Utrecht University

Bachelorscriptie

De zeldzaamheid van polynomen met niet-maximale Galoisgroep

Geschreven door

Mees Verheije

4144805

Met dank aan mijn begeleider prof. dr. G.L.M. Cornelissen, die op Goede Vrijdag het Duitstalige artikel van van der Waerden voor mij heeft vertaald.

16 juni 2016

Inhoudsopgave

Conventies voor symbolen

$\mathbb{N}$ De natuurlijke getallen. Hier is 0 geen onderdeel van.

$\subset$ Het symbool voor een niet-stricte deelverzameling.

$\subsetneq$ Het symbool voor een stricte deelverzameling.

F/E De notatie voor *Het uitbreidingslichaam F van E.*

Inleiding

In 1934 bracht Nederlands wiskundige Bartel Leenderd van der Waerden een Duitstalig artikel uit met de titel "Die Seltenheit der Gleichungen mit Affekt"[6].

In dat artikel maakte hij de bewering: *"Asymptotisch gezien, heeft 100% van alle polynomen met gehele coëfficiënten een maximale Galoisgroep"*. Dit zou moeten betekenen dat als we een compleet willekeurig polynoom $f \in \mathbb{Z}$ kiezen, de kans 100% is dat dit polynoom een maximale Galoisgroep heeft. Dit is echter duidelijk niet altijd het geval, kijk bijvoorbeeld maar naar het polynoom $x^4 - 2$, dit polynoom heeft zeker geen maximale Galoisgroep. De volgende stelling maakt duidelijk wat het citaat echt betekent.

Stelling 0.0.1. *Beschouw voor $N \in \mathbb{N}$ de verzameling Box_N van polynomen met gehele coëfficienten*

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad met \quad -|N| \leq a_0, a_1, \cdots, a_n \leq |N|.$$

De verhouding tussen het aantal polynomen in Box_N met maximale Galoisgroep en het totaal aantal polynomen in Box_N convergeert naar 1 als N stijgt, oftewel

$$\lim_{N\to\infty} \frac{|\{f \in \mathrm{Box}_N \mid \mathrm{Gal}\,(f/\mathbb{Q}) \simeq S_n\}|}{|\mathrm{Box}_N|} = 1.$$

■

De verzameling Box_N, is een eindig aantal functies (er zijn $(2\,|N| + 1)^n$ mogelijkheden).

Aangezien het artikel van van der Waerden relatief lang geleden is geschreven, kan zijn schrijfstijl als ouderwets worden beschouwd. Zijn artikel stond niet in de vorm die wij tegenwoordig gewend zijn, waarbij we duidelijk aangeven waar de stellingen, definities en bewijzen staan. In mijn scriptie zal ik het bewijs van stelling 0.0.1 geven op dezelfde manier als van der Waerden, maar ik zal het bewijs op een modernere manier brengen.

Ook bewees van der Waerden niet alle stellingen die hij gebruikte voor zijn bewijs. In mijn scriptie zal ik zo veel mogelijk van de stof behandelen die nodig is voor het bewijs. Ik ga er echter wel van uit dat de lezer een basale kennis heeft van algebra. Begrippen zoals *groep*, *ring*, *homomorfisme* en *isomorfisme* worden niet uitgelegd. Ik geef in het eerste hoofdstuk een herhaling van de definities en stellingen over lichamen en Galoistheorie die nodig zijn voor het bewijs, maar ik zal deze stellingen niet bewijzen, daarvoor kunt u terecht bij vele algebraboeken, maar het boek dat ik heb gebruikt is Algebra: Chapter 0 van Paolo Aluffi [1] hoofdstuk VII.1, 4, 5 en 6.

In hoofdstuk 2 behandel ik de stof over symmetrische functies en de Galoisgroep van het algemene polynoom

$$f = (x - t_1)\,(x - t_2)\cdots(x - t_n)$$

met $t_1, t_2, \cdots, t_n$ algebraïsch onafhankelijke variabelen behandelen. Ook behandel ik hier het begrip Galois resolvent. Deze stof heb ik nodig voor het bewijs van de stelling van Dedekind, die op zijn beurt weer nodig is voor het bewijs van stelling 0.0.1.

In het laatste hoofdstuk ga ik stelling 0.0.1 bewijzen. Ik volg daarbij de werkwijze van het artikel van van der Waerden.

In de conclusie zal ik het kort hebben over de bevindingen die we hebben gedaan in deze scriptie en over het onderzoek dat er verder nog is gepleegd naar dit onderwerp.

Hoofdstuk 1

Herhaling van lichamen- en Galoistheorie

1.1 Lichamen en uitbreidingen

1.1.1 Lichamen

Het begrip *lichaam* heeft u al meerdere keren langs zien komen. Als u weet wat een ring is, dan heeft u waarschijnlijk ook wel eens gehoord wat een lichaam is. Een lichaam is een bijzonder geval van een ring. De beste manier om een lichaam te beschrijven zonder de daadwerkelijke definitie op te lezen, is om te zeggen dat het een ring is waarin er geen narigheden zijn; alles is prettig binnen een lichaam.

Dat wil zeggen dat zich geen elementen in een lichaam bevinden die:

- nuldelers zijn,
- geen eenheid zijn of
- niet commuteren ten opzichte van vermenigvuldiging.

We gaan nu naar de officiële definitie.

Definitie 1.1.1. Een **lichaam** F is een commutatieve ring met 1, waarin voor elk element $0 \neq a \in F$, een element $0 \neq a^{-1} \in F$ bestaat met de eigenschap dat $a \cdot a^{-1} = 1$. ■

De eigenschap dat er geen nuldelers in een lichaam kunnen zitten, volgt vanzelf uit de definitie.

1.1.2 Lichaamsuitbreidingen

Waar het in de leer van lichamen veelal om draait is de notie van wat lichamen zijn met betrekking tot elkaar. Zoals we voor groepen en ringen de begrippen *deelgroep* en *deelring* hebben, is er net zo'n begrip voor lichamen. Op vergelijkbare manier als bij groepen en ringen, definiëren we een deellichaam van een lichaam als een deelverzameling die aan de eigenschappen van een lichaam voldoet. De definitie is zoals we zouden verwachten.

Definitie 1.1.2. Zij E en F twee lichamen waarbij $E \subset F$. Als E gesloten is onder de operatoren van F en dezelfde inverses als F heeft onder die operatoren, dan noemen we E het **deellichaam** van F. Andersom noemen we F het **uitbreidingslichaam** (of gewoon uitbreiding) van E.

We zullen de notatie F/E gebruiken voor "de uitbreiding F van E". ■

We krijgen dus een uitbreidingslichaam door een bestaand lichaam te nemen, en daar iets nieuws aan toe te voegen.

Voorbeeld 1.1.3. Beschouw het lichaam $\mathbb{Q}$. Het mag duidelijk zijn dat $\sqrt{2}$ niet in dit lichaam zit. Neem nu $\mathbb{Q}[x]$ en een ringhomomorphisme $\phi : \mathbb{Q}[x] \to \mathbb{C}$ dat alle rationale getallen naar zichzelf afbeeldt en $\phi(x) = \sqrt{2}$. Het beeld van ϕ noemen we $\mathbb{Q}\left[\sqrt{2}\right]$ en is een ring onder optelling en vermenigvuldiging. Alle elementen zijn dus van de vorm

$$a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \cdots + a_n\sqrt{2}^n$$

voor een $n \in \mathbb{N}$ en $a_0, \cdots a_n \in \mathbb{Q}$. We zullen nu laten zien dat deze ring een uitbreidingslichaam is van $\mathbb{Q}$.

Omdat $\sqrt{2}^2 = 2$, kunnen we elke even term $a_{2i}\sqrt{2}^{2i}$ herschrijven tot $a_{2i} \cdot 2^i$ en elke oneven term $a_{2i+1}\sqrt{2}^{2i+1}$ tot $a_{2i+1} \cdot 2^i\sqrt{2}$. Op die manier kunnen we elk element in $\mathbb{Q}\left[\sqrt{2}\right]$ herschrijven tot de vorm $a\sqrt{2} + b$ voor zekere $a, b \in \mathbb{Q}$.

Het is niet moeilijk in te zien dat sommen en producten van zulke elementen weer een element zijn van $\mathbb{Q}\left[\sqrt{2}\right]$:

$$\begin{aligned}\left(a\sqrt{2}+b\right) + \left(c\sqrt{2}+d\right) &= (a+c)\sqrt{2} + (b+d)\\ \left(a\sqrt{2}+b\right) \cdot \left(c\sqrt{2}+d\right) &= (ad+bc)\sqrt{2} + (2ac+bd)\end{aligned}$$

Nu moeten we nog laten zien dat elk element een inverse heeft. Kies een willekeurig element $a\sqrt{2} + b$ met $a, b \neq 0$. Beschouw de volgende gelijkheid:

$$\begin{aligned}\left(a\sqrt{2}+b\right) \cdot \left(a \cdot \sqrt{2} - b\right) &= 2a^2 - b^2\\ \left(a\sqrt{2}+b\right) \cdot \frac{a \cdot \sqrt{2} - b}{2a^2 - b^2} &= 1\\ \left(a\sqrt{2}+b\right) \cdot \left(\frac{a}{2a^2 - b^2} \cdot \sqrt{2} - \frac{b}{2a^2 - b^2}\right) &= 1\\ \left(a\sqrt{2}+b\right)^{-1} &= \left(\frac{a}{2a^2 - b^2} \cdot \sqrt{2} - \frac{b}{2a^2 - b^2}\right).\end{aligned}$$

Het lijkt er nu sterk op dat $\frac{a}{2a^2-b^2} \cdot \sqrt{2} - \frac{b}{2a^2-b^2}$ de inverse is van $a\sqrt{2} + b$, maar dit mogen we niet zomaar aannemen voor elke a en b, het klopt immers niet als $2a^2 - b^2 = 0$. We laten zien dat voor alle $a, b \in \mathbb{Q}$ geldt dat $2a^2 - b^2 \neq 0$:

$$\begin{aligned}2a^2 - b^2 &= 0\\ 2a^2 &= b^2\\ \sqrt{2}a = b \text{ of } \sqrt{2}a &= -b\\ \sqrt{2} = \frac{b}{a} \text{ of } \sqrt{2} &= -\frac{b}{a}.\end{aligned}$$

We hebben nu dus dat $\frac{a}{2a^2-b^2} \cdot \sqrt{2} - \frac{b}{2a^2-b^2}$ voor alle $a, b \in \mathbb{Q}$ goed gedefinieerd is. Omdat het een lineaire combinatie is van 1 en $\sqrt{2}$, zit dit element in $\mathbb{Q}\left[\sqrt{2}\right]$ en kunnen we dus stellen dat

$$\left(a\sqrt{2}+b\right)^{-1} = \left(\frac{a}{2a^2-b^2} \cdot \sqrt{2} - \frac{b}{2a^2-b^2}\right).$$

Elk element (behalve 0) is dus een eenheid. Hieruit volgt dat $\mathbb{Q}\left[\sqrt{2}\right]$ een lichaam is, en in het bijzonder een uitbreidingslichaam van $\mathbb{Q}$. Immers geldt dat $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{2}\right]$. ■

In het voorbeeld kun je $\mathbb{Q}\left[\sqrt{2}\right]$ zien als een vectorruimte over $\mathbb{Q}$. Hierbij vormen de vectoren 1 en $\sqrt{2}$ een basis. Als we het zo zien, zou $\mathbb{Q}\left[\sqrt{2}\right]$ een 2-dimensionaal vectorruimte zijn, en dit geeft betekenis aan het begrip *graad van een uitbreidingslichaam.*

Definitie 1.1.4. Als een uitbreiding F/E dimensie Dim $F = n$ heeft als een vectorruimte over E (met n eindig), dan zeggen we dat F/E **graad** n heeft. Als zo'n n niet te vinden is, dan zeggen we dat dat F/E oneindig is (of van oneindige graad).

We gebruiken de notatie $[F : E] = n$ voor "F/E heeft graad n" en we schrijven $[F : E] = \infty$ als F/E oneindig is. ■

In het voorbeeld heeft $\mathbb{Q}\left[\sqrt{2}\right]$ dus graad $\left[\mathbb{Q}\left[\sqrt{2}\right] : \mathbb{Q}\right] = 2$.

Definitie 1.1.5. Zij $E \subset F \subset K$ lichamen zodat K/E, K/F en F/E, dan is F een **tussenlichaam** van K en E. ■

De graad van een uitbreiding F/E hangt multiplicatief af van de graden van de tussenlichamen van F en E.

Stelling 1.1.6. *Zij K/F en F/E uitbreidingen van eindige graad, dan geldt*

$$[K : E] = [K : F]\,[F : E].$$

■

Voorbeeld 1.1.7. Beschouw $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, de kleinste uitbreiding van $\mathbb{Q}$ waar $\sqrt{2}$ en $\sqrt{3}$ in zitten. Hierbij is zowel $\mathbb{Q}\left(\sqrt{2}\right)$ als $\mathbb{Q}\left(\sqrt{2}\right)$ een tussenlichaam van $F/\mathbb{Q}$.

