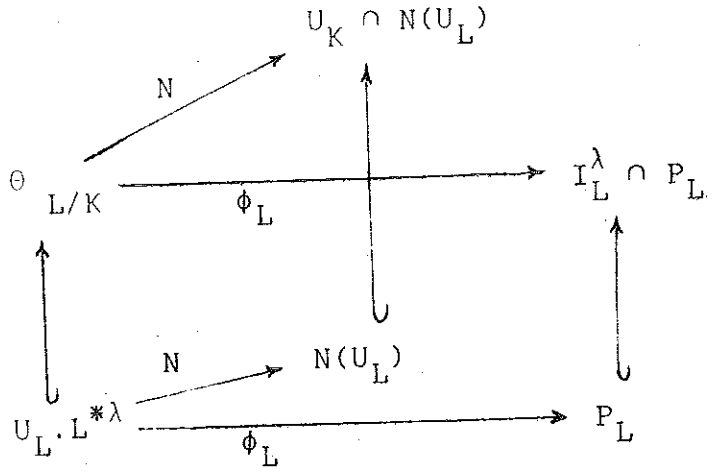
- $(\Theta_{L/K})_N = \text{Ker } N \cap (\Theta_{L/K})_N = \text{Ker } N$ (aangezien $\text{Ker } N \subset \Theta_{L/K}$)
- $(U_L.L^{*\lambda})_N = L^{*\lambda} = \text{Ker } N$, wegens stelling III.3.2.1.

Dus geldt :

$$(\Theta_{L/K} : U_L.L^{*\lambda}) = (N(\Theta_{L/K}) : N(U_L.L^{*\lambda}))$$
$$= (U_K \cap N(L^*) : N(U_L)).$$

Vult men dit in de formule (1), en houdt men rekening met de formule voor $a_{L/K}$ in de voorgaande stelling, dan bekomt men het gestelde.

De isomorfismen die men in het bewijs ontmoet vindt men terug in volgend diagram :



Hierin zijn de vertikale pijlen de natuurlijke inklusies : dat ze evenwijdig getekend zijn duidt op het isomorf zijn van de quotiëntgroepen gevormd door de bovenste groep te delen door de onderste.

Gevolg. Er geldt :

$$h_{L/K} = h_K \cdot \frac{Q_{I_L}(I_K)}{Q_{P_L}(P_K)} \cdot (N(L^*) \cap U_K : N(U_K)).$$

Dit leidt men af uit de definitie van $v_{L/K}$ en het resultaat van

stelling V.1.3.2., waarbij gebruik gemaakt wordt van de relatie

$$(U_K : N(U_K)) = (U_K : N(L^*) \cap U_K).(N(L^*) \cap U_K : N(U_K)).$$

De formule van Chevalley vindt belangrijke toepassingen in de studie van de ideaalklassengroepen van de velden K en L. We verwijzen de lezer o.m. naar [9] en [13], en naar het laatste paragraaf waar we de meest klassieke toepassing zullen uiteenzetten.

§2. KWADRATISCHE UITBREIDINGEN VAN EEN GETALLENVELD

Doorheen deze paragraaf zal K een getallenveld van graad m zijn over $\mathbb{Q}$. Het getallenveld L is kwadratisch over K, i.e. : $L = K(\sqrt{\mu})$ voor een $\mu \in K^*$, $\mu \notin K^{*2}$. De uitbreiding L/K is klaarblijkelijk cyclisch, en zijn galoisgroep is $\{1,\sigma\}$, waarbij σ het automorfisme is van L over K dat $\sqrt{\mu}$ afbeeldt in $-\sqrt{\mu}$.

2.1. De relatieve regulator.

Zij F de verzameling van alle inbeddingen van L in $\mathbb{C}$. Het is duidelijk dat $\# F = 2m$. Verder geldt dat er voor elke $\alpha \in F$ één en slechts één β van F, verschillend van α, bestaat zodanig dat $\alpha|K = \beta|K$. Dit element β is namelijk niets anders dan de inbedding $\alpha \circ \sigma$. We noteren :

$$\alpha^* = \alpha \circ \sigma.$$

Zij F_1 de verzameling van alle reële inbeddingen van L in $\mathbb{C}$, m.a.w. :

$$F_1 = \{\alpha | \alpha \in F \text{ en } \alpha(L) \subset \mathbb{R}\}.$$

Het is duidelijk dat $\alpha \in F_1 \Leftrightarrow \alpha^* \in F_1$, zodat we F_1 kunnen schrijven als

$$F_1 = \{\sigma_1, \sigma_1^*, \sigma_2, \sigma_2^*, \ldots, \sigma_a, \sigma_a^*\}$$

Zij F_2 de verzameling van alle komplekse inbeddingen van L die de eigenschap hebben dat hun beperking tot K eveneens kompleks is, i.e. :

$$F_2 = \{\alpha | \alpha \in F;\ \alpha(L) \not\subset \mathbb{R} \text{ en } \alpha(K) \not\subset \mathbb{R}\}$$

Het is duidelijk dat F_2 met α ook de kompleks-toegevoegde $\bar{\alpha}$ van α bezit. Verder geldt :

$$\bar{\alpha}|K \neq \alpha|K,$$

aangezien $\alpha(K) \not\subset \mathbb{R}$. Men heeft eveneens : $\alpha \in F_2 \Leftrightarrow \alpha^* \in F_2$, en : $\alpha^* \neq \bar{\alpha}$. De vier elementen, α , $\bar{\alpha}$, α^* en $\bar{\alpha}^*$ zijn dus vier verschillende inbeddingen van L in $\mathbb{C}$. Men kan dus F_2 als volgt aangeven :

$$F_2 = \{\sigma_{a+1}, \bar{\sigma}_{a+1}, \sigma_{a+1}^*, \bar{\sigma}_{a+1}^*, \ldots, \sigma_{a+b}, \bar{\sigma}_{a+b}, \sigma_{a+b}^*, \bar{\sigma}_{a+b}^*\}$$

Tenslotte, zij F_3 de verzameling van alle komplekse inbeddingen van L waarvan de beperking tot K reëel is, i.e. :

$$F_3 = \{\alpha | \alpha \in F \text{ en } : \alpha(L) \not\subset \mathbb{R},\ \alpha(K) \subset \mathbb{R}\}$$

Hier geldt eveneens : $\alpha \in F_3 \Leftrightarrow \bar{\alpha} \in F_3$; in dit geval is $\bar{\alpha}$ echter niets ander dan α^*, aangezien $\bar{\alpha}|K = \alpha|K$. Bijgevolg kan F_3 aangegeven worden als volgt :

$$F_3 = \{\tau_1, \tau_1^*, \tau_2, \tau_2^*, \ldots, \tau_v, \tau_v^*\}, \text{ met } \tau_i^* = \bar{\tau}_i.$$

Klaarblijkelijk geldt : $F = F_1 \cup F_2 \cup F_3$ (disjunkt). In termen

van valuaties (zie I.2.2.) is v niets anders dan het aantal (niet-equivalente) archimedische valuaties van K die vertakken in L. Inderdaad, is w een valuatie van L geassocieerd aan een element uit F_1 of F_2, dan valt zijn vervollediging $\tilde{L}_w$ samen met de vervollediging $\tilde{K}_{w|K}$ van K t.o.v. $w|K$, terwijl dit niet meer het geval is voor een valuatie geassocieerd aan een element uit F_3, aangezien $\tilde{L}_w = \mathbb{C}$ en $\tilde{K}_{w|K} = \mathbb{R}$.
We zien verder dat het aantal reëele inbeddingen van L gelijk is aan $2a$, terwijl het aantal komplekse gelijk is aan $4b+2v$. De vrije groep U_L/W_L is dus van rang $2a+2b+v-1$ (zie I.3.1.). Verder vindt men gemakkelijk de reëele inbeddingen van K, nl. :

$$\sigma_{1|K},\cdots,\sigma_{a|K};\quad \tau_{1|K},\ \tau_{2|K},\cdots,\tau_{v|K}.$$

De komplekse zijn dan :

$$\sigma_{a+1|K},\bar{\sigma}_{a+1|K},\sigma_{a+2|K},\bar{\sigma}_{a+1|K},\cdots,\sigma_{a+b|K},\bar{\sigma}_{a+b|K}$$

Dit betekent dat de vrije groep U_K/W_K van rang $a+b+v-1$ is.

Teneinde de notaties wat in te korten stellen we verder :

- $a+v+b-1 = d$
- $2a+2b+v-1 = t$
- $a+b = u$,

waarbij op te merken valt dat :

$$t - d = u.$$

Een relatief fundamenteel systeem van eenheden voor L/K (zie definitie II.1.2.2.) zal dus steeds u elementen bevatten (zie stelling IV.1.2.).

DEFINITIE V.2.1. Zij $\Delta = \{\delta_1,\ldots,\delta_u\}$ een relatief fundamenteel systeem van eenheden voor L/K. De relatieve regulator van Δ is de absolute waarde van de determinant :

$$\begin{vmatrix} \ln|\sigma_1(\delta_1^\lambda)| & \ldots & \ln|\sigma_a(\delta_1^\lambda)| & 2\ln|\sigma_{a+1}(\delta_1^\lambda)| & \ldots & 2\ln|\sigma_u(\delta_1^\lambda)| \\ \\ \ln|\sigma_1(\delta_u^\lambda)| & \ldots & \ln|\sigma_a(\delta_u^\lambda)| & 2\ln|\sigma_{a+1}(\delta_u^\lambda)| & \ldots & 2\ln|\sigma_u(\delta_u^\lambda)| \end{vmatrix}$$

(waarin λ dezelfde betekenis heeft als in §1, i.e. : $\lambda(\xi) = \xi^\lambda = \xi^{1-\sigma}$). We noteren de relatieve regulator van Δ als $R_{L/K}(\Delta)$.

