Hoofdstuk

2 Ringen

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

$$\begin{aligned} R \times R \to R\colon (s,t) &\mapsto s+t\,, && \text{(optelling)} \\ R \times R \to R\colon (s,t) &\mapsto s\cdot t = st\,, && \text{(vermenigvuldiging)} \end{aligned}$$

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.

[1] Het 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.

[2] Niet 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) nuldeler*. Een commutatieve ring met 1 zonder nuldelers[4] 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 (mod 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

[3]Verwarrend 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.

[4]Uiteraard is het element 0 zelf een nuldeler, 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 nuldeler 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 $\mathsf{GF}(q)$. 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 $\mathrm{Mat}_n(R)$ van alle $(n \times n)$-matrices over de ring R, met de gebruikelijke optelling en vermenigvuldiging. Dan vormt $\mathrm{Mat}_n(R)$ een ring. Als $n = 1$ is deze ring uiteraard isomorf[5] met de ring R zelf. Zodra $n \geq 2$, is de ring $\mathrm{Mat}_n(R)$ een niet-commutatieve ring met nuldelers. De groep der eenheden in $\mathrm{Mat}_n(R)$ noteren we als $\mathsf{GL}_n(R)$, 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 nuldeler.

(9) Er bestaan ringen met elementen die wel een linkse nuldeler zijn maar geen rechtse nuldeler 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

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

[5] We 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 dit inderdaad een ring definieert.) Dan is het element $(2, 1, 0)$ een linkse nuldeler maar geen rechtse nuldeler.

(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 coëfficienten 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 definieren 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 coëfficienten 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 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in R[\![x]\!]$ 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 $x_1, \ldots, x_n$ 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 $\alpha := (\alpha_1, \ldots, \alpha_n)$ 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 $x_1, \ldots, x_n$ met coëfficiënten in R is dan een eindige lineaire combinatie van monomen, met coëfficiënten in R, en kunnen we dus kort noteren als

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

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 $x_1, \ldots, x_n$ noteren we als $R[x_1, \ldots, x_n]$, 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 $R[\![x_1, \ldots, x_n]\!]$ van formele machtreeksen 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

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

waarbij $\overline{d}$ 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

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

(Merk op dat de noemers $a\overline{a} + b\overline{b}$ 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

95. Zij R een commutatieve ring, en zij $r \in R$ een nilpotent element. Toon aan dat $1 + r$ een eenheid is in R.

96. Geef een voorbeeld van een geheel getal n zodat $\mathbb{Z}/n$ ten minste 4 verschillende idempotente elementen heeft.

97. Beschouw het lichaam $\mathbb{H}$ der reële quaternionen, en beschouw de elementen

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

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

98. 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 **??**.

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

$$\theta\colon R \to S$$

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

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

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 $\theta\colon R \to S$ een groepsmorfisme induceert tussen de onderliggende additieve groepen, $\theta_+\colon (R, +) \to (S, +)$. In het bijzonder is steeds $\theta(0_R) = 0_S$. Merk ook op dat $\ker(\theta) = \ker(\theta_+)$ en $\mathrm{im}(\theta) = \mathrm{im}(\theta_+)$ (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 $S = \mathrm{Mat}_2(\mathbb{Q})$, en stel

$$\theta\colon R \to S\colon x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}.$$

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

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

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

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

$$\theta\colon \mathbb{Z} \to \mathbb{Z}/m$$

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 $\overline{x}$ 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 $\theta\colon R \to S$ een ringmorfisme.*

(i) *Gegeven is een element $s \in S$. Dan is er een uniek ringmorfisme $\Phi\colon R[x] \to S$, 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 $s_1, \ldots, s_n \in S$. Dan is er een uniek ringmorfisme $\Phi\colon R[x_1, \ldots, x_n] \to S$, 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

$$\varphi\colon R[x] \to S\colon \sum_i r_i x^i \mapsto \sum_i \theta(r_i) s^i\,.$$

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

$$\varphi(fg) = \varphi\Big(\sum a_i b_j x^{i+j}\Big) = \sum \varphi\big(a_i b_j x^{i+j}\big) = \sum \theta(a_i b_j) s^{i+j}$$
$$= \sum \theta(a_i)\theta(b_j) s^{i+j} = \Big(\sum_i \theta(a_i) s^i\Big)\Big(\sum_j \theta(b_j) s^j\Big) = \varphi(f)\varphi(g)\,.$$

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 $x \in R[x]$. □

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

$$\Phi\colon R[x] \to R\colon f(x) \mapsto f(s).$$

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

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

$$\Phi\colon R[x] \to S[x]\colon a_0 + a_1 x + \cdots + a_k x^k \mapsto \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_k)x^k.$$