Als vectorruimte over $\mathbb{Q}$ heeft F lichaam vier basisvectoren: 1, $\sqrt{2}$, $\sqrt{3}$ en $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$. Hieruit volgt dat $[F : \mathbb{Q}] = 4$.

Aan de andere kant zien we dat F als vectorruimte over het tussenlichaam $\mathbb{Q}\left(\sqrt{2}\right)$ maar twee basisvectoren heeft: 1 en $\sqrt{3}$ ($\sqrt{2}$ kan immers gemaakt worden door vector 1 te vermenigvuldigen met scalair $\sqrt{2}$ en $\sqrt{6}$ kan op dezelfde manier gemaakt worden met de vector$\sqrt{3}$). We krijgen dus $\left[F : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$. We wisten al dat $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$.

Nu zien we inderdaad dat

$$[F : \mathbb{Q}] = 4 = \left[F : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right].$$

■

1.1.3 Algebraïsche uitbreidingen

In voorbeeld 1.1.3 hebben we een uitbreiding gecreëerd door $\sqrt{2}$ toe te voegen aan $\mathbb{Q}$. Dit is niet de enige uitbreiding van $\mathbb{Q}$ waar $\sqrt{2}$ in zit, de gehele reële getallen zijn bijvoorbeeld ook een uitbreiding van $\mathbb{Q}$. Het lichaam in het voorbeeld is echter van extra interesse omdat het *de kleinste uitbreiding van* $\mathbb{Q}$ *met* $\sqrt{2}$ is. Je moet dit zien als de uitbreiding van $\mathbb{Q}$ met $\sqrt{2}$ eraan toegevoegd die precies alle elementen bevat die nodig zijn om te voldoen aan de definitie van een lichaam en verder niets.

Definitie 1.1.8. Zij F een lichaam en $\alpha \notin F$, dan is **de kleinste uitbreiding van F die α bevat** de doorsnede van alle uitbreidingen van F die α bevatten. We noteren deze kleinste uitbreiding als $F(\alpha)$. Zij $\bar{F}$ de algebraïsche afsluiting van F, en $A = \{F' \text{ tussenlichaam van } \bar{F} \text{ en } F | \alpha \in F'\}$, dan is

$$F(\alpha) = \bigcap_{F' \in A} F'.$$

■

Je kunt aan zo'n uitbreiding $F(\alpha)$ ook nog een element β toe voegen, dan krijg je $F(\alpha)(\beta)$. Dit schrijven we ook wel als $F(\alpha, \beta)$ en dit is de kleinste uitbreiding van F die de elementen α en β bevat. Dit kun je zo vaak doen als je wilt.

Voorbeeld 1.1.9. Beschouw het lichaam $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dit is de kleinste uitbreiding van $\mathbb{Q}$ die $\sqrt{2}$ en $\sqrt{3}$ bevat. Dit lichaam is een uitbreiding van zowel $\mathbb{Q}$ als van $\mathbb{Q}(\sqrt{2})$ en van $\mathbb{Q}(\sqrt{3})$. Dit lichaam bevat ook $\sqrt{2}\sqrt{3} = \sqrt{6}$ en is dus ook een uitbreiding van het lichaam $\mathbb{Q}(\sqrt{6})$. ■

We noemen een uitbreiding van de vorm $F(\alpha)$ ook wel een *simpele uitbreiding* van F.

In sommige gevallen, zoals in het voorbeeld, is $F(\alpha)$ gelijk aan $F[\alpha]$. Dit blijkt precies te gebeuren als α *algebraïsch* is.

Definitie 1.1.10. Een element $\alpha \in F/E$ is **algebraïsch over E met graad** n, als er een irreducibel monisch polynoom $p \in E[x]$ van graad n bestaat zodat $p(\alpha) = 0$.

Als zo'n polynoom bestaat, noemen we dit het **minimale polynoom** van α over E. ■

Het algebraïsch zijn van een element α over een lichaam E hangt dus samen met het bestaan van een bepaald polynoom. De graad van het polynoom blijkt ook samen te hangen met de graad van het kleinste uitbreidingslichaam $E[\alpha]$ van E met α.

Stelling 1.1.11. *Een element is α algebraïsch is met graad n over een lichaam E, dan en slechts dan als geldt dat $[E(\alpha) : E] = n$.* ■

We kunnen het begrip algebraïsch ook definiëren voor uitbreidingen.

Definitie 1.1.12. Zij F/E een uitbreiding. We zeggen dat F een **algebraïsche uitbreiding** is als elke $\alpha \in F$ algebraïsch is over E. ■

1.1.4 Normale uitbreidingen

Definitie 1.1.13. Zij E een lichaam. We zeggen dat een polynoom $p \in E[x]$ **splijt** over F/E, als zij te factoriseren is als een product van lineaire termen die ieder ook in $F[x]$ zitten. ■

Voorbeeld 1.1.14. Het polynoom $f = x^2 - 2 \in \mathbb{Q}$ splijt niet over $\mathbb{Q}$ zelf omdat het niet te factoriseren is in lineaire termen (het is een irreduciebele polynoom in $\mathbb{Q}$). Zij splijt echter wel over $\mathbb{Q}(\sqrt{2})$ omdat $f = (x - \sqrt{2})(x + \sqrt{2})$. De lineaire factoren waar je f in opsplitst zitten allebei in $\mathbb{Q}(\sqrt{2})[x]$. ■

Definitie 1.1.15. Zij E een lichaam en $f \in F[x]$ een polynoom van graad n, dan is het **splijtlichaam** van f over E een uitbreiding F/E zodat f over F splijt en zodat

$$f = c \prod_{i=1}^{n} (x - \alpha_i)$$

waarbij $c \in E$ en $F = E(\alpha_1, \alpha_2, \cdots, \alpha_n)$. ■

Stelling 1.1.16. *Zij F een lichaam en $f \in F[x]$. Dan is het splijtlichaam K van f over F uniek. Er geldt:* $[K : F] \leq \deg f!$ ■

Definitie 1.1.17. Een uitbreiding F/E is **normaal** als elke irreduciebele polynoom $f \in E[x]$, een wortel heeft in F dan en slechts dan als F een splijtlichaam van f is. ■

Als F/E dus een normale uitbreiding is en $\alpha \in F$ een wortel is van een polynoom $f \in E[x]$, dan moet F ook alle andere wortels van f bevatten. Hieruit kunnen we de volgende stelling herleiden:

Stelling 1.1.18. *Een uitbreiding F/E is **normaal** als er een polynoom $f \in E[x]$ bestaat zodat F het splijtlichaam is van f.* ■

Voorbeeld 1.1.19. Beschouw $F = \mathbb{Q}(\sqrt{2})$. Dit is duidelijk het splijtlichaam van het polynoom $f = x^2 - 2$, F is dus normaal. ■

Voorbeeld 1.1.20. Een goed voorbeeld van een uitbreiding die *niet* normaal is, is $\mathbb{Q}(\sqrt[3]{2})$. We kijken naar het element $\sqrt[3]{2}$. Dit is een wortel van het polynoom $f = x^3 - 2 \in \mathbb{Q}[x]$. Volgens definitie 1.1.17 is $\mathbb{Q}(\sqrt[3]{2})$ alleen normaal als het een splijtlichaam is van f. Als we f in $\mathbb{C}[x]$ bekijken, zien we dat zij factoriseert als $(x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$ waarbij ω een derdemachtswortel van 1 is ($\omega = \frac{-1+i\sqrt{3}}{2}$). Hier gaat het fout, want ω zit niet in $\mathbb{Q}(\sqrt[3]{2})$. We zien dus dat $\mathbb{Q}(\sqrt[3]{2})$ volgens de definitie niet normaal is. ■

1.1.5 Separabele uitbreidingen

Definitie 1.1.21. Zij F een lichaam. Een polynoom $f \in F[x]$ heet **separabel** als zij géén dubbele wortels heeft in haar splijtlichaam. Anders heet zij **inseparabel**. ■

Definitie 1.1.22. Zij F/E een uitbreiding. Een element $\alpha \in F$ heet **separabel over** E als haar minimale polynoom separabel over E separabel is.

Een algebraïsche uitbreiding F/E is separabel als elke $\alpha \in F$ separabel is over E. ■

Stelling 1.1.23. *Elk lichaam van karakteristiek 0 is separabel.* ■

Stelling 1.1.24. *Elk eindig lichaam is separabel.* ■

1.2 Eindige lichamen

Stelling 1.2.1 ([4] Theorem 11.1.2)**.** *Beschouw $\mathbb{F}_{p^n}$ voor een $n \in \mathbb{N}$. Er gelden de volgende beweringen.*

1. $\forall \alpha \in \mathbb{F}_{p^n},\ \alpha^{p^n} = \alpha$.
2. $x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha)$.
3. *Het splijtlichaam van $x^{p^n} - x$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^n}$*

■

Gevolg 1.2.2. *Zij $f \in \mathbb{F}_p[x]$ separabel, dan splijt f over $\mathbb{F}_{p^n}$ dan en slechts dan als f een deler is van*

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha).$$

■

Stelling 1.2.3 ([4] Proposition 11.2.1)**.** *Zij $f \in \mathbb{F}_p[x]$ een irreducibel polynoom van graad n. Dan*

1. *f deelt $x^{p^m} - x$.*
2. *f is separabel.*
3. *$\forall m \in \mathbb{N}$, $f | x^{p^m} - x \iff f$ heeft een wortel in $\mathbb{F}_{p^m} \iff n|m$.*

■

1.3 Galoistheorie

Het onderwerp van deze scriptie is Galoistheorie, daar gaan we nu een begin aan maken. De Galoistheorie brengt een prachtig verband tussen lichamen- en groepentheorie aan het licht.

1.3.1 Galois-correspondentie

De *Galois-correspondentie* is een manier om de tussenlichamen van een lichaam en haar uitbreiding, te linken aan groepen van automorfismes. We moeten eerst wat begrippen introduceren.

Definitie 1.3.1. Zij F/E een uitbreiding. Beschouw de verzameling $\mathrm{Aut}_E(F)$ van ringautomorfismes $\phi : F \to F$ waarbij $\phi|_E = \mathrm{Id}_E$. Deze verzameling noemen we de verzameling van **E-automorfismes** van F naar F. Deze verzameling vormt een groep $(\mathrm{Aut}_E(F), \circ)$ onder compositie ($\circ$) waarbij Id (de identiteitsafbeelding $\mathrm{Id} : x \mapsto x$ die ook in $\mathrm{Aut}_E(F)$ zit) het identiteitselement van de groep is.

Laat nu $G \subset \mathrm{Aut}_E(F)$ een deelgroep van E-automorfismes zijn met compositie, dan noemen we de verzameling

$$F^G := \{\alpha \in F | \forall \phi \in G, \phi(\alpha) = \alpha\}$$

het **fixlichaam** van G. ■

Het fixlichaam van een deelgroep G van de E-automorfismes is het grootste tussenlichaam van E en F dat vast wordt gehouden door alle automorfismes in G.

Er bestaat een verband tussen de tussenlichamen van een uitbreiding F/E en E en de deelgroepen van $\mathrm{Aut}_E(F)$. Laat $T_{F/E} = \{\text{tussenlichamen van } F \text{ en } E\}$ en $D_{F/E} = \{\text{deelgroepen van } \mathrm{Aut}_E(F)\}$. We kunnen nu een functie $\gamma_{F/E} : T \to D$ definiëren die elk tussenlichaam K naar de deelgroep $\mathrm{Aut}_K(F) < \mathrm{Aut}_E(F)$ stuurt en een functie $\delta_{F/E} : D \to T$ die elke deelgroep G naar het fixlichaam F^G stuurt. Dit verband noemen we de *Galois-correspondentie*.

De Galois-correspondentie is *inclusie-omkerend*. Dit is een verwarrende eigenschap waar even over nagedacht dient te worden voordat er verder wordt gelezen. Dit houdt het volgende in:

- als $L \subset K$ tussenlichamen zijn van F/E, dan geldt $\mathrm{Aut}_K(F) < \mathrm{Aut}_L(F)$ en
- als $A < B$ deelgroepen zijn van $\mathrm{Aut}_E(F)$, dan geldt $F^B \subset F^A$.

Er geldt in het algemeen dat $G \subset \mathrm{Aut}_{F^G}(F)$ en dat $K \subset F^{\mathrm{Aut}_K(F)}$. G is niet altijd gelijk aan $\mathrm{Aut}_{F^G}(F)$ en K is niet altijd gelijk aan $F^{\mathrm{Aut}_K(F)}$. De functies $\gamma_{F/E}$ en $\delta_{F/E}$ zijn dus niet altijd elkaars inversen.

