Ringen en lichamen

door

H.W. Lenstra, Jr en F. Oort

(Herziene versie, augustus 2015)

Inhoudsopgave

Voorwoord

Deze syllabus is een bewerkte editie van twee syllabi geschreven door H.W. Lenstra en F. Oort (Algebra, delen B en C). Deze syllabi stammen uit de jaren 1980 en zijn lange tijd in Utrecht en Amsterdam gebruikt. Er is een hele generatie van Nederlandse wiskundigen die hun Algebra uit deze syllabi hebben geleerd.

De oorspronkelijke syllabi Algebra van Lenstra en Oort zijn met de typmachine geschreven; ze stammen uit de tijd dat TEX nog niet algemeen in gebruik was. In de jaren 1990 is door B. van Geemen en J. Top in LATEX een bewerking gemaakt van de delen over ringen en lichamen.

De voorliggende syllabus is feitelijk een terugkeer naar de versie van Lenstra en Oort. Deze is in 2013 in Nijmegen door Ben Moonen en Johan Commelin in LATEX overgezet. Grote delen zijn een letterlijke reproductie van de oorspronkelijke tekst. De belangrijkste wijziging is dat de moderne conventie gevolgd wordt die zegt dat ringen, deelringen en ringhomomorfismen per definitie unitair zijn.

We dank Lenstra en Oort voor hun permissie dit materiaal opnieuw in gebruik te nemen. Correcties en suggesties voor verbeteringen zijn zeer welkom, bij voorkeur per email aan b.moonen@science.ru.nl of l.d.j.taelman@uva.nl.

B.J.J. Moonen, L.D.J. Taelman

Augustus 2014

Deel I

RINGEN

Hoofdstuk 1

Definitie, voorbeelden, elementaire eigenschappen

Definitie 1.1. Een *ring* is een vijftupel $(R, +, \cdot, 0, 1)$ met R een verzameling, $+$ en $\cdot$ afbeeldingen:

$$+ \colon R \times R \to R, \quad (a, b) \mapsto a + b \qquad \cdot \colon R \times R \to R, \quad (a, b) \mapsto ab,$$

en 0 en 1 elementen van R, zodanig dat de volgende eigenschappen (R1) t/m (R4) gelden:

(R1) $(R, +, 0)$ is een *abelse groep*; dit houdt dus in:

- **(G1)** $a + (b + c) = (a + b) + c$ voor alle $a, b, c \in R$;
- **(G2)** $0 + a = a + 0 = a$ voor alle $a \in R$;
- **(G3)** voor elke $a \in R$ is er een tegengestelde $-a \in R$ waarvoor geldt $a + (-a) = (-a) + a = 0$;
- **(G4)** $a + b = b + a$ voor alle $a, b \in R$.

(R2) $a(bc) = (ab)c$ voor alle $a, b, c \in R$ (*associativiteit* van $\cdot$);

(R3) $a(b + c) = ab + ac$ en $(b + c)a = ba + ca$ voor alle $a, b, c \in R$ (de *distributieve* wetten).

(R4) $1a = a1 = a$ voor alle $a \in R$.

Een ring R heet *commutatief* als bovendien voldaan is aan (R5):

(R5) $ab = ba$ voor alle $a, b \in R$.

Als $a, b \in R$ dan heten $a + b$ en ab de som en het product van a en b; het product ab wordt soms ook genoteerd als $a \cdot b$. De afbeeldingen $+$ en $\cdot$ heten de optelling en de vermenigvuldiging in R. Als $(R, +, \cdot, 0, 1)$ een ring is zegt men wel dat R een ring is met optelling $+$, vermenigvuldiging $\cdot$, nulelement 0 en eenheidselement 1. Een triviaal voorbeeld van een ring is de *nulring* $(\{0\}, +, \cdot, 0, 0)$, met $0 + 0 = 0 \cdot 0 = 0$.

Een *delingsring* (of *scheeflichaam*) is een ring R die behalve aan (R1) t/m (R4) ook voldoet aan (R6):

(R6) $1 \neq 0$, en voor alle $a \in R, a \neq 0$ is er een inverse $a^{-1} \in R$ waarvoor geldt $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Een *lichaam* (Engels: field; Frans: corps; Duits: Körper) is een *commutatieve* delingsring (dus (R1) t/m (R6)). Een eenvoudig voorbeeld van een lichaam is de verzameling $\{0,1\}$ met optelling als in de abelse groep $\mathbb{Z}/2\mathbb{Z}$ en product $0\cdot 0 = 0\cdot 1 = 1\cdot 0 = 0$ en $1\cdot 1 = 1$. Het eenheidselement is 1, dit lichaam geven we aan met $\mathbb{F}_2$.

Voorbeeld 1.2. De verzamelingen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ der gehele, rationale, reële, complexe getallen (respectievelijk) zijn met de gebruikelijke optelling en vermenigvuldiging ringen. Verder zijn $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ commutatief. De ringen $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ zijn lichamen, maar $\mathbb{Z}$ niet (aan (R6) is niet voldaan).

Voorbeeld 1.3. Laat $n \in \mathbb{Z}_{>0}$. Op de verzameling $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ met $\overline{i} = i + n\mathbb{Z} \subset \mathbb{Z}$, is een optelling gedefinieerd, omdat dit de nevenklassen zijn van de normale ondergroep $n\mathbb{Z}$ van $\mathbb{Z}$. De regel

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

waarbij de $\cdot$ rechts de gewone vermenigvuldiging in $\mathbb{Z}$ is, definieert een product (ga na dat als $\overline{a} = \overline{a_1}$ en $\overline{b} = \overline{b_1}$ dat dan $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$).

Ten opzichte van deze bewerkingen is $\mathbb{Z}/n\mathbb{Z}$ een commutatieve ring met eenheidselement $\overline{1}$. In 1.20 zullen we zien dat $\mathbb{Z}/n\mathbb{Z}$ een lichaam is dan en slechts dan als n een priemgetal is. Voor $n = 1$ is $\mathbb{Z}/n\mathbb{Z}$ de nulring.

Voorbeeld 1.4. Laat $n \in \mathbb{Z}_{\geq 0}$. De verzameling $\mathrm{M}(n, \mathbb{R})$ der $n \times n$-matrices met reële coëfficiënten is, met de gebruikelijke matrix-optelling en matrix-vermenigvuldiging, een ring. Voor $n \geq 2$ is deze ring niet commutatief.

Op analoge wijze kan men voor een willekeurige ring R en $n \in \mathbb{Z}_{\geq 0}$ de ring $\mathrm{M}(n, R)$ definiëren.

Voorbeeld 1.5. De ring $\mathbb{H}$ van Hamiltonse *quaternionen* (naar Sir William Rowan Hamilton, Engels-Iers wiskundige, 1805–1865) bestaat uit uitdrukkingen (quaternionen) van de vorm

$$a + bi + cj + dk, \qquad \text{met} \quad a, b, c, d \in \mathbb{R}.$$

Twee quaternionen zijn gelijk als de componenten het zijn:

$$a + bi + cj + dk = a' + b'i + c'j + d'k \quad \Longleftrightarrow \quad a = a', b = b', c = c', d = d'.$$

Quaternionen worden componentsgewijs opgeteld:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k\,.$$

De vermenigvuldiging van quaternionen berust op de regels

$$i^2 = j^2 = k^2 = -1$$

samen met

$$\begin{array}{lll} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Om een ring te verkrijgen moet (R3) gelden en daarmee kunnen we de vermenigvuldiging in $\mathbb{H}$ uitwerken. We vinden:

$$(a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) = (aa'-bb'-cc'-dd') + (ab'+ba'+cd'-dc')i \\ + (ac'-bd'+ca'+db')j + (ad'+bc'-cb'+da')k$$

Men kan nu rechtstreeks verifiëren dat de quaternionen een ring vormen. We vatten $\mathbb{R}$ op als deelverzameling van $\mathbb{H}$ door $a \mapsto a+0i+0j+0k$.

Voor een quaternion $q = a+bi+cj+dk$ schrijven we

$$\overline{q} = a-bi-cj-dk\,,$$

en we definiëren

$$N(q) = q\overline{q} = (a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2\,.$$

I.h.b. geldt $N(q) \in \mathbb{R}$ voor elk quaternion q. Merk verder op dat $q\overline{q} = \overline{q}q$ en dat

$$N(q) \neq 0 \quad \Longleftrightarrow \quad q \neq 0.$$

Dit impliceert dat $\mathbb{H}$ een delingsring is, aangezien $1/N(q)\cdot\bar{q}$ een inverse van q is als $q \neq 0$. Uiteraard is deze ring niet-commutatief, zoals duidelijk is uit de rekenregels voor i, j en k.

Voor meer voorbeelden van ringen en methoden om ringen te construeren verwijzen we naar het einde van dit hoofdstuk.

Definitie 1.6. Een deelverzameling R' van een ring R heet een *deelring* van R als aan (D1), (D2) en (D3) voldaan is:

(D1) $1 \in R'$;

(D2) R' is een ondergroep van de additieve groep van R;

(D3) $ab \in R'$ voor alle $a, b \in R'$.

Voorwaarde (D2) is equivalent met $0 \in R'$ en $a-b \in R'$ voor alle $a, b \in R'$.

Een deelring R' van een ring R is zelf een ring, met de optelling en vermenigvuldiging van R. Is R commutatief, dan is R' het ook.

Een triviaal voorbeeld van een deelring van R is R zelf.

Voorbeeld 1.7. De verzameling $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ is met de gewone optelling en vermenigvuldiging van complexe getallen een ring, en is dus een deelring van $\mathbb{C}$. We noemen $\mathbb{Z}[i]$ wel de *ring van gehele getallen van Gauss*. Het is een commutatieve ring, maar geen lichaam. De verzameling $\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\}$ is ook een deelring van $\mathbb{C}$ en is wél een lichaam: de inverse van $a+bi(\neq 0)$ wordt gegeven door $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$. Analoge opmerkingen zijn van toepassing op

$$\mathbb{Z}[\sqrt{m}] = \{a+b\sqrt{m} \mid a,b \in \mathbb{Z}\},$$
$$\mathbb{Q}[\sqrt{m}] = \{a+b\sqrt{m} \mid a,b \in \mathbb{Q}\},$$

waar m een geheel getal voorstelt dat niet een kwadraat is (dus met $m=-1$ vindt men $\mathbb{Z}[i]$ en $\mathbb{Q}[i]$).

Stelling 1.8. *Laat R een ring zijn. Dan geldt voor alle $a, b, b_1, \ldots, b_n, c \in R$:*

$$\begin{aligned} a(b_1 + b_2 + \cdots + b_n) &= ab_1 + ab_2 + \cdots + ab_n, \\ (b_1 + b_2 + \cdots + b_n)a &= b_1a + b_2a + \cdots + b_na, \\ a(b - c) &= ab - ac \\ a \cdot 0 &= 0 \cdot a = 0. \end{aligned}$$

Bewijs. De eerste twee volgen met volledige inductie naar n uit de distributieve wet (R3). Verder geldt

$$a(b - c) + ac = a((b - c) + c) = ab$$

dus $a(b - c) = ab - ac$. Tenslotte

$$a \cdot 0 = a \cdot (0 - 0) = a \cdot 0 - a \cdot 0 = 0$$

en analoog $0 \cdot a = 0$. Dit bewijst de stelling. □

Wegens (R1) is elke ring R een abelse groep ten opzichte van de optelling. Deze groep geeft men wel aan met R^+; dus R^+ is dezelfde verzameling als R, met dezelfde optelling, maar de vermenigvuldiging is "vergeten".

Ten opzichte van de vermenigvuldiging vormt een ring R nooit een groep, tenzij $R = \{0\}$. De volgende definitie geeft ons de mogelijkheid toch over een multiplicatieve groep te spreken.

Definitie 1.9. Zij R een ring. Een element $a \in R$ heet een *eenheid* (of inverteerbaar) als er een $b \in R$ bestaat met $ab = ba = 1$. (Let op het merkwaardige taalgebruik: het eenheidselement is wel een eenheid, maar niet andersom.) De verzameling eenheden van R wordt genoteerd R^* en heet de *eenhedengroep* van R (het is namelijk een groep, zie Stelling 1.12). Men vindt ook wel de notatie $U(R)$ (unit (Engels) = eenheid).

Een element $a \in R$ noemt men een *linkseenheid* als er een $b \in R$ is met $ab = 1$ en een *rechtseenheid* als er een $c \in R$ bestaat met $ca = 1$.

1.10 Als $a \in R$ zowel een links- als rechtseenheid is, dan is a een eenheid; immers, uit $ab = 1$ en $ca = 1$ volgt dat $b = cab = c$.

In een commutatieve ring is "linkseenheid" (of "rechtseenheid") natuurlijk hetzelfde als "eenheid", maar in een niet-commutatieve ring hoeft een linkseenheid niet een rechtseenheid te zijn; zie 1.27.

Uit (R6) volgt:

$$R \text{ is een delingsring} \quad \Longleftrightarrow \quad R^* = R - \{0\}.$$

Voorbeeld 1.11. Er geldt:

$$\mathbb{Z}^* = \{1, -1\}, \quad \mathbb{Q}^* = \mathbb{Q} - \{0\}, \quad \mathbb{R}^* = \mathbb{R} - \{0\}, \quad \mathbb{C}^* = \mathbb{C} - \{0\}, \quad \mathbb{H}^* = \mathbb{H} - \{0\}\,.$$

Stelling 1.12. *De eenhedengroep R^* van een ring R is een groep ten opzichte van de vermenigvuldiging.*

Bewijs. Eerst tonen we aan dat $ab \in R^*$ als $a, b \in R^*$. Welnu, als $a, b \in R^*$ dan zijn er $c, d \in R$ met $ac = ca = 1$, $bd = db = 1$, en hieruit volgt dat $(ab) \cdot (dc) = (dc) \cdot (ab) = 1$, met $dc \in R$; dus $ab \in R^*$.

De associativiteit van het product volgt direct uit (R2).

Er is een neutraal element in R^*; immers, $1 \in R^*$ want $1 \cdot 1 = 1$, en uit (R4) laat zien dat 1 aan de eis $a \cdot 1 = 1 \cdot a = a$ voldoet.

Als tenslotte $a \in R^*$ dan is er een $b \in R$ met $ab = ba = 1$; voor deze b geldt natuurlijk $b \in R^*$, dus elk element van R^* heeft een inverse in R^*.

Hiermee zijn de axioma's voor een groep geverifieerd en is de stelling bewezen. □

Als R commutatief is, dan is R^* natuurlijk abels. De omkering geldt niet: men kan een niet-commutatieve ring R construeren waarvoor R^* abels is, zie opgave 15.

Voorbeeld 1.13. Indien $A \in \mathrm{M}(n, \mathbb{R})$ inverteerbaar is met inverse B dan geldt $AB = BA = I$, met I de identiteitsmatrix. Bovendien geldt:

$$A \text{ is een linkseenheid} \quad \Longleftrightarrow \quad A \text{ is een rechtseenheid} \quad \Longleftrightarrow \quad \det(A) \neq 0.$$

Dus $\mathrm{M}(n, \mathbb{R})^* = \mathrm{GL}(n, \mathbb{R})$ (dit is in feite de definitie van de groep $\mathrm{GL}(n, \mathbb{R})$). We kunnen hier $\mathbb{R}$ ook vervangen door een willekeurige andere commutatieve ring.

Voorbeeld 1.14. Zij $R = \mathbb{Z}[\sqrt{m}]$ als in 1.7, waar m een geheel getal is dat geen kwadraat is. We definieren de *norm*

$$N \colon R \to \mathbb{Z} \quad \text{door} \quad N(a + b\sqrt{m}) = (a + b\sqrt{m}) \cdot (a - b\sqrt{m}) = a^2 - mb^2.$$

Gemakkelijk rekent men na: $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ voor alle $\alpha, \beta \in R$, en verder $N(0) = 0$ en $N(1) = 1$. We beweren:

$$\alpha \in R^* \quad \Longleftrightarrow \quad N(\alpha) = \pm 1.$$

Voor $\Leftarrow$: als $\alpha = a + b\sqrt{m}$ en $N(\alpha) = \pm 1$, dan geldt $(a + b\sqrt{m}) \cdot (a - b\sqrt{m}) = \pm 1$, dus $\pm(a - b\sqrt{m})$ is een inverse van α. Voor $\Rightarrow$: als $\alpha\beta = 1$ dan $N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(1) = 1$, en $N(\alpha)$, $N(\beta) \in \mathbb{Z}$, dus $N(\alpha) = N(\beta) = \pm 1$.

Hiermee zien we dat het zoeken van eenheden in $\mathbb{Z}[\sqrt{m}]$ equivalent is met het oplossen van de vergelijking

$$a^2 - m \cdot b^2 = \pm 1$$

in gehele getallen a, b.

Voor $m < 0$ is het oplossen van deze vergelijking eenvoudig: er geldt $a^2 - m \cdot b^2 = a^2 + |m| \cdot b^2$, en omdat kwadraten positief zijn kan dit alleen gelijk aan ± 1 zijn in de gevallen

$$a = \pm 1, b = 0, \qquad \text{en} \qquad a = 0, b = \pm 1, |m| = 1.$$

Dus er geldt

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\} \qquad (\text{het geval } m = -1),$$

$$\mathbb{Z}[\sqrt{m}]^* = \{1, -1\} \qquad \text{als} \quad m < -1.$$

Voor $m > 0$ (maar geen kwadraat) is de vergelijking $x^2 - my^2 = \pm 1$ veel interessanter. Men kan bewijzen dat de "vergelijking van Pell" $x^2 - my^2 = 1$ steeds een oplossing $x, y \in \mathbb{Z}_{>0}$ heeft. Dit levert een eenheid $\epsilon = x + y\sqrt{m} > 1$ van R, en oneindig veel eenheden van R worden dan gegeven door $\ldots, \pm\epsilon^{-2}, \pm\epsilon^{-1}, \pm 1, \pm\epsilon, \pm\epsilon^2, \ldots$. Blijkbaar heeft de vergelijking van Pell dus ook oneindig veel oplossingen.

Voorbeeld: voor $m = 2$ is $x_1 = y_1 = 1$ een oplossing van $x^2 - 2y^2 = \pm 1$, dus $\epsilon = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$. Beschouwing van $\epsilon^n, n \geq 0$, levert de oplossingen

$$\begin{array}{llll} x_0 = 1 & y_0 = 0 & x_5 = 41 & y_5 = 29 \\ x_1 = 1 & y_1 = 1 & x_6 = 99 & y_6 = 70 \\ x_2 = 3 & y_2 = 2 & x_7 = 239 & y_7 = 169 \\ x_3 = 7 & y_3 = 5 & & \\ x_4 = 17 & y_4 = 12 & & \end{array}$$

(Algemeen: $x_{n+1} = 2x_n + x_{n-1}$ en $y_{n+1} = 2y_n + y_{n-1}$.)

Voor $m = 67$ is de "eenvoudigste eenheid" die met $x = 48842$ en $y = 5967$. Voor meer informatie zie: H. Davenport, The higher arithmetic, Ch. IV, section 11. Daar vindt men ook uitgelegd dat de naam van John Pell (1611-1685) ten onrechte aan de vergelijking verbonden is.

In een willekeurige ring kan het gebeuren dat $a \cdot b = 0$ terwijl $a \neq 0$ en $b \neq 0$. Bijvoorbeeld geldt $\overline{2} \cdot \overline{3} = \overline{0}$ in $\mathbb{Z}/6\mathbb{Z}$. In $\mathbb{Z}/8\mathbb{Z}$ geldt zelfs $\overline{2}^3 = \overline{0}$.

Definitie 1.15. Een element a van een ring R heet een *linkernuldeler* als $a \neq 0$ en er een $b \in R$ bestaat zo dat $b \neq 0$ en $ab = 0$. Evenzo heet a een *rechternuldeler* als $a \neq 0$ en er een $c \in R$ bestaat met $c \neq 0$ en $ca = 0$. We noemen $a \in R$ een *nuldeler* als het een linker- of rechternuldeler is.

Een *nilpotent element* is een $a \in R - \{0\}$ zo dat $a^n = 0$ voor zekere $n \in \mathbb{N}$. Een nilpotent element is i.h.b. een nuldeler, zowel links als rechts.

Een element $a \in R$ noemt men een *idempotent element*, of *idempotent*, als $a^2 = a$. Een idempotent element a met $a \notin \{0, 1\}$ is een nuldeler (zowel links als rechts), want $a^2 = a$ impliceert $a(a-1) = (a-1)a = 0$ en $0 \neq a \neq 1$ impliceert dat a en $a - 1$ ongelijk aan 0 zijn.

Voorbeeld 1.16. In $\mathrm{M}(2, \mathbb{R})$ bekijken we de volgende elementen:

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad c = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ga na dat $ab = 0$, dus a is een linkernuldeler en b is een rechternuldeler. Merk op dat $ba \neq 0$, maar $ca = 0$, dus a is (toch) een rechternuldeler. Bovendien is $a^2 = 0$, dus a is een nilpotent element (dit toont ook aan dat a zowel rechter- als linkernuldeler is).

Merk op dat $b^2 = b$ en $c^2 = c$, dus b en c zijn idempotente elementen.

Stelling 1.17. *Een element a van een ring R kan niet tegelijk nuldeler en eenheid zijn.*

Bewijs. Stel dat a een linkernuldeler is: $a \neq 0$, en $ab = 0$, met $b \in R, b \neq 0$; en tevens een eenheid: $ac = ca = 1$ ($c \in R$). Dan geldt $c \cdot a \cdot b = 1 \cdot b = b$ en ook $c \cdot a \cdot b = c \cdot 0 = 0$, dus $b = 0$, een tegenspraak. Het geval dat a een rechternuldeler is wordt analoog afgehandeld. Dit bewijst 1.17. □

Opmerking 1.18. Het bewijs van 1.17 laat zien dat in een willekeurige (niet noodzakelijk commutatieve) ring een linkernuldeler geen rechtseenheid kan zijn. Evenzo kan een rechternuldeler geen linkseenheid zijn. In 1.28 zullen we aan de hand van een voorbeeld zien dat een linkernuldeler wel een linkseenheid kan zijn.

Gevolg 1.19. *Een delingsring heeft geen nuldelers.*

Bewijs. Dit volgt uit 1.17, want alle elementen $\neq 0$ van een delingsring zijn eenheden. □

Stelling 1.20. *Voor $n \in \mathbb{Z}_{>0}$ geldt:*

$$\mathbb{Z}/n\mathbb{Z} \text{ is een lichaam} \quad \Longleftrightarrow \quad n \text{ is een priemgetal.}$$

Bewijs. Voor een commutatieve ring R geldt:

$$R \text{ is een lichaam} \quad \Longleftrightarrow \quad R^* = R - \{0\}$$

Als n niet priem is, dan kunnen we schrijven $n = ab$, met $0 < a, b < n$ en dus

$$\bar{a}, \bar{b} \neq \bar{0} \in \mathbb{Z}/n\mathbb{Z} \qquad \text{maar} \quad \bar{a}\bar{b} = \bar{n} = \bar{0}.$$

Het element $\bar{a} \in \mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}$ is dan een nuldeler, en wegens Gevolg 1.19 is is $\mathbb{Z}/n\mathbb{Z}$ geen delingsring, en dus geen lichaam.

Als n wel priem is, en $\bar{a} \neq \bar{0}$, dan moeten we laten zien dat $\bar{a}$ een inverse heeft. Welnu, de optelgroep $(\mathbb{Z}/n\mathbb{Z})^+$ heeft orde n, een priem. De ondergroep voortgebracht door $\bar{a}$ is dus heel $(\mathbb{Z}/n\mathbb{Z})^+$. Omdat $\bar{1} \in (\mathbb{Z}/n\mathbb{Z})^+$, is er dan een $m \in \mathbb{Z}$ zodat $m\bar{a} = \bar{a} + \ldots + \bar{a}$ (m keer) gelijk is aan $\bar{1}$. Dan is dus $\bar{m}\bar{a} = \bar{a}\bar{m} = \bar{1}$, en $\bar{m}$ is de gezochte inverse van $\bar{a}$.

Hiermee is Stelling 1.20 bewezen. □

Voor een priemgetal p schrijven we $\mathbb{F}_p$ voor het lichaam $\mathbb{Z}/p\mathbb{Z}$; dus $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In Hoofdstuk 12 zullen we ook voor zekere andere getallen q een lichaam $\mathbb{F}_q$ definiëren; als q niet priem is, is $\mathbb{F}_q$ *niet* hetzelfde als $\mathbb{Z}/q\mathbb{Z}$.

Definitie 1.21. Een *domein* (of *integriteitsgebied*) is een commutatieve ring met $1 \neq 0$ zonder nuldelers.

Voorbeeld 1.22. Voorbeelden van domeinen zijn lichamen (wegens 1.19), zoals $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ en $\mathbb{F}_{59}$, en ook deelringen van lichamen, zoals $\mathbb{Z}, \mathbb{Z}[i]$. In 1.26 zullen we zien dat ieder domein deelring van een lichaam is.

Geen domeinen zijn $\mathbb{H}$ (niet commutatief), $\mathbb{Z}/1\mathbb{Z}$ ($1 = 0$) en $\mathbb{Z}/57\mathbb{Z}$ ($\overline{3} \cdot \overline{19} = \bar{0}$, dus nuldelers).

Stelling 1.23. *Zij R een ring zonder nuldelers (bijv. een domein).*

(a) *Voor alle a, $b \in R$ geldt: $ab = 0 \quad \Leftrightarrow \quad a = 0$ of $b = 0$,*

(b) *Voor alle a, b en c in R geldt: $ab = ac \quad \Leftrightarrow \quad a = 0$ of $b = c$.*

Bewijs. (a) $\Leftarrow$ is een gevolg van 1.8; $\Rightarrow$: als $ab = 0$ en $a \neq 0 \neq b$, dan zouden a en b nuldelers zijn, een tegenspraak.

(b) Er geldt:

$$\begin{aligned} ab = ac &\Leftrightarrow ab - ac = 0 \\ &\Leftrightarrow a(b-c) = 0 && \text{(wegens 1.8)} \\ &\Leftrightarrow a = 0 \quad \text{of} \quad b - c = 0 && \text{(wegens onderdeel (a))} \\ &\Leftrightarrow a = 0 \quad \text{of} \quad b = c \end{aligned}$$

Dit bewijst 1.23. □

We geven enkele belangrijke manieren om ringen te construeren.

1.24 Product van ringen. Als R_1 en R_2 ringen zijn, dan definiëren we op $R = R_1 \times R_2$ een optelling en een vermenigvuldiging door

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2), \qquad (r_1, r_2) \cdot (s_1, s_2) = (r_1 s_1, r_2 s_2)$$

Hierin zijn $r_1, s_1 \in R_1, r_2, s_2 \in R_2$. Het is eenvoudig na te gaan dat R hiermee een ring wordt. Als we het nulelement en het eenheidselement van R met 0_R en 1_R resp. aanduiden dan geldt $0_R = (0, 0)$ en $1_R = (1, 1)$. Deze ring is commutatief dan en slechts dan als R_1 en R_2 beide commutatief zijn. Er geldt $R^* = R_1^* \times R_2^*$. De bewijzen van deze beweringen worden aan de lezer overgelaten (zie opgave 8).

Een ring $R_1 \times R_2$ met $R_1 \neq \{0\}$ en $R_2 \neq \{0\}$ heeft altijd nuldelers, want

$$(a, 0) \cdot (0, b) = (a \cdot 0, 0 \cdot b) = (0, 0),$$

voor alle $a \in R_1$ en $b \in R_2$.

Tenslotte merken we op dat de elementen $(1, 0)$ en $(0, 1)$ idempotenten van $R_1 \times R_2$ zijn.

1.25 Polynoomringen. Laat R een ring zijn. Een *polynoom* (of veelterm) met coëfficiënten in R is een uitdrukking $\sum_{i=0}^{\infty} a_i X^i$, met $a_i \in R$ voor alle $i \geq 0$, en bijna alle a_i gelijk aan nul (d.w.z., er is een n zo dat $a_i = 0$ voor alle $i > n$). De a_i heten de *coëfficiënten* van het polynoom $\sum_{i=0}^{\infty} a_i X^i$. Twee polynomen $\sum_{i=0}^{\infty} a_i X^i$ en $\sum_{i=0}^{\infty} b_i X^i$ zijn gelijk dan en slechts dan als $a_i = b_i$ voor alle i.

In plaats van het symbool X gebruikt men ook wel andere letters, zoals Y, Z, U, T, X_0, $X_1, \ldots$. Als $a_i = 0$ voor $i > n$ dan schrijft men het polynoom $\sum_{i=0}^{\infty} a_i X^i$ ook wel als

$$a_0 + a_1 X + \cdots + a_n X^n \,.$$

Termen $a_i X^i$ met $a_i = 0$ kan men hierin weglaten. Verder schrijft men $1 \cdot X^i$ als X^i, en $(-a) \cdot X^i$ als $-aX^i$. Bijvoorbeeld:

$$1 - 2X + X^3 = 1 + (-2) \cdot X + 0 \cdot X^2 + 1 \cdot X^3 \,.$$

De *graad* $\mathrm{gr}(f)$ (of $\mathrm{graad}(f)$ of $\deg(f)$; Engels: degree) van een polynoom $f = \sum_{i=0}^{\infty} a_i X^i$ is de grootste n met $a_n \neq 0$; dus $\mathrm{gr}(1 - 2X + X^3) = 3$. Voor het *nulpolynoom* $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$ is de definitie

van de graad een kwestie van conventie. Men kan de graad van het nulpolynoom beschouwen als zijnde ongedefinieerd. Een andere mogelijkheid, die voor veel uitspraken goed werkt, is om af te spreken dat we definiëren $\mathrm{gr}(0) = -\infty$. (Men komt ook nog andere definities voor $\mathrm{gr}(0)$ tegen.) We zullen in deze syllabus uitgaan van deze laatste conventie, maar in gevallen waar er verwarring zou kunnen optreden, noemen we het nulpolynoom apart.

De *j-de coëfficiënt* van een polynoom $f = \sum_{i=0}^{\infty} a_i X^i$ is a_j. De *constante* coëfficiënt is de nulde coëfficiënt a_0. Een *constant polynoom* f is een polynoom met $\mathrm{gr}(f) \leq 0$, d.w.z., met $a_n = 0$ voor $n \geq 1$. Als $f \neq 0$ en $n = \mathrm{gr}(f)$, dan heet a_n de *kopcoëfficiënt* van f. Een polynoom met kopcoëfficiënt 1 heet *monisch*.

We definiëren nu een optelling en een product op de verzameling van polynomen. De *som* van twee polynomen is gedefinieerd door:

$$\left(\sum_{i=0}^{\infty} a_i \cdot X^i\right) + \left(\sum_{i=0}^{\infty} b_i \cdot X^i\right) = \sum_{i=0}^{\infty} (a_i + b_i) \cdot X^i.$$

Vermenigvuldiging van polynomen is bepaald door de regel

$$(a_i X^i) \cdot (b_j X^j) = (a_i \cdot b_j) X^{i+j}$$

en de distributieve wet; dus:

$$\left(\sum_{i=0}^{\infty} a_i \cdot X^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j \cdot X^j\right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j\right) \cdot X^k.$$

Bijvoorbeeld,

$$\begin{aligned}(7 + 3X)(5 - X + 2X^2) &= 7 \cdot 5 + (7 \cdot (-1) + 3 \cdot 5)X + (7 \cdot 2 + 3 \cdot (-1))X^2 + 3 \cdot 2X^3 \\ &= 35 + 8X + 11X^2 + 6X^3\,.\end{aligned}$$

De verzameling van alle polynomen met coëfficiënten in R wordt aangegeven met $R[X]$. We beweren nu: $R[X]$ is met de zojuist gedefinieerde optelling en vermenigvuldiging een *ring*, de *polynoomring in één veranderlijke* over R.

Het bewijs hiervan is rechttoe rechtaan. Bij wijze van voorbeeld controleren we (R3), de associativiteit van de vermenigvuldiging:

$$\begin{aligned}\left(\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j X^j\right)\right) \cdot \left(\sum_{k=0}^{\infty} c_k X^k\right) &= \left(\sum_{l=0}^{\infty} \left(\sum_{\substack{i,j \\ i+j=l}} a_i b_j\right) X^l\right) \cdot \left(\sum_{k=0}^{\infty} c_k X^k\right) \\ &= \sum_{m=0}^{\infty} \left(\sum_{\substack{l,k \\ l+k=m}} \left(\sum_{\substack{i,j \\ i+j=l}} a_i b_j\right) c_k\right) X^m = \sum_{m=0}^{\infty} \left(\sum_{\substack{i,j,k \\ i+j+k=m}} a_i b_j c_k\right) X^m,\end{aligned}$$

en analoog laat men zien dat ook $\left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\left(\sum_{j=0}^{\infty} b_j X^j\right) \cdot \left(\sum_{k=0}^{\infty} c_k X^k\right)\right)$ hieraan gelijk is. Dit bewijst (R3). We laten (R1), (R2) en (R4) aan de lezer over.

Als R commutatief is, is $R[X]$ het ook. We kunnen R opvatten als deelring van $R[X]$ (nl. de verzameling "constante" polynomen). Het constante polynoom 1 is ook het eenheidselement van $R[X]$. Als R geen nuldelers heeft, dan heeft $R[X]$ evenmin nuldelers (zie Opgave 26), en er geldt dan

$$\mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g) \qquad \text{voor } f, g \in R[X] - \{0\}.$$

Als R een domein is dan is ook $R[X]$ een domein.

Met inductie definieert men de polynoomring in n variabelen over R door

$$R[X_1, X_2, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])\,[X_n].$$

Elementen van $R[X_1, X_2, \ldots, X_n]$ zijn eindige sommen

$$f = \sum_{i_1 \geq 0, i_2 \geq 0, \ldots, i_n \geq 0} a_{i_1 i_2 \ldots i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

met coëfficiënten $a_{i_1 i_2 \ldots i_n} \in R$. Eenvoudshalve gebruikt men ook wel de "multi-index"-notatie

$$f = \sum_i a_i X^i$$

waarbij de "multi-index" $i = (i_1, i_2, \ldots, i_n)$ loopt over een eindige verzameling n-tallen van niet-negatieve gehele getallen, en X^i een afkorting is voor $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$.

Voor polynomen in meer variabelen laten zich verschillende graden definiëren. Voor elke j met $1 \leq j \leq n$ is de *graad in* X_j van het bovenstaande polynoom gedefinieerd door

$$\mathrm{gr}_j(f) = \max\bigl\{m \in \mathbb{Z}_{\geq 0} \;\big|\; \exists i_1, \ldots, i_n \text{ met } a_{i_1 i_2 \ldots i_n} \neq 0 \text{ en } i_j = m\bigr\}$$

(dus de "hoogste macht van X_j die echt voorkomt"). De *totale graad* is gedefinieerd door

$$\mathrm{totgr}(f) = \max\bigl\{m \in \mathbb{Z}_{\geq 0} \;\big|\; \exists i_1, \ldots, i_n \text{ met } a_{i_1 i_2 \ldots i_n} \neq 0 \text{ en } \sum_{j=1}^{n} i_j = m\bigr\}.$$

Voor het nulpolynoom zijn deze graden weer te beschouwen als zijnde niet gedefnieerd, of als $-\infty$.

Voorbeeld: Voor $f = X_1 X_2^4 - X_1^2 X_2^2$ geldt $\mathrm{gr}_1(f) = 2$, $\mathrm{gr}_2(f) = 4$ en $\mathrm{totgr}(f) = 5$.

1.26 Quotiëntenlichamen. Laat R een domein zijn. We gaan een lichaam construeren, het *quotiëntenlichaam* (ook wel breukenlichaam genoemd) van R, notatie: $Q(R)$, dat R omvat, en waarvan elk element geschreven kan worden als $a \cdot s^{-1}$, met $a, s \in R$, $s \neq 0$. De constructie is een directe generalisatie van de constructie van $\mathbb{Q} = Q(\mathbb{Z})$ uitgaande van $\mathbb{Z}$.

Laat $S = R - \{0\}$. Op de verzameling $R \times S = \bigl\{(a, s) \;\big|\; a, s \in R\,, s \neq 0\bigr\}$ definiëren we een equivalentierelatie $\sim$ door

$$(a, s) \sim (b, t) \qquad \Longleftrightarrow \qquad at = bs.$$

We gaan na dat dit inderdaad een equivalentierelatie is: Dat $(a, s) \sim (a, s)$ voor alle (a, s) (reflexiviteit) en dat $(a, s) \sim (b, t) \implies (b, t) \sim (a, s)$ (symmetrie) is triviaal. Rest nog de transitiviteit te bewijzen, d.w.z.

$$(a, s) \sim (b, t) \quad \text{en} \quad (b, t) \sim (c, u) \qquad \Rightarrow \qquad (a, s) \sim (c, u))\,.$$

Dit gaat als volgt: Uit $(a,s)\sim(b,t)$ volgt $at=bs$, dus ook $atu=bsu$. Uit $(b,t)\sim(c,u)$ volgt $bu=ct$, dus ook $bus=cts$. Maar R is commutatief, dus $aut=atu=bsu=bus=cts=cst$. Omdat

$$aut=cst \quad\Longrightarrow\quad (au-cs)t=0$$

en $t\neq 0$, volgt uit 1.21(b) dat $au=cs$. Hieruit volgt dat $(a,s)\sim(c,u)$, zoals verlangd.

Laat nu $Q(R)$ de verzameling equivalentieklassen van $\sim$ zijn:

$$Q(R)=(R\times S)/\sim .$$

Voor de equivalentieklasse waar (a,s) in zit voeren we de suggestieve notatie $\frac{a}{s}$ (of a/s) in. Dus er geldt:

$$Q(R)=\Big\{\frac{a}{s}\;\Big|\; a,s\in R, s\neq 0\Big\},\quad \text{met}\qquad \frac{a}{s}=\frac{b}{t}\quad\Longleftrightarrow\quad at=bs.$$

We definieren op $Q(R)$ nu een optelling en een vermenigvuldiging door

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}\quad(\text{merk op: } st\neq 0 \text{ want } R \text{ is een domein}),\qquad \frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}.$$

Natuurlijk moeten we wel nagaan dat dit niet afhangt van de keuze van de representanten, d.w.z., als $\frac{a'}{s'}=\frac{a}{s}$ en $\frac{b'}{t'}=\frac{b}{t}$ dan moeten we nagaan dat $\frac{a't'+b's'}{s't'}=\frac{at+bs}{st}$ en $\frac{a'b'}{s't'}=\frac{ab}{st}$. Inderdaad volgt uit $\frac{a'}{s'}=\frac{a}{s}$ en $\frac{b'}{t'}=\frac{b}{t}$ dat $a's=as'$ en $b't=bt'$, zodat

$$(a't'+b's')st=a'st't+b'ts's=as't't+bt's's=(at+bs)s't'$$

hetgeen betekent dat $\frac{a't'+b's'}{s't'}=\frac{at+bs}{st}$. Voor het product is het nog eenvoudiger.

De verificatie dat $Q(R)$ met deze optelling en vermenigvuldiging aan (R1) t/m (R6) voldoet is enigszins tijdrovend maar biedt in het geheel geen moeilijkheden. We concluderen dat $Q(R)$ een lichaam is.

We beschouwen R als een deelring van $Q(R)$ door het element $a\in R$ te identificeren met $\frac{a}{1}\in Q(R)$:

$$R\subset Q(R),\qquad r=\frac{r}{1}.$$

Merk hierbij op dat er zo geen twee verschillende elementen van R aan elkaar gelijk gemaakt worden, want $\frac{a}{1}=\frac{b}{1}\iff a\cdot 1=b\cdot 1\iff a=b$. Verder verandert ook de optelling of vermenigvuldiging niet, want $\frac{a}{1}+\frac{b}{1}=\frac{a\cdot 1+b\cdot 1}{1\cdot 1}=\frac{a+b}{1}$ en evenzo $\frac{a}{1}+\frac{b}{1}=\frac{ab}{1}$.

Voor $\frac{a}{s}\in Q(R)$ geldt tenslotte $\frac{a}{s}\cdot s=\frac{a}{s}\cdot\frac{s}{1}=\frac{as}{s}=\frac{a}{1}=a$, dus $\frac{a}{s}=as^{-1}$. Hiermee is de constructie van het quotiëntenlichaam van R met de aan het begin aangekondigde eigenschappen voltooid. De in voorbeeld 1.22 gedane bewering dat elk domein deelring van een lichaam is hebben we hiermee tevens bewezen.

Als K een lichaam is dan is de polynoomring $K[X]$ een domein, en we definiëren het *lichaam van rationale functies in één variabele* over K door

$$K(X)=Q(K[X])\,.$$

Elementen van $K(X)$ zijn bijvoorbeeld $\frac{1}{1+X}=\frac{X}{X+X^2}$ en $\frac{1-X^2}{1-X+X^3}$.

Voor een in de theorie van de commutatieve ringen belangrijke generalisatie van de constructie van het quotiëntenlichaam verwijzen we naar Opgave 28.

1.27 Endomorfismenringen. Zij A een additief geschreven abelse groep, en $\mathrm{End}(A)$ de verzameling endomorfismen van A:

$$\mathrm{End}(A) = \big\{ f\colon A \to A \;\big|\; f(a+b) = f(a) + f(b) \quad \forall a, b \in A \big\}.$$

Voor $f, g \in \mathrm{End}(A)$ definiëren we $f+g\colon A \to A$ en $fg\colon A \to A$ door

$$(f+g)(a) = f(a) + g(a), \quad fg(a) = f(g(a)).$$

Omdat A abels is geldt $f+g \in \mathrm{End}(A)$, en ook geldt $fg \in \mathrm{End}(A)$. Het is gemakkelijk na te gaan dat $\mathrm{End}(A)$ met deze optelling en vermenigvuldiging een ring vormt, de *endomorfismenring* van A. Het is een ring met als eenheidslement id_A, de identieke afbeelding. Deze is niet het nulelement, behalve in het geval $A = 0$.

Voorbeeld 1.28. We geven nu een voorbeeld van een linkseenheid die linkernuldeler is.

Laat $A = \mathbb{R}^n$, met $n \in \mathbb{Z}_{>0}$. Aangezien elke $n \times n$-matrix over $\mathbb{R}$ is op te vatten als een $\mathbb{R}$-lineair endomorfisme van de vectorruimte A, en matrixoptelling en -vermenigvuldiging corresponderen met de boven gedefinieerde optelling en vermenigvuldiging van endomorfismen, zien we dat $\mathrm{M}(n, \mathbb{R})$ te beschouwen is als deelring van $\mathrm{End}(A)$.

Omdat $\mathrm{M}(n, \mathbb{R})$ niet-commutatief is voor $n \geq 2$ zien we dat $\mathrm{End}(A)$ niet voor elke abelse groep A commutatief is.

Vervolgens nemen we $A = \mathbb{R}[X]^+$ (de additieve groep van de polynoomring over $\mathbb{R}$), een 'oneindigdimensionale vectorruimte' over $\mathbb{R}$. Definieer $f, g, x \in \mathrm{End}(A)$ door

$$\begin{aligned}
f\colon &\quad a_0 + a_1X + \cdots + a_nX^n \mapsto a_1 + a_2X + \ldots + a_nX^{n-1}, \\
g\colon &\quad a_0 + a_1X + \cdots + a_nX^n \mapsto a_0, \\
x\colon &\quad a_0 + a_1X + \cdots + a_nX^n \mapsto a_0X + a_1X^2 \ldots + a_nX^{n+1}.
\end{aligned}$$

We schrijven verder $1 = \mathrm{id}_A$, het eenheidselement van $\mathrm{End}(A)$. Men rekent nu eenvoudig na, dat in $\mathrm{End}(A)$ geldt:

$$fx = 1, \quad fg = 0, \quad gx = 0.$$

Dus f is een linkseenheid en een linkernuldeler in $\mathrm{End}(A)$. Wegens opmerking 1.18 kan f geen rechtseenheid of rechternuldeler zijn. Evenzo is x een rechtseenheid en een rechternuldeler, maar geen linkseenheid of linkernuldeler.

1.29 Ringen van functies. Zij V een verzameling, R een ring, en $T = R^V$ de verzameling afbeeldingen van V naar R. Men maakt T tot een ring door voor $f, g\colon V \to R$ som $f+g$ en product fg als volgt te definiëren:

$$(f+g)(v) = f(v) + g(v) \in R, \qquad (fg)(v) = f(v) \cdot g(v) \in R,$$

voor $v \in V$. Geldt $V = \{v_1, v_2, \ldots, v_n\}$, met $n \in \mathbb{Z}_{>0}$ en $v_i \neq v_j$ voor $i \neq j$, dan zien we dat R^V "dezelfde" ring is als $R \times R \times \cdots \times R$ (product van ringen: zie 1.24; n factoren) door $f \in R^V$ te laten

corresponderen met $\big(f(v_1),\ldots,f(v_n)\big)$. Net als in 1.24 ziet men in dat R^V voor $\#V \geq 2$ en $R \neq \{0\}$ steeds nuldelers heeft.

Andere interessante ringen krijgt men door extra voorwaarden aan de functie in T op te leggen. Zij bijvoorbeeld $V = [0,1]$, het gesloten interval van 0 tot 1, en $R = \mathbb{R}$, en beschouw

$$C\big([0,1]\big) = \big\{f\colon [0,1] \to \mathbb{R} \;\big|\; f \text{ is continu}\big\}.$$

Dit is een deelring van de zojuist gedefinieerde ring $\mathbb{R}^{[0,1]}$, en deze deelring heeft nog steeds nuldelers: definieer $f, g \in C([0,1])$ door

$$f(x) = \begin{cases} 0 & x \leq \frac{1}{2} \\ x - \frac{1}{2}, & x \geq \frac{1}{2} \end{cases} \qquad g(x) = \begin{cases} \frac{1}{2} - x, & x \leq \frac{1}{2} \\ 0 & x \geq \frac{1}{2} \end{cases}$$

dan geldt $f \neq 0 \neq g$ en $fg = 0$.

1.30 Groepenring. Zij R een ring en G een multiplicatief genoteerde groep. De *groepenring* $R[G]$ van G over R bestaat uit alle uitdrukkingen

$$\sum_{g \in G} a_g \cdot g$$

met $a_g \in R$ voor alle $g \in G$, en $a_g = 0$ voor bijna alle $g \in G$. Twee dergelijke uitdrukkingen $\sum_{g\in G} a_g \cdot g$ en $\sum_{g\in G} b_g \cdot g$ beschouwt men alleen als gelijk als $a_g = b_g$ voor alle $g \in G$. Optelling geschiedt componentsgewijs:

$$\left(\sum_{g\in G} a_g \cdot g\right) + \left(\sum_{g\in G} b_g \cdot g\right) = \sum_{g\in G} (a_g + b_g) \cdot g,$$

en de vermenigvuldiging vindt men door de vermenigvuldiging in R met die in G te combineren:

$$(a_g \cdot g) \cdot (b_h \cdot h) = (a_g b_h) \cdot gh \qquad (a_g, b_h \in R, g, h \in G).$$

Uitgewerkt met de distributieve wet levert dit:

$$\Big(\sum_{g\in G} a_g g\Big) \cdot \Big(\sum_{h\in G} b_h h\Big) = \sum_{k\in G} \Big(\sum_{g,h,gh=k} a_g b_h\Big) k.$$

We laten het aan de lezer over na te gaan dat $R[G]$ met deze bewerkingen inderdaad een ring is.

Het eenheidselement van $R[G]$ is $1 \cdot e$, waarbij e het neutrale element van G aangeeft; in het vervolg schrijven we hiervoor gewoon 1. Als R en G beide commutatief zijn, is ook $R[G]$ commutatief.

We kunnen G opvatten als ondergroep van $R[G]^*$, door

$$g = \sum_{h\in G} a_h h, \quad \text{met} \quad a_h = \begin{cases} 0 & \text{als } h \neq g \\ 1 & \text{als } h = g. \end{cases}$$

Heeft g orde n, met $1 < n < \infty$, dan is

$$1 + g + g^2 + \cdots + g^{n-1}$$

een nuldeler van $R[G]$, want

$$(1-g) \cdot (1 + g + \cdots + g^{n-1}) = 1 - g^n = 0, \quad \text{en} \quad 1 - g \neq 0\,.$$

Opgaven

1. Stel dat een element $1'$ in een ring R de eigenschap heeft dat $1'a = a1' = a$ voor alle $a \in R$. Bewijs dat $1' = 1$.

2. Zij R een ring. Bewijs dat elke $a \in R^*$ precies één inverse heeft.

3. Zij m een geheel getal dat geen kwadraat is, en $\alpha := \frac{1+\sqrt{m}}{2} \in \mathbb{C}$.

   (a) Voor welke m is $\mathbb{Z}[\alpha] = \left\{a + b\alpha \;\middle|\; a, b \in \mathbb{Z}\right\}$ een deelring van $\mathbb{C}$?

   (b) Hoe ziet $\mathbb{Z}[\alpha]$ er als deelverzameling van het complexe vlak uit als $m = -3$?

4. Zij $(R, +, \cdot, 0)$ een viertupel wat voldoet aan (R1)–(R3). We eisen dus niet dat R een eenheidselement heeft. Zo'n viertupel wordt soms wel een ring zonder één of een *rng* genoemd. Definieer op $\mathbb{Z} \times R$ een optelling en een vermenigvuldiging door

$$(n, r) + (m, s) = (n + m, r + s),$$

$$(n, r) \cdot (m, s) = (nm, ns + mr + rs)$$

   voor $n, m \in \mathbb{Z}, r, s, \in R$ (met

$$ns = s + s + \cdots + s \qquad (n \text{ keer})$$

   voor $n > 0$, etc.).

   (a) Bewijs dat $\mathbb{Z} \times R$ hiermee een ring wordt.

   (b) Bewijs dat iedere rng kan worden ingebed als deelrng in een ring.

5. Zij R een ring, en H een additieve ondergroep van R. Laat

$$R_0 = \left\{x \in R \;\middle|\; xh \in H \text{ voor alle } h \in H\right\}.$$

   Bewijs dat R_0 een deelring van R is.

6. Laat R een ring zijn, en $a \in R$. Definieer $\lambda_a, \phi_a \colon R \to R$ door $\lambda_a(x) = ax$ en $\phi_a(x) = xa$. Bewijs dat λ_a en ϕ_a endomorfismen van de additieve groep R^+ van R zijn.

7. Laat R een ring zijn. Definieer op R een nieuwe vermenigvuldiging $*$ door $a * b = ba$, voor $a, b \in R$. Bewijs dat R met zijn oorspronkelijke optelling en deze nieuwe vermenivuldiging een ring is. Deze ring heet de *tegengestelde* ring van R, notatie: R^0.

8. Laat R_1 en R_2 ringen zijn, en $R = R_1 \times R_2$ de productring. Laat zien dat R commutatief is dan en slechts dan als zowel R_1 als R_2 commutatief zijn. Bewijs $R^* = R_1^* \times R_2^*$.

9. Zij R een ring. Het *centrum* van R is

$$Z(R) = \left\{a \in R \;\middle|\; ax = xa \text{ voor alle } x \in R\right\}.$$

   Bewijs dat dit een deelring van R is.

10. Laat R een ring zijn met de eigenschap: $x^3 = x$ voor alle $x \in R$. Bewijs: $x+x+x+x+x+x = 0$ voor alle $x \in R$.

11. Stel dat R een ring is die uit 10 elementen bestaat. Bewijs dat R commutatief is.

12. (*Binomium van Newton*). Laat R een ring zijn. Voor $n \in \mathbb{Z}, r \in R$ definiëren we $nr \in R$ als in opgave 4.

    (a) Stel R is commutatief. Bewijs dat

    $$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k b^{n-k} \qquad (*)$$

    voor alle $a, b \in R$ en $n \in \mathbb{Z}_{>0}$.

    (b) Bewijs omgekeerd, dat als $(*)$ voor alle $a, b \in R$ en $n \in \mathbb{Z}_{>0}$ geldt, de ring R commutatief is.

13. Zij $\alpha = 1,3247\ldots$ het reële getal waarvoor geldt $\alpha^3 = \alpha + 1$. Bewijs dat $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$ een deelring van $\mathbb{R}$ is, en dat $\alpha, \alpha - 1, \alpha^2 - 1, \alpha^3 - 1 \in \mathbb{Z}[\alpha]^*$.

14. Zij R een commutatieve ring en $n \in \mathbb{Z}_{>0}$. Voor $A \in \mathrm{M}(n, R)$ is $\det(A)$ volgens de uit de lineaire algebra bekende formule gedefinieerd:

    $$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \qquad \text{als } A = \big(a_{ij}\big)_{1 \le i,j \le n}.$$

    Bewijs: $A \in \mathrm{M}(n, R)^* \iff \det(A) \in R^*$.

15. Zij R een ring met $1 \neq 0$, en $T = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}(2, R) \mid c = 0 \right\}$.

    (a) Bewijs dat T een deelring van $\mathrm{M}(2, R)$ is, en dat T niet commutatief is.

    (b) Bewijs: $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in T^* \iff a \in R^*$ en $d \in R^*$.

    (c) Bewijs: T^* is commutatief $\iff R^* = \{1\}$.

    (d) Stel dat $R = \mathbb{Z}/2\mathbb{Z}$. Bewijs: T is een niet-commutatieve ring met een commutatieve eenhedengroep.

16. Zij $R = \mathbb{Z}/4\mathbb{Z}$. Bewijs: voor alle $r \in R[X]$ is $1 + 2r$ een eenheid in $R[X]$.

17. Zij $m \in \mathbb{Z}_{>0}$ een geheel getal dat niet een kwadraat is.

    (a) Laat $\epsilon = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]^*$. Bewijs: $\{\epsilon, \epsilon^{-1}, -\epsilon, -\epsilon^{-1}\} = \{\pm a \pm b\sqrt{m}\}$, en concludeer hieruit: $\epsilon > 1 \iff a > 0$ en $b > 0$.

    (b) Laat gegeven zijn dat $\mathbb{Z}[\sqrt{m}]^* \neq \{\pm 1\}$. Bewijs dat $\mathbb{Z}[\sqrt{m}]$ een kleinste eenheid ϵ_1 met $\epsilon_1 > 1$ bezit, en dat $\mathbb{Z}[\sqrt{m}]^* = \langle -1, \epsilon_1 \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.

18. Laat R een ring zijn, en $a \in R$. Definieer

$$S = \{x \in R \mid ax = xa\}.$$

(a) Bewijs dat S een deelring van R is.

(b) Bewijs: $S^* = R^* \cap S$.

19. Laat $A \in \mathrm{M}(n, \mathbb{R})$. Bewijs: A is een linkernuldeler $\iff$ A is een rechternuldeler $\iff$ $A \neq 0$ en $\det(A) = 0$.

20. Geef een voorbeeld van een commutatieve ring R, die een element a bevat met de eigenschappen: $a \neq 0$, a is geen eenheid van R, en a is geen nuldeler van R.

21. Geef een voorbeeld van een oneindige commutatieve ring die nuldelers bezit.

22. Zij R een commutatieve ring, en R' een deelring van R. Geef voor elk van de volgende beweringen een bewijs of een tegenvoorbeeld:

(a) als R een lichaam is, is R' ook een lichaam;

(b) als R een domein is, is R' ook een domein;

(c) als R' een domein is, is R ook een domein.

23. Laten R_1 en R_2 ringen zijn. Bewijs: $R_1 \times R_2$ is een domein $\iff$ één van beide ringen R_1, R_2 is een domein en de ander is de nulring $\{0\}$. Zelfde opgave met "domein" vervangen door "delingsring", of door "lichaam".

24. Een *arithmetische functie* is een functie $f\colon \mathbb{Z}_{>0} \to \mathbb{C}$. De *som* $f_1 + f_2$ van twee arithmetische functies f_1 en f_2 is gedefinieerd door

$$(f_1 + f_2)(n) = f_1(n) + f_2(n), \text{door } n \in \mathbb{Z}_{>0}.$$

Het *convolutieproduct* $f_1 * f_2$ van twee arithmetische functies f_1 en f_2 is gedefinieerd door

$$(f_1 * f_2)(n) = \sum_{d|n} f_1(d) f_2\left(\tfrac{n}{d}\right) \qquad \text{voor } n \in \mathbb{Z}_{>0};$$

hierbij wordt gesommeerd over de positieve delers d van n.

(a) Bewijs dat de verzameling R van alle arithmetische functies een *domein* is ten opzichte van deze twee bewerkingen.

(b) Laat $f \in R$. Bewijs: $f \in R^* \iff f(1) \neq 0$.

25. Laat R een ring zijn en $f, g \in R[X]$. Bewijs:

$$\begin{aligned} \mathrm{gr}(f+g) &\leq \max(\mathrm{gr}(f), \mathrm{gr}(g)), \\ \mathrm{gr}(f+g) &= \max(\mathrm{gr}(f), \mathrm{gr}(g)) \qquad \text{als } \mathrm{gr}(f) \neq \mathrm{gr}(g), \\ \mathrm{gr}(f \cdot g) &\leq \mathrm{gr}(f) + \mathrm{gr}(g). \end{aligned}$$

(Hierbij laten we $\mathrm{gr}(0) = -\infty$.)

26. Laat R een ring zonder nuldelers zijn, en $f, g \in R[X]$. Bewijs: $\mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g)$. Bewijs dat $R[X]$ geen nuldelers heeft.

27. (a) Zij R een domein en R' een deelring van R. Laat zien dat $Q(R')$ kan worden opgevat als deelring van $Q(R)$.

    (b) Bewijs, voor een domein R:

    $$R = Q(R) \iff R \text{ is een lichaam.}$$

    (c) Laat $m \in \mathbb{Z}, \sqrt{m} \notin \mathbb{Z}$. Bewijs dat $Q(\mathbb{Z}[\sqrt{m}])$ kan worden geïdentificeerd met $\mathbb{Q}[\sqrt{m}]$.

28. Zij R een commutatieve ring, en $S \subset R$ een niet-lege deelverzameling met de eigenschap

    $$s, t \in S \implies st \in S.$$

    (a) Bewijs dat de relatie $\sim$ gedefinieerd door

    $$(a, s) \sim (b, t) \iff \exists u \in S : \ atu = bsu$$

    een equivalentierelatie op $R \times S$ is.

    (b) Laat $S^{-1}R = (R \times S)/\sim$, en zij $\frac{a}{s} \in S^{-1}R$ de klasse waar (a, s) in zit. Bewijs dat $S^{-1}R$ met de volgende optelling en vermenigvuldiging een commutatieve ring wordt:

    $$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

    (c) Bewijs: $S^{-1}R$ is de nulring $\iff 0 \in S$.

29. Zij A een abelse groep. Bewijs: $\mathrm{End}(A)^* = \mathrm{Aut}(A)$.

30. Bewijs dat $\{f \in C([0,1]) \mid f \text{ is driemaal continu differentieerbaar}\}$ een deelring van $C([0,1])$ is.

31. Zij R een ring, en $a, b \in R$ zo dat $ab = 0$. Dan geldt $(ba)^2 = 0$ en $1 + ba \in R^*$. Bewijs dit.

32. (G. Higman, Proc. London Math. Soc. 46 (1940), 231–248).

    (a) Laat $R = \mathbb{Z}[S_3]$, $a = (13) \cdot \{1 - (12)\}$ en $b = 1 + (12) \in R$. Bewijs dat $ab = 0$, en vind een eenheid van $\mathbb{Z}[S_3]$ die niet van de vorm $\pm\sigma$, met $\sigma \in S_3$, is.

    (b) Zij G een groep en $g \in G$ een element van G van eindige orde waarvoor $\langle g \rangle$ geen normaaldeler in G is. Bewijs dat $\mathbb{Z}[G]$ een eenheid heeft die niet van de vorm $\pm h$, met $h \in G$, is.