STELLING V.2.1. *Voor elk relatief fundamenteel systeem van eenheden* $\{\delta_1,\ldots,\delta_u\} = \Delta$ *voor* L/K *geldt :*

$$R_{L/K}(\Delta) = \frac{q_L(U_K).R_L}{2^{v-1}\,R_K},$$

waarbij R_K *en* R_L *de (klassieke) regulatoren van* K, *resp.* L *zijn. De relatieve regulator is dus onafhankelijke van de keuze van het relatief fundamenteel systeem van eenheden* Δ.

BEWIJS. Wegens stelling IV.1.2.2. bestaat er een fundamenteel systeem van eenheden $\{\eta_1,\ldots,\eta_d\}$ voor K en een fundamenteel systeem $\{\varepsilon_1,\ldots,\varepsilon_d, \varepsilon_{d+1},\ldots,\varepsilon_t\}$ van eenheden voor L, zódanig dat volgende relaties gelden :

$$(1) \qquad \begin{cases} \eta_1 = \zeta_1\varepsilon_1^{a_1} \\ \quad \ldots \\ \eta_d = \zeta_d\varepsilon_d^{a_d}, \end{cases}$$

waarin $\zeta_i \in W_L$ en $a_i \in \mathbb{N}_0$ voor $i = 1,2,\ldots,d$. Hierbij is, wegens voornoemde stelling :

$$(2) \qquad a_1a_2\ldots a_d = q_L(U_K) = q.$$

Vooraleer de berekening van $R_{L/K}(\Delta)$ aan te vatten, voeren we nog de volgende notaties in :

- voor $j = 1,2,\ldots,t$ en $i = 1,2,\ldots,u$ stellen we :

$$S_j^i = m_i \ln|\sigma_i(\varepsilon_j)|$$

(3)

$$S_j^{*i} = m_i \ln|\sigma_i^*(\varepsilon_j)|,$$

waarbij

$$m_i = \begin{cases} 1 & \text{voor} \quad i = 1,2,\ldots,a \\ 2 & \text{voor} \quad i = a+1,\ldots,u \ ; \end{cases}$$

Dit betekent niet anders dan dat m_i de lokale graad is van de archimedische valuatie : $\xi \to |\sigma_i(\xi)|$ van K in L.

- voor $j = 1,2,\ldots,t$ en $i = 1,2,\ldots,v$ stellen we :

(3') $$T_j^i = 2\ln|\tau_i(\varepsilon_j)| \quad .$$

Met deze notatie kunnen we de regulator van L als volgt schrijven :

(4) $$R_L = \left|\begin{vmatrix} S_1^2 & \ldots & S_1^u & S_1^{*1} & \ldots & S_1^{*u} & T_1^1 & \ldots & T_1^v \\ . & \ldots & . & . & \ldots & . & . & \ldots & . \\ S_t^2 & \ldots & S_t^u & S_t^{*1} & \ldots & S_t^{*u} & T_t^1 & \ldots & T_1^v \end{vmatrix}\right|$$

(de buitenste streepjes duiden op de absolute waarde).

Wat betreft de regulator van K noteren we het volgende :

- voor elke $\alpha \in F$ en elke $j \in \{1,2,\ldots,d\}$ geldt :

$$\ln|\alpha(\eta_j)| = \ln|\alpha(\zeta_j \varepsilon_j^{a_j})| = \ln|\alpha(\zeta_j).\alpha(\varepsilon_j)^{a_j}| =$$

$$\ln|\alpha(\zeta_j)| + a_j \ln|\alpha(\varepsilon_j)|.$$

In deze laatste som vervalt de eerste term aangezien $\alpha(\zeta_j)$ een

eenheidswortel is, waardoor $|\alpha(\zeta_j)|$ gelijk aan 1 is.

- Hieruit volgt :

$$(5)\qquad \begin{aligned} m_i \ln|\sigma_i(\eta_j)| &= a_j S_j^i \quad \text{voor } i = 1,2,\ldots,u \ ; \ j = 1,\ldots,d \\ \ln|\tau_i(\eta_j)| &= \tfrac{1}{2} a_j T_j^i \quad \text{voor } i = 1,2,\ldots,v \ ; \ j = 1,\ldots,d \end{aligned}$$

De regulator van K kan dus, gebruik makend van (1), als volgt geschreven worden :

$$R_K = \frac{q}{2^v} \cdot \left| \begin{vmatrix} S_1^2 & \ldots & S_1^u & T_1^1 & \ldots & T_1^v \\ . & \ldots & . & . & \ldots & . \\ S_d^2 & \ldots & S_d^u & T_d^1 & \ldots & T_d^v \end{vmatrix} \right|$$

Verder volgt uit (5) en uit het feit dat $\alpha^*|K = \alpha|K$ voor alle $\alpha \in F$:

$$S_j^i = S_j^{*i}$$

voor $i = 1,2,\ldots,u$ en $j = 1,2,\ldots,d$. Dit geeft in (4), na van elke i^{de} kolom ($i = 1,2,\ldots,a-1$) de $(a+i)^{de}$ te hebben afgetrokken :

$$(7)\quad R_L = \begin{vmatrix} 0 & \ldots & 0 & S_1^1 & \ldots & S_1^u & T_1^1 & \ldots & T_1^v \\ . & \ldots & . & . & \ldots & . & . & \ldots & . \\ 0 & \ldots & 0 & S_d^1 & \ldots & S_d^u & T_d^1 & \ldots & T_d^v \\ \overset{\circ}{S}{}_{d+1}^2 & \ldots & \overset{\circ}{S}{}_{d+1}^u & S_{d+1}^{*1} & \ldots & S_{d+1}^{*u} & T_{d+1}^1 & \ldots & T_{d+1}^v \\ . & \ldots & . & . & \ldots & . & . & \ldots & . \\ \overset{\circ}{S}{}_t^1 & \ldots & \overset{\circ}{S}{}_t^u & S_t^{*1} & \ldots & S_t^{*u} & T_t^1 & \ldots & T_t^v \end{vmatrix} ,$$

waarin voor $j = d+1,d+2,\ldots,t$ en $i = 2,3,\ldots,u$:

$$\overset{\circ}{S}{}_j^i = S_j^i - S_j^{*i}.$$

Verder geldt voor $j = 1,2,\ldots,d$:

$$\sum_{i=1}^{u} S_j^i + \frac{1}{2} \sum_{i=1}^{v} T_j^i = 0.$$

Dit volgt onmiddellijk uit het feit dat voor $j = 1,2,\ldots,d$:

$$1 = |N_{K/\mathbb{Q}}(\eta_j)| = |\prod_{\alpha} \alpha(\eta_j)|,$$

waarbij, in het produkt, α alle inbeddingen van K in $\mathbb{C}$ doorloopt. Dit laat ons toe de determinant in (7) te schrijven als volgt :

$$\begin{vmatrix} 0 & \ldots & 0 & 0 & S_1^2 & \ldots & S_1^u & T_1^1 & \ldots & T_1^v \\ 0 & \ldots & 0 & 0 & S_d^2 & \ldots & S_d^u & T_d^1 & \ldots & T_d^v \\ \overset{\circ}{S}{}_{d+1}^2 & \ldots & \overset{\circ}{S}{}_{d+1}^u & M_{d+1} & S_{d+1}^2 & \ldots & S_{d+1}^u & T_{d+1}^1 & \ldots & T_{d+1}^u \\ \overset{\circ}{S}{}_t^2 & \ldots & \overset{\circ}{S}{}_t^u & M_t & S_t^2 & \ldots & S_t^u & T_t^1 & \ldots & T_t^v \end{vmatrix},$$

waarbij, voor $j = d+1,\ldots,t$:

$$(8) \qquad M_j = \sum_{i=1}^{u} S_j^i + \frac{1}{2} \sum_{i=1}^{v} T_j^i.$$

Deze determinant is nu van het type :

$$\begin{vmatrix} 0 & A \\ B & C \end{vmatrix},$$

waarbij A een $d \times d$-matrix is en B een $u \times u$-matrix. Het is welbekend dat voor dergelijke determinanten geldt :

$$(9) \qquad \left|\begin{vmatrix} 0 & A \\ B & C \end{vmatrix}\right| = |\det(A)|.|\det(B)|.$$

Hierbij is $|\det(A)|$ echter niets anders dan $2^v.q^{-1}R_K$ (zie : (6)). Wat betreft $|\det(B)|$ geldt :

$$(10) \qquad \det(B) = \begin{vmatrix} \overset{\circ}{S}{}^{2}_{d+1} & \cdots & \overset{\circ}{S}{}^{u}_{d+1} & M_{d+1} \\ \cdot & \cdots & \cdot & \cdot \\ \overset{\circ}{S}{}^{2}_{t} & \cdots & \overset{\circ}{S}{}^{2}_{t} & M_{t} \end{vmatrix} .$$

Beschouw dan de relatie :

$$\ln(|N_{L/\mathbb{Q}}(\varepsilon_i)|) = 0 \quad \text{voor } i = 1,2,\ldots,t,$$

dan bekomt men :

$$\sum_{i=1}^{u} S_j^i + \sum_{i=1}^{u} S_j^{*i} + \sum_{i=1}^{v} T_j^i = 0.$$

Gebruikt men hierbij (8), dan volgt :

$$M_j = \frac{1}{2}\left(\sum_{i=1}^{u} (S_j^{*i} - S_j^i)\right) = -\frac{1}{2} \sum_{i=1}^{u} \overset{\circ}{S}{}^{i}_{j} ,$$

(waarin vanzelfsprekend $\overset{\circ}{S}{}^{1}_{j}$ niets anders is dan $S_j^1 - S_j^{*1}$).

