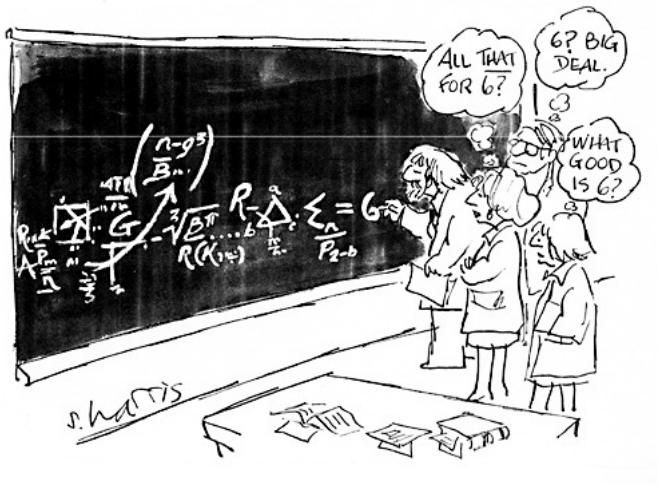
Inhoudsopgave



Hoofdstuk 1

Nilpotente en oplosbare groepen

In de cursus "Algebra I" hebben we reeds een stevige basis aan groepentheorie opgedaan. Deze basis wordt nu verder uitgebreid, en vooreerst bestuderen we de belangrijke begrippen van nilpotentie en oplosbaarheid van groepen.

We spreken af dat in deze cursus 0 een natuurlijk getal is; we gebruiken dan ook de notatie

$$\mathbb{N} := \mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}.$$

1.1 Groepen bouwen

Vooraleer we ingaan op nilpotentie en oplosbaarheid, staan we stil bij het probleem over hoe we groepen kunnen opbouwen uit kleinere groepen. Concreet vragen we ons af hoe we, gegeven twee groepen N en H, een nieuwe groep G kunnen maken die N als normaaldeler heeft, en zodanig dat $G/N \cong H$. Uiteraard kunnen we het direct product van groepen beschouwen, maar we willen graag alle mogelijke dergelijke groepen beschrijven. Dit is het zogenaamde *extensieprobleem*.

Definitie 1.1.1. Zij G een groep, en $H \leq G$ een deelgroep. Een *complement* voor H in G is een deelgroep $K \leq G$ zodat $G = HK$ en $H \cap K = 1$. We zeggen dan ook dat H en K *complementaire deelgroepen* zijn. Niet elke deelgroep heeft een complement, en als een deelgroep een complement heeft, is dat niet noodzakelijk uniek.

Definitie 1.1.2. Beschouw twee willekeurige groepen N en H.

(i) Een groep G die een normaaldeler M bevat zodat $M \cong N$ en $G/M \cong H$, wordt een *extensie van H door N* genoemd. (Sommige auteurs noemen dit een extensie van N door H — opgelet dus bij het raadplegen van andere werken!)

(ii) Een extensie G van H door N is *gespleten* als M een complement K heeft in G. In dat geval geldt dan steeds dat

$$K = K/(K \cap M) \cong KM/M = G/M \cong H.$$

Merk op dat M een *normaal* complement $K \trianglelefteq G$ heeft als en slechts als G het direct product is van M en K. Bij een algemene gespleten extensie hebben we enkel $K \leq G$, maar doordat $M \trianglelefteq G$ hebben we wel een werking van K op M gegeven door toevoeging in G.

Als we nu omgekeerd vertrekkend van N en H alle mogelijke gespleten extensies willen construeren, zullen we moeten weergeven hoe deze werking van $K \cong H$ op $M \cong N$ er uit ziet. Aangezien er (nog) geen overkoepelende groep G is, kunnen we die niet beschrijven met inwendige automorfismen, maar wel met automorfismen.

Definitie 1.1.3. Beschouw twee willekeurige groepen N en H. Een actie van H op de verzameling N is een *actie via automorfismen* als voor elke $h \in H$ geldt dat de permutatie van N geïnduceerd door h een automorfisme van N is, i.e. als

$$(xy)^h = x^h y^h \quad \text{voor alle } x, y \in N,$$

voor alle $h \in H$. In de notatie van de cursus "Algebra I" kunnen we dit ook nog uitdrukken als het feit dat de permutatie $\alpha_h \in \mathrm{Sym}(N)$ tot $\mathrm{Aut}(N)$ behoort. De corresponderende permutatierepresentatie is dus in dit geval een morfisme $\alpha\colon H \to \mathrm{Aut}(N)$.

Met behulp van dergelijke data kunnen we nu alle gespleten extensies beschrijven.

Stelling 1.1.4. *Beschouw twee willekeurige groepen N en H, en een actie van H op N via automorfismen. Dan is er een unieke groep G met een deelgroep $\overline{H}$ en een normaaldeler $\overline{N}$, met $\overline{N} \cong N$ en $\overline{H} \cong H$, zodat*

(a) $G = \overline{H}\,\overline{N}$;

(b) $\overline{H} \cap \overline{N} = 1$;

(c) $(\overline{n})^{\overline{h}} = \overline{n^h}$ *voor alle $n \in N$ en alle $h \in H$.*

Hierbij hebben we in (c) de isomorfismen $N \to \overline{N}$ en $H \to \overline{H}$ genoteerd met respectievelijk $n \mapsto \overline{n}$ en $h \mapsto \overline{h}$. Merk op dat het linkerlid en het rechterlid in (c) a priori een verschillende betekenis hebben: $(\overline{n})^{\overline{h}}$ is gewoon toevoeging in de groep G, terwijl n^h het beeld van n is onder de gegeven actie van H op N. Het punt is dus net dat we door deze constructie van de (willekeurige) automorfismen $\alpha_h \in \mathrm{Aut}(N)$ *inwendige* automorfismen in G hebben gemaakt.

Bewijs. We definiëren de groep G als de verzameling van koppels

$$G = \{(h, n) \mid h \in H, n \in N\},$$

met groepsbewerking

$$(h,n)\cdot(k,m) := (hk, n^k m) \tag{1.1}$$

voor alle $h,k \in H$ en $n,m \in N$, waarbij n^k het beeld van de gegeven actie van $k \in H$ op $n \in N$ voorstelt. Men gaat eenvoudig na dat deze bewerking associatief is, neutraal element $(1,1)$ heeft, en inverse

$$(h,n)^{-1} = \left(h^{-1}, n^{-h^{-1}}\right)$$

bezit, en bijgevolg een groep is.

Duidelijkerwijze is

$$\begin{aligned} \overline{N} &:= \{(1,n) \in G\} \trianglelefteq G, \qquad & \overline{N} &\cong N, \\ \overline{H} &:= \{(h,1) \in G\} \leq G, \qquad & \overline{H} &\cong H. \end{aligned}$$

Het is nu evident dat $\overline{N}$ en $\overline{H}$ voldoen aan (a) en (b). We gaan nu (c) na door middel van een eenvoudige berekening. Voor alle $n \in N$ en alle $h \in H$ geldt

$$(\overline{n})^{\overline{h}} = (1,n)^{(h,1)} = (h^{-1},1)\cdot(1,n)\cdot(h,1) = (1,n^h) = \overline{n^h},$$

wat aantoont dat G aan alle gewenste eigenschappen voldoet.

De uniciteit is ook duidelijk: als G' een andere groep is met deelgroepen $\widetilde{H}$ en $\widetilde{N}$ met de gewenste eigenschappen (a), (b) en (c), dan volgt uit (a) en (b) dat elk element van G' uniek te schrijven is als product van een element uit $\widetilde{H}$ met een element uit $\widetilde{N}$. De vermenigvuldiging van twee willekeurige elementen in G' wordt dan gegeven door de regel in (c), en we krijgen precies

$$\widetilde{h}\widetilde{n}\cdot\widetilde{k}\widetilde{m} = \widetilde{h}\,\widetilde{k}\cdot\widetilde{k}^{-1}\widetilde{n}\widetilde{k}\cdot\widetilde{m} = \widetilde{hk}\cdot\widetilde{n^k}\cdot\widetilde{m} = \widetilde{hk}\cdot\widetilde{n^k m},$$

en we vinden formule (1.1) terug, wat bewijst dat $G' \cong G$. □

Definitie 1.1.5. (i) Beschouw twee willekeurige groepen N en H, en een actie van H op N via automorfismen. De groep G die we geconstrueerd hebben in Stelling 1.1.4 wordt het *(uitwendig) semidirect product* van N en H genoemd (met betrekking tot de gegeven actie). We noteren dit als $G = N \rtimes H$ of als $G = N : H$. (We zullen dus in het vervolg de streep in $\overline{N}$ en $\overline{H}$ weglaten.)

Als we de actie expliciet willen vermelden in de notatie, kunnen we dit doen door het corresponderend morfisme $\alpha\colon H \to \mathrm{Aut}(N)$ expliciet weer te geven, en we schrijven dan $G = N \rtimes_\alpha H$.

(ii) Veronderstel dat G een groep is met gegeven deelgroep $H \leq G$ en normaaldeler $N \trianglelefteq G$. Dan is G het *(inwendig) semidirect product* van N en H, als $G = NH$ en $N \cap H = 1$, met andere woorden, als N en H complementaire deelgroepen zijn.

Opmerking 1.1.6. (i) Als G het uitwendig semidirect product is van twee groepen N en H met betrekking tot een zekere actie van H op N, stel $G = N \rtimes_\alpha H$, dan is G het inwendig semidirect product van de corresponderende deelgroepen $N \leq G$ en $H \leq G$.
Omgekeerd, als G een inwendig semidirect product is van twee deelgroepen $N \leq G$ en $H \leq G$, dan is G isomorf met het uitwendig semidirect product van N en H met betrekking tot de actie van H op N gegeven door toevoeging in G.

(ii) Stelling 1.1.4 zegt dus dat een extensie G van H door N gespleten is als en slechts als G een semidirect product is van N en H.

Voorbeelden 1.1.7. (1) Beschouw twee willekeurige groepen N en H. Dan is het direct product $N \times H$ een semidirect product, waarbij de actie van H op N triviaal is, i.e. $n^h = n$ voor alle $n \in N$ en $h \in H$. Met andere woorden,

$$N \times H \cong N \rtimes_{\mathrm{id}} H.$$

Dit blijkt bijvoorbeeld uit formule (1.1).

(2) Beschouw $N = \mathbf{C}_n$ en $H = \mathbf{C}_2 = \{1, z\}$, waarbij de actie van H op N gegeven is door

$$g^z = g^{-1}$$

voor alle $g \in N$. (Bemerk dat dit een automorfisme van N is omdat N abels is.) Dan is $N \rtimes H \cong \mathbf{D}_{2n}$.
Merk op dat in $\mathbf{D}_{2n}$ de groep N precies de groep van de rotaties is, terwijl H een groep is voortgebracht door één willekeurige puntspiegeling. Dit is dus een voorbeeld waarin het complement H van N duidelijk niet uniek is.

(3) Zij $n \in \mathbb{N}$, $n \geq 2$. Beschouw $G = \mathbf{S}_n$, $N = \mathbf{A}_n$, en $H = \{\mathrm{id}, (1\ 2)\} \cong \mathbf{C}_2$, zodat $N \trianglelefteq G$ en $H \leq G$. Dan is $G = N \rtimes H$.

(4) De groep $G = \mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ kan niet geschreven worden als het semidirect product van twee echte deelgroepen. Inderdaad, elke niet-triviale deelgroep van G bevat het centrum $Z(G) = \{\pm 1\}$, zodat de voorwaarde $N \cap H = 1$ nooit voldaan kan zijn.

(5) Zij G een willekeurige groep, en beschouw de werking van G op zichzelf door toevoeging. Met betrekking tot deze actie is $G \rtimes G \cong G \times G$. (Ga dit zelf na als oefening.)

(6) Zij G een willekeurige groep. Dan werkt $\mathrm{Aut}(G)$ op natuurlijke wijze op G via automorfismen, en dus kunnen we het semidirect product $A := G \rtimes \mathrm{Aut}(G)$ beschouwen. In deze groep is dus elk automorfisme van G een inwendig automorfisme geworden (wat natuurlijk nog niet wil zeggen dat elk automorfisme van A inwendig is). Deze groep A wordt de *holomorf* van G genoemd, en wordt genoteerd als $A = \mathrm{Hol}(G)$.

(7) Zij A een willekeurige groep, en H een eindige permutatiegroep, i.e. $H \leq \mathrm{Sym}(d)$ voor een zekere $d \in \mathbb{N}$, $d \geq 1$. Beschouw dan de groep $N = A^d := A \times \cdots \times A$ (d keer), en de actie van H op N gegeven door het permuteren van de d kopieën van A, i.e.

$$(a_1, \ldots, a_d)^\sigma = \left(a_{\sigma(1)}, \ldots, a_{\sigma(d)}\right)$$

voor alle $a_1, \ldots, a_d \in A$ en alle $\sigma \in H$. Het semidirect product $N \rtimes H$ met betrekking tot deze actie wordt het *kransproduct*[1] van A en H genoemd, en wordt genoteerd als $G = A \,\mathrm{wr}\, H = A \wr H$.

Opmerking 1.1.8. Stelling 1.1.4 construeert enkel de *gespleten* extensies van H door N. Het bepalen van alle mogelijke extensies is een veel moeilijker probleem, dat geen eenvoudig antwoord heeft. Vermeldenswaardig in deze context is het feit dat de verzameling van alle *centrale* extensies van een groep H door een (noodzakelijkerwijze abelse) groep N, i.e. de extensies G zodat $N \leq Z(G)$, in bijectief verband staat met $H^2(H, N)$, de tweede cohomologiegroep van H met coëfficiënten in N met triviale actie van H op N.

Het belang van het extensieprobleem blijkt zeer sterk als we de structuur van willekeurige groepen willen onderzoeken. Het is natuurlijk om een groep "op te delen" in kleinere stukken, die we hopelijk beter begrijpen. Een dergelijke opdeling kunnen we verkrijgen door een normaaldeler N van de groep G te beschouwen, en vervolgens de studie van G te herleiden tot die van N en G/N. De vraag rijst dan in welke mate de structuur en eigenschappen van G bepaald zijn door die van N en G/N, en dit is precies waar het extensieprobleem opduikt.

Het is zinvol om deze opdeling zo fijn mogelijk te doen. Dit kunnen we verkrijgen door een *maximale* normaaldeler N van G te beschouwen.

Definitie 1.1.9. Zij G een groep.

(i) Een deelgroep $M \leq G$ is een *maximale deelgroep* als $M < G$, en als er geen deelgroep $H \leq G$ bestaat met $M < H < G$.

[1] In het Engels: *wreath product*.

(ii) Een normaaldeler $N \trianglelefteq G$ is een *maximale normaaldeler* als $N < G$, en als er geen normaaldeler $H \trianglelefteq G$ bestaat met $N < H < G$.

Als N een maximale normaaldeler is, dan weten we immers uit de correspondentiestelling (zie Gevolg 1.2.3 verderop) dat G/N enkelvoudig is. Als we dit proces nu herhalen op N en zo verder gaan, hebben we onze groep "opgedeeld" in allemaal enkelvoudige groepen. Dit is één van de sterke motivaties waarom enkelvoudige groepen van zo groot belang zijn in de groepentheorie; we gaan hier in Hoofdstuk 2 verder op in.

We geven een formele definitie van zo'n "opdeling".

Definitie 1.1.10. Zij G een willekeurige groep. Een rij van deelgroepen[2]

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

wordt een *compositierij* genoemd als elke G_i een maximale normaaldeler is in G_{i+1} (voor alle $0 \leq i \leq n-1$), of equivalent, als elk quotiënt G_{i+1}/G_i een enkelvoudige groep is. Deze enkelvoudige factoren G_{i+1}/G_i worden de *compositiefactoren* van de compositierij genoemd.

We geven de volgende belangrijke stelling mee zonder bewijs.

Stelling 1.1.11 (Jordan–Hölder)**.** *Zij G een willekeurige groep, en veronderstel dat G twee verschillende compositierijen*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G,$$
$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{m-1} \trianglelefteq H_m = G$$

heeft. Dan is $m = n$, en de compositiefactoren van beide rijen zijn, op een permutatie na, isomorf aan elkaar.

Zonder bewijs. □

Opmerking 1.1.12. De compositierijen zelf zijn dus *niet uniek*! Beschouw, bij wijze van eenvoudig voorbeeld, de groep $G = \mathbf{C}_6$. Dan heeft G twee verschillende compositierijen

$$1 \trianglelefteq \mathbf{C}_2 \trianglelefteq G,$$
$$1 \trianglelefteq \mathbf{C}_3 \trianglelefteq G.$$

Echter, beide rijen hebben dezelfde lijst van compositiefactoren, nl. $\{\mathbf{C}_2, \mathbf{C}_3\}$.

[2]Merk op dat de G_i in het algemeen *geen* normaaldelers van G zijn, want een normaaldeler van een normaaldeler is niet noodzakelijk een normaaldeler. Het zijn zogenaamde *subnormaaldelers*.

Opmerking 1.1.13. Het is duidelijk dat elke *eindige* groep een compositierij heeft. Inderdaad, we kunnen in elke stap een maximale normaaldeler nemen, en omdat de groep eindig is, zal dit proces eindigen. Het is echter niet zo dat elke oneindige groep een compositierij heeft; het eenvoudigste voorbeeld hiervan is de oneindige cyclische groep $(\mathbb{Z}, +)$, waarvan elke maximale normaaldeler opnieuw isomorf is met $(\mathbb{Z}, +)$ zelf.

1.2 De correspondentiestelling

Daarnet merkten we op dat indien G een groep is met een maximale normaaldeler $N \trianglelefteq G$, dan G/N enkelvoudig is. Dit is een bijzonder geval van de algemenere correspondentiestelling, die een verband geeft tussen deelgroepen van een quotiëntgroep G/N en deelgroepen van G die N bevatten.

We formuleren de stelling eerst in termen van groepsmorfismen; uiteindelijk zal vooral Gevolg 1.2.2 van belang zijn. Merk op dat we Gevolg 1.2.2(i) reeds ontmoet hebben in de cursus "Algebra I".

Stelling 1.2.1 (Correspondentiestelling)**.** *Zij $\theta\colon G \to H$ een surjectief groepsmorfisme, met kern $N = \ker(\theta) \trianglelefteq G$. Definieer*

$$\mathcal{S} := \{U \mid N \leq U \leq G\}$$

en

$$\mathcal{T} := \{V \mid V \leq H\}.$$

Dan induceren θ en θ^{-1} inverse bijecties tussen $\mathcal{S}$ en $\mathcal{T}$. Bovendien bewaren deze bijecties inclusies, indices, normaliteit, en quotiëntgroepen.

Met de laatste zin bedoelen we het volgende: zij $U_1, U_2 \in \mathcal{S}$, en stel $V_1 = U_1^\theta, V_2 = U_2^\theta \in \mathcal{T}$. Dan zal

- $U_1 \leq U_2$ als en slechts als $V_1 \leq V_2$, en in dat geval is $[U_2\colon U_1] = [V_2\colon V_1]$;
- $U_1 \trianglelefteq U_2$ als en slechts als $V_1 \trianglelefteq V_2$, en in dat geval is $U_2/U_1 \cong V_2/V_1$.

Bewijs. Het bewijs is een elementaire maar interessante oefening. □

Deze stelling zal voornamelijk toegepast worden in het geval dat $H = G/N$ en $\theta\colon G \to G/N$ de canonieke projectie is. In het bijzonder geeft deze stelling een beschrijving van de deelgroepen en normaaldelers van een quotiëntgroep:

Gevolg 1.2.2. *Zij G een groep, en $N \trianglelefteq G$ een normaaldeler.*

(i) *Elke deelgroep van G/N is van de vorm H/N voor een (unieke) deelgroep $H \leq G$ die N bevat. Bovendien is $H/N \trianglelefteq G/N$ als en slechts als $H \trianglelefteq G$.*

(ii) *Veronderstel dat $N \leq M \trianglelefteq G$. Dan is $G/M \cong (G/N) \,/\, (M/N)$.*

Bewijs. Pas Stelling 1.2.1 toe op $\theta\colon G \to G/N$. Merk op dat indien $H \leq G$ met $N \leq H$, dan $H^\theta = H/N$. De uitspraak in (ii) is precies de bewering dat θ quotiëntgroepen bewaart. □

Gevolg 1.2.3. *Zij G een groep, en $N \trianglelefteq G$ een maximale normaaldeler. Dan is G/N enkelvoudig.*

Bewijs. Wegens Gevolg 1.2.2 is elke normaaldeler van G/N van de vorm H/N, voor een normaaldeler $H \leq G$ die N bevat. Aangezien N een maximale normaaldeler is, kan dit enkel indien $H = N$ of $H = G$, en bijgevolg $H/N = 1$ of $H/N = G/N$. □

1.3 Nilpotente en oplosbare groepen

We voeren nu de beloofde concepten van nilpotentie en oplosbaarheid in. De items (i)–(iv) in de volgende definitie hebben we reeds eerder ontmoet, maar we vullen die nu verder aan met (v)–(ix).

Definitie 1.3.1. Zij G een willekeurige groep.

(i) Zij $g, h \in G$. De *commutator* van g en h definiëren we als

$$[g, h] := g^{-1}h^{-1}gh\,.$$

(ii) De verzameling van alle commutators

$$S = \{[g, h] \mid g, h \in G\}$$

vormt in het algemeen *geen* deelgroep van G. Daarom definiëren we

$$[G, G] := \langle [g, h] \mid g, h \in G \rangle\,,$$

en we noemen dit de *commutatordeelgroep van G* of de *afgeleide groep van G*. Ook de notaties G', $G^{(1)}$ en $\delta(G)$ worden hiervoor gebruikt. Merk op dat $[G, G] = 1$ als en slechts als G abels is.

(iii) Als $A, B \leq G$ twee deelgroepen zijn, dan definiëren we algemener

$$[A, B] := \langle [a, b] \mid a \in A, b \in B \rangle ,$$

en we noemen dit de *commutator* van A en B. We zeggen dat twee deelgroepen A en B *(met elkaar) commuteren* als $[A, B] = 1$, of dus als elk element van A commuteert met elk element van B. Merk op dat dit *niet* equivalent is met de uitspraak $AB = BA$!

(iv) Het *centrum* van G bestaat uit de elementen van G die met alle elementen van G commuteren:

$$Z(G) := \{g \in G \mid gh = hg \text{ voor alle } h \in G\} .$$

(v) We definiëren inductief de *n-de (normale) afgeleide* van G als

$$G^{(n)} = \delta\big(G^{(n-1)}\big)$$

voor alle $n > 0$, waarbij $G^{(0)} = G$ en dus $G^{(1)} = \delta(G)$. De *afgeleide rij* van G is dan de (mogelijks oneindige) dalende rij van deelgroepen

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

(vi) We definiëren inductief de *n-de centrale afgeleide* van G als

$$G^{[n]} = \big[G, G^{[n-1]}\big]$$

voor alle $n > 0$, waarbij $G^{[0]} = G$ en dus ook $G^{[1]} = G^{(1)}$. De *dalende centrale rij*[3] van G is dan de (mogelijks oneindige) dalende rij van deelgroepen

$$G = G^{[0]} \geq G^{[1]} \geq G^{[2]} \geq \cdots$$

(vii) We definiëren inductief het *n-de centrum* van G als

$$Z_n(G) = \{g \in G \mid [g, h] \in Z_{n-1}(G) \text{ voor alle } h \in G\}$$

voor alle $n > 0$, waarbij $Z_0(G) = 1$ (en dus ook $Z_1(G) = Z(G)$). Anders gezegd, $Z_n(G)$ is de grootst mogelijke deelgroep van G zodat

$$[Z_n(G), G] \leq Z_{n-1}(G).$$

De *stijgende centrale rij*[4] van G is dan de (mogelijks oneindige) stijgende rij van deelgroepen

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

[3] In het Engels spreekt men van de *lower central series*.
[4] In het Engels spreekt men van de *upper central series*.

(viii) De groep G is *oplosbaar* indien $G^{(n)} = 1$ voor een zekere $n \in \mathbb{N}$. In dat geval wordt de kleinste n waarvoor dit geldt, de *oplosbaarheidslengte* van G genoemd. We zeggen ook dat G oplosbaar is *van lengte* n.

(ix) De groep G is *nilpotent* indien $G^{[n]} = 1$ voor een zekere $n \in \mathbb{N}$. In dat geval wordt de kleinste n waarvoor dit geldt, de *nilpotentieklasse* van G genoemd. We zeggen ook dat G nilpotent is *van klasse* n. Merk op dat elke nilpotente groep ook oplosbaar is, omdat $G^{(n)} \leq G^{[n]}$ voor alle n.

Opmerking 1.3.2. (i) Het is niet helemaal triviaal om te bewijzen dat de definitie van het n-de centrum,

$$Z_n(G) = \{g \in G \mid [g, h] \in Z_{n-1}(G) \text{ voor alle } h \in G\},$$

een deelgroep oplevert. Men bewijst dit makkelijkst door per inductie op n te bewijzen dat $Z_n(G)$ een *normaaldeler* is, en gebruik te maken van de identiteit

$$[ab, h] = [a, h]^b[b, h]$$

voor alle $a, b, h \in G$. Werk zelf de details uit als oefening.

(ii) Men kan het *n-de centrum* van G eveneens inductief definiëren als de unieke deelgroep $Z_n(G) \leq G$ zodat

$$Z_n(G)/Z_{n-1}(G) = Z\big(G/Z_{n-1}(G)\big)$$

voor alle $n > 0$, waarbij $Z_0(G) = 1$ (en dus ook $Z_1(G) = Z(G)$). Merk op dat dit inderdaad de groepen $Z_n(G)$ uniek bepaalt omwille van Gevolg 1.2.2(i). Ga zelf na dat deze definitie equivalent is met Definitie 1.3.1(vii).

(iii) De deelgroepen $G^{(n)}$, $G^{[n]}$ en $Z_n(G)$ zijn allemaal karakteristieke deelgroepen van G. Het is immers duidelijk uit hun definitie dat ze invariant zijn onder willekeurige automorfismen van G, omdat elk automorfisme een commutator afbeeldt op een commutator. Zie ook Lemma 1.3.4 verderop.

Voorbeelden 1.3.3. (1) De abelse groepen zijn precies de groepen die oplosbaar zijn van lengte 1, en dit zijn ook precies de groepen die nilpotent zijn van klasse 1.

(2) Beschouw de niet-abelse groep $G = \mathbf{S}_3 \cong \mathbf{D}_6$ van orde 6. Dan is $G' = [G, G] \cong \mathbf{C}_3$, en dus is $G^{(2)} = 1$. Dus G is oplosbaar van lengte 2. Anderzijds is $[G, G'] = G'$, zodat $G^{[1]} = G^{[2]} = \cdots \neq 1$; bijgevolg is G niet nilpotent.

(3) Beschouw de niet-abelse groep $G = \mathbf{A}_4$. Dan is $G' = [G, G]$ gelijk aan

$$G' = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong \mathbf{C}_2 \times \mathbf{C}_2.$$

Bijgevolg is G oplosbaar van lengte 2. Ook hier geldt dat G niet nilpotent is.

(4) Beschouw de niet-abelse groep $G = \mathbf{A}_n$, $n \geq 5$. We zullen later aantonen dat G enkelvoudig is, i.e. G heeft geen echte niet-triviale normaaldelers (zie Stelling 2.1.9). In het bijzonder is G perfect, i.e. $[G, G] = G$. Inderdaad, $[G, G]$ is een normaaldeler van G, die niet-trivaal is omdat G niet abels is, en wegens de enkelvoudigheid van G moet dan $[G, G] = G$. In het bijzonder is G niet oplosbaar (en dus zeker ook niet nilpotent).

(5) Beschouw de niet-abelse groep $G = \mathbf{D}_8 = \{1, \rho, \rho^2, \rho^3, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, waarbij ρ de rotatie over 90° is, en de σ_i de vier orthogonale spiegelingen zijn. Dan is $[G, G] = Z(G) = \{1, \rho^2\}$, en dus is $G^{[2]} = [G, Z(G)] = 1$, zodat G nilpotent van klasse 2 is. Bijgevolg is G ook oplosbaar, van lengte 2. Merk op dat uit $[G, G] = Z(G)$ ook volgt dat $Z_2(G) = G$ (en dus ook $Z_n(G) = G$ voor alle $n \geq 2$).

Lemma 1.3.4. *Zij G, H twee groepen.*

(i) *Zij $\theta\colon G \to H$ een morfisme, en $n \in \mathbb{N}$. Dan is*

$$(G^{(n)})^\theta \leq H^{(n)} \quad \textit{en} \quad (G^{[n]})^\theta \leq H^{[n]}.$$

(ii) *Zij $\theta\colon G \to H$ een epimorfisme, en $n \in \mathbb{N}$. Dan is*

$$(G^{(n)})^\theta = H^{(n)} \quad \textit{en} \quad (G^{[n]})^\theta = H^{[n]}.$$

(iii) *Zij $N \trianglelefteq G$, en $n \in \mathbb{N}$. Dan is*

$$(G/N)^{(n)} = G^{(n)}N/N \quad \textit{en} \quad (G/N)^{[n]} = G^{[n]}N/N.$$

(iv) *Zij $N \trianglelefteq G$. Dan is G/N abels als en slechts als $G' \leq N$.*

Bewijs. We bewijzen eerst (i) en (ii). Voor $n = 0$ zijn deze uitspraken triviaal; we gaan verder met inductie op n. Neem dus aan dat de uitspraken bewezen zijn voor $n - 1$. Merk op dat $[g, h]^\theta = [g^\theta, h^\theta]$ voor alle $g, h \in G$. In het bijzonder geldt enerzijds

$$(G^{(n)})^\theta = [G^{(n-1)}, G^{(n-1)}]^\theta = \big[(G^{(n-1)})^\theta, (G^{(n-1)})^\theta\big],$$

en anderzijds

$$(G^{[n]})^\theta = [G, G^{[n-1]}]^\theta = \big[G^\theta, (G^{[n-1]})^\theta\big],$$

waaruit het gestelde volgt. Merk ten slotte op dat (iii) volgt door (ii) toe te passen op de canonieke projectie $\theta\colon G \to G/N$, en dat (iv) volgt uit (iii) voor $n = 1$. □

Lemma 1.3.5. *Deelgroepen en quotiëntgroepen van een oplosbare groep (van lengte k) zijn oplosbaar (van lengte $\leq k$). Deelgroepen en quotiëntgroepen van een nilpotente groep (van klasse k) zijn nilpotent (van klasse $\leq k$).*

Bewijs. De uitspraken voor deelgroepen volgen onmiddellijk uit het feit dat voor $H \leq G$ geldt dat $H^{(n)} \leq G^{(n)}$ en $H^{[n]} \leq G^{[n]}$ voor alle $n \in \mathbb{N}$. De uitspraken voor quotiëntgroepen volgen uit Lemma 1.3.4(iii). □

Opmerking 1.3.6. Zoals we reeds opmerkten is elke nilpotente groep uiteraard ook oplosbaar. Interessant is dat de lengte van oplosbaarheid sterk begrensd wordt door de nilpotentieklasse. Zo kan men aantonen dat indien G nilpotent is van klasse c, dan G oplosbaar is van lengte d waarbij

$$d < 1 + \log_2(c+1).$$

Als voorbeeld hiervan hebben we dat een groep G die nilpotent is van klasse 3 steeds de eigenschap heeft dat G' abels is (want $G'' = 1$).

Voor *eindige* groepen bestaan er interessante alternatieve karakterisaties voor nilpotentie en oplosbaarheid. De eindige oplosbare groepen zijn precies die met de eenvoudigst mogelijke compositierijen, zoals we straks zullen zien in Gevolg 1.3.10; de eindige nilpotente groepen zijn precies de groepen die het direct product zijn van hun Sylow deelgroepen, zoals we zullen zien in Stelling 1.3.18 verderop.

We beginnen met de oplosbare groepen wat nader te bekijken. Oplosbaarheid gedraagt zich goed met betrekking tot extensies:

Stelling 1.3.7. *Zij G een willekeurige groep met normaaldeler $N \trianglelefteq G$, en veronderstel dat zowel N als G/N oplosbaar zijn, stel van lengte respectievelijk k en ℓ. Dan is ook G oplosbaar, van lengte ten hoogste $k + \ell$.*

Bewijs. Beschouw het canonieke epimorfisme $\pi\colon G \to G/N$. Uit Lemma 1.3.4 weten we dat

$$(G^{(\ell)})^{\pi} = (G/N)^{(\ell)} = 1.$$

Dus $G^{(\ell)} \leq \ker(\pi) = N$. Uit Lemma 1.3.5 volgt nu dat $G^{(\ell)}$ oplosbaar is van lengte ten hoogste k, en dus is $G^{(\ell+k)} = (G^{(\ell)})^{(k)} = 1$. □

Opmerking 1.3.8. De analoge bewering voor nilpotentie is fout. Dit volgt reeds uit het heel eenvoudig voorbeeld $G = \mathbf{S}_3$ met normaaldeler $N = \mathbf{C}_3$, waarbij zowel N als G/N nilpotent zijn, maar G niet nilpotent is. Merk op dat het bovenstaande "bewijs" voor nilpotentie misloopt omdat in het algemeen $G^{[\ell+k]} \neq (G^{[\ell]})^{[k]}$.

Stelling 1.3.9. *Zij G een willekeurige groep. Dan zijn volgende uitspraken equivalent:*

(a) *G is oplosbaar (van lengte ten hoogste n);*

(b) *er is een rij normaaldelers $G_i \trianglelefteq G$ zodat*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

waarbij elke factor G_{i+1}/G_i abels is;

(c) *er is een rij deelgroepen $G_i \leq G$ zodat*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

waarbij elke factor G_{i+1}/G_i abels is.

Bewijs. De implicatie (b) $\Rightarrow$ (c) is triviaal.

Veronderstel nu dat G oplosbaar is van lengte ten hoogste n, en beschouw de afgeleide rij

$$1 = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

Dan voldoet deze rij (met $G_i = G^{(n-i)}$) aan de voorwaarden in (b), en dus (a) $\Rightarrow$ (b).

Ten slotte bewijzen we dat (c) $\Rightarrow$ (a). Veronderstel dus dat er een dergelijke rij deelgroepen $G_i \leq G$ bestaat. Uit het feit dat G_{i+1}/G_i abels is, volgt dat $G'_{i+1} \leq G_i$, voor elke i. In het bijzonder is $G' \leq G_{n-1}$. Maar dan is $G'' \leq G'_{n-1} \leq G_{n-2}$, en zo verder gaand vinden we dat $G^{(k)} \leq G_{n-k}$ voor alle k, en dus $G^{(n)} \leq G_0 = 1$. Dus G is oplosbaar, van lengte ten hoogste n. □

Gevolg 1.3.10. *Zij G een willekeurige groep, en veronderstel dat*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

een compositierij is voor G. Dan is G oplosbaar als en slechts als elke compositiefactor een eindige groep van priemorde is.

Bewijs. Indien G een compositierij heeft waarvan elke factor een eindige groep van priemorde is, dan volgt het gestelde onmiddellijk uit Stelling 1.3.9.

Veronderstel omgekeerd dat G oplosbaar is. Per definitie is elke compositiefactor G_{i+1}/G_i een enkelvoudige groep, die echter wegens Lemma 1.3.5 oplosbaar moet zijn. Echter, als H een oplosbare enkelvoudige groep is, dan is $H' \trianglelefteq H$ een echte normaaldeler van H, dus $H' = 1$ en dus is H abels. De enige abelse enkelvoudige groepen zijn de cyclische groepen van priemorde (zie "Algebra I"), en dit bewijst het gestelde. □

Voorbeeld 1.3.11. Beschouw de oplosbare groep $G = \mathbf{A}_4$. We hebben reeds gezien dat G oplosbaar is van lengte 2, met $G' \cong \mathbf{C}_2 \times \mathbf{C}_2$. Kies een willekeurige deelgroep $H \leq G'$ van orde 2; dan is de rij

$$1 \trianglelefteq H \trianglelefteq G' \trianglelefteq G$$

een compositierij voor G, met compositiefactoren $\{\mathbf{C}_2, \mathbf{C}_2, \mathbf{C}_3\}$.

We gaan nu wat dieper in op nilpotentie. We hebben nilpotentie gedefinieerd aan de hand van de dalende centrale rij, maar zoals we nu zullen aantonen, hadden we evenzeer de stijgende centrale rij kunnen gebruiken.

Stelling 1.3.12. *Zij G een willekeurige groep, en $n \in \mathbb{N}$. Dan is $G^{[n]} = 1$ als en slechts als $Z_n(G) = G$.*

Bewijs. Veronderstel eerst dat $G^{[n]} = 1$. Beschouw de dalende centrale rij

$$1 = G^{[n]} \trianglelefteq G^{[n-1]} \trianglelefteq \cdots \trianglelefteq G^{[1]} \trianglelefteq G^{[0]} = G,$$

en stel $N_i := G^{[n-i]}$ voor alle i. Noteer verder ook $Z_i := Z_i(G)$. We zullen per inductie aantonen dat $N_i \leq Z_i$ voor elke i, wat dan in het bijzonder zal bewijzen dat $Z_n = G$.

Voor $i = 0$ is $N_i \leq Z_i$ triviaal; stel dus $i > 0$ en $N_{i-1} \leq Z_{i-1}$. Dan is $[N_i, G] = N_{i-1} \leq Z_{i-1}$. Uit de definitie van Z_i volgt nu dat $N_i \leq Z_i$.

Veronderstel nu omgekeerd dat $Z_n = G$, en beschouw de stijgende centrale rij

$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_{n-1} \trianglelefteq Z_n = G.$$

We bewijzen per inductie op k dat $G^{[k]} \leq Z_{n-k}$ voor alle k; deze uitspraak is triviaal voor $k = 0$.

Stel dus $k > 0$ en $G^{[k-1]} \leq Z_{n-k+1}$. Dan is

$$G^{[k]} = [G^{[k-1]}, G] \leq [Z_{n-k+1}, G] \leq Z_{n-k},$$

wat de inductie-uitspraak bewijst. We besluiten dat $G^{[n]} \leq Z_0 = 1$. □

Gevolg 1.3.13. *Zij G een eindige groep, zodanig dat $Z(G/N) > 1$ voor elke echte normaaldeler $N \lhd G$. Dan is G nilpotent.*

Bewijs. Veronderstel dat G niet nilpotent is, en beschouw de stijgende centrale rij

$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots .$$

Uit Stelling 1.3.12 volgt dan dat $Z_i \neq G$ voor alle $i \in \mathbb{N}$, zodat wegens Opmerking 1.3.2(ii) $Z_i/Z_{i-1} = Z(G/Z_{i-1}) > 1$. Bijgevolg is $Z_i > Z_{i-1}$ voor elke $i \in \mathbb{N}$, en omdat G eindig is, bekomen we een strijdigheid. We besluiten dat G wel nilpotent is. □

Gevolg 1.3.14. *Elke eindige p-groep is nilpotent.*

Bewijs. Aangezien elke quotiëntgroep van een p-groep opnieuw een p-groep is, en omdat elke p-groep een niet-triviaal centrum heeft (zie "Algebra I"), volgt het gestelde onmiddellijk uit Gevolg 1.3.13. □

We geven nog een interessant gevolg hiervan mee.

Gevolg 1.3.15. *Elke eindige p-groep heeft een normaaldeler van index p.*

Bewijs. Zij G een eindige p-groep. Wegens Gevolg 1.3.14 is G nilpotent, en dus ook oplosbaar. Beschouw een compositierij

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

voor G. Uit Gevolg 1.3.10 volgt dat G/G_{n-1} een eindige groep van priemorde is; aangezien $|G|$ een macht is van p kan dit enkel als $[G : G_{n-1}] = p$, zodat G_{n-1} de gezochte normaaldeler van index p is. □

Uiteraard is het direct product van nilpotente groepen nog steeds nilpotent, en dus zien we dat het direct product van p-groepen (voor mogelijks verschillende priemen p) eveneens nilpotent is. Misschien verrassend is het feit dat dit ook de enige eindige nilpotente groepen zijn.

Eerst bewijzen we nog een eenvoudig maar krachtig lemma, het zogenaamde Frattini argument.

Lemma 1.3.16 (Frattini argument)**.** *Zij G een willekeurige groep, $N \trianglelefteq G$ een eindige normaaldeler, en $P \in \mathrm{Syl}_p(N)$ een Sylow p-deelgroep van N, voor een zekere priem p. Dan is $G = N_G(P)N$.*

Bewijs. Zij $g \in G$ willekeurig, en beschouw P^g. Dan is $P^g \leq N^g = N$, en dus $P^g \in \mathrm{Syl}_p(N)$. Uit de stelling van Sylow volgt dat P en P^g toegevoegd zijn in N, dus er bestaat een $n \in N$ zodat $P^n = P^g$. Maar dan is $gn^{-1} \in N_G(P)$, en bijgevolg $g \in N_G(P)n \subseteq N_G(P)N$. □

Lemma 1.3.17. *Zij G een groep, en H en K deelgroepen van G. Dan is $K \leq N_G(H)$ als en slechts als $[H, K] \leq H$.*

Bewijs. Veronderstel eerst dat $K \leq N_G(H)$, en beschouw een voortbrenger $[h, k]$ van $[H, K]$, met $h \in H$ en $k \in K$. Dan is $[h, k] = h^{-1}h^k \in H$. Bijgevolg is $[H, K] \leq H$.

