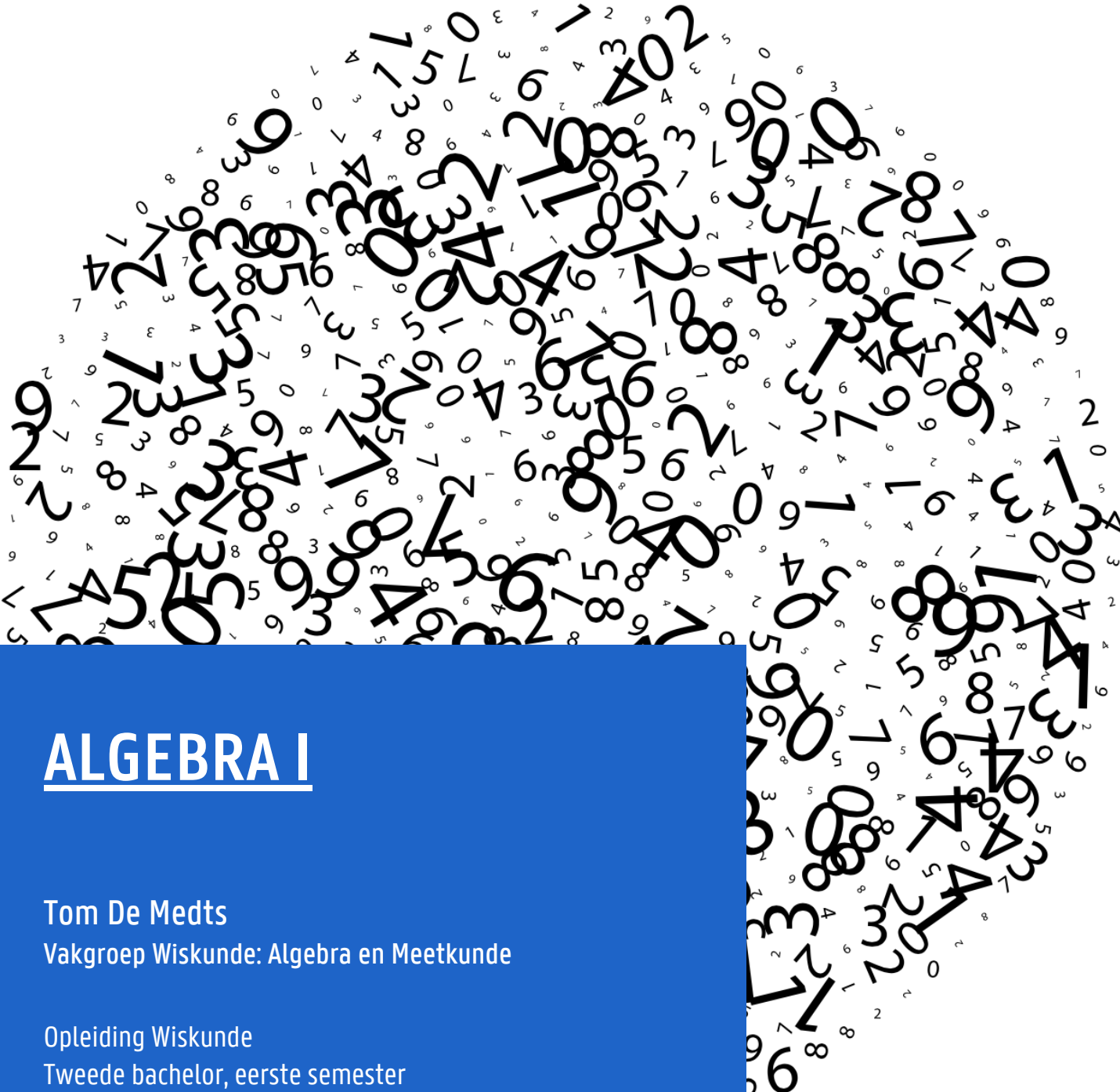




ALGEBRA I

Tom De Medts

Vakgroep Wiskunde: Algebra en Meetkunde

Opleiding Wiskunde

Tweede bachelor, eerste semester

Academiejaar 2022–2023



Inhoudsopgave

1	Groepen	1
1.1	Groepen, deelgroepen en voorbeelden	1
1.2	Verdere definities en eigenschappen	8
1.3	Groepsmorfismen	15
1.4	Cyclische groepen	18
1.5	Toevoeging en normaaldelers	20
1.6	Quotiëntgroepen	24
1.7	Directe producten	31
1.8	Acties van groepen op verzamelingen	34
1.9	De stellingen van Sylow	47
1.10	Groepen van orde ≤ 15	54
2	Ringen	63
2.1	Definitie en voorbeelden	63
2.2	Ringmorfismen	71
2.3	Idealen	74
2.4	Hoofdideaaldomeinen en Euclidische domeinen	77
2.5	Quotiëntringen	80
2.6	Maximale idealen en priemidealen	82
2.7	Unieke factorisatie	87
2.8	Directe producten en de Chinese reststelling	98
3	Modulen	101
3.1	Definitie en voorbeelden	101
3.2	Deelmodulen, morfismen, quotiënten, directe sommen	103
3.3	Matrices, vrije modulen, basissen	107
3.4	De Smith normaalvorm	115
3.5	Eindig voortgebrachte modulen over hoofdideaaldomeinen	118



crotchetycomics.blogspot.com



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/4.0/>.

Zowat het eenvoudigste, maar zeker niet onmiddellijk het meest intuïtieve, concept in de abstracte algebra, is een groep. Inderdaad, dergelijke structuren duiken constant op in alle takken van de wiskunde. In de cursus “Discrete Wiskunde I” hebben we al kennisgemaakt met abstracte groepen, en in de cursus “Discrete Wiskunde II” zijn we dieper ingegaan op permutatiegroepen en groepsacties. In dit hoofdstuk van deze cursus gaan we voornamelijk verder met het bestuderen van abstracte groepen.

(Ons gebruik van het woord “abstract” is misschien wat abstract, en slaat hierbij voornamelijk op “niet concreet”, d.w.z. dat de groepen niet a priori gegeven worden als automorfismengroepen van andere objecten, en dus niet a priori iets “doen”, zoals dit wel het geval is bij permutatiegroepen.)

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

$$\begin{aligned}\mathbb{N} &:= \mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}; \\ \mathbb{N}^* &:= \mathbb{Z}_{> 0} = \{1, 2, \dots\}.\end{aligned}$$

1.1 Groepen, deelgroepen en voorbeelden

Voor de volledigheid herhalen we de definities, en geven we een groot aantal voorbeelden. Bij het opbouwen van een abstracte theorie is het immers belangrijk om steeds een grote verscheidenheid van verschillende voorbeelden in gedachten te houden.

Definitie 1.1.1. Een *groep* is een verzameling G met daarop een *samenstellingswet* (ook wel *operatie* genoemd)

$$G \times G \rightarrow G: (s, t) \mapsto s * t,$$

met de volgende eigenschappen:

- voor alle $x, y, z \in G$ geldt $(x * y) * z = x * (y * z)$ (*associativiteit*);

- er is een element $e \in G$ zodat voor alle $g \in G$ geldt dat $e * g = g = g * e$ (het *neutraal element*, de *identiteit*, het *eenheidselement* of het *triviaal element* genoemd);
- voor alle $g \in G$ is er een element $h \in G$ zodat $h * g = g * h = e$; we noteren dan $h = g^{-1}$ en noemen dit het *invers element* van g (of kortweg de *inverse* van g).

We spreken van een *abelse groep*¹ als de samenstellingswet *commutatief* is, d.w.z. als

- voor alle $g, h \in G$ geldt $g * h = h * g$.

Bij abelse groepen wordt de samenstellingswet vaak (maar zeker niet altijd) additief genoteerd; dit wil zeggen dat we de bewerking noteren als $g + h$, het inverse als $-g$, en het neutraal element als 0. Heel soms wordt de additieve notatie ook gebruikt voor niet-abelse groepen.

Multiplicatieve notaties, d.w.z. een punt als bewerking of het achter elkaar schrijven van de elementen, kunnen zowel voor commutatieve als niet commutatieve samenstellingswetten gebruikt worden. Als er geen verwarring mogelijk is, wordt het neutraal element dan vaak als 1 genoteerd.

Opmerking 1.1.2. Het is belangrijk om zich te realiseren dat het additief of multiplicatief noteren van de samenstellingswet slechts een kwestie van *notatie* is; er is dus *niet* zoiets als een “additieve groep” of een “multiplicatieve groep”. Anderzijds weten we reeds dat er rijkere algebraïsche structuren bestaan (velden, ringen, ...) waarop meerdere samenstellingswetten gedefinieerd zijn.

We herinneren eraan dat het neutraal element van een groep en het invers element van een element van een groep uniek bepaald zijn; dit verantwoordt waarom we in de definitie van een groep kunnen spreken over *het* neutraal element en *het* invers van een element.

Lemma 1.1.3. *Zij G een groep.*

- Als $f \in G$ met $f * g = g = g * f$ voor alle $g \in G$, dan is $f = e$.
- Gegeven $g \in G$, en $a, b \in G$ met $a * g = e = g * b$, dan is $a = b$.

Bewijs. (i) Dit volgt uit $f = f * e = e$.

¹genoemd naar N.H. Abel (5 augustus 1802 – 6 april 1829), die bij zijn onderzoek in verband met het oplossen in radicalen van algebraïsche vergelijkingen het belang inzag van de commutativiteit, nog lang voor het begrip van een groep formeel was ingevoerd.

(ii) Dit volgt uit $a = a * e = a * (g * b) = (a * g) * b = e * b = b$. $\square$

Merk op dat deel (ii) van voorgaand lemma meer aantoont dan enkel de uniciteit van het invers element: het bewijst ook dat een *links inverse* of een *rechts inverse* noodzakelijk een *tweezijdig inverse* is.

Lemma 1.1.4. *Zij G een groep, en zij $g \in G$; dan is $(g^{-1})^{-1} = g$.*

Bewijs. Dit volgt uit $((g^{-1})^{-1} * g^{-1}) * g = (g^{-1})^{-1} * (g^{-1} * g)$. $\square$

Lemma 1.1.5. *Zij G een groep, en $x, y, z \in G$. Dan gelden de linkse en rechtse schrappingswetten*

$$\begin{aligned} x * y = x * z &\implies y = z; \\ x * z = y * z &\implies x = y. \end{aligned}$$

Bewijs. Stel $x * y = x * z$. Beide leden voor-vermenigvuldigen met x^{-1} geeft $x^{-1} * (x * y) = x^{-1} * (x * z)$; uit de associativiteit en de definitie van het invers element volgt $y = z$. Analoog voor de rechtse schrappingswet. $\square$

We zullen in het vervolg de samenstellingswet $*$ zelden expliciet noteren, en zullen in plaats daarvan de multiplicatieve notatie gebruiken, als we met willekeurige groepen werken. In dat geval noteren we het neutraal element e ook heel vaak als 1.

Definitie 1.1.6. Beschouw het singleton $G = \{1\}$, met de enige mogelijke samenstellingswet, namelijk $1 * 1 = 1$. Dan is G een groep met deze operatie; dit wordt de *triviale groep* genoemd. We noteren deze vaak kortweg als $G = 1$.

Een deelgroep van een groep is een deelverzameling van een groep die zelf een nieuwe groep vormt, in de volgende precieze betekenis.

Definitie 1.1.7. (i) Zij G een groep en $H \subseteq G$. Dan is H een *deelgroep* van G , als de verzameling H samen met *dezelfde* samenstellingwet en hetzelfde neutraal element als in G , een groep vormt. We noteren dit als $H \leq G$.

(ii) Als bovendien $H \neq G$, dan gebruiken we de notatie $H < G$, of ook soms $H \lneq G$ of $H \subsetneq G$, en we spreken dan van een *echte* of *eigenlijke* deelgroep.

(iii) Als G een groep is met neutraal element e , dan is het singleton $\{e\}$ steeds een deelgroep van G ; we noemen het de *triviale deelgroep* van G , en we noteren die vaak als $1 \leq G$. Een deelgroep $H \leq G$ met $H \neq 1$ noemen we dan een *niet-triviale deelgroep* van G .

Lemma 1.1.8 (Criterium voor deelgroepen). *Zij G een groep en $H \subseteq G$. Dan zijn de volgende uitspraken equivalent.*

- (a) H is een deelgroep van G ;
- (b) H bevat e , en is gesloten onder inversen en gesloten onder de samenstellingswet van G ;
- (c) H is niet ledig, en voor alle $h_1, h_2 \in H$ geldt dat $h_1 h_2^{-1} \in H$.

Bewijs. Zie cursus “Discrete Wiskunde I”. □

We geven nu een aantal voorbeelden van groepen en deelgroepen.

Voorbeelden 1.1.9. (1) Beschouw de verzameling $\mathbb{Z}$ van de gehele getallen. Dan is $\mathbb{Z}$ met de operatie $+$ een abelse groep.

(2) Zij $n \in \mathbb{Z}$ vast gekozen, en beschouw de verzameling $n\mathbb{Z}$ van de gehele getallen deelbaar door n . Dan is $(n\mathbb{Z}, +)$ een abelse groep. Dit is tevens een deelgroep van de groep $(\mathbb{Z}, +)$.

(3) Zij $m \in \mathbb{N}^*$ vast gekozen, en beschouw de verzameling $\mathbb{Z}/m\mathbb{Z}$ van *restklassen modulo m* . Dan is $\mathbb{Z}/m\mathbb{Z}$ met de operatie $+$ een abelse groep. We zullen later de notatie $\mathbb{Z}/m\mathbb{Z}$ verklaren; zoals we zullen zien is dit een quotiëntgroep (zie Definitie 1.6.1). Het is echter gebruikelijk om $\mathbb{Z}/m\mathbb{Z}$ te noteren² als $\mathbb{Z}/m$.

(4) Beschouw opnieuw de verzameling $\mathbb{Z}/m = \mathbb{Z}/m\mathbb{Z}$. We noteren nu

$$(\mathbb{Z}/m)^\times := \{\bar{a} \in \mathbb{Z}/m \mid \gcd(a, m) = 1\}.$$

Dan is $(\mathbb{Z}/m)^\times$ met de vermenigvuldiging als operatie een abelse groep. (Merk op dat de verzameling $(\mathbb{Z}/m)^\times$ inderdaad gesloten is onder de vermenigvuldiging.)

(5) De verzameling $\mathbb{Z}$ met de vermenigvuldiging als operatie is *geen* groep. Inderdaad, de enige elementen van $\mathbb{Z}$ die een inverse hebben voor deze operatie zijn 1 en -1 . De verzameling $\{1, -1\}$ met de vermenigvuldiging als operatie vormt dus wel een groep.

(6) Zij V een vectorruimte over een willekeurig veld K . Dan is V met de operatie $+$ (optelling van vectoren) een abelse groep.

²Men vindt ook soms de notatie $\mathbb{Z}_m$ terug, maar die notatie is ten eerste af te raden, omdat $\mathbb{Z}_p$ (met p priem) in de algebra is voorbehouden voor de zogenaamde p -adische gehelen.

- (7) Zij K een willekeurig veld, en beschouw de verzameling

$$\mathbf{GL}(n, K) := \{A \in \text{Mat}(n, K) \mid \det(A) \neq 0\}$$

van inverteerbare $n \times n$ -matrices over K . Dan is $\mathbf{GL}(n, K)$ met de vermenigvuldiging als operatie een groep, die niet-abels is zodra $n \geq 2$. Deze groep bevat veel interessante deelgroepen, bijvoorbeeld

$$\mathbf{SL}(n, K) := \{A \in \text{Mat}(n, K) \mid \det(A) = 1\}$$

en

$$\mathbf{O}(n, K) := \{A \in \text{Mat}(n, K) \mid AA^t = 1\}.$$

- (8) Zij X een willekeurige verzameling, en beschouw de verzameling $\text{Sym}(X)$ bestaande uit alle mogelijke permutaties van de verzameling X . Beschouw de samenstellingswet op $\text{Sym}(X)$ gegeven door de samenstelling van permutaties. Dan vormt $\text{Sym}(X)$ met deze operatie een groep, die niet-abels is zodra $|X| \geq 3$.

Als $X = \{1, 2, \dots, n\}$ voor een zekere $n \in \mathbb{N}^*$, dan noteren we $\text{Sym}(X)$ ook als $\text{Sym}(n)$ of als $\mathbf{S}_n$, en we noemen dit *de symmetrische groep op n letters*.

We hebben deze groepen en hun deelgroepen, de zogenaamde *permutatiegroepen*, reeds bestudeerd in de cursus “Discrete Wiskunde II”. In het bijzonder hebben we gezien dat elk element van $\mathbf{S}_n$ kan geschreven worden als product van disjuncte cykels, op een unieke manier (op de volgorde van de cykels na). We schrijven een dergelijke cykeldecompositie voor $g \in \mathbf{S}_n$ als

$$g = (a_1 \ a_2 \ \dots \ a_k)(b_1 \ b_2 \ \dots \ b_\ell) \cdots (z_1 \ z_2 \ \dots \ z_m).$$

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 $c_1 m_1 + \cdots + c_d m_d = n$. Bijvoorbeeld, 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.

- (9) De symmetrische groep $\mathbf{S}_n$ bevat een belangrijke deelgroep, namelijk de *alternerende groep* $\mathbf{A}_n$, de deelgroep die bestaat uit de *even permutaties*, i.e. de permutaties die te schrijven zijn als het product van een even aantal transposities. (Ter herinnering: een *transpositie* is een cykel van

lengte 2.) We hebben deze groepen reeds ingevoerd in de cursus “Discrete Wiskunde I” en er wat meer aandacht aan besteed in de cursus “Discrete Wiskunde II”.

- (10) Beschouw de n -dimensionale Euclidische ruimte $\mathbb{R}^n$. Een *isometrie* van $\mathbb{R}^n$ is een bijectie van de puntenverzameling van $\mathbb{R}^n$ die de afstand bewaart (zie cursus “Lineaire Algebra en Meetkunde I”). De verzameling van alle *isometrieën* van $\mathbb{R}^n$, met de samenstelling als operatie, vormt een groep, die we noteren als $\text{ISO}(n)$ of $\text{E}(n)$.
- (11) Beschouw een regelmatige n -hoek in het Euclidische vlak $\mathbb{R}^2$. De verzameling van alle isometrieën van $\mathbb{R}^2$ die deze n -hoek op zichzelf afbeelden, vormt een groep, die we een *diëdergroep* noemen, en noteren als $\mathbf{D}_{2n}$. Deze groepen zijn dus deelgroepen van $\text{ISO}(2)$.
- (12) De groep $\mathbf{D}_{2n}$ bevat n rotaties (waaronder de triviale rotatie) en n loodrechte spiegelingen. De verzameling van de rotaties vormt een deelgroep van $\mathbf{D}_{2n}$, die we een *cyclische groep* noemen, en noteren als $\mathbf{C}_n$. Anderzijds vormt de verzameling van de spiegelingen uiteraard géén deelgroep van $\mathbf{D}_{2n}$.
- (13) Beschouw een graaf $\Gamma = (V, E)$. Dan vormt de verzameling van alle permutaties van V die bogen op bogen en niet-bogen op niet-bogen afbeelden, een groep $\text{Aut}(\Gamma)$, de *automorfismengroep* van de graaf Γ . Dergelijke groepen hebben we uitgebreid bestudeerd in de cursus “Discrete Wiskunde II”.
- (14) We beschrijven nu de *quaternionengroep* $\mathbf{Q}_8$, een groep met 8 elementen, die we ook reeds hebben ontmoet in de cursus “Discrete Wiskunde II”. Als verzameling schrijven we

$$\mathbf{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Het neutraal element van de groep is het element 1; de bewerking leggen we verder volledig vast door de volgende regels.

$$\begin{aligned} (-1)^2 &= 1, & i^2 &= -1, & j^2 &= -1, & k^2 &= -1, \\ (-1)i &= i(-1) = -i, & (-1)j &= j(-1) = -j, & (-1)k &= k(-1) = -k, \\ ij &= k, & ji &= -k, & jk &= i, & kj &= -i, & ki &= j, & ik &= -j. \end{aligned}$$

Merk op dat omwille van de associativiteit de bewerking hierdoor helemaal vast ligt. De groep $\mathbf{Q}_8$ is duidelijk(erwijze een niet-abelse groep.

Oefeningen

1. Zij G een groep, en $x, y \in G$. Toon aan dat $(xy)^{-1} = y^{-1}x^{-1}$.
2. Zij G een verzameling uitgerust met een associatieve samenstellingswet $*$. Veronderstel verder dat er een $e \in G$ bestaat zodat $a * e = a$ voor alle $a \in G$, en dat er voor elke $a \in G$ een element $a^{-1} \in G$ bestaat zodat $a * a^{-1} = e$. Toon aan dat G een groep is.
- *3. Toon aan, door middel van een tegenvoorbeeld, dat voorgaande opgave niet correct is indien we de voorwaarde " $a * a^{-1} = e$ " zouden vervangen door " $a^{-1} * a = e$ ".
4. Beschouw de verzameling van alle complexe getallen met norm 1:

$$S = \{z \in \mathbb{C} \mid z\bar{z} = 1\}.$$

Toon aan dat S een groep is met als operatie de vermenigvuldiging in $\mathbb{C}$.

5. Zij $G = \mathbb{R} \setminus \{0\}$ voorzien van de bewerking

$$a \bullet b := \frac{ab}{2}$$

voor alle $a, b \in G$. Is $(G, \bullet)$ een groep?

6. Zij $G = \mathbb{R} \setminus \{-1\}$ voorzien van de bewerking

$$a \bullet b := a + b + ab$$

voor alle $a, b \in G$. Is $(G, \bullet)$ een groep?

7. Zij $G = \mathbb{R}$ voorzien van de bewerking

$$a \bullet b := |a + b|$$

voor alle $a, b \in G$. Is $(G, \bullet)$ een groep?

8. Beschouw de verzameling $G = \{(a, b) \in \mathbb{R}^2 \mid a \neq 0\}$, en stel

$$(a, b) \bullet (c, d) := (ac, ad + b)$$

voor alle $(a, b), (c, d) \in G$. Toon aan dat $(G, \bullet)$ een niet-abelse groep is.

9. Beschouw de volgende zes functies gedefinieerd op $\mathbb{R} \setminus \{0, 1\}$:

$$\begin{aligned} f_1(x) &= x, & f_2(x) &= \frac{1}{x}, & f_3(x) &= 1 - x, \\ f_4(x) &= \frac{x}{x-1}, & f_5(x) &= \frac{1}{1-x}, & f_6(x) &= 1 - \frac{1}{x}. \end{aligned}$$

Toon dat de verzameling $\{f_1, \dots, f_6\}$ een niet-abelse groep vormt onder de samenstelling van functies.

10. Stel, voor elke $c \in \mathbb{R}$, $A(c) := \begin{pmatrix} c & c \\ c & c \end{pmatrix} \in \text{Mat}_2(\mathbb{R})$. Toon aan dat de verzameling $G = \{A(c) \mid c \in \mathbb{R} \setminus \{0\}\}$ een groep vormt onder de matrixvermenigvuldiging. Merk echter op dat de elementen van G niet inverteerbaar zijn als matrix! In het bijzonder is G geen deelgroep van $\text{GL}_2(\mathbb{R})$.
11. Beschouw de groep $G = \mathbf{S}_3$, en de deelverzameling $H = \{g \in G \mid g^2 = 1\}$. Is H een deelgroep van G ?

1.2 Verdere definities en eigenschappen

Lemma 1.2.1. *De doorsnede $\bigcap_{H \in \mathcal{S}} H$ van een collectie $\mathcal{S}$ van deelgroepen van een groep G is opnieuw een deelgroep van G .*

Bewijs. Merk op dat het neutraal element 1 in elke $H \in \mathcal{S}$ ligt, en dus ook in de doorsnede, die bijgevolg niet ledig is. Als h_1 en h_2 in H liggen voor elke $H \in \mathcal{S}$, dan ligt ook $h_1 h_2^{-1}$ in H voor elke $H \in \mathcal{S}$. Uit het criterium van deelgroepen volgt nu het gestelde. $\square$

Definitie 1.2.2. Zij $X \subseteq G$. De *deelgroep van G voortgebracht door X* is per definitie de kleinste deelgroep van G die X bevat:

$$\langle X \rangle := \bigcap_{X \subseteq H \leq G} H.$$

Uit Lemma 1.2.1 weten we dat bovenstaande doorsnede inderdaad een deelgroep van G is.

Als $X = \{x_1, \dots, x_n\}$, dan gebruiken we ook de notatie

$$\langle x_1, \dots, x_n \rangle := \langle \{x_1, \dots, x_n\} \rangle.$$

Als er voor een groep G een eindige deelverzameling $X \subseteq G$ bestaat zodat $G = \langle X \rangle$, dan noemen we G een *eindig voortgebrachte groep*.

Opmerking 1.2.3. Het kan soms nuttig zijn om voor een gegeven deelverzameling $X \subseteq G$ de elementen van $\langle X \rangle$ expliciet te kunnen beschrijven. Dit kan als volgt:

$$\langle X \rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_k^{\epsilon_k} \mid k \in \mathbb{N}, x_i \in X, \epsilon_i \in \{1, -1\}\}.$$

(Als $k = 0$ bedoelen we hierbij het neutraal element van de groep G .) Merk op dat de verzameling in het rechterlid inderdaad gesloten is onder de groepsbewerking en onder het nemen van inversen, het neutraal element bevat, en de verzameling X bevat; het is tevens de kleinste mogelijke groep die hieraan voldoet, omdat elke deelgroep die X bevat duidelijkerwijze alle elementen van de vorm $x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_k^{\epsilon_k}$ moet bevatten.

Definitie 1.2.4. De *orde* van een groep G is per definitie de kardinaliteit van G (als een verzameling). We noteren dit als $|G|$ of ook soms als $o(G)$ of $\#G$. Als $|G|$ eindig is, noemen we G een *eindige groep*.

Ook het belangrijke begrip van *nevenklassen* van een deelgroep in een groep kennen we reeds vanuit de cursus “Discrete Wiskunde I”, en herhalen we hier nogmaals.

Definitie 1.2.5. Zij $g \in G$ en $H \leq G$. De verzameling

$$gH := \{gh \mid h \in H\}$$

noemen we een *linkse nevenklasse* van H in G . Analoog noemen we

$$Hg := \{hg \mid h \in H\}$$

een *rechtse nevenklasse* van H in G . We noteren

$$\begin{aligned} L_G(H) &:= \{\text{linkse nevenklassen van } H \text{ in } G\} = \{gH \mid g \in G\}; \\ R_G(H) &:= \{\text{rechtse nevenklassen van } H \text{ in } G\} = \{Hg \mid g \in G\}. \end{aligned}$$

We noemen een (linkse of rechtse) nevenklasse van H in G *triviaal* als ze gelijk is aan H zelf. Het volgende lemma zegt ons precies wanneer dit het geval is.

Lemma 1.2.6 (Opslorplemma). *Zij G een groep, $H \leq G$ een deelgroep, en $g \in G$. Dan is $gH = H$ als en slechts als $g \in H$ (en analoog voor rechtse nevenklassen).*

Bewijs. Als $gH = H$, dan is in het bijzonder $g = g \cdot 1 \in gH = H$. Stel omgekeerd dat $g \in H$. Dan geldt voor elke $h \in H$ dat $gh \in H$; bijgevolg is $gH \subseteq H$. Analoog is $g^{-1}H \subseteq H$ en dus $H \subseteq gH$. We besluiten dat $gH = H$. $\square$

Stelling 1.2.7 (Lagrange). (i) *Zij G een groep en $H \leq G$. Dan vormen de linkse (resp. rechtse) nevenklassen van H in G een partitie van G .*

(ii) *Zij G een eindige groep en $H \leq G$. Dan is $|H|$ een deler van $|G|$.*

Bewijs. Zie cursus “Discrete Wiskunde I”. De eerste uitspraak is in essentie een gevolg van het opslorplemma; de tweede uitspraak volgt onmiddellijk uit de eerste omdat elke nevenklasse van H in G precies $|H|$ elementen bevat. $\square$

We hebben vroeger reeds het begrip van de *index* van een deelgroep H van een eindige groep G ingevoerd, als $[G : H] = |G|/|H|$. Dit begrip kan echter ook zinvol zijn voor oneindige groepen. We bewijzen eerst een lemma.

Lemma 1.2.8. *Zij G een groep en $H \leq G$. Dan is $|R_G(H)| = |L_G(H)|$.*

Bewijs. Beschouw de afbeelding $\alpha: R_G(H) \rightarrow L_G(H): Hg \mapsto g^{-1}H$. Deze afbeelding is goed gedefinieerd, want als $Hg_1 = Hg_2$, dan is $g_2g_1^{-1} \in H$ en bijgevolg $g_2^{-1}H = g_2^{-1} \cdot g_2g_1^{-1}H = g_1^{-1}H$. Op gelijkaardige wijze gaat men na dat α injectief is. Vervolgens is α duidelijkertwijze surjectief, en bijgevolg bijectief. We besluiten dat $|R_G(H)| = |L_G(H)|$. $\square$

Definitie 1.2.9. Zij G een groep en $H \leq G$. De *index* van H in G definiëren we als

$$[G : H] := |R_G(H)| = |L_G(H)|.$$

Uit de stelling van Lagrange (1.2.7) weten we dat voor een eindige groep G geldt dat

$$[G : H] = |G|/|H|,$$

in overeenstemming met de definitie die we reeds kenden. De index is nu echter ook gedefinieerd voor oneindige groepen G , en ook dan kan de index $[G : H]$ eindig zijn.

Voorbeeld 1.2.10. Zij $G = (\mathbb{Z}, +)$, en stel $H = n\mathbb{Z} \leq G$ met $n \in \mathbb{N}^*$. Dan is $|G| = |H| = \infty$, maar $[G : H] = n$.

Notatie 1.2.11. We zullen de notatie-conventie die we hebben toegepast voor de nevenklassen gH en Hg algemeen toepassen. Als bijvoorbeeld A en B willekeurige deelverzamelingen zijn van een groep G , dan gebruiken we de notatie

$$AB := \{ab \mid a \in A, b \in B\}.$$

Opmerking 1.2.12. Deze notaties stellen ons in staat om gemakkelijk te redeneren met hele verzamelingen ineens, maar de nodige voorzichtigheid is natuurlijk geboden. Toon bijvoorbeeld zelf aan als oefening dat als A en B deelverzamelingen zijn van G , en $g \in G$, dan is $A = gB$ equivalent met $g^{-1}A = B$.

Oefeningen

12. Zij G een groep, en A en B twee deelverzamelingen van G . Bewijs de ongelijkheid $|AB| \leq |A| \cdot |B|$.
13. Zij G een groep, A en B twee deelverzamelingen van G , en $g \in G$. Toon aan dat $g(A \cap B) = gA \cap gB$.
14. Beschouw de groep $G = \mathrm{GL}_2(\mathbb{R})$ en de deelgroep $H = \mathrm{SL}_2(\mathbb{R})$. Beschouw nu de deelverzameling $S = \{A \in G \mid \det(A) = 2\}$ van G . Toon aan dat S een nevenklasse is van H in G .
15. Beschouw de drie *Pauli spin matrices* $\sigma_x, \sigma_y, \sigma_z$ in $\mathrm{GL}_2(\mathbb{C})$ gegeven door

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Zij nu $H = \langle \sigma_x, \sigma_y, \sigma_z \rangle \leq \mathrm{GL}_2(\mathbb{C})$, de groep voortgebracht door de Pauli spin matrices. Toon aan dat $|H| = 16$.

16. Zij G een eindige groep, en zij $A \leq B \leq G$. Toon aan dat $[G : A] = [G : B][B : A]$.
- *17. Zij G een groep, en zij $A \leq B \leq G$. Toon aan dat $[G : A] = [G : B][B : A]$.

18. Het omgekeerde van de Stelling van Lagrange is in het algemeen niet geldig: als G een groep is van orde n , en $d \mid n$, dan bezit G niet noodzakelijk een deelgroep van orde d . Toon dit aan door te bewijzen dat $\mathbf{A}_4$, een groep van orde 12, geen deelgroep van orde 6 bezit.

Definitie 1.2.13. Zij G een groep, $g \in G$ en $n \in \mathbb{Z}$. Dan definiëren we

$$g^n := \begin{cases} e & \text{als } n = 0; \\ \underbrace{gg \cdots g}_{n \text{ keer}} & \text{als } n > 0; \\ \underbrace{g^{-1}g^{-1} \cdots g^{-1}}_{|n| \text{ keer}} & \text{als } n < 0. \end{cases}$$

Lemma 1.2.14. Zij G een groep, $g \in G$, en $m, n \in \mathbb{Z}$. Dan geldt

- (i) $g^{m+n} = g^m g^n$ en $(g^m)^n = g^{mn}$;
- (ii) $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

Bewijs. (i) Dit volgt eenvoudig uit de definitie.

(ii) Dit volgt onmiddellijk uit Opmerking 1.2.3. □

Opmerking 1.2.15. Als we een (abelse) groep additief noteren, zullen we eveneens de exponent-notatie vervangen door een vermenigvuldigings-notatie, en we zullen dus $n \cdot g$ of ng schrijven in plaats van g^n .

Definitie 1.2.16. Een groep $G = \langle g \rangle$ voorgebracht door één element $g \in G$ noemen we een *cyclische groep*. Merk op dat een cyclische groep steeds abels is. Als G cyclisch is, dan noemen we een element g zodat $G = \langle g \rangle$ een *voortbrenger* of een *generator* voor G . Deze voortbrenger is geenszins uniek bepaald.

Cyclische groepen kennen we reeds uit de cursus “Discrete Wiskunde I”. In paragraaf 1.4 zullen we nogmaals de belangrijkste eigenschappen van cyclische groepen herhalen.

Definitie 1.2.17. Zij G een groep en $g \in G$. Het kleinste positieve gehele getal $n \in \mathbb{N}^*$ zodat $g^n = e$ noemen we de *orde van g* , en noteren we als $|g|$ of als $o(g)$. Als er geen dergelijke n bestaat, dan zeggen we dat de orde van g oneindig is: $|g| = \infty$. Als $|g| = 2$, dan wordt g een *involutie* genoemd.

Lemma 1.2.18. Zij G een groep en $g \in G$ een element met eindige orde. Zij $d \in \mathbb{Z}$; dan is $g^d = 1$ als en slechts als $o(g) \mid d$.

Bewijs. Stel $o(g) = n$; we kunnen d op unieke wijze schrijven als $d = qn + r$ met $0 \leq r < n$ via Euclidische deling. Dan is $g^d = g^{qn+r} = (g^n)^q \cdot g^r = g^r$; bijgevolg is $g^d = 1$ als en slechts als $g^r = 1$. Omdat $0 \leq r < n = o(g)$, kan g^r enkel maar gelijk zijn aan 1 als $r = 0$. $\square$

Stelling 1.2.19. *Zij G een groep en $g \in G$, en stel $|g| = n$.*

(i) *Als n eindig is, dan*

$$g^i = g^j \iff i \equiv j \pmod{n},$$

en bijgevolg

$$\langle g \rangle = \{g^0, g^1, \dots, g^{n-1}\}.$$

(ii) *Als $n = \infty$, dan*

$$g^i = g^j \iff i = j,$$

en bijgevolg

$$\langle g \rangle = \{\dots, g^{-k}, \dots, g^{-1}, g^0, g^1, \dots, g^k, \dots\}.$$

(iii) *In beide gevallen geldt $|g| = |\langle g \rangle|$.*

Bewijs. (i) Stel $i, j \in \mathbb{Z}$ willekeurig, en stel $k = i - j$. Dan is $g^i = g^j$ als en slechts als $g^k = 1$. Uit Lemma 1.2.18 weten we dat dit equivalent is met $n \mid k$, of nog, $k \equiv 0 \pmod{n}$ of dus $i \equiv j \pmod{n}$.

(ii) Stel $i, j \in \mathbb{Z}$ willekeurig. Als $i = j$ dan is uiteraard $g^i = g^j$. Omgekeerd, als $g^i = g^j$, dan is $g^{|i-j|} = 1$, maar omdat $o(g) = \infty$ kan dit enkel als $i = j$.

(iii) Dit volgt uit (i) en (ii). $\square$

Gevolg 1.2.20. *Zij G een eindige groep en $g \in G$. Dan is $|g|$ een deler van $|G|$. Bovendien geldt voor elke $g \in G$ dat $g^{|G|} = 1$.*

Bewijs. De eerste bewering volgt uit de stelling van Lagrange (1.2.7) en Stelling 1.2.19(iii). De tweede bewering volgt nu uit Lemma 1.2.18. $\square$

Opmerking 1.2.21. We zullen dit gevolg vaak ook “de stelling van Lagrange” noemen.

Gevolg 1.2.22 (Stelling van Euler). *Zij $n \in \mathbb{N}^*$. Dan geldt voor elke $x \in \mathbb{Z}$ die onderling ondeelbaar is met n , dat*

$$x^{\varphi(n)} \equiv 1 \pmod{n},$$

waarbij φ de Euler totiënt-functie is.

Bewijs. De verzameling $G = (\mathbb{Z}/n)^\times$ is een groep met $\varphi(n)$ elementen. Stel g gelijk aan de restklasse van $x \pmod{n}$, dus $g \in G$. Uit de stelling van Lagrange volgt nu dat $g^{\varphi(n)} = 1$. $\square$

Definitie 1.2.23. Zij G een willekeurige groep. Dan definiëren we de *exponent van G* als

$$\exp(G) := \operatorname{lcm}_{g \in G} o(g).$$

Een equivalente definitie is dat $\exp(G)$ het kleinste natuurlijke getal d is zodat $g^d = 1$ voor alle $g \in G$; als er geen dergelijke d bestaat dan is $\exp(G) = \infty$.

Merk op dat $\exp(G)$ kan gelijk zijn aan ∞ , zelfs als elk element van G eindige orde heeft. Voor eindige groepen is $\exp(G)$ wel steeds eindig:

Lemma 1.2.24. *Zij G een eindige groep. Dan is $\exp(G)$ een deler van $|G|$. In het bijzonder is $\exp(G)$ eindig.*

Bewijs. Uit de stelling van Lagrange weten we dat voor elke $g \in G$ geldt dat $g^{|G|} = 1$. Hieruit volgt het gestelde. $\square$

Zoals we hebben gezien is de samenstellingswet in een groep niet steeds commutatief. We willen echter nauwkeuriger kunnen uitdrukken in welke mate de commutativiteit wel of niet geldt; daarom de volgende definities.

Definitie 1.2.25. Zij G een willekeurige groep.

- (i) Als $g, h \in G$, dan zeggen we dat g en h (*met elkaar*) *commuteren* als en slechts als $gh = hg$.
- (ii) Zij $g, h \in G$. De *commutator* van g en h definiëren we als

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

Merk op dat $[h, g] = [g, h]^{-1}$, en dat $[g, h] = 1$ als en slechts als g en h commuteren. De commutator drukt dus in zekere zin uit in welke mate g en h niet-commuterend zijn.

- (iii) 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.

- (iv) 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 $AB = BA$!

- (v) Een groep G wordt *perfect* genoemd als $[G, G] = G$. Perfecte groepen zijn dus in zekere zin de “minst abelse” groepen.
- (vi) Het *centrum* van G bestaat uit de elementen van G die met *alle* elementen van G commuteren:

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

Het is eenvoudig in te zien dat $Z(G)$ inderdaad een deelgroep is van G ; bovendien is $Z(G)$ zelf abels.

Oefeningen

19. Zij G een groep die uitsluitend uit involuties en een neutraal element bestaat. Toon aan dat G abels is.
20. Zij G een eindige groep, en $A, B \leq G$ deelgroepen met $\gcd(|A|, |B|) = 1$. Bewijs dat $A \cap B = 1$.
21. Zij $g, h \in G$ twee commuterende elementen met $\gcd(o(g), o(h)) = 1$. Bewijs dat $o(gh) = o(g)o(h)$. Toon aan met tegenvoorbeelden dat de conclusie niet geldig is als één van beide voorwaarden (nl. het commuteren en het onderling ondeelbaar zijn van de ordes) wordt weggelaten.
22. Bepaal de orde van $\mathbf{S}_n$. Hoeveel involuties bevat $\mathbf{S}_4$? Bepaal $\exp(\mathbf{S}_5)$ en $\exp(\mathbf{S}_6)$.
23. Bepaal de orde van $\mathbf{D}_{2n}$. Toon aan dat $\mathbf{D}_{2n}$ niet-abels is zodra $n \geq 3$.
24. Bepaal het centrum van de groep $\mathbf{SL}_2(\mathbb{R})$.
25. Beschouw de groep S uit Oefening 4 (p. 7). Zoek een oneindige deelgroep G van S , met de eigenschap dat elk element van G eindige orde heeft, terwijl $\exp(G) = \infty$.
26. Zij $g \in \mathbf{S}_n$ een element met cykelstructuur $c_1^{m_1} \cdot c_2^{m_2} \cdots c_d^{m_d}$. Toon aan dat $o(g) = \text{lcm}(c_1, \dots, c_d)$. (Zie ook de cursus “Discrete Wiskunde II”.)
27. Toon aan dat de groep $\mathbf{S}_n$ ($n \geq 2$) niet perfect is.

1.3 Groepsmorfismen

Net zoals we in de cursus “Lineaire Algebra en Meetkunde I” gezien hebben dat we niet over vectorruimten kunnen denken zonder de bijhorende lineaire afbeeldingen te beschouwen, zo geldt dat we niet over groepen kunnen denken zonder de bijhorende morfismen. Ook dit begrip kennen we reeds vanuit de cursus “Discrete Wiskunde I”, maar we zullen er in deze cursus veel meer aandacht aan besteden.

We zullen morfismen meestal *exponentieel* noteren.

Definitie 1.3.1. Zij G, H twee groepen, met samenstellingswetten $*_G$ en $*_H$, respectievelijk. Een afbeelding

$$\theta: G \rightarrow H$$

is een *morfisme* (ook *homomorfisme* of *groepsmorfisme* genoemd) als θ de groepsbewerking bewaart, in de zin dat

$$(g_1 *_G g_2)^\theta = g_1^\theta *_H g_2^\theta$$

voor alle $g_1, g_2 \in G$.

Als θ een morfisme is van G naar H , dan definiëren we de *kern van θ* als

$$\ker(\theta) := \{g \in G \mid g^\theta = 1_H\},$$

en het *beeld van θ* als

$$\text{im}(\theta) := \{g^\theta \mid g \in G\} = \{h \in H \mid \exists g \in G: g^\theta = h\}.$$

Stelling 1.3.2. Zij G, H twee groepen, en zij $\theta: G \rightarrow H$ een morfisme.