Hierdoor wordt (10), na een behoorlijke verwisseling van kolommen :

$$(11) \qquad |\det(B)| = \left|\begin{vmatrix} \overset{\circ}{S}{}^{1}_{d+1} & \cdots & \overset{\circ}{S}{}^{u}_{d+1} \\ & & \\ \overset{\circ}{S}{}^{1}_{t} & \cdots & \overset{\circ}{S}{}^{u}_{t} \end{vmatrix}\right| .$$

Men vindt hierin :

$$\overset{\circ}{S}{}^{i}_{j} = S_j^i - S_j^{*i} = m_i . \ln\left(\left|\frac{\sigma_i(\varepsilon_j)}{\sigma_i^*(\varepsilon_j)}\right|\right) ;$$

dit laatste is echter, wegens $\sigma_i^*(\varepsilon_j) = \sigma_i(\sigma(\varepsilon_j))$, niets anders dan $m_i \ln(|\sigma_i(\varepsilon_j^{\lambda})|)$. In (11) herkennen we dus de relatieve regulator $R_{L/K}(\varepsilon_{d+1},\ldots,\varepsilon_t)$, zodat uit (10) het bewijs van de stelling volgt.

Opmerking. Deze stelling laat ons toe voortaan over de relatieve regulator van de uitbreiding L/K te spreken in plaats van de relatieve regulator van een relatief fundamenteel systeem van eenheden

voor L/K. Is in het voorgaande u = 0, dan komt men overeen $R_{L/K}$ gelijk aan 1 te nemen. De relatie in de stelling blijft daarbij nog van kracht, zoals de lezer gemakkelijk kan nagaan. Op dit bijzonder geval komen we terug in V.2.3..

2.2. Het quotiënt h_L/h_K.

Hier zullen we de rol van de relatieve regulator in de analytische uitdrukking voor de verhouding h_L/h_K nader onderzoeken.

Wegens I.3.3. beschikken we over de volgende twee gelijkheden :

$$h_L = \frac{(W_L : 1)\sqrt{|D_L|}}{2^{2a+2b+v}\pi^{2b+v}R_L} \lim_{\substack{s\to 1\\ s>1}} \zeta_L(s).$$

$$h_K = \frac{(W_K : 1)\sqrt{|D_K|}}{2^{a+b+v}.\pi^b.R_K} \lim_{\substack{s\to 1\\ s>1}} \zeta_K(s).$$

Hierin zijn alle voorkomende notaties hoger gedefinieerd. Er geldt dus voor de verhouding h_L/h_K :

$$\frac{h_L}{h_K} = (W_L : W_K)\sqrt{\frac{|D_L|}{|D_K|}} \cdot \frac{R_L}{2^{a+b}\pi^{b+v}R_L} \cdot \lim_{\substack{s\to 1\\ s>1}} \frac{\zeta_L(s)}{\zeta_K(s)}$$

Met : $R_L = 2^{v-1}(q_L(U_K))^{-1} R_K R_{L/K}$ (stelling V.2.1.) wordt dit :

$$\frac{h_L}{h_K} = (W_L : W_K)\sqrt{\frac{|D_L|}{|D_K|}} \cdot \frac{q}{2^{a+b+v-1}\pi^{b+v}R_{L/K}} \lim_{\substack{s\to 1\\ s>1}} \frac{\zeta_L(s)}{\zeta_K(s)} .$$

De laatste limiet kan nog met behulp van Euler's identiteit (I.3.3.) omgekeerd worden. Men heeft nl., voor s > 1 :

$$(1)\qquad \begin{cases} \zeta_L(s) = \sum\limits_{A\in I_L'} \dfrac{1}{N_L(A)^s} = \prod\limits_{P\in Q_L} \left(1 - \dfrac{1}{N_L(P)^s}\right)^{-1} \\ \zeta_K(s) = \sum\limits_{a\in I_K'} \dfrac{1}{N_K(a)^s} = \prod\limits_{p\in Q_K} \left(1 - \dfrac{1}{N_K(p)^s}\right)^{-1}, \end{cases}$$

waarin I_L', (resp. I_K') de verzameling is van alle gehele idealen van L (resp. K) en Q_L (resp. Q_K) de verzameling is van alle priemidealen van L(resp. K). We krijgen dus :

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \prod_{p\in Q_K} c_p(s) ,$$

waarbij $c_p(s)$ gedefinieerd is als :

$$c_p(s) = \frac{1 - \dfrac{1}{N_K(p)^s}}{\prod\limits_{P|p} \left(1 - \dfrac{1}{N_L(P)^s}\right)} .$$

Dat het produkt $\prod\limits_p c_p(s)$ konvergeert volgt uit de absolute konvergentie van de produkten in (1). De waarde van $c_p(s)$ wordt verder bepaald door de aard van de kanonieke faktorisatie van p in L. Het is duidelijk dat er zich slechts drie gevallen kunnen voordoen, nl. :

(i). $p = P_1P_2$, $P_1 \neq P_2$: $f(P_i|p) = 1$, $N_{L/K}(P_i) = p$ voor $i = 1,2$.

In dit geval heeft men voor $i = 1,2$:

$$N_L(P_i) = N_K(N_{L/K}(P_i)) = N_K(p),$$

waaruit volgt :

$$c_p(s) = \left(1 - \frac{1}{N_K(p)^s}\right)^{-1} .$$

(ii). $p = P$; $f(P|p) = 2$; $N_{L/K}(P) = p^2$.

In dit geval geldt :

$$N_L(P) = N_K(N_{L/K}(P)) = N_K(p^2) = (N_K(p))^2,$$

waaruit volgt :

$$c_p(s) = (1 + \frac{1}{N_K(p)^1})^{-1}$$

(iii). $p = P^2$; $f(P|p) = 1$; $N_{L/K}(P) = p$.

In dit geval geldt :

$$N_L(P) = N_K(N_{L/K}(P)) = N_K(p),$$

zodat :

$$c_p(s) = 1.$$

We voeren nu het homomorfisme $\chi_{L/K} : I_L \to \{+1,-1\}$, in als volgt :

$$\chi_{L/K}(p) = \begin{cases} +1 & \text{indien (i) geldt} \\ -1 & \text{indien (ii) geldt} \\ 0 & \text{indien (iii) geldt} , \end{cases}$$

en we breiden deze funktie uit naar I_L door multiplikativiteit. Hierdoor kan $c_p(s)$ als volgt geschreven worden :

$$c_p(s) = (1 - \frac{\chi_{L/K}(p)}{N_K(p)^s})^{-1}$$

Het produkt $\prod_p c_p$ is echter een kontinue funktie van s in het interval (δ,∞), zodat men heeft :

$$\lim_{\substack{s\to 1 \\ s>1}} \frac{\zeta_L(s)}{\zeta_K(s)} = \prod_p \frac{1}{1 - \frac{\chi_{L/K}(p)}{N_K(p)^s}}$$

Dit laatste produkt staat bekend onder de benaming : de L-funktie voor het karakter $\chi_{L/K}$, en het wordt afgekort tot $L(s,\chi_{L/K})$. Voor $s > 0$ geldt verder nog :

$$L(s,\chi_{L/K}) = \sum_{a\in I_K'} \frac{\chi_{L/K}(a)}{N_K(a)^s} \quad ,$$

waarbij de laatste som uniform konvergeert in het interval $[\delta,\infty]$ voor elke $\delta \in \mathbb{R}$, $\delta > 0$.

Voor $h_L h_K^{-1}$ vinden we dan uiteindelijk, gebruik maken van het feit dat $(W_L : W_K)q_L(U_K) = Q_L(U_K)$ (zie stelling III.1.2.1.) :

$$\boxed{\frac{h_L}{h_K} = Q_L(U_K).\sqrt{\left|\frac{D_L}{D_K}\right|}\ \frac{L(1,\chi_{L/K})}{2^{d_\pi b+v} R_{L/K}}}$$

(Hierin is $d = a+b+v-1 = \text{rang}(U_K/W_K)$, zoals in het voorgaande punt).

Aangezien we in deze uitdrukking nagenoeg dezelfde "karakteristieken" aantreffen als in de gewone formule voor het klassegetal noemen we de verhouding h_L/h_K het relatieve klassegetal van de uitbreiding L/K.

2.3. Bijzonder geval.

DEFINITIE V.2.3. Een getallenveld F heet totaal-reëel als elke inbedding van F in $\mathbb{C}$ een reëel beeld heeft; is daarentegen het beeld van elke inbedding van F in $\mathbb{C}$ kompleks, dan noemt men F totaal-kompleks.

