

Cyclotome lichaamsuitbreidingen van \mathbb{Q} en $\mathbb{F}_q(T)$

Jan Willem de Jong

30 september 2004

Inhoudsopgave

1	Inleiding	2
2	Ringen der gehele over \mathbb{Q}	3
3	Dedekinddomeinen, splijten en het Frobenius automorfisme	9
4	Cyclotome lichaamsuitbreidingen van \mathbb{Q}	21
5	Cyclotome lichaamsuitbreidingen van $\mathbb{F}_q[T]$	26
	Bibliografie	35

Hoofdstuk 1

Inleiding

In deze scriptie wordt het splijten van priemenvan in lichaamsuitbreidingen bekeken. Ik zal hier kort proberen uit te leggen wat dat is zonder de strikte definities te geven. Aan bepaalde lichamen kan een ring toegekend worden, namelijk de ring der gehelen (voor \mathbb{Q} is dit bijvoorbeeld \mathbb{Z} , voor $\mathbb{Q}[\sqrt{2}]$ is dit $\mathbb{Z}[\sqrt{2}]$). Dit hoeft geen uniek factorisatie domein te zijn, maar ik zal laten zien dat ieder ideaal in deze ring op unieke wijze (op permutaties na) te schrijven is als product van priemidealen. Als je een lichaamsuitbreiding bekijkt van een lichaam, dan zal de ring der gehelen van die uitbreiding de oorspronkelijke bevatten. Je kunt je nu het volgende afvragen: Gegeven een priemideaal in de oorspronkelijke ring, welke priemenvan zitten er nu in de uitgebreide ring, zodanig dat als ik hem beperk tot de originele ring ik het oude priemideaal terugkrijg, het onderzoeken van deze vraag is in wiskundige taal de vraag hoe een priem 'splijt' in een lichaamsuitbreiding. Het blijkt dat hier een hele verrassende theorie achter zit, die een soort van karakterisering geeft, wanneer en hoe dit dan gebeurt, welke ik (tot zekere hoogte) zal behandelen.

Deze scriptie zal zich vooral richten op cyclotome lichaamsuitbreidingen van \mathbb{Q} en uitbreidingen van $\mathbb{F}_q(T)$ gekarakteriseerd door het Carlitz moduul, welke cyclotome lichaamsuitbreidingen van $\mathbb{F}_q(T)$ genoemd worden. Deze naamgeving is gerechtvaardigd gezien de grote analogon tussen de genoemde lichaamsuitbreidingen, samengevat in onderstaande tabel:

lichaam	\mathbb{Q}	$k = \mathbb{F}_q(T)$
ring der gehelen	\mathbb{Z} (vb. 2.2)	$A = \mathbb{F}_q[T]$
lichaamsuitbreiding	$\mathbb{Q}(\omega_m)$, $m \in \mathbb{Z}$	$k(\lambda_m)$, $m \in A$
Galoisgroep	$(\mathbb{Z}/m)^*$ (st. 4.4)	$(A/mA)^*$ (st. 5.9)
graad	$\phi(m)$ (st. 4.3)	$\Phi(m)$ (st. 5.9)
ring der gehelen	$\mathbb{Z}[\omega_m]$ (st. 4.6)	$A[\lambda_m]$ (st. 5.12)
splijten van (p)	splijt in $\phi(m)/f$ idealen van graad f als $p \nmid m$, $p \in \mathbb{Z}$ (lemma 4.8)	splijt in $\Phi(m)/f$ idealen van graad f als $p \nmid m$, $p \in A$ (st. 5.13)

Hoofdstuk 2

Ringen der gehelen over \mathbb{Q}

Definitie 2.1. Een eindige lichaamsuitbreiding is een deellichaam van \mathbb{C} van eindige graad over \mathbb{Q} .

Definitie 2.2. Een complex getal heet een algebraïsch geheel als het een wortel is van een monische veelterm over \mathbb{Z} .

Voorbeeld 2.1. $\sqrt{2}$ en $\frac{1+\sqrt{5}}{2}$ zijn algebraïsche gehelen, zijnde wortels van $x^2 - 2$ en $x^2 - x - 1$ respectievelijk. $\frac{\sqrt{2}}{2}$ is geen algebraïsch geheel.

Lemma 2.1. Stel f is een monische veelterm met coëfficiënten in \mathbb{Z} en stel dat $f = gh$ met g en h monische polynomen over \mathbb{Q} , dan hebben g en h coëfficiënten in \mathbb{Z} .

Bewijs. Definieer m en n zodanig dat mg en nh coëfficiënten in \mathbb{Z} hebben met m en n minimaal, merk op dat de coëfficiënten van mg geen gemeenschappelijke factor hebben (volgt uit moniciteit en het minimaal zijn van m) en nh ook niet. We laten nu zien dat $m = n = 1$. Stel dat $mn > 1$ en stel dat $p|mn$ met p priem. Merk op dat $mnf = (mg)(nh)$, reduceer nu modulo p , dan $\bar{0} = \overline{mg} \overline{nh}$, maar $\mathbb{Z}_p[x]$ is een domein, dus $\overline{mg} = \bar{0}$ of $\overline{nh} = \bar{0}$, maar dan deelt p alle coëfficiënten van mg of nh , hetgeen onmogelijk is. \square

Dit lemma gebruiken we voor de volgende belangrijke stelling:

Stelling 2.1. Stel dat α een algebraïsch geheel is en stel dat $f \in \mathbb{Z}[x]$ een polynoom is met α als wortel met minimale graad, dan is f irreducibel over \mathbb{Q} .

Bewijs. Stel dat f reducibel is, dan zijn er monische polynomen g en h over \mathbb{Q} zodanig dat $f = gh$, dus (lemma) g en h zijn monische polynomen in \mathbb{Z} , maar α is wortel van g en/of h , hetgeen in tegenspraak is met de minimale graad van f . \square

Voorbeeld 2.2. De algebraïsche gehelen van \mathbb{Q} zijn de gehele getallen.

Noteer met \mathbb{A} de verzameling van alle algebraïsche gehelen. Deze blijkt een hele mooie structuur te hebben, het is namelijk een ring. Dus als je twee algebraïsche gehelen hebt, deze vermenigvuldigt, dan wel optelt krijg je weer een algebraïsch geheel. Om dit te bewijzen is het handig eerst het volgende lemma te bewijzen:

Lemma 2.2. Voor $\alpha \in \mathbb{C}$ zijn equivalent:

1. α is een algebraïsch geheel
2. De additieve groep van de ring $\mathbb{Z}[\alpha]$ is eindig voortgebracht
3. α behoort tot een deelring van \mathbb{C} met eindig voortgebrachte additieve deelgroep
4. Er is een eindig voortgebrachte deelring van \mathbb{C} zodanig dat $\alpha A \subset A$

Bewijs. (1) \rightarrow (2): α is wortel van een monisch irreducibel polynoom over \mathbb{Z} van eindige graad

(2) \rightarrow (3) \rightarrow (4): triviaal

(4) \rightarrow (1): Dit is de niet-triviale implicatie. Stel dat A voortgebracht wordt door $a_1, \dots, a_n \in A$. Ontwikkel αa_i als lineaire combinatie van de a_j 's over \mathbb{Z} . Dit kan bondig worden weergegeven door: $\alpha a = Ma$, met a de kolomvector (a_1, \dots, a_n) en M een $n \times n$ matrix. Oftewel: $(\alpha I - M)a = 0$, oftewel $\det(\alpha I - M) = 0$, α voldoet dus aan $\det(xI - M) = 0$ dit is het gevraagde monische polynoom. \square

Stelling 2.2. \mathbb{A} is een ring

Bewijs. Stel dat α en β algebraïsche gehelen zijn, dan hebben $\mathbb{Z}[\alpha]$ en $\mathbb{Z}[\beta]$ eindig voortgebrachte additieve groepen. En dus ook $\mathbb{Z}[\alpha, \beta]$ (hebbende $\alpha_i \beta_j$ als basis als de α_i en β_j de ring $\mathbb{Z}[\alpha]$ respectievelijk $\mathbb{Z}[\beta]$ voortbrengen). Merk nu op dat $\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$ en dat uit lemma 2.2 (3) \rightarrow (1) volgt dat deze algebraïsch zijn. \square

Voorbeeld 2.3. $\sqrt{2} + i$ is algebraïsch

Stel nu dat K een eindige lichaamsuitbreiding over \mathbb{Q} is, het is nu interessant om te kijken naar $\mathbb{A} \cap K$, dit wordt de ring van gehelen behorende bij K genoemd. Dit is uiteraard weer een ring, aangezien de doorsnede van twee ringen weer een ring is.

Ter herinnering: Stel dat K een eindige lichaamsuitbreiding is van \mathbb{Q} met graad n , dan zijn er precies n inbeddingen van K in \mathbb{C} . Schrijven we $K = \mathbb{Q}[\alpha]$ en stel dat f het minimaalpolynoom over \mathbb{Q} van α is dan wordt deze inbedding σ uniek vastgelegd door $\sigma(\alpha)$ welke een ander nulpunt van f moet zijn aangezien $\sigma(f(\alpha)) = f(\sigma(\alpha)) = \sigma(0) = 0$. Dit geeft precies n inbeddingen, ze worden dus gekarakteriseerd door $\sigma(\alpha) = \beta_i$ met β_i een wortel van f .

Definitie 2.3 (spoor en norm). Stel dat K een eindige lichaamsuitbreiding over \mathbb{Q} is en dat $\sigma_1, \dots, \sigma_n$ de inbeddingen van K in \mathbb{C} zijn. Stel $\alpha \in K$ dan definiëren we het spoor van α als: $T(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$ En we definiëren de norm van α als: $N(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_n(\alpha)$.

Voorbeeld 2.4. Stel $K = \mathbb{Q}[\sqrt{2}]$. $\sqrt{2}$ voldoet aan $x^2 - 2 = 0$, dus er zijn 2 inbeddingen, welke gegeven worden door: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ en $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ en dus $T(a + b\sqrt{2}) = 2a$ en $N(a + b\sqrt{2}) = a^2 - 2b^2$.

Opmerking 2.1. Uit de definitie volgen meteen de volgende gelijkheden voor $\alpha, \beta \in K$ en $r \in \mathbb{Q}$: $T(\alpha + \beta) = T(\alpha) + T(\beta)$, $N(\alpha\beta) = N(\alpha)N(\beta)$, $T(r) = nr$, $N(r) = r^n$, $T(r\alpha) = rT(\alpha)$, $N(r\alpha) = r^n N(\alpha)$ met n de graad van de lichaamsuitbreiding.

Waarom zijn 'het spoor' en 'de norm' nou handig, wel ze zijn rationaal, wat we na het volgende lemma makkelijk kunnen bewijzen.

Lemma 2.3. *Stel $[K : \mathbb{Q}] = n$ en $\alpha \in K$ en stel dat α graad d heeft over \mathbb{Q} en dat $t(\alpha)$ en $n(\alpha)$ de som respectievelijk het produkt van de d geconjugeerden (de wortels van het minimaalpolynoom) van α zijn. Dan geldt: $T(\alpha) = n/d \cdot t(\alpha)$ en $N(\alpha) = n(\alpha)^{n/d}$.*

Bewijs. Het minimaalpolynoom van α geeft d inbeddingen in \mathbb{C} , iedere inbedding kan uitgebreid worden tot n/d inbeddingen (graad van $K/\mathbb{Q}[\alpha]$) van K in \mathbb{C} die $\mathbb{Q}[\alpha]$ vasthouden. \square

Stelling 2.3. *$T(\alpha)$ en $N(\alpha)$ zijn rationaal*

Bewijs. Het is voldoende te bewijzen dat $t(\alpha)$ en $n(\alpha)$ rationaal zijn. Dit is evident aangezien $\pm n(\alpha)$ de constante term is van het minimaalpolynoom van α en $-t(\alpha)$ de term na de leidende term. \square

Stelling 2.4. *Als $\alpha \in \mathbb{A}$ geldt $T(\alpha) \in \mathbb{Z}$ en $N(\alpha) \in \mathbb{Z}$*

Bewijs. Zie het vorige bewijs en merk op dat de constante term nu een geheel getal is en de kop term 1 is, oftewel $t(\alpha) = -c_{n-1}$ en $n(\alpha) = \pm c_0$ als α het minimaal polynoom $x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ heeft. Lemma 2.3 geeft nu dat $T(\alpha) \in \mathbb{Z}$ en $N(\alpha) \in \mathbb{Z}$. \square

Definitie 2.4. *Stel dat K en L eindige lichaamsuitbreidingen over \mathbb{Q} zijn met $K \subset L$ en $n = [L : K]$ en $\sigma_1, \dots, \sigma_n$ de n inbeddingen van L in \mathbb{C} die K vast houden, dan wordt het relatieve spoor en de relatieve norm gegeven door: $T_K^L(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$ en $N_K^L(\alpha) = \sigma_1(\alpha) \cdot \dots \cdot \sigma_n(\alpha)$ respectievelijk.*

Opmerking 2.2. *Aangezien de theorie veel algemener is, kan bij lemma 2.3 en stelling 2.3 \mathbb{Q} vervangen worden door een willekeurig ander lichaam k en de zin 'zijn rationaal' vervangen wordt door 'liggen in k en spoor en norm vervangen worden door relatieve spoor en relatieve norm respectievelijk, de bewijzen veranderen niet.*

Het is nu goed te vertellen waar dit allemaal heen gaat. Uiteindelijk wil ik aan het einde van dit hoofdstuk laten zien dat voor K een eindige lichaamsuitbreiding van \mathbb{Q} er een eindige integrale basis bestaat voor $R = K \cap \mathbb{A}$ (i.e. er zijn elementen $b_1, \dots, b_s \in R$ zodat iedere $x \in R$ geschreven kan worden als $m_1b_1 + \dots + m_sb_s$ met $m_i \in \mathbb{Z}$). Hiervoor zullen we het begrip discriminant nodig hebben met enkele stellingen daarover. In het vervolg geldt $R \equiv \mathbb{A} \cap K$. Met $[a_{ij}]$ wordt de matrix bedoeld met waarden a_{ij} op positie i, j (i 'de rij, j 'de kolom).

Definitie 2.5. *Stel $n = [K : \mathbb{Q}]$ en $\alpha_1, \dots, \alpha_n \in K$ en $\sigma_1, \dots, \sigma_n$ de inbeddingen van K in \mathbb{C} , dan definiëren we de discriminant van $\alpha_1, \dots, \alpha_n$ als $disc(\alpha_1, \dots, \alpha_n) = \det([\sigma_i(\alpha_j)])^2$*

Opmerking 2.3. *De discriminant hangt niet af van de nummering van de inbeddingen, aangezien de determinant dan hoogstens van teken verandert, welk opgegeven wordt bij het kwadrateren.*

Voorbeeld 2.5. Als $K = \mathbb{Q}[\sqrt{2}]$ en $\alpha_1 = a + b\sqrt{2}$ en $\alpha_2 = c + d\sqrt{2}$, met de inbeddingen als in voorbeeld 2.4:

$$\begin{aligned} \text{disc}(\alpha_1, \alpha_2) &= \left(\det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) \end{pmatrix} \right)^2 \\ &= \left(\det \begin{pmatrix} a + b\sqrt{2} & c + d\sqrt{2} \\ a - b\sqrt{2} & c - d\sqrt{2} \end{pmatrix} \right)^2 = 8(a^2d^2 - 2abcd + b^2c^2) \end{aligned}$$

Stelling 2.5. $\text{disc}(\alpha_1, \dots, \alpha_n) = \det([T(\alpha_i\alpha_j)])$

Bewijs. Merk op dat $[\sigma_j(\alpha_i)] \cdot [\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i) \cdot \sigma_1(\alpha_j) + \dots + \sigma_n(\alpha_i)\sigma_n(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) \cdot \dots + \sigma_n(\alpha_i\alpha_j)] = [T(\alpha_i\alpha_j)]$, de gelijkheid volgt nu uit $\det(A) = \det(A^T)$ en $\det(AB) = \det(A) \cdot \det(B)$. \square

Stelling 2.6. Stel $\alpha_i \in K$ dan $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$ als $\alpha_1, \dots, \alpha_n \in \mathbb{A}$ dan $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$

Bewijs. We gebruiken de vorige stelling in combinatie met stelling 2.3 en stelling 2.4 (merk op dat $\alpha_i\alpha_j \in \mathbb{A}$ als $\alpha_i, \alpha_j \in \mathbb{A}$). \square

Stelling 2.7. $\text{disc}(\alpha_1, \dots, \alpha_n) = 0$ dan en slechts dan als $\alpha_1, \dots, \alpha_n$ lineair onafhankelijk zijn over \mathbb{Q} .

Bewijs. Stel dat $\alpha_1, \dots, \alpha_n$ lineair afhankelijk zijn. Stel $\sum_{i=1}^n c_i\alpha_i = 0$ dan ook $\sigma_j(\sum_{i=1}^n c_i\alpha_i) = \sum_{i=1}^n c_i\sigma_j(\alpha_i) = 0$ voor iedere j , oftewel de kolumnen van de matrix $[\sigma_i(\alpha_j)]$ zijn afhankelijk, dus is de discriminant 0. Stel nu dat $\text{disc}(\alpha_1, \dots, \alpha_n) = 0$, dan zijn de rijen van $[T(\alpha_i\alpha_j)]$ afhankelijk, stel dat $a_1R_1 + \dots + a_nR_n = 0$ voor zekere $a_j \in \mathbb{Q}$ en de R_j de vector corresponderende met de j 'de kolumn in de matrix $[T(\alpha_i\alpha_j)]$. Stel nu dat de α_i onafhankelijk zijn. Definieer $\alpha \equiv a_1\alpha_1 + \dots + a_n\alpha_n$. Onder de aanname van onafhankelijkheid geldt zeker $\alpha \neq 0$. Dan geldt voor iedere j , $T(\alpha\alpha_j) = a_1T(\alpha_1\alpha_j) + \dots + a_nT(\alpha_n\alpha_j) = (a_1R_1 + \dots + a_nR_n)_j = 0$, omdat de α_j 's onafhankelijk zijn vormen deze een basis en aangezien K een lichaam is en $\alpha \neq 0$ vormen de $\alpha\alpha_j$ ook een basis, waaruit we concluderen dat $T(\beta) = 0$ voor iedere $\beta \in K$, hetgeen onmogelijk is (bijv. $T(1) = n$). \square

Stelling 2.8. Stel dat $K = \mathbb{Q}[\alpha]$ en stel dat $\alpha_1, \dots, \alpha_n$ de geconjugeerden zijn van α , dan: $\text{disc}(\alpha) \equiv \text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \pm N^K(f'(\alpha))$ met f het monisch irreducibele polynoom van α over \mathbb{Q}

Bewijs. Voor de eerste gelijkheid zullen we gebruik maken van $\det(a_i^{j-1}) = \prod_{1 \leq r < s \leq n} (a_s - a_r)$, dit is in te zien met inductie, maar hier zal er niet verder op ingegaan worden. Hiermee krijgen we: $\text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i(\alpha^{j-1}))^2 = \det(\sigma_i(\alpha)^{j-1})^2 = \det(\alpha_i^{j-1})^2 = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2$ waarbij in de derde gelijkheid gebruikt is dat iedere inbedding α naar een andere wortel stuurt en dat de determinant door een permutatie van de kolumnen ten hoogste van teken verandert, de eerste gelijkheid in de stelling is hiermee bewezen. Voor de laatste gelijkheid: $N^K(f'(\alpha)) = \prod_{r=1}^n \sigma_r(f'(\alpha)) = \prod_{r=1}^n f'(\sigma_r(\alpha)) = \prod_{r=1}^n f'(\alpha_r) = \prod_{s \neq r} (\alpha_r - \alpha_s) = \pm \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2$ \square

Nu gaan we kijken naar een basis voor $R (\equiv \mathbb{A} \cap K)$, we zullen bewijzen dat R een vrije abelse groep is van rank $n = [K : \mathbb{Q}]$:

Definitie 2.6. Een vrije abelse groep van rang n is een groep die de directe som is van n deelgroepen welke elk isomorf is met \mathbb{Z} .