    (c) Zij G een groep, en $g \in G$ van orde 5. Bewijs: $1 - g - g^{-1} \in \mathbb{Z}[G]^*$.

33. Een *Boolese ring* (naar de Engelse wiskundige George Boole, (1815–1864)) is een ring R waarin geldt $x^2 = x$ voor alle $x \in R$.

    (a) Bewijs: $x + x = 0$ voor alle x in een Boolese ring R.

    (b) Bewijs dat elke Boolese ring commutatief is.

(c) Stel dat de Boolese ring R een lichaam is. Bewijs dat R uit precies twee elementen bestaat.

34. Zij X een verzameling, en $R = P(X)$ de verzameling deelverzamelingen van X. Voor $A, B \in R$ (dus $A, B \subset X$) definiëren we

$$A + B = (A \cup B) - (A \cap B), \quad AB = A \cap B.$$

Bewijs dat R hiermee een commutatieve ring wordt, en dat R een lichaam is dan en slechts dan als $\#X = 1$. Bewijs ook dat R een *Boolese* ring is (zie Opgave 33).

35. Zij R een ring. Zij $v \in R$ een rechtsinverse van $u \in R$: $uv = 1$. Bewijs dat de volgende 3 beweringen equivalent zijn:

(a) u heeft meer dan één rechtsinverse;

(b) u is geen eenheid;

(c) u is een linksnuldeler, d.w.z. er is een $x \neq 0$ zodat $ux = 0$.

36. (Kaplansky) Zij R een ring. Zij u een element van R dat meer dan één rechtsinverse heeft. Bewijs dat u oneindig veel rechtsinverses heeft. (Hint: als $uv = 1$ en $vu \neq 1$, beschouw dan de rechtsinverses $v + (1 - vu)u^n$.)

37. Zij R een eindige ring en zij $u \in R$ met $u \neq 0$. Bewijs dat de volgende uitspraken equivalent zijn:

(a) u heeft een rechtsinverse;

(b) u heeft een linksinverse;

(c) u is geen linksnuldeler;

(d) u is geen rechtsnuldeler;

(e) u is een eenheid.

38. Zij R een ring. Bewijs dat voor $a, b \in R$ geldt:

$$1 - ab \in R^* \iff 1 - ba \in R^* \iff \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix} \in \mathrm{M}(2, R)^*.$$

Hoofdstuk 2

Ringhomomorfismen en idealen

Definitie 2.1. Laten R_1 en R_2 ringen zijn. Een afbeelding $f\colon R_1 \to R_2$ heet een *ringhomomorfisme* als $f(1) = 1$ en als voor alle $a, b \in R_1$ geldt

$$f(a+b) = f(a) + f(b)\,,$$
$$f(ab) = f(a) \cdot f(b).$$

Een *bijectief* ringhomomorfisme heet een *isomorfisme van ringen*; de inverse is dan nl. ook een ringhomomorfisme. Twee ringen R_1 en R_2 heten *isomorf* als er een isomorfisme $R_1 \to R_2$ bestaat; notatie: $R_1 \cong R_2$. Een isomorfisme van een R naar zichzelf heet een (*ring-*)*automorfisme* van R.

Een ringhomomorfisme van een lichaam naar een lichaam heet een *lichaamshomomorfisme*, en analoog spreken we van een *lichaamsisomorfisme* en een *lichaamsautomorfisme*.

Voorbeelden 2.2. (a) Is R' een deelring van een ring R, dan is de inclusie-afbeelding $R' \to R$ een injectief ringhomomorfisme.

(b) Laat $n \in \mathbb{Z}_{>0}$. De kanonieke afbeelding

$$f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,, \qquad f(a) = \overline{a}$$

is een ringhomomorfisme, omdat $\overline{a} + \overline{b} = \overline{a+b}$ en $\overline{a} \cdot \overline{b} = \overline{ab}$ voor alle gehele getallen a en b.

(c) Voor iedere $s \in R^*$ is de afbeelding (conjugatie met s):

$$\gamma_s\colon R \to R, \qquad r \mapsto srs^{-1}$$

een ringautomorfisme. Als R commutatief is, geldt uiteraard dat $\gamma_s = \mathrm{id}_R$ voor elke $s \in R^*$. In geval $R = \mathrm{M}(n, \mathbb{R})$ induceert de overgang op een andere basis van $\mathbb{R}^n$ een conjugatie op $\mathrm{M}(n, \mathbb{R})$.

(d) Zijn R_1 en R_2 ringen, dan is de projectie $f\colon R_1 \times R_2 \to R_1$, gegeven door $f((a,b)) = a$, een ringhomomorfisme.

Definitie 2.3. Zij $f\colon R_1 \to R_2$ een ringhomomorfisme, dan is het *beeld* van f:

$$\mathrm{Im}(f) = f(R_1) = \big\{ y \in R_2 \;\big|\; \exists x \in R_1 \text{ met } y = f(x) \big\}.$$

De *kern* van f is (als bij additieve groepen):

$$\mathrm{Ker}(f) = \big\{ x \in R_1 \;\big|\; f(x) = 0 \big\}\,.$$

Ringhomomorfismen hebben eigenschappen die in verscheidene opzichten analoog zijn aan die van groepshomomorfismen. Bijvoorbeeld: is $f\colon R_1 \to R_2$ een ringhomomorfisme, dan is het beeld $f(R_1)$ van f een *deelring* van R_2. Het eenvoudige bewijs laten we aan de lezer over (zie opgave 1).

Omdat een ringhomomorfisme een homomorfisme op de optelgroepen geeft, geldt:

$$\mathrm{Ker}(f) = \{0\} \quad \Leftrightarrow \quad f \text{ is injectief.}$$

Als $1 \neq 0$ in R_2, dan is $\mathrm{Ker}(f)$ *geen* deelring van R_1, immers $f(1) = 1 \neq 0$, dus $1 \notin \mathrm{Ker}(f)$.

In de groepentheorie bleek dat de kernen van groepshomomorfismen precies de *normaaldelers* zijn. Evenzo zullen we nu zien dat de deelverzamelingen van ringen die als kernen van ringhomomorfismen optreden de *idealen* zijn, die we nu definiëren.

Definitie 2.4. Laat R een ring zijn. Een *ideaal* van R is een deelverzameling $I \subset R$ die de volgende twee eigenschappen heeft:

(I1) I is een ondergroep van de additieve groep van R, d.w.z.:

- **(H0)** $0 \in I$;
- **(H1)** $a - b \in I$ voor alle $a, b \in I$;

(I2) voor alle $r \in R$ en $a \in I$ geldt $ra \in I$ en $ar \in I$.

Triviale voorbeelden van idealen zijn $\{0\}$ en R zelf.

Opmerking 2.5. In plaats van "ideaal" zegt men ook wel "tweezijdig ideaal". Vervangt men (I2) door de zwakkere eis

(I2') voor alle $r \in R$ en $a \in I$ geldt $ra \in I$

dan krijgt men de definitie van een *linksideaal* van R. De definitie van een rechtsideaal verkrijgt men door ra door ar te vervangen.

Voor een voorbeeld van een linksideaal dat geen rechtsideaal—en dus ook geen ideaal—is, zie Opgave 26. We zullen voornamelijk in commutatieve ringen geïnteresseerd zijn, en daar vallen de drie begrippen natuurlijk samen.

Voorbeeld 2.6. Voor iedere $n \in \mathbb{Z}$ is de deelverzameling:

$$n\mathbb{Z} = \left\{ nk \in \mathbb{Z} \;\middle|\; k \in \mathbb{Z} \right\}$$

een ideaal van $\mathbb{Z}$ (ga na). Voor $n = 0$ vinden we $0\mathbb{Z} = \{0\}$; voor $n = 1$ vinden we $1\mathbb{Z} = \mathbb{Z}$.

Het is gemakkelijk in te zien dat ieder ideaal van $\mathbb{Z}$ van de vorm $n\mathbb{Z}$ is; we weten immers uit de groepentheorie dat elke ondergroep van de optelgroep $\mathbb{Z}$ van deze vorm is.

Opmerking 2.7. Een ideaal in een ring is gesloten onder optelling en vermenigvuldiging, maar in het algemeen geen deelring, want het ideaal hoeft 1 niet te bevatten. In het algemeen zien we: is R een ring met 1, en I een ideaal van R met $1 \in I$, dan is $I = R$ (want pas (I2) op $a = 1$ toe); zie Stelling 2.16 voor een generalisatie hiervan.

Stelling 2.8. *Zij* $f\colon R_1 \to R_2$ *een ringhomomorfisme. Dan is* $\mathrm{Ker}(f)$ *een ideaal van* R_1.

Bewijs. We controleren (I1) en (I2) voor $I = \mathrm{Ker}(f)$.

(I1). Dit volgt uit het feit dat f ook een groepshomomorfisme $R_1^+ \to R_2^+$ is.

(I2). Voor $r \in R_1$, $a \in \mathrm{Ker}(f)$ geldt $f(a) = 0$, dus

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0, \qquad f(ar) = f(a)f(r) = 0 \cdot f(r) = 0,$$

waaruit blijkt dat ra en $ar \in \mathrm{Ker}(f)$, zoals verlangd. Dit bewijst 2.8. □

Verderop (zie 2.21) zullen we zien dat ook de omkering van 2.8 geldt: elk ideaal I is de kern van een geschikt gekozen ringhomomorfisme.

Voorbeeld 2.9. Voor $n > 1$ is de kern van het kanonieke ringhomomorfisme

$$f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad a \mapsto \bar{a}$$

gelijk aan het ideaal $n\mathbb{Z}$ uit Voorbeeld 2.6.

Voorbeeld 2.10. Men rekent eenvoudig na dat:

$$f\colon \mathbb{Z}[i] \to \mathbb{F}_2\,(= \mathbb{Z}/2\mathbb{Z}), \qquad a + bi \mapsto \bar{a} + \bar{b} \qquad (a, b \in \mathbb{Z})$$

een (surjectief) ringhomomorfisme is (zie opgave 19). We beweren:

$$\mathrm{Ker}(f) = \left\{2r + (1+i)s \in \mathbb{Z}[i] \;\middle|\; r, s \in \mathbb{Z}[i]\right\} = \left\{(1+i)t \in \mathbb{Z}[i] \;\middle|\; t \in \mathbb{Z}[i]\right\}.$$

Om te beginnen bewijzen we de eerste inclusie "$\supset$": omdat f een ringhomomorfisme is, geldt voor alle $r, s \in \mathbb{Z}[i]$:

$$f(2r + (1+i)s) = f(2)f(r) + f(1+i)f(s) = 0 \cdot f(r) + 0 \cdot f(s) = 0.$$

Voor de omkering "$\subset$": Als $a + bi \in \mathrm{Ker}(f)$ met a, $b \in \mathbb{Z}$, dan geldt $a + b \equiv 0 \bmod 2$ en dus $a = b + 2k$ voor zekere $k \in \mathbb{Z}$. Dan is inderdaad $a + bi = b + 2k + bi = 2k + (1+i)b$ met $k, b \in \mathbb{Z} \subset \mathbb{Z}[i]$.

Voor het tweede '$=$' teken merken we op:

$$2r + (1+i)s = (1+i)(1-i)r + (1+i)s = (1+i) \cdot ((1-i)r + s) = (1+i)t,$$

met $t = (1-i)r + s$, hetgeen '$\subset$' bewijst. Anderzijds is '$\supset$' evident omdat we $r = 0$, $s = t$ kunnen nemen.

Volgens Stelling 2.8 zijn beide verzamelingen idealen. Ga dit ook zelf na met de definitie van ideaal.

2.11 Zoals we in het vorige voorbeeld zagen, zijn de deelverzamelingen

$$2\mathbb{Z}[i] + (1+i)\mathbb{Z}[i]\,, \qquad (1+i)\mathbb{Z}[i]$$

idealen in $\mathbb{Z}[i]$; ze bleken zelfs gelijk te zijn. Algemener: Zij R een commutatieve ring en laat $a_1,\, a_2 \ldots, a_n \in R$. Het door $a_1,\, a_2, \ldots, a_n$ *voortgebrachte* ideaal is gedefinieerd als:

$$Ra_1 + Ra_2 + \cdots + Ra_n = \left\{ r_1a_1 + r_2a_2 + \cdots + r_na_n \;\middle|\; r_1,\, r_2, \ldots, r_n \in R \right\}.$$

Ga na, met Definitie 2.4, dat dit inderdaad een ideaal is (indien R niet commutatief is, dan is dit i.h.a. slechts een linksideaal). Als het duidelijk is om welke ring het gaat noteren we dit ideaal ook wel als:

$$(a_1,\, a_2, \ldots, a_n)\,.$$

In geval $n = 1$, d.w.z. het ideaal is voortgebracht door één element a, noemen we het door a voortgebrachte ideaal een *hoofdideaal*:

$$(a) = aR = Ra = \left\{ ra \;\middle|\; r \in R \right\}.$$

Een voorbeeld van een hoofdideaal is dus het ideaal $(2,\, 1+i) \subset \mathbb{Z}[i]$, want $(2,\, 1+i) = (1+i)$.

Ook het ideaal $I = (4,\, 6) \subset \mathbb{Z}$ blijkt een hoofdideaal te zijn, nl. $2 = (-1)4 + 6 \in I$ dus ook $2\mathbb{Z} \subset I$ (gebruik (I2)) terwijl anderzijds $4,\, 6 \in 2\mathbb{Z}$ dus ook $I = 4\mathbb{Z} + 6\mathbb{Z} \subset 2\mathbb{Z}$ waarmee aangetoond is dat $(4, 6) = (2)$.

Merk op dat $a_1, a_2, \ldots, a_t$ zelf bevat zijn in het ideaal $Ra_1 + Ra_2 + \cdots + Ra_t$, (immers $0,\, 1 \in R$). Ieder ideaal I dat alle a_i bevat, bevat ook alle elementen uit $Ra_1,\, Ra_2, \ldots, Ra_n$ (I2) en bevat dan ook alle elementen uit $Ra_1 + Ra_2 + \cdots + Ra_t$. Dus $Ra_1 + \cdots + Ra_t$ is het *kleinste* ideaal waar $a_1, a_2, \ldots, a_t$ in zitten.

In Voorbeeld 2.6 zagen we dat elk ideaal van $\mathbb{Z}$ een hoofdideaal is. In Hoofdstuk 5 zullen we domeinen met deze eigenschap, de zogenaamde *hoofdideaaldomeinen* uitvoeriger bestuderen.

Voorbeeld 2.12. Het ideaal $(X, Y) \subset \mathbb{R}[X, Y]$ is geen hoofdideaal. Immers, zou $g \in \mathbb{R}[X, Y]$ een voortbrenger van dit ideaal zijn, dan waren X en Y veelvouden van g, waaruit volgt dat $g \neq 0$ en $\mathrm{gr}_X(g) = \mathrm{gr}_Y(g) \leq 0$. Maar dan is g een constant polynoom en uit 2.16 volgt dat $(g) = \mathbb{R}[X, Y]$, terwijl (X, Y) niet de hele ring is.

Stelling 2.13. *Laat R een commutatieve ring zijn en $\alpha \in R$. Dan is de afbeelding*

$$\Phi_\alpha \colon R[X] \to R\,, \quad \textit{gegeven door} \quad \Phi_\alpha\left(\sum_{i=0}^{n} a_iX^i\right) = \sum_{i=0}^{n} a_i \cdot \alpha^i$$

een surjectief ringhomomorfisme. (Merk op dat $\Phi_\alpha(f) = f(\alpha)$.) Bovendien geldt:

$$\mathrm{Ker}(\Phi_\alpha) = (X - \alpha) = \left\{ (X-\alpha)g \;\middle|\; g \in R[X] \right\}.$$

Bewijs. Dat Φ_α een ringhomorfisme is, is eenvoudig na te rekenen; merk op dat we nodig hebben dat R commutatief is! Duidelijk is verder dat Φ_α surjectief is, want een element $a \in R$ is het beeld onder Φ_α van het constante polynoom a.

We bewijzen nu dat $\mathrm{Ker}(\Phi_\alpha) = (X - \alpha)$. Voor "$\supset$": Er geldt $\Phi_\alpha(X - \alpha) = \alpha - \alpha = 0$, dus $X - \alpha \in \mathrm{Ker}(\Phi_\alpha)$, en omdat $\mathrm{Ker}(\Phi_\alpha)$ een ideaal is geldt dan ook $R[X](X - \alpha) \subset \mathrm{Ker}(\Phi_\alpha)$.

"$\subset$": Stel dat $f = \sum_{i=0}^{n} a_i X^i \in \mathrm{Ker}(\Phi_\alpha)$, dan geldt $\sum_{i=0}^{n} a_i \alpha^i = 0$, dus

$$f = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} a_i X^i - \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i (X^i - \alpha^i)\,.$$

Omdat

$$X^i - \alpha^i = (X^{i-1} + \alpha X^{i-2} + \cdots + \alpha^{i-3} X^2 + \alpha^{i-2} X + \alpha^{i-1}) \cdot (X - \alpha)$$

volgt hieruit dat $f \in (X - \alpha)$. Hiermee is 2.13 bewezen. □

Voorbeeld 2.14. Een eenvoudig voorbeeld is het ringhomomorfisme

$$\Phi_0 \colon \mathbb{R}[X] \to \mathbb{R}, \qquad f \mapsto f(0).$$

Als $f = \sum a_i X^i$, dan is $f(0) = a_0$ en dus:

$$\mathrm{Ker}(\Phi_0) = \big\{ f \in \mathbb{R}[X] \;\big|\; f = \sum a_i X^i \text{ en } a_0 = 0 \big\}.$$

Omdat $a_0 = 0$ d.e.s.d.a. $f = Xg$ met $g = \sum_{i=1}^{n} a_i X^{i-1} \in \mathbb{R}[X]$ volgt inderdaad dat $\mathrm{Ker}(\Phi_0) = X\mathbb{R}[X]$.

Voor een tweede voorbeeld merken we op dat in $\mathbb{R}[X, Y]$ elk polynoom te schrijven is als:

$$\sum_{i,j} a_{ij} X^i Y^j = \sum_{j=0}^{m} \left(\sum_{i=0}^{n} a_{ij} X^i \right) Y^j = \sum_{j=0}^{m} f_j(X) Y^j.$$

met $f_j(X) = \sum_{i=0}^{n} a_{ij} X^i$. Een polynoom in twee variabelen X, Y kan dus worden gezien als een polynoom in één variabele Y met coëfficiënten uit de ring $\mathbb{R}[X]$:

$$\mathbb{R}[X, Y] = (\mathbb{R}[X])[Y].$$

Voor iedere $f \in \mathbb{R}[X]$ is er dan een ringhomomorfisme:

$$\Phi_f \colon \mathbb{R}[X, Y] = (\mathbb{R}[X])[Y] \to \mathbb{R}[X], \qquad F(X, Y) \mapsto F(X, f(X)).$$

De kern van dit ringhomomorfisme is volgens de stelling het ideaal

$$\mathrm{Ker}(\Phi_f) = \big\{ (Y - f(X)) G(X, Y) \;\big|\; G(X, Y) \in \mathbb{R}[X, Y] \big\}\,.$$

Een speciaal geval hiervan krijgt men voor $f = 0$. Ga na (zonder de stelling te gebruiken) dat dan bovenstaande inderdaad de kern is.

Voorbeeld 2.15. Niet alle idealen zijn hoofdidealen, zoals we al in 2.12 hebben gezien, en zoals ook het volgende voorbeeld laat zien. Laat $R = \mathbb{Z}[X]$ en zij $I \subset R$ gedefnieerd door

$$I = \{f \in \mathbb{Z}[X] \mid f(0) \text{ is even}\} = \{a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X] \mid a_0 \in 2\mathbb{Z}\}.$$

Om te bewijzen dat I een ideaal is van $\mathbb{Z}[X]$ kan men bijvoorbeeld opmerken dat I de kern is van het samengestelde ringhomomorfisme

$$\mathbb{Z}[X] \xrightarrow{f \mapsto f(0)} \mathbb{Z} \xrightarrow{a \mapsto (a \bmod 2)} \mathbb{Z}/2\mathbb{Z}$$

en dan Stelling 2.8 toepassen.

Stel dat I een hoofdideaal is: $I = (g) = \mathbb{Z}[X] \cdot g$ met $g \in \mathbb{Z}[X]$. Uit $2 \in I = (g)$ volgt dan dat $2 = h \cdot g$ voor een zekere $h \in \mathbb{Z}[X]$. Kijken we naar de graden van deze polynomen, dan zien we dat dit alleen kan als h en g constanten in $\mathbb{Z}$ zijn, dus $g = \pm 1$ of ± 2. Ook is $X \in I = (g)$, maar dit is voor $g = \pm 2$ onmogelijk. Dus $g = \pm 1$. Uit de definitie van I blijkt echter dat $\pm 1 \notin I$, een tegenspraak.

We concluderen dat I geen hoofdideaal is. Wel kan I door twee elementen worden voortgebracht, bijvoorbeeld $I = (2, X)$, zoals de lezer kan nagaan.

Stelling 2.16. *Zij R een ring en I een ideaal van R met $I \cap R^* \neq \emptyset$. Dan geldt $I = R$.*

Bewijs. Laat $a \in I \cap R^*$. Uit $a \in R^*$ volgt dat er een $b \in R$ is met $ab = 1$. Uit (I2) volgt nu dat $1 \in I$. Weer met (I2) volgt nu dat elke $r = r \cdot 1$ tot I behoort, dus $I = R$. □

Gevolg 2.17. *De enige idealen in een delingsring R zijn (0) en R.*

Bewijs. Zij I een ideaal. Als $I \neq (0)$ dan bevat I een element $a \neq 0$. Omdat R een delingsring is, geldt $a \in R^*$; dus $I \cap R^* \neq \emptyset$ en uit 2.16 volgt dat $I = R$. □

Gevolg 2.18. *Elk ringhomomorfisme $f\colon K \to R$ van een lichaam K naar een ring $R \neq \{0\}$ is injectief. In het bijzonder is elk lichaamshomomorfisme injectief.*

Bewijs. De kern van f is een ideaal van K, dus (wegens 2.17) $\mathrm{Ker}(f) = (0)$ of $\mathrm{Ker}(f) = K$. Maar $f(1) = 1 \neq 0$, dus $1 \notin \mathrm{Ker}(f)$ en $\mathrm{Ker}(f) \neq K$. Daarom geldt: $\mathrm{Ker}(f) = (0)$, d.w.z. f is injectief. De laatste bewering volgt direct uit de eerste. □

2.19 Laat R een ring zijn en $I \subset R$ een ideaal. Dan is I een *normaaldeler* van de additieve groep van R (wegens (I1) en het feit dat R^+ abels is). We hebben dus de groep R/I, waarvan de elementen de nevenklassen $a + I$ van I in R zijn ($a \in R$), en waarvan de groepsbewerking gegeven wordt door

$$(a + I) + (b + I) = (a + b) + I$$

of, als we $\bar{a} = a + I$ schrijven,

$$\bar{a} + \bar{b} = \overline{a + b}.$$

We definiëren op R/I een *vermenigvuldiging* door:

$$\bar{a} \cdot \bar{b} = \overline{ab}.$$

Om na te gaan dat dit goed gedefinieerd is, moeten we bewijzen: als $\bar{a}_1 = \bar{a}_2$ en $\bar{b}_1 = \bar{b}_2$ dan geldt $\overline{a_1 b_1} = \overline{a_2 b_2}$. Inderdaad:

$$a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

met $a_1 \in R$ en $b_1 - b_2 \in I$ (want $\bar{b}_1 = \bar{b}_2$) dus $a_1(b_1 - b_2)$ wegens (I2); evenzo $b_2 \in R$ en $a_1 - a_2 \in I$, dus $(a_1 - a_2)b_2 \in I$. Omdat I een ondergroep is, volgt nu dat $a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I$, dus $a_1 b_1 - a_2 b_2 \in I$, hetgeen betekent dat $\overline{a_1 b_1} = \overline{a_2 b_2}$ zoals bewezen moest worden. Hiermee is aangetoond dat de vermenigvuldiging op R/I goed gedefinieerd is.

We beweren dat R/I met deze optelling en vermenigvuldiging een *ring* is. Het eenheidselement is $\bar{1}$. Bij wijze van voorbeeld controleren we één der distributieve wetten (R4):

$$\begin{aligned}
\bar{a}(\bar{b} + \bar{c}) &= \bar{a}(\overline{b + c}) && \text{(per definitie van } +) \\
&= \overline{a(b + c)} && \text{(per definitie van } \cdot) \\
&= \overline{ab + ac} && \text{(omdat (R4) geldt in } R) \\
&= \overline{ab} + \overline{ac} && \text{(per definitie van } +) \\
&= \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} && \text{(per definitie van } \cdot).
\end{aligned}$$

Op analoge wijze controleert men de overige ring-axioma's.

Is R commutatief, dan is R/I het natuurlijk ook.

De ringen $\mathbb{Z}/n\mathbb{Z}$ zijn speciale gevallen van deze constructie. Nemen we bijvoorbeeld $n = 6$, dan zien we dat R/I best nuldelers kan hebben als R ze niet heeft.

De afbeelding

$$\phi\colon R \to R/I\,, \qquad \phi(a) = \bar{a} = a + I\,,$$

heet de *natuurlijke* of *canonieke* afbeelding.

Stelling 2.20. *Laat R een ring zijn en I een ideaal van R. Dan is de natuurlijke afbeelding $\phi\colon R \to R/I$ een surjectief* ringhomomorfisme *met* $\mathrm{Ker}(\phi) = I$.

Bewijs. Surjectiviteit van ϕ is duidelijk. Uit

$$\phi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \phi(a) + \phi(b),$$

$$\phi(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = \phi(a) \cdot \phi(b),$$

en $\phi(1) = \bar{1}$ blijkt dat ϕ een ringhomomorfisme is. Tenslotte geldt

$$\phi(a) = \bar{0} \quad \Longleftrightarrow \quad \bar{a} = \bar{0} \quad \Longleftrightarrow \quad a \in I$$

dus $I = \mathrm{Ker}(\phi)$. Dit bewijst Stelling 2.20. □

Gevolg 2.21. *Zij R een ring en $I \subset R$ een deelverzameling. Dan is I een ideaal van R dan en slechts dan als er een ringhomomorfisme $f\colon R \to R_1$ bestaat met* $\mathrm{Ker}(f) = I$.

Bewijs. $\Leftarrow$: dit is 2.8. $\Rightarrow$: neem $R_1 = R/I$ en $f = \phi$ als in 2.20. Dit bewijst 2.21. □

Bovenstaande twee resultaten zijn analoog aan resultaten uit de groepentheorie. We zullen nu de resultaten die overeenkomen met de homomorfie- en isomorfiestellingen formuleren. Wegens de verregaande analogie zal het niet nodig zijn lang stil te staan bij de bewijzen.

Stelling 2.22 (De homomorfiestelling voor ringen)**.** *Laat $f\colon R_1 \to R_2$ een ringhomomorfisme zijn, en $I \subset R_1$ een ideaal waarvoor geldt $I \subset \mathrm{Ker}(f)$. Zij $\phi\colon R_1 \to R_1/I$ het canonieke ringhomomorfisme. Dan is er precies één ringhomomorfisme $g\colon R_1/I \to R_2$ waarvoor geldt $f = g \circ \phi$. Bovendien geldt* $\mathrm{Ker}(g) = \phi(\mathrm{Ker}(f))$.

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ {\scriptstyle\phi}\downarrow & \nearrow_{g} & \\ R_1/I & & \end{array}$$

Bewijs. Voor $a \in R_1$ schrijven we weer $\bar{a} = a+I = \phi(a) \in R_1/I$. Passen we de homomorfiestelling voor groepen toe op de optelgroepen van R_1, R_2 en R_1/I dan vinden we dat er precies één homomorfisme van groepen $g\colon (R_1/I)^+ \to R_2^+$ bestaat waarvoor $f = g\circ\phi$, en dat voor deze geldt dat $\mathrm{Ker}(g) = \phi(\mathrm{Ker}(f))$. Om de stelling te bewijzen is het nu voldoende te laten zien dat deze g een homomorfisme van ringen is. Inderdaad geldt $g(\bar{1}) = g(\phi(1)) = f(1) = 1$, en

$$g\big(\bar{a}\cdot\bar{b}\big) = g\big(\overline{ab}\big) = g\big(\phi(ab)\big) = f(ab) = f(a)f(b) = g\big(\phi(a)\big)\,g\big(\phi(b)\big) = g\big(\bar{a}\big)g\big(\bar{b}\big)\,.$$

Hiermee is 2.22 bewezen. □

Stelling 2.23 (De eerste isomorfiestelling voor ringen)**.** *Laat $f\colon R_1 \to R_2$ een ringhomomorfisme zijn. Dan is er een isomorfisme van ringen:*

$$R_1/\mathrm{Ker}(f) \xrightarrow{\sim} f(R_1)$$

dat $\bar{a} = a + \mathrm{Ker}(f)$ afbeeldt op $f(a)$, voor $a \in R_1$. In het bijzonder, als f surjectief is dan geldt

$$R_1/\mathrm{Ker}(f) \cong R_2.$$

Bewijs. We passen de vorige stelling toe met $I = \mathrm{Ker}(f)$. Dan geeft $g\colon R_1/\mathrm{Ker}(f) \to R_2$ een ringhomomorfisme met $\mathrm{Ker}(g) = \phi(\mathrm{Ker}(f)) = \bar{0}$, d.w.z. g is injectief. Maar dan is $g\colon R_1/\mathrm{Ker}(f) \to f(R_1) \subset R_2$ een bijectief ringhomomorfisme, en is dus een isomorfisme van ringen. Dit bewijst 2.23. □

Voor het ringentheoretische equivalent van de tweede isomorfiestelling verwijzen we naar Opgave 34. Met de derde isomorfiestelling correspondeert de volgende stelling.

Stelling 2.24. *Zij $J \subset R$ een ideaal met $J \supset I$. Dan is J/I een ideaal van R/I en J/I is het beeld van J onder het kanonieke homomorfisme $R \to R/I$. Omgekeerd is ieder ideaal van R/I van deze vorm. Tenslotte geldt:*

$$(R/I)/(J/I) \cong R/J\,.$$

Bewijs. Dit is geheel analoog aan het bewijs van de analoge stelling in de groepentheorie, zie Opgave 28 op blz. 36. □

Voorbeeld 2.25. Definieer $\phi\colon \mathbb{R}[X] \to \mathbb{C}$ door $\phi(f) = f(i)$. Dit is een surjectief ringhomomorfisme en het is niet moeilijk te bewijzen dat $\mathrm{Ker}(\phi) = (X^2+1)$; vgl. Opgave 37. Dus Stelling 2.23 levert

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}\,.$$

Men kan dit in feite als de definitie van $\mathbb{C}$ nemen; vgl. Cauchy, Œuvres (1), X nr. 369, pp. 312–323 (1847).

Voorbeeld 2.26. Voorbeeld 2.10, gecombineerd met de eerste isomorfiestelling, laat zien dat

$$\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2\,.$$

2.27 Rekenen met idealen. We passen het voorgaande toe om een aantal regeltjes te bewijzen die in de praktijk het uitdelen naar idealen zeer vergemakkelijken. Steeds is R een commutatieve ring.

2.28 Stapsgewijs uitdelen. Dit is niets anders dan het isomorfisme

$$R/J \cong (R/I)/(J/I)$$

uit Stelling 2.24, voor idealen $I \subset J$ van R. Belangrijk speciaal geval: $J = (a,b)$ met a, $b \in R$. Kies $I = (a)$, dan vinden we

$$R/(a,b) \cong \bar{R}/(\bar{b})$$

met $\bar{R} = R/(a)$ en $\bar{b} = b + (a)$ het beeld van b in $\bar{R}$. Analoog voor idealen die door meer elementen voortgebracht worden.

2.29 Idealen voortgebracht door constanten. Laat $I \subset R$ een ideaal zijn. Het door I voortgebrachte ideaal in $R[X]$ is precies de verzameling $I[X]$ van polynomen uit $R[X]$ waarvan alle coëfficiënten tot I behoren, en er geldt:

$$R[X]/I[X] \cong (R/I)\big[X\big]\,.$$

Bewijs hiervan: de afbeelding $R[X] \to (R/I)[X]$ die $\sum_{i=0}^{n} a_i X^i$ afbeeldt op $\sum_{i=0}^{n} \bar{a}_i X^i$ (met $\bar{a}_i \in R/I$ de restklasse van a_i modulo I), is een surjectief homomorfisme van ringen met kern $I[X]$; dus $I[X]$ is een ideaal van $R[X]$ en het bovenstaande isomorfisme volgt uit de eerste isomorfiestelling. Het is duidelijk dat $I[X]$ door I wordt voortgebracht.

Nemen we voor I een hoofdideaal, dan ziet het regeltje er zo uit:

$$R[X]/aR[X] \cong (R/aR)\big[X\big]\,.$$

2.30 Lineaire polynomen. Als $a \in R$ dan geldt

$$R[X]/(X-a) \cong R\,.$$

Dit volgt door Stelling 2.13 te combineren met de eerste isomorfiestelling.

2.31 Voortbrengers wijzigen. Voor a, b, $c \in R$ geldt bijvoorbeeld

$$(a, b) = (a, b + ca)$$

zoals men gemakkelijk nagaat. Door dit soort transformaties kan men soms geschiktere voortbrengers vinden om 2.28 op toe te passen.

Voorbeeld 2.32. Laat $I = (X + Y, X^2 + X + Y + 1) \subset \mathbb{R}[X, Y]$. Dan

$$\begin{aligned}
\mathbb{R}[X,Y]/I &\cong \mathbb{R}[X,Y]/(X+Y, X^2+1) && \text{wegens 2.31}\\
&\cong \big(\mathbb{R}[X][Y]/(Y-(-X))\big)/(\bar{X}^2+\bar{1}) && \text{wegens 2.28}\\
&\cong \mathbb{R}[X]/(X^2+1) && \text{wegens 2.30}\\
&\cong \mathbb{C} && \text{zie Voorbeeld 2.25.}
\end{aligned}$$

2.33 Laat R een ring zijn, en I en J idealen van R. We definiëren de *som* van I en J door

$$I + J = \big\{x + y \;\big|\; x \in I, y \in J\big\}.$$

Aan de hand van Definitie 2.4 gaat men direct na dat $I + J$ een ideaal van R is. Voorts is het duidelijk dat $I + J$ de beide idealen I en J omvat, en dat ieder ideaal dat I en J omvat ook $I + J$ omvat. Dus $I + J$ is het *kleinste* ideaal dat I en J omvat.

Men noemt I en J *onderling ondeelbaar* of *relatief priem* als

$$I + J = R;$$

beneden lichten we deze terminologie toe aan de hand van het geval $R = \mathbb{Z}$. Er geldt

$$\begin{aligned}
I + J = R \quad &\Leftrightarrow \quad 1 \in I + J \qquad \text{(wegens 2.16)}\\
&\Leftrightarrow \quad \exists x \in I, y \in J: \quad x + y = 1.
\end{aligned}$$

De *doorsnede* $I \cap J$ van twee idealen I en J is ook een ideaal van R, zoals men aan de hand van 2.4 nagaat. Dit is kennelijk het *grootste* ideaal dat zowel in I als in J bevat is.

Het *product* van I en J is gedefinieerd door

$$I \cdot J = \Big\{\sum_{i=1}^{n} x_i y_i \;\Big|\; n \in \mathbb{Z}_{\geq 0}, x_i \in I, y_i \in J\Big\}.$$

Hiervan is ook weer makkelijk na te gaan dat het een ideaal van R is; uit Opgave 38 blijkt dat $\big\{xy \;\big|\; x \in I, y \in J\big\}$ geen ideaal van R hoeft te zijn. Aangezien $x_i y_i \in I$ voor elke $x_i \in I$ en $y_i \in J$ (wegens (I2)), zit elk element $\sum_{i=1}^{n} x_i \cdot y_i$ van $I \cdot J$ in I. Omdat evenzo volgt dat $I \cdot J \subset J$, is hiermee bewezen dat $I \cdot J \subset I \cap J$.

$$\begin{array}{ccccc}
 & & & \subset I & \\
I \cdot J & \subset & I \cap J & & \subset I + J \quad \subset \quad R.\\
 & & & \subset J &
\end{array}$$

Sommen, doorsneden en producten kunnen in het algemeen ook voor meer dan twee idealen (maar wel eindig veel, in het geval van producten) gedefinieerd worden, en zijn ook weer idealen.

Voorbeeld 2.34. We gaan nu kijken waar deze begrippen op neerkomen in het geval $R = \mathbb{Z}$. Ieder ideaal van $\mathbb{Z}$ is een hoofdideaal $\mathbb{Z}a$ (zie 2.6).

Het nemen van de *som* van twee idealen (beide $\neq \{0\}$) correspondeert nu met het nemen van de ggd van de voortbrengers:

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d \quad \text{met} \quad d = \text{ggd}(a, b).$$

Bewijs: Omdat a en b deelbaar zijn door d geldt "$\subset$". Anderzijds weten we dat er k, $l \in \mathbb{Z}$ zijn met $ak + bl = d$, dus $d \in \mathbb{Z}a + \mathbb{Z}b$ en daarom geldt "$\supset$".

In het bijzonder zien we dat de idealen $\mathbb{Z}a$ en $\mathbb{Z}b$ onderling ondeelbaar zijn dan en slechts dan als $\text{ggd}(a, b) = 1$, d.w.z. als a en b onderling ondeelbaar zijn. Hiermee is de boven ingevoerde terminologie verklaard.

Het nemen van de *doorsnee* van twee idealen correspondeert met het nemen van de *kgv* van de voortbrengers:

$$\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}c \quad \text{met} \quad c = \text{kgv}(a, b)\,.$$

Immers, er geldt:

$$\begin{aligned} x \in \mathbb{Z}a \cap \mathbb{Z}b \quad &\Leftrightarrow \quad x \text{ is een veelvoud van zowel } a \text{ als } b \\ &\Leftrightarrow \quad x \text{ is een veelvoud van } c \\ &\Leftrightarrow \quad x \in \mathbb{Z}c\,. \end{aligned}$$

Tenslotte komt het nemen van het *product* van twee idealen neer op het nemen van het product van de voortbrengers:

$$\mathbb{Z}a \cdot \mathbb{Z}b = \mathbb{Z}ab.$$

Het eenvoudige bewijs hiervan laten we aan de lezer over.

Voorbeeld 2.35. Als R een commutatieve ring is, dan geldt:

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots b_m) = (a_1b_1, a_1b_2, \ldots, a_ib_j, \ldots, a_nb_m)\,,$$

zoals eenvoudig volgt uit de definities.

Als twee gehele getallen onderling ondeelbaar zijn, dan is hun kgv gelijk aan hun product. Dit feit wordt gegeneraliseerd in de volgende stelling.

Stelling 2.36 (Chinese reststelling voor ringen)**.** *Laat R een commutatieve ring zijn, en laat I, J onderling ondeelbare idealen van R zijn. Dan geldt $I \cap J = I \cdot J$, en er is een ringisomorfisme*

$$R/(I \cdot J) \cong (R/I) \times (R/J)\,.$$

Bewijs. Kies $x \in I$ en $y \in J$ met $x + y = 1$; dit kan omdat I en J onderling ondeelbaar zijn.

De inclusie $I \cap J \supset I \cdot J$ is algemeen geldig. Kies, om de omgekeerde inclusie te bewijzen, een element $z \in I \cap J$. Dan geldt:

$$z = z \cdot 1 = z \cdot (x + y) = x \cdot z + z \cdot y$$

met $x \cdot z \in I \cdot J$ (want $x \in I$ en $z \in J$) en $z \cdot y \in I \cdot J$ (want $z \in I$ en $y \in J$). Dus $z \in I \cdot J$. Hiermee is $I \cap J = I \cdot J$ bewezen.

Laten $\phi_1 \colon R \to R/I$ en $\phi_2 \colon R \to R/J$ de canonieke ringhomomorfismen met kern I resp. J zijn, en definieer

$$\phi \colon R \to (R/I) \times (R/J)$$

door $\phi(a) = \big(\phi_1(a), \phi_2(a)\big)$. We gaan bewijzen dat ϕ een surjectief ringhomomorfisme met kern $I \cdot J$ is. Dan volgt de verlangde isomorfie $R/I \cdot J \cong (R/I) \times (R/J)$ direct uit de eerste isomorfiestelling 2.23.

Bewijs dat ϕ een ringhomomorfisme is:

$$\begin{aligned}
\phi(ab) &= \big(\phi_1(ab),\, \phi_2(ab)\big) \\
&= \big(\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)\big) && \text{(want } \phi_1, \phi_2 \text{ zijn ringhomomorfismen)} \\
&= \big(\phi_1(a), \phi_2(a)\big) \cdot \big(\phi_1(b), \phi_2(b)\big) && \text{(wegens de definities in 1.24)} \\
&= \phi(a) \cdot \phi(b)
\end{aligned}$$

voor alle a, $b \in R$. Evenzo $\phi(1) = 1$ en $\phi(a + b) = \phi(a) + \phi(b)$. Dus ϕ is een ringhomomorfisme.

Bewijs dat $\mathrm{Ker}(\phi) = I \cdot J$: Er geldt

$$\begin{aligned}
a \in \mathrm{Ker}(\phi) \quad &\Leftrightarrow \quad \big(\phi_1(a), \phi_2(a)\big) = (0, 0) \\
&\Leftrightarrow \quad a \in \mathrm{Ker}(\phi_1) \text{ en } a \in \mathrm{Ker}(\phi_2) \\
&\Leftrightarrow \quad a \in I \cap J \\
&\Leftrightarrow \quad a \in I \cdot J
\end{aligned}$$

(want we weten al dat $I \cdot J = I \cap J$).

Bewijs dat ϕ surjectief is: Laat $x + y = 1$ als boven, met $x \in I$ en $y \in J$. Dan is $\phi_1(x) = 0$ en $\phi_2(y) = 0$ en uit $x = 1 - y$ volgt

$$\phi_2(x) = \phi_2(1) - \phi_2(y) = 1 - 0 = 1 \in R/J\,, \qquad \phi_1(y) = \phi_1(1 - x) = 1 \in R/I\,.$$

Al met al hebben we

$$\phi(x) = (0, 1)\,, \quad \text{en} \quad \phi(y) = (1, 0)\,.$$

Laat nu $z = \big(\phi_1(a), \phi_2(b)\big)$ een willekeurig element van $(R/I) \times (R/J)$ zijn, met a, $b \in R$ (elk element van $(R/I) \times (R/J)$ heeft deze vorm, want ϕ_1 en ϕ_2 zijn surjectief). Met $c = bx + ay$ geldt nu

$$\begin{aligned}
\phi(c) = \phi_1(b)\phi(x) + \phi(a)\phi(y) &= \big(\phi_1(b), \phi_2(b)\big) \cdot (0, 1) + \big(\phi_1(a), \phi - 2(a)\big) \cdot (1, 0) \\
&= \big(\phi_1(a), \phi_2(b)\big) = z\,,
\end{aligned}$$

waarmee de surjectiviteit van ϕ bewezen is.

Dit bewijst de Chinese reststelling. □

Gevolg 2.37. *Laten n, $m \in \mathbb{Z}$ onderling ondeelbaar zijn. Dan is er een ringisomorfisme*

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\,,$$

gegeven door $a + nm\mathbb{Z} \mapsto \big(a + n\mathbb{Z},\, a + m\mathbb{Z}\big)$.

Bewijs. Dit volgt direct uit 2.36. □

Merk op dat de eis dat $\gcd(m,n) = 1$ niet gemist kan worden. Bijvoorbeeld $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, immers de optelgroepen zijn niet isomorf.

Gevolg 2.38. *Laten n, $m \in \mathbb{Z}$ onderling ondeelbaar zijn. Dan is er een isomorfisme van groepen*

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* .$$

Verder geldt $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Hierbij is φ de Euler φ-functie.

Bewijs. Dit volgt uit 2.37 en de opmerking dat $(R_1 \times R_2)^* = R_1^* \times R_2^*$; vgl. 1.24. De laatste bewering is een gevolg van de eerste want $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. □

Voorbeeld 2.39. Laat $R = \mathbb{Q}[X]$ en laat

$$I = \mathbb{Q}[X] \cdot (X-1) \qquad \text{en} \qquad J = \mathbb{Q}[X] \cdot (X+1).$$

Er geldt

$$-\frac{1}{2}(X-1) \in I, \quad \frac{1}{2}(X+1) \in J, \qquad \text{en} \quad -\frac{1}{2}(X-1) + \frac{1}{2}(X+1) = 1,$$

dus de idealen I en J zijn onderling ondeelbaar. Verder is:

$$I \cdot J = \mathbb{Q}[X] \cdot (X+1)(X-1) = \mathbb{Q}[X] \cdot (X^2-1)\,,$$

en uit 2.36 volgt dan:

$$\mathbb{Q}[X]/\mathbb{Q}[X](X^2-1) \cong (\mathbb{Q}[X]/I) \times (\mathbb{Q}[X]/J).$$

Blijkens 2.13 geldt $\mathbb{Q}[X]/I \cong \mathbb{Q}$ via $f \mapsto f(1)$ en $\mathbb{Q}[X]/J \cong \mathbb{Q}$ door $f \mapsto f(-1)$; dus

$$\mathbb{Q}[X]/\mathbb{Q}[X](X^2-1) \cong \mathbb{Q} \times \mathbb{Q}, \qquad (f \bmod (X^2-1)) \mapsto \big(f(1), f(-1)\big)\,.$$

2.40 Idempotenten Als $R = R_1 \times R_2$, waarbij R_1, R_2 ringen zijn, dan zijn $(1,0)$ en $(0,1)$ idempotenten van R. We gaan nu bewijzen dat in het commutatieve geval alle idempotenten zo verkregen worden.

Laat R dus een commutatieve ring zijn, en $e \in R$ een idempotent. We passen 2.36 toe op $I = R \cdot e$ en $J = R \cdot (1-e)$. Uit $e + (1-e) = 1$ blijkt dat I en J inderdaad onderling ondeelbaar zijn. Verder geldt $I \cdot J \cong Re(1-e) \cong R(e-e^2) = \{0\}$, omdat e idempotent is. Dus $R/I \cdot J \cong R/\{0\} \cong R$, en 2.36 levert

$$R \cong (R/Re) \times (R/R(1-e))\,.$$

Onder dit isomorfisme wordt e op $(0,1)$ afgebeeld, en $1-e$ op $(1,0)$. Blijkbaar is $1-e$ ook een idempotent, hetgeen ook gemakkelijk direct na te rekenen is.

We concluderen dat er een eenduidig verband bestaat, voor een commutatieve ring R, tussen de idempotenten van R en de manieren waarop men R als product van twee ringen R_1 en R_2 kan schrijven.

Een expliciet voorbeeld: met $R = \mathbb{Z}/6\mathbb{Z}$ en $e = \bar{4}$ vindt men het isomorfisme $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ uit 2.37 terug.

Opgaven

1. Laat zien dat het beeld $f(R_1)$ van een ringhomomorfisme $f\colon R_1 \to R_2$ een deelring is van R_2.

2. Zij R een ring. Bewijs dat er precies één ringhomomorfisme $f\colon \mathbb{Z} \to R$ bestaat.
   N.B. De niet-negatieve voortbrenger van $\mathrm{Ker}(f)$ noemt men wel de *karakteristiek* van R, notatie: $\mathrm{char}(R)$.

3. Bewijs dat de karakteristiek van een domein 0 of een priemgetal is.

4. Laat R_1, R_2 en R ringen zijn, en laat $f_1\colon R \to R_1$ en $f_2\colon R \to R_2$ afbeeldingen zijn. Laat zien dat de afbeelding $f\colon R \to R_1 \times R_2$, $x \mapsto (f_1(x), f_2(x))$ een ringhomomorfisme is dan en slechts dan als zowel f_1 als f_2 ringhomomorfismen zijn.

5. Laat R_1, R_2 ringen zijn, en laat R een *domein* zijn. Laat $f\colon R_1 \times R_2 \to R$ een ringhomomorfisme zijn. Laat zien dat een van volgende uitspraken geldt:

   (a) er is een ringhomomorfisme $g\colon R_1 \to R$ zodat voor alle $x \in R_1, y \in R_2$ geldt $f(x,y) = g(x)$;

   (b) er is een ringhomomorfisme $h\colon R_2 \to R$ zodat voor alle $x \in R_1, y \in R_2$ geldt $f(x,y) = h(y)$.

6. Bewijs dat de volgende ringen geen ringautomorfismen verschillend van de identiteit hebben:

$$\mathbb{Z}, \quad \mathbb{Z}/n\mathbb{Z} \text{ (voor } n \in \mathbb{Z}_{>0}), \quad \mathbb{Q}.$$

7. Laat zien dat $\mathbb{C}$ een ringautomorfisme verschillend van de identiteit heeft.

8. Laten R_1 en R_2 ringen zijn. Bewijs dat $(R_1 \times R_2)[X] \cong R_1[X] \times R_2[X]$.

9. Laat R een ring zijn, en zijn G_1 en G_2 groepen. Bewijs dat $R[G_1 \times G_2] \cong R[G_1]\big[G_2\big]$.

10. Zij K een lichaam, $R \subset K$ een deelring, en veronderstel dat elk element van K geschreven kan worden als as^{-1}, met $a, s \in R$ en $s \neq 0$. Bewijs: K is isomorf met het quotientenlichaam $Q(R)$ van R.

11. Is $\det\colon \mathrm{M}(n,\mathbb{R}) \to \mathbb{R}$ een ringhomomorfisme?

12. Laat $f\colon R_1 \to R_2$ een ringhomomorfisme zijn. Bewijs dat $g = f|R_1^*$ een groephomomorfisme $R_1^* \to R_2^*$ is, en laat aan de hand van een voorbeeld zien dat g niet surjectief hoeft te zijn als f het is.

13. Zij $G = \{1, \sigma\}$ een multiplicatief geschreven groep van orde twee. Definieer $f\colon \mathbb{R}[G] \to \mathbb{R} \times \mathbb{R}$ door $f(a + b\sigma) = (a + b, a - b)$, voor $a, b \in \mathbb{R}$. Bewijs dat f een ringisomorfisme is.

14. Bewijs: $\mathrm{End}(\mathbb{Z}^+) \cong \mathbb{Z}$, $\mathrm{End}(\mathbb{Q}^+) \cong \mathbb{Q}$ en $\mathrm{End}((\mathbb{Z}/n\mathbb{Z})^+) \cong \mathbb{Z}/n\mathbb{Z}$ als ringen.

15. Zij A een additief geschreven abelse groep, en $B = \{a \in A \mid a \text{ heeft eindige orde}\}$. Definieer $I \subset \mathrm{End}(A)$ door
$$I = \{\sigma \in \mathrm{End}(A) \mid \sigma(x) = 0 \text{ voor alle } x \in B\}.$$
Bewijs dat I een ideaal van $\mathrm{End}(A)$ is, en dat $\mathrm{End}(A)/I$ isomorf is met een deelring van $\mathrm{End}(B)$.

16. Zij R een ring. Voor $a \in R$ definiëren we $\lambda_a, \rho_a \colon R \to R$ door $\lambda_a(x) = ax, \rho_a(x) = xa$.

    (a) Bewijs: $\lambda_a, \rho_a \in \mathrm{End}(R^+)$ voor alle $a \in R$.

    (b) Bewijs dat de afbeelding $f \colon R \to \mathrm{End}(R^+),\ f(a) = \lambda_a$, een ringhomomorfisme is.

    (c) Bewijs dat de afbeelding $g \colon R^0 \to \mathrm{End}(R^+),\ g(a) = \rho_a$, een ringhomomorfisme is, met R^0 de "tegengestelde ring" gedefinieerd in Opgave 7 van Hoofdstuk 1.

17. Een *Cauchyrij* over $\mathbb{Q}$ is een rij $(a_n)_{n=1}^{\infty}$, met $a_n \in \mathbb{Q}$, waarvoor geldt:
$$\forall \epsilon \in \mathbb{Q}_{>0} : \exists n_0 : \forall n, m > n_0 : \quad |a_n - a_m| < \epsilon.$$
De verzameling Cauchyrijen over $\mathbb{Q}$ vormt een ring R, met componentsgewijze bewerkingen. Een *nulrij* is een rij $(a_n)_{n=1}^{\infty}$ met $a_n \in \mathbb{Q}$ waarvoor geldt: $\lim_{n\to\infty} a_n = 0$. Bewijs dat de verzameling $I \subset R$ bestaande uit alle nulrijen een *ideaal* van R is, en dat $R/I \cong \mathbb{R}$, het lichaam der reële getallen.

18. Laat R een ring zijn en G een groep. Definieer $f \colon R[G] \to R$ door $f(\sum_{g\in G}\ a_g g) = \sum_{g\in G}\ a_g$. Bewijs dat f een ringhomomorfisme is, en dat $\mathrm{Ker}(f)$ wordt voortgebracht door $\{g - 1 \mid g \in G\}$.

19. Laat zien dat de afbeelding $f \colon \mathbb{Z}[i] \to \mathbb{F}_2,\ a + bi \mapsto \bar{a} + \bar{b}$ uit Voorbeeld 2.10 een surjectief ringhomomorfisme is.

20. Zij $R = \mathbb{Z}[\sqrt{-5}]$ en zij
$$\phi \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/3\mathbb{Z}, \qquad a + b\sqrt{-5} \mapsto \overline{a + b} \qquad (a,\, b \in \mathbb{Z}).$$

    (a) Bewijs dat ϕ een surjectief ringhomomorfisme is.

    (b) Bewijs dat $\mathrm{Ker}(\phi) = (3,\, 1 - \sqrt{-5})$

    (c) Bewijs dat $\mathrm{Ker}(\phi)$ geen hoofdideaal is. (Aanwijzing: stel $\mathrm{Ker}(\phi) = (x)$, met $3 = xy$ en $1 - \sqrt{-5} = xz$, bekijk dan $N(xy)$ en $N(xz)$ met N uit 1.14.)

    (d) Bewijs ook dat $(2,\, 1 - \sqrt{-5})$ geen hoofdideaal is.

    (e) Is het ideaal $(3,\, 1 - \sqrt{-5}) \cdot (2,\, 1 - \sqrt{-5})$ een hoofdideaal?

21. Definieer $\varphi \colon \mathbb{Z}[i] \to \mathbb{F}_{13}$ door $\varphi(a + bi) = a + 5b \bmod 13$. Bewijs dat φ een homomorfisme is, en dat $\mathrm{Ker}(\varphi)$ wordt voortgebracht door 13 en $i - 5$. Laat zien dat $\mathrm{Ker}(\varphi)$ een hoofdideaal is.

22. Zij R een ring en $I \subset R$ een linksideaal dat een rechtseenheid bevat. Bewijs: $I = R$.

23. Laten R_1 en R_2 ringen zijn, en $I = \{0\} \times R_2 \subset R_1 \times R_2$. Bewijs dat I een hoofdideaal van $R_1 \times R_2$ is.

24. Laten R_1 en R_2 ringen zijn. Bewijs dat alle idealen van $R_1 \times R_2$ van de vorm $I_1 \times I_2$ zijn, met I_i een ideaal van R_i $(i = 1, 2)$.

25. Zij R een ring met de eigenschap dat $f\colon R \to R$, $f(x) = x^2$, een ringhomomorfisme van R naar zichzelf is. Bewijs: R is commutatief, en $\mathrm{char}(R) = 1$ of 2 (zie Opgave 2). Bewijs ook dat $1 + x \in R^*$ voor alle $x \in \mathrm{Ker}(f)$.

26. (a) Bewijs dat
$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2, \mathbb{R}) \;\middle|\; b = d = 0 \right\}$$
een linksideaal maar geen rechtsideaal van $\mathrm{M}(2, \mathbb{R})$ is.

(b) Vind een rechtsideaal van $\mathrm{M}(2, \mathbb{R})$ dat geen linksideaal is.

27. Laat $n \in \mathbb{Z}_{>0}$. In deze opgave vatten we de elementen van $\mathrm{M}(n, \mathbb{R})$ op als $\mathbb{R}$-lineaire endomorfismen van $\mathbb{R}^n$. Met W geven we een $\mathbb{R}$-lineaire deelruimte van $\mathbb{R}^n$ aan.

(a) Bewijs dat $\{A \in \mathrm{M}(n, \mathbb{R}) \mid Aw = 0 \text{ voor alle } w \in W\}$ een linksideaal van $\mathrm{M}(n, \mathbb{R})$ is.

(b) Bewijs dat $\{A \in \mathrm{M}(n, \mathbb{R}) \mid Av \in W \text{ voor alle } v \in \mathbb{R}^n\}$ een rechtsideaal van $\mathrm{M}(n, \mathbb{R})$ is.

(c) Bewijs: elk linksideaal van $\mathrm{M}(n, \mathbb{R})$ is van de onder (a) aangegeven vorm, en elk rechtsideaal van $\mathrm{M}(n, \mathbb{R})$ is van de onder (b) aangegeven vorm.

(d) Bewijs dat $\{0\}$ en $\mathrm{M}(n, \mathbb{R})$ de enige tweezijdige idealen van $\mathrm{M}(n, \mathbb{R})$ zijn.

28. Zij $I \subset R$ een ideaal in een ring en zij $\phi\colon R \to R/I$ de natuurlijke afbeelding.

(a) Zij $J' \subset R/I$ een ideaal. Bewijs dat
$$\phi^{-1}(J') = \{x \in R \mid \phi(x) \in J'\}$$
een ideaal van R is. Merk op dat $I \subset \phi^{-1}(J')$.

(b) Bewijs dat $J' \mapsto \phi^{-1}(J')$ een bijectie geeft tussen de idealen J' van R/I en de idealen J van R met $I \subset J$.

(c) Bewijs dat voor een ideaal J met $I \subset J$ geldt: $(R/I)/\phi(J) \cong R/J$.

29. Laat zien dat $\mathbb{Z}[X]/(X^2 + 1)$ isomorf is met $\mathbb{Z}[i]$.

30. Zij R een commutatieve ring. Laat zien dat er een bijectie is tussen de verzameling van ringhomomorfismen $\mathbb{Z}[i] \to R$, en de verzameling van $x \in R$ met $x^2 + 1 = 0$.

31. Bepaal voor $p \in \{2, 3, 5, \ldots, 19\}$ het aantal ringhomomorfismen $\mathbb{Z}[i] \to \mathbb{F}_p$.

32. Zij K een lichaam. De *ring van de duale getallen* over K, notatie: $K[\epsilon]$, bestaat uit de uitdrukkingen $a + b\epsilon$, met $a, b \in K$, die als volgt opgeteld en vermenigvuldigd worden:
$$(a + b\epsilon) + (c + d\epsilon) = (a + c) + (b + d)\epsilon,$$
$$(a + b\epsilon) \cdot (c + d\epsilon) = (ac) + (ad + bc)\epsilon$$
(dus $\epsilon^2 = 0$), voor $a, b, c, d \in K$.

(a) Bewijs: $K[\epsilon] \cong K[X]/(X^2)$.

(b) Bewijs dat $K[\epsilon]$ precies *drie* idealen heeft.

(c) Bewijs: $K[\epsilon]^* \cong K^* \times K^+$ (als groepen).

33. Zij R een ring met $1 \neq 0$, en $I = R - R^*$. Stel dat er voor elke $x \in I$ een $n \in \mathbb{Z}_{>0}$ bestaat met $x^n = 0$. Bewijs dat I een tweezijdig ideaal van R is, en dat R/I een delingsring is.