We veronderstellen thans dat in het voorgaande K totaal-reëel

is, terwijl L totaal-kompleks is. Voor het veld K betekent dit dat het van de gedaante $\mathbb{Q}(\theta)$ is, waarbij θ een wortel is van een irreduciebele polynoom $f(X) = irr(\theta,\mathbb{Q},X) \in \mathbb{Q}[X]$ die slechts reëele wortels bezit. Voor $L = K(\sqrt{\mu})$ betekent dit niets anders dan dat μ een element is van K dat door alle inbeddingen van K in $\mathbb{C}$ op een negatief reëel getal afgebeeld wordt. In de notatie van V.2.1. geeft dit :

$$\sigma_i(\mu) < 0 \quad \text{voor } i = 1,2,\ldots,a$$

$$\tau_j(\mu) < 0 \quad \text{voor } j = 1,2,\ldots,v$$

Het is echter duidelijk dat $a = 0 = b$. Dit betekent dat de vrije groepen U_L/W_L en U_K/W_K dezelfde rang hebben. Dus, U_L/U_K en U_L/W_LU_K zijn eindige groepen, zodat :

$$R_L(U_K) = R_{U_L}(U_K) \text{ (zie stelling IV.1.1.1.)} = R_{U_L}(U_KW_L)$$

$$= R_L(U_KW_L) = U_L.$$

Opmerking. De index $(U_L : W_LU_K)$ wordt de eenhedenindex (einheitenindex) genoemd. Het feit dat zijn waarde 1 of 2 is werd voor het eerst opgemerkt door Hasse in het geval dat L abels is over $\mathbb{Q}$ (zie [14], waar men tevens een uitvoerige behandeling van de rol die $q_L(U_K)$ speelt in het bepalen van het relatieve klassegetal aantreft). De uitbreiding naar willekeurige totaal-komplekse velden L die kwadratisch zijn over een totaal-reëel veld K vindt men in Uchida's recente werken over het klassegetal van komplekse abelse velden (zie [27] en [28]).

Wat betreft de relatieve regulator $R_{L/K}$ heeft men vanzelfsprekend :

$$R_{L/K} = 1$$

De formule voor het relatieve klassegetal luidt dus als volgt :

$$\frac{h_L}{h_K} = Q_L(U_K)\sqrt{\left|\frac{D_L}{D_K}\right|} \cdot \frac{1}{2^{v-1}\pi^v} L(1,\chi_{L/K}).$$

Deze uitdrukking is het uitgangspunt van een recent werk van Goldstein over het relatieve klassegetal, waarin –onder de voorwaarde dat K nog een deelveld K' bezit waarover K kwadratisch is– de faktor $L(1,\chi_{L/K})$ nog verder omgerekend wordt tot een eindige som (zie [12]).

§3. RADIKALEN IN KWADRATISCHE, BIKWADRATISCHE EN CYCLOTOME VELDEN

1. Kwadratische velden.

Zij $K = \mathbb{Q}(\sqrt{d})$, d een kwadraatvrij geheel getal. De notaties en konventies van de vorige hoofdstukken blijven ook hier van kracht.

We stellen on hier tot doel de grootheden $q_K(\mathbb{Q}^*)$, $q_K(U_{\mathbb{Q}})$, $q_{I_K}(I_{\mathbb{Q}})$, $q_{P_K}(P_{\mathbb{Q}})$ en $h_{K/\mathbb{Q}}$ te berekenen; de kennis van deze laatste zal ons dan toelaten een resultaat in verband met de pariteit van het klassegetal h_K van K af te leiden. Via de in hoofdstuk II uiteengezette theorie der bikwadratische velden zullen we dan zien dat dit resultaat equivalent is met een stelling uit de theorie van de klassenvelden (Classfield Theory).

Ons eerste resultaat luidt dan als volgt :

STELLING V.3.1.1. *Er geldt :*

$$q_K(\mathbb{Q}^*) = 2.$$

BEWIJS. Stelling V.1.2. geeft ons :

$$q_K(\mathbb{Q}^*) = (W_{\mathbb{Q}} : N(W_K))$$

(hier is N niets anders dan de norm van K tot $\mathbb{Q}$). Hierin is $W_{\mathbb{Q}} = \{+1,-1\}$. Het is verder gemakkelijk na te gaan dat men heeft : $N(W_L) = \{1\}$, waaruit het gestelde volgt.

Opmerking. Het is niet moeilijk een representant ρ in $R_K(\mathbb{Q}^*)$ voor de quotiëntgroep $R_K(\mathbb{Q}^*)/W_K\mathbb{Q}^*)$ te vinden. In de gevallen waarbij W_L slechts de elementen +1 en -1 bevat (i.e. : $W_K\mathbb{Q}^* = \mathbb{Q}^*$) kan men wegens de beschouwingen van hoofdstuk II, §2.1., $\rho = \sqrt{d}$ kiezen. Is $d = 3$, dan volgt uit $(\sqrt{-3})^2 \in \mathbb{Q}^2$ en $\sqrt{-3} \notin W_K\mathbb{Q}^*$ dat ook hier $\rho = \sqrt{d}$ kan genomen worden. De enige uitzondering ontmoet men dan voor $d = -1$; men heeft immers klaarblijkelijk : $\rho \neq \sqrt{-1}$. Wegens de gelijkheid :

$$(1 + i)^2 = 2i, \ (\in W_K\mathbb{Q}^*)$$

en het feit dat $1 + i \notin W_K\mathbb{Q}^*$ kan echter $\rho = 1 + i$ genomen worden.

Wat betreft $q_K(U_{\mathbb{Q}})$ noteren we eerst het volgende. Is L een getallenveld waarvoor geldt : $W_L = U_L$ (wat het geval is indien $L = \mathbb{Q}$ of indien L een imaginair kwadratisch veld is), en is F een willekeurige uitbreiding van L, dan is het duidelijk dat $R_F(U_L)$ niets anders kan zijn dan W_F. In ons geval, i.e. : $L = \mathbb{Q}$ en $F = \mathbb{Q}(\sqrt{d})$ leidt dit tot :

STELLING V.3.1.2. *Er geldt :*

$$q_K(U_{\mathbb{Q}}) = 1.$$

Wat betreft de index $q_{I_K}(I_{\mathbb{Q}}) = v_{K/\mathbb{Q}}$ noteerden we reeds eerder

dat deze gelijk is aan 2^t, waarbij t het aantal priemdelers van de diskriminant D_K van K is (zie : IV,2.1., opmerking 1). Wegens stelling II.1.1., gevolg, hebben we dan :

STELLING V.3.1.3. *Is r het aantal priemdelers van d, dan geldt :*

$$v_{K/\mathbb{Q}} = \begin{cases} 2^r & \text{indien } d \not\equiv 3 \pmod 4 \\ 2^{r+1} & \text{indien } d \equiv 3 \pmod 4. \end{cases}$$

We bereken thans de index $q_{P_K}(P_{\mathbb{Q}}) = Q_K(U_K\mathbb{Q}^*)$. In de formule van stelling V.1.3.2., i.e. :

$$Q_K(U_K\mathbb{Q}^*) = \frac{2.(U_{\mathbb{Q}} : N(U_K))}{\prod\limits_{v\in S_0} N_v}$$

is S_0 een singleton : het bestaat namelijk uit de gewone absolute waarde van $\mathbb{Q}$. Het produkt in de noemer bestaat dus uit één enkele term, N_v, en deze is wegens de definitie (zie I.3.2.) gelijk aan 2 indien d negatief is en gelijk aan 1 indien d positief is. Wat betreft de index $(U_{\mathbb{Q}} : N(U_K))$, deze is duidelijk gelijk aan 2 indien d negatief is, aangezien men in dat geval $U_{\mathbb{Q}} = W_{\mathbb{Q}}$ en $U_K = W_K$ heeft. Is $d > 0$, dan zal deze index gelijk zijn aan 2 indien de fundamentele eenheid η_K van K norm +1 heeft en gelijk aan 1 indien $N(\eta_K) = -1$. Samengevat levert dit :

STELLING V.3.1.4. *Er geldt :*

$$Q_K(U_K\mathbb{Q}^*) = \begin{cases} 2 & \textit{indien } d < 0 \textit{ of, indien } d > 0 \textit{ en } N(\eta_K) = -1 \\ 4 & \textit{indien } d > 0 \textit{ en } N(\eta_K) = +1. \end{cases}$$

Als $Q_K(U_K\mathbb{Q}^*)$ de waarde 2 heeft, dan is de struktuur van de quotiëntgroep $R_K(U_K\mathbb{Q}^*)/U_K\mathbb{Q}^*$ volledig bekend; als representant ervoor kan men dan dezelfde nemen als voor $R_K(\mathbb{Q}^*)/W_K\mathbb{Q}^*$. Is $Q_K(U_K\mathbb{Q}^*)$ gelijk aan 4, dan volgt uit stelling IV.2.4.1. dat de groep $R_K(U_K\mathbb{Q}^*)$ niets anders kan zijn dan de Viergroep van Klein. Ook hiervoor kan men representanten bepalen. Is namelijk $\rho = x + y\sqrt{d}$ $(x,y \in \mathbb{Q})$ er een, dan zal gelden :

$$\rho^2 = (x + y\sqrt{d})^2 = \eta_K^m Z,$$

voor een $m \in \mathbb{Z}$ en een $Z \in \mathbb{Q}^*$. Aangezien elk element uit $\rho U_K\mathbb{Q}^*$ representant is voor dezelfde klasse modulo $U_K\mathbb{Q}^*$ als ρ, mogen we veronderstellen dat aan één van de volgende twee vergelijkingen zal voldaan zijn :