(3) We passen nu voorgaand voorbeeld toe op het morfisme $\varphi\colon \mathbb{Z} \to \mathbb{Z}/m$ uit Voorbeeld 2.2.3(2). Dan is het corresponderend substitutiemorfisme gegeven door

$$\Phi\colon \mathbb{Z}[x] \to (\mathbb{Z}/m)[x]\colon a_0 + a_1 x + \cdots + a_k x^k \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_k}x^k.$$

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

99. Beschouw twee ringen R en S, en zij $\theta\colon R \to S$ een rngmorfisme. Toon aan dat $\theta(1_R)$ een idempotent element in S is.

100. (a) Beschouw de afbeelding $\alpha\colon \mathbb{R}[x,y] \to \mathbb{R}$ die $f(x,y)$ afbeeldt op $f(0,0)$. Toon aan dat α een morfisme is, en bepaal $\ker(\alpha)$.

(b) Beschouw de afbeelding $\beta\colon \mathbb{R}[x] \to \mathbb{C}$ die $f(x)$ afbeeldt op $f(1+\sqrt{2})$. Toon aan dat β een morfisme is, en bepaal $\ker(\beta)$.

101. Zij p een priemgetal en $R = (\mathbb{Z}/p)[x]$. Beschouw de afbeelding $\varphi\colon R \to R\colon f \mapsto f^p$. Toon aan dat φ een morfisme is. (Dit morfisme wordt het *Frobenius-morfisme* van R genoemd.)

102. Zij R een ring, en zij $f(y) \in R[y]$. Toon aan dat de afbeelding $\theta\colon R[x,y] \to R[x,y]$ 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 $R = I$. □

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

$$ar = \sum\nolimits_i x_i(y_i r) = \sum\nolimits_i x_i y_i'$$

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 $xy \in yR \subseteq J$. □

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 110.

Definitie 2.3.7. (i) Zij R een ring, en $a_1, \ldots, a_k \in R$. Het kleinste ideaal in R dat de elementen $a_1, \ldots, a_k$ bevat, noemen we het *ideaal voortgebracht door* $a_1, \ldots, a_k$, en noteren we als $I = (a_1, \ldots, a_k)$, of ook soms als $I = \langle a_1, \ldots, a_k \rangle$.

(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 $I = (a_1, \ldots, a_k)$ 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 $a_1, \ldots, a_k \in R$. Dan is*

$$(a_1, \ldots, a_k) = a_1R + \cdots + a_kR = \{a_1r_1 + \cdots + a_kr_k \mid r_1, \ldots, r_k \in R\}.$$

Bewijs. Stel $J = a_1R + \cdots + a_kR$. Het is duidelijk dat J een additieve deelgroep van $(R, +)$ is die de gegeven elementen $a_1, \ldots, a_k$ bevat. Bovendien is J een ideaal van R, want stel $j = a_1r_1 + \cdots + a_kr_k$ en $r \in R$ willekeurig, dan is $jr = a_1(r_1r) + \cdots + a_k(r_kr) \in J$.

Zij nu I een willekeurig ideaal van R dat $a_1, \ldots, a_k$ 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 $a_1, \ldots, a_k$ bevat. □

Oefeningen

103. Zij R een ring, en $a, a_1, \ldots, a_n, b, b_1, \ldots, b_m \in R$. Toon aan dat $(a)(b) = (ab)$. Toon vervolgens aan dat algemener geldt dat

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = \big(a_ib_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\big).$$

104. 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 $\mathbb{Z}/n$.

[6]Voor polynomenringen spelen zogenaamde Gröbner basissen een fundamentele rol in dit soort probleemstellingen.

105. Beschouw de ring $R = \mathbb{Z}[x]$ en de idealen $I = (x, 2)$ en $J = (x, 3)$. Toon aan dat de verzameling $\{xy \mid x \in I, y \in J\}$ geen ideaal is in R.