34. Zij R een ring, $I \subset R$ een ideaal, en $R' \subset R$ een deelring. Bewijs:

(a) $R' \cap I$ is een ideaal van R';

(b) $R' + I = \left\{ r + s \;\middle|\; r \in R', s \in I \right\}$ is een deelring van R;

(c) $R'/(R' \cap I) \cong (R' + I)/I$.

35. Zij R een ring, en definieer

$$[R, R] = \left\{ \sum_{i=1}^{n} r_i(x_i y_i - y_i x_i) \;\middle|\; n \in \mathbb{Z}_{>0}, r_i, x_i, y_i \in R \right\}.$$

Bewijs dat $[R, R]$ een ideaal van R is, en dat $R/[R, R]$ een commutatieve ring is.

36. Laat

$$R = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}(2, \mathbb{R}) \;\middle|\; c = 0 \right\} \qquad \text{en} \qquad I = \left\{ \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \in \mathrm{M}(2, \mathbb{R}) \;\middle|\; b \in \mathbb{R} \right\}.$$

Bewijs de volgende uitspraken:

(a) R is een deelring van $\mathrm{M}(2, \mathbb{R})$;

(b) I is een ideaal van R, en $R/I \cong \mathbb{R} \times \mathbb{R}$;

(c) R is niet commutatief maar R/I wel.

37. Laat $f = \sum_{j \geq 0} a_j X^j \in \mathbb{R}[X]$, en schrijf $g = \sum_{j \geq 0} a_{2j} X^j$ en $h = \sum_{j \geq 0} a_{2j+1} X^j$. Bewijs dat de volgende uitspraken equivalent zijn:

(a) $f(i) = 0$;

(b) $g(-1) = h(-1) = 0$;

(c) $f \in \mathbb{R}[X] \cdot (X^2 + 1)$.

38. Zij $R = \mathbb{Z}[X]$ en $I = (2, X) \subset R$. Bewijs dat $X^2 + 4 \in I \cdot I$, maar dat $X^2 + 4$ niet geschreven kan worden als xy, met $x, y \in I$. Concludeer dat $\left\{ xy \;\middle|\; x, y \in I \right\}$ geen ideaal van R is.

39. Zij R een ring, en I, J idealen van R. Bewijs:

$$(I + J) \cdot (I \cap J) \subset (I \cdot J) + (J \cdot I).$$

Bewijs dat gelijkheid geldt als $R = \mathbb{Z}$.

40. Bewijs dat Stelling 2.36 ook geldig is voor niet-commutatieve ringen, als men op beide plaatsen $I \cdot J$ door $I \cdot J + J \cdot I$ vervangt.

41. Laat R een ring zijn, en I_1, I_2, I_3 idealen van R. Als $I_1 + I_3 = R$ en $I_2 + I_3 = R$, bewijs dat $(I_1 \cdot I_2) + I_3 = R$.

42. (Chinese reststelling voor meer idealen). Zij R een commutatieve ring, en laten $I_1, I_2, ..., I_t$ idealen van R zijn die paarsgewijs onderling ondeelbaar zijn, d.w.z. $I_i + I_j = R$ voor $1 \leq i < j \leq t$. Bewijs: $R/(\prod_{i=1}^{t} I_i) \cong \prod_{i=1}^{t}(R/I_i)$. (Aanwijzing: bewijs $(I_1 \cdot I_2 \cdots I_{t-1}) + I_t = R$ als in opgave 41, en pas inductie naar t toe.)

43. Zij R een commutatieve ring zodanig dat $1 + 1 \in R^*$. Bewijs:

$$R[X]/R[X](X^2 - 1) \cong R \times R.$$

44. Laat $R = \big\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \;\big|\; a \equiv b \bmod 2\big\}$.

    (a) Bewijs dat R een deelring van $\mathbb{Z} \times \mathbb{Z}$ is.

    (b) Bewijs: $\mathbb{Z}[X]/\mathbb{Z}[X] \cdot (X^2 - 1) \cong R$.

    (c) Bewijs: $\mathbb{Z}[X]/\mathbb{Z}[X] \cdot (X^2 - 1)$ is *niet* isomorf met $\mathbb{Z} \times \mathbb{Z}$ (aanwijzing: bepaal de idempotenten van R en $\mathbb{Z} \times \mathbb{Z}$).

    (d) Laat zien: er is geen $f \in \mathbb{Z}[X]$ met $f(1) = 1$, $f(-1) = 0$. (Wat is het verband tussen dit onderdeel en de rest van de som?)

45. Zij R een commutatieve ring, en laten $w_1, w_2, ..., w_m$ elementen van R zijn met $w_i - w_j \in R^*$ voor alle i, j met $1 \leq i < j \leq m$. Laat $f = \prod_{i=1}^{m}(X - w_i) \in R[X]$. Bewijs: $R[X]/R[X]f \cong R \times R \times \cdots \times R$ (m factoren).

46. Bewijs:

$$\mathbb{Q}[X]/(X^3 + X) \cong \mathbb{Q} \times \mathbb{Q}[X]/(X^2 + 1),$$

    en

$$\mathbb{R}[X]/(X^4 - 1) \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C}.$$

47. Zij R een commutatieve ring, en $\mathrm{Idemp}(R)$ de verzameling idempotenten van R (inclusief de triviale idempotenten 0 en 1). Bewijs:

$$e_1, e_2 \in \mathrm{Idemp}(R) \implies e_1 + e_2 - 2e_1e_2 \in \mathrm{Idemp}(R)\,, \quad e_1e_2 \in \mathrm{Idemp}(R)\,.$$

    Laat zien dat $\mathrm{Idemp}(R)$ een commutatieve ring vormt als de optelling $\oplus$ en de vermenigvuldiging $\circ$ gedefinieerd worden door

$$e_1 \oplus e_2 = e_1 + e_2 - 2e_1e_2\,, \quad e_1 \circ e_2 = e_1e_2\,.$$

    Onder welke omstandigheden is $\mathrm{Idemp}(R)$ een deelring van R?

Hoofdstuk 3

Nulpunten van polynomen

Laat R een ring zijn. Voor $f = \sum_{i=0}^{n} a_i X^i$ en $\alpha \in R$ hebben we in 2.13 gedefineerd: $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in R$. Op deze wijze geeft elk polynoom $f \in R[X]$ aanleiding tot een functie $R \to R$. Merk evenwel op dat twee verschillende polynomen best aanleiding kunnen geven tot dezelfde functie $R \to R$. De polynomen X en X^2 in $\mathbb{F}_2[X]$ zijn bijvoorbeeld verschillend, maar ze geven aanleiding tot dezelfde functie $\mathbb{F}_2 \to \mathbb{F}_2$, daar $0^2 = 0$ en $1^2 = 1$. Dit verschijnsel doet zich echter niet voor in het geval van de ring $\mathbb{R}$ der reële getallen: als f, $g \in \mathbb{R}[X]$ de eigenschap hebben dat $f(\alpha) = g(\alpha)$ voor alle $\alpha \in \mathbb{R}$, dan heeft het polynoom $h = f - g$ alle reële getallen als nulpunt; omdat een polynoom $\neq 0$ niet meer nulpunten kan hebben dan zijn graad bedraagt (vgl. 3.7) is dit alleen mogelijk als $h = 0$, d.w.z., $f = g$.

In dit hoofdstuk zijn we geïnteresseerd in nulpunten van polynomen over algemene ringen; hierbij noemen we $\alpha \in R$ *nulpunt* van $f \in R[X]$ als $f(\alpha) = 0$. Ons voornaamste hulpmiddel is de volgende stelling, die de mogelijkheid van *deling met rest* voor polynomen uitspreekt en analoog is aan de deling met rest voor gehele getallen.

Stelling 3.1. *Zij R een ring, en f, $g \in R[X]$. Neem aan dat $g \neq 0$ en dat de kopcoëfficiënt van g een* eenheid *van R is. Dan bestaan er unieke q, $r \in R[X]$ zodanig dat*

$$f = qg + r\,, \qquad \text{en } r = 0 \text{ of } \operatorname{gr}(r) < \operatorname{gr}(g).$$

Men noemt q en r het quotiënt en de rest bij de deling door g. Indien we de conventie aanhouden dat het nulpolynoom graad $-\infty$ heeft, dan hoeven we de mogelijk dat $r = 0$ niet apart te vermelden.

Bewijs. We gaan eerst de existentie van q en r bewijzen, de uniciteit komt daarna. Laat $n = \operatorname{gr}(f)$ en $m = \operatorname{gr}(g) \geq 0$. We voeren het bewijs, bij vaste g, met inductie naar n.

Als $n < m$ dan kunnen we $q = 0$ en $r = f$ nemen; dit geval is het begin van de inductie.

Laat nu $n \geq m$. Zij a de kopcoëfficiënt van f, en b die van g. Er is gegeven dat b een eenheid is, dus er is een $c \in R$ met $cb = 1$. Het polynoom $acX^{n-m} \cdot g$ heeft dan graad n en kopcoëfficiënt $a \cdot cb = a$, evenals het polynoom f. Hieruit volgt dat

$$f_1 = f - acX^{n-m} \cdot g$$

een graad heeft die *kleiner* dan n is; de n-de graads termen vallen immers tegen elkaar weg. We kunnen op f_1 nu de inductiehypothese toepassen, en we vinden dat er q_1, $r_1 \in R[X]$ bestaan met:

$$f_1 = q_1 g + r_1 \qquad \text{en } r_1 = 0 \text{ of } \mathrm{gr}(r_1) < \mathrm{gr}(g).$$

Er geldt dus:

$$f = f_1 + acX^{n-m}g = \big(acX^{n-m} + q_1\big) \cdot g + r_1\,.$$

Laat nu $q = acX^{n-m} + q_1$ en $r = r_1$, dan hebben we:

$$f = qg + r\,, \qquad r = 0 \text{ of } \mathrm{gr}(r) < \mathrm{gr}(g),$$

zoals verlangd.

Nu bewijzen we de uniciteit van q en r. Stel dat ook $f = q'g + r'$ en dat $r' = 0$ of $\mathrm{gr}(r') < \mathrm{gr}(g)$. Dan hebben we:

$$(q - q')g = r' - r\,.$$

De graad van het rechterlid is kleiner dan $\mathrm{gr}(g)$. Zou nu $q \neq q'$, dan was de graad van de linkerkant groter dan of gelijk aan $\mathrm{gr}(g)$, aangezien de kopcoëfficient van g een eenheid is. Dit levert een tegenspraak, dus moet wel $q = q'$, en dan ook $r' - r = 0$ dus $r = r'$.

Hiermee is Stelling 3.1 bewezen. Merk op dat we niet verondersteld hebben dat R commutatief is. □

Voorbeeld 3.2. Het delen van polynomen gaat in de praktijk met een staartdeling. Zij $R = \mathbb{Z}$ en laat $f, g \in \mathbb{Z}[X]$:

$$f = X^4 - X^3 - 2X^2 + 3X - 4, \qquad g = X^2 - 1.$$

het quotiënt q en de rest r worden alsvolgt bepaald:

$$\begin{array}{rrrrrrl}
X^2-1\,/ & X^4 & -X^3 & -2X^2 & +3X & -4 & \big\backslash X^2 - X - 1 \\
 & X^4 & & -X^2 & & & \\
\cline{2-4}
 & & -X^3 & -X^2 & & & \\
 & & -X^3 & & +X & & \\
\cline{3-5}
 & & & -X^2 & +2X & & \\
 & & & -X^2 & & +1 & \\
\cline{4-6}
 & & & & 2X & -5 &
\end{array}$$

Dus $q = X^2 - X - 1,\ r = 2X - 5$.

Voorbeeld 3.3. We gebruiken deling met rest om de kern van een evaluatiehomorfisme te bepalen. Zij R een domein en zij $\Phi\colon R[X,Y] \to R[T]$ het homomorfisme gegeven door $\Phi(f) = f(T^3, T^7)$. Voor een polynoom $f = \sum_{i,j} a_{ij}X^iY^j$ is dus $\Phi(f) = \sum_{i,j} a_{ij}T^{3i+7j}$. Het is duidelijk dat $X^7 - Y^3 \in \mathrm{Ker}(\Phi)$. Met behulp van dit element gaan we de kern van Φ bepalen.

Zij $f \in \mathrm{Ker}(\Phi) \subset R[X,Y]$. Dan kunnen we f delen door $X^7 - Y^3$ met rest in de polynoomring $\big(R[X]\big)[Y]$. (Immers, -1 is een eenheid in $R[X]$.) Dit geeft een relatie $f = q \cdot (X^7 - Y^3) + r$ waarbij de rest van de vorm $r = f_0 + f_1Y + f_2Y^2$ is met $f_i \in R[X]$. Passen we Φ toe dan vinden we

$$0 = \Phi(f) = \Phi(r) = f_0(T^3) + f_1(T^3) \cdot T^7 + f_2(T^3) \cdot T^{14}\,.$$

Dus alle coëfficiënten van het polynoom in het rechterlid zijn nul. Echter, $f_j(T^3)$ is een som van termen a_iT^i met $i \equiv 0 \bmod 3$, dus $f_1(T^3) \cdot T^7$ is een som van termen a_iT^i met $i \equiv 1 \bmod 3$ en $f_2(T^3) \cdot T^{14}$ is een som van termen a_iT^i met $i \equiv 2 \bmod 3$. We concluderen dat de termen $f_0(T^3)$, $f_1(T^3) \cdot T^7$ en $f_2(T^3) \cdot T^{14}$ elk afzonderlijk nul zijn. Dit is equivalent met $f_0 = f_1 = f_2 = 0$, d.w.z. met $r = 0$. Dus de kern van Φ is het ideaal $(X^7 - Y^3)$.

Gevolg 3.4. *Zij K een* lichaam. *Dan is ieder ideaal van $K[X]$ een hoofdideaal.*

Bewijs. Zij $I \subset K[X]$ een ideaal. We moeten een $g \in I$ vinden met $I = K[X] \cdot g$. Als $I = \{0\}$, dan kunnen we $g = 0$ kiezen. Laat nu $I \neq \{0\}$ en kies $g \in I, g \neq 0$, zódanig dat $\mathrm{gr}(g)$ zo klein mogelijk is. We beweren dat

$$I = K[X] \cdot g\,.$$

De inclusie $\supseteq$ is duidelijk, want $g \in I$ en I is een ideaal dus $fg \in I$ voor alle $f \in K[X]$. De inclusie $\subseteq$ wordt als volgt bewezen. Zij $f \in I$ willekeurig. Omdat K een lichaam is, is de kopcoëfficiënt van g een eenheid in K, dus we mogen Stelling 3.1 toepassen. Dit levert q, $r \in K[X]$ met

$$f = qg + r, \qquad r = 0 \text{ of } \mathrm{gr}(r) < \mathrm{gr}(g).$$

Merk op dat $r = f - qg$ tot I behoort. Als $r \neq 0$, dan is r een element van I, niet 0, met een graad kleiner dan die van g, in tegenspraak met de keuze van g. Dus moeten we hebben $r = 0$, en $f = qg \in K[X]g$. Iedere $f \in I$ zit dus in $K[X] \cdot g$ en dit bewijst $\subseteq$. Hiermee is Gevolg 3.4 bewezen. □

Het bewijs laat zien dat (voor $I \neq 0$) ieder polynoom $0 \neq g \in I$ van minimale graad een voortbrenger van I is; d.w.z., $I = (g)$.

De voorwaarde in Gevolg 3.4 dat K een lichaam is, kan niet gemist worden want in 2.15 hebben we al gezien dat $(2,\, X) \subset \mathbb{Z}[X]$ geen hoofdideaal is.

Stelling 3.5. *Zij R een commutatieve ring, $\alpha \in R$ en $f \in R[X]$. Dan is er een $q \in R[X]$ met*

$$f = q \cdot (X - \alpha) + f(\alpha)\,.$$

Bewijs. Passen we 3.1 toe met $g = X - \alpha$ dan vinden we $f = q \cdot (X - \alpha) + r$ met $r = 0$ of $\mathrm{gr}(r) < 1$. Dan is r een constant polynoom, dus $r \in R$, en invullen van α voor X geeft $f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r = r$. □

Stelling 3.6. *Laat R een* domein *zijn, laat $f \in R[X]$, en laat $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ onderling* verschillende *nulpunten van f zijn. Dan is er een $q \in R[X]$ met*

$$f = q \cdot (X - \alpha_1) \cdot (X - \alpha_2) \cdots (X - \alpha_n)\,.$$

Bewijs. We gebruiken inductie naar n. Voor $n = 1$ is het voldoende 3.5 toe te passen (met $f(\alpha) = 0$). Laat nu $n > 1$. Uit $f(\alpha_n) = 0$ en 3.5 volgt dat er een $f_1 \in R[X]$ is met

$$f = f_1 \cdot (X - \alpha_n)\,.$$

Voor $1 \leq i \leq n - 1$ geldt:

$$f_1(\alpha_i) \cdot (\alpha_i - \alpha_n) = f(\alpha_i) = 0\,,$$

en $\alpha_i - \alpha_n \neq 0$ (want alle α_i zijn verschillend); omdat R geen nuldelers heeft volgt hieruit

$$f_1(\alpha_i) = 0 \qquad (1 \leq i \leq n-1)\,.$$

De inductiehypothese, toegepast op f_1, laat zien dat

$$f_1 = q \cdot (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_{n-1})$$

voor zekere $q \in R[X]$, dus

$$f = f_1(X - \alpha_n) = q \cdot (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)\,,$$

zoals verlangd. Hiermee is Stelling 3.6 bewezen. □

Stelling 3.7. *Zij R een domein, en $f \in R[X]$ een polynoom ongelijk aan nul. Dan is het aantal onderling verschillende nulpunten van f in R ten hoogste gelijk aan* $\mathrm{gr}(f)$.

Bewijs. Dit volgt uit Stelling 3.6, want als $\alpha_1, \ldots, \alpha_n$ verschillende nulpunten zijn van f dan is $f = q \cdot (X - \alpha_1) \ldots (X - \alpha_n)$. Dit geeft $\mathrm{gr}(f) = \mathrm{gr}(q) + n$, dus $\mathrm{gr}(f) \geq n$. □

3.8 Uit 3.7 volgt dat twee polynomen f, $g \in R[X]$ (R een domein) van graad $\leq n$ gelijk zijn zodra ze in $n+1$ elementen van R dezelfde waarde aannemen; immers, het verschil $f - g$ heeft dan graad $\leq n$ en $\geq n+1$ nulpunten, en het moet wegens 3.7 dus gelijk zijn aan het nulpolynoom. Dit argument wordt vaak gebruikt om aan te tonen dat twee polynomen gelijk zijn. Voor een expliciete formule voor het eenduidig bepaalde polynoom van graad $\leq n$ dat in $n+1$ punten een gegeven waarde aanneemt, zie Opgave 2.

Er zijn verschillende redenen waarom een n-de graads polynoom f *minder* dan n verschillende nulpunten kan hebben. Enerzijds kan het gebeuren dat het domein "te klein" is: $2X - 1 \in \mathbb{Z}[X]$ heeft geen nulpunt in $\mathbb{Z}$, maar wel in het quotiëntenlichaam $\mathbb{Q}$ van $\mathbb{Z}$; en $X^2 - 2$ heeft geen nulpunt in $\mathbb{Q}$ maar wel in het "uitbreidingslichaam" $\mathbb{Q}\big(\sqrt{2}\big)$ van $\mathbb{Q}$. In de hoofdstukken over lichamen zullen we zien hoe men een gegeven lichaam zodanig kan uitbreiden dat een gegeven polynoom een nulpunt krijgt.

Anderzijds kan het voorkomen dat het polynoom f minder dan $\mathrm{gr}(f)$ nulpunten heeft doordat er nulpunten "samenvallen": het polynoom $X^2 - 2X + 1 = (X-1)^2 \in \mathbb{Q}[X]$ heeft slechts één nulpunt in $\mathbb{Q}$, nl. 1. Dergelijke dubbele nulpunten kan men op het spoor komen door *differentiatie*, zoals we aan het eind van dit hoofdstuk zullen zien.

Opmerking 3.9. De eis in 3.7 dat R een domein is, is essentieel. Het polynoom $X^2 - \bar{1}$ in $(\mathbb{Z}/8\mathbb{Z})\big[X\big]$ van graad 2 heeft 4 nulpunten in $\mathbb{Z}/8\mathbb{Z}$ en $X^2 + 1 \in \mathbb{H}[X]$ heeft zelfs oneindig veel nulpunten in $\mathbb{H}$, zie Opgaven 3 en 4. De ringen $\mathbb{Z}/8\mathbb{Z}$ en $\mathbb{H}$ zijn dan ook geen domeinen: $\mathbb{Z}/8\mathbb{Z}$ heeft nuldelers en $\mathbb{H}$ is niet commutatief.

Stelling 3.10. *Zij p een priemgetal. Dan geldt*

$$\prod_{a \in \mathbb{F}_p} (X - a) = X^p - X$$

in $\mathbb{F}_p[X]$.

Bewijs. Uit de Kleine Stelling van Fermat weten we dat $a^p = a$ voor alle $a \in \mathbb{F}_p$. Alle p elementen van $\mathbb{F}_p$ zijn dus nulpunten van $X^p - X$. Passen we Stelling 3.6 toe op $f = X^p - X$ dan vinden we dat

$$X^p - X = q \cdot \prod_{a \in \mathbb{F}_p} (X - a)$$

voor zekere $q \in \mathbb{F}_p[X]$. Berekenen we aan beide zijden de graad, dan zien we dat $\mathrm{gr}(q) = 0$, dus q is een constante. Vergelijken we de kopcoëfficiënten, dan ontdekken we dat $q = 1$. Hiermee is 3.10 bewezen. □

Voorbeeld 3.11. In $\mathbb{F}_5[X]$ geldt:

$$\begin{aligned}\prod_{a \in \mathbb{F}_5} (X - a) &= (X - \bar{2}) \cdot (X - \bar{1}) \cdot X \cdot (X + \bar{1}) \cdot (X + \bar{2}) \\ &= (X^2 - \bar{2}^2) \cdot (X^2 - \bar{1}^2) \cdot X \\ &= (X^2 + \bar{1}) \cdot (X^2 - \bar{1}) \cdot X \\ &= (X^4 - \bar{1}) \cdot X = X^5 - X\,,\end{aligned}$$

in overeenstemming met 3.10.

Gevolg 3.12 (Stelling van Wilson; Sir John Wilson, 1741–1793)**.** *Zij p een priemgetal. Dan geldt* $(p-1)! \equiv -1 \bmod p$.

Bewijs. Deel de gelijkheid in 3.10 door X, dan vinden we $\prod_{a=1}^{p-1}(X - \bar{a}) = X^{p-1} - \bar{1}$ in $\mathbb{F}_p[X]$. Substitueren we $X = 0$ dan komt er $(-1)^{p-1} \cdot \prod_{a=1}^{p-1} \bar{a} = -\bar{1}$, dus $(-1)^{p-1} \cdot (p-1)! \equiv -1 \bmod p$. Aangezien $(-1)^{p-1} \equiv 1 \bmod p$ (ook voor $p = 2$!) volgt hieruit de Stelling van Wilson. □

Bijvoorbeeld, $6! = 720 = -1 + 7 \cdot 103$ en $10! = 3628800 = -1 + 11 \cdot 329891$. Ook de omkering van 3.12 geldt; zie Opgave 5.

In het bewijs van Stelling 3.14 zullen we een resultaat uit de groepentheorie gebruiken. Volledigheidshalve zullen we eerst het bewijs geven van dat resultaat.

Lemma 3.13. *Zij G een abelse groep.*

(a) *Stel x en y zijn elementen van G van eindige orde. Veronderstel dat* $\mathrm{orde}(x)$ *en* $\mathrm{orde}(y)$ *onderling ondeelbaar zijn. Dan geldt* $\mathrm{orde}(xy) = \mathrm{orde}(x) \cdot \mathrm{orde}(y)$.

(b) *Stel G is een eindige groep en $a \in G$ is een element waarvan de orde* $\mathrm{orde}(a)$ *zo groot mogelijk is, d.w.z.,*

$$\mathrm{orde}(a) = \max\big\{\mathrm{orde}(x) \;\big|\; x \in G\big\}\,.$$

Dan geldt voor elke $b \in G$ dat $\mathrm{orde}(b)$ *een* deler *van* $\mathrm{orde}(a)$ *is.*

Bewijs. (a) Laat $k = \mathrm{orde}(x)$, $l = \mathrm{orde}(y)$ en $m = \mathrm{orde}(xy)$. We moeten bewijzen dat $m = k \cdot l$. Omdat G abels is geldt $(xy)^{kl} = x^{kl} \cdot y^{kl} = e \cdot e = e$, dus kl is in elk geval deelbaar door $\mathrm{orde}(xy) = m$.

Wegens $(xy)^m = e$ geldt $e = (xy)^{km} = x^{km} \cdot y^{km} = e \cdot y^{km} = y^{km}$ dus km is deelbaar door $\mathrm{orde}(y) = l$. Maar $\mathrm{ggd}(k, l) = 1$, dus m is deelbaar door l. Evenzo ziet men dat m deelbaar is door k. Dus m is deelbaar door $\mathrm{kgv}(k, l) = kl$. We zagen net al dat kl deelbaar is door m, dus $m = kl$, zoals verlangd.

(b) Laat $b \in G$. Om te bewijzen dat orde(b) een deler is van orde(a), is het voldoende te bewijzen dat voor elk priemgetal p het aantal factoren p in orde(a) groter dan of gelijk is aan het aantal factoren p in orde(b). Laat dus p een priemgetal zijn, en schrijf orde$(a) = p^i \cdot m$ en orde$(b) = p^j \cdot n$ met $p \nmid m$ en $p \nmid n$. Te bewijzen: $i \geq j$.

Uit orde$(a) = p^i \cdot m$ volgt dat orde$(a^{p^i}) = m$; uit orde$(b) = p^j \cdot n$ volgt orde$(b^n) = p^j$. Omdat ggd$(m, p^j) = 1$ volgt uit onderdeel (a) dat orde$(a^{p^i} \cdot b^n) = m \cdot p^j$. Maar a heeft maximale orde, dus $m \cdot p^j \leq$ orde$(a) = m \cdot p^i$, en hieruit volgt dat $j \leq i$, zoals velangd. □

Stelling 3.14. *Zij R een* domein *en G een* eindige *ondergroep van de eenhedengroep R^* van R. Dan is G* cyclisch.

Bewijs. Omdat R commutatief is, is G abels. Laat $a \in G$ een element zijn waarvan de orde zo groot mogelijk is, zegt orde$(a) = m$. Wegens Lemma 3.13(b) geldt voor alle $b \in G$ dat orde(b) een deler is van m. Dus alle $b \in G$ zijn nulpunten van het polynoom $X^m - 1$. Omdat $X^m - 1$ niet meer dan m nulpunten in R heeft (zie 3.7), volgt hieruit dat $\#G \leq m$. Maar ook is $m =$ orde(a) een deler van $\#G$, dus $m = \#G$ en a brengt de hele groep voort. Hiermee is 3.14 bewezen. □

Opmerking 3.15. De conclusie van 3.14 kan fout zijn als R niet een domein is: $\mathbb{Z}/8\mathbb{Z}$ is geen domein en $(\mathbb{Z}/8\mathbb{Z})^*$ is niet cyclisch maar isomorf met de viergroep van Klein. Ook de eindigheid van G is essentieel: $\mathbb{Q}^*$ is oneindig en zeker niet cyclisch.

Is R een domein en $G \subset R^*$ een eindige ondergroep, dan heeft elke $x \in G$ eindige orde. Elementen van R^* van eindige orde noemt men eenheidswortels. In $\mathbb{Q}^*$ en $\mathbb{R}^*$ zijn er alleen de eenheidswortels ± 1. In $\mathbb{C}^*$ zijn er oneindig veel eenheidswortels, nl. de elementen $e^{2\pi iq}$ met $q \in \mathbb{Q}$. Voor elke $n \in \mathbb{Z}_{>0}$ heeft $\mathbb{C}^*$ precies één ondergroep van orde n, nl. $\left\{e^{2\pi i\alpha/n} \;\middle|\; \alpha = 0, 1, \ldots, n-1\right\}$. Van deze groep kunnen we, in overeenstemming met 3.14, direct inzien dat hij cyclisch is: $e^{2\pi i/n}$ is een voortbrenger. In Hoofdstuk 14 zullen we uitvoeriger ingaan op eenheidswortels.

Gevolg 3.16. *Zij p een priemgetal. Dan is $\mathbb{F}_p^*$ cyclisch van orde $p - 1$.*

Bewijs. Dit is een direct gevolg van 3.14 aangezien $\mathbb{F}_p$ een domein is (zelfs een lichaam). □

Bijvoorbeeld, $\mathbb{F}_7^* = \langle\bar{3}\rangle$, want de machten van 3 modulo 7 zijn

$$\bar{3}^1 = \bar{3}\,, \quad \bar{3}^2 = \bar{2}\,, \quad \bar{3}^3 = \bar{6}\,, \quad \bar{3}^4 = \bar{4}\,, \quad \bar{3}^5 = \bar{5}\,, \quad \bar{3}^6 = \bar{1}\,.$$

3.17 Laat in het vervolg van dit hoofdstuk R een commutatieve ring zijn. Zij $f \in R[X]$, en beschouw het polynoom in twee variabelen

$$f(X+Y) - f(X) \in R[X, Y]\,.$$

Vullen we in dit polynoom 0 voor Y in, dan is de uitkomst 0. Wegens 2.13 (toegepast op $\alpha = 0$, en met als grondring $R[X]$) heeft $f(X+Y) - f(X)$ een factor Y:

$$f(X+Y) - f(X) = Y \cdot H\,, \qquad H \in R[X, Y]\,.$$

De *afgeleide* f' van f is nu gedefinieerd door

$$f' = H(X, 0)$$

wat we ook kunnen schrijven als

$$\Big(\frac{f(X+Y) - f(X)}{Y}\Big)|_{Y=0}$$

(èèrst door Y delen, dan $Y = 0$ substitueren!). Andere notaties voor de afgeleide zijn $\frac{df}{dX}$ of $\frac{d}{dX}f$ of, als f ook als polynoom in een andere variabele kan worden opgevat: $\frac{\partial f}{\partial X}$. Merk op dat in de definitie niet over limieten wordt gesproken.

Uit de volgende stelling blijkt dat het nemen van de afgeleide geschiedt volgens de uit het college analyse bekende formule.

Stelling 3.18. *Zij R een commutatieve ring.*

(a) *Voor alle $f, g \in R[X]$ geldt*

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'.$$

(b) *Als $f = \sum_{k=0}^{n} a_k X^k \in R[X]$, dan*

$$f' = \sum_{k=1}^{n} k a_k \, X^{k-1}.$$

(Hier is $ka_k = a_k + a_k + \cdots + a_k$ (k termen).)

Bewijs. (a) Als $f(X+Y) - f(X) = Y \cdot H_1$ en $g(X+Y) - g(X) = Y \cdot H_2$, met $H_1, H_2 \in R[X, Y]$, dan geldt

$$\big(f(X+Y) + g(X+Y)\big) - \big(f(X) + g(X)\big) = Y \cdot (H_1 + H_2)$$

en

$$f(X+Y) \cdot g(X+Y) - f(X) \cdot g(X) = Y \cdot \big(f(X) \cdot H_2 + g(X) \cdot H_1 + Y \cdot H_1 \cdot H_2\big).$$

Deel door Y en substitueer $Y = 0$; dan vinden we

$$\begin{aligned}(f+g)' &= H_1(X,0) + H_2(X,0) = f' + g', \\ (fg)' &= f \cdot H_2(X,0) + g \cdot H_1(X,0) + 0 = fg' + gf'.\end{aligned}$$

(b) We bewijzen eerst met inductie naar k dat

$$(a \cdot X^k)' = ka \, X^{k-1} \qquad \text{voor } a \in R \text{ en } k \in \mathbb{Z}_{>0}.$$

Voor $k = 1$ rekent men dit direct na. Voor $k \geq 2$ schrijven we $a \cdot X^k = (a \cdot X^{k-1}) \cdot X$, en met (a) en de inductiehypothese vinden we

$$(a \cdot X^k)' = (a \cdot X^{k-1})' \cdot X + (a \cdot X^{k-1}) \cdot X' = (k-1)aX^{k-2} \cdot X + aX^{k-1} \cdot 1 = kaX^{k-1},$$

zoals verlangd.

Verder geldt $(aX^0)' = 0$, en met (a) vinden we nu

$$\big(\sum_{k=0}^{n} a_k X^k\big)' = \sum_{k=0}^{n} (a_k X^k)' = \sum_{k=1}^{n} k a_k \, X^{k-1} \,,$$

zoals verlangd. Dit bewijst stelling 3.18. □

Met de formule uit 3.18(b) hadden we f' natuurlijk ook kunnen definiëren. Dan moet (a) wel anders bewezen worden.

3.19 De belangrijkste toepassing van de afgeleide is voor ons gelegen in het ontdekken van *dubbele nulpunten*. Als $\alpha \in R$ een nulpunt van $f \in R[X]$ is, dan kunnen we volgens 3.5 of 3.6 schrijven: $f = (X - \alpha) \cdot q$, met $q \in R[X]$. Als we zelfs kunnen schrijven $f = (X - \alpha)^2 \cdot q_1$, met $q_1 \in R[X]$, dan noemen we α een *dubbel* of *meervoudig* nulpunt van f.

Stelling 3.20. *Zij R een commutatieve ring, en $f \in R[X]$. Stel dat $\alpha \in R$ een nulpunt van f is. Dan geldt:*

$$\alpha \text{ is een dubbel nulpunt van } f \quad \Longleftrightarrow \quad \alpha \text{ is een nulpunt van } f'.$$

Bewijs. Schrijf $f = (X - \alpha) \cdot q$, met $q \in R[X]$. Kennelijk geldt:

$$\begin{aligned} \alpha \text{ is een dubbel nulpunt van } f \quad &\Leftrightarrow \quad \text{er is een } q_1 \in R[X] \text{ met } q = (X - \alpha) q_1 \\ &\Leftrightarrow \quad q(\alpha) = 0 \,. \end{aligned}$$

Uit $f = (X - \alpha) \cdot q$ en 3.18(a) volgt

$$f' = (X - \alpha)' \cdot q + (X - \alpha) \cdot q' = q + (X - \alpha) q'.$$

Vul α voor X in, dan vinden we

$$f'(\alpha) = q(\alpha) \,.$$

We zien dus: $q(\alpha) = 0 \Leftrightarrow f'(\alpha) = 0$. Hiermee is Stelling 3.20 bewezen. □

Opgaven

1. Laat aan de hand van een voorbeeld zien dat de voorwaarde dat de kopcoëfficiënt van g een eenheid van R is in 3.1 niet gemist kan worden.

2. Zij K een lichaam, $f \in K[X]$ een polynoom, en $\alpha_0, \alpha_1, \ldots \alpha_n$ een $n+1$-tal verschillende elementen van K, met $n \geq \mathrm{gr}(f)$. Bewijs:

$$f = \sum_{i=0}^{n} f(\alpha_i) \frac{\prod_{j=0, j\neq i}^{n} (X - \alpha_j)}{\prod_{j=0, j\neq i}^{n} (\alpha_i - \alpha_j)},$$

   de interpolatieformule van Lagrange.

3. Bewijs dat $X^2 - \bar{1} \in (\mathbb{Z}/8\mathbb{Z})\big[X\big]$ de nulpunten $\bar{1}$, $\bar{3}$, $\bar{5}$ en $\bar{7}$ heeft.

4. Zij $x = a + bi + cj + dk \in \mathbb{H}$, met a, b, c, $d \in \mathbb{R}$. Bewijs:

$$x \text{ is een nulpunt van } X^2 + 1 \quad \Leftrightarrow \quad x\bar{x} = 1 \text{ en } \bar{x} = -x \quad \Leftrightarrow \quad a = 0 \text{ en } b^2 + c^2 + d^2 = 1\,.$$

   Concludeer dat $X^2 + 1$ oneindig veel nulpunten in $\mathbb{H}$ heeft.

5. (Omkering van de Stelling van Wilson.) Laat $n \in \mathbb{Z}_{>1}$.

   (a) Stel dat n *geen* priemgetal is. Bewijs: $\mathrm{ggd}\big((n-1)!, n\big) > 1$.

   (b) Bewijs: $(n-1)! \equiv -1 \bmod n \implies n$ is een priemgetal.

   (c) Stel dat $(n-1)! \not\equiv -1 \bmod n$ en $\not\equiv 0 \bmod n$. Bewijs: $n = 4$.

6. Zij R een commutatieve ring. Laat $f, g \in R[X]$ en $k \in \mathbb{Z}_{>0}$.

   (a) Toon aan dat $f \in R[X] \cdot g^k \implies f' \in R[X] \cdot g^{k-1}$.

   (b) Laat aan een voorbeeld zien dat omgekeerd als $f' \in R[X] \cdot g^{k-1}$, dan hoeft niet te gelden $f \in R[X] \cdot g^k$.

7. Laat $R = \mathbb{F}_2$ en $f \in R[X]$.

   (a) Bewijs: $f' = 0 \Leftrightarrow f$ kan geschreven worden als $f = \sum_{k=0}^{n} a_k X^{2k}$ met $a_k \in \mathbb{F}_2$

$$\Leftrightarrow \exists g \in \mathbb{F}_2[X] : \; f = g^2.$$

   (b) Bewijs: $(f')' = 0$.

8. Zij R een commutatieve ring. Voor $f \in R[X]$ en $k \in \mathbb{Z}_{\geq 0}$ definiëren we $f^{(k)}$ inductief door $f^{(0)} = f$ en $f^{(k)} = (f^{(k-1)})'$. Bewijs dat voor alle $f, g \in R[X]$ en $n \in \mathbb{Z}_{\geq 0}$ geldt:

$$(f \cdot g)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$$

   (*formule van Leibniz*).

9. Zij R een eindige ring. Bewijs: $\exists n, m \in \mathbb{Z} :\ n > m > 0$, zodat $x^n = x^m$ voor alle $x \in R$.

10. Laat R een domein zijn, en $f, g \in R[X]$ polynomen met $\max\{\mathrm{gr}(f), \mathrm{gr}(g)\} < \#R$ (dat geldt bijvoorbeeld als R oneindig is). Bewijs: $(\forall x \in R : f(x) = g(x)) \Leftrightarrow f = g$.

11. Zij p een priemgetal, en $f, g \in \mathbb{F}_p[X]$. Bewijs:

$$(\forall x \in \mathbb{F}_p : f(x) = g(x)) \Leftrightarrow f - g \in \mathbb{F}_p[X] \cdot (X^p - X).$$

12. We definiëren een evaluatiehomomorfisme:

$$\Phi\colon \mathbb{R}[X,Y] \longrightarrow \mathbb{R}[T], \qquad f(X,Y) \mapsto f(T^2, T^3).$$

Bewijs dat $\mathrm{Ker}(\Phi) = (X^3 - Y^2)$ en dat $\Phi(\mathbb{R}[X,Y]) = \left\{\sum a_i T^i \;\middle|\; a_1 = 0\right\}$.

13. (a) Zij $z = a + bi \in \mathbb{C}$ en $z \notin \mathbb{R}$. Bewijs dat het evaluatiehomomorfisme

$$\Phi_z\colon \mathbb{R}[X] \longrightarrow \mathbb{C}, \qquad f \mapsto f(z),$$

(waarbij we de inclusie $\mathbb{R} \subset \mathbb{C}$ gebruiken), surjectief is.

(b) Zij $z = a + bi \in \mathbb{C}$ en $z \notin \mathbb{R}$. Zij $g = X^2 - 2aX + a^2 + b^2$. Bewijs dat:

$$\mathrm{Ker}(\Phi_z) = (g), \qquad \text{en dat} \qquad \mathbb{R}[X]/(g) \cong \mathbb{C}.$$

(c) Zij $f = aX^2 + bX + c \in \mathbb{R}[X]$. Bewijs dat:

$$\begin{array}{rcll} \mathbb{R}[X]/(f) & \cong & \mathbb{C} & \text{als} \quad b^2 - 4ac < 0, \\ & \cong & \mathbb{R}[\epsilon] & \text{als} \quad b^2 - 4ac = 0, \\ & \cong & \mathbb{R} \times \mathbb{R} & \text{als} \quad b^2 - 4ac > 0, \end{array}$$

hierin is $\mathbb{R}[\epsilon]$ de ring van duale getallen (zie Opgave 32 op blz. 36). Probeer ook expliciete isomorfismen aan te geven.

14. Laat $z, w \in \mathbb{C} - \mathbb{R}$ en zij

$$\Phi_{z,w}\colon \mathbb{R}[X,Y] \longrightarrow \mathbb{C}, \qquad f \mapsto f(z,w),$$

het evaluatiehomomorfisme. Laat zien dat $\mathrm{Ker}(\Phi_{z,w})$ wordt voortgebracht door één lineair polynoom en één polynoom van graad 2. Bepaal zulke polynomen expliciet als $z = 1+i,\ \ w = 3-2i$.

15. Zij K een lichaam en zij $R = K[X]/(X^n)$ voor $n \in \mathbb{N}_{\geq 1}$. We schrijven $x = (X \bmod X^n) \in R$, ieder element r van R is dan van de vorm:

$$r = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \qquad a_i \in K.$$

(a) Laat zien dat $r \in R$ een eenheid is precies dan als $a_0 \neq 0$. Bepaal ook de inverse van een eenheid.

(b) Laat zien dat elke nuldeler in R nilpotent is. Wat is de kleinste k met $r^k = 0$ voor elke nuldeler r in R ?

(c) Geef voor elke $a \in K$ een ringisomorfisme:

$$K[X]/\left((X-a)^n\right) \to K[X]/(X^n).$$

(d) Geef voor $n > 1$ een $f \in K[X]$ zodat f mod X^n een eenheid is in R, maar zodat $f + (X-1)^n \in K[X]/((X-1)^n)$ een nilpotent is.

Hoofdstuk 4

Priemidealen en maximale idealen

In dit hoofdstuk is R steeds een *commutatieve* ring.

Een belangrijke eigenschap van priemgetallen p is, dat

$$p \mid ab \implies p \mid a \text{ of } p \mid b$$

voor $a, b \in \mathbb{Z}$. Anders geformuleerd:

$$ab \in p\mathbb{Z} \implies a \in p\mathbb{Z} \text{ of } b \in p\mathbb{Z}.$$

In het algemeen worden idealen die deze eigenschap hebben *priemidealen* genoemd:

Definitie 4.1. Laat R een commutatieve ring zijn. Een *priemideaal* van R is een ideaal $I \subset R$ dat voldoet aan:

(P1) $I \neq R$;

(P2) Voor alle $a, b \in R$ met $ab \in I$ geldt: $a \in I$ of $b \in I$.

Voorbeeld 4.2. Boven hebben we gezien dat $p\mathbb{Z}$ een priemideaal van $\mathbb{Z}$ is voor elk priemgetal p. Voor getallen $n \in \mathbb{Z}_{>0}$ die niet priem zijn is $n\mathbb{Z}$ *geen* priemideaal van $\mathbb{Z}$: immers, voor $n = 1$ is niet aan (P1) voldaan, en als $n > 1$ dan kunnen we schrijven $n = ab$ met $1 < a, b < n$; dan $ab = n \in n\mathbb{Z}$ maar $a \notin n\mathbb{Z}, b \notin n\mathbb{Z}$, dus $n\mathbb{Z}$ voldoet niet aan (P2).

Het ideaal $\{0\} \subset \mathbb{Z}$ is wel een priemideaal.

Stelling 4.3. *Zij R een commutatieve ring. Het ideaal $\{0\} \subset R$ is een priemideaal dan en slechts dan als R een domein is.*

Bewijs. Als R een domein is, dan is $1 \neq 0$ dus $\{0\} \neq R$ en bovendien geldt $ab = 0 \implies a = 0$ of $b = 0$ zodat ook aan (P2) voldaan is. Omgekeerd, als $\{0\}$ een priemideaal is, dan geeft (P2) dat er geen nuldelers zijn. □

Voorbeeld 4.4. Het ideaal $\mathbb{R}[X] \cdot (X^2 - 1) \subset \mathbb{R}[X]$ is geen priemideaal, want het bevat wél het element $(X + 1)(X - 1)$ maar niet $(X + 1)$ of $(X - 1)$.

Het ideaal $\mathbb{R}[X] \cdot (X^2+1) \subset \mathbb{R}[X]$ is echter wel een priemideaal. Om dit te bewijzen maken we gebruik van het in Opgave 2.37 bewezen feit dat

$$f \in \mathbb{R}[X] \cdot (X^2+1) \iff \text{het complexe getal } f(i) \text{ is } 0,$$

voor $f \in \mathbb{R}[X]$. Voor $f, g \in \mathbb{R}[X]$ geldt nu:

$$\begin{aligned} fg \in \mathbb{R}[X] \cdot (X^2+1) &\implies (fg)(i) = f(i)g(i) = 0 \\ &\implies f(i) = 0 \text{ of } g(i) = 0 \\ &\implies f \in \mathbb{R}[X] \cdot (X^2+1) \text{ of } g \in \mathbb{R}[X] \cdot (X^2+1). \end{aligned}$$

Hiermee is (P2) gecontroleerd; we laten (P1) aan de lezer over.

De volgende stelling, die een generalisatie is van 4.3, zegt dat men kan zien of een ideaal I priem is door naar de restklassenring R/I te kijken.

Stelling 4.5. *Zij R een commutatieve ring, en $I \subset R$ een ideaal. Dan geldt:*

$$I \text{ is een priemideaal van } R \iff R/I \text{ is een domein.}$$

Bewijs. Voor $a \in R$ schrijven we $\bar{a} = (a+I) \in R/I$. De ring R/I is volgens de definitie in 1.21 een domein dan en slechts dan als $\bar{1} \neq \bar{0}$ en R/I geen nuldelers heeft. Nu geldt:

$$\bar{1} \neq \bar{0} \iff 1 \notin I \iff I \neq R \iff \text{(P1) geldt,}$$

en

$$\begin{aligned} R/I \text{ heeft geen nuldelers} &\iff (\forall \bar{a}, \bar{b} \in R/I : \bar{a}\bar{b} = \bar{0} \implies \bar{a} = \bar{0} \text{ of } \bar{b} = \bar{0}) \\ &\iff (\forall a, b \in R : ab \in I \implies a \in I \text{ of } b \in I) \\ &\iff \text{(P2) geldt.} \end{aligned}$$

Hier hebben we steeds gebruikt dat $\bar{c} = \bar{0}$ hetzelfde wil zeggen als $c \in I$. Al met al vinden we: R/I is een domein $\iff$ $(P1)$ en $(P2)$ gelden $\iff$ I is een priemideaal van R. Dit bewijst 4.5. □

Voorbeeld 4.6. We kijken opnieuw naar het tweede voorbeeld in 4.4. Er geldt $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$, en dit is een domein. Met stelling 4.5 zien we nu direct dat (X^2+1) een priemideaal is van $\mathbb{R}[X]$.

Een snelle manier om te zien of een ideaal $I \subset R$ priem is bestaat vaak uit het berekenen van de ring R/I en dan 4.5 toepassen. Voor speciale ringen bestaan er ook andere manieren: zie bijvoorbeeld Stelling 5.8 verderop.

Voorbeelden 4.7. (a) Laat $I = (X+Y, X^2+X+Y+1) \subset R = \mathbb{R}[X,Y]$. In Hoofdstuk 2 zagen we dat $R/I \cong \mathbb{C}$, dus I is een priemideaal van R.

(b) Laat $I = (5, X^2+Y+1) \subset R = \mathbb{Z}[X,Y]$. Met behulp van 2.28–2.31 berekent men $R/J \cong \mathbb{F}_5[X]$; dit is een domein, dus I een priemideaal van R.

(c) Laat $I = (YZ - X^2, X^2 - Z) \subset \mathbb{C}[X,Y,Z] = R$. Dan $R/I \cong \mathbb{C}[X,Y]/(YX^2 - X^2)$. Uit

$$X^2 \cdot (Y-1) \in (YX^2 - X^2),$$

terwijl

$$X^2 \notin (YX^2 - X^2), \quad Y - 1 \notin (YX^2 - X^2),$$

blijkt dat $(YX^2 - X^2)$ geen priemideaal van $\mathbb{C}[X,Y]$ is. Dus R/I is geen domein, en I is geen priemideaal van R.

Definitie 4.8. Zij R een commutatieve ring. Een ideaal M van R heet *maximaal* als geldt

(M1) $M \neq R$;

(M2) voor elk ideaal J van R met $M \subset J \subset R$ geldt $J = M$ of $J = R$.

Dus een maximaal ideaal is "niet meer groter te maken" zonder meteen de hele ring te krijgen.

Voorbeelden van idealen die niet maximaal zijn: $9\mathbb{Z} \subset \mathbb{Z}$, want het ideaal $3\mathbb{Z}$ ligt "er tussenin"; en $(2) \subset \mathbb{Z}[X]$, want $(2, X)$ ligt er tussenin.

Voorbeelden van idealen die wél maximaal zijn kunnen het gemakkelijkst gegeven worden als we eenmaal het analogon van 4.5 voor maximale idealen bewezen hebben. We beginnen met het analogon van 4.3.

Stelling 4.9. *Zij R een commutatieve ring. Het ideaal $\{0\} \subset R$ is maximaal dan en slechts dan als R een lichaam is.*

Bewijs. In een lichaam geldt $1 \neq 0$, dus $\{0\} \neq R$, en $\{0\}$ voldoet aan (M1). Verder zijn er in een lichaam geen idealen behalve $\{0\}$ en R, wegens 2.17, dus ook aan (M2) is voldaan. Dit bewijst dat in een lichaam het nulideaal maximaal is.

Omgekeerd, stel dat (0) een maximaal ideaal is. We bewijzen dat elke $a \in R, a \neq 0$, een inverse heeft. Hiertoe passen we (M2) op het ideaal $J = Ra$ toe. Dit ideaal is niet gelijk aan $\{0\}$, dus volgens (M2) (met $M = \{0\}$) moet gelden $Ra = R$. Dan geldt $1 \in Ra$, dus $1 = ba$ voor een $b \in R$, en a heeft een inverse. Hiermee is 4.9 bewezen. □

Stelling 4.10. *Zij R een commutatieve ring, en $M \subset R$ een ideaal. Dan geldt:*

$$M \text{ is een maximaal ideaal van } R \iff R/M \text{ is een lichaam.}$$

Bewijs. Het idee van het bewijs bestaat er uit de bewering terug te voeren tot het speciale geval 4.9, door gebruik te maken van 2.24.

Schrijf $\bar{R} = R/M$. Volgens 2.24 corresponderen de idealen J in R met $M \subset J \subset R$ éénduidig met de idealen $\bar{J} = J/M$ van $\bar{R}$. Dus een R-ideaal J dat "echt" tussen M en R in ligt geeft aanleiding tot een $\bar{R}$-ideaal dat "echt" tussen $\{\bar{0}\}$ en $\bar{R}$ in ligt, en omgekeerd. Hieruit zien we: M is een maximaal ideaal van $R \iff \{\bar{0}\}$ is een maximaal ideaal van $\bar{R} = R/M$.

Volgens 4.9 is dit weer hetzelfde als: $\bar{R} = R/M$ is een lichaam. Hiermee is 4.10 bewezen. □

Men gebruikt Stelling 4.10 op dezelfde manier om te zien of een ideaal maximaal is als men Stelling 4.5 gebruikt om te zien of een ideaal priem is.

Voorbeelden 4.11. Laat $n \in \mathbb{Z}_{>0}$ Dan is $\mathbb{Z}/n\mathbb{Z}$ een lichaam, precies dan als n priem is (zie 1.20), dus

$$p\mathbb{Z} \subset \mathbb{Z} \quad \text{is maximaal, voor } p \text{ priem}$$

en de idealen (n) met n niet priem zijn niet maximaal. Inderdaad geldt als $n = ab$ met $1 < a, b < n$ dat $(n) \subset (a)$ en $(a) \neq \mathbb{Z}$ want $a \neq \pm 1$.

Zoals we eerder zagen geldt:

$$\mathbb{Z}[X, Y]/(5, X^2 + Y + 1) \cong \mathbb{F}_5[X]$$

dit is een domein, maar geen lichaam ($X^{-1} \notin \mathbb{F}_5[X]$), dus het priemideaal $(5, X^2 + Y + 1) \subset \mathbb{Z}[X, Y]$ is niet maximaal.

Voor elke $(a, b) \in \mathbb{R} \times \mathbb{R}$ geldt dat $(X - a, Y - b)$ een maximaal ideaal in $\mathbb{R}[X, Y]$ is omdat (zie 2.30)

$$\mathbb{R}[X, Y]/(X - a, Y - b) \cong \mathbb{R}[X]/(X - a) \cong \mathbb{R},$$

en $\mathbb{R}$ is een lichaam.

Gevolg 4.12. *Elk maximaal ideaal is priem.*

Bewijs. Dit volgt direct uit 4.5, 4.10 en de opmerking dat elk lichaam een domein is. □

Opmerking 4.13. Zoals uit het bovengegeven voorbeeld $(5, X^2 + Y + 1) \subset \mathbb{Z}[X, Y]$ blijkt, is de omkering van 4.12 fout. Een nog simpeler voorbeeld is $\{0\} \subset \mathbb{Z}$: de ring $\mathbb{Z}$ is wel een domein maar geen lichaam, dus $\{0\} \subset \mathbb{Z}$ is wel priem maar niet maximaal.

Stelling 4.14. *Elke commutatieve ring R met $1 \neq 0$ bezit een maximaal ideaal.*

Het idee van het bewijs is erg eenvoudig: begin met het nul-ideaal $\{0\}$, en maak dit net zo lang groter tot dit niet meer kan zonder de hele ring te krijgen. We doen het eerst voor een geval waar het bewijs met gewone middelen voltooid kan worden. Voor het algemene geval hebben we namelijk een hulpmiddel uit de verzamelingenleer nodig: het lemma van Zorn (genoemd naar Max Zorn, 1906–1993).

4.15 Speciaal geval. Elke commutatieve ring R met aftelbaar veel elementen en met $1 \neq 0$ bezit een maximaal ideaal.

Bewijs van het speciale geval. De ring is aftelbaar en we zetten de elementen van de ring dus op een rij: $r_1, r_2, \ldots$. Definieer inductief de rij idealen $I_0 \subseteq I_1 \subseteq \ldots$ door te beginnen met $I_0 = (0)$ en inductief verder te gaan met:

$$I_n = \begin{cases} I_{n-1} + (r_n) & \text{als } I_{n-1} + (r_n) \neq R \\ I_{n-1} & \text{anders} \end{cases}$$

Laat nu

$$M = \bigcup_{n \in \mathbb{N}} I_n.$$

We beweren dat M het gezochte maximale ideaal is. Daartoe moeten we eerst nagaan dat M een ideaal is. Welnu, als $a, b \in M$ dan zijn er $n, m \in \mathbb{N}$ met $a \in I_n$ en $b \in I_m$. Als $n \leq m$ dan is $I_n \subseteq I_m$, dus $a, b \in I_m$, een ideaal. I.h.b. geldt $a - b \in I_m \subseteq M$. Het geval $n > m$ gaat analoog. Verder geldt als $r \in R$ en $a \in M$ dat $ra \in M$ omdat immers $a \in I_n$, een ideaal, dus ook $ra \in I_n \subset M$.

Als M geen maximaal ideaal is dan kan dat aan twee dingen liggen. Het eenheidselement zou in M kunnen liggen of er zou een nog groter echt ideaal N kunnen zijn. In het eerste geval zou het eenheidselement al in een van de I_n moeten liggen, en deze I_n is dan gelijk aan R, in tegenspraak met de definitie van de idealen I_n. In het andere geval zou er een r_n zijn die er nog wel bij had gemogen, maar die we er toch niet bij hebben gedaan. Merk echter op dat als $M + (r_n) \neq R$ dat dan zeker $I_{n-1} + (r_n) \neq R$, immers $I_{n-1} \subset M$. De definitie van I_n laat zien dat dan $r_n \in I_n \subset M$. Zulke r_n zijn er dus niet. Hiermee is 4.15 bewezen. □

4.16 Hoe moet het nu als R niet aftelbaar is? Om toch alle elementen van R aan de beurt te laten komen, heb je meer dan aftelbaar veel beurten nodig. Dus n zou "voorbij oneindig door moeten tellen". Dat kan, en leidt dan tot een bewijs "met transfiniete inductie". Maar wij geven er de voorkeur aan om een principe uit de verzamelingenleer aan te roepen waarmee als het ware het inductieproces in een klap voltooid wordt. Dit is het zogenaamde lemma van Zorn. (Om historische redenen heet het geen "stelling van Zorn", wat wel logischer zou zijn.) Men kan bewijzen dat het lemma van Zorn equivalent is met het "Keuze-axioma", en voor het gemak nemen we het lemma van Zorn dus ook maar als axioma aan. (Het "Keuze-axioma" is de uitspraak dat elke surjectieve afbeelding ten minste één rechtsinverse heeft.)

Lemma 4.17 (Lemma van Zorn)**.** *Zij P een* partieel geordende verzameling. *Dan bezit P tenminste één* maximale keten.

4.18 Verklaringen van de terminologie: een *partieel geordende verzameling* is een verzameling P die voorzien is van een binaire relatie $\leq$ met de volgende twee eigenschappen:

$$\begin{aligned} \forall x, y, z \in P: \quad & (x \leq y \wedge y \leq z) \implies x \leq z, \\ \forall x, y \in P: \quad & (x \leq y \wedge y \leq x) \iff x = y; \end{aligned}$$

een *keten* in een partieel geordende verzameling P is een deelverzameling $K \subset P$ met de eigenschap

$$\forall x, y \in K: \quad x \leq y \vee y \leq x.$$

Merk op dat de *lege* deelverzameling $\emptyset \subset P$ een keten is. Een keten K heet *maximaal* als er geen deelverzameling van P is die K strikt bevat en ook weer een keten is. Dus een keten is maximaal als voor elke y in het complement van K in P een $x \in K$ bestaat waarvoor niet $x \leq y$ en ook niet $y \leq x$. In de praktijk is het lemma van Zorn alleen goed bruikbaar als P *niet leeg* is. Voor een bewijs van het lemma van Zorn, uitgaande van het keuze-axioma, verwijzen we naar de literatuur, bijvoorbeeld Van der Waerden, Algebra I, § 69.

Bewijs van stelling 4.14. Neem als partieel geordende verzameling P de verzameling van alle idealen in R verschillend van R:

$$P = \{I \mid I \text{ is een ideaal van } R, \text{ en } 1 \notin I\}.$$

met als partieële ordening de *inclusierelatie*. Dus $I \leq J$ in P als $I \subseteq J$.

Merk op dat in het bewijs van 4.15 de verzameling van idealen $\{I_n\}_{n\in\mathbb{N}}$ een (genummerde) keten in P definieert. Waarschijnlijk geen maximale keten overigens, (er past waarschijnlijk nog wel een ideaal tussen I_0 en I_1), maar wel een die zo ver mogelijk groeit.

Daarom proberen we in het algemene geval het zelfde idee: Volgens het lemma van Zorn mogen we een maximale keten K in P kiezen, zeg

$$K = \{I_n\}_{n\in X},$$

waarbij de indexverzameling X nu dus willekeurig groot mag zijn. Zo'n keten is een collectie idealen in P met de eigenschap dat $\forall I, J \in K\colon\ I \subset J \vee J \subset I$. Merk wel even op dat P in ieder geval niet leeg is, immers $\{0\} \subset R$ is een ideaal. Dus de maximale keten K is ook niet leeg. We bekijken nu $M = \bigcup_{n\in X} I_n$.