(1) $\qquad \rho^2 = Z$

(2) $\qquad \rho^2 = \eta_K Z,$

waarin we Z kwadraatvrij kunnen onderstellen. Uit (1) volgt : $\rho = \pm\sqrt{Z}$, zodat Z slechts 1 of d kan zijn. Dit levert ons dan twee representanten op, nl. : 1 en $\sqrt{d}$. Wat betreft (2), stel $\eta_K = u + v\sqrt{d}$ (waarbij $u^2 - v^2d = 1$). Men heeft dan :

$$\begin{cases} x^2 + y^2d = u.Z \\ 2xy = v.Z \ . \end{cases}$$

Hieruit vindt men twee oplossingen voor x^2, i.e. :

$$x_1^2 = Z(\frac{u+1}{2}) \quad \text{en} \quad x_2^2 = Z(\frac{u-1}{2}).$$

Opdat de 1^e oplossing (resp. de 2^e) zou opgaan, zal Z dus het kwadraatvrij deel van het geheel getal 2(u+1) (resp. : 2(u-1)) moeten zijn, i.e. : $Z = 2(u+1)\xi_1^2$ (resp. : $Z = Z(u-1)\xi_2^2$), waarbij ξ_1 en ξ_2 gepaste rationale getallen zijn. Daaruit volgt dan :

$$x_1 = (u+1)\xi_1^2 \; ; \; y_1 = v\xi_1 \quad (\text{resp. } : x_2 = (u-1)\xi_2 \; ; \; y_2 = v\xi_2).$$

Hierdoor zijn twee andere representanten bepaald, nl. :

$$\rho_1 = u + 1 + v\sqrt{d} \quad \text{en} \quad \rho_2 = u - 1 + v\sqrt{d}.$$

Het is nuttig hier te wijzen op het feit dat de kennis van de representanten voor $R_K(U_K\mathbb{Q}^*)/U_K\mathbb{Q}^*$ erop neerkomt dat men zonder moeite de algemene gedaante van alle oplossingen x,y,Z in $\mathbb{Q}$ van vergelijkingen van de vorm :

$$(x + y\sqrt{d})^2 = \eta_K^m Z$$

kan neerschrijven.

We resumeren dit alles in :

STELLING V.1.3.5. *Is* K *een reëel kwadratisch veld met fundamentele eenheid* η_K, *dan geldt :* $N(\eta_K) = +1$ *dan en slechts dan als de vergelijking :* $\rho^2 = \eta_K.Z$ *oplosbaar is met* $\rho \in K^*$ *en* $Z \in \mathbb{Q}^*$. *In geval van oplosbaarheid zal het kwadraatvrije deel van* Z *dit zijn van* $2(u+1)$ *of* $2(u-1)$. *Omgekeerd, is* $N(\eta_K) = +1$, *en is* Z *het kwadraatvrije deel van* $2(u+1)$ *of* $2(u-1)$, *dan zal* $\eta_K.Z \in K^{*2}$.

Het zij hier opgemerkt dat in Ince's tabellen (zie [16]) gebruik gemaakt wordt van het feit dat de fundamentele eenheid (zo zijn norm +1 is) geschreven kan worden in de gedaante

$$\frac{(x + y\sqrt{d})^2}{Z},$$

met Z kwadraatvrij en geheel (en bijgevolg : $x + y\sqrt{d} \in \mathcal{O}_K$). Men ziet verder ook dat het ideaal $Z\mathcal{O}_K$ een kwadraat is in I_K, wat betekent dat Z een produkt van vertakte priemdelers zal zijn. Over de betekenis van Z in de theorie van de radikalen wordt in volgend

punt uitgeweid.

Wat nu het inertie-klassegetal betreft, dit wordt gegeven door de formule in stelling V.1.4.2., i.e. :

$$h_{K/\mathbb{Q}} = \frac{h_{\mathbb{Q}} \cdot v_{K/\mathbb{Q}} \cdot N_v}{2.(U_{\mathbb{Q}} : U_{\mathbb{Q}} \cap N(K^*))} .$$

Daarin is $h_{\mathbb{Q}} = 1$, en is de index in de noemer gelijk aan 1 of 2 al naargelang -1 norm is van een element uit K^* of niet. Met $v_{K/\mathbb{Q}} = 2^t$ verkrijgen we dan :

STELLING V.3.1.6. *Er geldt :*

$$h_{K/\mathbb{Q}} = \begin{cases} 2^{t-1} & \textit{indien } d < 0 \textit{ of indien } d > 0 \textit{ en } -1 \in N(K^*) \\ 2^{t-2} & \textit{indien } d > 0 \textit{ en } -1 \notin N(K^*) \end{cases}$$

Opmerking 1. Voor $d > 0$ volgt uit de stelling van Hasse-Minkowski (zie [3], ch. I) :

$-1 \in N(K^*) \Leftrightarrow$ alle oneven priemdelers van d zijn van de vorm $4m + 1$.

Hiermee rekening houdend kan de stelling in termen van het aantal priemdelers r van d als volgt geformuleerd worden :

$$h_{K/\mathbb{Q}} = \begin{cases} 2^r & \text{indien } d < 0,\ d \equiv 3 \pmod 4 \\ 2^{r-1} & \text{indien } d < 0 \text{ en } d \not\equiv 3 \pmod 4 \text{ of :} \\ & \qquad d > 0 \text{ en } -1 \in N(K^*) \text{ of :} \\ & \qquad d > 0 \text{ en } d \equiv 3 \pmod 4 \\ 2^{r-2} & \text{indien } d > 0,\ -1 \notin N(K^*) \text{ en } d \not\equiv 3 \pmod 4 \end{cases}$$

De rol van $h_{K/\mathbb{Q}}$ bij het bepalen van de pariteit van het klassegetal h_K van K komt duidelijk naar voor in hetgeen nu volgt :

LEMMA V.3.1.1. Er geldt :

$$h_{K/\mathbb{Q}} = 1 \Leftrightarrow h_K \text{ is oneven.}$$

BEWIJS. Veronderstel h_K even. Er bestaat dan een ideaal a van K, niet in P_K, met de eigenschap : $a^2 \in P_K$, of :

$$a^2 = \alpha.\mathcal{O}_K \quad (\alpha \in K^*).$$

Anderzijds, aangezien de norm $N_{K/\mathbb{Q}}$ van a een ideaal is van $\mathbb{Q}$, en aangezien $I_{\mathbb{Q}} = P_{\mathbb{Q}}$ (m.a.w. : $\mathbb{Z}$ is een hoofdideaalring), bestaat er een element a van $\mathbb{Q}^*$ zo dat :

$$a.a^{\sigma} = N_{K/\mathbb{Q}}(a)\mathcal{O}_K = a.\mathcal{O}_K.$$

Combineert men dit met bovenstaande betrekking, dan vindt men :

$$a^{1-\sigma} = \alpha.a^{-1}.\mathcal{O}_K \in P_K.$$

Er bestaat dus minstens één ideaalklasse die inert is, namelijk $a.P_K$, waaruit volgt : $h_{K/\mathbb{Q}} \neq 1$. Dit bewijst "$\Rightarrow$". De omgekeerde implikatie volgt uit het feit dat $h_{K/\mathbb{Q}}$ een deler is van h_K.

De alternatieve formulering van stelling 6 laat ons toe alle kwadratische velden met oneven klassegetal aan te duiden, i.e. :

STELLING V.3.1.7. *Het klassegetal van het veld* $\mathbb{Q}(\sqrt{d})$ (*d kwadraatvrije geheel getal*) *is oneven dan en slechts dan als aan een van de volgende voorwaarden voldaan is :*

(i) $d < 0$; $-d$ *een priemgetal van de vorm* $4m + 3$

(ii) $d = -2$

(iii) $d > 0$, d *een priemgetal*

(iv) $d = 2.p$, p *een priemgetal,* $\equiv 3 \pmod 4$

(v) $d = p_1p_2$, p_1 *en* p_2 *priemgetallen,* $\equiv 3 \pmod 4$.

We zijn thans in staat volgend resultaat uit de theorie van de klassenvelden te bewijzen :

STELLING V.3.1.8. *Een kwadratisch veld* K *heeft even klassegetal dan en slechts dan als er een kwadratisch onvertakte uitbreiding van* K *bestaat.*

(Onder een onvertakte uitbreiding van K verstaat men een uitbreiding waarin alle valuaties van K onvertakt zijn).

BEWIJS. Veronderstel h_K even. Uit de voorgaande stelling kan men dan zonder moeite afleiden dat er twee kwadraatvrije gehele getallen d_1 en d_2 kunnen gevonden worden die voldoen aan de volgende voorwaarden :

(1) $d = d_1d_2$

(2) d_1 en d_2 niet beide negatief

(3) $d_1 \neq 1$

(4) $d_2 \equiv 1 \pmod 4$.

Beschouw dan het veld $L = K(\sqrt{d_2}) = \mathbb{Q}(\sqrt{d},\sqrt{d_1},\sqrt{d_2})$. Dat de archimedische valuaties van K onvertakt zijn in L volgt uit de voorwaarde (2). De priemdelers van K zijn onvertakt wegens I.1.4. : (2). Dus, L/K is onvertakt. Dat, omgekeerd, het even zijn van h_K volgt uit de existentie van een onvertakte uitbreiding van K is een rechtstreekse toepassing van stelling V.1.3.6..

Opmerking 2. De implikatie : "h_K oneven $\Rightarrow$ L/K is vertakt voor alle

kwadratische uitbreidingen L van K", kan ook rechtstreeks uit stelling 7 afgeleid worden. Men kan immers met behulp van I.1.4. en stelling II.3.2.2. gemakkelijk nagaan dat elk bikwadratisch veld L dat K bevat vertakt zal zijn zohaast d aan een van de vijf voorwaarden van stelling 7 voldoet. Dat men zich mag beperken tot bikwadratische velden L volgt uit :

LEMMA V.3.1.2. Is K een kwadratisch veld, en is L een kwadratische onvertakte uitbreiding van K, dan is L bikwadratisch over $\mathbb{Q}$.