Veronderstel omgekeerd dat $[H, K] \leq H$; dan is $[h, k] \in H$ voor alle $h \in H$ en alle $k \in K$. Hieruit volgt dat $h^k \in H$ voor alle $h \in H$ en alle $k \in K$, en dus $k \in N_G(H)$ voor alle $k \in K$. Dus $K \leq N_G(H)$. □

Stelling 1.3.18. *Zij G een eindige groep. Dan zijn volgende uitspraken equivalent:*

(a) *G is nilpotent;*

(b) *$N_G(H) > H$ voor elke echte deelgroep $H < G$;*

(c) *elke maximale deelgroep van G is een normaaldeler;*

(d) *elke Sylow deelgroep van G is een normaaldeler;*

(e) *G is isomorf met het direct product van p-groepen (voor verschillende priemen p).*

Bewijs. (a) $\Rightarrow$ (b). Veronderstel dat G nilpotent is, en stel $H < G$ willekeurig. Zij $k \in \mathbb{N}$ minimaal zodat $G^{[k]} \leq H$; dan is $G^{[k-1]} \not\leq H$. Anderzijds is $[H, G^{[k-1]}] \leq [G, G^{[k-1]}] = G^{[k]} \leq H$, en uit Lemma 1.3.17 volgt dat $G^{[k-1]} \leq N_G(H)$. We besluiten dat $H \neq N_G(H)$, dus (b) geldt.

(b) $\Rightarrow$ (c). Als $M < G$ een maximale deelgroep is, dan is $N_G(M) > M$ wegens (b), en dus $N_G(M) = G$, met andere woorden, $M \trianglelefteq G$.

(c) $\Rightarrow$ (d). Zij $P \in \mathrm{Syl}_p(G)$ willekeurig, en veronderstel dat P geen normaaldeler zou zijn, dus $N_G(P) < G$. Kies een maximale deelgroep M die $N_G(P)$ bevat; wegens (c) is dan $M \trianglelefteq G$, en ook $P \in \mathrm{Syl}_p(M)$. We kunnen dus het Frattini argument (Lemma 1.3.16) toepassen, en we besluiten dat $G = N_G(P)M$, in strijd met $N_G(P) \leq M$.

(d) $\Rightarrow$ (e). Om te bewijzen dat G het direct product is van deelgroepen $S_1, \ldots, S_\ell$, volstaat het om na te gaan dat

- elke S_i een normaaldeler is;
- $S_i \cap S_{i+1} \cdots S_\ell = 1$ voor elke $i \in \{1, \ldots, \ell - 1\}$;
- $G = S_1 S_2 \cdots S_\ell$.

(Zie opnieuw "Algebra I".) Stel dus dat $p_1, \ldots, p_\ell$ de verschillende priemdelers zijn van G, en stel S_i gelijk aan de (unieke) Sylow p_i-deelgroep van G. Dan zijn de S_i inderdaad normaaldelers, en aangezien de orde van S_i een macht van p_i is terwijl de orde van $S_{i+1} \cdots S_\ell$ niet deelbaar is door p_i, volgt het gestelde.

(e) $\Rightarrow$ (a). Dit hebben we reeds aangetoond. $\square$

Opmerking 1.3.19. De implicaties (a) $\Rightarrow$ (b) $\Rightarrow$ (c) uit voorgaande stelling blijven geldig voor oneindige groepen, maar (b) noch (c) zijn equivalent met (a).

Tot slot vermelden we nog twee zeer diepe resultaten in verband met oplosbare groepen.

Stelling 1.3.20 (Burnside, 1904)**.** *Zij G een eindige groep met $|G| = p^k q^\ell$ voor zekere priemen p en q, en zekere $k, \ell \in \mathbb{N}$. Dan is G oplosbaar.*

Het oorspronkelijke, en nog steeds meest elegante, bewijs van deze stelling maakt gebruik van karaktertheorie. In het begin van de jaren 1970 hebben Goldschmidt (voor p en q oneven), en nadien Bender en Matsumaya (voor p en q algemeen), een karaktervrij, maar erg geavanceerd, alternatief bewijs gegeven van deze stelling.

Stelling 1.3.21 (Feit–Thompson, 1963)**.** *Zij G een eindige groep van oneven orde. Dan is G oplosbaar.*

Het bewijs van deze stelling is onvoorstelbaar diep, en het neemt 255 bladzijden in beslag.

Hoofdstuk

2 Enkelvoudige groepen

Zoals we reeds hebben aangehaald, zijn de eindige enkelvoudige groepen de bouwstenen voor alle eindige groepen, in die zin dat heel wat structuur van een groep gegeven wordt door zijn compositierij, waarvan de compositiefactoren enkelvoudige groepen zijn.

Ook voor oneindige groepen spelen enkelvoudige groepen een belangrijke rol, al moet hier wel aan toegevoegd worden dat het niet langer correct is dat die de bouwstenen zijn voor willekeurige groepen. (Denk maar aan een abelse groep zoals $(\mathbb{Q}, +)$, die in geen enkele zin opgebouwd kan worden uit enkelvoudige groepen.) Vaak wordt het begrip van enkelvoudigheid dan gecombineerd met bijkomende structuur. Bijvoorbeeld, wanneer G een *topologische* groep is, dan is het natuurlijk om te kijken naar groepen die geen echte niet-triviale *gesloten* normaaldelers hebben. Ook dan is het nog interessant om na te gaan of een groep die "topologisch enkelvoudig" is, ook "abstract enkelvoudig" is. Op deze aspecten gaan we in deze cursus echter niet verder in.

De eindige enkelvoudige groepen zijn geclassificeerd, en deze classificatie wordt door sommigen beschouwd als de belangrijkste wiskundige verwezenlijking van de twintigste eeuw. Op het einde van dit hoofdstuk geven we een overzicht van het resultaat van deze classificatie, zonder evenwel in detail te kunnen gaan.

2.1 Enkelvoudigheid van $\mathbf{A}_n$, $n \geq 5$

Tot dusver hebben we nog niet veel enkelvoudige groepen ontmoet: de cyclische groepen van priemorde zijn de enige waarvan we al enkelvoudigheid kunnen bewijzen hebben. In Voorbeeld 1.3.3(4) hebben we al aangereikt dat de alternerende groepen $\mathbf{A}_n$ voor $n \geq 5$ enkelvoudig zijn, en dit gaan we dadelijk ook effectief bewijzen.

We herhalen eerst een nuttige definitie om de structuur van elementen van $\mathbf{S}_n$ te beschrijven.

Definitie 2.1.1. Zij g een willekeurig element van de symmetrische groep $\mathbf{S}_n$. Dan kan g op unieke manier geschreven worden als product van disjuncte

cykels. De *cykelstructuur* van g is de data die de lengtes van deze disjuncte cykels weergeeft. We noteren de cykelstructuur als

$$c_1^{m_1} \cdot c_2^{m_2} \cdots c_d^{m_d},$$

waarbij er m_i cykels zijn van lengte c_i, en dus $c_1 m_1 + \cdots + c_d m_d = n$.

Voorbeeld 2.1.2. Zij $g = (1\ 3\ 4)(2\ 6)(7\ 9) \in \mathbf{S}_9$. Dan heeft g cykelstructuur $1^2 \cdot 2^2 \cdot 3^1$, want g heeft 2 fixpunten, 2 cykels van lengte 2, en 1 cykel van lengte 3.

Het resultaat van toevoeging van een element $g \in \mathbf{S}_n$ met een ander element $h \in \mathbf{S}_n$ is heel gemakkelijk af te lezen uit de cykeldecompositie.

Lemma 2.1.3. *Zij*

$$g = (a_1\ \ldots\ a_k)(b_1\ \ldots\ b_\ell)\cdots(z_1\ \ldots\ z_m) \in \mathbf{S}_n$$

gegeven als product van disjuncte cykels, en zij $h \in \mathbf{S}_n$ willekeurig. Dan is

$$g^h = (a_1^h\ \ldots\ a_k^h)(b_1^h\ \ldots\ b_\ell^h)\cdots(z_1^h\ \ldots\ z_m^h).$$

In het bijzonder hebben g en g^h dezelfde cykelstructuur.

Bewijs. Dit is een eenvoudige oefening. □

Stelling 2.1.4. *Twee elementen $g, g' \in \mathbf{S}_n$ zijn toegevoegd aan elkaar als en slechts als ze dezelfde cykelstructuur hebben.*

Bewijs. De "slechts als" implicatie is precies Lemma 2.1.3. Veronderstel dus dat g en g' dezelfde cykelstructuur hebben. Schrijf de cykels van g en g' neer van kort naar lang, startend met de cykels van lengte 1, i.e. de fixpunten. (Deze schrijfwijze is niet uniek, maar dat maakt niet uit.) We bekomen dan

$$\begin{aligned} g &= (a_1\ \ldots\ a_k)(b_1\ \ldots\ b_\ell)\cdots(z_1\ \ldots\ z_m), \\ g' &= (a'_1\ \ldots\ a'_k)(b'_1\ \ldots\ b'_\ell)\cdots(z'_1\ \ldots\ z'_m), \end{aligned}$$

met $k \leq \ell \leq \cdots \leq m$. Dan is er een unieke $h \in \mathbf{S}_n$ die elke x_i afbeeldt op de overeenkomstige x'_i, en voor deze h geldt duidelijkerwijze dat $g^h = g'$. □

Gevolg 2.1.5. *Het centrum van $\mathbf{S}_n$, $n \geq 3$, is triviaal.*

Bewijs. Veronderstel dat er een $z \in Z(\mathbf{S}_n) \setminus \{1\}$ zou zijn. Aangezien $z \neq 1$ is z van de gedaante $z = (a_1\ a_2\ \ldots\ a_k)\cdots$. Kies nu $c \in \{1, \ldots, n\} \setminus \{a_1, a_2\}$ willekeurig, en stel $h = (a_2\ c) \in \mathbf{S}_n$; dan is $z^h = (a_1\ c\ \ldots)\cdots$, en dus $z^h \neq z$, in strijd met $z \in Z(\mathbf{S}_n)$. □

Opmerking 2.1.6. Op analoge wijze toont men aan dat het centrum van $\mathbf{A}_n$, $n \geq 4$, triviaal is. Werk zelf de details uit.

We beginnen nu met het bewijs van de enkelvoudigheid van $\mathbf{A}_5$; deze groep van orde $60 = 2^2 \cdot 3 \cdot 5$ is tevens de kleinste niet-abelse enkelvoudige groep.

Lemma 2.1.7. *De alternerende groep $\mathbf{A}_5$ is enkelvoudig.*

Bewijs. De cykelstructuren van de elementen van $\mathbf{A}_5$ zijn

$$1^5, \quad 1 \cdot 2^2, \quad 1^2 \cdot 3, \quad 5,$$

en het is niet moeilijk om te tellen dat er respectievelijk 1, 15, 20 en 24 elementen van elke soort zijn. Veronderstel nu dat $1 < N \lhd \mathbf{A}_5$.

Indien $3 \mid |N|$, dan bevat N een Sylow 3-deelgroep van $\mathbf{A}_5$, en uit de stelling van Sylow volgt dan dat N alle Sylow 3-deelgroepen van $\mathbf{A}_5$ bevat, en dus alle 20 elementen van orde 3. Dus $|N| > 20$, en de enige echte deler van 60 groter dan 20 is 30, dus $|N| = 30$.

Indien $5 \mid |N|$, dan volgt geheel analoog dat N alle 24 elementen van orde 5 bevat, dus $|N| > 24$, en dus opnieuw $|N| = 30$.

We stellen dus reeds vast dat indien $3 \mid |N|$ of $5 \mid |N|$, dan in feite $3 \mid |N|$ én $5 \mid |N|$, en dus bevat N reeds 20 elementen van orde 3 en 24 elementen van orde 5, wat onmogelijk is.

Dus de enige priemdeler van $|N|$ is 2. Indien $|N| = 4$, dan bevat N een Sylow 2-deelgroep van $\mathbf{A}_5$, en dus alle 15 elementen van orde 2, wat uiteraard niet kan.

Er blijft dus nog enkel het geval $|N| = 2$ over. Het niet-triviale element $n \in N$ heeft cykelstructuur $1 \cdot 2^2$ en heeft dus een cykeldecompositie $n = (a\ b)(c\ d)$. Het element $h = (b\ c\ d) \in \mathbf{A}_5$ houdt echter het element n niet vast onder toevoeging, en deze contradictie besluit het bewijs. □

Opmerking 2.1.8. In $\mathbf{S}_5$ vormt de verzameling van alle 5-cykels één toevoegingsklasse (wegens Stelling 2.1.4), en deze klasse is volledig bevat in $\mathbf{A}_5$, maar deze toevoegingsklasse splitst op in twee toevoegingsklassen in $\mathbf{A}_5$. (Ga dit zelf na als oefening.)

Stelling 2.1.9. *Voor elke $n \geq 5$ is de alternerende groep $\mathbf{A}_n$ enkelvoudig.*

Bewijs. We bewijzen dit per inductie op n, waarbij het geval $n = 5$ precies Lemma 2.1.7 is. Zij dus $n \geq 6$, stel $G = \mathbf{A}_n$, en veronderstel dat $1 \neq N \lhd G$ een echte niet-triviale normaaldeler is. Zij $H = \mathrm{Stab}_G(n)$; dan is $H \cong \mathbf{A}_{n-1}$,

en door de inductiehypothese weten we dat H enkelvoudig is. Aangezien $N \cap H \trianglelefteq H$, volgt hieruit dat ofwel $N \cap H = 1$, ofwel $H \leq N$.

Veronderstel eerst dat $H \leq N$. Omdat N een normaaldeler is, volgt hieruit dat ook $H^g \leq N$ voor alle $g \in \mathbf{A}_n$, en omdat $\mathbf{A}_n$ uiteraard transitief werkt op $\{1, \ldots, n\}$, halen we hieruit dat $\mathrm{Stab}_G(i) \leq N$ voor alle $i \in \{1, \ldots, n\}$. In het bijzonder bevat N dus alle elementen die het product zijn van twee transposities, maar dan is $N = \mathbf{A}_n$, strijdig.

Veronderstel nu dat $N \cap H = 1$. Dan is ook $N \cap H^g = (N \cap H)^g = 1$, en dus $N \cap \mathrm{Stab}_G(i) = 1$ voor alle i, i.e. enkel het triviale element van N heeft fixpunten. Kies nu een $g \in N \setminus \{1\}$ willekeurig. De cykeldecompositie van g bevat ofwel een m-cykel met $m \geq 3$, ofwel bestaat het volledig uit 2-cykels, maar dan zijn er ten minste twee 2-cykels. Door de elementen $\{1, \ldots, n\}$ te hernummeren mogen we dus veronderstellen dat g de gedaante

$$g = (1\ 2\ 3\ \ldots\ m)\cdots \quad \text{of} \quad g = (1\ 2)(3\ 4)\cdots$$

heeft. Beschouw nu $h = g^{(3\ 5\ 6)} \in N$. Dan is

$$h = (1\ 2\ 5\ \ldots)\cdots \quad \text{of} \quad h = (1\ 2)(5\ 4)\cdots$$

In beide gevallen is $g \neq h$ en fixeert gh^{-1} het punt 1. Aangezien $gh^{-1} \in N$ is dit een strijdigheid. □

Gevolg 2.1.10. *De enige normaaldelers van* $\mathbf{S}_n$*,* $n \geq 5$*, zijn* 1*,* $\mathbf{A}_n$ *en* $\mathbf{S}_n$*.*

Bewijs. Zij $N \trianglelefteq \mathbf{S}_n$. Dan is $\mathbf{A}_n \cap N \trianglelefteq \mathbf{A}_n$, en uit Stelling 2.1.9 volgt dan dat ofwel $\mathbf{A}_n \leq N$, ofwel $\mathbf{A}_n \cap N = 1$.

In het eerste geval moet ofwel $N = \mathbf{A}_n$, ofwel $N = \mathbf{S}_n$. Stel dus nu dat $\mathbf{A}_n \cap N = 1$; dan is $|\mathbf{A}_n N| = |\mathbf{A}_n| \cdot |N|$, en bijgevolg $|N| \leq [\mathbf{S}_n \colon \mathbf{A}_n] = 2$. Er rest ons enkel nog het geval $|N| = 2$ uit te sluiten. Een normaaldeler van orde 2 is echter steeds bevat in het centrum, en dus zou $N \leq Z(\mathbf{S}_n)$. Dit is in strijd met Gevolg 2.1.5. □

2.2 Enkelvoudigheid van $\mathsf{PSL}_2(k)$

Een grote klasse van enkelvoudige groepen zijn de zogenaamde *Chevalleygroepen*, die in het eindig geval vaak ook de *groepen van Lie-type* genoemd worden. De theorie van de Chevalleygroepen ontwikkelen zou een cursus op zich in beslag nemen, dus we beperken ons tot het eenvoudigste maar in zekere zin voornaamste voorbeeld, namelijk $\mathsf{PSL}_n(k)$.

We herhalen eerst de definitie van deze groepen, die reeds bestudeerd werden in de cursus "Projectieve meetkunde".

Definitie 2.2.1. Zij k een willekeurig veld, en $n \in \mathbb{N}$ met $n \geq 2$. De *algemene lineaire groep* $\mathsf{GL}_n(k)$ is de groep van alle inverteerbare $n \times n$ matrices over k; de *speciale lineaire groep* $\mathsf{SL}_n(k)$ is de groep van alle $n \times n$ matrices over k met determinant gelijk aan 1.

De groepen $\mathsf{GL}_n(k)$ en $\mathsf{SL}_n(k)$ hebben een niet noodzakelijk triviaal centrum; we definiëren dan ook de *projectieve lineaire groep* $\mathsf{PGL}_n(k)$ en de *projectieve speciale lineaire groep* $\mathsf{PSL}_n(k)$ als

$$\mathsf{PGL}_n(k) = \mathsf{GL}_n(k) \,/\, Z(\mathsf{GL}_n(k)),$$
$$\mathsf{PSL}_n(k) = \mathsf{SL}_n(k) \,/\, Z(\mathsf{SL}_n(k)).$$

Merk op dat $\mathsf{PSL}_n(k)$ een deelgroep is van $\mathsf{PGL}_n(k)$, namelijk het beeld van $\mathsf{SL}_n(k)$ onder de canonieke projectie $\pi\colon \mathsf{GL}_n(k) \to \mathsf{PGL}_n(k)$. Het is gebruikelijk om de matrices in $\mathsf{GL}_n(k)$ met ronde haken te noteren, en hun overeenkomstig beeld onder de projectie π met vierkante haken. Als $A \in \mathsf{GL}_n(k)$, dan noteren we ook $[A]$ voor de overeenkomstige matrix $\pi(A) \in \mathsf{PGL}_n(k)$, en er geldt:

$$[A] \in \mathsf{PSL}_n(k) \iff \det(A) \in k^n.$$

Bijgevolg geldt ook dat

$$[\mathsf{PGL}_n(k) : \mathsf{PSL}_n(k)] = [k^\times : (k^\times)^n], \tag{2.1}$$

waarbij $k^\times$ de multiplicatieve groep van k is, en $(k^\times)^n$ de deelgroep van $k^\times$ bestaande uit alle n-de machten.

De groepen $\mathsf{PSL}_n(k)$ zijn altijd enkelvoudig, behalve als $n = 2$ en $k = \mathbb{F}_2$ of $\mathbb{F}_3$. We zullen dit resultaat bewijzen voor $n = 2$. Het bewijs voor grotere n loopt volgens dezelfde lijnen, maar vraagt meer werk, en zullen we dus achterwege laten.

Beschouw dus de groep $G = \mathsf{PSL}_2(k)$ voor een willekeurig veld k, en stel $S = \mathbb{P}^1(k)$, de projectieve rechte[1] over k, die we als verzameling kunnen voorstellen als $S = k \cup \{\infty\}$. De werking van G op S wordt dan expliciet gegeven (zie cursus "Projectieve meetkunde") door

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : x \mapsto \frac{ax + b}{cx + d}, \tag{2.2}$$

[1] In de cursus "Projectieve meetkunde" werd de projectieve rechte genoteerd als $\mathrm{PG}(V)$ met V een 2-dimensionale vectorruimte over k, of ook als $\mathrm{PG}(1, k)$, maar de notatie $\mathbb{P}^1(k)$ wordt vaker gebruikt in de algebra, en benadrukt in feite dat deze meetkunde de bijkomende structuur heeft van een algebraïsche variëteit.

waarbij ∞ wordt afgebeeld op a/c, en waarbij delen door 0 als resultaat ∞ geeft.

We bekijken eerst kort de twee uitzonderingsgevallen.

Lemma 2.2.2. *De groepen* $\mathsf{PSL}_2(\mathbb{F}_2)$ *en* $\mathsf{PSL}_2(\mathbb{F}_3)$ *zijn niet enkelvoudig. Meer bepaald is* $\mathsf{PSL}_2(\mathbb{F}_2) \cong \mathbf{S}_3$ *en is* $\mathsf{PSL}_2(\mathbb{F}_3) \cong \mathbf{A}_4$.

Bewijs. Deze groepen zijn zo klein (nl. orde 6 en 12) dat het mogelijk is om deze isomorfismen expliciet neer te schrijven, maar we zullen een conceptueler bewijs geven.

Beschouw de actie van $\mathsf{PGL}_2(k)$ op de projectieve rechte $\mathbb{P}^1(k)$. Deze actie is getrouw en drievoudig transitief (zie opnieuw cursus "Projectieve meetkunde"). In het geval dat k een eindig veld $\mathbb{F}_q$ is, betekent dit dus dat er een monomorfisme

$$\varphi\colon \mathsf{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathbf{S}_{q+1}$$

is, waarbij het beeld een drievoudig transitieve deelgroep van $\mathbf{S}_{q+1}$ is. Indien $q = 2$ of $q = 3$, dan kan dit enkel als $\operatorname{im}\varphi = \mathbf{S}_{q+1}$, met andere woorden,

$$\mathsf{PGL}_2(\mathbb{F}_2) \cong \mathbf{S}_3, \qquad \mathsf{PGL}_2(\mathbb{F}_3) \cong \mathbf{S}_4.$$

Anderzijds volgt uit (2.1) dat $\mathsf{PSL}_2(\mathbb{F}_2) = \mathsf{PGL}_2(\mathbb{F}_2)$, terwijl $\mathsf{PSL}_2(\mathbb{F}_3)$ een deelgroep van index 2 is in $\mathsf{PGL}_3(\mathbb{F}_3)$. De enige deelgroep van index 2 van $\mathbf{S}_4$ is echter $\mathbf{A}_4$ (ga dit zelf na als oefening); dit toont aan dat $\mathsf{PSL}_2(\mathbb{F}_3) \cong \mathbf{A}_4$. $\square$

Opmerking 2.2.3. Als $\mathbb{F}_q$ een eindig veld is, dan noteren we $\mathsf{PSL}_n(\mathbb{F}_q)$ ook nog als $\mathsf{PSL}_n(q)$. Sommige auteurs verkiezen de notatie $\mathsf{PSL}(n, q)$.

Ook in het verder verloop zal de actie van $\mathsf{PSL}_2(k)$ op de projectieve rechte een belangrijke rol spelen. Het cruciale aspect is dat deze actie een zogenaamde primitieve actie is.

Definitie 2.2.4. Zij G een willekeurige groep die werkt op een willekeurige verzameling S.

(i) Een niet-ledige deelverzameling $B \subseteq S$ wordt een *imprimitiviteitsblok* (of soms kortweg *blok*) genoemd, als voor alle $g \in G$ geldt dat

$$\text{ofwel } B^g = B, \quad \text{ofwel } B^g \cap B = \emptyset.$$

(ii) Een blok $B \subseteq S$ wordt *triviaal* genoemd als ofwel $|B| = 1$, ofwel $B = S$. Merk op dat voor elke actie deze verzamelingen B inderdaad imprimitiviteitsblokken zijn, wat verklaart waarom we dergelijke blokken triviaal noemen.

(iii) De actie van G op S wordt *primitief* genoemd, als ze transitief is en geen niet-triviale imprimitiviteitsblokken heeft.

Opmerking 2.2.5. (i) Als de actie van G op S geen niet-triviale imprimitiviteitsblokken heeft, en $|S| \geq 3$, dan is ze automatisch transitief. Inderdaad: merk vooreerst op dat de actie niet-triviaal is, want anders zou elke deelverzameling B van S een imprimitiviteitsblok zijn, wat niet mag. Als de actie nu niet transitief zou zijn, dan zou er een baan $B \subsetneq S$ zijn met $|B| > 1$ en $B \neq S$, maar dan geldt voor elke $g \in G$ dat $B^g = B$, zodat B een niet-triviaal imprimitiviteitsblok zou zijn.
Echter, voor $|S| = 2$ geldt dit niet: als G een groep is die triviaal werkt op een dergelijke S, dan heeft deze actie geen niet-triviale imprimitiviteitsblokken, maar uiteraard is ze niet transitief.

(ii) Als G transitief werkt op S, en B is een imprimitiviteitsblok, dan vormen alle blokken B^g samen een *G-invariante partitie* van de verzameling S. Omgekeerd geldt ook dat als G transitief werkt, en er een G-invariante partitie is van S, dan zal elke verzameling van die partitie een imprimitiviteitsblok vormen voor de actie van G op S. We kunnen dus ook nog zeggen dat de actie primitief is als ze transitief is en S geen niet-triviale G-invariante partitie heeft, waarbij we onder een triviale partitie verstaan dat we S ofwel opdelen in 1 verzameling (S zelf), ofwel in $|S|$ singletons (elk element van S in een eigen verzameling).

De primitieve acties situeren zich tussen de transitieve en de tweevoudig transitieve acties:

Lemma 2.2.6. *Elke tweevoudig transitieve actie is primitief.*

Bewijs. Zij G een groep die tweevoudig transitief werkt op een verzameling S. We mogen uiteraard aannemen dat $|S| \geq 2$. Veronderstel dat B een imprimitiviteitsblok is met $|B| > 1$; we moeten aantonen dat dan $B = S$. Veronderstel het tegendeel; dan vinden we elementen $x \neq y \in B$ en $z \in S \setminus B$. Wegens de tweevoudige transitiviteit is er een $g \in G$ die het paar (x, y) afbeeldt op (x, z), i.e. $x^g = x$ en $y^g = z$. Maar dan is $B^g \cap B \neq \emptyset$, terwijl toch $B^g \neq B$, in strijd met het feit dat B een blok is. □

Voorbeeld 2.2.7. We geven een voorbeeld van een actie die primitief is, maar niet tweevoudig transitief. Zij G de cyclische groep $\mathbb{Z}/p$, waarbij $p \geq 3$ priem is, en beschouw de actie van G op de verzameling $S = \{0, 1, \ldots, p-1\}$ door optelling modulo p. Uiteraard is deze actie transitief. Omdat elke puntstabilisator G_s triviaal is, is de actie zeker niet tweevoudig transitief. (In feite is deze actie *scherp transitief*.)

Veronderstel dat $B \subsetneq S$ een niet-triviaal imprimitiviteitsblok is, en stel $x \neq y \in B$. Neem $g = (y - x \mod p) \in G$; dan is $x^g = y$, dus $B^g \cap B \neq \emptyset$, en dus moet $B^g = B$. Hieruit volgt dan dat ook $y^g \in B$, maar dan ook $(y^g)^g \in B$, en zo verder, zodat dus $y^{\langle g \rangle} \subseteq B$. Echter, G heeft geen echte niet-triviale deelgroepen, en dus $\langle g \rangle = G$, zodat $B = y^G = S$, strijdig.

Merk op dat de gelijkaardige actie van $G = \mathbb{Z}/n$ op $S = \{0, 1, \ldots, n-1\}$ waarbij n niet priem is, geen primitieve actie is. (Zoek zelf een niet-trivaal blok voor deze actie.)

Het belang van primitieve acties blijkt ondermeer uit de volgende stelling.

Stelling 2.2.8. *Zij G een groep die transitief werkt op een verzameling S met $|S| \geq 2$, en zij $s \in S$ willekeurig. Dan werkt G primitief op S als en slechts als $G_s := \mathrm{Stab}_G(s)$ een maximale deelgroep is van G.*

Bewijs. Merk vooraf op dat $G_s \neq G$ omdat anders $\{s\}$ een baan zou zijn en G dan niet transitief zou werken. We zullen aantonen dat G *niet* primitief werkt op S als en slechts als G_s *geen* maximale deegroep is van G.

Stel dus eerst dat G_s geen maximale deelgroep is van G; dan is er een deelgroep H van G zodat

$$G_s < H < G.$$

Stel dan $B = s^H$; we beweren dat B een niet-triviaal blok is. Om aan te tonen dat het een blok is, moeten we voor elke $g \in G$ met $B^g \cap B \neq \emptyset$ bewijzen dat $B^g = B$. Inderdaad, stel $t \in B^g \cap B = s^{Hg} \cap s^H$, zodat we $h, h' \in H$ vinden met $t = s^{h'g} = s^h$. Dan is $h'gh^{-1} \in G_s \leq H$, en bijgevolg $g \in H$. Hieruit volgt dat $B^g = s^{Hg} = s^H = B$. Dit bewijst dat B een blok is.

Veronderstel dat B een triviaal blok zou zijn. Als enerzijds $|B| = 1$, dan zou $s^H = B = \{s\}$, zodat $H \leq G_s$, in strijd met $G_s < H$. Als anderzijds $B = S$, dan zou $s^H = S$. Maar dan is er voor elke $g \in G$ ook een $h \in H$ zodat $s^g = s^h$, waaruit dan $gh^{-1} \in G_s \leq H$ en dus $g \in H$, in strijd met $H < G$.

We besluiten dat B een niet-triviaal blok is, en dus is de actie van G op S niet primitief.

Stel nu omgekeerd dat G niet primitief werkt op S. Beschouw een niet-triviaal blok B, kies een $t \in B$, en beschouw

$$H := \{h \in G \mid B^h = B\} = \{h \in G \mid B^h \cap B \neq \emptyset\}.$$

We zullen aantonen dat $G_t < H < G$, waaruit dan volgt dat G_t geen maximale deelgroep is. Omdat G transitief werkt, volgt hieruit dan ook dat G_s geen maximale deelgroep is.

Merk op dat de inclusies $G_t \leq H \leq G$ evident zijn. Kies nu elementen $x \in B \setminus \{t\}$ en $y \in S \setminus B$ willekeurig. Wegens de onderstelde transitiviteit bestaat er een $g \in G$ met $t^g = x$; het is duidelijk dat $g \in H$ terwijl $g \notin G_t$, wat aantoont dat $G_t < H$.

Anderzijds bestaat er een $g' \in G$ met $t^{g'} = y$; dan is $g' \notin H$, wat aantoont dat $H < G$.

We besluiten dat G_t, en dus ook G_s, geen maximale deelgroep is van G. □

Voorbeeld 2.2.9. Beschouw opnieuw de actie van $G = \mathbb{Z}/n$ op de verzameling $S = \{0, 1, \ldots, n-1\}$ door optelling modulo n. Het is duidelijk dat $\mathrm{Stab}_G(0) = 1$. De triviale groep is een maximale deelgroep van G als en slechts als G geen echte niet-triviale deelgroepen heeft, en voor $G = \mathbb{Z}/n$ is dit uiteraard equivalent met het feit dat n priem is; we vinden dus de resultaten uit Voorbeeld 2.2.7 terug.

Opmerking 2.2.10. Stelling 2.2.8 zegt *niet* dat bij een primitieve actie elke maximale deelgroep een punt-stabilisator zou zijn. Zo heeft de groep $\mathbf{S}_5$, die primitief werkt op $S = \{1, \ldots, 5\}$, een maximale deelgroep $\mathbf{A}_5 \leq \mathbf{S}_5$, maar $\mathbf{A}_5$ is geen punt-stabilisator voor deze actie.

Lemma 2.2.11. *Zij G een groep die transitief werkt op een verzameling S, en zij $N \trianglelefteq G$.*

(i) *De banen van N worden door G onderling gepermuteerd, en elke baan van de actie van N op S heeft dezelfde lengte.*

(ii) *Als de actie van G op S primitief en getrouw is, en $N \neq 1$, dan werkt N transitief op S.*

Bewijs. (i) Voor elke $g \in G$ en elke $x \in S$ is

$$(x^N)^g = x^{Ng} = x^{gN} = (x^g)^N,$$

zodat G elke baan van N afbeeldt op een baan van N.
Beschouw nu twee willekeurige banen x^N en y^N van N. Omdat G transitief werkt, is er een $g \in G$ met $y = x^g$, en dan is $y^N = (x^N)^g$, zodat in het bijzonder $|y^N| = |x^N|$.

(ii) Uit (i) volgt dat elke baan van N een imprimitiviteitsblok voor de actie van G op S vormt. Uit de primitiviteit volgt dan voor elke $x \in S$ dat ofwel $x^N = \{x\}$, ofwel $x^N = S$.
In het eerste geval zou $|y^N| = 1$ voor alle $y \in S$, zodat N triviaal werkt, wat dan wegens de getrouwheid impliceert dat $N = 1$, strijdig. □

We komen nu tot een belangrijk enkelvoudigheidscriterium, dat we zullen aanwenden om de enkelvoudigheid van $\mathsf{PSL}_2(k)$ te bewijzen.

Stelling 2.2.12 (Stelling van Iwasawa)**.** *Zij G een groep die werkt op een verzameling S met $|S| \geq 2$, en zij $s \in S$. Veronderstel bovendien:*

(a) *De actie van G op S is primitief en getrouw;*

(b) *G is perfect, i.e. $[G, G] = G$;*

(c) *$G_s = \mathrm{Stab}_G(s)$ bevat een oplosbare normaaldeler U;*

(d) *G wordt voortgebracht door de toegevoegden van U in G.*

Dan is G enkelvoudig.

Bewijs. Zij $1 \neq N \trianglelefteq G$. Uit Stelling 2.2.8 weten we dat $G_s \leq G$ een maximale deelgroep is. Anderzijds weten we uit Lemma 2.2.11 dat N transitief werkt op S, zodat in het bijzonder $N \not\leq G_s$. Uit $G_s \leq NG_s \leq G$ volgt dan dat $NG_s = G$.

Omdat $U \trianglelefteq G_s$ is ook $NU \trianglelefteq NG_s = G$, en dus is, voor elke $g \in G$,

$$U^g \leq (NU)^g = NU.$$

Omdat $G = \langle U^g \mid g \in G \rangle$, volgt hieruit dat $G \leq NU$ en dus $G = NU$. Hieruit volgt dat $G/N = NU/N \cong U/(N \cap U)$ een quotiënt is van de oplosbare groep U, en dus is G/N zelf ook oplosbaar.

Anderzijds is G/N perfect, want het is een quotiënt van de perfecte groep G. De enige perfecte oplosbare groep is echter de triviale groep, en dus is $G/N = 1$, waaruit $G = N$. □

Vanaf nu veronderstellen we dat $G = \mathsf{PSL}_2(k)$ voor een willekeurig veld k, en dat $S = \mathbb{P}^1(k) = k \cup \{\infty\}$, waarbij de werking van G op S gegeven wordt door formule (2.2).

We beschouwen nu de puntstabilisator $B := G_\infty \leq G$. (De letter B staat hier voor "Borel", omdat deze groep een zogenaamde *Borel deelgroep* is.) Het is duidelijk dat

$$B = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \;\middle|\; a \in k^\times, b \in k \right\}.$$

Deze groep B bevat een oplosbare[2] (zelfs abelse) normaaldeler

$$U = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \;\middle|\; b \in k \right\} \trianglelefteq B.$$

[2]In feite is de groep $B = G_\infty$ hier reeds zelf oplosbaar, maar dat is "toevallig" zo voor $\mathsf{PSL}_2(k)$ en dit is niet langer het geval voor $\mathsf{PSL}_n(k)$.

Lemma 2.2.13. *De groep $G = \mathsf{PSL}_2(k)$ wordt voortgebracht door de toegevoegden van U in G.*

Bewijs. Beschouw de groep

$$V = \left\{ \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \mid c \in k \right\} \trianglelefteq G_0 \,.$$

Men rekent eenvoudig na dat het element $h := \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ de groep U toevoegt naar V. Het volstaat dus te bewijzen dat G wordt voortgebracht door U en V.

Zij $g := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in G$ willekeurig. Als $b \neq 0$, dan is

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (d-1)/b & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (a-1)/b & 1 \end{bmatrix},$$

en als $c \neq 0$, dan is

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & (a-1)/c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} 1 & (d-1)/c \\ 0 & 1 \end{bmatrix}.$$

Als $b = 0$ en $c = 0$, dan is

$$g = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (1-a)/a & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix}.$$

Dit bewijst in alle gevallen dat $g \in \langle U, V \rangle$. Dus $G = \langle U^h \mid h \in G \rangle$. □

Lemma 2.2.14. *Als $|k| \geq 4$, dan is de groep $G = \mathsf{PSL}_2(k)$ perfect.*

Bewijs. Wegens Lemma 2.2.13 volstaat het te bewijzen dat $U \leq [G, G]$. Beschouw nu, voor elke $a \in k^\times$, het element $h_a = \left[\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right] \in G$. Dan is

$$h_a^{-1} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} h_a = \begin{bmatrix} 1 & a^2 b \\ 0 & 1 \end{bmatrix},$$

en bijgevolg bevat $[G, G]$ het element

$$h_a^{-1} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} h_a \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (1-a^2)b \\ 0 & 1 \end{bmatrix},$$

voor alle $a \in k^\times$ en alle $b \in k$. Aangezien $|k| \geq 4$, bestaat er een $a \in k^\times$ met $a^2 \neq 1$, en door b te laten variëren zien we dat inderdaad $U \leq [G, G]$. □

Stelling 2.2.15. *Als $|k| \geq 4$, dan is de groep $G = \mathsf{PSL}_2(k)$ enkelvoudig.*

Bewijs. Dit volgt nu onmiddellijk uit Lemma 2.2.13, Lemma 2.2.14, en de stelling van Iwasawa (Stelling 2.2.12). □

Opmerking 2.2.16. We hebben reeds gezien dat $\mathsf{PSL}_2(2) \cong \mathbf{S}_3$ en $\mathsf{PSL}_2(3) \cong \mathbf{A}_4$. Er zijn nog meer dergelijke *sporadische isomorfismen*, met name

$$\mathsf{PSL}_2(4) \cong \mathsf{PSL}_2(5) \cong \mathbf{A}_5;$$
$$\mathsf{PSL}_2(9) \cong \mathbf{A}_6;$$
$$\mathsf{PSL}_3(2) \cong \mathsf{PSL}_2(7);$$
$$\mathsf{PSL}_4(2) \cong \mathbf{A}_8.$$

We zullen deze isomorfismen niet aantonen, aangezien het bewijs ervan eerder technisch is.

2.3 De classificatie van de eindige enkelvoudige groepen

In 1892 bewees Otto Hölder dat elke niet-abelse eindige enkelvoudige groep een orde heeft die deelbaar is door ten minste vier (niet noodzakelijk verschillende) priemgetallen. Daarbij stelde hij openlijk de vraag of er een classificatie mogelijk zou zijn van alle eindige enkelvoudige groepen.

Het eerste belangrijke positieve resultaat in die richting kwam van Burnside, die in 1899 een classificatie kon geven van alle eindige enkelvoudige groepen waarvoor de centralisator van elke involutie een niet-triviale elementair abelse 2-groep is. Vanaf toen reeds werd duidelijk dat de structuur van de centralisatoren van involuties een cruciale rol speelt in het begrijpen van eindige enkelvoudige groepen.

Nadien werden uiteraard tal van belangrijke resultaten bewezen die ongetwijfeld een rol hebben gespeeld in het classificatieprogramma (waaronder de stelling van Feit en Thompson die we reeds eerder vermeld hebben), maar het echte startschot werd gegeven in 1972, toen Daniel Gorenstein een 16-stappenplan had uitgewerkt voor de classificatie. Gorenstein had een ongelooflijk sterk inzicht in dit —toen hopeloos uitziende— probleem, want de uiteindelijke classificatie blijkt dit 16-stappenplan zeer dicht te volgen. Dit is bewonderenswaardig, temeer daar op dat moment nog niet alle eindige enkelvoudige groepen waren ontdekt! (De laatste sporadische groep is de Janko groep $\mathbf{J}_4$, die in 1976 werd ontdekt.)

Sinds 2004 is het *eerste-generatie-bewijs* van de classificatie helemaal voltooid. Het geheel is echter verspreid over honderden artikels, met een totaal van tienduizenden bladzijden.

Er is dus nog steeds werk aan de gang om alles op een overzichtelijke manier neer te schrijven. Het totaal aantal pagina's van het zogenaamde *tweede-generatie-bewijs* wordt op ongeveer 5000 geschat, en zal over 11 boeken verspreid worden. De eerste 6 hiervan zijn reeds verschenen (Daniel Gorenstein, Richard Lyons en Ron Solomon, 1994, 1996, 1998, 1999, 2002, 2005). Boek 7 heeft lang op zich laten wachten, en zou op 1 maart 2018 moeten verschijnen. (Intussen is men natuurlijk ook al volop aan het werk aan de overige vier boeken.)