We beweren dat M het gezochte maximale ideaal is. Daartoe moeten we eerst nagaan dat het een ideaal is, en dat gaat als in het bewijs van 4.15. Als het geen maximaal ideaal is dan kan dat aan twee dingen liggen. Het eenheidselement zou in M kunnen liggen of er zou een nog groter echt ideaal N kunnen zijn. In het eerste geval zou het eenheidselement al in een van de I_n moeten liggen, en in het andere geval zou de keten niet maximaal zijn (zie ook 4.15). We concluderen dat M inderdaad een maximaal ideaal is. □

Gevolg 4.19. *Zij R een commutatieve ring, en $I \subset R$ een ideaal, $I \neq R$. Dan bezit R een maximaal ideaal M met $I \subset M$.*

Bewijs. Wegens 4.14 heeft de ring R/I een maximaal ideaal, en dit moet wegens 2.24 van de vorm M/I zijn, waar M een ideaal van R is met $M \supset I$. Voorts zegt 2.24 dat $R/M \cong (R/I)/(M/I)$ en dit is een lichaam; dus M is maximaal in R (stelling 4.10). Hiermee is 4.19 bewezen.

(Alternatief bewijs: pas het lemma van Zorn toe op de verzameling idealen $\neq R$ van R die I omvatten.) □

Gevolg 4.20. *Zij R een commutatieve ring. Dan geldt*

$$\bigcup_M M = R - R^*,$$

waar de vereniging genomen wordt over alle maximale idealen M van R.

Bewijs. $\subset$: Is M maximaal, dan $M \subset R - R^*$ wegens 2.16 en 4.8(M1). Dus $\cup_M M \subset R - R^*$.

$\supset$: Als $a \in R - R^*$ dan $Ra \neq R$, en Ra is een ideaal van R. Wegens 4.19 is er dus een maximaal ideaal M van R met $Ra \subset M$. Dus $a \in \cup_M M$ voor alle $a \in R - R^*$.

Hiermee is 4.20 bewezen. □

Voorbeeld 4.21. Laat $R = C([0,1])$ de ring van continue functies $f\colon [0,1] \to \mathbb{R}$ zijn. Voor $x \in [0,1]$ zij

$$M_x = \big\{ f \in R \;\big|\; f(x) = 0 \big\}.$$

Dit is de kern van het surjectieve ringhomomorfisme

$$R \to \mathbb{R},\ f \mapsto f(x),$$

dus $R/M_x \cong \mathbb{R}$, en dus is $M_x \subset R$ maximaal. Uit Opgave 17 blijkt dat elk maximaal ideaal van R van deze vorm is. Er geldt

$$R - \bigcup_{x\in[0,1]} M_x = \big\{ f \in R \;\big|\; f(x) \neq 0 \text{ voor alle } x \in [0,1] \big\}.$$

Dit is juist de eenhedengroep R^* van R, in overeenstemming met 4.20.

Een typische toepassing van Stelling 4.14 is het volgende resultaat, dat iets zegt over de oplosbaarheid van een stelsel vergelijkingen over een lichaam.

Gevolg 4.22. *Laat K een lichaam zijn, $n, t \in \mathbb{Z}_{>0}$, en $f_1, f_2, \ldots, f_t \in K[X_1, X_2, \ldots, X_n]$. Dan zijn de volgende twee beweringen equivalent.*

(a) *Er bestaan* geen $g_1, g_2, \ldots, g_t \in K[X_1, X_2, \ldots, X_n]$ *met* $g_1 f_1 + g_2 f_2 + \cdots + g_t f_t = 1$.

(b) *Er bestaat een lichaam L, met $K \subset L$, en er zijn $x_1, x_2, \ldots, x_n \in L$ met*

$$f_1(x_1, x_2, \ldots, x_n) = f_2(x_1, x_2, \ldots, x_n) = \ldots = f_t(x_1, x_2, \ldots, x_n) = 0.$$

Bewijs. (b) $\Rightarrow$ (a). Laten $L, x_1, \ldots, x_n$ als in (b) zijn, en stel dat toch

$$g_1 f_1 + \ldots + g_t f_t = 1, \qquad \text{met} \quad g_1, \ldots, g_t \in K[X_1, \ldots, X_n].$$

Substitueer $x_1, x_2, \ldots, x_n$ voor $X_1, X_2, \ldots, X_n$ in deze relatie, dan vinden we $0 = 1$, een tegenspraak.

(a) $\Rightarrow$ (b). Laat $I \subset K[X_1, \ldots, X_n]$ het door $f_1, f_2, \ldots, f_t$ voortgebrachte ideaal van $K[X_1, \ldots, X_n]$ zijn. Dan wil (a) precies zeggen dat $1 \notin I$, dus $I \neq K[X_1, \ldots, X_n]$. Volgens 4.14 is er nu een maximaal ideaal M van $K[X_1, \ldots, X_n]$ met $I \subset M$. Neem $L = K[X_1, \ldots, X_n]/M$. Dit is volgens 4.10 een lichaam. Stellen we de ringhomomorfismen

$$K \hookrightarrow K[X_1, \ldots, X_n] \to L = K[X_1, \ldots, X_n]/M,$$

samen, dan vinden we een ringhomomorfisme $K \to L$, dat volgens 2.18 injectief is.

We kunnen K dus als deellichaam van L opvatten. Voor de x_i nemen we tenslotte $x_i = X_i + M \in L$, voor $1 \leq i \leq n$. Dan geldt

$$f_j(x_1, \ldots, x_n) = f_j(X_1, \ldots, X_n) + M = 0 + M$$

aangezien $f_j(X_1, \ldots, X_n) = f_j \in I \subset M$, voor $1 \leq j \leq t$, zoals verlangd. Hiermee is 4.22 bewezen. $\square$

Voorbeeld 4.23. Neem

$$K = \mathbb{R}, \qquad n = t = 1, \qquad f_1 = X^2 + 1 \in \mathbb{R}[X].$$

Door naar de graad te kijken zien we dat er geen $g_1 \in \mathbb{R}[X]$ is met $g_1 f_1 = 1$, dus aan voorwaarde a. is voldaan. Volgens de stelling is er nu een "uitbreidingslichaam" L van $\mathbb{R}$ met een element $x \in L$ dat voldoet aan $x^2 + 1 = 0$. Inderdaad kunnen we hiervoor nemen $L = \mathbb{C}$ en $x = i$. Aan dit voorbeeld zien we ook dat het niet steeds mogelijk is $L = K$ te nemen.

Opmerking 4.24. Men kan bewijzen dat elk maximaal ideaal van $\mathbb{C}[X_1, \ldots, X_n]$ van de vorm:

$$M = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \qquad (a_i \in \mathbb{C})$$

is. De maximale idealen corresponderen dus met de punten van $\mathbb{C}^n$ (het ideaal M correspondeert uiteraard met het punt $(a_1, a_2, \ldots, a_n) \in \mathbb{C}^n$).

Stelling 4.22 impliceert dan: Als een stel polynomen $f_1, \ldots f_k \in \mathbb{C}[X_1, \ldots, X_n]$ geen gemeenschappelijk nulpunt in $\mathbb{C}^n$ heeft, dan bestaat er een relatie $g_1 f_1 + g_2 f_2 + \cdots + g_t f_t = 1$ tussen de f_i.

Opgaven

1. Laat R een domein zijn. Bewijs: het door X en Y voortgebrachte ideaal van $R[X,Y]$ is gelijk aan
$$\big\{f \in R[X,Y] \;\big|\; f(0,0) = 0\big\}$$
en dit is een priemideaal van $R[X,Y]$. Bereken het quotiënt $R[X,Y]/(X,Y)$.

2. Laat K een lichaam zijn, $n \in \mathbb{Z}_{>0}$, en $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Bewijs: het door $X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_n - \alpha_n$ voortgebrachte ideaal van $K[X_1, X_2, \ldots, X_n]$ is maximaal.

3. Bewijs: $5\mathbb{Z}[i] \subset \mathbb{Z}[i]$ is geen priemideaal.

4. Zij K een lichaam. Bewijs dat het door Y en Z voortgebrachte ideaal van $K[X,Y,Z]$ wel priem maar niet maximaal is.

5. Ga voor elk van de volgende idealen van $\mathbb{Z}[X]$ na, of het een priemideaal is, en of het een maximaal ideaal is:
$$(X,3); \quad (X^2-3); \quad (5, X^2+3).$$

6. Zij $M = (X-a, Y-b) \subset \mathbb{R}[X,Y]$. Laat zien $f \in M \iff f(a,b) = 0$ en bewijs dat M maximaal is.

7. Ga voor elk van de volgende idealen van $\mathbb{Q}[X,Y]$ na, of het een priemideaal is, en of het een maximaal ideaal is:
$$(X^2+1); \quad (X-Y, Y^2+1); \quad (X^2+1, Y^2+1); \quad (X^2+1, Y^2-2).$$

8. Zij R een commutatieve ring en $I \subset R$ een ideaal. Bewijs: I is een priemideaal van $R \iff$ er is een lichaam K en een ringhomomorfisme $f\colon R \to K$ met $I = \mathrm{Ker}(f)$.

9. Laat R een commutatieve ring zijn, $I \subset R$ een ideaal en $\phi\colon R \to R/I$ de natuurlijke afbeelding. Laat $J \subset R$ een priemideaal zijn met $I \subset J$. Bewijs dat $\phi(J)$ een priemideaal is van R/I, en dat omgekeerd elk priemideaal van R/I van deze vorm is. (Aanwijzing: combineer 4.5 en 2.24).

10. Als Opgave 9, met overal "priemideaal" vervangen door "maximaal ideaal".

11. Zij $f\colon R_1 \to R_2$ een homomorfisme van commutatieve ringen, $I_2 \subset R_2$ een ideaal, en $I_1 = f^{-1}(I_2) \subset R_1$.
    (a) Bewijs: I_1 is een ideaal in R_1, en R_1/I_1 is isomorf met een deelring van R_2/I_2.
    (b) Bewijs: als I_2 priem is in R_2 dan is I_1 priem in R_1.
    (c) Laat aan de hand van een voorbeeld zien dat (b) fout kan zijn als "priem" beide malen vervangen wordt door "maximaal".

12. Zij R een Boolese ring (zie Opgave 33 op blz. 19).

(a) Bewijs: R is een domein $\iff$ R is een lichaam $\iff$ $R \cong \mathbb{F}_2$.

(b) Zij $I \subset R$ een ideaal. Bewijs: I is een priemideaal $\iff$ I is een maximaal ideaal $\iff$ $R/I \cong \mathbb{F}_2$.

13. Zij R een commutatieve ring, en $I \subset R$ een ideaal, $I \neq R$. Gegeven is, dat voor elke $x \in R$ met $x \notin I$, geldt dat $x^2 - 1 \in I$.

(a) Bewijs: $R/I \cong \mathbb{F}_2$ of $R/I \cong \mathbb{F}_3$.

(b) Is I een priemideaal van R?

14. Zij R een commutatieve ring, en $I \subset R$ een ideaal van *eindige* index. Bewijs: I is een priemideaal $\iff$ I is een maximaal ideaal.

15. Zij R een commutatieve ring met $1 \neq 0$ waarvan *elk* ideaal $I \neq R$ een priemideaal is. Bewijs dat R een lichaam is.

16. Zij R een commutatieve ring, met de eigenschap dat $I \cap J \neq \{0\}$ voor elk tweetal idealen $I \neq \{0\}, J \neq \{0\}$ van R. Bewijs dat $\big\{a \in R \;\big|\; a \text{ is een nuldeler}\big\} \cup \{0\}$ een priemideaal van R is.

17. Laat $R = C([0,1])$, en zij $M_x \subset R$ voor $x \in [0,1]$ gedefinieerd als in voorbeeld 4.21.

(a) Zij $I \subset R$ een ideaal met $\forall x \in [0,1] : I \not\subset M_x$. Bewijs: voor alle $x \in [0,1]$ bestaat er een $f_x \in I$ met $f_x(x) \neq 0$.

Laat voor alle x zo'n f_x gekozen zijn. Bewijs dat er $x_1, x_2, \ldots, x_n \in [0,1]$ zijn zo dat voor alle $x \in [0,1]$ geldt $\sum_{i=1}^{n} f_{x_i}(x)^2 > 0$. (Aanwijzing: gebruik compactheid van $[0,1]$, d.w.z. als $[0,1] = \cup_{i \in I} U_i$ met U_i open, dan is er een *eindige* deelverzameling $J \subset I$ zodat $[0,1] = \cup_{j \in J} U_j$.) Concludeer: $I = R$.

(b) Zij $M \subset R$ een maximaal ideaal. Bewijs: er is een $x \in [0,1]$ zo dat $M = M_x$. Laat ook zien dat deze x eenduidig bepaald is door M.

18. Zij $R = \mathbb{R}[X,Y]/I$ met $I = (X^2 + Y^2 - 1)$. Laat $x = X + I$ en $y = Y + I \in R$.

(a) Bewijs dat $(x-a, y-b)$ met $a, b \in \mathbb{R}$ een maximaal ideaal van R is precies dan als $a^2 + b^2 = 1$.

(b) Voor welke $b \in \mathbb{R}$ is $(y - b)$ een maximaal ideaal in R ?

19. Zij R een commutatieve ring, en $a \in R$ een element met $a^n \neq 0$ voor alle $n \in \mathbb{Z}_{>0}$. Bewijs dat R een priemideaal I bezit met $a \notin I$. (Aanwijzing: pas het lemma van Zorn toe op de verzameling idealen die geen enkele macht van a bevatten.)

20. Het *radicaal* $\sqrt{0}$ van een commutatieve ring R is gedefinieerd door

$$\sqrt{0} = \big\{a \in R \;\big|\; \exists n \in \mathbb{Z}_{>0} : \; a^n = 0\big\}.$$

(Dus: alle nilpotente elementen.) Bewijs dat $\sqrt{0}$ een ideaal van R is. Bewijs dat $\sqrt{0} = \cap_I I$, waar I loopt over alle priemidealen van R. (Aanwijzing: gebruik Opgave 19.)

21. Het *Jacobson-radicaal* $J(R)$ van een commutatieve ring R is gedefinieerd door

$$J(R) = \{x \in R \mid \forall r \in R : \ 1 + rx \in R^*\}.$$

(a) Zij $x \in J(R)$, zij $M \subset R$ een maximaal ideaal en defineer een ideaal I van R door $I = M + xR$. Bewijs dat $I \neq R$ en concludeer dat $x \in M$.

(b) Zij M een maximaal ideaal van R en zij $x \in M$. Bewijs dat $1 + x \notin M$.

(c) Bewijs dat $J(R) = \cap_M M$, waar M loopt over alle maximale idealen van R.

(d) Bewijs dat $J(R)$ een ideaal van R is.

22. Zij R een commutatieve ring, en $S \subset R$ een niet-lege deelverzameling met de eigenschap $0 \notin S$ en $st \in S$ voor alle $s, t \in S$. Laat zien dat er een priemideaal I van R is met $I \cap S = \emptyset$. (Aanwijzing: gebruik de ring $S^{-1}R$ uit Opgave 28 op blz. 19, en pas 4.14 en Opgave 11(b) toe). Wat is de relatie met Opgave 19?

23. Zij R een commutatieve ring. We noemen R een *locale ring* als $R - R^*$ een ideaal van R is.

(a) Bewijs: R is een locale ring $\iff$ R heeft precies één maximaal ideaal.

(b) Zij R een locale ring, $x \in R$, en stel dat $x^2 = x$. Bewijs: $x = 0$ of $x = 1$.

24. Zij R een commutatieve ring en $I \subset R$ een priemideaal. Laat $S = R - I$.

(a) Bewijs: $\forall s, t \in S : st \in S$.

(b) Bewijs dat de ring $S^{-1}R$ uit Opgave 28 op blz. 19 een locale ring is (zie Opgave 23).

25. Zij $R = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, b \not\equiv 0 \bmod 5\}$. Bewijs dat R een locale ring is. Wat is het maximale ideaal M van R? Bewijs: $R/M \cong \mathbb{F}_5$.

26. Zij X een verzameling. Een *filter* op X is een collectie $\mathcal{F}$ van deelverzamelingen van X met de volgende eigenschappen:

$$\begin{aligned} &X \in \mathcal{F}, \quad \emptyset \notin \mathcal{F} \\ &A, B \in \mathcal{F} \implies A \cap B \in \mathcal{F} \\ &\text{als } A \subset B \subset X \text{ en } A \in \mathcal{F}, \text{ dan } B \in \mathcal{F}. \end{aligned}$$

Een *ultrafilter* is een filter $\mathcal{F}$ met de eigenschap:

$$\forall A, B \subset X : \quad (A \cup B \in \mathcal{F} \implies A \in \mathcal{F} \text{ of } B \in \mathcal{F}).$$

Laat R de ring $P(X)$ uit Opgave 34 op blz. 20 zijn.

(a) Zij $\mathcal{F}$ een collectie deelverzamelingen van X. Bewijs:

$$\mathcal{F} \text{ is een filter op } X \iff \{A \subset X \mid X - A \in \mathcal{F}\} \text{ is een ideaal} \neq R \text{ van } R,$$

en

$$\mathcal{F} \text{ is een ultrafilter op } X \iff \{A \subset X \mid X - A \in \mathcal{F}\} \text{ is een maximaal ideaal van } R.$$

(Aanwijzing: Opgave 12(b).)

(b) Een ultrafilter $\mathcal{F}$ op X heet *vrij* als $\forall x \in X : \{x\} \notin \mathcal{F}$. Bewijs: vrije ultrafilters op X bestaan dan en slechts dan als X oneindig is. (Aanwijzing: 4.19).

27. Zij X een verzameling, en K_x een lichaam voor elke $x \in X$. Laat $R = \prod_{x \in X} K_x$; dit is, met componentsgewijze bewerkingen, een commutatieve ring. Voor een ultrafilter $\mathcal{F}$ op X definiëren we $I_{\mathcal{F}} \subset R$ door

$$(\alpha_x)_{x \in X} \in I_{\mathcal{F}} \iff \big\{x \in X \;\big|\; \alpha_x = 0\big\} \in \mathcal{F}.$$

Bewijs dat $I_{\mathcal{F}}$ een maximaal ideaal van R is, en dat alle maximale idealen van R van deze vorm zijn.

Hoofdstuk 5

Deling in ringen

In de ring $\mathbb{Z}$ der gehele getallen geldt de stelling van de eenduidige priemfactorontbinding: elk positief geheel getal kan op eenduidige wijze in priemfactoren worden ontbonden. In dit hoofdstuk gaan we onderzoeken in hoeverre deze stelling zich voor algemenere ringen R laat generaliseren. We zullen ons hierbij voortdurend tot *domeinen* R beperken (zie 1.21).

Het ligt voor de hand eerst te onderzoeken welke elementen van R de rol van "priemgetallen" moeten gaan spelen. Als $p \in \mathbb{Z}$ een priemgetal is, dan geldt:

(a) als $p = ab$, met $a, b \in \mathbb{Z}$ dan is $a = \pm 1$ of $b = \pm 1$.

(b) $\mathbb{Z}p = \{np \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ is een priemideaal.

We gaan de eerste eigenschap generaliseren, maar we zullen zien dat de tweede eigenschap in sommige gevallen verloren gaat, zie bijvoorbeeld 5.5 en Opgave 1.

Definitie 5.1. Een element a van een domein R heet *irreducibel* als a geen eenheid is, en als voor alle $b, c \in R$ met $bc = a$ geldt, dat $b \in R^*$ of $c \in R^*$.

Met andere woorden: een element is irreducibel als het alleen maar "triviale" ontbindingen toelaat, zoals $5 = (-1)\cdot(-5)$. De irreducibele elementen van $\mathbb{Z}$ zijn de priemgetallen p en hun tegengestelden $-p$.

5.2 Als R een domein is, en $f, g \in R[X]$, dan geldt $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$. Omdat $\mathrm{gr}(1) = 0$ zijn de eenheden in $R[X]$ die polynomen van graad 0 die een inverse hebben. De eenheden van $R[X]$ zijn dus precies de eenheden van R:

$$(R[X])^* = R^*.$$

Een polynoom van graad 1 is in het algemeen *niet* irreducibel: $2X - 2 = 2 \cdot (X - 1)$ is reducibel in $\mathbb{Z}[X]$; dit polynoom is echter wel irreducibel in $\mathbb{Q}[X]$, want daar is 2 een eenheid.

Algemener, als $R = K$ een lichaam is, dan is ieder polynoom ($\neq 0$) van graad 0 een eenheid, en dus is ieder polynoom van graad 1 irreducibel. Voor polynomen van hogere graad is het in het algemeen moeilijker te bepalen of ze irreducibel zijn of niet; we zullen daar verderop in dit hoofdstuk op ingaan.

Stelling 5.3. *Zij K een lichaam en zij $f \in K[X]$ een polynoom met $\mathrm{gr}(f) = 2$ of $\mathrm{gr}(f) = 3$. Dan is f irreducibel in $K[X]$ precies dan als f geen nulpunt in K heeft.*

Bewijs. Als $\alpha \in K$ een nulpunt van f is, dan is $f = (X - \alpha)g$ (zie 3.6) en dus is f reducibel.

Stel nu dat f geen nulpunt in K heeft. Omdat $\mathrm{gr}(f) > 0$ is f geen eenheid. Stel $f = gh$, met $\mathrm{gr}(g) \leq \mathrm{gr}(h)$. Als $\mathrm{gr}(g) \neq 0$ dan moet gelden $\mathrm{gr}(g) = 1$ want $\mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$. Maar dan heeft g een nulpunt in K en f dus ook, in tegenspraak met de aanname. Daarom geldt $\mathrm{gr}(g) = 0$ en dus is g een eenheid in $K[X]$. We concluderen dat f irreducibel is. □

De volgende stelling geeft een verband tussen irreducibele elementen en priemidealen. Het er op volgende voorbeeld laat zien dat de omkering van de uitspraak van de stelling in het algemeen *niet* juist is. In de rest van dit hoofdstuk zullen we ringen onderzoeken waarvoor de omkering wel geldt.

Stelling 5.4. *Zij $a \in R$ met $a \neq 0$ en stel dat Ra een priemideaal is. Dan is a irreducibel.*

Bewijs. Er is gegeven dat $a \neq 0$, en dat Ra een priemideaal van R is. Uit (P1) van 4.1 blijkt dat $Ra \neq R$, dus a is geen eenheid (zie 2.16). Met (P2) volgt uit $bc = a \in Ra$ dat $b \in Ra$ of $c \in Ra$, laten we zeggen $b \in Ra$. Dan geldt $b = ra$ voor zekere $r \in R$. Uit $bc = a$ en $b = ra$ volgt dat $(rc - 1)a = 0$ en dus $rc = 1$, waarbij we gebruikten dat R commutatief is en dat R een domein is (uit $(rc - 1)a = 0$ en $a \neq 0$ volgt dan dat $rc - 1 = 0$). We zien dat c een eenheid is, met inverse r. In iedere schrijfwijze $bc = a$ geldt dus dat $b \in R^*$ of $c \in R^*$ en we concluderen dat a irreducibel is. Hiermee is Stelling 5.4 bewezen. □

Voorbeeld 5.5. Laat R de ring

$$R = \left\{ \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X] \;\middle|\; a_1 = 0\,, n \in \mathbb{Z}_{\geq 0} \right\}$$

zijn (overigens mag je voor $\mathbb{Q}$ een willekeurig lichaam K nemen); men gaat gemakkelijk na dat dit inderdaad een deelring van $\mathbb{Q}[X]$ is, en dat $X \notin R$.

We beweren nu, dat X^2 *wel* een irreducibel element van R is, maar dat RX^2 *geen* priemideaal in R is.

Eerst het bewijs dat X^2 irreducibel is: ga zelf na dat X^2 geen eenheid is. Dan moeten we nog laten zien: als $X^2 = f \cdot g$ met $f, g \in R$ dan $f \in R^*$ of $g \in R^*$. Uit $X^2 = f \cdot g$ volgt dat f en g samen graad twee hebben. Maar R bezit geen polynomen van graad één, dus dit kan alleen als f of g graad nul heeft, laten we zeggen f. Dan is f een constant polynoom: $f \in \mathbb{Q}$, en $f \neq 0$, dus heeft f een inverse in $\mathbb{Q}$, en dus zeker in R, d.w.z. $f \in R^*$. Dit bewijst dat X^2 irreducibel in R is. (Natuurlijk is X^2 niet irreducibel in $\mathbb{Q}[X]$, want $X^2 = X \cdot X$.)

Nu het bewijs dat RX^2 geen priemideaal van R is. Er geldt $X^3 \cdot X^3 \in R \cdot X^2$ (want $X^4 \in R$). Als nu RX^2 een priemideaal van R was, dan zou uit (P2) van 4.1 (met $a = b = X^3$) volgen dat $X^3 \in RX^2$, dus $X \in R$, tegenspraak.

We gaan nu een belangrijke klasse ringen definiëren waarin ieder irreducibel element wél een priemideaal, en zelfs een maximaal ideaal voortbrengt.

Definitie 5.6. Een *hoofdideaaldomein* (Engels: PID, principal ideal domain) is een domein R waarin elk ideaal een hoofdideaal is.

Voorbeeld 5.7. Zoals we in Voorbeeld 2.6 gezien hebben, is $\mathbb{Z}$ een hoofdideaaldomein. Uit Voorbeeld 2.12 blijkt dat $\mathbb{R}[X,Y]$ geen hoofdideaaldomein is. Alle lichamen zijn hoofdideaaldomeinen; dit volgt op triviale wijze uit 2.17. Volgens 3.4 is $K[X]$ een hoofdideaaldomein voor elk lichaam K.

De volgende stelling laat zien dat in een hoofdideaaldomein verscheidene van de ingevoerde begrippen samenvallen.

Stelling 5.8. *Laat R een* hoofdideaaldomein *zijn, en $a \in R, a \neq 0$. Dan zijn de volgende drie uitspraken equivalent:*

(i) *Ra is een maximaal ideaal van R;*

(ii) *Ra is een priemideaal van R;*

(iii) *a is irreducibel in R.*

Bewijs. (i) $\Rightarrow$ (ii): dit volgt direct uit 4.12.

(ii) $\Rightarrow$ (iii): dit is precies Stelling 5.4.

Tot zover hebben we geen gebruik gemaakt van het gegeven dat R een hoofdideaaldomein is. Dit gebeurt wel in het bewijs van de laatste implicatie.

(iii) $\Rightarrow$ (i). Gegeven is dat $a \in R$ irreducibel is. We moeten bewijzen dat het ideaal Ra voldoet aan de eisen (M1) en (M2) van 4.8.

(M1) a is irreducibel, dus geen eenheid. Hieruit volgt dat $Ra \neq R$.

(M2) Stel dat J een ideaal van R is met $Ra \subset J \subset R$. We moeten bewijzen dat $J = Ra$ of $J = R$. Omdat R een hoofdideaaldomein is kunnen we schrijven $J = Rb$ voor zekere $b \in R$. Uit $a \in Ra \subset J = Rb$ blijkt dat $a \in Rb$, dus $a = rb$ voor zekere $r \in R$. Maar a is irreducibel, dus dit kan alleen als $r \in R^*$ of $b \in R^*$. In het geval $r \in R^*$ geldt $b = r^{-1}a \in Ra$, dus $J = Rb \subset Ra$, dus $J = Ra$. In het geval dat $b \in R^*$ geldt $J = Rb = R$. Hiermee is (M2) gecontroleerd, en de stelling is bewezen. □

In het bijzonder zien we dat in hoofdideaaldomeinen de omkering van 4.12 geldt, voor idealen $\neq \{0\}$:

Gevolg 5.9. *In een hoofdideaaldomein is elk priemideaal $\neq \{0\}$ maximaal.*

Bewijs. Dit volgt uit 5.8, (ii) $\Rightarrow$ (i), aangezien elk ideaal $\neq \{0\}$ van de vorm Ra is, met $a \neq 0$. Dit bewijst 5.9. □

Voorbeeld 5.10. Uit Stelling 5.8 volgt dus dat de ring R uit Voorbeeld 5.5 geen hoofdideaaldomein is (deze R is overigens wel een domein). In feite is het ideaal voortgebracht door X^2 en X^3 geen hoofdideaal, zie Opgave 3.

We gaan ons nu bezighouden met een algemene methode om aan te tonen dat in bepaalde ringen irreducibele elementen priemidealen voortbrengen.

Definitie 5.11. Een *ontbindingsring* is een domein R met de eigenschap dat elke $a \in R, a \neq 0$, kan worden geschreven als product van een eenheid en een eindig aantal irreducibele elementen:

$$a = u \cdot p_1 \cdot p_2 \cdots p_t, \qquad u \in R^*, \;\; t \in \mathbb{Z}_{\geq 0}, \;\; p_i \in R \text{ irreducibel}$$

en een dergelijke ontbinding bovendien eenduidig bepaald is op volgorde en eenheden na, d.w.z. als ook

$$a = v \cdot q_1 \cdot q_2 \cdots q_s, \qquad v \in R^*, \;\; s \in \mathbb{Z}_{\geq 0}, \;\; q_i \in R \text{ irreducibel},$$

dan geldt $s = t$ en er is een permutatie σ van $\{1, 2, \ldots, t\}$ zodat

$$p_i = v_i \cdot q_{\sigma(i)} \qquad \text{voor zekere eenheden } v_i \in R^*, \; i = 1, 2, \ldots, t.$$

(Kennelijk geldt dan $v = uv_1v_2 \cdots v_t$.)

We noemen een schrijfwijze voor a als hierboven de *priemontbinding* van a, naar de analogie met de priemontbinding in $\mathbb{Z}$. (De idealen Rp_i zijn inderdaad priemidealen, zie Stelling 5.12.)

Informeel is een ontbindingsring dus een domein waarin de stelling van de eenduidige priemfactorontbinding geldt. In het engels schrijft men UFD, unique factorization domain, voor ontbindingsring.

Merk op dat de zorgvuldigheid ten aanzien van *eenheden* die in de definitie betracht wordt niet nodig was in het geval $R = \mathbb{Z}$, aangezien we ons daar indertijd tot *positieve* getallen beperkt hebben. Een dergelijke regeling is echter in willekeurige ringen niet zonder meer te treffen.

Stelling 5.12. *Zij R een ontbindingsring, en $a \in R$. Dan geldt:*

$$a \text{ is irreducibel} \quad \Longleftrightarrow \quad Ra \text{ is een priemideaal} \neq (0).$$

Bewijs. $\Leftarrow$: dit is algemeen waar, zie 5.4.

$\Rightarrow$: Laat $a \in R$ irreducibel zijn. Dan $a \neq 0$, en we moeten alleen nog bewijzen dat Ra een priemideaal is van R. Er geldt zeker (P1): $Ra \neq R$, want a is geen eenheid.

We controleren (P2). Stel dat $b, c \in R$ voldoen aan $bc \in Ra$, we moeten bewijzen dat $b \in Ra$ of $c \in Ra$. Dit is duidelijk als $b = 0$ of $c = 0$, dus stel dat $b, c \neq 0$. Dan geldt $bc \neq 0$, en omdat $bc \in Ra$ kunnen we schrijven $bc = da$, met $d \in R$, $d \neq 0$. Ontbinden we d in irreducibele factoren (en een eenheid), dan zien we dat bc zo'n ontbinding bezit waarin het irreducibele element a voorkomt. Een andere ontbinding van bc in irreducibele factoren (en een eenheid) wordt verkregen door zo'n ontbinding voor b met zo'n ontbinding voor c te combineren. Wegens de eenduidigheid van de ontbinding moet ook hierin het element a (eventueel vermenigvuldigd met een eenheid) voorkomen; d.w.z. a komt voor in de ontbinding van b of van c, dus $b \in Ra$ of $c \in Ra$. Hiermee is 5.12 bewezen. □

In een ontbindingsring geldt de omkering van Stelling 5.4 dus *wel*. Om te verifiëren of een ring een ontbindingsring is, is het volgende lemma van belang.

Lemma 5.13. *Laat R een domein zijn waarin elke $a \in R$, $a \neq 0$, geschreven kan worden als product van een eenheid en een eindig aantal elementen:*

$$a = u \cdot p_1 \cdot p_2 \cdots p_t, \quad u \in R^*, \; t \in \mathbb{Z}_{\geq 0}, \;\; p_i \in R$$

met de eigenschap dat voor iedere $i = 1, 2, \ldots, t$ geldt dat:

$$p_i R \quad \textit{is een priemideaal.}$$

Dan is R een ontbindingsring.

Bewijs. Merk op dat in zo'n ontbinding voor een $a \neq 0$ ook iedere $p_i \neq 0$ is. Omdat $p_i R$ een priemideaal is volgt dus uit Stelling 5.4 dat de p_i irreducibel zijn. We hoeven dus alleen de *eenduidigheid* van de ontbinding nog te bewijzen, want het *bestaan* hebben we al. Stel dus dat $a = up_1 \cdots p_t$ nog een ontbinding heeft:

$$up_1 p_2 \cdots p_t = vq_1 q_2 \cdots q_s$$

met $u, v \in R^*,\ t, s \in \mathbb{Z}_{\geq 0},\ p_i$ irreducibel met Rp_i een priemideaal voor $(1 \leq i \leq t)$ en irreducibele q_j $(1 \leq j \leq s)$.

We willen bewijzen dat $s = t$, en dat de q_j's op eenheden en volgorde na samenvallen met de p_i's. Dit doen we met inductie naar t.

Als $t = 0$ dan is $vq_1 q_2 \cdots q_s = u$ een eenheid. Aangezien irreducibele elementen geen eenheden zijn kan dit alleen als $s = 0$, $v = u$, zoals verlangd.

Laat nu $t > 0$. Dan geldt $q_1 q_2 \cdots q_s = v^{-1} \cdot up_1 p_2 \cdots p_t \in Rp_t$, en Rp_t is een priemideaal. Als $s = 0$ zou dit leveren $1 \in Rp_t$, hetgeen voor een priemideaal onmogelijk is ((P1) van 4.1). Dus $s > 0$. Het product van de s factoren $q_1, q_2, \ldots, q_s$ kan volgens (P2) van 4.1 alleen tot het priemideaal Rp_t behoren, als ten minste één van de factoren, zeg q_s, ertoe behoort: $q_s = r \cdot p_t$. Maar q_s is irreducibel, en p_t is geen eenheid, dus r moet een eenheid zijn. Omdat R een domein is, kunnen we nu onze oorspronkelijke gelijkheid door p_t delen:

$$up_1 p_2 \cdots p_{t-1} = (rv) q_1 q_2 \cdots q_{s-1}, \qquad rv \in R^*.$$

Dit is een dergelijke gelijkheid, met t één kleiner. De inductiehypothese zegt dus dat $t - 1 = s - 1$, en dat $p_1, p_2, \ldots, p_{t-1}$ op volgorde en eenheden na samenvallen met $q_1, q_2, \ldots, q_{s-1}$. Aangezien ook p_t op een eenheid na gelijk aan q_s is, concluderen we dat $s = t$, en dat $p_1, p_2, \ldots, p_t$ op volgorde en eenheden na samenvallen met $q_1, q_2, \ldots, q_s$. Hiermee is Lemma 5.13 bewezen. □

We bewijzen nu dat hoofdideaaldomeinen ontbindingsringen zijn.

Stelling 5.14. *Ieder hoofdideaaldomein is een ontbindingsring.*

Bewijs. Zij R een hoofdideaaldomein. We hoeven alleen maar te bewijzen dat elke $r \in R$ met $r \neq 0$ een ontbinding $r = up_1 \ldots p_t$, met Rp_i priemidealen) heeft, de eenduidigheid volgt dan uit Lemma 5.13.

Stel dat $a_1 \in R$, $a_1 \neq 0$, niet zo'n ontbinding heeft. Het ideaal Ra_1 is dan niet de hele ring R (want anders zou a_1 een eenheid zijn en dat was er wel een ontbinding). Dus volgt dat er een maximaal ideaal M bestaat met $Ra_1 \subset M$. Vanwege onze aanname dat R een hoofdideaaldomein is, geldt $M = Rp_1$ voor een $p_1 \in R$. Wegens $a_1 \in Ra_1 \subset M = Rp_1$ kunnen we schrijven $a_1 = a_2 p_1$ voor een $a_2 \in R$. Dan is $Ra_1 \subset Ra_2$, en, omdat p_1 geen eenheid is, ook $Ra_1 \neq Ra_2$.

We kunnen nu dit argument herhalen: $a_2 \neq 0$ en a_2 is geen eenheid (want we nemen aan dat a_1 geen ontbinding als product van een eenheid maal een stel voortbrengers van priemidealen heeft), dus

bestaat er een maximaal ideaal $Rp_2 \supset Ra_2$, enz. Zo verder gaande met a_2 vindt men een $a_3 \in R$ met $Ra_2 \subset Ra_3$, maar $Ra_2 \neq Ra_3$, en a_3 is geen eenheid, etcetera. Dit leidt nu tot een keten van idealen $(Ra_n)_{n=1}^{\infty}$ met $Ra_n \subset Ra_{n+1}$ maar $Ra_n \neq Ra_{n+1}$. Zij

$$I = \bigcup_{n \geq 1} Ra_n \qquad (\subset R).$$

Er geldt dat I een ideaal in R is. Als nl. $a, b \in I$ dan is $a \in Ra_k$ en $b \in Ra_l$ voor zekere $k, l \in \mathbb{N}$ en wegens de inclusies van de Ra_i geldt $a, b \in Ra_m$ met $m = \max\{k, l\}$. Omdat Ra_m een ideaal is zit dan ook $a - b \in Ra_m \subset I$. Als $r \in R$ en $a \in Ra_n$ dan zit uiteraard $ra \in Ra_n$, waarmee bewezen is dat I een ideaal in R is.

Omdat R een hoofdideaaldomein is, moet er een $d \in R$ zijn met:

$$I = Rd.$$

Omdat I de vereniging is van de Ra_n, moet er een m zijn met $d \in Ra_m$. Dan is echter:

$$Ra_m \subset Ra_{m+1} \subset I = Rd \subset Ra_m,$$

in tegenspraak met $Ra_m \neq Ra_{m+1}$.

De aanname dat er een element $a_1 \neq 0$ in R is dat geen ontbinding bezit als product van een eenheid maal een stel voortbrengers van priemidealen leidt dus tot een tegenspraak. We concluderen dat iedere $r \in R$, $r \neq 0$, wel zo'n ontbinding heeft en de stelling is bewezen. □

5.15 Als K een lichaam is, dan is $K[X]$ een hoofdideaaldomein, zie 3.4, en dus is $K[X]$ een ontbindingsring. Ieder irreducibel element g is i.h.b. een polynoom van graad groter dan 0. Omdat de kopcoëfficiënt a_n van g een eenheid is, kunnen we elk irreducibel element op unieke wijze schrijven als: $g = a_n h$ met h een monisch polynoom (d.w.z. kopcoëfficiënt 1). De priemontbinding van een willekeurige $f \in K[X]$ wordt dan gegeven door:

$$f = u h_1^{n_1} h_2^{n_2} \dots h_k^{n_k},$$

met $u \in K^* = K[X]^*$, de eenheden van $K[X]$, en de h_i zijn onderling verschillende monische irreducibele polynomen. Deze schrijfwijze is dan, gegeven f, uniek (op verwisseling van de h_i na). Vergelijk dit met de situatie in $\mathbb{Z}$ waar we irreducibele elementen positief kunnen nemen door met de juiste eenheid (± 1 dus) te vermenigvuldigen.

Stelling 5.16. *Zij K een lichaam en zij $f = u h_1^{n_1} \dots h_k^{n_k}$ de priemontbinding van f met verschillende monische irreducibele factoren. Neem aan dat $k \geq 1$, d.w.z. f is niet constant. Dan is*

$$K[X]/(f) \cong K[X]/(h_1^{n_1}) \times \dots \times K[X]/(h_k^{n_k}).$$

Bewijs. We voeren inductie naar het aantal irreducibele factoren k van f. Als $k = 1$ is de uitspraak triviaal waar.

Laat nu $k > 1$. Dan schrijven we

$$f = f_{k-1} h_k^{n_k}$$

met $f_{k-1} = uh_1^{n_1} \dots h_{k-1}^{n_{k-1}}$. We definiëren idealen I en J in $K[X]$ door

$$I = (f_{k-1}) \qquad J = (h_k^{n_k}),$$

en we zullen laten zien dat $I + J = K[X]$, zodat we de Chinese reststelling 2.36 kunnen toepassen om $K[X]/(f) = K[X]/IJ$ te berekenen.

Omdat $K[X]$ een hoofdideaaldomein is, geldt $I + J = (g)$ voor een polynoom $g \in K[X]$. Omdat $h_k^{n_k} \in J \subset (g)$ is er een $r \in K[X]$ met $h_k^{n_k} = rg$. Beschouwen we de priemontbinding van r en g in $K[X]$ en gebruiken we dat h_k irreducibel is, dan zien we dat $g = vh_k^m$ voor zekere m (zelfs $m \leq n_k$), met v een eenheid.

Anderzijds geldt ook $f_{k-1} \in I \subset (g)$, dus er is een $s \in K[X]$ met $f_{k-1} = sg$, oftewel:

$$uh_1^{n_1} \dots h_{k-1}^{n-1} = svh_k^m.$$

Omdat de h_i monisch, irreducibel zijn en $K[X]$ een ontbindingsring is, moet gelden dat $h_k = h_i$ voor zekere $i \in \{1, \dots, k-1\}$ of dat $m = 0$. Omdat gegeven is dat de h_j, $1 \leq j \leq k$ onderling verschillende monische irreducibele polynomen zijn, is $h_i = h_k$ onmogelijk en dus is $m = 0$. Dan is $g = vh_k^m = v$, een eenheid in $K[X]$, en dus $I + J = (g) = K[X]$.

Uit de Chinese reststelling volgt

$$K[X]/(f) = K[X]/(f_{k-1}h_k^{n_k}) \cong K[X]/(f_{k-1}) \times K[X]/(h_k^{n_k}).$$

Op de ring $K[X]/(f_{k-1})$ passen we nu de inductiehypothese toe en we vinden

$$K[X]/(f) \cong K[X]/(h_1^{n_1}) \times K[X]/(h_2^{n_2}) \times \dots \times K[X]/(h_k^{n_k}),$$

zoals verlangd. Hiermee is 5.16 bewezen. □

Als K een lichaam is, dan is $K[X]$ een hoofdideaaldomein en dus in het bijzonder een ontbindingsring (Stelling 5.14). We gaan nu de volgende algemenere stelling bewijzen.

Stelling 5.17. *Als R een ontbindingsring is, dan is $R[X]$ ook een ontbindingsdomein.*

Gevolg 5.18. *Voor elke $n \in \mathbb{Z}_{>0}$ en elke ontbindingsring R is ook de polynoomring $R[X_1, X_2, \dots, X_n]$ een ontbindingsring. In het bijzonder zijn de ringen $\mathbb{Z}[X_1, X_2, \dots, X_n]$ en $K[X_1, X_2, \dots, X_n]$ (K een lichaam) ontbindingsringen.*

Bewijs. Dit volgt onmiddellijk met volledige inductie naar n uit Stelling 5.17. □

5.19 Voor het bewijs van Stelling 5.17 hebben we enige voorbereidingen nodig. We nemen steeds aan dat R een ontbindingsring is, en we geven het quotiëntenlichaam $Q(R)$ van R aan met K, zie 1.26. Aangezien K een lichaam is, weten we al dat $K[X]$ een ontbindingsring is; dit speelt een belangrijke rol in het bewijs. We zullen nl. een $f \in R[X]$ eerst ontbinden in irreducibele factoren in $K[X]$, en vervolgens proberen we met die ontbinding een ontbinding van f in $R[X]$ te vinden; zie het bewijs van Lemma 5.25.

5.20 Twee elementen a, $b \in R$ noemt men *geassocieerd* als $a = ub$ met $u \in R$ een eenheid. Zij $P \subset R$ een verzameling van irreducibele elementen van R met de eigenschap dat elk irreducibel element van R met precies één element van P geassocieerd is. In geval $R = \mathbb{Z}$ kan men voor P bijvoorbeeld de positieve irreducibele elementen nemen, als $R = K[X]$ met K een lichaam dan kan men de monische irreducibele elementen nemen.

Definitie 5.21. Zij R een ontbindingsring. Laat a, $b \in R - \{0\}$ met priemontbinding:

$$a = u \cdot \prod_{p \in P} p^{n(p)}, \qquad b = v \cdot \prod_{p \in P} p^{m(p)},$$

hierbij zijn $n(p)$, $m(p) \in \mathbb{Z}_{\geq 0}$ (slechts eindig veel $n(p)$, $m(p)$ zijn $\neq 0$) en P is een verzameling van priemelementen als boven.

We definiëren de *grootste gemene deler* (ggd) van a en b door:

$$\text{ggd}(a, b) = \prod_{p \in P} p^{min\{n(p), m(p)\}} \qquad (\in R),$$

de ggd is slechts op eenheden na (keuze van P (!)) bepaald. Zie Opgave 5 voor een verklaring van de terminologie.

5.22 Laat $f = \sum_{i=0}^{n} a_i X^i \in R[X]$, $f \neq 0$ een polynoom zijn, en laat d de grootste gemene deler van de coefficiënten $a_0, a_1, \ldots, a_n$ van f zijn. We noemen d de *inhoud* van f, notatie:

$$\text{inh}(f) = \text{ggd}(a_0, a_1, \ldots, a_n),$$

deze is slechts op eenheden na goed gedefinieerd. We kunnen $f = d \cdot f_0$ schrijven, waarbij $f_0 \in R[X]$ een polynoom met inhoud 1 is. Polynomen met inhoud 1 heten *primitief*. In het volgende lemma beschouwen we een dergelijke schrijfwijze voor polynomen met coefficienten uit K.

Lemma 5.23. *Elk polynoom $f \neq 0$ uit $K[X]$ kan worden geschreven als $f = d \cdot f_0$ met $d \in K^*$ en $f_0 \in R[X]$ een primitief polynoom. Deze schrijfwijze is bovendien op eenheden van R na eenduidig bepaald.*

Bewijs. Als c het product van de noemers van de coëfficiënten van f is, geldt $cf \in R[X]$ en $cf = \text{inh}(cf) \cdot f_0$ met $f_0 \in R[X]$ een primitief polynoom. Dan $f = c^{-1} \cdot cf = c^{-1} \cdot \text{inh}(cf) f_0$, dus we kunnen $d = c^{-1} \cdot \text{inh}(cf)$ nemen.

Stel nu dat $d \cdot f_0 = e \cdot g_0$, met $d, e \in K^*$, $f_0, g_0 \in R[X]$ primitief; we willen bewijzen dat $d = e \cdot u$, $f_0 = u^{-1} \cdot g_0$ voor een $u \in R^*$. Door d en e met een gemeenschappelijke noemer te vermenigvuldigen mogen we aannemen dat d, $e \in R$. Dan zijn d en e allebei gelijk aan de inhoud van het polynoom $d \cdot f_0 = e \cdot g_0$, dus ze vallen, op een eenheid na, samen, zoals verlangd. Hiermee is 5.23 bewezen. □

Uit het volgende lemma zien we, hoe de in 5.23 aangegeven schrijfwijze zich gedraagt als we producten van polynomen gaan vormen.

Lemma 5.24. *Het product van twee primitieve polynomen uit $R[X]$ is weer primitief.*

Bewijs. Stel dat $f = \sum a_i X^i$ en $g = \sum b_j X^j$ primitief zijn, maar dat $f \cdot g = \sum c_k X^k$ het niet is. Dan is er een irreducibel element p van R dat alle coefficienten c_k van $f \cdot g$ deelt: $c_k \in Rp$ voor alle k. Laat nu $\overline{f} = \sum \overline{a}_i X^i \in (R/pR)[X]$ en $\overline{g} = \sum \overline{b}_j X^j \in (R/pR)[X]$ (hier $\overline{a} = (a \bmod pR) \in R/pR$, voor $a \in R$). Dan geldt in $(R/pR)[X]$:

$$\overline{f} \cdot \overline{g} = (\sum \overline{a}_i X^i) \cdot (\sum \overline{b}_j X^j) = \sum \overline{c}_k X^k = \sum \overline{0} \cdot X^k = \overline{0}.$$

Omdat Rp een priemideaal van R is (Stelling 5.12), is R/pR een domein, en dan is ook $(R/pR)[X]$ een domein. Maar een domein heeft geen nuldelers, dus het product $\overline{f} \cdot \overline{g}$ kan alleen nul zijn als een der factoren $\overline{f}$ of $\overline{g}$ nul is; laten we zeggen $\overline{f}$. Dan zijn alle $\overline{a}_i$ nul, d.w.z. alle a_i zijn deelbaar door p, in tegenspraak met onze aanname dat f primitief is. Hiermee is Lemma 5.24 bewezen. □

Lemma 5.25. *Elke $f \in R[X], f \neq 0$, kan geschreven worden in de vorm*

$$f = u \cdot p_1 p_2 \cdots p_s \cdot g_1 g_2 \cdots g_t$$

met $u \in R^*, s, t \in \mathbb{Z}_{\geq 0}$, waarbij $p_1, p_2, \ldots, p_s$ irreducibele elementen uit R zijn, en $g_1, g_2, \ldots, g_t$ primitieve polynomen uit $R[X]$, die in $K[X]$ irreducibel zijn. Bovendien is deze schrijfwijze op volgorde en eenheden van R na eenduidig bepaald.

Bewijs. Omdat $K[X]$ een ontbindingsring is, kan f geschreven worden als

$$f = d \cdot g_1 g_2 \cdots g_t,$$

met $d \in K[X]^* = K^*, t \in \mathbb{Z}_{\geq 0}$, en $g_1, g_2, \ldots, g_t \in K[X]$ irreducibel. Verder is deze schrijfwijze op volgorde en elementen van K^* na eenduidig bepaald. Schrijf nu elke g_i in de door Lemma 5.23 aangegeven vorm, dan zien we dat we zelfs mogen aannemen dat elke g_i primitief in $R[X]$ is (hierbij wordt d eventueel veranderd). Bovendien liggen, met deze extra voorwaarde, de g_i op eenheden van R na vast, en wegens $f = dg_1 g_2 \cdots g_t$ geldt hetzelfde voor d.

Merk op dat, met de g_i, ook het product $g_1 g_2 \cdots g_t$ primitief is, wegens 5.24. Dus $f = d \cdot (g_1 g_2 \cdots g_t)$ is de eenduidig bepaalde schrijfwijze uit 5.23. Dit betekent dat d gelijk moet zijn aan de inhoud van f; in het bijzonder moet d tot R behoren. Ontbinden we d nu in R:

$$d = u \cdot p_1 p_2 \cdots p_s \qquad (u \in R^*, \ \ s \in \mathbb{Z}_{\geq 0}, \ \ p_i \in R \ \text{ irreducibel})$$

(dit is weer uniek, op volgorde en vermenigvuldiging met eenheden na), dan vinden we de verlangde schrijfwijze $f = up_1 p_2 \cdots p_s g_1 g_2 \cdots g_t$. De eenduidigheid hebben we in de loop van het bewijs gezien. Hiermee is Lemma 5.25 bewezen. □

Bewijs van Stelling 5.17. Zij $f \in R[X], f \neq 0$. We gaan bewijzen dat de ontbinding van f die door lemma 5.25 gegeven wordt de priemontbinding van f is. We hoeven alleen nog te bewijzen dat de irreducibele elementen van $R[X]$ precies de irreducibele elementen p van R en de primitieve, in $K[X]$ irreducibele polynomen g zijn.

Laat hiertoe eerst $f \in R[X]$ irreducibel zijn, en schrijf f als in 5.25. Dan $s+t \neq 0$ (want f is geen eenheid), en $s+t < 2$ (anders krijgen we een ontbinding van f in twee niet-eenheden). Dus $s+t = 1$, d.w.z. f is (op een eenheid na) gelijk aan een p of een g, zoals verlangd.

Omgekeerd, laat p (resp. g) een irreducibel element van R (resp. een primitief, in $K[X]$ irreducibel polynoom uit $R[X]$) zijn. Dit is dan geen eenheid van $R[X]$, want $R[X]^* = R^*$, en als het als product $f_1 f_2$ van twee niet-eenheden van $R[X]$ geschreven kon worden, zouden we direct een tegenspraak met de eenduidigheid van de schrijfwijze uit 5.25 krijgen door de ontbinding van f_1 en f_2 tot een ontbinding voor p (resp. g) $= f_1 f_2$ te combineren. We concluderen dat p (resp. g) irreducibel in $R[X]$ is. Hiermee is 5.17 bewezen. □

Aan dit bewijs verbinden we nog diverse conclusies.

Gevolg 5.26. *Zij R een ontbindingsring met quotiëntenlichaam K, en $f \in R[X]$ een* primitief *polynoom. Dan geldt:*

$$f \text{ is irreducibel in } K[X] \quad \Longleftrightarrow \quad f \text{ is irreducibel in } R[X].$$

Bewijs. $\Leftarrow$: We hebben net gezien dat elke irreducibele $f \in R[X]$ ofwel irreducibel is in $K[X]$, of een irreducibel element uit R is; maar deze laatste mogelijkheid valt af omdat f primitief is.

$\Rightarrow$: Stel $f = g \cdot h$ met $g, h \in R[X]$. Omdat f in $K[X]$ irreducibel is moet één van beide factoren, zeg g, een eenheid in $K[X]$ zijn, dus $g \in K^* \cap R[X] = R - \{0\}$. Uit $f = g \cdot h$ blijkt nu dat g de inhoud van f deelt. Maar $\text{inh}(f) = 1$, dus g is een eenheid in R. Hieruit volgt dat f irreducibel in $R[X]$ is. Hiermee is Gevolg 5.26 bewezen. □

Gevolg 5.27 (Lemma van Gauss)**.** *Zij R een ontbindingsring met quotiëntenlichaam K, en $f \in R[X]$ een monisch polynoom. Stel dat $f = g \cdot h$, waar $g, h \in K[X]$ monisch zijn. Dan geldt $g, h \in R[X]$.*

Bewijs. Wegens 5.23 zijn er $u, v \in K^*$ zodat $u \cdot g$ en $v \cdot h$ primitief zijn in $R[X]$. Deze polynomen hebben kopcoëfficiënten u en v, dus $u, v \in R$. Nu is enerzijds f zelf primitief, want f is monisch. Anderzijds is ook $uv \cdot f$ primitief, wegens $uv \cdot f = (ug) \cdot (vh)$ en 5.24. Dit is alleen mogelijk als uv een eenheid van R is. Uit $uvz = 1$ volgt $u(vz) = v(uz) = 1$, dus u en v zijn eenheden van R. We concluderen: $g = u^{-1} \cdot ug \in R[X]$ en $h = v^{-1} \cdot vh \in R[X]$. Dit bewijst 5.27. □

We bespreken nu enkele practische methoden om polynomen in factoren te ontbinden.

5.28 Bepaling van een nulpunt van een polynoom. Laat K een lichaam zijn en $f \in K[X]$. Elk eerstegraads polynoom in $K[X]$ is (op een eenheid na) van de vorm $X - a$, met $a \in K$, en volgens 3.7 is $X - a$ een factor van f dan en slechts dan a een nulpunt van f is. Het zoeken van eerstegraads factoren van f is dus gelijkwaardige met het zoeken van nulpunten van f. De volgende drie opmerkingen kunnen hierbij behulpzaam zijn.

(a) Als $f = aX^2 + bX + c$, met $a \neq 0$, dan geldt

$$4a \cdot f = (2aX + b)^2 - (b^2 - 4ac)$$

("kwadraat afsplitsen"). Hieruit zien we dat f een nulpunt in K heeft dan en slechts dan als $b^2 - 4ac$ een kwadraat in K is. We moeten hierbij wel aannemen dat $2 \neq 0$ in K geldt (anders $4af = 0$; in het lichaam $K = \mathbb{F}_2$ geldt wél $2 = 0$).

(b) Als K *eindig* is kan men alle elementen van K proberen. Voorbeeld: $K = \mathbb{F}_3, f = X^3 + X + \overline{1}$; dan $f(\overline{0}) = \overline{1}, f(\overline{1}) = \overline{0}$, $f(\overline{2}) = \overline{11} = \overline{2}$, dus $\overline{1}$ is het enige nulpunt van f in K.

(c) Als $K = \mathbb{Q}$, dan mogen we aannemen dat f primitief is:

$$f = a_n X^n + \cdots + a_1 X + a_0, \quad a_i \in \mathbb{Z},\ a_n \neq 0,\ a_0 \neq 0.$$

Er geldt nu: elk *rationaal* nulpunt van f heeft de vorm $\frac{b}{c}$, met b een positieve of negatieve deler van a_0 en c een positieve deler van a_n. Bewijs hiervan: stel dat b/c een nulpunt is van f, met $b, c \in \mathbb{Z}$, $c > 0, \mathrm{ggd}(b, c) = 1$. Dan geldt $f = (cX - b) \cdot g$ met $g \in \mathbb{Q}[X]$, en omdat $cX - b$ primitief is moet zelfs gelden $g \in \mathbb{Z}[X]$. Door vergelijking van de hoogstegraadscoëfficiënten ziet men nu $c|a_n$, en de laagstegraadscoëfficiënten geven $b|a_0$. Einde bewijs.

Voorbeeld: $f = 2X^3 + X^2 - X + 3$. Voor b komen $\pm 1, \pm 3$ in aanmerking, voor c alleen 1 en 2. Probeert men alle acht waarden voor b/c dan vindt men dat f als enige rationale nulpunt $-3/2$ heeft.

Belangrijk speciaal geval: f is monisch ($a_n = 1$). Dan moet $c = 1$, dus elk rationaal nulpunt is *geheel* en een deler van a_0.

Vaak kan men het aantal te proberen getallen verkleinen door op het *teken* van $f(x)$ te letten of modulo een klein priemgetal te rekenen. Voorbeeld: $f = X^3 + X^2 + X + 6$. Voor b/c komen in aanmerking: $\pm 1, \pm 2, \pm 3, \pm 6$. Maar het is duidelijk dat: $x > 0 \Rightarrow f(x) > 0$, en: x oneven $\Rightarrow f(x)$ oneven. Dus alleen -2 en -6 hoeven bekeken te worden, en het blijkt dat alleen -2 een nulpunt is.

5.29 Reduceren modulo een priemgetal. Is $f \in \mathbb{Z}[X]$ *monisch*, en bestaat er een priemgetal p zodat $(f \bmod p) \in \mathbb{F}_p[X]$ irreducibel is, dan is f irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$. Immers, een ontbinding $f = g \cdot h$ in $\mathbb{Z}[X]$ zou een ontbinding $\overline{f} = \overline{g} \cdot \overline{h}$ van $\overline{f} = (f \bmod p)$ in $\mathbb{F}_p[X]$ geven, tegenspraak. Dus f is irreducibel in $\mathbb{Z}[X]$, en wegens het lemma van Gauss dan ook in $\mathbb{Q}[X]$.