- (i) $1_G^\theta = 1_H$;
- (ii) voor alle $g \in G$ geldt $(g^{-1})^\theta = (g^\theta)^{-1}$;
- (iii) $\ker(\theta) \leq G$;
- (iv) $\text{im}(\theta) \leq H$;
- (v) gegeven een deelgroep $K \leq H$; dan is het inverse beeld³ van K onder θ ,

$$K^{\theta^{-1}} := \{g \in G \mid g^\theta \in K\},$$

een deelgroep van G ;

³Merk op dat θ^{-1} geen afbeelding is, want het beeldt elementen af op deelverzamelingen. Zie ook Lemma 1.3.3.

(vi) θ is injectief als en slechts als $\ker(\theta) = 1$.

Bewijs. Het bewijs van uitspraken (i)–(iv) hebben we reeds gezien in de cursus “Discrete Wiskunde I”; het is zinvol om deze uitspraken nog eens zelf als oefening opnieuw te bewijzen.

(v) Zij $K \leq H$, en beschouw $g_1, g_2 \in K^{\theta^{-1}}$. Dan is $g_1^\theta = k_1$ en $g_2^\theta = k_2$ voor zekere $k_1, k_2 \in K$. Hieruit volgt

$$(g_1 g_2^{-1})^\theta = g_1^\theta (g_2^\theta)^{-1} = k_1 k_2^{-1} \in K,$$

en bijgevolg $g_1 g_2^{-1} \in K^{\theta^{-1}}$. Uit het criterium voor deelgroepen volgt dus dat $K^{\theta^{-1}} \leq G$.

(vi) Als θ injectief is, dan is uiteraard $\ker(\theta) = 1$. Veronderstel omgekeerd dat $\ker(\theta) = 1$, en zij $g_1, g_2 \in G$ met $g_1^\theta = g_2^\theta$. Dan is

$$(g_1 g_2^{-1})^\theta = g_1^\theta (g_2^\theta)^{-1} = 1_H,$$

en omdat $\ker(\theta) = 1$ impliceert dit dat $g_1 g_2^{-1} = 1_G$, of dus $g_1 = g_2$. Dit toont aan dat θ injectief is. $\square$

Het feit dat een morfisme θ injectief is als en slechts als $\ker(\theta) = 1$ kan sterk veralgemeend worden, als volgt.

Lemma 1.3.3. *Zij G, H twee groepen, en zij $\theta: G \rightarrow H$ een morfisme. Dan geldt voor elke $h \in \text{im}(\theta) \leq H$ dat*

$$h^{\theta^{-1}} := \{g \in G \mid g^\theta = h\}$$

een (linkse en rechtse) nevenklasse van $\ker(\theta)$ is. In het bijzonder geldt dat elk element van $\text{im}(\theta)$ precies $|\ker(\theta)|$ keer bereikt wordt door θ .

Bewijs. Zij $h \in \text{im}(\theta)$, en schrijf $h = g^\theta$. Voor een willekeurige $k \in G$ geldt nu dat $k^\theta = h$ als en slechts als $(kg^{-1})^\theta = 1_H$, of nog, als en slechts als k bevat is in de rechtse nevenklasse $\ker(\theta)g$. Analooog geldt dit als en slechts als $(g^{-1}k)^\theta = 1_H$, of nog, als en slechts als k bevat is in de linkse nevenklasse $g\ker(\theta)$. We besluiten dat $h^{\theta^{-1}} = \ker(\theta)g = g\ker(\theta)$. $\square$

Definitie 1.3.4. Een injectief morfisme wordt ook een *monomorfisme* genoemd; een surjectief morfisme noemen we ook een *epimorfisme*. Als een morfisme $\theta: G \rightarrow H$ een monomorfisme is, noteren we het ook wel als $\theta: G \hookrightarrow H$; als het een epimorfisme is, noteren we dit als $\theta: G \twoheadrightarrow H$. Als $\theta: G \rightarrow H$ een epimorfisme is, dan zeggen we dat H een *homomorf beeld van G* is.

Een bijectief morfisme noemen we een *isomorfisme*. Als θ een isomorfisme is, dan is θ^{-1} opnieuw een morfisme (ga dit zelf na!), en bijgevolg is θ^{-1} zelf ook een isomorfisme. Als $\theta: G \rightarrow H$ een isomorfisme is, dan zeggen we dat de groepen G en H *isomorf* zijn, en we noteren dit als $G \cong H$. We noteren het isomorfisme θ dan ook wel als $\theta: G \xrightarrow{\sim} H$.

Als θ een morfisme is van een groep G naar zichzelf, dan noemen we θ een *endomorfisme*; als θ bovendien bijectief is, dan noemen we θ een *automorfisme*.

Opmerking 1.3.5. Als $\theta: G \hookrightarrow H$ een monomorfisme is, dan is $G \cong \text{im}(\theta)$.

Groepen die isomorf zijn, zijn in zekere zin “gelijk”: ze hebben precies dezelfde intrinsieke eigenschappen. De nodige voorzichtigheid is geboden: een groep G kan uiteraard isomorfe *deel*groepen hebben die toch verschillend zijn.

Voorbeelden 1.3.6. (1) Beschouw de groep $G = \{1, -1\}$ met de vermenigvuldiging als operatie, en de groep $H = \mathbb{Z}/2$ met de optelling als operatie. Dan zijn G en H isomorfe groepen. Inderdaad, de afbeelding

$$\varphi: G \rightarrow H: \begin{cases} 1 \mapsto 0 \pmod{2} \\ -1 \mapsto 1 \pmod{2} \end{cases}$$

is een bijectief morfisme.

(2) Beschouw de groep $G = (\mathbb{Z}, +)$ van de gehele getallen en de deelgroep $H = (2\mathbb{Z}, +)$ van de even getallen. Dan zijn G en H isomorfe groepen. Inderdaad, de afbeelding

$$\varphi: G \rightarrow H: n \mapsto 2n$$

is een bijectief morfisme. We zien dus dat G isomorf is met een echte deelgroep van zichzelf. Merk ook op dat de afbeelding

$$\psi: G \rightarrow G: n \mapsto 2n$$

een endomorfisme is van G , dat echter geen automorfisme is.

(3) We hebben $(\mathbb{Z}/8)^\times \cong \mathbf{D}_4$. Als we de elementen van $\mathbf{D}_4$ noteren als $\mathbf{D}_4 = \{e, a, b, c\}$, dan wordt een expliciet isomorfisme φ van $(\mathbb{Z}/8)^\times$ naar $\mathbf{D}_4$ gegeven door

$$\varphi(1) = e, \quad \varphi(3) = a, \quad \varphi(5) = b, \quad \varphi(7) = c.$$

Opmerking 1.3.7. We zeggen vaak dat een uitspraak geldt *op isomorfisme na*. Zo hebben we bijvoorbeeld reeds gezien in de cursus “Discrete Wiskunde I” dat er op isomorfisme na slechts twee groepen van orde 4 zijn, namelijk $\mathbf{C}_4$ en $\mathbf{D}_4$. De betekenis hiervan is duidelijk: elke groep van orde 4 is ofwel isomorf met $\mathbf{C}_4$, ofwel isomorf met $\mathbf{D}_4$. (Zie ook Oefeningen 29 en 34.)

Oefeningen

28. Zij G, H twee groepen. Bewijs dat G een deelgroep bezit die isomorf is met H , als en slechts als er een monomorfisme bestaat van H naar G .
29. Toon aan dat elke groep van orde 2 isomorf is met $\mathbf{C}_2$, en dat elke groep van orde 3 isomorf is met $\mathbf{C}_3$. Toon anderzijds aan dat een groep van orde 4 ofwel isomorf is met $\mathbf{C}_4$, ofwel met $\mathbf{D}_4$.
30. Bewijs dat de multiplicatieve groepen $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$ en $(\mathbb{C}^\times, \cdot)$ twee aan twee niet-isomorf zijn.
31. Bewijs dat $\mathbf{S}_3 \cong \mathbf{D}_6$.
32. Toon aan dat er een monomorfisme bestaat van $\mathbf{D}_{2m}$ naar $\mathbf{D}_{2n}$ als en slechts als $m \mid n$.
33. Zij $n \geq 2$, en stel

$$G = \left\{ \begin{pmatrix} e^{2k\pi i/n} & 0 \\ 0 & e^{-2k\pi i/n} \end{pmatrix} \mid k \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} 0 & e^{2k\pi i/n} \\ e^{-2k\pi i/n} & 0 \end{pmatrix} \mid k \in \mathbb{Z} \right\}.$$
 Toon aan dat G een groep vormt onder de vermenigvuldiging in $\text{Mat}(2, \mathbb{C})$, en dat $G \cong \mathbf{D}_{2n}$.
- *34. Toon aan dat elke niet-abelse groep van orde 8 isomorf is met $\mathbf{D}_8$ of met $\mathbf{Q}_8$.
35. Zij $R = (\mathbb{R}_{>0}, \cdot)$ de groep van de reële getallen > 0 met de vermenigvuldiging als bewerking. Toon aan dat $R \cong (\mathbb{R}, +)$.

1.4 Cyclische groepen

In deze paragraaf herhalen we kort een aantal belangrijke eigenschappen van cyclische groepen uit de cursus “Discrete Wiskunde I”. Aangezien een willekeurige groep heel veel cyclische deelgroepen bevat (voor elke $g \in G$ is $\langle g \rangle$ immers een cyclische deelgroep), is het belangrijk om deze goed te begrijpen.

Stelling 1.4.1. (i) *Zij $G = \langle g \rangle$ een cyclische groep van orde n . Dan is $G \cong \mathbb{Z}/n$. Een expliciet isomorfisme wordt gegeven door*

$$\varphi: G \rightarrow \mathbb{Z}/n: g^k \mapsto k + n\mathbb{Z}.$$

- (ii) Zij $G = \langle g \rangle$ een oneindige cyclische groep. Dan is $G \cong \mathbb{Z}$. Een expliciet isomorfisme wordt gegeven door

$$\varphi: G \rightarrow \mathbb{Z}: g^k \mapsto k.$$

Bewijs. Dit hebben we bewezen in de cursus “Discrete Wiskunde I”. Het belangrijkste punt in het bewijs is het feit dat φ goed gedefinieerd is, d.w.z. onafhankelijk is van de keuze van de schrijfwijze van een willekeurig element van G in de vorm g^k . $\square$

We gebruiken bijna altijd de notatie $\mathbf{C}_n$ (zie Voorbeeld 1.1.9(12)) voor “de” cyclische groep van orde n . “De” oneindige cyclische groep wordt meestal eenvoudigweg als $\mathbb{Z}$ genoteerd, al ziet men ook soms de notatie $\mathbf{C}_\infty$ opduiken.

Opmerking 1.4.2. Het is dus niet zo dat er voor elke mogelijke orde een cyclische groep bestaat. Elke cyclische groep is immers aftelbaar; er bestaat dus bijvoorbeeld geen cyclische groep waarvan de orde gelijk is aan $|\mathbb{R}|$.

We kunnen nu zonder veel moeite de structuur van de cyclische groepen verder analyseren.

Stelling 1.4.3. Zij $G = \langle g \rangle$ een eindige cyclische groep van orde n .

- (i) Voor elke $k \in \mathbb{Z}$ geldt $o(g^k) = n / \gcd(k, n)$.
- (ii) Voor elke $k \in \mathbb{Z}$ geldt $\langle g^k \rangle = \langle g^{\gcd(k, n)} \rangle$.
- (iii) Elke deelgroep van G is zelf ook cyclisch.
- (iv) Voor elke deler $d \mid n$ is er precies één deelgroep $H \leq G$ met $|H| = d$, namelijk de deelgroep $H = \langle g^{n/d} \rangle$.
- (v) Zij $k \in \mathbb{Z}$. Dan is g^k een generator voor G (i.e. $G = \langle g^k \rangle$) als en slechts als $\gcd(k, n) = 1$. Er zijn dus $\varphi(n)$ dergelijke generatoren.
- (vi) Zij $k \in \mathbb{N}^*$. Het aantal elementen van orde k in G is gelijk aan 0 als $k \nmid n$, en is gelijk aan $\varphi(k)$ als $k \mid n$. In het bijzonder is $\exp(G) = n$.

Bewijs. De eigenschappen (iii)–(vi) werden reeds bewezen in de cursus “Discrete Wiskunde I”. Toon zelf als oefening de resterende eigenschappen (i) en (ii) aan. Het bewijs van elk van deze eigenschappen maakt slechts gebruik van eenvoudige arithmetiek. $\square$

We geven ook een korte analyse van de oneindige cyclische groep.

Stelling 1.4.4. Zij $G = \langle g \rangle$ een oneindige cyclische groep.

- (i) *Elk niet-triviaal element van G heeft oneindige orde.*
- (ii) *Elke deelgroep van G is zelf ook cyclisch.*
- (iii) *Voor elke $k \in \mathbb{N}^*$ is er precies één deelgroep $H \leq G$ met $[G : H] = k$, namelijk de deelgroep $H = \langle g^k \rangle$.*
- (iv) *Zij $k \in \mathbb{Z}$. Dan is g^k een generator voor G als en slechts als $k \in \{1, -1\}$.*

Bewijs. Het bewijs is analoog aan dat van Stelling 1.4.3, maar eenvoudiger. Werk zelf de details uit. $\square$

Oefeningen

36. Beschouw de deelgroep

$$G = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\} \leq \mathrm{SL}(2, \mathbb{Z}).$$

Toon aan dat G cyclisch is, en bepaal alle $g \in G$ zodat $G = \langle g \rangle$.

37. Bepaal voor elke $n \geq 1$ het aantal involuties in de cyclische groep $\mathbf{C}_n$. Bepaal ook het aantal involuties in de diëdergroep $\mathbf{D}_{2n}$.

1.5 Toevoeging en normaaldelers

Het feit dat $\ker(\theta)$ een deelgroep is van G waarvan de rechtse nevenklassen gelijk zijn aan de linkse nevenklassen, is een bijzondere eigenschap van deze deelgroep.

Definitie 1.5.1. Zij $N \leq G$. Dan wordt N een *normaaldeler* van G genoemd als

$$g^{-1}Ng = N$$

voor alle $g \in G$, of equivalent, als elke rechtse nevenklasse van N ook een linkse nevenklasse van N is. We noteren dit als $N \trianglelefteq G$. Als $N \trianglelefteq G$ en tegelijk $N \neq G$, dan gebruiken we ook de notatie $N \triangleleft G$, en we noemen N dan een *echte* of *eigenlijke* normaaldeeler.

Definitie 1.5.2. Zij $g, h \in G$. Het element $g^{-1}hg$ noemen we de *toegevoegde van h met g* , en noteren we als h^g . De afbeelding

$$\iota_g: G \rightarrow G: h \mapsto h^g := g^{-1}hg$$

noemen we *toevoeging met g* , of ook wel het *inwendig automorfisme bepaald door g* . (Ga zelf na dat een inwendig automorfisme inderdaad een automorfisme is!)

Voor een willekeurige deelverzameling $D \subseteq G$ noteren we ook

$$D^g := \{d^g \mid d \in D\}.$$

Zij $g, h \in G$. We zeggen dat g en h *toegevoegd zijn aan elkaar*, of kortweg dat ze *toegevoegd zijn*, als er een $k \in G$ bestaat zodat $g^k = h$. De relatie “toegevoegd zijn” is een equivalentierelatie (ga dit na!); de equivalentieklassen van deze relatie noemen we de *klassen van toegevoegde elementen* of *toevoegingsklassen* van G . Nog anders gesteld, de *toevoegingsklasse van g in G* is precies

$$g^G := \{g^h \mid h \in G\}.$$

Opmerking 1.5.3. We zien dus dat een normaaldeler niets anders is dan een deelgroep die *invariant is onder toevoeging*, waaronder we verstaan dat toevoeging met *elk* element van G de deelgroep invariant (i.e. globaal onveranderd) laat. Een deelgroep $N \leq G$ is dus een normaaldeler als en slechts als $N^g = N$ voor alle $g \in G$.

Opmerking 1.5.4. Het feit dat $N^g = N$ voor alle $g \in G$ impliceert geenszins dat $n^g = n$ voor alle $n \in N$! Het zegt enkel dat $n^g \in N$ voor elke $n \in N$ en elke $g \in G$.

Om praktisch na te gaan of een gegeven deelgroep een normaaldeler is, is het volgend criterium handig.

Stelling 1.5.5 (Criterium voor normaaldelers). *Zij G een groep, en $N \leq G$. Als voor alle $n \in N$ en alle $g \in G$ geldt dat $n^g \in N$, dan is $N \trianglelefteq G$.*

Bewijs. De veronderstelling zegt precies dat $N^g \subseteq N$ voor alle $g \in G$. Als we hierin g vervangen door g^{-1} , bekommen we $N^{g^{-1}} \subseteq N$, en beide leden toevoegen met g geeft $N \subseteq N^g$. We hebben dus beide inclusies van de gelijkheid $N^g = N$ bewezen voor alle g , en dus is $N \trianglelefteq G$. $\square$

Opmerking 1.5.6. Als G een oneindige groep is en $H \leq G$, dan kan het voorkomen dat voor een *individuele* $g \in G$ wel geldt dat $H^g \leq H$, maar toch $H^g \neq H$. Voorgaand criterium zegt precies dat als $H^g \leq H$ voor alle $g \in G$, dan $H \trianglelefteq G$ en bijgevolg $H^g = H$ voor alle $g \in G$.

Lemma 1.5.7. (i) *Als G een abelse groep is, dan werkt toevoeging triviaal (i.e. $h^g = h$ voor alle $g, h \in G$); in het bijzonder is elke deelgroep een normaaldeler.*

(ii) *Zij G een willekeurige groep en zij $g, h \in G$. Dan zijn gh en hg aan elkaar toegevoegd. In het bijzonder is $o(gh) = o(hg)$.*

- (iii) *Zij G een willekeurige groep. De doorsnede van normaaldelers van G is opnieuw een normaaldeeler van G .*

Bewijs. Oefening. □

Definitie 1.5.8. Zij G een willekeurige groep. De verzameling van alle automorfismen van G vormt zelf ook een groep, met de samenstelling als groepsoperatie. We noteren deze als $\text{Aut}(G)$ en noemen dit de *automorfismengroep van G* .

De verzameling van alle inwendige automorfismen van G vormt een deelgroep van $\text{Aut}(G)$, die we noteren als $\text{Inn}(G)$, en de *inwendige automorfismengroep van G* noemen.

Lemma 1.5.9. $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.

Bewijs. We tonen eerst aan dat wel degelijk $\text{Inn}(G) \leq \text{Aut}(G)$. Zij $\iota_g, \iota_h \in \text{Inn}(G)$, en beschouw $\theta = \iota_g \iota_h^{-1}$. Dan is, voor elke $x \in G$,

$$x^\theta = (g^{-1}xg)^{\iota_h^{-1}} = hg^{-1}xgh^{-1} = x^{\iota_{gh^{-1}}},$$

en bijgevolg is $\theta = \iota_{gh^{-1}} \in \text{Inn}(G)$.

We tonen vervolgens aan dat $\text{Inn}(G)$ invariant is onder toevoeging met elementen van $\text{Aut}(G)$. Zij dus $\iota_g \in \text{Inn}(G)$ en $\theta \in \text{Aut}(G)$ willekeurig; we moeten aantonen dat $\iota_g^\theta = \theta^{-1} \iota_g \theta \in \text{Inn}(G)$. We beweren dat $\iota_g^\theta = \iota_{g^\theta}$. Inderdaad, voor elke $x \in G$ hebben we

$$x^{\iota_g^\theta} = x^{\theta^{-1} \iota_g \theta} = (g^{-1} x^{\theta^{-1}} g)^\theta = (g^\theta)^{-1} x g^\theta = x^{\iota_{g^\theta}},$$

en dus is inderdaad $\iota_g^\theta = \iota_{g^\theta} \in \text{Inn}(G)$. □

Het volgende lemma is eenvoudig maar bewijst geregeld zijn nut.

Lemma 1.5.10. *Zij G een groep, en H een deelgroep van index 2. Dan is $H \trianglelefteq G$.*

Bewijs. Neem $g \in G \setminus H$ willekeurig. De linkse nevenklassen van H in G vormen een partitie, en dus is G de disjuncte unie van H en gH . Analoog is G de disjuncte unie van H en Hg . Hieruit volgt $gH = Hg$, en dus is elke rechtse nevenklasse van H ook een linkse nevenklasse van H ; bijgevolg is $H \trianglelefteq G$. □

Definitie 1.5.11. Als G een niet-triviale groep is zonder echte niet-triviale normaaldelers (d.w.z. de enige normaaldelers van G zijn $1 \trianglelefteq G$ en $G \trianglelefteq G$), dan noemen we G een *enkelvoudige groep*. Deze groepen spelen een zeer

belangrijke rol in de groepentheorie; ze vormen als het ware de bouwstenen voor willekeurige groepen⁴. In de cursus “Algebra II” wordt hier dieper op ingegaan.

Op dit moment hebben we nog maar twee klassen van enkelvoudige groepen ontmoet.

Voorbeeld 1.5.12. (1) Zij p een willekeurig priemgetal. Dan is de cyclische groep C_p een enkelvoudige groep. (Inderdaad, uit de stelling van Lagrange volgt dat een dergelijke groep geen echte deelgroepen bezit.) Zoals we zo dadelijk zullen zien in Stelling 1.5.13 zijn dit de enige *abelse* enkelvoudige groepen.

(2) Zij $n \geq 5$. Dan is de alternerende groep A_n een enkelvoudige groep. Het vraagt wel wat werk om dit te bewijzen, en we stellen dit uit tot de cursus “Algebra II”.

(3) De alternerende groep A_4 is *niet* enkelvoudig. Ga zelf na dat $N = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ een normaaldeler is van A_4 .

We hebben intussen wel al voldoende informatie vergaard om de abelse enkelvoudige groepen volledig te classificeren.

Stelling 1.5.13. *Zij G een abelse enkelvoudige groep. Dan bestaat er een priemgetal p zodat $G \cong C_p$.*

Bewijs. Uit Lemma 1.5.7(i) weten we dat elke deelgroep een normaaldeler is, en bijgevolg is G een groep zonder echte deelgroepen. Kies een $g \in G$ met $g \neq 1$ willekeurig. Dan is $\langle g \rangle \leq G$, en bijgevolg moet $\langle g \rangle = G$, en dus is G cyclisch. Als G oneindig is, dan heeft G wel echte deelgroepen; bijgevolg is G eindig, en dus $G \cong C_n$ voor een zekere $n \in \mathbb{N}^*$. Zij p een priemdelers van n ; dan geldt wegens Stelling 1.4.3(iv) dat G een deelgroep heeft van orde p . Dit kan enkel als reeds $|G| = p$ en dus $G \cong C_p$. $\square$

Tot slot van deze sectie voeren we nog een begrip in dat nauw verwant is met normaaldelers, maar nog restrictiever is.

Definitie 1.5.14. Zij G een groep en $H \leq G$. We noemen H een *karacteristieke deelgroep* van G , als H invariant is onder elk automorfisme van G , dit wil zeggen, als voor elke $\theta \in \text{Aut}(G)$ geldt dat $H^\theta = H$. We noteren dit als $H \text{ char } G$ of als $H \trianglelefteq_{\text{char}} G$.

⁴Dit geldt in zeer sterke mate voor eindige groepen, maar ook in de theorie van de oneindige groepen spelen enkelvoudige groepen een belangrijke rol.

Aangezien elk inwendig automorfisme ook een automorfisme is, is elke karakteristieke deelgroep ook een normaaldeler. Het omgekeerde geldt niet.

We kennen reeds een belangrijke karakteristieke deelgroep:

Lemma 1.5.15. *Zij G een willekeurige groep. Dan is $Z(G) \trianglelefteq_{\text{char}} G$, waarbij $Z(G)$ het centrum van de groep G is zoals ingevoerd in Definitie 1.2.25(vi).*

Bewijs. We weten reeds dat $Z(G) \leq G$. Zij nu $z \in Z(G)$ en $\theta \in \text{Aut}(G)$. Dan geldt voor een willekeurige $g \in G$ dat

$$z^\theta g = (zg^{\theta^{-1}})^\theta = (g^{\theta^{-1}}z)^\theta = gz^\theta,$$

en dus is $z^\theta \in Z(G)$. □

Oefeningen

38. Zij G een groep. Toon aan dat $\text{Inn}(G) = 1$ als en slechts als G abels is.
39. Zij G een groep. Toon aan dat de afbeelding $\iota: G \rightarrow \text{Inn}(G): g \mapsto \iota_g$ een epimorfisme is, met $\ker(\iota) = Z(G)$.
40. Zij G een groep en $H_1, H_2 \trianglelefteq_{\text{char}} G$. Toon aan dat $H_1 \cap H_2 \trianglelefteq_{\text{char}} G$.
41. Zij G een groep. Toon aan dat $[G, G] \trianglelefteq_{\text{char}} G$.
42. Zij G een groep, en $K \trianglelefteq_{\text{char}} N \trianglelefteq G$. Toon aan dat $K \trianglelefteq G$. Bewijs ook dat indien bovendien $N \trianglelefteq_{\text{char}} G$, dan ook $K \trianglelefteq_{\text{char}} G$.
Toon anderzijds aan, door middel van een tegenvoorbeeld, dat uit $K \trianglelefteq N \trianglelefteq G$ *niet* noodzakelijk volgt dat $K \trianglelefteq G$.
43. Zij G een groep, $H \leq G$, en $g \in G$. Toon aan dat ook $H^g \leq G$, en dat bovendien $H^g \cong H$.
44. Zij G een groep, en $A, B \leq G$ twee abelse deelgroepen. Veronderstel bovendien dat $G = \langle A \cup B \rangle$. Bewijs dat $A \cap B \trianglelefteq G$.
45. Zij G een groep, en $N \trianglelefteq G$ met $|N| = 2$. Toon aan dat $N \leq Z(G)$.
46. Zij G een groep met $|G| \neq 4$, en $H \leq G$ met $[G : H] = 2$. Onderstel dat H enkelvoudig is. Toon aan dat H de enige deelgroep is van G van index 2, en leid daaruit af dat $H \trianglelefteq_{\text{char}} G$. Wat als $|G| = 4$?

1.6 Quotiëntgroepen

Het begrip van een quotiëntgroep, dat we al ingevoerd hebben in de cursus “Discrete Wiskunde II”, is uitermate belangrijk, voornamelijk omwille van het sterke verband met groepsomorfismen (zie Stelling 1.6.7 en Gevolg 1.6.10 verderop). We herhalen de definitie.

Definitie 1.6.1. Zij G een groep, en $H \leq G$ een deelgroep. We definiëren de *quotiëntverzameling* of *quotiëntruimte* G/H als

$$G/H := R_G(H) = \{Hx \mid x \in G\}.$$

In het algemeen is dit een verzameling zonder bijkomende structuur, maar als H een normaaldeler is, kunnen we een groepsoperatie $*$ definiëren op G/H door

$$Hx * Hy := H(xy)$$

te stellen voor alle $x, y \in G$, met neutraal element H (de *triviale nevenklasse*). We noemen de verzameling G/H met deze groepswet de *quotiëntgroep van G met betrekking tot H* ; in de spreektaal gebruiken we kortweg de bewoording *het quotiënt van G met H , G over H , G modulo H , of G uitgedeeld naar H* .

We gaan eerst na dat de groepsoperatie $*$ goed gedefinieerd is, m.a.w. onafhankelijk is van de keuze van de representanten x en y van de twee nevenklassen Hx en Hy .

Lemma 1.6.2. *Zij G een groep en $H \trianglelefteq G$. Veronderstel dat $Hx = Hx'$ en $Hy = Hy'$. Dan is $H(xy) = H(x'y')$.*

Bewijs. Aangezien $H \trianglelefteq G$, is $gH = Hg$ voor alle $g \in G$. We hebben dus

$$\begin{aligned} H(xy) &= (Hx)y = (Hx')y = (x'H)y = x'(Hy) \\ &= x'(Hy') = (x'H)y' = (Hx')y' = H(x'y'). \quad \square \end{aligned}$$

Opmerking 1.6.3. Als H geen normaaldeler is, dan zal de operatie $*$ niet goed gedefinieerd zijn. Inderdaad, in dat geval bestaan er een $g \in G$ en een $h \in H$ zodat $g^{-1}hg \notin H$. Beschouw dan de nevenklassen Hg^{-1} en Hg , en merk op dat $Hg = H(hg)$. Dan is $H(g^{-1} \cdot g) = H$, terwijl $H(g^{-1} \cdot hg) \neq H$. De “definitie” $Hx * Hy = H(xy)$ hangt in dat geval dus af van de keuze van de representanten, en is dus geen goede definitie.

Opmerking 1.6.4. Als H een normaaldeler is, dan is de bewerking $*$ compatibel met Notatie 1.2.11 in de zin dat $(Hx) * (Hy) = Hx \cdot Hy$, waarbij Hx en Hy als deelverzamelingen van G opgevat worden; om die reden zullen we in het vervolg het symbool $*$ niet meer schrijven.

Met elke quotiëntgroep kan men op natuurlijke wijze een epimorfisme associëren, dat we de *canonieke surjectie* of (*canonieke*) *projectie* noemen.

Lemma 1.6.5. *Zij G een willekeurige groep, en $N \trianglelefteq G$. Dan is de afbeelding*

$$\pi: G \rightarrow G/N: g \mapsto Ng$$

een epimorfisme, met kern gelijk aan N .

Bewijs. Uit Definitie 1.6.1 en Lemma 1.6.2 volgt onmiddellijk dat π een morfisme is. Het is evident dat π surjectief is. De kern $\ker(\pi)$ bestaat precies uit de elementen $g \in G$ waarvoor Ng het neutraal element van G/N is, m.a.w. waarvoor $Ng = N$. Hieruit volgt $\ker(\pi) = N$. $\square$

We gaan nu even in op de structuur van deelgroepen en normaaldelers van quotiëntgroepen. De volgende stelling is een eenvoudig geval van de zogenaamde correspondentiestelling (zie “Algebra II”).

Stelling 1.6.6. *Zij G een groep, $N \trianglelefteq G$ een normaaldeler van G , en zij $H = G/N$ de corresponderende quotiëntgroep.*

- (i) *Zij $K \leq H$. Dan is er een unieke $A \leq G$ die N bevat, zodat $K = A/N$.*
- (ii) *Zij $K \trianglelefteq H$. Dan is er een unieke $A \trianglelefteq G$ die N bevat, zodat $K = A/N$.*

In beide gevallen is $A = K^{\pi^{-1}}$, waarbij $\pi: G \rightarrow H$ de canonieke projectie is.

Bewijs. (i) Zij A een willekeurige deelgroep van G die N bevat. Dan is $N \trianglelefteq A$, en A is een unie van nevenklassen van N in G . Maar dan is A/N precies gelijk aan de verzameling van die nevenklassen. Er kan dus in elk geval ten hoogste één dergelijke A bestaan.

We tonen nu aan dat $A = K^{\pi^{-1}}$ voldoet. Inderdaad, deze A bevat uiteraard $\ker(\pi) = N$, en $A/N = A^\pi = (K^{\pi^{-1}})^\pi = K$, waarbij de allerlaatste gelijkheid geldt omdat π surjectief is.

- (ii) Wegens (i) volstaat het om na te gaan dat indien $K \trianglelefteq H$, dan ook $A = K^{\pi^{-1}} \trianglelefteq G$. Stel dus $a \in A$ en $g \in G$ willekeurig; dan is $a^\pi \in K$, en dus $(a^g)^\pi = (a^\pi)^{(g^\pi)} \in K^{(g^\pi)} = K$, zodat ook $a^g \in A$. Via het criterium van normaaldelers toont dit aan dat $A \trianglelefteq G$. $\square$

Om de structuur van quotiëntgroepen goed te begrijpen, is de volgende *isomorfiestelling* (en het bijhorend Gevolg 1.6.10) onmisbaar.

Stelling 1.6.7 (Eerste isomorfiestelling). *Zij $\theta: G \rightarrow H$ een groepsmorphisme. Dan is*

$$\text{im}(\theta) \cong G / \ker(\theta).$$

Bewijs. Stel $K = \ker(\theta)$, en beschouw de afbeelding

$$\Theta: G/K \rightarrow \text{im}(\theta): Kg \mapsto g^\theta.$$

De afbeelding Θ is goed gedefinieerd, want als $Kg = Kh$ voor zekere $g, h \in G$, dan is $h = kg$ voor een zekere $k \in K$, maar dan is

$$h^\theta = (kg)^\theta = k^\theta g^\theta = g^\theta.$$

We tonen vervolgens aan dat Θ een morfisme is. Inderdaad, zij $Kg, Kh \in G/K$ willekeurig; dan is

$$\Theta(Kg \cdot Kh) = \Theta(K(gh)) = (gh)^\theta = g^\theta h^\theta = \Theta(Kg)\Theta(Kh).$$

Het is evident dat Θ surjectief is. We tonen ten slotte aan dat Θ injectief is, door te bewijzen dat $\ker(\Theta) = 1$. Beschouw dus $Kg \in G/K$ met $\Theta(Kg) = 1$; dan is $g^\theta = 1$, en dus is $g \in K$. Dit impliceert dat $Kg = K$, hetgeen aantoont dat $\ker(\Theta) = 1$. We hebben bewezen dat Θ een isomorfisme is. $\square$

Opmerking 1.6.8. Als $\theta: G \rightarrow H$ een monomorfisme is, dan zegt de eerste isomorfiestelling dat $G \cong \text{im}(\theta)$, in overeenstemming met wat we al wisten (zie Opmerking 1.3.5).

Opmerking 1.6.9. We kunnen de eerste isomorfiestelling ook interpreteren als de uitspraak dat elk morfisme $\theta: G \rightarrow H$ een decompositie heeft in een projectie (= canonieke surjectie), een isomorfisme, en een inclusie (= canonieke injectie):

$$G \twoheadrightarrow G/\ker(\theta) \xrightarrow{\sim} \text{im}(\theta) \hookrightarrow H.$$

Een belangrijk gevolg van de eerste isomorfiestelling is het feit dat normaaldelers precies kernen van morfismen zijn, terwijl quotiëntgroepen precies homomorfe beelden zijn:

Gevolg 1.6.10. *Zij G een willekeurige groep. Dan geldt:*

$$\begin{aligned} N \trianglelefteq G &\iff \left[\begin{array}{l} N \text{ is de kern van een morfisme} \\ \text{vertrekkend uit } G \end{array} \right. \\ H \text{ is een quotiënt van } G &\iff \left[\begin{array}{l} H \text{ is het beeld van een morfisme} \\ \text{vertrekkend uit } G \end{array} \right. \end{aligned}$$

Bewijs. Veronderstel eerst dat $\theta: G \rightarrow H$ een morfisme is. Dan is $\ker(\theta)$ inderdaad een normaaldeeler van G , en uit de eerste isomorfiestelling volgt dat $\text{im}(\theta)$ een quotiëntgroep is van G .

Omgekeerd, als N een normaaldeeler is van G , dan is N precies de kern van de projectie-afbeelding $\pi: G \rightarrow G/N$; en als H een quotiënt is van G , dan bestaat er een normaaldeeler $N \trianglelefteq G$ zodat $H = G/N$; de projectie-afbeelding $\pi: G \rightarrow G/N$ heeft precies H als beeld. $\square$

Een ander interessant gevolg van de eerste isomorfiestelling is de volgende observatie.

Gevolg 1.6.11. *Zij G en H eindige groepen, en $\theta: G \rightarrow H$ een willekeurig morfisme. Dan geldt:*

- (i) $|\ker(\theta)|$ is een deler van $|G|$;
- (ii) $|\operatorname{im}(\theta)|$ is een deler van zowel $|G|$ als $|H|$;
- (iii) als $\gcd(|G|, |H|) = 1$, dan is θ triviaal, i.e. $g^\theta = 1$ voor alle $g \in G$;
- (iv) voor elke $g \in G$ is $o(g^\theta)$ een deler van zowel $o(g)$ als $|H|$;
- (v) als $g \in G$ met $\gcd(o(g), |H|) = 1$, dan is $g^\theta = 1$.

Bewijs. Bewijs dit zelf als oefening. Denk hierbij voor (iv) en (v) aan de restrictie $\theta|_{\langle g \rangle}$. $\square$

We tonen nu een gevolg van de eerste isomorfiestelling aan, dat bekend staat onder de naam “tweede isomorfiestelling”. Eerst geven we een andere eigenschap aan, die ondermeer zegt dat we een deelgroep en een normaaldeeler van een zelfde groep G “aan elkaar kunnen plakken” om er een grotere deelgroep van G van te maken.

Lemma 1.6.12. *Zij G een willekeurige groep, en zij $H \leq G$ en $N \trianglelefteq G$. Dan is $HN = NH$, en $HN \leq G$. Ook is $H \cap N \trianglelefteq H$. Als bovendien $H \trianglelefteq G$, dan is $HN \trianglelefteq G$.*

Bewijs. Aangezien $N \trianglelefteq G$, is $hN = Nh$ voor alle $h \in H$. Bijgevolg is

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH.$$

We tonen vervolgens aan met het criterium van deelgroepen dat $HN \leq G$. Zij dus $g_1, g_2 \in HN$ willekeurig; dan is $g_1 = h_1n_1$ en $g_2 = h_2n_2$ voor zekere $h_1, h_2 \in H$ en $n_1, n_2 \in N$. Hieruit volgt

$$g_1g_2^{-1} = h_1n_1n_2^{-1}h_2^{-1} \in h_1Nh_2^{-1},$$

en gebruik makend van het feit dat $Nh_2^{-1} = h_2^{-1}N$ vinden we $g_1g_2^{-1} \in h_1h_2^{-1}N \subseteq HN$.

We tonen vervolgens aan dat $H \cap N \trianglelefteq H$. Uiteraard is $H \cap N \leq H$; we tonen nu aan dat $H \cap N$ invariant is onder toevoeging met elementen van H . Neem dus $h \in H$ willekeurig. Dan is $H^h = H$, en $N^h = N$ omdat N een normaaldeeler is van G . Hieruit volgt dat $(H \cap N)^h = H^h \cap N^h = H \cap N$.

Ten slotte nemen we aan dat $H \trianglelefteq G$, en tonen we aan dat dan ook $HN \trianglelefteq G$. We weten reeds dat $HN \leq G$, dus we gebruiken het criterium voor normaaldelers. Zij dus $hn \in HN$ en $g \in G$ willekeurig; dan is $(hn)^g = h^g n^g \in H^g N^g = HN$. Dit bewijst dat inderdaad $HN \trianglelefteq G$. $\square$

Opmerking 1.6.13. Merk op dat HN precies gelijk is aan $(H^\pi)^{\pi^{-1}}$, waarbij π de canonieke projectie is van G naar G/N . Dit geeft een alternatief bewijs voor de uitspraak dat $HN \leq G$.

Opmerking 1.6.14. Als $A \leq G$ en $B \leq G$, dan geldt in het algemeen *niet* dat AB een deelgroep is van G . We hebben met name dat $AB \leq G$ als en slechts als $AB = BA$ (toon dit zelf aan!), en deze voorwaarde is niet steeds voldaan; zie Oefening 49.

Stelling 1.6.15 (Tweede isomorfiestelling). *Zij G een willekeurige groep, en zij $H \leq G$ en $N \trianglelefteq G$. Dan is*

$$HN/N \cong H/(H \cap N).$$

Bewijs. Beschouw de afbeelding

$$\psi: H \rightarrow G/N: h \mapsto hN.$$

Dit is een morfisme omdat $N \trianglelefteq G$. Duidelijkerwijze bestaat $\text{im}(\psi)$ precies uit de nevenklassen van N (in G) die bevat zijn in HN , dus $\text{im}(\psi) = HN/N$. Het is evenzeer duidelijk dat $\ker(\psi)$ precies bestaat uit de elementen $h \in H$ waarvoor $hN = N$, of dus $h \in N$; bijgevolg is $\ker(\psi) = H \cap N$. Uit de eerste isomorfiestelling volgt nu het gestelde. $\square$

In het geval dat H en N eindig zijn, kunnen we uit de tweede isomorfiestelling afleiden dat $|HN| = |H| |N| / |H \cap N|$. Dit geldt echter ook voor twee willekeurige deelgroepen (waarvan dus niet noodzakelijk één van beide een normaaldeler is). Merk echter op dat $H_1 H_2$ niet noodzakelijk een groep is (zie Opmerking 1.6.14).

Stelling 1.6.16. *Zij G een willekeurige groep, en H_1, H_2 twee eindige deelgroepen van G . Dan is*

$$|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}.$$

Bewijs. Beschouw de verzameling

$$H_1 \times H_2 := \{(h_1, h_2) \mid h_1 \in H_1, h_2 \in H_2\}.$$

(We zullen zo dadelijk zien dat deze verzameling ook een natuurlijke groepsstructuur heeft, maar dit is voor dit bewijs niet relevant.) Merk op dat $|H_1 \times H_2| = |H_1| \cdot |H_2|$. Beschouw nu de afbeelding

$$\varphi: H_1 \times H_2 \rightarrow H_1 H_2: (h_1, h_2) \mapsto h_1 h_2.$$

Per definitie van H_1H_2 geldt dat φ surjectief is. We tonen nu aan dat elk element precies $|H_1 \cap H_2|$ keer bereikt wordt; hieruit volgt dan de formule.

Zij dus $x = h_1h_2 \in H_1H_2$ willekeurig. Voor elke $h \in H_1 \cap H_2$ geldt dat $(h_1h^{-1}) \cdot (hh_2) = x$, en dit levert ons dus alvast $|H_1 \cap H_2|$ verschillende koppels in $H_1 \times H_2$ die door φ worden afgebeeld op x . Omgekeerd, als $\varphi(h_3, h_4) = x$, dan is $h_1h_2 = h_3h_4$ en dus $h_3^{-1}h_1 = h_4h_2^{-1}$. Noem dit laatste element h ; dan is $h \in H_1 \cap H_2$. Maar dan is $h_3 = h_1h^{-1}$ en $h_4 = hh_2$, en dus heeft (h_3, h_4) inderdaad de gekende gedaante. $\square$

Oefeningen

47. Bewijs dat elke quotiëntgroep van een abelse groep abels is.
48. Bepaal alle deelgroepen, normaaldelers en quotiëntgroepen van $\mathbf{C}_8$ en van $\mathbf{D}_8$.
49. Beschouw de groep $G = \mathbf{D}_6$. Beschrijf deelgroepen $A \leq G$ en $B \leq G$ met $|A| = 2$ en $|B| = 2$, en toon aan dat $AB \neq BA$.
50. Zij G een groep met normaaldeler $N \trianglelefteq G$, en zij π de projectie $G \rightarrow G/N$. Zij H een tweede groep, en zij $\theta: G \rightarrow H$ een morfisme. Toon aan dat er een morfisme $\psi: G/N \rightarrow H$ bestaat zodat $\theta = \pi\psi$, als en slechts als $N \leq \ker(\theta)$.
51. Zij G een groep met $N_1, N_2 \trianglelefteq G$ en $N \trianglelefteq N_1, N_2$. Bewijs dat $(N_1/N)(N_2/N) = (N_1N_2)/N$.
52. Bewijs dat elke quotiëntgroep van een perfecte groep perfect is.
53. Toon aan dat $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \cong (K^\times, \cdot)$.
54. Beschouw de matrixgroepen

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in \mathbb{R}, a > 0 \right\}, \quad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}.$$

Toon aan dat $N \trianglelefteq G$, en dat $G/N \cong (\mathbb{R}_{>0}, \cdot)$.