Opmerking 2.4. n wordt eenduidig vastgelegd aangezien de groep isomorf is met \mathbb{Z}^n en $(\mathbb{Z}/2\mathbb{Z})^n$ 2^n elementen heeft. Iedere deelgroep van een vrije abelse groep is wederom een vrije abelse groep. Dit is in eenvoudig in te zien, door projecties te bekijken van die deelgroep (via het isomorfisme) op één van de componenten van de directe som en vervolgens te bedenken dat deelgroepen van \mathbb{Z} dan wel isomorf zijn met $\{0\}$, dan wel met \mathbb{Z} , dit levert dus door components gewijs te kijken na evt. permutatie een bijectie op met $\mathbb{Z}^m \times \{0\}^{n-m} \approx \mathbb{Z}^m$ en is dus een abelse groep van rang m .

Stelling 2.9. Zij K een eindige uitbreiding van \mathbb{Q} dan bestaat er een basis voor K bestaande uit algebraïsche gehelen

Bewijs. Het is voldoende te laten zien, dat als α een algebraïsch getal is, dat er dan een $m \in \mathbb{Z}$ bestaat zodat $m\alpha \in \mathbb{A}$, we passen dit dan gewoon toe op de basis elementen van K . Stel dus dat α algebraïsch is, stel dat α voldoet aan: $c_n\alpha^n + \dots + c_0 = 0$ door eventueel noemers eruit te vermenigvuldigen kunnen we aannemen dat $c_i \in \mathbb{Z}$, kies $m = c_n$, dan voldoet $m\alpha$ aan $x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_{n-1}c_0 = 0$ (vermenigvuldig de eerdere vergelijking met c_n^{n-1}) \square

Stelling 2.10. Stel dat $\{\alpha_1, \dots, \alpha_n\}$ een basis is voor K over \mathbb{Q} met $\alpha_i \in \mathbb{A}$ en $d = \text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$, dan zijn er voor iedere $\alpha \in R$ $m_i \in \mathbb{Z}$ zodanig dat $x = (m_1\alpha_1 + \dots + m_n\alpha_n)/d$ met $d|m_j^2$

Bewijs. Schrijf $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$ voor zekere $x_j \in \mathbb{Q}$. Stel dat $\sigma_1, \dots, \sigma_n$ de inbeddingen van K in \mathbb{C} . Deze toepassende op de relatie wordt het volgende systeem van vergelijkingen gekregen: $\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \dots + x_n\sigma_i(\alpha_n)$. De regel van Cramer geeft nu dat $x_j = Y_j/\delta$ met $\delta = \det([\sigma_i(\alpha_j)])$. En Y_j is de determinant van de matrix die verkregen wordt door de j' de kolom van $[\sigma_i(\alpha_j)]$ door $\sigma_i(\alpha)$ te vervangen. Y_j en δ zijn volgens stelling 2.6 algebraïsch (kwadraat ligt in \mathbb{Z} ($d = \delta^2$)). Invullen geeft $dx_j = \delta Y_j$, wat aantoonst dat $dx_j \in \mathbb{A}$, oftewel een geheel getal, zeg $dx_j = m_j$. Het rest nu nog aan te tonen dat $m_j^2/d \in \mathbb{Z}$. We hebben $Y_j^2 = x_j^2\delta^2 = d^2x_j^2/d = m_j^2/d \in \mathbb{A}$, oftewel $m_j^2/d \in \mathbb{Z}$ (omdat $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$). \square

Stelling 2.11. R is een vrije abelse groep van graad n

Bewijs. Kies een basis $\{\alpha_1, \dots, \alpha_n\}$ voor K bestaande uit algebraïsche gehelen. Definieer $A = \{m_1\alpha_1 + \dots + m_n\alpha_n \mid m_i \in \mathbb{Z}\} \subset R$, dit is duidelijk een vrije abelse groep van rang n . Stelling 2.10 geeft dat $R \subset d^{-1}A$. Nu gebruiken we opmerking 2.4 en merken we op dat als een vrije abelse groep ingeklemd wordt door twee vrije abelse groepen van graad n de groep zelf graad n moet hebben. \square

Stelling 2.12. Stel dat $\{\beta_1, \dots, \beta_n\}$ en $\{\gamma_1, \dots, \gamma_n\}$ twee integrale basissen zijn, dan $\text{disc}(\beta_1, \dots, \beta_n) = \text{disc}(\gamma_1, \dots, \gamma_n)$.

Bewijs. Schrijf $\beta = M\gamma$, met β en γ vectoren gevormt door de β_i en γ_i respectievelijk, en M een matrix over \mathbb{Z} , dit kan omdat de γ_i 's een basis vormen. De j' de inbedding op de vergelijking toepassen geeft $\sigma_j(\beta_i) = M(\sigma_j(\gamma_i))$ voor iedere i en j . Beschouw nu deze vergelijkingen als een matrix vergelijking. De determinant van beide vergelijkingen nemen en kwadrateren geeft $\text{disc}(\beta_1, \dots, \beta_n) = \det(M)^2 \text{disc}(\gamma_1, \dots, \gamma_n)$. Omdat $\det(M) \in \mathbb{Z}$ geldt dus $\text{disc}(\gamma_1, \dots, \gamma_n) \mid \text{disc}(\beta_1, \dots, \beta_n)$.

De β 's en de γ 's omdraaien geeft analoog $disc(\beta_1, \dots, \beta_n) \mid disc(\gamma_1, \dots, \gamma_n)$. We concluderen (aangezien ze beide postief zijn) dat $disc(\beta_1, \dots, \beta_n) = disc(\gamma_1, \dots, \gamma_n)$. \square

De discriminant is dus een invariant, een getal behorende bij een bepaalde ring der gehelen, genoteerd als $disc(R)$ of $disc(K)$. We geven nu nog een definitie en een stelling die we in een later hoofdstuk nodig zullen hebben:

Definitie 2.7. *Stel dat K en L lichamen zijn, dan $KL = \{\alpha_1\beta_1 + \dots + \alpha_r\beta_r \mid \alpha_i \in K, \beta_i \in L\}$. Stel dat R en S de ringen der gehelen zijn, dan $RS = \{\alpha_1\beta_1 + \dots + \alpha_r\beta_r \mid \alpha_i \in R, \beta_i \in S\}$*

Stelling 2.13. *Stel dat $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L, T = \mathbb{A} \cap KL$, $[K : \mathbb{Q}] = m$, $[L : \mathbb{Q}] = n$ én dat $[KL : \mathbb{Q}] = mn$. Definieer dan $d = (disc(R), disc(S))$, dan $T \subset \frac{1}{d}RS$, als $d = 1$, dan $T = RS$.*

Bewijs. Eerst een lemma over inbeddingen:

Lemma 2.4. *K, L, KL als in vorige stelling. Stel dat σ een inbedding is van K in \mathbb{C} en τ een inbedding is van L dan is er een inbedding ρ van KL zodat $\rho|_K = \sigma$ en $\rho|_L = \tau$*

Bewijs lemma:

Iedere inbedding σ van K breidt uit tot n inbeddingen van KL , op die manier krijg je alle mn inbeddingen van KL , de uitbreiding beperkt tot L geeft m verschillende inbeddingen van L , ééntje daarvan moet τ zijn.

Bewijs stelling:

Stel dat $\{\alpha_1, \dots, \alpha_m\}$ een basis is van R (over \mathbb{Z}) en $\{\beta_1, \dots, \beta_n\}$ een basis voor S . Dan vormen de $\alpha_i\beta_j$ een basis voor RS over \mathbb{Z} deze vormen tevens een basis voor K, L, KL respectievelijk over \mathbb{Q} . Iedere $\alpha \in T$ kan geschreven worden als: $\alpha = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j$, $r, m_{ij} \in \mathbb{Z}$ met $(r, \text{ggd}(m_{ij})) = 1$. Het is voldoende te laten zien dat $r \mid d$. Het is zelfs voldoende te laten zien dat $r \mid disc(R)$: vanwege symmetrie volgt dan dat $r \mid disc(S)$ en dan dus ook $r \mid (disc(R), disc(S))$. Zij σ_j een inbedding van K in \mathbb{C} , de uitbreiding van σ_j tot KL die L vasthoudt (lemma), wordt ook met σ_j genoteerd, dan geldt dat $\sigma_j(\alpha) = \sum_{i,k} \frac{m_{ik}}{r} \sigma_j(\alpha_i) \beta_k$, definiëer nu $x_i = \sum_{j=1}^n \frac{m_{ij} \beta_j}{r}$ voor iedere (uitgebreide) σ (in totaal m) krijgen we de vergelijking: $\sum_{i=1}^m \sigma_j(\alpha_i) x_i = \sigma_j(\alpha)$. De regel van Kramer geeft de oplossing: $x_i = Y_i / \delta$ met δ de determinant van $[\sigma_j(\alpha_i)]$ en Y_i wordt verkregen uit δ door de i 'de kolom te vervangen door $\sigma_j(\alpha_i)$. δ en de Y_i zijn algebraïsche gehelen omdat $\sigma(\alpha)$ en $\sigma(\alpha_i)$ het allemaal zijn. Verder geldt $\delta^2 = disc(R)$, als we definiëren $e = disc(R)$, dan $e x_i = \delta Y_i \in \mathbb{A}$. En bovendien geldt dat $e x_i \in L$, dus $e x_i \in \mathbb{A} \cap L = S$. Omdat de β_j een basis vormen geldt dus dat $e m_{ij} / r \in \mathbb{Z}$, dus $r \mid e m_{ij}$ voor alle i, j , omdat $(r, \text{ggd}(m_{ij})) = 1$ volgt dat $r \mid e = disc(R)$. Omdat altijd al $RS \subset T$ volgt het tweede deel van de stelling onmiddellijk. \square

Hoofdstuk 3

Dedekinddomeinen, splijten en het Frobenius automorfisme

Net zoals in \mathbb{Z} ieder getal op een unieke manier (op eenheden na) geschreven kan worden als een produkt van priemgetallen zal in $\mathbb{A} \cap K$ ook wel iets dergelijks gelden. Dat is inderdaad het geval, al ligt het complexer dan men op het eerste gezicht zou vermoeden. Dit komt omdat niet iedere ring der gehelen unieke priemfactorisatie heeft, dit komt al voor in betrekkelijk eenvoudige ringen der gehelen als bijv. $\mathbb{Z}[\sqrt{-5}]$ ($2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$). Wat een getallenring wel heeft is dat ieder ideaal in $\mathbb{A} \cap K$ uniek te schrijven is (op eenheden na) als produkt van priemidealen, wat we zullen gaan bewijzen. We zullen beginnen met het definiëren van een Dedekind-domein, we zullen bewijzen dat daarin unieke priemfactorisatie in priemidealen in bestaat. Uiteraard zullen we vervolgens bewijzen dat iedere ring der gehelen een Dedekind domein is.

Definitie 3.1. Een Dedekind Domein is een integraal domein R zodat:

1. Ieder ideaal in R eindig wordt voortgebracht.
2. Ieder niet triviaal priemideaal ($\neq 0, R$) een maximaal ideaal is.
3. R integraal gesloten is in zijn breukenlichaam $K = \{\alpha/\beta \mid \alpha, \beta \in R, \beta \neq 0\}$ i.e. Als α/β wortel is van een monische veelterm over R dan $\beta \mid \alpha$ in R .

Stelling 3.1. Voorwaarde (1) van definitie 3.1 is equivalent met:

- (1') Iedere stijgende rij van idealen is vanaf een gegeven moment constant. Oftewel als $I_1 \subset I_2 \subset \dots$ dan is er een n zodanig dat $I_n = I_k$ voor iedere $k \geq n$
- (1'') Iedere (niet lege) verzameling van idealen heeft een maximaal ideaal, i.e. er is een M zodanig dat als $M \subset I \in S$, dan $M = I$

Bewijs. (1) \rightarrow (1'): Bekijk het ideaal dat gegenereerd wordt door alle idealen in de stijgende rij, noem deze I . Stel dat $I_1 \subsetneq I_2 \subsetneq \dots$. Merk op dat voor alle j , $I_j \subset I$. Stel dat m_1, \dots, m_n de generatoren van I zijn, dan is er voor iedere i een I_{j_i} zodanig dat $m_i \in I_{j_i}$, en geldt voor $j \geq k = \max(j_1, \dots, j_n)$ dat $I_j = I$,

aangezien die alle generatoren bevatten.

(1') \rightarrow (1''): Zij S een verzameling van idealen. Kies een ideaal I , als er geen ideaal is dat I strikt bevat zijn we klaar. Als die wel bestaat, zeg I_1 , hebben we $I \subsetneq I_1$ en doen we hetzelfde met I_1 . Dit is een eindig procedé aangezien we anders een oneindige strikt stijgende rij van idealen zouden construeren.

(1'') \rightarrow (1): Zij I een ideaal. Definieer $S = \{\text{eindig voortgebracht idealen die in } I \text{ liggen}\}$. Deze verzameling is niet leeg en heeft dus een maximaal ideaal. We bewijzen nu dat I het maximale ideaal is. Stel niet, zij $J_1 \in S$, omdat J_1 eindig voortgebracht is en I niet, bestaat er een $\alpha_1 \in I \setminus J_1$, bekijk nu het ideaal voortgebracht door (α) en J_1 en noem deze J_2 en herhaal dit procedé, zo wordt een strikt stijgende rij idealen $J_1 \subsetneq J_2 \subsetneq \dots$ verkregen, welke dus geen maximaal ideaal heeft. Aangezien J_1 willekeurig was bewijst dit dat I het maximale ideaal moet zijn. \square

Stelling 3.2. *Iedere ring der gehelen is een Dedekind domein*

Bewijs. (1) volgt meteen uit stelling 2.11, aangezien ieder ideaal een additieve deelgroep is van R en dus ook weer eindig is voortgebracht.

(2) Het is voldoende te bewijzen dat R/P een lichaam is, met P een primideaal. Daarvoor is het voldoende te bewijzen dat deze eindig is (bekijk voor een willekeurige $\alpha \neq 0$, de rij α, α^2, \dots en merk op dat er m, n met $m \neq n$ moeten zijn met $\alpha^m = \alpha^n$, gebruik nu de schrapwet (geldig in integrale domeinen), voor de inverse van α). Zij $\alpha \neq 0 \in I$ en stel dat $m = N(\alpha) \in \mathbb{Z}$, de norm genomen met betrekking tot M als $R = \mathbb{A} \cap M$. Dan geldt ook dat $m \neq 0$, omdat anders $\sigma_j(\alpha) = 0$ voor zekere j hetgeen impliceert dat $\alpha = 0$. Schrijf $m = \alpha\beta$ met β het produkt van de geconjugeerden van α , omdat de geconjugeerden van α in \mathbb{A} liggen, geldt dat $\beta \in \mathbb{A}$ (\mathbb{A} was immers een ring). En bovendien $\beta = m/\alpha \in K$, dus $\beta \in R$ dus $m = \alpha\beta \in I$. Wel nu zijn we er want $R/(m)$ is eindig aangezien R een abelse groep is van eindige graad, omdat $(m) \subset I$ geldt nu dat R/I eindig is.

(3) Stel $\alpha/\beta \in K$ is wortel van een monische veelterm over R . Stel dat $(\alpha/\beta)^n + a_{n-1}(\alpha/\beta)^{n-1} + \dots + a_0 = 0$ met $a_i \in R$. Bekijk $\mathbb{Z}[a_0, \dots, a_{n-1}, a_n = \alpha/\beta]$. Deze verzameling is eindig voortgebracht door $a_0^{m_0} \cdot \dots \cdot a_n^{m_n}$ met als $i \neq n$ $m_i = 0, \dots, \deg(a_i)$ en $m_n = 0, \dots, n - 1$. Omdat $\mathbb{Z}[\alpha/\beta] \subset \mathbb{Z}[a_0, \dots, a_{n-1}, a_n = \alpha/\beta]$ is $\mathbb{Z}[\alpha/\beta]$ eindig voortgebracht, volgens lemma 2.2 is α/β algebraïsch. \square

Nu gaan we wat algemene dingen bewijzen over Dedekind domeinen, wat dus van toepassing is op iedere ring der gehelen. Zoals beloofd zullen gaan bewijzen dat ieder ideaal in een Dedekind domein op een unieke manier te schrijven is als produkt van priemidealen.

Lemma 3.1. *In een Dedekind domein bevat ieder ideaal een produkt van priemidealen.*

Bewijs. Stel niet, dan is de verzameling van idealen die die geen produkt van priemidealen bevat niet leeg en heeft dus volgens (1'') van stelling 3.1 een maximaal element M . M is uiteraard zelf geen priem, dus zijn er $r, s \in R - M$ zodat $rs \in M$. De idealen $M + (r)$ en $M + (s)$ zijn strikt groter dan M , dus, bevatten deze een produkt van priemidealen of een van beiden is R . In het eerste geval bevat ook $(M + (r))(M + (s))$ een produkt van priemidealen en deze is bevat in M , hetgeen in tegenspraak is. In het tweede geval geldt nog steeds dat

$(M + (r))(M + (s))$ bevat is in M , maar als een van beiden gelijk aan R is, dan r of $s \in M$, hetgeen wederom in tegenspraak is. \square

Lemma 3.2. *Stel dat A een niet-triviaal ideaal is ($\neq 0, R$) in een Dedekind domein R . En stel dat K het bijbehorende breukenlichaam is; dan is er een $Y \in K - R$ zodat $YA \subset R$*

Bewijs. Kies $a \neq 0 \in A$. Lemma 3.1 geeft dat (a) een produkt van priemidealen bevat. Dus stel $P_1 \dots P_r \subset (a)$ met r minimaal gekozen. Ieder ideaal ($\neq 0, R$) is bevat in een maximaal ideaal (de verzameling van idealen die I omvatten is niet leeg) en is dus een priemideaal (een maximaal ideaal is altijd priem). Dus $A \subset P$ voor zekere priem P . Dus P bevat ook het produkt van priemidealen $P_1 \dots P_r$. Dus bevat P een van de P_i , immers, stel niet, kies $a_i \in P_i - P$, dan $a_1 \dots a_r \in P$, dus $a_i \in P$ voor zekere i , hetgeen in tegenspraak is met de keuze van de a_i . Stel dat $P_1 \subset P$. Uit conditie (2) voor Dedekind domeinen, volgt dat $P = P_1$. Als $r = 1$, i.e. (a) is een priemideaal, kies dan $b \in R - (a)$ en kies $Y = b/a$. Stel nu $r \geq 2$, omdat r minimaal is, is er een $b \in (P_2 \dots P_r) - (a)$. $Y = b/a \notin R$, omdat anders anders $b = b/a \cdot a \in (a)$. Dus $Y \in K - R$. Nu nog te bewijzen dat $YA \subset R$. We hebben $P_1 \dots P_r \subset (a) \subset A \subset P = P_1$. Zij nu $xb/a \in YA$, voor zekere $x \in A$, dan $x \in P_1$ en dus $xb \in P_1 \dots P_r \subset (a)$, dus $xb = a\gamma$ voor $\gamma \in R$. En dus is $xb/a = a\gamma/a = \gamma \in R$ \square

De vorige twee lemma's waren nodig voor de volgende stelling.