Voorbeeld 1.3.2. Laat $F = \mathbb{Q}\left(\sqrt[3]{2}\right)$ en $E = \mathbb{Q}$. Omdat $[F : E] = 3$ en de graad van uitbreidingen multiplicatief is, kunnen er geen tussenlichamen zijn behalve F en E zelf (want 3 is een priemgetal).

We zien dat $\gamma_{F/E}(E) = \mathrm{Aut}_E(F)$. Dat is de groep die alle automorfismes $\sigma : F \to F$ bevat die alle elementen van E op hun plek laten. We weten dat voor elke $\sigma \in \mathrm{Aut}_E(F)$ geldt dat

$$2 = \sigma(2) = \sigma\left(\sqrt[3]{2}^3\right) = \sigma\left(\sqrt[3]{2}\right)^3$$

dus $\sigma\left(\sqrt[3]{2}\right)$ moet een wortel zijn van het polynoom $f = x^3 - 2$. Zoals we in voorbeeld 1.1.20 zagen, zit er maar één van de drie wortels van f in F. Er is dus maar één element waar we $\sqrt[3]{2}$ naartoe kunnen sturen, en dat is $\sqrt[3]{2}$ zelf. Elke σ stuurt dus elk rationaal getal, maar ook $\sqrt[3]{2}$ naar zichzelf, wat betekent dat $\sigma = \mathrm{Id}$.

We zien dus dat $\mathrm{Aut}_E(F) = \{\mathrm{Id}\}$, maar per definitie geldt ook dat $\mathrm{Aut}_F(F) = \{\mathrm{Id}\}$ (want dit zijn alle automorfismes die alle elementen op hun plaats houden). Tot slot zien we dat $E \subsetneq F = F^{\mathrm{Aut}_E(F)}$, dus

$$\delta_{F/E}\left(\gamma_{F/E}(E)\right) = \delta_{F/E}\left(\mathrm{Aut}_E(F)\right) = F^{\mathrm{Aut}_E(F)} = F \neq E$$

dus $\gamma_{F/E}$ en $\delta_{F/E}$ zijn niet elkaars inversen. ■

Dit zit hem er in dat het lichaam F in het voorbeeld niet normaal is. Voor uitbreidingen die normaal, algebraïsch en separabel zijn, zijn $\gamma_{F/E}$ en $\delta_{F/E}$ wel elkaars inversen.

Stelling 1.3.3. *Zij F/E een algebraïsche uitbreiding. Dan zijn de volgende beweringen equivalent:*

- *F is normaal en separabel*
- *$\gamma_{F/E}$ en $\delta_{F/E}$ zijn elkaars inversen en vormen allebei een bijectie*
- *$G = \mathrm{Aut}_{F^G}(F)$ voor elke deelgroep $G < \mathrm{Aut}_E(F)$*
- *$K = F^{\mathrm{Aut}_K(F)}$ voor elk tussenlichaam $E \subset K \subset F$*
- *$|\mathrm{Aut}_E(F)| = [F : E]$*

■

1.3.2 Galois-uitbreidingen

Tot slot komen we aan bij de laatste sectie. Hier gaan we dan eindelijk praten over Galois-uitbreidingen. Dit is wat we krijgen als we een uitbreiding nemen die alle "leuke" eigenschappen heeft.

Definitie 1.3.4. Als een algebraïsche uitbreiding F/E voldoet aan één van de eigenschappen van stelling 1.3.3 (en dus aan alle), dan noemen we dit een **Galois-uitbreiding**.

In dit geval schrijven we $\mathrm{Aut}_E(F) = \mathrm{Gal}(F/E)$. Voor een $f \in E[X]$ definiëren we $\mathrm{Gal}(f/E)$ als de galoisgroep van het splijtlichaam van f over E. ■

Voorbeeld 1.3.5. Beschouw het lichaam $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$. We gaan laten zien dat dit een Galois-uitbreiding is.

Eerst willen we laten zien dat F algebraïsch is. Omdat we in voorbeeld 1.1.7 hebben gezien dat $[F : \mathbb{Q}] = 4$, volgt dit uit stelling 1.1.11.

Nu moet F nog voldoen aan een (en dus alle) van de eigenschappen van stelling 1.3.3. We gaan laten zien dat F normaal is door een polynoom te vinden dat splijt over F. Beschouw het polynoom $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Dit polynoom factoriseert als $\left(x - \sqrt{2} - \sqrt{3}\right)\left(x - \sqrt{2} + \sqrt{3}\right)\left(x + \sqrt{2} - \sqrt{3}\right)\left(x + \sqrt{2} + \sqrt{3}\right)$ in $F[x]$. Ook

zien we dat $F = \mathbb{Q}\left(\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}\right)$. Hieruit volgt dat F het splijtlichaam is van f en dus dat F normaal is. Lichamen van karakteristiek 0 zijn automatisch separabel, dus F voldoet aan alle eigenschappen van stelling 1.3.3.

We weten nu dat F Galois is. Dit betekent dat er een bijectief verband is tussen de tussenlichamen van $F/\mathbb{Q}$ en de ondergroepen van $\mathrm{Aut}_{\mathbb{Q}}(F)$. We gaan een kijkje nemen naar dit verband.

Laten we eerst kijken hoe $\mathrm{Aut}_{\mathbb{Q}}(F)$ er nu eigenlijk uitziet. We weten dat het de groep is van alle $\mathbb{Q}$-automorfismes van F naar zichzelf, dit zijn dus bijectieve afbeeldingen die alle rationale getallen op hun plaats moeten laten, maar alle 'nieuwe' elementen mogen veranderen.

We moeten eerst inzien dat een $\mathbb{Q}$-automorfisme de wortels van een polynoom altijd naar elkaar af moet beelden, stel immers dat $\phi \in \mathrm{Aut}_{\mathbb{Q}}(K)$ voor een uitbreiding $K/\mathbb{Q}$, dat $g \in \mathbb{Q}[x]$ en dat $g(\alpha) = 0$. Omdat automorfismes optelling en vermenigvuldiging behouden, moet $g(\phi(\alpha)) = \phi(g(\alpha)) = 0$, $\phi(\alpha)$ moet dus ook een wortel van g zijn.

Als we willen weten wat een specifiek automorfisme doet, is het genoeg om te weten wat het doet met $\sqrt{2}$ en $\sqrt{3}$, alle andere elementen in F zijn te herleiden tot producten of sommen van deze twee wortels. We kunnen elk van de twee wortels echter maar naar een beperkt aantal elementen sturen, de afbeeldingen van $\sqrt{2}$ en $\sqrt{3}$ moeten immers ook wortels zijn van x^2-2 en x^2-3 respectievelijk. We kunnen $\sqrt{2}$ dus alleen naar zichzelf of naar $-\sqrt{2}$ sturen, voor $\sqrt{3}$ geldt hetzelfde verhaal. Laten we dus twee afbeeldingen definiëren:

$$\sigma : \sqrt{2} \mapsto -\sqrt{2} \qquad \tau : \sqrt{3} \mapsto -\sqrt{3}.$$

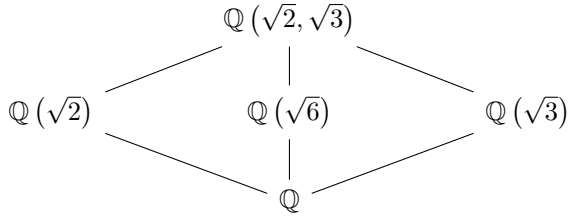
Alle afbeeldingen in $\mathrm{Aut}_{\mathbb{Q}}(F)$ moeten combinaties van deze twee afbeeldingen zijn. Op die manier vinden we het volgende:

$$\mathrm{Aut}_{\mathbb{Q}}(F) = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\}.$$

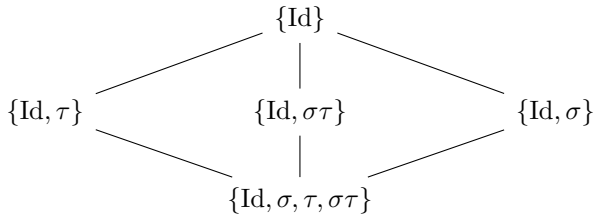
Nu gaan we even kijken hoe de tussenlichamen van $F/\mathbb{Q}$ eruitzien. We hebben in voorbeeld 1.1.7 al laten zien dat F een uitbreiding is van de lichamen $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{3}\right)$ en $\mathbb{Q}\left(\sqrt{6}\right)$. Dit zijn ook de enige mogelijke tussenlichamen.

Nu zijn we klaar om de Galois-correspondentie in beeld te brengen. Om dit te doen, maken we twee schema's, links is het schema van de tussenlichamen van $F/\mathbb{Q}$ te zien en rechts het schema van de ondergroepen van $\mathrm{Aut}_{\mathbb{Q}}(F)$:

Tussenlichamen van $F/\mathbb{Q}$



Ondergroepen van $\mathrm{Aut}_{\mathbb{Q}}(F)$



Hier wordt gelijk duidelijk waarom de Galois-correspondentie inclusion-reversing is. ■

Stelling 1.3.6. *Zij F/E een Galois-uitbreiding, en $E \subset K \subset F$ een tussenlichaam, dan is F/K ook Galois. Er hoeft niet altijd te gelden dat K/E Galois is.* ■

Stelling 1.3.7. *Zij p een priemgetal, $n \in \mathbb{N}$ en $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ een afbeelding zo dat $\phi : \alpha \mapsto \alpha^p$ voor alle $\alpha \in \mathbb{F}_{p^n}$. dan geldt:*

1. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois.*

2. $\phi \in \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$

3. $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) \simeq \mathbb{Z}/n\mathbb{Z}$ *is cyclisch van orde* n*, en wordt gegenereerd door* ϕ*.*

■

Hoofdstuk 2

Symmetrische functies

Voor we stelling 0.0.1 op gaan lossen, is het leuk om eerst te kijken wat er gebeurt als we de Galoisgroep nemen van het algemene polynoom

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

waarbij de coëfficiënten algebraïsch onafhankelijke variabelen zijn. In dit hoofdstuk zullen we bewijzen dat dit polynoom een maximale Galoisgroep heeft. Ook behandelen we in dit hoofdstuk de theorie over symmetrische functies die we nodig gaan hebben voor het bewijs van 0.0.1.

2.1 Het algemene polynoom

Het doel van deze paragraaf, is om te bewijzen dat elk algemeen polynoom

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in E = \mathbb{Q}\left(a_0, a_1, \cdots, a_{n-1}\right),$$

met $a_0, \cdots, a_{n-1}$ variabelen (dit zijn algebraïsch onafhankelijke elementen), een Galoisgroep heeft (we hebben het hier over de Galoisgroep van het splijtlichaam van f over E) die isomorf is met de symmetrische groep S_n. Dit doen we door middel van symmetrische functies. Voor de stellingen over symmetrische functies heb ik het boek [1] hoofdstuk VII.7 gebruikt.

Definitie 2.1.1. Een functie $s\left(t_1, t_2, \cdots, t_n\right)$ heet **symmetrisch** als zij behouden blijft onder permutatie van de argumenten:

zij σ een permutatie van $1, \cdots, n$, dan is $s\left(t_{\sigma 1}, \cdots, t_{\sigma n}\right) = s\left(t_1, \cdots, t_n\right)\ \forall \sigma \in S_n$.

■

Definitie 2.1.2. Voor elke $n \in \mathbb{Z}_+$ zijn de **elementaire symmetrische functies van graad** n, de functies $s_{n,i}$ voor alle $i \in \{1, 2, \cdots, n\}$, waarbij $s_{n,i}\left(t_1, t_2, \cdots, t_n\right)$ gegeven wordt door de som over alle verschillende producten van i verschillende factoren gekozen uit $t_1, t_2, \cdots, t_n$:

$$s_{n,i}\left(t_1, t_2, \cdots, t_k\right) = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} t_{j_1} \cdots t_{j_i}.$$

■

Voorbeeld 2.1.3. We bekijken de vierdegraads elementaire symmetrische functies:

$$\begin{aligned} s_{4,1}(a,b,c,d) &= a+b+c+d \\ s_{4,2}(a,b,c,d) &= ab+ac+ad+bc+bd+cd \\ s_{4,3}(a,b,c,d) &= abc+abd+acd+bcd \\ s_{4,4}(a,b,c,d) &= abcd \end{aligned}$$

■

Dat de elementaire symmetrische functies ook echt voldoen aan de definitie van symmetrie bewijzen we hier.