BEWIJS. Zij $L = K(\sqrt{\mu})$ een onvertakte uitbreiding van K, en zij :

$$\mu\mathcal{O}_K = p_1^{a_1}\ldots p_r^{a_r}$$

de kanonieke faktorisatie van het ideaal $\mu\mathcal{O}_K$ in K. Aangezien dit ideaal een kwadraat is in I_L (nl. : $(\sqrt{\mu}\mathcal{O}_L)^2$), en aangezien geen enkel priemideaal p_i (i = 1,2,...,r) een kwadraat is in I_L (wat volgt uit het onvertakt zijn van L/K), vindt men onmiddellijk :

$$a_1 \equiv a_2 \equiv \ldots \equiv a_r \equiv 0 \pmod 2.$$

Dus : $\mu\mathcal{O}_K = a^2$ $(a \in I_K)$. De norm $N_{K/\mathbb{Q}}$ nemend vindt men dan :

$$N(\mu)\mathbb{Z} = (N_{K/\mathbb{Q}}(a))^2$$

Wegens het feit dat $N_{K/\mathbb{Q}}(a)$ element is van $P_{\mathbb{Q}}$ vindt men :

$$N(\mu) \in \mathbb{Q}^{*2} \quad \text{of} \quad N(\mu) \in -\mathbb{Q}^{*2}.$$

Het onvertakt zijn van de archimedische valuaties van K verhindert de tweede mogelijkheid. Men kan bijgevolg stelling II.2.2. toepassen, wat het gestelde oplevert.

Gevolg. Is L een veld van graad 4 over $\mathbb{Q}$ dat K bevat, en is L

geen bikwadratisch veld, dan is L/K vertakt.

Is, bijvoorbeeld, L totaal-reëel en cyclisch over $\mathbb{Q}$, dan is dit resultaat een bijzonder geval van stelling van Hasse die zegt dat er in elk deelveld van een totaal-reële cyclische uitbreiding van $\mathbb{Q}$ minstens één priemdeler voorhanden is die vertakt in L. (De lezer vindt een eenvoudig bewijs van Hasse's stelling in [9].)

Opmerking 3. Stelling 8 kan men gemakkelijk rechtstreeks bewijzen met behulp van de theorie der klassenvelden. Daar wordt namelijk aangetoond dat er voor elk getallenveld K een maximaal onvertakte abelse uitbreiding H_K bestaat waarvan de galoisgroep $Gal(H_K/K)$ isomorf is met de ideaalklassengroep I_K/P_K van K. Dus, als h_K even is, dan zal $Gal(H_K/K)$ een deelgroep van index 2 bezitten : het vast veld voor deze deelgroep is dan een kwadratische onvertakte uitbreiding van K.

Stelling 7 is dan eveneens uit stelling 8 af te leiden. Men gebruike hiertoe I.1.4. en stelling II.2.4. als volgt : onderzoek alle getallen d waarvoor er een bikwadratisch veld $L = \mathbb{Q}(\sqrt{d},\sqrt{d'},\sqrt{dd'})$ bestaat dat onvertakt is over $\mathbb{Q}(\sqrt{d})$. (Dat slechts bikwadratische velden onderzocht worden volgt uit Lemma V.3.1.2.)

Wegens opmerking 2 ziet men dat stelling 7 en 8 dus equivalent zijn.

3.2. Eenhedenindices in bikwadratische velden.

Zij $K = \mathbb{Q}(\sqrt{d})$, d positief, geheel en kwadraatvrij.

We stellen ons hier de vraag : voor welke bikwadratische velden L die K bevatten is $q_L(U_K) = 2$? Voor de komplekse bikwadratische velden zal dan wegens stelling II.3.4.2. het klassegetal h_L gelijk

zijn aan het produkt van de klassegetallen van drie kwadratische deelvelden van L.

Zij $\eta_K = \eta = u + v\sqrt{d}$ de fundamentele eenheid van K. Noteer dat $u,v \in \mathbb{N}_0$ indien $d \equiv 2,3 \pmod 4$ en dat $u,v \in \frac{1}{2}\mathbb{Z}$, $u-v \in \mathbb{Z}$ indien $d \equiv 1 \pmod 4$. Het kwadraatvrije deel van $2(u+1)$ (resp. : $2(u-1)$) duiden we met d' (resp. : d") aan. Noteer dan d'.d" = d of 4d.

STELLING V.3.2.1. *Zij* L *een bikwadratisch veld dat* K *bevat. Indien* $N(\eta_K) = N_{K/\mathbb{Q}}(\eta) = -1$, *dan geldt :* $q_L(U_K) = 1$. *Is* $N(\eta) = +1$, *dan geldt :*

(i) $2 \notin \{d',d"\} \Rightarrow : q_L(U_K) = 2 \Leftrightarrow L = \mathbb{Q}(\sqrt{d},\sqrt{d'},\sqrt{d"})$,
of $L = \mathbb{Q}(\sqrt{d},\sqrt{-d'},\sqrt{-d"})$,

(ii) $2 \in \{d',d"\} \Rightarrow : q_L(U_K) = 2 \Leftrightarrow L = \mathbb{Q}(\sqrt{d},\sqrt{d'},\sqrt{d"})$,
$L = \mathbb{Q}(\sqrt{d},\sqrt{-d'},\sqrt{-d"})$,
of $L = \mathbb{Q}(\sqrt{d},\sqrt{-1},\sqrt{-d})$.

BEWIJS. Veronderstel : $q_L(U_K) = 2$. Er is dan wegens stelling IV. 1.2.2. een eenheid ε van L te vinden waarvoor geldt :

$$\eta = \zeta\,\varepsilon^2, \tag{1}$$

met : $\zeta \in W_L$. Veronderstel eerst dat $\zeta = +1$ of -1 (wat niet betekent dat $W_K = \{1,-1\}$). Het veld L zal dan niets anders zijn dan $K(\sqrt{\eta_K})$ of $K(\sqrt{-\eta_K})$. Uit de bikwadraticiteit van L volgt dan : $N(\eta) = +1$ (zie stelling II.2.2.). Hieruit volgt dat er een element ρ van $\mathcal{O}_K$ bestaat zo dat

$$\rho^2 = \eta Z,$$

waarbij Z ofwel d', ofwel d" is. Het is dan duidelijk dat men

heeft :

$$L = K(\sqrt{\xi\eta}) = K(\sqrt{\xi d'}) = K(\sqrt{\xi d''}), \text{ met } \xi = 1 \text{ of } -1.$$

Omgekeerd is het vanzelfsprekend dat de RT-index van U_K in het veld $K(\sqrt{\xi\eta})$ gelijk aan 2 zal zijn aangezien η het kwadraat van een eenheid van dat veld wordt.

Veronderstel vervolgens : $\zeta \notin \{1,-1\}$. Aangezien K reëel is betekent dit : $L = K(\zeta)$. Het is welbekend dat de irreduciebele polynoom van ζ over K gelijk is aan $(X-\zeta)(X-\zeta^{-1})$. Dus, het element $\zeta + \zeta^{-1} = a$ behoort tot K, en er geldt :

$$\zeta^2 = a\zeta - 1$$

Stel nu : $\varepsilon = p + q\zeta$ met $p,q \in K$. Uit (1) volgt dan onmiddellijk :

$$\eta = -2pq - aq^2 + \zeta[(p + qa)^2 - q^2].$$

Dit impliceert : $(p + aq)^2 = q^2$, d.w.z. : $p = \xi q - aq$, waarbij $\xi = 1$ of -1. De oplosbaarheid van (1) komt dus neer op de oplosbaarheid van :

(2) $$\eta = q^2(a - 2\xi).$$

De mogelijke waarden van a worden door stelling II.3.3.1. geleverd, i.e. :

(i) $a = \pm\sqrt{3}$ indien ζ een primitieve 12^{de} eenheidswortel is.

(ii) $a = \pm\sqrt{2}$ indien ζ een primitieve 8^{ste} eenheidswortel is.

(iii) $a = \pm 1$ indien ζ een zesde eenheidswortel, $(\neq \pm 1)$ is.

(iv) $a = 0$ indien $\zeta = +i$ of $-i$.

Indien (i) opgaat heeft men : $\# W_L = 12$, d.w.z. : $d = 3$, $L = K(\sqrt{-1}) = \mathbb{Q}(\sqrt{3},\sqrt{-1},\sqrt{-3})$. In dit veld heeft men (wegens $\eta = 2 + \sqrt{3}$) :

$$\eta = \frac{\sqrt{3}+i}{2} \cdot \left(1 + \sqrt{3} - \frac{\sqrt{3}+i}{2}\right)^2 ,$$

d.w.z. : $q_L(U_K) = 2$. Noteren we ook nog dat hier geldt : $d'' = 2$ en $N(\eta) = +1$.

Indien (ii) opgaat, dan zal $d = 2$. Wegens $\eta = 1 + \sqrt{2}$ heeft men echter onmiddellijk onoplosbaarheid van (2). Hierbij merken we eveneens op : $N(\eta) = -1$.

Indien (iii) geldig is heeft men onmiddellijk : $L = K(\sqrt{-3})$. De vergelijking (2) kan echter dan en slechts dan opgelost worden voor $a = +1$, $\xi = -1$, i.e. :

$$\eta = 3q^2.$$

Dit betekent echter : $3 \in \{d', d''\}$ (zie stelling V.3.1.6.) en $N(\eta) = +1$, zodat we hieruit kunnen besluiten : $L = K(\sqrt{-\eta_K})$. Dit komt hierop neer dat men in (1) de eenheid ε ook zodanig had kunnen kiezen dat de relatie

$$\eta = -\varepsilon^2$$

geldt. Dit volgt eveneens uit het feit dat $a = 1$ impliceert dat ζ een primitieve 6^{de} eenheidswortel is, en dus : $\zeta = -\zeta^{-2}$, zodat (1) dan wordt : $\eta = -\zeta^{-2}\varepsilon^2 = -(\zeta^{-1}\varepsilon)^2$.