106. 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

$$d\colon R \setminus \{0\} \to \mathbb{N}$$

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

$$b = aq + r\,, \qquad \text{en ofwel } \; r = 0 \; \text{ ofwel } \; d(r) < d(a)\,.$$

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

$$d\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}\colon a \mapsto |a|\,.$$

(2) Zij K een willekeurig veld. De polynomenring $K[x]$ is een Euclidisch domein, met Euclidische functie

$$d\colon K[x] \setminus \{0\} \to \mathbb{N}\colon f \mapsto \deg(f)\,.$$

(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 *norm*afbeelding, gegeven door

$$\mathsf{N}\colon \mathbb{C} \to \mathbb{R}_{\geq 0}\colon z = a + bi \mapsto z\overline{z} = (a + bi)(a - bi) = a^2 + b^2\,.$$

Merk op dat N multiplicatief is, i.e. voor alle $x, y \in \mathbb{C}$ geldt $\mathsf{N}(xy) = \mathsf{N}(x)\mathsf{N}(y)$. Stel nu d gelijk aan de restrictie van N tot $\mathbb{Z}[i]$, dus

$$d\colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}\colon a + bi \mapsto a^2 + b^2\,. \tag{2.1}$$

Stelling 2.4.5. *De ring $\mathbb{Z}[i]$ van gehelen van Gauss is een Euclidisch domein, met Euclidische functie gegeven door* (2.1)*.*

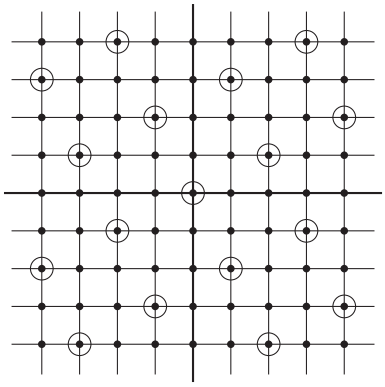
Bewijs. Beschouw $x = a + bi \in \mathbb{Z}[i] \setminus \{0\}$, en $y = c + di \in \mathbb{Z}[i]$. Stel $z = y/x = s + ti$ met $s, t \in \mathbb{R}$ (waarbij we gewoon de deling in $\mathbb{C}$ uitvoeren). Stel nu $q = m + ni$ gelijk aan het element van $\mathbb{Z}[i]$ dat het dichtst bij z ligt in 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

$$\mathsf{N}(y - xq) = \mathsf{N}(x)\mathsf{N}(z - q) \leq \mathsf{N}(x)\big((1/2)^2 + (1/2)^2\big) = \mathsf{N}(x)/2 < \mathsf{N}(x)\,.$$

Dit toont aan dat N een Euclidische functie is voor $\mathbb{Z}[i]$. □

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 verkijgen 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

$$\mathsf{N}(y - xq) = \mathrm{dist}(y, xq)^2 \leq 1/2 \cdot |x|^2 = \mathsf{N}(x)/2\,.$$

Voorbeeld 2.4.7. (1) Niet elk hoofdideaaldomein is een Euclidisch domein. Een voorbeeld wordt gegeven door de ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. (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

107. Toon aan dat de ringen $\mathbb{Z}\left[e^{2\pi i/3}\right]$ en $\mathbb{Z}\left[\sqrt{-2}\right]$ Euclidische domeinen zijn.

108. Zij $a, b \in \mathbb{Z}$, en veronderstel dat $a \mid b$ in $\mathbb{Z}[i]$. Toon aan dat dan $a \mid b$ in $\mathbb{Z}$.

109. 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.)

110. 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 normaaldeler 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 nevenklasse 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

$$(r + I) + (s + I) := (r + s) + I\,,$$
$$(r + I) \cdot (s + I) := rs + I\,.$$

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. □

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*

$$\pi\colon R \to R/I\colon r \mapsto r + I$$

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 $\theta\colon R \to S$ een ringmorfisme. Dan is* $\ker(\theta) \trianglelefteq R$*, en*

$$\operatorname{im}(\theta) \cong R/\ker(\theta)\,.$$

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 *groeps*isomorfisme

$$\alpha\colon R/\ker(\theta) \to \operatorname{im}(\theta)\colon r + \ker(\theta) \mapsto \theta(r)$$

is. We moeten enkel nog aantonen dat α ook een *ring*morfisme 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 $\theta\colon R \to S$ een decompositie heeft in een projectie (= canonieke surjectie), een isomorfisme, en een inclusie (= canonieke injectie):

$$R \twoheadrightarrow R/\ker(\theta) \xrightarrow{\sim} \operatorname{im}(\theta) \hookrightarrow S.$$

Gevolg 2.5.6. *Zij R een ring. Dan geldt:*

$$I \trianglelefteq R \iff \left[\begin{array}{r} I \text{ is de kern van een ringmorfisme} \\ \text{vertrekkend uit } R \end{array}\right.$$

$$S \text{ is een quotiënt van } R \iff \left[\begin{array}{r} S \text{ is het beeld van een ringmorfisme} \\ \text{vertrekkend uit } R \end{array}\right.$$