Stelling 3.3. *Stel dat I een ideaal is in een Dedekind domein R . Dan bestaat er een ideaal $J \neq \{0\}$ zodanig dat IJ een hoofdideaal is.*

Bewijs. Als I het nulideaal is dan is $IJ = \{0\}$ een hoofdideaal voor ieder ideaal J . Zij $\alpha \neq 0 \in I$, definieer dan $J = \{\beta \in R \mid \beta I \subset (\alpha)\}$. Dan is J een ideaal en $IJ \subset (\alpha)$. Maar er geldt zelfs gelijkheid. Bekijk het ideaal $A = IJ/\alpha \subset R$. Als $A = R$ zijn we klaar, immers dan is $IJ = (\alpha)$. Zo niet, dan kunnen we lemma 3.2 toepassen. Dus er bestaat een $Y \in K - R$ zodanig dat $YA \subset R$. Aangezien R integraal gesloten is (nummer (3) van een Dedekind domein) hebben we tegenspraak als Y wortel is van een monische veelterm over R . Omdat $\alpha \in I$ geldt $J \subset A$. Oftewel $YJ \subset YA \subset R$. Hieruit volgt dat $YJ \subset J$ immers $YIJ/\alpha \subset R$ impliceert $YIJ \subset \alpha R = (\alpha)$, dus als $\beta \in J$, dan $Y\beta I \subset (\alpha)$, oftewel $Y\beta \in J$ (per definitie). Kies een genererende set $\alpha_1, \dots, \alpha_n$ voor J en ontwikkel de $Y\alpha_j$'s hierin. Hiermee wordt de vergelijking $Y\alpha = M\alpha$ verkregen met M een matrix over R . Maar dan voldoet Y aan $\det(xI - M) = 0$, met I hier de identiteitsmatrix. \square

Lemma 3.3. *Als A, B, C idealen zijn in een Dedekind domein en $AB = AC$, dan geldt $B = C$*

Bewijs. Er bestaat een ideaal J zodat AJ een hoofdideaal domein is, zeg $AJ = (\alpha)$, dan $ABJ = ACJ$, oftewel $\alpha B = \alpha C$, oftewel, omdat R een domein is $B = C$. \square

Lemma 3.4. *Stel dat A en B idealen zijn in een Dedekind domein, dan $A \mid B$ dan en slechts dan als $B \subset A$*

Bewijs. Triviaal is de implicatie $A \mid B \rightarrow B \subset A$. Stel dat $B \subset A$. Kies J zodat AJ een hoofdideaal is, zeg $AJ = (\alpha)$. Definieer $C = \frac{1}{\alpha}JB$, dit is een ideaal in R (merk op dat $C \subset \frac{1}{\alpha}AJ = R$) en $AC = B$. \square

Stelling 3.4. *Ieder niet-triviaal ideaal in een Dedekind domein is uniek (op volgorde na) te schrijven als produkt van niet-triviale priemidealen.*

Bewijs. Eerst existentie. Stel dat niet ieder niet-triviaal ideaal te schrijven is als produkt van priemidealen, de verzameling van idealen waarbij dat niet kan is dan niet leeg en heeft dus een maximaal ideaal. $M \neq R$, dus $M \subset P$ met P een priemideaal (zie lemma 3.2). Dus $M = PI$ (lemma 3.4) en dus $M \subset I$, en deze inclusie is strict aangezien anders $R = P$. Dus I is te schrijven als product van priemidealen, hetgeen onmogelijk is, omdat anders M dat ook is via de relatie $M = PI$. Nu nog de uniciteit. Stel dat $P_1 \dots P_r = Q_1 \dots Q_s$. Dan geldt $P_1 \supset Q_1 \dots Q_s$, oftewel $P_1 \supset Q_1$ (na evt. permutatie van de indices) (zie bewijs lemma 3.2). Uit conditie (2) voor een Dedekind domein volgt nu dat $P_1 = Q_1$. Zo doorgaand vinden we $r = s$ en $P_i = Q_i$ voor iedere i . \square

Stelling 3.5. *Stel I en J idealen zijn idealen in een Dedekinddomein, I en J zijn relatief priem, dan en slechts dan als I en J geen gemeenschappelijke priemfactoren hebben.*

Bewijs. Stel dat P een gemeenschappelijke factor is. Dan geldt: $R = I + J = PA + PB = P(A + B) \subset P$, dus $P = R$, tegenspraak. Nu de andere kant. We bewijzen eerst: als K en L relatief priem zijn dan ook K^m en L^n voor iedere $m, n \in \mathbb{N}$. Stel $x \in K$ en $y \in L$, zodat $x + y = 1$, dan $1 = (x + y)^{m+n} = \sum a_i x^i y^{m+n-i} \in K^m + L^n$ met $a_i \in \mathbb{N}$. Nu bewijzen we: Als I, J, K onderling relatief priem zijn, dan ook IK en J : $R = (I + J)(I + K)(J + K) = I^2 J + I J^2 + I^2 K + I J K + I J K + J^2 K + I K^2 + J K^2 \subset IK + J$, oftewel $IK + J = R$. We hebben dus nu bewezen dat als je een verzameling idealen hebt zodat ieder paar idealen relatief priem is, dan ook twee produkten van idealen die geen gemeenschappelijke factor hebben. Stel nu dat I en J geen gemeenschappelijke priemfactoren heeft, stel $I = P_1^{n_1} \dots P_r^{n_r}$ en $J = Q_1^{m_1} \dots Q_s^{m_s}$. Beschouw de verzameling $C = \{P_1, \dots, P_r, Q_1, \dots, Q_s\}$, de vorige opmerking daarop toepassende volgt nu dat I en J relatief priem zijn (merk op dat in een Dedekind domein priemidealen maximaal zijn en dus relatief priem als ze verschillend zijn). \square

We kunnen nu analoog aan \mathbb{Z} de grootste gemene deler en het kleinste gemene veelvoud definiëren.

Stelling 3.6. $(I, J) = I + J$ en $lcm(I, J) = I \cap J$

Bewijs. (I, J) is het kleinste ideaal ($\neq R$) dat zowel I en J bevat $I + J$ zit daar altijd in bevat, maar $I + J$ is een ideaal. $lcm(I, J)$ is het grootste ideaal dat bevat zit in beide en is dus altijd bevat in $I \cap J$, maar $I \cap J$ is een ideaal. \square

Stelling 3.7. *Stel dat I een ideaal is in een Dedekind domein R en stel dat $\alpha \neq 0 \in I$. Dan is er een $\beta \in I$ zodat $I = (\alpha, \beta)$ (i.e. voortgebracht door α en β).*

Bewijs. Stel $I = P_1^{n_1} \dots P_r^{n_r}$ met de P_i 's verschillend. Dan $P_i^{n_i} \mid (\alpha)$. Stel dat Q_1, \dots, Q_s de (eventuele) extra priemen die (α) delen (mogelijkerwijs nog P_i 's), dus zeg $(\alpha) = P_1^{n_1+f_1} \dots P_r^{n_r+f_r} Q_1^{m_1} \dots Q_s^{m_s}$. Het is voldoende om een β te vinden die voldoet aan: $(\beta) = P_1^{n_1} \dots P_r^{n_r} S_1^{k_1} \dots S_t^{k_t}$ met $S_i \neq Q_j, P_j$ (dus relatief priem) aangezien dan: $(\alpha) + (\beta) = P_1^{n_1} \dots P_r^{n_r} (P_1^{f_1} \dots P_r^{f_r} Q_1^{m_1} \dots Q_s^{m_s} + S_1^{k_1} \dots S_t^{k_t}) = P_1^{n_1} \dots P_r^{n_r} = I$ (zie stelling 3.5). Nu nog de existentie van zo'n β . Eerst zorgen

we ervoor dat de ontwikkeling van (β) de goeie machten van de P_i 's heeft (dit impliceert $S_i \neq P_j$) oftewel $(\beta) \subset P^{n_i}$ maar $(\beta) \not\subset P^{n_i+1}$, dit doen we als volgt, kies $\beta_i \in P^{n_i} - P^{n_i+1}$ (deze is niet leeg wegens door de wegstreepregel) en eis $\beta \equiv \beta_i \pmod{P_i^{n_i+1}}$. Verder moet Q_i niet in de ontwikkeling van (β) zitten oftewel $(\beta) \not\subset Q_j$, hieraan is voldaan als $\beta \equiv 1 \pmod{Q_j}$. De vorige stelling geeft dat de Q_j 's te samen met de $P_i^{n_i+1}$'s relatief priem zijn en dus geeft de Chinese reststelling dat er een oplossing β bestaat. \square

Stelling 3.8. *Een Dedekind domein is een uniek factorisatie domein dan en slechts dan als het een hoofdideaal domein is.*

Bewijs. Een hoofdideaal domein is altijd een uniek factorisatie domein. We hoeven dus alleen maar de andere kant op. Stel dat het geen hoofdideaal domein is, maar wel een uniek factorisatie domein, stel dat P een niet-hoofdideaal priem ideaal is, welke moet bestaan, omdat anders alle idealen hoofdidealen zijn (aangezien we factorisatie in priemidealen hebben en het produkt van hoofdidealene weer een hoofdideaal is). Definieer nu S als de verzameling van idealen I zodat PI een hoofdideaal is, deze is niet leeg wegens lemma 3.3, zij M een maximaal ideaal van S en stel dat $PM = (\alpha)$, dan is α een irreducibel element, immers als $\alpha = \beta\gamma$, dan geeft unieke factorisatie, dat (β) dan wel (γ) van de vorm PJ moet zijn, stel $(\beta) = PJ$ merk op dat $J \mid M$, dus $M \subset J$, dus $J = M$, wat impliceert dat $PM = PM\gamma$, oftewel $(\gamma) = R$, oftewel γ is een eenheid. Kies nu $\delta \in P - (\alpha)$ en $\epsilon \in M - (\alpha)$ (dit kan aangezien anders $P = (\alpha)$ en dus $M = R$, hetgeen een tegenspraak is, een zelfde verhaal voor M). Merk nu op dat $\delta\epsilon \in PM = (\alpha)$, dus $\alpha \mid \delta\epsilon$, maar $\alpha \nmid \delta$ en $\alpha \nmid \epsilon$, hetgeen onmogelijk is. \square

Nu gaan we weer terug van algemene Dedekind domeinen naar ringen der gehelen, welke dus ook Dedekind domeinen zijn. Stel dat $K \subset L$ eindige lichamen over \mathbb{Q} zijn, definieer dan $R = \mathbb{A} \cap K$ en $S = \mathbb{A} \cap L$. Als we een ideaal P van R hebben kunnen we daar een ideaal in S mee maken, door te definiëren $PS = \{\sum_{i=1}^n \alpha_i \beta_i \mid \alpha_i \in P, \beta_i \in S\}$, dit ideaal is heel bijzonder, hetgeen wordt samengevat in de volgende stelling:

Stelling 3.9. *Stel dat P een priem is in R en Q een priem is in S , dan zijn equivalent:*

1. $Q \mid PS$
2. $PS \subset Q$
3. $P \subset Q$
4. $Q \cap R = P$
5. $Q \cap K = P$

Bewijs. (1) \leftrightarrow (2): Lemma 3.4

(2) \leftrightarrow (3): Als $P \subset Q$, dan $PS \subset QS = Q$, andere kant op is triviaal, omdat $1 \in S$

(4) \rightarrow (3): triviaal

(4) \leftrightarrow (5): triviaal omdat $Q \subset \mathbb{A}$

(3) \rightarrow (4): Er geldt dat $P \subset Q \cap R$ en $Q \cap R$ is een ideaal in R , omdat P maximaal is (is priem), geldt $Q \cap R = P$ of $Q \cap R = R$. Het laatste zou impliceren dat $1 \in Q$, oftewel $Q = S$. Hetgeen in tegenspraak is. \square

Als aan één van de equivalenties van de stelling voldaan wordt (en dus allemaal), dan zeggen we dat Q boven P ligt, of dat P onder Q ligt.

Stelling 3.10. *Ieder priem Q van S ligt boven een unieke priem P van R . Ieder priem P van R ligt onder minstens één priem van S .*

Bewijs. Voor het eerste deel is het voldoende te laten zien dat $Q \cap R$ een priemideaal is: als $ab \in Q \cap R$ volgt meteen dat danwel a , dan wel b er in moet liggen. Omdat $1 \notin Q$ is $Q \neq R$. En $Q \cap R \neq \{0\}$: kies $\alpha \neq 0 \in Q$, dan $N(\alpha) \in Q \cap \mathbb{Z} \subset Q \cap R$. Voor de tweede uitspraak bewijzen, we dat $PS \neq S$. Priemontwikkeling van PS geeft dan dat tenminste 1 priem boven P volgens (1) van de vorige stelling. We moeten dus laten zien dat $1 \notin PS$. Kies $Y \in K - R$ zodat $YP \subset R$ als in lemma 3.2. Dan hebben we dat $YPS \subset RS = S$, als $1 \in PS$, dan $Y \in S$, maar dan is Y een algebraïsch geheel dus $Y \in K \cap \mathbb{A} = R$, tegenspraak. \square

Definitie 3.2. *Stel dat Q boven P ligt, e is de macht van Q in de priemontwikkeling van PS , dan heet e de vertakkingsgraad van Q boven P , notatie $e(Q | P)$.*

Opmerking 3.1. *Volgens stelling 3.9 is e tenminste 1.*

Omdat P en Q priemidealen zijn en dus maximaal, zijn R/P en S/Q lichamen. Omdat $R \subset S$, is er een homomorfisme $R \rightarrow S/Q$ met kernel $R \cap Q = P$, dus is er een injectief homomorfisme $R/P \rightarrow S/Q$. Verder zijn R/P en S/Q eindig, wat bewezen is in het bewijs van stelling 3.2. Dus is S/Q een eindige lichaamsuitbreiding van R/P als we R/P via de injectie in S/Q denken.

Definitie 3.3. $f = f(Q | P) = [S/Q : R/P]$. f wordt de traagheidsgraad van Q over P genoemd.

Stelling 3.11. *Stel $R \subset S \subset T$ ringen der gehelen en $P \subset Q \subset U$ zijn zijn primen in R, S, T respectievelijk dan:*

$$\begin{aligned} e(U | P) &= e(U | Q)e(Q | P) \\ f(U | P) &= f(U | Q)f(Q | P) \end{aligned}$$

Bewijs. Stel dat $e(U_1 | P) = e_1, e(U_1 | Q_1) = \widehat{e}_1, e(Q_1 | P) = \widehat{\widehat{e}}_1$, dan geldt dus:
 $PT = U_1^{e_1} \dots U_n^{e_n}$
 $Q_1T = U_1^{\widehat{e}_1} \dots U_n^{\widehat{e}_r}$
 $PS = Q_1^{\widehat{\widehat{e}}_1} \dots Q_n^{\widehat{\widehat{e}}_s}$

We moeten dus bewijzen dat $e_1 = \widehat{e}_1 \widehat{\widehat{e}}_1$. Merk nu op dat PST een ideaal is in T . Deze heeft dus unieke priemfactorisatie in idealen in T . We hebben de volgende identiteit:

$$\begin{aligned} U_1^{e_1} \dots U_n^{e_n} &= (U_1^{e_1} \dots U_n^{e_n})S = (PT)S = PST = (PS)T = (Q_1^{\widehat{\widehat{e}}_1} \dots Q_n^{\widehat{\widehat{e}}_s})T = \\ &= (Q_1^{\widehat{\widehat{e}}_1} T) \dots (Q_n^{\widehat{\widehat{e}}_s} T) = (U_1^{\widehat{e}_1} \dots U_n^{\widehat{e}_r})^{\widehat{\widehat{e}}_1} (Q_2 T)^{\widehat{\widehat{e}}_2} \dots (Q_s T)^{\widehat{\widehat{e}}_s} = U_1^{\widehat{e}_1 \widehat{\widehat{e}}_1} \dots U_n^{\widehat{e}_r \widehat{\widehat{e}}_1} (Q_2 T)^{\widehat{\widehat{e}}_2} \dots (Q_s T)^{\widehat{\widehat{e}}_s} \end{aligned}$$

Aan beide kanten van de identiteit hebben we nu een ontwikkeling van PST in idealen in T . Kijkend naar het priemideaal U_1 geldt dus $e_1 \geq \widehat{e}_1 \widehat{\widehat{e}}_1$. Het is nu voldoende te laten zien dat $U_1 \nmid Q_2 T$ (we kiezen voor het gemak Q_2). De delers van $Q_2 T$ zijn precies de idealen in T die boven Q_2 liggen, maar U_1 ligt al boven Q_1 , hetgeen niet kan (stelling 3.10).

De multiplicativiteit van f is gewoon de bekende de torenregel van lichamen en tussenlichamen: $f(U | P) = [T/U : R/P] = [T/U : S/Q][S/Q : R/P] = f(U | Q)f(Q | P)$ \square

De traagheidsgraden en vertakkingsgraden en de graad van de uitbreiding blijken aan elkaar gekoppeld te zijn en wel op de volgende manier:

Stelling 3.12. *Stel L en K lichamen over \mathbb{Q} , $n = [L : K]$, $R = \mathbb{A} \cap K$, $S = \mathbb{A} \cap L$. Stel P is een priemideaal in R en Q_1, \dots, Q_r zijn de priemenvan S die boven P liggen en stel dat e_1, \dots, e_r en f_1, \dots, f_r de desbetreffende vertakkings- en traagheidsgraden zijn, dan geldt: $\sum_{i=1}^r e_i f_i = n$*

Het is handig deze stelling tegelijkertijd met de volgende stelling te bewijzen. Noteer $\|I\| = |R/I|$ voor I een ideaal in R .