In het geval (iv) kan de vergelijking (2) slechts opgelost worden indien $\xi = -1$, i.e. :

$$\eta = 2q^2.$$

D.w.z. : $2 \in \{d', d''\}$ en $N(\eta) = +1$ (cfr. eveneens stelling V.3.1.6.). Wegens de relaties :

$$\eta = 2q^2 = i(1-i)^2q^2 = i(q - iq)^2$$

(waarbij wegens lemma IV.1.1. : $q - iq \in U_L$) vindt men, omgekeerd, dat $q_L(U_K) = 2$ indien $L = K(\sqrt{-1})$. Hiermee is de stelling volledig bewezen.

We kunnen de voorwaarde : $2 \in \{d', d''\}$ ook nog anders uitdrukken, i.e. :

STELLING V.3.2.2. *Is* $N(\eta) = 1$ *dan geldt :* $2 \in \{d', d''\}$ *dan en slechts dan als* $2.\mathcal{O}_K$ *het kwadraat is van een hoofdideaal in* K.

BEWIJS. Uit $2 \in \{d', d''\}$ en $N(\eta) = +1$ volgt :

$$2 = q^2.\eta_K,$$

voor een getal q uit K^*. Dit impliceert :

$$2\mathcal{O}_K = (q\mathcal{O}_K)^2.$$

Omgekeerd, uit

$$2\mathcal{O}_K = (y\mathcal{O}_K)^2 \quad \text{voor een } y \in K^*$$

volgt :

$$2 = \pm y^2 \eta^m, \text{ met } m \in \mathbb{Z}.$$

Aangezien $2 \notin K^{*2}$ of $-K^{*2}$ (anders was $N(\eta) = -1$) volgt hieruit dat m oneven moet zijn, wat neerkomt op :

$$2 = q^2 \eta,$$

i.e. : $2 \in \{d', d''\}$, Q.E.D.

Gevolg. Is $d = p$ of $2p$, waarbij p een priemgetal $\equiv 3 \pmod 4$ is, dan geldt steeds : $2 \in \{d', d''\}$. Inderdaad is, wegens de opmerking 1 van vorig punt : $N(\eta) = +1$. Men weet ook dat het ideaal $2\mathbb{Z}$ van

$\mathbb{Q}$ vertakt is in K, d.w.z. :

$$2O_K = p^2, \quad p \text{ een priemgetal van K.}$$

Uit stelling V.3.1.7. volgt echter : h_K is oneven, zodat uit $p^2 \in P_K$ volgt : $p \in P_K$. De stelling is bijgevolg toepasbaar.

Er is dus een oneindige rij van getallen d waarvoor 2 een element is van {d',d"}. De elementen < 200 van deze rij zijn :

3, 6, 7, 11, 14, 19, 22, 23, 31, 34, 38, 43, 46, 47,
51, 59, 62, 66, 67, 71, 83, 86, 94, 102, 103, 107,
114, 118, 119, 123, 127, 131, 134, 139, 142, 146, 151,
158, 163, 166, 167, 178, 179, 187, 191, 194, 199.

(zie [16]).

Indien d een priemgetal is van de vorm 4m + 3, dan zien we dus dat het unieke totaal-reëel bikwadratisch veld L waarvoor $q_L(U_K) = 2$ niets anders is dan $\mathbb{Q}(\sqrt{p},\sqrt{2p},\sqrt{2})$. Stelt men : $K' = \mathbb{Q}(\sqrt{2p})$ en $K'' = \mathbb{Q}(\sqrt{2p})$, dan volgt aanstonds :

$$q_L(U_{K'}) = 2; \quad q_L(U_{K''}) = 1$$

Men kan hieruit (met behulp van technieken zoals die welke in het bewijs van stelling IV.1.2.1. voorkomen) aantonen dat de groep $U_K U_{K'} U_{K''}$ van index 4 zal zijn in U_L. Voor het klassegetal van L geldt dan, wegens stelling II.3.4.2. (2^{de} deel) :

$$h_L = h_K h_{K'} h_{K''}.$$

Aangezien $h_{K''} = 1$, en de getallen h_K en $h_{K'}$ oneven zijn (stelling V.3.1.7.) volgt dat h_L eveneens oneven zal zijn, i.e. :

STELLING V.3.2.3. *Het klassegetal van het bikwadratisch veld*

$\mathbb{Q}(\sqrt{p},\sqrt{2p},\sqrt{2})$, *waarbij* p *priem is*, $\equiv 3 \pmod 4$, *is oneven.*

We vestigen hier de aandacht op enige recente gelijkaardige resultaten in verband met kubische uitbreidingen (zie [1]) en uitbreidingen van het type $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_k})$ (cfr. [6]).

3.3. Eenhedengroepen in cyclotome velden.

Tot slot geven we nog een toepassing van stelling IV.1.2.2. in de theorie van de cyclotome velden.

Zij p een oneven priemgetal, > 3 en zij $\zeta = \exp(2\pi i/p)$. Het p^{de} cyclotome veld $F = \mathbb{Q}(\zeta)$ heeft een maximaal totaal-reëel deelveld $F_0 = \mathbb{Q}(\zeta + \zeta^{-1})$.

Het is bekend dat elke eenheid van F kan geschreven worden als het produkt van een eenheidswortel ζ' met een eenheid van F_0 (zie [3], ch. V; d.i. het zogenaamde Lemma van Kummmer). Wegens stelling IV.1.2.2. komt dit neer op :

$$q_F(U_{F_0}) = 1.$$

Voor wat betreft de eenheden van F_0 heeft men algemeen :

STELLING V.3.3.1. *Zijn* K *en* L *twee deelvelden van* F_0, *en is* $K \subset L$, *dan geldt :*

$$q_L(U_K) = 1.$$

BEWIJS. Zij $n = [L : K]$. We herinneren eraan dat $[F : \mathbb{Q}] = p-1$, zodat geldt : $n \mid p-1$. Veronderstel nu : $q_L(U_K) \neq 1$. Wegens stelling IV.1.2.2. kan dan steeds een eenheid η van K gevonden

worden en een eenheid ε van L zódanig dat :

$$\eta = \varepsilon^a, \quad a \neq 1;\ a|n$$

(we maken hier gebruik van het totaal-reëel zijn van F_0, waardoor de aanwezigheid van een eenheidswortel in deze relatie onnodig is). Bovendien is η, als element van een fundamenteel systeem van eenheden voor K, geen macht van een element uit K^*. Hieruit volgt dat de uitbreiding $K(\sqrt[a]{\eta})$ bevat is in L. Men kan bovendien ook nog stelling III.4.1.1. toepassen, i.e. :

$$[K(\sqrt[a]{\eta}) : K] = a.$$

Over de uitbreidingen van de vorm $K(\sqrt[a]{\eta})/K$ is anderzijds bekend dat de priemdelers van K die geen deler zijn van $a.\mathcal{O}_K$ onvertakt zijn in L. Wegens $a|n$, $n|p-1$ heeft men : $p \nmid a$, i.e. : de priemdelers van $p\mathcal{O}_K$ in K zijn onvertakt. Dit is echter in tegenstrijd met het welbekende feit dat $p\mathbb{Z}$ totaal vertakt is in F(d.w.z. : de ramifikatie-index van $p\mathbb{Z}$ in F is gelijk aan $[F : \mathbb{Q}] = p-1$), waardoor de ramifikatie-index van elke priemdeler p van K boven $p\mathbb{Z}$ in L de waarde $[L : K]$ heeft. Bijgevolg geldt $q_L(U_K) = 1$, Q.E.D.

Een toepassing hiervan is :

STELLING V.3.3.2. *Is* $\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n = F_0$ *een keten van tussenuitbreidingen van* F_0, *dan bestaat er een stel eenheden :*

$$\{\varepsilon_1^{(1)}, \ldots, \varepsilon_{k_1}^{(1)}, \varepsilon_1^{(2)}, \ldots, \varepsilon_{k_2}^{(2)}, \ldots, \varepsilon_1^{(n)}, \ldots, \varepsilon_{k_n}^{(n)}\}$$

met de eigenschap dat, voor elke $i \in \{1,2,\ldots,n\}$ *de verzameling*

$$\{\varepsilon_1^{(1)}, \ldots, \varepsilon_{k_1}^{(1)}, \ldots, \varepsilon_1^{(i)}, \ldots, \varepsilon_{k_i}^{(i)}\}$$

een fundamenteel systeem van eenheden is voor K_i.

BEWIJS. Zijn L en K twee getallenvelden, $K \subset L$, waarvoor geldt : $q_L(U_K) = 1$, dan kunnen de eenheden $\varepsilon_1,\ldots,\varepsilon_h$ waarvan sprake in stelling IV.1.2.2. steeds zódanig gekozen worden dat de relaties er als volgt uitzien :

$$\begin{cases} \eta_1 = \varepsilon_1 \\ \quad \ldots \\ \eta_d = \varepsilon_d \end{cases}$$

Dit betekent eenvoudig dat elk fundamenteel systeem van eenheden van K kan aangevuld worden tot een fundamenteel systeem van eenheden voor L. Dat we dit kunnen toepassen in onze situatie volgt dus onmiddellijk uit de voorgaande stelling, i.e. : $q_{K_i}(U_{K_{i-1}}) = 1$ voor $i = 2,3,\ldots,n$. Een fundamenteel systeem van eenheden voor K_1, zegge $\{\varepsilon_1^{(1)},\ldots,\varepsilon_{k_1}^{(1)}\}$ kan dus aangevuld worden met eenheden $\varepsilon_1^{(2)},\ldots,\varepsilon_{k_2}^{(2)}$ van K_2 tot een fundamenteel systeem van eenheden van K_2, enz...