We hebben reeds een aantal klassen van enkelvoudige groepen ontmoet: de cyclische groepen van priemorde, de alternerende groepen, en de projectieve speciale lineaire groepen.

Behalve deze zijn er nog een vijftal klassen van eindige enkelvoudige groepen die te vinden zijn als deelgroep van $\mathsf{PGL}_n(q)$, voor oneindig veel waarden van n en voor alle priemmachten q, en een tiental klassen van eindige enkelvoudige groepen die betrekking hebben op $\mathsf{PGL}_n(q)$ voor een bepaalde n en variërende q. Deze groepen worden de *Chevalleygroepen* en de *verdraaide* of *getwiste Chevalleygroepen* genoemd. Ten slotte zijn er precies 26 sporadische gevallen die thuishoren in geen enkele van al deze oneindige klassen, maar die soms per drie à vier samengenomen zelf een kleine klasse vormen. Deze laatste staan bekend onder de naam *sporadische groepen*. De classificatie kan dus héél bondig als volgt worden samengevat.

Stelling 2.3.1. *Zij G een eindige enkelvoudige groep. Dan is G isomorf met ten minste één van de volgende:*

(a) *een cyclische groep van priemorde;*

(b) *een alternerende groep $\mathbf{A}_n$;*

(c) *een enkelvoudige groep van Lie-type, onderverdeeld in*

- *de klassieke groepen van Lie-type, met name de enkelvoudige groepen gerelateerd aan de speciale lineaire, unitaire, symplectische of orthogonale groepen over een eindig veld (type A_n, B_n, C_n, D_n);*
- *de exceptionele groepen van Lie-type (G_2, F_4, E_6, E_7, E_8);*
- *de getwiste groepen van Lie-type (${}^2A_n$, ${}^2D_n$, ${}^2E_6$, ${}^3D_4$, ${}^2B_2$, ${}^2G_2$, ${}^2F_4$);*

(d) *één van de* 26 *sporadische enkelvoudige groepen.*

Ter illustratie geven we nu een bondig overzicht van deze sporadische groepen.

Tussen 1861 en 1873 vond de Franse Wiskundige Emil Mathieu vijf eindige enkelvoudige groepen, die later de *Mathieu groepen* zouden genoemd worden.

Deze vijf groepen worden genoteerd als $\mathbf{M}_{11}$, $\mathbf{M}_{12}$, $\mathbf{M}_{22}$, $\mathbf{M}_{23}$ en $\mathbf{M}_{24}$. Elk van deze groepen $\mathbf{M}_n$ heeft een natuurlijke actie op n elementen, en werkt 3- 4- of 5-voudig transitief.

Alle andere sporadische groepen zijn ontdekt in de twintigste eeuw. De grootste van alle sporadische groepen is de groep $\mathbf{M}$, bekend onder de passende, welluidende naam *het monster (van Fischer)*, of *de vriendelijke reus (van Griess)*: deze groep heeft orde

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \approx 8 \cdot 10^{53}.$$

Vele andere sporadische groepen komen nu naar voor als compositiefactoren van centralisatoren van elementen van het Monster. Er zijn echter zes sporadische groepen die niets met het Monster te maken hebben, en deze zijn de *Janko groepen* $\mathbf{J}_1$, $\mathbf{J}_3$ en $\mathbf{J}_4$, en de groepen $\mathbf{Ru}$, $\mathbf{O'N}$ en $\mathbf{Ly}$, respectievelijk de *Rudvalis*, de *O'Nan*, en de *Lyons groep*. De naam van de sporadische groep verwijst telkens naar de persoon of personen die de betreffende groep voorspelden of tegelijk construeerden. In vele gevallen is dit echter verschillend van diegene die de groep effectief construeerde. Bijvoorbeeld, de Janko groepen $\mathbf{J}_3$ en $\mathbf{J}_4$ werden door Janko voorspeld, maar uiteindelijk geconstrueerd door respectievelijk Higman, McKay, en Norton, Parker, Benson, Conway, Thackray. De Rudvalis groep werd door Conway en Wales geconstrueerd, en de O'Nan groep door Sims, evenals de Lyons groep.

Sporadische groepen die naar voor komen als compositiefactor van de centralisator van een bepaald element van $\mathbf{M}$ worden soms genoteerd door $\mathbf{F}_n$, waarbij n een symbool is dat het betreffende element aangeeft, waarin meestal de orde van het element vervat zit. Bijvoorbeeld, trivialerwijs is $\mathbf{M} = \mathbf{F}_1$, omdat $\mathbf{M}$ de centralisator is van het eenheidselement in $\mathbf{M}$, en dit heeft orde 1. Zo heeft men nog de groepen $\mathbf{F}_{2+}$, $\mathbf{F}_{3|3}$, $\mathbf{F}_{5+}$, $\mathbf{F}_{7+}$, $\mathbf{F}_{2-}$ en $\mathbf{F}_{3+}$. Deze worden normaal genoteerd naar hun voorspeller (op uitzondering van de eerste), respectievelijk als $\mathbf{B}$ (het *Babymonster*, voorspeld door Fischer en geconstrueerd door Sims en Leon), $\mathbf{Th}$ (*Thompson groep*, geconstrueerd door Smith), $\mathbf{HN}$ (*Harada–Norton groep*, geconstrueerd door Smith), $\mathbf{He}$ (*Held groep*, geconstrueerd door Higman en McKay), $\mathbf{Co}_1$ (de eerste *Conway groep*, of Conway's 'dot one', geconstrueerd door Conway en Leech), en $\mathbf{Fi}'_{24}$ (een *Fischer groep*).

De andere acht sporadische groepen zijn allemaal quotiëntgroepen van deelgroepen van het Monster, maar werden niet op die manier voor het eerst geconstrueerd. Het betreft de *Hall–Janko groep* $\mathbf{J}_2 = \mathbf{HJ}$, de *Suzuki groep* $\mathbf{Suz}$, de *Higman–Sims groep* $\mathbf{HS}$, de *McLaughlin groep* $\mathbf{McL}$, de *Conway groepen* $\mathbf{Co}_2$ en $\mathbf{Co}_3$ (respectievelijk ook 'dot two' en 'dot three') en de *Fi-*

scher groepen $\mathbf{Fi}_{22}$ en $\mathbf{Fi}_{23}$. Deze laatste worden ook soms als $\mathbf{M}(22)$ en $\mathbf{M}(23)$ genoteerd.

We verwijzen de geïnteresseerde lezer naar de Wikipedia-pagina

`http://en.wikipedia.org/wiki/Classification_of_finite_simple_groups`

voor meer historische informatie over de classificatie van de eindige enkelvoudige groepen.

Ten slotte geven we een overzicht van de ordes van de sporadische enkelvoudige groepen.

Naam	Groep	Orde
Mathieu	$\mathbf{M}_{11}$	$2^4.3^2.5.11$
Mathieu	$\mathbf{M}_{12}$	$2^6.3^3.7.11$
Mathieu	$\mathbf{M}_{22}$	$2^7.3^2.5.7.11$
Mathieu	$\mathbf{M}_{23}$	$2^7.3^2.5.7.11.23$
Mathieu	$\mathbf{M}_{24}$	$2^{10}.3^3.5.7.11.23$
Janko	$\mathbf{J}_1$	$2^3.3.5.7.11.19$
Hall–Janko	$\mathbf{J}_2$	$2^7.3^3.5^2.7$
Janko	$\mathbf{J}_3$	$2^7.3^5.5.17.19$
Janko	$\mathbf{J}_4$	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$
Conway	$\mathbf{Co}_1$	$2^{21}.3^9.5^4.7^2.11.13.23$
Conway	$\mathbf{Co}_2$	$2^{18}.3^6.5^3.7.11.23$
Conway	$\mathbf{Co}_3$	$2^{10}.3^7.5^3.7.11.23$
Fischer	$\mathbf{Fi}_{22}$	$2^{17}.3^9.5^2.7.11.13$
Fischer	$\mathbf{Fi}_{23}$	$2^{18}.3^{13}.5^2.7.11.13.17.23$
Fischer	$\mathbf{Fi}_{24}$	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$
Higman–Sims	**HS**	$2^9.3^2.5^3.7.11$
MacLaughlin	**McL**	$2^7.3^6.5^3.7.11$
Suzuki	**Suz**	$2^{13}.3^7.5^2.7.11.13$
Lyons	**Ly**	$2^8.3^7.5^6.7.11.31.37.67$
Held	**He**	$2^{10}.3^3.5^2.7^3.17$
Rudvalis	**Ru**	$2^{14}.3^3.5^3.7.13.29$
O'Nan	**O'N**	$2^9.3^4.5.7^3.11.19.31$
Thompson	**Th**	$2^{15}.3^{10}.5^3.7^2.13.19.31$
Harada–Norton	**HN**	$2^{14}.3^6.5^6.7.11.19$
Baby Monster	**B**	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$
Monster	**M**	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$

Hoofdstuk

3 Velduitbreidingen

Een belangrijk deel van de theorie van de velden behandelt paren van velden $F \leq K$, het ene bevat in het andere. In tegenstelling tot de groepentheorie, waar de deelgroepen van een gegeven groep een belangrijke rol spelen, zullen we hier typisch het veld K als een *uitbreiding* van F beschouwen; het veld F wordt dus beschouwd als het "basisveld" of "grondveld", en K wordt in verband gebracht met F.

3.1 Algebraïsche en transcendente elementen

Definitie 3.1.1. Zij F een veld.

(i) Een *velduitbreiding*[1] van F is een veld K dat F bevat als deelveld. Het is gebruikelijk om de velduitbreiding te noteren als K/F als we het basisveld expliciet willen vermelden[2].

(ii) Zij K/F en L/F twee velduitbreidingen. Een *F-morfisme* van K naar L is een (ring)morfisme $\sigma\colon K \to L$ dat alle elementen van F fixeert. Merk op dat een ringmorfisme tussen velden steeds injectief is, omdat de kern een ideaal is, terwijl een veld geen echte niet-nul idealen heeft.

(iii) Een *F-isomorfisme* is een F-morfisme dat tevens een isomorfisme is. Twee velduitbreidingen K/F en L/F noemen we *F-isomorf* als er een F-isomorfisme van K naar L bestaat. Soms noteren we dit als $K \cong_F L$.

(iv) Op analoge wijze definiëren we F-monomorfismen, F-epimorfismen, F-endomorfismen en F-automorfismen. De groep van alle F-automorfismen zal een cruciale rol spelen in Hoofdstuk 4; zie Definitie 4.1.1.

Wanneer we een veld uitbreiden, maken we het volgende belangrijke onderscheid tussen de elementen die we toevoegen.

[1] In het Engels wordt het onderscheid gemaakt tussen "field extension" en "extension field", waarbij het eerste slaat op de extensie in zijn geheel (het paar K/F), terwijl het tweede slaat op het grotere veld (K). In het Nederlands wordt dit onderscheid zelden gemaakt, en we spreken in beide gevallen van een "velduitbreiding".

[2] Merk op dat het symbool "/" hier geen formele betekenis heeft, en enkel een afkorting is voor de uitdrukking "met betrekking tot", vaak kortweg uitgesproken als "over".

Definitie 3.1.2. Zij F een veld, en K/F een velduitbreiding. Een element $\alpha \in K$ wordt *algebraïsch* genoemd, als het de wortel is van een niet-nul polynoom met coëfficiënten in F. Een element dat niet algebraïsch is, noemen we *transcendent*.

Omdat F een veld is, geldt dat $\alpha \in K$ algebraïsch is als er een *monisch* polynoom $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ bestaat waarvan α een wortel is.

Opmerking 3.1.3. Het algebraïsch zijn van een element $\alpha \in K$ hangt uiteraard af van het basisveld F. Zo is het complexe getal $2\pi i$ algebraïsch over $\mathbb{R}$, maar transcendent over $\mathbb{Q}$. Merk ook op dat elk element $\alpha \in K$ algebraïsch is over K zelf, omdat het daar de wortel is van het polynoom $x - \alpha$.

Lemma 3.1.4. *Zij F een veld, K/F een velduitbreiding, en $\alpha \in K$. Beschouw het substitutiemorfisme*[3]

$$\Phi\colon F[x] \to K\colon f(x) \mapsto f(\alpha).$$

Dan geldt:

(i) *Het element α is transcendent over F als en slechts als Φ injectief is.*

(ii) *Als α algebraïsch is, dan is er een uniek monisch irreducibel polynoom $f \in F[x]$ zodat* $\ker(\Phi) = (f)$.

Bewijs. Veronderstel eerst dat α transcendent is. Dan is er geen enkel niet-nul polynoom $f \in F[x]$ waarvoor $f(\alpha) = 0$, en dus is $\ker(\Phi) = 0$.

Veronderstel nu dat α algebraïsch is; dan bestaat er een polynoom $p \in F[x]$ waarvoor $p(\alpha) = 0$, en bijgevolg is $\ker(\Phi) \neq 0$. Omdat $\ker(\Phi)$ een ideaal is in het hoofdideaaldomein $F[x]$, kunnen we $\ker(\Phi) = (f)$ schrijven voor een niet-nul monisch polynoom $f \in F[x]$. Als f reducibel zou zijn, stel $f = gh$, dan zou $g(\alpha)h(\alpha) = 0$, en omdat K een veld is zou hieruit volgen dat $g \in \ker(\Phi)$ of $h \in \ker(\Phi)$, strijdig. Dus f is irreducibel; het is bijgevolg het unieke monisch irreducibel polynoom in $\ker(\Phi)$. □

Definitie 3.1.5. Zij F een veld, K/F een velduitbreiding, en $\alpha \in K$ een algebraïsch element. Het uniek monisch irreducibel polynoom $f \in F[x]$ zodat $\ker(\Phi) = (f)$, noemen we *het irreducibel (monisch) polynoom voor α over F*, of ook wel *het minimaalpolynoom voor α over F*. We noteren het kortweg als $f = \min_F(\alpha)$.

[3]Zie "Algebra I". Het morfisme Φ is het unieke ringmorfisme van $F[x]$ naar K dat een uitbreiding is van de inclusie $\iota\colon F \hookrightarrow K$ en voldoet aan $\Phi(x) = \alpha$.

Opmerking 3.1.6. Als $f \in F[x]$ een irreducibel monisch polynoom is, dan geldt voor elke wortel α van f (in een velduitbreiding van F) dat $f = \min_F(\alpha)$. Deze observatie volgt trivialerwijze uit de definitie, maar zal heel vaak van pas komen.

Definitie 3.1.7. Zij F een veld, en K/F een velduitbreiding.

(i) Zij $\alpha_1, \ldots, \alpha_n \in K$. Het kleinste deelveld van K dat F en elke α_i bevat, noteren we als $F(\alpha_1, \ldots, \alpha_n)$.

(ii) Zij $\alpha_1, \ldots, \alpha_n \in K$. De kleinste deelring van K die F en elke α_i bevat, noteren we als $F[\alpha_1, \ldots, \alpha_n]$.

De ring $F[\alpha_1, \ldots, \alpha_n]$ en het veld $F(\alpha_1, \ldots, \alpha_n)$ zijn in sterke mate aan elkaar gerelateerd: het veld is het *breukenveld* van de ring. Hiermee bedoelen we het volgende.

Stelling 3.1.8. *Zij R een (commutatief) domein. Dan kunnen we R inbedden in een veld, d.w.z. er bestaat een ringmonomorfisme $\iota\colon R \to F$, waarbij F een veld is. Het kleinste veld F met deze eigenschap noemen we het* breukenveld van R, *en noteren we als* $\mathrm{Frac}(R)$ *of ook soms als* $\mathrm{Quot}(R)$.

Bewijs. We geven een expliciete constructie van het breukenveld van R. We laten ons hierbij inspireren door de gebruikelijke voorstelling van $\mathbb{Q}$ als breukenveld van $\mathbb{Z}$.

We definiëren een *breuk* in R als een symbool a/b, waarbij $a, b \in R$ met $b \neq 0$. We noemen twee breuken a/b en c/d *equivalent* als

$$ad = bc\,.$$

Uit het feit dat R een domein is leiden we eenvoudig af dat deze relatie inderdaad een equivalentierelatie is (doe dit zelf als oefening). We definiëren nu $\mathrm{Frac}(R)$ als de verzameling van de equivalentieklassen van deze relatie op de breuken in R. We leggen een optelling en een vermenigvuldiging op $\mathrm{Frac}(R)$ op de gebruikelijke manier:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}\,, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}\,.$$

Men gaat eenvoudig na dat deze bewerkingen goed gedefinieerd zijn, en dat $\mathrm{Frac}(R)$ hiermee de structuur van een veld krijgt. (Ga zelf de details na.) Ten slotte stellen we vast dat R ingebed kan worden in $\mathrm{Frac}(R)$ via het monomorfisme $\iota\colon R \to \mathrm{Frac}(R)\colon a \mapsto a/1$.

We tonen nu aan dat $\mathrm{Frac}(R)$ het kleinste veld is met deze eigenschappen. Zij dus F een ander veld waarvoor er een ringmonomorfisme $\kappa\colon R \to F$ is. Dan definiëren we een afbeelding

$$\lambda\colon \mathrm{Frac}(R) \to F\colon \frac{a}{b} \mapsto \kappa(a)\kappa(b)^{-1}.$$

Het is niet moeilijk om na te gaan dat λ opnieuw een ringmorfisme is. Aangezien $\ker(\lambda)$ een ideaal moet zijn, maar $\mathrm{Frac}(R)$ een veld is, moet λ noodzakelijkerwijze een monomorfisme zijn, en dus is $\mathrm{Frac}(R)$ isomorf met een deelveld van F. □

Voorbeelden 3.1.9. (1) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(2) Zij $R = \mathbb{Z}[i]$, de ring van gehelen van Gauss. Dan is

$$\mathrm{Frac}(R) = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

(3) Zij F een veld, en $R = F[x]$ de veeltermring in één veranderlijke over F. Dan is $\mathrm{Frac}(R) = F(x)$, het veld der *rationale functies in één veranderlijke*. Per definitie bestaat dit uit alle elementen van de vorm f/g, waarbij $f, g \in F[x]$, waarbij g niet het nul-polynoom is. Merk dus in het bijzonder op dat een rationale functie niet noodzakelijk in elk element van F kan geëvalueerd worden, omdat voor een specifieke $\alpha \in F$ wel $g(\alpha) = 0$ kan zijn.

Gevolg 3.1.10. *Zij F een veld, K/F een velduitbreiding, en $\alpha_1, \ldots, \alpha_n \in K$. Dan is $F(\alpha_1, \ldots, \alpha_n) = \mathrm{Frac}(F[\alpha_1, \ldots, \alpha_n])$.*

Bewijs. Dit volgt onmiddellijk uit de definities. □

Gevolg 3.1.11. *Zij F een veld, K/F een velduitbreiding, en $\alpha \in K$ een transcendent element. Dan is de afbeelding $\Phi\colon F[x] \to F[\alpha]$ een isomorfisme, en bijgevolg is $F(\alpha)$ isomorf met het veld der rationale functies $F(x)$.*

Bewijs. Omdat α transcendent is, is het substitutiemorfisme $\Phi\colon F[x] \to K$ injectief, en dus is $F[x]$ isomorf met $\mathrm{im}(\Phi)$. Omdat Φ de constanten fixeert en x op α afbeeldt, is $\mathrm{im}(\Phi)$ de kleinste deelring van K die F en α bevat, dus $\mathrm{im}(\Phi) = F[\alpha]$. De rest is nu duidelijk. □

Voorbeeld 3.1.12. De elementen π en e zijn transcendent over $\mathbb{Q}$. (We hebben dit niet aangetoond, en het bewijs hiervan is zeker niet evident.) Uit Gevolg 3.1.11 volgt dat de velden $\mathbb{Q}(\pi)$ en $\mathbb{Q}(e)$ isomorf zijn, waarbij het isomorfisme de elementen van $\mathbb{Q}$ fixeert en π op e afbeeldt.

De situatie is behoorlijk anders als α algebraïsch is.

Stelling 3.1.13. *Zij F een veld, K/F een velduitbreiding, en $\alpha \in K$ een algebraïsch element. Zij $f = \min_F(\alpha)$. De afbeelding*

$$\overline{\Phi}\colon F[x]/(f) \to F[\alpha]\colon g + (f) \mapsto g(\alpha)$$

is een isomorfisme, en $F[\alpha]$ is een veld. Dus $F(\alpha) = F[\alpha]$.

Bewijs. Het feit dat $\overline{\Phi}$ een isomorfisme is, volgt onmiddellijk uit de eerste isomorfiestelling, samen met het feit dat $\ker(\Phi) = (f)$ waarbij $f = \min_F(\alpha)$. Omdat f irreducibel is over F, is (f) een maximaal ideaal in $F[x]$, en bijgevolg is $F[x]/(f)$ een veld. De rest is nu duidelijk. □

Het is in het algemeen niet gemakkelijk om te zien of twee verschillende algebraïsche elementen $\alpha, \beta \in K$ toch F-isomorfe velden $F(\alpha), F(\beta)$ voortbrengen. Een nodige voorwaarde is wel dat de graad van hun irreducibele veeltermen moet gelijk zijn.

Lemma 3.1.14. *Zij F een veld, K/F een velduitbreiding, en $\alpha \in K$ een algebraïsch element. Zij $f = \min_F(\alpha)$, en stel $\deg(f) = n$. Dan is $(1, \alpha, \ldots, \alpha^{n-1})$ een basis voor $F[\alpha]$ beschouwd als vectorruimte over F.*

Bewijs. We tonen eerst aan dat $(1, \alpha, \ldots, \alpha^{n-1})$ een voortbrengende verzameling is. Stel dus $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ met $a_i \in F$, zij $g \in F[\alpha]$ willekeurig, en stel $g = b_k\alpha^k + \cdots + b_1\alpha + b_0$ met $b_i \in F$. In $F[\alpha]$ geldt $f(\alpha) = 0$, en dus

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0\,.$$

Door in elke term $b_k\alpha^k$ van g met $k \geq n$ bovenstaande vergelijking te substitueren, verkrijgen we uiteindelijk een voorstelling van g als een lineaire combinatie van de elementen $1, \alpha, \ldots, \alpha^{n-1}$.

We tonen vervolgens aan dat $(1, \alpha, \ldots, \alpha^{n-1})$ een lineair onafhankelijke verzameling is. Veronderstel dus dat er een niet-triviale lineaire combinatie is van deze elementen die nul is, i.e.

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0\,.$$

Dan is het polynoom $h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ een niet-nul polynoom waarvan α een wortel is, en dus $h \in \ker(\Phi)$ met $\deg(h) < n$, strijdig met het feit dat $\ker(\Phi) = (f)$. □

Deze voorwaarde is zeker niet voldoende; zo is bijvoorbeeld $\mathbb{Q}(i)$ niet isomorf met $\mathbb{Q}(\sqrt{2})$, hoewel beide elementen een irreducibel polynoom van

graad 2 hebben. Anderzijds kan het wel gebeuren dat verschillende polynomen isomorfe velden geven. Bijvoorbeeld, als α een wortel is van $x^3 - x + 1$ in $\mathbb{C}$, dan is $\beta = \alpha^2$ een wortel van $x^3 - 2x^2 + x - 1$, en de velden $\mathbb{Q}(\alpha)$ en $\mathbb{Q}(\beta)$ zijn gelijk.

Wat we wel gemakkelijk kunnen beschrijven, zijn de omstandigheden waarin er een isomorfisme is van $F(\alpha)$ naar $F(\beta)$ dat F fixeert en tegelijk α op β afbeeldt. De volgende stelling is van fundamenteel belang voor het begrijpen van velduitbreidingen.

Stelling 3.1.15. *Zij F een veld, en zij K/F en L/F twee velduitbreidingen. Zij $\alpha \in K$ en $\beta \in L$ algebraïsche elementen. Dan is er een F-isomorfisme*

$$\sigma\colon F(\alpha) \to F(\beta)$$

dat α op β afbeeldt, als en slechts als $\min_F(\alpha) = \min_F(\beta)$.

Bewijs. Veronderstel eerst dat f het monisch irreducibel polynoom is voor zowel α als β. Dan volgt uit Stelling 3.1.13 dat er isomorfismen

$$\overline{\Phi}_\alpha\colon F[x]/(f) \to F[\alpha]\colon g + (f) \mapsto g(\alpha) \text{ en}$$
$$\overline{\Phi}_\beta\colon F[x]/(f) \to F[\beta]\colon g + (f) \mapsto g(\beta)$$

zijn, en de samenstelling $\sigma = \overline{\Phi}_\beta \circ \overline{\Phi}_\alpha^{-1}$ voldoet aan de gestelde voorwaarden.

Omgekeerd, zij σ zoals vooropgegeven. Dan geldt voor elke $f \in F[x]$ dat $\sigma(f(\alpha)) = f(\beta)$, en in het bijzonder is $f(\alpha) = 0$ als en slechts als $f(\beta) = 0$. Bijgevolg hebben α en β hetzelfde monisch irreducibel polynoom. □

Voorbeeld 3.1.16. Het polynoom $x^3 - 2$ is irreducibel over $\mathbb{Q}$. Zij $\alpha = \sqrt[3]{2}$ de reële wortel van dit polynoom, en $\zeta = e^{2\pi i/3}$ een complexe derdemachtswortel van 1. De drie complexe wortels van $x^3 - 2$ zijn α, $\zeta\alpha$ en $\zeta^2\alpha$. Er is dus een isomorfisme

$$\sigma\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\zeta\alpha)$$

dat α op $\zeta\alpha$ afbeeldt. In dit geval zijn de elementen van $\mathbb{Q}(\alpha)$ reële getallen, terwijl $\mathbb{Q}(\zeta\alpha)$ geen deelveld van $\mathbb{R}$ is. Het is dus belangrijk om ons niet te focussen op deze velden als deelvelden van $\mathbb{C}$, maar om enkel te kijken naar hun interne algebraïsche structuur.

Opmerking 3.1.17. We zullen bij onze studie van splijtvelden de volgende lichte veralgemening van Stelling 3.1.15 nodig hebben.

> *Zij F en F' twee velden en $\theta\colon F \to F'$ een isomorfisme, en zij K/F en L/F' twee velduitbreidingen. Zij $\alpha \in K$ en $\beta \in L$ algebraïsche elementen. Dan is er een isomorfisme van velden*
>
> $$\sigma\colon F(\alpha) \to F'(\beta)$$

zodat de restrictie $\sigma_{|F}$ gelijk is aan θ en zodat $\sigma(\alpha) = \beta$, als en slechts als $\min_F(\alpha)$ door θ wordt afgebeeld[4] *op* $\min_{F'}(\beta)$.

Het bewijs hiervan is volledig analoog aan het bewijs van Stelling 3.1.15 (werk zelf de details uit als oefening).

3.2 De graad van een velduitbreiding

Een velduitbreiding K van een veld F kunnen we steeds bekijken als een F-vectorruimte, waarbij de optelling gewoon de optelling in K is, en waarbij de scalaire vermenigvuldiging wordt gegeven door de vermenigvuldiging in het grotere veld K uit te voeren.

Definitie 3.2.1. Zij F een veld, en K/F een velduitbreiding. De *graad* van K/F definiëren we als

$$[K : F] := \dim_F K\,,$$

de dimensie van K als vectorruimte over het veld F. We noemen een velduitbreiding *eindig* als zijn graad eindig is. Een velduitbreiding van graad 2 noemen we ook een *kwadratische velduitbreiding*, en een van graad 3 een *kubische velduitbreiding*.

Voorbeeld 3.2.2. Voor het veld $\mathbb{C}$ is $(1, i)$ een basis over $\mathbb{R}$, dus $[\mathbb{C} : \mathbb{R}] = 2$.

Opmerking 3.2.3. De benaming "graad" komt van het geval waarin $K = F(\alpha)$ voortgebracht is door één algebraïsch element α. In dat geval is de graad van de velduitbreiding immers precies de graad van $\min_F(\alpha)$ (zie Lemma 3.1.14), en we noemen dit ook de *graad van* α. Als α transcendent is over F, dan is $[F(\alpha) : F] = \infty$, en we zeggen dan ook dat de graad van α gelijk is aan ∞.

Een belangrijke eigenschap van de graad is de multiplicativiteit in een *toren* van velden.

Stelling 3.2.4. *Zij $F \leq K \leq L$ velden. Dan is $[L : F] = [L : K][K : F]$.*

Bewijs. Zij $\mathbf{B} = (y_1, \ldots, y_n)$ een basis voor L als K-vectorruimte, en zij $\mathbf{C} = (x_1, \ldots, x_m)$ een basis voor K als F-vectorruimte; dan is $[L : K] = n$ en $[K : F] = m$. Dan is $(x_1y_1, \ldots, x_iy_j, \ldots, x_my_n)$ een basis voor L als F-vectorruimte (toon dit zelf aan als oefening). Hieruit volgt dat inderdaad

[4] Als $\theta\colon F \to F'$ een isomorfisme is van velden, dan zullen we het overeenkomstig ringisomorfisme $F[x] \to F'[x]$ dat een uitbreiding is van θ en x op x afbeeldt, eveneens noteren als θ, zonder dit expliciet te vermelden.

$[L : F] = mn$. Merk op dat deze redenering ook geldt als m of n oneindig is. □

Een interessant gevolg hiervan is het volgende.

Gevolg 3.2.5. *Zij F een veld, en K/F een velduitbreiding van graad $n < \infty$. Dan is elke $\alpha \in K$ algebraïsch over F, en* $\deg(\alpha) \mid n$.

Bewijs. Dit volgt onmiddellijk door Stelling 3.2.4 toe te passen op de toren $F \leq F(\alpha) \leq K$. □

Voorbeelden 3.2.6. (1) De velduitbreiding $\mathbb{C}/\mathbb{R}$ heeft graad 2. Beschouw nu een willekeurig irreducibel polynoom f in $\mathbb{R}[x]$. Uit de grondstelling van de algebra (zie Gevolg 4.10.3) weten we dat f een wortel $\alpha \in \mathbb{C}$ heeft, en uit Gevolg 3.2.5 volgt dat $\deg(\alpha) = 1$ of 2. Dus is $\deg(f) = \deg(\alpha) =$ 1 of 2, en we bekomen dus het (welbekende) feit dat elk irreducibel polynoom in $\mathbb{R}[x]$ graad 1 of 2 heeft.

(2) Zij $\alpha = \sqrt[3]{2}$ en $\beta = \sqrt[4]{5}$, en beschouw het veld $L = \mathbb{Q}(\alpha, \beta)$. We beweren dat $[L : \mathbb{Q}] = 12$. Inderdaad, merk op dat $\deg_{\mathbb{Q}}(\alpha) = 3$ en $\deg_{\mathbb{Q}}(\beta) = 4$, zodat uit Gevolg 3.2.5 volgt dat $3 \mid [L : \mathbb{Q}]$ en $4 \mid [L : \mathbb{Q}]$. Anderzijds is de graad van β over $\mathbb{Q}(\alpha)$ ten hoogste 4, omdat β een wortel is van het polynoom $x^4 - 5 \in \mathbb{Q}(\alpha)[x]$. Uit de toren $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\alpha, \beta) = L$ volgt dus dat $[L : \mathbb{Q}] \leq 12$. We besluiten dus dat $[L : \mathbb{Q}] = 12$.

We geven een aantal belangrijke gevolgen van de multiplicatieve eigenschap van graden.

Lemma 3.2.7. *Zij F een veld, en K/F een velduitbreiding. Veronderstel dat $\alpha_1, \ldots, \alpha_n \in K$ algebraïsche elementen zijn over F. Dan is $F(\alpha_1, \ldots, \alpha_n)/F$ een eindige velduitbreiding.*

Bewijs. Beschouw de toren

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n)\,.$$

Voor elke i is het element α_{i+1} algebraïsch over $F(\alpha_1, \ldots, \alpha_i)$ omdat het algebraïsch is over F. Wegens Opmerking 3.2.3 is dan elke uitbreiding tussen twee opeenvolgende velden in de toren eindig, en uit Stelling 3.2.4 volgt dat ook $[F(\alpha_1, \ldots, \alpha_n) : F]$ eindig is. □

Stelling 3.2.8. *Zij F een veld, en K/F een velduitbreiding. De elementen van K die algebraïsch zijn over F, vormen een deelveld van K.*

Bewijs. Zij $\alpha, \beta \in K$ willekeurige elementen die algebraïsch zijn over F. Uit Lemma 3.2.7 weten we dat $F(\alpha, \beta)/F$ een eindige velduitbreiding is, en Wegens Gevolg 3.2.5 zijn dan alle elementen van $F(\alpha, \beta)$ algebraïsch over F. Hieruit volgt in het bijzonder dat de elementen $\alpha + \beta$, $\alpha\beta$, $-\alpha$ en α^{-1} (als $\alpha \neq 0$) algebraïsch zijn over F. □

Opmerking 3.2.9. Ondanks de eenvoud van dit bewijs, is het beduidend meer werk om voor gegeven algebraïsche elementen $\alpha, \beta \in K$ een expliciet polynoom te vinden waar $\alpha + \beta$ of $\alpha\beta$ een wortel van is (en het is nog moeilijker om een dergelijk irreducibel polynoom te vinden).

Beschouw bijvoorbeeld $a, b \in F$ en $\alpha = \sqrt{a}$, $\beta = \sqrt{b}$, en stel $\gamma = \alpha + \beta$. Dan is γ een wortel van het polynoom $x^4 - 2(a+b)x^2 + (a-b)^2$. Afhankelijk van het veld F en van de waarden voor a en b zal dit polynoom al dan niet irreducibel zijn.

Definitie 3.2.10. Zij F een veld, en K/F een velduitbreiding. Als alle elementen van K algebraïsch zijn over F, dan noemen we K/F een *algebraische uitbreiding*, en we zeggen ook nog dat K *algebraïsch is over* F.

Merk op dat wegens Gevolg 3.2.5 een eindige velduitbreiding steeds algebraïsch is, maar het omgekeerde is niet waar. Beschouw bijvoorbeeld de (niet-algebraïsche) velduitbreiding $\mathbb{C}/\mathbb{Q}$. Het deelveld van $\mathbb{C}$ bestaande uit alle elementen die algebraïsch zijn over $\mathbb{Q}$ (zie Stelling 3.2.8) is een algebraische uitbreiding van $\mathbb{Q}$ die niet eindig is.

Stelling 3.2.11. *Zij $F \leq K \leq L$ velden. Als L algebraïsch is over K, en K algebraïsch is over F, dan is ook L algebraïsch over F.*

Bewijs. Zij $\alpha \in L$; we moeten aantonen dat α algebraïsch is over F. Omdat α algebraïsch is over K, voldoet het aan een vergelijking van de vorm

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0\,,$$

met $c_i \in K$; het element α is dan algebraïsch over $F(c_0, \ldots, c_{n-1})$. Merk op dat elke c_i algebraïsch is over F omdat K/F algebraïsch is. Beschouw nu de toren

$$F \leq F(c_0, \ldots, c_{n-1}) \leq F(c_0, \ldots, c_{n-1}, \alpha)\,.$$

Uit Lemma 3.2.7 weten we dat $[F(c_0, \ldots, c_{n-1}) : F]$ eindig is, en omdat α algebraïsch is over $F(c_0, \ldots, c_{n-1})$, is ook $[F(c_0, \ldots, c_{n-1}, \alpha) : F(c_0, \ldots, c_{n-1})]$ eindig. Uit Stelling 3.2.4 volgt dus dat $[F(c_0, \ldots, c_{n-1}, \alpha) : F] < \infty$, zodat, wegens Gevolg 3.2.5, α algebraïsch is over F. □

3.3 Splijtvelden

Definitie 3.3.1. Zij F een veld, en f een niet-nul polynoom in $F[x]$. We zeggen dat f *splijt over* F (of *gespleten is over* F) als elke irreducibele deler van f graad 1 heeft. (In het bijzonder splijt elk niet-nul constant polynoom.) Anders gezegd, f splijt over F als het de vorm

$$f(x) = \beta \prod_{i=1}^{\deg(f)} (x - \alpha_i)$$

heeft, waarbij β en elke α_i in F liggen.

Voorbeeld 3.3.2. Het polynoom $x^4 - 1$ splijt niet over $\mathbb{Q}$, omdat het een irreducibele factor $x^2 + 1$ heeft van graad 2. Ditzelfde polynoom splijt wel over $\mathbb{C}$, aangezien het factoriseert in lineaire factoren als

$$x^4 - 1 = (x + 1)(x - 1)(x + i)(x - i).$$

In feite is elk niet-nul polynoom in $\mathbb{C}[x]$ gespleten. Dit feit, dat gekend staat als de grondstelling van de algebra, zullen we bewijzen in Gevolg 4.10.3 verderop.

Als een polynoom niet splijt, kunnen we trachten het veld uit te breiden, om op die manier het polynoom te doen splijten. Dit brengt ons tot het concept van een splijtveld.

Definitie 3.3.3. Zij F een veld, en f een niet-nul polynoom in $F[x]$. Een *splijtveld van* f *over* F is een velduitbreiding K van F zodat f splijt over K, stel

$$f(x) = \beta \prod_{i=1}^{\deg(f)} (x - \alpha_i),$$

en zodat de wortels α_i het veld K voortbrengen over F, i.e.

$$K = F(\alpha_1, \ldots, \alpha_{\deg(f)}).$$

(Deze laatste voorwaarde drukt in feite uit dat K een *minimale* velduitbreiding is waarover f splijt.)

Opmerking 3.3.4. Merk op dat een splijtveld E van een polynoom f over F dus steeds een uitbreiding is van *eindige graad* over F, en in het bijzonder dus steeds een *algebraïsche* velduitbreiding is van F.

We zullen dadelijk aantonen dat elk niet-nul polynoom f een splijtveld heeft. Omwille van het volgend lemma zal het volstaan om aan te tonen dat we een velduitbreiding vinden waarover f splijt.

Lemma 3.3.5. *Zij F een veld, en f een niet-nul polynoom in $F[x]$. Zij verder L/F een velduitbreiding zodat f splijt over L. Dan bevat L een uniek splijtveld E voor f over F.*

Bewijs. Stel $n = \deg f$. Omdat f splijt over L is

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

waarbij alle $\alpha_i \in L$, en waarbij $\beta \in F$ omdat $f \in F[x]$. Het deelveld $E = F(\alpha_1, \ldots, \alpha_n)$ van L is dan het gezochte (uniek) splijtveld voor f bevat in L. □

Stelling 3.3.6. *Zij F een veld, en f een niet-nul polynoom in $F[x]$. Dan bestaat er een splijtveld voor f over F.*

Bewijs. We bewijzen per inductie op $\deg(f)$ dat er een velduitbreiding van F bestaat waarover f splijt; wegens Lemma 3.3.5 bewijst dit dan ook het bestaan van een splijtveld voor f over F. De inductiebasis $\deg(f) = 0$ is triviaal; stel dus $\deg(f) \geq 1$. Kies een irreducibele factor g van f, en beschouw de velduitbreiding $F_1 = F[x]/(g)$ van F. (Dit is een veld omdat (g) een maximaal ideaal is in $F[x]$.) Dan heeft g een wortel α in F_1, namelijk het element $\alpha = x + (g) \in F_1$. Over F_1 factoriseert f dus als $f(x) = (x - \alpha)h(x)$ voor een zekere $h \in F_1[x]$. Door de inductiehypothese toe te passen op $h \in F_1[x]$ vinden we het gezochte splijtveld. □

Opmerking 3.3.7. Zij F een veld, en f een irreducibel polynoom in $F[x]$. Dan is het veld $K = F[x]/(f)$ *niet* steeds een splijtveld voor f over F. (Dit is een vaak gemaakte fout!) Een eenvoudig voorbeeld wordt gegeven door het polynoom $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, dat we reeds hebben ontmoet in Voorbeeld 3.1.16 en dat nog uitgebreid besproken wordt in Voorbeeld 4.1.17 verderop.

We bewijzen nu de uniciteit. Het volgend lemma bevat de essentie van het bewijs.

Lemma 3.3.8. *Zij F een veld, en f een niet-nul polynoom in $F[x]$. Zij E een splijtveld van f over F, en zij $\theta\colon F \to M$ een (ring)morfisme[5] van velden. Dan breidt θ uit tot een morfisme $E \to M$ als en slechts als $\theta(f)$ splijt over M.*

[5]Merk nogmaals op dat een ringmorfisme tussen velden steeds injectief is.

Bewijs. We zullen het veld $\theta(F)$ noteren als F'; merk op dat $F \cong F'$.

Veronderstel eerst dat θ uitbreidt tot een morfisme $E \to M$ (dat we eveneens als θ zullen noteren). Dan is $\theta(E)$ een splijtveld van $\theta(f)$ over F', en in het bijzonder splijt $\theta(f)$ over M.

Veronderstel omgekeerd dat $\theta(f)$ splijt over M. We bewijzen per inductie op $[E : F]$ dat θ uitbreidt tot een morfisme $E \to M$. (Merk op dat $[E : F]$ eindig is.) Indien $[E : F] = 1$, dan valt er niks te bewijzen.