Als voorbeeld kijken we naar $f = X^4 + 3X^3 - X^2 - X + 27$. Kies $p = 2$. Het polynoom $\overline{f} = X^4 + X^3 + X^2 + X + \overline{1}$ is irreducibel in $\mathbb{F}_2[X]$, want het heeft geen nulpunt in $\mathbb{F}_2$, en het is ook niet deelbaar door het enige tweedegraads irreducibele polynoom in $\mathbb{F}_2[X]$, nl. $X^2 + X + \overline{1}$. Er volgt dat f irreducibel is in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

Ook als $\overline{f}$ *niet* irreducibel is levert deze methode informatie. Voorbeeld: $f = X^4 - X^2 + X + 2$. Met methode 5.28(c) gaat men na dat f geen nulpunt in $\mathbb{Q}$ heeft, dus als f reducibel is in $\mathbb{Z}[X]$ dan $f = g \cdot h$ met g, h van de graad twee. Dit geeft $\overline{f} = \overline{g} \cdot \overline{h}$ in $\mathbb{F}_2[X]$. Maar in $\mathbb{F}_2[X]$ splitst $\overline{f}$ in de irreducibele factoren X en $X^3 + X + \overline{1}$, dus $\overline{f}$ kan niet ontbonden worden in tweedegraads factoren. Conclusie: f is irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

5.30 Laat R een ontbindingsring zijn, p een irreducibel element van R, en

$$f = a_n X^n + \cdots + a_1 X + a_0 \in R[X], \quad n > 0.$$

We zeggen dat f een *Eisensteinpolynoom* (bij p) is als geldt:

$$\begin{aligned} &p \nmid a_n, \\ &p|a_i \qquad \text{voor } i = 0, 1, \ldots, n-1, \\ &p^2 \nmid a_0 \qquad (\text{maar } \ p|a_0). \end{aligned}$$

(Dit begrip is genoemd naar Gotthold Eisenstein, Duits wiskundige, 1823–1852).

Propositie 5.31 (Het kenmerk van Eisenstein)**.** *Zij R een ontbindingsring, en laat K het quotiëntenlichaam zijn van R. Zij $p \in R$ een irreducibel element en $f \in R[X]$ een Eisensteinpolynoom bij p. Dan is f irreducibel in $K[X]$. Als f primitief is, is f ook irreducibel in $R[X]$.*

Bewijs. Omdat $\mathrm{inh}(f)$ niet door p deelbaar is, is ook het primitieve polynoom $f/\mathrm{inh}(f)$ een Eisensteinpolynoom. Zonder beperking der algemeenheid mogen we dus aannemen dat f primitief is. Stel nu

$$f = g \cdot h, \qquad g, h \in R[X], \quad \mathrm{gr}(g) > 0, \ \ \mathrm{gr}(h) > 0.$$

In $(R/pR)[X]$ geldt wegens $p \nmid a_n, \ p|a_i \ \ (i = 0, 1, \ldots, n-1)$:

$$\overline{f} = (f \bmod p) = \overline{a}_n X^n \quad \text{met} \quad \overline{a}_n = (a_n \bmod p) \neq 0,$$

en bovendien

$$\overline{f} = \overline{g} \cdot \overline{h}, \quad \mathrm{gr}(\overline{g}) > 0, \ \mathrm{gr}(\overline{h}) > 0\,.$$

Dit kan alleen als

$$\overline{g} = \overline{b} X^k, \qquad \overline{h} = \overline{c} X^\ell$$

voor zekere $b, c \in R$ en $k, \ell \in \mathbb{Z}_{>0}$. Dan moeten de constante coëfficiënten van g en h allebei door p deelbaar zijn, en hieruit volgt dat de constante coëfficiënt a_0 van f door p^2 deelbaar is, in tegenspraak met het gegeven. Het primitieve polynoom f is dus irreducibel in $R[X]$ en daarom ook in $K[X]$ (Gevolg 5.26). □

Voorbeeld 5.32. Neem $R = \mathbb{Z}$ en $f = X^5 + 2X^3 - 6$; dit is een Eisensteinpolynoom bij $p = 2$, dus irreducibel.

In $R = \mathbb{R}[Y]$ is $f = X^3 + (Y^4 - 1)X - (Y^2 + 1)$ een Eisensteinpolynoom bij $p = Y^2 + 1$, en ook primitief, dus irreducibel in $\mathbb{R}[X, Y]$. Hetzelfde geldt voor het polynoom $X^2 + Y^2 - 1 \in (\mathbb{R}[Y])[X]$ met $p = Y - 1$.

5.33 Coëfficiënten vergelijken Wil men bijvoorbeeld $\sum_{i=0}^{4} a_i X^i$ in $\mathbb{Z}[X]$ ontbinden, $a_0 \neq 0$, $a_4 \neq 0$, en weet men dat er geen factor van graad ≤ 1 is (methode 5.28(c)), dan kan men schrijven

$$\sum_{i=0}^{4} a_i X^i = (b_2 X^2 + b_1 X + b_0) \cdot (c_2 X^2 + c_1 X + c_0)$$

dus

(a) $b_2c_2 = a_4$

(b) $b_2c_1 + b_1c_2 = a_3$

(c) $b_2c_0 + b_1c_1 + b_0c_2 = a_2$

(d) $b_1c_0 + b_0c_1 = a_1$

(e) $b_0c_0 = a_0$.

Voor b_2, c_2, b_0 en c_0 zijn er wegens (a) en (e) slechts eindig veel mogelijkheden: voor vaste b_2, c_2, b_0 en c_0 kan men b_1c_1 uit (c) bepalen, enzovoort. Deze methode is meestal tijdrovend maar leidt, in het vierdegraads geval, gegarandeerd in een eindig aantal stappen tot een ontbinding van f in irreducibele factoren.

Opmerking 5.34. In Van der Waerden, Algebra I, §32, staat een algoritme waarmee elke $f \in \mathbb{Z}[X]$ in een eindig aantal stappen in factoren kan worden ontbonden. Dit algoritme is voornamelijk van theoretische waarde. Voor verdere literatuur zie men: H.G. Zimmer, Computational problems, methods, and results in algebraic number theory, Chapter 2.

Opgaven

1. We beschouwen de ring
$$R = \mathbb{Z}\big[\sqrt{-5}\big] = \big\{a + b\sqrt{-5} \;\big|\; a, b \in \mathbb{Z}\big\}.$$
   (a) Bewijs dat $2,\ 3 \in R$ irreducibel zijn. (Aanwijzing: gebruik, zie 1.14, de afbeelding $N\colon R \to \mathbb{Z}$ gegeven door $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Deze heeft de eigenschap dat $r \in R^*$ dan en slechts dan als $N(r) = \pm 1$.)
   (b) Bewijs dat $R2$ en $R3$ geen priemidealen zijn. Is R een ontbindingsring?
   (c) Is dit niet in tegenspraak met Stelling 5.8 ?
   (d) Laat zien dat $6 = 2 \cdot 3$ en $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ twee verschillende ontbindingen van 6 als product van irreducibele elementen zijn.

2. Geef van elk van de volgende elementen van $\mathbb{Z}[\sqrt{-3}]$ aan of ze irreducibel zijn en of ze een priemideaal voortbrengen:
$$\sqrt{-3},\ \ 1,\ \ 2,\ \ 1 + \sqrt{-3},\ \ 5.$$

3. Zij $R = \big\{\sum a_i X^i \in \mathbb{Q}[X] \;\big|\; a_1 = 0\big\}$, zie Voorbeeld 5.5.
   (a) Zij $\Phi_0\colon R \to \mathbb{R}$ het evaluatiehomomorfisme in 0, dus $f \mapsto f(0)$. Bewijs dat
$$\mathrm{Ker}(\Phi_0) = (X^2, X^3) = \big\{f = X^2 g + X^3 h \in R \;\big|\; g, h \in R\big\}.$$
   (b) Bewijs dat $\mathrm{Ker}(\Phi_0)$ geen hoofdideaal is, maar wel een maximaal ideaal.

4. Zij $R = \mathbb{Z}[X]/(5X,\ X^2)$.
   (a) Bewijs dat elk element van R op eenduidige wijze geschreven kan worden als
$$\overline{a} + \overline{b} \cdot \overline{X} \quad \text{met} \quad a \in \mathbb{Z},\ b \in \mathbb{Z},\ 0 \le b < 5.$$
   waarbij $\overline{\ }$ de restklasse modulo $(5X,\ X^2)$ aangeeft.
   (b) Bewijs: $\overline{a} + \overline{bX} \in R^* \iff a \in \{\pm 1\}$.
   (c) Bewijs: als $\alpha = \overline{X},\ \beta = \overline{2} \cdot \overline{X}$, dan geldt
$$R \cdot \alpha = R \cdot \beta \qquad \text{en} \quad \alpha \notin R^* \cdot \beta.$$

5. Zij R een ontbindingsring en zij $d \in R$ de ggd van $a, b \in R$, dus $d = \mathrm{ggd}(a, b)$. Stel $c \in R$ is een deler van a en van b, d.w.z. er zijn $a_1,\ b_1 \in R$ met $a = ca_1,\ \ b = cb_1$. Bewijs dat c een deler van d is.

6. Ontbind $X^8 - 16$ en $X^6 + 27$ in irreducibele factoren in $\mathbb{Q}[X]$.

7. Is $5X^4 + 10X + 10$ een Eisensteinpolynoom in $\mathbb{Z}[X]$? Is het irreducibel in $\mathbb{Z}[X]$? en in $\mathbb{Q}[X]$?

8. Bewijs dat $X^n + 2$ irreducibel in $\mathbb{Z}[X]$ is voor alle $n \in \mathbb{Z}_{\geq 0}$.
   Bewijs dat $Y^n - X$ irreducibel is in $K[X, Y]$ (K een lichaam) voor alle $n \in \mathbb{Z}_{\geq 0}$.

9. (a) Vind een voorbeeld van een irreducibel polynoom $f \in \mathbb{Z}[X]$ met de eigenschap dat $f(X^2)$ *niet* irreducibel is.

   (b) Laat $f \in \mathbb{Z}[X]$ een monisch Eisensteinpolynoom zijn. Bewijs dat $f(X^2)$ irreducibel in $\mathbb{Z}[X]$ is.

10. Zij R een ontbindingsring. Bewijs dat

$$\bigcup_{n \geq 0} R[X_1, X_2, \ldots, X_n]$$

    een ontbindingsring is.

11. Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$:

$$\begin{aligned}
&4X^2 + 4,\\
&2X^{10} + 4X^5 + 3,\\
&X^4 - 7X^2 + 5X - 3,\\
&X^{111} + 9X^{74} + 27X^{37} + 27,\\
&X^3 + X + 3.
\end{aligned}$$

12. Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$:

$$\begin{aligned}
&\tfrac{1}{7}((X+1)^7 - X^7 - 1),\\
&X^3 + 3X^2 + 6X + 9,\\
&X^4 + 2X^3 + 3X^2 + 9X + 6,\\
&X^{12} - 1,\\
&X^4 - X^3 + X^2 - X + 1.
\end{aligned}$$

13. Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Q}[X, Y]$:

$$\begin{aligned}
&Y^4 + X^2 + 1,\\
&Y^3 - (X+1)Y^2 + Y + X(X-1),\\
&X^n + Y^3 + Y \quad (n \geq 1),\\
&X^4 + 4Y^4,\\
&X^4 + 2X^3 + X^2 - Y^2 - 2Y - 1,\\
&Y^n - 13X^4 \qquad (n \geq 1).
\end{aligned}$$

14. Zij $I \subset \mathbb{Z}[X]$ een priemideaal.

    (a) Bewijs dat $I \cap \mathbb{Z}$ een priemideaal in $\mathbb{Z}$ is.

    (b) Bewijs dat ofwel $I = \{0\}$ ofwel $I = (f)$ met $f \in \mathbb{Z}[X]$ irreducibel, ofwel $I = (p)$ met $p \in \mathbb{Z}$ een priemgetal ofwel $I = (p,\, f)$ met $f \in \mathbb{Z}[X]$ een polynoom dat modulo het priemgetal p irreducibel is.

(c) Bepaal alle maximale idealen van $\mathbb{Z}[X]$.

15. Stel dat n een positief geheel getal is waarvoor $n^4 + 4^n$ een priemgetal is. Bewijs dat $n = 1$.

16. Laat $f \in \mathbb{Z}[X]$ een monisch polynoom zijn waarvoor $f(0)$ een *priemgetal* is. Bewijs dat f ten hoogste *drie* verschillende nulpunten in $\mathbb{Q}$ heeft.

17. Bepaal alle irreducibele polynomen $f \in \mathbb{F}_2[X]$ met $\mathrm{gr}(f) \leq 3$.

18. Zij $R = \mathbb{C}[U, V]/(UV - 1)$.

    (a) Bewijs dat
    $$\mathbb{C}[T, T^{-1}] = \left\{ \frac{f(T)}{T^i} \in \mathbb{C}(T) \;\middle|\; f(T) \in \mathbb{C}[T],\ i \in \mathbb{Z} \right\}$$
    een deelring van het lichaam $\mathbb{C}(T)$ is.

    (b) Bewijs dat $R \cong \mathbb{C}[T, T^{-1}]$.

    (c) Bewijs dat R een hoofdideaaldomein is.

    (d) Bewijs dat $R \cong \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ (hint: $X^2 + Y^2 = (X + iY)(X - iY)$).

    (e) Bepaal een $r \in \mathbb{C}[X, Y]/(X^2+Y^2-1)$ met $(r) = (x-1, y)$ waarin $x = (X \bmod X^2 + Y^2 - 1)$ en $y = (Y \bmod X^2 + Y^2 - 1)$.

Hoofdstuk 6

Euclidische ringen

In dit hoofdstuk beginnen we met de vraag welke gehele getallen als som van twee kwadraten geschreven kunnen worden. We gebruiken hierbij de theorie van ontbindingsringen en Stelling 3.14.

6.1 Als $n \in \mathbb{Z}$ te schrijven is als som van 2 kwadraten, $n = a^2 + b^2$ met $a, b \in \mathbb{Z}$, dan kunnen we dat opvatten als een ontbinding van n in de ring $\mathbb{Z}[i]$:

$$n = a^2 + b^2 \quad \Longleftrightarrow \quad n = (a + bi)(a - bi).$$

Omgekeerd correspondeert elke ontbinding van n in $\mathbb{Z}[i]$ in twee complex geconjugeerde factoren $n = \alpha \cdot \bar{\alpha}$ met een schrijfwijze voor n als som van twee kwadraten.

We noemen de ring $\mathbb{Z}[i]$ de *ring van gehele getallen van Gauss*. In dit hoofdstuk laten we zien dat $\mathbb{Z}[i]$ een hoofdideaaldomein en dus ook een ontbindingsring is. Iedere $n \in \mathbb{Z}_{>0}$ heeft dus een priemontbinding in $\mathbb{Z}[i]$, d.w.z. een (essentieel unieke) schrijfwijze als product van een eenheid en een aantal irreducibele elementen van $\mathbb{Z}[i]$.

Merk bijvoorbeeld op dat 5 irreducibel is in $\mathbb{Z}$ maar dat

$$5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i),$$

en zoals we zullen zien zijn $1 + 2i$ en $1 - 2i$ irreducibel in $\mathbb{Z}[i]$, dus 5 heeft een niet-triviale priemfactorisatie in $\mathbb{Z}[i]$.

6.2 Zij

$$n = p_1^{n_1} \dots p_t^{n_t}, \qquad n_j \in \mathbb{Z}_{>0}$$

en p_j priem, de priemontbinding van n in $\mathbb{Z}$. Als we weten hoe we iedere p_j kunnen schrijven als een product van irreducibele elementen van $\mathbb{Z}[i]$, dan verkrijgen een schrijfwijze voor n als product van irreducibele elementen in $\mathbb{Z}[i]$. Deze schrijfwijze is dan de priemontbinding van n in $\mathbb{Z}[i]$.

Stelling 6.3. (a) *De eenheden van* $\mathbb{Z}[i]$ *zijn:*

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}.$$

(b) *Er geldt*

$$2 = -i \cdot (1+i)^2,$$

waarbij $-i \in \mathbb{Z}[i]^*$*, en* $1+i$ *is irreducibel in* $\mathbb{Z}[i]$.

(c) *Als* q *een priemgetal is en* $q \equiv 3 \bmod 4$ *dan is* q *irreducibel in* $\mathbb{Z}[i]$.

(d) *Als* p *een priemgetal is en* $p \equiv 1 \bmod 4$ *dan is er een* $\pi \in \mathbb{Z}[i]$ *zo dat*

$$p = \pi \cdot \bar{\pi}, \qquad \text{en} \quad \pi \neq u\bar{\pi}$$

voor elke eenheid $u \in \mathbb{Z}[i]^*$*. Zowel* π *als zijn complex geconjugeerde* $\bar{\pi}$ *is irreducibel in* $\mathbb{Z}[i]$.

Bewijs. (a) In 1.14 zagen we al:

$$a + bi \in \mathbb{Z}[i]^* \quad \Longleftrightarrow \quad N(a+bi) = a^2 + b^2 = \pm 1,$$

hieruit volgt (a) direkt.

(b) Merk op dat

$$N(1+i) = 1^2 + 1^2 = 2,$$

en dat $N(\alpha)N(\beta) = N(\alpha\beta)$. Als dus $\alpha\beta = 1+i$, dan moet ofwel $N(\alpha) = 1$ ofwel $N(\beta) = 1$, en met bovenstaande volgt dan dat α of β een eenheid is. Hiermee is bewezen dat $1+i$ irreducibel is in $\mathbb{Z}[i]$.

(c) Stel $q = \alpha\beta$, waarbij α en β geen van beide eenheden zijn. Dan geldt:

$$N(\alpha)N(\beta) = q^2, \qquad N(\alpha) > 1, \quad N(\beta) > 1.$$

Omdat q priem is in $\mathbb{Z}$, kan dat alleen als $N(\alpha) = N(\beta) = q$. Schrijf

$$\alpha = a + bi, \qquad \text{dan is} \quad N(\alpha) = a^2 + b^2 = q.$$

Als zowel a als b even zijn, dan zijn a^2 en b^2 4-vouden maar dat is in tegenspraak met het feit dat q geen 4-voud is. Als bijvoorbeeld a oneven is dan kunnen we schrijven:

$$a = 2k+1 \qquad \text{dus} \quad a^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1.$$

We zien dat $a^2 + b^2 \equiv 1 \bmod 4$ als a of b oneven is, en dat $a^2 + b^2 \equiv 2 \bmod 4$ als a én b oneven zijn. Er is dus geen $\alpha \in \mathbb{Z}[i]$ met $N(\alpha) = q$ ($\equiv 3 \bmod 4$) en we concluderen dat q irreducibel is.

(d) Als $p \equiv 1 \bmod 4$ dan is de groep $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ een cyclische groep van orde $p-1$, zie Stelling 3.14. Merk op dat $p-1$ deelbaar is door 4. Als α een voortbrenger van deze groep is, definieer dan

$$x = \alpha^{\frac{p-1}{4}} \qquad (\in \mathbb{F}_p).$$

De orde van x is dan 4, dus $x^2 = -1$. Men rekent eenvoudig na dat de afbeelding:

$$\phi\colon \mathbb{Z}[i] \to \mathbb{F}_p, \qquad a + bi \mapsto \bar{a} + \bar{b}x,$$

een (surjectief) ringhomomorfisme is. Omdat de ring $\mathbb{Z}[i]$ een hoofdideaaldomein is, zie 6.12 verderop, is er een $\pi \in \mathbb{Z}[i]$ met

$$(\pi) = \pi\mathbb{Z}[i] = \mathrm{Ker}(\phi), \qquad \text{i.h.b.} \quad \mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p.$$

Omdat $p \in \mathrm{Ker}(\phi)$, geldt $p = \pi\beta$ voor zekere $\beta \in \mathbb{Z}[i]$. Dan is $N(p) = p^2 = N(\pi)N(\beta)$. Als $N(\pi) = 1$, dan is π een eenheid, dus $(\pi) = \mathbb{Z}[i]$ in tegenspraak met $\mathbb{Z}[i]/(\pi) = \mathbb{F}_p$. Als $N(\pi) = p^2$ dan is $N(\beta) = 1$, dus β is een eenheid en dus geldt $(\pi) = (\pi\beta) = (p)$. Dit is onmogelijk, want $\mathbb{Z}[i]/(p)$ is een ring met p^2 elementen (repesentanten van de nevenklassen worden gegeven door $a+bi$ met a, $b \in \{0, 1, \ldots, p-1\}$) terwijl $\mathbb{Z}[i]/(\pi)$ maar p elementen heeft. We concluderen dat $N(\pi) = p$. Merk op dat $p = N(\pi) = \pi\bar{\pi}$ (dus blijkbaar is $\beta = \bar{\pi}$), waarmee een ontbinding van p gevonden is.

De irreducibiliteit van π volgt uit de opmerking dat $\pi = \alpha\gamma$ impliceert dat $N(\pi) = p = N(\alpha)N(\gamma)$, dus $N(\alpha) = 1$ of $N(\gamma) = 1$, dus α is een eenheid of γ is een eenheid. Geheel analoog bewijst men de irreducibiliteit van $\bar{\pi}$.

Tenslotte bewijzen we dat er geen eenheid u is met $\pi = u\bar{\pi}$. Schrijf $\pi = a + bi$ en merk op $N(\pi) = p = a^2 + b^2$. Stel

$$a + bi = u(a - bi) \qquad \text{met} \quad u \in \mathbb{Z}[i]^* = \{1, i, -1, -i\}.$$

Als $u = 1$ of $u = -1$ dan levert dit $a = 0$ of $b = 0$ in tegenspraak met $p = a^2 + b^2$. Als $u = \pm i$ dan volgt $a = \pm b$, hetgeen wederom in strijd is met $p = a^2 + b^2$.

Hiermee is Stelling 6.3 bewezen. □

Opmerking 6.4. Het moeilijkste deel van deze stelling, het ontbinden van een priem $p \equiv 1 \bmod 4$ in $\mathbb{Z}[i]$, kan ook op elementaire wijze bewezen worden. In het bijzonder kan het gebruik van Stelling 3.14 in dit bewijs vermeden worden. Het elementaire bewijs is niet erg lang, zie D. Zagier: A one-sentence proof that every prime $\equiv 1 \bmod 4$ is a sum of two squares, The American Mathematical Monthly, Vol. 97, p. 144.

Gevolg 6.5. *Zij $n \in \mathbb{Z}_{>0}$, met priemontbinding:*

$$n = 2^k p_1^{n_1} \cdots p_r^{n_r} q_1^{m_1} \cdots q_s^{m_s}, \qquad n_j, m_j \in \mathbb{Z}_{>0},$$

waarbij de p_j en q_j onderling verschillende priemgetallen zijn met $p_j \equiv 1 \bmod 4$ en $q_j \equiv 3 \bmod 4$. Dan is n te schrijven als som van twee kwadraten precies dan als m_j even is voor alle $j \in \{1, \ldots, s\}$.

Bewijs. Merk op dat n te schrijven is als de som van twee kwadraten:

$$n = a^2 + b^2 = (a + bi)(a - bi) = \alpha\bar{\alpha}$$

precies dan als er een $\alpha \in \mathbb{Z}[i]$ is met $\alpha\bar{\alpha} = n$.

Volgens de stelling wordt de priemontbinding van n in $\mathbb{Z}[i]$, waarbij we de factor 2^k echter niet ontbinden, gegeven door:

$$n = 2^k(\pi_1^{n_1}\bar{\pi}_1^{n_1}) \cdots (\pi_r^{n_r}\bar{\pi}_r^{n_r}) q_1^{m_1} \cdots q_s^{m_s}.$$

Als $n = \alpha\bar{\alpha}$ is de priemontbinding van α van de vorm:

$$\alpha = u(1 + i)^l(\pi_1^{a_1}\bar{\pi}_1^{b_1}) \ldots (\pi_r^{a_r}\bar{\pi}_r^{b_r}) q_1^{c_1} \ldots q_s^{c_s},$$

met u een eenheid. Dan geldt (merk op dat $u\bar{u} = 1$):

$$\alpha\bar{\alpha} = 2^l p_1^{a_1+b_1} \dots p_r^{a_r+b_r} q_1^{2c_1} \dots q_s^{2c_s}.$$

Hieruit zien we meteen: als $n = \alpha\bar{\alpha}$ dan geldt $m_j = 2c_j$ dus $m_j \equiv 0 \bmod 2$ voor alle j.

Omgekeerd, stel alle m_j zijn even. We kunnen dan als volgt een $\alpha \in \mathbb{Z}[i]$ vinden met $\alpha\bar{\alpha} = n$. Allereerst kiezen we

$$c_j = \frac{m_j}{2}, \qquad l = k.$$

Voor a_j kiezen we een geheel getal tussen 0 en n_j:

$$a_j \in \{0, 1, \dots, n_j\} \qquad \text{en} \quad b_j := n_j - a_j,$$

dus b_j is volledig bepaald door de keuze van a_j. Voor u kiezen we tenslotte één van de 4 eenheden van $\mathbb{Z}[i]$. Dan hebben we een α met de gewenste eigenschappen.

We merken nog op dat we zo $4 \cdot \prod_{i=1}^{r}(n_j + 1)$ mogelijke α's vinden, dit is dus ook precies het aantal elementen van de verzameling:

$$\left\{(a, b) \in \mathbb{Z}^2 \;\middle|\; a^2 + b^2 = n\right\}.$$

Hiermee is 6.5 bewezen. □

Voorbeeld 6.6. Zij $n = 41$, dan is n een priemgetal dat congruent 1 modulo 4 is, en het is dus de som van twee kwadraten. Er geldt:

$$41 = 16 + 25 = (4 + 5i)(4 - 5i) = \pi\bar{\pi},$$

waarbij $\pi = 4 + 5i$ en $\bar{\pi}$ irreducibel zijn in $\mathbb{Z}[i]$.

Zij $n = 45$, dan geldt:

$$45 = 5 \cdot 3^2 = (1 + 2i)(1 - 2i)3^2.$$

met $1 \pm 2i$ en 3 irreducibel in $\mathbb{Z}[i]$. Kiezen we

$$\alpha = (1 + 2i)3 = 3 + 6i, \qquad \text{dan} \quad 45 = \alpha\bar{\alpha} = 3^2 + 6^2.$$

Zij $n = 65 = 5 \cdot 13$. Omdat $5 = (1 + 2i)(1 - 2i)$ en $13 = (2 + 3i)(2 - 3i)$ is de priemontbinding van 65 in $\mathbb{Z}[i]$:

$$65 = \pi_1\bar{\pi}_1\pi_2\bar{\pi}_2, \qquad \text{met} \quad \pi_1 = 1 + 2i, \quad \pi_2 = 2 + 3i.$$

Nemen we

$$\alpha = \pi_1\pi_2 \qquad \text{dan} \quad \alpha = -4 + 7i \quad \text{en} \quad 65 = (-4)^2 + 7^2.$$

Nemen we

$$\alpha = \pi_1\bar{\pi}_2 \qquad \text{dan} \quad \alpha = 8 + i \quad \text{en} \quad 65 = 8^2 + 1^2.$$

Dit zijn, op tekens en volgorde van a, b na, de enige twee schrijfwijzes van 65 als som van twee kwadraten.

6.7 We gaan ons nu bezighouden met een algemene methode om aan te tonen dat bepaalde ringen hoofdideaaldomeinen zijn. Wanneer we onderzoeken hoe we dat gedaan hebben voor de ringen $\mathbb{Z}$ en $K[X]$ (K een lichaam) dan zien we dat in beide gevallen een belangrijke rol is gespeeld door de mogelijkheid van *deling met rest*. (Zie Stelling 3.4 in het geval $K[X]$.) Ringen waarin zo'n deling met rest mogelijk is heten *Euclidisch*. De precieze definitie luidt als volgt.

Definitie 6.8. Een domein R heet een *Euclidische ring* als er een functie

$$g\colon R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

bestaat met de volgende eigenschappen:

(E1) $g(a) \leq g(ab)$ voor alle $a,\, b \in R - \{0\}$;

(E2) voor alle $a,\, b \in R$ met $b \neq 0$ bestaan er $q, r \in R$ met

$$a = qb + r \qquad \text{en} \quad r = 0 \text{ of } g(r) < g(b).$$

Opmerking 6.9. Eigenschap (E2) drukt de mogelijkheid van "deling met rest" uit. De functie g wordt gebruikt om tot uitdrukking te kunnen brengen dat de "rest" r *kleiner* moet zijn dan het element b waardoor gedeeld wordt.

Voor $R = \mathbb{Z}$ kan men $g(n) = |n|$ nemen, en voor $R = K[X]$, met K een lichaam, voldoet $g(f) = \mathrm{gr}(f)$. We zien dat we in het algemeen bij $g(a)$ aan iets als de "grootte" van a moeten denken. We merken voorts op, dat voorwaarde (E1) in zekere zin overbodig is, zie Opgave 1.

Een lichaam K is op triviale wijze een Euclidische ring, als we $g(a) = 0$ zetten, voor alle $a \in K - \{0\}$.

Stelling 6.10. *Elke Euclidische ring R is een hoofdideaaldomein.*

Bewijs. We weten al dat R een domein is. Laat nu $I \subset R$ een willekeurig ideaal zijn. We moeten bewijzen dat I een hoofdideaal is. In het geval $I = \{0\}$ is dit duidelijk: dan geldt immers $I = R \cdot 0$. We nemen dus aan dat $I \neq \{0\}$. Dan is $I - \{0\}$ niet leeg, dus $g[I - \{0\}]$ is een niet-lege deelverzameling van $\mathbb{Z}_{\geq 0}$. Aangezien iedere niet-lege deelverzameling van $\mathbb{Z}_{\geq 0}$ een kleinste element bevat, kunnen we $b \in I - \{0\}$ kiezen met

$$g(b) = \min\bigl\{ g(x) \;\big|\; x \in I - \{0\} \bigr\}.$$

We beweren dat geldt $I = Rb$. De inclusie $\supset$ is duidelijk, want $b \in I$. We bewijzen de inclusie $\subset$. Laat $a \in I$. Omdat R Euclidisch is, zijn er $q, r \in R$ met $a = qb + r$, en $r = 0$ of $g(r) < g(b)$. Als $r = 0$ dan geldt $a = qb \in Rb$, precies wat we willen bewijzen. Als $r \neq 0$ geldt $g(r) < g(b)$, en bovendien $r \in I$, want $r = a - qb$ met $a, qb \in I$. Dit is in tegenspraak met de minimale keuze van b.

We concluderen dat $I = Rb$, dus I is een hoofdideaal. Hiermee is Stelling 6.10 bewezen. □

6.11 Merk op dat het bewijs van deze stelling geheel analoog verloopt aan de bewijzen die we kennen voor $R = \mathbb{Z}$ en $R = K[X]$.

De omkering van 6.10 geldt niet: er bestaan hoofdideaaldomeinen die niet Euclidisch zijn. Een dergelijk voorbeeld wordt gegeven door de ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$, zie Opgaven 3 en 4.

Stelling 6.12. *De ring $\mathbb{Z}[i]$ van getallen van Gauss is een Euclidische ring met g de norm afbeelding:*

$$g(a+bi) = N(a+bi) = a^2 + b^2, \quad \text{voor } a, b \in \mathbb{Z}.$$

In het bijzonder is $\mathbb{Z}[i]$ een hoofdideaaldomein.

Bewijs. We controleren de voorwaarde op g. Laat $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$. We moeten $\gamma, \rho \in \mathbb{Z}[i]$ vinden met

$$\alpha = \gamma\beta + \rho \qquad \text{en} \quad N(\rho) < N(\beta)$$

(merk op dat $N(0) = 0$). Deling door β van de gelijkheid laat zien dat $\alpha/\beta = \gamma + \rho/\beta$ en $N(\rho) < N(\beta)$ betekent dat $N(\rho/\beta) < 1$. We kunnen dit interpreteren door te zeggen dat γ een goede benadering, in $\mathbb{Z}[i]$, moet zijn van α/β.

Deling van de complexe getallen α en β (in $\mathbb{C}$) geeft

$$\frac{\alpha}{\beta} = u + vi, \qquad \text{met} \quad u,\, v \in \mathbb{R}$$

(in feite $u,\, v \in \mathbb{Q}$). Kies

$$u',\, v' \in \mathbb{Z} \quad \text{met} \quad |u - u'| \leq \frac{1}{2} \quad \text{en} \quad |v - v'| \leq \frac{1}{2}.$$

Een goede benadering, in $\mathbb{Z}[i]$, van α/β is dan:

$$\gamma = u' + v'i \ \in \mathbb{Z}[i].$$

Defineer vervolgens de "rest" ρ door:

$$\rho = \alpha - \gamma\beta \in \ \mathbb{Z}[i], \qquad \text{dan} \qquad \alpha = \gamma\beta + \rho.$$

Hiermee is een (niet noodzakelijk unieke) manier aangegeven om te delen met rest in $\mathbb{Z}[i]$.

Omdat $N(\alpha)N(\beta) = N(\alpha\beta)$ voor alle complexe getallen, volgt de ongelijkheid $N(\rho) < N(\beta)$ uit $N(\rho/\beta) < 1$:

$$\begin{aligned} N(\frac{\rho}{\beta}) &= N(\frac{\alpha}{\beta} - \gamma) \\ &= N(\,(u-u') + (v-v')i\,) \\ &= (u-u')^2 + (v-v')^2 \\ &\leq (\frac{1}{2})^2 + (\frac{1}{2})^2 \\ &= \frac{1}{2} \\ &< 1\,. \end{aligned}$$

Hiermee is bewezen dat $\mathbb{Z}[i]$ een Euclidische ring is, en uit Stelling 6.10 volgt dat $\mathbb{Z}[i]$ een hoofdideaaldomein is. □

Voorbeeld 6.13. We voeren de deling met rest uit voor

$$\alpha = 5 + 6i, \qquad \beta = 2 + i.$$

Om te beginnen delen we deze getallen in $\mathbb{C}$:

$$\frac{\alpha}{\beta} = \frac{(5+6i)(2-i)}{(2+i)(2-i)} = \frac{16+7i}{5} = (3+\frac{1}{5}) + (1+\frac{2}{5})i.$$

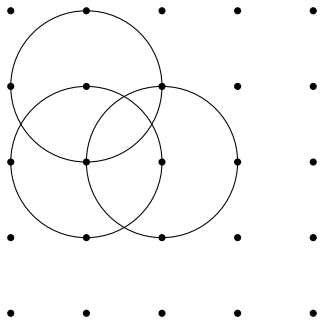
Als "goede benadering" γ nemen we:

$$\gamma = 3 + i \quad \Longrightarrow \rho = \alpha - \gamma\beta = 5 + 6i - (3+i)(2+i) = i.$$

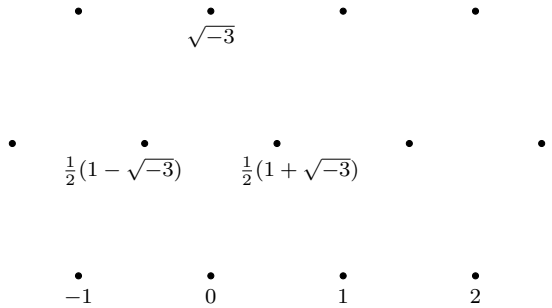
De deling met rest is dus:

$$5 + 6i = (3+i)(2+i) + i, \qquad \text{en inderdaad} \quad N(i) = 1 < 5 = N(2+i).$$

6.14 Het gegeven bewijs van Stelling 6.12 laat zich als volgt meetkundig interpreteren: we hebben nagegaan dat elk complex getal $x(= \frac{\alpha}{\beta}$ in het bewijs) zodanig door een element van $\mathbb{Z}[i]$ kan worden benaderd, dat het verschil absolute waarde < 1 heeft. Met andere woorden: de cirkelschijven met straal 1 en met als middelpunten de elementen van $\mathbb{Z}[i]$, overdekken samen het hele complexe vlak. De juistheid van deze bewering ziet men direct in aan de hand van een plaatje.

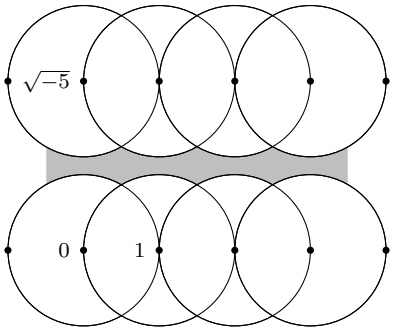


Er zijn verscheidene ringen van hetzelfde soort waarvan op precies dezelfde manier bewezen kan worden dat ze Euclidisch zijn. Dit geldt bijvoorbeeld voor de ring $\mathbb{Z}[\sqrt{-2}]$, en ook voor de ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})] = \left\{a + \frac{1}{2}(1+\sqrt{-3})b \;\middle|\; a, b \in \mathbb{Z}\right\}$. Deze laatste ring vormt in het complexe vlak de verzameling hoekpunten van een regelmatige patroon bestaande uit gelijkzijdige driehoeken.



Het feit dat deze ring Euclidisch is kan gebruikt worden om de *"laatste stelling van Fermat"* voor $n = 3$ te bewijzen: deze stelling zegt dat er geen $x, y, z \in \mathbb{Z}_{>0}$ bestaan met $x^n + y^n = z^n$, als n een geheel getal groter dan 2 is. Fermat beweerde een bewijs hiervoor te hebben, maar het is niet bekend of dat ook echt zo was. Vele wiskundigen en hobbyisten hebben eeuwenlang zonder succes gepoogd de stelling te bewijzen. In juni 1993 kondigde Andrew Wiles aan dat hij, voortbouwend op het werk van een lange rij algebraïci en meetkundigen, daar eindelijk in geslaagd was. In dit eerste bewijs bleek helaas toch nog een probleem te zitten, maar een jaar later wist Wiles dit samen met Richard Taylor te omzeilen. Het uiteindelijke bewijs is verschenen in Annals of Mathematics *142*, (1995).

6.15 De ring $\mathbb{Z}[\sqrt{-5}]$ is geen hoofdideaaldomein, zie opgave 20 op blz. 35, en is daarom zeker niet Euclidisch. De cirkelschijven van straal 1 met de elementen van $\mathbb{Z}[\sqrt{-5}]$ als middelpunten overdekken dan ook niet het gehele complexe vlak.



Op dezelfde wijze als voor $\mathbb{Z}[\sqrt{-5}]$ kan men laten zien dat $\mathbb{Z}[\sqrt{-3}]$ geen hoofdideaaldomein is, dus ook niet Euclidisch. In dit geval blijkt het niet overdekte gedeelte van het complexe vlak uit een stel losse punten te bestaan.

6.16 Ook voor $m > 0$ zijn er Euclidische ringen van de vorm $\mathbb{Z}[\sqrt{m}]$. De ringen $\mathbb{Z}[\sqrt{2}]$ en $\mathbb{Z}[\sqrt{3}]$ zijn bijvoorbeeld Euclidisch, met

$$g(\alpha) = |N(\alpha)|, \qquad \text{met } N \text{ als in 1.14.} \tag{6.16.1}$$

Voor meer voorbeelden zie men de opgaven. De bewijzen zijn steeds analoog aan het bewijs voor $\mathbb{Z}[i]$.

In de rest van dit hoofdstuk is R steeds een Euclidische ring.

6.17 In een hoofdideaaldomein (zoals bijvoorbeeld R, zie Stelling 6.10) geldt voor elke a, $b \in R$ dat het ideaal $(a, b) = aR + bR$ dat ze voortbrengen een hoofdideaal is. Er is dus een d in R met $(a, b) = (d)$ en in het bijzonder geldt $ar + bs = d$ voor zekere r, s in R. We noemen d "de" *grootste gemene deler* van a en b, we schrijven $\text{ggd}(a, b) = d$. Merk op dat d i.h.a. niet uniek bepaald is, als $u \in R$ een eenheid is, dan is $(d) = (ud)$ en ook ud is "de" grootste gemene deler van a en b.

Opmerking 6.18. Een hoofdideaaldomein is ook een ontbindingsring, zie 5.14. In ontbindingsringen hebben we eerder al een ggd gedefinieerd, zie 5.21. Opgave 12 laat zien dat de definities overeenstemmen.

In een Euclidische ring is er een algoritme, het Euclidische algoritme, waarmee de grootste gemene deler bepaald kan worden.

6.19 Laat a, b in een Euclidische ring R geven zijn. Neem aan dat $g(b) \leq g(a)$ (verwissel anders a en b). Delen we met rest, dan vinden we q_0, $r_1 \in R$ zodat:

$$a = q_0 b + r_1 \qquad \text{met} \quad r_1 = 0 \quad \text{of} \quad g(r_1) < g(b).$$

Als $r_1 = 0$, dan is $(a,\, b) = (q_0 b,\, b) = (b)$, waarmee de ggd bepaald is, $\text{ggd}(a, b) = b$. I.h.a. geldt, omdat $a,\, b \in (a,\, b)$, dat ook $r_1 = a - q_0 b \in (a,\, b)$. Er geldt zelfs:

$$(a,\, b) = (q_0 b + r_1,\, b) = (b,\, r_1), \qquad \text{met} \quad g(r_1) < g(b) \leq g(a).$$

We hebben dus "kleinere" voortbrengers b, r_1 van het ideaal $(a,\, b)$ gevonden.

Als $r_1 \neq 0$, dan delen we r_1 op b:

$$b = q_1 r_1 + r_2, \qquad \text{met} \quad r_2 = 0 \;\text{ of }\; g(r_2) < g(r_1).$$

Bovendien geldt:

$$(a,\, b) = (b,\, r_1) = (q_1 r_1 + r_2,\, r_1) = (r_1,\, r_2).$$

Als $r_2 \neq 0$, dan delen we r_2 op r_1:

$$r_1 = q_2 r_2 + r_3 \qquad \text{met} \quad r_3 = 0 \;\text{ of }\; g(r_3) < g(r_2)$$

en $(a,\, b) = (b,\, r_1) = (r_1,\, r_2) = (r_2,\, r_3)$.

Omdat $g(r_k) < g(r_{k-1})$ en $g(r_k) \in \mathbb{Z}_{\geq 0}$ is er na eindig veel stappen een n met

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \qquad \text{en} \quad r_n = 0.$$

Dan geldt:

$$(a, b) = (r_{n-1},\, r_n) = (r_{n-1}), \qquad \text{dus} \quad \text{ggd}(a,\, b) = r_{n-1},$$

waarmee we de ggd van a en b gevonden hebben.

6.20 De elementen r, $s \in R$ met $ar + bs = d$ zijn nu eenvoudig te bepalen.

$$\left.\begin{array}{rcl} a - q_0 b & = & r_1 \\ b - q_1 r_1 & = & r_2 \end{array}\right\} \Longrightarrow\; b - q_1(a - q_0 b) = r_2, \quad \text{ofwel} \quad (-q_1)a + (1 + q_0 q_1)b = r_2,$$

waarbij we de eerste vergelijking in de tweede gesubstitueerd hebben. Algemener, als

$$\left.\begin{array}{rcl} h_{i-1}a + \quad k_{i-1}b & = & r_{i-1} \\ h_i a + \quad\; k_i b & = & r_i \end{array}\right\} \qquad \text{en} \quad r_{i-1} - q_i r_i = r_{i+1},$$

dan volgt door substitutie:

$$(h_{i-1} - q_i h_i)a \;+\; (k_{i-1} - q_i k_i)b = r_{i+1},$$

dus

$$h_{i+1} = (h_{i-1} - q_i h_i), \quad k_{i+1} = (k_{i-1} - q_i k_i)$$

zodat we na een aantal stappen de gewenste schrijfwijze voor de ggd vinden.

Een andere manier om de boekhouding te voeren is door te definiëren:

$$r_{-1} = a, \qquad r_0 = b.$$

Vervolgens merk je op dat de vergelijking $r_{i-1} = q_i r_i + r_{i+1}$ equivalent is met:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$

Door te kijken naar de tweede coördinaat van de vector:

$$\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

vinden we r, s met $r_{n-1} = ra + bs$. Omdat $d = r_{n-1}$ hebben we dus de gezochte schrijfwijze voor de ggd gevonden.

Voorbeeld 6.21. We bepalen met het algoritme de ggd van 84 en 30 in de euclidische ring $\mathbb{Z}$ (dus $g(n) = |n|$). Merk op:

$$84 = 2 \cdot 30 + 24, \qquad 30 = 1 \cdot 24 + 6, \qquad 24 = 4 \cdot 6 + 0,$$

dus $(84, 30) = (30, 24) = (24, 6) = (6)$ en ggd$(84, 30) = 6$. Verder geldt:

$$24 = 84 - 2 \cdot 30, \quad 30 - 1 \cdot 24 = 6 \quad \Longrightarrow \quad 30 - 1 \cdot (84 - 2 \cdot 30) = (-1) \cdot 84 + 3 \cdot 30 = 6,$$

zodat we $r = -1$ en $s = 3$ kunnen nemen.

Voorbeeld 6.22. We gebruiken het Euclidische algoritme om de inverse van een element in een enkelvoudige uitbreiding te berekenen. We doen dit aan de hand van een voorbeeld.

Zij

$$f = X^3 + X^2 - 1 \quad \in \mathbb{Q}[X],$$

dan is f irreducibel omdat hij geen nulpunt in $\mathbb{Z}$ en dus ook niet in $\mathbb{Q}$ heeft. Zij

$$K = \mathbb{Q}[X]/(f), \qquad \alpha = X + (f).$$

Dan is $K = \mathbb{Q}[\alpha]$ een lichaam en elk element van K kan op unieke wijze geschreven worden als

$$a_0 + a_1\alpha + a_2\alpha^2, \qquad a_i \in \mathbb{Q}.$$

We bepalen de inverse van

$$b(\alpha) = 1 + \alpha^2, \qquad \text{met} \quad b = X^2 + 1 \quad (\in \mathbb{Q}[X]).$$

Omdat $\mathbb{Q}[X]$ een hoofdideaaldomein is en f irreducibel is met $\mathrm{gr}(f) > \mathrm{gr}(b)$, is $\mathrm{ggd}(f, b) = 1$. Er zijn dus r, $s \in \mathbb{Q}[X]$ met

$$fr + sb = 1 \quad (\in \mathbb{Q}[X]) \qquad \text{dus} \quad s(\alpha)(\alpha^2 + 1) = 1 \quad (\in K = \mathbb{Q}[X]/(f)),$$

immers $f(\alpha) = 0$. Dus $s(\alpha)$ is de inverse van $b(\alpha) = \alpha^2 + 1$.

Omdat $\mathbb{Q}[X]$ een Euclidische ring is (met $g(f) = \mathrm{gr}(f)$) kunnen we s met het Euclidische algoritme bepalen. Er geldt:

$$X^3 + X^2 - 1 = (X + 1)(X^2 + 1) + (-X - 2), \qquad \text{dus} \quad q_0 = X + 1, \quad r_1 = -(X + 2).$$

Verder is:

$$X^2 + 1 = (-X + 2)(-X - 2) + 5, \qquad \text{dus} \quad q_1 = -X + 2, \quad r_2 = 5.$$

Omdat 5 een eenheid in $\mathbb{Q}[X]$ is, geldt inderdaad dat $\mathrm{ggd}(f, b) = 1$. Deze vergelijkingen kunnen we herschrijven als:

$$-X - 2 = f - (X + 1)b, \qquad 5 = b + (X - 2)(-X - 2).$$

Door de eerste vergelijking in de tweede te substitueren komt er:

$$5 = b + (X - 2)\,(f - (X + 1)b) = (X - 2)f + (1 - (X - 2)(X + 1))\,b.$$

Dit kunnen we schrijven als $rf + sb = 1$ met $r = \frac{1}{5}(X - 2)$ en $s = \frac{1}{5}(3 + X - X^2)$. Substitueren we $X = \alpha$ in deze vergelijking dan zien we dat

$$(\alpha^2 + 1)^{-1} = \frac{1}{5}(3 + \alpha - \alpha^2).$$

Opgaven

1. Laat R een domein zijn en $g\colon R-\{0\}\to\mathbb{Z}_{\geq 0}$ een afbeelding die eigenschap (E2) uit 6.8 heeft. Definieer $g^*\colon R-\{0\}\to\mathbb{Z}_{\geq 0}$ door

$$g^*(b)=\min\bigl\{g(sb)\;\big|\;s\in R-\{0\}\bigr\}.$$

   Bewijs dat g^* eigenschappen (E1) en (E2) uit 6.8 heeft.

2. Zij $\gamma=\frac{1}{2}(1+\sqrt{-19})$, en $R=\mathbb{Z}[\gamma]=\bigl\{a+b\gamma\;\big|\;a,b\in\mathbb{Z}\bigr\}\subset\mathbb{C}$. Definieer

$$N\colon R\longrightarrow\mathbb{Z}_{\geq 0},\qquad N(a+b\gamma)=a^2+ab+5b^2.$$

   (a) Bewijs dat $\gamma^2=\gamma-5$, en dat R een deelring van $\mathbb{C}$ is.

   (b) Bewijs: $N(\alpha\beta)=N(\alpha)N(\beta)$ voor alle $\alpha,\beta\in R$.

   (c) Laat $\alpha\in R$. Bewijs:

$$\alpha\in R^*\iff N(\alpha)=1\iff\alpha\in\{\pm 1\},$$

   dus $R^*=\{1,-1\}$.

   (d) Bewijs dat er geen ringhomomorfismen

$$\varphi\colon R\to\mathbb{F}_2\quad\text{of}\quad\varphi\colon R\to\mathbb{F}_3$$

   bestaan (aanwijzing: gebruik $\gamma^2=\gamma-5$, en kijk waar $\varphi(\gamma)$ aan gelijk zou kunnen zijn).

3. Laat $R=\mathbb{Z}[\gamma]$ zijn als in de vorige opgave. Stel dat $g\colon R-\{0\}\to\mathbb{Z}_{\geq 0}$ voldoet aan de voorwaarde uit 6.8, en kies $b\in R-\{0,1,-1\}$ met $g(b)$ zo klein mogelijk.

   (a) Bewijs dat b geen eenheid is, en dat geldt:

$$\forall a\in R:\;\;\exists r\in\{0,1,-1\}:\quad a\equiv r \bmod Rb\,.$$

   (b) Bewijs: $R/Rb=\{\bar{0},\bar{1},-\bar{1}\}$, met $\bar{r}=(r+Rb)$. Leid hieruit af, dat $R/Rb\cong\mathbb{F}_2$ of $\mathbb{F}_3$.

   (c) Leid met behulp van opgave 2 (d) een tegenspraak af.

   Conclusie van dit vraagstuk: zo'n g bestaat niet, dus R is *niet* Euclidisch.

4. Laten R en N als in Opgave 2 zijn. Als $a,b\in R$, $b\neq 0$, laten we dan zeggen dat de deling met rest mogelijk is voor het paar (a,b), als er $q,r\in R$ bestaan met

$$a=qb+r\quad\text{en}\quad N(r)<N(b).$$

   (a) Stel dat (a,b) een paar elementen van R is, met $b\neq 0$, waarvoor de deling met rest *niet* mogelijk is. Bewijs dat de deling met rest dan *wel* mogelijk is voor $(2a,b)$, en ook voor een van beide paren $(\gamma a,b)$, $((1-\gamma)a,b)$. (Aanwijzing: teken een plaatje).

   (b) Bewijs: $R2+R\gamma=R$, $R2+R(1-\gamma)=R$.

(c) Bewijs dat R een hoofdideaaldomein is (aanwijzing: imiteer het bewijs van 6.10, gebruik makend van a. i.p.v. de eis van 6.8).

5. Definieer $\varphi\colon \mathbb{Z}[i] \to \mathbb{F}_{13}$ door $\varphi(a+bi) = ((a+5b) \bmod 13)$. Bewijs dat φ een homomorfisme is, en dat $\ker(\varphi)$ wordt voortgebracht door 13 en $i-5$. Vind één voortbrenger voor $\ker(\varphi)$.

6. Bereken $\text{ggd}(4+7i, 7-9i)$ in $\mathbb{Z}[i]$, en ontbind $4+7i$ en $7-9i$ in $\mathbb{Z}[i]$ in irreducibele factoren.

7. Zij $n = a^2+b^2$. Bepaal p, q in termen van a en b zodat $2n = p^2+q^2$. Bepaal ook r, s zodat $5n = r^2+s^2$.

8. Bewijs dat de ringen $\mathbb{Z}[\sqrt{m}],\ \ m = -2,\ 2,\ 3$, Euclidisch zijn, met $g(\alpha) = |N(\alpha)|$.

9. Laat zien dat de ringen $\mathbb{Z}[\frac{1}{2}(1+\sqrt{m})],\ m = -11,\ -7,\ -3,\ 5,\ 13$, Euclidisch zijn met

$$g(a+\frac{1}{2}(1+\sqrt{m})b) = |a^2+ab-\frac{m-1}{4}b^2|.$$

(Hint: ga na dat $g(x+y\sqrt{m}) = |(x+y\sqrt{m})(x-y\sqrt{m})|$ als $x,\ y \in \mathbb{Q}$.)

10. Laat $R = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}\,, b \text{ is oneven}\}$. Dit is een deelring van $\mathbb{Q}$.

(a) Bepaal R^*.

(b) Bewijs dat elke $x \in R,\ x \neq 0$, een eenduidige schrijfwijze $x = 2^k \cdot u$ heeft, met $k \in \mathbb{Z}_{\geq 0},\ u \in R^*$.

(c) Laat zien dat de functie

$$g\colon R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}, \qquad g(x) = k \quad \text{als} \quad x = 2^k \cdot u,$$

met x als in b, de ring R tot een Euclidische ring maakt.

(d) Laat zien dat 2, op eenheden na, het enige irreducibele element van R is. Is $2R$ een priemideaal van R ?

11. De ring $R[[X]]$ van *formele machtreeksen* over een ring R bestaat uit alle uitdrukkingen $\sum_{i=0}^{\infty} a_i X^i$ met $a_i \in R$. De optelling en vermenigvuldiging zijn de voor machtreeksen gebruikelijke.

(a) Laat $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$. Bewijs:

$$f \in R[[X]]^* \iff a_0 \in R^*.$$

(b) Stel dat R een *lichaam* is. Definieer

$$g\colon R[[X]] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

door

$$g(\sum_{i=0}^{\infty} a_i X^i) = \min\{i \mid a_i \neq 0\}\,.$$

Bewijs dat deze functie de ring $R[[X]]$ tot een Euclidische ring maakt.

12. Zij R een hoofdideaaldomein, zij $a, b \in R$ met priemontbinding:

$$a = up_1^{n_1} \cdots p_r^{n_r}, \qquad b = vp_1^{m_1} \cdots p_r^{n_r}, \qquad n_i, m_i \in \mathbb{Z}_{\geq 0}.$$

Definieer $d \in R$ als in Definitie 5.21:

$$d = p_1^{k_1} \cdots p_r^{k_r}, \qquad \text{met} \quad k_i = \min\{n_i, m_i\}.$$

Bewijs dat $(a, b) = (d)$ (hint: bekijk het bewijs van Stelling 5.16).

Hoofdstuk 7

Symmetrische polynomen

Laat R een commutatieve ring zijn, en n een geheel getal ≥ 1. Een polynoom $f \in R[X_1, \ldots, X_n]$ heet *symmetrisch* als f in zichzelf overgaat bij *elke* permutatie van $X_1, X_2, \ldots, X_n$. Voorbeelden zijn:

$$\sum_{i=1}^{n} X_i, \qquad \prod_{i=1}^{n} X_i, \qquad \sum_{i=1}^{n} X_i^k \qquad (\text{met } k \in \mathbb{Z}_{\geq 0}).$$

Het polynoom $X_1X_2 + X_2X_3 + X_3X_4 + X_4X_1$ in $\mathbb{Z}[X_1, \ldots, X_4]$ is *niet* symmetrisch: het gaat niet in zichzelf over bij verwisseling van X_1 en X_2.

Werken we, met een nieuwe variabele Z, het polynoom

$$(Z - X_1)(Z - X_2) \cdots (Z - X_n) \in R[X_1, X_2, \ldots, X_n][Z]$$

uit, dan vinden we dat dit gelijk is aan

$$Z^n - \sigma_1 Z^{n-1} + \sigma_2 Z^{n-2} - \cdots + (-1)^{n-1}\sigma_{n-1}Z + (-1)^n\sigma_n$$

waarbij

$$\begin{aligned}
\sigma_1 &= X_1 + X_2 + \cdots + X_n \\
\sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n, \\
\sigma_3 &= X_1X_2X_3 + \cdots = \sum_{1 \leq i < j < k \leq n} X_iX_jX_k, \\
&\vdots \\
\sigma_t &= \sum_{1 \leq i_1 < i_2 < \ldots < i_t \leq n} X_{i_1}X_{i_2} \cdots X_{i_t}, \\
&\vdots \\
\sigma_n &= X_1X_2 \cdots X_n.
\end{aligned}$$

De coëfficiënten $\sigma_1, \sigma_2, \ldots, \sigma_n$ zijn allemaal symmetrische polynomen, de zogenaamde *elementaire symmetrische polynomen*. Uit $\sigma_1, \sigma_2, \ldots, \sigma_n$ kan men andere symmetrische polynomen krijgen door optellen, vermenigvuldigen en het vermenigvuldigen met elementen van R.

Voorbeeld 7.1 (met $n = 2$)**.**

$$\sigma_1 = X_1 + X_2, \qquad \sigma_2 = X_1X_2, \qquad \sigma_1^2 = X_1^2 + 2X_1X_2 + X_2^2,$$

$$\sigma_1^2 - 2\sigma_2 = X_1^2 + X_2^2, \qquad \sigma_1^3 - 3\sigma_1\sigma_2 = X_1^3 + X_2^3, \qquad \text{etcetera.}$$

In het algemeen zien we dat elk polynoom in $\sigma_1, \sigma_2, \ldots, \sigma_n$, met coëfficiënten uit R, een symmetrische polynoom is. Hiervan is de omkering ook waar:

Stelling 7.2 (Hoofdstelling over symmetrische polynomen)**.** *Zij $f \in R[X_1, X_2, \ldots, X_n]$ een symmetrisch polynoom. Dan is f te schrijven als polynoom in $\sigma_1, \sigma_2, \ldots, \sigma_n$ met coëfficiënten uit R. Deze schrijfwijze is bovendien eenduidig.*

Bewijs. Zij $f \neq 0$. Orden de termen $rX_1^{a_2}X_2^{a_2}\cdots X_n^{a_n}$ die in f voorkomen zodanig dat een term $r{\cdot}X_1^{a_1}X_2^{a_2}\cdots X_n^{a_n}$ vóór $r'{\cdot}X_1^{b_1}X_2^{b_2}\cdots X_n^{b_n}$ staat als $a_i > b_i$ voor de kleinste i met $a_i \neq b_i$ ("lexicografische ordening").

De "kopterm"

$$rX_1^{c_1}X_2^{c_2}\cdots X_n^{c_n} \qquad (r \in R,\ r \neq 0)$$

van f heeft dus

$$c_1 = (\text{grootste } a_1 \text{ die in } f \text{ als exponent bij } X_1 \text{ voorkomt}),$$
$$c_2 = (\text{grootste } a_2 \text{ die bij gegeven } a_1 = c_1 \text{ voorkomt}),$$

etcetera. We noemen r de *kopcoëfficiënt* van f.

Omdat f symmetrisch is, geldt $c_1 \geq c_2 \geq \ldots \geq c_n$ anders zou verwisseling van twee der X-en een "eerdere" term van f geven.

We beweren dat het symmetrische polynoom

$$r\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\cdots\sigma_{n-1}^{c_{n-1}-c_n}\sigma_n^{c_n}$$

óók kopterm $rX_1^{c_1}X_2^{c_2}\cdots X_n^{c_n}$ heeft. Immers,

$$\begin{aligned}
&\sigma_1 \text{ heeft kopterm } X_1,\\
&\sigma_2 \text{ heeft kopterm } X_1X_2\\
&\quad\vdots\\
&\sigma_n \text{ heeft kopterm } X_1X_2\cdots X_n
\end{aligned}$$

en maakt men nu gebruik van het regeltje

$$\text{kopterm}(g)\cdot\text{kopterm}(h) = \text{kopterm}(g\cdot h)$$

(geldig voor polynomen g en h met kopcoëfficiënt 1), dan vindt men

$$\begin{aligned}
\text{kopterm}(\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\ldots\sigma_n^{c_n}) &= X_1^{c_1-c_2}\cdot(X_1X_2)^{c_2-c_3}\cdots(X_1X_2\cdots X_n)^{c_n}\\
&= X_1^{c_1}X_2^{c_2}\cdots X_n^{c_n},
\end{aligned}$$

zoals beweerd.