Stelling 3.13. *Met de definities als in stelling 3.12 geldt:*

1. $\|IJ\| = \|I\|\|J\|$ voor I en J idealen in R
2. $\|IS\| = \|I\|^n$ voor I een ideaal in R en IS het geassocieerde ideaal in S
3. $\|(\alpha)\| = |N_{\mathbb{Q}}^K(\alpha)|$ voor $\alpha \neq 0 \in R$

Bewijs. Bewijs stelling 3.13 onderdeel 1:

Het is voldoende te bewijzen dat $\|P^n\| = \|P\|^n$ voor P een priemideaal en dat het gestelde geldt voor I en J relatief priem, immers: Priemfactoriseer I en J , stel: $I = P_1^{n_1} \dots P_r^{n_r}$ en $J = P_1^{m_1} \dots P_r^{m_r}$ (hierbij mag n_i dan wel $m_i = 0$ zijn).
 $\|IJ\| = \|P_1^{n_1+m_1} \dots P_r^{n_r+m_r}\| = \|P_1^{n_1+m_1}\| \dots \|P_r^{n_r+m_r}\| = \|P_1\|^{n_1+m_1} \dots \|P_r\|^{n_r+m_r} = \|P_1\|^{n_1} \dots \|P_r\|^{n_r} \|P_1\|^{m_1} \dots \|P_r\|^{m_r} = \|P_1^{n_1} \dots P_r^{n_r}\| \|P_1^{m_1} \dots P_r^{m_r}\| = \|I\| \|J\|$
Dus stel I en J relatief priem, dan geldt dus $I+J = R$ en bovendien $I \cap J = IJ$, want: altijd geldt $IJ \subset I \cap J$, merk nu op dat $I \cap J \subset I$ en $I \cap J \subset J$, oftewel $I \mid I \cap J$ en $J \mid I \cap J$ en omdat I en J relatief priem zijn geldt nu dat $IJ \mid I \cap J$, oftewel $I \cap J \subset IJ$, conclusie $I \cap J = IJ$. Nu gebruiken we de chinese reststelling, er is dus een isomorfisme $R/IJ = R/I \cap J \rightarrow R/I \times R/J$, oftewel $\|IJ\| = \|I\| \|J\|$. Nu nog te bewijzen voor P een priemideaal dat $\|P^m\| = \|P\|^m$. Merk op dat $R \supset P \supset P^2 \supset \dots \supset P^m$, het is voldoende te laten zien dat $\|P\| = |P^k/P^{k+1}|$, waarbij de P^k beschouwd worden als additieve groepen: We hebben de surjectie $R/P^{j+1} \rightarrow R/P^j$ met kern P^j/P^{j+1} , dus $(R/P^{j+1})/(P^j/P^{j+1}) \cong R/P^j$. En dus $|R/P^{j+1}| = |R/P^j| |P^j/P^{j+1}|$. Het gestelde volgt dan dus met inductie. Er is zelfs een groepsisomorfisme $R/P \rightarrow P^k/P^{k+1}$. Kies $\alpha \in P^k - P^{k+1}$ (dit kan anders $P = R$). Er is dan een groeps-isomorfisme van $R/P \rightarrow \alpha R/\alpha P$ (omdat R/P een lichaam is en α dus een inverse heeft). Merk nu op dat $\alpha R \subset P^k$, we krijgen dus een homomorfisme (inclusie) $\alpha R \rightarrow P^k/P^{k+1}$. Met kern $(\alpha R) \cap P^{k+1}$ en beeld $(\alpha R + P^{k+1})/P^{k+1}$. Maar $(\alpha R) \cap P^{k+1} = \alpha P$ omdat aan beide kanten het kleinste gemene veelvoud staat van αR en P^{k+1} , immers P^k is de exacte deler van αR , deze moet worden aangevuld met één P om de goeie macht van P te krijgen, namelijk $k+1$, verder moeten alle priemfactoren van αR toegevoegd worden, oftewel $(\alpha R)P = \alpha P$, verder geeft stelling 3.6 de linkerkant. En ook geldt $(\alpha R) + P^{k+1} = P^k$, nu staat aan beide kanten de kleinste gemene deler van αR en P^{k+1} , linkerkant is stelling 3.6, voor de rechterkant merk je weer op dat P^k de exacte deler is van αR . De homomorfiestelling geeft nu dat $\alpha R/\alpha P \approx P^k/P^{k+1}$, samenstellen met het eerste isomorfisme geeft het gevraagde isomorfisme.

Bewijs stelling 3.12 in een bijzonder geval:

Stel $K = \mathbb{Q}$, dan $R = \mathbb{Z}$ en dan is dus $P = p\mathbb{Z}$ voor een zeker priemgetal p . Schrijf: $pS = \prod_{i=1}^r Q_i^{e_i}$, dan $\|pS\| = \prod_{i=1}^r \|Q_i\|^{e_i} = \prod_{i=1}^r |S/Q_i|^{e_i} =$

$\prod_{i=1}^r (p^{f_i})^{e_i} = p^{\sum_{i=1}^r e_i f_i}$, anderzijds is $\|pS\| = |S/pS| = p^n$ (zie stelling 2.11).

Bewijs stelling 3.13 deel 2:

Gezien deel 1 van stelling 3.13 is het voldoende het gestelde te bewijzen voor I een priemideaal P (door factorisatie wordt dan het algemene resultaat verkregen). Bekijk de inclusie $R \rightarrow S/pS$, de kernel van dit morfisme is $PS \cap R = P$ (stelling 3.9), dus is $R/P \rightarrow S/pS$ een injectie. S/pS is dus een vectorruimte over het lichaam R/P . Het is nu voldoende te bewijzen dat de dimensie van S/pS over R/P n is. We laten eerst zien dat de dimensie maximaal n is. We moeten dus bewijzen dat iedere $n+1$ elementen in S geassocieerd in S/pS afhankelijk zijn over R/P . We weten dat de elementen afhankelijk zijn over K , het bewijs van stelling 2.9 geeft dat deze elementen dan ook afhankelijk zijn over R . Dus stel $\alpha_1, \dots, \alpha_{n+1} \in S$, dan zijn er $\beta_1, \dots, \beta_{n+1} \in R$ zodat $\beta_1 \alpha_1 + \dots + \beta_{n+1} \alpha_{n+1} = 0$ (*) met niet alle β_i nul. Het probleem dat nu opduikt is dat we naar $\beta_i \pmod{P}$ willen kijken en dat deze nu wel 0 kunnen worden. Als $(\beta_1, \dots, \beta_{n+1}) \notin P$ dan gaat alles goed, aangezien er dan een $\beta_j \not\equiv 0 \pmod{P}$ is. Stel nu dat $B = (\beta_1, \dots, \beta_{n+1}) \subset P$. Er is een (niet nul) ideaal C en een $\alpha \in R$ zodanig dat $BC = (\alpha)$ (stelling 3.3), dan $BC \not\subset \alpha P$ (anders $P = R$). Er is dus een $\gamma \in C$ zodanig dat $\gamma B \not\subset \alpha P$, definieer $Y = \gamma/\alpha$, dan geldt $YB \not\subset P$, maar wel $YB \subset R$, omdat $YB = \gamma/\alpha B \subset BC/\alpha = \alpha^{-1}(\alpha) = R$. Uitschrijvend wat we nu hebben, krijgen we, er is een $x \in (R \cap YB) - P$, stel $x = \sum_{i=1}^m r_i Y \beta_i$, dan is er dus een $r_j Y \beta_j \in (R \cap YB) - P$. Door de hele vergelijking (*) nu te vermenigvuldigen met $r_j Y$ krijgen we $\beta_1 r_j Y \alpha_1 + \dots + \beta_{n+1} r_j Y \alpha_{n+1} = 0$. Omdat $\beta_i r_j Y \in R$ en $\beta_j r_j Y \not\equiv 0 \pmod{P}$ hebben we nu een niet-triviale afhankelijkheids relatie in S/pS over R/P , dus $\|PS\| \leq \|P\|^n$. We laten nu zien dat de dimensie minimaal n is. Stel dat $P \cap \mathbb{Z} = p\mathbb{Z} = (p)$. Bekijk alle priemmen P_i van R die boven (p) liggen, we weten dat $S/P_i S$ als vectorruimte over R/P_i van dimensie $n_i \leq n$ is. We zullen bewijzen dat $n_i = n$ voor iedere i in het bijzonder dus voor $P = P_i$. Definieer $e_i = e(P_i|p)$ en $f_i = f(P_i|p)$, in het speciale geval van stelling 3.12 dat al bewezen is, geldt dus $\sum_i e_i f_i = m$ met $m = [K : \mathbb{Q}]$. We hebben $pR = \prod_i P_i^{e_i}$, oftewel $pS = \prod_i (P_i S)^{e_i}$. Dus $\|pS\| = \prod_i \|P_i S\|^{e_i} = \prod_i \|P_i\|^{n_i e_i} = \prod_i (p^{f_i})^{n_i e_i} = p^{\sum_i f_i n_i e_i}$, anderzijds hebben we dat S een vrije abelse groep is van graad $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = nm$, dus $\|pS\| = |S/pS| = p^{nm}$. We krijgen dus: $mn = \sum_i f_i n_i e_i$, omdat $n_i \leq n$ en $\sum_i e_i f_i = m$, moet dus gelden $n_i = n$ voor iedere i .

Bewijs stelling 3.12 voor het algemene geval:

Schrijf: $PS = \prod_i Q_i^{e_i}$, dan geldt vanwege de definitie van f_i en stelling 3.13 deel 1 $\|PS\| = \prod_i \|Q_i\|^{e_i} = \prod_i \|P\|^{f_i e_i}$. Anderzijds hebben we uit stelling 3.13 deel 2 dat $\|PS\| = \|P\|^n$. We krijgen dus $n = \sum_i e_i f_i$

Bewijs stelling 3.13 deel 3:

Breidt K uit naar een normale uitbreiding M over \mathbb{Q} met $m = [M : K]$. Definieer $T = \mathbb{A} \cap M$ en definieer $n = [K : \mathbb{Q}]$. Iedere inbedding van K in \mathbb{C} breidt uit tot precies m lichaamsautomorfismen van M . Schrijf S als de verzameling inbeddingen van K over \mathbb{Q} . Er geldt dat $\|\sigma(\alpha)T\| = \|\alpha T\|$ voor iedere $\sigma \in \text{Gal}(T/\mathbb{Q})$ en $\alpha \in T$, immers: definieer $\phi : T \rightarrow T/\alpha T : x \mapsto \sigma^{-1}(x)$ ($\sigma^{-1}(x) \in T$ als $x \in T$, zijnde een ander nulpunt van het monische minimaalpolynoom van x over \mathbb{Q}), dan $\phi(x) = 0 \Leftrightarrow x \in \sigma(\alpha)T$, ϕ is duidelijk surjectief, dus $T/\sigma(\alpha)T \approx T/\alpha T$, in het bijzonder hebben ze dus evenveel elementen. Voor $\alpha \in R$ geldt dit dus

voor iedere $\sigma \in S$, zijnde de restrictie van een automorfisme van T . Stelling 3.13 deel 1 geeft nu dat: $\|N_{\mathbb{Q}}^K(\alpha)T\| = \prod_{\sigma \in S} \|\sigma(\alpha)T\| = \|\alpha T\|^n$. Ook hebben we omdat $N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$, dat $\|N_{\mathbb{Q}}^K(\alpha)T\| = |N_{\mathbb{Q}}^K(\alpha)|^{[M:\mathbb{Q}]} = |N^K(\alpha)^{nm}|$, waarbij gebruikt is dat $[M:\mathbb{Q}] = [M:K][K:\mathbb{Q}] = mn$. Verder geeft stelling 3.13 deel 2 toegepast op het ideaal $(\alpha) \subset R$ dat $\|\alpha T\| = \|(\alpha)\|^m$, alles bij elkaar invullend geeft: $|N_{\mathbb{Q}}^K(\alpha)|^{nm} = \|(\alpha)\|^{nm}$, oftewel $|N_{\mathbb{Q}}^K(\alpha)| = \|(\alpha)\|$. \square

Als Q boven P ligt en L een normale uitbreiding is van K dan is $\sigma(Q) \subset S$ voor $\sigma \in \text{Gal}(L/K)$ weer een priemideaal dat boven P ligt. De volgende stelling geeft dat op deze manier alle priemidealen boven P verkregen worden.

Stelling 3.14. *Stel dat $K \subset L$ een normale uitbreiding is. En stel dat Q, Q' twee priemen in S zijn die beide boven P liggen, dan is er een $\sigma \in G = \text{Gal}(L/K)$ zodat $\sigma(Q) = Q'$.*

Bewijs. Stel dat $\sigma(Q) \neq Q'$ voor alle $\sigma \in G$. $\sigma(Q)$ en Q' zijn dan relatief priem, dus is er een oplossing $\alpha \in S$ van het volgende stelsel $x \equiv 0 \pmod{Q'}$ en $x \equiv 1 \pmod{\sigma(Q)}$, dit hoeven niet allemaal verschillende vergelijkingen te zijn, maar als $\sigma_i(Q) \neq \sigma_j(Q)$ dan zijn deze weer relatief priem. $N_K^L(\alpha) \in R \cap Q' = P$ omdat één van de factoren α is en de norm altijd in R ligt. Merk op dat $\sigma^{-1}(\alpha) \notin Q$, omdat $N_K^L(\alpha)$ ook geschreven kan worden als het produkt van $\sigma^{-1}(\alpha)$ en Q een priemideaal is geldt dat $N_K^L(\alpha) \notin Q$, maar $P \subset Q$. \square

Stelling 3.15. *Als L een normale uitbreiding is over K van graad n en Q en Q' liggen boven P , dan $e(Q|P) = e(Q'|P)$ en $f(Q|P) = f(Q'|P)$. Er geldt dan $n = rf$ met r het aantal priemen boven P .*

Bewijs. Priemfactoriseer PS . Kies een $\sigma \in G$ zodat $\sigma(Q) = Q'$ en schrijf (ook met σ^{-1}) Q en Q' in de priemfactorisatie in elkaar over. Unieke priemfactorisatie geeft dat er dezelfde machten moeten staan, oftewel $e(Q|P) = e(Q'|P)$. Het homomorfisme $\bar{\sigma} : S \rightarrow S/Q' = S/\sigma(Q)$ heeft kern Q , oftewel S/Q is isomorf met S/Q' , hetgeen dus in het bijzonder geeft $f(Q|P) = f(Q'|P)$. Het laatste resultaat volgt meteen uit stelling 3.12 \square

Definitie 3.4. *Een priem $P \subset R$ heet vertakt in S als er een priem Q boven P is met $e(Q|P) > 1$.*

Stelling 3.16. *Stel dat (p) een priemideaal is in \mathbb{Z} en stel dat (p) vertakt is in R , dan $p \mid \text{disc}(R)$.*

Bewijs. Stel dat P een priem is in R met $e(P|(p)) > 1$ dan is $pR = PI$ en I is deelbaar door alle priemen die boven (p) liggen. Stel dat $\sigma_1, \dots, \sigma_n$ de inbeddingen zijn van K (K zodanig dat $R = K \cap \mathbb{A}$). Breidt de σ_i zo nodig uit tot automorfismen van een uitbreiding L van K , zodanig dat de uitbreiding L normaal is over \mathbb{Q} . Stel dat $\{\alpha_1, \dots, \alpha_n\}$ een basis is voor R over \mathbb{Z} . Kies $\alpha \in I - pR$. Dan ligt α in ieder priemideaal in R dat boven (p) ligt, maar niet in pR . Schrijf $\alpha = m_1\alpha_1 + \dots + m_n\alpha_n$, omdat $\alpha \notin pR$ geldt dat er een i is, zeg $i = 1$ met $p \nmid m_1$. Definieer $d = \text{disc}(R) = \text{disc}(\alpha_1, \dots, \alpha_n)$. Dan is $\text{disc}(\alpha, \alpha_2, \dots, \alpha_n) = m_1^2 d$ (alle andere termen in α zijn afhankelijk van een andere kolloid). Omdat $p \nmid m_1$ is het nu voldoende te laten zien dat $p \mid \text{disc}(\alpha, \alpha_2, \dots, \alpha_n)$. Omdat α in ieder ideaal in R , dat boven (p) ligt zit ligt α ook in ieder ideaal dat in $S = L \cap \mathbb{A}$ boven (p) ligt, immers, zij Q een priemideaal in S boven (p) dan is $Q \cap R$ een

priemideaal in R welke ook (p) bevat, omdat $\alpha \in Q \cap R$ volgt dus $\alpha \in Q$. $\sigma(\alpha) \in Q$ voor alle $\sigma \in \text{Gal}(L/K)$, omdat $\alpha \in \sigma^{-1}(Q)$ (ligt immers boven P), hieruit volgt dat $\text{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in Q$, en omdat $\text{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}$ volgt dat $\text{disc}(\alpha, \alpha_2, \dots, \alpha_n) \in Q \cap \mathbb{Z} = (p)$, hetgeen aantoont dat $p \mid \text{disc}(R)$. \square

We gaan nu Galois theorie toepassen. Uit $n = \text{ref}$ (bij normale uitbreidingen) krijg je het vermoeden dat er een keten tussenlichamen bestaat met uitbreidingen r, e, f in zekere volgorde. Dit is inderdaad het geval, zie stelling 3.17. De tussenlichamen corresponderen, zoals bekend met deelgroepen van de Galoisgroep. We zullen van nu af aan veronderstellen dat L een normale uitbreiding is van K . De priemen Q boven P hebben dus allemaal dezelfde vertakkings- en traagheidsgraad. We definiëren nu de volgende deelgroep, de decompositie-groep:

Definitie 3.5. $D = D(Q \mid P) = \{\sigma \in G \mid \sigma(Q) = Q\}$

En we definiëren de traagheidsgroep:

Definitie 3.6. $E = E(Q \mid P) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{Q} \forall \alpha \in S\}$

Uiteraard geldt dat $E \subset D$ (immers $\sigma(Q) = Q$ kan worden uitgedrukt als $\sigma(\alpha) \equiv 0 \pmod{Q}$ als $\alpha \equiv 0 \pmod{Q}$). Verder hebben we dat $\sigma \in D$ een automorfisme van S/Q induceert: Als $\sigma \in G$ kan deze worden beperkt tot een automorfisme van S . Als bovendien $\sigma \in D$, heeft de map $\bar{\sigma} : S \rightarrow S/Q$ als kern Q en dus is $\bar{\sigma}$ een automorfisme van S/Q . Omdat σK vasthoudt, houdt $\bar{\sigma}$ R/P vast en dus is $\bar{\sigma}$ een element van de galoisgroep \bar{G} van S/Q over R/P . We hebben dus een homomorfisme van $D \rightarrow \bar{G}$, welke trivaliter kern E heeft en dus hebben we een inbedding $D/E \rightarrow \bar{G}$. We zullen later zien dat deze afbeelding een isomorfisme is.

We voeren eerst notatie in: Zij H een deelgroep van G , dan noteren we met L_H het fixlichaam van H in L . En voor een $X \subset L$ noteren we X_H voor $X \cap L_H$. Dus: S_H is de ring der gehelen van L_H , Q_H is het unieke priemideaal dat onder Q ligt in L_H en S_H/Q_H is een tussenlichaam van S/Q en R/P .