Veronderstel dus $[E : F] > 1$. Dan splijt f niet over F, en dus kunnen we een irreducibele factor $g \in F[x]$ van f kiezen met $\deg(g) \geq 2$. Aangezien f splijt over E, zal ook g splijten over E, en we kiezen een wortel $\alpha \in E$ van g. Anderzijds splijt $\theta(f)$, en dus ook $\theta(g)$, over M per veronderstelling, en we kiezen een wortel $\beta \in M$ van $\theta(g)$. Merk op dat $\theta(g)$ irreducibel is over F'. Dan is $\min_F(\alpha) = g$ en $\min_{F'}(\beta) = \theta(g)$. Wegens Opmerking 3.1.17 vinden we een isomorfisme $\sigma\colon F(\alpha) \to F'(\beta)$ met $\sigma_{|F} = \theta$ en $\sigma(\alpha) = \beta$. De samenstelling van σ met de inclusie $\iota\colon F'(\beta) \to M$ levert dus een morfisme $\sigma\colon F(\alpha) \to M$ dat een uitbreiding is van θ.

Merk nu op dat $[E : F] = [E : F(\alpha)][F(\alpha) : F] > [E : F(\alpha)]$ wegens Stelling 3.2.4 en wegens het feit dat $\deg(\alpha) = \deg(g) > 1$. We kunnen dus de inductiehypothese toepassen om te besluiten dat σ uitbreidt tot een morfisme $\tau\colon E \to M$, en aangezien σ een uitbreiding was van θ is ook τ een uitbreiding van θ, zoals gewenst. □

Stelling 3.3.9. *Zij F een veld, en f een niet-nul polynoom in $F[x]$. Veronderstel dat E en M twee splijtvelden zijn voor f over F. Dan zijn E en M F-isomorf.*

Bewijs. Beschouw de natuurlijke inclusie $\iota\colon F \to M$. Aangezien $\iota(f) = f$ splijt over M, en E een splijtveld is van f over F, kunnen we Lemma 3.3.8 toepassen, en we besluiten dat ι uitbreidt tot een F-morfisme $\tau\colon E \to M$. Aangezien f splijt over E, zal $f = \tau(f)$ splijten over $\tau(E)$, maar aangezien M een splijtveld is impliceert dit dat $\tau(E) = M$. Dus τ is een surjectief morfisme van velden, en is bijgevolg een isomorfisme. □

We vermelden nog een ander gevolg van Lemma 3.3.8, dat aantoont dat velduitbreidingen die optreden als splijtveld van een polynoom bijzondere eigenschappen hebben. We zullen dit fenomeen later dieper bestuderen; zie bijvoorbeeld Stelling 4.2.4.

Gevolg 3.3.10. *Zij F een veld, en f een niet-nul polynoom in $F[x]$. Zij E een splijtveld van f over F, en zij $F \leq K \leq E$. Dan breidt elk F-morfisme $\theta\colon K \to E$ uit tot een F-automorfisme van E.*

Bewijs. Door Lemma 3.3.8 toe te passen met $M = E$ en K in plaats van F, volgt reeds dat θ uitbreidt tot een endomorfisme $\sigma\colon E \to E$. Aangezien $[E : F]$ eindig is, zal het injectief F-morfisme σ een F-automorfisme zijn. $\square$

Voor het vervolg zal het ook zinvol zijn om controle te hebben over meervoudige wortels van een polynoom.

Lemma 3.3.11. *Zij F een veld, $f \in F[x]$, en $\alpha \in F$ een wortel van f. Dan is α een meervoudige wortel, hetgeen wil zeggen dat $(x-\alpha)^2 \mid f$, als en slechts als $f(\alpha) = f'(\alpha) = 0$, waarbij f' de (formele) afgeleide van f is.*

Bewijs. Als α een wortel is van f, dan is $f(x) = (x-\alpha)g(x)$ voor een zekere $g \in F[x]$; α is een meervoudige wortel van f als en slechts als α een wortel is van g. Uit de productregel voor afleiden volgt

$$f'(x) = (x-\alpha)g'(x) + g(x)\,;$$

door $x = \alpha$ te stellen zien we dat $f'(\alpha) = 0$ als en slechts als $g(\alpha) = 0$. $\square$

3.4 Algebraïsch gesloten velden

Gegeven een veld F vragen we ons af of er een velduitbreiding E/F bestaat zodat *elk* niet-nul polynoom $f \in F[x]$ splijt over E. Dit leidt tot de volgende definities.

Definitie 3.4.1. (i) Een veld E wordt *algebraïsch gesloten* genoemd als elk niet-nul polynoom $f \in E[x]$ splijt.

(ii) Een velduitbreiding E van F wordt een *algebraïsche sluiting* van F genoemd, als E/F algebraïsch is, en elk niet-nul polynoom $f \in F[x]$ splijt over E.

Een veld is dus algebraïsch gesloten als en slechts als het een algebraïsche sluiting is van zichzelf.

Deze twee begrippen zijn, niet geheel verwonderlijk, zeer nauw aan elkaar gerelateerd, maar zoals we verder zullen vaststellen zijn er toch soms subtiele maar belangrijke verschillen. We beginnen met een resultaat dat het verband duidelijk maakt.

Lemma 3.4.2. *Zij E/F een algebraïsche velduitbreiding. Dan zijn de volgende uitspraken equivalent:*

(a) *E is algebraïsch gesloten;*

(b) *E is een algebraïsche sluiting van F;*

(c) *er bestaat geen algebraïsche velduitbreiding L/F met $E \lneq L$;*

(d) *er bestaat geen algebraïsche velduitbreiding L/E met $L \neq E$.*

Bewijs. (a) $\Rightarrow$ (b). Dit is evident, want als elk niet-nul polynoom $f \in E[x]$ splijt over E, dan splijt ook elk niet-nul polynoom $f \in F[x]$ over E.

(b) $\Rightarrow$ (c). Zij L/F een algebraïsche velduitbreiding met $E \leq L$; we moeten bewijzen dat $L = E$. Zij dus $\alpha \in L$ willekeurig. Per veronderstelling is α algebraïsch over F; beschouw dus $f = \min_F(\alpha)$. Omdat E een algebraïsche sluiting is van F zal f splijten over E, en dus is $\alpha \in E$. Dus $L = E$.

(c) $\Rightarrow$ (d). Zij L/E een algebraïsche velduitbreiding; we moeten bewijzen dat $L = E$. Omdat ook E/F een algebraïsche velduitbreiding is, volgt echter uit Stelling 3.2.11 dat ook L/F een algebraïsche velduitbreiding is, met $E \leq L$, en per veronderstelling moet dan $L = E$.

(d) $\Rightarrow$ (a). Zij f een willekeurig niet-nul polynoom in $E[x]$, en zij L/E een splijtveld voor f over E. Dan is L/E een algebraïsche velduitbreiding, zodat per veronderstelling $L = E$. Dus f splijt over E, en omdat f willekeurig was besluiten we dat E algebraïsch gesloten is. □

Gevolg 3.4.3. *Zij L/F een velduitbreiding, en veronderstel dat L algebraïsch gesloten is. Stel*

$$E = \{\alpha \in L \mid \alpha \text{ is algebraïsch over } F\}.$$

Dan is E de unieke algebraïsche sluiting van F die bevat is in L.

Bewijs. Wegens Stelling 3.2.8 is E een veld, en uiteraard is E/F dan een algebraïsche velduitbreiding. Als $f \in F[x]$ een willekeurig niet-nul polynoom is, dan splijt f over L, en dus bevat L een splijtveld K voor f over F (zie Lemma 3.3.5). Maar dan is $K \leq E$, en dus splijt f ook over E. Aangezien f willekeurig was, toont dit aan dat E een algebraïsche sluiting is van F.

Veronderstel nu dat $E' \leq L$ ook een algebraïsche sluiting is van F. Dan is uiteraard elk element van E' algebraïsch over F, en dus $E' \leq E$. Maar dan is E/E' een algebraïsche velduitbreiding, en uit Lemma 3.4.2 volgt dan dat $E = E'$. □

Voorbeeld 3.4.4. Beschouw de velduitbreiding $\mathbb{C}/\mathbb{Q}$. Het veld $\mathbb{C}$ is algebraisch gesloten (zie Gevolg 4.10.3). Het deelveld van $\mathbb{C}$ bestaande uit alle elementen van $\mathbb{C}$ die algebraïsch zijn over $\mathbb{Q}$, wordt genoteerd als $\overline{\mathbb{Q}}$, en wordt het *veld van de algebraïsche getallen* genoemd. Dit veld is het kleinste

algebraïsch gesloten veld van karakteristiek 0. Merk op dat $\overline{\mathbb{Q}}$ veel kleiner is dan $\mathbb{C}$, want $\mathbb{C}$ is overaftelbaar terwijl $\overline{\mathbb{Q}}$ aftelbaar is.

Een ander eenvoudig criterium is het volgende.

Stelling 3.4.5. *Zij E een veld met de eigenschap dat elk polynoom $f \in E[x]$ met $\deg(f) \geq 1$ ten minste 1 wortel heeft in E. Dan is E algebraïsch gesloten.*

Bewijs. Zij $0 \neq f \in E[x]$. We moeten bewijzen dat f splijt, en dus beschouwen we een willekeurige irreducibele factor g van f in $E[x]$, en we tonen aan dat $\deg(g) = 1$. Inderdaad, per veronderstelling heeft g een wortel $\alpha \in E$, en dus is $(x - \alpha) \mid g(x)$ in $E[x]$. Omdat g irreducibel is, volgt hieruit echter dat g een scalair veelvoud is van $(x - \alpha)$, en dus dat $\deg(g) = 1$, wat we moesten bewijzen. □

Met het oog op het sterke verband tussen algebraïsch gesloten velden en algebraïsche sluitingen kunnen we ons afvragen of voorgaande stelling zich laat veralgemenen tot algebraïsche sluitingen. Dit blijkt te kloppen, maar het bewijs van deze uitspraak is verrassend moeilijk en vereist het nodige inzicht in de theorie van separabele en inseparable velduitbreidingen (zie later).

Stelling 3.4.6. *Zij E/F een algebraïsche velduitbreiding met de eigenschap dat elk polynoom $f \in F[x]$ met $\deg(f) \geq 1$ ten minste 1 wortel heeft in E. Dan is E een algebraïsche sluiting van F.*

Bewijs. Zie Stelling 4.8.19 verderop (p. 89). □

We willen nu aantonen dat elk veld een algebraïsche sluiting heeft. Niet geheel verwonderlijk hangt deze uitspraak af van het keuze-axioma, of equivalent, van het lemma van Zorn. We zullen een constructie geven die terugvalt op het bestaan van maximale idealen in commutatieve ringen, een feit dat we in de cursus "Algebra I" hebben aangetoond (met behulp van het lemma van Zorn!).

Stelling 3.4.7. *Zij F een willekeurig veld. Dan bestaat er een algebraïsche sluiting van F.*

Bewijs. Beschouw de verzameling S bestaande uit alle polynomen $f \in F[x]$ met $\deg(f) \geq 1$. Zij R de polynomenring

$$R = F\big[X_f \mid f \in S\big],$$

i.e. een polynomenring met één variabele voor elk element in S. Beschouw het ideaal I van R voortgebracht door de polynomen $f(X_f)$, i.e.

$$I = \big\langle f(X_f) \mid f \in S \big\rangle.$$

Dan is I een echt ideaal. Inderdaad, veronderstel dat $1 \in I$ zou zijn; dan bestaan er $f_1, \ldots, f_n \in S$ en veeltermen $g_1, \ldots, g_n \in R$ zodat

$$1 = g_1(X)f_1(X_{f_1}) + \cdots + g_n(X)f_n(X_{f_n}),$$

waarbij X een afkorting is voor $(X_f \mid f \in S)$. Beschouw nu een splijtveld L/F voor het polynoom $\prod_i f_i$, en kies voor elke f_i een wortel $\alpha_i \in L$. Door voor elke variabele X_{f_i} de corresponderende α_i te substitueren, volgt er dat $1 = 0$, en deze contradictie toont aan dat I een echt ideaal is.

Bijgevolg kunnen we een maximaal ideaal M in R vinden dat I bevat (zie "Algebra I"). De quotiëntring $E_1 = R/M$ is dan een veld (zie opnieuw "Algebra I"), en duidelijkerwijze heeft elke veelterm $f \in F[x]$ met $\deg(f) \geq 1$ een wortel in E_1, namelijk de nevenklasse $X_f \mod M$.

We kunnen dit proces nu itereren, en we bekomen dan een keten van velduitbreidingen

$$F = E_0 \leq E_1 \leq E_2 \leq \cdots$$

waarbij elke veelterm in $E_i[x]$ van graad ≥ 1 een wortel heeft in E_{i+1}.

Beschouw nu $E = \cup_i E_i$, en merk op dat E opnieuw een veld is. Dan is E algebraïsch gesloten. Inderdaad, zij $g \in E[x]$ willekeurig met $\deg(g) \geq 1$; dan is er een E_ℓ zodat $g \in E_\ell[x]$, zodat per constructie g een wortel heeft in $E_{\ell+1}$, en bijgevolg in E.

Het resultaat volgt nu uit Stelling 3.4.5 en Gevolg 3.4.3. □

Opmerking 3.4.8. Uit Stelling 3.4.6 volgt dat in het voorgaand bewijs in feite reeds E_1 zelf een algebraïsche sluiting van F bevat. Inderdaad, stel $E = \{\alpha \in E_1 \mid \alpha \text{ is algebraïsch over } F\}$; dan is E/F een algebraïsche velduitbreiding (zie Stelling 3.2.8). Ook heeft, per constructie, elk polynoom van graad ten minste 1 een wortel in E_1, maar een dergelijke wortel is uiteraard algebraïsch over F en dus bevat in E. Uit Stelling 3.4.6 toegepast op de uitbreiding E/F volgt dan dat E/F een algebraïsche sluiting is van F.

Verrassender is het feit dat ook het bewijs van de uniciteit van algebraische sluitingen gebruik maakt van het lemma van Zorn.

Stelling 3.4.9. *Zij F een willekeurig veld, en zij E en L twee algebraïsche sluitingen van F. Dan zijn E en L twee F-isomorfe velden.*

Bewijs. Zij Ω de verzameling van alle paren (M, θ) waarbij M een veld is met $F \leq M \leq E$ en waarbij $\theta\colon M \to L$ een F-monomorfisme is. Definieer een orderelatie op Ω als volgt:

$$(M, \theta) \preceq (M', \theta') \iff M \leq M' \text{ en } \theta'_{|M} = \theta.$$

Merk op dat Ω niet ledig is omdat $(F, \mathrm{inc}) \in \Omega$.

We willen nu het lemma van Zorn toepassen op de verzameling Ω, en we zullen dus aantonen dat elke keten in Ω een bovengrens heeft. Zij dus $\{(M_i, \theta_i)\}$ een willekeurige keten in Ω, en stel $M = \cup M_i$. Definieer $\theta\colon M \to L$ als volgt: gegeven een $\alpha \in M$, kies een i zodat $\alpha \in M_i$, en stel $\theta(\alpha) := \theta_i(\alpha)$. Het is niet moeilijk om na te gaan dat θ op die manier goed gedefinieerd is, en dat $(M, \theta) \in \Omega$ een bovengrens is voor de keten $\{(M_i, \theta_i)\}$.

Uit het lemma van Zorn volgt nu dat Ω een maximaal element heeft, stel (N, σ). We beweren dat N een algebraïsche sluiting is van F. Inderdaad, veronderstel het tegendeel, en beschouw een niet-nul polynoom $f \in F[x]$ dat niet splijt over N. Aangezien f splijt over E bestaat er een splijtveld K voor f over N met $K \leq E$, en omdat f niet splijt over N is dus $N \lneq K \leq E$. Beschouw nu $\sigma(f) \in L[x]$; omdat L algebraïsch gesloten is, splijt $\sigma(f)$ over L. We kunnen dus Lemma 3.3.8 toepassen, en hieruit besluiten dat het morfisme $\sigma\colon N \to L$ uitbreidt tot een morfisme $\hat{\sigma}\colon K \to L$. Maar dan is $(K, \hat{\sigma}) \in \Omega$ en $(N, \sigma) \prec (K, \hat{\sigma})$, in strijd met de maximaliteit van (N, σ).

Bijgevolg is N een algebraïsche sluiting van F. Omdat E/N een algebraische velduitbreiding is, volgt nu wegens Lemma 3.4.2 dat $E = N$; in het bijzonder is σ een F-monomorfisme van E naar L. Hieruit volgt echter dat $\sigma(E)$ zelf ook een algebraïsche sluiting is van F, en aangezien $L/\sigma(E)$ een algebraïsche velduitbreiding is, volgt opnieuw wegens Lemma 3.4.2 dat $\sigma(E) = L$. We besluiten dat σ een F-isomorfisme van E naar L is. □

3.5 Eindige velden

We bespreken nu eindige velden, i.e. velden met slechts eindig veel elementen.

Lemma 3.5.1. *Zij K een eindig veld. Dan is K een velduitbreiding van $\mathbb{F}_p$ voor een zeker priemgetal p. In het bijzonder heeft K juist p^r elementen, voor een zeker natuurlijk getal $r \geq 1$.*

Bewijs. Beschouw het unieke ringmorfisme $\theta\colon \mathbb{Z} \to K$. Dan is $\mathrm{im}(\theta)$ een deelring van K, en dus een domein; hieruit volgt dat $\ker(\theta)$ een priemideaal is in $\mathbb{Z}$. Anderzijds is $\ker(\theta) \neq 0$ omdat K eindig is, en dus is $\ker(\theta) = (p)$ voor een zeker priemgetal $p \in \mathbb{Z}$. Dan is $\mathrm{im}(\theta) \cong \mathbb{Z}/\ker(\theta) = \mathbb{Z}/(p) \cong \mathbb{F}_p$, het unieke veld met p elementen. We zien dus dat K een velduitbreiding is van $\mathbb{F}_p$, en omdat K zelf ook eindig is, is deze uitbreiding eindig. In het bijzonder is K een vectorruimte over $\mathbb{F}_p$ van dimensie r, waarbij $r = [K : \mathbb{F}_p]$, en het veld K heeft dus p^r elementen. □

Stelling 3.5.2. *Zij K een eindig veld met $q = p^r$ elementen. Dan zijn de elementen van K precies de wortels van het polynoom $x^q - x \in K[x]$. Dit polynoom heeft q verschillende wortels, en factoriseert volledig in $K[x]$.*

Bewijs. Beschouw de multiplicatieve groep $K^\times$ van K; deze groep heeft $q-1$ elementen. Uit de stelling van Lagrange weten we dat voor elke $\alpha \in K^\times$ geldt dat $\alpha^{q-1} = 1$, en dus is α een wortel van het polynoom $x^{q-1} - 1 \in K[x]$. Het overblijvende element $0 \in K$ is een wortel van het polynoom $x \in K[x]$, en dus is elk element van K een wortel van $x^q - x$. Aangezien dit polynoom in het bijzonder q verschillende wortels heeft (namelijk de q elementen van K), factoriseert het volledig in lineaire factoren over K:

$$x^q - x = \prod_{\alpha \in K} (x - \alpha)\,. \qquad \square$$

De structuur van de multiplicatieve groep blijkt bijzonder eenvoudig te zijn.

Stelling 3.5.3. *Zij K een eindig veld met $q = p^r$ elementen. Dan is de multiplicatieve groep van K cyclisch, i.e. $K^\times \cong \mathbf{C}_{q-1}$.*

Bewijs. Omdat K een eindig veld is, is $K^\times$ een eindige abelse groep. Uit de classificatie van de eindige abelse groepen (zie "Algebra I") volgt dat er natuurlijke getallen $d_1 \mid \cdots \mid d_k$ bestaan ($d_i > 1$), zodat

$$K^\times \cong \mathbf{C}_{d_1} \times \cdots \times \mathbf{C}_{d_k}\,.$$

Omdat elke d_i een deler is van d_k, voldoet elk element van $K^\times$ aan de vergelijking $x^{d_k} - 1 = 0$. Echter, dit polynoom heeft ten hoogste d_k wortels in het veld K, en dus is $|K^\times| = d_1 \cdots d_k \leq d_k$. Dit kan enkel als $|K^\times| = d_k$ en $k = 1$, en dus is $K^\times$ cyclisch. $\square$

Opmerking 3.5.4. Dezelfde redenering toont ook aan dat elke eindige deelgroep van de multiplicatieve groep van een *willekeurig* veld cyclisch is. Deze uitspraak is niet langer geldig voor willekeurige deelgroepen van de multiplicatieve groep; zo is bijvoorbeeld $\mathbb{Q}^\times$ niet cyclisch.

Sterker nog: als K een willekeurig oneindig veld is, dan kan men aantonen dat $K^\times$ een abelse groep is die niet eindig voortgebracht is (en dus in zeer sterke mate niet-cyclisch is!).

Definitie 3.5.5. Zij K een eindig veld. Een voortbrenger van de cyclische groep $K^\times$ wordt een *primitief element* van K genoemd.

Opmerking 3.5.6. Het is verrassend moeilijk om voor een gegeven eindig veld expliciet te bepalen welke elementen primitief zijn. Zo is bijvoorbeeld voor het veld $\mathbb{F}_7$ het element 2 geen voortbrenger voor $\mathbb{F}_7^\times$, want $\langle 2\rangle = \{1, 2, 4\}$, omdat $2^3 = 1$. Anderzijds is 3 wel een voortbrenger, want $\langle 3\rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{F}_7^\times$.

Vervolgens willen we voor elke priemmacht $q = p^r$ een veld van orde q construeren. We zullen de volgende aangename rekenregel nodig hebben.

Lemma 3.5.7 (Freshman's dream)**.** *Zij F een veld met $\mathrm{char}(F) = p > 0$, en stel $q = p^r$. Dan geldt de gelijkheid $(x + y)^q = x^q + y^q$ in de polynomenring $F[x, y]$.*

Bewijs. We bewijzen dit eerst voor $q = p$. Door $(x + y)^p$ te ontwikkelen in $\mathbb{Z}[x, y]$ met het binomium van Newton, krijgen we

$$(x + y)^p = x^p + \tbinom{p}{1}x^{p-1}y + \cdots + \tbinom{p}{p-1}xy^{p-1} + y^p\,,$$

en omdat p priem is, geldt voor elke $i \in \{1, \ldots, p - 1\}$ dat $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ deelbaar is door p. De natuurlijke afbeelding $\mathbb{Z}[x, y] \to F[x, y]$ beeldt elk van deze coëfficiënten af op 0, waardoor we de gezochte gelijkheid verkrijgen.

De gelijkheid voor algemene $q = p^r$ volgt nu per inductie op r. □

We komen nu tot de constructie van een veld van orde $q = p^r$.

Stelling 3.5.8. *Zij p een priemgetal, $r \in \mathbb{N}$, en stel $q = p^r$. Dan bestaat er een veld van orde q.*

Bewijs. We vertrekken van het veld $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Beschouw het monisch polynoom $f = x^q - x \in F[x]$. Uit Stelling 3.3.6 weten we dat er een splijtveld K voor f over F bestaat. Omdat K een velduitbreiding is van F, geldt in het bijzonder dat $\mathrm{char}(K) = p$. Stel nu

$$L := \{\alpha \in K \mid f(\alpha) = 0\} = \{\alpha \in K \mid \alpha^q = \alpha\}\,.$$

We beweren dat $|L| = q$. Merk op dat $f'(x) = qx^{q-1} - 1 = -1$ in $K[x]$ omdat $q = 0$, en dus heeft f' geen wortels in K. Uit Lemma 3.3.11 volgt dat f geen meervoudige wortels heeft in K. Omdat het polynoom f graad q heeft, en het in K volledig factoriseert in lineaire factoren, volgt hieruit dat het precies q verschillende wortels heeft in K; dit toont aan dat inderdaad $|L| = q$.

We tonen tenslotte aan dat L een deelveld is van K. Stel dus $\alpha, \beta \in L$ willekeurig, dus $\alpha^q = \alpha$ en $\beta^q = \beta$. We moeten aantonen dat de elementen $\alpha + \beta$, $\alpha\beta$, $-\alpha$ en α^{-1} (als $\alpha \neq 0$) eveneens tot L behoren. Dit is evident

voor $\alpha\beta$ en voor α^{-1}. Voor $-\alpha$ volgt dit uit het feit dat $(-1)^q = -1$ in K. Voor $\alpha + \beta$ ten slotte is dit precies Lemma 3.5.7. We besluiten dat L het gezochte veld van orde q is. □

Nu we aangetoond hebben dat er voor elke priemmacht $q = p^r$ een veld van orde q bestaat, stellen we ons de natuurlijke vraag of een dergelijk veld uniek is (op isomorfisme na). Dit is inderdaad het geval.

Stelling 3.5.9. *Zij p een priemgetal, $r \in \mathbb{N}$, en stel $q = p^r$. Als K en K' velden zijn met $|K| = |K'| = q$, dan is $K \cong K'$.*

Bewijs. Uit Stelling 3.5.3 weten we dat $K^\times$ een cyclische groep is. Zij α een voortbrenger voor $K^\times$; dan is $K = \mathbb{F}_p(\alpha)$. Zij $f = \min_{\mathbb{F}_p}(\alpha)$; dan is $K \cong \mathbb{F}_p[x]/(f)$. Maar dan is α een wortel van twee polynomen in $\mathbb{F}_p[x]$, namelijk van $f(x)$ en van $x^q - x$. Aangezien f irreducibel is over $\mathbb{F}_p$, kan dit enkel als $f \mid x^q - x$.

We gaan nu over naar het tweede veld K'. Aangezien $x^q - x$ volledig factoriseert over K' in lineaire factoren, heeft f een wortel α' in K'. Maar dan is $K \cong \mathbb{F}_p[x]/(f) \cong \mathbb{F}_p(\alpha')$. Aangezien $|K| = |K'|$, kan dit enkel als het deelveld $\mathbb{F}_p(\alpha')$ van K' gelijk is aan K' zelf. We besluiten dat $K \cong K'$. □

Uit Stelling 3.5.8 en 3.5.9 besluiten we dat er voor elke priemmacht $q = p^r$ een uniek eindig veld is van orde q. We noteren dit veld als $\mathbb{F}_q$, of ook soms als $\mathsf{GF}(q)$, waarbij de afkorting GF staat voor *Galois Field*.

Ten slotte willen we de deelvelden van een eindig veld bestuderen. We zullen hierbij gebruik maken van het volgend lemma.

Lemma 3.5.10. *Zij p een priemgetal, $r \in \mathbb{N}$ en $q = p^r$. Zij $k \in \mathbb{N}$ een deler van r, en stel $q' = p^k$. Dan is $x^{q'} - x \mid x^q - x$.*

Bewijs. Stel $s = r/k \in \mathbb{N}$. We zullen twee maal gebruik maken van de identiteit

$$y^d - 1 = (y-1)(y^{d-1} + \cdots + y + 1)\,.$$

We stellen eerst $y = q'$ en $d = s$ om te besluiten dat $q' - 1 \mid q - 1$. Vervolgens gebruiken we de identiteit opnieuw met $y = x^{q'-1}$ en $d = (q-1)/(q'-1) \in \mathbb{N}$, en we concluderen dat $x^{q'-1} - 1 \mid x^{q-1} - 1$. □

Stelling 3.5.11. *Zij p een priemgetal, $r \in \mathbb{N}$, $q = p^r$, en zij $K = \mathbb{F}_q$. Dan bevat K een deelveld van orde $q' = p^k$ als en slechts als $k \mid r$.*

Bewijs. Als $k \nmid r$, dan is $q = p^r$ geen macht van $q' = p^k$, en dus kan het veld $K = \mathbb{F}_q$ onmogelijk een velduitbreiding zijn van het veld $\mathbb{F}_{q'}$. Omgekeerd, als

$k \mid r$, dan volgt uit Lemma 3.5.10 dat $x^{q'} - x \mid x^q - x$. Het polynoom $x^{q'} - x$ heeft dus al zijn wortels in het veld K van orde q. Stel nu

$$L := \{\alpha \in K \mid \alpha^{q'} - \alpha = 0\}\,.$$

Dan tonen we precies zoals in het bewijs van Stelling 3.5.8 aan dat $|L| = q'$, en dat L een deelveld is van K. Dit bewijst de stelling. $\square$

Hoofdstuk

4 Galoistheorie

4.1 Inleiding

In de Galoistheorie associëren we een eindige groep, de zogenaamde *Galoisgroep*, met elke velduitbreiding van eindige graad. Zoals we zullen zien, zullen we vaak in staat zijn om vragen over de velduitbreiding te beantwoorden door deze groep te onderzoeken.

Een belangrijk voorbeeld van deze situatie, en in feite de situatie waarin Galois zelf voornamelijk in geïnteresseerd was, is de volgende. Gegeven een polynoom $f \in \mathbb{Q}[x]$; kunnen we de oplossingen van de vergelijking $f(x) = 0$ in $\mathbb{C}$ expliciet neerschrijven? Om aan te geven wat we precies bedoelen met "expliciet", geven we een voorbeeld. Beschouw het polynoom $f(x) = x^3 - 2$. Dan zijn de wortels in $\mathbb{C}$ de waarden $\sqrt[3]{2}$ en $\sqrt[3]{2}(-1 \pm \sqrt{-3})/2$, en deze kunnen "expliciet" bekomen worden door enkel gebruik te maken van de elementen van $\mathbb{Q}$ en de elementaire operaties optellen, aftrekken, vermenigvuldigen, delen en n-de machtswortels nemen. We zeggen dat f "oplosbaar is in radicalen". Een natuurlijke vraag is, of een dergelijke procedure mogelijk is voor elke $f \in \mathbb{Q}[x]$.

Wat is nu het verband met velduitbreidingen en de corresponderende Galoisgroep waarvan sprake? Gegeven een polynoom $f \in \mathbb{Q}[x]$, dan kunnen we het splijtveld van f over $\mathbb{Q}$ in $\mathbb{C}$ beschouwen. Dit is een velduitbreiding $E/\mathbb{Q}$ van eindige graad, en deze heeft een corresponderende Galoisgroep, die we zullen noteren als $\mathrm{Gal}(E/\mathbb{Q})$. Galois heeft bewezen dat de vergelijking $f(x) = 0$ oplosbaar is in radicalen als en slechts als de Galoisgroep $\mathrm{Gal}(E/\mathbb{Q})$ een oplosbare groep is.

Zoals we later zullen zien, bestaan er polynomen van graad 5 waarvan de geassocieerde Galoisgroep de symmetrische groep $\mathbf{S}_5$ is, en we weten dat deze groep niet oplosbaar is. Hieruit volgt dan dat er geen algemene "formule" kan bestaan om algemene polynoomvergelijkingen van graad 5 op te lossen (waarbij we met "formule" een uitdrukking bedoelen die niks exotischer bevat dan n-de machtswortels).

In de tijd van Galois (omstreeks 1830) waren reeds formules gekend voor het oplossen van polynomen van graad ≤ 4, en het was dus enorm verrassend

dat er geen dergelijke algemene formule kan bestaan voor polynomen van graad ≥ 5. Interessant hierbij is dat deze stelling van Galois over polynomen van graad 5 onafhankelijk en ongeveer gelijktijdig werd bewezen door N. Abel (naar wie de abelse groepen genoemd zijn). Het is een tragisch toeval dat elk van beide mannen dit resultaat heeft bewezen op zeer jonge leeftijd en dan kort daarna overleden is; Galois kwam om het leven in een dubieus duel op 21-jarige leeftijd, en Abel werd niet ouder dan 27.

Definitie 4.1.1. Zij E/F een willekeurige velduitbreiding. De verzameling van alle F-automorfismen van E (zie Definitie 3.1.1(iv)) vormt een groep onder de samenstelling, die we de *Galoisgroep* van de velduitbreiding E/F noemen, en noteren als $\mathrm{Gal}(E/F)$.

De definitie $\mathrm{Gal}(E/F)$ is zinvol in deze algemeenheid, maar we zullen in het vervolg bijna altijd werken met velduitbreidingen van eindige graad.

Voorbeeld 4.1.2. Als voorbeeld bepalen we de groep $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Merk vooreerst op dat indien $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, dan

$$-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2,$$

en dus $\sigma(i) \in \{i, -i\}$. Merk ook op dat voor alle $a, b \in \mathbb{R}$ geldt dat

$$\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i),$$

zodat σ volledig bepaald is door het element $\sigma(i)$. Indien $\sigma(i) = i$, dan is $\sigma = \mathrm{id}$; indien $\sigma(i) = -i$, dan is $\sigma(a + bi) = a - bi$ voor alle $a, b \in \mathbb{R}$, i.e. σ is de complexe toevoeging. We besluiten dat $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbf{C}_2$.

Opmerking 4.1.3. De oorspronkelijke definitie die Galois gebruikte was niet dezelfde als degene die we hier gegeven hebben. Galois definieerde zijn groepen enkel in het geval dat E het splijtveld was over F van een polynoom $f \in F[x]$, en zijn constructie hing af van het polynoom f zelf. Bovendien bestond zijn groep niet uit veldautomorfismen, maar uit zekere permutaties van de wortels van f. Zie ook Gevolg 4.1.15 verderop.

We hebben nu reeds een definitie die met elke velduitbreiding een groep associeert, maar we willen ook in de andere richting kunnen gaan.

Definitie 4.1.4. Zij E een willekeurig veld, en $H \leq \mathrm{Aut}(E)$ een deelgroep van de groep van alle automorfismen van E. Dan definiëren we

$$\mathrm{Fix}(H) := \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ voor alle } \sigma \in H\}.$$

Vaak schrijven we ook $\mathrm{Fix}_E(H)$ in plaats van $\mathrm{Fix}(H)$. Men gaat eenvoudig na dat $\mathrm{Fix}(H)$ een deelveld is van E; we noemen het het *fixveld* van H.

Lemma 4.1.5. (i) *Zij E/F een velduitbreiding. Dan is*

$$\mathrm{Fix}_E(\mathrm{Gal}(E/F)) \geq F.$$

(ii) *Zij E een veld, en zij H een deelgroep van* $\mathrm{Aut}(E)$*. Dan is*

$$\mathrm{Gal}(E/\mathrm{Fix}(H)) \geq H.$$

Bewijs. Dit volgt onmiddellijk uit de definities. □

Beschouw nu een willekeurige velduitbreiding E/F, met Galoisgroep $G = \mathrm{Gal}(E/F)$. We willen een verband leggen tussen de *tussenvelden* van E/F, i.e. de velden K met $F \leq K \leq E$, en de deelgroepen H van G. Het volgend lemma is een evidente uitbreiding van het voorgaand lemma.

Lemma 4.1.6. *Beschouw nu een willekeurige velduitbreiding E/F, met Galoisgroep $G = \mathrm{Gal}(E/F)$. Stel*

$$\mathcal{F} := \{K \mid F \leq K \leq E\};$$
$$\mathcal{G} := \{H \mid H \leq G\}.$$

Definieer afbeeldingen

$$f\colon \mathcal{G} \to \mathcal{F}\colon H \mapsto \mathrm{Fix}_E(H);$$
$$g\colon \mathcal{F} \to \mathcal{G}\colon K \mapsto \mathrm{Gal}(E/K).$$

Dan geldt:

(i) *$g(f(H)) \geq H$ en $f(g(K)) \geq K$ voor alle $H \in \mathcal{G}$ en alle $K \in \mathcal{F}$;*

(ii) *als $H_1 \leq H_2$, dan $f(H_1) \geq f(H_2)$ voor alle $H_1, H_2 \in \mathcal{G}$;*

(iii) *als $K_1 \leq K_2$, dan $g(K_1) \geq g(K_2)$ voor alle $K_1, K_2 \in \mathcal{F}$.*

Bewijs. Dit volgt opnieuw onmiddellijk uit de definities. □

Telkens we twee partieel geordende verzamelingen $(\mathcal{F}, \leq)$ en $(\mathcal{G}, \leq)$ hebben met afbeeldingen $f\colon \mathcal{G} \to \mathcal{F}$ en $g\colon \mathcal{F} \to \mathcal{G}$ die voldoen aan de eigenschappen (i), (ii) en (iii) van Lemma 4.1.6, zeggen we dat deze afbeeldingen een *Galois-connectie* leggen tussen deze partieel geordende verzamelingen. Galois-connecties komen voor in verschillende gebieden van de wiskunde, niet enkel in de Galoistheorie.

Voorbeeld 4.1.7. Zij V een vectorruimte, met duale ruimte V^*. Voor elke deelverzameling $X \subseteq V$ definiëren we de *annihilator* van X als

$$\mathrm{Ann}(X) = \{\varphi \in V^* \mid \varphi(v) = 0 \text{ voor alle } v \in X\}.$$

Analoog definiëren we voor elke deelverzameling Y van V^* de *nulpuntenverzameling* van Y als

$$\mathrm{Zero}(Y) = \{v \in V \mid \varphi(v) = 0 \text{ voor alle } \varphi \in Y\}.$$

Stel dan $\mathcal{F}$ gelijk aan de verzameling van alle deelverzamelingen van V, geordend met de inclusie, en stel analoog $\mathcal{G}$ gelijk aan de verzameling van alle deelverzamelingen van V^*, geordend met de inclusie. Dan vormen Ann en Zero een Galois-connectie tussen $\mathcal{F}$ en $\mathcal{G}$.

Definitie 4.1.8. Zij $\mathcal{F}$ en $\mathcal{G}$ twee partieel geordende verzamelingen met een Galois-connectie $f\colon \mathcal{G} \to \mathcal{F}$ en $g\colon \mathcal{F} \to \mathcal{G}$. Dan definiëren we

$$\mathcal{F}_0 := \{K \in \mathcal{F} \mid f(g(K)) = K\};$$
$$\mathcal{G}_0 := \{H \in \mathcal{G} \mid g(f(H)) = H\}.$$

We noemen de elementen van $\mathcal{F}_0$ en $\mathcal{G}_0$ de *gesloten elementen* van respectievelijk $\mathcal{F}$ en $\mathcal{G}$.

Voorbeeld 4.1.9. In Voorbeeld 4.1.7 zijn de gesloten elementen van $\mathcal{F}$ precies de deelruimten van V, en analoog zijn de gesloten elementen van $\mathcal{G}$ precies de deelruimten van V^*.

Zoals misschien blijkt uit het voorgaande voorbeeld, spelen de gesloten elementen een bijzondere rol in een Galois-connectie. Dit zal ook zo blijken te zijn in de situatie van de Galoisgroepen. We geven eerst nog een algemeen lemma mee in deze context, dat duidelijk maakt dat de Galois-connectie het sterkst is voor gesloten elementen.

Lemma 4.1.10. *Zij $\mathcal{F}$ en $\mathcal{G}$ twee partieel geordende verzamelingen met een Galois-connectie $f\colon \mathcal{G} \to \mathcal{F}$ en $g\colon \mathcal{F} \to \mathcal{G}$. Dan is*

$$\mathcal{F}_0 = \{f(H) \mid H \in \mathcal{G}\};$$
$$\mathcal{G}_0 = \{g(K) \mid K \in \mathcal{F}\}.$$

Bovendien definiëren f en g inverse bijecties tussen $\mathcal{F}_0$ en $\mathcal{G}_0$.

Bewijs. Het volstaat om aan te tonen dat

$$f(g(f(H))) = f(H) \text{ voor alle } H \in \mathcal{G};$$
$$g(f(g(K))) = g(K) \text{ voor alle } K \in \mathcal{F}.$$

(Ga zelf na waarom dit volstaat!) We zullen enkel de eerste uitspraak bewijzen; het bewijs van de tweede uitspraak is volledig analoog. Zij dus $H \in \mathcal{G}$ willekeurig. Wegens eigenschap (i) van een Galois-connectie is $g(f(H)) \geq H$, en door hierop eigenschap (ii) toe te passen, bekomen we $f(g(f(H))) \leq f(H)$. Anderzijds kunnen we eigenschap (i) toepassen op $K = f(H)$, en we bekomen uit $f(g(K)) \geq K$ dat $f(g(f(H))) \geq f(H)$. We besluiten dat $f(g(f(H))) = f(H)$. □

Opmerking 4.1.11. We benadrukken nog eens dat de afbeeldingen f en g de orderelatie omdraaien. Soms worden dergelijke Galois-connecties ook wel *antitone Galois-connecties* genoemd, en definieert men op analoge wijze *monotone Galois-connecties* die de orderelatie behouden in plaats van omdraaien.

We keren nu terug naar de specifieke situatie waarin E/F een velduitbreiding is met Galoisgroep $G = \mathrm{Gal}(E/F)$. Zoals we zullen zien, zijn er in deze situatie heel veel gesloten elementen in de Galois-connectie. Zo zal voor een velduitbreiding E/F van eindige graad gelden dat $\mathcal{G} = \mathcal{G}_0$, i.e. elke deelgroep van G is gesloten. Het is in het algemeen niet waar dat elk element van $\mathcal{F}$ gesloten is, maar als het grondveld F gesloten is, dan is het wel waar dat elk element van $\mathcal{F}$ gesloten is. Deze resultaten zijn natuurlijk niet zomaar het gevolg van het feit dat we een Galois-connectie hebben, en maken gebruik van heel wat diepere algebraïsche resultaten, zoals we zullen zien.

De voorwaarde $F \in \mathcal{F}_0$ is niet steeds waar voor velduitbreidingen van eindige graad, dus we zullen een bijzondere naam geven aan deze gunstige situatie.

Definitie 4.1.12. Zij E/F een velduitbreiding. We noemen E/F een *Galois-uitbreiding* als $[E : F]$ eindig is en bovendien $F = \mathrm{Fix}(\mathrm{Gal}(E/F))$, of anders gezegd, als $F \in \mathcal{F}_0$. We gebruiken hiervoor vaak de uitdrukking "*E is Galois over F*".