Stelling 2.1.4. *De elementaire symmetrische functies zijn symmetrisch.* ■

Bewijs. Laat $t_1, t_2, \cdots, t_n$ algebraïsch onafhankelijke variabelen zijn. Beschouw de functie

$$P_n = (x-t_1)(x-t_2)\cdots(x-t_n).$$

Door uitwerken van de producten krijgen we

$$P_n = x^n - s_1 x^{n-1} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n \in \mathbb{Q}(s_1, s_2, \cdots, s_n)[x],$$

waarbij $s_i := s_{n,i}(t_1, t_2, \cdots, t_n)$ voor alle i. Zij $\sigma \in S_n$ een permutatie van $t_1, \cdots, t_n$. Zoals hieronder beschreven, zien we dat $x^n - s_1 x^{n-1} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n$ behouden blijft onder permutatie van de argumenten.

$$\begin{aligned} \sigma\left(x^n - s_1 x^{n-1} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n\right) &= \sigma\left((x-t_1)(x-t_2)\cdots(x-t_n)\right) \\ &= (x-\sigma t_1)(x-\sigma t_2)\cdots(x-\sigma t_n) \\ &= (x-t_1)(x-t_2)\cdots(x-t_n) \\ &= x^n - s_1 x^{n-1} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n. \end{aligned}$$

Daaruit volgt dat alle $s_1, s_2, \cdots, s_n$ behouden blijven onder permutatie en dus inderdaad symmetrisch zijn.

□

Stelling 2.1.5. *Laat P_n, $t_1, \cdots, t_n$ en $s_1, \cdots, s_n$ zijn zoals in het vorige bewijs en laat $S := \mathbb{Q}(s_1, \cdots, s_n)$ en $T := \mathbb{Q}(t_1, \cdots, t_n)$. Dan is T/S Galois en* $\mathrm{Gal}(T/S) \simeq S_n$. ■

Bewijs. Om aan te tonen dat T/S Galois is, moeten we volgens definitie 1.3.4 laten zien dat T/S algebraïsch en normaal is. Beide eigenschappen volgen uit het feit dat T het splijtlichaam van P_n over S is. Hierdoor zijn alle $t_1, t_2, \cdots, t_n$ (en daarmee ook T) algebraïsch, en is T normaal; T/S is dus Galois.

Voor het tweede deel van het bewijs, combineren we stellingen 1.1.16 en 1.3.3 om in te zien dat

$$|\mathrm{Gal}(T/S)| = [T:S] \leq n!.$$

Voor elke permutatie $\sigma \in S_n$ van $t_1, \cdots, t_n$, geldt dat σ een automorfisme van T naar zichzelf is. Omdat $s_1, \cdots, s_n$ behouden blijven onder permutatie van $t_1, \cdots, t_n$, geldt dat σ een S-automorfisme van T naar zichzelf is. Hieruit volgt dat $\sigma \in \mathrm{Gal}(T/S)$ voor elke $\sigma \in S_n$ dus $S_n \leq \mathrm{Gal}(T/S)$. We hebben nu dat

$$n! = |S_n| \leq |\mathrm{Gal}(T/S)| = [T:S] \leq n!,$$

dus moet $|\mathrm{Gal}(T/S)| = n!$ en dus $\mathrm{Gal}(T/S) = S_n$. □

2.2 Galois resolventen

In deze paragraaf behandelen we het begrip *Galois resolvent*, wat we nodig gaan hebben voor het bewijs van de stelling van Dedekind in het volgende hoofdstuk. Voor de stof over Galois resolventen heb ik het boek [4] hoofdstuk 12.2 gebruikt.

Definitie 2.2.1. Zij $f \in F[x]$ een separabel polynoom waarbij $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ in het splijtlichaam L van f over F. Beschouw voor $v_1, v_2, \cdots, v_n \in F$ de polynoom

$$r(y) = \prod_{\sigma \in S_n} \left(y - \left(v_1\alpha_{\sigma(1)} + \cdots + v_n\alpha_{\sigma(n)}\right)\right).$$

Als de elementen $v_1, v_2, \cdots, v_n$ zó gekozen worden dat de elementen $v_1\alpha_{\sigma(1)} + \cdots + v_n\alpha_{\sigma(n)}$ voor alle $\sigma \in S_n$ verschillend zijn, dan noemen we $r(y)$ een **Galois resolvent** van f. ■

Lemma 2.2.2. *Zij $g \in F[t_1, t_2, \cdots, t_n]$ en zij s_i als in het bewijs van stelling 2.1.4, dan is g symmetrisch dan en slechts dan als $g \in F[s_1, s_2, \cdots, s_n]$.* ■

Bewijs. Uit stelling 2.1.5 volgt dat T/S Galois is en dat dus $S = T^{S_n}$. Als $g \in F[t_1, t_2, \cdots, t_n]$ dan is g invariant onder alle permutaties van $t_1, t_2, \cdots, t_n$ (dus onder alle elementen uit S_n) dan en slechts dan als $g \in S$. Aangezien g een polynoom moet zijn, moet $g \in F[s_1, s_2, \cdots, s_n]$. □

Lemma 2.2.3. *Zij $f \in F[x]$ een monisch, separabel polynoom met wortels $\alpha_1, \alpha_2, \cdots, \alpha_n$ in het splijtlichaam L van f over F en zij $g \in F[t_1, t_2, \cdots, t_n]$ een symmetrisch polynoom, dan is*

$$g(\alpha_1, \alpha_2, \cdots, \alpha_n) \in F.$$

■

Bewijs. Definieer de afbeelding $\phi : F[t_1, t_2, \cdots, t_n] \to L$ zo dat $\phi(g) = g(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Dit is een ring homomorfisme. Omdat g symmetrisch is, kunnen we volgens lemma 2.2.2 g schrijven als een polynoom in $F[s_1, s_2, \cdots, s_n]$ (waarbij s_i gedefinieerd is zoals in het bewijs van stelling 2.1.4). Als we g evalueren in $\alpha_1, \alpha_2, \cdots, \alpha_n$, dan krijgen we dat $g(\alpha_1, \alpha_2, \cdots, \alpha_n)$ een polynoom is in de variabelen $s_{n,i}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ voor $i = 1, 2, \cdots, n$ met coëfficiënten in F. Maar de elementen $s_{n,i}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ voor $i = 1, 2, \cdots, n$ zijn bovendien (soms vermenigvuldigd met -1) de coëfficiënten van $f \in F[x]$. Deze elementen moeten dus in F zitten dus is

$$g(\alpha_1, \alpha_2, \cdots, \alpha_n) \in F.$$

□

Stelling 2.2.4. *Zij $r(y)$ een Galois resolvent van f, dan is $r(y) \in F[y]$.* ■

Bewijs. Zij f en $r(y)$ zoals in definitie 2.2.1. Laat

$$R(y) = \prod_{\sigma \in S_n} \left(y - \left(v_1 t_{\sigma(1)} + \cdots + v_n t_{\sigma(n)}\right)\right) \in F[t_1, t_2, \cdots, t_n]$$

voor $t_1, t_2, \cdots, t_n$ algebraïsch onafhankelijke variabelen. Het permuteren van $t_1, t_2, \cdots, t_n$, permuteert de factoren, dus $R(y)$ is symmetrisch met betrekking tot de elementen $t_1, t_2, \cdots, t_n$. Als we $R(y)$ uitwerken krijgen we

$$R(y) = \sum_{i=0}^{n!} g_i(t_1, t_2, \cdots, t_n)\, y^i$$

voor zekere symmetrische functies $g_1, g_2, \cdots, g_{n!} \in F[t_1, t_2, \cdots, t_n]$. Volgens lemma 2.2.3, is $g_i(\alpha_1, \alpha_2, \cdots, \alpha_n) \in F$ voor alle $i = 1, 2, \cdots, n!$, dus

$$r(y) = \sum_{i=0}^{n!} g_i(\alpha_1, \alpha_2, \cdots, \alpha_n) y^i \in F(y).$$

□

Stelling 2.2.5. *Zij f zoals in definitie 2.2.1. Je kunt altijd $v_1, v_2, \cdots, v_n$ vinden zo dat de elementen $v_1\alpha_{\sigma(1)} + \cdots + v_n\alpha_{\sigma(n)}$ voor alle $\sigma \in S_n$ verschillend zijn. Er is dus altijd een Galois resolvent te vinden voor een polynoom f.* ■

Om stelling 2.2.5 te bewijzen hebben we eerst een lemma nodig.

Lemma 2.2.6. *Zij V een eindig-dimensionale vectorruimte over een oneindig lichaam F en zij $V_1, V_2, \cdots, V_m$ stricte deelruimtes van V. Dan is*

$$V \neq \bigcup_{i=1}^{m} V_i.$$

■

Bewijs. We nemen, met het doel op een tegenspraak uit te komen, aan dat $V = \bigcup_{i=1}^{m} V_i$. We mogen aannemen dat er geen deelruimte V_k bestaat zo dat $V_j \subset V_k \, \forall j \neq k$, anders zou $V == \bigcup_{i=1}^{m} V_i = V_k$ en zou V_k geen stricte deelruimte zijn. Neem dus aan dat er een deelruimte (voor het gemak kiezen we V_1) bestaat die geen deelverzameling is van een andere deelruimte. Dan hebben we dat $V_1 \not\subset V_i \, \forall i > 1$. Dan geldt dus $\forall i > 1 \, \exists \alpha_i \in V_1 : \alpha_i \notin V_i$. Definieer nu $\alpha := \alpha_2 + \alpha_3 + \cdots + \alpha_m$, dan is $\forall i > 1 \; \alpha \notin V_i$ dus $\alpha \notin \bigcup_{i=2}^{m} V_i$ dus $V_1 \not\subset \bigcup_{i=2}^{m} V_i$.

Er bestaat dus een element $\beta \in V \setminus V_1$. Nu hebben we dat $\lambda\alpha + \beta \in V \, \forall \lambda \in F$. We weten dat $\lambda\alpha \in V_1$ dus als $\lambda\alpha + \beta \in V_1$ dan is $\lambda\alpha + \beta - \lambda\alpha = \beta \in V_1$ en dat klopt niet, $\lambda\alpha + \beta$ zit dus niet in V_1, maar in een andere stricte deelruimte van V. We weten dus dat $\forall \lambda \in F \, \exists V_i \, (i > 1) \; : \lambda\alpha + \beta \in V_i$. Kies nu m verschillende elementen $\lambda_1, \lambda_2, \cdots, \lambda_m$ uit F, dan krijgen we m verschillende elementen $\lambda_i\alpha + \beta$, die verspreid zijn over $m-1$ verschillende deelruimtes $V_2, V_3, \cdots, V_m$. Volgens het duiventilprincipe van Dirichlet, moet er minstens één deelruimte V_i zijn die twee van deze elementen bevat. Stel dus $\lambda_1\alpha + \beta, \lambda_2\alpha + \beta \in V_i$, dan moet $\frac{\lambda_1\alpha+\beta-\lambda_2\alpha+\beta}{\lambda_1-\lambda_2} = \frac{(\lambda_1-\lambda_2)\alpha}{\lambda_1-\lambda_2} = \alpha \in V_i$. Wat een contradictie oplevert, want $\alpha \notin V_i$. □

Bewijs van stelling 2.2.5. Zij L/F een uitbreiding van een oneindig lichaam en $\alpha_1, \alpha_2, \cdots, \alpha_n \in L$ verschillende elementen. Voor elke twee verschillende permutaties $\sigma, \tau \in S_n$ definiëren we de verzameling

$$V_{\sigma,\tau} := \left\{ (v_1, v_2, \cdots, v_n) \in F^n | \sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right) v_i = 0 \right\}.$$

We weten dat $V_{\sigma,\tau} \subset F^n$, ook moet $V_{\sigma,\tau}$ een vectorruimte zijn: stel $\vec{v} = (v_1, v_2, \cdots, v_n) \in V_{\sigma,\tau}, \vec{v'} = (v'_1, v'_2, \cdots, v'_n) \in V_{\sigma,\tau}$ en $\lambda \in F$, dan is

$$\sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right)(v_i + \lambda v'_i) = \sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right) v_i + \lambda \sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right) v'_i = 0$$

dus $\vec{v} + \lambda\vec{v'} \in V_{\sigma,\tau}$. Ook is $V_{\sigma,\tau}$ niet gelijk aan F^n, immers is er voor elke $\sigma \neq \tau$ een α_k zo dat $\alpha_{\sigma(k)} \neq \alpha_{\tau(k)}$, dus als we $\vec{v}(v_1, v_2, \cdots, v_n \in F^n)$ kiezen zo dat $v_j = 0 \, \forall j \neq k$ en $v_k = 1$, dan is $\sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right) v_i = \alpha_{\sigma(k)} - \alpha_{\tau(k)} \neq 0$ dus $\vec{v} \notin V_{\sigma,\tau}$.