Bewijs. Volledig analoog aan het bewijs van Gevolg 1.6.10. □

Voorbeeld 2.5.7. Zij R een ring. We beweren dat $R[x]/(x) \cong R$. Beschouw daartoe het evaluatiemorfisme $\Phi = \text{eval}_0 \colon R[x] \to R \colon f(x) \mapsto f(0)$; 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

111. Toon aan dat de ring $\mathbb{Z}[i]/(1 + 3i)$ isomorf is met de ring $\mathbb{Z}/10$.

112. Bepaal de structuur van de ring $\mathbb{Z}[x]/(x^2 + 3, p)$, voor de keuzes $p = 3$ en $p = 5$.

113. 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 inverteerbaar 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 inverteerbaar, 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. □

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 $I = (0)$. □

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 volgend 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.*

[7] Zie 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. □

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 $I = (0)$. □

Gevolg 2.6.8. *Elk maximaal ideaal is een priemideaal.*

Bewijs. Dit volgt onmiddellijk uit Stelling 2.6.2 en Stelling 2.6.6. □

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. □

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 orderelatie* "$<$" 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 orderelatie noemen we ook een *poset*[8].

(ii) Een partiële orderelatie 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 keten*[9] *van idealen $I_1 \subseteq I_2 \subseteq \ldots$ is zelf een ideaal.*

[8] partially ordered set.

[9] Het is gebruikelijk om een stijgende keten te noteren als $I_1 \subseteq I_2 \subseteq \ldots$, 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 $I \trianglelefteq R$. □

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 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 $J = \cup_k I_k$. 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. □

Oefeningen

114. 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.

115. 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.

*__116.__ Het *radicaal* van een ideaal I in een ring R wordt gedefinieerd als

$$\mathrm{rad}(I) = \{r \in R \mid r^n \in I \text{ voor een zekere } n \in \mathbb{N}^*\}.$$

Toon aan dat $\mathrm{rad}(I)$ zelf opnieuw een ideaal is. Toon vervolgens aan dat $I = \mathrm{rad}(I)$ als en slechts als I de doorsnede is van priemidealen. Is $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$ voor elk ideaal I?

*__117.__ In oefening 109 (p. 74) hebben we het nilradicaal N van een ring R ingevoerd. Toon aan dat $N = \mathrm{rad}(0)$. 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 tekens 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 gebruikt 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 priemgetal[10]). 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 $p_1, \ldots, p_k, q_1, \ldots, q_\ell$. De tekens van beide leden moeten duidelijk gelijk zijn. We passen nu de fundamentele eigenschap toe

[10]Een 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 hoogstegraadscoëfficient 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 *normaalvorm* 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 volgend 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". □

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 domeinen[11], 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.

[11] Het 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:*

$$\begin{aligned} a \text{ is een eenheid} &\iff (a) = R\,; \\ a \text{ is een deler van } b &\iff (a) \supseteq (b)\,; \\ a \text{ en } b \text{ zijn geassocieerd} &\iff (a) = (b)\,; \\ a \text{ is een eigenlijke deler van } b &\iff R \supsetneq (a) \supsetneq (b)\,; \\ a \text{ is priem} &\iff (a) \trianglelefteq R \text{ is een priemideaal}. \end{aligned}$$

Bewijs. Dit is een eenvoudige oefening. □

Men zou geneigd kunnen zijn te denken dat $a \in R$ irreducibel is als en slechts als $(a) \trianglelefteq R$ 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 onder*[12] *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

[12] Hiermee 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. □

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 stabiliseert[13]". 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

$$(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq \dots$$

[13]Dit 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 element[14] 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. □

[14] Als 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 $\pi\colon \mathbb{C}[x_1, x_2, \dots] \to R$. Dit is een zeer courant "misbruik van notatie" voor quotiënten van veeltermringen.

[15] genoemd naar Emmy Noether.

Bovendien zijn quotiëntringen van noetherse ringen zelf ook opnieuw noethers[16], 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 $p_1, \ldots, p_k, q_1, \ldots, q_\ell$, 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 $a = a_1 \ldots a_k$, $b = b_1 \ldots b_\ell$, en $q = q_1 \ldots q_m$. Dan is $pq_1 \ldots q_m = a_1 \ldots a_k b_1 \ldots b_\ell$, 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 $p \mid b$. □

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

$$6 = 2 \cdot 3 = \big(1 + \sqrt{-5}\big)\big(1 - \sqrt{-5}\big).$$

Het is niet erg moeilijk[17] 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 $2 \mid \big(1 + \sqrt{-5}\big)\big(1 - \sqrt{-5}\big)$, terwijl $2 \nmid 1 \pm \sqrt{-5}$.