55. Zij $S = \{q \in \mathbb{Q} \mid 0 \leq q < 1\}$, en beschouw de bewerking

$$p \bullet q := \begin{cases} p + q & \text{als } 0 \leq p + q < 1, \\ p + q - 1 & \text{als } p + q \geq 1, \end{cases}$$

voor alle $p, q \in S$. Toon aan dat $(S, \bullet)$ een abelse groep is. Toon vervolgens aan dat $(S, \bullet) \cong \mathbb{Q}/\mathbb{Z}$.

56. Zij G een groep zodat $G/Z(G)$ cyclisch is. Bewijs dat G abels is.

1.7 Directe producten

We voeren nu een eenvoudige maar belangrijke constructie in om vanuit een aantal groepen een nieuwe groep te construeren.

Definitie 1.7.1. Zij $G_1, \dots, G_n$ willekeurige groepen. Dan definiëren we een nieuwe groep $G = G_1 \times \dots \times G_n$, die we het *direct product* of het *cartesisch product* van de groepen $G_1, \dots, G_n$ noemen, als volgt:

$$G = \{(g_1, \dots, g_n) \mid g_i \in G_i \text{ voor elke } i\},$$

met de componentsgewijze groepsbewerking, i.e.

$$(g_1, \dots, g_n) \cdot (g'_1, \dots, g'_n) = (g_1 g'_1, \dots, g_n g'_n),$$

voor alle $g_i, g'_i \in G_i$. Het is eenvoudig om in te zien dat G met deze samenstellingswet opnieuw een groep is, met neutraal element $(1_{G_1}, \dots, 1_{G_n})$.

Definitie 1.7.2. Zij p een priemgetal en $n \geq 1$. De groep

$$\mathbf{E}_{p^n} := \mathbf{C}_p \times \mathbf{C}_p \times \dots \times \mathbf{C}_p \text{ (} n \text{ factoren)}$$

noemen we de *elementair abelse groep* van orde p^n . Wanneer we n niet nader specificeren (maar p wel), dan spreken we van een *elementair abelse p -groep*. Merk op dat elk niet-triviaal element van $\mathbf{E}_{p^n}$ orde p heeft, m.a.w., $\exp(\mathbf{E}_{p^n}) = p$. Zie ook Oefening 63.

Het direct product wordt gekenmerkt door de aanwezigheid van normaaldelers die triviaal snijden.

Lemma 1.7.3. Zij $G_1, \dots, G_n$ willekeurige groepen, en $G = G_1 \times \dots \times G_n$. Stel, voor elke i , $H_i := 1 \times \dots \times G_i \times \dots \times 1 \leq G$. Dan is $G_i \cong H_i \trianglelefteq G$ voor elke i , en $H_i \cap H_j = 1$ voor alle $i \neq j$. Bovendien commuteren H_i en H_j voor alle $i \neq j$.

Bewijs. Het is evident dat $G_i \cong H_i$ en dat $H_i \cap H_j = 1$ voor $i \neq j$. Zij nu $g = (g_1, \dots, g_n) \in G$ en $h = (1, \dots, h_i, \dots, 1) \in H_i$ willekeurig; dan is

$$\begin{aligned} g^{-1} h g &= (g_1^{-1} 1 g_1, \dots, g_i^{-1} h_i g_i, \dots, g_n^{-1} 1 g_n) \\ &= (1, \dots, g_i^{-1} h_i g_i, \dots, 1) \in H_i, \end{aligned}$$

en dus $H_i \trianglelefteq G$. Zij ten slotte $i \neq j$, en neem $a = (1, \dots, h_i, \dots, 1) \in H_i$ en $b = (1, \dots, h_j, \dots, 1) \in H_j$ willekeurig. Dan is

$$ab = (1, \dots, h_i, \dots, h_j, \dots, 1) = ba,$$

en dus commuteren H_i en H_j met elkaar. □

Interessant is dat dit soort van eigenschappen ook volstaat om directe producten te herkennen binnen een gegeven groep G . We beginnen met een lemma dat ook in andere situaties nuttig kan zijn.

Lemma 1.7.4. *Zij G een groep, en zij A en B normaaldelers van G met $A \cap B = 1$. Dan commuteren A en B met elkaar, i.e. $[A, B] = 1$.*

Bewijs. Zij $a \in A$ en $b \in B$ willekeurig, en beschouw hun commutator $g = [a, b] = a^{-1}b^{-1}ab$. Omdat $A \trianglelefteq G$ is $g = a^{-1} \cdot a^b \in A$, en omdat $B \trianglelefteq G$ is $g = (b^{-1})^a \cdot b \in B$; bijgevolg is $g \in A \cap B = 1$, dus $ab = ba$. $\square$

Stelling 1.7.5. *Zij G een willekeurige groep, en veronderstel dat $G_1, \dots, G_n$ normaaldelers zijn van G , met de eigenschap dat*

$$G_i \cap G_{i+1} \cdots G_n = 1 \quad \text{voor elke } i \in \{1, \dots, n-1\}.$$

Dan is $G_1 \cdots G_n \trianglelefteq G$, en $G_1 \cdots G_n \cong G_1 \times \cdots \times G_n$.

Bewijs. Voor elke i stellen we $H_i := G_i \cdots G_n$; het feit dat $H_i \trianglelefteq G$ volgt uit Lemma 1.6.12. Merk op dat de voorwaarden op de normaaldelers impliceren dat $G_i \cap G_j = 1$ voor elke $i \neq j$. Uit Lemma 1.7.4 volgt dus dat $[G_i, G_j] = 1$ voor alle $i \neq j$.

Beschouw nu de afbeelding

$$\theta: G_1 \times \cdots \times G_n \rightarrow H_1: (g_1, \dots, g_n) \mapsto g_1 \cdots g_n.$$

Uit het feit dat de deelgroepen G_i twee aan twee commuteren, volgt nu dat θ een morfisme is. De surjectiviteit is triviaal (per definitie van H_1). We tonen ten slotte de injectiviteit aan door uit het ongerijmde te bewijzen dat $\ker(\theta) = 1$. Stel dus dat $g_1 \cdots g_n = 1$ voor zekere $g_i \in G_i$, en zij k het kleinste natuurlijk getal zodat $g_k \neq 1$. Dan is

$$g_k^{-1} = g_{k+1} \cdots g_n \in H_{k+1},$$

en dus $g_k^{-1} \in G_k \cap H_{k+1} = 1$. Deze strijdigheid bewijst de injectiviteit. We besluiten dat θ een isomorfisme is. $\square$

We kunnen dit ook nog herformuleren als volgt.

Gevolg 1.7.6. *Zij G een willekeurige groep, en veronderstel dat $G_1, \dots, G_n$ normaaldelers zijn van G . Dan zijn de volgende uitspraken equivalent.*

- (a) *De afbeelding $\theta: G_1 \times \cdots \times G_n \rightarrow G: (g_1, \dots, g_n) \mapsto g_1 \cdots g_n$ is een isomorfisme;*

- (b) elke $g \in G$ is op unieke wijze te schrijven als $g = g_1 \cdots g_n$ met $g_i \in G_i$ voor elke i ;
- (c) elke $g \in G$ is te schrijven als $g = g_1 \cdots g_n$ met $g_i \in G_i$ voor elke i , en $G_i \cap (\prod_{j \neq i} G_j) = 1$ voor alle i .

(Merk op dat de notatie $\prod_{j \neq i} G_j$ in (c) hierboven ondubbelzinnig is, omdat elke G_j een normaaldeler is, waardoor $G_j G_k = G_k G_j$ voor alle j, k .)

Opmerking 1.7.7. (i) De bewering dat de afbeelding $\theta: G_1 \times \cdots \times G_n \rightarrow G: (g_1, \dots, g_n) \mapsto g_1 \cdots g_n$ een isomorfisme is, is sterker dan enkel uitdrukken dat $G \cong G_1 \times \cdots \times G_n$. Bijvoorbeeld, als $G = H_1 \times H_2$ met $H_1 \cong H_2$, dan is uiteraard $G \cong H_1 \times H_1$, terwijl de afbeelding $\theta: H_1 \times H_1 \rightarrow G: (h_1, h'_1) \mapsto h_1 h'_1$ niet surjectief is.

- (ii) Als de uitspraken van Gevolg 1.7.6 voldaan zijn, dan schrijven we dit ook wel als $G = G_1 \times \cdots \times G_n$ (met een gelijkheidsteken). We zeggen dan ook wel dat G het *inwendige direct product* is van de deelgroepen $G_1, \dots, G_n$. De constructie in Definitie 1.7.1 wordt dan het *uitwendige direct product* genoemd.

Als onmiddellijke toepassing op de voorgaande stelling tonen we aan dat elke cyclische groep kan ontbonden worden in cyclische groepen van priemmachtorde.

Stelling 1.7.8. Zij $G = \mathbf{C}_n$ een cyclische groep van orde n , en ontbind n in priemfactoren, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Dan is

$$\mathbf{C}_n \cong \mathbf{C}_{p_1^{\alpha_1}} \times \cdots \times \mathbf{C}_{p_k^{\alpha_k}}.$$

Bewijs. Uit Stelling 1.4.3 weten we dat er voor elke $i \in \{1, \dots, k\}$ precies één deelgroep $G_i \leq G$ bestaat van orde $p_i^{\alpha_i}$, en dat die opnieuw cyclisch is, m.a.w. $G_i \cong \mathbf{C}_{p_i^{\alpha_i}}$. Omdat G abels is, is elke G_i een normaaldeler.

Stel $H_i := G_i \cdots G_k \leq G$; dan is H_i een deelgroep, en wegens Stelling 1.6.16 is de orde van H_i een deler van $|G_i| \cdots |G_k|$. In elk geval is $\gcd(|G_i|, |H_{i+1}|) = 1$ voor elke i , en uit de stelling van Lagrange volgt dat $G_i \cap H_{i+1} = 1$ voor elke i . De voorwaarden van Stelling 1.7.5 zijn dus voldaan, en we besluiten dat

$$H_1 \cong G_1 \times \cdots \times G_k \cong \mathbf{C}_{p_1^{\alpha_1}} \times \cdots \times \mathbf{C}_{p_k^{\alpha_k}}. \quad (1.1)$$

Het resultaat volgt nu uit het feit dat $H_1 \leq G$, terwijl het rechterlid van (1.1) een groep is van orde $n = |G|$, zodat noodzakelijk $H_1 = G$. $\square$

Opmerking 1.7.9. We zullen later (zie Stelling 3.5.3 en Opmerking 3.5.4(i)) zien dat elke eindige abelse groep isomorf is met het direct product van cyclische groepen van priemmachtorde (waarbij hetzelfde priemgetal dan meerdere keren kan voorkomen).

Oefeningen

57. Zij G_1, G_2 groepen, en $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$. Toon aan dat $N_1 \times N_2 \trianglelefteq G_1 \times G_2$.
 58. Bewijs dat, als G_1 en G_2 abels zijn, dan ook $G_1 \times G_2$ abels is. Is het omgekeerde ook waar?
 59. Beschouw het direct product $G = G_1 \times G_2$ van twee groepen G_1, G_2 . Is de deelgroep $1 \times G_2$ een karakteristieke deelgroep van G ?
 60. Bewijs dat $\mathbf{D}_4 \cong \mathbf{C}_2 \times \mathbf{C}_2$. Bewijs dan algemener dat voor elke *oneven* n geldt dat $\mathbf{D}_{4n} \cong \mathbf{D}_{2n} \times \mathbf{C}_2$.
 61. Zij G een eindige groep met $|G|$ kwadraatvrij, i.e. $|G| = p_1 p_2 \cdots p_k$, waarbij $p_1, \dots, p_k$ twee aan twee verschillende priemgetallen zijn. Veronderstel dat G voor elke $i \in \{1, \dots, k\}$ een unieke deelgroep van orde p_i bezit. Bewijs dat G cyclisch is.
 62. Zij p een priemgetal. Toon aan dat de groepen $\mathbf{C}_{p^2}$ en $\mathbf{C}_p \times \mathbf{C}_p$ niet isomorf zijn.
 63. Zij p een priemgetal. Toon aan dat een eindige abelse groep waarin elk element orde 1 of p heeft, een elementair abelse p -groep is.
 64. Toon aan dat een eindige groep waarin elk element orde 1 of 2 heeft, steeds abels is, en bijgevolg een elementair abelse 2-groep is.
 65. Toon aan dat $\mathbf{E}_{p^n}$ isomorf is met de additieve groep is van de n -dimensionale vectorruimte $\mathbb{F}_p^n$ over het eindig veld $\mathbb{F}_p$. Is deze groep ook isomorf met de additieve groep van het veld $\mathbb{F}_{p^n}$?
 66. Zij G een groep en A, B twee deelgroepen van G . We zeggen dat G het *centraal product* is van A en B (notatie: $G = A \circ B$), als $G = AB$ en $[A, B] = 1$. Toon aan dat in dat geval A en B noodzakelijk normaaldelers zijn van G , en dat bovendien $A \cap B \leq Z(G)$.
-

1.8 Acties van groepen op verzamelingen

In de cursus “Discrete Wiskunde II” hebben we zeer veel aandacht besteed aan permutatiegroepen, en algemener aan acties van groepen op verzamelingen. We zullen later zien dat dit ook zeer zinvol is in de studie van abstracte groepen, waarbij a priori geen actie gegeven is.

Definitie 1.8.1. Zij G een groep en S een verzameling. Een afbeelding

$$\alpha: S \times G \rightarrow S,$$

die we zullen noteren met een exponentiële notatie als $s^g := \alpha(s, g)$, noemen we een *actie* van de groep G op de verzameling S , als voldaan is aan de volgende eigenschappen:

$$s^1 = s \quad \text{voor alle } s \in S; \tag{A}$$

$$(s^g)^h = s^{gh} \quad \text{voor alle } s \in S \text{ en alle } g, h \in G. \quad (\text{B})$$

We zeggen dan ook dat de groep G *werkt* op de verzameling S . Soms noemt men de verzameling S voorzien van een actie van de groep G een *G-verzameling*.

Voorbeelden 1.8.2. (1) De groep $\mathbf{S}_n$ werkt op de verzameling $\{1, \dots, n\}$.

Ook elke deelgroep $G \leq \mathbf{S}_n$ werkt op deze verzameling.

(2) Als $\Gamma = (V, E)$ een graaf is, dan werkt $\text{Aut}(\Gamma)$ zowel op de toppenverzameling V als op de bogenverzameling E .

(3) Zij K een veld, en $n \in \mathbb{N}^*$. Dan werkt de groep $\text{GL}(n, K)$ op de vectorruimte K^n van rijvectoren (door rechtse vermenigvuldiging).

Het volgend lemma is eenvoudig maar zeer nuttig. Vooral Lemma 1.8.3(ii) is het onthouden waard.

Lemma 1.8.3. *Zij G een groep die werkt op een verzameling S .*

(i) *Zij $s, t \in S$ en $g \in G$. Als $t = s^g$, dan is $s = t^{g^{-1}}$.*

$$\begin{array}{ccc} & g & \\ s & \xrightarrow{\quad} & t \\ & g^{-1} & \end{array}$$

(ii) *Zij $s, t \in S$ en $g, h \in G$. Als $s^g = t$, dan is $(s^h)^{(g^h)} = t^h$; hierbij is g^h de toegevoegde van g met h , terwijl s^h en t^h de actie is van h op s en t , respectievelijk.*

$$\begin{array}{ccc} s & \xrightarrow{g} & t \\ h \downarrow & & \downarrow h \\ s^h & \xrightarrow{g^h} & t^h \end{array}$$

(iii) *Als $H \leq G$, dan werkt ook H op de verzameling S .*

Bewijs. (i) Zij $s, t \in S$ en $g \in G$ met $t = s^g$. Uit (B) volgt dat $t^{g^{-1}} = (s^g)^{g^{-1}} = s^{gg^{-1}} = s^e$, en uit (A) volgt dan het gestelde.

(ii) Zij $s, t \in S$ en $g, h \in G$, met $s^g = t$. Dan is

$$(s^h)^{(g^h)} = (s^h)^{(h^{-1}gh)} = s^{hh^{-1}gh} = s^{gh} = (s^g)^h = t^h.$$

(iii) Men gaat onmiddellijk na dat de eigenschappen (A) en (B) voldaan zijn. $\square$

Met behulp van deze observaties kunnen we de volgende zeer belangrijke rekenregel voor toevoeging in $\mathbf{S}_n$ opstellen.

Gevolg 1.8.4. *Zij $G = \mathbf{S}_n$, en beschouw een willekeurig element $g \in G$, stel*

$$g = (a_1 \ a_2 \ \dots \ a_k)(b_1 \ b_2 \ \dots \ b_\ell) \cdots (z_1 \ z_2 \ \dots \ z_m).$$

Zij $h \in G$ willekeurig; dan is

$$g^h = (a_1^h \ a_2^h \ \dots \ a_k^h)(b_1^h \ b_2^h \ \dots \ b_\ell^h) \cdots (z_1^h \ z_2^h \ \dots \ z_m^h).$$

In het bijzonder hebben alle elementen van de toevoegingsklasse g^G dezelfde cykelstructuur. Sterker nog, de toevoegingsklasse g^G bestaat precies uit alle elementen van G die dezelfde cykelstructuur als g hebben.

Bewijs. De eerste uitspraak volgt onmiddellijk uit Lemma 1.8.3(ii). We bewijzen nu dat twee elementen g, g' met dezelfde cykelstructuur ook steeds toegevoegd zijn aan elkaar. Stel dus

$$\begin{aligned} g &= (a_1 \ a_2 \ \dots \ a_k)(b_1 \ b_2 \ \dots \ b_\ell) \cdots (z_1 \ z_2 \ \dots \ z_m), \\ g' &= (a'_1 \ a'_2 \ \dots \ a'_k)(b'_1 \ b'_2 \ \dots \ b'_\ell) \cdots (z'_1 \ z'_2 \ \dots \ z'_m). \end{aligned}$$

Stel dan h gelijk aan de permutatie die elke x_i afbeeldt op x'_i ; dan is, opnieuw omwille van Lemma 1.8.3(ii), inderdaad $g^h = g'$. $\square$

Zoals we reeds weten vanuit de cursus “Discrete Wiskunde II” kunnen we aan elke actie van G op S een morfisme $G \rightarrow \text{Sym}(S)$ koppelen.

Lemma 1.8.5. (i) *Voor elke vaste $g \in G$ is de afbeelding*

$$\alpha_g: S \rightarrow S: s \mapsto s^g$$

een permutatie van S .

(ii) *De afbeelding*

$$\varphi: G \rightarrow \text{Sym}(S): g \mapsto \alpha_g$$

is een morfisme.

Bewijs. Dit hebben we bewezen in de cursus “Discrete Wiskunde II”. $\square$

Definitie 1.8.6. Beschouw een actie van een groep G op een verzameling S . Het morfisme φ gedefinieerd in Lemma 1.8.5(ii) noemen we de *permutatierepresentatie* of de *permutatievoorstelling* geassocieerd met de actie.

Anders gezegd, een permutatierepresentatie van een groep G is een morfisme van G naar $\text{Sym}(S)$ voor een zekere verzameling S .

Gevolg 1.8.7. *Zij G een groep en S een verzameling. Dan is er een bijjectief verband tussen de acties van G op S enerzijds, en de morfismen van G naar $\text{Sym}(S)$ anderzijds.*

Bewijs. Uit Lemma 1.8.5(ii) weten we reeds dat er voor elke actie van G op S een corresponderend morfisme van G naar $\text{Sym}(S)$ is. Omgekeerd, zij $\varphi: G \rightarrow \text{Sym}(S)$ een morfisme. Dan definieert $s^g := s^{\varphi(g)}$ duidelijkerwijze een actie van G op S . Deze twee correspondenties zijn elkaars invers, zodat we inderdaad een bijjectief verband hebben. $\square$

Opmerking 1.8.8. Precies omwille van dit verband tussen acties en permutatierepresentaties wordt de terminologie vaak ook verwisseld gebruikt, en spreekt men soms van “de actie gegeven door $\varphi: G \rightarrow \text{Sym}(S)$ ” of van “de permutatievoorstelling (G, S) ”.

In de cursus “Discrete Wiskunde II” hebben we gezien dat de actie (G, S) aanleiding geeft tot een permutatiegroep precies als de actie getrouw is. We herhalen dit begrip.

Definitie 1.8.9. Beschouw een actie van een groep G op een verzameling S . Als geen enkel niet-triviaal element van G triviaal werkt op S (d.w.z. alle elementen van S fixeert), dan noemen we de actie *getrouw*. (In sommige contexten spreekt men ook van een *effectieve* actie.)

Getrouw zijn is een zeer natuurlijk begrip: het zegt in feite dat men elk element $g \in G$ kan herkennen aan zijn actie op de verzameling S :

Lemma 1.8.10. *Zij G een groep die werkt op een verzameling S . De volgende uitspraken zijn equivalent.*

- (a) *De actie is getrouw.*
- (b) *Voor alle $g \in G$ geldt: als voor alle $s \in S$ geldt $s^g = s$, dan is $g = 1$.*
- (c) *Voor alle $g, h \in G$ geldt: als voor alle $s \in S$ geldt $s^g = s^h$, dan is $g = h$.*
- (d) *De permutatierepresentatie geassocieerd met de actie is een monomorfisme (i.e. ze is injectief).*

Bewijs. Uitspraak (b) is precies de definitie van getrouw zijn, dus (a) en (b) zijn equivalent. Trivialerwijze impliceert (c) ook (b) (namelijk via de keuze $h = 1$). Veronderstel nu dat (b) geldt, en stel dat $g, h \in G$ zodanig zijn dat $s^g = s^h$ voor alle $s \in S$. Dan is $s^{gh^{-1}} = s$ voor alle $s \in S$, en uit (b) volgt dan dat $gh^{-1} = 1$. Hieruit volgt $g = h$, en dit bewijst (c). Dus uit (b) volgt (c).

Ten slotte tonen we aan dat (b) en (d) equivalent zijn. Zij φ de permutatierepresentatie geïnduceerd door de actie; merk op dat φ injectief is als en slechts als $\ker(\varphi) = 1$. Uit de definitie van φ volgt ook nog dat dit equivalent is met de uitspraak “als $\alpha_g = 1$, dan is ook $g = 1$ ”. Maar per definitie is $\alpha_g = 1$ als en slechts als $s^g = s$ voor alle $s \in S$. We verkrijgen dus precies uitspraak (b). $\square$

Opmerking 1.8.11. Een vaak gemaakte beginnersfout is om, voor een getrouwe actie van G op S , uit een gelijkheid $s^g = s^h$ voor zekere $s \in S$ te concluderen dat $g = h$. Vergelijk dit met uitspraak (c) hierboven.

Definitie 1.8.12. Zij G een groep die werkt op een verzameling S . De *kern* van de actie definiëren we als de kern $\ker(\varphi)$ van de geassocieerde permutatierepresentatie $\varphi: G \rightarrow \text{Sym}(S)$. In het bijzonder zien we dat de kern van een actie steeds een normaaldeeler is van G , en dat de kern triviaal is als en slechts als de actie getrouw is.

Als een actie niet getrouw is, kunnen we er op natuurlijke wijze een getrouwe actie mee associëren door de kern “uit te delen”:

Lemma 1.8.13. *Beschouw een actie van een groep G op een verzameling S , en zij $N \trianglelefteq G$ de kern van deze actie. Dan werkt G/N op S via de actie*

$$s^{Ng} := s^g,$$

en deze actie is getrouw.

Bewijs. Dit hebben we bewezen in de cursus “Discrete Wiskunde II”. $\square$

Als G een groep is die werkt op een verzameling S , dan kunnen we met deze actie verscheidene interessante deelgroepen van G associëren. Omgekeerd kunnen we met elementen en deelgroepen van G interessante deelverzamelingen van S associëren.

Definitie 1.8.14. (i) Zij $s \in S$. Dan definiëren we de *stabilisator van s* als

$$G_s := \text{Stab}_G(s) := \{g \in G \mid s^g = s\}.$$

De stabilisator bestaat dus precies uit alle elementen van de groep G die het element s fixeren (i.e. op zichzelf afbeelden). Als we het element s niet nader specificeren, spreken we van *een puntstabilisator*.

- (ii) Zij $T \subseteq S$ een willekeurige deelverzameling. Dan definiëren we de *puntsgewijze stabilisator van T* als

$$G_T := \bigcap_{s \in T} G_s = \{g \in G \mid s^g = s \text{ voor alle } s \in T\}.$$

De puntsgewijze stabilisator bestaat dus precies uit alle elementen van de groep G die elk element van T fixeren. Deze deelgroep wordt ook soms de *fixator van T* of de *isotropiedeelgroep van T* genoemd.

- (iii) Zij $T \subseteq S$ een willekeurige deelverzameling. Dan definiëren we de *(globale) stabilisator van T* als

$$G_{\{T\}} := \{g \in G \mid T^g = T\}.$$

De stabilisator bestaat dus precies uit alle elementen van de groep G die de verzameling T op zichzelf afbeelden (maar dus niet noodzakelijk elk element van T fixeren).

- (iv) Zij nu $g \in G$. Dan definiëren we de *fixpuntverzameling van g* als

$$\text{Fix}_S(g) := \{s \in S \mid s^g = s\}.$$

De fixpuntverzameling bestaat dus precies uit alle elementen van S die door g gefixeerd worden.

- (v) Zij $H \leq G$. Dan definiëren we de *fixpuntverzameling van H* als

$$\text{Fix}_S(H) := \bigcap_{h \in H} \text{Fix}_S(h) = \{s \in S \mid s^h = s \text{ voor alle } h \in H\}.$$

De fixpuntverzameling bestaat dus precies uit alle elementen van S die door elk element van H gefixeerd worden. Merk op dat $\text{Fix}_S(g) = \text{Fix}_S(\langle g \rangle)$ voor alle $g \in G$.

- (vi) Zij $T \subseteq S$. We zeggen dat T een *G -invariante* of *G -stabiele* deelverzameling is, als $T^g \subseteq T$ voor alle $g \in G$, of equivalent, als $T^g = T$ voor alle $g \in G$, of nog anders gezegd, als $G_{\{T\}} = G$. (Toon zelf aan dat deze drie uitspraken equivalent zijn.)

Opmerking 1.8.15. De notaties voor puntsgewijze en globale stabilisatoren worden niet steeds op dezelfde manier gebruikt; zo gebruiken sommige auteurs de notatie G_T waar wij $G_{\{T\}}$ gebruiken, en $G_{[T]}$ of $G_{(T)}$ waar wij G_T gebruiken. De nodige voorzichtigheid is dus steeds geboden bij het nalezen van literatuur.

Een actie van een groep G op een verzameling S die echte G -invariante deelverzamelingen heeft, kan worden “opgedeeld” in nieuwe acties van dezelfde groep G op deze invariante deelverzamelingen. De acties die niet verder kunnen opgedeeld worden, spelen dus een belangrijke rol. We kennen deze reeds uit de cursus “Discrete Wiskunde II”:

Definitie 1.8.16. Beschouw een actie van een groep G op een verzameling S .

- (i) Een *baan* voor de actie is een deelverzameling van S van de vorm

$$s^G := \{s^g \mid g \in G\}.$$

- (ii) De actie is *transitief* als er slechts één baan is.

Lemma 1.8.17. Beschouw een actie van een groep G op een verzameling S .

- (i) De verzameling van alle banen is een partitie van de verzameling S .
- (ii) De actie is transitief als en slechts als er voor elke $s, t \in S$ een $g \in G$ bestaat zodat $s^g = t$.
- (iii) De banen voor de actie zijn precies de niet-ledige G -invariante deelverzamelingen van S waarop G transitief werkt. Anders gezegd, de banen zijn de minimale niet-ledige G -invariante deelverzamelingen van S .
- (iv) De actie is transitief als en slechts als de enige G -invariante deelverzamelingen van S de gehele verzameling S en de ledige deelverzameling $\emptyset$ zijn.

Bewijs. Uitspraken (i) en (ii) hebben we bewezen in de cursus “Discrete Wiskunde II”. Bewijs zelf uitspraken (iii) en (iv) als eenvoudige oefening. $\square$

We zien dus dat de transitieve acties precies die acties zijn die niet verder opgedeeld kunnen worden. Bemerkt immers dat indien de actie niet transitief is en $B \subset S$ een baan is, we de actie kunnen opdelen in twee “kleinere” acties, met name (G, B) en $(G, S \setminus B)$.

We gaan nu wat nader in op sterkere vormen van transitiviteit.

Definitie 1.8.18. Beschouw een actie van een groep G op een verzameling S . We noemen deze actie *n -voudig transitief* (of kortweg *n -transitief*) als G transitief werkt op de verzameling van geordende n -tallen van verschillende elementen van S . Expliciet eisen we dus dat er voor alle $s_1, \dots, s_n \in S$ (onderling verschillend) en alle $t_1, \dots, t_n \in S$ (onderling verschillend) een element $g \in G$ bestaat zodat $s_i^g = t_i$ voor elke $i \in \{1, \dots, n\}$.

Als bovendien geldt dat dit element g uniek is (voor gegeven s_i, t_i), dan noemen we de actie *scherp n -voudig transitief*. Een scherp 1-voudig transitieve actie wordt kortweg *scherp transitief* (of ook soms *regulier*) genoemd.

Merk op dat een n -voudig transitieve actie ook steeds t -voudig transitief is voor alle $t < n$. Anderzijds is een scherp n -voudig transitieve actie in het algemeen niet scherp t -voudig transitief voor $t \neq n$. (Zie ook Oefening 74.)

Stelling 1.8.19. *Beschouw een transitieve actie van een groep G op een verzameling S , en zij $s \in S$ willekeurig. Dan geldt:*

- (i) *De actie van G op S is n -voudig transitief als en slechts als de actie van G_s op $S \setminus \{s\}$ een $(n-1)$ -voudig transitieve actie is.*
- (ii) *De actie van G op S is scherp n -voudig transitief als en slechts als de actie van G_s op $S \setminus \{s\}$ een scherp $(n-1)$ -voudig transitieve actie is.*

Bewijs. We bewijzen enkel (i); werk zelf de details van (ii) uit.

Veronderstel eerst dat de actie van G op S inderdaad n -transitief is. Beschouw dan willekeurig twee $(n-1)$ -tallen $s_1, \dots, s_{n-1} \in S \setminus \{s\}$ (onderling verschillend) en $t_1, \dots, t_{n-1} \in S \setminus \{s\}$ (onderling verschillend). Stel dan $s_n := s$ en $t_n := s$. Wegens de gegeven n -transitiviteit bestaat er een $g \in G$ met $s_i^g = t_i$ voor elke i , dus in het bijzonder $s^g = s$, en dus $g \in G_s$. We besluiten dat de actie van G_s op $S \setminus \{s\}$ een $(n-1)$ -transitieve actie is.

Veronderstel omgekeerd dat de actie van G_s op $S \setminus \{s\}$ een $(n-1)$ -transitieve actie is. Beschouw willekeurig $s_1, \dots, s_n \in S$ (onderling verschillend) en $t_1, \dots, t_n \in S$ (onderling verschillend). Omdat de actie van G op S transitief ondersteld is, bestaan er $g, h \in G$ met $s_1^g = s$ en $t_1^h = s$, en wegens de gegeven $(n-1)$ -transitiviteit van G_s vinden we een $a \in G_s$ met $(s_i^g)^a = t_i^h$ voor alle $i \in \{2, \dots, n\}$. De samenstelling gah^{-1} is het gezochte element dat elke s_i op t_i afbeeldt; we besluiten dat de actie van G op S een n -transitieve actie is. $\square$

Voorbeelden 1.8.20. (1) De groep $G = \mathbf{S}_n$ werkt scherp n -voudig transitief op de verzameling $\{1, \dots, n\}$.

(2) De groep $G = \mathbf{A}_n$ werkt scherp $(n-2)$ -voudig transitief op de verzameling $\{1, \dots, n\}$. Inderdaad, voor twee gegeven $(n-2)$ -tallen $s_1, \dots, s_{n-2}$ en $t_1, \dots, t_{n-2}$ bestaan er precies twee elementen $g, h \in \mathbf{S}_n$ die elke s_i op t_i afbeelden, en precies één van beide zal een even permutatie zijn. (Meer bepaald is $h = ga$ waarbij a de transpositie $(t_{n-1}t_n)$ van de twee overblijvende elementen is.)

(3) Beschouw de diëdergroep $G = \mathbf{D}_{2n}$ werkend op de hoekpunten van een regelmatige n -hoek. Deze actie is transitief maar niet scherp transitief. De deelgroep $H = \mathbf{C}_n$ werkt wel scherp transitief op de hoekpunten.

(4) Beschouw een groep G werkend op een graaf Γ . Deze actie is tweevoudig transitief op de toppen als en slechts als Γ hetzij compleet hetzij cocom-

pleet is. (Een graaf wordt cocomplete genoemd als hij geen enkele boog heeft.)

Opmerking 1.8.21. De enige *eindige* n -voudig transitieve permutatiegroepen waarbij $n \geq 6$, zijn symmetrische en alternerende groepen. Dit is een zeer diep resultaat, dat gebruik maakt van de classificatie van de eindige enkelvoudige groepen. Voor $n = 5$ is dit niet langer waar, en zijn er precies twee bijkomende voorbeelden, met name twee van de vijf zogenaamde (enkelvoudige!) Mathieugroepen, M_{12} en M_{24} , die werken op verzamelingen van grootte 12 en 24, respectievelijk. Deze groepen hebben respectieve orde

$$95040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \quad \text{en} \quad 244823040 = 48 \cdot (24 \cdot 23 \cdot 22 \cdot 21 \cdot 20).$$

De groep M_{12} werkt dus zelfs scherp 5-voudig transitief; zie ook Oefening 74.

Oefeningen

67. Zij G een groep die werkt op een verzameling S , en zij $H \leq G$. Toon aan dat elke baan onder H bevat is in een baan onder G , en bijgevolg dat de banen onder H een partitie vormen van S die “fijner” is dan de partitie van S in de banen onder G .
68. Zij G een groep die werkt op een verzameling S . Zij $a \in S$ willekeurig maar vast. Toon aan dat de actie transitief is als en slechts als er voor elke $t \in S$ een $g \in G$ bestaat zodat $a^g = t$.
69. Zij G een groep die werkt op een verzameling S , en zij $g \in G$ en $s \in S$. Beschouw de puntstabilisator $G_s \leq G$. Toon aan dat $(G_s)^g = G_{s^g}$.
70. Zij G een groep die werkt op een verzameling S . Beschouw de puntstabilisator $G_s \leq G$ voor een zekere $s \in S$. Toon aan dat G_s werkt op $S \setminus \{s\}$. Als G transitief werkt op S , volgt hieruit dan dat G_s transitief werkt op $S \setminus \{s\}$? Omgekeerd, veronderstel dat G_s transitief werkt op $S \setminus \{s\}$ voor *elke* $s \in S$. Volgt hieruit dat G transitief werkt op S ?
71. Zij G een groep die werkt op een verzameling S , en $T \subseteq S$. Bewijs dat $G_T \trianglelefteq G_{\{T\}}$.
72. Zij G een eindige groep die transitief werkt op een eindige verzameling S , en zij $s \in S$ en $H \leq G$. Bewijs dat H transitief werkt op S als en slechts als $G = G_s H$.
- *73. Zoek een voorbeeld van een groep G die werkt op een verzameling S , en een deelverzameling $T \subseteq S$, zodat er elementen $g \in G$ bestaan zodat $T^g \subset T$ maar $T^g \neq T$.
74. Beschouw een actie van een groep G op een eindige verzameling S met $|S| = k$. Veronderstel dat de actie n -voudig transitief is. Toon aan dat $|G| \geq k!/(k-n)!$, en dat de gelijkheid geldt als en slechts als de actie *scherp* n -voudig transitief is.

Voorbeelden 1.8.22. We geven nu enkele belangrijke voorbeelden van vaak voorkomende acties. Merk op dat elk van deze voorbeelden vertrekt van een abstracte groep die a priori niet werkt op een gegeven verzameling.

- (1) Zij G een willekeurige groep. Dan werkt G op zichzelf *via toevoeging*⁵:

$$s^g := g^{-1}sg$$

voor alle $s \in G$ en alle $g \in G$. Het is niet moeilijk om na te gaan dat de voorwaarden (A) en (B) van p. 34 inderdaad vervuld zijn. Deze actie is niet steeds getrouw; de kern van de actie is precies het centrum $Z(G)$ van G .

De banen van deze actie zijn juist de klassen van toegevoegde elementen

$$h^G = \{h^g \mid g \in G\}.$$

De geïnduceerde actie van G op een klasse van toegevoegde elementen is dus een transitieve actie.

- (2) Zij G een willekeurige groep, en beschouw de *machtsverzameling* $\mathcal{P}(G)$, dit is de verzameling bestaande uit alle deelverzamelingen van G . Dan werkt G op $\mathcal{P}(G)$ via toevoeging:

$$D^g := g^{-1}Dg = \{g^{-1}hg \mid h \in D\}$$

voor alle $D \in \mathcal{P}(G)$ en alle $g \in G$. Het is opnieuw eenvoudig in te zien dat de voorwaarden (A) en (B) van p. 34 vervuld zijn.

De banen van deze actie zijn precies de “klassen van toegevoegde deelverzamelingen”

$$D^G = \{D^g \mid g \in G\};$$

de corresponderende actie van G op de verzameling D^G is dus transitief. Voornamelijk het geval waar D een *deelgroep* is van G wordt vaak gebruikt.

- (3) Beschouw opnieuw een willekeurige groep G . Dan werkt G op zichzelf *via rechtse vermenigvuldiging*:

$$s^g := sg$$

voor alle $s \in G$ en alle $g \in G$. Opnieuw zijn de voorwaarden (A) en (B) inderdaad vervuld.

De banen van deze actie zijn nu de deelverzamelingen van G van de vorm $s^G = sG$ voor $s \in G$. Maar uiteraard is $sG = G$ voor elke $s \in G$, en dus

⁵Het is dus geen toeval dat we dezelfde notatie hebben gebruikt voor toevoeging als voor de actie van een groep op een willekeurige verzameling, maar het is uiteraard belangrijk om beide concepten niet met elkaar te verwarren. In het bijzonder dient de terminologie “toevoeging” dus ook enkel en alleen gebruikt te worden voor deze welbepaalde actie.

is er maar één baan: G zelf. De actie is dus transitief. Het is eveneens gemakkelijk in te zien dat deze actie getrouw is.

De corresponderende permutatierepresentatie $\varphi: G \rightarrow \text{Sym}(G)$ wordt de *Cayley representatie van G* genoemd. Aangezien φ een monomorfisme is (want de actie is getrouw), toont dit aan dat elke groep isomorf is met een deelgroep van een symmetrische groep!

- (4) Beschouw nu een groep G en een deelgroep $H \leq G$. Dan werkt G op de verzameling⁶ $R_G(H)$:

$$(Hs)^g := Hsg$$

voor alle $Hs \in R_G(H)$ en alle $g \in G$. Deze actie is uiteraard goed gedefinieerd, en het is een actie want ze voldoet duidelijk aan de voorwaarden (A) en (B).

Opnieuw gaat men na dat deze actie transitief is. Ze is niet steeds getrouw; zie Oefening 79. Als $H = 1$ bekomen we precies het vorige voorbeeld.

De volgende observatie is het vermelden waard.

Lemma 1.8.23. *Zij G een willekeurige groep, en $H \leq G$ een deelgroep van eindige index n . Dan bestaat er een morfisme $\varphi: G \rightarrow \mathbf{S}_n$ met $\ker \varphi \leq H$.*

Bewijs. Beschouw de werking van G op $R_G(H)$ zoals in Voorbeeld 1.8.22(4). Aangezien $|R_G(H)| = n$, is de corresponderende permutatierepresentatie een morfisme $\varphi: G \rightarrow \mathbf{S}_n$. Als $g \in \ker \varphi$, dan fixeert g in het bijzonder de triviale nevenklasse H , dus $Hg = H$, dus $g \in H$. $\square$

In het geval we een actie hebben van G op zichzelf door toevoeging, geven we aan sommige van de algemeen ingevoerde begrippen een bijzondere naam.

Definitie 1.8.24. Zij G een willekeurige groep, en beschouw de actie van G op zichzelf door toevoeging.

- (i) Zij $h \in G$; de stabilisator G_h noemen we nu de *centralisator van h* , en we schrijven

$$C_G(h) := \{g \in G \mid h^g = h\} = \{g \in G \mid gh = hg\}.$$

We zien dus dat de centralisator van een element h precies bestaat uit alle elementen van G die met h commuteren.

⁶Soms wordt de verzameling $R_G(H)$ de *quotiëntruimte van G met betrekking tot H* genoemd, en sommige auteurs noteren dit ook als G/H . Zoals we weten, is dit in het algemeen geen groep, en we zullen de notatie G/H zelf enkel gebruiken indien $H \trianglelefteq G$.

- (ii) Zij $H \leq G$; de puntsgewijze stabilisator G_H noemen we nu de *centralisator van H* , en we schrijven

$$\begin{aligned} C_G(H) &:= \{g \in G \mid h^g = h \text{ voor alle } h \in H\} \\ &= \{g \in G \mid gh = hg \text{ voor alle } h \in H\}. \end{aligned}$$

We zien dus dat de centralisator van een deelgroep H precies bestaat uit alle elementen van G die met elk element van H commuteren.

- (iii) Zij $H \leq G$; de (globale) stabilisator $G_{\{H\}}$ noemen we nu de *normalisator van H* , en we schrijven

$$\begin{aligned} N_G(H) &:= \{g \in G \mid H^g = H\} \\ &= \{g \in G \mid h^g \in H \text{ en } h^{g^{-1}} \in H \text{ voor alle } h \in H\}. \end{aligned}$$

We zien dus dat de normalisator van een deelgroep H precies bestaat uit alle elementen van G die H invariant laten onder toevoeging.

Opmerking 1.8.25. Zij G een willekeurige groep en $H \leq G$. Dan is steeds $H \trianglelefteq N_G(H) \leq G$. Meer nog, $N_G(H)$ is de grootste deelgroep van G waarin H een normaaldeler is. (Toon dit zelf aan als oefening.) Dit verklaart de naam “normalisator”.

Opmerking 1.8.26. We gebruiken ook vaak de terminologie *centraliseren* en *normaliseren*. We zeggen dat een deelgroep A een deelgroep B centraliseert als $A \leq C_G(B)$, en we zeggen dat de deelgroep A de deelgroep B normaliseert als $A \leq N_G(B)$. (We gebruiken deze uitdrukkingen uiteraard ook met elementen in plaats van deelgroepen.)