We hebben nu de volgende belangrijke stelling:

	graad	lichaam	priem	vertakkingsgraad	traagheidsgraad
		L	Q		
	e			e	1
Stelling 3.17.		L_E	Q_E		
	f			1	f
		L_D	Q_D		
	r			1	1
		K	P		

Bewijs. We beginnen met $[L_D : K] = r$: $[L_D : K]$ is hetzelfde als de index van D in G . Ieder element van σD stuurt Q naar $\sigma(Q)$. Bovendien hebben we per definitie dat $\sigma D = \tau D$ dan en slechts dan als $\sigma(Q) = \tau(Q)$, we weten dat op deze manier alle priemen geraakt worden (zie stelling 3.14), we krijgen dus een bijectie tussen priemen boven P en het aantal cosets van D , hetgeen we moesten laten zien. Nu laten we zien dat $e(Q_D \mid P) = f(Q_D \mid P) = 1$. Merk op dat Q het enige priem is boven Q_D , aangezien D de galois groep van L/L_D is, deze permuteert de priemen boven Q_D (L is een normale uitbreiding van L_D), maar

D houdt Q vast, we hebben dus: $[L : L_D] = e(Q | Q_D)f(Q | Q_D)$, we weten ook dat $[L : L_D] = ef$, omdat $[L_D : K] = r$. We hebben dus dat $e(Q | Q_D) = e$ en $f(Q | Q_D) = f$, daaruit volgt dus dat $e(Q_D | P) = f(Q_D | P) = 1$.

Nu laten we zien dat $f(Q | Q_E) = 1$, per definitie dus dat $[S/Q : S_E/Q_E] = 1$. We doen dit als volgt: We laten zien dat voor iedere $\theta \in S/Q$ er een m is zodat $(x - \theta)^m$ coëfficiënten heeft in S_E/Q_E , hieruit volgt dat ieder element uit de Galoisgroep E van S/Q over S_E/Q_E θ naar een andere wortel van $(x - \theta)^m$ stuurt welke θ moet zijn en dus dat het wel de identiteit moet zijn aangezien dit voor iedere θ geldt. Kies een $\alpha \in S$, zodanig dat $\alpha \equiv \theta \pmod{Q}$. Het polynoom $g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha))$ heeft coëfficiënten in S_E . Het polynoom reduceren modulo Q geeft dat $\bar{g} \in S_E/Q_E$, maar per definitie van E reduceren alle $\sigma(\alpha)$ tot θ en dus $\bar{g} = (x - \theta)^{|E|}$. We hebben dus nu bewezen dat $f(Q | Q_E) = 1$. Uit de torenregel krijgen we dus dat $f(Q_E | Q_D) = f$. Hieruit volgt dat $[L_E : L_D] \geq f$. We hebben dat D/E ingebed is in \bar{G} , wat een groep is van orde f en dus: $[L_E : L_D] = |D/E| \leq f$. We concluderen dat $[L_E : L_D] = f$ en dus $e(Q_E : Q_D) = 1$. $[L : L_E] = e$ en $e(Q | Q_E) = e$ volgen uit de al gevonden graden. \square

Stelling 3.18. *De afbeelding $D \rightarrow \bar{G} : \sigma \mapsto \bar{\sigma}$ is surjectief met kern E en dus is $D/E \approx \bar{G}$ en D/E is cyclisch van orde f*

Bewijs. We wisten al dat $D/E \rightarrow \bar{G}$ een injectie was. Verder heeft D/E f elementen omdat $|D/E| = [L_E : L_D] = f$ (zie bewijs vorige stelling), verder weten we al dat \bar{G} cyclisch is en dus ook D/E . \square

Zij K' een deellichaam van L dat K omvat. We weten dan dat K' fixlichaam is van een zekere deelgroep van de Galoisgroep van L/K , zeg $K' = L_H$. Stel dat Q boven P ligt, dan ligt $P' = Q \cap K'$ boven P in K' . Uit de definities volgt onmiddellijk dat dan $D(Q | P') = D \cap H$ en $E(Q | P') = E \cap H$. En dus $L_{D \cap H} = L_D K'$ en $L_{E \cap H} = L_H K'$, het decompositie- en traagheidslichaam van Q over P' respectievelijk.

Lemma 3.5. *L_E is de grootste K' zodat $e(P' | P) = 1$*

Bewijs. Noteer met accenten de graden van L/K' (i.e. r', e', f').

Stel dat $e(P' | P) = 1$. Dan geldt wegens de torenformule dat $e = e'$, omdat $L_E \subset L_E K'$ en $[L : L_E] = e$ en $[L : L_E K'] = e'$, moet gelden dat $L_E = L_E K'$ en dus dat $K' \subset L_E$. \square

Stelling 3.19. *Zij K een lichaam en P een priem van K en L en M eindige lichaamsuitbreidingen van K . Als P onvertakt is in zowel L als M , dan is P onvertakt in LM*

Bewijs. Stel dat P' in LM boven P ligt. Zij F een normale uitbreiding van LM . En stel dat Q in F boven P' ligt, deze ligt dan boven P . Zij $E(Q | P)$ de traagheidsgroep met lichaam F_E , dan geldt wegens bovenstaand lemma dat $L \subset F_E$ en $M \subset F_E$ en dus dat $LM \subset F_E$. Omdat $e(Q_E | P) = 1$ volgt uit de torenregel het gestelde. \square

Stel dat P onvertakt is in L . Dan is $E(Q | P)$ triviaal. We krijgen dan dus een isomorfisme van $D(Q | P)$ naar de Galoisgroep van S/Q over R/P . De Galois groep heeft een speciale voortbrenger namelijk $\sigma : x \rightarrow x^{\|P\|}$, het element $\phi \in D$ heeft de eigenschap dat $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q} \forall \alpha \in S$, omdat $\phi \in D$

en beide groepen isomorf zijn, is er precies 1 met deze eigenschap. We noteren dit automorfisme met $\phi(Q|P)$ en noemen het het Frobenius automorfisme van Q over P . Definieer $\hat{\phi} = \sigma\phi(Q|P)\sigma^{-1}$, dan voldoet $\hat{\phi}$ aan $\hat{\phi}(\alpha) \equiv \alpha^{\|P\|} \pmod{\sigma(Q)}$. We concluderen dus dat $\hat{\sigma} = \phi(\sigma(Q)|P)$. Alle priemenvoren P zijn van de vorm $\sigma(Q)$, de conjugatieklasse van $\phi(Q|P)$ wordt dus uniek vastgelegd door P . Als bovendien G abels is, dan bestaat de conjugatieklasse uit 1 element, ϕ voldoet dan aan de congruentie voor alle Q en dus voldoet $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS}$, omdat PS het product is van alle priemenvoren P . Omdat ϕ correspondeert met een voortbrenger van \overline{G} , is de orde van $\phi(Q|P)$ f . Laten we dit samenvatten in een stelling:

Stelling 3.20. *Zij L een normale uitbreiding van K en P een priem die onvertakt is in L , Voor iedere Q boven P is er een unieke $\phi \in D \subset G$, zodat $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$, de orde van $\phi(Q|P)$ is f . Als G abels is, dan hangt ϕ alleen van P af en dan geldt: $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS}$.*

Hoofdstuk 4

Cyclotome lichaamsuitbreidingen van \mathbb{Q}

We gaan nu onze kennis toepassen op cyclotome lichamen.

Definitie 4.1. Stel $\omega_m = e^{2\pi i/m}$. $\mathbb{Q}[\omega_m]$ heet het m 'de cyclotome lichaam.

Stelling 4.1. Zij m oneven dan $\mathbb{Q}[\omega_m] = \mathbb{Q}[\omega_{2m}]$

Bewijs. Uiteraard geldt $\mathbb{Q}[\omega_m] \subset \mathbb{Q}[\omega_{2m}]$. We laten nu zien dat $\omega_{2m} \in \mathbb{Q}[\omega_m]$, merk op dat $\omega_{2m}^m = -1$ oftewel $\omega_{2m} = -\omega_{2m}^{m+1} = -(\omega_{2m}^2)^{(m+1)/2} = -\omega_m^{(m+1)/2} \in \mathbb{Q}[\omega_m]$ \square

Definitie 4.2. De Euler ϕ functie is gedefinieerd door:

$$\phi(m) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq m, (k, m) = 1\}|$$

Stelling 4.2. Als $n = p_1^{n_1} \dots p_r^{n_r}$, dan $\phi(n) = \prod_i (p_i^{n_i} - p_i^{n_i-1})$

Bewijs. Merk op dat $\phi(m) = |(\mathbb{Z}/m)^*|$. Stel dat $(k, l) = 1$, dan is $\phi(kl) = \phi(k)\phi(l)$ vanwege de chinese reststelling: $\mathbb{Z}_{kl}^* \approx \mathbb{Z}_k^* \times \mathbb{Z}_l^*$. Het is dus voldoende te bewijzen dat $\phi(p^k) = p^k - p^{k-1}$, dit volgt gelijk uit de definitie. \square

Stelling 4.3. $[\mathbb{Q}[\omega_m] : \mathbb{Q}] = \phi(m)$

Bewijs. We laten zien dat de geconjugeerden van ω_m precies ω_m^k zijn met $(k, m) = 1$. Merk op dat ω_m voldoet aan $x^m - 1 = 0$. Het irreducibele polynoom moet dus delen op $x^m - 1$. Verder zijn de geconjugeerden van ω_m geen n 'de machten voor $n < m$, anders zou het irreducibele polynoom moeten delen op $x^n - 1$, maar omdat $\omega_m^n \neq 1$ is dit onmogelijk, dit geeft de eis dat $(k, m) = 1$. Nu laten we zien dat dit een voldoende eis is. Het is nu voldoende te laten zien dat als θ een geconjugeerde is die voldoet aan de eis, dat dan ook θ^p een geconjugeerde is voor iedere $p \nmid m$ (dit komt namelijk neer op het priemfactoriseren van k en dan het procedé te beginnen met ω_m en daaruit ω_m^k te vormen). Laat f het monisch irreducibele polynoom van θ zijn. Dan is $x^m - 1 = f(x)g(x)$ met f, g zo gekozen dat $f(x), g(x)$ monische polynomen over \mathbb{Q} zijn. Lemma 2.1 geeft nu dat dan

$f \in \mathbb{Z}[x]$. θ^p is een wortel van $x^m - 1$ en is dus een wortel van minstens één van beide. We laten zien dat het een wortel van f is. Stel $g(\theta^p) = 0$, dan is θ een wortel van $g(x^p)$, hieruit volgt dat $f(x)$ deelt op $g(x^p)$ en wederom in $\mathbb{Z}[x]$. Reduceer nu de coëfficiënten modulo p . We krijgen dan dat \bar{f} deelt op $\bar{g}(x^p)$. Maar $\bar{g}(x^p) = (\bar{g}(x))^p$ omdat $\mathbb{Z}_p[x]$ een uniek factorisatie domein is, hebben \bar{f} en \bar{g} een gemeenschappelijke factor, zeg \bar{h} . Dit impliceert dat $\bar{h}^2 \mid \bar{f}\bar{g} = x^m - \bar{1}$. Stel $\bar{k}\bar{h}^2 = x^m - 1$, de formele afgeide nemen geeft $\bar{k}'\bar{h}^2 + 2\bar{h}\bar{h}'\bar{k} = \bar{m}x^{m-1}$, oftewel $\bar{h} \mid \bar{m}x^{m-1}$, omdat $\bar{m} \not\equiv 0 \pmod{p}$ is \bar{h} van de vorm $\bar{a}x^\beta$, maar \bar{h} deelt $x^m - \bar{1}$, hetgeen niet kan. \square

Stelling 4.4. $Gal(\mathbb{Q}[\omega_m]/\mathbb{Q}) \approx \mathbb{Z}_m^*$ i.e. de eenhedengroep van \mathbb{Z} modulo m .

Bewijs. Een lichaamsautomorfisme ligt vast als opgegeven wordt wat hij moet doen met ω_m , wat weer een wortel is van het irreducibele polynoom, dus $\sigma(\omega_m) = \omega_m^{k_\sigma}$ met $(k_\sigma, m) = 1$. Dit geeft dus een bijjectie ψ tussen de Galoisgroep en \mathbb{Z}_m^* , namelijk $\psi(\sigma) = k_\sigma$. Het is nu voldoende te laten zien dat dit een homomorfisme is: $\psi(\sigma \circ \tau) = \psi(x \mapsto x^{k_\sigma k_\tau}) = k_\sigma k_\tau = \psi(\sigma)\psi(\tau)$. \square

Stelling 4.5. Voor even m zijn de $\mathbb{Q}[\omega_m]$ niet isomorf.

Bewijs. We bewijzen dat in $\mathbb{Q}[\omega_m]$ precies de m 'de machts eenheidswortels voorkomen. Stel $\theta = e^{2\pi i h/k}$ met $(h, k) = 1$ is een k 'de machtswortel in $\mathbb{Q}[\omega_m]$, dan bevat $\mathbb{Q}[\omega_m]$ ook een r 'de machtswortel met $r = lcm(k, m) = km/(k, m)$: kies $u, v \in \mathbb{Z}$ zodat $ku + hmv = (k, hm) = (k, m)$ dan is $e^{2\pi i/r} = \omega_m^u \theta^v$. Maar dan $\mathbb{Q}[\omega_r] \subset \mathbb{Q}[\omega_m]$ wat impliceert dat $\phi(r) \leq \phi(m)$. We gebruiken de formule voor ϕ , als $x = p_1^{n_1} \dots p_r^{n_r}$, dan $\phi(x) = \prod_i (p_i^{n_i} - p_i^{n_i-1})$. Schrijf nu $r = cm$, als $c \neq 1, 2$, dan geldt kijkend naar de formule dat $\phi(cm) > \phi(m)$ voor iedere m , als $c = 2$ merken we op dat m even is en geldt dus als nog $\phi(cm) > \phi(m)$, we komen dus tot de conclusie dat $c = 1$ en dus dat $r = m$, wat impliceert dat $k \mid m$, zeg $m = kl$, dan $\theta = \omega_m^{hl}$. θ is dus een m 'de machtswortel van één. Omdat een isomorfisme eenheidswortels respecteert volgt hieruit meteen de stelling door te kijken naar het aantal eenheidswortels. \square

Stelling 4.6. $\mathbb{A} \cap \mathbb{Q}[\omega_m] = \mathbb{Z}[\omega_m]$

Bewijs. We bewijzen eerst de volgende lemma's:

Lemma 4.1. $\mathbb{Z}[1 - \omega_m] = \mathbb{Z}[\omega_m]$ en $disc(\omega_m) = disc(1 - \omega_m)$.

Bewijs. Het eerste is triviaal, omdat $\omega_m = 1 - (1 - \omega_m)$. Het tweede volgt uit stelling 2.8: $disc(\omega_m) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \prod_{1 \leq r < s \leq n} ((1 - \alpha_r) - (1 - \alpha_s))^2 = disc(1 - \omega_m)$ \square

Lemma 4.2. Als $m = p^r$ met p een priemgetal dan is $\prod_{1 \leq k \leq m, p \nmid k} (1 - \omega_m^k) = p$

Bewijs. Merk op dat $f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + \dots + x^{(p-1)p^{r-1}}$ en dat ω_m^k , met k als in de stelling, wortel is van de teller, maar niet van de noemer. Merk verder op dat $\phi(p^r) = (p-1)p^{r-1}$ het aantal waarden is dat k aanneemt, kennelijk zijn de ω_m^k alle wortels van $f(x)$ maar dan is dus $f(x) = \prod_{1 \leq k \leq m, p \nmid k} (x - \omega_m^k)$, omdat $f(1) = p$ volgt nu het lemma. \square

Lemma 4.3. $disc(\omega_m) \mid m^{\phi(\omega_m)}$

Bewijs. We weten dat $x^m - 1 = f(x)g(x)$ met $f(x)$ het irreducibele polynoom voor ω_m . Differentiëren en $x = \omega_m$ invullen geeft $m = \omega_m f'(\omega_m)g(\omega_m)$, de norm aan beide kanten nemend geeft $m^{\phi(m)} = \pm \text{disc}(\omega_m)N(\omega_m g(\omega_m))$ (Stelling 2.8). Omdat $xg(x) \in \mathbb{Z}[x]$ geldt dat $N(\omega_m g(\omega_m)) \in \mathbb{Z}$ (Stelling 2.2 en 2.4), dus $\text{disc}(\omega_m) \mid m^{\phi(\omega_m)}$. \square

Lemma 4.4. *Als $m = p^r$ met p een priemgetal dan is $\mathbb{A} \cap \mathbb{Q}[\omega_m] = \mathbb{Z}[\omega_m]$*

Bewijs. Stelling 2.10 zegt dat iedere $\alpha \in R = \mathbb{A} \cap \mathbb{Q}[\omega_m]$ geschreven kan worden als $\frac{m_1 + m_2(1-\omega_m) + \dots + m_n(1-\omega_m)^{n-1}}{d}$ met $n = \phi(m) = \phi(p^r)$ en $d = \text{disc}(1-\omega_m) = \text{disc}(\omega_m)$. Het vorige lemma geeft dat d een macht van p moet zijn. We weten dat geldt $\mathbb{Z}[\omega_m] \subset R \subset \frac{\mathbb{Z}[\omega_m]}{d}$, stel dat $\mathbb{Z}[\omega_m] \neq R$. Zeg $x \in R - \mathbb{Z}[\omega_m]$, zeg $x = \frac{m_1 + m_2(1-\omega_m) + \dots + m_n(1-\omega_m)^{n-1}}{d}$, dan is er een kleinste i met $d \nmid m_i$, dan ook $\beta = \frac{m_i(1-\omega_m)^{i-1} + \dots + m_n(1-\omega_m)^{n-1}}{p} \in R - \mathbb{Z}[\omega_m]$ met $p \nmid m_i$. Lemma 4.2 geeft dat $p/(1-\omega_m)^n \in \mathbb{Z}[\omega_m]$ omdat $(1-\omega_m^k)/(1-\omega_m) \in \mathbb{Z}[\omega_m]$. Hieruit volgt dat $p/(1-\omega_m)^i \in \mathbb{Z}[\omega_m]$ en dus dat $\beta p/(1-\omega_m)^i \in R$, dit uitschrijvend en opmerkend dat afgezien van de eerste term alle andere termen in $\mathbb{Z}[\omega_m]$ en dus in R zitten, komen we tot de conclusie dat $m_i/(1-\omega_m) \in R$. Normen nemen geeft dat $N(1-\omega_m) \mid N(m_i)$, maar lemma 4.2 geeft dat $N(1-\omega_m) = p$ en $N(m_i) = m_i^n$, tegenspraak met $p \nmid m_i$. \square

Bewijs stelling 4.6:

Gezien het vorige lemma is het voldoende te bewijzen dan als m_1, m_2 relatief priem zijn en $\mathbb{A} \cap \mathbb{Q}[\omega_{m_1}] = \mathbb{Z}[\omega_{m_1}]$ en $\mathbb{A} \cap \mathbb{Q}[\omega_{m_2}] = \mathbb{Z}[\omega_{m_2}]$, dat dan $\mathbb{A} \cap \mathbb{Q}[\omega_m] = \mathbb{Z}[\omega_m]$ met $m = m_1 m_2$. We gebruiken stelling 2.13. We gaan daar dus de voorwaarden van na. Eerst $\mathbb{Q}[\omega_m] = \mathbb{Q}[\omega_{m_1}]\mathbb{Q}[\omega_{m_2}]$: omdat $(m_1, m_2) = 1$ zijn er $u, v \in \mathbb{Z}$ zodat $um_1 + vm_2 = 1$, hieruit volgt dat $\omega_m = \omega_{m_1}^v \omega_{m_2}^u$, oftewel $\mathbb{Q}[\omega_m] \subset \mathbb{Q}[\omega_{m_1}]\mathbb{Q}[\omega_{m_2}]$, de andere inclusie geldt altijd, oftewel $\mathbb{Q}[\omega_m] = \mathbb{Q}[\omega_{m_1}]\mathbb{Q}[\omega_{m_2}]$, analoog geldt $\mathbb{Z}[\omega_{m_1}]\mathbb{Z}[\omega_{m_2}] = \mathbb{Z}[\omega_m]$. Omdat m_1 en m_2 relatief priem zijn geldt dat $[\mathbb{Q}[\omega_m] : \mathbb{Q}] = \phi(m) = \phi(m_1)\phi(m_2)$. Uit lemma 4.3 volgt dat $\text{disc}(\omega_i) \mid m_i^{\phi(m_i)}$, omdat $(m_1, m_2) = 1$ volgt hieruit dat $\text{disc}(\omega_{m_1})$ en $\text{disc}(\omega_{m_2})$ geen gemeenschappelijke delers hebben en dus dat $(\text{disc}(\omega_{m_1}), \text{disc}(\omega_{m_2})) = 1$. Stelling 2.13 geeft nu dat $\mathbb{A} \cap \mathbb{Q}[\omega_m] = \mathbb{Z}[\omega_{m_1}]\mathbb{Z}[\omega_{m_2}] = \mathbb{Z}[\omega_m]$. \square

Omdat $\mathbb{Q}[\omega_m]$ een normale uitbreiding is (alle nulpunten van het irreducibele polynoom zitten er in) geeft stelling 3.15 dat alle traagsheids- en vertakkingsgraden hetzelfde zijn. Als er r priemen boven (p) in $\mathbb{Z}[\omega_m]$ liggen dan geldt dus dat $\phi(m) = \text{ref}$. De volgende stelling geeft uitdrukkingen voor e en f .