De volgende observatie benadrukt het feit dat het Galois zijn een eigenschap is van een velduitbreiding, niet van een veld op zich.

Lemma 4.1.13. *Zij E/F een willekeurige velduitbreiding van eindige graad, en beschouw het tussenveld $K = \mathrm{Fix}_E(\mathrm{Gal}(E/F))$ (dus $F \leq K \leq E$). Dan is E/K een Galois-uitbreiding met $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/F)$. In het bijzonder is de triviale velduitbreiding F/F altijd Galois.*

Bewijs. Zij f en g zoals in Lemma 4.1.6. Dan is $\mathrm{Gal}(E/K) = g(f(g(F))) = g(F) = \mathrm{Gal}(E/F)$, en dus is $\mathrm{Fix}_E(\mathrm{Gal}(E/K)) = \mathrm{Fix}_E(\mathrm{Gal}(E/F)) = K$, wat precies uitdrukt dat E/K Galois is. De laatste uitspraak volgt hieruit door $E = F$ te kiezen, aangezien dan noodzakelijk ook $K = F$. □

Welke methoden zouden we kunnen aanwenden om aan te tonen dat een welbepaalde velduitbreiding E/F van eindige graad Galois is? We moeten daarvoor kunnen aantonen dat elk element $\alpha \in E \setminus F$ verplaatst[1] wordt door een element $\sigma \in \mathrm{Gal}(E/F)$. We moeten dus in zekere zin voldoende elementen vinden in de Galoisgroep. De middelen die we zullen aanwenden om F-automorfismen van E te produceren, zijn Stelling 3.1.15 en Gevolg 3.3.10.

Stelling 4.1.14. *Zij E/F een velduitbreiding, en zij $G = \mathrm{Gal}(E/F)$. Zij verder $f \in F[x]$ een niet-nul polynoom, en stel $\Omega = \{\alpha \in E \mid f(\alpha) = 0\}$. Veronderstel dat $\Omega \neq \emptyset$. Dan geldt:*

(i) *De actie van G op E permuteert de elementen van Ω.*

(ii) *Als de elementen van Ω het veld E voortbrengen over F, dan is de actie van G op Ω getrouw.*

(iii) *Als f irreducibel is en E is een splijtveld over F van een polynoom $g \in F[x]$, dan is de actie van G op Ω transitief.*

Bewijs. (i) Zij $\alpha \in \Omega$ en $\sigma \in G$. Dan volgt uit $f(\alpha) = 0$ dat ook $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, waarbij de eerste gelijkheid volgt omdat σ de coëfficiënten van f fixeert. We besluiten dat $\sigma(\alpha) \in \Omega$.

(ii) Zij $N \leq G$ de kern van de actie van G op Ω; we moeten bewijzen dat $N = 1$. Neem dus $\sigma \in N$ willekeurig; dan fixeert σ alle elementen van Ω. Uiteraard fixeert $\sigma \in \mathrm{Gal}(E/F)$ ook alle elementen van F. Wegens de assumptie dat de elementen van Ω het veld E voortbrengen over F volgt nu dat σ alle elementen van E fixeert, m.a.w. $\sigma = 1$.

(iii) Zij $\alpha, \beta \in \Omega$ willekeurig; we moeten een $\sigma \in G$ vinden zodat $\sigma(\alpha) = \beta$. Aangezien f irreducibel is en zowel α als β wortels zijn van f, kunnen we Stelling 3.1.15 toepassen, en we vinden dus een F-isomorfisme φ van $F[\alpha]$ naar $F[\beta]$ dat α op β afbeeldt. Stel nu $\theta\colon F[\alpha] \to E$ gelijk aan de samenstelling van φ met de inclusie $F[\beta] \hookrightarrow E$. Uit Gevolg 3.3.10 weten we nu dat θ uitbreidt tot een F-automorfisme $\sigma\colon E \to E$. Merk op dat inderdaad $\sigma \in G$, en $\sigma(\alpha) = \theta(\alpha) = \varphi(\alpha) = \beta$. □

We zullen deze stelling vaak gebruiken in de volgende gedaante.

[1] Als G een groep is die werkt op een verzameling S, dan zeggen we dat $s \in S$ *verplaatst* wordt door een $g \in G$ als $s^g \neq s$, m.a.w. als s niet gefixeerd wordt door g.

Gevolg 4.1.15. *Zij F een veld, en $f \in F[x]$ een irreducibel polynoom. Zij E een splijtveld van f over F, en stel $\Omega = \{\alpha \in E \mid f(\alpha) = 0\}$. Stel dan $G = \mathrm{Gal}(E/F)$. Dan werkt G transitief en getrouw op Ω.*

Bewijs. Het volstaat om op te merken dat zowel de voorwaarden in (ii) als (iii) van Stelling 4.1.14 voldaan zijn. □

Voorbeeld 4.1.16. Beschouw de velduitbreiding $\mathbb{C}/\mathbb{R}$ van graad 2, en stel $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbf{C}_2$. Beschouw het polynoom $f(x) = x^2 - 2x + 2$ over $\mathbb{R}$. Dan is $\Omega = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0\} = \{1 + i, 1 - i\}$. We stellen vast dat de actie van G op $\mathbb{C}$ inderdaad de twee elementen van Ω permuteert, en dat deze actie transitief en getrouw is.

Voorbeeld 4.1.17. Beschouw het polynoom $f(x) = x^3 - 2$ over $\mathbb{Q}$. Stel $\alpha = \sqrt[3]{2} \in \mathbb{R}$ en $\zeta = e^{2\pi i/3} \in \mathbb{C}$. Dan is $E = \mathbb{Q}(\alpha, \zeta)$ een splijtveld voor f over $\mathbb{Q}$; de verzameling van wortels van f in E is $\Omega = \{\alpha, \alpha\zeta, \alpha\zeta^2\}$. (Merk op dat f niet splijt over $\mathbb{Q}(\alpha)$ want f heeft niet-reële wortels over $\mathbb{C}$, terwijl $\mathbb{Q}(\alpha) \leq \mathbb{R}$.)

Beschouw nu $G = \mathrm{Gal}(E/\mathbb{Q})$. Enerzijds vinden we een involutie in G: de complexe toevoeging $\sigma\colon \mathbb{C} \to \mathbb{C}$ beeldt duidelijk E op zichzelf af, dus de restrictie $\sigma|_E$ is een element van G, en heeft orde 2. In zijn werking op Ω fixeert het α en verwisselt het $\alpha\zeta$ en $\alpha\zeta^2$.

Een ander element van G vinden we als volgt. Merk op dat $\mathbb{Q}(\alpha) \cong_{\mathbb{Q}} \mathbb{Q}(\alpha\zeta)$, want beide elementen α en $\alpha\zeta$ hebben f als minimaalpolynoom. Door samenstelling met de inclusie $\mathbb{Q}(\alpha\zeta) \hookrightarrow E$ vinden we dus een $\mathbb{Q}$-morfisme $\tau\colon \mathbb{Q}(\alpha) \to E$ met $\tau(\alpha) = \alpha\zeta$. Wegens Gevolg 3.3.10 breidt τ uit tot een $\mathbb{Q}$-morfisme $\tau\colon E \to E$, met andere woorden, tot een element van $G = \mathrm{Gal}(E/\mathbb{Q})$. Merk op dat $\min_{\mathbb{Q}}(\zeta)(x) = x^2 + x + 1$, zodat $\tau(\zeta)$ eveneens een wortel moet zijn van dit polynoom, m.a.w., $\tau(\zeta) \in \{\zeta, \zeta^2\}$. Indien $\tau(\zeta) = \zeta$, dan zal τ in zijn werking op Ω gegeven worden door de 3-cykel $(\alpha\ \alpha\zeta\ \alpha\zeta^2)$; Indien $\tau(\zeta) = \zeta^2$, dan zal τ in zijn werking op Ω gegeven worden door de transpositie $(\alpha\ \alpha\zeta)$. In beide gevallen zien we dat σ en τ samen de volledige groep $\mathbf{S}_3$ voortbrengen; deze groep werkt uiteraard transitief op Ω. Aangezien deze actie wegens Gevolg 4.1.15 getrouw moet zijn, weten we zeker dat we de volledige Galoisgroep $G = \mathrm{Gal}(E/\mathbb{Q})$ gevonden hebben: $G = \langle \sigma, \tau \rangle \cong \mathbf{S}_3$.

Een ander gevolg van Stelling 4.1.14 is de vaststelling dat een eindige velduitbreiding steeds een eindige Galoisgroep heeft.

Lemma 4.1.18. *Zij E/F een velduitbreiding van eindige graad. Dan is $G = \mathrm{Gal}(E/F)$ een eindige groep.*

Bewijs. Kies elementen $\alpha_i \in E$ zodat $E = F[\alpha_1, \ldots, \alpha_n]$, en stel $f = \prod_{i=1}^{n} \min_F(\alpha_i)$. Zij Ω de verzameling van alle wortels van f in E. Dan is Ω eindig en brengt het E voort over F, zodat we Stelling 4.1.14(ii) kunnen toepassen. We besluiten dat G getrouw werkt op een eindige verzameling Ω, zodat G isomorf is met een deelgroep van de eindige groep $\mathrm{Sym}(\Omega)$. □

We zullen dit resultaat drastisch verbeteren in Stelling 4.5.4 verderop.

Onze volgende doelstelling is om aan te tonen (zie Stelling 4.4.2) dat een velduitbreiding E/F van eindige graad een Galois-uitbreiding is als en slechts als ze normaal en separabel is. Het eerste van deze begrippen bespreken we in sectie 4.2; het tweede in sectie 4.3.

4.2 Normale uitbreidingen

Definitie 4.2.1. Zij E/F een algebraïsche velduitbreiding. We noemen E/F *normaal*, als voor elk element $\alpha \in E$ geldt dat $\min_F(\alpha)$ splijt over E. Een equivalente definitie is dat E/F normaal is, als elk irreducibel polynoom in $F[x]$ dat een wortel heeft in E splijt over E.

Voorbeeld 4.2.2. (1) Zij F een willekeurig veld. Dan is de triviale uitbreiding F/F normaal.

(2) Als E een algebraïsche sluiting is van F, dan is E/F normaal.

(3) Als E/F een algebraïsche uitbreiding is van graad 2, dan is E/F steeds normaal. Inderdaad, zij $\alpha \in E$ willekeurig, en zij $f = \min_F(\alpha)$. Dan is $\deg(f) \leq 2$. Als $\deg(f) = 1$, dan splijt f uiteraard over E. Als $\deg(f) = 2$, dan kunnen we f over E ontbinden als $f(x) = (x - \alpha)g(x)$, en dus moet noodzakelijk $\deg(g) = 1$, zodat we ook in dit geval besluiten dat f splijt over E.

(4) Een algebraïsche uitbreiding E/F van graad 3 is niet noodzakelijk normaal. Inderdaad, beschouw het irreducibel polynoom $f(x) = x^3 - 2$ over $\mathbb{Q}$ uit Voorbeeld 4.1.17, en stel opnieuw $\alpha = \sqrt[3]{2}$. Dan heeft f een wortel in $K = \mathbb{Q}(\alpha)$, maar splijt niet over K; dus K/F is niet normaal.

Stelling 4.2.4 geeft een nuttige karakterisatie voor normale uitbreidingen. We zullen het volgend eenvoudig lemma nodig hebben.

Lemma 4.2.3. *Zij E/F een velduitbreiding van eindige graad, en zij $\alpha \in E$. Dan bestaat er een velduitbreiding L/E en een polynoom $g \in F[x]$ zodat L een splijtveld is voor g over F, elke irreducibele factor van g in $F[x]$ een wortel heeft in E, en $g(\alpha) = 0$.*

Bewijs. Kies een basis $\{\alpha_1, \ldots, \alpha_n\}$ voor E over F. Definieer $g \in F[x]$ als het product van de monische irreducibele polynomen van α en van alle α_i over F. Dan is het reeds duidelijk dat elke irreducibele factor van g in $F[x]$ een wortel heeft in E, en dat $g(\alpha) = 0$.

Zij nu L een splijtveld voor g over E. Om aan te tonen dat L ook een splijtveld is voor g over F, volstaat het nog om aan te tonen dat L wordt voortgebracht over F door de wortels van g. Per definitie van splijtveld is L voortgebracht over E door de wortels van g, en per constructie van g weten we ook dat E is voortgebracht over F door wortels van g. Het resultaat volgt. □

Stelling 4.2.4. *Zij E/F een velduitbreiding van eindige graad. Dan zijn de volgende eigenschappen equivalent:*

(a) *E is normaal over F.*

(b) *E is een splijtveld over F voor een zeker polynoom $g \in F[x]$.*

(c) *Voor elke velduitbreiding L/E geldt dat elk F-monomorfisme van E in L het veld E op zichzelf afbeeldt.*

(d) *Voor elke velduitbreiding L/E geldt dat elke $\sigma \in \mathrm{Gal}(L/F)$ het veld E op zichzelf afbeeldt.*

Bewijs. (a) ⇒ (b). Wegens Lemma 4.2.3 is er een $g \in F[x]$ en een splijtveld L/E voor g over F zodat elke irreducibele factor van g een wortel heeft in E. Omdat E/F een normale uitbreiding is, zal elk van deze irreducibele factoren van g splijten over E, en dus splijt g zelf over E. Maar dan is $L = E$, en dit toont aan dat E een splijtveld is over F voor $g \in F[x]$.

(b) ⇒ (c). Zij L/E een willekeurige velduitbreiding, en $\theta\colon E \to L$ een willekeurig F-monomorfisme. Aangezien E een splijtveld is voor g over F, zal $\theta(E)$ een splijtveld zijn voor $\theta(g) = g$ over $\theta(F) = F$. Maar dan is zowel E als $\theta(E)$ een splijtveld voor g over F bevat in L, en uit Lemma 3.3.5 volgt dan dat $\theta(E) = E$.

(c) ⇒ (d). Triviaal.

(d) ⇒ (a). Zij $\alpha \in E$ willekeurig, en zij $f = \min_F(\alpha)$. We moeten bewijzen dat f splijt over E. We gebruiken Lemma 4.2.3 om een L/E en een $g \in F[x]$ te vinden zodat L een splijtveld is voor g over F en $g(\alpha) = 0$. Dan is $f \mid g$, zodat in het bijzonder f splijt over L. Uit Stelling 4.1.14(iii) volgt nu dat voor elke wortel β van f in L er een $\sigma \in \mathrm{Gal}(L/F)$ bestaat zodat $\sigma(\alpha) = \beta$. Wegens de veronderstelling echter moet σ het veld E op zichzelf afbeelden, en uit $\alpha \in E$ volgt dus

dat ook $\beta \in E$. Dit toont aan dat alle wortels van f in L eigenlijk in E liggen, en omdat f splijt over L, besluiten we dat f ook splijt over E. □

Een belangrijk gevolg hiervan is het feit dat elke velduitbreiding van eindige graad verder kan uitgebreid worden tot een normale velduitbreiding:

Gevolg 4.2.5. *Zij E/F een velduitbreiding van eindige graad. Dan bestaat er een velduitbreiding L/E zodanig dat L/F een normale velduitbreiding van eindige graad is.*

Bewijs. Wegens Lemma 4.2.3 is er een velduitbreiding L/E zodanig dat L het splijtveld is van een polynoom $g \in F[x]$ over F. Uit Stelling 4.2.4 volgt dan dat L normaal is over F. □

4.3 Separabele uitbreidingen

Definitie 4.3.1. Zij $f \in F[x]$ een polynoom van graad n. Dan zeggen we dat f *geen meervoudige wortels heeft* als het n verschillende wortels heeft over elk veld $E \geq F$ waarover het splijt.

Het volstaat om dit na te gaan in een algebraïsche sluiting:

Lemma 4.3.2. *Zij $f \in F[x]$ een polynoom van graad n, en zij L een algebraische sluiting van F. Dan heeft f geen meervoudige wortels als en slechts als f precies n verschillende wortels heeft in L.*

Bewijs. Veronderstel dat f precies n verschillende wortels heeft in L, en zij $E \geq F$ een willekeurig veld waarover f splijt. Wegens Lemma 3.3.5 bevat L een uniek splijtveld K voor f over F, en bevat E een uniek splijtveld K' voor f over F. Uit de uniciteit van splijtvelden (Stelling 3.3.9) volgt dat er een F-isomorfisme is van K naar K'. Aangezien f precies n verschillende wortels heeft in K, heeft het dan ook precies n verschillende wortels in K', en dus ook in E.

De omgekeerde implicatie is triviaal. □

De volgende beweringen zijn intuïtief duidelijk, en we laten hun (eenvoudig) bewijs als oefening.

Lemma 4.3.3. *Zij $f \in F[x]$ een niet-nul polynoom. Dan zijn de volgende uitspraken equivalent:*

(a) *f heeft geen meervoudige wortels.*

(b) *Voor elke velduitbreiding K/F en elke $\alpha \in K$ geldt dat $(x-\alpha)^2$ geen deler is van f in $K[x]$.*

(c) *Voor elke velduitbreiding K/F geldt dat f en f' geen gemeenschappelijke wortel hebben.*

(d) *Er is een velduitbreiding K/F zodat f precies $\deg(f)$ verschillende wortels heeft in K.*

Bewijs als oefening. (Maak voor (b) $\Leftrightarrow$ (c) gebruik van Lemma 3.3.11.) □

Lemma 4.3.4. *Zij $f \in F[x]$ een niet-nul polynoom, en zij K/F een velduitbreiding. Dan heeft f geen meervoudige wortels als polynoom in $F[x]$ als en slechts als het geen meervoudige wortels heeft als polynoom in $K[x]$.*

Bewijs als oefening. □

Lemma 4.3.5. *Zij $f \in F[x]$ een polynoom dat geen meervoudige wortels heeft. Als $g \mid f$ in $F[x]$, dan heeft ook g geen meervoudige wortels.*

Bewijs als oefening. □

We komen nu tot het begrip van separabiliteit, eerst voor polynomen, en nadien voor velduitbreidingen.

Definitie 4.3.6. Zij $f \in F[x]$ een niet-nul polynoom. Dan is f *separabel over F* als elke irreducibele factor van f in $F[x]$ geen meervoudige wortels heeft.

Merk dus op dat we niet eisen dat f zelf geen meervoudige wortels heeft. De separabiliteit van een polynoom hangt bovendien af van het grondveld F. Merk immers op dat als $f \in F[x]$ en E een splijtveld is voor f over F, dan f over E steeds separabel is, ook al was het inseparabel over F.

In de omgekeerde richting blijft separabiliteit wel bewaard:

Lemma 4.3.7. *Zij $f \in F[x]$ een niet-nul polynoom en E/F een velduitbreiding. Als f separabel is over F, dan is het ook separabel over E.*

Bewijs. Zij h een irreducibele factor van f in $E[x]$. Omwille van de unieke factorisatie in $E[x]$ is er een irreducibele factor g van f in $F[x]$ zodat $h \mid g$ in $E[x]$. Aangezien g geen meervoudige wortels heeft, volgt uit Lemma 4.3.5 dat ook h geen meervoudige wortels heeft. □

De "meeste" polynomen blijken separabel te zijn: zoals we later zullen zien, bestaan inseparabele polynomen enkel over (sommige) oneindige velden met positieve karakteristiek (zie Stelling 4.8.7 verderop). We geven zo dadelijk een voorbeeld. Om de irreducibiliteit na te gaan, zullen we gebruik maken van het criterium van Eisenstein, dat we reeds ontmoet hebben in de cursus "Algebra I", maar dat we hier iets algemener formuleren.

Stelling 4.3.8. *Zij R een uniek factorisatiedomein, en $F = \mathrm{Frac}(R)$ het breukenveld van R. Zij $p \in R$ een priemelement (of equivalent, een irreducibel element). Zij*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

een polynoom in $R[x]$, met $p \mid a_i$ voor alle $i < n$, $p \nmid a_n$, en $p^2 \nmid a_0$. Dan is f irreducibel over F.

Bewijs. Volledig analoog aan het bewijs voor $\mathbb{Z}$ (met breukenveld $\mathbb{Q}$). □

We komen nu tot het beloofde voorbeeld van een inseparabel polynoom.

Voorbeeld 4.3.9. Zij K een willekeurig veld met $\mathrm{char}(K) = p$, en zij $F = K(y)$ het veld van rationale functies over K in de variabele y. Aangezien F het breukenveld is van $K[y]$, en aangezien y een priemelement is in het uniek factorisatiedomein $K[y]$, kunnen we het criterium van Eisenstein toepassen om te besluiten dat het polynoom $f(x) = x^p - y \in F[x]$ irreducibel is.

We beweren dat f inseparabel is over F. Aangezien f zelf irreducibel is, moeten we hiervoor aantonen dat het meervoudige wortels heeft. We maken hiervoor gebruik van Lemma 4.3.3. Zij dus L een algebraïsche sluiting van F, en zij $\alpha \in L$ een wortel van f. Merk op dat $f'(x) = px^{p-1} = 0$ omdat $\mathrm{char}(F) = p$; uit Lemma 4.3.3 volgt nu dat α een meervoudige wortel is van f. In dit voorbeeld is α zelfs de enige wortel van f! Inderdaad, uit Lemma 3.5.7 volgt dat

$$f(x) = x^p - y = x^p - \alpha^p = (x - \alpha)^p,$$

zodat α een wortel is met multipliciteit p.

We komen nu tot het begrip (in)separabiliteit van velduitbreidingen.

Definitie 4.3.10. Zij E/F een willekeurige velduitbreiding (niet noodzakelijk van eindige graad).

(i) Zij $\alpha \in E$ een algebraïsch element over F. Dan is α *separabel over* F als $f = \min_F(\alpha)$ separabel is over F, of equivalent, als f geen meervoudige wortels heeft.

(ii) De velduitbreiding E/F wordt *separabel* genoemd als E/F algebraïsch is, en elk element $\alpha \in E$ separabel is over F.

Separabiliteit blijft bewaard bij overgang naar tussenvelden, aan beide kanten.

Lemma 4.3.11. *Zij E/F een separabele velduitbreiding, en zij $F \leq K \leq E$. Dan zijn zowel E/K als K/F separabele velduitbreidingen.*

Bewijs. Het feit dat K/F separabel is, is triviaal. We bewijzen nu dat E/K separabel is. Zij dus $\alpha \in E$ willekeurig, en zij $f = \min_F(\alpha)$; dan is f separabel over F. Wegens Lemma 4.3.7 is f dus ook separabel over K. Zij nu $g = \min_K(\alpha)$, en merk op dat $g \mid f$ aangezien $f \in K[x]$ en $f(\alpha) = 0$. Dan is g ook separabel over K, en we besluiten dat α separabel is over K. □

Opmerking 4.3.12. Ook het omgekeerde van Lemma 4.3.11 geldt; zie Gevolg 4.8.17 op p. 89 verderop.

4.4 Galois-uitbreidingen

We komen dadelijk tot een van de belangrijke resultaten van de Galoistheorie, met name de karakterisatie van Galois-uitbreidingen als de velduitbreidingen van eindige graad die tegelijk normaal en separabel zijn. Het volgend lemma is daar een cruciaal ingrediënt voor.

Lemma 4.4.1. *Zij E een willekeurig veld, zij $G \leq \mathrm{Aut}(E)$ een willekeurige groep van automorfismen van E, en stel $F = \mathrm{Fix}(G)$. Zij $\alpha \in E$ willekeurig, en veronderstel dat de baan van α onder G,*

$$\Lambda = \{\sigma(\alpha) \mid \sigma \in G\},$$

een eindige verzameling is. Dan geldt:

(i) *α is algebraïsch over F;*

(ii) *$f := \min_F(\alpha)$ heeft geen meervoudige wortels;*

(iii) *f splijt over E;*

(iv) *Λ is de verzameling van alle wortels van f in E;*

(v) *$|\Lambda| = \deg(f)$.*

Bewijs. Definieer het polynoom $p \in E[x]$ als

$$p(x) = \prod_{\beta \in \Lambda} (x - \beta).$$

Aangezien elk element $\sigma \in G$ de elementen van Λ permuteert, zal σ de factoren van p permuteren, zodat $\sigma(p) = p$. Bijgevolg fixeert σ de coëfficienten van het polynoom p. Aangezien dit geldt voor alle $\sigma \in G$, volgt hieruit dat $p \in F[x]$, per definitie van F. Aangezien $\alpha \in \Lambda$ hebben we $p(\alpha) = 0$, zodat α algebraïsch is over F en $f \mid p$.

Wegens Stelling 4.1.14(i) is elk element van Λ een wortel van f, en dus is $\deg(f) \geq |\Lambda| = \deg(p)$. Uit $f \mid p$ volgt nu dat $f = p$, en alle uitspraken zijn nu bewezen. □

We komen nu tot de beloofde karakterisatie.

Stelling 4.4.2. *Zij E/F een velduitbreiding van eindige graad. Dan zijn de volgende uitspraken equivalent:*

(a) *E/F is een Galois-uitbreiding.*

(b) *E/F is een normale separabele velduitbreiding.*

(c) *E is een splijtveld over F van een separabel polynoom over F.*

Bewijs. (a) ⇒ (b). Zij $\alpha \in E$ willekeurig; we moeten bewijzen dat $f = \min_F(\alpha)$ geen meervoudige wortels heeft en splijt over E. Stel $G = \mathrm{Gal}(E/F)$ en $\Lambda = \{\sigma(\alpha) \mid \sigma \in G\}$. Uit Stelling 4.1.14(i) weten we dat elk element van Λ een wortel is van f, en dus is $|\Lambda| \leq \deg(f) < \infty$. Omdat E/F een Galois-uitbreiding is, is $F = \mathrm{Fix}(G)$, en we kunnen Lemma 4.4.1 toepassen, waaruit het te bewijzen volgt.

(b) ⇒ (c). Omdat E normaal is over F, weten we uit Stelling 4.2.4 dat E een splijtveld is over F van een polynoom $g \in F[x]$. We beweren dat g separabel is over F. Inderdaad, zij f een willekeurige monische irreducibele factor van g; dan heeft f een wortel $\alpha \in E$, en aangezien α separabel is over F per veronderstelling, heeft het polynoom f geen meervoudige wortels, wat we moesten bewijzen.

(c) ⇒ (a). Per veronderstelling is E een splijtveld over F van een polynoom $g \in F[x]$ dat separabel is over F. Stel $G = \mathrm{Gal}(E/F)$, en stel $K = \mathrm{Fix}(G)$; we moeten bewijzen dat $K = F$.
Indien $E = F$ valt er niets te bewijzen. We werken per inductie op de graad $[E : F]$, en we veronderstellen dat $E > F$. Aangezien E is voortgebracht over F door de wortels van g, is er zeker een wortel α van g bevat in $E \setminus F$. Dan is $[E : F(\alpha)] < [E : F]$, en uiteraard is E een splijtveld voor g over $F(\alpha)$. Bovendien is g nog steeds separabel over $F(\alpha)$ wegens Lemma 4.3.7, en de inductiehypothese leert ons nu dat E Galois is over $F(\alpha)$.

Stel $H = \mathrm{Gal}(E/F(\alpha))$; dan is $H \leq G$, en

$$F(\alpha) = \mathrm{Fix}(H) \geq \mathrm{Fix}(G) = K.$$

Zij $f = \min_F(\alpha)$. Aangezien $g(\alpha) = 0$ hebben we $f \mid g$, en bijgevolg splijt f over E. Zij Ω de verzameling van alle wortels van f in E. Omdat g separabel is, heeft f geen meervoudige wortels, en dus is $|\Omega| = \deg(f)$. Anderzijds weten we wegens Stelling 4.1.14(iii) dat G transitief werkt op Ω.
Zij nu $h = \min_K(\alpha)$. Aangezien $K = \mathrm{Fix}(G)$ is $G = \mathrm{Gal}(E/K)$, en wegens Stelling 4.1.14(i) permuteert G de wortels van h in E. Aangezien α een wortel is van h, impliceert dit dat ook $\sigma(\alpha)$ een wortel is van h, voor alle $\sigma \in G$. Hieruit volgt dat elk element van Ω een wortel is van h, en dus

$$[K(\alpha) : K] = \deg(h) \geq |\Omega| = \deg(f) = [F(\alpha) : F].$$

Aangezien $F \leq K \leq F(\alpha)$ is echter $K(\alpha) = F(\alpha)$, zodat de vorige ongelijkheid zegt dat $[K(\alpha) : K] \geq [K(\alpha) : F]$, wat wegens Stelling 3.2.4 enkel kan als $K = F$, wat we moesten bewijzen. □

Deze stelling is uiteraard op zich al zeer belangrijk en krachtig, maar heeft ook een belangrijk gevolg: als E/F een Galois-uitbreiding is, dan is elk tussenveld gesloten in de Galois connectie.

Gevolg 4.4.3. *Zij E/F een Galois-uitbreiding en $F \leq K \leq E$ een tussenveld. Dan is ook E/K een Galois-uitbreiding.*

Bewijs. We gebuiken de equivalentie tussen (a) en (c) in Stelling 4.4.2. Omdat E/F Galois is, is E het splijtveld over F van een polynoom $g \in F[x]$ dat separabel is over F. Wegens Lemma 4.3.7 is g dan ook separabel over K, en uiteraard is E ook een splijtveld voor g over K. Hieruit volgt dat E/K Galois is. □

Opmerking 4.4.4. Als E/F een Galois-uitbreiding is, en K een tussenveld, dan is in het algemeen K/F geen Galois-uitbreiding. Zie ook Stelling 4.5.7(iv) verderop.

Net zoals we elke eindige velduitbreiding verder kunnen uitbreiden tot een normale uitbreiding, zo kunnen we ook elke eindige *separabele* velduitbreiding verder uitbreiden tot een Galois-uitbreiding.

Lemma 4.4.5. *Zij E/F een separabele velduitbreiding van eindige graad. Dan is er een velduitbreiding L/E van eindige graad zodat L/F Galois is.*

Bewijs. Wegens Lemma 4.2.3 bestaat er een velduitbreiding L/E en een polynoom $g \in F[x]$ zodat L een splijtveld is voor g over F, en zodat elke monische irreducibele factor f_i van g in $F[x]$ een wortel heeft in E. Elke f_i is bijgevolg het irreducibel polynoom over F van een zekere $\alpha_i \in E$, en uit de separabiliteit van E/F volgt dat f_i geen meervoudige wortels heeft over F. Bijgevolg is g separabel over F, en we besluiten dat L Galois is over F wegens Stelling 4.4.2. □

4.5 De hoofdstelling van de Galoistheorie

Zoals reeds aangegeven wordt door Gevolg 4.4.3, is er een sterk verband tussen de tussenvelden van een Galois-uitbreiding E/F en de deelgroepen van de corresponderende Galoisgroep $G = \mathrm{Gal}(E/F)$. De hoofdstelling van de Galoistheorie, die we dadelijk zullen formuleren en bewijzen, maakt dit verband concreet en zeer krachtig.

Voor we daar toe komen, is het belangrijk om enerzijds meer controle te krijgen over de orde van een Galoisgroep, en anderzijds separabele uitbreidingen beter te kunnen beschrijven. We beginnen met dit laatste: we komen nu tot het belangrijke inzicht dat een separabele velduitbreiding E/F van eindige graad wordt voortgebracht over F door één enkel element.

Stelling 4.5.1 (Primitief element)**.** *Zij E/F een separabele velduitbreiding van eindige graad. Dan is $E = F[\alpha]$ voor een zekere $\alpha \in E$.*

We noemen een element $\alpha \in E$ zodat $E = F[\alpha]$ een *primitief element* voor E/F.

Bewijs. Veronderstel eerst dat F eindig is. Dan is ook E eindig, en wegens Stelling 3.5.3 is $E^\times$ een cyclische groep, stel $E^\times = \langle\alpha\rangle$, waaruit volgt dat $E = F[\alpha]$.

We veronderstellen vanaf nu dat F oneindig is. Wegens Lemma 4.4.5 bestaat er een velduitbreiding L/E zodat L/F Galois is. Uit Gevolg 4.4.3 en Lemma 4.1.10 volgt nu dat de verzameling van tussenvelden K (met dus $F \leq K \leq L$) in bijectief verband staat met de verzameling van gesloten deelgroepen H van $G = \mathrm{Gal}(L/F)$. Aangezien G wegens Lemma 4.1.18 een eindige groep is, heeft G uiteraard slechts eindig veel deelgroepen, en het vermelde bijectief verband impliceert dan dat er slechts eindig veel tussenvelden K bestaan tussen F en L. In het bijzonder zijn er slechts eindig veel tussenvelden tussen F en E.

We bewijzen nu per inductie op $[E : F]$ dat dit impliceert dat er een primitief element α voor E/F bestaat. Indien $E = F$ is dit triviaal; ver-

onderstel dus dat $E \neq F$, en kies een $\alpha \in E \setminus F$. Dan is $E \geq F[\alpha] > F$, en dus $[E : F[\alpha]] < [E : F]$. Aangezien er slechts eindig veel tussenvelden bestaan tussen $F[\alpha]$ en E, kunnen we de inductiehypothese toepassen, en we besluiten hieruit dat $E = F[\alpha][\beta] = F[\alpha, \beta]$ voor een zekere $\beta \in E$.

Definieer nu, voor elke $t \in F$, het veld

$$K_t = F[\alpha + t\beta].$$

Elke K_t is een veld gelegen tussen F en E, en aangezien F oneindig is en er slechts eindig veel tussenvelden zijn, bestaan er noodzakelijk twee verschillende elementen $s, t \in F$ zodat $K_s = K_t$. In het bijzonder is dan

$$(\alpha + s\beta) - (\alpha + t\beta) \in K_s,$$

en omdat $s \neq t$ impliceert dit dat $\beta \in K_s$, wat dan op zijn beurt als gevolg heeft dat ook $\alpha = (\alpha + s\beta) - s\beta \in K_s$. Dus

$$E = F[\alpha, \beta] \leq K_s = F[\alpha + s\beta] \leq E,$$

en we besluiten dat $E = F[\alpha + s\beta]$, zodat $\alpha + s\beta$ het gezochte primitief element voor E/F is. □

Opmerking 4.5.2. In de loop van het bewijs hebben we aangetoond dat als E/F een willekeurige velduitbreiding van eindige graad is met de eigenschap dat E/F slechts eindig veel tussenvelden heeft, dan $E = F[\alpha]$ voor een zekere $\alpha \in E$. Ook het omgekeerde geldt: als E/F een velduitbreiding is van eindige graad met $E = F[\alpha]$ voor een zekere $\alpha \in E$, dan heeft E/F slechts eindig veel tussenvelden. Aangezien we dit resultaat verder niet nodig hebben, laten we het bewijs ervan achterwege.

Merk op dat we ook een soort omgekeerde van Stelling 4.5.1 kunnen formuleren:

Lemma 4.5.3. *Zij F een veld, en $E = F[\alpha]$ met α separabel over F. Dan is E/F een separabele velduitbreiding.*

Bewijs. Zij $f = \min_F(\alpha)$; dan is f separabel over F. Zij L een splijtveld van f over E; dan is L ook een splijtveld van f over F, want $E = F[\alpha]$, en α is een wortel van f. Uit Stelling 4.4.2 volgt dan dat L/F separabel (en zelfs Galois) is, en dus is ook E/F separabel. □

We zullen voorgaand resultaat later sterk veralgemenen; zie Stelling 4.8.16 verderop.

Er is een nauw verband tussen de graad van een velduitbreiding en de orde van de corresponderende Galoisgroep.

Stelling 4.5.4. *Zij E/F een velduitbreiding van eindige graad. Dan is* $|\mathrm{Gal}(E/F)|$ *een deler van* $[E : F]$. *Bovendien is* $|\mathrm{Gal}(E/F)| = [E : F]$ *als en slechts als E/F Galois is.*

Bewijs. Stel $G = \mathrm{Gal}(E/F)$. Veronderstel eerst dat E/F Galois is. Dan is E/F een separabele uitbreiding van eindige graad, en Stelling 4.5.1 levert ons een $\alpha \in E$ zodat $E = F[\alpha]$. Zij $f = \min_F(\alpha)$, en merk op dat $[E : F] = \deg(f)$. Zij Λ de baan van α onder de werking van de eindige groep G.

We berekenen $|\Lambda|$ op twee verschillende manieren. Enerzijds gebruiken we het feit dat E/F Galois is, waardoor $F = \mathrm{Fix}(G)$; uit Lemma 4.4.1 volgt nu dat $|\Lambda| = \deg(f)$. Dus $|\Lambda| = [E : F]$.

Anderzijds gebruiken we de baanformule voor de actie van G op Λ, die zegt dat $|G| = |\Lambda| \cdot |G_\alpha|$, waarbij G_α de stabilisator is in G van $\alpha \in \Lambda$. Echter, aangezien $E = F[\alpha]$ zal elk element van G dat α fixeert, automatisch alle elementen van E fixeren, en dus is $G_\alpha = 1$. Hieruit volgt dat $|\Lambda| = |G| = |\mathrm{Gal}(E/F)|$, en we bekomen de gezochte gelijkheid $|\mathrm{Gal}(E/F)| = [E : F]$.

We beschouwen nu het algemene geval, waarbij E/F niet noodzakelijk Galois is. Stel nu $K = \mathrm{Fix}(G)$, en merk op dat $G = \mathrm{Gal}(E/K)$ wegens Lemma 4.1.10. Bijgevolg is E Galois over K, en uit het eerste deel van het bewijs volgt dat $|G| = [E : K]$. Hieruit volgt dat

$$[E : F] = |\mathrm{Gal}(E/F)| \cdot [K : F].$$

Aangezien E/F Galois is als en slechts als $K = F$, volgen hieruit de resterende beweringen. □

Voor het volgend resultaat beginnen we, net zoals in Lemma 4.4.1, met een groep in plaats van met een velduitbreiding. Merk op dat we in deze stelling *a priori* niet weten dat E/F een eindige uitbreiding is.

Stelling 4.5.5. *Zij E een veld, zij G een eindige deelgroep van* $\mathrm{Aut}(E)$*, en stel* $F = \mathrm{Fix}(G)$. *Dan geldt:*

(i) $|G| = [E : F]$*;*

(ii) $G = \mathrm{Gal}(E/F)$*;*

(iii) *E is Galois over F.*

Bewijs. We bewijzen de drie uitspraken gelijktijdig. Stel $\alpha \in E$, en zij Λ de baan van α onder G; uiteraard is Λ eindig. Uit Lemma 4.4.1 volgt dat α algebraïsch en separabel is over F, en dat $f = \min_F(\alpha)$ voldoet aan

$$[F[\alpha] : F] = \deg(f) = |\Lambda| \leq |G|.$$

Aangezien de graad $[F[\alpha] : F]$ voor variërende $\alpha \in E$ steeds begrensd is door $|G|$, kunnen we een $\alpha \in E$ vinden die deze graad maximaliseert, i.e.

$$[F[\alpha] : F] \geq [F[\gamma] : F] \quad \text{voor alle } \gamma \in E.$$

We beweren dat $F[\alpha] = E$. Inderdaad, indien dit niet zo zou zijn, dan zou er een $\beta \in E$ bestaan met $F[\alpha, \beta] > F[\alpha]$. Echter, elk element van $F[\alpha, \beta]$ is separabel over F, zodat uit Stelling 4.5.1 volgt dat $F[\alpha, \beta] = F[\gamma]$ voor een zekere $\gamma \in E$. Maar dan zou $[F[\gamma] : F] > [F[\alpha] : F]$, in contradictie met de keuze van α. Hieruit volgt dat inderdaad $E = F[\alpha]$, en in het bijzonder is $[E : F] \leq |G|$.

Aangezien $F = \mathrm{Fix}(G)$, is $G \leq \mathrm{Gal}(E/F)$. Anderzijds weten we uit Stelling 4.5.4 dat $|\mathrm{Gal}(E/F)| \leq [E : F]$, met gelijkheid als en slechts als E/F Galois is. Het samenvoegen van deze ongelijkheden levert

$$|G| \leq |\mathrm{Gal}(E/F)| \leq [E : F] \leq |G|,$$

zodat de gelijkheid geldt en $G = \mathrm{Gal}(E/F)$. Alle uitspraken zijn nu bewezen. □

Opmerking 4.5.6. Zij E/F een willekeurige velduitbreiding met Galoisgroep $G = \mathrm{Gal}(E/F)$. Het is gebruikelijk om de actie van de elementen van G op elementen van E exponentieel te noteren, m.a.w. we schrijven a^σ in plaats van $\sigma(a)$ met $a \in E$ en $\sigma \in G$.

We zijn nu helemaal voorbereid om de hoofdstelling van de Galoistheorie onder handen te nemen.