We beschouwen nu opnieuw algemene acties van groepen op verzamelingen. Het volgend verband tussen banen en puntstabilisatoren is zeer belangrijk, en kennen we ook reeds vanuit de cursus “Discrete Wiskunde II”.

Stelling 1.8.27. *Beschouw een actie van een groep G op een verzameling S , en zij $s \in S$ willekeurig.*

- (i) *De afbeelding*

$$\delta: R_G(G_s) \rightarrow s^G: G_s g \mapsto s^g$$

is een bijectie.

- (ii) *Als G eindig is, dan geldt de baan-stabilisatorformule*

$$|G| = |G_s| \cdot |s^G|.$$

In het bijzonder is de lengte van elke baan een deler van $|G|$.

Bewijs. Dit hebben we bewezen in de cursus “Discrete Wiskunde II”. $\square$

Deze stelling is op zich al krachtig, maar wordt nog interessanter wanneer we ze combineren met de vaststelling dat de banen een partitie van S vormen (zie Lemma 1.8.17(ii)). Immers, veronderstel dat de actie k banen heeft, en noem die $S_1, \dots, S_k$. Dan geldt

$$|S| = |S_1| + \dots + |S_k|,$$

en elk van de termen van het rechterlid is een deler van G wegens de baan-stabilisatorformule.

In het bijzondere geval dat we de actie van G op zichzelf beschouwen door toevoeging, geven we deze laatste formule een bijzondere naam: de *klasseformule*.

Stelling 1.8.28. *Zij G een willekeurige groep.*

- (i) *Een klasse van toegevoegde elementen x^G is triviaal (i.e. $x^G = \{x\}$) als en slechts als $x \in Z(G)$.*
- (ii) *Als G eindig is, dan geldt de klasseformule*

$$|G| = |Z(G)| + \sum |x^G|,$$

waarbij de som wordt genomen over de niet-triviale klassen⁷. Bovendien is elke term van het rechterlid zelf een deler van $|G|$.

- Bewijs.* (i) We hebben $x^G = \{x\}$ als en slechts als $g^{-1}xg = x$ voor alle $g \in G$, of nog, als en slechts als x commuteert met elke $g \in G$.
- (ii) Beschouw de actie van G op zichzelf door toevoeging. Het feit dat de banen van deze actie een partitie vormen, vertaalt zich nu in het feit dat de klassen van toegevoegde elementen van G een partitie van G vormen. De overeenkomstige formule wordt

$$|G| = \sum |x^G|,$$

waarbij de som wordt genomen over *alle* klassen. Uit (i) volgt nu dat we dit ook nog kunnen herschrijven als

$$|G| = |Z(G)| + \sum |x^G|,$$

⁷Elke niet-triviale klasse wordt dus juist één keer geteld; we sommeren dus *niet* over de elementen $x \in G$.

waarbij de som nu wordt genomen over de niet-triviale klassen. Enerzijds weten we uit de baan-stabilisatorformule dat de lengte van een baan, die in dit geval de grootte van een klasse van toegevoegde elementen is, een deler is van $|G|$; anderzijds is $Z(G) \leq G$ en dus volgt uit de stelling van Lagrange dat ook $|Z(G)|$ een deler is van $|G|$. $\square$

Oefeningen

- 75.** Zij G een groep en $H \leq G$. Toon aan dat $C_G(H) \trianglelefteq N_G(H)$.
- 76.** Zij G een groep en $A \trianglelefteq B \leq G$. Toon aan dat $B \leq N_G(A)$.
- 77.** Zij G een groep. Bewijs dat de verzameling $A = \{g \in G \mid |g^G| < \infty\}$ een karakteristieke deelgroep is van G .
- 78.** Zij G een oneindige enkelvoudige groep, en A een eindige klasse van toegevoegde elementen in G . Bewijs dat $A = \{1\}$.
- 79.** Zij G een groep en $H \leq G$.
- (i) Definieer $\text{core}_G(H)$ als de grootste normaaldeeler van G die bevat is in H . Toon aan dat $\text{core}_G(H) = \bigcap_{g \in G} H^g$.
 - (ii) Beschouw de actie van G op G/H zoals in Voorbeeld 1.8.22(4). Toon aan dat de actie van G op G/H getrouw is als en slechts als $\text{core}_G(H) = 1$.
- *80.** Zij H een deelgroep van G met de eigenschap dat, voor alle $a, b \in G$, $b \notin H$, er een unieke $h \in H$ bestaat waarvoor $aba^{-1} = h b h^{-1}$. Bewijs dat $H \trianglelefteq G$. Onderstel nu bovendien dat H eindig is. Bewijs dat voor willekeurige $g \in G \setminus H$ geldt dat $g^G = gH$. Bewijs verder dat H in dit geval bestaat uit de verzameling van alle commutators in G , en dus $H = G'$.
-

1.9 De stellingen van Sylow

In het algemeen kunnen we niet veel zeggen over de deelgroepen van een willekeurige eindige groep. De stelling van Lagrange is de eenvoudigste zeer algemene uitspraak. De stellingen van Sylow, die we nu zullen bespreken, vormen wellicht het sterkste en meest nuttige resultaat dat relatief elementair is, en toch in sterke mate de mogelijkheden voor de deelgroepen van een groep beperkt.

Definitie 1.9.1. Zij p een priemgetal.

- (i) Een (*eindige*) p -groep is een eindige groep waarvan de orde een macht van p is.
- (ii) Zij G een willekeurige eindige groep, en zij $e \in \mathbb{N}$ zodanig dat p^e de hoogste macht van p is die $|G|$ deelt. (We laten dus in principe $e = 0$

toe, hoewel dit voor het vervolg niet erg nuttig zal blijken.) Een *Sylow p -deelgroep* (ook wel *p -Sylow deelgroep* genoemd) is een deelgroep van G van orde p^e .

- (iii) We noteren de verzameling van alle Sylow p -deelgroepen van een eindige groep G als $\text{Syl}_p(G)$. Het aantal Sylow p -deelgroepen van G noteren we als $n_p(G) := |\text{Syl}_p(G)|$.

Merk op dat we op dit moment nog niet weten of de groep G wel dergelijke deelgroepen heeft.

Voor we tot de eigenlijke stellingen van Sylow komen, bewijzen we eerst een lemma over eindige abelse groepen. We zullen later alle eindige abelse groepen classificeren (zie Stelling 3.5.3), en in feite zal dit lemma daar heel eenvoudig uit volgen; voor de volledigheid geven we hier een rechtstreeks bewijs.

Lemma 1.9.2. *Zij G een eindige abelse groep, en zij p een priemdelers van $|G|$. Dan bestaat er een $g \in G$ met $o(g) = p$.*

Bewijs. Kies p vast. We bewijzen het lemma per inductie op de orde van G (onder de voorwaarde dat p een deler is van $|G|$). Als $|G| = p$, dan heeft elk niet-triviaal element van G orde p .

Zij nu $|G| > p$, en kies een willekeurige $g \in G$ met $g \neq 1$. Als $p \mid o(g)$, dan is $g^{o(g)/p}$ een element van G van orde p , en dan is het lemma bewezen. Stel dus $p \nmid o(g)$, en beschouw de deelgroep $N = \langle g \rangle \leq G$. Omdat G abels is, is $N \trianglelefteq G$; beschouw dus de quotiëntgroep $H = G/N$. Omdat $p \nmid |N|$ is $|H|$ nog steeds deelbaar door p , en anderzijds is $|H| < |G|$. Wegens de inductiehypothese hebben we een $h \in H$ met $o(h) = p$.

We “liften” het element h nu naar G , d.w.z. we nemen een willekeurig element $a \in h^{\pi^{-1}}$, waarbij $\pi: G \rightarrow G/N$ de projectie-afbeelding is. Met andere woorden, h is precies de nevenklasse Na . Omdat $a^\pi = h$ hebben we $o(h) \mid o(a)$ (zie Gevolg 1.6.11), en dus is $p \mid o(a)$. Het element $a^{o(a)/p}$ is het gezochte element van orde p . $\square$

Zoals we verder zullen zien, geldt voorgaande stelling in feite voor willekeurige eindige groepen, en hoewel we dit resultaat nu al zouden kunnen bewijzen, zal het eenvoudiger zijn om het uit te stellen tot we de stellingen van Sylow behandeld zullen hebben.

We zullen ook gebruik maken van de volgende eenvoudige maar belangrijke stelling over p -groepen.

Stelling 1.9.3. *Zij G een niet-triviale eindige p -groep. Dan is $Z(G) \neq 1$.*

Bewijs. De klasseformule leert ons dat

$$|G| = |Z(G)| + \sum |x^G|,$$

waarbij de som wordt genomen over de niet-triviale klassen; bovendien is elke term van het rechterlid een deler van $|G|$. Aangezien $|G|$ een macht van p is, moet dus ook elke term $|x^G|$ een macht van p zijn, die echter strikt groter is dan 1 en bijgevolg deelbaar is door p . Dus moet ook de resterende term $|Z(G)|$ deelbaar zijn door p , en in het bijzonder $Z(G) \neq 1$. $\square$

We komen nu tot de eigenlijke stellingen van Sylow.

Stelling 1.9.4 (Sylow). *Zij G een eindige groep en p een priemgetal. Veronderstel dat p^e de hoogste macht van p is die $|G|$ deelt.*

- (i) $\text{Syl}_p(G) \neq \emptyset$, d.w.z. G heeft minstens één Sylow p -deelgroep;
- (ii) het aantal Sylow p -deelgroepen van G voldoet aan

$$n_p(G) \mid |G|/p^e \quad \text{en} \quad n_p(G) \equiv 1 \pmod{p};$$

- (iii) elke twee Sylow p -deelgroepen zijn toegevoegd aan elkaar;
- (iv) elke p -deelgroep van G is bevat in een Sylow p -deelgroep;
- (v) voor een willekeurige Sylow p -deelgroep $P \in \text{Syl}_p(G)$ geldt

$$n_p(G) = [G : N_G(P)].$$

Bewijs. (i) We gebruiken inductie op $|G|$ (waarbij we p vasthouden). Schrijf $|G| = p^e t$ met $p \nmid t$. Als $e = 0$, dan is een Sylow p -deelgroep een triviale deelgroep, en valt er niks te bewijzen. Stel dus $e \geq 1$. Als $t = 1$, dan valt er opnieuw niks te bewijzen; stel dus $t > 1$.

Als G een echte deelgroep $H < G$ bevat zodat $p^e \mid |H|$, dan bestaat er per inductie een Sylow p -deelgroep P van H ; maar dan is $P \leq G$ en $|P| = p^e$, dus is P ook een Sylow p -deelgroep van G .

Veronderstel dus dat geen enkele echte deelgroep van G een orde heeft die deelbaar is door p^e ; dan geldt voor elke echte deelgroep $H < G$ dat $[G : H]$ deelbaar is door p . We herschrijven de klasseformule nu, met behulp van de baan-stabilisatorformule, als

$$|G| = |Z(G)| + \sum [G : C_G(x)],$$

waarbij de som wordt genomen over de niet-triviale klassen van toegevoegde elementen van G . Voor elke niet-triviale klasse x^G is $C_G(x) < G$,

en dus is wegens voorgaande vaststelling $[G : C_G(x)]$ deelbaar door p . Omdat ook $|G|$ deelbaar is door p , besluiten we hieruit dat $|Z(G)|$ deelbaar is door p . Wegens Lemma 1.9.2 bestaat er een element $z \in Z(G)$ van orde p . Stel $N = \langle z \rangle$; dan is $|N| = p$, en $N \trianglelefteq G$. Beschouw de quotiëntgroep $K = G/N$, met bijhorende projectie-afbeelding π . Dan is $|K| = |G|/p$, en dus heeft een Sylow p -deelgroep van K orde p^{e-1} . We kunnen dus de inductiehypothese toepassen op K , en we halen hieruit dat er een deelgroep $Q \leq K$ bestaat met $|Q| = p^{e-1}$. We liften nu Q terug naar G (zie Stelling 1.6.6), en we bekomen een deelgroep $P = Q^{\pi^{-1}}$, met

$$|P| = |Q^{\pi^{-1}}| = |\ker(\pi)| \cdot |Q| = p \cdot p^{e-1} = p^e.$$

Dus P is een Sylow p -deelgroep van G . (Merk op dat dit nu in feite een contradictie is, aangezien we ondersteld hebben dat geen enkele echte deelgroep van G een orde heeft die deelbaar is door p^e .)

- (ii.b) Beschouw de actie van G op $\text{Syl}_p(G)$ via toevoeging. Zij X een willekeurige G -stabiele deelverzameling van $\text{Syl}_p(G)$. Zij $Q \leq G$ een willekeurige deelgroep met als orde een macht van p (dus niet noodzakelijk in X noch in $\text{Syl}_p(G)$). Dan werkt Q op de verzameling X via toevoeging. De stabilisator van een element $P \in X$ onder deze actie is gelijk aan $Q \cap N_G(P)$; we zullen hiervoor de notatie $N_Q(P)$ gebruiken⁸. Door X op te splitsen in zijn banen onder deze Q -actie krijgen we dan

$$|X| = \sum_P |P^Q| = \sum_P [Q : N_Q(P)], \quad (1.2)$$

waarbij de som wordt genomen over deze banen (waarbij P dus een representant van de baan P^Q is). Merk op dat elke term $[Q : N_Q(P)]$ van het rechterlid een macht van p is.

We willen nu de gelijkheid (1.2) modulo p gaan bekijken, en de termen $[Q : N_Q(P)]$ die hierin een niet-nul bijdrage leveren, zijn precies die waarvoor $N_Q(P) = Q$ (en die zijn dus afkomstig van banen $P^Q = \{P\}$ van lengte 1). We moeten dus nagaan wanneer $N_Q(P) = Q$, met andere woorden, wanneer P door Q genormaliseerd wordt, of nog, wanneer $Q \leq N_G(P)$.

We willen nu aantonen dat $Q \leq N_G(P)$ als en slechts als $Q \leq P$; merk op dat de “als”-implicatie triviaal is omdat $P \leq N_G(P)$. Veronderstel dus dat de Sylow p -deelgroep P zodanig is dat $Q \leq N_G(P)$. Omdat ook $P \trianglelefteq N_G(P)$, volgt hieruit dat $PQ \leq N_G(P) \leq G$ (zie Lemma 1.6.12).

⁸Merk op dat dit in feite een veralgemening is van Definitie 1.8.24(iii), die een dergelijke notatie enkel toeliet voor $P \leq Q$, wat hier niet het geval is.

Uit Stelling 1.6.16 halen we echter dat $|PQ| = |P| \cdot |Q| / |P \cap Q|$, hetgeen een macht van p is. Omdat P een Sylow p -deelgroep is, kan dit enkel als $PQ = P$, en dus is $Q \leq P$.

Uit de gelijkheid (1.2) volgt nu dat

$$|X| \equiv |\{P \in X \mid Q \leq P\}| \pmod{p}. \quad (1.3)$$

We passen nu de voorgaande formule toe op de keuze $X = \text{Syl}_p(G)$ en $Q \in \text{Syl}_p(G)$; we weten reeds uit (i) dat een dergelijke Q inderdaad bestaat. Dan krijgen we

$$|\text{Syl}_p(G)| \equiv 1 \pmod{p},$$

wat we moesten bewijzen.

- (iii) We kiezen nu X gelijk aan een enkele baan in de werking van G op $\text{Syl}_p(G)$. Neem een $R \in X$; dan volgt uit de baan-stabilisatorformule dat $|X| = [G : N_G(R)]$. Aangezien $R \leq N_G(R)$ is de index $[G : N_G(R)]$ niet deelbaar door p , en dus is $|X| \not\equiv 0 \pmod{p}$. Neem nu een $Q \in \text{Syl}_p(G)$ willekeurig. Uit de congruentie (1.3) weten we dan dat

$$|X| \equiv |\{P \in X \mid Q \leq P\}| \pmod{p},$$

en bijgevolg is

$$|\{P \in X \mid Q \leq P\}| \neq 0. \quad (1.4)$$

Aangezien zowel Q als de elementen van X Sylow p -deelgroepen zijn, is $Q \leq P$ als en slechts als $Q = P$ voor alle $P \in X$, en uit (1.4) volgt dus dat $Q \in X$. Aangezien $Q \in \text{Syl}_p(G)$ willekeurig was, besluiten we dat $X = \text{Syl}_p(G)$, en de werking van G op $\text{Syl}_p(G)$ heeft dus maar één baan (i.e. de werking is transitief). Dus zijn elke twee Sylow p -deelgroepen toegevoegd aan elkaar.

- (v) Zij $P \in \text{Syl}_p(G)$ willekeurig. Uit (iii) en de baan-stabilisatorformule volgt nu $|G| = |\text{Syl}_p(G)| \cdot |N_G(P)|$.
- (ii.a) Uit (v) volgt dat $n_p(G) \mid |G|$, maar omdat we uit (ii.b) reeds weten dat $\gcd(n_p(G), p) = 1$, volgt hieruit de sterkere voorwaarde $n_p(G) \mid |G|/p^e$.
- (iv) Zij $Q \leq G$ een willekeurige p -deelgroep van G . We passen opnieuw de gelijkheid (1.3) toe met $X = \text{Syl}_p(G)$, en samen met (ii.b) halen we hieruit dat

$$|\{P \in \text{Syl}_p(G) \mid Q \leq P\}| \equiv |X| \equiv 1 \pmod{p},$$

zodat

$$\{P \in \text{Syl}_p(G) \mid Q \leq P\} \neq \emptyset;$$

dit zegt precies dat Q in minstens één Sylow p -deelgroep bevat is. $\square$

Een onmiddellijk gevolg hiervan is dat we Lemma 1.9.2 kunnen uitbreiden naar willekeurige groepen.

Gevolg 1.9.5 (Stelling van Cauchy). *Zij G een eindige groep, en p een priemdelers van $|G|$. Dan heeft G een element van orde p .*

Bewijs. Uit de stellingen van Sylow weten we dat G een Sylow p -deelgroep P bezit. Neem nu $g \in P$ willekeurig met $g \neq 1$; dan is $o(g) = p^k$ voor een zekere $k \in \mathbb{N}^*$. Maar dan is $g^{p^{k-1}}$ een element van orde p . $\square$

Een ander zeer nuttig gevolg van de stellingen van Sylow is het volgende.

Gevolg 1.9.6. *Zij G een eindige groep en p een priemdelers van $|G|$, en zij $P \in \text{Syl}_p(G)$. Dan is $P \trianglelefteq G$ als en slechts als $n_p(G) = 1$.*

Bewijs. Dit volgt onmiddellijk uit Stelling 1.9.4(v). $\square$

Dit gevolg kan vaak gebruikt worden om aan te tonen dat een willekeurige groep met een vooropgegeven orde niet enkelvoudig kan zijn. We geven drie voorbeelden.

Voorbeeld 1.9.7. Beschouw een groep G met $|G| = 28 = 2^2 \cdot 7$. Dan is $n_7(G) \mid 2^2$ en $n_7(G) \equiv 1 \pmod{7}$; dit kan enkel als $n_7(G) = 1$. Uit Gevolg 1.9.6 volgt dan dat de unieke Sylow 7-deelgroep een normaaldeeler is, en dus is G niet enkelvoudig.

Voor we het volgend voorbeeld geven, vermelden we eerst een nuttig lemma dat we in deze context vaak kunnen gebruiken.

Lemma 1.9.8. *Zij G een eindige groep, en p een priemdelers van G met $p^2 \nmid |G|$. Dan zijn er precies $n_p(G) \cdot (p - 1)$ elementen van orde p in G .*

Bewijs. Uit de voorwaarde op p volgt dat de Sylow p -deelgroepen van G orde p hebben. Als P en Q twee verschillende Sylow p -deelgroepen zijn, dan snijden die bijgevolg triviaal, i.e. $P \cap Q = 1$. Dus elk element van orde p van G zit in precies één Sylow p -deelgroep. Omdat omgekeerd elke Sylow p -deelgroep juist $p - 1$ elementen van orde p bevat, vinden we $n_p(G) \cdot (p - 1)$ elementen van orde p in G . $\square$

Voorbeeld 1.9.9. Beschouw een groep G met $|G| = 56 = 2^3 \cdot 7$. Dan is $n_7(G) \mid 2^3$ en $n_7(G) \equiv 1 \pmod{7}$; dit kan enkel als $n_7(G) = 1$ of $n_7(G) = 8$. Indien $n_7(G) = 8$, dan volgt uit Lemma 1.9.8 dat er $8 \cdot 6 = 48$ elementen van orde 7 zijn in G . Maar dan zijn er slechts $56 - 48 = 8$ elementen meer over. Aangezien G minstens één Sylow 2-deelgroep moet bevatten, en een

dergelijke deelgroep $2^3 = 8$ elementen bevat (die allen als orde een macht van 2 hebben), volgt hieruit dat er juist één Sylow 2-deelgroep is. Samengevat: er is ofwel juist één Sylow 7-deelgroep, ofwel juist één Sylow 2-deelgroep (of beide). Uit Gevolg 1.9.6 volgt dat G niet enkelvoudig kan zijn.

Ons derde voorbeeld gebruikt nog een ander soort redenering. Zoals we hebben gezien werkt G op de verzameling $\text{Syl}_p(G)$ via toevoeging, en uit de stellingen van Sylow weten we dat deze actie transitief is. Als G enkelvoudig is, dan moet deze actie bovendien getrouw zijn, en vaak kan dit om numerieke redenen niet voldaan zijn.

Voorbeeld 1.9.10. Beschouw een groep G met $|G| = 48 = 2^4 \cdot 3$. Dan is $n_3(G) \mid 2^4$ en $n_3(G) \equiv 1 \pmod{3}$; dit kan enkel als $n_3(G) \in \{1, 4, 16\}$. Als $n_3(G) = 16$, dan kunnen we zoals in het vorige voorbeeld berekenen dat er 32 elementen van orde 3 zijn in G ; de resterende 16 elementen vormen dan een unieke Sylow 2-deelgroep, dus dan is $n_2(G) = 1$.

We werken nu verder uit het ongerijmde. Veronderstel dus dat G enkelvoudig is; uit de voorgaande beschouwingen zien we dat de enige resterende mogelijkheid het geval $n_3(G) = 4$ is. Omdat de actie van G op $\text{Syl}_3(G)$ getrouw is —de kern van de actie is immers een normaaldeeler van G — is de corresponderende permutatierepresentatie $\varphi: G \rightarrow \mathbf{S}_4$ een monomorfisme. Dus moet $|\text{im}(\varphi)| = |G|$ een deler zijn van $|\mathbf{S}_4|$, en dat geeft ons $48 \mid (4!)$. Door deze strijdigheid besluiten we dat G niet enkelvoudig kan zijn.

Opmerking 1.9.11. De mogelijke ordes voor eindige enkelvoudige groepen zijn vrij “dun bezaaid”. Zo heeft de kleinste niet-abelse enkelvoudige groep orde 60, en de tweede kleinste orde 168.

De stellingen van Sylow kunnen ook van pas komen om de structuur te achterhalen van Sylow deelgroepen van een gegeven groep.

Voorbeeld 1.9.12. We willen achterhalen wat de structuur is van een Sylow 2-deelgroep van $G = \mathbf{S}_4$. We stellen vast dat $|G| = 24 = 2^3 \cdot 3$, dus als $P \in \text{Syl}_2(G)$, dan is $|P| = 8$.

We kennen echter een groep van orde 8 die getrouw werkt op een verzameling van 4 elementen, namelijk de groep $H = \mathbf{D}_8$ (in zijn werking op de hoekpunten van een vierkant). Deze werking heeft een corresponderende getrouwe permutatierepresentatie $\varphi: H \hookrightarrow \mathbf{S}_4$, en dus is $Q = \varphi(H)$ een deelgroep van $\mathbf{S}_4$ van orde 8, en dus $Q \in \text{Syl}_2(G)$.

We passen nu de stelling van Sylow toe die ons vertelt dat P en Q toegevoegd zijn aan elkaar, en dus in het bijzonder $P \cong Q$, want toevoeging is een automorfisme. We besluiten dat onze willekeurige Sylow 2-deelgroep P isomorf is met $\mathbf{D}_8$.

Oefeningen

81. Zij G een eindige groep waarvoor de orde van elk element een macht van een vast priemgetal p is. Bewijs dat G een p -groep is.
 82. Bestaat er een eindige groep G die geen p -groep is, waarvoor de orde van elk element een macht van een priemgetal is?
 83. Zij G een eindige groep met $|G| = p^2q$, met p, q twee verschillende priemgetallen. Toon aan dat G ofwel een unieke Sylow p -deelgroep bezit, ofwel een unieke Sylow q -deelgroep (of beide); leid hieruit af dat G niet enkelvoudig kan zijn.
 84. Zij G een eindige groep, zij $N \trianglelefteq G$, en zij p een priemgetal. Bewijs dat voor elke $P \in \text{Syl}_p(N)$ geldt dat $G = N_G(P)N$. (Dit is het zogenaamde *Frattini argument*.)
 85. Zij G een enkelvoudige groep met $|G| = 168$. Tel het aantal elementen van orde 7 in G .
 86. Bewijs dat er geen enkelvoudige groepen van de orde 40, 200 of 700 zijn.
 87. Beschrijf alle Sylow deelgroepen van de groep $\mathbf{D}_{2n}$.
 88. Zij G een eindige groep met de eigenschap dat $\text{Aut}(G)$ transitief werkt op $G \setminus \{1\}$. Bewijs dat G elementair abels is.
 89. Toon aan dat elke groep van orde 84 deelgroepen bezit van index 3, 4 en 6.
 90. Zij G een groep met $|G| = 280$. Toon aan dat G niet enkelvoudig is, en dat het een deelgroep bezit van de orde 35.
 91. Zij p een oneven priemgetal, zij $G = \mathbf{S}_{2p}$, en zij $P \in \text{Syl}_p(G)$. Toon aan dat $P \cong \mathbf{C}_p \times \mathbf{C}_p$.
 92. Zij G een eindige groep waarin elke Sylow deelgroep een normaaldeler is. Toon aan dat G isomorf is met het directe product van al zijn Sylow deelgroepen. Toon eveneens aan dat er, voor elke deler n van $|G|$, een deelgroep $H \leq G$ bestaat met $|H| = n$.
 - *93. Zij G een enkelvoudige groep met $|G| = 60$. Toon aan dat G isomorf is met $\mathbf{A}_5$.
 - *94. Zij $p > 2$ een priemgetal, en zij G een p -groep die slechts één deelgroep van de orde p bezit. Toon aan dat G cyclisch is. Geef een tegenvoorbeeld voor het geval $p = 2$.
-

1.10 Groepen van orde ≤ 15

We zullen, bij wijze van illustratie van de tot dusver opgebouwde theorie, een classificatie geven van alle groepen van orde kleiner dan of gelijk aan 15. Er is een goede reden om niet verder dan 15 te gaan: er blijken immers, op isomorfisme na, al 14 verschillende groepen van orde 16 te bestaan. (Dit is een typisch fenomeen voor p -groepen. Zo bestaan er maar liefst 49487365422 verschillende groepen van orde $1024 = 2^{10}$.)

We starten met groepen van orde p en p^2 (met p priem). Alle uniciteitsuitspraken in deze sectie zijn uiteraard op isomorfisme na.

Stelling 1.10.1. *Zij p een priemgetal.*

- (i) *Er is een unieke groep van orde p , namelijk $\mathbf{C}_p$.*
- (ii) *Er zijn precies twee groepen van orde p^2 , namelijk $\mathbf{C}_{p^2}$ en $\mathbf{C}_p \times \mathbf{C}_p$.*

Bewijs. (i) Zij G een willekeurige groep van orde p . Zij dan $g \in G$ een willekeurig niet-triviaal element. Omdat G wegens Lagrange geen echte deelgroepen kan hebben, is $G = \langle g \rangle$, dus $G \cong \mathbf{C}_p$.

- (ii) Zij G een willekeurige groep van orde p^2 . Wegens Stelling 1.9.3 is $Z(G) \neq 1$.

Veronderstel eerst dat $|Z(G)| = p$. Dan is ook $|G/Z(G)| = p$, en uit (i) volgt dan dat $G/Z(G)$ cyclisch is. Uit Oefening 56 volgt dan echter dat G abels is, een contradictie.

Bijgevolg is $Z(G) = G$, dus G is abels. Als G een element van orde p^2 heeft, dan is $G \cong \mathbf{C}_{p^2}$. Indien niet, dan heeft elk niet-triviaal element van G orde p . Kies nu willekeurig twee verschillende deelgroepen A en B van G van orde p . Dan is $A \cap B = 1$, en uit Stelling 1.7.5 volgt dan dat $G \cong \mathbf{C}_p \times \mathbf{C}_p$. $\square$

Vervolgens willen we de groepen klasseren van orde $2p$ waarbij p een oneven priemgetal is. In deze classificatie zullen we ondermeer de diëdergroepen moeten tegenkomen. We zullen hiervoor handig gebruik maken van de volgende herkenningmethode voor bepaalde groepen van even orde.

Lemma 1.10.2. *Zij G een groep van orde $2n$ die een element g van orde n bevat. Stel $N = \langle g \rangle$, en zij $h \in G \setminus N$. Dan geldt:*

- (i) $G = \{1, g, g^2, \dots, g^{n-1}, h, hg, hg^2, \dots, hg^{n-1}\}$.
- (ii) $h^2 \in N$ en $gh \in hN$. In het bijzonder bestaan er gehele getallen i, j (die we in $\{0, \dots, n-1\}$ kunnen kiezen) zodat $h^2 = g^i$ en $gh = hg^j$.
- (iii) De groep G is volledig bepaald door de relaties $h^2 = g^i$ en $gh = hg^j$. Met andere woorden, indien $\hat{G}$ een groep is van orde $2n$ met een element $\hat{g}$ van orde n en een element $\hat{h} \in \hat{G} \setminus \langle \hat{g} \rangle$ zodat $\hat{h}^2 = \hat{g}^i$ en $\hat{g}\hat{h} = \hat{h}\hat{g}^j$, dan is $G \cong \hat{G}$.
- (iv) Als n even is, stel $n = 2t$, dan is $g^t \in Z(G)$.

Bewijs. (i) Merk op dat $[G : N] = 2$, zodat $N \trianglelefteq G$. Aangezien $h \in G \setminus N$ is $Nh = hN$ de unieke niet-triviale nevenklasse van N in G . In het bijzonder is $G = N \cup hN$, waaruit (i) volgt.

- (ii) De quotiëntgroep G/N heeft orde 2; bijgevolg heeft het element $hN \in G/N$ orde 2, en dus is $h^2N = N$. Anderzijds is $gh \in Nh = hN$. De rest van de bewering volgt uit het feit dat $N = \langle g \rangle$.
- (iii) We lijsten de elementen van G op zoals in (i). De groepsbewerking van G ligt dan volledig vast indien we voor deze elementen een vermenigvuldigingstabel kennen. Uit de gegeven relaties $h^2 = g^i$ en $gh = hg^j$ halen we nu, voor elke $a, b \in \{0, \dots, n-1\}$:

$$\begin{aligned} g^a \cdot g^b &= g^{a+b}, \\ hg^a \cdot g^b &= hg^{a+b}, \\ g^a \cdot hg^b &= hg^{aj+b}, \\ hg^a \cdot hg^b &= g^{i+aj+b}. \end{aligned}$$

- (iv) Merk op dat $z = g^t$ de unieke involutie is in N . Anderzijds is elke toegevoegde van z opnieuw een involutie (want toevoeging is een automorfisme, dus bewaart de orde), en is opnieuw bevat in N (want N is een normaaldeler), en is dus opnieuw gelijk aan z zelf. Dus $z \in Z(G)$. $\square$

We kunnen dit lemma in het bijzonder toepassen om de diëdergroepen te herkennen.

Gevolg 1.10.3. *Zij G een groep van orde $2n$ die een element g van orde n bevat. Zij $h \in G \setminus \langle g \rangle$. Als $h^2 = 1$ en $gh = hg^{-1}$, dan is $G \cong \mathbf{D}_{2n}$.*

Bewijs. We passen Lemma 1.10.2 toe. Het volstaat hiertoe om vast te stellen dat we ook in $\hat{G} = \mathbf{D}_{2n}$ elementen $\hat{g}$ en $\hat{h} \in \hat{G} \setminus \langle \hat{g} \rangle$ kunnen vinden zodat $\hat{g}$ orde n heeft, $\hat{h}^2 = 1$ en $\hat{g}\hat{h} = \hat{h}\hat{g}^{-1}$. Kies daartoe voor $\hat{g}$ de rotatie over een hoek $2\pi/n$ en voor $\hat{h}$ een willekeurige loodrechte spiegeling. Uit Lemma 1.10.2(iii) volgt nu dat $G \cong \mathbf{D}_{2n}$. $\square$

We komen nu tot de beloofde classificatie van groepen van orde $2p$.

Stelling 1.10.4. *Zij p een priemgetal. Er zijn precies twee groepen van orde $2p$, namelijk $\mathbf{C}_{2p}$ en $\mathbf{D}_{2p}$.*

Bewijs. Zij G een willekeurige groep van orde $2p$. Veronderstel dat $p > 2$; indien $p = 2$ is $2p = p^2$ en verwijzen we naar Stelling 1.10.1. Wegens de stelling van Cauchy bezit G een element g van orde p en een involutie h . Merk op dat $G = \langle g, h \rangle$. Dan heeft $\langle g \rangle$ index 2 in G , en dus is $\langle g \rangle \trianglelefteq G$; hieruit volgt in het bijzonder dat $g^h = g^t$ voor een zeker natuurlijk getal $t \leq p-1$. Omdat h een involutie is, volgt hieruit dat

$$g = (g^h)^h = (g^t)^h = (g^h)^t = (g^t)^t = g^{t^2}$$

en dus $g^{t^2-1} = 1$; hieruit halen we dat $p \mid t^2 - 1$. Bijgevolg is ofwel $p \mid t + 1$ ofwel $p \mid t - 1$, en omdat $t \leq p - 1$ volgt hieruit dat $t = 1$ of $t = p - 1$.

Veronderstel eerst dat $t = 1$. Dan is $g^h = g$, zodat g en h met elkaar commuteren, maar dan is $G = \langle g, h \rangle$ abels. Omdat $\langle g \rangle$ en $\langle h \rangle$ dan twee normaaldelers zijn die elkaar triviaal snijden, volgt nu uit Stellingen 1.7.5 en 1.7.8 dat $G \cong \mathbf{C}_p \times \mathbf{C}_2 \cong \mathbf{C}_{2p}$.

Veronderstel nu dat $t = p - 1$. Dan is $g^h = g^{-1}$, of nog, $gh = hg^{-1}$. Uit Gevolg 1.10.3 volgt nu dat $G \cong \mathbf{D}_{2p}$. $\square$

Als we nu de getallen tot en met 15 overlopen, dan zien we dat enkel nog 8, 12 en 15 niet door voorgaande stellingen worden gedekt. We handelen eerst groepen van orde 15 af.

Stelling 1.10.5. *Zij G een groep van orde pq met $p < q$ verschillende priemgetallen. Als p geen deler is van $q - 1$, dan is G cyclisch.*

Bewijs. Uit de stellingen van Sylow halen we dat

$$n_p(G) \mid q, \quad n_p(G) \equiv 1 \pmod{p}, \quad (1.5)$$

$$n_q(G) \mid p, \quad n_q(G) \equiv 1 \pmod{q}. \quad (1.6)$$

Uit (1.6) volgt, wegens $q > p$, dat $n_q(G) = 1$. Anderzijds volgt uit (1.5), waarbij q priem is, dat $n_p(G) \in \{1, q\}$, en indien $n_p(G) = q$, dan zou $q \equiv 1 \pmod{p}$, in strijd met het gegeven dat $p \nmid q - 1$; dus ook $n_p(G) = 1$.

Uit Gevolg 1.9.6 volgt nu dat G normaaldelers P en Q van respectieve orde p en q heeft, en opnieuw volgt uit Stellingen 1.7.5 en 1.7.8 dat $G \cong P \times Q \cong \mathbf{C}_{pq}$. $\square$

Door deze stelling toe te passen met $p = 3$ en $q = 5$, besluiten we dat elke groep van orde 15 cyclisch is.

Vervolgens bekijken we groepen van orde 8.

Stelling 1.10.6. *Er zijn op isomorfisme na precies vijf groepen van orde 8, met name*

$$\mathbf{C}_8, \quad \mathbf{C}_4 \times \mathbf{C}_2, \quad \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2, \quad \mathbf{D}_8, \quad \mathbf{Q}_8.$$

Bewijs. Zij G een groep van orde 8. Als G een element van orde 8 bevat, dan is $G \cong \mathbf{C}_8$. Als elk element van G orde 1 of 2 heeft, dan is $G \cong \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$ (zie Oefening 64).

Veronderstel nu dat elk element van G orde 1, 2 of 4 heeft, en dat G een element g van orde 4 bevat. We zitten nu in de situatie van Lemma 1.10.2.

Stel dus $N := \langle g \rangle \trianglelefteq G$ en zij $h \in G \setminus N$ willekeurig; dan kunnen we G oplijsten als

$$G = \{1, g, g^2, g^3, h, hg, hg^2, hg^3\},$$

en er bestaan gehele getallen $i, j \in \{0, 1, 2, 3\}$ zodat $h^2 = g^i$ en $gh = hg^j$. Merk op dat h^2 niet kan gelijk zijn aan g of g^3 omdat anders $o(h) = 8$. Dus

$$h^2 \in \{1, g^2\}.$$

Anderzijds kan gh niet gelijk zijn aan h of aan hg^2 . (Als $gh = hg^2$ zouden g en g^2 immers toegevoegd zijn, wat niet kan omdat ze verschillende orde hebben.) Dus

$$gh \in \{hg, hg^3\}.$$

Veronderstel eerst dat $gh = hg$. Dan is G abels. Als $h^2 = 1$, dan zien we onmiddellijk dat $G \cong N \times \langle h \rangle \cong \mathbf{C}_4 \times \mathbf{C}_2$. Als $h^2 = g^2$, dan is $o(gh) = 2$, en $gh \notin N$, dus volgt op dezelfde manier dat $G \cong N \times \langle gh \rangle \cong \mathbf{C}_4 \times \mathbf{C}_2$.

We mogen nu veronderstellen dat $gh = hg^3 = hg^{-1}$, dus G is niet abels. Als $h^2 = 1$, dan volgt uit Gevolg 1.10.3 dat $G \cong \mathbf{D}_8$. Veronderstel dus ten slotte dat $h^2 = g^2$. We beweren dat nu $G \cong \mathbf{Q}_8$. Stel dus $\hat{G} = \mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ en stel $\hat{g} = i$ en $\hat{h} = j$. Dan heeft $\hat{g}$ orde 4 en is $\hat{h} \in \hat{G} \setminus \langle \hat{g} \rangle$, $\hat{h}^2 = \hat{g}^2$ en $\hat{g}\hat{h} = \hat{h}\hat{g}^{-1}$. Uit Lemma 1.10.2(iii) volgt nu inderdaad $G \cong \mathbf{Q}_8$. $\square$

We zijn nu aangekomen bij het moeilijkste geval, de groepen van orde 12. We kennen reeds vier dergelijke groepen, namelijk $\mathbf{C}_{12}$, $\mathbf{C}_6 \times \mathbf{C}_2$ (ook te schrijven als $\mathbf{C}_3 \times \mathbf{C}_2 \times \mathbf{C}_2$), $\mathbf{D}_{12}$ en $\mathbf{A}_4$. We beginnen met de vaststelling dat de enige deelgroep van $\mathbf{S}_4$ van orde 12 precies $\mathbf{A}_4$ is.

Stelling 1.10.7. *Zij $G = \mathbf{S}_4$ en zij $H \leq G$ een deelgroep van orde 12. Dan is $H \cong \mathbf{A}_4$.*

Bewijs. Merk op dat H index 2 heeft in G , dus $H \trianglelefteq G$. Wegens de stelling van Cauchy bevat H een element h van orde 3, dat dan noodzakelijk een 3-cykel is, stel $h = (abc)$. Wegens Gevolg 1.8.4 bestaat de toevoegingsklasse h^G precies uit alle 3-cykels, en omdat $H \trianglelefteq G$, is $h^G \subset H$. Dus H bevat alle elementen van orde 3 van G , maar deze 8 elementen uit $\mathbf{A}_4$ brengen $\mathbf{A}_4$ voort, en dus moet $H = \mathbf{A}_4$. $\square$

Merk op dat $\mathbf{A}_4$ geen elementen van orde 6 bevat. Interessant is dat we nu reeds kunnen aantonen dat dit de enige groep van orde 12 is met die eigenschap.

Lemma 1.10.8. *Zij G een groep van orde 12, en veronderstel dat $G \not\cong \mathbf{A}_4$. Dan heeft G een element van orde 6.*

Bewijs. Wegens de stelling van Cauchy bestaat er een element $g \in G$ met $o(g) = 3$. Stel $H := \langle g \rangle$; dan is $[G : H] = 4$. Uit Lemma 1.8.23 halen we een morfisme $\varphi: G \rightarrow \mathbf{S}_4$ met $\ker \varphi \leq H$. Als $\ker \varphi$ triviaal zou zijn, dan zou G isomorf zijn met een deelgroep van $\mathbf{S}_4$, en dan zou uit Stelling 1.10.7 volgen dat $G \cong \mathbf{A}_4$, in strijd met onze onderstelling.

Dus $\ker \varphi = H$, maar dan is $H \trianglelefteq G$. Echter, H is een Sylow 3-deelgroep van G , en uit Gevolg 1.9.6 volgt dat H de enige Sylow 3-deelgroep van G is. Elk element van orde 3 is echter bevat in een Sylow 3-deelgroep, en dus heeft G precies 2 elementen van orde 3. In het bijzonder is $|g^G|$ gelijk aan 1 of 2, en uit de baan-stabilisatorformule volgt dan dat $|C_G(g)| = 12$ of 6. Bijgevolg bezit $C_G(g)$ een element van orde 2, stel h , en dan is inderdaad $o(gh) = 6$ (zie Oefening 21). $\square$

We komen nu tot de beloofde classificatie van groepen van orde 12. In dit proces zullen we een nieuwe groep tegenkomen, die we op dit moment nog niet erg elegant kunnen beschrijven. Deze groep blijkt een semidirect product te zijn van $\mathbf{C}_3$ met $\mathbf{C}_4$, een begrip dat we pas in de cursus “Algebra II” zullen invoeren. Zie echter ook Oefening 99 op p. 70.

Definitie 1.10.9. Zij $\mathbf{T}$ de groep van orde 12 met onderliggende verzameling $\mathbb{Z}/3 \times \mathbb{Z}/4$, en met bewerking gegeven door

$$(x, y) \bullet (z, w) := \begin{cases} (x + z, y + w) & \text{als } y \in \{0, 2\}, \\ (x + 2z, y + w) & \text{als } y \in \{1, 3\}. \end{cases}$$

Ga zelf na dat $\mathbf{T}$ inderdaad een groep definieert, dat het element $\hat{g} := (1, 2)$ orde 6 heeft, dat $\hat{h} := (0, 1)$ orde 4 heeft, en dat $\hat{h}^2 = \hat{g}^3$ en $\hat{g}\hat{h} = \hat{h}\hat{g}^{-1}$.