[16] Gebruik hiervoor het feit dat elk ideaal van een quotiëntring R/I van de vorm J/I is, met $I \subseteq J \trianglelefteq R$.

[17] Beschouw hiertoe de afbeelding $\mathsf{N}\colon R \to \mathbb{Z}\colon z \mapsto z\overline{z}$ 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 hernummering van de factoren p_i geassocieerd is aan q_i voor elke $i = 1, \ldots, k$.*

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 hoofideaal 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 $(a_1) \subseteq (a_2) \subseteq \ldots$ 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). □

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. □

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. □

In het bijzonder zien we dat de ringen $\mathbb{Z}[x]$, $\mathbb{Z}[x_1, \ldots, x_n]$ en $F[x_1, \ldots, x_n]$ met F een veld, unieke factorisatiedomeinen zijn.

Oefeningen

118. 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 $p = \pi\overline{\pi}$.

(b) Zij π een Gauss priem. Bewijs dat $\pi\overline{\pi}$ ofwel een geheel priemgetal is, ofwel het kwadraat is van een geheel priemgetal.

119. 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 polynoom $f \in \mathbb{Z}[x]$ gegeven door $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ wordt *primitief* genoemd, als de coëfficiënten $a_0, \ldots, a_n$ 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 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

$$\Theta \colon \mathbb{Z}[x] \to (\mathbb{Z}/p)[x]$$

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. □

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 irreducibel*[18] *is in $\mathbb{Z}[x]$, dan is het ook irreducibel in $\mathbb{Q}[x]$.*

Bewijs. Neem zonder verlies van algemeenheid aan dat de hoogstegraadscoefficiënt van f positief is. Aangezien f irreducibel is in $\mathbb{Z}[x]$ en niet-constant

[18] We 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 $\mathbb{Q}[x]$. □

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 $f(x) = a_0 + a_1x + \cdots + a_nx^n$, en zij p een priemgetal zodat $p \nmid a_n$, terwijl $p \mid a_i$ voor alle $i \in \{0, \ldots, n-1\}$, 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 $\Theta\colon \mathbb{Z}[x] \to (\mathbb{Z}/p)[x]$, 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 $\mathbb{Q}$. □

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*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}\,.$$

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

120. 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.

121. Zij $f \in \mathbb{Z}[x]$ een *monisch* polynoom, en $r \in \mathbb{Q}$ een wortel van f. Toon aan dat $r \in \mathbb{Z}$.

122. Bewijs dat de kern van het morfisme $\mathbb{Z}[x] \to \mathbb{R}$ dat x afbeeldt op $1 + \sqrt{2}$ een hoofdideaal is, en zoek een voortbrenger voor dit ideaal.

123. 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 $R_1, \ldots, R_n$ 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 $R_1, \ldots, R_n$ noemen, als volgt:

$$R = \{(r_1, \ldots, r_n) \mid r_i \in R_i \text{ voor elke } i\},$$

met de componentsgewijze optelling en vermenigvuldiging, i.e.

$$(r_1, \ldots, r_n) + (r'_1, \ldots, r'_n) = (r_1 + r'_1, \ldots, r_n + r'_n),$$

$$(r_1, \ldots, r_n) \cdot (r'_1, \ldots, r'_n) = (r_1 r'_1, \ldots, r_n r'_n)\,,$$

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 $(0_{R_1}, \ldots, 0_{R_n})$ en eenheid $(1_{R_1}, \ldots, 1_{R_n})$.

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 $I, J \trianglelefteq R$ 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 $I_1, \ldots, I_s$ 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 $J = I_1 \cdots I_{s-1} \trianglelefteq R$. 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 $JI_s = J \cap I_s$, en het gestelde volgt nu door de inductiehypothese toe te passen op de idealen $I_1, \ldots, I_{s-1}$. □

Stelling 2.8.5 (Chinese reststelling)**.** *Zij R een ring, en beschouw idealen $I_1, \ldots, I_s$ van R die paarsgewijze copriem zijn; stel $I = I_1 \cdots I_s$. Dan is de afbeelding*

$$\varphi\colon R/I \to R/I_1 \times \cdots \times R/I_s\colon r + I \mapsto (r + I_1, \ldots, r + I_s)$$

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 $e_i := (0 + I_1, \ldots, 1 + I_i, \ldots, 0 + I_s)$ 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 $z = (r_1 + I_1, \ldots, r_s + I_s) \in R/I_1 \times \cdots \times R/I_s$ willekeurig. Dan is $\varphi(r_1 b_1 + \cdots + r_s b_s + I) = z$, en we besluiten dat φ surjectief is. □

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 129.

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

124. 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.)

125. 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.

126. 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.