Stelling 4.7. *Schrijf $m = p^k n$ met $p \nmid n$. Dan is de vertakkingsgraad e van een priem in $\mathbb{Z}[\omega_m]$ $\phi(p^k)$ en de traagheidsgraad f is de multiplicatieve orde van $p \pmod{n}$ (i.e. de kleinste waarde l zodat $p^l \equiv 1 \pmod{n}$), zo'n getal bestaat omdat $(p, n) = 1$)*

Bewijs. Eerst een lemma:

Lemma 4.5. *Stel dat p een priemgetal dan is $p = u(1 - \omega_{p^r})^{\phi(p^r)}$ met u een eenheid in $\mathbb{Z}[\omega_{p^r}]$*

Bewijs. Definieer $m = p^r$ (alleen hier in dit lemma!). We gebruiken lemma 4.2: $\prod_{1 \leq k \leq m, p \nmid k} (1 - \omega_m^k) = p$, delen door $(1 - \omega_m)^{\phi(m)}$ geeft $\frac{p}{(1 - \omega_m)^{\phi(m)}} = \prod_{1 \leq k \leq m, p \nmid k} \frac{(1 - \omega_m^k)}{(1 - \omega_m)} = \prod_{1 \leq k \leq m, p \nmid k} (1 + \omega_m + \dots + \omega_m^{k-1})$. We bewijzen nu dat $(1 + \omega_m + \dots + \omega_m^{k-1})$ een eenheid is. De kandidaat inverse is uiteraard $\frac{(\omega_m^k - 1)}{(\omega_m - 1)}$. We moeten alleen nog bewijzen dat deze ook in $\mathbb{Z}[\omega_m]$ zit. Merk op dat $(k, m) = (k, p^r) = 1$. Kies h, k zodat $hk + lm = 1$ dan is $\omega_m = \omega_m^{hk}$, maar dan $\frac{(\omega_m^{hk} - 1)}{(\omega_m^k - 1)} \in \mathbb{Z}[\omega_m]$. \square

We bekijken $\omega_m^n = \omega_{p^k}$ en $\omega_m^{p^k} = \omega_n$. We gaan eerst onderzoeken hoe (p) splijt in $\mathbb{Z}[\omega_{p^k}]$ en $\mathbb{Z}[\omega_n]$. Als $p \mid m$ (als $p \nmid m$ is alles ook ok, alleen zijn dan dingen triviaal/overbodig) dan hebben we de ontbinding van p in $\mathbb{Z}[\omega_{p^k}]$ als in het lemma. $1 - \omega_{p^k}$ is geen eenheid en dus is $(1 - \omega_{p^k})$ een niet-triviaal ideaal in $\mathbb{Z}[\omega_{p^k}]$. Dus $p\mathbb{Z}[\omega_{p^k}] = (1 - \omega_{p^k})^{\phi(p^k)}$, stelling 3.15 geeft dat $(1 - \omega_{p^k})$ een priemideaal moet zijn aangezien $\phi(p^k) = [\mathbb{Q}[\omega_{p^k}] : \mathbb{Q}] = \text{ref}$, verdere factorisatie zou een te hoge e geven. We hebben dus $p\mathbb{Z}[\omega_{p^k}]$ gepriemfactoriseerd! Nu gaan we naar $\mathbb{Z}[\omega_n]$ kijken. Omdat $p \nmid n$ is (p) onvertakt (stelling 3.16). Schrijf dus $p\mathbb{Z}[\omega_n] = P_1 \dots P_s$ met de P_i onderling verschillend en stel dat g de traagheidsgraad is van $P = P_i$ (zijn allemaal hetzelfde). We hebben dan dat $\phi(n) = sg$. We gaan bewijzen dat g de orde is van $p \pmod n$ i.e. $g = f$. De Galoisgroep van $\mathbb{Q}[\omega_n]$ is isomorf met \mathbb{Z}_n^* . Laat σ het automorfisme zijn dat bij $p \pmod n$ hoort ($p \in \mathbb{Z}_n^*$ omdat $(p, n) = 1$), i.e. $\sigma(\omega_n) = \omega_n^p$, we hebben nu dat $|\langle \sigma \rangle| = \text{ord}(\sigma) = \text{ord}(p \pmod n) = f$, met f als in de stelling. De Galoisgroep van $\mathbb{Z}[\omega_n]/P$ over \mathbb{Z}_p is van orde g , omdat $g = [\mathbb{Z}[\omega_n]/P : \mathbb{Z}_p]$ (per definitie). Bovendien is de Galoisgroep cyclisch:

Lemma 4.6. *De galoisgroep van $F = \mathbb{Z}[\omega_n]/P$ over \mathbb{Z}_p is cyclisch en wordt voortgebracht door $\tau(x) = x^p$. De orde van τ is g .*

Bewijs. F is een lichaam met eindig veel elementen, derhalve moet de groep $F^* = F - \{0\}$ cyclisch zijn, immers, als we F^* schrijven als: $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r}$ (additief) met $d_i \mid d_{i+1}$ (dit kan met iedere eindige abelse groep, zie Armstrong, Groups and Symmetry: Theorem 21.1), dan voldoet ieder element van de groep aan $x^{d_r} = 1$ en heeft $p^g - 1$ wortels (aantal elementen van F^*), dus $d_r \geq p^n - 1 = |F^*|$, oftewel $d_r = |F^*|$, maar dan is $F^* \approx \mathbb{Z}_{d_r}$. Met binomiaal ontwikkeling is makkelijk in te zien dat τ een homomorfisme is. τ is ook een isomorfisme aangezien hij injectief is (omdat het lichaam eindig is volgt hier onmiddellijk uit dat deze ook surjectief is): De vergelijking $x^p = y^p$ is dezelfde als $(x - y)^p = 0$ en dus $x = y$. Verder is de orde van τ g : $\tau^g(x) = x^{p^g} = x$, omdat $p^g - 1$ het aantal elementen in de Galoisgroep is, de orde kan niet lager zijn, aangezien er een element van orde $p^g - 1$ in zit (F^* is immers cyclisch). \square

We willen nu bewijzen dat $f = g$. We bewijzen dat σ en τ dezelfde orde hebben, het is voldoende te laten zien dat $\sigma^a = 1$ dan en slechts dan als $\tau^a = 1$ voor iedere $a \in \mathbb{Z}$. Duidelijk is dat $\sigma^a(x) = x$ dan en slechts dan als $\omega_n^{p^a} = \omega_n$ en dat is waar dan en slechts dan als $p^a \equiv 1 \pmod n$. Anderzijds is omdat τ additief is, is $\tau^a(x) = x^{p^a} = x$ dan en slechts dan als $\omega_n^{p^a} \equiv \omega_n \pmod P$. Als $p^a \equiv 1 \pmod n$ is het evident dat $\omega_n^{p^a} \equiv \omega_n \pmod P$. Stel nu $\omega_n^{p^a} \equiv \omega_n \pmod P$, stel dat $p^a \equiv b \pmod n$, we moeten bewijzen $b = 1$. Er geldt

$\omega_n \equiv \omega_n^{p^a} \equiv \omega_n^b \pmod{P}$. Omdat ω_n een eenheid is in $\mathbb{Z}[\omega_n]$ volgt hieruit dat $\omega_n^{b-1} \equiv 1 \pmod{P}$. We hebben nu nog een lemma nodig:

Lemma 4.7. $n = (1 - \omega_n) \dots (1 - \omega_n^{n-1})$

Bewijs. Merk op dat $x^n - 1$ als wortels ω_n^k met $k = 0, 1, \dots, n-1$ heeft. Dus $x^n - 1 = (x - 1) \prod_{k=1}^{n-1} (x - \omega_n^k)$, aan beide kanten delen door $x - 1$ en $x = 1$ invullen geeft het gewenste resultaat. \square

Stel nu dat $b > 1$ dan zit één van de factoren in het produkt, maar dan $n \in P$, maar omdat $(n, p) = 1$ en $p \in P$ impliceert dit $1 \in P$, oftewel $P = \mathbb{Z}[\omega_n]$, tegenspraak. Dus $f = g$. Nu zijn we er bijna:

Kies voor iedere P_i priem in $\mathbb{Z}[\omega_n]$ een priem Q_i in $\mathbb{Z}[\omega_m]$, alle Q_i liggen boven (p) omdat de P_i dat liggen. Q_i moet boven $(1 - \omega_{p^k})$ in $\mathbb{Z}[\omega_{p^k}]$ liggen, omdat dat het enige priem was dat boven (p) lag. Er geldt zeker dat $e(Q_i | (p)) \geq e((1 - \omega_{p^k}) | (p)) = \phi(p^k)$ en dat $f(Q_i | (p)) \geq f(P_i | (p)) = f$ (zie stelling 3.11). Stelling 3.15 geeft dat $rf = \phi(n)$, en dus dat $\phi(m) = \phi(p^k)rf$ (omdat $(p^k, n) = 1$). Aan de andere kant hebben we ook dat $\phi(m) = \hat{r}e(Q_i | (p))f(Q_i | (p))$ met \hat{r} het aantal priemen Q_i boven (p) in $\mathbb{Z}[\omega_m]$ (merk op dat $\hat{r} \geq r$). We zien dus dat de ongelijkheden eigenlijk gelijkheden zijn en dat $\hat{r} = r$. \square

Een direct gevolg van de stelling, namelijk als $k = 0$ geeft het volgende lemma:

Lemma 4.8. *Stel dat $p \nmid m$ dan splitst (p) in $\phi(m)/f$ verschillende idealen in $\mathbb{Z}[\omega_m]$ met f de orde van $p \pmod{m}$*

Hoofdstuk 5

Cyclotome lichaamsuitbreidingen van $\mathbb{F}_q[T]$

Het laatste deel van het vorige hoofdstuk ging over cyclotome lichaamsuitbreidingen over \mathbb{Q} . We gaan nu een zelfde soort theorie ontwikkelen maar dan over het functielichaam $\mathbb{F}_q(T)$.

Definitie 5.1. *Zij k een lichaam. Een additief polynoom is een polynoom over k dat voldoet aan $f(x+y) = f(x) + f(y)$ voor alle $x, y \in k$*

Stelling 5.1. *Stel k is een lichaam en $f \in k[x]$ een additief polynoom. Als k karakteristiek 0 heeft dan is er een $a \in k$ zodat $f(x) = ax$ als k karakteristiek p met p een priemgetal dan is er een $r \in \mathbb{N}$ en $a_0, \dots, a_r \in K$ zodat $f(x) = a_0x + a_1x^p + \dots + a_rx^{p^r}$*

Bewijs. Omdat f een additief polynoom is geldt dus $f(x+y) = f(x) + f(y)$. De formele afgeleide naar x nemend en $x = 0$ in te vullen zien we dat $f'(y) = f'(0)$, oftewel $f'(y)$ is constant. Schrijf nu $f(x) = \sum_{j=1}^n b_j x^j$, dan is $f'(x) = \sum_{j=1}^n j b_j x^{j-1}$. Als de karakteristiek van k 0 is, volgt hieruit dat $f(x) = a + bx$ voor zekere $a, b \in k$. Maar uit $f(x+y) = f(x) + f(y)$ in $x = y = 0$ volgt dat $f(0) = 0$ oftewel $b = 0$. Stel nu dat de karakteristiek p is. Dan is f' constant dan en slechts dan als $b_i = 0$ voor alle $i > 1$ met $p \nmid i$. Schrijf dus $f(x) = b_1x + \sum_j b_{pj}x^{pj} = b_1x + (\sum_j b_{pj}^{\frac{1}{p}}x^j)^p = b_1x + g(x)^p$, waarbij gebruikt is dat $(v+w)^p = v^p + w^p$ in een lichaam van karakteristiek p , merk wel op dat $g(x)$ in het algemeen niet meer in $k[x]$ ligt, maar in $k_1[x]$ waar de p 'de machtswortels van de b_{pj} aan k toegevoegd zijn. Omdat f een additief polynoom is en a_0x ook is $g(x)^p$ dat ook in $k_1[x]$. Dus $g(x+y)^p = g(x)^p + g(y)^p = (g(x) + g(y))^p$. Omdat $k_1[x, y]$ een uniek factorisatie domein is (zie Serge Lang, Undergraduate Algebra, Chapter 4), volgt hieruit dat $g(x+y) = \xi(g(x) + g(y))$ met $\xi \in k_1$. $y = 0$ invullen geeft $\xi = 1$. g is dus weer een additief polynoom en dus is g van de vorm: $\sum_j c_j x^{p^j} + cx$ en dus is f van de vorm: $f(x) = e_1x + e_2x^p + \sum_j d_j x^{p^{2j}}$, hetzelfde procedé kunnen we weer toepassen op $\sum_j d_j x^{p^{2j}}$, uiteindelijk komen we uit dat f van de vorm is als in de stelling en deze f is duidelijk additief. \square

We definiëren $\mathcal{A}[k]$ als de verzameling van alle additieve polynomen over k . We maken er een ring van door de vermenigvuldiging van twee additieve polynomen de samen steling te laten zijn, i.e. $fg \equiv f \circ g$. We moeten natuurlijk controleren dat dit weer een additief polynoom is: $(f \circ g)(x+y) = f(g(x+y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y)) = (f \circ g)(x) + (f \circ g)(y)$. De optelling van additieve polynomen is de gewone components gewijze optelling, welke ook een additief polynoom geeft. De eenheid in de ring is de functie x en de 0 is de nulfunctie. In het vervolg nemen we aan dat we in karakteristiek $p > 0$ werken. Stel dat \mathbb{F} een lichaam is met p^s elementen (met karakteristiek $p > 0$). We nemen in het vervolg het lichaam $k = \mathbb{F}(T)$ (i.e. elementen van de vorm $f(T)/g(T)$ met $f(t), g(t) \in \mathbb{F}[T]$). We kunnen nu alle additieve polynomen over dit lichaam bekijken, maar dat zijn er te veel, we willen namelijk ook nog eisen dat $f(\alpha x) = \alpha f(x)$ voor alle $\alpha \in \mathbb{F}$ en $f \in k[x] = \mathbb{F}(T)[x]$. Dit komt er op neer dat $\alpha^{p^i} = \alpha$ voor iedere $\alpha \in \mathbb{F}$, hieraan is zeker voldaan als $s \mid i$, dit is zelfs noodzakelijk omdat F^* een cyclische groep is met $p^s - 1$ elementen (zie Lang, Undergraduate Algebra, Chapter 8 Theorem 3.1). We bekijken dus polynomen van de vorm $\sum_{i=0}^n a_i x^{p^{si}}$ met $a_i \in \mathbb{F}(T)$, we noemen deze verzameling $\mathcal{A}^{\mathbb{F}}$.

Definitie 5.2. Een Drinfeld moduul voor $\mathbb{F}[T]$ over $\mathbb{F}(T)$ is een ringhomomorfisme $\rho : \mathbb{F}[T] \rightarrow \mathcal{A}^{\mathbb{F}}$ dat \mathbb{F} vasthoudt en zodat voor iedere $f \in \mathbb{F}[T]$ de lineaire term van het additieve polynoom $\rho(f) \in \mathcal{A}^{\mathbb{F}}$ $x f(T)$ is en dat er bovendien een $f \in \mathbb{F}[T]$ bestaat met $\rho(f) \notin x \mathbb{F}(T)$.

Merk op dat in $\mathbb{F}[T]$ de vermenigvuldiging de gewone vermenigvuldiging is terwijl in $\mathcal{A}^{\mathbb{F}}$ de vermenigvuldiging gegeven wordt door samenstelling. Verder merken we op dat ρ helemaal vastligt door te specificeren wat er met T gebeurt, immers $\rho(\sum_{i=0}^n a_i T^i) = \sum_{i=0}^n \rho(a_i T^i) = \sum_{i=0}^n a_i \rho(T^i) = \sum_{i=0}^n a_i \rho(T)^i$, waarbij $\rho(T)^0 = x$. Verder moet $\rho(T)$ van de vorm $Tx + f(x)$ met $f(x) \in \mathcal{A}^{\mathbb{F}}$ met graad groter dan 1. We kunnen eens naar het Drinfeldmoduul kijken die gedefinieerd is door $\rho(T) = Tx + x^{p^s}$, de eenvoudigste die je kunt opschrijven. Er geldt dan bijvoorbeeld dat $\rho(T^2) = \rho(T) \circ \rho(T) = T^2x + Tx^{p^s} + T^{p^s}x^{p^s} + x^{p^{2s}}$. We moeten natuurlijk nog bewijzen dat op deze manier echt een Drinfeld moduul geconstrueerd wordt.