We weten dus dat voor elke twee verschillend permutaties $\sigma, \tau \in S_n$, $V_{\sigma,\tau}$ een stricte deelruimte is van F^n. Definieer $\mathcal{H} := \{V_{\sigma,\tau} | \sigma, \tau \in S_n, \sigma \neq \tau\}$. Dan is volgens lemma 2.2.6

$$F^n \neq \bigcup_{\sigma \neq \tau \in S_n} V_{\sigma,\tau}.$$

Er moet dus een $\vec{v} \in F^n \setminus \bigcup_{\sigma \neq \tau \in S_n} V_{\sigma,\tau}$ zijn zo dat $\forall \sigma \neq \tau \in S_n \ \sum_{i=1}^{n} \left(\alpha_{\sigma(i)} - \alpha_{\tau(i)}\right) v_i \neq 0$, anders zou $\vec{v} \in V_{\sigma,\tau}$. Er zijn dus altijd $v_1, v_2, \cdots, v_n \in F$ te vinden zo dat de elementen $v_1\alpha_{\sigma(1)} + \cdots + v_n\alpha_{\sigma(n)}$ voor alle $\sigma \in S_n$ verschillend zijn. Er is dus altijd een Galois resolvent te vinden voor een polynoom f. □

We kunnen de Galois resolvent ook op een andere manier bekijken, we laten deze keer de $v_1, v_2, \cdots, v_n$ geen elementen van F zijn, maar algebraïsch onafhankelijke variabelen. We geven ze nu aan met $u_1, u_2, \cdots, u_n$. We definiëren een nieuwe functie,

$$r_u(y) := \prod_{\sigma \in S_n} \left(y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)\right) \in F[u_1, u_2, \cdots, u_n, y].$$

Stelling 2.2.7. *Zij $f \in F[x]$ een monisch, separabel polynoom met wortels $\alpha_1, \alpha_2, \cdots, \alpha_n$ in haar splijtlichaam L/F en $h \in F[u_1, u_2, \cdots, u_n, y]$ een irreducibele factor van $r_u(y)$. Voor elke permutatie $\tau \in S_n$ definiëren we τ_u als een permutatie van de elementen $u_1, u_2, \cdots, u_n$, zo dat $\tau_u(u_i) = u_{\tau(i)}$. Dan is* $\mathrm{Gal}(L/F)$ *geconjugeerd aan de groep*

$$G = \{\tau_u | \tau \in S_n,\ \tau_u(h) = h\}.$$

■

Bewijs. Voor elke permutatie $\mu \in S_n$ van de getallen $1, 2, \cdots, n$ definiëren we $\mu : \alpha_i \mapsto \alpha_{\mu(i)}$ op $L[u_1, u_2, \cdots, u_n, y]$ als een permutatie van de wortels α. De elementen die in de Galoisgroep $\mathrm{Gal}(L/F)$ zitten werken op dezelfde manier. We kunnen een $\sigma \in S_n$ kiezen zodat $y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right) | h$. Beschouw nu de functie

$$\begin{aligned} g &= \prod_{\mu \in \mathrm{Gal}(L/F)} \mu\left(y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)\right) \\ &= \prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\mu\left(\alpha_{\sigma(1)}\right) + \cdots + u_n\mu\left(\alpha_{\sigma(n)}\right)\right)\right) \\ &= \prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\mu\sigma(1)} + \cdots + u_n\alpha_{\mu\sigma(n)}\right)\right) \end{aligned}$$

Definieer

$$g'(t_1, t_2, \cdots, t_n, y) := \prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1t_{\mu\sigma(1)} + \cdots + u_nt_{\mu\sigma(n)}\right)\right) \in F[t_1, t_2, \cdots, t_n, u_1, u_2, \cdots, u_n, y].$$

Elementen uit $\mathrm{Gal}(L/F)$ permuteren alleen de factoren van g dus g' is symmetrisch onder permutatie van $t_1, t_2, \cdots, t_n$. Volgens lemma 2.2.3 is

$$g'(\alpha_1, \alpha_2, \cdots, \alpha_n, y) = g \in F[u_1, u_2, \cdots, u_n, y].$$

Aangezien $y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right) | h$ moet gelden dat

$$\begin{aligned} \forall \phi \in \mathrm{Gal}(L/F) : &\phi\left(y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)\right) | \phi(h) \\ &\left(y - \left(u_1\phi\left(\alpha_{\sigma(1)}\right) + \cdots + u_n\phi\left(\alpha_{\sigma(n)}\right)\right)\right) | \phi(h) \end{aligned}$$

En omdat $h \in F[u_1, u_2, \cdots, u_n, y]$ coëfficiënten in F heeft, geldt $\forall \phi \in \mathrm{Gal}(L/F) : \phi(h) = h$. Dus alle factoren van g delen h in L, dus $g|h$. Omdat $g \in F[u_1, u_2, \cdots, u_n, y]$ geldt $g|h$ ook in $F[u_1, u_2, \cdots, u_n, y]$. Omdat h irreducibel is volgt daar uit dat $g = h$.

Neem een $\tau_u \in G$, dan is $\tau_u(h) = h$. Als we τ_u dus toepassen op $y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)$, moeten we weer een factor van h krijgen in $L[u_1, u_2, \cdots, u_n, y]$. We weten nu dat h factoriseert als $h = \prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\mu\sigma(1)} + \cdots + u_n\alpha_{\mu\sigma(n)}\right)\right)$ dus er moet een $\mu \in \mathrm{Gal}(L/F)$ bestaan zo dat

$$\begin{aligned}\tau_u\left(y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)\right) &= y - \left(u_{\tau(1)}\alpha_{\sigma(1)} + \cdots + u_{\tau(n)}\alpha_{\sigma(n)}\right) \\ &= \mu\left(y - \left(u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)}\right)\right) \\ &= y - \left(u_1\alpha_{\mu\sigma(1)} + \cdots + u_n\alpha_{\mu\sigma(n)}\right).\end{aligned}$$

Aangezien $u_1, u_2, \cdots, u_n$ algebraïsch onafhankelijke variabelen zijn, impliceert dit dat als $\tau(i) = j$, dan is

$$\tau_u\left(u_i\alpha_{\sigma(i)}\right) = u_j\alpha_{\sigma(j)},$$

dus dan is $\sigma(i) = \mu\sigma(j)$. Dan is $\tau^{-1}(j) = i$, dus dan moet gelden dat

$$\sigma(i) = \mu\sigma(j) = \sigma\tau^{-1}(j).$$

Omdat de elementen $\alpha_1, \alpha_2, \cdots, \alpha_n$ allemaal verschillend zijn, hebben we dus $\sigma\tau^{-1} = \mu\sigma$. Dit geeft ons $\tau_u = \sigma^{-1}\mu^{-1}\sigma \in \sigma^{-1}\,\mathrm{Gal}(L/F)\,\sigma$. We hebben nu dus dat $G \subset \sigma^{-1}\,\mathrm{Gal}(L/F)\,\sigma$.

Kies nu een willekeurige $\gamma \in \mathrm{Gal}(L/F)$, dan hebben we $\sigma^{-1}\gamma\sigma \in \sigma^{-1}\,\mathrm{Gal}(L/F)\,\sigma$.

$$\begin{aligned}\sigma^{-1}\gamma\sigma(h) &= \sigma^{-1}\gamma\sigma\left(\prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\mu\sigma(1)} + \cdots + u_n\alpha_{\mu\sigma(n)}\right)\right)\right) \\ &= \sigma^{-1}\gamma\left(\prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\sigma\mu\sigma(1)} + \cdots + u_n\alpha_{\sigma\mu\sigma(n)}\right)\right)\right)\end{aligned}$$

Omdat $\gamma \in \mathrm{Gal}(L/F)$, permuteert γ alleen de factoren.

$$\begin{aligned}&= \sigma^{-1}\left(\prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\sigma\mu\sigma(1)} + \cdots + u_n\alpha_{\sigma\mu\sigma(n)}\right)\right)\right) \\ &= \left(\prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\sigma^{-1}\sigma\mu\sigma(1)} + \cdots + u_n\alpha_{\sigma^{-1}\sigma\mu\sigma(n)}\right)\right)\right) \\ &= \sigma^{-1}\gamma\sigma\left(\prod_{\mu \in \mathrm{Gal}(L/F)} \left(y - \left(u_1\alpha_{\mu\sigma(1)} + \cdots + u_n\alpha_{\mu\sigma(n)}\right)\right)\right) \\ &= h.\end{aligned}$$

Dus $\forall \gamma \in \mathrm{Gal}(L/F) : \sigma^{-1}\gamma\sigma \in G$, dus $\sigma^{-1}\,\mathrm{Gal}(L/F)\,\sigma \subset G$. Nu volgt dat $\sigma^{-1}\,\mathrm{Gal}(L/F)\,\sigma = G$. □

Hoofdstuk 3

Galoisgroepen van polynomen

In dit hoofdstuk en het hoofdstuk dat hier op volgt, behandelen we het artikel van van der Waerden en gaan we stelling 0.0.1 bewijzen.

3.1 De stelling van Dedekind

Voor zijn bewijs, gebruikt van der Waerden de volgende stelling. Hij bewijst deze stelling niet in zijn artikel, dat ga ik wel doen.

Stelling 3.1.1. *Zij $f \in \mathbb{Z}[x]$ een polynoom van graad n en p_1, p_2 en p_3 drie verschillende priemgetallen. Als f modulo deze priemgetallen op de volgende manieren te ontbinden is in factoren:*

1. $f \mod p_1$ *ontbindt als een lineaire factor en een irreducibele factor van graad $n-1$,*
2. $f \mod p_2$ *ontbindt als een kwadratische factor en één of twee factoren van oneven graad en*
3. $f \mod p_3$ *is irreducibel*

dan is $\mathrm{Gal}(f/\mathbb{Q}) = S_n$. ■

Om stelling 3.1.1 te bewijzen, moeten we eerst kijken naar de stelling van Dedekind.

Stelling 3.1.2 (De stelling van Dedekind)**.** *([4] 13.4.5) Zij $f \in \mathbb{Z}[x]$ een monisch, separabel polynoom van graad n en zij p een priemgetal dat de discriminant van f niet deelt. Definieer $\bar{f}$ als de reductie van f modulo p en laat $\bar{f}$ op de volgende manier ontbinden in irreducibele factoren*

$$\bar{f} = \bar{f}_1 \bar{f}_2 \cdots \bar{f}_k$$

met $n_i := \deg \bar{f}_i$ en $d := \mathrm{kgv}(n_1, n_2, \cdots, n_k)$. Dan gelden de volgende eigenschappen:

1. *De Galoisgroep van $\bar{f}$ over $\mathbb{F}_p$ is cyclisch van orde d.*
2. *De Galoisgroep van f over $\mathbb{Q}$ bevat een element dat op de wortels van f werkt aan de hand van disjuncte cykels van de vorm*

$$\underbrace{(. \quad . \quad .)}_{n_1\text{-cykel}}\underbrace{(. \quad . \quad .)}_{n_2\text{-cykel}}\cdots\underbrace{(. \quad . \quad .)}_{n_k\text{-cykel}}.$$

   Dus de Galoisgroep van f bevat een element van graad d.

■

Bewijs. De discriminant van $\bar{f}$, is de reductie van de discriminant van f modulo p. We weten dat f separabel is, haar discriminant kan dus niet 0 zijn (anders zou zij dubbele nulpunten hebben). Ook weten we dat p de discriminant van f niet deelt. De discriminant van $\bar{f}$ kan dus niet 0 zijn, hieruit volgt dat ook $\bar{f}$ separabel is.

We willen nu weten wat het splijtlichaam van $\bar{f}$ is over $\mathbb{F}_p$. Stel dat $\mathbb{F}_{p^m}$ het splijtlichaam van $\bar{f}$ is. Dan weten we van stelling 1.2.2 dat $\bar{f}|x^{p^m}-x$ en dat dus ook $\bar{f}_i|x^{p^m}-x$ voor alle $i=1,2,\cdots,k$. Vanwege deel 3 van stelling 1.2.3, moet $n_i|m$ voor alle i. Daaruit volgt dat $d|m$. Het splijtlichaam moet dus het kleinste lichaam $\mathbb{F}_{p^m}$ zijn zodat $d|m$. Dit moet $\mathbb{F}_{p^d}$ zijn. Vanwege stelling 1.3.7 is $\mathrm{Gal}\left(\mathbb{F}_{p^d}/\mathbb{F}_p\right)$ cyclisch van orde d, dit bewijst deel (1).

De afbeelding $\phi:\alpha\mapsto\alpha^p$ genereert de Galoisgroep $\mathrm{Gal}\left(\mathbb{F}_{p^d}/\mathbb{F}_p\right)$. Als je één wortel van $\bar{f}$ weet, dan weet je ze allemaal. Stel dat $\bar{f}(\alpha)=0$, dan zijn alle wortels van $\bar{f}$ gegeven door herhaaldelijk toepassen van ϕ op α:

$$\alpha,\alpha^p,\alpha^{p^2},\cdots,\alpha^{p^d-1}.$$

Hetzelfde kun je doen voor elke irreducibele factor $\bar{f}_i$ van $\bar{f}$. Als $\bar{f}_i(\alpha_i)=0$, dan zijn de wortels van $\bar{f}_i$ gegeven door

$$\alpha_i,\alpha_i^p,\alpha_i^{p^2},\cdots,\alpha_i^{p^{n_i}-1}.$$

De afbeelding ϕ werkend op specifiek de wortels van $\bar{f}_i$ is dus een $n_i-cykel$, en ϕ werkend op de wortels van $\bar{f}$ is het product van disjuncte cykels van lengtes $n_1,n_2,\cdots,n_k$.