Lemma 1.10.10. Zij G een groep van orde 12, en veronderstel dat $G = \langle g, h \rangle$ met $o(g) = 6$, $o(h) = 4$, $h^2 = g^3$ en $gh = hg^{-1}$. Dan is $G \cong \mathbf{T}$.

Bewijs. Dit volgt onmiddellijk uit Lemma 1.10.2(iii). $\square$

Stelling 1.10.11. Er zijn op isomorfisme na precies vijf groepen van orde 12, met name

$$\mathbf{C}_{12}, \quad \mathbf{C}_6 \times \mathbf{C}_2, \quad \mathbf{D}_{12}, \quad \mathbf{A}_4, \quad \mathbf{T}.$$

Bewijs. Zij G een groep van orde 12, en veronderstel dat $G \not\cong \mathbf{A}_4$. Uit Lemma 1.10.8 weten we dat G een element g van orde 6 heeft. Stel dus $N = \langle g \rangle \trianglelefteq G$ en zij $h \in G \setminus N$ willekeurig. We passen opnieuw Lemma 1.10.2 toe. Uit Lemma 1.10.2(iv) weten we dat $z := g^3 \in Z(G)$. Wegens Lemma 1.10.2(ii)

hebben we $h^2 = g^i$ voor een zekere $i \in \{0, 1, 2, 3, 4, 5\}$; we maken nu een gevallenonderscheid. Merk hierbij op dat we door eventueel g te vervangen door g^{-1} zonder verlies van algemeenheid kunnen onderstellen dat

$$h^2 \in \{1, g, g^2, g^3\}.$$

Veronderstel eerst dat $h^2 = g$. Dan heeft h orde 12, en dus is $G \cong \mathbf{C}_{12}$.

Veronderstel nu dat $h^2 = g^2$. Dan is $h^3g = hg^3 = g^3h = h^2gh$ en bijgevolg $hg = gh$; hieruit volgt dat $G = \langle g, h \rangle$ abels is. In dat geval is $o(hg^2) = 2$, en $hg^2 \notin N$, dus $G \cong N \times \langle hg^2 \rangle \cong \mathbf{C}_6 \times \mathbf{C}_2$.

Veronderstel vervolgens dat $h^2 = 1$. Merk op dat ook $(hg)^2 \in N$, en als $(hg)^2 \in \{g, g^2, g^4, g^5\}$, dan hebben we opnieuw $G \cong \mathbf{C}_{12}$ of $G \cong \mathbf{C}_6 \times \mathbf{C}_2$. Als echter $(hg)^2 = g^3$, dan is $hgh = g^2$ en dan zijn g en g^2 aan elkaar toegevoegd, wat natuurlijk niet kan. De enige overblijvende mogelijkheid is $(hg)^2 = 1$. In dat geval is $gh = hg^{-1}$. We kunnen opnieuw Gevolg 1.10.3 toepassen om te besluiten dat $G \cong \mathbf{D}_{12}$.

Veronderstel ten slotte dat $h^2 = g^3$. Beschouw opnieuw het element hg , en stel opnieuw vast dat we mogen onderstellen dat $(hg)^2$ gelijk is aan 1 of g^3 . Als $(hg)^2 = 1$ bekomen we op analoge wijze als daarnet dat g en g^2 toegevoegd zouden zijn, wat niet kan. De enige overblijvende mogelijkheid is nu $(hg)^2 = g^3$. Dan is $(hg)^2 = h^2$ en dus $ghg = h$. Uit Lemma 1.10.10 volgt nu dat $G \cong \mathbf{T}$.

Merk tot slot nog op dat $\mathbf{T} \not\cong \mathbf{D}_{12}$, want $\mathbf{T}$ bevat een element van orde 4 maar $\mathbf{D}_{12}$ niet. Hieruit besluiten we dat de vijf mogelijke groepen twee aan twee niet isomorf zijn. $\square$

Opmerking 1.10.12. Door gebruik te maken van de classificatie van de eindige *abelse* groepen (Stelling 3.5.3) zouden op een aantal plaatsen in de bewijzen van deze sectie wat kleine vereenvoudigingen mogelijk geweest zijn.

Oefeningen

- 95.** Toon aan dat de delingsvoorwaarde in Stelling 1.10.5 nodig is, door voorbeelden te geven van niet-cyclische groepen van orde pq met $p < q$ priem, waarbij p wel een deler is van $q - 1$.

orde	#	abelse groepen	niet-abelse groepen
2	1	$\mathbf{C}_2$	
3	1	$\mathbf{C}_3$	
4	2	$\mathbf{C}_4, \mathbf{D}_4 \cong \mathbf{E}_4 = \mathbf{C}_2 \times \mathbf{C}_2$	
5	1	$\mathbf{C}_5$	
6	2	$\mathbf{C}_6$	$\mathbf{D}_6 \cong \mathbf{S}_3$
7	1	$\mathbf{C}_7$	
8	5	$\mathbf{C}_8, \mathbf{C}_4 \times \mathbf{C}_2, \mathbf{E}_8 = \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$	$\mathbf{D}_8, \mathbf{Q}_8$
9	2	$\mathbf{C}_9, \mathbf{E}_9 = \mathbf{C}_3 \times \mathbf{C}_3$	
10	2	$\mathbf{C}_{10}$	$\mathbf{D}_{10}$
11	1	$\mathbf{C}_{11}$	
12	5	$\mathbf{C}_{12}, \mathbf{C}_2 \times \mathbf{C}_6$	$\mathbf{D}_{12}, \mathbf{A}_4, \mathbf{T}$
13	1	$\mathbf{C}_{13}$	
14	2	$\mathbf{C}_{14}$	$\mathbf{D}_{14}$
15	1	$\mathbf{C}_{15}$	

Alle groepen van orde ≤ 15

In dit hoofdstuk gaan we dieper in op de structuur van ringen, waarbij we ons voornamelijk zullen toeleggen op commutatieve ringen met eenheid. De rol die normaaldelers spelen in de groepentheorie wordt hier overgenomen door *idealen* van een ring, en we zullen een aanzienlijk deel van dit hoofdstuk besteden aan de studie hiervan.

Een ander aspect dat de nodige aandacht zal krijgen, is unieke factorisatie. Deze fundamentele eigenschap van de gehele getallen is niet zonder meer geldig in willekeurige ringen, en we zullen dit fenomeen nauwkeurig bestuderen.

2.1 Definitie en voorbeelden

We herhalen eerst de definitie, en geven opnieuw een groot aantal voorbeelden.

Definitie 2.1.1. Een *ring* is een verzameling R met daarop twee bewerkingen

$$R \times R \rightarrow R: (s, t) \mapsto s + t, \quad (\text{optelling})$$

$$R \times R \rightarrow R: (s, t) \mapsto s \cdot t = st, \quad (\text{vermenigvuldiging})$$

met een bijzonder element $0 \in R$ en een bijzonder element $1 \in R$ (met niet noodzakelijk $1 \neq 0$!) met de volgende eigenschappen:

- $(R, +)$ is een abelse groep met neutraal element 0 , die we *de additieve groep van R* noemen;
- de vermenigvuldiging is associatief:

$$a(bc) = (ab)c \quad \text{voor alle } a, b, c \in R;$$

- de vermenigvuldiging heeft neutraal element 1 , i.e.

$$1 \cdot a = a = a \cdot 1 \quad \text{voor alle } a \in R;$$

- de vermenigvuldiging en de optelling hebben de links- en rechtsdistributieve eigenschappen:

$$a(b + c) = ab + ac \quad \text{en} \quad (a + b)c = ac + bc \quad \text{voor alle } a, b, c \in R.$$

Het element $1 \in R$ noemen we *de eenheid in R* , *het eenheidselement van R* of de *multiplicatieve identiteit in R* . Het element $0 \in R$ heeft geen bijzondere naam; we verwijzen ernaar als *de nul in R* .

Opmerking 2.1.2. (i) Sommige auteurs eisen niet dat de vermenigvuldiging een neutraal element $1 \in R$ heeft, en verwijzen dan naar de bovenstaande structuren als een *ring met eenheid* of een *ring met 1*. In deze cursus zijn ringen altijd met eenheid ondersteld, tenzij expliciet anders vermeld. De “ringen zonder eenheid” worden soms *rngen*¹ genoemd.

- (ii) De vermenigvuldiging is associatief en heeft een neutraal element, maar de elementen van R zijn niet noodzakelijk inverteerbaar voor deze bewerking. Een dergelijke structuur $(R, \cdot)$ wordt een *monoïde* genoemd.

Definitie 2.1.3. (i) Als de vermenigvuldiging commutatief is, d.w.z. als

$$ab = ba \quad \text{voor alle } a, b \in R,$$

dan noemen we R een *commutatieve ring*.

- (ii) Zij R een ring. Als er voor een gegeven element $a \in R$ een element $b \in R$ bestaat zodat $ab = 1 = ba$, dan noemen we b het *invers element van a* of *de inverse van a* , en we noteren dit element als $b = a^{-1}$. Als een element $a \in R$ een inverse heeft, dan noemen we dat element *een eenheid*² in R .

De verzameling van alle eenheden in R vormt een groep, die we als $R^\times$ noteren, en die we *de groep der eenheden in R* noemen.

- (iii) Als R een ring is zodat $R^\times = R \setminus \{0\}$, dan noemen we R een *lichaam*. Soms wordt ook de term *delingsring* gebruikt, hoewel vele auteurs dit voorbehouden voor lichamen die eindig-dimensionaal zijn over hun centrum.

¹Het begrip *rng* is afkomstig vanuit het Engels: “rings without identity” wordt “rings without i” en dus “rng”. Het wordt uitgesproken als het Engelse *rung*. De term zou afkomstig zijn van Louis Rowen.

²Niet te verwarren met *de eenheid in R* , hetgeen steeds slaat op het element 1. In het bijzonder is de eenheid steeds een eenheid.

- (iv) Een commutatief lichaam noemen we een *veld*³.
- (v) Zij R een willekeurige ring. Een element $r \in R$ waarvoor $r \cdot s = 0$ of $s \cdot r = 0$ voor een zeker element $s \in R \setminus \{0\}$, noemen we een (*linkse resp. rechtse*) *nuldeeler*. Een commutatieve ring met 1 zonder nuldelers⁴ noemen we een *integraal domein*, *integriteitsdomein*, *integriteitsgebied*, of kortweg *domein*. Soms wordt de term domein ook gebruikt voor willekeurige (niet noodzakelijk commutatieve) ringen met deze eigenschap, en soms eist men niet dat de ring een 1 heeft. Gelukkig blijkt meestal wel uit de context welk van deze conventies de auteur hanteert.
- (vi) Zij R een willekeurige ring en zij $r \in R$. We noemen r *idempotent* als $r^2 = r$, en we noemen r *nilpotent* als er een $n \in \mathbb{N}^*$ bestaat zodat $r^n = 0$. Merk op dat idempotente en nilpotente elementen altijd nuldelers zijn. Als r idempotent is, dan is ook $1 - r$ idempotent, en $r(1 - r) = 0$.

Voorbeelden 2.1.4. (1) De gehele getallen $\mathbb{Z}$ met de gebruikelijke optelling en vermenigvuldiging vormen een ring. Het is een commutatieve ring (met het getal 1 als eenheid). De enige elementen van $\mathbb{Z}$ die een inverse hebben zijn 1 en -1 ; de groep der eenheden in $\mathbb{Z}$ is dus de groep $\{1, -1\} \cong \mathbf{C}_2$. De ring $\mathbb{Z}$ heeft geen nuldelers, het is dus een domein.

(2) De verzameling van de even getallen $2\mathbb{Z}$ vormt een commutatieve ring zonder eenheid. Uiteraard heeft ook deze ring geen nuldelers.

(3) De *nulring* is de ring die bestaat uit één element. De nulring is een ring met een eenheidselement, namelijk $1 = 0$. Men toont gemakkelijk aan dat dit de enige ring is waarvoor $1 = 0$. Merk op dat de nulring geen veld is.

(4) Zij $m \in \mathbb{N}^*$. De verzameling $\mathbb{Z}/m$ van gehele getallen modulo m vormt een commutatieve ring (met als eenheid de restklasse $1 \pmod{m}$); het is gemakkelijk om na te gaan dat de optelling en de vermenigvuldiging inderdaad goed gedefinieerd zijn. De groep der eenheden van $\mathbb{Z}/m$ is precies de groep $(\mathbb{Z}/m)^\times$ zoals we vroeger gedefinieerd hebben in Voorbeeld 1.1.9(4).

Als m een priemgetal is, dan is $\mathbb{Z}/m$ een veld; als m geen priemgetal is, dan is $\mathbb{Z}/m$ een ring met nuldelers, want als $m = ab$ voor zekere

³Verwarrend genoeg spreekt men in Nederland en vaak ook in Antwerpen over een lichaam waar wij spreken over een veld, en over een *scheef-lichaam* waar wij spreken over een lichaam. Ook in het Engels is de term “field” niet ondubbelzinnig. Vaak gebruikt men de terminologie “commutative field” enerzijds, en “field or skew-field” anderzijds.

⁴Uiteraard is het element 0 zelf een nuldeeler, maar het is zeer gebruikelijk om te spreken over een ring zonder nuldelers waar we in feite een ring zonder niet-nul nuldelers bedoelen. Sommige auteurs verkiezen ook om het element 0 geen nuldeeler te noemen.

$a, b \in \mathbb{N}^* \setminus \{1\}$, dan vormen de restklassen $a \pmod{m}$ en $b \pmod{m}$ twee niet-nul elementen van $\mathbb{Z}/m$ waarvan het product 0 is.

- (5) We hebben reeds gezien in de cursus “Discrete Wiskunde I” dat een eindig veld steeds p^h elementen heeft voor een zeker priemgetal p en een zekere $h \in \mathbb{N}^*$. Omgekeerd is het zo dat er voor elke priemmacht $q = p^h$ precies één veld (op isomorfisme na) bestaat van orde q ; we noteren dit veld als $\mathbb{F}_q$ of ook soms als $\text{GF}(q)$. In de cursus “Algebra II” zullen we zeer uitgebreid aandacht besteden aan de theorie van de velden, en in het bijzonder zullen we dit resultaat over eindige velden op een abstracte en elegante manier kunnen bewijzen.
- (6) Zij R een commutatieve ring, zij $n \in \mathbb{N}^*$, en beschouw de verzameling $\text{Mat}_n(R)$ van alle $(n \times n)$ -matrices over de ring R , met de gebruikelijke optelling en vermenigvuldiging. Dan vormt $\text{Mat}_n(R)$ een ring. Als $n = 1$ is deze ring uiteraard isomorf⁵ met de ring R zelf. Zodra $n \geq 2$, is de ring $\text{Mat}_n(R)$ een niet-commutatieve ring met nuldelers. De groep der eenheden in $\text{Mat}_n(R)$ noteren we als $\text{GL}_n(R)$, en noemen we de *algemene lineaire groep van graad n over R* . We zullen verderop nog terugkomen op deze ring (zie Definitie 3.3.1 en het vervolg).
- (7) Zij $(R, +, \cdot)$ een commutatieve ring en $r \in R$ een idempotent element. Dan is $(rR, +, \cdot)$ een commutatieve ring met eenheid r .
- (8) Zij X een willekeurige verzameling, en beschouw de machtsverzameling $R = \mathcal{P}(X)$ van X , i.e. de verzameling van alle deelverzamelingen van X . Definieer een optelling op R als het *symmetrisch verschil*, en een vermenigvuldiging op R als de *doorsnede*, i.e.

$$\begin{aligned} a + b &:= a \triangle b = (a \cup b) \setminus (a \cap b), \\ a \cdot b &:= a \cap b, \end{aligned}$$

voor alle $a, b \in R$. Dan is R een commutatieve ring, met $0_R = \emptyset$ en $1_R = X$. Bovendien is elk element van R idempotent; we noemen een dergelijke ring een *Booleaanse ring*. Ook is elk element van $R \setminus \{1\}$ een nuldeeler.

- (9) Er bestaan ringen met elementen die wel een linkse nuldeeler zijn maar geen rechtse nuldeeler zijn. Beschouw bijvoorbeeld de ring R met onderliggende verzameling $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/2$, met componentsgewijze optelling, en met vermenigvuldiging gegeven door

$$(a, b, s) \cdot (c, d, t) := (ac, bd, at + sd \pmod{2})$$

⁵We hebben het concept “ringisomorfisme” nog niet formeel ingevoerd, maar het moge duidelijk zijn wat we bedoelen.

voor alle $a, b, c, d \in \mathbb{Z}$ en $s, t \in \mathbb{Z}/2$. (Ga zelf na dit inderdaad een ring definieert.) Dan is het element $(2, 1, 0)$ een linkse nuldeeler maar geen rechtse nuldeeler.

- (10) Zij R een commutatieve ring. Een polynoom in x met coëfficiënten in R is een uitdrukking van de vorm

$$a_n x^n + \cdots + a_1 x + a_0,$$

met alle $a_i \in R$. De verzameling van alle polynomen in x met coëfficiënten in R noteren we als $R[x]$. Het is dikwijls nuttig om een algemeen polynoom f te noteren als

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

waarbij we dus de coëfficiëntenrij verder aanvullen met nullen; er zijn dus slechts eindig veel van de coëfficiënten a_i verschillend van nul. We definiëren nu een optelling en vermenigvuldiging op $R[x]$ op de gebruikelijke manier: stel $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ en $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots$, dan stellen we

$$\begin{aligned} (f + g)(x) &:= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots \\ &= \sum_k (a_k + b_k)x^k; \\ (f \cdot g)(x) &:= p_0 + p_1 x + p_2 x^2 + \cdots, \text{ waarbij} \\ p_k &= a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j. \end{aligned}$$

De verzameling $R[x]$ uitgerust met deze twee bewerkingen is zelf opnieuw een commutatieve ring. Als R een domein is, dan is ook $R[x]$ een domein. De eenheden in $R[x]$ zijn dan precies de eenheden in R ; in het bijzonder geval dat R een veld is, zijn de eenheden dus precies de polynomen van graad 0.

- (11) Zij R een commutatieve ring. Een *formele machtreeks* in x met coëfficiënten in R is een uitdrukking van de vorm

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

waarbij we nu expliciet toelaten dat er oneindig veel van de coëfficiënten a_i verschillend van nul zijn. De verzameling van alle formele machtreeksen in x met coëfficiënten in R noteren we als $R[[x]]$. We definiëren opnieuw een optelling en vermenigvuldiging op $R[[x]]$ op de gebruikelijke

manier; de verzameling $R[[x]]$ uitgerust met deze twee bewerkingen is dan opnieuw een commutatieve ring. Als R een domein is, dan is ook $R[[x]]$ een domein. Er zijn veel meer eenheden in $R[[x]]$ dan in $R[x]$: een element $f(x) = a_0 + a_1x + a_2x^2 + \dots \in R[[x]]$ is een eenheid als en slechts als a_0 een eenheid is in R .

- (12) We kunnen beide voorgaande voorbeelden uitbreiden door ook een eindig aantal negatieve machten van x toe te laten. Een *Laurent polynoom* in x met coëfficiënten in R is een uitdrukking van de vorm

$$f(x) = \sum_{k=N}^M a_k x^k$$

voor zekere $N, M \in \mathbb{Z}$, en de verzameling van alle Laurent polynomen vormt opnieuw een ring, die we noteren als $R[x, x^{-1}]$. Een *formele Laurent reeks* in x met coëfficiënten in R is een uitdrukking van de vorm

$$f(x) = \sum_{k=N}^{\infty} a_k x^k$$

voor zekere $N \in \mathbb{Z}$, en de verzameling van alle formele Laurent reeksen vormt opnieuw een ring, die we noteren als $R((x))$. Indien R een veld is, dan is ook $R((x))$ een veld.

- (13) Polynomen zijn van fundamenteel belang in de ringtheorie, en het is noodzakelijk om ook polynomen in meerdere variabelen te beschouwen. Mits de juiste notatie is er geen fundamenteel verschil met polynomen in één variabele.

Veronderstel dus dat $x_1, \dots, x_n$ variabelen zijn. Een *monoom* is een formeel product van deze variabelen, van de vorm $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, waarbij de exponenten α_i gehele getallen ≥ 0 zijn. Het n -tupel $\alpha := (\alpha_1, \dots, \alpha_n)$ noemen we een *multi-index*, en we noteren een algemeen monoom als

$$\mathbf{x}^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Het monoom $\mathbf{x}^0 = x_1^0 \cdots x_n^0$ noteren we als 1. Een *polynoom* in de variabelen $x_1, \dots, x_n$ met coëfficiënten in R is dan een eindige lineaire combinatie van monomen, met coëfficiënten in R , en kunnen we dus kort noteren als

$$f(\mathbf{x}) = f(x_1, \dots, x_n) = \sum_{\alpha} a_{\alpha} \mathbf{x}^{\alpha},$$

waarbij α over alle multi-indices loopt, en waarbij slechts eindig veel a_{α} 's verschillend zijn van nul.

De optelling en vermenigvuldiging van polynomen in meerdere variabelen wordt gegeven door precies dezelfde formules als bij één variabele, maar waarbij de sommaties nu lopen over multi-indices:

$$(f + g)(\mathbf{x}) := \sum_{\alpha} (a_{\alpha} + b_{\alpha}) \mathbf{x}^{\alpha};$$

$$(f \cdot g)(\mathbf{x}) := \sum_{\gamma} \left(\sum_{\alpha + \beta = \gamma} a_{\alpha} b_{\beta} \right) \mathbf{x}^{\gamma}.$$

De verzameling van alle polynomen over R in de variabelen $x_1, \dots, x_n$ noteren we als $R[x_1, \dots, x_n]$, of ook soms kort als $R[\mathbf{x}]$; uitgerust met bovenstaande optelling en vermenigvuldiging vormt deze verzameling opnieuw een commutatieve ring.

Op analoge wijze kunnen we ook de ring $R[[x_1, \dots, x_n]]$ van formele machtreksen in meerdere variabelen definiëren. (Werk zelf de details uit.)

- (14) We geven een voorbeeld van een lichaam dat geen veld is. We vertrekken van het veld $\mathbb{C}$ der complexe getallen, en we beschouwen de verzameling

$$\mathbb{H} := \{(a, b) \mid a, b \in \mathbb{C}\},$$

uitgerust met de bewerkingen

$$(a, b) + (c, d) := (a + c, b + d),$$

$$(a, b) \cdot (c, d) := (ac - b\bar{d}, ad + b\bar{c}),$$

waarbij $\bar{d}$ staat voor de complex toegevoegde van d . Men gaat gemakkelijk na dat $\mathbb{H}$ een ring is, met $0 = (0, 0)$ en $1 = (1, 0)$ (doe dit zelf als oefening). Bovendien is elk niet-nul element $(a, b) \in \mathbb{H}$ een eenheid; we hebben

$$(a, b)^{-1} = \left(\frac{\bar{a}}{a\bar{a} + b\bar{b}}, \frac{-b}{a\bar{a} + b\bar{b}} \right).$$

(Merk op dat de noemers $a\bar{a} + b\bar{b}$ nooit nul zijn.) Dit bewijst dat $\mathbb{H}$ een lichaam is. Anderzijds is $\mathbb{H}$ geen veld, omdat bijvoorbeeld $(i, 0)$ en $(0, 1)$ niet commuteren. We noemen $\mathbb{H}$ het *lichaam van de reële quaternionen*.

We tonen nu enkele elementaire eigenschappen aan voor willekeurige ringen. Geen van deze eigenschappen is verrassend, maar toch vraagt het wat nauwkeurigheid om ze uit de definiërende eigenschappen af te leiden.

Lemma 2.1.5. *Zij R een ring.*

- (i) *Het element $1 \in R$ is het unieke element van R dat voldoet aan $1 \cdot r = r = r \cdot 1$ voor alle $r \in R$.*

- (ii) Het element $0 \in R$ voldoet aan $0 \cdot r = 0 = r \cdot 0$ voor alle $r \in R$; bovendien is het het unieke element van R dat hieraan voldoet voor alle $r \in R$.
- (iii) Zij -1 de additieve inverse van 1 . Dan geldt voor elke $r \in R$ dat $(-1) \cdot r = -r = r \cdot (-1)$, waarbij $-r$ zoals gewoonlijk de additieve inverse van r is.
- (iv) Voor alle $x, y \in R$ geldt $(-x) \cdot (-y) = xy$.

Bewijs. Oefening. □

In willekeurige ringen hebben we geen schrappingswet voor de vermenigvuldiging. In domeinen geldt dit wel, en we zullen dit later vaak gebruiken:

Lemma 2.1.6. *Zij R een domein, en zij $a, b, c \in R$. Als $ab = ac$ en $a \neq 0$, dan is $b = c$.*

Bewijs. Uit $ab = ac$ volgt dat $a(b - c) = 0$. Aangezien $a \neq 0$ en R geen nuldelers heeft, besluiten we dat $b - c = 0$ en dus $b = c$. □

Oefeningen

- 96. Zij R een commutatieve ring, en zij $r \in R$ een nilpotent element. Toon aan dat $1 + r$ een eenheid is in R .
- 97. Geef een voorbeeld van een geheel getal n zodat $\mathbb{Z}/n$ ten minste 4 verschillende idempotente elementen heeft.
- 98. Beschouw het lichaam $\mathbb{H}$ der reële quaternionen, en beschouw de elementen

$$\begin{aligned} 1 &:= (1, 0), & i &:= (i, 0), & j &:= (0, 1), & k &:= (0, i), \\ -1 &:= (-1, 0), & -i &:= (-i, 0), & -j &:= (0, -1), & -k &:= (0, -i). \end{aligned}$$

Toon aan dat deze acht elementen, met de vermenigvuldiging in $\mathbb{H}$ als groepswerking, precies de quaternionengroep $\mathbf{Q}_8$ vormen.

- 99. Zij $n \geq 1$ een geheel getal. Stel $a := e^{i\pi/n} = \cos \pi/n + i \sin \pi/n \in \mathbb{H}$, en definieer de *dicyclische groep* van orde $4n$ als de deelgroep

$$\mathbf{Dic}_{4n} := \langle a, j \rangle \leq \mathbb{H}^\times.$$

Toon aan dat $\mathbf{Dic}_{4n}$ inderdaad een groep is van orde $4n$, die niet-abels is zodra $n \geq 2$. Toon verder aan dat $\mathbf{Dic}_4 \cong \mathbf{C}_4$, dat $\mathbf{Dic}_8 \cong \mathbf{Q}_8$, en dat $\mathbf{Dic}_{12} \cong \mathbf{T}$, waarbij $\mathbf{T}$ de groep is die werd ingevoerd in Definitie 1.10.9.

2.2 Ringmorfismen

Net zoals groepsmorfismen een belangrijke rol spelen in de groepentheorie, zo spelen ringmorfismen een belangrijke rol in de ringtheorie.

Definitie 2.2.1. Zij R, S twee ringen. Een afbeelding

$$\theta: R \rightarrow S$$

is een *morfisme* (ook *homomorfisme* of *ringmorfisme* genoemd) als θ de ringstructuur bewaart, in de zin dat

$$\theta(r + r') = \theta(r) + \theta(r'), \quad \theta(rr') = \theta(r)\theta(r') \quad \text{en} \quad \theta(1_R) = 1_S$$

voor alle $r, r' \in R$. We noemen θ een *epimorfisme* als het surjectief is, een *monomorfisme* als het injectief is, en een *isomorfisme* als het bijectief is. De inverse afbeelding van een isomorfisme is ook zelf weer een morfisme (en dus een isomorfisme).

Als θ een morfisme is van R naar S , dan definiëren we de *kern van θ* als

$$\ker(\theta) := \{r \in R \mid \theta(r) = 0\},$$

en het *beeld van θ* als

$$\text{im}(\theta) := \{\theta(r) \mid r \in R\}.$$

Opmerking 2.2.2. (i) In tegenstelling tot de schrijfwijze die we bij groepen hebben gebruikt, zullen we ringmorfismen meestal functioneel noteren (en dus niet exponentieel).

(ii) Merk op dat een ringmorfisme $\theta: R \rightarrow S$ een groepsmorfisme induceert tussen de onderliggende additieve groepen, $\theta_+: (R, +) \rightarrow (S, +)$. In het bijzonder is steeds $\theta(0_R) = 0_S$. Merk ook op dat $\ker(\theta) = \ker(\theta_+)$ en $\text{im}(\theta) = \text{im}(\theta_+)$ (als verzameling).

(iii) We kunnen ook *rngmorfismen* definiëren, die enkel de bewerkingen $+$ en $\cdot$ bewaren, maar niet noodzakelijk de eenheid bewaren. Ook als de ringen R en S zelf een eenheid hebben, kunnen er rngmorfismen bestaan die geen ringmorfismen zijn.

Beschouw bijvoorbeeld $R = \mathbb{Q}$ en $S = \text{Mat}_2(\mathbb{Q})$, en stel

$$\theta: R \rightarrow S: x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}.$$

Dan is θ een rngmorfisme, maar $\theta(1)$ is niet gelijk aan het eenheidselement van $\text{Mat}_2(\mathbb{Q})$, dat $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is.

Voorbeelden 2.2.3. (1) Zij R een willekeurige ring. Dan is er een uniek ringmorfisme $\theta: \mathbb{Z} \rightarrow R$. Meer bepaald is

$$\theta(x) := \begin{cases} 0 & \text{als } x = 0; \\ 1_R + \cdots + 1_R \text{ (} x \text{ keer)} & \text{als } x > 0; \\ -1_R - \cdots - 1_R \text{ (} |x| \text{ keer)} & \text{als } x < 0. \end{cases}$$

Men gaat eenvoudig na dat dit inderdaad een morfisme is. De uniciteit is ook duidelijk, want $\mathbb{Z}$ wordt als ring voortgebracht door het element $1 \in \mathbb{Z}$, en dus ligt een ringmorfisme van $\mathbb{Z}$ naar een andere ring volledig vast van zodra het beeld van het element $1 \in \mathbb{Z}$ vast ligt; maar $\theta(1) = 1_R$.

(2) Zij $m \in \mathbb{N}^*$, en stel $R = \mathbb{Z}/m$ in het vorige voorbeeld. Het corresponderend ringmorfisme

$$\theta: \mathbb{Z} \rightarrow \mathbb{Z}/m$$

beeldt elk element $x \in \mathbb{Z}$ af op zijn restklasse modulo m . We noemen dit morfisme de *restrictie modulo m* . Het is gebruikelijk om het beeld van een element $x \in \mathbb{Z}$ onder dit morfisme te noteren als $\bar{x}$ indien het getal m duidelijk is uit de context.

Een interessante klasse van morfismen zijn de *substitutiemorfismen*, die gegeven worden door de volgende stelling.

Stelling 2.2.4 (Substitutieprincipe). *Zij R, S twee commutatieve ringen met eenheid, en zij $\theta: R \rightarrow S$ een ringmorfisme.*

- (i) *Gegeven is een element $s \in S$. Dan is er een uniek ringmorfisme $\Phi: R[x] \rightarrow S$, dat samenvalt met θ op de constante polynomen (i.e. op $R \subseteq R[x]$), en dat x op s afbeeldt.*
- (ii) *Gegeven zijn elementen $s_1, \dots, s_n \in S$. Dan is er een uniek ringmorfisme $\Phi: R[x_1, \dots, x_n] \rightarrow S$, dat samenvalt met θ op de constante polynomen, en dat elke x_k op de overeenkomstige s_k afbeeldt.*

Bewijs. We hoeven enkel (i) te bewijzen; het bewijs van (ii) volgt dan per inductie op n .

Zij dus $s \in S$ willekeurig, en definieer de afbeelding

$$\varphi: R[x] \rightarrow S: \sum_i r_i x^i \mapsto \sum_i \theta(r_i) s^i.$$

Merk op dat $\varphi(x) = s$ omdat $\theta(1) = 1$. We gaan na dat φ een ringmorfisme is; het is duidelijk dat het de optelling bewaart en de 1 bewaart. Stel nu $f, g \in R[x]$ willekeurig, en schrijf $f = \sum_i a_i x^i$ en $g = \sum_j b_j x^j$. Dan is

$$\begin{aligned}\varphi(fg) &= \varphi\left(\sum a_i b_j x^{i+j}\right) = \sum \varphi(a_i b_j x^{i+j}) = \sum \theta(a_i b_j) s^{i+j} \\ &= \sum \theta(a_i) \theta(b_j) s^{i+j} = \left(\sum_i \theta(a_i) s^i\right) \left(\sum_j \theta(b_j) s^j\right) = \varphi(f) \varphi(g).\end{aligned}$$

Dit toont aan dat φ inderdaad een ringmorfisme is, en het voldoet aan de gestelde eigenschappen.

Anderzijds is het duidelijk dat dit het enige morfisme kan zijn dat hieraan voldoet, omdat de ring $R[x]$ als ring wordt voortgebracht door $R \subset R[x]$ en het element $x \in R[x]$. $\square$

Voorbeelden 2.2.5. (1) Een interessant bijzonder geval is wanneer we vertrekken van het identiteitsmorfisme $\theta: R \rightarrow R: r \mapsto r$. Kies dus een $s \in R$ willekeurig; dan is het corresponderend substitutiemorfisme gegeven door

$$\Phi: R[x] \rightarrow R: f(x) \mapsto f(s).$$

We noemen het in dit geval ook wel een *evaluatiemorfisme*, en het wordt soms genoteerd als $\Phi = \text{eval}_s$.

(2) Beschouw nu een willekeurig ringmorfisme $\varphi: R \rightarrow S$, en beschouw het geïnduceerd morfisme $\theta: R \rightarrow S[x]$ met $\theta = \text{inc} \circ \varphi$, waarbij inc de inclusie is van S in $S[x]$. Kies nu $s = x \in S[x]$. Dan is het corresponderend substitutiemorfisme gegeven door

$$\begin{aligned}\Phi: R[x] \rightarrow S[x]: a_0 + a_1 x + \cdots + a_k x^k \\ \mapsto \varphi(a_0) + \varphi(a_1) x + \cdots + \varphi(a_k) x^k.\end{aligned}$$

(3) We passen nu voorgaand voorbeeld toe op het morfisme $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}/m$ uit Voorbeeld 2.2.3(2). Dan is het corresponderend substitutiemorfisme gegeven door

$$\Phi: \mathbb{Z}[x] \rightarrow (\mathbb{Z}/m)[x]: a_0 + a_1 x + \cdots + a_k x^k \mapsto \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_k} x^k.$$

Als $f \in \mathbb{Z}[x]$, dan noteren we $\Phi(f)$ ook als $\overline{f}$, en we noemen dit de *restrictie van f modulo m* .

Oefeningen

- 100.** Beschouw twee ringen R en S , en zij $\theta: R \rightarrow S$ een ringmorfisme. Toon aan dat $\theta(1_R)$ een idempotent element in S is.
- 101.** (a) Beschouw de afbeelding $\alpha: \mathbb{R}[x, y] \rightarrow \mathbb{R}$ die $f(x, y)$ afbeeldt op $f(0, 0)$. Toon aan dat α een morfisme is, en bepaal $\ker(\alpha)$.

- (b) Beschouw de afbeelding $\beta: \mathbb{R}[x] \rightarrow \mathbb{C}$ die $f(x)$ afbeeldt op $f(1 + \sqrt{2})$. Toon aan dat β een morfisme is, en bepaal $\ker(\beta)$.
102. Zij p een priemgetal en $R = (\mathbb{Z}/p)[x]$. Beschouw de afbeelding $\varphi: R \rightarrow R: f \mapsto f^p$. Toon aan dat φ een morfisme is. (Dit morfisme wordt het *Frobenius-morfisme* van R genoemd.)
103. Zij R een ring, en zij $f(y) \in R[y]$. Toon aan dat de afbeelding $\theta: R[x, y] \rightarrow R[x, y]$ gedefinieerd door $\theta(x) = x + f(y)$ en $\theta(y) = y$, een automorfisme is van $R[x, y]$.
-

2.3 Idealen

We zullen vanaf nu enkel werken met *commutatieve ringen*. Heel wat van de begrippen die we zullen invoeren, kunnen ook gedefinieerd worden voor willekeurige ringen, maar vaak met bijkomende specificaties (bv. linkszijdige, rechtszijdige en tweezijdige idealen); ook heel wat van de resultaten die we zullen aantonen zijn niet langer geldig voor niet-commutatieve ringen.

Vanaf nu zullen we kortweg spreken van een “ring” wanneer we een commutatieve ring (met eenheid) bedoelen.

Definitie 2.3.1. Zij R een ring.

- (1) Een *deelring* van R is een additieve deelgroep S van R die tevens gesloten is onder de vermenigvuldiging van R , en die het element $1 \in R$ bevat.
- (2) Een *ideaal* in R is een additieve deelgroep I van R zodanig dat $aR \subseteq I$ voor alle $a \in I$. We noteren dit als $I \trianglelefteq R$.

Zoals de notatie al doet uitschijnen, zullen idealen in een ring een vergelijkbare rol spelen als normaaldelers in een groep, hoewel het behoorlijk verschillende noties zijn.

Voorbeelden 2.3.2. (1) De ring $\mathbb{Z}$ is een deelring van $\mathbb{Q}$, en is ook een deelring van $\mathbb{Z}[x]$.

- (2) In elke ring R zijn $I = \{0\}$ en $I = R$ idealen. Een ideaal I wordt *echt* of *eigenlijk* genoemd als $I \neq R$. (Sommige auteurs veronderstellen bovendien dat $I \neq \{0\}$, maar dit is niet zo gebruikelijk.) Het ideaal $I = \{0\}$ noemen we het *triviaal ideaal* of het *nulideaal*, en we noteren het gemakshalve vaak als $I = 0$.

- (3) Zij $R = \mathbb{Z}$, en $m \in \mathbb{N}$. Dan is $I = m\mathbb{Z}$ een ideaal in R .

- (4) Zij K een veld, en $R = K[x]$. Beschouw een vast polynoom $f \in R$, en stel I gelijk aan de verzameling van alle polynomen die deelbaar zijn door f . Dan is I een ideaal in R .
- (5) Zij $R = \mathbb{Z}[x]$ en stel I gelijk aan de verzameling van alle polynomen waarvan de constante term even is. Dan is I een ideaal in R .

Lemma 2.3.3. *Zij R een ring en $I \trianglelefteq R$. Als I een eenheid bevat, dan is $I = R$. In het bijzonder bevat een veld geen echte niet-nul idealen.*

Bewijs. Zij $u \in I$ een eenheid. Voor een willekeurige $r \in R$ hebben we nu $r = u \cdot (u^{-1}r) \in uR \subseteq I$. Dus $R = I$. $\square$

Definitie 2.3.4. Als I en J twee idealen zijn van een ring R , dan definiëren we de *som* van I en J als

$$I + J := \{x + y \mid x \in I, y \in J\},$$

en het *product* van I en J als

$$I \cdot J := IJ := \left\{ \sum_{i=1}^N x_i y_i \mid x_i \in I, y_i \in J, N \in \mathbb{N}^* \right\}.$$

Merk op dat deze definitie verschilt van de definitie van het product van deelverzamelingen van groepen (zie Notatie 1.2.11).

Lemma 2.3.5. *Zij I en J twee idealen in een ring R . Dan is $I + J \trianglelefteq R$, $I \cap J \trianglelefteq R$, en $IJ \trianglelefteq R$. Bovendien geldt steeds $IJ \subseteq I \cap J$.*

Bewijs. Het is duidelijk dat zowel $I + J$, $I \cap J$ als IJ opnieuw additieve deelgroepen zijn van R . (Voor IJ is het feit dat we *sommen* van producten van elementen van I en J nemen, essentieel.)

Beschouw nu een willekeurig element $x + y \in I + J$, met $x \in I$ en $y \in J$. Dan geldt voor elke $r \in R$ dat $(x + y)r = xr + yr \in I + J$, en dus is $I + J \trianglelefteq R$.

Vervolgens beschouwen we een willekeurig element $a = \sum_i x_i y_i \in IJ$, met elke $x_i \in I$ en elke $y_i \in J$. Dan geldt voor elke $r \in R$ dat

$$ar = \sum_i x_i (y_i r) = \sum_i x_i y'_i$$

met $y'_i = y_i r \in J$, en dus $ar \in IJ$. Bijgevolg is $IJ \trianglelefteq R$.

Beschouw ten slotte een willekeurig element $x \in I \cap J$; dan geldt voor elke $r \in R$ dat $xr \in I$ omdat $I \trianglelefteq R$ en $xr \in J$ omdat $J \trianglelefteq R$, en dus $xr \in I \cap J$; bijgevolg is $I \cap J \trianglelefteq R$.

Om de laatste uitspraak te bewijzen, volstaat het om te bewijzen dat $xy \in I \cap J$ voor alle $x \in I$ en alle $y \in J$. Dit volgt echter onmiddellijk uit $xy \in xR \subseteq I$ en $xy \in yR \subseteq J$. $\square$

Opmerking 2.3.6. Voorgaand lemma verklaart ook de op het eerste gezicht eigenaardige definitie van het product van idealen in een ring. Als I en J twee idealen zijn, dan is de verzameling $\{xy \mid x \in I, y \in J\}$ in het algemeen *geen* ideaal; zie Oefening 106.

Definitie 2.3.7. (i) Zij R een ring, en $a_1, \dots, a_k \in R$. Het kleinste ideaal in R dat de elementen $a_1, \dots, a_k$ bevat, noemen we het *ideaal voortgebracht door $a_1, \dots, a_k$* , en noteren we als $I = (a_1, \dots, a_k)$, of ook soms als $I = \langle a_1, \dots, a_k \rangle$.

(ii) Een ideaal $I = (a)$ voortgebracht door één element $a \in R$ noemen we een *hoofdideaal*, of meer bepaald *het hoofdideaal voortgebracht door a* .

Het ideaal voortgebracht door een aantal elementen is gemakkelijk expliciet te omschrijven, zoals zal blijken uit het volgend lemma. Dit wil echter nog niet zeggen dat het ook gemakkelijk te bepalen is: zo is het (in een precieze wiskundige zin) al een heel moeilijk probleem om te bepalen of een ideaal $I = (a_1, \dots, a_k)$ gelijk is aan de volledige ring R ! Dit soort van probleemstellingen maken deel uit van de *computeralgebra*⁶, en vallen buiten het raam van deze cursus.

Lemma 2.3.8. *Zij R een ring, en $a_1, \dots, a_k \in R$. Dan is*

$$(a_1, \dots, a_k) = a_1R + \dots + a_kR = \{a_1r_1 + \dots + a_kr_k \mid r_1, \dots, r_k \in R\}.$$

Bewijs. Stel $J = a_1R + \dots + a_kR$. Het is duidelijk dat J een additieve deelgroep van $(R, +)$ is die de gegeven elementen $a_1, \dots, a_k$ bevat. Bovendien is J een ideaal van R , want stel $j = a_1r_1 + \dots + a_kr_k$ en $r \in R$ willekeurig, dan is $jr = a_1(r_1r) + \dots + a_k(r_kr) \in J$.