Stelling 5.2. Als je $\rho : \mathbb{F}[T] \rightarrow \mathcal{A}^{\mathbb{F}}$ definieerd door $\rho(T)(x) = Tx + c_1 x^{p^s} + \dots + c_r x^{p^{rs}}$ met $c_r \neq 0 \in \mathbb{F}(T)$ en $r > 0$, dan is ρ een Drinfeld moduul. De graad van $\rho(f)$ is $p^{\deg(f)sr}$, r heet de rang van ρ

Bewijs. Duidelijk is, omdat $c_r \neq 0$ dat $\rho(T) \notin x \mathbb{F}(T)$. Het is voldoende te laten zien dat de constante term van $\rho(T^n) x T^n$ is (omdat $\rho(T) \in \mathcal{A}^{\mathbb{F}}$), hetgeen meteen volgt aangezien de lineaire term van $\rho(T^n)$ T maal de lineaire term van $\rho(T^{n-1})$ is. We moeten nu nog bewijzen dat ρ een ringhomomorfisme is, hij is duidelijk additief, we moeten dus nog laten zien dat $\rho(f) \circ \rho(g) = \rho(fg)$, stel dat $f = \sum a_i T^i$ en $g = \sum b_j T^j$ dan $\rho(f) \circ \rho(g) = \rho(f)(\sum b_j \rho^j(T)) = \sum a_i b_j (\rho^i(T) \circ \rho^j(T)) = \sum a_i b_j \rho^{i+j}(T) = \sum a_i b_j \rho(T^{i+j}) = \rho(fg)$. Stel dat p^t is de hoogste macht van $\rho(x^m)$ dan is p^{rs+t} de hoogste macht van $\rho(x^{m+1})$, de graad van $\rho(x)$ is dus p^{rs} van $\rho(x^2)$ is p^{2rs} en in het algemeen is dus de graad van $\rho(x^k)$ p^{krs} , voor de graad van $\rho(f)$ moet je enkel naar $\rho(x^m)$ kijken met $m = \deg(f)$, waaruit het gestelde volgt. \square

De definitie van een Drinfeldmoduul ziet er op het eerste gezicht nogal gekunsteld uit, om de achterliggende redenen te zien definiëren we nu eerst een moduul:

Definitie 5.3. *Zij R een ring. Een (links) R -moduul M is een abelse (additieve) groep, met een actie van een ring, i.e. er is een afbeelding $R \times M \rightarrow M : (a, m) \mapsto am$ zodanig dat voor $a, b \in R$ en alle $m, n \in M$ geldt:*

$$\begin{aligned} a(m+n) &= am + an \\ (a+b)m &= am + bm \\ a(bm) &= (ab)m \\ 1m &= m \end{aligned}$$

Bekijk $\overline{\mathbb{F}(T)}$ (de algebraïsche sluiting van $\mathbb{F}(T)$), we kunnen nu een $\mathbb{F}[T]$ -moduul definiëren, $\overline{\mathbb{F}(T)}$ speelt de rol van de optelgroep en $\mathbb{F}[T]$ speelt de rol van de ring. De afbeelding is $\mathbb{F}[T] \times \overline{\mathbb{F}(T)} \rightarrow \overline{\mathbb{F}(T)} : a \cdot u = \rho(a)(u)$, waarbij u dus in het door ρ verkregen polynoom geëvalueerd wordt, we noteren dit moduul met $\overline{\mathbb{F}(T)}_\rho$.

Stelling 5.3. $\overline{\mathbb{F}(T)}_\rho$ is een $\mathbb{F}[T]$ -moduul.

Bewijs. Het bewijs is niet moeilijk maar geeft wel duidelijk weer waar de definities vandaan komen.

$$\begin{aligned} a(m+n) &= \rho(a)(m+n) = \rho(a)(m) + \rho(a)(n) = am + an \text{ (additiviteit van de polynomen),} \\ (a+b)m &= \rho(a+b)(m) = \rho(a)(m) + \rho(b)(m) = am + bm \text{ (ringhomomorfisme),} \\ a(bm) &= \rho(a)(bm) = \rho(a)(\rho(b)(m)) = (\rho(a) \circ \rho(b))(m) = \rho(ab)(m) = ab(m) \text{ (ringhomomorfisme),} \\ 1(m) &= \rho(1)(m) = x(m) = m \text{ (Drinfeld moduul)} \quad \square \end{aligned}$$

Definitie 5.4. *Een deelmoduul N van een (links) R -moduul is een deelgroep van M die gesloten is onder de actie van de ring i.e. een $N \subset M$ zodat voor $a, b \in N$ en alle $r \in R$ geldt:*

$$\begin{aligned} 0 &\in N, \quad a - b \in N \\ ra &\in N \end{aligned}$$

We kunnen nu deelmodulen definiëren als:

$$\Lambda_\rho[a] = \{\lambda \in \overline{\mathbb{F}(T)} \mid \rho(a)(\lambda) = 0\}$$

Laten we controleren dat dit inderdaad een deelmoduul is. Duidelijk geldt dat $\rho(a)(0) = 0$, stel dat $\rho(a)(\lambda_1) = 0$ en $\rho(a)(\lambda_2) = 0$ dan is $\rho(a)(\lambda_1 - \lambda_2) = \rho(a)(\lambda_1) - \rho(a)(\lambda_2) = 0$ en als $r \in \mathbb{F}[T]$ dan is $\rho(a)(r\lambda_1) = \rho(ar)(\lambda_1) = \rho(ra)(\lambda_1) = \rho(r) \circ \rho(a)(\lambda_1) = \rho(r)(0) = 0$.

We definiëren nu een R -moduulhomomorfisme:

Definitie 5.5. *Stel dat M, N (links) R -modulen zijn, en $f : M \rightarrow N$ een afbeelding. f heet een R -moduulhomomorfisme als voor alle $x, y \in M$ en $r \in R$ geldt:*

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(rx) &= rf(x) \end{aligned}$$

Als f bijectief is, heet f een isomorfisme, automatisch is dan $f^{-1} : N \rightarrow M$ ook een R -moduulhomomorfisme, als zo'n bijectie f bestaat schrijven we $M \approx N$, 'M is isomorf met N'.

Modulen kunnen ook uitgedeeld worden:

Definitie 5.6. Zij N een deelmoduul van het R -moduul M . N is een normale ondergroep van M en dus is M/N goed gedefinieerd, we definiëren de vermenigvuldiging: $R \times M/N \rightarrow M/N : (r, \overline{m}) \mapsto \overline{r\overline{m}}$

Er wordt eenvoudig nagegaan dat dit inderdaad goed gedefinieerd is.

Definitie 5.7. Stel dat M_1, \dots, M_r deelmodulen zijn van M als ieder element in $m \in M$ te schrijven is als $m = m_1 + \dots + m_r$ met $m_i \in M_i$ en $M_i \cap M_j = \{0\}$ als $i \neq j$ dan schrijven we $M = M_1 \oplus \dots \oplus M_r$.

We definiëren $A = \mathbb{F}[T]$ en $q = p^s = |\mathbb{F}|$. En tevens $\rho(a)(x) = \rho_a(x)$ en $k = \mathbb{F}(T)$

Stelling 5.4. Stel dat ρ een Drinfeld moduul is van rang r en $a \neq 0$, dan is $\Lambda_\rho[a] \approx A/aA \oplus \dots \oplus A/aA$ ($r \times$)

Bewijs. We bewijzen eerst dat $\Lambda_\rho[a]$ $q^{r \deg(a)}$ elementen heeft. Schrijf $\rho_a(x) = ax + \dots + b_{r \deg(a)} x^{r \deg(a)}$, dan is $\rho'_a(x) = a \neq 0$, ρ_a heeft dus geen dubbele nulpunten en dus heeft $\Lambda_\rho[a]$ $q^{r \deg(a)}$ elementen.

Schrijf nu $a = \alpha P_1^{e_1} \dots P_t^{e_t}$, met $\alpha \in F^*$ en $P_i \in A$ de irreducibele factoren van a . Dan is $\Lambda_\rho[a] \approx \bigoplus_{i=1}^t \Lambda_\rho[P_i^{e_i}]$: Het is voldoende te bewijzen dat als $h = fg$ met $(f, g) = 1$, dat dan $\Lambda_\rho[h] \approx \Lambda_\rho[f] \oplus \Lambda_\rho[g]$. Bekijk de volgende afbeelding: $\Psi : \Lambda_\rho[h] \rightarrow \Lambda_\rho[f] \oplus \Lambda_\rho[g] : \lambda \mapsto \rho(h/f)(\lambda) + \rho(h/g)(\lambda)$. Eerst laten we zien dat $\Lambda_\rho[f] \cap \Lambda_\rho[g] = \{0\}$. Schrijf $1 = fh_1 + gh_2$, dan is $\lambda = \rho(1)(\lambda) = \rho(h_1) \circ \rho(f)(\lambda) + \rho(h_2) \circ \rho(g)(\lambda) = 0$ als $\lambda \in \Lambda_\rho[f] \cap \Lambda_\rho[g]$. De afbeelding is injectief: als $\Psi(\mu) = 0$ dan is $\rho(f)(\mu) = -\rho(g)(\mu) \in \Lambda_\rho[f] \cap \Lambda_\rho[g] = \{0\}$ en dus $\mu \in \Lambda_\rho[f] \cap \Lambda_\rho[g] = \{0\}$. Aangezien beide verzamelingen evenveel elementen bevatten is de afbeelding dus een bijectie, verder is de afbeelding duidelijk een moduul-homomorfisme, waarmee het gestelde bewezen is. Vanwege de Chinese reststelling is het voldoende de stelling te bewijzen voor $a = P^e$ met P een irreducibel polynoom. We gebruiken nu de volgende stelling zonder bewijs (zie Serge Lang, Undergraduate Algebra, Chapter 5, stelling 7.2):

Stelling 5.5. Zij R een hoofd ideaal domein. Stel dat M een eindig voortgebracht R -moduul is en stel dat er een m is zodat $p^m M = \{0\}$ voor een priem $p \in M$, dan geldt dat: $M \approx \bigoplus R/p^{r_i} R$ voor zekere $r_i \in \mathbb{N}$

$\Lambda_\rho[a]$ heeft eindig veel elementen en is dus eindig voortgebracht. We voldoen aan de stelling met $m = e$ en $p = P$, dus we hebben: $\Lambda_\rho[P^e] \approx A/P^{f_1} A \oplus \dots \oplus A/P^{f_s} A$. Aan beide kanten het aantal elementen tellen geeft: $q^{r \deg(P^e)} = q^{\sum_{i=1}^s f_i \deg(P)}$. Er geldt zeker dat $f_i \leq e$, omdat $P^e \lambda = 0$ voor alle $\lambda \in \Lambda_\rho[a]$. Het is dus voldoende te laten zien dat $r = s$. Voor $e = 1$ is het duidelijk aangezien $0 < f_i \leq e$, dus $f_i = 1 = e$, kijkend naar het aantal elementen geldt $r = s$. De afbeelding $\Lambda_\rho[P^e] \rightarrow \Lambda_\rho[P^{e-1}] : x \mapsto Px$ is een surjectie met kern $\Lambda_\rho[P]$. Via het isomorfisme uit de stelling, induceert dit een afbeelding $A/P^{f_1} A \oplus \dots \oplus A/P^{f_s} A \rightarrow P(A/P^{f_1} A \oplus \dots \oplus A/P^{f_s} A) : x \mapsto Px$. Zij nu $\overline{x} \in A/P^{f_j} A$, dan geldt dat $P\overline{x} \equiv 0$, als $x \in P^{f_j-1} A$ en dus $\overline{x} \in P^{f_j-1} A/P^{f_j} A \approx A/P$. Dus de kern van de tweede afbeelding is isomorf met $(A/P)^s$. Van het geval $e = 1$ weten we dat $\Lambda_\rho[P] \approx (A/PA)^r$. Aangezien de beide kernen isomorf moeten zijn, geldt dus dat $r = s$. \square

We nemen van nu af aan $r = 1$. We kunnen nu naar lichaamsuitbreidingen van k gaan kijken door de wortels van $\rho(a)$ er aan toe te voegen. We definiëren $K_{\rho,a} = k(\Lambda_\rho[a])$. Omdat $\rho_a(x)$ een separabel polynoom is, is dit een

Galoisuitbreiding. Bovendien geldt dat als $\sigma \in \text{Gal}(K_{\rho,a}/k)$ en $\rho_a(\lambda) = 0$, dat dan $\rho_a(\sigma(\lambda)) = 0$. σ induceert dus een bijectie van $\Lambda_\rho[a]$ met zichzelf die bovendien de modulustructuur behoudt. We krijgen dus een homomorfisme van $\text{Gal}(K_{\rho,a}/k)$ naar de A/aA -moduul-automorfismen van $\Lambda_\rho[a] \approx A/aA$, met triviale kern aangezien aangezien een $\sigma \in \text{Gal}(K_{\rho,a}/k)$ vastligt als gespecificeerd is wat hij moet doen met $\Lambda_\rho[a]$. Zij σ een A/aA -moduul-automorfisme over A/aA , dan $\sigma(x) = x\sigma(1)$ dit is een automorfisme dan en slechts dan als $\sigma(1) \in (A/aA)^*$, er is dus een bijectie tussen de automorfismen en $(A/aA)^*$, eenvoudig wordt nagegaan dat dit een groeps isomorfisme is. We krijgen dus de volgende stelling:

Stelling 5.6. *Stel dat ρ een Drinfeldmoduul is van rang 1 en $a \neq 0$, dan is er een injectief homomorfisme: $\text{Gal}(K_{\rho,a}/k) \rightarrow (A/aA)^*$*

We gaan nu verder met het Carlitz-moduul C , deze heeft rang 1 en dus is bovenstaande stelling van toepassing. Uit voorgaande stelling volgt dat de Galoisgroep een deelgroep is van $(A/aA)^*$. We schrijven Λ_m voor $\Lambda_C[m]$ en K_m voor $k(\Lambda_C[m])$. Deze lichaamsuitbreidingen lijken erg op de cyclotomelichaamsuitbreidingen over \mathbb{Q} . Het eerste dat we nu zullen gaan bewijzen is dat $\text{Gal}(K_m/k) \approx (A/aA)^*$.

Stel dat m een polynoom is van graad d , dan:

$$C_m(x) = a_0x + a_1x^q + \dots + a_dx^{q^d} \text{ met } a_i \in A.$$

We weten dat $\Lambda_m \approx A/mA$ als A -moduul, A/mA wordt voortgebracht door de elementen $y \in A/aA$ waarvoor geldt dat $(m, y) = 1$ (is immers equivalent met dat 1 voortgebracht kan worden), als bovendien y een voortbrenger is dan is xy een voortbrenger dan en slechts dan als $(m, xy) = (m, x) = 1$. Als λ_m een voortbrenger is van Λ_m dan is $C_a(\lambda_m)$ een voortbrenger dan en slechts dan als er een b is met $C_{ab}(\lambda_m) = \lambda_m$, oftewel $C_{ab-1}(\lambda_m) = 0$, omdat λ_m Λ_m voortbrengt is er voor iedere wortel λ_k van C_m een k zodat $C_k(\lambda_m) = \lambda_k$, oftewel $C_{ab-1}(\lambda_k) = 0$, schrijf $ab - 1 = lm + g$ met $\deg(g) < \deg(m)$ dan $0 = C_{ab-1}(\lambda_k) = C_{lm+g}(\lambda_k) = C_g(\lambda_k)$, omdat $\deg(C_g) < \deg(C_m)$ is dus $C_a(\lambda_m)$ een voortbrenger dan en slechts dan als $g = 0$, oftewel dan en slechts dan als $(a, m) = 1$. We definiëren nu $\Phi(m) = |\{f \in A \mid (f, m) = 1 \text{ en } \deg(f) < \deg(m)\}| = |(A/mA)^*|$.

Onmiddellijk volgt voor $\alpha \in \mathbb{F}$ dat $C_{\alpha m} = C_\alpha \circ C_m = \alpha C_m$, we komen dus tot de conclusie dat $\Lambda_{\alpha m} = \Lambda_\alpha$.

Definitie 5.8. *We definiëren \mathcal{O}_m als de integrale afsluiting van A in K_m , i.e. de verzameling van nulpunten van monische polynomen over $\mathbb{F}[T]$ die bovendien in K_m liggen (vergelijk met \mathbb{A} uit het vorige hoofdstuk). Opm: \mathcal{O}_m is een ring (analoog aan hoofdstuk 2).*

We zullen nu de theorie uit hoofdstuk 2 en 3 gaan gebruiken. Strict genomen hebben we daar alles bewezen voor uitbreidingen van \mathbb{Q} . Maar modulo triviale aanpassingen kunnen alle bewijzen zo opgevijseld worden naar $\mathbb{F}(T)$ en separabele polynomen (i.e. een polynoom f zodat $f' \neq 0$). De ring der gehelen is dan $\mathbb{F}[T]$, dit is een hoofd ideaal domein. De priemenvormen zijn van de vorm $P\mathbb{F}[T]$ met P een irreducibel polynoom. Verder heeft $\mathbb{F}[T]/P\mathbb{F}[T]$ $q^{\deg(P)}$ elementen.

Stelling 5.7. *Stel dat λ_m een voortbrenger is van Λ_m en stel dat $a \in A$ met $(a, m) = 1$ dan is $C_a(\lambda_m)/\lambda_m$ een eenheid in \mathcal{O}_m . Als m deelbaar is door 2 (of meer) priemenvormen, dan is λ_m zelf een eenheid.*

Bewijs. Omdat we met het Carlitz moduul werken zit de coëfficiënt van de hoogste macht van $C_m(x)$ in \mathbb{F}^* , vermenigvuldigen met de inverse van dat element geeft dat $\lambda_m \in \mathcal{O}_m$. Verder is $C_a(\lambda_m)/\lambda_m \in \mathcal{O}_m$ omdat $C_a(x)$ deelbaar is door x en weer monisch is. Nu nog te bewijzen dat z'n inverse $\lambda_m/C_a(\lambda_m)$ ook in \mathcal{O}_m ligt. Omdat $(a, m) = 1$ zijn er b, f zodat $ab = 1 + fm$, dus $C_b \circ C_a(x) = x + C_f \circ C_m(x)$, λ_m invullend geeft $\lambda_m/C_a(\lambda_m) = C_b(C_a(\lambda_m))/C_a(\lambda_m) \in \mathcal{O}_m$. Nu nog de laatste bewering van de stelling.