We bekijken de algemene Galois resolvent

$$R(y)=\prod_{\sigma\in S_n}\left(y-\left(u_1t_{\sigma(1)}+\cdots+u_nt_{\sigma(n)}\right)\right)\in\mathbb{Z}\left[t_1,t_2,\cdots,t_n,u_1,u_2,\cdots,u_n,y\right]$$

voor de algebraïsch onafhankelijke variabelen $t_1,t_2,\cdots,t_n$. Deze functie is symmetrisch met betrekking tot $t_1,t_2,\cdots,t_n$, dus volgens lemma 2.2.2 moet $S(y)\in\mathbb{Z}\left[s_1,s_2,\cdots,s_n,u_1,u_2,\cdots,u_n,y\right]$ waarbij de elementen $s_1,s_2,\cdots,s_n$ zo zijn gedefinieerd als in stelling 2.1.4. Definieer nu $c_i:=s_{n,i}(\alpha_1,\alpha_2,\cdots,\alpha_n)$ voor alle $i=1,2,\cdots,n$, dan is

$$f=x^n-c_1+\cdots+(-1)^{n-1}c_{n-1}x+(-1)^n c_n\in\mathbb{Z}[x]$$
$$\bar{f}=x^n-\bar{c_1}+\cdots+(-1)^{n-1}\bar{c_{n-1}}x+(-1)^n\bar{c_n}\in\mathbb{F}_p[x].$$

Nu maken we $r_u(y)$ door $\alpha_1,\alpha_2,\cdots,\alpha_n$ in te vullen voor $t_1,t_2,\cdots,t_n$ in $R_u(y)$. Dat is hetzelfde als de elementen $c_1,c_2,\cdots,c_n$ invullen voor $s_1,s_2,\cdots,s_n$. Aangezien alle elementen c_i gehele getallen zijn, moet $r_u(y)\in\mathbb{Z}\left[u_1,u_2,\cdots,u_n,y\right]$. We definiëren ook $\bar{r_u}(y)$ als $r_u(y)$ gereduceerd modulo p. We krijgen $\bar{r_u}(y)$ dus door in $R_u(y)$ de elementen $\bar{c}_1,\bar{c}_2,\cdots,\bar{c}_n$ in te vullen voor $s_1,s_2,\cdots,s_n$. Nu moet $\bar{r_u}(y)\in\mathbb{F}_p\left[u_1,u_2,\cdots,u_n,y\right]$.

Zij h een irreducibele factor van $r_u(y)$. We mogen aannemen dat $h\in\mathbb{Z}\left[u_1,u_2,\cdots,u_n,y\right]$, want we kunnen elk rationaal polynoom vermenigvuldigen met een constante zodat het een polynoom met gehele coëfficiënten wordt. Volgens stelling 2.2.7 is $\mathrm{Gal}(f/\mathbb{Q})$ conjugent aan

$$G=\{\tau_u|\tau\in S_n,\ \tau_u(h)=h\}.$$

Zij $\bar{h}\in\mathbb{F}_p\left[u_1,u_2,\cdots,u_n,y\right]$ de reductie van h modulo p en zij $\bar{g}|\bar{h}$ een irreducibele factor van $\bar{h}$. Omdat $\bar{h}|\bar{r_u}(y)$, moet $\bar{g}$ een irreducibele factor van $\bar{r_u}(y)$ zijn. Weer vanwege stelling 2.2.7, moet de Galoisgroep $\mathrm{Gal}\left(\bar{f}/\mathbb{F}_p\right)$ conjugent zijn aan een groep

$$H=\{\tau_u|\tau\in S_n,\ \tau_u(\bar{g})=\bar{g}\}.$$

We gaan door middel van contradictie laten zien dat $H \subset G$. Stel dat $H \not\subset G$, dan is er een element $\tau_u \in H$ zo dat $\tau_u \notin G$. Voor dat element moet gelden $\tau_u(\bar{g}) = \bar{g}$ maar $\tau_u(h) = h' \neq h$. We weten dat $\tau_u(r_u(y)) = r_u(y)$, dus als $h|r_u(y)$, dan moet ook $h'|r_u(y)$, h' is dus ook een irreducibele factor van $r_u(y)$.

Omdat $\tau_u(h) = h'$, moet $\tau_u\left(\bar{h}\right) = \bar{h'}$. We weten dat $\bar{g}|\bar{h}$ en er moet ook gelden dat $\tau_u(\bar{g})\,|\tau_u\left(\bar{h}\right)$ dus $\bar{g}|\bar{h'}$. Omdat $\bar{h}$ en $\bar{h'}$ verschillende irreducibele delers zijn van $\bar{r_u}$, moet $\bar{g}$ twee keer een deler zijn van $\bar{r_u}$. Maar omdat $u_1, u_2, \cdots, u_n$ algebraïsch onafhankelijke variabelen zijn, zijn alle factoren van $\bar{r_u}$ verschillend en kan $\bar{r_u}$ geen meervoudige delers hebben. Dit is een contradictie, wat betekent dat $H \subset G$ dus

$$\forall \tau \in S_n, \tau_u(\bar{g}) = \bar{g} \Rightarrow \tau_u(h) = h.$$

We hadden gezien dat de Galoisgroep van $\bar{f}$ over $\mathbb{F}_p$ het element ϕ bevat; het product van k disjuncte cykels van lengtes $n_1, n_2, \cdots, n_k$.

We hebben nu dat H geconjugeerd is aan $\mathrm{Gal}\left(\bar{f}/\mathbb{F}_p\right)$. Een geconjugeerde van het product van k disjuncte cykels van lengtes $n_1, n_2, \cdots, n_k$ is weer een permutatie van dezelfde vorm, dus H bevat ook zo'n permutatie. Diezelfde permutatie zit dus ook in G omdat $H \subset G$. Tot slot hebben we dat G geconjugeerd is aan $\mathrm{Gal}(f/\mathbb{Q})$, dus ook $\mathrm{Gal}(f/\mathbb{Q})$ bevat zo'n permutatie. Dat element heeft orde d. □

3.2 Het voortbrengen van S_n met cykels

Door stelling 3.1.2 weten we dat een polynoom dat ontbindt op de manieren uit stelling 3.1.1, een n-cykel, een $(n-1)$-cykel en een product van een transpositie en één of twee cykels van oneven lengte. Als we kunnen bewijzen dat we met deze elementen, heel S_n kunnen genereren, dan hebben we stelling 3.1.1 bewezen. Voor de stof over het voortbrengen van S_n heb ik [3] gebruikt.

Allereerst is het handig om te bewijzen dat je met een product van een transpositie en één of twee cykels van oneven lengte, ook een transpositie kan maken.

Stelling 3.2.1. *Een permutatiegroep die een permutatie $\rho\sigma$ bevat die het product is van een transpositie ρ en het product σ van één of twee disjuncte cykels van oneven graad (die ook disjunct zijn met de transpositie), bevat een transpositie.* ■

Bewijs. De graad m van σ is het product van één of twee oneven getallen, en is dus zelf ook oneven. Als je $\rho\sigma$ m keer uitvoert, krijg je $(\rho\sigma)^m = \rho^m\sigma^m$, immers zijn de permutaties ρ en σ disjunct dus mogen we de exponent uitdelen. Nu hebben we dus $(\rho\sigma)^m = \rho^m\sigma^m = \rho^m = \rho$, we weten namelijk dat $\sigma^m = e$ de identiteit is, en dat het een oneven aantal keer toepassen van een transpositie, diezelfde transpositie weer teruggeeft. □

De symmetrische groep S_n is op verschillende manieren te genereren. De bekendste manier is door alle transposities.

Lemma 3.2.2. *De symmetrische groep S_n wordt gegenereerd door alle transposities.* ■

Bewijs. Zij $\sigma = (a_1 a_2 \cdots a_k) \in S_n$ een k-cykel. Beschouw het product van transposities $\tau := (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$. Voor een willekeurige $a_i, i = 1, 2, \cdots, k$ kijken we wat er mee gebeurt onder σ en τ.

Voor het gemak definiëren we $a_{k+1} := a_1$.

$$\sigma(a_i) = a_{i+1}$$

$$\begin{aligned}
\tau(a_i) &= (a_1 a_k) \cdots (a_1 a_{i+2})(a_1 a_{i+1})(a_1 a_i) \cdots (a_1 a_3)(a_1 a_2)\, a_i \\
&= (a_1 a_k) \cdots (a_1 a_{i+2})(a_1 a_{i+1})(a_1 a_i)\, a_i \text{ (immers doen de eerste } i-2 \text{ transposities niks met } a_i) \\
&= (a_1 a_k) \cdots (a_1 a_{i+2})(a_1 a_{i+1})\, a_1 \\
&= (a_1 a_k) \cdots (a_1 a_{i+2})\, a_{i+1} \\
&= a_{i+1} \text{ (immers doet de rest van de transposities ook niks met } a_{i+1})
\end{aligned}$$

Dus $\sigma = \tau$ dus voor elke $k \in \mathbb{N}$ is elke k-cykel σ te schrijven als het product van transposities. Elke permutatie is het product van cykels van verschillende lengtes, al die cykels, ongeacht hun lengte, kunnen geschreven worden als het product van transposities. Elke permutatie kan dus geschreven worden als het product van transposities. □

We weten nu dat S_n wordt gegenereerd door al haar transposities, maar we hebben niet eens alle transposities nodig.

Lemma 3.2.3. *De symmetrische groep S_n wordt gegenereerd door de transposities van opeenvolgende elementen*

$$(12), (23), \cdots, (n-1\ n).$$

■

Bewijs. We weten van lemma 3.2.2 dat S_n wordt gegenereerd door alle transposities. We gaan met behulp van volledige inductie bewijzen dat elke transpositie te schrijven is als het product van transposities van opeenvolgende elementen $(i\ i+1)$, dan zijn deze transposities namelijk genoeg om alle transposities, en dus heel S_n, te genereren. Zij (ij) een transpositie met $j-i=m$, dan willen we met inductie op m laten zien dat (ij) te schrijven is als het product van transposities van opeenvolgende elementen. Uiteraard is $(ji) = (ij)$ dus wat we voor (ij) bewijzen, geldt ook voor (ji).

Stel dat $m = 1$, dan is $(ij) = (i\ i+1)$, dat is het product van transposities van opeenvolgende elementen.

Stel nu dat $m = k > 1$ en dat de bewering klopt voor alle $m < k$. Beschouw de permutatie $\sigma = (j-1\ j)(i\ j-1)(j-1\ j)$, het is duidelijk dat deze permutatie alleen iets doet met de elementen $i, j-1$ en j, dus we gaan kijken wat er gebeurt met die elementen.

$$\begin{aligned}
\sigma(i) &= (j-1\ j)(i\ j-1)(j-1\ j)\, i \\
&= (j-1\ j)(i\ j-1)\, i \\
&= (j-1\ j)(j-1) \\
&= j
\end{aligned}$$

$$\begin{aligned}
\sigma(j-1) &= (j-1\ j)(i\ j-1)(j-1\ j)(j-1) \\
&= (j-1\ j)(i\ j-1)\, j \\
&= (j-1\ j)\, j \\
&= j-1
\end{aligned}$$

$$\begin{aligned}
\sigma(j) &= (j-1\ j)(i\ j-1)(j-1\ j)\, j \\
&= (j-1\ j)(i\ j-1)(j-1) \\
&= (j-1\ j)\, i \\
&= i
\end{aligned}$$

We zien dat $\sigma = (ij)$. We weten dat $(j-1\,j)$ een transpositie van opeenvolgende elementen is, verder is $(i\,j-1)$ ook een transpositie van opeenvolgende elementen omdat $j-1-i = k-1$ en de bewering klopte voor alle $m < k$. Nu weten we dus dat (ij) ook een product moet zijn van transposities van opeenvolgende elementen. De bewering klopt dus voor alle m. □

We kunnen S_n ook genereren met cykels van verschillende lengtes, een specifiek geval is de volgende stelling.