Opmerkelijk is hier het feit dat in het bewijs slechts gebruik gemaakt wordt van de eisen :

(1) $\qquad q_{K_i}(U_{K_{i-1}}) = 1 \quad$ voor $i = 2,3,\ldots,n$.

De stelling zal bijgevolg geldig zijn voor alle ketens van getallenvelden waarbij deze voorwaarden vervuld zijn. Een dergelijke situatie doet zich ondermeer voor wanneer de uitbreidingen K_i/K_{i-1} voor $i = 2,\ldots,n$ onoplosbaar zijn; de beschouwingen van hoofdstuk III, §2.1. tonen immers aan dat in dat geval de relatie $q_{K_i}(K_{i-1}) = 1$ zal gelden, wat wegens de relatie "$q_{K_i}(U_{K_{i-1}})$ deelt $q_{K_i}(K_{i-1}^*)$" (zie hoofdstuk IV, §1.1.) tot (1) aanleiding geeft.

BIBLIOGRAFIE

[1] P. BARRUCAND and H. COHN, A rational genus, class number divisibility, and unit theory for pure cubic fields, J. of Number Theory 2 (1970), 7-21.

[2] W.E.H. BERWICK, Integral Bases. Cambridge : Cambridge University Press, 1927.

[3] Z.I. BOREVICH and I.R. SHAFAREVICH, Number Theory. Academic Press, New York and London, 1966.

[4] J.W.S. CASSELS and A. FRÖHLICH, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C., 1967.

[5] C. CHEVALLEY, Sur la théorie du corps de classes dans les corps finis et les corps locaux, Jour. of the Fac. of Sc., Tokyo, Vol. II, Part 9 (1933).

[6] H. COHN, A numerical study of units in Composite real quartic and octic fields (to appear).

[7] L. FUCHS, Infinite Abelian Groups. Acad. Press, New York and London, 1970.

[8] P. FURTWÄNGLER, Über die Klassenzahlen Abelscher Zahlkörper. Jour. f.d. reine u. angew. Math., 134 (1908), 91-94.

[9] H. FURUYA, On divisibility by 2 of the relative class number of imaginary number field, Tôhoku Math. Journ., 23 (1971), 207-218

[10] L.J. GOLDSTEIN, Analytic Number Theory. Prentice-Hall, Inc.,

Englewood Cliffs, New Jersey, 1971.

[11] L.J. GOLDSTEIN, A generalization of Stark's theorem, J. of Number Theory, 3 (1971), 323-346.

[12] L.J. GOLDSTEIN, On a conjecture of Hecke concerning elementary class number formulas, Manuscripta Math., 9 (1973), 245-305.

[13] G. GRAS, Sur les l-classes d'ideaux dans les extensions cycliques relatives de degré premier l, Ann. de l'Inst. Fourier de l'Univ. de Grenoble, 23, 3 (1973) 1-48, 23, 4 (1973), 1-44.

[14] H. HASSE, Über die Klassenzahl abelscher Zahlkörper. Akademie-Verlag, Berlin, 1952.

[15] D. HILBERT, Bericht über die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung 4 (1894-1895), 175-546.

[16] E.L. INCE, Cycles of Reduced Ideals in Quadratic Fields, British Math. Ass. Tables Vol. 4, London, 1934.

[17] T. KUBOTA, Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J., 10-12 (1956), 65-85.

[18] S. LANG, Algebra. Addison-Wesley Publ. Co., Inc., Reading, Mass., 1965.

[19] S. LANG, Algebraic Number Theory. Addison-Wesley Publ. Co., Inc., Reading, Mass. - London - Don Mills, Ont., 1970.

[20] J. LIANG, On relations between units of normal algebraic number fields and their subfields, Acta Arithmetica, 20 (1972), 331-344.

[21] J. LIANG, On discriminants and maximal orders, Acta Math. Acad. Sci. Hung, 24 (1973), 41-57.

[22] D.L. Mc QUILLAN, A remark on Hilbert's Theorem 92. Acta Arithmetica, 22 (1973), 125-128.

[23] J.J. PAYAN, Sur les unités de Minkowski, Sém. Delange-Pisot-Poitou (Théorie des nombres), 15^{e} année, no. 19, 1-6.

[24] A. SCHINZEL, Les extensions pures et les résidus des puissances (te verschijnen in Acta Arithmetica).

[25] F. SEIDELMANN, Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich, Math. Ann., 78 (1918), 230-233.

[26] J.E. SUNLEY, On the class numbers of totally imaginary quadratic extensions of totally real fields, Bull. Amer. Math. Soc., 78 (1972), 74-76.

[27] K. UCHIDA, Class numbers of imaginary abelian number fields I, Tôhoku Math. Journ., 23 (1971), 97-104.

[28] K. UCHIDA, Imaginary abelian number fields with class number one, Tôhoku Math. Journ., 24 (1972), 487-499.

[29] I.M. VINOGRADOV, Elements of Number Theory. Dover Publ., Inc., New York, 1954.

[30] G.E. WAHLIN, The Class Number in the Algebraic Number Field. Bull. of the Nat. Research Council, nr. 62 (1928). Algebraic Numbers II, chapter I, 5-27.

INHOUDSTAFEL

Voorwoord i

Inleiding ii

HOOFDSTUK I. OVERZICHT VAN ENIGE KLASSIEKE RESULTATEN UIT DE ALGEBRAISCHE GETALLENTHEORIE 1

§1. Algemeenheden over Getallenvelden 1

1. Getallenvelden, gehelen, idealen 1

2. Uitbreidingen van Getallenvelden 2

3. De diskriminant 5

4. Onvertakte en volledig splitsende priemidealen 6

§2. Valuaties van getallenvelden 6

1. Algemeenheden over valuaties 6

2. Valuaties van getallenvelden 7

§3. Het klassegetal 9

1. De groep der S-eenheden 9

2. De eenhedengroep en de regulator 10

3. Het klassegetal van een getallenveld 11

HOOFDSTUK II. BIKWADRATISCHE VELDEN 13

§1. Overzicht van de theorie der kwadratische velden 13

1. De ring der gehelen 13

2. Priemidealen in kwadratische velden 14

3. De eenhedengroep 15

4. Het klassegetal 16

§2. Algemeenheden over bikwadratische velden 17

1. Definitie en eerste eigenschappen 17

2. Een kriterium voor bikwadraticiteit 19

§3. De ring der gehelen van bikwadratische velden 22

1. De integrale basis 22

2. Priemidealen 25

3. De eenhedengroep 28

4. Het klassegetal van L 30

HOOFDSTUK III. RADIKALEN IN MULTIPLIKATIEVE GROEPEN VAN VELDEN 35

§1. Het radikaal 35

1. Definities en eerste eigenschappen 35

2. Stellingen 36

§2. De R- en RT-index bij uitbreiding van een veld 38

1. Algemeenheden 38

2. Voorbeelden 39

§3. De RT-index bij cyclische uitbreidingen 41

1. Een Lemma 41

2. Cyclische uitbreidingen 43

3. Voorbeelden 48

§4. De RT-index bij eindige separabele uitbreidingen 50

1. Uitbreidingen van de vorm $K(\sqrt[n]{a})/K$; $a \in K$ 50

2. Uitbreidingen van de vorm $K(\sqrt[n_1]{a_1},\ldots,\sqrt[n_d]{a_d})/K$ 53

3. De RT-index bij uitbreidingen met konstante torsie .. 57

4. De RT-index bij ketens 59

5. De hoofdstelling over de RT-index 62

HOOFDSTUK IV. RADIKALEN IN GETALLENVELDEN 64

§1. Radikalen in S-eenhedengroepen 64

1. De RT-index van de S-eenhedengroep in L^* 64

2. Een andere karakterisering van $q_L(U_K(S))$ 68

§2. Radikalen in de idealengroep 73

1. Het radikaal van I_K in I_L en globale ramifikatie 73

2. Het radikaal van P_K in I_L en in P_L 80

3. Een relatie tussen $Q_L(K^*)$, $Q_L(U_K)$ en $Q_{P_L}(P_K)$ 83

4. De priemdelers van $Q_L(U_L K^*)$ 84

HOOFDSTUK V. BIJZONDERE GETALLENVELDEN EN TOEPASSINGEN 91

§1. De R- en RT-indices in cyclische uitbreidingen 91

1. Het Herbrand quotiënt 92

2. De index $q_L(K^*)$ 93

3. De index $q_L(U_L K^*)$ 94

4. De index $Q_L(U_L K^*)$ en de inerte ideaalklassen van L .. 101

§2. Kwadratische uitbreidingen van een getallenveld 107

1. De relatieve regulator 107

2. Het quotiënt h_L/h_K 115

3. Bijzonder geval 118

§3. Radikalen in kwadratische, bikwadratische en cyclotome velden 120

1. Kwadratische velden 120

2. Eenhedenindices in bikwadratische velden 129

3. Eenhedengroepen in cyclotome velden 135

BIBLIOGRAFIE 138