We kunnen natuurlijk aannemen dat m monisch is (nulpunten veranderen daardoor immers niet). Stel dat $m = m_1 m_2$. Definieer $\lambda_{m_1} = C_{m_2}(\lambda_m)$ en $\lambda_{m_2} = C_{m_1}(\lambda_m)$. Dan is λ_{m_i} een nulpunt van m_i . Bekijk nu: $\lambda_{m_1} = \lambda_m \cdot \frac{C_{m_2}(\lambda_m)}{\lambda_m^{m_2}}$ (dit kan altijd), we zien dus dat $\lambda_m \mid \lambda_{m_1}$ in \mathcal{O}_m en analoog $\lambda_m \mid \lambda_{m_2}$. We nemen aan beide kanten de norm van K_m over k , dit levert iets op in A (fixlichaam). We vinden dus dat $N_k^{K_m}(\lambda_m) \mid N_k^{K_m}(\lambda_{m_i}) = (N_k^{K_{m_i}}(\lambda_{m_i}))^{[K_m:K_{m_i}]} \in A$, waar we in de laatste identiteit gebruikt hebben dat ieder automorfisme van K_{m_i} uitbreidt tot $[K_m : K_{m_i}]$ automorfismen van K_m .

We hebben nu een lemma nodig dat we pas later zullen bewijzen:

Lemma 5.1. *Stel dat $P \in A$ een monische irreducibele veelterm van positieve graad. Stel dat $e \in \mathbb{N}_{>0}$, λ een voortbrenger van Λ_{P^e} en $g[x] \in k[x]$ het daarbij behorende irreducibele polynoom zijn. Dan is g een Eisenstein polynoom in P , i.e. de kopterm is niet deelbaar door P alle andere wel en P^2 deelt niet op de constante term. De constante term is zelfs P .*

We bewijzen het gestelde nu met inductie naar het aantal priemmen in de priemontwikkeling van m . Stel dus dat $m = P^e$. Er geldt dan dus dat de norm van λ_{P^e} P is. Als $m = P_1^{e_1} P_2^{e_2}$, dan deelt de norm van λ_m een macht van P_1 en P_2 , hetgeen impliceert dat de norm van λ_m in \mathbb{F}^* moet liggen, maar dan moet λ_m een eenheid zijn. Stel nu dat m deelbaar is door $t > 2$ verschillende priemmen. Stel $m = m_1 m_2$ met $m_1 = P_1^{e_1}$ en $m_2 = \prod_{i=2}^t P_i^{e_i}$. Dan is λ_{m_2} een eenheid (inductiehypothese), en de norm van λ_{m_2} ligt in \mathbb{F}^* . Omdat de norm van λ_m deze moet delen volgt hieruit dat de norm van λ_m in \mathbb{F}^* ligt. \square

We kunnen nu net zoals in het vorige hoofdstuk kijken naar priemidealen in A . Als P een irreducibel polynoom is dan is PA een priemideaal in A . We kunnen nu kijken welke priemmen Q er boven PA liggen in \mathcal{O}_m (i.e. $Q \cap A = P$). Geheel analoog aan het vorige hoofdstuk zijn dat precies de priemmen die voorkomen in de priemontwikkeling van $PA\mathcal{O}_m$. We kunnen weer vertakkingsgraden toekennen aan de macht waarin een bepaald priemideaal voorkomt, als al die machten één zijn, zeggen we dat PA onvertakt is. Een priemideaal heet volledig vertakt als er maar één priem in de ontwikkeling voorkomt. We hebben de volgende stelling:

Stelling 5.8. *Stel dat $P \in A$ een monische irreducibele polynoom is en $e \in \mathbb{Z}_{>0}$. Als $QA \neq PA$ dan is QA onvertakt in \mathcal{O}_{P^e} . Het priem PA is volledig vertakt met vertakkingsgraad $\Phi(P^e)$. We hebben $[K_{P^e} : k] = \Phi(P^e)$ en $\text{Gal}(K_{P^e}/k) \approx (A/P^e A)^*$. Het priemideaal dat boven PA ligt is $(\lambda) = \lambda\mathcal{O}_{P^e}$ met λ een voortbrenger van Λ_{P^e} .*

Bewijs. Stel dat λ een voortbrenger is van Λ_{P^e} (als A -moduul) en g het bijbehorende monische irreducibele polynoom over k . Dan moet gelden dat $g(x) \mid C_{P^e}(x)$ omdat λ wortel is van $C_{P^e}(x)$. Schrijf dus $C_{P^e}(x) = f(x)g(x)$. Differentiëren en $x = \lambda$ invullen geeft dat $C'_{P^e}(\lambda) = f(\lambda)g'(\lambda)$, merk nu op dat

$C'_{P^e}(x) = P^e$, oftewel $P^e = f(\lambda)g'(\lambda)$. Er geldt dat $K_{P^e} = k(\lambda)$: het is voldoende te laten zien dat iedere $\lambda_0 \in \Lambda_{P^e}$ geschreven kan worden als polynoom in λ , kies $a \in A$ met $a\lambda = \lambda_0$, oftewel $C_a(\lambda) = \lambda_0$, wat het gevraagde polynoom is. We concluderen dat de lichaamsdiscriminant een macht van P is (analogon stelling 2.8. Als een priem Q vertakt is, dan moet Q de discriminant delen (analogon stelling 3.16) en dus een macht van P en dus P , de enige mogelijkheid is dus $P = Q$).

Stel dat $d = \deg(P)$. Zoals al eerder genoemd zijn de andere primitieve generatoren van Λ_{P^e} :

$\{C_a(\lambda) \mid 0 \leq \deg(a) < \deg(P^e) = ed, (a, P) = 1\}$. Omdat $\Lambda_{P^e} \approx A/P^e A$ is λ een voortbrenger dan en slechts dan als $C_{P^e}(\lambda) = 0$ en $C_{P^{e-1}}(\lambda) \neq 0$, dus precies de wortels van: $\frac{C_{P^e}(x)}{C_{P^{e-1}}(x)} = \frac{C_{P(C_{P^{e-1}})(x)}}{C_{P^{e-1}}(x)} = P + \dots + hC_{P^{e-1}}(x)^{q^d-1}$.

De graad van het polynoom is $q^{\deg(P^{e-1})}(q^d - 1) = q^{(e-1)d}(q^d - 1) = \Phi(P^e)$. De generatoren zijn dus precies de nulpunten van dat polynoom, welke monisch is aangezien P monisch is met constante term P , we hebben dus $P = \prod_{a, \deg(a) < ed, (a, P) = 1} C_a(\lambda) = \lambda^{\Phi(P^e)} * \text{eenheid}$ volgens stelling 5.7. Dus $PA = (\lambda)^{\Phi(P^e)}$. PA kan niet verder ontbinden. Stel dat $\beta(\lambda)$ deelt. Dan deelt $\Phi(P^e)$ de vertakkingsgraad van β . Omdat λ een wortel is van een polynoom van graad $\Phi(P^e)$ geldt dat $[K_{P^e} : k] \leq \Phi(P^e)$ en omdat de vertakkingsgraad altijd kleiner is dan de lichaamsuitbreiding geldt dus dat de vertakkingsgraad van β $\Phi(P^e)$ is, wat de stelling bewijst. \square

Bewijs van lemma 5.1:

Uit de stelling (en het bewijs daarvan) volgt dat het minimaalpolynoom gegeven wordt door:

$g(x) = \prod_{(a, P) = 1, \deg(a) < ed} (x - C_a(\lambda))$. De voorcoëfficiënt van de kopterm is 1. De andere termen zijn sommen en produkten van primitive elementen welke volgens het de stelling allemaal in het ideaal (λ) liggen. Dus de niet-kopcoëfficiënten liggen in $(\lambda) \cap A = PA$. De constante term is P , dus is $g(x)$ een Eisensteinpolynoom.

Lemma 5.2. *Zij $P \in A$ een monisch irreducibel polynoom, dan is C_{P^e} een produkt van Eisenstein polynomen*

Bewijs. We doen dit met inductie. Voor $e = 1$ geldt dat $C_P(x) = xg(x)$ en is dus het produkt van Eisensteinpolynomen. Uit $C_{P^e}(x)/C_{P^{e-1}}(x) = \hat{g}(x)$, met \hat{g} het irreducibele polynoom behorende bij Λ_{P^e} , volgt met inductie het gestelde. \square

We gaan nu naar algemenere polynomen kijken:

Stelling 5.9. *Zij $m \in A$ en stel dat $\alpha P_1^{e_1} \dots P_t^{e_t}$ de priemdecompositie van m is, dan geldt: $K_m = K_{P_1^{e_1}} \dots K_{P_t^{e_t}}$. De enige vertakte idealen in A in \mathcal{O}_m zijn $P_i A$. Verder geldt $\text{Gal}(K_m/k) \approx (A/mA)^*$ en dus $[K_m : k] = \Phi(m)$.*

Bewijs. Definieer $m_i = m/P_i^{e_i}$. Zij λ een voortbrenger van Λ_m (als A -moduul). Dan is $C_{m_i}(\lambda_m)$ voortbrenger van $\Lambda_{P_i^{e_i}}$. Definieer $\lambda_{P_i^{e_i}} = C_{m_i}(\lambda_m)$. Dan geldt dus dat $K_{P_i^{e_i}} = k(\lambda_{P_i^{e_i}}) \subset k(\lambda_m) = K_m$ en dus $K_{P_1^{e_1}} \dots K_{P_t^{e_t}} \subset K_m$. De grootste gemene deler van de m_i is 1, we kunnen dus schrijven: $1 = \sum_{i=1}^t a_i m_i$ voor zekere a_i en dus $x = \sum_{i=1}^t C_{a_i}(C_{m_i}(x))$, λ_m invullen geeft vervolgens:

$\lambda_m = \sum_{i=1}^t C_{a_i}(\lambda_{P_i^{e_i}}) \in K_{P_1^{e_1}} \dots K_{P_t^{e_t}}$, wat de andere inclusie bewijst. Stel dat P vertakt is met $P \neq P_i$ voor alle i , dan is P onvertakt in de $K_{P_i^{e_i}}$ voor alle i wegens stelling 5.8 en dus ook niet in de samenstelling $K_{P_1^{e_1}} \dots K_{P_t^{e_t}}$ (zie hoofdstuk 3). Wegens dezelfde stelling weten we dat de $P_i A$ volledige vertakt zijn in de $K_{P_i^{e_i}}$ en dus zijn de priemenvertakt in de samenstelling K_m . We bewijzen eerst met inductie naar t dat de graad van de uitbreiding $\Phi(m)$ is. Voor $t = 1$ is het weer de stelling. Stel dat het waar is voor $t - 1$, dan is $[K_{m_t} : k] = \Phi(m)$ (zelfde notatie als begin bewijs). Omdat K_{m_t} onvertakt is in $P_t A$ en $K_{P_t^{e_t}}$ volledig vertakt is in $P_t A$ (weer die stelling) geldt dat: $K_{m_t} \cap K_{P_t^{e_t}} = k$ (merk op dat $e(K_{m_t} \cap K_{P_t^{e_t}}/k) = 1$ en dat $e(K_{P_t^{e_t}}/k) = [K_{P_t^{e_t}} : k]$).

We hebben dus: $[K_m : k] = [K_{m_t} : k][K_{P_t^{e_t}} : k] = \Phi(m_t)\Phi(P_t^{e_t}) = \Phi(m)$. Er is een injectief homomorfisme $Gal(K_m/k) \rightarrow (A/aA)^*$ en aangezien beide verzamelingen dus evenveel elementen hebben is het homomorfisme een isomorfisme wat de stelling bewijst. \square

We voeren eerst een hulpmiddel in voor het bewijzen van de volgende stelling:

Definitie 5.9. *Zij k een lichaam. Een niet-archimedische valuatie is een afbeelding $|\cdot| : k \mapsto \mathbb{R}$ zodanig dat voor $b, c \in k$:*

$$\begin{aligned} &|b| \geq 0 \text{ en } |b| = 0 \text{ dan en slechts dan als } b = 0 \\ &|bc| = |b| |c| \\ &|b+c| \leq \max(|b|, |c|) \end{aligned}$$

We gaan de volgende valuatie invoeren: Kies een vast priemideaal P in een ring der geheelen. Zij α een algebraïsch geheel in R , dan is αR een ideaal en heeft dus een unieke priemontwikkeling in priemidealen. Definieer $e(\alpha)$ als de macht van P waarin die (exact) voorkomt. Dan definiëren we: $|\alpha| = 2^{-e(\alpha)}$ als $\alpha \neq 0$ en 0 als $\alpha = 0$. Dit is een niet-archimedische valuatie. De eerste en tweede eigenschap zijn evident. Als $|a| \leq |b|$, dan geldt $e(a) \geq e(b)$. Merk op dat geldt dat $(a+b) \subset (a)+(b)$ en dus $(a+b) = ((a)+(b))I = P^{\min(e(a), e(b))}JI = P^{e(b)}JI$ en dus $e(a+b) \geq e(b)$ en dus $|a+b| \leq |b| = \max(|a|, |b|)$.

Op het breukenlichaam definiëren we de valuatie $|a/b| = |a| / |b|$.

Stelling 5.10. *Als $|\cdot|$ een niet-archimedische valuatie is en $|c| < |b|$, dan geldt dat $|b+c| = |b|$*

Bewijs. Zeker geldt dat $|b+c| \leq |b|$. Ook hebben we $b = (b+c) - c$ en dus $|b| \leq \max(|b+c|, |c|) = |b+c|$. \square

We gaan nu iets specifieker kijken naar \mathcal{O}_m :

Stelling 5.11. *Laat \mathcal{O}_m de integrale afsluiting zijn van A in K_m , dan geldt voor $m = P^e$ dat $\mathcal{O}_m = A[\lambda_m]$*

Bewijs. We beginnen het bewijs met $m = P^e$. Voor het gemak schrijven we $\lambda_{P^e} = \lambda$. We hebben zeker dat $A[\lambda] \subset \mathcal{O}_{P^e}$. Zij $g(x) \in k[x]$ het irreducibele polynoom van λ . We hebben weer dat de discriminant van $A[\lambda]/k$ een constante maal een macht van P is. Laat nu $\omega \in \mathcal{O}_{P^e} \subset K_m$, dan hebben we dat: $\omega = \sum_{i=0}^{\Phi(P^e-1)} a_i \lambda^i$, met $a_i \in k$. Dan geldt dat iedere a_i van de vorm b_i/P^n is met $b_i \in A$ en n voldoende hoog is, het analogon van stelling 2.10. We mogen aannemen dat er een b_i is die niet deelbaar is door P . We hebben $P^n \omega = \sum_{i=0}^{\Phi(P^e-1)} b_i \lambda^i$. We moeten laten zien dat $n = 0$. Nu gaan we de net ingevoerde

valuatie gebruiken. We hebben nu 2 priemidealen tot onze beschikking, namelijk PA in A en (λ) in \mathcal{O}_{P^e} . Merk op dat als $\alpha \in A$, dat dan $|\alpha|_{(\lambda)} = |\alpha|_{PA}^{\Phi(P^e)}$, omdat P volledig vertakt is met graad $\Phi(P^e)$. Laten we nu naar de vergelijking gaan kijken. De valuatie nemend aan het linkerlid zien we dat $|P^n \omega|_{(\lambda)} \leq 2^{-n\Phi(P^e)}$. Nu gaan we naar de individuele factoren in de som kijken, stel dat $(b_i) = P^{e_i} J_i$, dan geldt dat $|b_i \lambda^i|_{(\lambda)} = 2^{-(\Phi(P^e)e_i+i)}$, als i_0 de kleinste i is zodat $e_i = 0$, dan omdat $1 \leq i \leq \Phi(P^e) - 1$, kunnen we het maximum nemen en vinden we dat $|P^n \omega|_{(\lambda)} = 2^{-i_0}$, oftewel $i_0 \geq n\Phi(P^e)$ en omdat $0 \leq i_0 \leq \Phi(P^e) - 1$, moet dus gelden dat $n = 0$, wat we moesten bewijzen. \square

Bovenstaande stelling geldt ook voor algemene m , op het bewijs zal hier niet ingegaan worden.

Stelling 5.12. *Voor $m \in A$ geldt dat $\mathcal{O}_m = A[\lambda_m]$*

Om de overeenkomst met de cyclotome lichaamsuitbreidingen van \mathbb{Q} compleet te maken, eindigen we met de volgende stelling:

Stelling 5.13. *Laat $m \in A$ een polynoom van positieve graad zijn en $P \in A$ een monisch, irreducibel polynoom dat m niet deelt. Stel dat f het kleinste natuurlijke is zodat $P^f \equiv 1 \pmod{m}$, dan is $P\mathcal{O}_m$ het produkt van $\Phi(m)/f$ priemidealen van graad f*

Bewijs. De Galoisgroep van K_m over k is abels. Omdat P m niet deelt is PA onvertakt. Het Frobenius Automorfisme σ_P hangt dus alleen af van P en voldoet aan: $\sigma_P(\alpha) \equiv \alpha^{\|PA\|} \pmod{\beta}$ met β een priem boven PA , met $\|PA\| = \|A/PA\| = q^{\deg(P)}$. Het irreducibele polynoom van λ_P is $C_P(x)/x$ en is een Eisensteinpolynoom. We hebben dus $C_P(x) \equiv x^{\|P\|} \pmod{PA}$, omdat $PA \subset \beta$ geldt dus ook dat $C_P(x) \equiv x^{\|P\|} \pmod{\beta}$. We definiëren nu een automorfisme door te eisen $\sigma_P(\lambda_m) = C_m(\lambda_m)$ zijnde een andere wortel van het irreducibele polynoom van λ_m . We moeten nu checken dat dit inderdaad het Frobenius Automorfisme is: Er geldt in ieder geval dat $\sigma_P(\lambda_m) = \lambda_m^P \pmod{\beta}$, als $\omega \in \mathcal{O}_m$, dan hebben we dat $\omega = \sum_i a_i \lambda_m^i$, we hebben dan dat: $\sigma_P(\omega) = \sum_i a_i \sigma_P(\lambda_m)^i \equiv \sum_i a_i \lambda_m^{\|P\|i} \equiv \sum_i (a_i \lambda_m^i)^{\|P\|} \pmod{\beta}$. Waar we gebruik hebben gemaakt van de kleine stelling van Fermat voor polynomen ($\|P\|$ is een macht van karakteristiek). We hebben dus het Frobenius automorfisme gevonden. We weten dus nu dat PA splitst in $\Phi(m)/f$ priemen (omdat $e = 1$). We wisten al dat de Galois groep isomorf is met $(A/mA)^*$, kijkend naar de definitie van het isomorfisme zien we dat dit correspondeert met de kleinste f zodanig dat $P^f \equiv 1 \pmod{m}$ (λ_m is een voortbrenger, die stuur je bijvoorbeeld naar 1 in $(A/mA)^*$, stel dat $\sigma(\lambda_m) = C_a(\lambda_m) = a \cdot \lambda_m$, dan $\sigma \mapsto a$, het Frobenius automorfisme correspondeert dus met $P \pmod{m}$). \square

Bibliografie

- [1] Daniel A. Marcus. *Number Fields*. Springer-Verlag, 1977.
- [2] Michael Rosen. *Number Theory in Function Fields*. Springer-Verlag, 2002.
- [3] Serge Lang. *Undergraduate Algebra*. Springer-Verlag, 1990.
- [4] M.A. Armstrong. *Groups and Symmetry*. Springer-Verlag, 1988.
- [5] J.W.S. Cassels. *Local Fields*. Cambridge University Press, 1986.