Lemma 3.2.4. *De symmetrische groep S_n wordt gegenereerd door de transpositie* (12) *en de n-cykel* $(1, 2, \cdots, n)$. ■

Bewijs. Zij $\sigma = (12\cdots n)$ en $\rho = (12)$. Beschouw de permutatie $\rho_k := \sigma^{k-1}\rho\sigma^{1-k}$. Zij $i \in \{1, 2, \cdots, n\}$, we kijken wat ρ_n met de getallen $1, 2, \cdots, n$ doet. De getallen met haakjes er omheen in de onderstaande berekeningen, zijn geen permutaties, maar stellen de volgorde van getallen voor. Links daarvan zie je welke permutatie we uit hebben gevoerd om deze volgorde te krijgen.

$$\begin{aligned}
&(12\cdots k\,k+1\cdots n) && \text{(we beginnen met de normale volgorde)}\\
\sigma^{1-k}:\ &(k\,k+1\cdots k-1) && \text{(we schuiven één keer naar rechts en } k \text{ keer naar links)}\\
\rho:\ &(k+1\,k\cdots k-1) && \text{(we wisselen de eerste twee posities om, dus } k \text{ en } k+1)\\
\sigma^{k-1}:\ &(12\cdots k+1\,k\cdots n) && \text{(we schuiven weer terug).}
\end{aligned}$$

Wat we nu effecief hebben gedaan, is k en $k+1$ transponeren, ρ_k is dus de transpositie $(k\,k+1)$. Op deze manier kunnen we elke transpositie van die vorm maken. Volgens lemma 3.2.3 kunnen we nu ook heel S_n genereren. □

We hebben nu bewezen dat we S_n kunnen genereren met een specifieke transpositie en n-cykel, maar de vraag is nu of we dit ook kunnen met elke willekeurige transpositie en n-cykel. Helaas kan dit niet altijd.

Voorbeeld 3.2.5. Beschouw de transpositie (13) en de 4-cykel (1234). Met (1234) kun je de volgende permutaties maken:

- (1234)
- $(1234)^2 = (13)$
- $(1234)^3 = (1432)$.

Hier is (13) al in bevat, elke combinatie van (13) en (1234) is dus gelijk aan een bepaald aantal keer herhalen van (1234), en het is duidelijk dat met alleen een 4-cykel geen S_4 kan worden gegenereerd. ■

Dit probleem doet zich voor als, voor een bepaalde $m > 1$, elke twee getallen die hetzelfde zijn modulo m allebei naar dezelfde restklasse modulo m worden gestuurd door zowel je transpositie en je n-cykel. Als dit het geval is, dan heeft elke combinatie van je transpositie en je n-cykel namelijk deze eigenschap, terwijl er wel degelijk permutaties bestaan in S_n die dit niet doen. De permutatie (12) bijvoorbeeld, want 1 wordt daardoor naar 2 gestuurd, maar $m+1$ blijft $m+1$, terwijl $1 \equiv m+1 \mod m$, maar $2 \not\equiv m+1 \mod m$. Deze permutatie zou niet kunnen worden gemaakt met een transpositie en n-cykel die deze eigenschap hebben.

Lemma 3.2.6. *De symmetrische groep S_n wordt gegenereerd door een transpositie $\rho = (ab)$ en een n-cykel σ dan en slechts dan als* $\gcd(m, n) = 1$ *voor de kleinste m zo dat $\sigma^m(a) = b$.* ■

Bewijs. We nemen aan dat $\sigma^m(a) = b$ en dat $\text{ggd}(m,n) = d$. We schrijven $\sigma = (a_1 a_2 \cdots a_n)$ zo dat $a = a_i$ en $b = a_j$ voor $i < j$ en waarbij $a_{n+1} := a_1$. We hebben $\forall k : \sigma(a_k) = a_{k+1}$. Als $\sigma^m(a) = b$ dan is dus $\sigma^m(a_i) = a_{i+m} = a_j$ dus $j - i = m$. We definiëren ook nog twee permutaties: τ, zo dat $\forall k : \rho(a_k) = a_{\tau(k)}$ en π, zo dat $\forall k : \sigma(a_k) = a_{\pi(k)}$.

Neem eerst aan dat S_n wordt gegenereerd door ρ en σ. Voor twee getallen $k, l \neq i, j$ met $k \equiv l \mod d$, hebben we dat $\tau(k) = k$ en $\tau(l) = l$, dus $\tau(k) \equiv \tau(l) \mod d$. We hebben ook dat $d|m = j - i$ dus $j - i = c \cdot d$ voor een zekere $c \in \mathbb{Z}$ dus $j = c \cdot d + i$ dus $j \equiv i \mod d$. Dus we hebben dat $\tau(j) = i \equiv i \mod d$ en $\tau(i) = j \equiv i \mod d$. We weten dus dat τ congruentie modulo d behoudt voor elk getal.

We hebben dat $\pi(k) \equiv k + 1 \mod n$ en omdat $d|n$, moet dus ook gelden dat $\pi(k) \equiv k + 1 \mod d$. Dus als $k \equiv l \mod d$, dan is $\pi(k) \equiv k + 1 \equiv l + 1 \equiv \pi(l) \mod d$. Ook π behoudt dus gongruentie modulo d.

Als $d > 1$, dan weten we zeker dat er een permutatie in S_n bestaat die geen congruentie modulo d behoudt. Neem bijvoorbeeld (12). We zien dat $(12)1 \equiv 2 \mod d$, maar $(12)(d+1) \equiv 1 \mod d$, terwijl $d + 1 \equiv 1 \mod d$. We weten verder dat de permutatie $(a_1 a_2)$ in S_n zit, maar deze permutatie kan niet worden gemaakt met ρ en σ als $d > 1$ omdat deze twee permutaties congruenties modulo d in de subscripten van de a_k's bewaren, terwijl $(a_1 a_2)$ de subscripten permuteert volgens (12), wat geen congruentie modulo d behoudt. Hieruit volgt dat $d = 1$.

Neem nu aan $d = 1$. Uit $\sigma^m(a_i) = a_j$ kunnen we opmaken dat $\pi^m(i) = j$. Aangezien $\text{ggd}(m,n) = 1$, is de groep gegenereerd door π gelijk is aan de groep gegenereerd door π^m. De groep die gegenereerd wordt door τ en π is dus gelijk aan de groep die gegenereerd wordt door τ en π^m, een transpositie die i en j verwisselt, en een n-cykel die i naar j stuurt. We kunnen dit schrijven als $\langle (ij), (ij\cdots) \rangle$. Deze groep is geconjugeerd aan de groep $\langle (12), (12\cdots n) \rangle$ ([1] pagina 217), die volgens stelling 3.2.4 gelijk is aan S_n. Elke geconjugeerde van S_n is zelf ook S_n, de groep gegenereerd door τ en π is dus gelijk aan S_n. Als de groep gegenereerd door τ en π gelijk is aan S_n, dan moet de groep gegenereerd door ρ en σ gelijk zijn aan de groep die alle permutaties met betrekking tot de subscripten van de a_k's bevat, en dit moet ook S_n zijn. □

Stelling 3.2.7. *De symmetrische groep wordt gegenereerd door elke combinatie van een transpositie, een n-cykel en een $(n-1)$-cykel.* ■

Bewijs. Zei $\rho = (ab)$ een transpositie, σ een n-cykel en τ een $(n-1)$-cykel. Laat m het kleinste getal zijn zodat $\sigma^m(a) = b$.

Geval 1: $\text{ggd}(m,n) = 1$. In dit geval wordt S_n volgens lemma 3.2.6 gegenereerd door ρ en σ.

Geval 2: $\text{ggd}(m,n) = d > 1$. In dit geval moeten we kijken of we, door ρ, σ en τ te combineren, een combinatie van een transpositie en een n-cykel kunnen creëren die wel voldoet. Neem aan dat $\sigma = (a_1 a_2 \cdots a_n)$ zo dat $a = a_i$ en $b = a_j$ voor $i < j$ zoals in het bewijs van 3.2.6. Dan hebben we dus weer dat $j - i = m$. We weten niet wat τ doet, maar we weten dat hij één element, zeg a_n, op zijn plaats laat. We kunnen voor elk getal a_k, een nieuwe $(n-1)$-cykel maken die a_k op zijn plek laat. Beschouw $\pi_k := \sigma^k \tau \sigma^{-k}$, de geconjugeerde van een $(n-1)$-cykel. Geconjugeerde permutaties hebben dezelfde cykelstructuur ([2] pagina 75). We hebben dus dat pi_k zelf ook een $(n-1)$-cykel is. Bovendien laat deze permutatie het getal a_k op zijn plek:

$$\begin{aligned} \pi_k(a_k) &= \sigma^k \tau \sigma^{-k}(a_k) \\ &= \sigma^k \tau(a_n) \\ &= \sigma^k(a_n) \\ &= a_k. \end{aligned}$$

Er is een $l \in \mathbb{N}$ zodat $\pi_i^l(a_{i+1}) = a_j$. Beschouw nu de permutatie $\pi := \pi_i^l \sigma \pi_i^{-l}$, dit is de geconjugeerde van

een n-cykel en zelf dus ook een n-cykel, zo dat

$$\begin{aligned}\pi(a_i) &= \pi_i^l \sigma \pi_i^{-l}(a_i) \\ &= \pi_i^l \sigma(a_i) \\ &= \pi_i^l(a_{i+1}) \\ &= a_j\end{aligned}$$

We weten dat $\text{ggd}(m', n) = 1$ als m' het kleinste getal is zodat $\pi^{m'}(a) = b$, want $m' = 1$. Uit lemma 3.2.6 volgt nu dat S_n gegenereerd wordt door ρ en π, en dus door ρ, σ en τ. □

Bewijs van stelling 3.1.1. Zij f zoals in de stelling. Als f op de drie manieren die in de stelling worden genoemd, ontbindt, dan volgt uit stelling 3.1.2 dat $\text{Gal}(f/\mathbb{Q})$ een n-cykel, een $(n-1)$-cykel en een product van een transpositie en één of twee disjuncte cykels van oneven graad die disjunct zijn met de transpositie. Uit lemma 3.2.1 volgt dat $\text{Gal}(f/\mathbb{Q})$ een transpositie bevat. Uit stelling 3.2.7 volgt dat $\text{Gal}(f/\mathbb{Q}) = S_n$. □

Hoofdstuk 4

Van der Waerden

Nu we stelling 3.1.1 hebben bewezen, gaan we deze gebruiken bij het oplossen van stelling 0.0.1. Dit hoofdstuk zal de zelfde bewijswijze gebruiken als het artikel van van der Waerden [6].

4.1 Van der Waerden polynomen

Eerst stellen we voor ons gemak een definitie op.

Definitie 4.1.1. Van der Waerden noemde n-degraads polynomen die op de drie manieren uit stelling 3.1.1 factoriseren **polynomen van type 1, 2 en 3** respectievelijk.

Als een polynoom type 1 is modulo p_1, type 2 is modulo p_2 en type 3 is modulo p_3 voor drie verschillende priemgetallen p_1, p_2 en p_3, dan noem ik zo'n polynoom een **van der Waerden polynoom**. ■

Dat brengt ons op de volgende stelling.

Stelling 4.1.2. *Als N stijgt, convergeert de verhouding tussen het aantal van der Waerden polynomen in Box_N en het totaal aantal polynomen in Box_N naar 1, oftewel:*

$$\lim_{N\to\infty} \frac{|\{f \in \mathrm{Box}_N \,|f \text{ is van der Waerden}\}|}{|\mathrm{Box}_N|} = 1.$$

■

Stellingen 3.1.1 en 4.1.2 impliceren stelling 0.0.1, die ik hier nog een keer herhaal.

Stelling 0.0.1. *Beschouw voor $N \in \mathbb{N}$ de verzameling Box_N van polynomen met gehele coëfficienten*

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad met \quad -|N| \leq a_0, a_1, \cdots, a_n \leq |N|.$$

De verhouding tussen het aantal polynomen in Box_N met maximale Galoisgroep en het totaal aantal polynomen in Box_N convergeert naar 1 als N stijgt, oftewel

$$\lim_{N\to\infty} \frac{|\{f \in \mathrm{Box}_N \,|\, \mathrm{Gal}\,(f/\mathbb{Q}) \simeq S_n\}|}{|\mathrm{Box}_N|} = 1.$$

□

Het bewijs van stelling 4.1.2 bestaat uit meerdere delen. We gaan eerst afschatten hoeveel verschillende irreducibele polynomen van graad m er zijn modulo een priemgetal p. Voor elk van de drie types polynomen, gebruiken we dit om daarna af te schatten hoeveel mogelijkheden modulo p er zijn voor de factoren waarin de polynomen van dat type ontbinden en dus ook hoeveel mogelijkheden er zijn voor polynomen van type 1, 2 en 3 modulo p.

Daarna gaan we voor een groter wordende rij priemgetallen, afschatten hoeveel polynomen modulo hun product P *niet* van types 1, 2 of 3 zijn modulo welk van deze priemgetal dan ook. Nog minder dan dat aantal, is het aantal niet-van-der-Waerden polynomen modulo P. Laten we P groeien met N, dan wordt de afschatting van de niet-van-der-Waerden polynomen kleiner.