Stelling 4.5.7 (Hoofdstelling van de Galoistheorie)**.** *Zij E/F een Galois-uitbreiding, en stel $G = \mathrm{Gal}(E/F)$. Stel*

$$\mathcal{F} := \{K \mid F \leq K \leq E\};$$
$$\mathcal{G} := \{H \mid H \leq G\}.$$

Definieer afbeeldingen

$$f \colon \mathcal{G} \to \mathcal{F} \colon H \mapsto \mathrm{Fix}_E(H);$$
$$g \colon \mathcal{F} \to \mathcal{G} \colon K \mapsto \mathrm{Gal}(E/K).$$

Dan geldt:

(i) *De afbeeldingen f en g zijn inverse bijecties tussen $\mathcal{F}$ en $\mathcal{G}$, die de inclusie omdraaien.*

(ii) *Als* $g(K) = H$*, dan is* $[E : K] = |H|$ *en* $[K : F] = [G : H]$*. In het bijzonder is* $[E : F] = |G|$*.*

(iii) *Als* $g(K) = H$ *en* $\sigma \in G$*, dan is* $g(K^\sigma) = H^\sigma$*, de toegevoegde*[2] *van* H *door* σ *in* G*.*

(iv) *Zij* $g(K) = H$*. Dan is* $H \trianglelefteq G$ *als en slechts als* K/F *Galois is, en in dat geval geldt* $\mathrm{Gal}(K/F) \cong G/H$*.*

Bewijs. (i) We weten al uit Lemma 4.1.6 dat de afbeeldingen f en g de inclusie omdraaien, en wegens Lemma 4.1.10 induceren ze inverse bijecties tussen de deelverzamelingen $\mathcal{F}_0$ en $\mathcal{G}_0$ van gesloten elementen in respectievelijk $\mathcal{F}$ en $\mathcal{G}$. We zullen aantonen dat $\mathcal{F}_0 = \mathcal{F}$ en $\mathcal{G}_0 = \mathcal{G}$.
Merk op dat de elementen van $\mathcal{F}_0$ precies de tussenvelden K zijn zodat E/K Galois is, en dat de elementen van $\mathcal{G}_0$ precies de deelgroepen van G zijn die optreden als Galoisgroep van een uitbreiding E/K voor een tussenveld K. Omdat E/F Galois is, volgt nu uit Gevolg 4.4.3 dat $\mathcal{F}_0 = \mathcal{F}$. Anderzijds weten we dat G eindig is, zodat ook elke deelgroep van G eindig is; uit Stelling 4.5.5 volgt nu dat $\mathcal{G}_0 = \mathcal{G}$.

(ii) Zij nu $K \in \mathcal{F}$ en $H \in \mathcal{G}$ met $g(K) = H$, of equivalent, $f(H) = K$. Aangezien E/K Galois is wegens Gevolg 4.4.3, hebben we

$$|H| = |\mathrm{Gal}(E/K)| = [E : K]$$

wegens Stelling 4.5.4. Wegens diezelfde stelling is ook $|G| = [E : F]$, en hieruit halen we

$$[G : H] = [E : F]/[E : K] = [K : F].$$

(iii) Zij $\sigma \in G$; dan is K^σ uiteraard opnieuw een veld gelegen tussen F en E, i.e. $K^\sigma \in \mathcal{F}$. We willen aantonen dat $f(H^\sigma) = K^\sigma$. Nu geldt, voor elke $x \in E$, de equivalentie

$$H \text{ fixeert } x \iff H^\sigma \text{ fixeert } x^\sigma$$

(zie "Algebra I", of reken dit zelf na). Aangezien $f(H) = K$ volgt hier onmiddellijk uit dat $f(H^\sigma) = K^\sigma$.

(iv) Veronderstel eerst dat K/F Galois is. Dan is K/F een normale uitbreiding, en uit Stelling 4.2.4 volgt dat $K^\sigma = K$ voor elke $\sigma \in G$. Uit (iii) volgt dan dat $H^\sigma = H$ voor alle $\sigma \in G$, en dus is H een normaaldeler van G.

[2]Hierbij stelt de exponentiële notatie in K^σ een actie voor (zie Opmerking 4.5.6), terwijl die bij H^σ toevoeging voorstelt: $H^\sigma = \sigma^{-1}H\sigma$.

Veronderstel omgekeerd dat $H \trianglelefteq G$. Dan volgt uit (iii) dat $K^\sigma = K$ voor alle $\sigma \in G$. Voor elke $\sigma \in G$ geldt dus dat de restrictie van σ tot K een automorfisme van K definieert, dat alle elementen van F fixeert. We hebben dus een geïnduceerde afbeelding

$$\rho\colon G \to \mathrm{Gal}(K/F)\colon \sigma \mapsto \sigma_{|K},$$

en deze afbeelding is duidelijkerwijze een groepsmorfisme. Hieruit halen we

$$F \leq \mathrm{Fix}_K(\mathrm{Gal}(K/F)) \leq \mathrm{Fix}_K(\rho(G)) \leq \mathrm{Fix}_E(G) = F,$$

en dus is $F = \mathrm{Fix}(\mathrm{Gal}(K/F))$, met andere woorden, K is Galois over F. Uit (i) toegepast op K/F halen we dan uit de gelijkheid $\mathrm{Fix}_K(\mathrm{Gal}(K/F)) = \mathrm{Fix}_K(\rho(G))$ dat $\mathrm{Gal}(K/F) = \rho(G)$.
Merk ten slotte op dat een element $\sigma \in G$ in $\ker(\rho)$ ligt precies dan als σ alle elementen van K fixeert. Bijgevolg is $\ker(\rho) = \mathrm{Gal}(E/K) = H$. Uit de eerste isomorfiestelling voor groepen volgt nu dat

$$\mathrm{Gal}(K/F) = \rho(G) \cong G/\ker(\rho) = G/H,$$

wat we moesten bewijzen. □

4.6 Een voorbeeld

We zullen de hoofdstelling van de Galoistheorie illustreren aan de hand van een concreet voorbeeld. Beschouw daartoe het polynoom

$$f(x) = x^4 - 2 \in \mathbb{Q}[x],$$

en merk op dat f irreducibel is over $\mathbb{Q}$ (bijvoorbeeld wegens het criterium van Eisenstein). Stel $\alpha = \sqrt[4]{2}$, i.e. α is de unieke positieve wortel van f in $\mathbb{R}$. Dan heeft f over $\mathbb{C}$ de ontbinding

$$f(x) = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha),$$

zodat f geen meervoudige wortels heeft en dus in het bijzonder separabel is.

Zij nu E het splijtveld voor f over $\mathbb{Q}$ in $\mathbb{C}$. Uit Stelling 4.4.2 volgt dan dat E Galois is over $\mathbb{Q}$. We zullen de Galoisgroep $G = \mathrm{Gal}(E/\mathbb{Q})$ bepalen, en dan de hoofdstelling van de Galoistheorie gebruiken om alle tussenvelden tussen $\mathbb{Q}$ en E te vinden.

We bepalen eerst de graad van de uitbreiding $E/\mathbb{Q}$. Merk vooreerst op dat $\mathbb{Q}[\alpha] < E$, waarbij de inclusie een echte inclusie is omdat $\mathbb{Q}[\alpha]$ volledig

in $\mathbb{R}$ ligt, terwijl $i\alpha \in E \setminus \mathbb{R}$. Verder volgt uit het feit dat zowel α als $i\alpha$ tot E behoren, dat ook $i \in E$, en dus $\mathbb{Q}[\alpha, i] \leq E$. In feite is $\mathbb{Q}[\alpha, i] = E$, want de 4 wortels van f liggen alle in $\mathbb{Q}[\alpha, i]$, zodat f splijt over $\mathbb{Q}[\alpha, i]$. Dus

$$\mathbb{Q} < \mathbb{Q}[\alpha] < \mathbb{Q}[\alpha, i] = E.$$

Aangezien $f = \min_{\mathbb{Q}}(\alpha)$, hebben we $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(f) = 4$. Anderzijds is $[\mathbb{Q}[\alpha, i] : \mathbb{Q}[\alpha]] = 2$, want i is een wortel van het polynoom $x^2 + 1$ over $\mathbb{Q}[\alpha]$, dat noodzakelijk irreducibel is omdat we reeds weten dat $\mathbb{Q}[\alpha] \neq \mathbb{Q}[\alpha, i]$. Uit Stelling 3.2.4 besluiten we nu dat $[E : \mathbb{Q}] = 8$.

Stel nu $G = \mathrm{Gal}(E/\mathbb{Q})$; uit Stelling 4.5.4 volgt dan dat $|G| = 8$. We proberen nu de structuur van de groep G te achterhalen. We geven hiervoor twee verschillende methoden.

De eerste methode maakt gebruik van de hoofdstelling van de Galoistheorie, waarbij we onze kennis van sommige van de tussenvelden zullen vertalen naar eigenschappen over de deelgroepen van G. Het veld $\mathbb{Q}[\alpha]$ is een tussenveld van $E/\mathbb{Q}$ dat niet Galois is over $\mathbb{Q}$, want $\mathbb{Q}[\alpha]/\mathbb{Q}$ is geen normale uitbreiding. (Inderdaad, het $\mathbb{Q}$-irreducibel polynoom f heeft een wortel in $\mathbb{Q}[\alpha]$ maar splijt er niet.) Uit Stelling 4.5.7(ii) volgt dan dat er een deelgroep $H \leq G$ is met $|H| = [E : \mathbb{Q}[\alpha]] = 2$, die wegens Stelling 4.5.7(iv) géén normaaldeler is van G. Dus G is een groep van orde 8 die een deelgroep van orde 2 heeft die geen normaaldeler is; in het bijzonder is G niet abels. Echter, op isomorfisme na zijn er slechts twee niet-abelse groepen van orde 8, namelijk $\mathbf{D}_8$ en $\mathbf{Q}_8$. De quaternionengroep $\mathbf{Q}_8$ heeft een unieke deelgroep van orde 2, namelijk het centrum $Z(\mathbf{Q}_8) \trianglelefteq \mathbf{Q}_8$. We besluiten dat $G \cong \mathbf{D}_8$ moet zijn.

Een tweede methode die we hier kunnen toepassen, werkt enkel omdat G vrij "groot" is in vergelijking met het aantal wortels van f. Meer bepaald kunnen we gebuik maken van Stelling 4.1.14(ii), die ons zegt dat G getrouw werkt op de verzameling van de 4 wortels van f. Hieruit volgt dat G isomorf is met een deelgroep van $\mathbf{S}_4$. Merk echter op dat G een Sylow 2-deelgroep is van $\mathbf{S}_4$, terwijl we anderzijds weten dat $\mathbf{D}_8$ eveneens een groep is van orde 8 die getrouw werkt op een verzameling van 4 elementen (namelijk de hoekpunten van een vierkant), zodat zeker $\mathbf{D}_8 \leq \mathbf{S}_4$. Omdat wegens de stelling van Sylow alle Sylow 2-deelgroepen toegevoegd en dus isomorf zijn aan elkaar, besluiten we dat $G \cong \mathbf{D}_8$.

We zullen nu nog een stap verder gaan, en expliciet de actie van $G \cong \mathbf{D}_8$ op de verzameling $\Omega = \{\alpha, -\alpha, i\alpha, -i\alpha\}$ bepalen. Beschouw eerst de complexe toevoeging in $\mathbb{C}$, en merk op dat dit een $\mathbb{Q}$-automorfisme van $\mathbb{C}$ is. Omdat $E/\mathbb{Q}$ normaal is, volgt uit Stelling 4.2.4 dat E door de complexe toevoeging op zichzelf wordt afgebeeld, en dus een automorfisme $\tau \in \mathrm{Gal}(E/\mathbb{Q})$

induceert. Dus $\tau \in G$, en wordt gegeven in zijn actie op Ω door de transpositie $(i\alpha \ -i\alpha)$.

Aangezien G transitief is op Ω bestaat er een $\rho \in G$ met[3] $\alpha^\rho = i\alpha$. Anderzijds moet i^ρ opnieuw een wortel zijn van het polynoom x^2+1, en dus moet $i^\rho \in \{i, -i\}$. Indien $i^\rho = i$ stellen we $\sigma = \rho$; indien $i^\rho = -i$ stellen we $\sigma = \tau\rho$. In elk geval voldoet σ nu aan

$$\alpha^\sigma = i\alpha, \quad i^\sigma = i,$$

en dus is de actie van σ op Ω gegeven door de 4-cykel $(\alpha \ i\alpha \ -\alpha \ -i\alpha)$. Merk op dat $\langle\sigma\rangle$ dus een cyclische groep van orde 4 is en dat $\tau \notin \langle\sigma\rangle$; hieruit volgt dat $G = \langle\sigma, \tau\rangle$. We kunnen nu in principe voor elk element van G neerschrijven wat de corresponderende actie op Ω is, maar we zullen deze expliciete berekening achterwege laten.

Vervolgens beschouwen we tussenvelden. We beschouwen eerst tussenvelden van graad 2 over $\mathbb{Q}$. Merk op dat $G \cong \mathbf{D}_8$ precies 3 deelgroepen van index 2 heeft, zodat we uit de hoofdstelling van de Galoistheorie weten dat er precies 3 verschillende tussenvelden van graad 2 zijn. We vinden deze gemakkelijk expliciet: merk op dat $\sqrt{2}$, i, en $i\sqrt{2}$ alle in E liggen, zodat de velden

$$\mathbb{Q}[\sqrt{2}], \ \mathbb{Q}[i], \ \mathbb{Q}[i\sqrt{2}]$$

tussenvelden van $E/\mathbb{Q}$ van graad 2 zijn. Deze zijn duidelijk twee aan twee verschillend. Inderdaad, enkel $\mathbb{Q}[\sqrt{2}]$ is bevat in $\mathbb{R}$; en ook $\mathbb{Q}[i] \neq \mathbb{Q}[i\sqrt{2}]$ want indien ze gelijk zouden zijn, zou ook $\sqrt{2} \in \mathbb{Q}[i]$, wat natuurlijk niet het geval is. We hebben dus de drie tussenvelden van graad 2 gevonden.

We beschouwen nu de tussenvelden van graad 4 over $\mathbb{Q}$. Aangezien $\mathbf{D}_8$ precies 5 deelgroepen van index 4 heeft, moeten we 5 verschillende tussenvelden van graad 4 vinden. We laten de berekeningen hier achterwege, en geven enkel de lijst van deze tussenvelden:

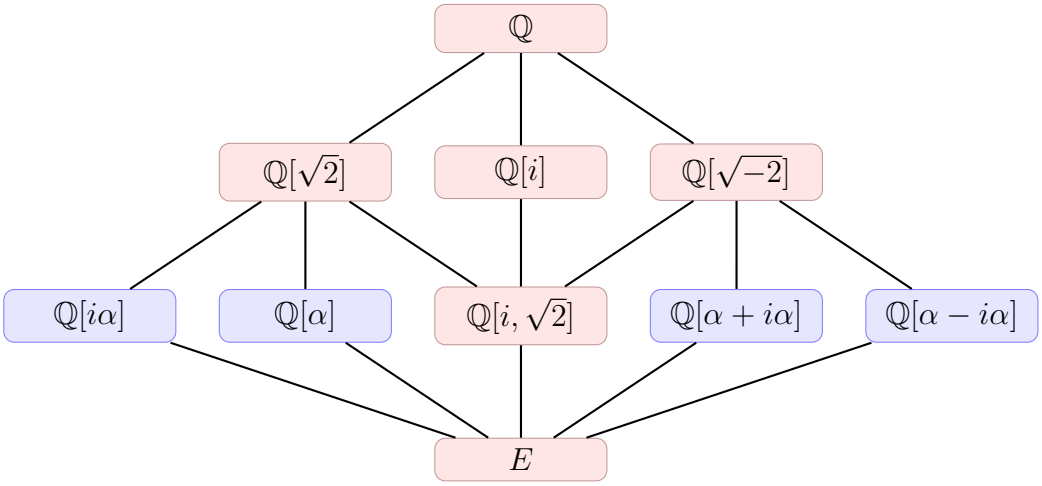
$$\mathbb{Q}[\alpha], \ \mathbb{Q}[i\alpha], \ \mathbb{Q}[\sqrt{2}, i], \ \mathbb{Q}[\alpha + i\alpha], \ \mathbb{Q}[\alpha - i\alpha].$$

Men gaat na dat deze 5 velden twee aan twee verschillend zijn.

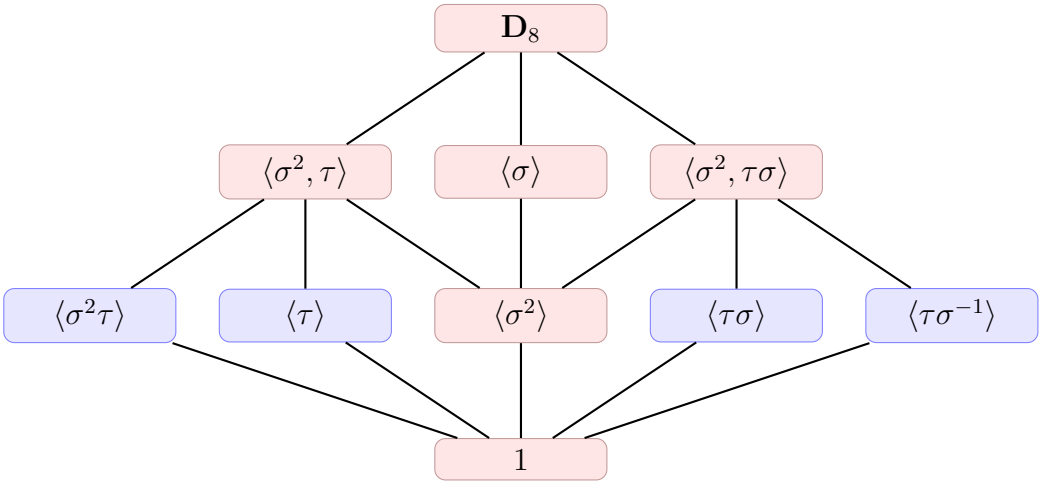
Eens we deze lijsten van tussenvelden hebben, is het overigens niet moeilijk om expliciet te bepalen welk van deze tussenvelden met welke deelgroep van G overeenkomt. We geven twee voorbeelden.

Beschouw de deelgroep $\langle\sigma\rangle \leq G$ van orde 4, en merk op dat $i^\sigma = i$, terwijl $\sqrt{2}^\sigma = (\alpha^2)^\sigma = (i\alpha)^2 = -\sqrt{2}$. Het enige van de 3 tussenvelden van graad 2 dat gefixeerd wordt door σ, is duidelijkerwijze $\mathbb{Q}[i]$, dus $f(\langle\sigma\rangle) = \mathbb{Q}[i]$.

[3]We herinneren nogmaals aan Opmerking 4.5.6.



Figuur 4.1: *De tussenvelden van $E/\mathbb{Q}$. Velden K waarvoor $K/\mathbb{Q}$ Galois is, staan in het rood.*



Figuur 4.2: *De deelgroepen van $\mathbf{D}_8$. Normaaldelers staan in het rood.*

Als tweede voorbeeld beschouwen we het element $\tau\sigma = (\alpha\ i\alpha)(-\alpha\ -i\alpha)$, en de corresponderende deelgroep $\langle\tau\sigma\rangle$ van orde 2. Merk op dat $\sqrt{2}^{\tau\sigma} = -\sqrt{2}$ en dat $i^{\tau\sigma} = -i$. Het enige van de 5 tussenvelden van graad 4 dat gefixeerd wordt door σ, is $\mathbb{Q}[\alpha + i\alpha]$, dus $f(\langle\tau\sigma\rangle) = \mathbb{Q}[\alpha + i\alpha]$.

Ten slotte gaan we na welke van de tussenvelden Galois zijn. Merk op dat $G \cong \mathbf{D}_8$ precies 4 echte niet-triviale normaaldelers heeft, namelijk elk van de drie deelgroepen van orde 4, en één van de deelgroepen van orde 2, namelijk het centrum $Z(G) = \langle\sigma^2\rangle$, met corresponderend tussenveld

$f(\langle\sigma^2\rangle) = \mathbb{Q}[\sqrt{2}, i]$. De Galois-tussenvelden van $E/\mathbb{Q}$ zijn dus

$$\mathbb{Q}[\sqrt{2}],\ \mathbb{Q}[i],\ \mathbb{Q}[i\sqrt{2}],\ \mathbb{Q}[\sqrt{2}, i].$$

(Merk op dat het feit dat elke deelgroep van index 2 een normaaldeler is, zich vertaalt in het feit dat elk tussenveld van graad 2 Galois is, in overeenstemming met Voorbeeld 4.2.2(3)!)

4.7 Natuurlijke irrationaliteiten

In deze korte sectie geven we een resultaat mee dat zeer nuttig kan zijn in toepassingen van Galoistheorie. We zullen het ondermeer nodig hebben in het bewijs van de stelling van Galois (Stelling 4.9.12) verderop. In feite is het zo dat het bewijs dat Galois gaf voor Stelling 4.9.12 (over $\mathbb{Q}$) oorspronkelijk niet helemaal accuraat was, en dat het gat in het bewijs van Galois precies werd opgevuld door onderstaande stelling, die pas later werd bewezen door Abel. Ook de benaming "natuurlijke irrationaliteiten" verwijst naar de toepassing in de stelling van Galois.

Stelling 4.7.1 (Natuurlijke irrationaliteiten)**.** *Zij C/F een willekeurige velduitbreiding, en zij E en L twee tussenvelden. Stel $M = E \cap L$, en stel $K = \langle E, L\rangle$, i.e. K is het kleinste deelveld van C dat zowel E als L bevat.*

Veronderstel dat E/M Galois is. Dan is ook K/L Galois, en restrictie tot E definieert een isomorfisme

$$\rho\colon\ \mathrm{Gal}(K/L) \to \mathrm{Gal}(E/M).$$

In het bijzonder is $[K : L] = [E : M]$.

Bewijs. Aangezien E/M Galois is, is er een separabel polynoom $f \in M[x]$ zodat E het splijtveld is van f over M. Dan splijt f uiteraard over K, en we beweren dat K in feite een splijtveld is van f over L.

Zij K_0 het splijtveld van f over L in K. Aangezien E is voortgebracht over M door de wortels van f, die allemaal in K_0 liggen, volgt er reeds dat $E \leq K_0$. Anderzijds is ook $L \leq K_0$, en dus is $K = \langle E, L\rangle \leq K_0$, waaruit volgt dat inderdaad $K = K_0$.

Aangezien f separabel is over L wegens Lemma 4.3.7, besluiten we dat K/L Galois is.

Zij nu $\sigma \in \mathrm{Gal}(K/L)$. Uit Stelling 4.2.4 volgt dat $\sigma(E) = E$, zodat de restrictie van σ tot E een automorfisme van E is, dat bovendien alle

elementen van $E \cap L = M$ fixeert. Bijgevolg definieert restrictie tot E een morfisme

$$\rho\colon \mathrm{Gal}(K/L) \to \mathrm{Gal}(E/M).$$

We bewijzen nu dat ρ injectief is. Stel dus $N = \ker(\rho)$; dan is $E \leq \mathrm{Fix}(N)$. Anderzijds is natuurlijk ook $L \leq \mathrm{Fix}(N)$, en dus $K = \langle E, L\rangle \leq \mathrm{Fix}(N)$, waaruit volgt dat $N = 1$.

Ten slotte bewijzen we dat ρ surjectief is. Stel $H = \mathrm{im}(\rho) \leq \mathrm{Gal}(E/M)$, en stel $M_1 = \mathrm{Fix}_E(H)$. Dan is uiteraard $M \leq M_1$, en elk element van M_1 wordt gefixeerd door elk automorfisme $\sigma \in \mathrm{Gal}(K/L)$. Hieruit volgt dat $M_1 \leq \mathrm{Fix}(\mathrm{Gal}(K/L)) = L$. Anderzijds is natuurlijk ook $M_1 \leq E$, en dus is $M_1 \leq L \cap E = M$, en we besluiten dat $M_1 = M$. Bijgevolg is $\mathrm{Fix}(H) = \mathrm{Fix}(\mathrm{Gal}(E/M))$, en uit de hoofdstelling van de Galoistheorie volgt nu dat $H = \mathrm{Gal}(E/M)$, wat bewijst dat ρ surjectief is. □

Opmerking 4.7.2. Er is geen enkele restrictie op de velduitbreidingen K/E en L/M; in het bijzonder hoeven deze uitbreidingen niet algebraïsch te zijn.

Voorbeeld 4.7.3. (1) Zij E/M een Galois-uitbreiding, en stel $K = E(x)$ en $L = M(x)$, de velden van rationale functies over E respectievelijk M. Dan is ook K/L Galois, en $\mathrm{Gal}(E(x)/M(x)) \cong \mathrm{Gal}(E/M)$.

(2) Beschouw de uitbreiding $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$. Stel $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{3})$ en $L = \mathbb{Q}(\sqrt{2})$, en zij $M = E \cap L = \mathbb{Q}$ en $K = \langle E, L\rangle = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We weten dat $E/M = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$ Galois is met Galoisgroep $\mathbf{C}_2$; uit de stelling van de natuurlijke irrationaliteiten volgt nu onmiddellijk dat ook $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ Galois is, en eveneens Galoisgroep $\mathbf{C}_2$ heeft. (We hadden dit uiteraard ook rechtstreeks kunnen verifiëren.)

4.8 Inseparabiliteit

Zoals we gezien hebben in Stelling 4.4.2, is het begrip van separabiliteit cruciaal in de Galoistheorie. Anderzijds hebben we nog maar één enkel voorbeeld gezien van inseparabiliteit. Het doel van deze sectie is om te bestuderen hoe en in welke mate separabiliteit kan falen.

Een belangrijk begrip in deze context is dat van perfecte velden.

Definitie 4.8.1. (i) Zij F een veld met $\mathrm{char}(F) = p > 0$. Beschouw de afbeelding

$$\mathrm{Frob}\colon F \to F\colon a \mapsto a^p.$$

Uit Lemma 3.5.7 volgt dat Frob een morfisme is; we noemen deze afbeelding het *Frobeniusmorfisme*, of kortweg *de Frobenius*. Merk op dat Frob steeds injectief is.

(ii) Zij F een veld met $\text{char}(F) = p > 0$. Beschouw de verzameling

$$F^p := \{a^p \mid a \in F\},$$

en merk op dat F^p een deelveld is van F; het is gelijk aan im(Frob).

(iii) Een willekeurig veld F wordt *perfect* genoemd, als hetzij $\text{char}(F) = 0$, hetzij $\text{char}(F) = p$ en $F^p = F$, i.e. elk element van F is een p-de macht in F, of equivalent, als het Frobeniusmorfisme een isomorfisme is.

Voorbeeld 4.8.2. (1) Zij F een eindig veld, en stel $p = \text{char}(F)$. Omdat Frob een injectieve afbeelding is van een eindige verzameling naar zichzelf, is ze automatisch bijectief, en bijgevolg is F perfect.

(2) Zij F een algebraïsch gesloten veld. Als $\text{char}(F) = 0$, dan is F uiteraard perfect; stel dus $\text{char}(F) = p$. Voor elke $a \in F$ heeft het polynoom $x^p - a$ een wortel $\beta \in F$, maar dan is $a = \beta^p \in F^p$. We besluiten dat F ook in dit geval perfect is.

(3) Zij K een willekeurig veld met $\text{char}(K) = p$, en stel $F = K(t)$, het veld van rationale functies over K in de variabele t. We beweren dat $t \notin F^p$, zodat F niet perfect is. Inderdaad, veronderstel dat $t = a^p$ voor een zekere $a \in F$, en schrijf $a = f(t)/g(t)$ met $f, g \in K[t]$ met $f, g \neq 0$. Dan is $tg(t)^p = f(t)^p$. Door de graad in t van beide leden te vergelijken, vinden we echter $1 + p\deg(g) = p\deg(f)$, wat uiteraard onmogelijk is.

We werken nu toe naar het verband tussen inseparabiliteit en niet-perfecte velden.

Lemma 4.8.3. *Zij $f \in F[x]$ een irreducibel polynoom met $\deg(f) \geq 1$. Dan heeft f meervoudige wortels als en slechts als $f' = 0$.*

Bewijs. Veronderstel eerst dat $f' = 0$, en zij E/F een willekeurige velduitbreiding waarin f een wortel α heeft. Dan is $f(\alpha) = 0$ en $f'(\alpha) = 0$ in E, en uit Lemma 4.3.3 volgt dat f meervoudige wortels heeft.

Veronderstel omgekeerd dat f meervoudige wortels heeft. Lemma 4.3.3 impliceert dan dat er een velduitbreiding E/F is en een $\alpha \in E$ zodat $f(\alpha) = f'(\alpha) = 0$. Aangezien f irreducibel is over F, deelt het elk polynoom in $F[x]$ dat α als wortel heeft. In het bijzonder is $f \mid f'$, maar omdat $\deg(f') < \deg(f)$ kan dit enkel als $f' = 0$. □

Opmerking 4.8.4. Zoals we reeds eerder gezien hebben, impliceert het feit dat $f' = 0$ *niet* dat f een constante veelterm is. Inderdaad, als $\text{char}(F) = p$,

en $f = \sum_{i=0}^{n} a_i x^i$ met $\deg(f) = n$, dan is $f' = 0$ als en slechts als $a_i = 0$ voor alle $i \in \mathbb{N} \setminus p\mathbb{N}$; in dat geval heeft f de gedaante

$$f(x) = \sum_{j=0}^{n/p} a_{pj} x^{pj} = g(x^p),$$

waarbij

$$g(x) = \sum_{j=0}^{n/p} a_{pj} x^j.$$

Merk anderzijds op dat als $\mathrm{char}(F) = 0$ en $f' = 0$, dan wel volgt dat f een constante veelterm is.

Gevolg 4.8.5. *Zij $f \in F[x]$ een irreducibel polynoom, en veronderstel dat f meervoudige wortels heeft. Dan is* $\mathrm{char}(F) = p > 0$ *en $f(x) = g(x^p)$ voor een zeker irreducibel polynoom $g \in F[x]$.*

Bewijs. Uit Lemma 4.8.3 weten we dat $f' = 0$, en uit Opmerking 4.8.4 volgt dan dat $\mathrm{char}(F) = p > 0$ en $f(x) = g(x^p)$ voor een zekere $g \in F[x]$. Veronderstel nu dat g reducibel zou zijn, stel $g = g_1 g_2$. Dan zou $f(x) = g(x^p) = g_1(x^p) g_2(x^p)$, in strijd met de irreducibiliteit van f. □

Gevolg 4.8.6. *Zij F een veld met* $\mathrm{char}(F) = p > 0$*, en $f \in F[x]$ een irreducibel polynoom. Dan is $f(x) = g\big(x^{p^n}\big)$ voor een zekere $n \geq 0$ en een zeker irreducibel separabel polynoom $g \in F[x]$.*

Bewijs. We bewijzen dit per inductie op $\deg(f)$. Indien $\deg(f) = 0$ valt er natuurlijk niets te bewijzen; stel dus $\deg(f) > 0$. Als f geen meervoudige wortels heeft, is de bewering voldaan voor $g = f$ en $n = 0$. In het andere geval volgt uit Gevolg 4.8.5 dat $f(x) = h(x^p)$ voor een zeker irreducibel polynoom h met $\deg(h) < \deg(f)$. Uit de inductiehypothese weten we dat $h(x) = g\big(x^{p^n}\big)$ voor een zekere $n \geq 0$ en een zeker irreducibel separabel polynoom $g \in F[x]$, en dus is $f(x) = g\big(x^{p^{n+1}}\big)$. □

We komen nu tot het beloofde verband met niet-perfecte velden.

Stelling 4.8.7. *Zij $f \in F[x]$ een inseparabel polynoom. Dan is F niet perfect. In het bijzonder is* $\mathrm{char}(F) > 0$ *en is F oneindig.*

Bewijs. Zonder verlies van algemeenheid mogen we aannemen dat f irreducibel is. Dan heeft f meervoudige wortels, en uit Gevolg 4.8.5 weten we dat $\mathrm{char}(F) = p > 0$ en $f(x) = g(x^p)$ voor een zekere $g \in F[x]$.

Als F wel perfect zou zijn, dan zou elke coëfficiënt van g een p-de macht zijn, zodat

$$g(x) = \sum_{i=0}^{n/p} b_i^p x^i$$

voor zekere $b_i \in F$. Maar dan zou

$$f(x) = g(x^p) = \sum_{i=0}^{n/p} b_i^p x^{pi} = \Big(\sum_{i=0}^{n/p} b_i x^i\Big)^p,$$

in strijd met de irreducibiliteit van f. We besluiten dat F niet perfect is. □

Gevolg 4.8.8. *Veronderstel dat F een perfect veld is. Dan is elke algebraische velduitbreiding van F separabel.*

Bewijs. Dit volgt onmiddellijk uit Stelling 4.8.7. □

In feite karakteriseert deze eigenschap perfecte velden; zie Gevolg 4.8.12 verderop.

Zij E/F een algebraïsche velduitbreiding. Per definitie is deze uitbreiding separabel als elk element van E separabel is over F. Het meest extreme tegenovergestelde van deze situatie is deze van de zuiver inseparabele velduitbreidingen.

Definitie 4.8.9. Zij E/F een algebraïsche velduitbreiding. Dan wordt E/F *zuiver inseparabel* genoemd als geen enkel element van $E \setminus F$ separabel is.

Een triviaal voorbeeld van een zuiver inseparabele velduitbreiding is F/F. Echter, een niet-triviale zuiver inseparabele velduitbreiding E/F is niet separabel, en kan dus enkel bestaan voor niet-perfecte velden F. Voor we meer voorbeelden geven, geven we eerst een zeer nuttige karakterisatie van deze uitbreidingen.

Stelling 4.8.10. *Zij E/F een algebraïsche velduitbreiding met* $\mathrm{char}(F) = p > 0$. *Dan zijn volgende eigenschappen equivalent:*

(a) *E/F is zuiver inseparabel.*

(b) *Voor elke $\alpha \in E$ bestaat er een $n \geq 0$ zodat $\alpha^{p^n} \in F$.*

(c) *Elk element van E heeft een irreducibel polynoom over F van de vorm $x^{p^n} - a$ voor een zekere $n \geq 0$ en een zekere $a \in F$.*

Bewijs. (a) $\Rightarrow$ (b). Veronderstel dat E/F zuiver inseparabel is, en zij $\alpha \in E$ willekeurig. Zij $f = \min_F(\alpha)$; wegens Gevolg 4.8.6 is $f(x) = g\big(x^{p^n}\big)$ voor een zekere $n \geq 0$ en een zeker irreducibel separabel polynoom $g \in F[x]$. Dan is $g\big(\alpha^{p^n}\big) = f(\alpha) = 0$, en bijgevolg is $g = \min_F\big(\alpha^{p^n}\big)$. Hieruit volgt dat α^{p^n} een separabel element is, maar omdat E/F zuiver inseparabel is, besluiten we dat $\alpha^{p^n} \in F$.

(b) $\Rightarrow$ (c). Zij $\alpha \in E$. Wegens de veronderstelling is er een $n \geq 0$ zodat $\alpha^{p^n} \in F$, en dus is α een wortel van $g(x) = x^{p^n} - \alpha^{p^n} \in F[x]$. Aangezien $g(x) = (x-\alpha)^{p^n}$ heeft elke monische irreducibele factor f van g in $F[x]$ noodzakelijk de vorm $f(x) = (x-\alpha)^r$ voor een zekere $r > 0$. In het bijzonder is $f(\alpha) = 0$, maar dan is $f = \min_F(\alpha)$. Aangezien f een willekeurige monische irreducibele factor van g was, besluiten we dat g een macht is van $\min_F(\alpha)(x) = (x-\alpha)^r$, en dus is $r \mid p^n$, stel $r = p^m$ voor een zekere $m \geq 0$. Dan is $f(x) = x^{p^m} - a$ met $a = \alpha^{p^m}$.

(c) $\Rightarrow$ (a). Veronderstel dat $\alpha \in E$ separabel is over F. Zij $f = \min_F(\alpha)$; per veronderstelling is dan $f(x) = x^{p^n} - a$ voor een zekere $n \geq 0$ en een zekere $a \in F$. Uiteraard is dan $a = \alpha^{p^n}$, en dus is $f(x) = (x-\alpha)^{p^n}$. Aangezien f irreducibel en separabel is over F, heeft het geen meervoudige wortels. Dit kan enkel als $n = 0$, en dan is $a = \alpha \in F$. □

Deze karakterisatie stelt ons in staat om zuiver inseparabele uitbreidingen te construeren.

Gevolg 4.8.11. *Zij F een veld met* $\mathrm{char}(F) = p > 0$. *Veronderstel dat $E = F[\alpha]$ en dat $\alpha^{p^n} \in F$ voor een zekere $n \geq 0$. Dan is E/F een zuiver inseparabele velduitbreiding.*

Bewijs. Zij $\beta \in E$ willekeurig. Wegens Stelling 4.8.10 volstaat het om een $\ell \geq 0$ te vinden zodat $\beta^{p^\ell} \in F$. Omdat $E = F[\alpha]$ kunnen we $\beta = f(\alpha)$ schrijven voor een zeker polynoom $f \in F[x]$, en dus is

$$\beta = a_m\alpha^m + \cdots + a_1\alpha + a_0,$$

waarbij de coëfficiënten a_i in F liggen. Dan is

$$\beta^{p^n} = a_m^{p^n}(\alpha^{p^n})^m + \cdots + a_1^{p^n}\alpha^{p^n} + a_0^{p^n},$$

en aangezien $\alpha^{p^n} \in F$ is ook $\beta^{p^n} \in F$. □

Met behulp van dit gevolg zien we dat elk niet-perfect veld een zuiver inseparabele uitbreiding heeft:

Gevolg 4.8.12. *Zij F een niet-perfect veld, en stel $p = \mathrm{char}(F)$. Zij $a \in F \setminus F^p$ willekeurig, en stel $f(x) = x^p - a \in F[x]$. Zij E het splijtveld van f over F. Dan is $E \cong F[x]/(x^p - a)$, en E/F is een zuiver inseparabele velduitbreiding.*

Bewijs. Het polynoom $f \in F[x]$ heeft geen wortels in F. Kies een $\alpha \in E$ met $f(\alpha) = 0$; dan is $F[\alpha] > F$. Aangezien $\alpha^p = a \in F$, volgt er uit Gevolg 4.8.11 dat $F[\alpha]/F$ een zuiver inseparabele uitbreiding is. Anderzijds is $f(x) = x^p - \alpha^p = (x-\alpha)^p$, zodat α de enige wortel is van f in E. Aangezien E als splijtveld is voortgebracht over F door de wortels van f, besluiten we dat $E = F[\alpha]$. □

Uiteraard is niet elke algebraïsche velduitbreiding separabel of zuiver inseparabel. Nochtans zullen we wel in staat zijn om voor elke algebraïsche uitbreiding E/F een tussenveld K te vinden zodat E/K zuiver inseparabel is en K/F separabel is. We stellen eerst vast dat inseparabiliteit een "stabiele" eigenschap is met betrekking tot tussenvelden.

Lemma 4.8.13. *Zij E/F een velduitbreiding, en K een tussenveld. Dan is E/F zuiver inseparabel als en slechts als E/K en K/F zuiver inseparabel zijn.*

Bewijs. Veronderstel eerst dat E/F zuiver inseparabel is, m.a.w. voor elke $\alpha \in E$ is er een $n \geq 0$ zodat $\alpha^{p^n} \in F$ (zie Stelling 4.8.10). Het is triviaal dat dan ook E/K en K/F aan deze eigenschap voldoen en dus ook zuiver inseparabel zijn.

Veronderstel omgekeerd dat E/K en K/F zuiver inseparabel zijn. We mogen uiteraard veronderstellen dat $E > F$, dus ten minste één van de uitbreidingen E/K of K/F is niet triviaal, en dus is $\mathrm{char}(F) = p > 0$. Zij nu $\alpha \in E$ willekeurig. Uit Stelling 4.8.10 toegepast op E/K weten we dat $\alpha^{p^n} \in K$ voor een zekere $n \geq 0$, en uit diezelfde stelling toegepast op K/F volgt dan dat $\left(\alpha^{p^n}\right)^{p^m} \in F$ voor een zekere $m \geq 0$. Dus $\alpha^{p^{n+m}} \in F$, en dus is E zuiver inseparabel over F. □

Lemma 4.8.14. *Zij E/F een zuiver inseparabele velduitbreiding van eindige graad. Dan is $[E : F]$ een macht van p.*

Bewijs. We bewijzen dit per inductie op $[E : F]$, waarbij we niets moeten bewijzen indien $[E : F] = 1$. Zij dus $E > F$, en kies een $\alpha \in E \setminus F$. Dan is $[E : F[\alpha]] < [E : F]$, zodat uit de inductiehypothese volgt dat $[E : F[\alpha]]$ een macht is van p, omdat $E/F[\alpha]$ opnieuw zuiver inseparabel is wegens Lemma 4.8.13. Anderzijds is $[F[\alpha] : F]$ gelijk aan de graad van $\min_F(\alpha)$, wat een macht van p is wegens Stelling 4.8.10. Het resultaat volgt. □

In het bewijs Stelling 4.8.16 zullen we het volgend hulpresultaat nodig hebben.

Lemma 4.8.15. *Zij E/F een velduitbreiding zodat $E = F[\alpha, \beta]$, waarbij α en β separabel zijn over F. Dan is E/F een separabele velduitbreiding.*

Bewijs. Zij $f = \min_F(\alpha) \min_F(\beta)$, en merk op dat f separabel is over F. Zij L het splijtveld van f over E; dan is L ook een splijtveld van f over F, want $E = F[\alpha, \beta]$, waarbij α en β wortels zijn van f. Uit Stelling 4.4.2 volgt dan dat L/F separabel (en zelfs Galois) is, en dus is ook E/F separabel. □

We komen nu tot het resultaat dat ons toelaat om op natuurlijke wijze een algebraïsche uitbreiding "op te splitsen" in een separabel en een zuiver inseparabel deel.