Zij nu I een willekeurig ideaal van R dat $a_1, \dots, a_k$ bevat. Per definitie moet dan $a_iR \subseteq I$ voor elke i , en omdat I een additieve deelgroep is volgt hieruit dat $J \subseteq I$. Dus J is het kleinste ideaal van R dat $a_1, \dots, a_k$ bevat. $\square$

Oefeningen

104. Zij R een ring, en $a, a_1, \dots, a_n, b, b_1, \dots, b_m \in R$. Toon aan dat $(a)(b) = (ab)$. Toon vervolgens aan dat algemener geldt dat

$$(a_1, \dots, a_n)(b_1, \dots, b_m) = (a_ib_j \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}).$$

105. Het *nilradicaal* N van een ring R is de verzameling van nilpotente elementen van R . Bewijs dat N een ideaal is in R . Bepaal het nilradicaal van de ring $\mathbb{Z}/n$.

⁶Voor polynomenringen spelen zogenaamde Gröbner basissen een fundamentele rol in dit soort probleemstellingen.

106. Beschouw de ring $R = \mathbb{Z}[x]$ en de idealen $I = (x, 2)$ en $J = (x, 3)$. Toon aan dat de verzameling $\{ab \mid a \in I, b \in J\}$ geen ideaal is in R .

107. Zij R een ring, en I, J, J' idealen in R . Is $I(J + J') = IJ + IJ'$?

2.4 Hoofdideaaldomeinen en Euclidische domeinen

Definitie 2.4.1. Een domein waarin elk ideaal een hoofdideaal is, noemen we een *hoofdideaaldomein*, of kortweg een *PID* (van het Engelse “principal ideal domain”).

Een belangrijke klasse van PID's zijn de zogenaamde Euclidische domeinen, dit zijn domeinen waarin we beschikken over het delingsalgoritme van Euclides:

Definitie 2.4.2. Een domein R wordt een *Euclidisch domein* genoemd, als er een functie

$$d: R \setminus \{0\} \rightarrow \mathbb{N}$$

bestaat (die we de *Euclidische functie* van R noemen), zodat voor alle $a, b \in R$ met $a \neq 0$ er elementen $q, r \in R$ bestaan zodat

$$b = aq + r, \quad \text{en ofwel } r = 0 \quad \text{ofwel } d(r) < d(a).$$

We eisen *niet* dat q en r uniek bepaald zijn door a en b .

We geven zo dadelijk een aantal voorbeelden van Euclidische domeinen, maar eerst tonen we aan dat dit inderdaad PID's zijn.

Stelling 2.4.3. *Elk Euclidisch domein is een hoofdideaaldomein.*

Bewijs. Zij R een Euclidisch domein met Euclidische functie d , en zij $I \trianglelefteq R$ een willekeurig ideaal met $I \neq 0$. Kies een element $a \in I$ met $a \neq 0$ waarvoor $d(a)$ minimaal is; we beweren dat $I = (a)$. Zij namelijk $b \in I$ willekeurig. Omdat R Euclidisch is, kunnen we $b = aq + r$ schrijven, met ofwel $r = 0$, ofwel $d(r) < d(a)$; merk op dat $r = b - aq \in I$. Uit de minimaliteit van $d(a)$ volgt dat de laatste mogelijkheid $d(r) < d(a)$ niet kan, dus is $r = 0$, en bijgevolg $b = aq$; hieruit volgt $b \in (a)$, en dus is $I \subseteq (a)$. Uiteraard is ook $(a) \subseteq I$ omdat $a \in I$, en dus volgt dat I gelijk is aan het hoofdideaal (a) . $\square$

We geven nu enkele voorbeelden van Euclidische domeinen.

Voorbeelden 2.4.4. (1) De ring $\mathbb{Z}$ is een Euclidisch domein, met Euclidische functie

$$d: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}: a \mapsto |a|.$$

(2) Zij K een willekeurig veld. De polynomenring $K[x]$ is een Euclidisch domein, met Euclidische functie

$$d: K[x] \setminus \{0\} \rightarrow \mathbb{N}: f \mapsto \deg(f).$$

(3) We beschouwen de *ring van gehelen van Gauss*

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

(Merk op dat dit een *rooster* is in het complexe vlak. Als abelse groep is dit precies de deelgroep van $(\mathbb{C}, +)$ voortgebracht door de elementen 1 en i .)

Het veld $\mathbb{C}$ der complexe getallen is voorzien van een *normafbeelding*, gegeven door

$$\mathbf{N}: \mathbb{C} \rightarrow \mathbb{R}_{\geq 0}: z = a + bi \mapsto z\bar{z} = (a + bi)(a - bi) = a^2 + b^2.$$

Merk op dat $\mathbf{N}$ multiplicatief is, i.e. voor alle $x, y \in \mathbb{C}$ geldt $\mathbf{N}(xy) = \mathbf{N}(x)\mathbf{N}(y)$. Stel nu d gelijk aan de restrictie van $\mathbf{N}$ tot $\mathbb{Z}[i]$, dus

$$d: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}: a + bi \mapsto a^2 + b^2. \quad (2.1)$$

Stelling 2.4.5. *De ring $\mathbb{Z}[i]$ van gehelen van Gauss is een Euclidisch domein, met Euclidische functie gegeven door (2.1).*

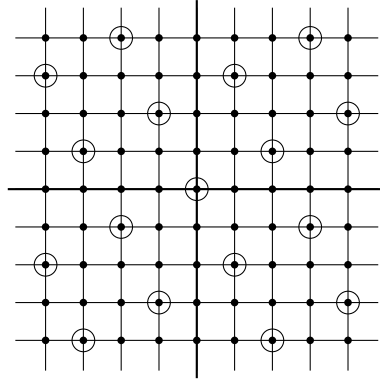
Bewijs. Beschouw $x = a + bi \in \mathbb{Z}[i] \setminus \{0\}$, en $y = c + di \in \mathbb{Z}[i]$. Stel $z = y/x = s + ti$ met $s, t \in \mathbb{R}$ (waarbij we gewoon de deling in $\mathbb{C}$ uitvoeren). Stel nu $q = m + ni$ gelijk aan het element van $\mathbb{Z}[i]$ dat het dichtst bij z ligt in het complexe vlak. (Als er meerdere dichtst gelegen punten zijn, kiezen we er willekeurig één van.) Dan is $z - q = (s - m) + (t - n)i$, en zowel $s - m$ als $t - n$ zijn reële getallen gelegen tussen $-1/2$ en $1/2$. Hieruit volgt

$$\mathbf{N}(y - xq) = \mathbf{N}(x)\mathbf{N}(z - q) \leq \mathbf{N}(x)((1/2)^2 + (1/2)^2) = \mathbf{N}(x)/2 < \mathbf{N}(x).$$

Dit toont aan dat $\mathbf{N}$ een Euclidische functie is voor $\mathbb{Z}[i]$. $\square$

Opmerking 2.4.6. Het is interessant om deze situatie te visualiseren in het complexe vlak. We vertrekken van de elementen van $\mathbb{Z}[i]$ die een vierkant rooster vormen. Het element $x = a + bi$ definieert een hoofdideaal $I = (x)$, en de elementen van I vormen zelf opnieuw een rooster dat gelijkvormig is

met het oorspronkelijke rooster $\mathbb{Z}[i]$. Inderdaad, als we $x = re^{i\theta}$ schrijven, dan verkrijgen we de elementen van (x) door het oorspronkelijke rooster te roteren over een hoek θ en vervolgens uit te rekken met de factor $r = |x|$.



Figuur 2.1: Het rooster $\mathbb{Z}[i]$ en het ideaal $I = (2 + i)$

Aangezien het nieuwe rooster nu een vierkant rooster is met zijdelengte $|x|$, is er voor elk punt in het complexe vlak minstens één punt van dat rooster dat op afstand $\leq \sqrt{2}/2 \cdot |x|$ ligt. Dat punt is precies het element xq uit het voorgaand bewijs; we zien nu ook meetkundig dat

$$N(y - xq) = \text{dist}(y, xq)^2 \leq 1/2 \cdot |x|^2 = N(x)/2.$$

Voorbeeld 2.4.7. (1) Niet elk hoofdideaaldomein is een Euclidisch domein.

Een voorbeeld wordt gegeven door de ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. (Het vergt behoorlijk wat werk om dit te bewijzen.)

(2) Niet elk domein is een hoofdideaaldomein. Een voorbeeld is $\mathbb{Z}[x]$, waarin het ideaal $(2, x)$ geen hoofdideaal is. Merk op dat ditzelfde ideaal $(2, x)$ wél een hoofdideaal is in de ring $\mathbb{Q}[x]$ (het is namelijk gelijk aan $\mathbb{Q}[x]$ zelf, omdat 2 inverteerbaar is).

Een ander voorbeeld is de polynomenring $K[x, y]$ in twee veranderlijken over een veld K , waarin het ideaal (x, y) geen hoofdideaal is.

Een derde voorbeeld is de ring $\mathbb{Z}[\sqrt{-5}]$, waar het ideaal $(2, 1 + \sqrt{-5})$ geen hoofdideaal is.

(3) Voor sommige domeinen is het erg moeilijk om na te gaan of ze al dan niet Euclidisch zijn. Zo werd bijvoorbeeld pas in 2004 bewezen door M. Harper dat $\mathbb{Z}[\sqrt{14}]$ een Euclidisch domein is.

Het belang van hoofdideaaldomeinen zal nog blijken uit het vervolg. Zo zullen we bijvoorbeeld zien dat we in een hoofdideaaldomein steeds unieke factorisatie van elementen hebben (Stelling 2.7.24).

Oefeningen

- 108.** Toon aan dat de ringen $\mathbb{Z}[e^{2\pi i/3}]$ en $\mathbb{Z}[\sqrt{-2}]$ Euclidische domeinen zijn.
- 109.** Zij $a, b \in \mathbb{Z}$, en veronderstel dat $a \mid b$ in $\mathbb{Z}[i]$. Toon aan dat dan $a \mid b$ in $\mathbb{Z}$.
- 110.** Zij R een PID. Toon aan dat er voor elk paar elementen $a, b \in R$, niet beide nul, een element d bestaat met de volgende eigenschappen:
- (i) $d = ar + bs$ voor zekere $r, s \in R$;
 - (ii) $d \mid a$ en $d \mid b$;
 - (iii) als $e \in R$ zodat $e \mid a$ en $e \mid b$, dan ook $e \mid d$.
- Een dergelijk element d noemen we een *grootste gemene deler* van a en b ; toon aan dat het uniek bepaald is op een eenheid na. (We zullen verderop de grootste gemene deler invoeren in een grotere klasse ringen; zie Definitie 2.7.21.)
- 111.** Zoek de grootste gemene deler van $(11 + 7i, 18 - i)$ in $\mathbb{Z}[i]$.
-

2.5 Quotiëntringen

Net zoals we uit een groep en een normaaldeleer een nieuwe groep kunnen construeren, zo kunnen we ook uit een ring en een ideaal een nieuwe ring construeren.

Definitie 2.5.1. Zij R een ring en $I \trianglelefteq R$ een ideaal. Een *nevenklasse* van I definiëren we als een evenklasse van I gezien als deelgroep van $(R, +)$; het is dus een deelverzameling van R van de vorm $r + I = \{r + a \mid a \in I\}$ voor een zekere $r \in R$.

De *quotiëntring* R/I definiëren we als de verzameling van alle nevenklassen van I , met daarop een optelling en een vermenigvuldiging gegeven door

$$\begin{aligned}(r + I) + (s + I) &:= (r + s) + I, \\ (r + I) \cdot (s + I) &:= rs + I.\end{aligned}$$

Het nul-element van R/I is de triviale nevenklasse $0 + I$, en het eenheidselement is $1 + I$.

Lemma 2.5.2. Zij R een ring en $I \trianglelefteq R$ een ideaal. Dan is R/I zoals hierboven gedefinieerd, een (commutatieve) ring.

Bewijs. Oefening. Vergeet niet aan te tonen dat de bewerkingen goed gedefinieerd zijn. $\square$

Net zoals bij groepen hebben we ook hier een natuurlijke projectie-afbeelding.

Lemma 2.5.3. *Zij R een ring en $I \trianglelefteq R$ een ideaal. De afbeelding*

$$\pi: R \rightarrow R/I: r \mapsto r + I$$

is een surjectief ringmorfisme. De kern van dit morfisme is precies I .

Bewijs. Oefening. □

Ook voor ringen geldt de eerste isomorfiestelling.

Stelling 2.5.4 (Eerste isomorfiestelling). *Zij R, S twee ringen, en $\theta: R \rightarrow S$ een ringmorfisme. Dan is $\ker(\theta) \trianglelefteq R$, en*

$$\text{im}(\theta) \cong R/\ker(\theta).$$

Bewijs. Het ringmorfisme θ induceert een groepsmorfisme θ_+ van $(R, +)$ naar $(S, +)$, en $\ker(\theta_+) = \ker(\theta)$. We weten dus reeds dat $\ker(\theta)$ een deelgroep van R is. De kern $\ker(\theta)$ is ook een ideaal, want als $r \in R$ en $a \in \ker(\theta)$, dan is $\theta(ar) = \theta(a)\theta(r) = 0$, en dus is ook $ar \in \ker(\theta)$. We besluiten reeds dat $\ker(\theta) \trianglelefteq R$, en uit de eerste isomorfiestelling voor groepen weten we dat er een *groepsisomorfisme*

$$\alpha: R/\ker(\theta) \rightarrow \text{im}(\theta): r + \ker(\theta) \mapsto \theta(r)$$

is. We moeten enkel nog aantonen dat α ook een *ringmorfisme* is. Dit volgt echter onmiddellijk uit de definitie van α samen met het feit dat θ een ringmorfisme is. □

Opmerking 2.5.5. Net zoals voor groepen kunnen we ook voor ringen de eerste isomorfiestelling interpreteren als de uitspraak dat elk morfisme $\theta: R \rightarrow S$ een decompositie heeft in een projectie (= canonieke surjectie), een isomorfisme, en een inclusie (= canonieke injectie):

$$R \twoheadrightarrow R/\ker(\theta) \xrightarrow{\sim} \text{im}(\theta) \hookrightarrow S.$$

Gevolg 2.5.6. *Zij R een ring. Dan geldt:*

$$\begin{aligned} I \trianglelefteq R &\iff \left[\begin{array}{l} I \text{ is de kern van een ringmorfisme} \\ \text{vertrekkend uit } R \end{array} \right] \\ S \text{ is een quotiënt van } R &\iff \left[\begin{array}{l} S \text{ is het beeld van een ringmorfisme} \\ \text{vertrekkend uit } R \end{array} \right] \end{aligned}$$

Bewijs. Volledig analoog aan het bewijs van Gevolg 1.6.10. $\square$

Voorbeeld 2.5.7. Zij R een ring. We beweren dat $R[x]/(x) \cong R$. Beschouw daartoe het evaluatiemorfisme $\Phi = \text{eval}_0: R[x] \rightarrow R: f(x) \mapsto f(0)$; zie Voorbeeld 2.2.5(1). Dit morfisme is uiteraard surjectief, en de kern van dit morfisme bestaat precies uit de veeltermen $f(x) \in R[x]$ waarvoor $f(0) = 0$, i.e. de veeltermen zonder constante term. Bijgevolg is $\ker(\Phi) = (x)$, en uit de eerste isomorfiestelling volgt nu dat inderdaad $R[x]/(x) \cong R$.

Op analoge wijze volgt dat $R[x]/(x+a) \cong R$ voor elke $a \in R$.

Oefeningen

112. Toon aan dat de ring $\mathbb{Z}[i]/(1+3i)$ isomorf is met de ring $\mathbb{Z}/10$.

113. Bepaal de structuur van de ring $\mathbb{Z}[x]/(x^2+3, p)$, voor de keuzes $p=3$ en $p=5$.

114. Zij R een ring en I, J twee idealen in R . Zij $r \in I \cap J$, en beschouw het element $r + IJ \in R/IJ$. Toon aan dat dit element nilpotent is.

2.6 Maximale idealen en priemidealen

We zullen nu zien hoe we *velden* kunnen maken door een ring uit te delen naar een maximaal ideaal, en *domeinen* door een ring uit te delen naar een priemideaal. Deze constructies zijn van zeer groot belang in de commutatieve algebra.

Definitie 2.6.1. Zij R een ring en $M \trianglelefteq R$ een ideaal. We noemen M een *maximaal ideaal* als $M \neq R$, en als voor elk ideaal $I \trianglelefteq R$ met $M \subseteq I$ geldt dat $I = R$ of $I = M$.

Stelling 2.6.2. Zij R een ring en $I \trianglelefteq R$ een ideaal. Dan is R/I een veld als en slechts als I een maximaal ideaal is.

Bewijs. Veronderstel eerst dat I een maximaal ideaal is. Zij $a + I$ een willekeurig niet-nul element van R/I ; dan is $a \notin I$. Beschouw nu het ideaal $aR + I$; omdat I maximaal is moet $aR + I = R$. In het bijzonder bestaan er een $r \in R$ en een $x \in I$ zodat $ar + x = 1$, en dus is $ar + I = 1 + I$, of nog, $(a + I)(r + I) = 1 + I$. Dit toont aan dat $a + I$ een inverseerbaar element van R/I is; bijgevolg is R/I een veld.

Veronderstel nu omgekeerd dat R/I een veld is; uiteraard is dan $I \neq R$. Veronderstel dat I niet maximaal is, en beschouw een ideaal $J \trianglelefteq R$ met $I \subsetneq J \subsetneq R$. Neem $a \in J \setminus I$ willekeurig. Dan is $a + I$ niet het nulelement van R/I , en dus is het inverseerbaar, stel met inverse $b + I$. Uit $(a + I)(b + I) = 1 + I$

volgt dan $1 \in ab + I$, en dus ook $1 \in aR + I$. Dus is $aR + I$ een ideaal dat een eenheid bevat, en bijgevolg $aR + I = R$. Dit is echter strijdig met het feit dat zowel a als I bevat zijn in J . We besluiten dat I een maximaal ideaal moet zijn. $\square$

Gevolg 2.6.3. *Zij R een ring. Dan is (0) een maximaal ideaal als en slechts als R een veld is.*

Bewijs. Dit volgt onmiddellijk uit Stelling 2.6.2 met $I = (0)$. $\square$

Voorbeelden 2.6.4. (1) Beschouw de ring $R = \mathbb{Z}$. Elk ideaal is een hoofdideaal, dus van de vorm $(m) = m\mathbb{Z}$ voor een zekere $m \in \mathbb{N}$. Stelling 2.6.2 zegt ons dat $\mathbb{Z}/m = \mathbb{Z}/(m)$ een veld is als en slechts als (m) een maximaal ideaal is. De maximale idealen zijn dus precies de idealen van de vorm (p) met p een priemgetal. Als $m = ab$ voor zekere $a, b \in \mathbb{N}^*$ verschillend van 1, dan is $(m) \subsetneq (a) \subsetneq (1) = \mathbb{Z}$, en dus is (m) niet maximaal.

(2) Zij K een veld, en beschouw de ring $R = K[x]$. Dit is opnieuw een hoofdideaaldomein, dus elk ideaal is van de vorm (f) voor een zeker polynoom $f \in K[x]$. Stelling 2.6.2 zegt ons dat $K[x]/(f)$ een veld is als en slechts als (f) een maximaal ideaal is.

Veronderstel nu eerst dat f *reducibel*⁷ is, d.w.z. f kan ontbonden worden als $f = gh$ met $\deg(g), \deg(h) \geq 1$. Dan is $(f) \subsetneq (g) \subsetneq (1) = K[x]$, en dan is (f) niet maximaal, zodat $K[x]/(f)$ geen veld is.

Omgekeerd, veronderstel dat (f) niet maximaal is. Omdat $K[x]$ een PID is, is er een $g \in K[x]$ zodat $(f) \subsetneq (g) \subsetneq K[x]$. In het bijzonder is $f \in (g)$, m.a.w. er is een $h \in K[x]$ zodat $f = gh$. Uit $(f) \neq (g)$ volgt dat $\deg(h) \neq 0$, en uit $(g) \neq K[x]$ volgt dat $\deg(g) \neq 0$. Dus f is reducibel. We hebben dus aangetoond dat $K[x]/(f)$ een veld is als en slechts als f een irreducibel polynoom is.

Vervolgens richten we ons tot de grotere klasse van de priemidealen.

Definitie 2.6.5. Zij R een ring en $P \trianglelefteq R$ een ideaal. We noemen P een *priemideaal* als $P \neq R$, en als voor alle $a, b \in R$ geldt:

$$ab \in P \Rightarrow a \in P \text{ of } b \in P.$$

Analoog aan Stelling 2.6.2 hebben we het volgende resultaat voor priemidealen.

Stelling 2.6.6. *Zij R een ring en $I \trianglelefteq R$ een ideaal. Dan is R/I een domein als en slechts als I een priemideaal is.*

⁷Zie ook Definities 2.7.2 en 2.7.8 verderop.

Bewijs. Veronderstel eerst dat I een priemideaal is. Onderstel dat x, y elementen van R zijn die voldoen aan

$$(x + I)(y + I) = 0 + I,$$

met andere woorden, $xy \in I$. Omdat I priem is, is ofwel $x \in I$, ofwel $y \in I$. Maar dit zegt precies dat ofwel $x + I = I$, ofwel $y + I = I$. Dit toont aan dat R/I een domein is.

Veronderstel nu omgekeerd dat R/I een domein is, en veronderstel dat $x, y \in R$ zodat $xy \in I$. Dan is $(x + I)(y + I) = xy + I = I$, en omdat R/I een domein is moet ofwel $x + I = I$ ofwel $y + I = I$. Hieruit volgt $x \in I$ of $y \in I$, en dus is I een priemideaal. $\square$

Gevolg 2.6.7. *Zij R een ring. Dan is (0) een priemideaal als en slechts als R een domein is.*

Bewijs. Dit volgt onmiddellijk uit Stelling 2.6.6 met $I = (0)$. $\square$

Gevolg 2.6.8. *Elk maximaal ideaal is een priemideaal.*

Bewijs. Dit volgt onmiddellijk uit Stelling 2.6.2 en Stelling 2.6.6. $\square$

Voor hoofdideaaldomeinen geldt in essentie ook het omgekeerde.

Stelling 2.6.9. *Zij R een PID. Dan is elk niet-nul priemideaal in R een maximaal ideaal.*

Bewijs. Zij I een niet-nul priemideaal, en veronderstel dat het niet maximaal is, zodat er een $J \trianglelefteq R$ bestaat met $I \subsetneq J \subsetneq R$. Omdat R een PID is, kunnen we $I = (a)$ en $J = (b)$ schrijven. In het bijzonder is $a \in (b)$, en dus bestaat er een $c \in R$ met $a = bc$. Omdat $bc = a \in I$ en I een priemideaal is, moet ofwel $b \in I$ ofwel $c \in I$. Echter, $b \in I$ zou leiden tot $(b) \subseteq I$ maar dan $I = J$, strijdig; dus moet $c \in I = (a)$. Schrijf $c = ar$ met $r \in R$; dan volgt uit $a = bc$ dat $a = abr$. Omdat R een domein is en $a \neq 0$, volgt hieruit $br = 1$ (zie Lemma 2.1.6), en dus is b een eenheid. Maar dan is $J = (b) = R$, strijdig. We besluiten dat I wel maximaal is. $\square$

Opmerking 2.6.10. De vorige stelling geldt niet voor willekeurige ringen of domeinen. Beschouw bijvoorbeeld de ring $R = \mathbb{Z}[x]$ en het ideaal $I = (x)$. Uit Voorbeeld 2.5.7 weten we dat $R/I \cong \mathbb{Z}$. Omdat $\mathbb{Z}$ een domein is maar geen veld, is het ideaal $I \trianglelefteq R$ een (niet-nul) priemideaal dat geen maximaal ideaal is.

Merk op dat het in een willekeurige ring niet meteen duidelijk is of er wel maximale idealen bestaan. Het zou immers kunnen dat er voor elk echt ideaal nog steeds een groter echt ideaal bestaat dat dit eerste ideaal bevat. Om te bewijzen dat deze situatie zich niet kan voordoen, moeten we het lemma van Zorn aannemen.

Definitie 2.6.11. (i) Een *partiële orderrelatie* “ $<$ ” op een verzameling S is een irreflexieve en transitieve relatie, met andere woorden, een relatie die voldoet aan $a \not< a$, en $a < b$ samen met $b < c$ impliceert $a < c$, voor alle $a, b, c \in S$. In het bijzonder is $a < b$ samen met $b < a$ onmogelijk. We gebruiken de notatie “ $a \leq b$ ” om aan te duiden dat $a = b$ of $a < b$. Een verzameling uitgerust met een partiële orderrelatie noemen we ook een *poset*⁸.

- (ii) Een partiële orderrelatie is *totaal* indien voor alle $a, b \in S$ geldt dat ofwel $a < b$, ofwel $b < a$, ofwel $a = b$.
- (iii) Een *keten* in een poset $(S, <)$ is een totaal geordende deelverzameling van S .
- (iv) Een *bovengrens* van een deelverzameling T van een poset $(S, <)$ is een element $b \in S$ (niet noodzakelijk in T) zodat $a \leq b$ voor alle $a \in T$. Een *maximaal element* $m \in S$ is een element zodat voor alle $a \in S$ geldt dat $a \not> m$, of anders gezegd, $m \leq a$ impliceert dat $m = a$.

Axioma 2.6.12 (Lemma van Zorn). *Een niet-ledige poset waarin elke keten een bovengrens heeft, bezit ten minste één maximaal element.*

Opmerking 2.6.13. In het begin van de jaren 1930 bewees Kurt Gödel dat het lemma van Zorn (of equivalent, het keuzeaxioma) consistent is met de andere axioma’s van de verzamelingenleer (in de Zermelo–Fraenkel eerste-orde axiomatisering). In 1963 toonde Paul Cohen aan dat het lemma van Zorn *onafhankelijk* is van de andere axioma’s. In de algebra is het gebruikelijk om het lemma van Zorn aan te nemen, ondermeer omwille van de volgende Stelling 2.6.15.

We zullen het volgend eenvoudig lemma nodig hebben.

Lemma 2.6.14. *Zij R een ring. De unie van een stijgende keten⁹ van idealen $I_1 \subseteq I_2 \subseteq \dots$ is zelf een ideaal.*

⁸partially ordered set.

⁹Het is gebruikelijk om een stijgende keten te noteren als $I_1 \subseteq I_2 \subseteq \dots$, hoewel deze notatie in feite enkel correct is voor *aftelbare* ketens. Dit doet echter niks af aan de geldigheid van de gebruikte argumenten.

Bewijs. Stel $I = \bigcup_{i \geq 1} I_i$. Als $u, v \in I$ zijn, dan zitten ze beide in I_k voor een zekere $k \in \mathbb{N}^*$. Maar dan zijn zowel $u + v$ als uR bevat in I_k en dus in I ; bijgevolg is $I \trianglelefteq R$. $\square$

Stelling 2.6.15. *Zij R een ring, en $I \trianglelefteq R$ een echt ideaal. Dan is I bevat in een maximaal ideaal $M \trianglelefteq R$. In het bijzonder heeft elke niet-nul ring maximale idealen.*

Bewijs. Beschouw de verzameling S van alle echte idealen in R die het ideaal I bevatten. Dan is $(S, \subset)$ een poset. Beschouw een willekeurige keten

$$I_1 \subseteq I_2 \subseteq \dots$$

van elementen van S , en stel $J = \bigcup_k I_k$. Uit Lemma 2.6.14 volgt dat J opnieuw een ideaal is. Belangrijk is echter dat J nog steeds een echt ideaal is. Inderdaad, indien $J = R$ zou zijn, dan is $1 \in J$, en dus zou er een k zijn met $1 \in I_k$. Maar dan zou $I_k = R$, en dit is strijdig met $I_k \in S$. We besluiten dat $J \in S$, en duidelijkerwijze is J een bovengrens voor de keten (I_k) .

We kunnen dus het lemma van Zorn toepassen op de poset S , waardoor S een maximaal element M heeft. Het element M is dan het gezochte maximale ideaal. $\square$

Oefeningen

- 115.** Zij R een ring die een idempotent element r bevat verschillend van 0 en 1 (i.e. $r^2 = r$). Toon aan dat elk priemideaal in R een idempotent element verschillend van 0 en 1 bevat.
- 116.** Beschouw de verzameling R bestaande uit rijen $a = (a_1, a_2, a_3, \dots)$ van reële getallen die uiteindelijk constant worden, i.e. $a_n = a_{n+1} = \dots$ voor n voldoende groot. We definiëren een optelling en vermenigvuldiging op R door deze bewerkingen componentsgewijze uit te voeren. Bewijs dat R een ring is, en bepaal de maximale idealen van R .
- *117.** Het *radicaal* van een ideaal I in een ring R wordt gedefinieerd als

$$\text{rad}(I) = \{r \in R \mid r^n \in I \text{ voor een zekere } n \in \mathbb{N}^*\}.$$

Toon aan dat $\text{rad}(I)$ zelf opnieuw een ideaal is. Toon vervolgens aan dat $I = \text{rad}(I)$ als en slechts als I de doorsnede is van priemidealén. Is $\text{rad}(\text{rad}(I)) = \text{rad}(I)$ voor elk ideaal I ?

- *118.** In oefening 105 (p. 76) hebben we het nilradicaal N van een ring R ingevoerd. Toon aan dat $N = \text{rad}(0)$. Toon vervolgens aan dat de volgende uitspraken equivalent zijn:

- (a) R heeft een uniek priemideaal;
- (b) elk element van R is ofwel nilpotent ofwel een eenheid;

(c) R/N is een veld.

2.7 Unieke factorisatie

Zoals we hebben gezien vormen priemidealen in een ring een natuurlijke uitbreiding van de notie van priemgetallen in $\mathbb{Z}$. Maar priemgetallen hebben nog een andere uitermate belangrijke eigenschap: elk geheel getal is, op teken en volgorde na, op unieke wijze te factoriseren in priemelementen. We willen nagaan in hoeverre we een gelijkaardige uitspraak kunnen doen in een willekeurige ring R (nog steeds commutatief en met eenheid).

De fundamentele eigenschap van priemen is precies diegene die we gebruiken hebben om priemidealen te definiëren: als p een priemgetal is en $a, b \in \mathbb{Z}$, dan volgt uit $p \mid ab$ dat $p \mid a$ of $p \mid b$. Dit leidt als volgt tot de unieke factorisatie in de ring $\mathbb{Z}$.

Stelling 2.7.1 (Fundamentele stelling van de rekenkunde). *Elke $a \in \mathbb{Z}$, $a \neq 0$, kan geschreven worden als een product*

$$a = c \cdot p_1 \cdots p_k,$$

waarbij $c = \pm 1$, $k \geq 0$, en de p_i positieve priemgetallen zijn. Deze uitdrukking is uniek op de ordening van de factoren p_i na.

Bewijs. We bewijzen eerst het bestaan van een factorisatie. Het volstaat dit te bewijzen voor $a > 1$, en we gebruiken inductie op a . Indien a een priemgetal is, is de bewering evident; als a geen priemgetal is, heeft het een echte deler $b < a$ (per definitie van priemgetal¹⁰). We schrijven dan $a = bb'$, en zowel b als b' zijn kleiner dan a , zodat we de inductiehypothese kunnen toepassen om een factorisatie van b en b' te bekomen. Deze beide factorisaties samenvoegen levert ons een factorisatie van a op.

Vervolgens tonen we aan dat de factorisatie uniek is. Stel dus

$$\pm p_1 \cdots p_k = \pm q_1 \cdots q_\ell$$

voor zekere priemgetallen $p_1, \dots, p_k, q_1, \dots, q_\ell$. De tekens van beide leden moeten duidelijk gelijk zijn. We passen nu de fundamentele eigenschap toe

¹⁰Een priemgetal wordt nog steeds gedefinieerd als een natuurlijk getal p dat precies 2 delers in $\mathbb{N}^*$ heeft, namelijk 1 en p . De fundamentele eigenschap waarop we ons gebaseerd hebben om priemidealen te definiëren, is voor de priemgetallen een *eigenschap*, die bewezen wordt vanuit de definitie.

met $p = p_1$. Omdat p het linkerlid deelt, moet het ook $q_1 \cdots q_\ell$ delen, en bijgevolg deelt het een zekere q_i . Omdat ook q_i priem is, moet $p_1 = q_i$. We kunnen dus p_1 en q_i schrappen, en verder gaan met inductie op $\min(k, \ell)$. $\square$

Zoals reeds werd bestudeerd in de cursus “Discrete Wiskunde I”, is de situatie voor polynomenringen $K[x]$ over een veld K zeer analoog aan de situatie voor $\mathbb{Z}$. De rol van priemgetallen in $\mathbb{Z}$ wordt overgenomen door irreducibele polynomen in $K[x]$.

Definitie 2.7.2. Een polynoom $f \in K[x]$ is *irreducibel* als het niet constant is, en als de enige delers van lagere graad in $K[x]$ constanten zijn. Dit betekent dus dat de enige manier om f te schrijven als product van twee polynomen, gegeven wordt door $f = cf_1$, waarbij $c \in K$ en f_1 een constant veelvoud van f is.

Een polynoom $f \in K[x]$ noemen we *monisch* als de hoogstegraadscoëfficiënt gelijk is aan 1. Voor elke $f \in K[x]$ is er een uniek constant veelvoud van f dat monisch is; we noemen dit de *normalisatie* of de *normaalkvorm* van f .

Stelling 2.7.3. *Zij K een veld en $R = K[x]$ de polynomenring in één variabele over K .*

- (i) *Als een irreducibel polynoom $p \in R$ een product fg deelt, dan deelt het ten minste één van de factoren f of g .*
- (ii) *Elk niet-nul polynoom $f \in R$ kan geschreven worden als een product*

$$f = c \cdot p_1 \cdots p_k,$$

waarbij c een niet-nul constante is, $k \geq 0$, en elke p_i is een monisch irreducibel polynoom in R . Deze factorisatie is uniek op de ordening van de factoren p_i na.

Bewijs. Geheel analoog aan het bewijs van deze eigenschappen voor $\mathbb{Z}$. Zie ook de cursus “Discrete Wiskunde I” voor meer details. $\square$

Opmerking 2.7.4. Merk op dat de waarden die c mag aannemen, precies de eenheden zijn in de overeenkomstige ring (met name $\mathbb{Z}$ of $K[x]$).

We merken ook nog het volgende welbekend feit op.

Lemma 2.7.5. *Zij K een veld, $R = K[x]$, en $f \in R$ een niet-nul polynoom met $\deg(f) = n$.*

- (i) *Zij $\alpha \in K$. Dan is $f(\alpha) = 0$ als en slechts als $x - \alpha$ een deler is van f .*
- (ii) *Het polynoom f heeft ten hoogste n wortels in K .*

Bewijs. Dit hebben we bewezen in de cursus “Discrete Wiskunde I”. $\square$

Opmerking 2.7.6. De assumptie dat K een veld is, is hierbij cruciaal. Stel bijvoorbeeld $R = (\mathbb{Z}/8)[x]$, en beschouw het polynoom $f = x^2 - 1 \in R$. Dan heeft f vier wortels modulo 8, namelijk 1, 3, 5 en 7. Ook de ontbinding in factoren is niet uniek in R , want

$$x^2 - 1 = (x + 1)(x - 1) = (x + 3)(x - 3).$$

Opmerking 2.7.7. Als $K = \mathbb{C}$, dan heeft elke veelterm van graad groter dan 1 een wortel $\alpha \in \mathbb{C}$ en bijgevolg een deler van de vorm $x - \alpha$. De irreducibele polynomen in $\mathbb{C}[x]$ zijn dus precies de lineaire polynomen, en de irreducibele factorisatie neemt de vorm

$$f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_k)$$

aan, waarbij de α_i precies de wortels van f zijn (herhaald volgens hun multipliciteit).

We willen nu de factorisatie bestuderen in willekeurige domeinen¹¹, en we beginnen met het invoeren van de nodige terminologie.

Definitie 2.7.8. Zij R een domein.

- (i) We zeggen dat een element a een element b *deelt*, of dat a een *deler* is van b , of dat b *deelbaar* is door a , als er een $q \in R$ bestaat met $b = aq$; we noteren dit als $a \mid b$. We noemen a een *echte deler* of een *eigenlijke deler* van b als bovendien noch a noch q een eenheid is in R .
- (ii) Een niet-nul element $a \in R$ noemen we *irreducibel* als het geen eenheid is en geen echte delers heeft.
- (iii) Twee elementen $a, b \in R$ worden *geassocieerd* genoemd als ze elkaar delen, m.a.w. als $a \mid b$ en $b \mid a$. Het is niet moeilijk in te zien dat a en b geassocieerd zijn als en slechts als ze op een eenheid na gelijk zijn, i.e. als er een eenheid u is zodat $b = ua$. We noteren dit als $a \sim b$.
- (iv) Een niet-nul element $p \in R$ noemen we *priem* als het geen eenheid is, en als voor alle $a, b \in R$ geldt dat $p \mid ab$ impliceert dat $p \mid a$ of $p \mid b$.

Deze concepten hebben een natuurlijke interpretatie in termen van de hoofdidealen van R . Immers, een hoofdideaal $(a) \trianglelefteq R$ bestaat precies uit alle elementen van R die deelbaar zijn door a .

¹¹Het bestuderen van deelbaarheid in ringen die geen domeinen zijn, is in principe mogelijk, maar leidt tot behoorlijk vreemde verschijnselen.

Lemma 2.7.9. *Zij R een domein, en $a, b \in R$. Dan geldt:*

$$\begin{aligned} a \text{ is een eenheid} &\iff (a) = R; \\ a \text{ is een deler van } b &\iff (a) \supseteq (b); \\ a \text{ en } b \text{ zijn geassocieerd} &\iff (a) = (b); \\ a \text{ is een eigenlijke deler van } b &\iff R \supsetneq (a) \supsetneq (b); \\ a \text{ is priem} &\iff (a) \leq R \text{ is een priemideaal.} \end{aligned}$$

Bewijs. Dit is een eenvoudige oefening. □

Men zou geneigd kunnen zijn te denken dat $a \in R$ irreducibel is als en slechts als $(a) \leq R$ een maximaal ideaal is. Dit is echter in het algemeen niet correct. (Zo is bijvoorbeeld in de ring $R = \mathbb{Z}[x]$ het element x irreducibel, maar (x) is geen maximaal ideaal.) In plaats daarvan hebben we volgende karakterisatie.

Lemma 2.7.10. *Zij $a \in R \setminus \{0\}$, geen eenheid. Dan is a irreducibel als en slechts als (a) maximaal is onder¹² de echte hoofdidealen. Anders gezegd, a is reducibel als en slechts als er een $b \in R$ is zodat $(a) \subsetneq (b) \subsetneq R$.*

Bewijs. Veronderstel eerst dat a reducibel is. Dan is $a = bc$ voor zekere $b, c \in R$ die beide geen eenheden zijn; in het bijzonder is $(b) \neq R$. Dus b is een echte deler van a , waaruit dan ook $(a) \subsetneq (b)$.

Veronderstel omgekeerd dat $(a) \subsetneq (b) \subsetneq R$ voor een zekere $b \in R$. Omdat $(b) \neq R$ is b geen eenheid. Anderzijds is $a \in (b)$, dus $a = bc$ voor een zekere $c \in R$. Omdat $(a) \neq (b)$ is $a \not\sim b$ en dus is ook c geen eenheid. Bijgevolg is a reducibel. □

De factorisatie-eigenschap in $\mathbb{Z}$ of in $K[x]$ is in feite tweeledig: enerzijds hebben we het bestaan van de factorisatie, en anderzijds de uniciteit ervan. Zoals we zullen zien is de uniciteit veel problematischer dan de existentie.

Een andere vaststelling is dat in $\mathbb{Z}$ en in $K[x]$ de begrippen “priem” en “irreducibel element” samenvallen; dit is niet het geval in een willekeurig domein. Wanneer we spreken over een factorisatie, is het natuurlijk om een factorisatie in irreducibele elementen te beschouwen. Zie echter ook Stelling 2.7.17 verderop.

Aan de hand van het bewijs van Stelling 2.7.1 kunnen we een algoritme bedenken om te proberen te factoriseren: als een element $a \in R \setminus \{0\}$ geen eenheid is, en a is zelf niet irreducibel, dan heeft het een echte factor b en

¹²Hiermee bedoelen we dat (a) een maximaal element is in de poset van de echte hoofdidealen van R geordend volgens inclusie.

dus is $a = bb'$. Vervolgens proberen we b en b' te factoriseren, enzovoort. Het enige probleem dat kan optreden, is het feit dat de factorisatie nooit stopt. De volgende stelling geeft een voldoende voorwaarde (die in iets subtielere zin ook een nodige voorwaarde is) om het bestaan van factorisatie te kunnen garanderen.

Stelling 2.7.11. *Zij R een domein, en veronderstel dat de ring R geen oneindige stijgende keten van hoofdidealen*

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

bevat. Dan heeft elk niet-nul element $a \in R \setminus R^\times$ een factorisatie in irreducibele elementen van R .

Bewijs. Zij $a \in R \setminus R^\times$. Dan kunnen we op recursieve wijze a beginnen factoriseren zoals beschreven in de vorige paragraaf. Veronderstel dat dit proces niet stopt. Dan bestaan er reducibele elementen $a = a_1, a_2, a_3, \dots$ en niet-eenheden $b_2, b_3, \dots$ zodat $a_i = a_{i+1}b_{i+1}$ voor alle $i \geq 1$. De keten $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$ is dan een oneindige stijgende keten van hoofdidealen, in strijd met het gegeven. Deze contradictie toont aan dat elke $a \in R$ factoriseerbaar is. $\square$

De voorwaarde op de ketens in Stelling 2.7.11 wordt vaak omschreven als de *stijgende keten voorwaarde* (of ACC, van het Engelse “ascending chain condition”) op hoofdidealen. We omschrijven deze voorwaarde ook als “elke stijgende keten van hoofdidealen stabiliseert¹³”. Analoog spreekt men ook van een *dalende keten voorwaarde* van objecten (of DCC, “descending chain condition”) als elke dalende keten van dergelijke objecten stabiliseert.

Voorbeeld 2.7.12. (1) Het hoofdideaaldomein $\mathbb{Z}$ heeft ACC op (hoofd)idealen, maar geen DCC. Inderdaad, als

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

een oneindige stijgende keten zou zijn, dan is a_i een echte deler van a_{i-1} , voor alle i , zodat a_1 oneindig veel verschillende delers zou hebben, wat natuurlijk niet kan. Anderszijds vinden we wel tal van oneindige dalende ketens van hoofdidealen, bijvoorbeeld

$$(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq \dots$$

¹³Dit gebruik van het woord “stabiliseren” heeft uiteraard niks te maken met hetzelfde woord in de groepentheorie, maar betekent dat vanaf een zekere $N \in \mathbb{N}^*$ alle objecten in de keten gelijk zijn; de keten wordt dus “stabiel”.