De polynomen f en $r\sigma_1^{c_1-c_2}\cdots\sigma_n^{c_n}$ hebben dezelfde kopterm. Deze valt bij aftrekken weg, dus in

$$f_1 = f - r\sigma_1^{c_1-c_2}\cdots\sigma_n^{c_n}$$

komen alleen maar termen voor die in onze lexicografische ordening later komen.

Als $f_1 = 0$ dan hebben we f op de verlangde wijze uitgedrukt:

$$f = r\sigma_1^{c_1-c_2}\cdots\sigma_n^{c_n}.$$

Als $f_1 \neq 0$, dan merken we op dat f_1 in elk geval weer symmetrisch is, dus we kunnen met f_1 op dezelfde wijze te werk gaan als met f. Dat geeft

$$f_2 = f_1 - r'\sigma_1^{c_1'-c_2'}\cdots\sigma_n^{c_n'}$$

waarbij alle termen van f_2 lexicografisch later komen dan de kopterm $r'X_1^{c_1'}\cdots X_n^{c_n'}$ van f_1. Als $f_2 = 0$ dan zijn we weer klaar:

$$f = r\sigma_1^{c_1-c_2}\cdots\sigma_n^{c_n} + r'\sigma_1^{c_1'-c_2'}\cdots\sigma_n^{c_n'}$$

en anders gaan we verder met f_2.

We moeten bewijzen dat het proces afbreekt, d.w.z. dat we in de rij $f_1, f_2, f_3, \ldots$ op een gegeven ogenblik $f_k = 0$ vinden.

Hiertoe beschouwen we de *totale graad* $\mathrm{totgr}(f)$ van f, d.w.z. de grootste waarde van $a_1+a_2+\ldots+a_n$ die er bij de termen $r\cdot X_1^{a_1}\cdots X_n^{a_n} (\neq 0)$ van f optreedt (vgl. 1.25). Kennelijk geldt: $\mathrm{totgr}(\sigma_i) = i$,

$$\mathrm{totgr}(\sigma_1^{c_1-c_2}\cdots\sigma_n^{c_n}) = c_1 + c_2 + \ldots + c_n \leq \mathrm{totgr}(f),$$

en hieruit volgt

$$\mathrm{totgr}(f_1) \leq \mathrm{totgr}(f)$$

en algemeen

$$\ldots \leq \mathrm{totgr}(f_m) \leq \mathrm{totgr}(f_{m-1}) \leq \ldots \leq \mathrm{totgr}(f)$$

Maar bij gegeven totale graad zijn er slechts eindig veel termen $X_1^{a_1}\cdots X_n^{a_n}$ mogelijk. Bij elke stap in het proces verdwijnt één dergelijke term en blijven slechts lexicografisch latere over. Op een gegeven ogenblik zijn dus alle termen uitgeput, en dan hebben we $f_k = 0$.

Hiermee is de eerste bewering van 7.2 aangetoond. Voordat we op de eenduidigheid ingaan geven we een voorbeeld.

Voorbeeld 7.3. Laat $n = 3$, en

$$f = X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3.$$

De termen staan hier al lexicografisch geordend, en de kopterm $X_1^3X_2$ heeft $c_1 = 3$, $c_2 = 1$ en $c_3 = 0$. Volgens het bovenstaande bewijs moeten we nu van f aftrekken

$$\begin{aligned}\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\sigma_3^{c_3} = \sigma_1^2\sigma_2 &= (X_1+X_2+X_3)^2\cdot(X_1X_2+X_1X_3+X_2X_3)\\ &= X_1^3X_2 + X_1^3X_3 + 2X_1^2X_2^2 + 5X_1^2X_2X_3 + 2X_1^2X_3^2\\ &\quad + X_1X_2^3 + 5X_1X_2^2X_3 + 5X_1X_2X_3^2 + X_1X_3^3 + X_2^3X_3 + 2X_2^2X_3^2 + X_2X_3^3,\end{aligned}$$

en dat levert

$$f_1 = -2X_1^2X_2^2 - 5X_1^2X_2X_3 - 2X_1^2X_3^2 - 5X_1X_2^2X_3 - 5X_1X_2X_3^2 - 2X_2^2X_3^2.$$

Hiervan wordt afgetrokken

$$-2\sigma_2^2 = -2X_1^2X_2^2 - 4X_1^2X_2X_3 - 2X_1^2X_3^2 - 4X_1X_2^2X_3 - 4X_1X_2X_3^2 - 2X_2^2X_3^2,$$

dus

$$f_2 = f_1 - (-2\sigma_2^2) = -X_1^2X_2X_3 - X_1X_2^2X_3 - X_1X_2X_3^2.$$

Trekt men hiervan $-\sigma_1\sigma_3$ af dan blijft nul over, dus al met al hebben we gevonden

$$f = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3.$$

We keren terug naar het bewijs van 7.2. We moeten nog aantonen: als g_1 en g_2 twee *verschillende* polynomen in n variabelen over R zijn, dan zijn ook $g_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ en $g_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$ verschillend. Schrijven we $g = g_1 - g_2$ dan zien we dat het voldoende is om aan te tonen:

$$\text{als } g \in R[Y_1, \ldots, Y_n], g \neq 0, \qquad \text{dan } g(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0.$$

Elke term die in g voorkomt kan in de vorm

$$rY_1^{a_1-a_2} \cdot Y_2^{a_2-a_3} \cdots Y_n^{a_n}$$

geschreven worden, met $r \in R, r \neq 0, a_i \in \mathbb{Z}_{\geq 0}$. Beschouw nu de term waarbij het rijtje $a_1, a_2, \ldots, a_n$ zo vroeg mogelijk komt in de boven geïntroduceerde lexicografische ordening. Substitueert men σ_i voor Y_i, dan geeft deze term een polynoom in $X_1, \ldots, X_n$ met als kopterm

$$rX_1^{a_1}X_2^{a_2} \cdots X_n^{a_n} \tag{7.3.1}$$

en de andere termen $r'\sigma^{a_1'-a_2'} \ldots \sigma_n^{a_n'}$ geven polynomen in $X_1, \ldots, X_n$ met een later komende kopterm. Dus 7.3.1 kan niet wegvallen, en inderdaad $g(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0$. Hiermee is 7.2 bewezen. □

Stelling 7.2 wordt meestal in de volgende situatie toegepast. Laat $f \in R[X_1, \ldots, X_n]$ een symmetrisch polynoom zijn, en $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Omdat f volgens 7.2 is uit te drukken in $\sigma_1, \sigma_2, \ldots, \sigma_n$, is $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ uit te drukken in

$$\begin{aligned}
\sigma_1(\alpha_1, \ldots, \alpha_n) &= \alpha_1 + \cdots + \alpha_n, \\
\sigma_2(\alpha_1, \ldots, \alpha_n) &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \\
&\vdots \\
\sigma_n(\alpha_1, \ldots, \alpha_n) &= \alpha_1\alpha_2 \cdots \alpha_n,
\end{aligned}$$

en dat zijn juist $\pm$ de coëfficiënten van

$$(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n).$$

Informeel betekent dit, dat elke symmetrische uitdrukking in "de n nulpunten" van een monisch polynoom van graad n in één variabele is uit te drukken in de coëfficiënten van dit polynoom. Bijzonder belangwekkend wordt deze bewering, als deze n nulpunten niet in de ring R zelf, maar pas in een uitbreidingsring R' te vinden zijn. We geven eerst een voorbeeld en daarna de algemene stelling.

Voorbeeld 7.4. Laat $h = X^3 - X - 1 \in \mathbb{Z}[X]$. In $\mathbb{Z}$, of zelfs in $\mathbb{Q}$, heeft h geen nulpunten (gebruik methode 5.28(c)), maar zoals blijkt uit Stelling 13.4 zijn er $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ waarvoor geldt

$$(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = h.$$

Coëfficiënten vergelijken levert

$$\begin{aligned}
\sigma_1(\alpha_1, \alpha_2, \alpha_3) &= \alpha_1 + \alpha_2 + \alpha_3 = 0 \\
\sigma_2(\alpha_1, \alpha_2, \alpha_3) &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -1 \\
\sigma_3(\alpha_1, \alpha_2, \alpha_3) &= \alpha_1\alpha_2\alpha_3 = 1.
\end{aligned}$$

Uit 7.2 volgt: is $f \in \mathbb{Z}[X_1, X_2, X_3]$ een willekeurig symmetrisch polynoom, dan geldt $f(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}$ (hoewel $\alpha_1, \alpha_2, \alpha_3 \notin \mathbb{Z}$).

Nemen we voor f het polynoom uit Voorbeeld 7.3

$$f = X_1^3X_2 + X_1^3X_3 + \cdots + X_2X_3^3 = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3$$

dan vinden we

$$\alpha_1^3\alpha_2 + \alpha_1^3\alpha_3 + \cdots + \alpha_2\alpha_3^3 = 0^2 \cdot (-1) - 2 \cdot (-1)^2 - 0 \cdot 1 = -2.$$

Algemeen hebben we de volgende stelling.

Stelling 7.5. *Laat R' een commutatieve ring zijn, en R een deelring van R'. Laat $h \in R[X]$ een* monisch *polynoom van de graad n zijn met de eigenschap dat er $\alpha_1, \alpha_2, \ldots, \alpha_n \in R'$ zijn met*

$$h = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n).$$

Dan geldt voor elk symmetrisch *polynoom $f \in R[X_1, X_2, \ldots, X_n]$ dat*

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in R.$$

Bewijs. Het bewijs van 7.5 is duidelijk uit het voorgaande. Immers, voor elke i geldt:

$$\sigma_i(\alpha_1, \ldots, \alpha_n) \in R$$

omdat het $\pm$ de coëfficiënten van $h \in R[X]$ zijn. Verder weten we uit 7.2 dat het symmetrische polynoom $f \in R[X_1, \ldots, X_n]$ te schrijven is als $f = g(\sigma_1, \ldots, \sigma_n)$ voor zekere $g \in R[X_1, \ldots, X_n]$. Invullen van de α_i in $g(\sigma_1, \ldots, \sigma_n)$ geeft dus een element in R, zoals gewenst. □

Een belangrijk symmetrisch polynoom is

$$D = \prod_{1 \le i < j \le n} (X_i - X_j)^2.$$

De *discriminant* van een polynoom

$$h = X^n + a_1 X^{n-1} + \cdots + a_n = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

is gedefinieerd als

$$\Delta(h) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = D(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Deze kan in $a_1, a_2, \ldots, a_n$ uitgedrukt worden. Zo heeft men voor $n = 2, 3, 4$ de volgende formules:

$$\begin{aligned}
\Delta(X^2 + aX + b) &= a^2 - 4b, \\
\Delta(X^3 + aX^2 + bX + c) &= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc, \\
\Delta(X^4 + aX^3 + bX^2 + cX + d) &= \frac{1}{27}\big(4(b^2 - 3ac + 12d)^3 - (2b^3 - 72bd + 27a^2d - 9abc + 27c^2)^2\big)
\end{aligned}$$

(bij uitwerken blijkt de 27 in de noemer weg te vallen).

Door deze formules kan men de discriminant van een monisch polynoom $h = X^n + a_1 X^{n-1} + \cdots + a_n \in R[X]$ ook definiëren als h niet in $R[X]$ in n factoren $(X - \alpha_i)$ te splitsen is.

De betekenis van de discriminant berust er op, dat voor een domein R geldt

$$\Delta(h) = 0 \iff \exists i < j : \alpha_i = \alpha_j,$$

dus: de discriminant is nul dan en slechts dan als het polynoom een dubbel nulpunt heeft.

Als K een lichaam is met $\mathrm{char}(K) \neq 3$ (zodat $\frac{1}{3} \in K$), geeft de substitutie $X = X - \frac{1}{3}a$ in een derdegraads polynoom $f = X^3 + aX^2 + bX + c$ een derdegraads polynoom $g = X^3 + pX + q$. Merk op dat $\Delta(f) = \Delta(g)$, immers de nulpunten van g zijn $\beta_i = \alpha_i + \frac{1}{3}a$ en $\alpha_i - \alpha_j = \beta_i - \beta_j$. De discriminant van g is eenvoudig: $\Delta(g) = -(4p^3 + 27q^2)$.

Voorbeeld 7.6. We gebruiken de symmetrische polynomen om de nulpunten van een derdegraads polynoom te vinden.

Zij $f \in K[X]$, met K een lichaam met $\mathrm{char}(K) \neq 2, 3$, en $\mathrm{gr}(f) = 3$ een monisch polynoom:

$$f = X^3 + aX^2 + bX + c.$$

Laat $\alpha_1, \alpha_2, \alpha_3$ de nulpunten van f zijn (in een uitbreiding van K, zie 11.1). Dan geldt:

$$\begin{aligned}
-a &= \alpha_1 + \alpha_2 + \alpha_3, \\
b &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\
-c &= \alpha_1\alpha_2\alpha_3.
\end{aligned}$$

Zij ω een primitieve derde eenheidswortel (in een uitbreiding van K, d.w.z. $\omega \neq 1, \omega^3 = 1$). Definieer:

$$\begin{aligned}
A_1 &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \\
A_2 &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3
\end{aligned}$$

We bestuderen wat er met de A_i gebeurt als de α_i gepermuteerd worden. Zij $\rho = (123) \in S_3$, dan:

$$\rho = (123)\colon A_1 \mapsto \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega^2 A_1,$$
$$A_2 \mapsto \alpha_2 + \omega^2\alpha_3 + \omega\alpha_1 = \omega A_2$$

Verder geldt:

$$\tau = (23)\colon A_1 \mapsto A_2, \qquad (23)\colon A_2 \mapsto A_1.$$

Omdat de groep S_3 wordt voortgebracht door ρ en τ zijn

$$A_1^3 + A_2^3, \qquad A_1 A_2$$

symmetrische polynomen in $\alpha_1, \alpha_2, \alpha_3$.

Volgens Stelling 7.2 zijn ze dan uit te drukken in elementair symmetrische funkties σ_i en deze zijn weer, op teken na, gelijk aan de coëfficiënten van f (zie boven). Na enig rekenwerk vindt men:

$$2B = A_1^3 + A_2^3 = -2a^3 + 9ab - 27c,$$
$$A = A_1 A_2 = a^2 - 3b.$$

In het bijzonder zijn A, B direkt te berekenen uit de coëfficiënten van f. Merk op dat:

$$(T - A_1^3)(T - A_2^3) = T^2 - 2BT + A^3,$$

dus we kunnen A_1^3, A_2^3 bepalen:

$$A_i^3 = \frac{2B \pm \sqrt{4B^2 - 4A^3}}{2} = B \pm \sqrt{B^2 - A^3},$$

(we weten overigens niet welke i met welk teken correspondeert). Daarmee kunnen we nu ook A_i bepalen:

$$A_i = \sqrt[3]{B \pm \sqrt{B^2 - A^3}}$$

(hier zijn 3 keuzes voor de derdemachts wortels). Tenslotte bepalen we α_1 door op te merken:

$$3\alpha_1 = (\alpha_1 + \alpha_2 + \alpha_3) + (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) + (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) = -a + A_1 + A_2\,,$$

waarbij we gebruiken dat $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$ en $\omega \neq 1$.

Een expliciet voorbeeld: Zij

$$f = X^3 + 2X^2 - X - 2 \in \mathbb{Q}[X].$$

Dan vinden we:

$$B = 10, \qquad A = 7, \qquad A_1 = \sqrt[3]{10 + \sqrt{10^2 - 7^3}} = \sqrt[3]{10 + 9i\sqrt{3}}$$

(we kozen een + teken, dat blijkt niet belangrijk te zijn). Er zijn 3 oplossingen voor $A_1^3 = 10 + 9i\sqrt{3}$ in $\mathbb{C}$ (gebruik bv. poolcoördinaten voor complexe getallen), en in ons geval blijken die er vrij eenvoudig uit te zien:

$$A_1 = -2 + i\sqrt{3} \qquad \text{of} \qquad A_1 = \frac{1}{2}(-1 + 3i\sqrt{3}) \qquad \text{of} \qquad A_1 = \frac{1}{2}(5 + i\sqrt{3}).$$

Omdat $A_1A_2 = A$ zijn de corresponderende A_2's dan:

$$A_2 = -2 - i\sqrt{3}, \qquad A_2 = \frac{1}{2}(-1 + 3i\sqrt{3}), \qquad A_2 = \frac{1}{2}(5 - i\sqrt{3}).$$

Tenslotte vinden we de drie nulpunten van f uit $\alpha = \frac{1}{3}(-a + A_1 + A_2)$, namelijk -2, -1 en 1.

Deze formules werden, langs een andere weg, gevonden door Cardano en Tartaglia rond 1540. Ze worden de Cardano formules genoemd.

Opgaven

1. Druk het symmetrische polynoom $X_1^3 + X_2^3 + X_3^3$ (met $n = 3$) uit in $\sigma_1, \sigma_2, \sigma_3$.

2. In het bewijs van 7.2 maakten we gebruik van de regel

$$\text{kopterm}(g) \cdot \text{kopterm}(h) = \text{kopterm}(g \cdot h)$$

   voor polynomen g, h waarvan de kopcoëfficiënt 1 is. Laat zien dat de regel fout kan zijn als g, h *nuldelers* als kopcoëfficënten hebben.

3. Laat $(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = X^3 - X - 1$, met $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ en $s_k = \alpha_1^k + \alpha_2^k + \alpha_3^k$ voor $k \in \mathbb{Z}$. Bewijs:

$$s_{-1} = -1, \qquad s_0 = 3, \qquad s_1 = 0,$$

$$\begin{aligned} &s_k = s_{k-2} + s_{k-3} && \text{voor alle } k \in \mathbb{Z}, \\ &s_k \in \mathbb{Z} && \text{voor alle } k \in \mathbb{Z} \text{ (ook negatief!)}. \end{aligned}$$

Deel II

LICHAMEN

Hoofdstuk 8

Priemlichamen en karakteristiek; lineaire algebra

8.1 Laat K een lichaam zijn. Een deelverzameling $K' \subset K$ heet een *deellichaam* als aan de volgende drie voorwaarden is voldaan:

(a) $1 \in K'$,

(b) $a, b \in K' \implies a - b \in K'$,

(c) $a, b \in K',\ b \neq 0 \implies ab^{-1} \in K'$.

Een deellichaam K' van K is, met de op K gedefinieerde bewerkingen, zelf ook een lichaam. Het is gemakkelijk na te gaan dat de doorsnede van een willekeurige collectie deellichamen ook een deellichaam is. De doorsnede van *alle* deellichamen van een lichaam K wordt het *priemlichaam* K_0 van K genoemd:

$$K_0 = \bigcap_{K' \subset K} K',$$

waarbij de doorsnede over alle deellichamen K' van K genomen wordt. Dit is het kleinste deellichaam van K (kleinste m.b.t. de inclusierelatie). Merk op dat $0, 1 \in K_0$.

Stelling 8.2. *Laat K een lichaam zijn. Dan is het priemlichaam van K isomorf met ofwel het lichaam $\mathbb{Q}$ der rationale getallen, danwel een van de lichamen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, met p een priemgetal.*

Bewijs. Laat K_0 het priemlichaam van K zijn. Definieer

$$\kappa \colon \mathbb{Z} \to K_0$$

door

$$\begin{array}{lcll} \kappa(n) & = & 1 + 1 + \cdots + 1 \in K_0 & (n \text{ termen}) \\ \kappa(0) & = & 0 \in K_0 & \\ \kappa(-n) & = & -(1 + 1 + \cdots + 1) \in K_0 & (n \text{ termen}) \end{array}$$

waarbij de 1 in het rechterlid steeds de één van K is. Uit de lichaamsaxioma's volgt op gemakkelijke wijze dat κ een ringhomomorfisme is. Dat $\kappa(\mathbb{Z}) \subset K_0$ volgt uit het feit dat K_0 een lichaam is en $1 \in K_0$.

Het beeld $\kappa(\mathbb{Z})$ is een deelring van K_0. Deze heeft geen nuldelers omdat K_0 een lichaam is. Verder heeft $\kappa(\mathbb{Z})$ een eenheidselement verschillend van nul. We concluderen dat $\kappa(\mathbb{Z})$ een *domein* is. Omdat $\kappa(\mathbb{Z}) \cong \mathbb{Z}/\mathrm{Ker}(\kappa)$ (Stelling 2.23), is $\mathrm{Ker}(\kappa)$ een priemideaal van $\mathbb{Z}$, dus $\mathrm{Ker}(\kappa) = \{0\}$ of $\mathrm{Ker}(\kappa) = p\mathbb{Z}$, waarbij p een priemgetal is.

Laat eerst $\mathrm{Ker}(\kappa) = 0$. Dan is κ injectief, en $\kappa(\mathbb{Z}) \cong \mathbb{Z}$. We kunnen κ voortzetten tot een functie

$$\kappa_1 \colon \mathbb{Q} \to K_0, \qquad \kappa_1(a/b) = \kappa(a) \cdot (\kappa(b))^{-1}, \quad (a,\, b \in \mathbb{Z},\ b \neq 0).$$

Men gaat gemakkelijk na dat dit een goed gedefinieerde afbeelding is, en dat $\kappa_1 \colon \mathbb{Q} \to K_0$ een lichaamshomomorfisme is. Wegens Gevolg 2.18 is κ_1 injectief, dus $\mathbb{Q} \cong \kappa_1(\mathbb{Q})$, en $\kappa_1(\mathbb{Q})$ is een deellichaam dat in K_0 bevat is. Maar K_0 is het kleinste deellichaam van K, dus noodzakelijkerwijze $K_0 = \kappa_1(\mathbb{Q}) \cong \mathbb{Q}$.

Veronderstel vervolgens dat $\mathrm{Ker}(\kappa) = p\mathbb{Z}$, waarbij p een priemgetal is. Dan is $\kappa(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, hetgeen volgens Stelling 1.20 een lichaam is. Dus $\kappa(\mathbb{Z})$ is een deellichaam van K dat in K_0 bevat is, hetgeen weer alleen kan als $\kappa(\mathbb{Z}) = K_0$, dus inderdaad $K_0 \cong \mathbb{Z}/p\mathbb{Z}$. □

Definitie 8.3. Laat K een lichaam zijn met priemlichaam K_0. Als $K_0 \cong \mathbb{Q}$ zeggen we dat K *karakteristiek nul* heeft, notatie $\mathrm{char}(K) = 0$. Als $K_0 \cong \mathbb{F}_p$ zeggen we dat K *karakteristiek* p heeft, notatie $\mathrm{char}(K) = p$.

We zien dat in beide gevallen $\mathrm{char}(K)$ de niet-negatieve voortbrenger van het ideaal $\mathrm{Ker}(\kappa) \subset \mathbb{Z}$ is, waarin $\kappa \colon \mathbb{Z} \to K$ het unieke ringhomomorfisme is. Op deze wijze kan men $\mathrm{char}(R)$ definiëren voor een willekeurige ring R; als R geen domein is kan het gebeuren dat $\mathrm{char}(R)$ niet een priemgetal of nul is.

Stelling 8.4. *Laat K een lichaam zijn met* $\mathrm{char}(K) = p > 0$. *Dan geldt voor alle $a,\, b \in K$ en alle $n \in \mathbb{Z}_{\geq 0}$:*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}\,, \qquad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

Bewijs. Het is voldoende alleen de eerste formule te bewijzen, want de tweede volgt er direct uit. (Substitueer $a - b$ voor a in de eerste formule.)

Laat eerst $n = 1$. Volgens het binomium van Newton, dat geldig is in iedere commutatieve ring (zie Opgave 12 in Hoofdstuk 1), hebben we

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}, \quad \text{waarbij} \quad \binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}\,.$$

Als $0 < k < p$ dan is de teller van $\binom{p}{k}$ deelbaar door p, maar de noemer niet, omdat p een priemgetal is. Dus $\binom{p}{k}$ is deelbaar door p voor $0 < k < p$ en we vinden dat

$$(a+b)^p = a^p + b^p + p \cdot c\,,$$

voor zekere $c \in K$. Maar

$$\begin{aligned} p \cdot c &= c + c + \cdots + c \qquad (p \text{ termen}) \\ &= (1 + 1 + \cdots + 1) \cdot c \\ &= 0 \cdot c = 0 \end{aligned}$$

dus inderdaad $(a+b)^p = a^p + b^p$.

Het algemene geval gaat nu met volledige inductie naar n:

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

Hiermee is 8.4 bewezen. □

Voor een bewijs dat geen gebruik maakt van het binomium van Newton, zie Opgave 4.

Gevolg 8.5. *Zij K een lichaam met* $\mathrm{char}(K) = p > 0$. *Dan is de afbeelding $F\colon K \to K$ gedefinieerd door $F(x) = x^p$ een lichaamshomomorfisme van K naar zichzelf. Verder is F injectief, en als K eindig is, is F zelfs een lichaamsautomorfisme.*

Bewijs. Er geldt $F(1) = 1$. Uit $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$ (want K is commutatief) en $F(a+b) = (a+b)^p$ (Stelling 8.4 met $n = 1$) blijkt dat F een lichaamshomomorfisme is. Wegens 2.18 is F injectief. Omdat elke injectieve afbeelding van een eindige verzameling naar zichzelf bijectief is, is F bijectief in het geval K eindig is. Hiermee is 8.5 bewezen. □

De laatste zin van 8.5 kan men ook zo formuleren: in een lichaam van karakteristiek $p > 0$ heeft elk element ten hoogste één p-de machts wortel, en in een eindig lichaam van karakteristiek p heeft elk element precies één p-de machts wortel.

De afbeelding F uit 8.5 wordt het *Frobenius-homomorfisme* (Georg Frobenius, Duits wiskundige, 1849–1917) genoemd. Als F bijectief is dan wordt het lichaam K *perfect* genoemd. Ook lichamen van karakteristiek nul worden perfect genoemd.

Voorbeeld 8.6. Zij $K = \mathbb{F}_p(T)$, het lichaam van rationale functies in één variabele met coëfficiënten in $\mathbb{F}_p$. Als $f(T) = \frac{a_0+a_1T+\cdots+a_nT^n}{b_0+b_1T+\cdots+b_mT^m} \in \mathbb{F}_p(T)$ dan is

$$\begin{aligned} F(f(T)) &= F\left(\frac{a_0 + a_1T + \cdots + a_nT^n}{b_0 + b_1T + \cdots + b_mT^m}\right) \\ &= \frac{F(a_0 + a_1T + \cdots + a_nT^n)}{F(b_0 + b_1T + \cdots + b_mT^m)} \\ &= \frac{F(a_0) + F(a_1)F(T) + \cdots + F(a_n)F(T^n)}{F(b_0) + F(b_1)F(T) + \cdots + F(b_m)F(T^m)} \\ &= \frac{a_0 + a_1T^p + \cdots + a_nT^{pn}}{b_0 + b_1T^p + \cdots + b_mT^{pm}} = f(T^p), \end{aligned}$$

want $F(a) = a$ voor alle $a \in \mathbb{F}_p$, het priemlichaam van $\mathbb{F}_p(T)$. Het beeld van het Frobeniushomomorfisme F bestaat dan precies uit alle rationale functies in de variabele T^p met coëfficiënten in $\mathbb{F}_p$. Daarom is F niet surjectief op $\mathbb{F}_p(T)$, immers $T \notin \mathrm{Im}(F)$. In het bijzonder is het lichaam $\mathbb{F}_p(T)$ niet perfect.

We besluiten dit hoofdstuk met enkele resultaten over vectorruimten, die in het geval $K = \mathbb{R}$ welbekend zijn uit de lineaire algebra. De bewijzen zijn identiek aan die in het geval $K = \mathbb{R}$, en we zullen deze niet herhalen. Het enige dat terzake doet is dat K een *lichaam* is. (Voor vele resultaten kan men zelfs de commutativiteit van K laten vallen.)

8.7 Laat K een lichaam zijn. Een *vectorruimte over* K is een additief geschreven abelse groep V samen met een afbeelding $K \times V \to V$ die aan elk paar $(\lambda, v) \in K \times V$ een "scalair product" $\lambda v \in V$ toevoegt, zodanig dat aan de volgende voorwaarden voldaan is:

(V1) $\lambda(v + w) = \lambda v + \lambda w$

(V2) $(\lambda + \mu)v = \lambda v + \mu v$

(V3) $\lambda(\mu v) = (\lambda\mu)v$

(V4) $1 \cdot v = v$

voor alle λ, $\mu \in K$ en v, $w \in V$.

Is K geen lichaam maar enkel een ring, dan spreken we van *modulen* in plaats van vectorruimten.

De vectorruimte V heet *eindig dimensionaal* over K als er een eindig aantal elementen $v_1, \ldots, v_m \in V$ is met de eigenschap dat elke $v \in V$ geschreven kan worden in de vorm

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m \qquad \lambda_1, \ldots, \lambda_m \in K\,.$$

Als deze uitdrukking voor elke $v \in V$ eenduidig bepaald is, heet $v_1, \ldots, v_m$ een *basis* van V over K. Elke eindig dimensionale vectorruimte heeft een basis, en alle bases hebben evenveel elementen. Het aantal elementen van een basis heet de *dimensie* van V over K, notatie $\dim_K(V)$ of $\dim(V)$.

Voor elke $m \in \mathbb{Z}_{\geq 0}$ wordt een vectorruimte van dimensie m over K gegeven door

$$K^m = \left\{(x_1, x_2, \ldots, x_m) \;\middle|\; x_1, x_2, \ldots, x_m \in K\right\}$$

met scalairvermenigvuldiging

$$\lambda \cdot (x_1, x_2, \ldots, x_m) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_m)$$

en componentsgewijze optelling. Elke vectorruimte van dimensie m over K is isomorf met K^m; het formuleren van de voor de hand liggende definitie van "isomorf" en "isomorfisme" laten we hierbij aan de lezer over, evenals voor "homomorfisme" en "endomorfisme".

Laat V een m-dimensionale vectorruimte over K zijn. Een stelsel vectoren $w_1, w_2, \ldots, w_k$ heet *lineair onafhankelijk* over K als voor alle $\lambda_1, \lambda_2, \ldots, \lambda_k \in K$ geldt:

$$\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_k w_k = 0 \implies \lambda_1 = \lambda_2 = \cdots = \lambda_k = 0\,.$$

Zo'n lineair onafhankelijk stelsel kan steeds worden aangevuld tot een basis; dus $k \leq m$. Hieruit volgt dat elke deelvectorruimte (d.w.z., een ondergroep $W \subset V$ zo dat voor alle $w \in W$ en $\lambda \in K$ geldt $\lambda w \in W$) dimensie $\leq m$ heeft: $\dim(W) \leq \dim(V)$, of preciezer: $\dim(V) = \dim(W) + \dim(V/W)$, waarbij de groep V/W op natuurlijke wijze weer een vectorruimte is.

Voor de bewijzen van deze en andere beweringen verwijzen we naar het college lineaire algebra. Einige voorzichtigheid is wel te betrachten: een aantal stellingen betreffende kwadratische vormen, inproducten en lengtes van vectoren is wel voor het geval $K = \mathbb{R}$ geldig, maar niet algemeen.

Opgaven

1. Laat K een lichaam zijn en $\sigma\colon K \to K$ een lichaamshomomorfisme.
   (a) Bewijs dat $K^\sigma = \{x \in K \mid \sigma(x) = x\}$ een deellichaam van K is.
   (b) Wat is K^σ in het geval dat $K = \mathbb{C}$ en $\sigma =$ complexe conjugatie ?
   (c) Leid uit (a) af, dat $\sigma(x) = x$ voor alle $x \in K_0$, het priemlichaam van K
2. Laat $f\colon K \to L$ een lichaamshomomorfisme zijn. Bewijs dat f een isomorfisme van het priemlichaam van K met dat van L induceert, en dat K en L dezelfde karakteristiek hebben.
3. Laat K een eindig lichaam zijn. Bewijs dat $\mathrm{char}(K) \neq 0$.
4. Laat K een lichaam zijn met $\mathrm{char}(K) = p > 0$, en laat $f = (X+1)^p - X^p - 1 \in K[X]$.
   (a) Laat zien met behulp van de Kleine Stelling van Fermat, dat $f(a) = 0$ voor alle $a \in \mathbb{F}_p \subset K$.
   (b) Toon aan dat de graad van f kleiner dan p is.
   (c) Concludeer dat $f = 0$.
   (d) Bewijs dat $(a+b)^p = a^p + b^p$ door ab^{-1} voor X te substitueren in f.
5. Laat K een lichaam van karakteristiek $p >$ zijn en $n \in \mathbb{Z}_{>0}$. Bewijs dat $\{x \in K \mid x^{p^n} = x\}$ een deellichaam van K is dat ten hoogste p^n elementen bevat.
6. Zij σ een lichaamsautomorfisme van het lichaam $\mathbb{R}$ der reële getallen.
   (a) Bewijs: $\sigma(x) = x$ voor alle $x \in \mathbb{Q}$.
   (b) Bewijs: $x \geq 0 \implies \sigma(x) \geq 0$.
   (c) Bewijs: $\sigma = \mathrm{id}_{\mathbb{R}}$.
7. Bewijs dat $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ een deellichaam van $\mathbb{R}$ is. Bewijs ook dat de afbeelding $\sigma\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ gegeven door $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ een lichaamsautomorfisme van $\mathbb{Q}(\sqrt{2})$ is, en dat het het enige lichaamsautomorfisme van $\mathbb{Q}(\sqrt{2})$ is behalve $\mathrm{id}_{\mathbb{Q}(\sqrt{2})}$.

Hoofdstuk 9

Enkelvoudige uitbreidingen

9.1 Een *uitbreiding* of *lichaamsuitbreiding* van een lichaam K is een lichaam L waarin K als deellichaam bevat is. Laat L een uitbreiding van K zijn, en $\alpha \in L$. We noteren

$$K[\alpha] = \left\{ a_0 + a_1\alpha + \cdots + a_n\alpha^n \;\middle|\; n \in \mathbb{Z}_{\geq 0}\,, a_0, \ldots, a_n \in K \right\};$$

dit is een deelring van L, en wel de kleinste deelring waar zowel K als α in zitten; voorts

$$K(\alpha) = \left\{ x/y \;\middle|\; x, y \in K[\alpha]\,, y \neq 0 \right\};$$

dit is een deellichaam van L, en wel het kleinste deellichaam waar zowel K als α in zitten. Een lichaam van de vorm $K(\alpha)$ heet een *enkelvoudige uitbreiding* van K, en men zegt dat $K(\alpha)$ uit K verkregen wordt door het *adjungeren* van α.

Als L een uitbreiding van een lichaam K is, dan kunnen we L als vectorruimte over K opvatten door voor het scalaire product λv (met $\lambda \in K$ en $v \in L$) het product van λ en v in het lichaam L te nemen.

Voorbeelden 9.2. (a) Laat $K = \mathbb{R}$ en neem $L = \mathbb{C}$ en $\alpha = i$. Er geldt $\mathbb{R}[i] = \mathbb{C}$, en dit is een lichaam, dus ook geldt $\mathbb{R}(i) = \mathbb{C}$.

(b) Laat $K = \mathbb{Q}$ en $\alpha = \sqrt{2}$. Uit $\sqrt{2}^2 = 2$ volgt dat $\mathbb{Q}\big[\sqrt{2}\big] = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\}$. Dit is een lichaam, want

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

voor a, $b \in \mathbb{Q}$ niet beide nul (en merk op dat in dat geval ook $a^2 - 2b^2 \neq 0$). Hieruit volgt dat $\mathbb{Q}\big[\sqrt{2}\big] = \mathbb{Q}\big(\sqrt{2}\big)$.

(c) Uit $\sqrt[3]{2}^3 = 2$ blijkt dat $\mathbb{Q}\big[\sqrt[3]{2}\big] = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \;\middle|\; a, b, c \in \mathbb{Q} \right\}$. We beweren dat dit opnieuw een lichaam is, zodat geldt $\mathbb{Q}\big[\sqrt[3]{2}\big] = \mathbb{Q}\big(\sqrt[3]{2}\big)$. Om dit te bewijzen, is het voldoende om aan te tonen dat

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} \in \mathbb{Q}\big[\sqrt[3]{2}\big]$$

voor a, b, $c \in \mathbb{Q}$ niet alledrie gelijk aan nul. In het geval $c = 0$ ziet men dit door teller en noemer met $a^2 - ab\sqrt[3]{2} + b^2\sqrt[3]{4}$ te vermenigvuldigen. In het geval $c \neq 0$ vermenigvuldigt men teller en noemer eerst met $b - c\sqrt[3]{2}$, waardoor dit geval op het vorige wordt teruggebracht.

We zien dus dat in vele gevallen geldt dat $K[\alpha] = K(\alpha)$. In dit hoofdstuk zullen we algemeen de structuur van enkelvoudige uitbreidingen $K(\alpha)$ van K bestuderen. We zullen zien dat in het algemeen de gelijkheid $K[\alpha] = K(\alpha)$ geldt, als α algebraïsch over K is, in de zin van de volgende definitie.

Definitie 9.3. Laat L een uitbreiding van een lichaam K zijn, en $\alpha \in L$. Als er een polynoom $f \in K[X]$ met $f \neq 0$ bestaat waarvoor $f(\alpha) = 0$, dan zeggen we dat α *algebraïsch* over K is. Als er niet zo'n f bestaat, dan heet α *transcendent* over K.

9.4 Voorbeelden van algebraïsche elementen. Elk element α van K zelf is algebraïsch over K: neem $f = X - \alpha$. Het complexe getal i is algebraïsch over $\mathbb{R}$, want $f(i) = 0$ voor $f = X^2 + 1$. In feite is *ieder* complex getal $a + bi$ (met a, $b \in \mathbb{R}$) algebraïsch over $\mathbb{R}$: neem $f = X^2 - 2aX + (a^2 + b^2)$. De getallen $\sqrt{2}$ en $\sqrt[3]{2}$ zijn algebraïsch over $\mathbb{Q}$: neem $f = X^2 - 2$, respectievelijk $f = X^3 - 2$.

9.5 Voorbeelden van transcendente elementen. Nemen we $L = K(X)$, en $\alpha = X \in K(X)$ dan hebben we een eenvoudig voorbeeld van een enkelvoudige uitbreiding L van K met een transcendente α.

Een complex of reëel getal heet transcendent (zonder meer) als het transcendent over $\mathbb{Q}$ is. Met een telargument (zie Opgave 2) kan men laten zien dat er transcendente getallen bestaan, maar het is lastig er expliciet een op te schrijven. Dit werd voor het eerst gedaan door Liouville (Joseph Liouville, Frans wiskundige, 1809–1882) die aantoonde dat $\sum_{k=1}^{\infty} 10^{-k!}$ transcendent is. Tegenwoordig is ook bekend dat een getal als $0,12345678910111213\ldots$ transcendent is. In 1873 werd door Hermite (Charles Hermite, Frans wiskundige, 1822–1901) bewezen dat het getal e, de basis der natuurlijke logarithmen, transcendent is, en in 1882 deed Lindemann (Carl Louis Ferdinand von Lindemann, Duits wiskundige, 1852–1939) hetzelfde voor π, de halve omtrek van een cirkel met straal 1. Literatuur hierover: I. Stewart, Galois Theory, Ch. 6.

Stelling 9.6. *Laat L een uitbreiding van een lichaam K zijn, en zij $\alpha \in L$ transcendent over K. Dan is de ring $K[\alpha]$ isomorf met $K[X]$, de polynoomring in één variabele over K, en $K(\alpha)$ is isomorf met het quotiëntenlichaam $K(X)$ van $K[X]$.*

Bewijs. Definieer $\psi\colon K[X] \to K[\alpha]$ door $\psi(f) = f(\alpha)$, d.w.z.,

$$\psi(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n\,.$$

Dit is een ringhomomorfisme, dat wegens de definitie van $K[\alpha]$ surjectief is. Omdat α transcendent over K is, geldt $\psi(f) = 0$ alleen voor $f = 0$, dus $\mathrm{Ker}(\psi) = \{0\}$ en ψ is injectief. We concluderen dat $\psi\colon K[X] \to K[\alpha]$ het verlangde isomorfisme is. We laten het aan de lezer over, te controleren dat de afbeelding $K(X) \to K(\alpha)$ gegeven door $f/g \mapsto \psi(f)/\psi(g)$ (voor f, $g \in K[X]$ en $g \neq 0$) welgedefinieerd is, en een isomorfisme van lichamen $K(X) \cong K(\alpha)$ levert. □

9.7 Vervolgens beschouwen we het geval dat α algebraïsch over K is. Dan zijn er $a_0, a_1, \ldots, a_n \in K$ met $n \in \mathbb{Z}_{>0}$ en $a_n \neq 0$, waarvoor geldt

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0\,.$$

Kies nu een dergelijke relatie waarin n zo klein mogelijk is. Door met a_n^{-1} te vermenigvuldigen mogen we aannemen dat $a_n = 1$. We beweren dat alle a_i nu vastliggen. Immers, als we ook zouden hebben

$$a'_0 + a'_1\alpha + a'_2\alpha^2 + \cdots + a'_n\alpha^n = 0 \qquad \text{met } a'_i \in K \text{ en } a'_n = 1$$

waarin niet voor alle i zou gelden dat $a_i = a'_i$, dan zouden we door deze relatie van de vorige af te trekken een relatie vinden waarvan de hoogstegraads term graad *kleiner* dan n heeft (want $a_n - a'_n = 1-1 = 0$), in tegenspraak met de keuze van n. We concluderen dat er onder alle niet-nul polynomen $f \in K[X]$ van minimale graad n waarvoor $f(\alpha) = 0$, zich precies één bevindt waarvan de kopcoëfficiënt 1 is, d.w.z., die monisch is. Dit polynoom heet het *minimumpolynoom van α over K*, notatie f_K^α.

Voorbeelden:

$$f_{\mathbb{Q}}^{\sqrt{2}} = X^2 - 2\,, \quad f_{\mathbb{R}}^{\sqrt{2}} = X - \sqrt{2}\,.$$

Een andere manier om het voorgaande te belichten, is door te kijken naar het evaluatiehomomorfisme $\psi\colon K[X] \to K[\alpha]$ gegeven door $\psi(f) = f(\alpha)$. Uit Gevolg 3.4 weten we dat $\mathrm{Ker}(\psi)$ een hoofdideaal is, en de aanname dat α algebraïsch over K is, betekent precies dat $\mathrm{Ker}(\psi) \neq \{0\}$. Het minimumpolynoom f_K^α is dan de unieke monische voortbrenger van het ideaal $\mathrm{Ker}(\psi)$. (De constructie hierboven maakt duidelijk, dat f_K^α een polynoom van minimale graad in $\mathrm{Ker}(\psi)$ is; zoals reeds opgemerkt na het bewijs van Gevolg 3.4, volgt hieruit dat f_K^α inderdaad een voortbrenger is van $\mathrm{Ker}(\psi)$.)

Stelling 9.8. *Laat L een uitbreiding van een lichaam K zijn, en zij $\alpha \in L$ algebraïsch over K met minimumpolynoom $f_K^\alpha \in K[X]$.*

(a) *Het minimumpolynoom f_K^α is irreducibel in $K[X]$ en f_K^α is het enige monische irreducibele polynoom $f \in K[X]$ met $f(\alpha) = 0$.*

(b) *Voor elke $g \in K[X]$ geldt: $g(\alpha) = 0 \iff g$ is deelbaar door f in $K[X]$.*

(c) *Er geldt $K[\alpha] = K(\alpha)$ en $K(\alpha) \cong K[X]/(f_K^\alpha)$.*

(d) *Als vectorruimte over K is $K(\alpha)$ eindig-dimensionaal, $\dim_K\big(K(\alpha)\big) = \mathrm{gr}(f_K^\alpha)$, en een basis van $K(\alpha)$ over K wordt gevormd door $1, \alpha, \ldots, \alpha^{n-1}$ met $n = \mathrm{gr}(f_K^\alpha)$.*

Bewijs. Het evaluatiehomomorfisme $\psi\colon K[X] \to K[\alpha]$ gegeven door $\psi(f) = f(\alpha)$ is surjectief, per definitie van $K[\alpha]$. Bewering (b) is een herformulering van het feit dat f_K^α een voortbrenger is van $\mathrm{Ker}(\psi)$. De eerste isomorfiestelling geeft dan een isomorfisme

$$K[X]/(f_K^\alpha) \cong K[\alpha]\,.$$

Omdat $K[\alpha]$ een domein is (het is een deelring van een lichaam), volgt dat (f_K^α) een priemideaal is. Maar $K[X]$ is een hoofdideaaldomein (Gevolg 3.4), dus uit Stelling 5.8 volgt dat f_K^α irreducibel is en dat (f_K^α) zelfs een maximaal ideaal is. Dus $K[\alpha] \cong K[X]/(f_K^\alpha)$ is een lichaam, waaruit blijkt dat $K[\alpha] = K(\alpha)$. De tweede uitspraak in (a) volgt nu onmiddellijk uit (b).

Om (d) te bewijzen merken we op elk element $y \in K[\alpha] = K(\alpha)$ te schrijven is als $y = g(\alpha)$ voor een polynoom $g \in K[X]$. Deling met rest (Stelling 3.1) geeft het bestaan van polynomen q en r zo dat $g = q \cdot f_K^\alpha + r$ en $r = 0$ of $\mathrm{gr}(r) < n = \mathrm{gr}(f)$. Substitueren we $X = \alpha$ dan vinden we dat $y = g(\alpha) = q(\alpha) \cdot f_K^\alpha(\alpha) + r(\alpha) = r(\alpha)$. Dit bewijst dat elk element van $K[\alpha] = K(\alpha)$ te schrijven is als een lineaire combinatie $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$. Anderzijds zijn de elementen

$1, \alpha, \ldots, \alpha^{n-1}$ lineair onafhankelijk, want als er $b_0, b_1, \ldots, b_{n-1} \in K$ bestonden, niet allemaal nul, zo dat $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$ dan zou dit een tegenspraak geven met de aanname dat n de minimale graad is van een polynoom f met $f(\alpha) = 0$. Dus $1, \alpha, \ldots, \alpha^{n-1}$ is een basis van de vectorruimte $K(\alpha)$ over K. □

Opmerking 9.9. Merk op dat het onderscheid transcendent/algebraïsch in deze paragraaf analoog is aan het onderscheid karakteristiek nul/karakteristiek $p > 0$ in Stelling 8.2. In deze analogie correspondeert het evaluatiehomomorfisme $\psi\colon K[X] \to K[\alpha]$ in de bewijzen van 9.6 en 9.8 met het ringhomomorfisme $\kappa\colon \mathbb{Z} \to K, \quad \kappa(1) = 1$ in het bewijs van 8.2, en f_K^α correspondeert met p.

9.10 Rekenen in $K(\alpha)$. Laat weer L een uitbreiding van een lichaam K zijn, $\alpha \in L$ algebraïsch over K, en zij $n = \mathrm{gr}(f_K^\alpha)$. Volgens 9.8(d) kan elk element van $K(\alpha)$ eenduidig worden geschreven als

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} \qquad \text{met } b_i \in K \text{ voor } i = 0, \ldots, n-1.$$

We gaan nu na hoe de rekenkundige bewerkingen $+$, $-$, $\times$ en $:$ op deze uitdrukkingen uitgevoerd moeten worden. Optelling is eenvoudig:

$$\begin{aligned}\big(b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}\big) + \big(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}\big)& \\ = (b_0 + c_0) + (b_1 + c_1)\alpha + (b_2 + c_2)\alpha^2 + \cdots + (b_{n-1} + c_{n-1})\alpha^{n-1}&\end{aligned}$$

en analoog voor aftrekken. Vermenigvuldigen is iets ingewikkelder. Werkt men een product

$$\big(b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}\big) \cdot \big(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}\big) \tag{9.10.1}$$

met behulp van de distributieve wet uit, dan krijgt men een uitdrukking

$$d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_{2n-3}\alpha^{2n-3} + d_{2n-2}\alpha^{2n-2} \tag{9.10.2}$$

met

$$d_0 = b_0c_0\,, \quad d_1 = b_0c_1 + b_1c_0\,, \ldots\,, d_{2n-2} = b_{n-1}c_{n-1}$$

waarvan de graad in α tot $2n-2$ kan oplopen. Om de graad weer kleiner te maken, maakt men gebruik van de relatie $f_K^\alpha(\alpha) = 0$. Schrijven we

$$f_K^\alpha = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + X^n$$

dan mogen we van (9.10.2) $d_{2n-2}\alpha^{2n-2} \cdot f_K^\alpha(\alpha) = 0$ aftrekken en dit geeft een uitdrukking van graad ten hoogste $2n-3$ in α. Door dit te herhalen, vinden we uiteindelijk een uitdrukking in α van graad ten hoogste $n-1$.

De hier geschetste methode is niet veel anders dan de deling met rest die we in het bewijs van 9.8(d) gebruikt hebben. Inderdaad kunnen we het polynoom $g = d_0 + d_1X + d_2X^2 + \cdots + d_{2n-3}X^{2n-3} + d_{2n-2}X^{2n-2}$ schrijven in de vorm $q \cdot f_K^\alpha + r$ met $r = 0$ of $\mathrm{gr}(r) \leq n-1$, en $r(\alpha)$ is dan de gezochte uitdrukking van het product in (9.10.1) als lineaire combinatie van $1, \alpha, \ldots, \alpha^{n-1}$.

Tenslotte geven we aan hoe een quotiënt

$$\big(b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}\big)/\big(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}\big)$$

(niet alle c_i gelijk aan nul) berekend kan worden. Eén methode maakt gebruik van technieken uit de lineaire algebra, en gaat als volgt. Indien we $x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}$ voor het quotiënt schrijven, dan dienen $x_0, x_1, \ldots, x_{n-1}$ opgelost te worden uit de vergelijking

$$\big(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}\big) \cdot \big(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}\big) = \big(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}\big)$$

Vermenigvuldig nu het linkerlid uit, en schrijf het door de relatie $f_K^\alpha(\alpha) = 0$ te gebruiken als lineaire combinatie van $1, \alpha, \ldots, \alpha^{n-1}$ met coëfficiënten die lineaire functies van $x_0, x_1, \ldots, x_{n-1}$ zijn. Vergelijken we nu links en rechts de coëfficiënten bij α^i, voor $i = 0, 1, \ldots, n-1$, dan vinden we n lineaire vergelijkingen waar $x_0, x_1, \ldots, x_{n-1}$ aan moeten voldoen, en dit stelsel kan met de methoden van de lineaire algebra worden opgelost.

Een tweede methode om de deling uit te voeren is de volgende. Omdat we al kunnen vermenigvuldigen, is het voldoende te laten zien hoe men de *inverse* van $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ kan bepalen.

Schrijf $h = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$; de vraag is $h(\alpha)^{-1}$ te bepalen. Omdat h een kleinere graad dan $f = f_K^\alpha$ heeft, en $h \neq 0$, is h in $K[X]$ niet deelbaar door f. Maar f is irreducibel, dus dit betekent dat f en h onderling ondeelbaar zijn. Het feit dat $K[X]$ een hoofdideaaldomein is (Gevolg 3.4) impliceert dus dat er λ, $\mu \in K[X]$ bestaan met $\lambda f + \mu h = 1$. Substitueer α voor X in deze relatie. Wegens $f(\alpha) = 0$ vinden we dan

$$\mu(\alpha) \cdot h(\alpha) = 1\,,$$

dus $\mu(\alpha) = h(\alpha)^{-1}$. Merk op dat we hiermee het *bestaan* van $g(\alpha)^{-1}$, dus de gelijkheid $K[\alpha] = K(\alpha)$ uit 9.8(c), opnieuw bewezen hebben.

De vraag is nu, hoe we μ kunnen bepalen. De methode hiervoor is volkomen analoog aan de manier waarop we voor gehele getallen a en b de vergelijking $xa + yb = \mathrm{ggd}(a, b)$ oplossen. In ons geval komt deze methode op het volgende neer. Men schrijft een rij gelijkheden

$$\begin{aligned} k_0(\alpha) \cdot h(\alpha) &= r_0(\alpha) \\ k_1(\alpha) \cdot h(\alpha) &= r_1(\alpha) \\ k_2(\alpha) \cdot h(\alpha) &= r_2(\alpha) \\ &\vdots \end{aligned}$$

op die als volgt verkregen wordt. In de nulde regel neemt men $k_0 = 0$ en $r_0 = f$; er staat dan $0 = 0$. In de volgende regel neemt men $k_1 = 1$ en $r_1 = h$; er staat dan $1 \cdot h(\alpha) = h(\alpha)$. Heeft men de $(n-1)$-ste regel en de n-de regel, dan vindt men de $(n+1)$-ste regel door een deling met rest (vgl. 3.1) toe te passen op r_{n-1} en r_n. Dit levert q_n en $r_{n+1} \in K[X]$ op met

$$r_{n-1} = q_n \cdot r_n + r_{n+1}\,, \qquad \mathrm{gr}(r_{n+1}) < \mathrm{gr}(r_n)\,.$$

Trekken we nu de n-de regel $q_n(\alpha)$ maal af van de $(n-1)$-ste regel, dan vinden we de $(n+1)$-ste regel:

$$\big(k_{n-1}(\alpha) - q_n(\alpha)k_n(\alpha)\big) \cdot h(\alpha) = r_{n+1}(\alpha)\,,$$

met $k_{n+1} = k_{n-1} - q_n \cdot k_n$. Aangezien $\mathrm{gr}(r_n)$ steeds daalt, vindt men op een gegeven moment $r_n = 0$, en dan is r_{n-1} de grootste gemene deler van f en h in $K[X]$. Omdat f en h onderling ondeelbaar zijn betekent dit dat $r_{n-1} \in K^*$, en uit $k_{n-1}(\alpha) \cdot h(\alpha) = r_{n-1}$ volgt nu

$$h(\alpha)^{-1} = r_{n-1}^{-1} \cdot k_{n-1}(\alpha)\,.$$

Voorbeeld 9.11. Laat $K = \mathbb{Q}$, en laat $\alpha \in \mathbb{C}$ voldoen aan $\alpha^3+\alpha^2 = 1$. Omdat $f = X^3+X^2-1 \in \mathbb{Q}[X]$ irreducibel is en $f(\alpha) = 0$, geldt $f^\alpha_{\mathbb{Q}} = f$ en $n = 3$. We berekenen $h(\alpha)^{-1}$ voor $h(\alpha) = \alpha^2 + 1$.

$$\begin{aligned}
0 \cdot h(\alpha) &= \alpha^3 + \alpha^2 - 1 \\
1 \cdot h(\alpha) &= \alpha^2 + 1 && (q_1(\alpha) = \alpha + 1) \\
(-\alpha - 1) \cdot h(\alpha) &= -\alpha - 2 && (q_2(\alpha) = -\alpha + 2) \\
\big(-\alpha^2 + \alpha + 3\big) \cdot h(\alpha) &= 5
\end{aligned}$$

dus

$$h(\alpha)^{-1} = -\frac{1}{5}\alpha^2 + \frac{1}{5}\alpha + \frac{3}{5}\,.$$

Het laatste resultaat van dit hoofdstuk toont aan dat elk monisch irreducibel polynoom optreedt als minimumpolynoom.

Stelling 9.12. *Laat K een lichaam zijn, en $f \in K[X]$ een monisch irreducibel polynoom. Dan bestaat er een uitbreiding L van K en een element $\alpha \in L$ dat algebraïsch over K is, zodanig dat $f^\alpha_K = f$.*

Bewijs. We kiezen $L = K[X]/K[X]f$. (Deze keuze wordt gesuggereerd door 9.8(c) !) Omdat f irreducibel is, is L wegens 5.8 een lichaam. Verder is het samengestelde homomorfisme $K \to K[X] \to K[X]/K[X]f = L$ injectief, omdat K een lichaam is (vgl. 2.18) dus we kunnen K als deellichaam van L en L als uitbreiding van K opvatten. Laat nu $\alpha = \big(X \bmod K[X]f\big)$, dan $f(\alpha) = \big(f(X) \bmod K[X]f\big) = 0$. Dus α is algebraïsch over K, en $f = f^\alpha_K$ wegens 9.8(a). Dit bewijst 9.12 □

Gevolg 9.13. *Voor elke irreducibele $f \in K[X]$ is er een uitbreiding L van K en een $\alpha \in L$ met $f(\alpha) = 0$.*

De constructie uit het bewijs van 9.12 staat bekend als de *symbolische adjungatie* van een nulpunt van f. Merk op dat 9.13 ook uit 4.22 volgt. De hier gegeven constructie is echter veel explicieter.

Opgaven

1. Bewijs dat elke $\alpha \in \mathbb{Q}(\sqrt{2})$ algebraïsch over $\mathbb{Q}$ is.

2. Bewijs dat de verzameling $\{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraïsch over } \mathbb{Q}\}$ aftelbaar is (aanwijzing: $\mathbb{Q}[X]$ is aftelbaar, en elke $f \in \mathbb{Q}[X]$ met $f \neq 0$, heeft maar eindig veel nulpunten in $\mathbb{C}$). Concludeer dat er complexe, en zelfs reële, getallen bestaan die transcendent over $\mathbb{Q}$ zijn.

3. Bestaat er een $\alpha \in \mathbb{R}$ met $\mathbb{Q}(\alpha) = \mathbb{R}$? (Aanwijzing: bereken de cardinaliteit.)

4. Bewijs: $f_{\mathbb{Q}}^{\sqrt[n]{2}} = X^n - 2$ voor elke $n \in \mathbb{Z}_{>0}$.

5. Laat α algebraïsch over een lichaam K zijn, en $f_K^\alpha = \sum_{i=0}^n a_i X^i$, met $a_n = 1$. Bewijs: als $\alpha \neq 0$ dan $a_0 \neq 0$, en $\alpha^{-1} = \sum_{i=1}^n -a_0^{-1} a_i \alpha^{i-1}$.

6. Bereken $f_{\mathbb{Q}}^\alpha$ en $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha)$ voor elk van de volgende α:

$$2 - \sqrt{3}\,, \quad \sqrt[3]{2} + \sqrt[3]{4}\,, \quad \sqrt{3 + 2\sqrt{2}}\,,$$

   en voor

$$\beta^{-1}\,, \quad \beta + 1$$

   als β voldoet aan $\beta^3 + 3\beta - 3 = 0$.

7. (a) Bewijs: $\mathbb{Q}(\sqrt{2})(\sqrt{7}) = \mathbb{Q}(\sqrt{2} + \sqrt{7})$, en $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + \sqrt{7}) = 4$.
   (b) Bereken $f_{\mathbb{Q}}^{\sqrt{2}+\sqrt{7}}$.

8. Laat $\alpha \in \mathbb{R}$ een getal zijn dat voldoet aan $\alpha^3 - \alpha - 1 = 0$. Schrijf elk van de volgende elementen in de vorm $a + b\alpha + c\alpha^2$, met $a, b, c \in \mathbb{Q}$:

$$\alpha^{10}, \quad \alpha^{-10}, \quad (\alpha^2 + \alpha + 1)^2, \quad (\alpha^2 + 1)^{-1}.$$

Hoofdstuk 10

Eindige en algebraïsche uitbreidingen

Definitie 10.1. Laat L een uitbreiding van een lichaam K zijn. We zeggen dat L *eindig* over K is, als de dimensie van L, opgevat als vectorruimte over K, eindig is.

De *graad* van L over K, notatie $[L : K]$, is de dimensie van L opgevat als K-vectorruimte: $[L : K] = \dim_K(L)$. We noemen L *algebraïsch* over K, als *elke* $\alpha \in L$ algebraïsch over K is (zie Definitie 9.3).