Stelling 4.8.16. *Zij E/F een algebraïsche velduitbreiding, en stel*

$$K = \{\alpha \in E \mid \alpha \text{ is separabel over } F\}.$$

Dan is K een veld. Het is het unieke tussenveld dat separabel is over F en waarover E zuiver inseparabel is.

Bewijs. Zij $\alpha, \beta \in K$. Uit Lemma 4.8.15 weten we dat het volledige veld $F[\alpha, \beta]$ bevat is in K, zodat in het bijzonder $\alpha - \beta$ en α/β (als $\beta \neq 0$) bevat zijn in K. Dit toont aan dat K een veld is, en uit de definitie van K is het evident dat K dan separabel is over F.

We tonen nu aan dat E zuiver inseparabel is over K. Als F perfect is, dan is $K = E$ en valt er niks te bewijzen; we veronderstellen dus dat F niet perfect is, en in het bijzonder is dan $\text{char}(F) = p > 0$. Zij $\alpha \in E$ willekeurig, en zij $f = \min_F(\alpha)$. We gebruiken Gevolg 4.8.6 om $f(x) = g(x^{p^n})$ te schrijven voor een zekere $n \geq 0$ en een zeker irreducibel separabel polynoom $g \in F[x]$. Dan is g het irreducibel polynoom over F van het element $\alpha^{p^n} \in E$. Omdat g separabel is, volgt hieruit dat $\alpha^{p^n} \in K$. Uit Stelling 4.8.10 volgt nu dat E/K zuiver inseparabel is.

Ten slotte veronderstellen we dat $F \leq T \leq E$ zodat T/F separabel is en E/T zuiver inseparabel is. Uit de definitie van K volgt dat $T \leq K \leq E$, en omdat E/T zuiver inseparabel is, volgt uit Lemma 4.8.13 dat ook K/T zuiver inseparabel is. Anderzijds echter is K separabel over F, zodat K ook separabel is over het tussenveld T (zie Lemma 4.3.11). Dus K/T is tegelijk separabel en zuiver inseparabel, wat enkel kan als $T = K$. □

Een gevolg van Stelling 4.8.16 is dat ook het omgekeerde van Lemma 4.3.11 geldig is.

Gevolg 4.8.17. *Zij E/F een velduitbreiding, en zij L een tussenveld. Veronderstel dat zowel E/L als L/F separabel zijn. Dan is ook E/F separabel.*

Bewijs. Zij $K = \{\alpha \in E \mid \alpha \text{ is separabel over } F\}$ zoals in Stelling 4.8.16. Aangezien L/F separabel is, is $L \leq K \leq E$. Verder is ook E/L separabel, en uit Lemma 4.3.11 volgt dan dat ook E/K separabel is. Wegens Stelling 4.8.16 echter is E/K zuiver inseparabel, en dus is $K = E$, waaruit volgt dat E/F separabel is. □

Opmerking 4.8.18. Stelling 4.8.16 vertelt ons dat een willekeurige algebraische uitbreiding E/F kan beschouwd worden als twee opeenvolgende uitbreidingen: eerst een separabele uitbreiding K/F, en vervolgens een inseparabele uitbreiding E/K. Het is een natuurlijke vraag of dit ook in de omgekeerde volgorde kan: kunnen we elke algebraïsche uitbreiding bekomen door eerst een inseparabele uitbreiding te beschouwen en die vervolgens separabel verder uit te breiden? Deze vraag heeft in het algemeen een negatief antwoord. Ze heeft wel een positief antwoord voor *normale* uitbreidingen van eindige graad. Meer bepaald geldt dat, indien E/F een normale uitbreiding is van eindige graad, en $K = \mathrm{Fix}(\mathrm{Gal}(E/F))$, dan is E/K separabel en is K/F zuiver inseparabel. (Het feit dat E/K separabel is volgt onmiddellijk uit Lemma 4.1.13; het feit dat K/F zuiver inseparabel is, is een interessante oefening.)

Tot slot geven we nog het bewijs mee van Stelling 3.4.6 (zie p. 49).

Stelling 4.8.19. *Zij E/F een algebraïsche velduitbreiding met de eigenschap dat elk polynoom $f \in F[x]$ met $\deg(f) \geq 1$ ten minste 1 wortel heeft in E. Dan is E een algebraïsche sluiting van F.*

Bewijs. We veronderstellen eerst dat E/F een separabele uitbreiding is. Zij $f \in F[x]$ een willekeurig niet-nul polynoom; we moeten bewijzen dat f splijt over E. We mogen veronderstellen dat f irreducibel is en monisch; aangezien f ten minste 1 wortel α heeft in E, is $f = \min_F(\alpha)$, en wegens de separabiliteit heeft f geen meervoudige wortels.

Zij nu L een splijtveld voor f over F. Aangezien f separabel is over F, is L/F wegens Stelling 4.4.2 Galois, en dus ook separabel. Uit de stelling van het primitieve element (Stelling 4.5.1) volgt dat $L = F[\beta]$ voor een zekere $\beta \in L$. Stel $g = \min_F(\beta)$.

Per veronderstelling heeft ook g een wortel $\gamma \in E$, en uit Stelling 3.1.15 volgt dat $L = F[\beta]$ isomorf is met $F[\gamma] \leq E$. Bijgevolg is $F[\gamma]$ een splijtveld voor f over F, en dus splijt f over E, wat we moesten bewijzen.

We veronderstellen nu dat $\text{char}(F) = p > 0$ en dat E/F niet noodzakelijk separabel is. Stel

$$K = \{\alpha \in E \mid \alpha^{p^n} \in F \text{ voor een zekere } n \geq 0\},$$

en merk op dat K een deelveld is van E. We beweren dat K perfect is. Inderdaad, zij $\alpha \in K$ willekeurig; dan is $\alpha^{p^n} \in F$ voor een zekere n, en dus ligt het polynoom $x^{p^{n+1}} - \alpha^{p^n}$ in $F[x]$, waaruit volgt dat het een wortel $\beta \in E$ heeft wegens de veronderstelling. Dan is

$$0 = \beta^{p^{n+1}} - \alpha^{p^n} = (\beta^p - \alpha)^{p^n},$$

en dus is $\beta^p = \alpha$. Merk op dat $\beta \in K$ omdat $\beta^{p^{n+1}} = \alpha^{p^n} \in F$, en dus is α de p-de macht van een ander element van K. Dit toont aan dat K inderdaad perfect is.

Aangezien K perfect is, is E/K separabel, en dus kunnen we het eerste deel van het bewijs toepassen op E/K, op voorwaarde dat we kunnen aantonen dat elk niet-constant polynoom $g \in K[x]$ een wortel heeft in E. Stel dus

$$g(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x].$$

Per definitie van K kunnen we een $r \geq 0$ vinden zodat $(a_i)^{p^r} \in F$ voor alle $i \in \{0, \ldots, n\}$. Hieruit volgt dan dat $g(x)^{p^r} \in F[x]$, en wegens de veronderstelling bestaat er een $\alpha \in E$ zodat $g(\alpha)^{p^r} = 0$, maar dan is ook $g(\alpha) = 0$, en dit besluit het bewijs. □

4.9 Radicale uitbreidingen

In deze voorlaatste sectie willen we het resultaat van Galois aantonen, dat de oplosbaarheid van polynomen in verband brengt met de oplosbaarheid van de corresponderende Galoisgroep. Zoals we hebben gezien in de inleiding van dit hoofdstuk (zie p. 57), zeggen we dat een polynoom oplosbaar is in radicalen, als we de wortels expliciet kunnen beschrijven met behulp van de elementaire operaties optellen, aftrekken, vermenigvuldigen, delen en n-de machtswortels nemen. Het cruciale begrip om controle te krijgen over de n-de machtwortels zijn de radicale velduitbreidingen.

Definitie 4.9.1. (i) Een velduitbreiding E/F wordt *radicaal* genoemd, als $E = F[\alpha]$ waarbij α een wortel is van een polynoom f van de vorm $f(x) = x^n - a$ (met $a \in F$). Anders gezegd, E/F is radicaal als het over F wordt voortgebracht door een element $\alpha \in E$ waarvoor $\alpha^n \in F$ voor zekere $n > 0$.

(ii) Een velduitbreiding E/F is een *herhaalde radicale uitbreiding* als er velden F_i zijn met

$$F = F_0 \leq F_1 \leq \cdots \leq F_r = E$$

zodat elke F_i een radicale uitbreiding van F_{i-1} is, voor $1 \leq i \leq r$.

(iii) Zij F een veld, en $f \in F[x]$. Dan is f *oplosbaar in radicalen* over F als er een herhaalde radicale uitbreiding is van F waarover f splijt.

De complexe getallen die we kunnen beschrijven vanuit de gehele getallen met behulp van de elementaire operaties optellen, aftrekken, vermenigvuldigen, delen en n-de machtswortels nemen, zijn precies die elementen die in een herhaalde radicale uitbreiding van $\mathbb{Q}$ liggen. Zie echter ook Opmerking 4.9.17 verderop.

Voorbeeld 4.9.2. (1) Als F een eindig veld is, dan is elke eindige velduitbreiding E/F een radicale uitbreiding. Inderdaad, als $E = \mathbb{F}_q$, dan volgt uit Stelling 3.5.2 dat elke $\alpha \in E^\times$ voldoet aan $\alpha^{q-1} - 1 = 0$.

(2) Zij $n \geq 1$ een natuurlijk getal, en $f \in \mathbb{Q}[x]$ het polynoom $f(x) = x^n - 1$. Het splijtveld L_n van f in $\mathbb{C}$ over $\mathbb{Q}$ noemen we het *n-de cyclotomische veld*. De velduitbreiding $L_n/\mathbb{Q}$ is een radicale uitbreiding, met Galoisgroep $\mathrm{Gal}(L_n/\mathbb{Q}) \cong \mathrm{Aut}(\mathbf{C}_n) \cong (\mathbb{Z}/n)^\times$, een abelse groep van orde $\phi(n)$ (waarbij ϕ de Euler totiënt-functie is). Zie ook Lemma 4.9.6 verderop.

Uiteraard zullen n-de machtswortels van 1 een bijzondere rol spelen bij het bestuderen van algemene n-de machtswortels. Daar gaan we nu eerst wat dieper op in.

Definitie 4.9.3. Zij F een veld, en $\zeta \in F \setminus \{0\}$.

(i) Het element ζ wordt een *eenheidswortel* genoemd, als ζ eindige orde heeft in de multiplicatieve groep $F^\times$, i.e. als $\zeta^n = 1$ voor een natuurlijk getal $n \geq 1$. In dat geval wordt het ook een *n-de eenheidswortel* genoemd.

(ii) Het element ζ wordt een *primitieve n-de eenheidswortel* genoemd, als ζ orde n heeft in de multiplicatieve groep $F^\times$, i.e. als $\zeta^n = 1$ maar $\zeta^m \neq 1$ voor $1 \leq m < n$.

(iii) De verzameling van alle n-de eenheidswortels van F noteren we als $\mu_n(F)$.

Lemma 4.9.4. *Zij F een veld, en stel $n \geq 1$. Dan vormt $\mu_n(F)$ een cyclische deelgroep van $F^\times$ met orde een deler van n. We hebben $|\mu_n(F)| = n$ als en slechts als F een primitieve n-de eenheidswortel bezit.*

Bewijs. Dit is een eenvoudige oefening, gebruik makend van Opmerking 3.5.4. □

We kunnen een veld van karakteristiek 0 altijd uitbreiden tot een veld dat een primitieve n-de eenheidswortel bevat:

Lemma 4.9.5. *Zij F een veld met $\mathrm{char}(F) = 0$, en n een positief geheel getal. Dan bestaat er een velduitbreiding E/F zodat E een primitieve n-de eenheidswortel ζ bevat, en $E = F[\zeta]$.*

Bewijs. Stel $f(x) = x^n - 1$; dan is $f \in F[x]$. Omdat $\mathrm{char}(F) = 0$ heeft $f'(x) = nx^{n-1}$ enkel $x = 0$ als wortel, en dus hebben f en f' geen gemeenschappelijke wortels (over elke uitbreiding L/F). Uit Lemma 4.3.3 volgt dan dat f geen meervoudige wortels heeft. Zij nu L een splijtveld voor f over F; dan heeft f juist n wortels in L, en uit Lemma 4.9.4 volgt dat L een primitieve n-de eenheidswortel ζ bezit. Stel nu $E = F[\zeta] \leq L$. □

Het is eenvoudig om de Galoisgroep te bepalen van de velduitbreiding die we krijgen door een n-de eenheidswortel toe te voegen:

Lemma 4.9.6. *Zij E/F een velduitbreiding met $E = F[\zeta]$, waarbij ζ een eenheidswortel is. Stel $C = \langle\zeta\rangle \leq E^\times$; dus C is een eindige cyclische groep. Dan is E/F Galois, en $G = \mathrm{Gal}(E/F)$ is isomorf met een deelgroep van $\mathrm{Aut}(C)$. In het bijzonder is G abels.*

Bewijs. Zij n de orde van ζ in $E^\times$; dan is ζ een primitieve n-de eenheidswortel, en E is een splijtveld voor $f(x) = x^n - 1$ over F. Aangezien f juist n verschillende wortels heeft in E, is f separabel over F. We besluiten dat E/F Galois is.

Als $\sigma \in G = \mathrm{Gal}(E/F)$, dan is ζ^σ opnieuw een n-de eenheidswortel, en dus is $\zeta^\sigma \in C$. Dus σ beeldt C af in zichzelf, en omdat C eindig is volgt hieruit dat de restrictie van σ tot C een automorfisme van C is. We krijgen dus een morfisme $\rho\colon G \to \mathrm{Aut}(C)$, en dit morfisme heeft een triviale kern, want als $\zeta^\sigma = \zeta$ voor een $\sigma \in G$, dan is $\sigma = 1$ want $E = F[\zeta]$. □

Ons eerste doel is om een methode te vinden om aan te tonen dat een velduitbreiding radicaal is. Dit zullen we doen met een resultaat van Kummer (Stelling 4.9.9), waarvoor we eerst twee lemma's bewijzen.

Lemma 4.9.7 (Dedekind)**.** *Zij E een veld. Dan is $\mathrm{Aut}(E)$ een lineair onafhankelijke deelverzameling van de E-vectorruimte van alle functies van E*

naar E. Anders gezegd: zij S een eindige verzameling van automorfismen van E, en zij voor elke $\sigma \in S$ een element $t_\sigma \in E$ gegeven zodat

$$\sum_{\sigma \in S} t_\sigma \alpha^\sigma = 0 \qquad (*)$$

voor alle $\alpha \in E$. Dan is $t_\sigma = 0$ voor alle $\sigma \in S$.

Bewijs. We bewijzen dit per inductie op $|S|$. Indien $|S| = 1$, stel $S = \{\sigma\}$, dan volgt uit $(*)$ dat $t_\sigma 1^\sigma = 0$ en dus $t_\sigma = 0$.

Veronderstel nu dat $|S| > 1$, en beschouw een vaste $\tau \in S$ en $\beta \in E$. Door $(*)$ te vermenigvuldigen met β^τ bekomen we

$$\sum_{\sigma \in S} t_\sigma \alpha^\sigma \beta^\tau = 0 \quad \text{voor alle } \alpha \in E.$$

Anderzijds kunnen we in $(*)$ $\alpha\beta$ substitueren voor α, en dus

$$\sum_{\sigma \in S} t_\sigma \alpha^\sigma \beta^\sigma = 0 \quad \text{voor alle } \alpha \in E.$$

De twee voorgaande vergelijkingen van elkaar aftrekken levert

$$\sum_{\sigma \in S \setminus \{\tau\}} t_\sigma (\beta^\tau - \beta^\sigma) \alpha^\sigma = 0 \quad \text{voor alle } \alpha \in E.$$

Wegens de inductiehypothese, toegepast op $S' = S \setminus \{\tau\}$ en $t'_\sigma = t_\sigma(\beta^\tau - \beta^\sigma)$ voor alle $\sigma \in S$, besluiten we hieruit dat

$$t_\sigma(\beta^\tau - \beta^\sigma) = 0 \quad \text{voor alle } \sigma \in S \setminus \{\tau\}.$$

Indien er een $\sigma \in S \setminus \{\tau\}$ zou zijn met $t_\sigma \neq 0$, dan zou $\beta^\sigma = \beta^\tau$, en dit voor alle $\beta \in E$, waaruit zou volgen dat $\sigma = \tau$, een contradictie. We besluiten dat $t_\sigma = 0$ voor alle $\sigma \in S \setminus \{\tau\}$, en aangezien $\tau \in S$ willekeurig gekozen was, besluiten we dat $t_\sigma = 0$ voor alle $\sigma \in S$. □

Lemma 4.9.8. *Zij E/F een eindige velduitbreiding met Galoisgroep $G = \mathrm{Gal}(E/F)$. Veronderstel dat $\theta\colon G \to F^\times$ een groepsmorfisme is. Dan bestaat er een $\alpha \in E^\times$ zodat $\theta(\tau) = \alpha^\tau/\alpha$ voor alle $\tau \in G$.*

Bewijs. Voor elke $\sigma \in G$ stellen we $t_\sigma = \theta(\sigma) \in E$; dan is $t_\sigma \neq 0$ voor alle $\sigma \in G$, en uit Lemma 4.9.7 volgt dat er een $\gamma \in E$ bestaat met

$$c := \sum_{\sigma \in G} \theta(\sigma) \gamma^\sigma \neq 0.$$

Stel $\alpha = c^{-1} \in E^\times$; we beweren dat $\theta(\tau) = \alpha^\tau/\alpha$ voor alle $\tau \in G$.

Zij dus $\tau \in G$ willekeurig. Aangezien $\sigma\tau$ loopt over alle elementen van G als σ dat doet, hebben we

$$\alpha^{-1} = \sum_\sigma \theta(\sigma\tau)\gamma^{\sigma\tau} = \sum_\sigma \theta(\sigma)\theta(\tau)\gamma^{\sigma\tau} = \Big(\sum_\sigma \theta(\sigma)\gamma^\sigma\Big)^\tau \theta(\tau),$$

waarbij we gebruikt hebben dat $\theta(\sigma) \in F = \mathrm{Fix}(G)$. Hieruit volgt dat $\alpha^{-1} = \alpha^{-\tau}\theta(\tau)$, waaruit het gestelde volgt. □

We komen nu tot het beloofde resultaat van Kummer.

Stelling 4.9.9 (Kummer)**.** *Zij E/F een velduitbreiding, en veronderstel dat F een primitieve n-de eenheidswortel ζ bevat. Dan zijn de volgende uitspraken equivalent:*

(a) *E/F is Galois, en $\mathrm{Gal}(E/F)$ is cyclisch van orde een deler van n.*

(b) *$E = F[\alpha]$ voor een $\alpha \in E$ met $\alpha^n \in F$.*

Bewijs. Zij $\zeta \in F$ een primitieve n-de eenheidswortel.

(a) $\Rightarrow$ (b). Zij $G = \mathrm{Gal}(E/F) = \langle\sigma\rangle$, met $o(\sigma) = m \mid n$. Anderzijds is $\langle\zeta\rangle$ cyclisch van orde n, dus is er een unieke cyclische deelgroep $H \leq \langle\zeta\rangle$ van orde m. Er bestaat dus een monomorfisme

$$\theta\colon G \to \langle\zeta\rangle \leq F^\times$$

met $\mathrm{im}(\theta) = H$. Uit Lemma 4.9.8 halen we een $\alpha \in E^\times$ zodat $\theta(\tau) = \alpha^\tau/\alpha$ voor alle $\tau \in G$. Stel dan $\delta = \theta(\sigma)$; dan is δ een n-de eenheidswortel in F, en $\delta = \alpha^\sigma/\alpha$. Hieruit volgt $(\alpha^n)^\sigma = (\alpha^\sigma)^n = (\alpha\delta)^n = \alpha^n$, en dus is $\alpha^n \in \mathrm{Fix}(\langle\sigma\rangle) = F$.
Om aan te tonen dat $E = F[\alpha]$ nemen we $\tau \in \mathrm{Gal}(E/F[\alpha]) \leq G$ willekeurig. Dan is $\theta(\tau) = \alpha^\tau/\alpha = 1$, en dus is $\tau = 1$ omdat θ injectief is. Hieruit volgt dat $\mathrm{Gal}(E/F[\alpha]) = 1$, en uit de hoofdstelling van de Galoistheorie volgt nu dat $F[\alpha] = E$, waaruit (b) volgt.

(b) $\Rightarrow$ (a). Veronderstel omgekeerd dat $E = F[\alpha]$ voor een $\alpha \in E$ met $\alpha^n \in F$; we mogen uiteraard veronderstellen dat $\alpha \neq 0$. Beschouw $f(x) = x^n - \alpha^n$, zodat $f \in F[x]$. Voor elke n-de eenheidswortel δ in E hebben we $f(\alpha\delta) = (\alpha\delta)^n - \alpha^n = 0$, dus is $\alpha\delta$ een wortel van f. Aangezien E juist n verschillende n-de eenheidswortels bezit, vinden we op die manier n verschillende wortels van f in E. Bijgevolg splijt f over E en heeft het geen meervoudige wortels. Aangezien α een wortel

is van f, zien we dat $E = F[\alpha]$ een splijtveld is voor f over F, en omdat f separabel is over F volgt er dat E/F Galois is.
Stel nu $G = \mathrm{Gal}(E/F)$. Het volstaat nu een monomorfisme $\theta\colon G \to \langle\zeta\rangle$ te construeren; daaruit volgt dan dat G cyclisch is van orde een deler van n. Aangezien G de wortels van f permuteert, hebben we, voor elke $\tau \in G$, dat $\alpha^\tau = \alpha\delta$ voor een zekere $\delta \in \langle\zeta\rangle$, of dus $\alpha^\tau/\alpha \in \langle\zeta\rangle$. Definieer nu

$$\theta\colon G \to \langle\zeta\rangle\colon \tau \mapsto \alpha^\tau/\alpha.$$

Voor alle $\sigma, \tau \in G$ hebben we dan

$$\theta(\sigma\tau) = \alpha^{\sigma\tau}/\alpha = \left(\alpha^\sigma/\alpha\right)^\tau\left(\alpha^\tau/\alpha\right) = \theta(\sigma)^\tau\theta(\tau).$$

Echter, $\zeta \in F$, en dus is $\theta(\sigma) \in F$ zodat $\theta(\sigma)^\tau = \theta(\sigma)$. Hieruit volgt dat θ een groepsmorfisme is. Veronderstel tot slot dat $\theta(\tau) = 1$ voor $\tau \in G$; dan is $\alpha^\tau = \alpha$, en omdat $E = F[\alpha]$ volgt hieruit dat $\tau = 1$, en dus is θ injectief. □

Opmerking 4.9.10. Een velduitbreiding E/F wordt een *Kummer-uitbreiding* genoemd als F een primitieve n-de eenheidswortel bevat en $\mathrm{Gal}(E/F)$ een abelse groep is van exponent n, voor een zekere n. Stelling 4.9.9 is een eerste resultaat in de zogenaamde Kummertheorie.

De stelling van Kummer geeft een verband tussen radicale uitbreidingen enerzijds, en Galois-uitbreidingen met een cyclische Galoisgroep anderzijds. Ons doel is om dit uit te breiden naar een verband tussen herhaalde radicale uitbreidingen enerzijds, en Galois-uitbreidingen met een oplosbare Galoisgroep anderzijds. Bovendien moeten we de extra assumptie aanwezig in de stelling van Kummer, met name het bestaan van een primitieve n-de eenheidswortel, zien kwijt te raken.

Het volgend resultaat, dat gebruik maakt van de stelling van de natuurlijke irrationaliteiten, laat ons toe om de stap te maken van abelse Galoisgroepen naar oplosbare Galoisgroepen.

Lemma 4.9.11. *Zij $F = F_0 \leq F_1 \leq \cdots \leq F_r = L$, waarbij elk van de uitbreidingen F_i/F_{i-1} Galois is met een abelse Galoisgroep. Zij E een tussenveld van L/F, en veronderstel dat E/F Galois is. Dan is* $\mathrm{Gal}(E/F)$ *een oplosbare groep.*

Bewijs. We bewijzen dit per inductie op r, waarbij het geval $r = 0$ triviaal is; stel dus $r > 0$. Stel $M = E \cap F_1$ en $K = \langle E, F_1\rangle \leq L$, en merk op dat E/M Galois is. Uit de stelling van de natuurlijke irrationaliteiten (Stelling 4.7.1) volgt nu dat ook K/F_1 Galois is, en dat

$$\mathrm{Gal}(K/F_1) \cong \mathrm{Gal}(E/M).$$

We kunnen dus de inductiehypothese toepassen op het tussenveld K van L/F_1, en we halen hieruit dat $\mathrm{Gal}(K/F_1)$ oplosbaar is; bijgevolg is ook $\mathrm{Gal}(E/M)$ oplosbaar.

Stel nu $G = \mathrm{Gal}(E/F)$ en $N = \mathrm{Gal}(E/M)$; we beweren dat $N \trianglelefteq G$ en dat zowel N als G/N oplosbaar zijn. Welnu, we hebben $F \leq M \leq F_1$, en $\mathrm{Gal}(F_1/M) \trianglelefteq \mathrm{Gal}(F_1/F)$ omdat $\mathrm{Gal}(F_1/F)$ een abelse groep is. Uit de hoofdstelling van de Galoistheorie, toegepast op de uitbreiding F_1/F, volgt dan dat M/F Galois is, en

$$\mathrm{Gal}(M/F) \cong \mathrm{Gal}(F_1/F) \,/\, \mathrm{Gal}(F_1/M);$$

in het bijzonder is $\mathrm{Gal}(M/F)$ abels. Door de hoofdstelling van de Galoistheorie nu nogmaals toe te passen, dit keer op de uitbreiding E/F, volgt dat inderdaad $N = \mathrm{Gal}(E/M) \trianglelefteq \mathrm{Gal}(E/F) = G$, en nog uit die hoofdstelling volgt ook dat

$$G/N = \mathrm{Gal}(E/F) \,/\, \mathrm{Gal}(E/M) \cong \mathrm{Gal}(M/F).$$

We besluiten dat G een groep is met een oplosbare normaaldeler N zodat G/N oplosbaar (zelfs abels) is, en uit Stelling 1.3.7 volgt dat ook G oplosbaar is. □

We zijn nu genoeg voorbereid om de stelling van Galois onder handen te nemen.

Stelling 4.9.12 (Galois)**.** *Zij F een veld met $\mathrm{char}(F) = 0$, zij $f \in F[x]$, en zij E een splijtveld van f over F. Dan is f oplosbaar in radicalen over F als en slechts als $\mathrm{Gal}(E/F)$ een oplosbare groep is.*

Bewijs. Veronderstel eerst dat $\mathrm{Gal}(E/F)$ oplosbaar is. Stel $n = [E : F]$. Om de stelling van Kummer te kunnen toepassen, willen we eerst een primitieve n-de eenheidswortel toevoegen aan E. Uit Lemma 4.9.5 weten we dat er een velduitbreiding E^*/E is zodat $E^* = E[\zeta]$, waarbij ζ een primitieve n-de eenheidswortel is.

Stel nu $F^* = F[\zeta] \leq E^*$, en merk op dat $E^* = \langle F^*, E\rangle$. Stel verder $M = F^* \cap E$, dus $F \leq M$. Uit de stelling van de natuurlijke irrationaliteiten (Stelling 4.7.1) volgt dat E^*/F^* Galois is, en dat

$$\mathrm{Gal}(E^*/F^*) \cong \mathrm{Gal}(E/M) \leq \mathrm{Gal}(E/F),$$

zodat in het bijzonder $\mathrm{Gal}(E^*/F^*)$ ook oplosbaar is.

Stel $G = \mathrm{Gal}(E^*/F^*)$, en zij

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

een compositierij voor G (zie Definitie 1.1.10). Uit Gevolg 1.3.10 weten we dat elke compositiefactor G_i/G_{i-1} cyclisch is van priemorde. Stel dus $[G_i : G_{i-1}] = p_i$ en $K_i = \mathrm{Fix}_{E^*}(G_i)$ voor elke i; dan is

$$F^* = K_r \leq K_{r-1} \leq \cdots \leq K_0 = E^*,$$

en K_{i-1}/K_i is Galois, met een cylische Galoisgroep van orde p_i, voor elke i. Merk ook op dat elke p_i een deler is van $|G|$, en dus ook van $n = |\mathrm{Gal}(E/F)|$.

Uit de stelling van Kummer (Stelling 4.9.9) volgt nu dat de uitbreidingen K_{i-1}/K_i radicaal zijn. Aangezien ook de uitbreiding F^*/F radicaal is, besluiten we dat E^* een herhaalde radicale uitbreiding is van F waarover f splijt. Anders gezegd, f is oplosbaar in radicalen over F.

Veronderstel nu omgekeerd dat $f \in F[x]$ oplosbaar is in radicalen over F, en zij L een herhaalde radicale uitbreiding van F waarover f splijt. Zij E het splijtveld van f over F in L. Onze doelstelling is om aan te tonen dat $\mathrm{Gal}(E/F)$ oplosbaar is. We hebben

$$F = F_0 \leq F_1 \leq \cdots \leq F_r = L$$

met $F_i = F_{i-1}[\alpha_i]$ en $\alpha_i^{n_i} \in F_{i-1}$ voor $1 \leq i \leq r$. Zij $n = \mathrm{lcm}(n_1, \ldots, n_r)$, en gebruik opnieuw Lemma 4.9.5 om een primitieve n-de eenheidswortel ζ toe te voegen aan L om het veld $L^* = L[\zeta]$ te bekomen. Stel nu $K_{-1} = F$, $K_0 = F[\zeta]$, en $K_i = K_{i-1}[\alpha_i]$ voor $1 \leq i \leq r$. Merk op dat

$$K_r = F[\zeta, \alpha_1, \ldots, \alpha_r] = L[\zeta] = L^*,$$

en dat $F_i \leq K_i$ voor $0 \leq i \leq r$. Dan is

$$F = K_{-1} \leq K_0 \leq K_1 \leq \cdots \leq K_r = L^*,$$

en E is een tussenveld van L^*/F.

Wegens Lemma 4.9.11 volstaat het nu aan te tonen dat elk van de uitbreidingen K_i/K_{i-1} Galois is met een abelse Galoisgroep, voor $0 \leq i \leq r$.

Voor $i = 0$ is dit de uitbreiding $F[\zeta]/F$, die Galois is met een abelse Galoisgroep wegens Lemma 4.9.6. Veronderstel nu $i > 0$; dan is $K_i = K_{i-1}[\alpha_i]$ met $\alpha_i^n \in F_{i-1} \leq K_{i-1}$, en aangezien K_{i-1} een primitieve n-de eenheidswortel bevat, kunnen we de stelling van Kummer (Stelling 4.9.9) toepassen. We besluiten dat K_i/K_{i-1} een Galois-uitbreiding is met cyclische Galoisgroep. □

Gevolg 4.9.13. *Zij F een veld met $\mathrm{char}(F) = 0$, en zij $f \in F[x]$ met $\deg(f) \leq 4$. Dan is f oplosbaar in radicalen over F.*

Bewijs. De Galoisgroep over F van een splijtveld van f over F werkt getrouw op de verzameling van de wortels van f, en is bijgevolg isomorf met een deelgroep van de oplosbare groep $\mathbf{S}_4$. Uit Stelling 4.9.12 volgt dat f oplosbaar is in radicalen over F. □

Dit resultaat is niet langer geldig voor polynomen van graad 5. Merk op dat $\mathbf{S}_5$ niet oplosbaar is, omdat het de enkelvoudige groep $\mathbf{A}_5$ bevat als deelgroep. We gaan nu op zoek naar een polynoom $f \in \mathbb{Q}[x]$ van graad 5 waarvan de Galoisgroep van het splijtveld van f de volledige groep $\mathbf{S}_5$ is.

Lemma 4.9.14. *Zij $f \in \mathbb{Q}[x]$ een irreducibel polynoom van graad p, met p priem, en zij E een splijtveld van f over $\mathbb{Q}$. Veronderstel dat f precies $p-2$ reële wortels en 2 niet-reële complexe wortels heeft. Dan is* $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbf{S}_p$.

Bewijs. We mogen aannemen dat $E \leq \mathbb{C}$, en we noteren de verzameling van alle wortels van f in E als Ω. Dan werkt $G = \mathrm{Gal}(E/\mathbb{Q})$ getrouw op Ω, en dus is G isomorf met een deelgroep van $\mathbf{S}_p$.

Aangezien f irreducibel is, werkt G transitief op Ω, en uit de baanformule volgt dat $p \mid |G|$. Bijgevolg bevat G (of preciezer, het beeld van G in $\mathbf{S}_p$) een element a van orde p, dat noodzakelijk een p-cykel is. Omdat $E/\mathbb{Q}$ een normale uitbreiding is, beeldt de complexe toevoeging E af op zichzelf, en wegens de onderstellingen op de wortels van f definieert de complexe toevoeging een element van G dat in $\mathbf{S}_p$ wordt voorgesteld als een transpositie b, i.e. een 2-cykel.

Zonder verlies van algemeenheid stellen we $b = (1\ 2)$ in cykel-notatie. Merk ook op dat de p-cykel a een zekere macht heeft die 1 op 2 afbeeldt, en door a te vervangen door deze macht kunnen we dus, opnieuw zonder verlies van algemeenheid, onderstellen dat $a = (1\ 2\ \cdots\ p)$. Het is nu een eenvoudige oefening om na te gaan dat $\mathbf{S}_p = \langle a, b \rangle$. □

Voorbeeld 4.9.15. Beschouw het polynoom $f(x) = 2x^5 - 10x + 5$ over $\mathbb{Q}$. Wegens het criterium van Eisenstein is f irreducibel. We zullen aantonen dat het precies 3 reële wortels heeft, door middel van een eenvoudig functieonderzoek. Merk daartoe op dat $f'(x) = 10(x^4 - 1)$, zodat de grafiek van $y = f(x)$ stijgt voor $-\infty < x < -1$ en voor $1 < x < \infty$, en daalt voor $-1 < x < 1$. Aangezien $f(-1) = 13 > 0$ en $f(1) = -3 < 0$, zien we dat f precies één wortel heeft in elk van de intervallen $(-\infty, -1)$, $(-1, 1)$ en $(1, \infty)$, en we besluiten dat er inderdaad precies 3 reële en dus 2 complexe niet-reële wortels zijn.

We kunnen dus Lemma 4.9.14 toepassen, en we zien dat f een voorbeeld oplevert van een polynoom dat niet oplosbaar is in radicalen over $\mathbb{Q}$.

Opmerking 4.9.16. Het is niet geweten of elke eindige groep G kan optreden als de Galoisgroep van een uitbreiding van $\mathbb{Q}$; dit beroemde open probleem staat bekend als het *inverse Galoisprobleem*. Het vorige voorbeeld laat zien dat $G = \mathbf{S}_5$ kan optreden, en het is niet vreselijk moeilijk om op gelijkaardige wijze in te zien dat $G = \mathbf{S}_p$ mogelijk is voor elk priemgetal p. In feite is het geweten dat $G = \mathbf{S}_n$ kan optreden als Galoisgroep over $\mathbb{Q}$ voor elke n, maar het bewijs van dat feit vergt diepere argumenten.

Het is een actief onderzoeksprobleem om van zoveel mogelijk eindige groepen te proberen bewijzen dat ze effectief kunnen optreden als Galoisgroep van een uitbreiding van $\mathbb{Q}$. Behalve de groepen $\mathbf{S}_n$ is dit eveneens geweten voor de alternerende groepen $\mathbf{A}_n$, voor alle oplosbare groepen (een zeer belangrijk resultaat van Shafarevich), en eveneens voor 25 van de 26 sporadische groepen. (De sporadische groep waarvoor het antwoord niet gekend is, is verrassend genoeg de eerder kleine Mathieugroep M_{23}.)

Opmerking 4.9.17. Hoewel we het probleem van de oplosbaarheid in radicalen over $\mathbb{Q}$ nu schijnbaar volledig hebben opgelost, is er nog een belangrijk aspect dat we onder de mat geveegd hebben. Als we namelijk de wortels van een polynoom over $\mathbb{Q}$ expliciet willen beschrijven met behulp van de standaard bewerkingen en het nemen van n-de machtswortels, dan bedoelen we hierbij in feite enkel dat we in staat zijn om *reële* n-de machtswortels te nemen. De resterende vraag is nog of we nu ook de niet-reële n-de machtswortels van 1 kunnen uitdrukken met behulp van de toegestane bewerkingen, zoals bijvoorbeeld $e^{2\pi i/3} = (-1 + \sqrt{-3})/2$.

Het antwoord op deze vraag is positief, maar het vergt nog een aanzienlijke inspanning om dit ook aan te tonen. We zullen in het kader van deze cursus hier niet verder op ingaan, maar we verwijzen de geïnteresseerde lezer naar het boek "Galois Theory" van Harold M. Edwards.

4.10 De grondstelling van de algebra

In deze laatste sectie van dit lange hoofdstuk willen we de grondstelling van de algebra bewijzen: het veld $\mathbb{C}$ is algebraïsch gesloten. We kunnen niet verwachten dat we een puur algebraïsch bewijs vinden van deze stelling, om de eenvoudige reden dat de definitie van het veld $\mathbb{C}$ gebaseerd is op die van het veld $\mathbb{R}$, waarvoor op de een of andere manier een analytische context nodig is.

Het bewijs dat we zullen geven, maakt echter slechts gebruik van twee zeer eenvoudige analytische eigenschappen van $\mathbb{R}$ en $\mathbb{C}$, en is verder volledig algebraïsch. We geven eerst deze twee eigenschappen als een lemma.

Lemma 4.10.1. (i) *Als $f \in \mathbb{R}[x]$ een polynoom is van oneven graad, dan heeft f een wortel in $\mathbb{R}$.*

(ii) *Elk element $\alpha \in \mathbb{C}$ is het kwadraat van een element $\beta \in \mathbb{C}$.*

Bewijs. (i) Zij $f \in \mathbb{R}[x]$ met $\deg(f)$ oneven, en veronderstel, zonder verlies van algemeenheid, dat f monisch is. Dan is $\lim_{x\to-\infty} f(x) = -\infty$ terwijl $\lim_{x\to+\infty} f(x) = +\infty$, zodat uit de tussenwaardestelling volgt dat er een $x \in (-\infty, +\infty)$ bestaat met $f(x) = 0$.

(ii) Zij $\alpha \in \mathbb{C}$, en schrijf α in poolcoördinaten als $\alpha = re^{i\theta}$ met $r \in \mathbb{R}$, $r \geq 0$, en $-\pi < \theta \leq \pi$. Dan voldoet $\beta = \sqrt{r}e^{i\theta/2}$ aan $\alpha = \beta^2$. □

Het zuiver algebraïsche deel van de stelling is bevat in het volgend resultaat.

Stelling 4.10.2. *Zij R een veld met $\mathrm{char}(R) = 0$, en zij C/R een kwadratische velduitbreiding. Veronderstel dat elk polynoom $f \in R[x]$ van oneven graad een wortel heeft in R, en dat elk element van C het kwadraat is van een element van C. Dan is C algebraïsch gesloten.*

Bewijs. Zij L/C een algebraïsche uitbreiding. Wegens Lemma 3.4.2 volstaat het te bewijzen dat $L = C$, en dus veronderstellen we dat er een $\alpha \in L$ zou zijn met $\alpha \notin C$, en gaan we op zoek naar een strijdigheid. Merk op dat $[C[\alpha] : C]$ eindig is, en dus is ook $[C[\alpha] : R]$ eindig. Aangezien $\mathrm{char}(R) = 0$ weten we ook dat $C[\alpha]/R$ separabel is. Uit Lemma 4.4.5 volgt dan dat er een velduitbreiding $E/C[\alpha]$ is zodat E/R Galois is.

Zij nu $G = \mathrm{Gal}(E/R)$, en zij $S \in \mathrm{Syl}_2(G)$. Stel $K = \mathrm{Fix}(S)$; dan is $[K : R] = [G : S]$, en dus is $[K : R]$ oneven. Beschouw nu een willekeurige $\beta \in K$, en zij $f = \min_R(\beta)$. Dan is $\deg(f) = [R[\beta] : R]$ een deler van $[K : R]$, en dus zelf ook oneven. Per veronderstelling heeft f dus een wortel in R, en aangezien f irreducibel is over R, concluderen we dat $\deg(f) = 1$, en dus $\beta \in R$. Aangezien $\beta \in K$ willekeurig was, halen we hieruit dat $K = R$, en dus ook $G = S$. Bijgevolg is G zelf een 2-groep.

Stel nu $H = \mathrm{Gal}(E/C) \leq G$; dan is ook H een 2-groep, en bovendien is $|H| = [E : C] > 1$ aangezien $\alpha \in E \setminus C$. Wegens Gevolg 1.3.15 bestaat er een deelgroep $M \leq H$ met $[H : M] = 2$. Stel $F = \mathrm{Fix}(M)$; dan is $[F : C] = [H : M] = 2$, en dus kunnen we een $\gamma \in F \setminus C$ kiezen.