4.2 Lemma's

Lemma 4.2.1. *Zij $m \in \mathbb{N}$ en p een priemgetal. Het aantal verschillende irreducibele polynomen*

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

van graad m modulo p is groter dan $\frac{p^{m+1}}{3m}$. ■

Bewijs. Dit zijn allemaal polynomen over $\mathbb{F}_p$, we willen weten wat hun splijtlichamen zijn. Het bepalen van de splijtlichamen gaat op dezelfde manier als bij het begin van het bewijs van stelling 3.1.2. Stel dat $\mathbb{F}_{p^k}$ het splijtlichaam van zo'n polynoom f is. Dan weten we van stelling 1.2.2 dat $f | x^{p^k} - x$. Vanwege deel 3 van stelling 1.2.3, moet $n|k$. Het splijtlichaam moet dus het kleinste lichaam $\mathbb{F}_{p^k}$ zijn zodat $n|k$. Dit moet $\mathbb{F}_{p^m}$ zijn.

Alle wortels van deze polynomen zitten dus in $\mathbb{F}_{p^m}$. Sterker nog, alle elementen van $\mathbb{F}_{p^m}$ zijn wortels van zulke polynomen, behalve de elementen die in strikte deellichamen ($\mathbb{F}_{p^d}$ voor een $d|m$) van $\mathbb{F}_{p^m}$ zitten. Dat zijn namelijk wortels van lageregraads polynomen, dus worden m-degraads polynomen waarvan het wortels zijn, gedeeld door lageregraads polynomen en kunnen ze dus niet irreducibel zijn.

Het aantal zulke wortels is dus gelijk aan $\left| \mathbb{F}_{p^m} \setminus \bigcup_{d \neq m, d|m} \mathbb{F}_{p^d} \right|$. Nu kunnen we het aantal wortels afschatten:

$$\left| \mathbb{F}_{p^m} \setminus \bigcup_{d|m} \mathbb{F}_{p^d} \right| \geq p^m - \sum_{d \neq m, d|m} p^d \geq p^m - \sum_{d=1}^{m-1} p^d = p^m - \frac{p^m - p}{p-1} \geq p^m - \frac{p^m}{p-1} = \frac{p^m (p-2)}{p-1}.$$

Elk element $\alpha \in \mathbb{F}_{p^m}$ dat een wortel is van zo'n polynoom f, is gelijk ook de wortel van $p-1$ polynomen, omdat het ook de wortel is van $2f, 3f, \cdots, (p-1) f$. We hadden al gezien dat elk polynoom precies m wortels heeft. Met die informatie kunnen we zeggen dat het aantal zulke polynomen groter is dan

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

Omdat we zelf mogen kiezen naar welke p we kijken, mogen we zeggen dat $p \geq 3$, dus $1 - \frac{2}{p} \geq \frac{1}{3}$. Nu is het aantal zulke polynomen dus groter dan $\frac{p^{m+1}}{3m}$. □

Lemma 4.2.2. *Er is een $k \in \mathbb{Z}_+$, onafhankelijk van p, zodat meer dan $\frac{1}{k}$ van alle n-degraads polynomen $f \in \mathbb{Z}[x]$ van type 1, 2 of 3 modulo p zijn.* ■

Bewijs. Polynomen van type 1 ontbinden als een lineaire factor en een factor van graad $n-1$. We weten dat er precies p lineaire polynomen bestaan in $\mathbb{F}_p$. Om het aantal mogelijkheden te vinden voor de factor van graad $n-1$, gebruiken we het resultaat van lemma 4.2.1. We krijgen dat het aantal polynomen van graad

$n-1$ groter is dan $\frac{p^n}{3(n-1)}$. Het aantal verschillende polynomen van type 1 modulo p kunnen we afschatten door deze twee getallen met elkaar te vermenigvuldigen, het aantal polynomen van type 1 modulo p is dus groter dan $\frac{p^{n+1}}{3(n-1)}$. Het totaal aantal verschillende polynomen van graad n modulo p, is p^{n+1}, dus meer dan een fractie van $\frac{1}{3(n-1)}$ van al deze polynomen is van type 1.

Polynomen van type 2 ontbinden als een kwadratische factor en één of twee factoren van oneven graad. We gebruiken weer het resultaat van lemma 4.2.1 om het aantal mogelijkheden voor deze factoren te vinden. Er zijn meer dan $\frac{p^3}{6}$ van zulke polynomen modulo p. Als n oneven is, komt er nog één factor van oneven graad bij, deze factor heeft dan graad $n-2$. Er zijn meer dan $\frac{p^{n-1}}{3(n-2)}$ van zulke polynomen modulo p. Als n oneven is, zijn er dus meer dan $\frac{p^{n+2}}{18(n-2)}$ polynomen modulo p van type 2. Dat is dus meer dan een fractie van $\frac{1}{18(n-2)}$ van alle polynomen modulo p.

Als n even is, komen er nog twee factoren van oneven graad bij. Neem aan dat f te ontbinden is in een irreducibele kwadratische factor, een irreducibele factor van graad $2a+1$ en een irreducibele factor van graad $n-2a-3$. Dan zijn er meer dan $\frac{p^{2a+2}}{3(2a+1)}$ irreducibele polynomen modulo p van graad $2a+1$ en meer dan $\frac{p^{n-2a-2}}{3(n-2a-3)}$ irreducibele polynomen modulo p van graad $n-2a-3$. In totaal zijn er dus meer dan $\frac{p^3}{6} \cdot \frac{p^{2a+2}}{3(2a+1)} \cdot \frac{p^{n-2a-2}}{3(n-2a-3)} = \frac{p^{n+3}}{54(2a+1)(n-2a-3)}$ polynomen van type 2 modulo p, dus meer dan een fractie van $\frac{1}{54(2a+1)(n-2a-3)}$ van al deze polynomen is van type 2. Er zijn verschillende getallen te kiezen voor a, als we 1 kiezen, krijgen we $\frac{1}{162(n-5)}$. Aangezien er meer keuzes voor a zijn, is de fractie van het aantal n-degraads polynomen van type 2 modulo p, gegeven dat n oneven is, dus zeker groter dan alleen $\frac{1}{162(n-5)}$.

Polynomen van type 3 zijn irreducibele polynomen van graad n. Het aantal vinden we op dezelfde manier door n in te vullen voor m in onze afschatting uit lemma 4.2.1. Er zijn meer dan $\frac{p^{n+1}}{3n}$ polynomen van type 3 modulo p, dat is dus meer dan een fractie van $\frac{1}{3n}$ van alle polynomen modulo p.

Deze fracties, $\frac{1}{3(n-1)}$, $\frac{1}{18(n-2)}$, $\frac{1}{162(n-5)}$ en $\frac{1}{3n}$, zijn allemaal onafhankelijk van p. Kies nu $k \in \mathbb{Z}_+$ zó dat $\frac{1}{k}$ kleiner is dan de kleinste van deze breuken. Dan is voor elk priemgetal p, meer dan een fractie van $\frac{1}{k}$ van de polynomen modulo p van type 1, 2 of 3 modulo p. Aangezien elk n-degraads polynoom $f \in \mathbb{Z}[x]$ te vertalen is naar een polynoom modulo p voor elk priemgetal p, is voor elk priemgetal p een fractie van $\frac{1}{k}$ van alle polynomen $f \in \mathbb{Z}[x]$ van type 1, 2 of 3 modulo p. □

4.3 Het bewijs van stelling 4.1.2

Bewijs. Definieer $p_1, p_2, \cdots$ als de rij van oneven priemgetallen en definieer $P := p_1 p_2 p_3 \cdots p_m$. We willen weten hoeveel polynomen modulo P *niet* van één van de drie types is modulo elk priemgetal dat P deelt. We doen dit eerst alleen voor type 1. Voor elke $i \in \{1, 2, \cdots, m\}$ zijn er p_i^n restklassen van polynomen modulo p_i waarvan er volgens lemma 4.2.2 minder dan $\frac{k-1}{k} p_i^n$ niet van type 1 modulo p_i zijn. Restklassen van polynomen modulo P krijg je door voor elk priemgetal p_i dat P deelt een restklasse van polynomen modulo p_i te kiezen en dan de doorsnede te nemen van al deze gekozen restklassen. Er zijn dus P^n verschillende restklassen van polynomen modulo P en daarvan zijn er minder dan $\left(\frac{k-1}{k}\right)^m P^n$ niet van type 1 modulo welk priemgetal p_i dat P deelt dan ook.

Voor elke $\epsilon > 0$ is er een m zodat $\left(\frac{k-1}{k}\right)^m < \epsilon$. Op die manier kunnen we voor elke ϵ een P kiezen zodat minder dan ϵP^n polynomen modulo P van type 1 zijn. Precies hetzelfde kunnen doen voor types 2 en 3. Op die manier zien we dat maximaal $3\epsilon P^n$ polynomen modulo P niet van types 1, 2 of 3 zijn modulo welk priemgetal p_i dat P deelt dan ook. Het aantal polynomen modulo P dat geen van der Waerden polynomen zijn is dus ook kleiner dan $3\epsilon P^n$.

Nu kiezen we onze N, zodanig dat $2N+1 \geq P$. Elke restklasse van gehele getallen modulo P, bevat maximaal $\frac{2N+1}{P} + 1$ gehele getallen z die tussen $-N$ en N liggen. Een bepaalde restklasse van n-degraads polynomen

modulo P bevat dus maximaal $\left(\frac{2N+1}{P}+1\right)^n$ polynomen in Box_N. Er zijn minder dan $3\epsilon P^n$ restklassen van niet-van-der-Waerden polynomen modulo P, dus zijn er minder dan

$$3\epsilon P^n \left(\frac{2N+1}{P}+1\right)^n = 3\epsilon \left(2N+1+P\right)^n \leq 3\epsilon 2^n \left(2N+1\right)^n$$

polynomen in Box_N niet van der Waerden. Meer dan $\left(1-3\cdot 2^n\epsilon\right)\left(2N+1\right)^n$ polynomen in Box_N zijn dus van der Waerden.

Als we N groter kiezen, kunnen we P ook groter kiezen en kunnen we ϵ kleiner kiezen. We kiezen nu voor elke N de kleinst mogelijke ϵ_N. Als N stijgt, dan daalt ϵ_N en convergeert $\left(1-3\cdot 2^n\epsilon\right)$ naar 1. Het aantal van der Waerden polynomen in Box_N convergeert dan naar $\left(2N+1\right)^n$, het totaal aantal polynomen in Box_N. Dus

$$\lim_{N\to\infty} \frac{\left|\{f \in \text{Box}_N \,|\, f \text{ is van der Waerden}\}\right|}{\left|\text{Box}_N\right|} = 1.$$

□

Omdat deze van der Waerden polynomen allemaal maximale Galoisgroep hebben, komen we tot de conclusie van deze scriptie.

Bewijs van stelling 0.0.1. De verhouding tussen het totaal aantal polynomen in Box_N en het aantal der Waerden polynomen in Box_N convergeert naar 1 als N stijgt. Deze polynomen hebben allemaal maximale Galoisgroep. De verhouding tussen het aantal polynomen in Box_N en het aantal polynomen met maximale Galoisgroep in Box_N convergeert dus ook naar 1 als N stijgt. □

Hoofdstuk 5

Conclusie en verder onderzoek

In deze scriptie heb ik verschillende onderwerpen binnen de Galoistheorie behandeld, en hebben we onder anderen gezien dat asymptotisch gezien, 100% van alle polynomen $f \in \mathbb{Z}[x]$ maximale Galoisgroep hebben.

Het onderzoek naar dit gebied gaat nog verder, er is ook nog veel onderzoek gedaan naar hoe groot de kans precies is dat een polynoom in Box_N een maximale Galoisgroep heeft. In 1936 kwam van der Waerden nogmaals met een artikel over het onderwerp genaamd "Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt" [7]. Daarin schatte hij de kans dat een polynoom $f \in \text{Box}_N$ geen maximale Galoisgroep af op $< N^{-\frac{1}{k\log(\log(N))}}$. De meest recente ontwikkeling is gedaan door Igor Rivin, die bewees in 2015[5] dat de Galoisgroep van een monisch polynoom van graad $n > 12$ in Box_N niet maximaal is met een kans $\ll \frac{\log^{f(n)} N}{N}$ voor een berekenbare functie f.

Bibliografie

[1] Paolo Aluffi, *Algebra: Chapter 0*, Graduate Studies in Mathematics, vol. 104, American Mathematical Society, Providence, RI, 2009. MR 2527940

[2] M.A. Armstrong, G. Iooss, and D.D. Joseph, *Groups and symmetry*, Springer Undergraduate Texts in Mathematics and Technology, Springer, 1988.

[3] Keith Conrad, *Generating sets*.

[4] Cox David, *Galois theory*, Pure and Applied Mathematics: A Wiley-Interscience Series of Texts, Monographs, and Tracts, Wiley, 2004.

[5] I. Rivin, *Galois groups of generic polynomials*, ArXiv e-prints (2015).

[6] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Mathematische Annalen **109** (1934), no. 1, 13–16.

[7] ———, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatshefte für Mathematik und Physik **43** (1936), no. 1, 133–147.