- (2) Een voorbeeld van een ring die geen ACC op hoofdidealen heeft, is de ring $R = \mathbb{C}[x_1, x_2, \dots]/I$, met $I = (x_1 - x_2^2, x_2 - x_3^2, \dots)$. Het element¹⁴ x_1 heeft hierin een niet-terminerende factorisatie $x_1 = x_2^2 = x_3^4 = x_4^8 = \dots$, en overeenkomstig hebben we de oneindige stijgende keten $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \dots$.

Het blijkt dat we, in zekere zin, oneindig veel voortbrengers nodig hebben om een dergelijke ring te construeren, en we zullen deze fenomenen zelden tegenkomen in voorbeelden. De meeste “natuurlijke” ringen zullen dus ACC op hoofdidealen hebben, en bijgevolg existentie van factorisatie.

Een belangrijke klasse van ringen zijn deze waarvoor ACC op *alle* idealen geldt.

Definitie 2.7.13. Een ring R wordt *noethers*¹⁵ genoemd, als elke stijgende keten van idealen stabiliseert, i.e. als ACC op (alle) idealen geldt.

Ook hier geldt dat niet-noetherse ringen in zekere zin oneindig veel voortbrengers vereisen, zodat de meeste ringen die we zullen ontmoeten, noethers zullen zijn.

Voorbeeld 2.7.14. (1) De ring $R = \mathbb{C}[x_1, x_2, \dots]$ is niet noethers, zoals blijkt uit de oneindige stijgende keten van idealen

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots$$

- (2) De ring R van alle continue functies van $\mathbb{R}$ naar $\mathbb{R}$ is een niet-noetherse ring. Merk immers op dat voor elk interval $[a, b] \subset \mathbb{R}$ de verzameling $I_{a,b}$ van alle continue functies die nul zijn op het interval $[a, b]$, een ideaal vormt van R .

In het bijzonder volgt uit Stelling 2.7.11 dat we in een noethers domein steeds kunnen factoriseren. Heel wat van de ringen die we al ontmoet hebben, zijn noethers. Zoals we zullen zien in het bewijs van Stelling 2.7.24, is elke PID ook noethers, maar de volgende belangrijke stelling geeft ons een grote klasse van noetherse ringen die niet noodzakelijk hoofdideaaldomeinen zijn.

Stelling 2.7.15 (Hilbert’s Basisstelling). *Als R een noetherse ring is, dan is ook $R[x]$ een noetherse ring.*

Zonder bewijs. □

¹⁴Als we spreken over “het element $x_1 \in R$ ” bedoelen we in feite het beeld $\pi(x_1)$ van $x_1 \in \mathbb{C}[x_1, x_2, \dots]$ onder de canonieke projectie $\pi: \mathbb{C}[x_1, x_2, \dots] \rightarrow R$. Dit is een zeer courant “misbruik van notatie” voor quotiënten van veeltermringen.

¹⁵genoemd naar Emmy Noether.

Bovendien zijn quotiëntringen van noetherse ringen zelf ook opnieuw noethers¹⁶, en in het bijzonder is elke ring die een quotiënt is van een polynomenring over $\mathbb{Z}$ of over een veld (in een eindig aantal variabelen) een noetherse ring.

We richten ons nu tot het uniciteitsaspect van de factorisatie.

Definitie 2.7.16. Zij R een domein. Dan noemen we R een *uniek factorisatiedomein*, of kortweg *UFD*, als ACC op hoofdidealen geldt in R , en als de irreducibele factorisatie van een element uniek is, in de volgende betekenis: als $p_1 \cdots p_k = q_1 \cdots q_\ell$ voor zekere irreducibele elementen $p_1, \dots, p_k, q_1, \dots, q_\ell$, dan is $k = \ell$, en na een hernummering van de factoren is p_i geassocieerd aan q_i voor elke i .

Stelling 2.7.17. *Zij R een domein met ACC op hoofdidealen. Dan is R een UFD als en slechts als elk irreducibel element priem is.*

Bewijs. Als elk irreducibel element priem is, dan volgt het bewijs van de uniciteit van de factorisatie op volledig analoge manier als in het bewijs van Stelling 2.7.1, en dan is R een UFD.

Veronderstel nu omgekeerd dat R een UFD is, en zij p een irreducibel element. Zij $a, b \in R$ willekeurige elementen waarvoor $p \mid ab$, en schrijf $ab = pq$. We ontbinden a , b en q in hun irreducibele factoren: stel $a = a_1 \dots a_k$, $b = b_1 \dots b_\ell$, en $q = q_1 \dots q_m$. Dan is $pq_1 \dots q_m = a_1 \dots a_k b_1 \dots b_\ell$, en alle factoren in beide leden zijn irreducibel. Uit het feit dat R een UFD is volgt nu dat p geassocieerd is aan een a_i of aan een b_i . In het eerste geval geldt $p \mid a$, in het tweede geval geldt $p \mid b$. $\square$

Opmerking 2.7.18. Uiteraard is in een willekeurig domein R elk priemelement irreducibel.

Voorbeeld 2.7.19. Stel $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Dan is R een domein, dat geen uniek factorisatiedomein is. De eenheden in R zijn ± 1 , en het element $6 \in R$ heeft twee essentieel verschillende factorisaties

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Het is niet erg moeilijk¹⁷ om aan te tonen dat de vier termen 2 , 3 , $1 + \sqrt{-5}$ en $1 - \sqrt{-5}$ irreducibel zijn in R . Aangezien de eenheden enkel ± 1 zijn, is 2 niet geassocieerd aan $1 \pm \sqrt{-5}$, zodat we inderdaad zien dat R geen UFD is.

Een voorbeeld van een element dat irreducibel is maar niet priem, is het element $2 \in R$, want $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, terwijl $2 \nmid 1 \pm \sqrt{-5}$.

¹⁶Gebruik hiervoor het feit dat elk ideaal van een quotiëntring R/I van de vorm J/I is, met $I \subseteq J \leq R$.

¹⁷Beschouw hiertoe de afbeelding $N: R \rightarrow \mathbb{Z}: z \mapsto z\bar{z}$ zoals in Voorbeeld 2.4.4(3).

In een UFD is het gemakkelijk om na te gaan of een element a een ander element b deelt, in termen van hun factorisatie in irreducibele elementen.

Lemma 2.7.20. *Zij R een UFD, en $a = p_1 \cdots p_k, b = q_1 \cdots q_\ell \in R$ twee elementen met hun bijhorende irreducibele factorisatie. Dan is $a \mid b$ als en slechts als $\ell \geq k$ en na een henummering van de factoren p_i geassocieerd is aan q_i voor elke $i = 1, \dots, k$.*

Bewijs. Oefening. □

Een onmiddellijk gevolg van deze observatie is het bestaan van grootste gemene delers in een UFD.

Definitie 2.7.21. *Zij R een domein, en $a, b \in R$, niet beide 0. Een *grootste gemene deler* van a en b is een element $d \in R$ zodat $d \mid a$ en $d \mid b$, en als $e \in R$ een element is met $e \mid a$ en $e \mid b$, dan is $e \mid d$.*

Gevolg 2.7.22. *Zij R een UFD, en $a, b \in R$ niet beide 0. Dan hebben a en b een grootste gemene deler. Bovendien zijn elke twee grootste gemene delers van a en b geassocieerd aan elkaar.*

Bewijs. Oefening. □

We zullen vaak spreken van *de* grootste gemene deler, hoewel deze dus slechts op een eenheid na bepaald is.

Opmerking 2.7.23. Een domein wordt een *GCD-domein* genoemd indien elke twee niet-nul elementen een grootste gemene deler hebben. In het bijzonder zien we dus dat elk UFD een GCD-domein is.

De eigenschap dat de grootste gemene deler van a en b kan geschreven worden in de vorm $ar+bs$ (die gekend staat als de stelling van Bézout) is in het algemeen *niet* geldig in een UFD. Zo is in $\mathbb{Z}[x]$ de grootste gemene deler van 2 en x gelijk aan 1, maar 1 kan niet geschreven worden in de vorm $2r + xb$. Dit heeft natuurlijk alles te maken met het feit dat $\mathbb{Z}[x]$ geen hoofdideaaldomein is, en dat in het bijzonder het ideaal $(2, x)$ geen hoofdideaal is.

Een domein wordt een *Bézout domein* genoemd indien de som van elke twee hoofdidealen opnieuw een hoofdideaal is. Een Bézout domein is dus een GCD-domein waarin de stelling van Bézout geldig is.

Merk op dat er Bézout domeinen bestaan die geen UFD zijn. Een voorbeeld hiervan is de ring van gehele complexe functies (functies die holomorf zijn op het hele complexe vlak).

Een belangrijke klasse van domeinen waarin we unieke factorisatie hebben, zijn de hoofdideaaldomeinen.

Stelling 2.7.24. *Elke PID is een UFD. In het bijzonder is elk Euclidisch domein een UFD.*

Bewijs. Zij R een PID. We tonen eerst aan dat ACC op hoofdidealen geldt. Stel dus dat $(a_1) \subseteq (a_2) \subseteq \dots$ een stijgende keten van hoofdidealen is. Uit Lemma 2.6.14 volgt dat de unie van deze idealen $\bigcup_{i \geq 1} (a_i)$ opnieuw een ideaal I is, en omdat R een PID is moet $I = (b)$ voor een zekere $b \in R$. Maar dan is $b \in (a_k)$ voor een zekere $k \in \mathbb{N}^*$, en dus is $(b) = (a_k)$. Hieruit volgt echter $(a_m) = (b)$ voor alle $m \geq k$, dus de keten stabiliseert.

Vervolgens gaan we na dat elk irreducibel element priem is; het resultaat volgt dan uit Stelling 2.7.17. Zij dus $p \in R$ irreducibel. Uit Lemma 2.7.10 volgt nu dat het ideaal (p) maximaal is onder de hoofdidealen, maar omdat elk ideaal een hoofdideaal is toont dit aan dat (p) een maximaal ideaal is, en bijgevolg een priemideaal. We besluiten dat het element $p \in R$ priem is.

De laatste bewering ten slotte volgt uit het feit dat elk Euclidisch domein een PID is (zie Stelling 2.4.3). $\square$

We kunnen nu ook Voorbeeld 2.6.4(2) veralgemenen voor willekeurige hoofdideaaldomeinen.

Stelling 2.7.25. *Zij R een PID, en $p \in R$ met $p \neq 0$. Dan is $R/(p)$ een veld als en slechts als p irreducibel is.*

Bewijs. Dit volgt nu onmiddellijk door Stelling 2.6.2 te combineren met Lemma 2.7.10, opnieuw gebruik makend van het feit dat elk ideaal een hoofdideaal is. $\square$

Hoofdideaaldomeinen zijn zeker niet de enige interessante unieke factorisatiedomeinen.

Stelling 2.7.26. *Als R een uniek factorisatiedomein is, dan is ook $R[x]$ een uniek factorisatiedomein.*

Zonder bewijs. $\square$

In het bijzonder zien we dat de ringen $\mathbb{Z}[x]$, $\mathbb{Z}[x_1, \dots, x_n]$ en $F[x_1, \dots, x_n]$ met F een veld, unieke factorisatiedomeinen zijn.

Oefeningen

119. Een *Gauss priem* is een priemelement in de ring $\mathbb{Z}[i]$.

- (a) Zij p een priemgetal. Bewijs dat ofwel p een Gauss priem is, ofwel het product is van twee complex toegevoegde Gauss priemen $p = \pi\bar{\pi}$.

- (b) Zij π een Gauss priem. Bewijs dat $\pi\bar{\pi}$ ofwel een geheel priemgetal is, ofwel het kwadraat is van een geheel priemgetal.

*120. Zij R een PID, en beschouw de ring van formele machtreeksen $R[[x]]$ zoals gedefinieerd in Voorbeeld 2.1.4(11). Toon aan dat de ring $R[[x]]$ een UFD is.

We gaan nog even wat nader in op de ring $\mathbb{Z}[x]$.

Definitie 2.7.27. Een niet-nul polynoom $f \in \mathbb{Z}[x]$ gegeven door $f(x) = a_0 + a_1x + \cdots + a_nx^n$ wordt *primitief* genoemd, als de coëfficiënten $a_0, \dots, a_n$ geen andere gemeenschappelijke factoren hebben dan de eenheden ± 1 in $\mathbb{Z}$, en als de hoogstegraadscoëfficiënt a_n positief is.

Uit de definitie volgt onmiddellijk dat we elk niet-nul polynoom $f \in \mathbb{Q}[x]$ op unieke wijze kunnen schrijven als een product $f(x) = c \cdot f_0(x)$ met $c \in \mathbb{Q}$ en f_0 een primitief polynoom in $\mathbb{Z}[x]$; het polynoom f heeft gehele coëfficiënten als en slechts als $c \in \mathbb{Z}$, en in dat geval is $|c|$ de grootste gemene deler van de coëfficiënten van f .

Stelling 2.7.28 (Lemma van Gauss). *Het product van primitieve polynomen in $\mathbb{Z}[x]$ is opnieuw een primitief polynoom in $\mathbb{Z}[x]$.*

Bewijs. Zij $f, g \in \mathbb{Z}[x]$ primitieve polynomen, en stel $h = fg$. Veronderstel dat h niet primitief is; dan bestaat er een priemgetal p zodat p een deler is van elk van de coëfficiënten van h . Beschouw nu het restrictiemorfisme modulo p

$$\Theta: \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p)[x]$$

zoals in Voorbeeld 2.2.5(3). Omdat f en g primitief zijn, zijn de polynomen $\Theta(f)$ en $\Theta(g)$ niet nul. Echter, wegens onze veronderstelling is $\Theta(h) = 0$, en dus $\Theta(f)\Theta(g) = 0$. Dit is in strijd met het feit dat $(\mathbb{Z}/p)[x]$ een domein is. $\square$

Het belang van het lemma van Gauss wordt duidelijk door het volgende gevolg, dat een concrete manier geeft om na te gaan wanneer een polynoom over $\mathbb{Q}[x]$ irreducibel is.

Gevolg 2.7.29. *Zij $f \in \mathbb{Z}[x]$ een niet-constant polynoom. Als f irreducibel¹⁸ is in $\mathbb{Z}[x]$, dan is het ook irreducibel in $\mathbb{Q}[x]$.*

Bewijs. Neem zonder verlies van algemeenheid aan dat de hoogstegraadscoëfficiënt van f positief is. Aangezien f irreducibel is in $\mathbb{Z}[x]$ en niet-constant

¹⁸We bedoelen hier irreducibel zoals in Definitie 2.7.8. Merk op dat dit iets sterker is dan irreducibel als veeltermen.

is, is het een primitief polynoom. Veronderstel dat f reducibel is in $\mathbb{Q}[x]$, stel $f = gh$ met $g, h \in \mathbb{Q}[x]$. We schrijven nu $g = cg_0$ en $h = dh_0$ met $c, d \in \mathbb{Q}$ en g_0, h_0 primitieve polynomen in $\mathbb{Z}[x]$. Uit het lemma van Gauss volgt dat g_0h_0 opnieuw een primitief polynoom is. Echter, uit $f = cd \cdot g_0h_0$ volgt dan dat $f = f_0 = g_0h_0$, zodat f toch reducibel is in $\mathbb{Z}[x]$. Onze veronderstelling is dus vals, en f is irreducibel in $\mathbb{Q}[x]$. $\square$

Het volgend criterium, dat steunt op het voorgaand gevolg, toont aan dat er heel wat polynomen over $\mathbb{Q}$ bestaan die irreducibel zijn; in het bijzonder zijn er irreducibele polynomen van willekeurige graad.

Stelling 2.7.30 (Criterium van Eisenstein). *Zij $f \in \mathbb{Z}[x]$ gegeven door $f(x) = a_0 + a_1x + \dots + a_nx^n$, en zij p een priemgetal zodat $p \nmid a_n$, terwijl $p \mid a_i$ voor alle $i \in \{0, \dots, n-1\}$, waarbij echter $p^2 \nmid a_0$. Dan is f irreducibel over $\mathbb{Q}$.*

Bewijs. Zonder verlies van algemeenheid mogen we onderstellen dat f primitief is. (Inderdaad, als de coëfficiënten van f een gemeenschappelijke deler d hebben, dan is zeker $p \nmid d$; als we alle coëfficiënten dan delen door d , blijven alle assumpties bewaard.) Veronderstel nu dat f reducibel is over $\mathbb{Q}$, en dus wegens Gevolg 2.7.29 ook reducibel over $\mathbb{Z}$. Schrijf $f = gh$, met $\deg(g) = r \geq 1$, $\deg(h) = s \geq 1$ en $r + s = n$.

Beschouw nu opnieuw het restrictiemorfisme $\Theta: \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p)[x]$, zoals in het bewijs van het Lemma van Gauss. Uit het gegeven volgt dat $\Theta(f) = \overline{a_n}x^n$. Omdat $R := (\mathbb{Z}/p)[x]$ een UFD is, volgt hieruit dat $\Theta(g) = bx^r$ en $\Theta(h) = cx^s$ voor zekere $b, c \in (\mathbb{Z}/p)^\times$. (Merk op dat de elementen van $(\mathbb{Z}/p)^\times$ precies de eenheden in R zijn, terwijl $x \in R$ een irreducibel element is.) Dit impliceert echter dat zowel g als h een constante term hebben die deelbaar is door p , maar dan zou de constante term van $f = gh$ deelbaar zijn door p^2 , in strijd met het gegeven.

We besluiten dat f irreducibel is over $\mathbb{Q}$. $\square$

Voorbeelden 2.7.31. (1) Zij p een priemgetal, en $n \geq 1$ een natuurlijk getal. Dan is het polynoom $x^n - p$ irreducibel in $\mathbb{Q}[x]$.

(2) Zij p een priemgetal, en beschouw het p -de cyclotomisch polynoom

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}.$$

We beweren dat Φ_p irreducibel is in $\mathbb{Q}[x]$. We kunnen het criterium van Eisenstein niet rechtstreeks toepassen op Φ_p , maar wel op het polynoom f gegeven door $f(x) = \Phi_p(x+1)$; het is duidelijk dat Φ_p irreducibel is

als en slechts als f dit is. Het is nu een eenvoudige oefening om na te rekenen dat

$$\begin{aligned} f(x) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}, \end{aligned}$$

en dat dit polynoom voldoet aan de eisen nodig om het criterium van Eisenstein te kunnen toepassen.

Oefeningen

121. Toon aan dat twee polynomen in $\mathbb{Z}[x]$ onderling ondeelbaar zijn in $\mathbb{Q}[x]$ als en slechts als het ideaal dat ze voortbrengen in $\mathbb{Z}[x]$ een niet-nul geheel getal bevat.
 122. Zij $f \in \mathbb{Z}[x]$ een *monisch* polynoom, en $r \in \mathbb{Q}$ een wortel van f . Toon aan dat $r \in \mathbb{Z}$.
 123. Bewijs dat de kern van het morfisme $\mathbb{Z}[x] \rightarrow \mathbb{R}$ dat x afbeeldt op $1 + \sqrt{2}$ een hoofdideaal is, en zoek een voortbrenger voor dit ideaal.
 124. Zij p een priemgetal, en $A \neq I$ een $(n \times n)$ -matrix over $\mathbb{Z}$ zodat $A^p = I$. Bewijs dat $n \geq p - 1$.
-

2.8 Directe producten en de Chinese reststelling

De Chinese reststelling voor de gehele getallen werd voor het eerst beschreven in de vierde eeuw na Christus, door de Chinese wiskundige Sunzi. De stelling werd opnieuw in 1247 gepubliceerd door de Chinese wiskundige Qin Jiushao.

We zullen deze beroemde stelling veralgemenen naar willekeurige commutatieve ringen met eenheid. We beginnen met de definitie van het direct product van ringen; dit begrip is geheel analoog aan het direct product van groepen dat we eerder al hebben ontmoet.

Definitie 2.8.1. Zij $R_1, \dots, R_n$ willekeurige ringen. Dan definiëren we een nieuwe ring $R = R_1 \times \cdots \times R_n$, die we het *direct product* of het *cartesisch product* van de ringen $R_1, \dots, R_n$ noemen, als volgt:

$$R = \{(r_1, \dots, r_n) \mid r_i \in R_i \text{ voor elke } i\},$$

met de componentsgewijze optelling en vermenigvuldiging, i.e.

$$(r_1, \dots, r_n) + (r'_1, \dots, r'_n) = (r_1 + r'_1, \dots, r_n + r'_n),$$

$$(r_1, \dots, r_n) \cdot (r'_1, \dots, r'_n) = (r_1 r'_1, \dots, r_n r'_n),$$

voor alle $r_i, r'_i \in R_i$. Het is eenvoudig om in te zien dat R met deze bewerkingen opnieuw een ring is, met nul-element $(0_{R_1}, \dots, 0_{R_n})$ en eenheid $(1_{R_1}, \dots, 1_{R_n})$.

Opmerking 2.8.2. Het direct product van ten minste twee niet-nul ringen is nooit een domein. Zo geldt bijvoorbeeld in $R_1 \times R_2$ dat $(1, 0) \cdot (0, 1) = (0, 0)$.

Definitie 2.8.3. Zij R een ring. Twee echte idealen $I, J \leq R$ noemen we *copriem* of *comaximaal* als $I + J = R$.

Lemma 2.8.4. *Zij R een ring.*

- (i) *Als I en J twee idealen zijn van R die copriem zijn, dan is $IJ = I \cap J$.*
- (ii) *Als $I_1, \dots, I_s$ idealen zijn van R die paarsgewijze copriem zijn, dan geldt voor elke i dat de idealen I_i en $\prod_{j \neq i} I_j$ copriem zijn, en*

$$I_1 \cdots I_s = I_1 \cap \cdots \cap I_s.$$

Bewijs. (i) De inclusie $IJ \subseteq I \cap J$ volgt uit Lemma 2.3.5. Omgekeerd, zij $a \in I \cap J$. Omdat $I + J = R$ bestaan er een $i \in I$ en een $j \in J$ zodat $1 = i + j$. Dan is $a = ai + aj$; omdat $a \in J$ is $ai \in IJ$, en omdat $a \in I$ is $aj \in IJ$. Dus $a \in IJ$.

- (ii) Voor $s = 1$ valt er niks te bewijzen; stel dus $s \geq 2$. Beschouw het ideaal $J = I_1 \cdots I_{s-1} \leq R$. We tonen aan dat $J + I_s = R$. Voor elke $i \leq s - 1$ is $I_i + I_s = R$, en dus zijn er $a_i \in I_i$ en $r_i \in I_s$ zodat $1 = a_i + r_i$. Maar dan is

$$1 = (a_1 + r_1) \cdots (a_{s-1} + r_{s-1}) \in a_1 \cdots a_{s-1} + I_s.$$

Omdat $a_1 \cdots a_{s-1} \in J$, toont dit aan dat $1 \in J + I_s$, en bijgevolg $J + I_s = R$.

We tonen nu de gelijkheid $I_1 \cdots I_s = I_1 \cap \cdots \cap I_s$ aan per inductie op s , waarbij het geval $s = 1$ triviaal is; stel dus opnieuw $s \geq 2$. Uit (i) volgt nu dat $J I_s = J \cap I_s$, en het gestelde volgt nu door de inductiehypothese toe te passen op de idealen $I_1, \dots, I_{s-1}$. $\square$

Stelling 2.8.5 (Chinese reststelling). *Zij R een ring, en beschouw idealen $I_1, \dots, I_s$ van R die paarsgewijze copriem zijn; stel $I = I_1 \cdots I_s$. Dan is de afbeelding*

$$\varphi: R/I \rightarrow R/I_1 \times \cdots \times R/I_s: r + I \mapsto (r + I_1, \dots, r + I_s)$$

is een ringisomorfisme.

Bewijs. Omdat $I \subseteq I_i$ voor elke i , is de afbeelding φ in elk geval goed gedefinieerd. Het is evident dat φ dan ook een ringmorfisme is. De injectiviteit is ook duidelijk, want als $\varphi(r + I) = 0$, dan is $r \in I_i$ voor alle i , en dus $r \in \bigcap_{i=1}^s I_i = I$, wegens Lemma 2.8.4(ii).

Om aan te tonen dat φ surjectief is, tonen we eerst aan dat voor elke i het element $e_i := (0 + I_1, \dots, 1 + I_i, \dots, 0 + I_s)$ bereikt wordt door φ . Inderdaad, uit Lemma 2.8.4(ii) volgt dat I_i en $\prod_{j \neq i} I_j$ copriem zijn, en dus bestaan er elementen $a_i \in I_i$ en $b_i \in \prod_{j \neq i} I_j$ zodat $a_i + b_i = 1$. Het beeld van het element $b_i + I = 1 - a_i + I$ onder φ is precies het element e_i .

Zij nu $z = (r_1 + I_1, \dots, r_s + I_s) \in R/I_1 \times \dots \times R/I_s$ willekeurig. Dan is $\varphi(r_1 b_1 + \dots + r_s b_s + I) = z$, en we besluiten dat φ surjectief is. $\square$

Opmerking 2.8.6. Als $R = \mathbb{Z}$, dan zijn twee idealen $I = a\mathbb{Z}$ en $J = b\mathbb{Z}$ copriem als en slechts als $\gcd(a, b) = 1$. In dat geval vinden we dus de klassieke versie van de Chinese reststelling terug. Zie ook Oefening 125.

Voorbeeld 2.8.7. We beweren dat $\mathbb{C}[x]/(x^2 + 1) \cong \mathbb{C} \times \mathbb{C}$. Merk op dat $(x^2 + 1) = (x + i)(x - i)$, en dat de idealen $I = (x + i)$ en $J = (x - i)$ copriem zijn. Uit de Chinese reststelling volgt dan dat $\mathbb{C}[x]/(x^2 + 1) \cong \mathbb{C}[x]/(x + i) \times \mathbb{C}[x]/(x - i)$, en uit Voorbeeld 2.5.7 volgt dat dit op zijn beurt isomorf is met $\mathbb{C} \times \mathbb{C}$.

Oefeningen

125. Zij R een willekeurig hoofdideaaldomein. Toon aan dat $(a) + (b) = (\gcd(a, b))$ voor alle $a, b \in R \setminus \{0\}$. In het bijzonder zijn (a) en (b) copriem als en slechts als $\gcd(a, b) \in R^\times$. (Merk op dat R een UFD is, zodat de grootste gemene deler op een eenheid na gedefinieerd is door Definitie 2.7.21.)
126. Herinner je dat een element e in een ring S idempotent is als $e^2 = e$; merk op dat in een product $R \times R'$ van ringen het element $e = (1, 0)$ idempotent is. De bedoeling van deze oefening is om het omgekeerde hiervan aan te tonen.
 - (a) Zij $e \in S$ idempotent. Toon aan dat $e' = 1 - e$ ook idempotent is.
 - (b) Zij $e \in S$ idempotent. Bewijs dat het hoofdideaal eS een ring is, met eenheidselement e . (Deze ring zal in het algemeen dus geen deelring zijn van S , tenzij $e = 1$.)
 - (c) Zij $e \in S$ een idempotent, en stel $e' = 1 - e$. Toon aan dat $S \cong (eS) \times (e'S)$ als ringen.
127. Zij F een veld, en $R = F[x]$. Beschouw een kwadraatvrij polynoom $f \in F[x]$, i.e. als g een niet-constant polynoom is met $g \mid f$, dan is $g^2 \nmid f$. Zij S ten slotte de quotiëntring $S = R/(f)$. Bewijs dat S isomorf is met het direct product van een eindig aantal velden.

Het hoeft geen betoog dat vectorruimten belangrijke algebraïsche structuren zijn. Vectorruimten zijn steeds gedefinieerd over een zeker veld K , en we willen graag dit begrip uitbreiden tot structuren die gedefinieerd zijn over een ring R . Zo komen we tot het begrip van modulen.

Tegelijk is er ook een analogie met groepsacties. Het is in vele situaties zinvol om R -modulen te interpreteren als verzamelingen “waar de ring R op werkt”.

Het uiteindelijke doel van dit hoofdstuk is de classificatie van eindig voortgebrachte modulen over een hoofdideaaldomein. We zullen dit resultaat dan toepassen op de ring $\mathbb{Z}$ en op veeltermenringen $F[x]$, en hieruit twee heel verschillende resultaten afleiden.

3.1 Definitie en voorbeelden

Definitie 3.1.1. Zij R een commutatieve ring. Een R -*moduul* is een abelse groep $(M, +)$, voorzien van een *scalaire vermenigvuldiging*

$$R \times M \rightarrow M: (r, v) \mapsto r \cdot v = rv,$$

die voldoet aan de volgende axioma's:

$$\begin{aligned} 1 \cdot v &= v, \\ (rs) \cdot v &= r \cdot (s \cdot v), \\ (r + s) \cdot v &= r \cdot v + s \cdot v, \\ r \cdot (v + w) &= r \cdot v + r \cdot w, \end{aligned}$$

voor alle $r, s \in R$ en alle $v, w \in M$.

Als K een veld is, dan is een K -moduul precies hetzelfde als een K -vectorruimte. Maar terwijl de structuur van een K -vectorruimte op isomorfisme na volledig bepaald is door zijn dimensie, kan de structuur van R -modulen heel wat gevarieerder zijn.

Voorbeelden 3.1.2. (1) Zij R een ring. Dan is R een R -moduul, met als optelling de optelling in R , en als scalaire vermenigvuldiging de vermenigvuldiging in R .

(2) Zij R een ring, en stel R^n gelijk aan de verzameling van $(n \times 1)$ -kolommatrices over R , met de optelling en de scalaire vermenigvuldiging gegeven door

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad \text{en} \quad r \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}.$$

Dan is R^n een R -moduul.

De volgende voorbeelden illustreren het feit dat heel wat R -modulen niet van de vorm R^n zijn, en zich essentieel anders gedragen dan vectorruimten.

Voorbeelden 3.1.3. (1) Zij R een ring, en $I \trianglelefteq R$ een ideaal. Dan is I een R -moduul, met als optelling de optelling in I , en als scalaire vermenigvuldiging de restrictie van de vermenigvuldiging in R tot $I \times R$.

(2) Zij $R = \mathbb{Z}$, en M een willekeurige abelse groep. We beweren dat M dan een $\mathbb{Z}$ -moduul is. Inderdaad, we definiëren $n \cdot v = v + \cdots + v$ (n keer) en $(-n) \cdot v = -(n \cdot v)$ voor elke $n \in \mathbb{N}$. Het is duidelijk dat alle axioma's van een $\mathbb{Z}$ -moduul dan zijn voldaan. Aangezien omgekeerd elk moduul een abelse groep is, verkrijgen we:

Abelse groepen en $\mathbb{Z}$ -modulen zijn equivalente concepten.

(3) Zij F een veld, en $R = F[x]$ de polynomenring over F in één variabele. We beweren dat de volgende twee concepten equivalent zijn:

- (a) een $F[x]$ -moduul;
- (b) een F -vectorruimte V samen met een lineaire operator $f: V \rightarrow V$.

Inderdaad, als V een $F[x]$ -moduul is, dan is V in het bijzonder ook een F -moduul, m.a.w. een F -vectorruimte. We kunnen dan een afbeelding $f: V \rightarrow V$ definiëren door de formule

$$f(v) := x \cdot v \quad \text{voor alle } v \in V.$$

Uit de definitie van modulen volgt nu dat f een lineaire operator is. Omgekeerd, als V een F -vectorruimte is en $f \in \text{End}_F(V)$, dan definiëren we een $F[x]$ -moduulstructuur via de scalaire vermenigvuldiging

$$\varphi(x) \cdot v := \varphi(f)(v) \quad \text{voor alle } \varphi(x) \in F[x].$$

Men gaat na dat deze definitie inderdaad van V een $F[x]$ -moduul maakt.

Opmerking 3.1.4. Waar het bij vectorruimten bijna altijd evident is wat de scalaire vermenigvuldiging is die we beschouwen, is de scalaire vermenigvuldiging bij modulen vaak een essentieel onderdeel van de structuur. Dit blijkt heel sterk uit Voorbeeld 3.1.3(3): dezelfde abelse groep F^n kan op heel veel verschillende manieren de structuur van een $F[x]$ -moduul krijgen door er een andere scalaire vermenigvuldiging op te leggen.

Oefeningen

128. Zij G een abelse groep. Bewijs dat, indien G de structuur heeft van een $\mathbb{Q}$ -moduul met de groepsbewerking als optelling, dat deze $\mathbb{Q}$ -moduulstructuur dan uniek bepaald is. Toon vervolgens ook aan dat een *eindige* abelse groep nooit een $\mathbb{Q}$ -moduulstructuur kan hebben.

129. Bewijs dat de volgende twee concepten equivalent zijn:

- (a) een $\mathbb{Z}[i]$ -moduul;
- (b) een abelse groep M samen met een groeps morfisme $\varphi: M \rightarrow M$ met de eigenschap dat $\varphi \circ \varphi = -\text{id}$.

130. Zij R een ring en M een R -moduul. De *annihilator* van M is de verzameling

$$I = \text{Ann}(M) := \{r \in R \mid rM = 0\}.$$

Bewijs dat I een ideaal van R is. Bepaal de annihilator van het $\mathbb{Z}$ -moduul $\mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/4$, en van het $\mathbb{Z}$ -moduul $\mathbb{Z}$.

3.2 Deelmodulen, morfismen, quotiënten, directe sommen

Definitie 3.2.1. Zij R een ring en M een R -moduul. Een *deelmoduul* van M is een additieve deelgroep N van M die tevens gesloten is onder de scalaire vermenigvuldiging. We noteren dit als $N \leq M$.

Lemma 3.2.2. *De deelmodulen van het R -moduul R zijn precies de idealen van R .*

Bewijs. Dit volgt onmiddellijk uit de definities. □

De definitie van morfismen tussen modulen is precies dezelfde als bij vectorruimten.

Definitie 3.2.3. Zij R een ring, en M en N twee R -modulen. Een afbeelding $\theta: M \rightarrow N$ is een *moduulmorfisme* of kortweg een *morfisme*, als de afbeelding compatibel is met de optelling en de scalaire vermenigvuldiging, in de zin dat

$$\theta(v + w) = \theta(v) + \theta(w) \quad \text{en} \quad \theta(rv) = r\theta(v)$$

voor alle $v, w \in M$ en alle $r \in R$. De begrippen *epimorfisme*, *monomorfisme* en *isomorfisme* worden gedefinieerd op de gebruikelijke manier, evenals de begrippen *kern* en *beeld* van een morfisme.

Lemma 3.2.4. Zij R een ring, M, N twee R -modulen, en $\theta: M \rightarrow N$ een morfisme. Dan is $\ker(\theta) \leq M$ en $\text{im}(\theta) \leq N$.

Bewijs. Oefening. □

Voorbeeld 3.2.5. Zij R een domein, en beschouw de R -modulen $M = R$ en $N = aR$, met $a \in R \setminus \{0\}$. Dan is $M \cong N$ als R -modulen. Inderdaad, de afbeelding $\theta: M \rightarrow N: r \mapsto ar$ is een moduulisomorfisme. (Merk op dat $\ker(\theta) = 0$ omdat R een domein is.)

Vervolgens zullen we ook het concept van quotiëntgroepen uitbreiden tot modulen.

Definitie 3.2.6. Zij R een ring, M een R -moduul, en $N \leq M$ een deelmoduul. In het bijzonder is M een abelse groep en N een deelgroep (en dus normaaldeeler) van M . Beschouw de quotiëntgroep M/N ; de elementen van deze groep zijn de nevenklassen van N in M . Dan kunnen we van deze quotiëntgroep een R -moduul maken door

$$r \cdot (v + N) := rv + N \tag{3.1}$$

te stellen, voor elke $r \in R$ en elke $v \in M$. We noemen M/N met deze scalaire vermenigvuldiging het *quotiëntmoduul*, of kortweg het *quotiënt* van M met N .

Voorbeeld 3.2.7. Zij R een ring en $I \trianglelefteq R$ een ideaal van R . Dan is de quotiëntring R/I ook een R -moduul, namelijk het quotiëntmoduul van het R -moduul R met het deelmoduul $I \leq R$ (zie Lemma 3.2.2). Deze R -modulen zullen een belangrijke rol spelen voor eindig voortgebrachte modulen over hoofdideaaldomeinen; zie Stelling 3.5.1 verderop.

Net zoals bij de quotiëntconstructies die we al eerder ontmoet hebben, kunnen we de volgende resultaten afleiden.

Stelling 3.2.8. Zij R een ring.

- (i) Zij M een R -moduul, en $N \leq M$ een deelmoduul. De scalaire vermenigvuldiging (3.1) is goed gedefinieerd, en M/N is een R -moduul. De projectie-afbeelding

$$\pi: M \rightarrow M/N: v \mapsto v + N$$

is een epimorfisme van R -modulen, en de kern is precies $N \leq M$.

- (ii) [Eerste isomorfiestelling] Zij A, B twee R -modulen, en $\theta: A \rightarrow B$ een moduulmorfisme. Dan is $\text{im}(\theta) \cong A/\ker(\theta)$ als R -modulen.
- (iii) Zij A, B twee R -modulen, en $\theta: A \rightarrow B$ een moduulmorfisme. Dan heeft θ een decompositie in een projectie (= canonieke surjectie), een isomorfisme, en een inclusie (= canonieke injectie):

$$A \twoheadrightarrow A/\ker(\theta) \xrightarrow{\sim} \text{im}(\theta) \hookrightarrow B.$$

- (iv) Zij M een R -moduul.

$$\begin{aligned} N \leq M &\iff \left[\begin{array}{l} N \text{ is de kern van een moduul-} \\ \text{morfisme vertrekkend uit } M \end{array} \right] \\ S \text{ is een quotiënt van } M &\iff \left[\begin{array}{l} S \text{ is het beeld van een moduul-} \\ \text{morfisme vertrekkend uit } M \end{array} \right] \end{aligned}$$

Bewijs. Oefening. □

Ten slotte geven we een eenvoudige maar belangrijke constructie om van een collectie R -modulen een nieuw R -moduul te maken.

Definitie 3.2.9. Zij R een ring, en beschouw R -modulen $M_1, \dots, M_n$. Dan definiëren we een nieuw R -moduul $M = M_1 \oplus \dots \oplus M_n$, dat we de *directe som* van de modulen $M_1, \dots, M_n$ noemen, als volgt:

$$M = \{(m_1, \dots, m_n) \mid m_i \in M_i \text{ voor elke } i\},$$

met de componentsgewijze optelling en scalaire vermenigvuldiging, i.e.

$$\begin{aligned} (m_1, \dots, m_n) + (m'_1, \dots, m'_n) &= (m_1 + m'_1, \dots, m_n + m'_n), \\ r \cdot (m_1, \dots, m_n) &= (rm_1, \dots, rm_n), \end{aligned}$$

voor alle $m_i, m'_i \in M_i$ en $r \in R$. Het is eenvoudig om in te zien dat de directe som van R -modulen opnieuw een R -moduul is.

De volgende “inwendige” karakterisatie van directe sommen is zeer nuttig.

Lemma 3.2.10. *Zij R een ring, M een R -moduul, en $M_1, \dots, M_n$ deelmodulen van M . Dan zijn de volgende uitspraken equivalent.*

- (a) *De afbeelding $\theta: M_1 \oplus \dots \oplus M_n \rightarrow M: (a_1, \dots, a_n) \mapsto a_1 + \dots + a_n$ is een R -moduul-isomorfisme;*
- (b) *elke $a \in M$ is op unieke wijze te schrijven als $a = a_1 + \dots + a_n$ met $a_i \in M_i$ voor elke i ;*
- (c) *$M_i \cap (\sum_{j \neq i} M_j) = 0$ voor alle i , en elke $a \in M$ is te schrijven als $a = a_1 + \dots + a_n$ met $a_i \in M_i$ voor elke i .*

Bewijs. Dit is een onmiddellijke toepassing van Gevolg 1.7.6. Merk op dat de ring R geen rol speelt; enkel het feit dat $M_1, \dots, M_n$ abelse groepen zijn, is relevant. $\square$

Voorbeeld 3.2.11. In Voorbeeld 3.1.3(3) (p. 102) zagen we dat $F[x]$ -modulen equivalent zijn met F -vectorruimten voorzien van een lineaire operator. Beschouw dus een paar (V, f) bestaande uit een F -vectorruimte V voorzien van een lineaire operator f .

Zij nu $W \leq V$ een F -vectordeelruimte. Dan is W een $F[x]$ -deelmoduul van V juist dan als $x \cdot W \subseteq W$, want de ring $F[x]$ is als ring voortgebracht door F en het element x . Uit Voorbeeld 3.1.3(3) volgt nu dat de $F[x]$ -deelmodulen W precies de F -deelruimten W zijn die f -invariant zijn, i.e. $f(W) \subseteq W$.

In het bijzonder zien we dat als het $F[x]$ -moduul V een directe som is van deelmodulen, dat dan V als vectorruimte de directe som is van f -invariante deelruimten. Als V eindig-dimensionaal is vinden we in het bijzonder een basis voor V zodat de matrix van f een blokmatrix is, waarvan de blokken precies overeenkomen met deze deelruimten.

Oefeningen

- 131.** Zij R een ring, beschouwd als een R -moduul. Bepaal alle R -moduulmorfismen van R naar zichzelf.
- 132.** Zij R een ring en M een R -moduul. Zij E de verzameling van alle *endomorfismen* van M , i.e. de morfismen van M naar zichzelf. Bewijs dat E een niet noodzakelijk commutatieve ring is, met samenstelling van functies als vermenigvuldiging, en met optelling gedefinieerd op de natuurlijke manier als $(\varphi + \psi)(v) = \varphi(v) + \psi(v)$ voor alle $v \in M$.
- 133.** Een moduul wordt *enkelvoudig* of *simpel* genoemd als het niet het nul-moduul is, en geen eigenlijke deelmodulen heeft.
 - (i) Bewijs dat elk enkelvoudig moduul isomorf is met R/M voor een zeker maximaal ideaal M van R .

- (ii) Bewijs *het lemma van Schur*: als $\varphi: M \rightarrow N$ een morfisme is tussen twee enkelvoudige modulen, dan is ofwel $\varphi = 0$, ofwel is φ een isomorfisme.

134. Zij $P \leq N \leq M$ drie R -modulen. Beschrijf natuurlijke morfismen die de drie quotientmodulen M/P , M/N en N/P met elkaar in verband brengen, en bewijs met behulp hiervan de *derde isomorfiestelling*: $M/N \cong (M/P) / (N/P)$.

3.3 Matrices, vrije modulen, basissen

Voor we overgaan tot een diepere studie van willekeurige modulen, richten we ons eerst tot de modulen van de vorm R^n . Deze vertonen veel gelijkenissen met vectorruimten, maar zoals we zullen zien zijn er toch belangrijke verschillen.