Voorbeeld 10.2. Er geldt

$$[\mathbb{C} : \mathbb{R}] = 2\,, \qquad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3\,.$$

Omdat een eindigdimensionale vectorruimte over $\mathbb{Q}$ aftelbaar is, is $\mathbb{R}$ *niet* eindig over $\mathbb{Q}$.

Stelling 10.3. *Laat L een uitbreiding van het lichaam K zijn, en $\alpha \in L$. Dan geldt:*

$$\alpha \textit{ is algebraïsch over } K \quad \Longleftrightarrow \quad K(\alpha) \textit{ is eindig over } K.$$

Voorts geldt: als α algebraïsch over K is, dan is $[K(\alpha) : K] = \mathrm{gr}(f_K^\alpha)$.

Bewijs. $\Leftarrow$: Stel $[K(\alpha) : K] = n < \infty$. Omdat in een n-dimensionale vectorruimte elk $(n+1)$-tal vectoren lineair afhankelijk is, moet er tussen de $n+1$ elementen $1, \alpha, \alpha^2, \ldots, \alpha^n \in K(\alpha)$ een relatie

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0$$

bestaan, met $a_0, a_1, \ldots, a_n \in K$, niet alle nul. Hieruit blijkt dat α algebraïsch over K is.

$\Rightarrow$: Stel, omgekeerd, dat α algebraïsch over K is. Dan weten we uit 9.8(d) dat $\big[K(\alpha) : K\big] = \mathrm{gr}(f_K^\alpha)$ en dit is inderdaad eindig. Hiermee is 10.3 bewezen. □

Stelling 10.4. *Stel dat L een* eindige *lichaamsuitbreiding van K is. Dan is L* algebraïsch *over K.*

Bewijs. Laat $\alpha \in L$. Omdat L eindig over K is, en $K(\alpha)$ een deelvectorruimte van L is, is ook $K(\alpha)$ eindig over K. Uit 10.3 volgt nu dat α algebraïsch over K is. Aangezien α willekeurig gekozen was concluderen we dat L algebraïsch over K is. Dit bewijst 10.4. □

10.5 Uit 10.3 en 10.4 volgt direct: als α algebraïsch over K is, dan is $K(\alpha)$ algebraïsch over K, d.w.z. elke $\beta \in K(\alpha)$ is algebraïsch over K. Aan het eind van dit hoofdstuk zullen we methoden aangeven om in zulke gevallen het minimumpolynoom van β over K te berekenen, zie 10.10. Zoals uit Opgave 1 blijkt geldt de omkering van 10.4 niet: er bestaat een algebraïsche uitbreiding die niet eindig is.

Stelling 10.6. *Laat K een lichaam zijn, L een uitbreiding van K en M een uitbreiding van L (dus $K \subset L \subset M$). Dan geldt:*

$$M \text{ is eindig over } K \quad \Longleftrightarrow \quad M \text{ is eindig over } L \text{ en } L \text{ is eindig over } K.$$

Voorts geldt, als M eindig over K:

$$[M : K] = [M : L] \cdot [L : K].$$

Bewijs. $\Rightarrow$: Stel dat M eindig over K is. Omdat L een deel-K-vectorruimte van M is, is dan ook L eindig over K. Als $\alpha_1, \ldots, \alpha_n$ de vectorruimte M over K opspannen, dan kan elke $x \in M$ uitgedrukt worden als $\sum_{i=1}^{n} a_i \alpha_i$, met $a_i \in K$. Dan geldt zeker $a_i \in L$, dus ook over L wordt M opgespannen door $\alpha_1, \ldots, \alpha_n$, en $[M : L] \leq n$ dus M is eindig over L.

$\Leftarrow$: Stel dat $[M : L] = n$ en $[L : K] = m$ allebei eindig zijn. Kies een basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ van L over K en een basis $\beta_1, \beta_2, \ldots, \beta_n$ van M over L. We gaan bewijzen dat $\{\alpha_i \beta_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ een basis van M over K is.

Elk $x \in M$ kan geschreven worden als

$$x = \sum_{j=1}^{n} y_j \beta_j \quad \text{met} \quad y_1, \ldots, y_n \in L\,.$$

Omdat $\alpha_1, \ldots, \alpha_m$ een basis van L over K is, kan elke y_j geschreven worden als

$$y_j = \sum_{i=1}^{m} a_{ij} \alpha_i \quad \text{met} \quad a_{ij} \in K \quad (1 \leq i \leq m, 1 \leq j \leq n)\,.$$

We vinden

$$x = \sum_{1 \leq i \leq m, 1 \leq j \leq n} a_{ij} \alpha_i \beta_j\,.$$

en omdat $x \in M$ willekeurig was bewijst dit dat de K-vectorruimte M wordt opgespannen door de $\alpha_i \beta_j$.

Om te laten zien dat $\{\alpha_i \beta_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ een *basis* van M over K is moeten we nog aantonen dat het een lineair onafhankelijk stelsel is. Stel dus dat

$$\sum_{1 \leq i \leq m, 1 \leq j \leq n} c_{ij} \alpha_i \beta_j = 0, \quad \text{met} \quad c_{ij} \in K\,.$$

Dan geldt

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} c_{ij} \alpha_i \Big) \beta_j = 0 \quad \text{met} \quad \sum_{i=1}^{m} c_{ij} \alpha_i \in L$$

en omdat de β_j's lineair onafhankelijk over L zijn is dit alleen mogelijk als

$$\sum_{i=1}^{m} c_{ij}\alpha_i = 0$$

voor elke $j = 1, 2, \ldots, n$. Maar de α_i's zijn lineair onafhankelijk over K, dus tenslotte vinden we

$$c_{ij} = 0$$

voor alle i en j. De $\alpha_i\beta_j$ zijn dus inderdaad lineair onafhankelijk over K.

Hiermee is aangetoond dat de dimensie van M over K gelijk is aan mn, dus inderdaad eindig. De laatste formule uit de stelling volgt nu direct:

$$[M : K] = m \cdot n = [L : K] \cdot [M : L]\,.$$

Hiermee is 10.6 bewezen. □

Is L een uitbreiding van een lichaam K, en $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, dan definiëren we inductief

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})\big(\alpha_n\big)\,.$$

Gevolg 10.7. *Laat L een lichaamsuitbreiding van K zijn, en stel dat $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ algebraïsch over K zijn. Dan is $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ eindig over K.*

Bewijs. Met inductie naar n. Voor $n = 1$ kan men 10.3 toepassen. Laat vervolgens $n > 1$, en $K' = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. Uit de inductiehypothese volgt dat K' eindig is over K. Omdat α_n algebraïsch over K is, is α_n zeker algebraïsch over K', dus $K'(\alpha_n)$ is eindig over K'. Uit Stelling 10.6 (met $L = K'$ en $M = K'(\alpha_n)$) volgt nu dat $K'(\alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ eindig over K is, zoals verlangd. Dit bewijst 10.7. □

Stelling 10.8. *Laat L een uitbreiding van een lichaam K zijn.*

(a) *Als $\alpha, \beta \in L$ algebraïsch over K zijn, dan zijn ook*

$$\alpha + \beta\,, \quad \alpha - \beta\,, \quad \alpha\beta\,, \quad \textit{en} \quad \alpha/\beta \quad (\beta \neq 0)$$

algebraïsch over K.

(b) *De verzameling $\big\{\alpha \in L \;\big|\; \alpha$ is algebraïsch over $K\big\}$ is een deellichaam van L dat K omvat.*

De verzameling in (b) noemt men wel de *algebraïsche afsluiting van K in L*.

Bewijs. (a) Wegens 10.7 is $K(\alpha, \beta)$ eindig over K, dus ook algebraïsch (zie 10.4). Volgens Definitie 10.1 betekent dit dat alle elementen van $K(\alpha, \beta)$, in het bijzonder $\alpha \pm \beta$, $\alpha\beta$ en α/β (voor $\beta \neq 0$), algebraïsch over K zijn.

(b) Uit (a) en de definitie van deellichaam volgt dat de verzameling een deellichaam M van L vormt. Uiteraard is elke $\alpha \in K$ algebraïsch over K, zodat K een deellichaam van M is. Hiermee is 10.8 bewezen. □

De laatste stelling van deze paragraaf is het analogon van 10.6, met "eindig" vervangen door "algebraïsch".

Stelling 10.9. *Laat K een lichaam zijn, L een uitbreiding van K, en M een uitbreiding van L. Dan geldt:*

$$M \text{ is algebraïsch over } K \iff M \text{ is algebraïsch over } L \text{ en } L \text{ is algebraïsch over } K.$$

Bewijs. $\Rightarrow$: Deze implicatie volgt onmiddelijk uit de definities, zoals de lezer als opgave mag controleren.

$\Leftarrow$: Stel dat M algebraïsch is over L, en L algebraïsch over K, en zij $\alpha \in M$ willekeurig. We moeten bewijzen dat α algebraïsch over K is. Omdat M algebraïsch over L is, zijn er $n \in \mathbb{Z}_{>0}$ en $\beta_1, \beta_2, \ldots, \beta_n \in L$ zodanig dat

$$\alpha^n + \beta_1\alpha^{n-1} + \cdots + \beta_{n-1}\alpha + \beta_n = 0\,.$$

Kennelijk is α ook algebraïsch over het deellichaam $K' = K(\beta_1, \beta_2, \ldots, \beta_n)$ van L, dus $K'(\alpha)$ is eindig over K'. Omdat L algebraïsch is over K, zijn alle β_i algebraïsch over K, dus wegens 10.7 is $K' = K(\beta_1, \beta_2, \ldots, \beta_n)$ eindig over K. Passen we nu 10.6 toe op $K \subset K' \subset K'(\alpha)$ dan vinden we dat $K'(\alpha)$ eindig is over K. Wegens 10.4 is $K'(\alpha)$ dan algebraïsch over K, en in het bijzonder is α algebraïsch over K, zoals verlangd. Hiermee is 10.9 aangetoond. □

10.10 Het bepalen van het minimumpolynoom Stel dat L een gegeven eindige uitbreiding van K is, en $\beta \in L$ een gegeven element, hoe kunnen we dan het minimumpolynoom f_K^β bepalen? (Uit 10.4 weten we dat het *bestaat*.) Drie methoden hiervoor zullen we illustreren aan de hand van het geval $K = \mathbb{Q}$, $L = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ (vgl. Opgave 3), $\beta = 1 + \sqrt{2} + \sqrt{3}$.

(a) De eerste methode maakt gebruik van technieken uit de lineaire algebra. We kiezen een basis van $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, bijvoorbeeld 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{2}\cdot\sqrt{3}$ (zie het bewijs van 10.6 en Opgave 3). Met behulp van deze basis drukken we elementen van $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ uit als rijvectoren; de vector (a, b, c, d) staat dan voor het element $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3}$. Schrijf nu de machten $\beta^0, \beta^1, \beta^2, \ldots$ van β als rijvectoren:

$$\begin{aligned}
\beta^0 &= \quad 1 \quad &&= (1,0,0,0)\\
\beta^1 &= \quad \beta \quad &&= (1,1,1,0)\\
\beta^2 &= &&= (6,2,2,2)\\
\beta^3 &= &&= (16,14,12,6)\\
\beta^4 &= &&= (80,48,40,32).
\end{aligned}$$

Hiermee gaat men door totdat de vectoren die men heeft opgeschreven lineair afhankelijk zijn. In dit geval ziet men dat dit pas bij β^4 gebeurt, en met de technieken die bij lineaire algebra worden onderwezen vindt men de lineaire afhankelijkheid

$$\beta^4 - 4\beta^3 - 4\beta^2 + 16\beta - 8 = 0\,.$$

Er moet nu gelden $f_{\mathbb{Q}}^\beta = X^4 - 4X^3 - 4X^2 + 16X - 8$, want als er een relatie van lagere graad zou bestaan dan zouden de vectoren $\beta^0, \beta^1, \ldots$ eerder lineair afhankelijk worden.

Bij het bepalen wanneer precies de vectoren $\beta^0, \beta^1, \ldots$ afhankelijk worden kan in het algemene geval Opgave 5 behulpzaam zijn.

(b) De tweede methode berust op gedachten uit de Galoistheorie. Zij gaat er van uit dat aangezien $f_{\mathbb{Q}}^{\sqrt{2}} = X^2 - 2$ de nulpunten $\sqrt{2}$ en $-\sqrt{2}$ heeft, en $f_{\mathbb{Q}}^{\sqrt{3}}$ de nulpunten $\pm\sqrt{3}$, het voor de hand ligt te veronderstellen dat $f_{\mathbb{Q}}^{1+\sqrt{2}+\sqrt{3}}$ als nulpunten de vier getallen $1 \pm \sqrt{2} \pm \sqrt{3}$ zal hebben. Berekent men het vierdegraads monische polynoom

$$(X - (1 + \sqrt{2} + \sqrt{3})) \cdot (X - (1 + \sqrt{2} - \sqrt{3})) \cdot (X - (1 - \sqrt{2} + \sqrt{3})) \cdot (X - (1 - \sqrt{2} - \sqrt{3}))$$

dat deze vier nulpunten bezit dan vindt men het polynoom

$$X^4 - 4X^3 - 4X^2 + 16X - 8$$

dat *rationale* coëfficiënten heeft, en natuurlijk $1+\sqrt{2}+\sqrt{3}$ als nulpunt. Met behulp van de hoofdstelling over symmetrische functies, zie Stelling 7.2, is het niet lastig in te zien dat men op deze wijze een polynoom met coëfficiënten in het grondlichaam verkrijgt, maar het is niet altijd waar (in dit geval wèl) dat dit polynoom irreducibel is. Dit moet dus nog apart gecontroleerd worden, vgl. Opgave 6. Wel is het zo verkregen polynoom steeds *deelbaar* door het minimumpolynoom.

(c) De derde methode bestaat uit "handig rekenen": men probeert de worteltekens uit $\beta = 1+\sqrt{2}+\sqrt{3}$ weg te werken. Dit kan bijvoorbeeld zo geschieden:

$$\begin{aligned} \beta - 1 &= \sqrt{2} + \sqrt{3} \\ (\beta - 1)^2 &= (\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{2} \cdot \sqrt{3} + 3 = 5 + 2\sqrt{2} \cdot \sqrt{3} \\ \big((\beta - 1)^2 - 5\big)^2 &= \big(2\sqrt{2} \cdot \sqrt{3}\big)^2 = 24 \end{aligned}$$

en als men de gevonden relatie uitwerkt ontdekt men weer dat β een nulpunt is van het polynoom

$$\big((X - 1)^2 - 5\big)^2 - 24 = X^4 - 4X^3 - 4X^2 + 16X - 8\,.$$

Om aan te tonen dat dit polynoom irreducibel over $\mathbb{Q}$ is, is het voldoende na te gaan dat het minimumpolynoom van β graad 4 over $\mathbb{Q}$ heeft, hetgeen wegens 10.3 neerkomt op $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Inderdaad: de bovenstaande berekening levert ons $\sqrt{2} \cdot \sqrt{3} \in \mathbb{Q}(\beta)$, dus ook $(\beta - 1)\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\beta)$. Door $2\sqrt{3} + 3\sqrt{2}$ geschikt met $\beta - 1 = \sqrt{2} + \sqrt{3}$ te combineren vindt men $\sqrt{2}$, $\sqrt{3} \in \mathbb{Q}(\beta)$, en dan moet het hele lichaam $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ bevat zijn in $\mathbb{Q}(\beta)$. Uiteraard ook $\mathbb{Q}(\beta) \subset \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$, dus $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ en wegens Opgave 3 heeft dit lichaam graad 4 over $\mathbb{Q}$, zoals verlangd.

Opgaven

1. Laat $L = \cup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$. Bewijs:

   (a) L is een lichaam (aanwijzing: $\mathbb{Q}(\sqrt[n]{2}) \cup \mathbb{Q}(\sqrt[m]{2}) \subset \mathbb{Q}(\sqrt[nm]{2})$);

   (b) L is algebraïsch over $\mathbb{Q}$;

   (c) L bevat voor elke $n \in \mathbb{Z}_{\geq 1}$ een deellichaam van graad n over $\mathbb{Q}$, en is dus zelf *niet* eindig over $\mathbb{Q}$.

2. Als $\alpha, \beta \in L$ algebraïsch over K zijn, dan geldt

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K].$$

   Bewijs dit.

3. (a) Bewijs dat er geen $a, b \in \mathbb{Q}$ zijn met $(a + b\sqrt{2})^2 = 3$, en concludeer hieruit dat $X^2 - 3$ irreducibel is in $\mathbb{Q}(\sqrt{2})[X]$.

   (b) Bewijs: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

4. Bewijs:

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, i\sqrt[4]{2}\right) : \mathbb{Q}\right] = 8 < 16 = \left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] \cdot \left[\mathbb{Q}\left(i\sqrt[4]{2}\right) : \mathbb{Q}\right]$$

5. Laat L een *eindige* uitbreiding van een lichaam K zijn, en $\alpha \in L$. Bewijs dat $\mathrm{gr}(f_K^\alpha)$ een *deler* van $[L : K]$ is.

6. Laat $f = X^4 - 4X^3 - 4X^2 + 16X - 8$. Bewijs dat $\frac{1}{8} \cdot X^4 f(2/X)$ een Eisensteinpolynoom bij 2 is. Concludeer dat f irreducibel is in $\mathbb{Q}[X]$.

7. Laat $\beta = 1 + \sqrt{2} + \sqrt{3}$. Druk $\sqrt{2}$, $\sqrt{3}$ en β^{-1} uit op de $\mathbb{Q}$-basis $1, \beta, \beta^2, \beta^3$ voor $\mathbb{Q}(\beta)$.

8. (a) Bewijs: $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} \cdot \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$.

   (b) Bereken $f_{\mathbb{Q}}^{\alpha}$ voor $\alpha = \sqrt{2} \cdot \sqrt[3]{5}$ en voor $\alpha = \sqrt{2} + \sqrt[3]{5}$.

9. Laat $\alpha \in \mathbb{R}$ een getal zijn met $\alpha^3 - \alpha - 1 = 0$. Bereken van elk van de volgende elementen het minimumpolynoom over $\mathbb{Q}$:

$$\alpha - 1\,, \quad \alpha^2 + \alpha + 1\,, \quad (\alpha^2 + 1)^{-1}\,.$$

10. Laat α algebraïsch over een lichaam K zijn, en stel dat $[K(\alpha) : K]$ *oneven* is. Bewijs: $K(\alpha) = K(\alpha^2)$.

11. Laat L een uitbreiding van een lichaam K zijn, en laten α, $\beta \in L$ algebraïsch over K zijn. Veronderstel dat $[K(\alpha) : K]$ en $[K(\beta) : K]$ *onderling ondeelbaar* zijn. Bewijs: $[K(\alpha, \beta) : K] = [K(\alpha) : K] \cdot [K(\beta) : K]$

12. Laat L een uitbreiding van K zijn, en zij K_0 de algebraïsche afsluiting van K in L (zie na 10.8). Bewijs: elke $\alpha \in L$ met $\alpha \notin K_0$ is transcendent over K_0.

13. Laat α transcendent over een lichaam K zijn, en zij $\beta \in K(\alpha)$ een element met $\beta \notin K$. Bewijs:

    (a) α is algebraïsch over $K(\beta)$ (aanwijzing: laat $\beta = f(\alpha)/g(\alpha)$, en beschouw het polynoom $f(X) - \beta g(X) \in K(\beta)[X]$);

    (b) β is transcendent over K.

14. Laat K een lichaam zijn.

    (a) ("Breuk-splitsen"). Bewijs dat de volgende collectie een basis van $K(X)$ over K is:

    $$\left\{X^n \;\middle|\; n \in \mathbb{Z}_{\geq 0}\right\} \cup \left\{X^i \cdot f^{-m} \;\middle|\; f \in K[X]\,, m \in \mathbb{Z}_{>0}\,, 0 \leq i < \mathrm{gr}(f)\right\},$$

    met in de tweede verzameling alleen irreducibele en monische $f \in K[X]$.

    (b) Laat α transcendent over K zijn. Bewijs dat $[K(\alpha) : K]$ gelijk is aan de cardinaliteit van K als K oneindig is, en dat $[K(\alpha) : K]$ aftelbaar oneindig is als K eindig is.

15. Zij $K = \mathbb{F}_2(X, Y) = Q(\mathbb{F}_2[X, Y])$, (het quotiënten lichaam van de polynoomring $\mathbb{F}_2[X, Y]$).

    (a) Zij $f = T^2 + X \in K[T]$. Bewijs dat f irreducibel is en zij

    $$L = K[T]/(f), \qquad t = T + (f) \;\; \in L.$$

    (b) Zij $g = S^2 + Y \in L[S]$. Bewijs dat g irreducibel is en zij

    $$M = L[S]/(g), \qquad s = S + (g) \;\; \in M.$$

    (c) Merk op dat $K \subset L \subset M$ en bewijs dat $1,\ t,\ s,\ st$ een K-basis van M vormen.

    (d) Bewijs dat voor elke $\alpha \in M$, $\alpha \notin K$, geldt: $\mathrm{gr}(f_K^\alpha) = 2$. Concludeer dat de uitbreiding M van K niet enkelvoudig is.

16. (a) Definieer $\Phi_5 = (X^4 + X^3 + X^2 + X + 1)$. Ga na dat $X^5 - 1 = (X - 1)\Phi_5$ en bewijs dat Φ_5 irreducibel is in $\mathbb{Q}[X]$. (Aanwijzing: substitueer $X + 1$ voor X in Φ_5.)

    (b) Zij $M = \mathbb{Q}[X]/(\Phi_5)$ en zij ζ de klasse van X in M. Laat $\beta = \zeta + \zeta^4$ en $L = \mathbb{Q}[\beta] \subset M$. Bepaal $a, b \in \mathbb{Q}$ zo dat $\beta^2 = a\beta + b$ en bepaal $f_{\mathbb{Q}}^{\beta}$.

    (c) Bepaal $[M : L]$ en f_L^ζ.

    (d) Geef een formule voor $\cos\frac{2\pi}{5}$ waarin alleen wortels van rationale getallen voorkomen.

Hoofdstuk 11

Ontbindingslichamen

Definitie 11.1. Laat K een lichaam zijn, en $f \in K[X]$ een monisch polynoom. Een uitbreiding L van K heet een *ontbindingslichaam* (ook wel *splijtlichaam*) van f over K, als er $\alpha_1, \ldots, \alpha_n \in L$ zijn zodanig dat

(a) $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $L[X]$,

(b) $L = K(\alpha_1, \ldots, \alpha_n)$.

Onnauwkeurig kan men dit uitdrukken door te zeggen: een ontbindingslichaam van f over K ontstaat door "alle" nulpunten van f aan K te adjungeren. Men make goed onderscheid tussen een ontbindingslichaam van f over K en het in 9.12 geconstrueerde lichaam $K(\alpha)$ dat ontstaat door één nulpunt van f te adjungeren. Merk op dat een ontbindingslichaam van f *eindig* over K is, wegens Gevolg 10.7.

Voorbeeld 11.2. Zij $f = X^3 - 2 \in \mathbb{Q}[X]$. De complexe nulpunten van f zijn

$$\sqrt[3]{2}, \quad \sqrt[3]{2} \cdot \frac{-1 + i\sqrt{3}}{2}, \quad \sqrt[3]{2} \cdot \frac{-1 - i\sqrt{3}}{2}.$$

Hieruit ziet men dat $\mathbb{Q}\big(\sqrt[3]{2}, i\sqrt{3}\big)$ een ontbindingslichaam van f over $\mathbb{Q}$ is. Omdat $X^2 + 3$ irreducibel in $\mathbb{Q}(\sqrt[3]{2})[X]$ is (zelfs in $\mathbb{R}[X]$) leidt men uit 10.6, toegepast op $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}\big(\sqrt[3]{2}, i\sqrt{3}\big)$, af: $\big[\mathbb{Q}\big(\sqrt[3]{2}, i\sqrt{3}\big) : \mathbb{Q}\big] = 6$.

Stelling 11.3. *Laat K een lichaam zijn en $f \in K[X]$ een monisch polynoom. Dan bestaat er een ontbindingslichaam van f over K.*

Bewijs. We voeren het bewijs met inductie naar $n = \mathrm{gr}(f)$. Als $n = 1$ dan is K kennelijk zelf een ontbindingslichaam van f over K. Laat vervolgens $n > 1$. We onderscheiden twee gevallen: f is irreducibel of niet.

Stel eerst dat f te ontbinden is: $f = g \cdot h$, met $g, h \in K[X]$ monisch van graad $< n$. Uit de inductiehypothese weten we dan dat er een ontbindingslichaam $E = K(\beta_1, \beta_2, \ldots, \beta_m)$ van g over K is, met $g = \prod_{i=1}^{m}(X - \beta_i)$ in $E[X]$. Verder weten we uit de inductiehypothese, nu toegepast met E als het grondlichaam, dat er een ontbindingslichaam $L = E(\gamma_1, \gamma_2, \ldots, \gamma_k)$ van h over E is, met

$h = \prod_{i=1}^{k}(X-\gamma_i)$ in $L[X]$. Dan is L een ontbindingslichaam van f over K, want $f = \prod_{i=1}^{m}(X-\beta_i)\cdot\prod_{i=1}^{k}(X-\gamma_i)$ in $L[X]$ en $L = E(\gamma_1,\gamma_2,\ldots,\gamma_k) = K(\beta_1,\ldots,\beta_m,\gamma_1,\ldots,\gamma_k)$.

Neem vervolgens aan dat f irreducibel is in $K[X]$. Dan is er wegens 9.13 een uitbreiding $K(\alpha)$ met $f(\alpha)=0$. Volgens 3.5 bestaat er dan een $h \in K(\alpha)[X]$ met $f = (X-\alpha)h$. Kennelijk is h een monisch polynoom van graad $n-1$. Passen we dus de inductiehypothese toe, met $K(\alpha)$ als grondlichaam, dan vinden we dat er een ontbindingslichaam $L = K(\alpha)(\alpha_1,\ldots,\alpha_{n-1})$ van h over $K(\alpha)$ bestaat, met $h = \prod_{i=1}^{n-1}(X-\alpha_i)$ in $L[X]$. Met $\alpha_n = \alpha$ hebben we dan $L = K(\alpha_1,\alpha_2,\ldots,\alpha_n)$ en $f = \prod_{i=1}^{n}(X-\alpha_i)$ in $L[X]$, dus L is een ontbindingslichaam van f over K. Dit bewijst 11.3. □

We gaan vervolgens de *eenduidigheid* van het ontbindingslichaam bewijzen.

Stelling 11.4. *Laat $\phi\colon K_0 \to K_1$ een isomorfisme van een lichaam K_0 naar een lichaam K_1 zijn, en zij*

$$\Phi\colon K_0[X] \to K_1[X], \qquad \sum_i a_i X^i \mapsto \sum_i \phi(a_i)X^i$$

het door ϕ geinduceerde isomorfisme van polynoomringen. Zij $f_0 \in K_0[X]$ een monisch polynoom en zij $f_1 = \Phi(f_0) \in K_1[X]$. Laat verder L_0 een ontbindingslichaam van f_0 over K_0 zijn, en L_1 een ontbindingslichaam van f_1 over K_1. Dan is er een isomorfisme $\psi\colon L_0 \to L_1$ waarvoor geldt dat $\psi_{|K_0} = \phi$.

$$\begin{array}{ccc} L_0 & \overset{\psi}{-\!\!\to} & L_1 \\ \bigcup & & \bigcup \\ K_0 & \longrightarrow & K_1 \end{array}$$

Bewijs. Uit 11.1(b) en 10.7 volgt dat de graad $[L_0 : K_0]$ *eindig* is. We voeren het bewijs met inductie naar deze graad.

Als $[L_0 : K_0] = 1$ dan geldt $L_0 = K_0$, dus $f_0 = \prod_{i=1}^{n}(X-\beta_i)$ met $\beta_1,\ldots,\beta_n \in K_0$. Dan is $f_1 = \Phi(f_0) = \prod_{i=1}^{n}\Phi(X-\beta_i) = \prod_{i=1}^{n}\big(X-\Phi(\beta_i)\big) \in K_1[X]$. De nulpunten van f_1 in L_1 liggen dus allemaal binnen K_1, en omdat L_1 ontstaat door het adjugeren van deze nulpunten geldt $L_1 = K_1$. We kunnen dus $\psi = \phi$ nemen.

Laat vervolgens $[L_0 : K_0] > 1$. We construeren enkelvoudige uitbreidingen $K_0(\alpha_0)$ en $K_1(\alpha_1)$ en een isomorfisme $\chi\colon K_0(\alpha_0) \to K_1(\alpha_1)$ met $\chi_{|K_0} = \phi$.

Omdat $[L_0 : K_0] > 1$ is er een nulpunt $\alpha_0 \in L_0$ van f_0 waarvoor geldt $\alpha_0 \notin K_0$. Zij $h_0 = f_{K_0}^{\alpha_0} \in K_0[X]$ het minimumpolynoom van α_0 over K_0 en zij $h_1 = \Phi(h_0) \in K_1[X]$. Uit $f_0(\alpha_0) = 0$ en 9.8(b) volgt dat h_0 een deler is van f_0 in $K_0[X]$, en wegens het isomorfisme $\Phi\colon K_0[X] \xrightarrow{\sim} K_1[X]$ betekent dit dat h_1 ook een deler is van f_1 in $K_1[X]$. Maar f_1 ontbindt in $L_1[X]$ in lineaire factoren, dus hetzelfde moet voor de deler h_1 van f_1 het geval zijn. Dit impliceert dat h_1 een nulpunt α_1 in L_1 heeft.

Wegens Stelling 9.8(c) is er een isomorfisme

$$K_0[X]/K_0[X]h_0 \cong K_0(\alpha_0) \tag{11.4.1}$$

waarbij α_0 met de restklasse van X correspondeert. Omdat h_0 irreducibel is in $K_0[X]$, is h_1 irreducibel in $K_1[X]$ en moet wegens 9.8(a) het minimumpolynoom van α_1 over K_1 zijn. Opnieuw wegens 9.8(c)

is er dus een isomorfisme

$$K_1[X]/K_1[X]h_1 \cong K_1(\alpha_1)\,, \qquad (X \bmod h_1) \mapsto \alpha_1\,. \tag{11.4.2}$$

Tenslotte beeldt het isomorfisme $K_0[X] \cong K_1[X]$ het ideaal voortgebracht door h_0 af op het ideaal voortgebracht door h_1, en levert dus een isomorfisme

$$K_0[X]/K_0[X]h_0 \cong K_1[X]/K_1[X]h_1 \tag{11.4.3}$$

dat de respectievelijke restklassen van X met elkaar laat corresponderen en dat beperkt tot K_0 gelijk is aan ϕ.

Combineren we de isomorfismen (11.4.1), (11.4.2) en (11.4.3) dan vinden we een isomorfisme $\chi\colon K_0(\alpha_0) \xrightarrow{\sim} K_1(\alpha_1)$ dat α_0 op α_1 afbeeldt en dat beperkt tot K_0 gelijk is aan ϕ.

Om ψ te verkrijgen passen we nu de inductiehypothese toe op de bovenste helft van het diagram

$$\begin{array}{ccc} L_0 & -\overset{\psi}{-}\!\to & L_1 \\ \bigcup & & \bigcup \\ K_0(\alpha_0) & \xrightarrow{\quad\chi\quad} & K_1(\alpha_1) \\ \bigcup & & \bigcup \\ K_0 & \xrightarrow{\quad\phi\quad} & K_1 \end{array}$$

We hadden α_0 buiten K_0 gekozen, dus $[K_0(\alpha_0) : K_0] > 1$ en

$$\big[L_0 : K_0(\alpha_0)\big] = \frac{[L_0 : K_0]}{[K_0(\alpha_0) : K_0]} < [L_0 : K_0]\,,$$

d.w.z. de graad is *kleiner* geworden en de inductiehypothese is inderdaad van toepassing, mits we nagaan dat L_0 een ontbindingslichaam van f_0 over $K_0(\alpha_0)$ is, en analoog voor L_1. Maar dit is evident: als we alle nulpunten van f_0 in L_0 aan K_0 adjungeren krijgen we L_0, dus dit geldt zeker als we ze aan $K_0(\alpha_0)$ adjungeren; en dito voor L_1.

Passen we de inductiehypothese toe dan vinden we een lichaamsisomorfisme $\psi\colon L_0 \xrightarrow{\sim} L_1$ met $\psi_{|K_0(\alpha_0)} = \chi$, dus $\psi_{|K_0} = \phi$. Hiermee is het bewijs van 11.4 geleverd. □

Definitie 11.5. Als L en L' twee uitbreidingen van een lichaam K zijn, dan is een *K-homomorfisme* $L \to L'$ een homomorfisme $\phi\colon L \to L'$ met $\phi_{|K} = \mathrm{id}_K$, de identiteit op K. Een *K-isomorfisme* is een bijectief K-homomorfisme.

L en L' heten *K-isomorf*, notatie $L \cong_K L'$, als er een K-isomorfisme $L \to L'$ bestaat. Een *K-automorfisme* is een K-isomorfisme met $L = L'$.

We kunnen nu de belangrijkste stelling betreffende ontbindingslichamen uitspreken en bewijzen.

Stelling 11.6. *Laat K een lichaam zijn en $f \in K[X]$. Dan bestaat er een ontbindingslichaam van f over K, en dit ontbindingslichaam is op K-isomorfie na eenduidig bepaald.*

Krachtens 11.6 kunnen we in het vervolg over *het* ontbindingslichaam van f over K spreken. Dit lichaam wordt aangegeven met Ω_K^f.

Bewijs. Het bestaan van een ontbindingslichaam is al bewezen in 11.3. Stel nu dat L en L' twee ontbindingslichamen van f over K zijn; we moeten bewijzen dat er een K-isomorfisme $\psi\colon L \to L'$ bestaat. Maar dit volgt direct door 11.4 toe te passen op $K_0 = K_1 = K$, $f_0 = f_1 = f$, $\phi = \mathrm{id}_K$ en $L_0 = L$, $L_1 = L'$. Hiermee is 11.6 bewezen. □

Opmerking 11.7. Het K-isomorfisme $\psi\colon L \to L'$ tussen twee ontbindingslichamen van f over K hoeft niet eenduidig bepaald te zijn. Als σ een K-automorfisme van L is, is ook $\psi' = \psi \circ \sigma\colon L \to L'$ een K-isomorfisme, en men ziet gemakkelijk in dat zo uit één vaste ψ *alle* mogelijke K-isomorfismen $\psi'\colon L \to L'$ verkregen worden.

De K-automorfismen van L vormen een groep, notatie $\mathrm{Aut}_K(L)$, die meestal niet alleen uit de identieke afbeelding bestaat, en die in de Galoistheorie uitgebreid bestudeerd wordt.

Is K het *priemlichaam* van L, dan geldt $\mathrm{Aut}_K(L) = \mathrm{Aut}(L)$; zie Hoofdstuk 8, Opgave 1.

Opgaven

1. Laat L een ontbindingslichaam van f over K zijn, en $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $L[X]$. Bewijs: $L = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ (dus met één α minder!).

2. Zij $f \in K[X]$ monisch van graad n. Bewijs: $[\Omega_K^f : K]$ is een deler van $n!$. (Aanwijzing: gebruik de constructie in het bewijs van 11.3.)

3. Bewijs dat $L = \mathbb{Q}(\sqrt[4]{2}, i)$ een ontbindingslichaam van $X^4 - 2$ over $\mathbb{Q}$ is. Bepaal ook $[L : \mathbb{Q}]$.

4. Wat is een ontbindingslichaam van $X^2 - 101$ over $\mathbb{Q}$?

5. Laat $\zeta \in \mathbb{C}$ een nulpunt van $f = X^4 + X^3 + X^2 + X + 1$ zijn. Bewijs dat $\zeta^5 = 1$, en dat ζ^2, ζ^3, ζ^4 de andere nulpunten van f in $\mathbb{C}$ zijn. Bewijs dat $\mathbb{Q}(\zeta)$ een ontbindingslichaam van f over $\mathbb{Q}$ is.

6. Bewijs: $\Omega_{\mathbb{Q}}^{X^2-2} \ncong \Omega_{\mathbb{Q}}^{X^2-3}$, maar $\Omega_K^{X^2-\bar{2}} \simeq \Omega_K^{X^2-\bar{3}}$ voor $K = \mathbb{F}_5$.

7. Bewijs dat $\mathbb{Q}\big(i, \sqrt{2}\big)$ een ontbindingslichaam van $f_{\mathbb{Q}}^{i+\sqrt{2}}$ over $\mathbb{Q}$ is. Bewijs: $\mathrm{Aut}\big(\mathbb{Q}(i, \sqrt{2})\big) \cong V_4$, de viergroep van Klein.

8. Laat L een ontbindingslichaam van f over K zijn, met $\mathrm{gr}(f) = n$.

   (a) Bewijs: elke K-automorfisme van L permuteert de nulpunten van f in L,

   (b) de groep $\mathrm{Aut}_K(L)$ is isomorf met een ondergroep van S_n;

   (c) $\#\mathrm{Aut}_K(L)$ is een deler van $n!$.

9. Bewijs: $\mathrm{Aut}\big(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})\big) \simeq S_3$.

10. Laat $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, en zij $\alpha \in \Omega_{\mathbb{Q}}^f$ een nulpunt van f. Bereken $f_{\mathbb{Q}}^{\alpha^2-2}$, en bewijs dat $\mathbb{Q}(\alpha) = \Omega_{\mathbb{Q}}^f$.

11. Zij K een lichaam. Bewijs dat de afbeelding $\phi\colon K(X) \to K(X)$ gegeven door $f \mapsto f(X+1)$ een lichaamsautomorfisme is. Bepaal de orde van ϕ in $\mathrm{Aut}(K(X))$.

Hoofdstuk 12

Eindige lichamen

Een lichaam K heet *eindig* als het aantal elementen van K eindig is. De volgende stelling classificeert de eindige lichamen.

Stelling 12.1. (a) *Is K een eindig lichaam, dan is er een priemgetal p en een geheel getal $n \geq 1$ met $\#K = p^n$.*

(b) *Omgekeerd is er voor elk priemgetal p en elk geheel getal $n \geq 1$ een eindig lichaam met p^n elementen, en dit lichaam is op isomorfie na eenduidig bepaald.*

Notatie 12.2. Is q een macht van een priemgetal, $q > 1$, dan wordt het volgens deze stelling eenduidig bepaalde lichaam met $q = p^n$ elementen aangegeven met $\mathbb{F}_q$. In de literatuur vindt men soms ook de notatie $\mathrm{GF}(q)$, voor "Galois field", naar Evariste Galois (Frans wiskundige, 1811–1832) die eindige lichamen het eerst bestudeerde.

Als q een priemgetal is, dan $\mathbb{F}_q \cong \mathbb{Z}/q\mathbb{Z}$; maar als q *geen* priemgetal is dan is $\mathbb{Z}/q\mathbb{Z}$, geen lichaam (Stelling 1.20), dus dan $\mathbb{F}_q \ncong \mathbb{Z}/q\mathbb{Z}$.

Bewijs van 12.1. (a) Laat K een eindig lichaam zijn. Dan kan K niet het lichaam $\mathbb{Q}$ als deellichaam hebben, dus $\mathrm{char}(K) \neq 0$ (zie 8.3). De karakteristiek van K is dus een priemgetal p, en K bevat het lichaam $\mathbb{F}_p$ als deellichaam. Omdat K eindig is, is K zeker eindig dimensionaal als vectorruimte over $\mathbb{F}_p$. Laat $n = [K : \mathbb{F}_p]$, en kies een basis $e_1, e_2, \ldots, e_n$ voor K over $\mathbb{F}_p$. Elk element $x \in K$ kan dan eenduidig geschreven worden als

$$x = a_1e_1 + a_2e_2 + \cdots + a_ne_n \qquad \text{met } a_i \in \mathbb{F}_p \text{ voor } 1 \leq i \leq n.$$

Deze schrijfwijze kunnen we gebruiken om het aantal elementen van K te tellen. Voor elk van a_i zijn er p mogelijkheden, en ze kunnen onafhankelijk van elkaar gekozen worden, dus het totale aantal mogelijkheden is $p \times p \times \cdots \times p = p^n$. Dit bewijst $\#K = p^n$.

(b) Laat p een priemgetal zijn, laat $n \in \mathbb{Z}_{>0}$, en laat $q = p^n$. Zij K het ontbindingslichaam van $X^q - X$ over $\mathbb{F}_p$ We laten zien dat K een lichaam met q elementen is, dit bewijst de *existentie*.

Omdat K het ontbindingslichaam van $X^q - X$ over $\mathbb{F}_p$ is, zijn er $\alpha_1, \alpha_2, \ldots, \alpha_q \in K$ met $X^q - X = \prod_{i=1}^{q}(X - \alpha_i)$ in $K[X]$. De verzameling $A = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ gaan we nu nader onderzoeken.

We bewijzen eerst: (i) $\#A = q$, en (ii) A is een *deellichaam* van K.

Bewijs van (i): Als $\#A < q$, dan zouden twee α's samenvallen: $\alpha_i = \alpha_j$, met $i \neq j$; dan is α_i een dubbel nulpunt van $f = X^q - X$, dus volgens Stelling 3.20 ook een nulpunt van de afgeleide $f' = q \cdot X^{q-1} - 1 = -1$ (want $q = 0$ in $\mathbb{F}_p$); maar het constante polynoom -1 heeft helemaal geen nulpunt, en deze tegenspraak bewijst dat $\#A = q$.

Bewijs van (ii): De verzameling A bestaat precies uit de nulpunten van $X^q - X$ in K, dus voor $\alpha \in K$ geldt: $\alpha \in A \iff \alpha^q = \alpha$. Hieruit is duidelijk dat $1 \in A$. Verder geldt dat als α, $\beta \in A$ en $\beta \neq 0$, dan is $(\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1}$, dus $\alpha\beta^{-1} \in A$; en gebruik makende van 8.4 vinden we:

$$\alpha, \beta \in A \implies (\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta \implies \alpha + \beta \in A\,.$$

Dus A is gesloten onder optelling en deling, en $-1 = 1 + 1 + \cdots + 1 \in A$ ($p - 1$ termen). Hieruit volgt dat A een deellichaam van K is.

Vervolgens tonen we aan dat $A = K$. Het priemlichaam $\mathbb{F}_p$ van K moet (per definitie van priemlichaam) ook in A bevat zijn, en A bevat alle α_i ($1 \leq i \leq q$). Omdat A een lichaam is, moet ook het door $\mathbb{F}_p$ en $\alpha_1, \ldots, \alpha_q$ voortgebrachte lichaam in A bevat zijn:

$$\mathbb{F}_p(\alpha_1, \alpha_2, \ldots, \alpha_q) \subset A\,.$$

Maar uit de definitie van ontbindingslichaam 11.1(b) volgt dat $K = \mathbb{F}_p(\alpha_1, \alpha_2, \ldots, \alpha_q)$. We concluderen dat $K \subset A$, en omdat natuurlijk ook $A \subset K$ volgt hieruit $K = A$. Wegens (i) is hiermee het bestaan van een lichaam van q elementen aangetoond. Dit bewijst de eerste bewering van 12.1(b).

We willen nu *eenduidigheid* bewijzen. Zij dus L ook een lichaam met q elementen, we willen aantonen $L \cong K$. Hiertoe merken we ten eerste op dat de karakteristiek van L ook gelijk is aan p, anders zou immers $\#L$ een macht van een ánder priemgetal zijn, hetgeen wegens de eenduidige priemfactorontbinding onmogelijk is. Laat nu $\alpha \in L^*$. Omdat L^* een groep van orde $q - 1$ is, is de (multiplicatieve) orde van α een deler van $q - 1$, dus $\alpha^{q-1} = 1$. Hieruit volgt dat $\alpha^q = \alpha$, dus α is een nulpunt van het polynoom $X^q - X$, hetgeen natuurlijk ook voor $\alpha = 0$ het geval is. Dus alle q elementen van L zijn nulpunten van $X^q - X$, en omdat dit polynoom graad q heeft moeten we hebben: $X^q - X = \prod_{\alpha \in L}(X - \alpha)$. Met behulp hiervan is het aan de hand van Definitie 11.1 gemakkelijk te controleren dat L een ontbindingslichaam van $X^q - X$ over het priemlichaam $\mathbb{F}_p$ van L is. Hetzelfde geldt voor K, en de eenduidigheidsstelling 11.6 voor ontbindingslichamen impliceert dus dat L en K isomorf zijn. Hiermee is Stelling 12.1 bewezen. □

Voorbeeld 12.3. De polynomen f, $g \in \mathbb{F}_2[X]$:

$$f = X^3 + X^2 + 1 \qquad \text{en} \qquad g = X^3 + X + 1$$

zijn irreducibel omdat ze graad drie hebben en geen nulpunten hebben in $\mathbb{F}_2$. De lichamen

$$K = \mathbb{F}_2[X]/(f) \qquad \text{en} \qquad L = \mathbb{F}_2[X]/(g)$$

hebben beide 8 elementen, en zijn volgens de stelling isomorf. We geven een expliciet isomorfisme.

Merk op dat $\alpha = (X \bmod f)$ een nulpunt van f in K is. Als K en L isomorf zijn, moet f dus een nulpunt in L hebben; dat gaan we eerst zoeken. Zij $\beta = (X \bmod g) \in L$. Dan is $\beta^3 = \beta + 1$. Merk op

dat:

$$f(\beta+1) = (\beta+1)^3 + (\beta+1)^2 + 1 = (\beta^3+\beta^2+\beta+1) + (\beta^2+1) + 1 = \beta^2 + (\beta^2+1) + 1 = 0$$

(we rekenen modulo 2 met de coëfficiënten), waarmee het nulpunt gevonden is. Om een lichaamsisomorfisme tussen K en L aan te geven bekijken we eerst het evaluatiehomomorfisme $\Phi_{\beta+1}\colon \mathbb{F}_2[X] \to L$ gegeven door $X \mapsto \beta+1$. Ga na dat $\Phi_{\beta+1}$ surjectief is. De kern van $\Phi_{\beta+1}$ wordt voortgebracht door f, want f is irreducibel en zit in de kern. Met de eerste isomorfiestelling 2.23 volgt dan: $K = \mathbb{F}_2[X]/(f) \cong \mathrm{Im}(\Phi_{\beta+1}) = L$; het isomorfisme wordt dus expliciet gegeven door:

$$a_0 + a_1\alpha + a_2\alpha^2 \mapsto a_0 + a_1(\beta+1) + a_2(\beta+1)^2 = (a_0+a_1+a_2) + a_1\beta + a_2\beta^2.$$

Gevolg 12.4. *Laat q een macht van een priemgetal p zijn, $q > 1$. Dan is $\mathbb{F}_q$ het ontbindingslichaam van $X^q - X$ over $\mathbb{F}_p$, en in $\mathbb{F}_q[X]$ geldt: $X^q - X = \prod_{\alpha\in\mathbb{F}_q}(X-\alpha)$.*

Bewijs. Beide beweringen van 12.4 zijn in de loop van het bewijs van 12.1 aangetoond. □

Uit het feit dat een eindig lichaam $\mathbb{F}_{p^n}$ een n-dimensionale vectorruimte over $\mathbb{F}_p$ is, volgt direct dat de optelgroep van $\mathbb{F}_{p^n}$ isomorf is met

$$(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p\mathbb{Z}) \qquad (n \text{ factoren})$$

Elk element $\neq 0$ van $\mathbb{F}_{p^n}$ heeft dus additieve orde p.

De volgende stelling geeft de structuur van de multiplicatieve groep van $\mathbb{F}_{p^n}$.

Stelling 12.5. *Voor elke priemmacht $q > 1$ is de groep $\mathbb{F}_q^*$ cyclisch van orde $q-1$.*

Bewijs. De orde van $\mathbb{F}_q^*$ is $q-1$, en de groep is cyclisch wegens Stelling 3.14. □

Een element $\alpha \in \mathbb{F}_q^*$ dat de multiplicatieve groep $\mathbb{F}_q^*$ voortbrengt heet een *primitieve wortel* van $\mathbb{F}_q$. De multiplicatieve orde van een primitieve wortel is gelijk aan $q-1$.

Gevolg 12.6. *Laat p een priemgetal zijn en $n \in \mathbb{Z}_{\geq 1}$. Dan is er een $\alpha \in \mathbb{F}_q$ met $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$.*

Bewijs. Laat α een primitieve wortel van $\mathbb{F}_{p^n}$ zijn. Dan kan elk element $\neq 0$ als macht van α geschreven worden, en behoort dus zeker tot $\mathbb{F}_p(\alpha)$. Dit bewijst 12.6. □

Gevolg 12.7. *Laat p een priemgetal zijn en $n \in \mathbb{Z}_{\geq 1}$. Dan bestaat er een monisch irreducibel polynoom $f \in \mathbb{F}_p[X]$ van graad n, en voor elke dergelijke f geldt $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/\mathbb{F}_p[X]f$.*

Bewijs. Zij α als in 12.6. Dan is $f = f_{\mathbb{F}_p}^{\alpha} \in \mathbb{F}_p[X]$ een monisch irreducibel polynoom, en uit 10.3 volgt $\mathrm{gr}(f) = \big[\mathbb{F}_p(\alpha) : \mathbb{F}_p\big] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, zoals verlangd. Omgekeerd, is $f \in \mathbb{F}_p[X]$ irreducibel en van graad n, dan is $\mathbb{F}_p[X]/\mathbb{F}_p[X]f$ een lichaam dat graad n over $\mathbb{F}_p$ heeft; dus $\#\big(\mathbb{F}_p[X]/\mathbb{F}_p[X]f\big) = p^n$ en dus is dit lichaam isomorf met $\mathbb{F}_{p^n}$. Dit bewijs 12.7. □

De voorgaande gevolgen tonen aan dat men in $\mathbb{F}_{p^n}$ kan rekenen volgens de in Hoofdstuk 9 aangegeven methoden, mits men een irreducibel n-de graads polynoom $f \in \mathbb{F}_p[X]$ kent. Zo'n polynoom is niet altijd gemakkelijk te vinden, maar het bestaan ervan is in elk geval gegarandeerd door 12.7. In Opgave 13 zullen we zien dat de "kans" dat een willekeurig gekozen n-de graads polynoom in $\mathbb{F}_p[X]$ irreducibel is, ongeveer gelijk is aan $1/n$.

Voorbeeld 12.8. Om in $\mathbb{F}_{5^3}$ te kunnen rekenen, zoeken we een irreducibel polynoom van graad 3 in $\mathbb{F}_5[X]$. Ieder polynoom van de vorm $X^3 - a$ met $a \in \mathbb{F}_5$ blijkt een nulpunt te hebben in $\mathbb{F}_5$ (dit volgt bijvoorbeeld uit Stelling 12.5!) en is dus reducibel.

Zij $f = X^3 + X - 1 \in \mathbb{F}_5[X]$, deze f is irreducibel want f heeft graad 3 en heeft geen nulpunt in $\mathbb{F}_5$ (ga na). Dan is $L = \mathbb{F}_5[X]/(f)$ een lichaam en $[L : \mathbb{F}_5] = 3$ dus $\#L = 5^3$. Schrijven we α voor de restklasse van X dan is ieder element van L te schrijven in de vorm

$$x = a_0 + a_1\alpha + a_2\alpha^2$$

met $a_i \in \mathbb{F}_5$. Omdat α een nulpunt is van f, geldt $\alpha^3 = -\alpha + 1$. Gebruik makend van deze relatie kunnen we producten in L uitwerken; zo is bijvoorbeeld

$$\begin{aligned}(3\alpha + 1)(4\alpha^2 + 2) &= 2\alpha^3 + 4\alpha^2 + \alpha + 2\\ &= 2(-\alpha + 1) + 4\alpha^2 + \alpha + 2\\ &= 4\alpha^2 + 4\alpha + 4,\\ &= -(\alpha^2 + \alpha + 1).\end{aligned}$$

waarbij de coëfficiënten modulo 5 genomen worden.

Tot nu toe hebben we ons in dit hoofdstuk beziggehouden met de structuur van een eindig lichaam van een vaste orde p^n. De volgende stelling zegt hoe eindige lichamen van verschillende ordes in elkaar geschakeld kunnen liggen.

Stelling 12.9. *Laten q en r twee priemmachten zijn. Dan zijn de volgende drie uitspraken equivalent:*

(a) *$\mathbb{F}_q$ is isomorf met een deellichaam van $\mathbb{F}_r$;*

(b) *r is een macht van q;*

(c) *er is een priemgetal p zo dat $q = p^k$ en $r = p^m$ voor positieve gehele getallen k en m met $k \mid m$.*

Bewijs. (a) $\Rightarrow$ (b): Als $\mathbb{F}_q$ een deellichaam van $\mathbb{F}_r$ is, dan is $\mathbb{F}_r$ een eindig dimensionale vectorruimte over $\mathbb{F}_q$ en net als in het eerste deel van het bewijs van 12.1 volgt hieruit $r = q^d$.

(b) $\Rightarrow$ (c): Triviaal.

(c) $\Rightarrow$ (a): Laat M een ontbindingslichaam van $(X^q - X)(X^r - X)$ over $\mathbb{F}_p$ zijn. Laat verder $F\colon M \to M$ het Frobenius-automorfisme $F(x) = x^p$ zijn; vgl. 8.5. De lichamen $\mathbb{F}_q$ en $\mathbb{F}_r$ zijn de ontbindingslichamen van $X^q - X$ en $X^r - X$ over $\mathbb{F}_p$ en kunnen dus als deellichamen van M opgevat

worden. Voor $\alpha \in M$ geldt:

$$\begin{aligned} \alpha \in \mathbb{F}_q \quad &\Leftrightarrow \quad \alpha \text{ is een nulpunt van } X^q - X \\ &\Leftrightarrow \quad \alpha^{p^k} = \alpha \\ &\Leftrightarrow \quad F^k(\alpha) = \alpha\,, \end{aligned}$$

en evenzo

$$\alpha \in \mathbb{F}_r \quad \Leftrightarrow \quad F^m(\alpha) = \alpha\,.$$

Als nu $k|m$, zeg $m = kd$, dan geldt voor $\alpha \in \mathbb{F}_q$:

$$\alpha = F^k(\alpha) = F^{2k}(\alpha) = \cdots = F^{dk}(\alpha) = F^m(\alpha)$$

en dus $\alpha \in \mathbb{F}_r$. Dit bewijst $\mathbb{F}_q \subset \mathbb{F}_r$, zoals verlangd. □

Opmerking 12.10. Als $\mathbb{F}_q$ isomorf is met een deellichaam van $\mathbb{F}_r$, dan is dit deellichaam ook eenduidig bepaald: het bestaat namelijk uit de q nulpunten van $X^q - X$ in $\mathbb{F}_r$.

Stelling 12.11. *Laat $q > 1$ een priemmacht zijn en laat $n \in \mathbb{Z}_{\geq 1}$. Dan is*

$$X^{q^n} - X = \prod f \qquad \text{in } \mathbb{F}_q[X]$$

waarbij het product is uitgestrekt over de verzameling monische irreducibele polynomen $f \in \mathbb{F}_q[X]$ met $\mathrm{gr}(f)$ *een deler van n.*

Bewijs. Omdat $\mathbb{F}_q[X]$ een ontbindingsring is, kan $X^{q^n} - X$ op een unieke wijze ontbonden worden in monische irreducibele factoren in $\mathbb{F}_q[X]$. Al deze factoren zijn bovendien *verschillend* want een dubbele factor zou een deler zijn van de afgeleide $(X^{q^n} - X)' = q^n X^{q^n - 1} - 1 = -1$, hetgeen niet mogelijk is. Om de stelling te bewijzen is het dus voldoende aan te tonen dat de optredende irreducibele factoren precies de irreducibele polynomen zijn waarvan de graad een deler van n is. Dat wil zeggen, voor $f \in \mathbb{F}_q[X]$ monisch en irreducibel moeten we aantonen:

$$f \mid X^{q^n} - X \quad \Leftrightarrow \quad \mathrm{gr}(f) \mid n\,.$$

Laat $d = \mathrm{gr}(f)$ en zij α een nulpunt van f in een uitbreiding M van $\mathbb{F}_q$ die ook $\mathbb{F}_{q^n}$ omvat (bijvoorbeeld $M = \Omega^f_{\mathbb{F}_{q^n}}$). Dan geldt $f = f^\alpha_{\mathbb{F}_q}$ (Stelling 9.8), dus $\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = \mathrm{gr}(f) = d$ en daarom $\mathbb{F}_{q^d} \cong \mathbb{F}_q(\alpha)$. Er geldt nu:

$$\begin{aligned} d \mid n \quad &\Leftrightarrow \quad \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \\ &\Leftrightarrow \quad \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n} \\ &\Leftrightarrow \quad \alpha \in \mathbb{F}_{q^n} \\ &\Leftrightarrow \quad \alpha \text{ is een nulpunt van } X^{q^n} - X \\ &\Leftrightarrow \quad f \mid X^{q^n} - X \qquad \text{(wegens 9.8(b))} \end{aligned}$$

Hiermee is 12.11 bewezen. □

Gevolg 12.12. *Zij x_d het aantal monische irreducibele d-de graads polynomen in $\mathbb{F}_q[X]$. Dan geldt voor alle $n \in \mathbb{Z}_{\geq 1}$:*

$$\sum_{d|n} d x_d = q^n \,.$$

Bewijs. Dit volgt uit de identiteit in Stelling 12.11 door de graden te vergelijken. □

Voorbeeld 12.13. Met behulp van 12.12 kan men x_n, het aantal irreducibele polynomen van graad n, recursief bepalen. Bijvoorbeeld, uit 12.12 vindt men voor $n = 1$, 2, 3 en 6:

$$\begin{array}{llllll} 1 \cdot x_1 & & & = & q^1 & \Rightarrow \quad x_1 = q \\ 1 \cdot x_1 & +2 \cdot x_2 & & = & q^2 & \Rightarrow \quad x_2 = \frac{1}{2}(q^2 - q) \\ 1 \cdot x_1 & & +3 \cdot x_3 & = & q^3 & \Rightarrow \quad x_3 = \frac{1}{3}(q^3 - q) \\ 1 \cdot x_1 & +2 \cdot x_2 & +3 \cdot x_3 \quad +6 \cdot x_6 & = & q^6 & \Rightarrow \quad x_6 = \frac{1}{6}(q^6 - q^3 - q^2 + q). \end{array}$$

In het algemeen vindt men met behulp van de *Moebius-inversie-formule* (zie Opgave 16):

$$x_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \,, \tag{12.13.1}$$

waarbij μ de *Moebiusfunctie* is (August Ferdinand Moebius, Duits wis- en sterrenkundige, 1790–1868):

$$\begin{cases} \mu(n) = 0 & \text{als er een priemgetal } p \text{ is met } p^2 | n \\ \mu(p_1 p_2 \ldots p_r) = (-1)^r, & \text{als } p_1, \ldots, p_r \text{ verschillende priemgetallen zijn.} \end{cases}$$

(I.h.b. is $\mu(1) = 1$ want dan is $r = 0$.)

Een ander bewijs van 12.12 kan gegeven worden door uitsluitend gebruik te maken van de eenduidigheid van priemfactorontbinding in $\mathbb{F}_q[X]$; zie Opgaven 9 en 12.

Volgens 8.5 is voor elk eindig lichaam $\mathbb{F}_{p^n}$ de afbeelding $F \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ met $F(x) = x^p$ een lichaamsautomorfisme. De volgende stelling spreekt uit dat de machten van F de enige automorfismen van $\mathbb{F}_{p^n}$ zijn.