Zij $q = \min_C(\gamma)$; dan is $\deg(q) = 2$. Echter, aangezien C gesloten is onder het nemen van vierkantswortels, kunnen we de formule voor de oplossingen een vierkantsvergelijking gebruiken om een wortel voor q te vinden in C. Dit is in strijd met het feit dat q irreducibel is over C, en deze contradictie besluit het bewijs. □

Gevolg 4.10.3 (Grondstelling van de algebra)**.** *Het veld* $\mathbb{C}$ *is algebraïsch gesloten.*

Bewijs. Dit volgt uit Stelling 4.10.2 met $R = \mathbb{R}$ en $C = \mathbb{C}$, gebruik makend van Lemma 4.10.1. □

Hoofdstuk

5 Vrije groepen

In dit laatste hoofdstuk gaan we kort in op vrije groepen, en het belangrijke concept van presentaties van groepen. We bewijzen ondermeer dat deelgroepen van vrije groepen opnieuw vrij zijn, en we volgen hierbij de elegante aanpak van Jean-Pierre Serre, gebruik makend van bomen.

5.1 Inleiding

We zullen vrije groepen definiëren aan de hand van een universele eigenschap. Dit is op het eerste gezicht niet erg inzichtelijk, maar we zullen spoedig een expliciete constructie geven van vrije groepen.

Definitie 5.1.1. Zij F een groep, en $X \subseteq F$ een deelverzameling van F. We zeggen dat F *vrij is over* X, als voor elke groep G en elke afbeelding $\theta\colon X \to G$ geldt dat er een uniek groepsmorfisme $\Theta\colon F \to G$ bestaat dat een uitbreiding is van θ.

De structuur van een vrije groep wordt volledig bepaald door de kardinaliteit van de verzameling $|X|$. Merk op dat we geen restrictie leggen op de grootte van deze verzameling; deze kardinaliteit kan dus ook oneindig zijn.

Stelling 5.1.2. *Zij F_1 een groep die vrij is over $X_1 \subseteq F_1$, en zij F_2 een groep die vrij is over $X_2 \subseteq F_2$. Dan is $F_1 \cong F_2$ als en slechts als $|X_1| = |X_2|$.*

Bewijs. Merk op dat $|X_1| = |X_2|$ als en slechts als er een bijectie $\beta\colon X_1 \to X_2$ bestaat.

Veronderstel eerst dat een dergelijke β bestaat, en beschouw de inclusieafbeeldingen

$$\iota_1\colon X_1 \to F_1 \quad \text{en} \quad \iota_2\colon X_2 \to F_2.$$

Beschouw de afbeelding $\iota_2 \circ \beta\colon X_1 \to F_2$. Omdat F_1 vrij is over X_1, is er een uniek groepsmorfisme $\Theta_1\colon F_1 \to F_2$ dat een uitbreiding is van $\iota_2 \circ \beta$. Analoog beschouwen we de afbeelding $\iota_1 \circ \beta^{-1}\colon X_2 \to F_1$; omdat F_2 vrij is over X_2, is er een uniek groepsmorfisme $\Theta_2\colon F_2 \to F_1$ dat een uitbreiding is van $\iota_1 \circ \beta^{-1}$.

Beschouw nu de afbeelding $\alpha := \Theta_2 \circ \Theta_1\colon F_1 \to F_1$, en merk op dat $\alpha_{|X_1} = \mathrm{id}_{X_1}$. Anderzijds is ook $\mathrm{id}_{F_1}\colon F_1 \to F_1$ een afbeelding met de eigenschap

dat $(\mathrm{id}_{F_1})_{|X_1} = \mathrm{id}_{X_1}$. Echter, omdat F_1 vrij is over X_1, is er een *uniek* groepsmorfisme van F_1 naar F_1 dat een uitbreiding is van id_{X_1}, en dus is

$$\Theta_2 \circ \Theta_1 = \alpha = \mathrm{id}_{F_1}\,.$$

Analoog is

$$\Theta_1 \circ \Theta_2 = \mathrm{id}_{F_2},$$

en we besluiten dat Θ_1 een groepsisomorfisme is van F_1 naar F_2.

Veronderstel nu omgekeerd dat $F_1 \cong F_2$, en stel $i \in \{1, 2\}$. Merk op dat er precies $2^{|X_i|}$ afbeeldingen bestaan van X_i naar de groep $G = \mathbf{C}_2$. Omdat F_i vrij is over X_i, impliceert dit dat er precies $2^{|X_i|}$ morfismen bestaan van F_i naar $\mathbf{C}_2$. Bijgevolg is $2^{|X_1|} = 2^{|X_2|}$, en als X_1 of X_2 eindig is, impliceert dit[1] dat $|X_1| = |X_2|$.

In het algemene geval (als X_1 en X_2 niet noodzakelijk eindig zijn) vereist dit een ander argument, dat we enkel kort schetsen. Stel A_i gelijk aan de abelianisatie van F_i, i.e. $A_i := F_i/[F_i, F_i]$, en stel vervolgens $B_i := A_i/A_i^2$, waarbij $A_i^2 = \{a^2 \mid a \in A_i\}$. Dan is B_i een elementair abelse 2-groep, en men kan aantonen dat de 2-rang van B_i precies gelijk is aan $|X_i|$. Uit $F_1 \cong F_2$ volgt dan $B_1 \cong B_2$ en bijgevolg $|X_1| = |X_2|$. □

We komen nu tot de constructie van vrije groepen.

Definitie 5.1.3. Zij X een willekeurige verzameling, en definieer een nieuwe verzameling

$$X^{-1} := \{x^{-1} \mid x \in X\},$$

waarbij de elementen x^{-1} nieuwe formele symbolen zijn. Voor elk symbool $y = x^{-1} \in X^{-1}$ definiëren we nu $y^{-1} := x$. Stel verder

$$X^{\pm} := X \cup X^{-1},$$

waarbij de unie dus een disjuncte unie is. Definieer vervolgens de verzameling

$$X^* := \{x_1 x_2 \cdots x_r \mid x_i \in X^{\pm}\}$$

bestaande uit alle strings (*woorden* genoemd) bestaande uit elementen van $X^{\pm}$. (We noemen de verzameling $X^{\pm}$ dan ook wel het *alfabet*.) De bewerking "concatenatie" (aan-elkaar-voeging) maakt van X^* een *monoïde*, i.e. een verzameling met een associatieve bewerking en een neutraal element (hier het

[1] Als X_1 en X_2 oneindig zijn, is deze implicatie enkel waar als de GCH, de veralgemeende continuumhypothese, ondersteld wordt.

"lege woord"); we noemen deze monoïde de *vrije monoïde* over het alfabet $X^{\pm}$.

We noemen een woord $w = x_1 x_2 \cdots x_r \in X^*$ *gereduceerd* als $x_{i+1} \neq x_i^{-1}$ voor alle $i \in \{1, \ldots, r-1\}$. Als $w \in X^*$ een willekeurig woord is, dan definieren we de *reductie van* w als het gereduceerde woord $\overline{w}$ dat we verkrijgen uit w door opeenvolgende paren xx^{-1} (met $x \in X^{\pm}$) te schrappen uit het woord. Stel nu

$$F(X) := \{w \in X^* \mid w \text{ is gereduceerd}\}.$$

We definiëren een bewerking op $F(X)$, gegeven door "concateneren en reduceren":

$$w_1 \cdot w_2 := \overline{w_1 w_2}.$$

Stelling 5.1.4. *De verzameling $F(X)$, voorzien van de bewerking "concatenatie en reductie", is een vrije groep over X.*

Bewijs. We tonen eerst aan dat $F(X)$ een groep is, met als neutraal element het lege woord. Inderdaad, de associativiteit van de bewerking is evident; en als $g = x_1 x_2 \cdots x_r \in F(X)$, met $x_i \in X^{\pm}$, dan is $h = x_r^{-1} \cdots x_2^{-1} x_1^{-1}$ een invers voor g.

We tonen nu aan dat $F(X)$ vrij is over X. Zij dus G een willekeurige groep, en $\theta\colon X \to G$ een willekeurige afbeelding. Stel nu

$$\Theta\colon F(X) \to G\colon x_1^{\epsilon_1} \cdots x_r^{\epsilon_r} \mapsto \theta(x_1)^{\epsilon_1} \cdots \theta(x_r)^{\epsilon_r},$$

waarbij $x_1, \ldots, x_r \in X$ en $\epsilon_1, \ldots, \epsilon_r \in \{1, -1\}$. Dan is Θ inderdaad een groepsmorfisme, en $\Theta_{|X} = \theta$. Omdat $F(X)$ als groep wordt voortgebracht door de verzameling X, is het eveneens duidelijk dat Θ de *unieke* uitbreiding van θ is. □

Definitie 5.1.5. Als X een eindige verzameling is met n elementen, dan noteren we de groep $F(X)$ ook als F_n, en we noemen dit de *vrije groep op n letters*, of de *vrije groep van rang n*.

Voorbeeld 5.1.6. (1) We beweren dat $F_1 \cong (\mathbb{Z}, +)$. Inderdaad, stel $X = \{a\}$, zodat $X^{\pm} = \{a, a^{-1}\}$, en dus $F(X) = \{a^n \mid n \in \mathbb{Z}\}$. Duidelijkerwijze is $F(X)$, voorzien van de bewerking "concatenatie en reductie", isomorf met $(\mathbb{Z}, +)$.

We hadden ook rechtstreeks uit de definitie kunnen halen dat $(\mathbb{Z}, +)$ vrij is over de deelverzameling $\{1\} \subset \mathbb{Z}$. Inderdaad, zij G een willekeurige groep, en $\theta\colon \{1\} \to G$ een willekeurige afbeelding (of dus anders gezegd, $g := \theta(1)$ is een willekeurig element van G). Dan is er een uniek groepsmorfisme $\Theta\colon \mathbb{Z} \to G$ met $\Theta(1) = g$, namelijk $\Theta\colon \mathbb{Z} \to G\colon n \mapsto g^n$.

(2) Zij $1 \leq m \leq n$ natuurlijke getallen, en beschouw verzamelingen $X \subseteq Y$ met $|X| = m$ en $|Y| = n$. Dan induceert de inclusie $X \subseteq Y$ een inclusie van groepen $F(X) \leq F(Y)$. Dus F_m is "op natuurlijke wijze" bevat in F_n.

(3) De structuur van de groep F_2 is al meteen veel complexer dan die van F_1. Stel $X = \{a, b\}$, en dus $X^{\pm} = \{a, a^{-1}, b, b^{-1}\}$. De groep $F(X)$ bestaat nu uit alle gereduceerde woorden gevormd met dit alfabet, bijvoorbeeld

$$a^{-1}b^2a^3baba^{-1}b^{-3}a \in F(X).$$

Om in te zien dat de structuur van deze groep niet eenvoudig kan zijn, proberen we de afgeleide groep F_2' te begrijpen. Merk op dat, voor alle $m, n \in \mathbb{Z} \setminus \{0\}$, de commutator

$$[a^m, b^n] = a^{-m}b^{-n}a^mb^n$$

een niet-triviaal element in F_2' is. Het is niet zo moeilijk om in te zien dat

$$F_2' = \big\langle [a^m, b^n] \mid m, n \in \mathbb{Z} \setminus \{0\} \big\rangle,$$

en met meer moeite kan men aantonen dat F_2' een vrije groep is over de verzameling van al deze commutators. Met andere woorden, F_2' is vrij van rang $\aleph_0$ (aftelbaar oneindig). In het bijzonder volgt nu dat F_2', en dus ook F_2, deelgroepen bevat isomorf met F_n voor elk mogelijk natuurlijk getal n. Of dus:

> Als $m, n \in \mathbb{N}$ met $m \geq 1$ en $n \geq 2$, dan is F_m isomorf met een deelgroep van F_n.

Stelling 5.1.7. *Als $|X| \geq 2$, dan heeft $F(X)$ een triviaal centrum.*

Bewijs. Stel $w = x_1x_2 \cdots x_r \in F(X)$ een niet-leeg gereduceerd woord met $x_i \in X^{\pm}$, en veronderstel dat $w \in Z(F(X))$. Kies $a \in X$ willekeurig; omdat $aw = wa$, hebben we

$$ax_1 \cdots x_r = x_1 \cdots x_r a.$$

Veronderstel dat $x_r = b \notin \{a, a^{-1}\}$. Dan zou het woord $ax_1 \cdots x_r$ eindigen op de letter b, terwijl het woord $x_1 \cdots x_r a$ eindigt op de letters ba (en dus zeker gereduceerd blijft). Deze contradictie toont aan dat $x_r \in \{a, a^{-1}\}$. Echter, a was willekeurig gekozen, dus als we een $b \in X \setminus \{a\}$ kiezen, besluiten we dat ook $x_r \in \{b, b^{-1}\}$. Dit kan natuurlijk niet, dus de onderstelling dat $w \in Z(F(X))$ is vals. □

Opmerking 5.1.8. In het bewijs hebben we eigenlijk algemener aangetoond dat voor elke letter $a \in X$ geldt dat $C_{F(X)}(a) = \langle a \rangle$. Nog algemener kan men bewijzen dat twee elementen in $F(X)$ commuteren met elkaar als en slechts als ze machten zijn van eenzelfde element.

5.2 Presentaties

Intuïtief zou men kunnen stellen dat de vrije groep F_n een groep is die voortgebracht is door n elementen $x_1, \ldots, x_n$, waar men geen verdere relaties oplegt. We kunnen deze intuïtie formeel maken, en dit leidt tot het belangrijke begrip van presentaties van willekeurige groepen.

We beginnen met een eenvoudige maar in deze context zeer relevante observatie.

Stelling 5.2.1. *Elke groep is het quotiënt van een vrije groep.*

Bewijs. Zij G een willekeurige groep, en zij X een willekeurige voortbrengende verzameling voor G (bijvoorbeeld $X = G$ zelf). Beschouw de vrije groep $F(X)$, en beschouw de inclusie-afbeelding ι van X in G. Dan bestaat er, per definitie van vrije groep, een uniek groepsmorfisme $\Theta\colon F(X) \to G$, dat een uitbreiding is van ι. Dan is $X = \operatorname{im}\iota \subseteq \operatorname{im}\Theta$, en omdat $G = \langle X\rangle$ en $\operatorname{im}\Theta \leq G$, besluiten we dat $\operatorname{im}\Theta = G$. Uit de eerste isomorfiestelling volgt nu dat $G \cong F(X)/\ker(\Theta)$. □

Aansluitend bij onze intuïtieve inleiding kunnen we het isomorfisme $G \cong F(X)/\ker(\Theta)$ interpreteren als het feit dat G de groep is die wordt voortgebracht door de elementen van X, waarbij $\ker(\Theta)$ bijkomende relaties oplegt op deze elementen. Dit leidt tot de volgende definitie.

Definitie 5.2.2. (i) Zij G een groep en $S \subseteq G$ een deelverzameling van G. De *normale sluiting van S in G* is de kleinste normaaldeler van G die S bevat; we noteren die als $\langle S^G\rangle$. Dit is consistent met het feit dat de normale sluiting precies de deelgroep van G is voortgebracht door alle toegevoegden van S in G.

(ii) Zij X een verzameling, en zij R een deelverzameling van $F(X)$. Dan definiëren we *de groep met voortbrengers X en relatoren R*, die we noteren als $\langle X \mid R\rangle$, als de groep

$$\langle X \mid R\rangle := F(X) \,\big/\, \langle R^{F(X)}\rangle.$$

(iii) Zij G een groep, en zij $X \subseteq G$ een voortbrengende verzameling voor G. Als $R \subseteq F(X)$ met $G \cong \langle X \mid R\rangle$, dan zeggen we dat (X, R) een *presentatie voor G* is. We schrijven vaak $G = \langle X \mid R\rangle$ in plaats van $G \cong \langle X \mid R\rangle$.

(iv) In de praktijk zullen we vaak *relaties* schrijven in plaats van *relatoren*, waarbij een relatie $g = h$ dan overeenkomt met een relator $gh^{-1} \in R$.

(v) Een groep G is *eindig voortgebracht* als er een eindige voortbrengende verzameling X bestaat voor G. Een groep G is *eindig gepresenteerd* als er een eindige voortbrengende verzameling X bestaat voor G, en een eindige verzameling $R \subseteq F(X)$, zodat $G = \langle X \mid R \rangle$.

Voorbeeld 5.2.3. (1) De vrije groep F_n heeft presentatie $F_n = \langle x_1, \ldots, x_n \mid \emptyset \rangle$, in overeenstemming met onze intuïtie dat de groep n voortbrengers heeft zonder bijkomende relaties.

(2) De eindige cyclische groep $\mathbf{C}_n$ heeft presentatie $\mathbf{C}_n = \langle a \mid a^n \rangle$, hetgeen we ook noteren als $\mathbf{C}_n = \langle a \mid a^n = 1 \rangle$.

(3) De diëdergroep $\mathbf{D}_{2n}$ heeft presentatie $\langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$. Merk op dat deze voorstelling overeenkomt met het semidirect product $\mathbf{D}_{2n} = \langle a \rangle \rtimes \langle b \rangle$ dat we reeds vroeger hebben ontmoet.

(4) Als G een groep is met presentatie $\langle X \mid R \rangle$ en H is een groep met presentatie $\langle Y \mid S \rangle$, dan heeft $G \times H$ presentatie $\langle X \dot\cup Y \mid R, S, [X, Y] \rangle$, waarbij de notatie $\dot\cup$ benadrukt dat de unie een disjuncte unie is, en de notatie $[X, Y]$ staat voor de verzameling van elementen van de vorm $[x, y]$ met $x \in X$ en $y \in Y$. Zo heeft bijvoorbeeld de groep $\mathbb{Z} \times \mathbb{Z}$ presentatie $\langle a, b \mid [a, b] = 1 \rangle$.

(5) Het is in het algemeen een moeilijk probleem om de structuur te achterhalen van een groep die gegeven is door een presentatie. Zo blijkt bijvoorbeeld dat $\langle a, b \mid a^3 = b^2 = 1 \rangle$ een presentatie is voor $\mathsf{PSL}_2(\mathbb{Z})$.

(6) Een voorbeeld van een groep G die eindig voortgebracht is, maar niet eindig gepresenteerd, is de groep $\mathbb{Z} \wr \mathbb{Z}$, het kransproduct van $\mathbb{Z}$ met zichzelf.

Interessant is dat we een visuele voorstelling kunnen maken van een groep met een gegeven voortbrengende verzameling: de zogenaamde Cayleygraaf. We herhalen eerst de definitie van een (gerichte) graaf.

Definitie 5.2.4. (i) Een *(ongerichte) graaf* is een koppel $\Gamma = (V, E)$, waarbij V een verzameling is met elementen die we *toppen* of *knopen* noemen, en waarbij E een verzameling is van ongeordende paren uit V, die we *bogen* of *kanten* noemen. We maken een grafische voorstelling van een graaf door de toppen als bollen of punten te tekenen, en de bogen als (rechte of gebogen) lijnstukken die de toppen verbinden. Als Γ een graaf is, dan noteren we de toppen- en bogenverzameling als $V(\Gamma)$ respectievelijk $E(\Gamma)$.

(ii) Een *cykel* in een graaf Γ is een rij van toppen $v_1, \ldots, v_n$ met $v_n = v_1$, zodat elke twee opeenvolgende toppen een boog vormen, en zodat

$v_{i-1} \neq v_{i+1}$ voor alle i. Een *boom* is een graaf Γ zonder cykels.

(iii) Een *gerichte graaf* is een koppel $\Gamma = (V, E)$, waarbij V een verzameling is met elementen die we *toppen* of *knopen* noemen, en waarbij E een verzameling is van geordende paren uit V, die we *bogen* of *pijlen* noemen. We maken een grafische voorstelling van een graaf door de toppen als bollen of punten te tekenen, en de bogen als (rechte of gebogen) lijnstukken voorzien van een pijl, die de toppen verbinden. Het is hierbij toegestaan dat er tussen twee toppen een pijl is in beide richtingen.

(iv) Een (gerichte of ongerichte) graaf Γ noemen we *(boog)gekleurd*, als we ze voorzien van een verzameling *kleuren* $\mathcal{C}$, en een afbeelding $c\colon E(\Gamma) \to \mathcal{C}$.

(v) Een *automorfisme* van een (ongerichte of gerichte) graaf $\Gamma = (V, E)$ is een permutatie α van de toppenverzameling V zodat voor alle $x, y \in V$ geldt dat $(x, y) \in E$ als en slechts als $(x^\alpha, y^\alpha) \in E$. De verzameling van alle automorfismen van Γ vormt een groep onder de samenstelling, die we de *automorfismengroep* van Γ noemen, en noteren als $\mathrm{Aut}(\Gamma)$.

Definitie 5.2.5. Zij G een groep met voortbrengende verzameling S die het element $1 \in G$ niet bevat. De *Cayleygraaf* van G met betrekking tot S is de gerichte gekleurde graaf $\Gamma = \mathrm{Cay}(G, S)$, gedefinieerd als volgt.

- De toppenverzameling $V(\Gamma)$ is precies de verzameling G.
- We associëren een kleur c_s met elke voortbrenger $s \in S$.
- Voor elke $g \in G$ en elke $s \in S$ verbinden we de top g met de top gs met een gerichte boog van kleur c_s. In het bijzonder is dus

$$E(\Gamma) = \{(g, gs) \mid g \in G, s \in S\}.$$

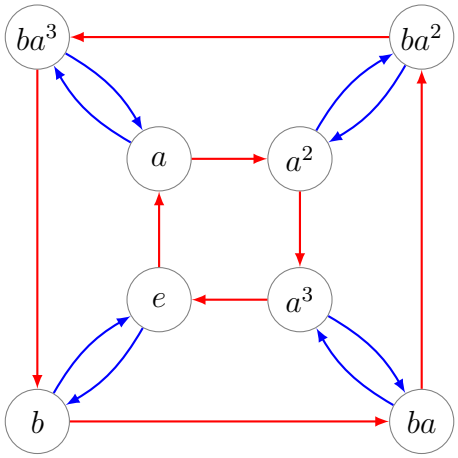
Vaak (maar zeker niet altijd) wordt bijkomend ondersteld dat de voortbrengende verzameling S gesloten is onder inversen; in dat geval kunnen we de Cayleygraaf interpreteren als een ongerichte graaf.

Voorbeeld 5.2.6. Beschouw de groep

$$\mathbf{D}_8 = \langle a, b \mid a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle,$$

met voortbrengende verzameling $S = \{a, b\}$. Als we c_a rood kiezen en c_b

blauw kiezen, dan ziet de Cayleygraaf $\mathrm{Cay}(\mathbf{D}_8, S)$ er als volgt uit.



Merk op dat cykels in de Cayleygraaf in verband staan met relaties tussen de elementen. In het bijzonder geldt dat, als we een cykel beschouwen die start en eindigt in het neutraal element $e \in G$, en we het woord opschrijven dat we verkrijgen als opeenvolging van de voortbrengers die overeenkomen met de kleuren van de bogen in deze cykel, we een niet-triviale relatie krijgen in termen van de voortbrengers. Bijvoorbeeld, als we de cykel e–a–a^2–a^3–e volgen, zien we dat $a^4 = 1$. Als we anderzijds de cyckel e–a–ba^3–b–e volgen, zien we dat $abab = 1$.

Een andere interessante vaststelling is dat de groep G op natuurlijke wijze werkt op de Cayleygraaf $\mathrm{Cay}(G, S)$.

Lemma 5.2.7. *Zij G een groep met voortbrengende verzameling S, en zij $\Gamma = \mathrm{Cay}(G, S)$. Elke $g \in G$ induceert door linksvermenigvuldiging een (richting- en kleurbewarend) fixpunt-vrij automorfisme van de graaf Γ. In het bijzonder induceert de Cayley-permutatierepresentatie $G \hookrightarrow \mathrm{Sym}(G)$, die elke $g \in G$ afbeeldt op linksvermenigvuldiging met G, een inclusie $G \hookrightarrow \mathrm{Aut}(\Gamma)$.*

Bewijs. Dit volgt onmiddellijk uit het feit dat (g, gs) een gerichte boog is met kleur c_s als en slechts als (hg, hgs) een gerichte boog is met kleur c_s, voor alle $h \in G$. □

5.3 Vrije acties op bomen

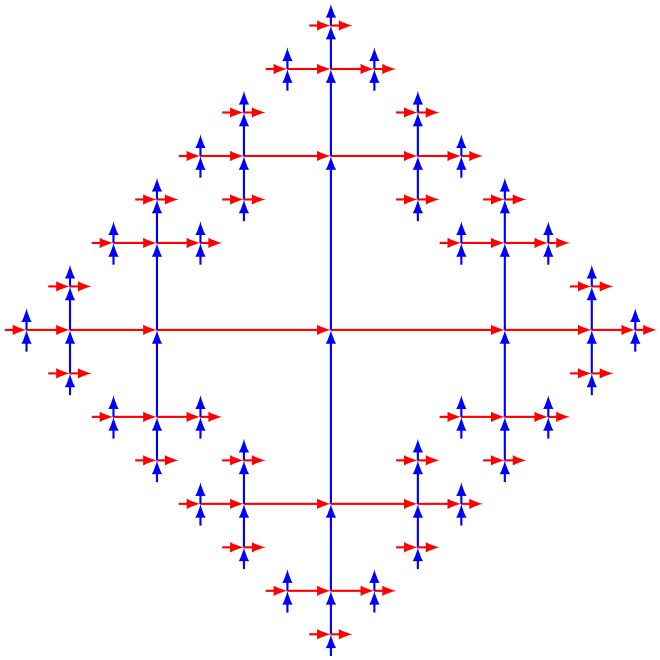
We richten ons nu opnieuw tot vrije groepen. Het feit dat we in een vrije groep geen relaties hebben tussen de voortbrengers, vertaalt zich naar het feit dat de Cayleygraaf geen cykels heeft.

Lemma 5.3.1. *Zij F een vrije groep over $X \subseteq F$. Dan is* $\mathrm{Cay}(F, X)$ *een boom.*

Bewijs. Veronderstel dat $\mathrm{Cay}(F, X)$ een cykel g_0–g_1–$\cdots$–g_{r-1}–g_r met $g_r = g_0$ bevat. Dan zijn er elementen $x_i \in X^{\pm}$ zodat $g_{i+1} = g_i x_i$ voor alle $i \in \{0, \ldots, r-1\}$, waaruit volgt dat $x_0 x_1 \cdots x_{r-1} = 1$. Merk op dat $x_{i+1} \neq x_i^{-1}$ voor alle $i \in \{0, \ldots, r-2\}$, omdat anders $g_i = g_{i+2}$ zou zijn, in strijd met de definitie van een cykel. Bijgevolg is het woord $x_0 x_1 \cdots x_{r-1}$ gereduceerd. Dit is strijdig met de definitie van $F(X)$. We besluiten dat $\mathrm{Cay}(F, X)$ geen cykels bevat, en dus een boom is. □

Ter illustratie schetsen we de Cayleygraaf van de vrije groep F_2 op twee letters.

Voorbeeld 5.3.2. Zij $F_2 = \langle a, b \mid \emptyset \rangle$, met $S = \{a, b\}$. Als we c_a rood kiezen en c_b blauw kiezen, dan ziet de Cayleygraaf $\mathrm{Cay}(F_2, S)$ er als volgt uit.



In het bijzonder heeft een vrije groep een *vrije actie* op een boom, zoals we nu verklaren.

Definitie 5.3.3. Zij T een boom, en $G \leq \mathrm{Aut}(T)$ een groep van automorfismen van T. We zeggen dat G *vrij werkt* op T als geen enkel niet-triviaal element van G een top of een (ongerichte) boog van T fixeert.

Opmerking 5.3.4. Als er een element $g \in G \leq \mathrm{Aut}(T)$ bestaat dat een boog fixeert maar geen enkele top fixeert, dan wordt deze boog geïnverteerd, en we zeggen dan dat G *met inversie* werkt. In het andere geval, dus als geen dergelijk element g bestaat, dan werkt G *zonder inversie*. We kunnen dus zeggen dat G vrij werkt op T als G zonder inversie werkt en geen enkel niet-triviaal element van G een top fixeert.

Gevolg 5.3.5. *Zij F een vrije groep. Dan heeft F een vrije actie op een boom.*

Bewijs. Zij F een vrije groep over $X \subseteq F$, en beschouw de actie van F op de boom $T = \mathrm{Cay}(F, X)$ die geïnduceerd wordt door de Cayley-representatie. Zij $g \in F$ een willekeurig niet-triviaal element. Aangezien g een top $h \in V(T)$ afbeeldt op de top gh, houdt g al zeker geen top vast. Veronderstel dat g een boog (h, hs) zou vasthouden, voor een zekere $h \in G$ en $s \in X$; dan is $gh = hs$ en $ghs = h$. Hieruit volgt echter $s^2 = 1$, een contradictie. We besluiten dat de actie vrij is. □

Het doel van deze sectie is om ook het omgekeerde te bewijzen: als een groep G een vrije actie heeft op een boom, dan is G een vrije groep. Om aan te tonen dat een groep vrij is, zullen we gebruik maken van (een eenvoudige versie van) het pingpong lemma.

Lemma 5.3.6 (Pingpong lemma)**.** *Zij G een groep werkend op een verzameling Ω, en zij X een voortbrengende verzameling voor G. Veronderstel dat er voor elk element $x \in X^{\pm}$ een deelverzameling $A_x \subseteq \Omega$ gegeven is, en zij $p \in \Omega$ een element dat in geen enkel van deze deelverzamelingen A_x bevat is. Veronderstel verder dat*

$$\begin{cases} p^x \in A_x & \text{voor alle } x \in X^{\pm}; \\ (A_y)^x \subseteq A_x & \text{voor alle } y \in X^{\pm} \setminus \{x^{-1}\}. \end{cases}$$

Dan is $G \cong F(X)$.

Bewijs. Beschouw de vrije groep $F(X)$ over X, en het bijhorend surjectief groepsmorfisme $\varphi\colon F(X) \to G$ met $\varphi(x) = x$ voor alle $x \in X$. Het volstaat om aan te tonen dat als $w = x_1 \cdots x_n \in F(X)$ een gereduceerd woord is, dat dan ook $\varphi(w) \neq 1$; dat bewijst dan immers dat φ injectief is, en bijgevolg een isomorfisme is.

Beschouw hiertoe de actie van $F(X)$ op Ω geïnduceerd door φ, i.e. we definiëren $s^w := s^{\varphi(w)}$ voor alle $s \in \Omega$ en alle $w \in F(X)$. We zullen aantonen dat $p^w \neq p$ indien $w \neq 1$. Meer bepaald beweren we:

$$p^{x_1 \cdots x_n} \in A_{x_n}. \qquad (*)$$

We gebruiken inductie op de lengte n van het woord $w = x_1 \cdots x_n$. Voor $n = 1$ volgt dit onmiddellijk uit het gegeven dat $p^x \in A_x$ voor alle $x \in X^{\pm}$.

Stel nu $n > 1$, en stel $v = x_1 \cdots x_{n-1}$; dan is v een gereduceerd woord van lengte $n - 1 < n$. Wegens de inductiehypothese is $p^v \in A_{x_{n-1}}$. Omdat w gereduceerd is, is $x_n \neq x_{n-1}^{-1}$, en uit het gegeven volgt nu dat

$$p^w = p^{vx_n} \in (A_{x_{n-1}})^{x_n} \subseteq A_{x_n},$$

wat de bewering $(*)$ aantoont, en het bewijs voltooit. □

Opmerking 5.3.7. De benaming van dit lemma komt van het feit dat het woord $w = x_1 \cdots x_n$ pingpong speelt (met het pingpong-balletje p) tussen de verzamelingen A_x.

We trachten nu meer inzicht te krijgen in groepen die vrij werken op een boom. We beginnen met een eenvoudig lemma.

Lemma 5.3.8. *Zij G een groep die vrij werkt op een boom T. Dan bevat G geen involuties.*

Bewijs. Veronderstel dat $g \in G$ met $g \neq 1$ en $g^2 = 1$. Kies een willekeurige top v van T, en beschouw het unieke kortste pad van v naar v^g. Omdat $g^2 = 1$ zal g de toppen v en v^g verwisselen, en daarbij dus dat kortste pad op zichzelf afbeelden, maar in omgekeerde richting. Het midden van dat pad, dat een top of een boog kan zijn, wordt dan door g vastgehouden, in strijd met het feit dat G vrij werkt op T. □

Definitie 5.3.9. Zij G een groep die werkt op een boom T. Een *fundamentaalgebied* voor deze actie is een deelboom D van T zodanig dat de toppenverzameling $V(D)$ precies één top van elke G-baan bevat.

Het belang van een fundamentaalgebied is duidelijk: als D een fundamentaalgebied is voor de actie van G op T, dan is elke top $v \in V(T)$ op unieke wijze te schrijven als $v = w^g$ voor een $w \in V(D)$ en een $g \in G$. Merk ook op dat een fundamentaalgebied een imprimitiviteitsblok is voor de actie van G op $V(T)$, in een zeer sterke zin: voor alle $g \in G$ met $g \neq 1$ geldt dat $V(D) \cap V(D)^g = \emptyset$.

Het is echter niet evident dat een fundamentaalgebied altijd bestaat; dit is wat we bewijzen in het volgend lemma.

Lemma 5.3.10. *Zij G een groep die vrij werkt op een boom T. Dan is er een fundamentaalgebied voor de actie van G op T.*

Bewijs. We gebruiken eerst het lemma van Zorn om aan te tonen dat er een deelboom D van T is die maximaal is in de familie $\mathcal{F}$ van alle deelbomen die *ten hoogste één* top van elke G-baan bevatten. Uiteraard is $\mathcal{F}$ niet ledig (beschouw bijvoorbeeld een boom met 1 top). Beschouw nu een willekeurige keten $\mathcal{C} \subseteq \mathcal{F}$, en stel U gelijk aan de unie van alle deelbomen in $\mathcal{C}$. Dan is U samenhangend, en dus opnieuw een deelboom. Veronderstel nu dat U twee toppen van eenzelfde G-baan zou bevatten, stel v en v^g, voor een zekere $g \neq 1$. Dan zijn v en v^g beide bevat in een zekere boom S van de keten $\mathcal{C}$, wat in strijd is met $S \in \mathcal{F}$. Dus is inderdaad $U \in \mathcal{F}$ een bovengrens voor de keten $\mathcal{C}$. Uit het lemma van Zorn volgt nu dat $\mathcal{F}$ een maximaal element D bevat.

Veronderstel nu dat D niet uit elke G-baan een top bevat. Dan is

$$V(T) \neq \bigcup_{g \in G} V(D^g).$$

Er bestaat dus een boog $e \in E(T)$ waarvan de begintop in $V(D^h)$ bevat is voor een zekere $h \in G$, maar de eindtop in geen enkele $V(D^g)$ bevat is. Stel dan $f := e^{h^{-1}}$; dan is de begintop van f bevat in $V(D)$, en de eindtop w van f in geen enkele $V(D^g)$. Stel dan E gelijk aan de boom die we verkrijgen uit D door de boog f en de top w toe te voegen. Aangezien D maximaal was in de familie $\mathcal{F}$, is $E \notin \mathcal{F}$, en dus bestaat er een $v \in V(E)$ en een niet-triviaal element $g \in G$ zodat ook $v^g \in V(E)$. Omdat $D \in \mathcal{F}$ kan dit echter enkel als $v = w$ of $v^g = w$. In het eerste geval hebben we $w^g \in V(E)$, maar tevens $w^g \notin V(D)$, en dus $w^g = w$. In het tweede geval hebben we $w^{g^{-1}} \in V(E)$, maar tevens $w^{g^{-1}} \notin V(D)$, dus opnieuw $w^g = w$. In beide gevallen is dit in strijd met de onderstelling dat G vrij werkt op T. We besluiten dat D precies één top bevat uit elke G-baan. □

Definitie 5.3.11. Zij T een boom, en zij D een willekeurige deelboom van T. De (gerichte) bogen van T die hun begintop in D hebben maar hun eindtop niet in D, worden de *randbogen* van D genoemd. De verzameling van deze randbogen noteren we als ∂D.

Stelling 5.3.12. *Een groep is vrij als en slechts als hij vrij werkt op een boom.*

Bewijs. We weten reeds uit Stelling 5.3.5 dat een vrije groep een vrije actie heeft op een boom.

Veronderstel dus dat G een groep is die vrij werkt op een boom T, en zij D een fundamentaalgebied voor deze actie (wat bestaat wegens Lemma 5.3.10). Stel

$$S = \{g \in G \setminus \{1\} \mid \text{er is een boog tussen } D \text{ en } D^g\}.$$

Merk op dat $S = S^{-1}$. We beweren dat

$$G = \langle S \rangle.$$

Beschouw daartoe een vaste top $v \in V(D)$, en stel $B \subseteq E(T)$ gelijk aan de unie van alle G-banen van de bogen in ∂D, met andere woorden, B bestaat precies uit alle bogen die een D^g verbinden met een D^h, voor alle $g, h \in G$ met $g \neq h$. (Voor gegeven g, h bestaat er telkens ten hoogste één dergelijke boog.) Voor elke $g \in G$ stellen we $b(g)$ gelijk aan het aantal bogen in het unieke kortste pad van v naar v^g die in B liggen. Stel dan $G_n := \{g \in G \mid b(g) = n\}$. We zullen per inductie op n bewijzen dat $G_n \subseteq \langle S \rangle$.

Merk vooreerst op dat $G_1 = S$. Inderdaad, $g \in G_1$ als en slechts als g een niet-triviaal element is zodat het unieke pad van v naar v^g slechts 1 element van B bevat, maar dat element is dan noodzakelijk de unieke boog tussen D en D^g.

Veronderstel nu dat $g \in G_{n+1}$, en dat we al weten dat $G_n \subseteq \langle S \rangle$. Het unieke pad van v naar v^g bevat nu $n+1$ elementen van B. Zij e het element van B dat het dichtst bij v ligt op dit pad. Dan is e de unieke boog tussen D en D^s, voor een zekere $s \in S$. Bovendien liggen er tussen D^s en D^g precies n bogen van B, en in het bijzonder bevat het unieke pad tussen v^s en v^g juist n elementen van B. Hieruit volgt dat het unieke pad tussen v en $v^{gs^{-1}}$ juist n elementen van B bevat, en dus is $gs^{-1} \in G_n$. Wegens de inductiehypothese is dus $gs^{-1} \in \langle S \rangle$, maar dan ook $g \in \langle S \rangle$, en dit bewijst dat $G_{n+1} \leq \langle S \rangle$. Aangezien dit nu geldt voor alle n, besluiten we dat inderdaad $G = \langle S \rangle$.

We willen nu het pingpong lemma toepassen. Omdat G geen involuties bevat (Lemma 5.3.8), en $S = S^{-1}$, kunnen we een deelverzameling X van S kiezen zodat S de disjuncte unie $X^{\pm}$ is van X en X^{-1}. We stellen nu, voor elk element $s \in S$,

$$A_s := \{w \in V(T) \mid \text{het unieke pad van } v \text{ naar } w \text{ snijdt } V(D^s)\}.$$

Merk op dat het element $v \in V(T)$ in geen enkel van deze deelverzamelingen A_s bevat is.

Uiteraard is $v^s \in A_s$ voor alle $s \in S$, omdat $v^s \in V(D^s)$. Er rest ons enkel nog te bewijzen dat

$$(A_t)^s \subseteq A_s \quad \text{voor alle } t \in S \setminus \{s^{-1}\}. \tag{$*$}$$

Zij dus $w \in A_t$ willekeurig; dan snijdt het unieke pad van v naar w de toppenverzameling $V(D^t)$. Beschouw nu anderzijds $D^{s^{-1}}$; omdat $t \neq s^{-1}$, is $D^{s^{-1}} \neq D^t$, zodat het unieke pad van $v^{s^{-1}}$ naar w achtereenvolgens $D^{s^{-1}}$, D en D^t doorloopt. Door op dit alles s te laten inwerken, zien we dat het

unieke pad van v naar w^s achtereenvolgens D, D^s en D^{ts} doorloopt. In het bijzonder is $w^s \in A_s$, wat $(*)$ bewijst.

Alle voorwaarden van het pingpong lemma (Lemma 5.3.6) zijn dus voldaan, en we besluiten dat $G \cong F(X)$ een vrije groep is. □

Gevolg 5.3.13 (Stelling van Nielsen–Schreier)**.** *Een deelgroep van een vrije groep is opnieuw vrij.*

Bewijs. Als G een vrije groep is, dan werkt G vrij op een boom T, zodat ook elke deelgroep H vrij werkt op diezelfde boom T, en dus is ook H een vrije groep. □

Opmerking 5.3.14. (i) Het oorspronkelijke bewijs van deze stelling, zoals ze werd bewezen door Nielsen en Schreier, is van een heel andere aard, en bestaat uit een zeer nauwkeurige analyse van woorden in vrije groepen.

(ii) Door middel van een preciezer argument kan men ook bewijzen dat als F een vrije groep is van rang a, en $H \leq F$ een deelgroep van eindige index n, dan is H een vrije groep van rang b, waarbij

$$b - 1 = n(a - 1).$$

Deze formule staat bekend als de *Schreier index-formule*. (Merk dus op dat $b > a$ als $n > 1$: een deelgroep van eindige index heeft dus hogere rang dan de oorspronkelijke groep, in tegenstelling tot wat je misschien intuïtief zou verwachten.)