We zullen vaak werken met R -matrices, i.e. matrices met waarden in R . Het manipuleren van dergelijke matrices kan op dezelfde manier als voor matrices met waarden in een veld, en we zullen de courante rekenregels hier dan ook niet herhalen. In het bijzonder kunnen we van elke vierkante $(n \times n)$ R -matrix A de determinant berekenen als

$$\det(A) = \sum_{\sigma \in \mathbf{S}_n} \text{sign}(\sigma) a_{1,1^\sigma} \cdots a_{n,n^\sigma},$$

en deze voldoet aan de klassieke eigenschap

$$\det(AB) = \det(A) \det(B)$$

voor alle $(n \times n)$ -matrices A en B over R . Als $\det(A)$ een eenheid is in R , dan kunnen we de inverse matrix A^{-1} berekenen door middel van de gekende formule

$$A^{-1} = (\det A)^{-1} \cdot \text{adj}(A).$$

Omgekeerd is het duidelijk dat als $\det(A)$ geen eenheid is, dan de matrix A niet inverteerbaar kan zijn, omwille van de gelijkheid $\det(A) \det(A^{-1}) = 1$.

Definitie 3.3.1. Zij R een ring. De inverteerbare $(n \times n)$ -matrices met waarden in R vormen een groep

$$\text{GL}_n(R) := \{A \in \text{Mat}_n(R) \mid \det(A) \in R^\times\},$$

die we de *algemene lineaire groep over R* noemen.

Merk op dat de voorwaarde $\det(A) \in R^\times$ een sterke restrictie is voor ringen die weinig eenheden hebben, zoals bijvoorbeeld de ring $\mathbb{Z}$. Toch zijn

er steeds nog behoorlijk veel matrices die hieraan voldoen. Immers, alle matrices van de vorm

$$I + a \cdot e_{ij} = \begin{pmatrix} 1 & & a \\ & \ddots & \\ & & 1 \end{pmatrix}, \quad i \neq j, \quad a \in R$$

hebben determinant 1; alle permutatiematrices hebben determinant ± 1 ; en de diagonaalmatrices met waarden in $R^\times$ hebben een determinant in $R^\times$. De groep *voortgebracht* door al deze matrices is dus volledig bevat in $\mathbf{GL}_n(R)$.

We keren nu terug naar de studie van de R -modulen. De concepten *basis*, *onafhankelijkheid* en *voortbrengen* kunnen alle vertaald worden naar de moduultheorie, zonder wezenlijke aanpassingen.

Definitie 3.3.2. Zij R een ring, en M een R -moduul.

- (i) Een verzameling $S \subseteq M$ is een *voortbrengende* verzameling voor M , of *spant* M op, als elke $v \in M$ een *R -lineaire combinatie* is van de elementen van S , i.e.

$$v = r_1 v_1 + \cdots + r_n v_n,$$

met elke $r_i \in R$ en $v_i \in S$. (Merk dus op dat een R -lineaire combinatie altijd een *eindige* som is, ook als S oneindig groot is.)

- (ii) Het moduul M is *eindig voortgebracht* als het een eindige voortbrengende verzameling heeft. Merk op dat een abelse groep eindig voortgebracht is als groep als en slechts als hij eindig voortgebracht is als $\mathbb{Z}$ -moduul.
- (iii) Een verzameling $S \subseteq M$ noemen we (*lineair*) *onafhankelijk* als geen enkele niet-triviale R -lineaire combinatie nul is, i.e.

$$\text{als } r_1 v_1 + \cdots + r_n v_n = 0$$

(met $r_i \in R$ en v_i verschillende elementen uit S),

dan $r_i = 0$ voor alle i .

- (iv) Een *basis* is een verzameling die tegelijk voortbrengend en onafhankelijk is. Anders gezegd, $\mathbf{B} \subseteq M$ is een basis voor M als elke $v \in M$ op een *unieke* manier kan geschreven worden als een R -lineaire combinatie van de elementen van $\mathbf{B}$. Als een basis $\mathbf{B}$ eindig is, wordt die vaak ook als een *geordende* verzameling $\mathbf{B} = (v_1, \dots, v_n)$ genoteerd.

- (v) Het moduul R^n heeft een *standaardbasis* $(e_1, \dots, e_n)$, waarbij e_i de kolomvector is met een 1 op de i -de rij en een 0 op alle andere rijen.
- (vi) Het moduul M wordt *vrij* genoemd als het een basis heeft.

Niet alle modulen hebben een basis:

Lemma 3.3.3. *Zij R een ring, en M een R -moduul. Dan heeft M een basis met juist n elementen als en slechts als $M \cong R^n$.*

We noemen M in dit geval vrij van rang n .

Bewijs. We hebben reeds opgemerkt dat het moduul R^n een basis heeft, namelijk de standaardbasis.

Veronderstel omgekeerd dat $\mathbf{B} = (v_1, \dots, v_n)$ een basis is voor M . Beschouw het moduulmorfisme

$$\mu: R^n \rightarrow M: \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \mapsto r_1 v_1 + \dots + r_n v_n.$$

Aangezien $(v_1, \dots, v_n)$ een voortbrengende verzameling is voor M , is μ surjectief; en omdat $(v_1, \dots, v_n)$ een onafhankelijke verzameling is in M , is μ injectief. Bijgevolg is μ bijectief, en dus is $M \cong R^n$. $\square$

We kunnen ook vrije modulen van oneindige rang construeren.

Lemma 3.3.4. *Zij S een willekeurige verzameling. Voor elk element $s \in S$ beschouwen we een “symbool” e_s , en we beschouwen de verzameling M bestaande uit alle mogelijke (eindige!) R -lineaire combinaties van deze symbolen, met andere woorden, elk element van M kan (uniek) geschreven worden als een uitdrukking van de vorm*

$$m = r_1 e_{s_1} + \dots + r_n e_{s_n}$$

voor zekere $n \in \mathbb{N}$, zekere verschillende elementen $s_1, \dots, s_n \in S$ en zekere $r_1, \dots, r_n \in R$. Dan is M , voorzien van de evidente optelling en scalaire vermenigvuldiging, een vrij R -moduul van rang $|S|$.

Bewijs. Het is evident dat M een R -moduul is, en het is ook onmiddellijk duidelijk dat de verzameling $\mathbf{B} = \{e_s \mid s \in S\}$ een basis vormt voor M . $\square$

Opmerking 3.3.5. Het is vreemd dat men voor R -modulen het begrip “rang” gebruikt waar men voor vectorruimten “dimensie” gebruikt, maar dit is de gebruikelijke terminologie.

Opmerking 3.3.6. Het vrij R -moduul van rang $|S|$ dat we geconstrueerd hebben in Lemma 3.3.4 kan ook “concreter” beschreven worden als het R -moduul van alle mogelijke afbeeldingen van S naar R met *eindige support*, d.w.z., die slechts voor een eindig aantal elementen van S een niet-nul waarde hebben. (Ga zelf na als oefening dat dit een equivalente beschrijving is.)

Opmerking 3.3.7. Hoewel de noties die we hebben ingevoerd in Definitie 3.3.2 volledig analoog zijn aan de gelijknamige noties in vectorruimten, zijn er toch belangrijke verschillen, zelfs als we ons zouden beperken tot vrije modulen. Eén van de grootste verschillen, met vergaande gevolgen, is het feit dat een onafhankelijke verzameling in een vrij moduul niet steeds uitgebreid kan worden tot een basis. Zo is bijvoorbeeld het singleton $\{(2, 0)^t\} \subset \mathbb{Z}^2$ niet uitbreidbaar tot een basis voor $\mathbb{Z}^2$. (Ga dit zelf na.)

Voorbeeld 3.3.8. In Voorbeeld 3.1.3(3) (p. 102) zagen we dat $F[x]$ -modulen equivalent zijn met F -vectorruimten voorzien van een lineaire operator. Beschouw nu de F -vectorruimte

$$Z := \{(a_0, a_1, a_2, \dots) \mid a_i \in F, \text{ slechts eindig veel } a_i \neq 0\},$$

voorzien van de *shift-operator*

$$T: Z \rightarrow Z: (a_0, a_1, a_2, \dots) \mapsto (0, a_0, a_1, \dots).$$

We beweren dat (Z, T) onder voorgaande equivalentie overeenkomt met een vrij $F[x]$ -moduul van rang 1. Inderdaad, stel $M = F[x]$ als $F[x]$ -moduul, en beschouw de afbeelding

$$\rho: M \rightarrow Z: a_0 + a_1x + a_2x^2 + \dots \mapsto (a_0, a_1, a_2, \dots)$$

voor alle $a_i \in F$. Het is duidelijk dat ρ alvast een F -vectorruimte-isomorfisme is.

We stellen vast dat

$$\rho(x\varphi(x)) = T(\rho(\varphi(x))) = x \cdot \rho(\varphi(x))$$

voor elke veelterm $\varphi(x) \in F[x]$. Aangezien $F[x]$ als ring wordt voortgebracht door F en het element x , volgt hieruit dat ρ een $F[x]$ -moduulisomorfisme is van M naar Z . We besluiten dat Z vrij is van rang 1.

Het rekenen met basissen in vrije R -modulen van eindige rang gebeurt op dezelfde manier als bij vectorruimten, gebruik makend van matrices met waarden in R . We herhalen de belangrijkste concepten.

Definitie 3.3.9. (i) Zij M een vrij R -moduul met basis $\mathbf{B} = (v_1, \dots, v_n)$.

De *coördinaatvector* van een element $v \in M$ ten opzichte van een basis $\mathbf{B}$ is de unieke kolomvector $(r_1, \dots, r_n)^t \in R^n$ zodat $v = r_1 v_1 + \dots + r_n v_n$.

(ii) Zij M een vrij R -moduul van eindige rang, en $\mathbf{B} = (v_1, \dots, v_n)$ en $\mathbf{B}' = (v'_1, \dots, v'_n)$ twee basissen voor M . De *transitiematrix* of *matrix van basisovergang* is de matrix $Q = (q_{ij}) \in \text{GL}_n(R)$ gedefinieerd door de nieuwe basisvectoren te schrijven in functie van de oude basisvectoren, als

$$v'_j = \sum_{i=1}^n q_{ij} v_i$$

voor elke $j \in \{1, \dots, n\}$.

Opmerking 3.3.10. We hebben in de voorgaande definitie impliciet gebruik gemaakt van het feit dat elke twee basissen dezelfde kardinaliteit hebben. Dit is inderdaad het geval, en kan bewezen worden op gelijkaardige manier als voor vectorruimten, bijvoorbeeld door aan te tonen dat de matrix Q van basisovergang inverteerbaar is: de matrix P van de omgekeerde basisovergang (van $\mathbf{B}'$ naar $\mathbf{B}$) voldoet aan $PQ = QP = 1$. Men kan dan aantonen dat dit enkel kan als P en Q vierkante matrices zijn, omdat voor commutatieve ringen blijft gelden dat de rijrang en de kolomrang gelijk zijn, en dat de rang van het product van matrices nooit groter is dan de rang van deze matrices zelf.

Het is heel verrassend dat dit niet langer waar is voor niet-commutatieve ringen R . (De definities van modulen en vrije modulen zijn volledig analoog aan het commutatieve geval.) Er bestaan zelfs niet-commutatieve ringen R zodat de modulen R^n voor $n = 1, 2, 3, \dots$ allemaal isomorf zijn aan elkaar.

Definitie 3.3.11. Zij R een ring, M, N twee vrije R -modulen van eindige rang, en $\theta: M \rightarrow N$ een modulomorfisme. Als M basis $\mathbf{B} = (v_1, \dots, v_n)$ heeft en N basis $\mathbf{C} = (w_1, \dots, w_m)$, dan definiëren we de *matrix van θ ten opzichte van de basissen $\mathbf{B}$ en $\mathbf{C}$* als de matrix $A = (a_{ij})$ zodat

$$\theta(v_j) = \sum_{i=1}^m a_{ij} w_i$$

voor elke $j \in \{1, \dots, n\}$.

Als we voor beide vrije modulen een nieuwe basis $\mathbf{B}'$ respectievelijk $\mathbf{C}'$ kiezen, en de matrices van basisovergang voorstellen als Q respectievelijk P , dan wordt de nieuwe matrix A' van de afbeelding θ ten opzichte van de basissen $\mathbf{B}'$ en $\mathbf{C}'$ gegeven door

$$A' = P^{-1} A Q.$$

Vrije modulen worden gekarakteriseerd door een “universele eigenschap”.

Stelling 3.3.12 (Universele eigenschap van vrije modulen). *Zij R een ring, en M een vrij R -moduul met basis $\mathbf{B}$. Beschouw een willekeurig R -moduul N , en een afbeelding $\alpha: \mathbf{B} \rightarrow N$. Dan is er een uniek moduulmorfisme $\theta: M \rightarrow N$ zodat $\theta(v) = \alpha(v)$ voor elke $v \in \mathbf{B}$.*

Bewijs. Zij Θ de afbeelding van M naar N gedefinieerd door

$$\Theta(r_1v_1 + \cdots + r_nv_n) = r_1\alpha(v_1) + \cdots + r_n\alpha(v_n)$$

voor alle $r_1, \dots, r_n \in R$ en alle $v_1, \dots, v_n \in \mathbf{B}$ (twee aan twee verschillend). Omdat $\mathbf{B}$ een basis is, is Θ goed gedefinieerd: elk element van M kan op unieke wijze geschreven worden in de vorm $r_1v_1 + \cdots + r_nv_n$. Trivialerwijze geldt $\Theta(v) = \alpha(v)$ voor elke $v \in \mathbf{B}$. Bovendien is Θ een R -moduulmorfisme, zoals onmiddellijk blijkt door sommen en scalaire veelvouden te beschouwen.

De uniciteit is eveneens gemakkelijk in te zien, want uit de R -lineariteit van morfismen volgt dat een dergelijke θ moet voldoen aan

$$\theta(r_1v_1 + \cdots + r_nv_n) = r_1\theta(v_1) + \cdots + r_n\theta(v_n),$$

en dus moet $\theta = \Theta$. □

Opmerking 3.3.13. Deze stelling karakteriseert de vrije modulen: als M een R -moduul is dat een deelverzameling $\mathbf{B}$ bevat met de eigenschap dat voor elk R -moduul N en elke afbeelding $\alpha: \mathbf{B} \rightarrow N$ er een uniek moduulmorfisme $\theta: M \rightarrow N$ is zodat $\theta(v) = \alpha(v)$ voor elke $v \in \mathbf{B}$, dan is M een vrij moduul (en $\mathbf{B}$ is dan een basis voor M). Het is een goede oefening om dit zelf te bewijzen.

Gevolg 3.3.14. *Elk R -moduul is het quotiënt van een vrij R -moduul. Meer bepaald, als M een R -moduul is dat voortgebracht wordt door een verzameling S , dan is M het quotiënt van een vrij moduul van rang $|S|$.*

Bewijs. Beschouw een vrij R -moduul F met basis $\mathbf{B} = \{e_s \mid s \in S\}$ zoals in Lemma 3.3.4. Wegens Stelling 3.3.12 is er een moduulmorfisme $\theta: F \rightarrow M$ zodat $\theta(e_s) = s$ voor elke $s \in S$. Omdat S voortbrengend is, is θ een epimorfisme. Het resultaat volgt nu uit Stelling 3.2.8(iv). □

We gaan nu even wat dieper in op zogenaamde projectieve modulen.

Definitie 3.3.15. (i) Zij $\theta: A \rightarrow B$ een epimorfisme van R -modulen. Een morfisme $\sigma: B \rightarrow A$ met de eigenschap dat $\theta \circ \sigma = \text{id}_B$ noemen we een *sectie* van het epimorfisme θ . Merk op dat een sectie steeds injectief is. Niet elk epimorfisme heeft een sectie, en als een epimorfisme een sectie heeft, is het niet noodzakelijk uniek.

- (ii) Een R -moduul P met de eigenschap dat elk epimorfisme naar P een sectie heeft, noemen we een *projectief moduul*.

Stelling 3.3.16. *Zij R een ring. Dan is elk vrij R -moduul projectief.*

Bewijs. Zij F een vrij R -moduul en M een willekeurig R -moduul, en beschouw een epimorfisme $\theta: M \rightarrow F$; we moeten aantonen dat θ een sectie $\sigma: F \rightarrow M$ heeft.

Kies daartoe een basis $\mathbf{B}$ voor F . Omdat θ een epimorfisme is, bestaat er voor elke $v \in \mathbf{B}$ een $a_v \in M$ zodat $\theta(a_v) = v$. Zij

$$\alpha: \mathbf{B} \rightarrow M: v \mapsto a_v;$$

uit Stelling 3.3.12 weten we dat de afbeelding α op een unieke manier uitbreidt tot een morfisme $\sigma: F \rightarrow M$ zodat $\sigma(v) = a_v$. In het bijzonder is $\theta \circ \sigma$ een endomorfisme van F met $(\theta \circ \sigma)(v) = v$ voor alle $v \in \mathbf{B}$, en dus $\theta \circ \sigma = \text{id}_F$. $\square$

Het belang hiervan blijkt uit het feit dat elk epimorfisme $\theta: A \rightarrow B$ tussen twee R -modulen dat een sectie heeft, aanleiding geeft tot een natuurlijke decompositie van het moduul A .

Stelling 3.3.17. *Zij $\theta: A \rightarrow B$ een epimorfisme, en zij $\sigma: B \rightarrow A$ een sectie van θ . Dan is $A = \ker(\theta) \oplus \text{im}(\sigma) \cong \ker(\theta) \oplus B$.*

Bewijs. We zullen gebruik maken van Lemma 3.2.10. Stel $a \in \ker(\theta) \cap \text{im}(\sigma)$, en schrijf $a = \sigma(b)$ met $b \in B$. Dan is $0 = \theta(a) = \theta(\sigma(b)) = b$, en dus is $\ker(\theta) \cap \text{im}(\sigma) = 0$. Zij anderzijds $a \in A$ willekeurig; dan is $\sigma(\theta(a)) \in \text{im}(\sigma)$. Anderzijds is

$$\theta(a - \sigma(\theta(a))) = \theta(a) - \theta(\sigma(\theta(a))) = \theta(a) - \theta(a) = 0,$$

en dus is $a = (a - \sigma(\theta(a))) + \sigma(\theta(a)) \in \ker(\theta) + \text{im}(\sigma)$. Uit Lemma 3.2.10 volgt nu dat $A = \ker(\theta) \oplus \text{im}(\sigma)$.

Merk ten slotte op dat $\text{im}(\sigma) \cong B$ omdat σ injectief is. $\square$

Als gevolg hiervan bekomen we de volgende karakterisatie van projectieve modulen.

Stelling 3.3.18. *Zij P een R -moduul. Dan is P projectief als en slechts als het een directe sommand is van een vrij moduul, d.w.z., als en slechts als er een vrij moduul F bestaat en deelmodulen A en B van F zodat $F = A \oplus B$ met $A \cong P$.*

Bewijs. Veronderstel eerst dat P projectief is. Uit Gevolg 3.3.14 weten we dat er een epimorfisme θ bestaat van een vrij moduul F naar P . Omdat P projectief is, heeft θ een sectie $\sigma: P \rightarrow F$. Uit Stelling 3.3.17 volgt dan dat $F = \text{im}(\sigma) \oplus \ker(\theta)$, en aangezien $\text{im}(\sigma) \cong P$ volgt het gestelde.

Veronderstel omgekeerd dat F een vrij R -moduul is, en dat $F = A \oplus B$; we zullen bewijzen dat A projectief is. Beschouw dus een willekeurig epimorfisme $\theta: M \rightarrow A$. Dan is $\theta \oplus \text{id}_B: M \oplus B \rightarrow A \oplus B$ een epimorfisme naar een vrij (en dus projectief) moduul, dat bijgevolg een sectie $\sigma: A \oplus B \rightarrow M \oplus B$ heeft. Dan is $\sigma(A) \subseteq M$, en de restrictie $\sigma|_A: A \rightarrow M$ is een sectie van θ . $\square$

Tot slot tonen we aan dat deelmodulen van vrije modulen over een PID opnieuw vrij zijn. We zullen ons voor het bewijs beperken tot vrije modulen van eindige rang.

Stelling 3.3.19. *Zij R een hoofdideaaldomein, en M een vrij R -moduul van rang n . Zij $N \leq M$ een deelmoduul van M ; dan is N een vrij R -moduul van rang ten hoogste n .*

Bewijs. We bewijzen dit per inductie op de rang n . Stel eerst $n = 1$; dan is $M \cong R$, en uit Lemma 3.2.2 weten we dat $N \leq M$ een ideaal is in R . Omdat R een PID is, is $N = (a) = aR$ voor een zekere $a \in R$, en als $a \neq 0$ dan is $aR \cong R$ als R -modulen (zie Voorbeeld 3.2.5).

Zij nu $M = R^n$, en beschouw het projectiemorfisme

$$\pi: R^n \rightarrow R^{n-1}: (r_1, \dots, r_n) \mapsto (r_1, \dots, r_{n-1}).$$

De inductiehypothese leert ons dat $\pi(N)$ vrij is met rang ten hoogste $n - 1$. De restrictie $\pi|_N: N \rightarrow \pi(N)$ is dus een epimorfisme naar een vrij moduul, en uit Stellingen 3.3.16 en 3.3.17 volgt dat

$$N \cong \ker(\pi|_N) \oplus \pi(N).$$

Eenzijds merken we op dat $\ker(\pi|_N)$ een deelmoduul is van $\ker(\pi) \cong R$, zodat $\ker(\pi|_N)$ een vrij moduul van rang 0 of 1 is. Anderzijds weten we reeds dat $\pi(N)$ een vrij moduul is van rang ten hoogste $n - 1$. Omdat de directe som van vrije modulen duidelijkerwijze opnieuw vrij is van rang gelijk aan de som van de rangen, volgt hieruit dat N een vrij moduul is van rang ten hoogste n . $\square$

Opmerking 3.3.20. De voorwaarde dat onze ring een PID is is noodzakelijk, zoals reeds blijkt uit het rang 1 geval.

Gevolg 3.3.21. *Zij R een hoofdideaaldomein. Dan is elk projectief R -moduul ook vrij.*

Bewijs. Dit volgt onmiddellijk uit Stellingen 3.3.18 en 3.3.19. $\square$

Opmerking 3.3.22. We weten nu dat elk vrij moduul projectief is, en dat voor hoofdideaaldomeinen ook elk projectief moduul vrij is. De natuurlijke vraag stelt zich of dit laatste ook geldt voor willekeurige ringen. In het algemeen geldt dit niet; zie bijvoorbeeld Oefening 139. Anderzijds geldt dit wel voor een belangrijke klasse van ringen, namelijk voor polynomenringen over een veld, $k[x_1, \dots, x_n]$. Dit zeer belangrijke en diepgaande resultaat werd in 1976 bewezen door Daniel Quillen en Andrei Suslin. Quillen heeft in 1978, ondermeer voor dit werk, de prestigieuze Fields medaille gewonnen.

Oefeningen

- 135.** Zij $R = \mathbb{C}[x, y]$, en zij M het ideaal (x, y) in R . Is M een vrij R -moduul?
- 136.** Zij R een ring zodat elk eindig voortgebracht R -moduul vrij is. Bewijs dat ofwel $R = 0$, ofwel is R een veld.
- 137.** Zij A de matrix van een morfisme $\varphi: \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ van vrije $\mathbb{Z}$ -modulen.
- (i) Bewijs dat φ injectief is als en slechts als de rang van A gelijk is aan n .
 - (ii) Bewijs dat φ surjectief is als en slechts als de grootste gemene deler van de determinanten van alle $(m \times m)$ -minoren van A gelijk is aan 1.
- 138.** Zij R een ring, en $I \trianglelefteq R$. Bewijs dat I een vrij R -moduul is als en slechts als het een hoofdideaal is, voortgebracht door een element $\alpha \in R$ dat geen nuldeler is.
- 139.** Zij R en S twee niet-nul ringen, en beschouw de ring $R \times S$. Toon aan dat $R \times 0$ en $0 \times S$ projectieve $(R \times S)$ -modulen zijn die niet vrij zijn.
-

3.4 De Smith normaalvorm

Zij R een hoofdideaaldomein, M en N twee vrije R -modulen, en $\theta: M \rightarrow N$ een morfisme. We vragen ons af of we de basissen van M en N zodanig kunnen kiezen dat θ een zeer eenvoudige matrixvoorstelling heeft, en wat de eenvoudigste algemene gedaante is die we kunnen verwachten.

Als R een veld is, dan weten we reeds uit de cursus “Lineaire Algebra en Meetkunde I” dat we onze basissen steeds zodanig kunnen kiezen dat de matrix de gedaante

$$A = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array} \right)$$

heeft. Als R geen veld is, dan is dit resultaat zelfs al verkeerd voor (1×1) -matrices: als $r \in R$ niet nul en geen eenheid is, dan kunnen we de afbeelding

gegeven door de matrix (r) onmogelijk voorstellen door de matrix (0) of (1) ten opzichte van nieuwe basissen.

We kunnen wel “diagonaliseren”, en meer bepaald op de volgende manier.

Stelling 3.4.1. *Zij R een Euclidisch domein, en zij A een $(m \times n)$ -matrix over R . Dan bestaan er vierkante inverteerbare R -matrices P en Q (die het product zijn van elementaire matrices) zodat $A' = PAQ$ een $(m \times n)$ -matrix is van de vorm*

$$A' = \left(\begin{array}{ccc|c} d_1 & & & 0 \\ & \ddots & & \vdots \\ & & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array} \right),$$

waarbij elk diagonaalelement het volgende deelt, i.e. $d_1 \mid d_2 \mid \cdots \mid d_r$.

Bewijs. We zullen de matrix A stap voor stap omzetten in de matrix A' door middel van *elementaire rij- en kolomoperaties*:

- (a) twee rijen of twee kolommen verwisselen met elkaar;
- (b) een rij of kolom vermenigvuldigen met een *eenheid* in R ;
- (c) een veelvoud van een rij bij een andere rij optellen, of een veelvoud van een kolom bij een andere kolom optellen.

Het is duidelijk dat elk van deze operaties kan verkregen worden door de matrix A links of rechts te vermenigvuldigen met de gepaste elementaire matrix.

De strategie van het bewijs is om een opeenvolging van operaties uit te voeren om een matrix van de gedaante

$$\left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array} \right) \quad (3.2)$$

te bekomen, waarbij d_1 elk van de elementen van B deelt. Het resultaat volgt dan onmiddellijk per inductie.

We veronderstellen $A \neq 0$. Om onze strategie uit te werken, gaan we te werk in drie stappen.

Stap 1. Door rijen en kolommen te permuteren, plaatsen we linksbovenaan een niet-nul element $a \in R$ waarvoor $d(a)$ minimaal is onder alle elementen van A .

Stap 2. Stel $a = a_{11}$. Kies een niet-nul element a_{i1} in de eerste kolom, met $i > 1$, en voer de Euclidische deling uit door a_{11} :

$$a_{i1} = aq + r,$$

waarbij $r = 0$ of $d(r) < d(a)$. We trekken nu q keer de eerste rij af van de i -de rij; dit heeft (ondermeer) als effect dat a_{i1} verandert in r .

Als $r \neq 0$, dan is $d(r) < d(a)$; we keren dan terug naar stap 1. Als $r = 0$, dan hebben we een 0 aangemaakt in de eerste kolom. Na eindig veel herhalingen van stappen 1 en 2 bekomen we een matrix waarin $a_{i1} = 0$ voor alle $i > 1$. (Inderdaad, de Euclidische functie d neemt gehele waarden ≥ 0 aan, en kan dus niet oneindig vaak kleiner worden.)

Deze procedure herhalen we nu ook voor de eerste rij, en we verkrijgen dus een matrix van de gedaante (3.2), waarbij we echter nog niet weten of d_1 wel elk element van B deelt.

Stap 3. Veronderstel dat er een element b in B is dat niet deelbaar is door $a = a_{11}$. We voeren opnieuw een Euclidische deling uit van b door a , en schrijven $b = aq + r$ met $r \neq 0$ en $d(r) < d(a)$. We voegen nu de kolom van A die b bevat toe aan de eerste kolom, zodat we in die eerste kolom het element b zien verschijnen. We keren nu terug naar Stap 2, waar de Euclidische deling ons terug naar Stap 1 zal brengen, om het element a_{11} opnieuw te veranderen in een element waar de Euclidische functie een kleinere waarde aanneemt (namelijk de rest r van de deling die we daarnet uitvoerden). Na een eindig aantal stappen zal dit proces eindigen, en verkrijgen we een matrix A van de gedaante (3.2) met de bijkomende eigenschap dat d_1 een deler is van elk element van B . $\square$

Dit resultaat geldt algemener voor hoofdideaaldomeinen, maar het bewijs is beduidend moeilijker en vergt een diepere theoretische voorbereiding. We vermelden het volledige resultaat voor verdere referentie. Merk ook op dat we een uniciteitsuitspraak toevoegen voor de elementen d_i , die we ook voor Euclidische domeinen niet hebben aangetoond.

Stelling 3.4.2. *Zij R een hoofdideaaldomein, en zij A een $(m \times n)$ -matrix over R . Dan bestaan er vierkante inverteerbare R -matrices P en Q zodat $A' = PAQ$ een $(m \times n)$ -matrix is van de vorm*

$$A' = \left(\begin{array}{ccc|c} d_1 & & & 0 \\ & \ddots & & \vdots \\ & & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array} \right),$$

waarbij elk diagonaalelement het volgende deelt, i.e. $d_1 \mid d_2 \mid \cdots \mid d_r$. Bovendien zijn de elementen $d_1, \dots, d_r$ uniek bepaald op eenheden na. We noemen de matrix A' de Smith normaalvorm van de matrix A .

Zonder bewijs. □

We zullen deze stelling gebruiken in de volgende gedaante.

Gevolg 3.4.3. Zij R een hoofdideaaldomein, en zij $\theta: M \rightarrow N$ een morfisme tussen twee vrije R -modulen van eindige rang. Dan bestaan er basissen $\mathbf{B}$ voor M en $\mathbf{C}$ voor N zodat θ ten opzichte van deze basissen een matrixvoorstelling heeft zoals gegeven in Stelling 3.4.2.

Oefeningen

- 140.** Bepaal alle gehele oplossingen van het stelsel $AX = 0$, waarbij $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix}$.
- 141.** Bewijs dat $\text{SL}(2, \mathbb{Z})$ wordt voortgebracht door de matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
- 142.** Zij $\varphi: \mathbb{Z}^k \rightarrow \mathbb{Z}^k$ een morfisme gegeven door (linkse) vermenigvuldiging met een $(k \times k)$ -matrix A .
- (i) Bewijs dat $\text{im}(\varphi)$ eindige index heeft in $\mathbb{Z}^k$ als en slechts als A een niet-singuliere matrix is.
 - (ii) Toon aan dat in dat geval deze index gelijk is aan $|\det(A)|$.

3.5 Eindig voortgebrachte modulen over hoofdideaaldomeinen

We zullen nu kunnen komen tot een zeer sterke structuurstelling voor eindig voortgebrachte modulen over hoofdideaaldomeinen.

Stelling 3.5.1. Zij R een PID, en zij $M \neq 0$ een eindig voortgebracht R -modul. Dan zijn er een unieke gehele getallen $s, t \geq 0$ en uniek bepaalde echte niet-nul idealen

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_s$$

zodat

$$M \cong R/I_1 \oplus \cdots \oplus R/I_s \oplus R^t.$$

De idealen I_i noemen we de *elementaire delers* van M , en deze uitdrukking wordt de *elementaire delervorm* van M genoemd.

Bewijs. Beschouw een eindig stel voortbrengers $(v_1, \dots, v_n)$ voor M . Uit Gevolg 3.3.14 weten we dat $M \cong F/N$ waarbij F een vrij moduul van rang n is, en N een deelmoduul is van F . Uit Stelling 3.3.19 volgt dat N een vrij moduul is van rang $m \leq n$.

Beschouw de inclusieafbeelding $\iota: N \hookrightarrow F$. Uit Gevolg 3.4.3 weten we dat er basissen $\mathbf{C} = (w_1, \dots, w_m)$ voor N en $\mathbf{D} = (z_1, \dots, z_n)$ voor F bestaan, zodanig dat $\iota(w_i) = d_i z_i$ voor elke $i \in \{1, \dots, m\}$, waarbij $d_1 \mid \dots \mid d_m$, en de d_i 's zijn uniek bepaald op eenheden na. (Merk op dat ι injectief is, zodat de matrixvoorstelling geen nulkolommen heeft.)

We schrijven nu zowel F als het deelmoduul N (of preciezer, $\iota(N)$) neer door middel van hun coördinaten ten opzichte van de basis $\mathbf{D}$, en we verkrijgen

$$F = \{(r_1, \dots, r_m, r_{m+1}, \dots, r_n)^t \mid r_i \in R\}, \text{ en} \\ \iota(N) = \{(d_1 r_1, \dots, d_m r_m, 0, \dots, 0)^t \mid r_i \in R\}.$$

We besluiten dat

$$M \cong F/N \cong R/(d_1) \oplus \dots \oplus R/(d_m) \oplus R \oplus \dots \oplus R.$$

We merken nog op dat als d_1 een eenheid is, de term $R/(d_1)$ triviaal is en dus kan weggelaten worden, zodat we zonder verlies van algemeenheid kunnen stellen dat d_1 (en bijgevolg elke d_i) geen eenheid is, m.a.w. de idealen $I_i = (d_i)$ zijn echte idealen.

Het bewijs van de uniciteit laten we achterwege. $\square$

Het is interessant om deze structuurstelling nog in een andere vorm te herformuleren. Hiervoor hebben we de Chinese reststelling (Stelling 2.8.5) nodig.

Stelling 3.5.2. *Zij R een PID, en zij $M \neq 0$ een eindig voortgebracht R -moduul. Dan zijn er een unieke $s, t \in \mathbb{Z}_{\geq 0}$, unieke priemelementen $p_i \in R$, en unieke $\alpha_i \in \mathbb{N}$, zodat*

$$M \cong R/(p_1^{\alpha_1}) \oplus \dots \oplus R/(p_s^{\alpha_s}) \oplus R^t.$$

(De priemelementen hoeven niet verschillend te zijn; de uniciteit die we vermelden is uiteraard op een hernummering na, en de priemelementen zijn slechts op een eenheid na uniek bepaald.)

Bewijs. We tonen aan dat we voor elk echt niet-nul ideaal I de ring R/I nog verder kunnen ontbinden op de aangegeven manier. Stel dus $I = (a)$, en ontbind a in priemfactoren als $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, waarbij de priemelementen

$p_1, \dots, p_k$ twee aan twee verschillend zijn. (We maken hier gebruik van het feit dat elke PID ook een UFD is, en dat in een UFD elk irreducibel element ook priem is.) Merk op dat er een overeenkomstige ontbinding is van idealen

$$I = (a) = (p_1^{\alpha_1}) \cdots (p_k^{\alpha_k})$$

(zie Oefening 104). Omdat voor elke $i \neq j$ de idealen $(p_i^{\alpha_i})$ en $(p_j^{\alpha_j})$ copriem zijn (zie Oefening 125), kunnen we de Chinese reststelling¹ 2.8.5 toepassen, en dus is

$$R/I = R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k}).$$

Door dit te herhalen voor elk ideaal in de elementaire delervorm van M , verkrijgen we de gewenste gedaante. (Merk op dat hierin dus wel herhaling van priemelementen kan optreden.) $\square$

We zullen deze stelling nu toepassen voor $R = \mathbb{Z}$ en vervolgens voor $R = F[x]$. Het is verrassend dat we twee concrete stellingen terugvinden die ogenschijnlijk niks met elkaar te maken hebben, maar dus eigenlijk beide een gevolg zijn van een algemene structuurstelling in de modultheorie.

Classificatie van eindig voortgebrachte abelse groepen

We geven twee verschillende versies, die beide nuttig kunnen zijn.

Stelling 3.5.3 (Grondstelling van de eindig voortgebrachte abelse groepen). *Zij G een eindig voortgebrachte abelse groep.*

- (i) *Er bestaan unieke $s, t \in \mathbb{Z}_{\geq 0}$ en unieke $d_1, \dots, d_s \in \mathbb{N}_{>1}$ met $d_1 \mid \cdots \mid d_s$, zodat*

$$G \cong \mathbf{C}_{d_1} \times \cdots \times \mathbf{C}_{d_s} \times \mathbb{Z}^t.$$

- (ii) *Er bestaan unieke $s, t \in \mathbb{Z}_{\geq 0}$, unieke priemgetallen $p_1, \dots, p_s$ (niet noodzakelijk verschillend), en unieke $\alpha_1, \dots, \alpha_s \in \mathbb{N}$, zodat*

$$G \cong \mathbf{C}_{p_1^{\alpha_1}} \times \cdots \times \mathbf{C}_{p_s^{\alpha_s}} \times \mathbb{Z}^t.$$

Bewijs. De eerste gedaante volgt uit Stelling 3.5.1 en de tweede gedaante uit Stelling 3.5.2 door $R = \mathbb{Z}$ te stellen, en in gedachten te houden dat abelse groepen en $\mathbb{Z}$ -modulen equivalente begrippen zijn. $\square$

Opmerking 3.5.4. (i) In beide gedaantes is $t = 0$ als en slechts als G eindig is, en in het bijzonder hebben we dus een classificatie (in twee gedaantes) van alle eindige abelse groepen.

¹Merk op dat we in deze stelling een *ringisomorfisme* hebben geconstrueerd, maar het is onmiddellijk duidelijk dat dit isomorfisme ook de R -moduulstructuur respecteert.

- (ii) De voorwaarde dat de groep eindig voortgebracht moet zijn, is van cruciaal belang. De groep $(\mathbb{Q}, +)$ is een eenvoudig voorbeeld van een abelse groep die niet eindig voortgebracht is, en een classificatie geven van alle abelse groepen is niet haalbaar.

De Jordan normaalvorm voor lineaire operatoren

In Voorbeeld 3.1.3(3) (p. 102) en Voorbeeld 3.2.11 (p. 106) hebben we gezien dat $F[x]$ -modulen equivalent zijn met F -vectorruimten V voorzien van een lineaire operator f , en dat deelmodulen hierbij overeenkomen met f -invariante deelruimten van V .

Veronderstel nu dat de onderliggende vectorruimte V eindig-dimensionaal is en dat F algebraïsch gesloten is.

Definitie 3.5.5. Een veld F wordt *algebraïsch gesloten* genoemd als elke veelterm $f(x) \in F[x]$ van graad ten minste 1 kan geschreven worden als het product van lineaire factoren (i.e. veeltermen van graad 1) in $F[x]$.

Voorbeeld 3.5.6. De zogenaamde grondstelling van de algebra zegt precies dat het veld $\mathbb{C}$ algebraïsch gesloten is. Je hebt deze stelling bewezen in de cursus “Complexe Analyse” als gevolg van de stelling van Liouville, en we zullen ook in de cursus “Algebra II” een ander bewijs zien van deze belangrijke stelling.

Stelling 3.5.7 (Jordan normaalvorm). *Zij F een algebraïsch gesloten veld, zij V een eindig-dimensionale F -vectorruimte, en zij $f \in \text{End}_F(V)$.*

- (i) *Het $F[x]$ -moduul corresponderend met (V, f) kan geschreven worden in de vorm*

$$V \cong F[x]/((x - \lambda_1)^{\alpha_1}) \oplus \cdots \oplus F[x]/((x - \lambda_s)^{\alpha_s})$$

voor zekere $\lambda_1, \dots, \lambda_s \in F$ (niet noodzakelijk verschillend van elkaar) en zekere $\alpha_1, \dots, \alpha_s \in \mathbb{N}^$.*

- (ii) *Beschouw nu een deelmoduul van de vorm $W \cong F[x]/((x - \lambda)^\alpha)$. Dan is er een basis van W zodat de matrix van de lineaire operator $f|_W$ gegeven is door*

$$A = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \\ & & & 1 & \lambda \end{pmatrix}.$$

Een dergelijke matrix wordt een Jordan blok genoemd.

- (iii) *Er bestaat een basis voor V zodat de matrixvoorstelling van f een blokmatrix is bestaande uit Jordan blokken.*

Bewijs. Merk op dat $F[x]$ een hoofdideaaldomein is, zodat de priemelementen precies de irreducibele elementen zijn. Aangezien F algebraïsch gesloten is, zijn de irreducibele elementen precies de lineaire veeltermen, dus de veeltermen van de vorm $x - \lambda$ met $\lambda \in F$ (of scalaire veelvouden hiervan, maar scalaren zijn eenheden in $F[x]$).

- (i) Dit volgt nu onmiddellijk uit Stelling 3.5.2 samen met de vorige observaties. Merk op dat V eindig-dimensionaal is over F , zodat er geen vrij deelmoduul $F[x]^t$ kan optreden.
- (ii) Stel $q = (x - \lambda)^\alpha$, en kies $w = 1 + (q) \in W$. De elementen

$$w_1 = w, \quad w_2 = (x - \lambda) \cdot w, \quad \dots, \quad w_\alpha = (x - \lambda)^{\alpha-1} \cdot w$$

vormen een basis voor W over F . (Inderdaad, omdat deze elementen als veelterm in x verschillende graad hebben, zijn ze duidelijk lineair onafhankelijk; omdat $\dim_F W = \alpha$ vormen deze α elementen dan een basis.) Bovendien rekent men eenvoudig na dat $x \cdot w_i = \lambda w_i + w_{i+1}$ voor alle $i \in \{1, \dots, \alpha - 1\}$ en dat $x \cdot w_\alpha = \lambda w_\alpha$. Bijgevolg heeft de matrixvoorstelling A van x ten opzichte van deze basis de gezochte gedaante.

- (iii) Dit volgt nu onmiddellijk uit (i) en (ii) samen met het feit dat een directe som van $F[x]$ -deelmodulen overeenkomt met een ontbinding van de matrix als blokmatrix (zie ook Voorbeeld 3.2.11). $\square$

Opmerking 3.5.8. Ook als F niet algebraïsch gesloten is, kan men een gelijkaardige methode aanwenden om een lineaire operator zo eenvoudig mogelijk te schrijven. De resulterende gedaante wordt dan een *rationale canonieke vorm* genoemd.

Oefeningen

143. Toon aan dat de multiplicatieve groep $\mathbb{Q}^\times$ van de rationale getallen isomorf is met het direct product van een cyclische groep van orde 2 met een vrije abelse groep van oneindige rang.
144. Bepaal het aantal isomorfieklassen van abelse groepen van orde 1000.
145. Zij A een eindige abelse groep, en $\varphi: A \rightarrow \mathbb{C}^\times$ een morfisme dat niet triviaal is, i.e. $\varphi(A) \neq \{1\}$. Bewijs dat $\sum_{a \in A} \varphi(a) = 0$.
146. Zij F een algebraïsch gesloten veld. Kan je een zinvolle voorstelling geven van een willekeurige lineaire operator op een F -vectorruimte die niet noodzakelijk eindig-dimensionaal is, gelijkaardig aan de Jordan normaalvorm? Denk hierbij aan Voorbeeld 3.3.8 (p. 110).