Stelling 12.14. *Laat p een priemgetal zijn en $n \in \mathbb{Z}_{\geq 1}$. Dan is de automorfismengroep $\mathrm{Aut}(\mathbb{F}_{p^n})$ van het lichaam $\mathbb{F}_{p^n}$ een cyclische groep van orde n, voortgebracht door het Frobeniusautomorfisme F.*

Bewijs. Eerst bewijzen we dat F orde n heeft. Voor alle $x \in \mathbb{F}_{p^n}$ geldt

$$F^n(x) = x^{p^n} = x \,,$$

dus $F^n = \mathrm{id}$ (de identiteit). De orde van F is dus een deler van n. Omgekeerd, als $F^k = \mathrm{id}$, dan geldt $x^{p^k} = x$ voor alle $x \in \mathbb{F}_{p^n}$, dus het p^k-de graads polynoom $X^{p^k} - X$ heeft alle p^n elementen van $\mathbb{F}_{p^n}$ als nulpunten. Dit kan alleen als $k \geq n$ (wegens 3.7); dus de orde van F is precies n.

Hiermee hebben we bewezen dat de door F voortgebrachte ondergroep van $\mathrm{Aut}(\mathbb{F}_{p^n})$ orde n heeft. Stelling 12.14 zal dus bewezen zijn als we laten zien dat $\#\mathrm{Aut}(\mathbb{F}_{p^n})$ *hoogstens* n is.

Schrijf hiertoe $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, gebruik makend van 12.6. Het minimumpolynoom f van α over $\mathbb{F}_p$ heeft dan graad n, zeg $f = \sum_{i=0}^{n} a_i X^i$ met $a_i \in \mathbb{F}_p$ en $a_n = 1$. Uit $a_i \in \mathbb{F}_p$ (het priemlichaam)

volgt dat $\sigma(a_i) = a_i$ voor alle $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$; zie Hoofdstuk 8, Opgave 1. Laat nu $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$. Uit $\sum_{i=0}^{n} a_i\alpha^i = f(\alpha) = 0$ volgt, door σ toe te passen:

$$0 = \sigma(f(\alpha)) = \sum_{i=0}^{n} \sigma(a_i\alpha^i) = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i = \sum_{i=0}^{n} a_i\sigma(\alpha)^i = f\big(\sigma(\alpha)\big)\,.$$

Dus voor alle $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$ is $\sigma(\alpha)$ een nulpunt van f. Omdat f niet meer dan n nulpunten bezit (wegens 3.7), zijn er dus ten hoogste n mogelijkheden voor $\sigma(\alpha)$. Maar σ ligt helemaal vast door $\sigma(\alpha)$, want uit $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ blijkt dat elk element van $\mathbb{F}_{p^n}$ kan worden uitgedrukt in α. We concluderen dat het aantal σ's niet groter is dan n, d.w.z. $\#\mathrm{Aut}(\mathbb{F}_{p^n}) \leq n$, zoals verlangd. Hiermee is 12.14 bewezen. □

In de eerste helft van bovenstaand bewijs toonden we aan dat $\#\mathrm{Aut}(\mathbb{F}_{p^n}) \geq n$, in de tweede helft $\#\mathrm{Aut}(\mathbb{F}_{p^n}) \leq n$. Passen we de eerste bewering toe op wat we in het bewijs van de tweede bewering gezien hebben, dan vinden we dat het in dat bewijs voorkomende polynoom f kennelijk *precies* n nulpunten in $\mathbb{F}_{p^n}$ heeft, en dat deze gegeven worden door

$$\big\{\sigma(\alpha) \;\big|\; \sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})\big\}\,, \qquad \text{waarbij} \qquad \mathrm{Aut}(\mathbb{F}_{p^n}) = \{\mathrm{id}, F, F^2, \ldots, F^{n-1}\}$$

d.w.z. door

$$\alpha\,, \alpha^p\,, \alpha^{p^2}\,, \ldots, \alpha^{p^{n-1}}\,.$$

Dit leidt tot het volgende gevolg:

Gevolg 12.15. *Zij $f \in \mathbb{F}_p[X]$ een monisch irreducibel polynoom, en α een nulpunt van f in een uitbreiding van $\mathbb{F}_p$. Dan geldt in $\mathbb{F}_p(\alpha)\big[X\big]$:*

$$f = \prod_{i=0}^{n-1} \big(X - \alpha^{p^i}\big)\,, \qquad \textit{met } n = \mathrm{gr}(f)$$

en $\mathbb{F}_p(\alpha)$ is het ontbindingslichaam van f over $\mathbb{F}_p$.

Bewijs. De identiteit $f = \prod_{i=0}^{n-1} \big(X - \alpha^{p^i}\big)$ volgt omdat we gezien hebben dat het n-de graads polynoom f precies de n nulpunten $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ heeft. De bewering over het ontbindingslichaam volgt hier direct uit, aangezien $\mathbb{F}_p(\alpha) = \mathbb{F}_p(\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}})$. Dit bewijst 12.15. □

Opgaven

1. Is er een eindig lichaam van 143 elementen? Zelfde vraag voor 243 en 343.

2. Laat $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$. Bewijs dat de optel- en vermenigvuldig-tabel voor $\mathbb{F}_4$ er als volgt uitzien:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

   Controleer dat inderdaad geldt: $X \cdot (X-1) \cdot (X-\alpha) \cdot (X-\beta) = X^4 - X$, in $\mathbb{F}_4[X]$.

3. Laat M een lichaam zijn, en laten $K, L \subset M$ *eindige* deellichamen met evenveel elementen zijn. Bewijs $K = L$ (dus niet alleen $K \cong L$). (Aanwijzing: $X^q - X$ heeft niet meer dan q nulpunten.)

4. Bepaal alle primitieve wortels van $\mathbb{F}_4$ (zie Opgave 2). Bewijs dat elk eindig lichaam $\mathbb{F}_q$ precies $\phi(q-1)$ primitieve wortels bezit, waar ϕ de Euler-functie aangeeft.

5. Zij p een priemgetal met $p \equiv 3 \bmod 4$. Bewijs: $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{F}_{p^2}$.

6. Bepaal $f^{\alpha}_{\mathbb{F}_3}$ voor alle $\alpha \in \mathbb{F}_9$, en ontbind $X^8 - 1$ in irreducibele factoren in $\mathbb{F}_3[X]$.

7. Als $\alpha \in \mathbb{F}_{25}$ een element is met $\alpha^2 = 2$, bewijs dat $2 + \alpha \in \mathbb{F}_{25}$ een primitieve wortel is.

8. Bewijs dat $X^4 + 2$ irreducibel is in $\mathbb{F}_{125}[X]$.

9. (a) Bewijs dat het aantal monische tweedegraads polynomen $f \in \mathbb{F}_q[X]$ dat geschreven kan worden als $f = (X-\alpha)(X-\beta)$, $\alpha, \beta \in \mathbb{F}_q$ gelijk is aan $\frac{1}{2}q(q+1)$.

   (b) Concludeer uit 9a: het aantal monische *irreducibele* polynomen in $\mathbb{F}_q[X]$ van de graad twee bedraagt $q^2 - \frac{1}{2}q(q+1) = \frac{1}{2}(q^2 - q)$.

   (c) Bewijs op dezelfde manier: het aantal monische irreducibele polynomen in $\mathbb{F}_q[X]$ van de graad *drie* bedraagt $\frac{1}{3}(q^3 - q)$.

   (Dit zijn speciale gevallen van 12.12 en 12.13.1; zie ook Opgave 12.)

10. Bewijs, als $q = p^n$, $r = p^m$:

$$n \mid m \iff q - 1 \mid r - 1 \iff X^q - X \mid X^r - X \qquad (\text{in } \mathbb{F}_p[X])$$

    en leid hieruit een ander bewijs voor 12.9, (c) $\implies$ (a) af.

11. Ontbind de polynomen $X^2 - X$, $X^4 - X$, $X^8 - X$ en $X^{64} - X$ in $\mathbb{F}_2[X]$ in irreducibele factoren.

12. Zij $\mathbb{F}_q$ een eindig lichaam.

(a) Bewijs de volgende gelijkheid van machtreeksen, door gebruik te maken van de eenduidigheid van priemfactorontbinding in $\mathbb{F}_q[X]$:

$$\prod_{\substack{f\in\mathbb{F}_q[X]\\ \text{monisch en irr.}}} (1 + t^{\mathrm{gr}(f)} + t^{2\mathrm{gr}(f)} + t^{3\mathrm{gr}(f)} + \cdots) = \sum_{\substack{g\in\mathbb{F}_q[X]\\ \text{monisch}}} t^{\mathrm{gr}(g)}.$$

(b) Herschrijf 12a als volgt:

$$\prod_{n=1}^{\infty} \left(\frac{1}{1-t^n}\right)^{x_n} = \frac{1}{1-qt}$$

waarbij x_n het aantal monische irreducibele $f \in \mathbb{F}_q[X]$ met $\mathrm{gr}(f) = n$ voorstelt.

(c) Geef een nieuw bewijs van 12.12 door van de identiteit in 12b de logarithmische afgeleide te nemen.

13. Leid uit Gevolg 12.12 af:

$$\frac{1}{n}q^n \geq x_n \geq \frac{1}{n}\Big(q^n - \frac{q}{q-1}q^{\frac{1}{2}n}\Big).$$

14. Stel dat $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Bewijs rechtstreeks dat het in 12.15 voorkomende polynoom $\prod_{i=0}^{n-1}(X-\alpha^{p^i})$ coëfficiënten in $\mathbb{F}_p$ heeft, door na te gaan dat elke coëfficiënt c voldoet aan $c^p = c$.

15. Zij K een lichaam van karakteristiek $p > 0$, en laat $f \in K[X]$ een polynoom van de vorm $X^p - X - a$ zijn. Met α geven we een nulpunt van f in een uitbreidingslichaam van K aan.

(a) Bewijs: $f = \prod_{i\in\mathbb{F}_p}(X - \alpha - i)$, en $K(\alpha) = \Omega_K^f$.

(b) Bewijs dat f óf irreducibel in $K[X]$ is, óf in p lineaire factoren splitst in $K[X]$. (Aanwijzing: bewijs dat de irreducibele factoren van f alle dezelfde graad hebben.)

(c) Bewijs dat $X^p - X - a$ irreducibel in $\mathbb{F}_p[X]$ is, voor alle $a \in \mathbb{F}_p^*$.

16. Zij R de in Opgave 24 op blz. 18 gedefinieerde ring van alle aritmetische functies. Een element van R is een functie $f\colon \mathbb{Z}_{>0} \to \mathbb{C}$, en twee zulke functies f, g worden opgeteld en vermenigvuldigd door middel van de formules

$$(f+g)(n) = f(n) + g(n)$$
$$(f*g)(n) = \sum_{d|n} f(d)g(n/d)$$

(*convolutieproduct*), voor $n \in \mathbb{Z}_{>0}$. Definieer de functies $e, E \in R$ door

$$e(n) = \begin{cases} 1 & \text{als } n = 1 \\ 0 & \text{als } n > 1, \end{cases}$$
$$E(n) = 1 \quad \text{voor alle } n \in \mathbb{Z}_{>0}.$$

Laat verder $\mu \in R$ gedefinieerd zijn als in 12.13.1.

(a) Bewijs dat e het eenheidselement van de ring R is.

(b) Bewijs dat $\mu * E = e$ (dus μ is de *inverse* van E in R).

(c) Laat $f \in R$, en definieer $g \in R$ door

$$g(n) = \sum_{d|n} f(d) \quad \text{voor } n \in \mathbb{Z}_{>0}$$

(dus $g = f * E$). Leid uit (b) de *Moebius-inversieformule* af:

$$f(n) = \sum_{d|n} \mu(d) g(n/d) \quad \text{voor } n \in \mathbb{Z}_{>0}$$

(dus $f = \mu * g$).

(d) Bewijs 12.13.1.

17. (Vgl. Opgave 3 op blz. 124)

(a) Bewijs dat de lichamen $\mathbb{Q}[X]/(X^2-2)$ en $\mathbb{Q}[Y]/(Y^2-3)$ niet isomorf zijn.

(b) Bij gegeven priemgetal p, laat

$$R_2 = \mathbb{F}_p[X]/(X^2-2) \quad \text{en} \quad R_3 = \mathbb{F}_p[Y]/(Y^2-3).$$

Bepaal voor alle priemgetallen p vanaf 2 tot en met 23 de structuur van deze twee ringen, en beslis of ze isomorf zijn.

18. (Vgl. Stelling 12.15, en Definitie 14.5.) Als q een priemgetal is dan schrijven we $\Phi_q = X^{q-1} + \cdots + X^2 + X + 1 = (X^q - 1)/(X - 1) \in \mathbb{Z}[X]$; we nemen een priemgetal p en we schrijven $f_{q,p} = \Phi_q \bmod p \in \mathbb{F}_p[X]$.

Neem $q = 11$, neem p priem en beschouw

$$f_{11,p} = g_p = X^{10} + \cdots + X^2 + X + 1 \in \mathbb{F}_p[X].$$

Bewijs dat alle irreducibele factoren van g_p dezelfde graad hebben. Zij G een irreducibele factor van g_p. Bewijs:

$$\begin{aligned}
\mathrm{gr}(G) = 1 \qquad & \text{als } p = 11 \text{ of } p \equiv 1 \pmod{11}, \\
\mathrm{gr}(G) = 2 \qquad & \text{als } p \equiv -1 \pmod{11}, \\
\mathrm{gr}(G) = 5 \qquad & \text{als } p \equiv 3, 4, 5 \text{ of } 9 \pmod{11}, \\
\mathrm{gr}(G) = 10 \qquad & \text{als } p \equiv 2, 6, 7 \text{ of } 8 \pmod{11}.
\end{aligned}$$

19. Zij $g = f_{11,3}$ (notatie van Opgave 18), m.a.w. $g = X^{10} + \cdots + X + \bar{1} \in \mathbb{F}_3[X]$. Factoriseer g in irreducibele factoren. (Aanwijzing: zij a een nulpunt van G in een uitbreidingslichaam van $\mathbb{F}_3$, laat zien dat a^3 ook een nulpunt is, idem a^9, idem $a^{27} = a^5$, idem $a^{15} = a^4$. Wat is de constante term van G? Wat zijn de nulpunten van H als $g = G \cdot H$? Wat zijn de nulpunten van $X^5 \cdot G(1/X)$? Welke coëfficienten van G zijn ook nog gemakkelijk te berekenen?)

20. We gebruiken de notatie uit Opgave 18.

    (a) Factoriseer $f_{11,5} \in \mathbb{F}_5[X]$.

    (b) idem $f_{7,13} \in \mathbb{F}_{13}[X]$.

    (c) idem $f_{13,5} \in \mathbb{F}_5[X]$.

21. (a) Zij K een lichaam, $x \in K$ een element met $x^4 \neq 1$ en $x^8 = 1$. Bewijs dat $x^4 = -1$ en $(x + \frac{1}{x})^2 = 2$ (suggestie: teken x en $1/x$ in geval $K = \mathbb{C}$).

    (b) Bepaal de orde van $(3 \mod 41)$ in $\mathbb{F}_{41}^*$. Vind een $y \in \mathbb{Z}$ met $y^2 \equiv 2 \mod 41$.

    (c) Gegeven is een priemgetal p met $p \equiv 1 \mod 8$. Bewijs dat er een $z \in \mathbb{Z}$ bestaat met $z^2 \equiv 2 \mod p$.

22. (In opgave 21 probeerden we de vergelijking $z^2 \equiv 2 \mod p$ op te lossen, nu bestuderen we $x^2 \equiv 3 \mod p$). Zij p een priemgetal met $p \equiv 1 \mod 12$.

    (a) Bewijs dat er een $a \in \mathbb{F}_p^*$ bestaat met orde $(a \in \mathbb{F}_p^*) = 12$.

    (b) Kies een a als in (a), en zij $b = a^2$; bewijs dat $b + b^5 = 1$ (aanwijzing: laat zien dat $b^3 = -1$, $(b^2)^2 + b^2 + 1 = 0$, etc.).

    (c) Bewijs dat $(a^5 + a^7)^2 = 3 \in \mathbb{F}_p$.

    (d) Bewijs dat er een $x \in \mathbb{Z}$ is met $x^2 \equiv 3 \mod p$. (Suggestie: teken voor het complexe getal $z \in \mathbb{C}$ met $z = e^{2\pi i/12}$ plaatjes voor $z^2 + z^{10}$ en voor $z^5 + z^7$, etc.)

23. (Uit een wiskunde olympiade)

    (a) Vind $a, b \in \mathbb{Z}$ met:

        i. $ab(a + b) \neq 0 \mod 7$,

        ii. $(a + b)^7 \equiv a^7 + b^7 \mod 7^7$.

        Hoeveel oplossingen zijn er voor a en b in $(\mathbb{Z}/7^7)$?

    (b) (Een suggestie voor oplossingen) Zij $p \equiv 1 \mod 3$ een priemgetal, en $k \in \mathbb{Z}_{>0}$. Bewijs dat $X^2 + X + 1$ precies 2 nulpunten heeft in $\mathbb{Z}/p^k$. Vind die nulpunten voor $p^k = 7$, idem voor $p^k = 7^2$, etc.

    (c) (Idem) Zij $p \equiv 1 \mod 3$ een priemgetal, en $f = \frac{1}{p}((X + 1)^p - X^p - 1) \in \mathbb{Z}[X]$ (waarom heeft dat polynoom gehele coëfficienten?). Vind 4 irreducibele factoren (in $\mathbb{Z}[X]$ of in $\mathbb{Q}[X]$) van f (aanwijzing: als $w = e^{2\pi i/3}$, bereken dan $(w + 1)^6$, of teken een plaatje daarvan, substitueer w in f, etc.). Factoriseer f in geval $p = 7$.

Hoofdstuk 13

Algebraïsch afgesloten lichamen

Definitie 13.1. Een lichaam K heet *algebraïsch afgesloten* als er voor elke $f \in K[X]$ met $f \notin K$, een $\alpha \in K$ is met $f(\alpha) = 0$.

Uit de volgende stelling blijkt onder andere dat als K een algebraïsch afgesloten lichaam is, dat dan in feite elk polynoom $f \in K[X]$, $f \neq 0$, in $K[X]$ volledig in lineaire factoren splitst.

Stelling 13.2. *Laat K een lichaam zijn. Dan zijn de volgende uitspraken equivalent:*

(a) *K is algebraïsch afgesloten;*

(b) *elk irreducibel polynoom in $K[X]$ is lineair;*

(c) *de enige algebraïsche uitbreiding L van K is $L = K$;*

(d) *voor elke monische $f \in K[X]$ bestaan er $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ met $f = \prod_{i=1}^{n}(X - \alpha_i)$.*

Bewijs. (a) $\Rightarrow$ (b). Een irreducibel polynoom kan alleen een nulpunt in K hebben als het linear is (vgl. 5.2).

(b) $\Rightarrow$ (c). Laat L algebraïsch over K zijn. Dan is voor elke $\alpha \in L$ het polynoom f_K^α irreducibel in $K[X]$, dus graad $(f_K^\alpha) = 1$ wegens (b). Ook weten we uit Stelling 9.8(d) dat $[K(\alpha) : K] =$ graad (f_K^α), dus $[K(\alpha) : K] = 1$ en $K(\alpha) = K$. Dit bewijst $\alpha \in K$, voor alle $\alpha \in L$, dus $L = K$.

(c) $\Rightarrow$ (d). Omdat het ontbindingslichaam Ω_K^f algebraïsch over K is volgt uit (c) dat $\Omega_K^f = K$, hetgeen precies is wat we moesten bewijzen.

(d) $\Rightarrow$ (a). Dit is duidelijk, want elke α_i is een nulpunt van f. Hiermee is Stelling 13.2 bewezen. □

Stelling 13.3. *Elk algebraïsch afgesloten lichaam K is oneindig.*

Bewijs. Als K eindig is, $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, dan heeft het polynoom

$$f = 1 + \prod_{i=1}^{n}(X - \alpha_i)$$

geen nulpunt in K, want voor alle α_i geldt $f(\alpha_i) = 1 \neq 0$. Dit bewijst 13.3. □

De volgende stelling stond vroeger bekend als de "hoofdstelling van de algebra".

Stelling 13.4. *Het lichaam $\mathbb{C}$ der complexe getallen is algebraïsch afgesloten.*

Voor een eenvoudig analytisch bewijs van deze stelling, gebruik makend van de stelling van Liouville, verwijzen we naar het college functietheorie. We zullen hier een bewijs geven waarvan het enige niet-algebraïsche ingrediënt het volgend lemma is.

Lemma 13.5. *Zij $f \in \mathbb{R}[X]$, en veronderstel dat er $\beta, \gamma \in \mathbb{R}$ bestaan met $f(\beta) > 0$ en $f(\gamma) < 0$. Dan is er een $\alpha \in \mathbb{R}$ met $f(\alpha) = 0$.*

Bewijs. Dit is een speciaal geval van de tussenwaardestelling uit de analyse, want polynomen zijn continue functies. □

Merk op dat we, in 13.5, α tussen β en γ kunnen kiezen maar dit zullen we niet nodig hebben.

Voor we het volledige bewijs van Stelling 13.4 geven leiden we enkele hulpresultaten af.

Lemma 13.6. *Zij $f \in \mathbb{C}[X]$ een tweedegraads polynoom. Dan heeft f een nulpunt in $\mathbb{C}$.*

Bewijs. We mogen aannemen dat f monisch is: $f = X^2 + \beta X + \gamma$, met $\beta, \gamma \in \mathbb{C}$. Uit

$$f = (X + \frac{1}{2}\beta)^2 - (\frac{1}{4}\beta^2 - \gamma)$$

blijkt dat het voldoende is aan te tonen dat het complexe getal $\frac{1}{4}\beta^2 - \gamma$ een wortel in $\mathbb{C}$ heeft.

Schrijf $\frac{1}{4}\beta^2 - \gamma = a + bi$, met $a, b \in \mathbb{R}$. We beschouwen eerst het geval $b = 0$. Als $a > 0$ dan heeft a een wortel $\sqrt{a}$ in $\mathbb{R}$, zoals we zien door 13.5 op het polynoom $g = X^2 - a$ toe te passen en op te merken dat $g(0) < 0$, $g(a+1) > 0$. Als $a < 0$, dan heeft a een wortel $i\sqrt{|a|}$ in $\mathbb{C}$. Als $a = 0$ dan is 0 natuurlijk een wortel van a. Hiermee is het geval $b = 0$ afgehandeld.

We zoeken nu $c, d \in \mathbb{R}$ met:

$$(c + di)^2 = (c^2 - d^2) + 2cdi = a + bi.$$

Dit is equivalent met

$$c^2 - d^2 = a, \qquad 2cd = b.$$

Omdat $b \neq 0$ zijn ook c, $d \neq 0$, en dus kunnen we schrijven:

$$c = \frac{b}{2d}, \qquad \text{dus} \quad \frac{b^2}{4d^2} - d^2 = a.$$

Het reële getal d moet dus een nulpunt zijn van het polynoom:

$$g = 4X^4 + 4aX^2 - b^2 \in \mathbb{R}[X].$$

Er geldt $g(0) < 0$ en $g(x) > 0$ voor $x \in \mathbb{R}$ voldoende groot, dus er is wegens 13.5 inderdaad een $d \in \mathbb{R}$ met $g(d) = 0$. We vinden vervolgens c uit: $c = \frac{b}{2d}$.

Hiermee is bewezen dat $a + bi$ een wortel $c + di$ in $\mathbb{C}$ heeft, zoals verlangd. Dit bewijst 13.6. □

Lemma 13.7. *Zij $f \in \mathbb{R}[X]$ een polynoom van oneven graad. Dan heeft f een nulpunt in $\mathbb{R}$.*

Bewijs. We mogen aannemen dat de hoogstegraads coëfficiënt van f positief is. Dan geldt $f(x) > 0$ als $x \in \mathbb{R}$ voldoende groot is, en omdat f oneven graad heeft is $f(x) < 0$ als $x \in \mathbb{R}_{<0}$ voldoende klein is. Uit 13.5 volgt nu dat f een nulpunt in $\mathbb{R}$ heeft. Hiermee is 13.7 bewezen. □

Lemma 13.8. *Stel dat elk niet-constant polynoom $f \in \mathbb{R}[X]$ (dus met reële coëfficiënten) een nulpunt in $\mathbb{C}$ heeft. Dan is $\mathbb{C}$ algebraïsch afgesloten.*

Bewijs. Zij $g = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, $g \notin \mathbb{C}$. We moeten bewijzen dat g een nulpunt in $\mathbb{C}$ heeft. Definieer

$$\bar{g} := \sum_{i=0}^{n} \bar{a}_i X^i \quad (\in \mathbb{C}[X])$$

waar $\bar{a}_i$ de complex geconjugeerde van a_i aangeeft, en definieer

$$f := g \cdot \bar{g} \quad (\in \mathbb{C}[X]).$$

Gebruik makende van de eenvoudig te controleren regel $\overline{gh} = \bar{g} \cdot \bar{h}$ vinden we

$$\bar{f} = \overline{g \cdot \bar{g}} = \bar{g} \cdot \bar{\bar{g}} = \bar{g} \cdot g = f$$

dus *elke* coëfficiënt van f is gelijk aan zijn complex geconjugeerde, d.w.z. $f \in \mathbb{R}[X]$. Verder geldt $\mathrm{gr}(f) = 2 \cdot \mathrm{gr}(g)$, dus f is niet een constante. Op f kunnen we nu het gegeven van het lemma toepassen: er is een $\alpha \in \mathbb{C}$ met $f(\alpha) = 0$, d.w.z.

$$g(\alpha) \cdot \bar{g}(\alpha) = 0.$$

Als $g(\alpha) = 0$ dan hebben we het verlangde nulpunt α van g gevonden. Als $g(\alpha) \neq 0$, dan moeten we hebben $\bar{g}(\alpha) = 0$, dus

$$\sum_{i=0}^{n} \bar{a}_i \alpha^i = 0.$$

Neem hiervan de complex geconjugeerde, dan vinden we

$$\sum_{i=0}^{n} a_i \bar{\alpha}^i = 0,$$

d.w.z. $g(\bar{\alpha}) = 0$, dus ook in dit geval heeft g een nulpunt in $\mathbb{C}$. Hiermee is Lemma 13.8 bewezen. □

Bewijs van Stelling 13.4. Zij $f \in \mathbb{R}[X]$ een niet-constant polynoom. Volgens Lemma 13.8 is het voldoende aan te tonen dat f een nulpunt in $\mathbb{C}$ heeft. We mogen, en zullen, aannemen dat f monisch is. Laat $n = \mathrm{gr}(f)$. Dan geldt $n \geq 1$, en we kunnen schrijven $n = 2^k u$ met $k \in \mathbb{Z}_{\geq 0}$ en u een *oneven* positief geheel getal. Het bewijs zal nu worden gevoerd met volledige inductie naar k, d.w.z. naar het aantal factoren 2 in n.

Als $k = 0$ dan is de graad van f *oneven*, dus dan weten we uit 13.7 dat f een nulpunt in $\mathbb{C}$ (zelfs in $\mathbb{R}$) heeft.

Laat vervolgens $k \geq 1$, dus n *even*. We zullen gaan werken in het lichaam $L = \Omega_{\mathbb{C}}^{f}$, dat $\mathbb{C}$ omvat. (Natuurlijk blijkt uit Stelling 13.4 uiteindelijk dat $L = \mathbb{C}$, maar dat weten we nu nog niet, en dat zullen we ook niet nodig hebben.) In $L[X]$ kunnen we f volledig in lineaire factoren splitsen:

$$f = \prod_{i=1}^{n}(X - \alpha_i), \qquad \alpha_i \in L \quad (1 \leq i \leq n).$$

Zij c een willekeurig reëel getal, en beschouw het polynoom

$$g_c = \prod_{1 \leq i < j \leq n} (X - (\alpha_i + \alpha_j + c\alpha_i\alpha_j)) \qquad (\in L[X]).$$

We zullen nu in het bewijs gebruik maken van een resultaat uit Hoofdstuk 7. Elk van de coëfficiënten van g_c is een symmetrische uitdrukking in $\alpha_1, \alpha_2, \ldots, \alpha_n$, dus behoort wegens Stelling 7.5 (toegepast op $R = \mathbb{R}$, $R' = L$) tot $\mathbb{R}$. Dit bewijst dat $g_c \in \mathbb{R}[X]$.

De graad van g_c is gelijk aan het aantal keuzen voor i en j met $1 \leq i < j \leq n$, en dat is $\frac{1}{2}n(n-1) = 2^{k-1} \cdot u \cdot (n-1)$. Hier is $n-1$ *oneven*, dus we zien: het aantal factoren 2 in $\mathrm{gr}(g_c)$ is gelijk aan $k-1$. Op het polynoom g_c kunnen we dus de inductiehypothese toepassen, die ons vertelt dat g_c een nulpunt in $\mathbb{C}$ heeft. Maar de nulpunten van g_c zijn precies de $\frac{1}{2}n(n-1)$ uitdrukkingen $\alpha_i + \alpha_j + c\alpha_i\alpha_j$.

We concluderen: voor elk reëel getal c zijn er i en j met $1 \leq i < j \leq n$ en $\alpha_i + \alpha_j + c\alpha_i\alpha_j \in \mathbb{C}$. Hierbij hangen i en j van c af. Maar er is slechts een eindig aantal mogelijkheden voor i en j (nl. $\frac{1}{2}n(n-1)$), terwijl we oneindig veel reële getallen c tot onze beschikking hebben. Dit betekent dat er zeker twee *verschillende* reële getallen c en c' moeten bestaan die het *zelfde* paar i, j opleveren. Voor deze c, c', i, j, geldt dan

$$\alpha_i + \alpha_j + c\alpha_i\alpha_j \in \mathbb{C}, \qquad \alpha_i + \alpha_j + c'\alpha_i\alpha_j \in \mathbb{C}.$$

Nemen we hiervan geschikte lineaire combinaties, dan zien we dat ook de uitdrukkingen

$$\beta = \alpha_i + \alpha_j, \quad \gamma = \alpha_i\alpha_j \ \in \mathbb{C} \quad \text{dus} \quad (X - \alpha_i)(X - \alpha_j) = X^2 - \beta X + \gamma \in \mathbb{C}[X].$$

Uit lemma 13.6 volgt nu dat dit polynoom een nulpunt in $\mathbb{C}$ heeft, dus $\alpha_i \in \mathbb{C}$ of $\alpha_j \in \mathbb{C}$. Hiermee is aangetoond dat f een nulpunt in $\mathbb{C}$ heeft, zoals verlangd.

Dit besluit de inductiestap en het bewijs van Stelling 13.4. □

Het hier gegeven bewijs van 13.4 gaat terug op C.F. Gauss (1777–1855).

Gevolg 13.9. *Elk irreducibel polynoom $f \in \mathbb{R}[X]$ heeft graad 1 of 2. Een tweede graads polynoom $X^2 + bX + c \in \mathbb{R}[X]$ is irreducibel in $\mathbb{R}[X]$ dan en slechts dan als $b^2 - 4c < 0$.*

Bewijs. Zij $f \in \mathbb{R}[X]$ een monisch irreducibel polynoom, en $\alpha \in \mathbb{C}$ een nulpunt van f. Dan $f = f_{\mathbb{R}}^{\alpha}$, en met 10.3 vinden we

$$\mathrm{gr}(f) = [\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$$

waarbij we gebruiken dat $\mathbb{R}(\alpha) \subset \mathbb{C}$. Dit bewijst de eerste bewering van 13.9. De tweede bewering volgt uit

$$X^2 + bX + c = (X + \frac{1}{2}b)^2 - \frac{1}{4}(b^2 - 4c)$$

en het feit dat $X^2 - a$ irreducibel in $\mathbb{R}$ is dan en slechts dan als $a < 0$. Hiermee is 13.9 bewezen. □

Definitie 13.10. Een *algebraïsche afsluiting* van een lichaam K is een uitbreiding $K \subset \bar{K}$ met de eigenschappen

(a) $\bar{K}$ is algebraïsch over K;

(b) $\bar{K}$ is algebraïsch afgesloten.

Verwar dit begrip niet met de na Stelling 10.8 gedefinieerde algebraïsche afsluiting van K in een uitbreidingslichaam L.

Voorbeeld 13.11. Het lichaam $\mathbb{C}$ is een algebraïsche afsluiting van $\mathbb{R}$.

Stelling 13.12. *Het lichaam $\mathbb{Q}$ der rationale getallen bezit een algebraïsche afsluiting.*

Bewijs. Zij $\bar{\mathbb{Q}}$ de algebraïsche afsluiting van $\mathbb{Q}$ in $\mathbb{C}$:

$$\overline{\mathbb{Q}} = \left\{\alpha \in \mathbb{C} \;\middle|\; \alpha \text{ is algebraïsch over } \mathbb{Q}\right\}.$$

Dit is volgens 10.8(b) een lichaamsuitbreiding van $\mathbb{Q}$, die kennelijk voldoet aan voorwaarde (a) uit Definitie 13.10. We controleren voorwaarde (b), waarmee dan bewezen is dat $\bar{\mathbb{Q}}$ een algebraïsche afsluiting van $\mathbb{Q}$ is.

Laat $f \in \bar{\mathbb{Q}}[X]$ een niet-constant polynoom zijn. We moeten aantonen dat f een nulpunt in $\bar{\mathbb{Q}}$ heeft. Wegens 13.4 heeft f in ieder geval een nulpunt α in $\mathbb{C}$. Voor deze α geldt dan, dat $\overline{\mathbb{Q}}(\alpha)$ algebraïsch over $\overline{\mathbb{Q}}$ is. Omdat $\overline{\mathbb{Q}}$ op zijn beurt algebraïsch over $\mathbb{Q}$ is, volgt uit 10.9 dat $\overline{\mathbb{Q}}(\alpha)$ algebraïsch over $\mathbb{Q}$ is. In het bijzonder is α algebraïsch over $\mathbb{Q}$, d.w.z. $\alpha \in \bar{\mathbb{Q}}$, zoals verlangd. Dit bewijst 13.12. □

Opmerking 13.13. De algebraïsche afsluiting van $\mathbb{Q}$ is zeker *niet* gelijk aan $\mathbb{C}$, want er bestaan immers transcendente getallen, d.w.z. complexe getallen die niet algebraïsch over $\mathbb{Q}$ zijn, zie 9.5.

Algemener hebben we:

Stelling 13.14. *Elk lichaam K heeft een algebraïsche afsluiting $\bar{K}$. Bovendien is $\bar{K}$ op K-isomorfie na eenduidig bepaald, d.w.z.: zijn $\bar{K}$ en $\tilde{K}$ allebei algebraïsche afsluitingen van K, dan geldt $\bar{K} \cong_K \tilde{K}$.*

Bewijs. Laat K een lichaam zijn. Eerst gaan we het *bestaan* van een algebraïsche afsluiting bewijzen, en hiertoe gaan we eerst *alle* ontbindingslichamen van monische polynomen met coëfficiënten uit K combineren tot een ring R.

Laat V de verzameling van alle monische polynomen $f \in K[X]$ zijn. Voor elke $f \in V$ zij $R_f = \Omega_K^f$. We beschouwen de ring $R = \prod_{f \in V} R_f$. Elementen hiervan zijn rijtjes $x = (x_f)_{f \in V}$ met $x_f \in R_f$ voor alle $f \in V$, en deze rijtje worden componentsgewijs opgeteld en vermenigvuldigd. De 1 in R is het element waarvan alle componenten gelijk aan $1 \in K \subset R_f$ zijn. In het algemeen kunnen we voor elke

$c \in K$ het element van R beschouwen waarvan alle componenten gelijk aan c zijn; dit element zullen we gewoon met c aangeven; op deze manier wordt K dus opgevat als een deelring van R.

Zij nu $g \in V$ willekeurig. We gaan onderzoeken in hoeverre het waar is dat $g \in R[X]$ volledig in lineaire factoren kan worden ontbonden. In ieder geval kan g in $R_g[X]$ volledig in lineaire factoren worden ontbonden, want $R_g = \Omega_K^g$. Algemener, als g een deler is van f, dan ontbindt f, dus ook g, volledig in lineaire factoren in $R_f[X]$.

Laten we $n = \mathrm{gr}(g)$, dan zijn er voor elke $f \in V$ met $g|f$ dus $\alpha_{1,f}, \ldots, \alpha_{n,f} \in R_f$ te vinden waarvoor geldt

$$g = \prod_{i=1}^{n}(X - \alpha_{i,f}) \quad \text{in } R_f[X] \qquad \text{voor } g|f. \tag{13.14.1}$$

Voor $f \in V$ die *niet* deelbaar zijn door g kiezen we $\alpha_{i,f} \in R_f$ willekeurig, bijvoorbeeld $\alpha_{i,f} = 0$ $(1 \leq i \leq n)$. Natuurlijk hoeft (13.14.1) dan voor zulke f niet te gelden. Voor elke i met $1 \leq i \leq n$, zij $\alpha_i \in R$ nu het element met componenten $\alpha_{i,f}$; dus $\alpha_i = (\alpha_{i,f})_{f \in V}$. Beschouw nu het polynoom

$$g - \prod_{i=1}^{n}(X - \alpha_i) \in R[X].$$

De gelijkheid (13.14.1) wil juist zeggen dat de f-de component van de coëfficiënten van dit polynoom *nul* is, voor elke $f \in V$ die deelbaar is door g (voor de overige f weten we dat niet). Met andere woorden,

$$g - \prod_{i=1}^{n}(X - \alpha_i) \in I_g[X] \tag{13.14.2}$$

waar

$$I_g = \big\{(x_f)_{f \in V} \in R \;\big|\; x_f = 0 \text{ voor alle } f \text{ met } g \mid f\big\}.$$

Men gaat gemakkelijk na dat I_g een *ideaal* is van R met $1 \notin I_g$. We kunnen 13.14.2 ook uitdrukken door te zeggen dat g modulo het ideaal I_g, d.w.z. over de ring R/I_g, in lineaire factoren uiteenvalt. Deze ring R/I_g hangt echter nog van g af, en daar gaan we wat aan doen door naar een groter ideaal uit te delen.

We definiëren

$$I = \bigcup_{g \in V} I_g \subset R$$

en we beweren dat I een *ideaal* van R is. Bewijs hiervan: laten $x = (x_f)_{f \in V}$ en $y = (y_f)_{f \in V}$ tot I behoren, we gaan bewijzen dat $x - y = (x_f - y_f)_{f \in V}$ ook tot I behoort. Het feit dat x tot I behoort wil zeggen dat er een $g_1 \in V$ is met $x_f = 0$ voor alle f die deelbaar zijn door g_1; en evenzo, $y \in I$ betekent dat er een $g_2 \in V$ is met $y_f = 0$ voor alle f deelbaar door g_2. Dan geldt $x_f = y_f = 0$ voor alle f die deelbaar zijn door $g_1 g_2$, dus $x_f - y_f = 0$ voor die f, dus $x - y \in I_{g_1 g_2} \subset I$. Dit bewijst dat $x - y \in I$. Het controleren van de andere eigenschappen waar een ideaal aan moet voldoen is veel eenvoudiger, en wordt aan de lezer overgelaten.

Hiermee is aangetoond dat I een ideaal van R is. Omdat $1 \notin I_g$ voor alle $g \in V$ geldt $1 \notin I$. Wegens Gevolg 4.19 is er dus een maximaal ideaal $M \subset R$ met de eigenschap $I \subset M$. Deze M omvat

alle I_g, dus (13.14.2) impliceert:

$$\begin{aligned} &\text{voor elke } g \in V \text{ zijn er } \alpha_1, \alpha_2, \ldots, \alpha_n \in R, \text{ met } n = \mathrm{gr}(g), \\ &\text{waarvoor geldt } g - \prod_{i=1}^{n}(X - \alpha_i) \in M[X]. \end{aligned} \tag{13.14.3}$$

We gaan nu kijken naar $L = R/M$. Dit is een *lichaam* wegens 4.9. De samenstelling van de afbeeldingen $K \to R$ (de inclusie) en $R \to R/M$ (de canonieke afbeelding) is een ringhomomorfisme $K \to L$, en wegens 2.18 is het *injectief*. Dit stelt ons in staat K als een *deellichaam* van L op te vatten. Schrijven we $\beta_i =$ (beeld van α_i in L), dan betekent (13.14.3):

$$\begin{aligned} &\text{voor elke } g \in V \text{ zijn er } \beta_1, \alpha_2, \ldots, \beta_n \in L \\ &\text{met } g = \prod_{i=1}^{n}(X - \beta_i) \text{ in } L[X] = R[X]/M[X]. \end{aligned} \tag{13.14.4}$$

Deze β_i zijn nulpunten van $g \in K[X]$, dus ze zijn algebraïsch over K. Definiëren we

$$\overline{K} = \big\{\beta \in L \;\big|\; \beta \text{ is algebraïsch over } K\big\}$$

dan is (13.14.4) dus ook waar met L vervangen door $\overline{K}$.

Wegens 10.8(b) is $\overline{K}$ een lichaamsuitbreiding van K, en $\overline{K}$ is kennelijk algebraïsch over K. Om aan te tonen dat $\overline{K}$ een algebraïsche afsluiting van K is hoeven we dus nog slechts na te gaan dat $\overline{K}$ algebraïsch afgesloten is. Zij L' dus een willekeurige algebraïsche uitbreiding van $\overline{K}$; volgens 13.2 is het voldoende te bewijzen dat $L' = \overline{K}$. Laat $\alpha \in L'$. Merk op dat L' wegens 10.9 algebraïsch over K is, dus α heeft een minimumpolynoom g over K. Wegens (13.14.4) (met $\overline{K}$ i.p.v. L) zijn er $\beta_1, \ldots, \beta_n \in \overline{K}$ met $g = \prod_{i=1}^{n}(X - \beta_i)$, dus $0 = g(\alpha) = \prod_{i=1}^{n}(\alpha - \beta_i)$, d.w.z. er is een i met $\alpha = \beta_i$. Hieruit zien we dat $\alpha \in \overline{K}$, dus $L' = \overline{K}$.

Dit besluit het bewijs dat $\overline{K}$ een algebraïsche afsluiting van K is. Om het bewijs van 13.14 af te maken moeten we nog de *eenduidigheid* van de algebraïsche afsluiting aantonen.

Laten $\overline{K}$ en $\tilde{K}$ dus twee algebraïsche afsluitingen van K zijn. Om te bewijzen dat $\overline{K} \cong_K \tilde{K}$ passen we het lemma van Zorn (zie 4.17) toe op de verzameling

$$P = \left\{ (E_0, \phi, E_1) \;\middle|\; \begin{array}{l} E_0 \text{ is een deellichaam van } \overline{K} \text{ met } K \subset E_0, \\ E_1 \text{ is een deellichaam van } \tilde{K} \text{ met } K \subset E_1, \\ \phi\colon E_0 \to E_1, \text{ is een } K\text{-isomorfisme} \end{array} \right\}.$$

De verzameling P is zeker niet leeg, want $(K, \mathrm{id}_K, K) \in P$. Het is onze bedoeling een element van P van de vorm $(\overline{K}, \phi, \tilde{K})$ te vinden. Hiertoe definiëren we een ordening $\leq$ op P door

$(E_0, \phi, E_1) \leq (L_0, \psi, L_1)$ dan en slechts dan als $E_0 \subset L_0, E_1 \subset L_1$, en $\psi_{|E_0} = \phi$. (Zie diagram.)

$$\begin{array}{ccc} \overline{K} & & \tilde{K} \\ \bigcup & & \bigcup \\ L_0 & \xrightarrow{\psi} & L_0 \\ \bigcup & & \bigcup \\ E_0 & \xrightarrow{\phi} & E_1 \\ \bigcup & & \bigcup \\ K & \xrightarrow{\mathrm{id}} & K \end{array}$$

Het is gemakkelijk na te gaan dat P op deze manier een partieel geordende verzameling wordt. We beweren dat P voldoet aan de voorwaarde uit het lemma van Zorn: heeft men een *keten* elementen $(E_{0,i}, \phi_i, E_{1,i})$ van P, waarbij i een indexverzameling doorloopt, dan gaat men gemakkelijk na dat $E_0 = \cup_i E_{0,i}$ en $E_1 = \bigcup_i E_{1,i}$ deellichamen van $\overline{K}$ resp. $\tilde{K}$ zijn die K omvatten; dat er een welgedefinieerd K-isomorfisme $\phi\colon E_0 \to E_1$ is met $\phi(x) = \phi_i(x)$ voor alle $x \in E_{0,i}$ en voor alle i; en dat het element (E_0, ϕ, E_1) van P een bovengrens voor de hele keten is. Hiermee is dan de voorwaarde van het lemma van Zorn gecontroleerd.

Het lemma van Zorn zegt nu dat P een maximaal element (E_0, ϕ, E_1) heeft. We beweren dat daarvoor geldt $E_0 = \overline{K}$ en $E_1 = \tilde{K}$. Stel dat dit niet het geval is. Dan is er een $\alpha \in \overline{K}$ te vinden met $\alpha \notin E_0$ of anders wel een $\alpha \in \tilde{K}$ met $\alpha \notin E_1$. Zo'n α is algebraïsch over K, laat $f(\alpha) = 0$ met $f \in K[X]$ monisch.

Laat nu L_i het deellichaam van $\overline{K}$ resp. $\tilde{K}$ zijn dat voortgebracht wordt door E_i en de nulpunten van f, voor $i = 0$ en $i = 1$. Aangezien $\overline{K}$ en $\tilde{K}$ algebraïsch afgesloten zijn is L_i een ontbindigslichaam van f over E_i, en bovendien $\alpha \in L_0$ of L_1, dus er geldt $E_0 \neq L_0$ of $E_1 \neq L_1$. Passen we nu 11.4 toe (met K_0, K_1 vervangen door E_0, E_1, en $f_0 = f_1 = f$) dan zien we dat het isomorfisme $\phi\colon E_0 \to E_1$ zich voort laat zetten tot een isomorfisme $\psi\colon L_0 \to L_1$. Dit bewijst dat er een element (L_0, ψ, L_1) van P is, met

$$(E_0, \phi, E_1) < (L_0, \psi, L_1)$$

($<$ betekent $\leq$ maar niet $=$). Hiermee is een tegenspraak met de maximaliteit van (E_0, ϕ, E_1) bereikt.

We concluderen dat $E_0 = \overline{K}$, $E_1 = \tilde{K}$, dus er is een K-isomorfisme $\phi\colon \overline{K} \to \tilde{K}$, zoals verlangd. Hiermee is 13.14 bewezen. □

We merken op dat noch het bewijs van het bestaan noch het bewijs van de eenduidigheid van de algebraïsche afsluiting constructief is: in beide gevallen hebben we van het lemma van Zorn gebruik gemaakt, éénmaal via 4.19.

Voor een ander bewijs van het bestaan van de algebraïsche afsluiting verwijzen we naar S. Lang, Algebra, Ch. VII, §2.

Opgaven

1. Zij $K = \mathbb{F}_q$ een eindig lichaam van karakteristiek p en $f = 1 + \prod_{\alpha \in K}(X - \alpha)$ het polynoom dat optreedt in het bewijs van 13.3. Laat verder $L = \Omega_K^f$. Bewijs:

   (a) $f = X^q - X + 1$;

   (b) voor elke $\alpha \in L$ met $f(\alpha) = 0$ geldt

   $$\alpha^{q^i} = \alpha - \bar{i} \quad \text{voor alle } i \in \mathbb{Z}_{>0}$$

   met $\bar{i} = (i \bmod p) \in \mathbb{F}_p \subset K$, en

   $$\alpha^{q^p} = \alpha;$$

   (c) $L = \mathbb{F}_{q^p}$;

   (d) elke irreducibele factor van f in $K[X]$ heeft graad p.

2. Zij $\bar{K}$ een algebraïsche uitbreiding van een lichaam K met de eigenschap dat $\bar{K}$ voor elke monische $f \in K[X]$ een ontbindingslichaam van f over K bevat. Bewijs dat $\bar{K}$ een algebraïsche afsluiting van K is.

3. Zij $\bar{\mathbb{Q}}$ de algebraïsche afsluiting van $\mathbb{Q}$ in $\mathbb{C}$. Bewijs: $[\bar{\mathbb{Q}} : \bar{\mathbb{Q}} \cap \mathbb{R}] = 2$.

Hoofdstuk 14

Eenheidswortels en cyclotomische polynomen

Definitie 14.1. Laat K een lichaam zijn. Een element $\zeta \in K$ heet een *eenheidswortel* als er een $n \in \mathbb{Z}_{>0}$ is met $\zeta^n = 1$; met andere woorden, als ζ eindige orde heeft in de multiplicatieve groep $K^* = K \setminus \{0\}$. Als $\zeta^n = 1$ dan is de orde van ζ een deler van n; men noemt ζ dan een n-de machts eenheidswortel, of kortweg n-de eenheidswortel. Als de orde van ζ gelijk is aan n, dan heet ζ een *primitieve* n-de machts eenheidswortel.

Voorbeelden 14.2. De enige eenheidswortels in $\mathbb{Q}$ en $\mathbb{R}$ zijn 1 (een primitieve eerstemachts eenheidswortel) en -1 (een primitieve tweedemachts eenheidswortel). De primitieve n-de machts eenheidswortels in $\mathbb{C}$ zijn precies de getallen $e^{2\pi i a/n}$ met $a \in \{1, 2, \ldots, n\}$ en $\gcd(a, n) = 1$; het aantal hiervan is $\varphi(n)$. Elk element ongelijk aan nul van een eindig lichaam $\mathbb{F}_q$ is een $(q-1)$-ste eenheidswortel.

Stelling 14.3. *Zij K een lichaam, $n \in \mathbb{Z}_{>0}$, en $L = \Omega_K^{X^n-1}$ het ontbindingslichaam van $X^n - 1$ over K.*

(a) *Als n niet deelbaar is door* $\mathrm{char}(K)$*, dan is de verzameling n-de machts eenheidswortels in L een cyclische groep van orde n, en het aantal primitieve n-de eenheidswortels in L is gelijk aan $\varphi(n)$.*

(b) *Als n wel deelbaar is door* $\mathrm{char}(K)$ *en $n = n_0 \cdot p^m$ met $p = \mathrm{char}(K)$ en $p \nmid n_0$, dan valt de verzameling n-de eenheidswortels in L samen met de verzameling van n_0-de eenheidswortels in L; dit is een cyclische groep van orde n_0 en er bestaan geen primitieve n-de eenheidswortels in L.*

Bewijs. (a) Als $X^n - 1$ een dubbel nulpunt α heeft in L, dan is α ook een nulpunt van de afgeleide $n \cdot X^{n-1}$, dus $n \cdot \alpha^{n-1} = 0$. Maar $\alpha \neq 0$ (want $\alpha^n = 1$), dus $n = 0$, hetgeen betekent dat n deelbaar is door $\mathrm{char}(K)$, in tegenspraak met de aannamen van (a). We concluderen dat $X^n - 1$ geen dubbele nulpunten heeft, en dat $\{\alpha \in L \mid \alpha^n = 1\}$ dus precies $\mathrm{gr}(X^n - 1) = n$ elementen heeft. Het is duidelijk dat het een ondergroep van L^* is, en uit Stelling 3.14 volgt nu dat deze groep cyclisch is. Omdat een cyclische groep van orde n precies $\varphi(n)$ elementen van orde n heeft, is het aantal primitieve n-de eenheidswortels in L gelijk aan $\varphi(n)$. Dit bewijst (a).

(b) Als $n = n_0 p^m$ met $m \geq 1$ en $p \nmid n_0$, dan is

$$X^n - 1 = X^{n_0 p^m} - 1^{p^m} = (X^{n_0} - 1)^{p^m}$$

wegens Stelling 8.4 (toegepast op het quotiëntenlichaam van $K[X]$). Dus de verzameling van nulpunten van $X^n - 1$ valt samen met de verzameling van nulpunten van $X^{n_0} - 1$. Wegens (a) vormen deze een

cyclische groep van n_0 elementen. Deze hebben alle orde $\leq n_0 < n$ dus primitieve n-de eenheidswortels in L bestaan niet. Hiermee is 14.3 bewezen. □

Voorbeelden 14.4. De primitieve 3-de eenheidswortels in $\mathbb{F}_7$ zijn $\bar{2}$ en $\bar{2}^2 = \bar{4}$ want $2^3 = 8 \equiv 1$ en $4^3 = 64 \equiv 1$ modulo 7.

Merk op dat $\mathbb{F}_{25} \cong \mathbb{F}_5[X]/(X^2-2)$, omdat X^2-2 geen nulpunten heeft in $\mathbb{F}_5$. Als $\alpha \in \mathbb{F}_{25}$ een element is met $\alpha^2 = 2$ dan is ieder element van $\mathbb{F}_{25}$ te schrijven als $a+b\alpha$ met $a, b \in \mathbb{F}_5$. De primitieve 3-de eenheidswortels zijn dan $2(1 \pm \alpha)$, immers:

$$\big(2(1+\alpha)\big)^3 = 3 \cdot (1 + 3\alpha + 3\alpha^2 + \alpha^3) = 3 \cdot (1 + 3\alpha + 1 + 2\alpha) = 1$$

en analoog voor $2(1-\alpha)$. Ga zelf na dat $\big(2(1+\alpha)\big)^2 = 2(1-\alpha)$.

Definitie 14.5. Laat $n \in \mathbb{Z}_{>0}$, en zij K een uitbreidingslichaam van $\mathbb{Q}$ zo dat $X^n - 1$ in $K[X]$ in lineaire factoren splitst (bijv. $K = \Omega_{\mathbb{Q}}^{X^n-1}$ of $K = \mathbb{C}$). Dan is het n-de cyclotomische polynoom, notatie: Φ_n, gedefinieerd door

$$\Phi_n = \prod_{\zeta \in K^*, \mathrm{orde}(\zeta)=n} (X - \zeta) \quad \in K[X]\,.$$

We zullen dadelijk zien dat Φ_n niet van de keuze van K afhangt. Het woord *cyclotomie* is ontleend aan het Grieks ($\kappa\acute{\upsilon}\kappa\lambda o\varsigma$ = cirkel, $\tau o\mu\acute{\eta}$ = snede) en betekent *cirkeldeling* (Duits: Kreisteilung). De naamgeving berust op de observatie dat de n-de eenheidswortels in $\mathbb{C}$ de eenheidscirkel in n gelijke stukken delen.

Stelling 14.6. *Voor elke $n \in \mathbb{Z}_{>0}$ geldt*

$$\prod_{d|n} \Phi_d = X^n - 1\,.$$

Bewijs. Zij K als in 14.5. Dan geldt

$$\prod_{d|n} \Phi_d = \prod_{d|n} \prod_{\substack{\zeta \in K^* \\ \mathrm{orde}(\zeta)=n}} (X-\zeta) = \prod_{\substack{\zeta \in K^* \\ \mathrm{orde}(\zeta)|n}} (X-\zeta) = \prod_{\substack{\zeta \in K^* \\ \zeta^n - 1 = 0}} (X-\zeta) = X^n - 1\,,$$

omdat $X^n - 1$ geen dubbele nulpunten heeft (zie Stelling 3.20.) Dit bewijst 14.6. □

Voorbeeld 14.7. Op $n = 1, 2, 3, 6$ toegepast levert 14.6:

$$\begin{aligned} \Phi_1 &= X - 1 \\ \Phi_1 \cdot \Phi_2 &= X^2 - 1 \\ \Phi_1 \cdot \Phi_3 &= X^3 - 1 \\ \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 &= X^6 - 1\,. \end{aligned}$$

Hieruit leidt men achtereenvolgens af:

$$\Phi_1 = X - 1\,, \quad \Phi_2 = X + 1\,, \quad \Phi_3 = X^2 + X + 1\,, \quad \Phi_6 = X^2 - X + 1\,.$$

In het algemeen kan men met de formule uit 14.6 het n-de cyclotomische polynoom met volledige inductie naar n berekenen. Deze berekening verloopt geheel binnen $\mathbb{Q}[X]$, waaruit blijkt dat $\Phi_n \in \mathbb{Q}[X]$ en dat de keuze van K er niet toe doet.

Met Moebius-inversie (Hoofdstuk 12, Opgave 16) kan men uit 14.6 de volgende formule voor Φ_n afleiden:

$$\Phi_n = \prod_{d|n} \left(X^{n/d} - 1\right)^{\mu(d)}, \tag{14.7.1}$$

waarbij μ de Moebiusfunctie is.

Voor een minder tijdrovende berekening van Φ_n gebruike men de formule uit Opgave 3.

Gevolg 14.8. *Zij $n \in \mathbb{Z}_{>0}$. Dan is $\Phi_n \in \mathbb{Z}[X]$ en Φ_n is monisch van graad $\mathrm{gr}(\Phi_n) = \varphi(n)$.*

Bewijs. Uit de definitie is duidelijk dat Φ_n monisch is en graad $\varphi(n)$ heeft. Met inductie naar n bewijzen we dat $\Phi_n \in \mathbb{Z}[X]$. Voor $n = 1$ geldt inderdaad $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Laat nu $n > 1$. We kunnen 14.6 nu zo schrijven:

$$g \cdot \Phi_n = X^n - 1 \tag{14.8.1}$$

waarbij g het product is van alle Φ_d met d een deler van n en $d < n$. Uit de inductiehypothese volgt dat al deze Φ_d, en dus ook g, gehele coëfficiënten hebben. Verder is g monisch.

Stel nu dat er in Φ_n een term $a_j X^j$ voorkomt met $a_j \notin \mathbb{Z}$. Kies deze j zo groot mogelijk. Dan zien we dat de coëfficiënt van $X^{\mathrm{gr}(g)+j}$ van het product $g \cdot \Phi_n$ evenmin tot $\mathbb{Z}$ behoort, hetgeen met het oog op (14.8.1) absurd is. Deze tegenspraak besluit de inductiestap en daarmee is 14.8 bewezen. □

Als we eenmaal weten dat $\Phi_n \in \mathbb{Q}[X]$ dan kunnen we $\Phi_n \in \mathbb{Z}[X]$ natuurlijk ook uit het Lemma van Gauss afleiden.

Vergelijken we in 14.6 de graad van het linker- en rechterlid dan vinden we de volgende formule van Gauss:

$$\sum_{d|n} \varphi(d) = n\,.$$

14.9 Het geval $n = p^m$. Als $n = p^m$ een macht van een priemgetal is (p priem, $m \geq 1$) dan neemt Φ_n een bijzonder eenvoudige vorm aan. Passen we 14.6 toe op p^m en op p^{m-1}, dan vinden we:

$$\prod_{i=0}^{m} \Phi_{p^i} = X^{p^m} - 1\,, \qquad \prod_{i=0}^{m-1} \Phi_{p^i} = X^{p^{m-1}} - 1\,.$$

We delen de eerste gelijkheid door de tweede:

$$\Phi_{p^m} = \left(X^{p^m} - 1\right)/\left(X^{p^{m-1}} - 1\right) = X^{(p-1)p^{m-1}} + X^{(p-2)p^{m-1}} + \cdots + X^{p^{m-1}} + 1 = \sum_{i=0}^{p-1} X^{i \cdot p^{m-1}}\,. \tag{14.9.1}$$

Deze formule voor Φ_{p^m} gaan we nu gebruiken om te bewijzen dat Φ_{p^m} *irreducibel* is in $\mathbb{Q}[X]$. Volgens Propositie 5.31 is het hiertoe voldoende aan te tonen dat $f = \Phi_{p^m}(X + 1)$ een Eisensteinpolynoom bij p is; d.w.z., als $f = \sum_{i=0}^{t} a_i X^t$ (met $t = (p-1)p^{m-1}$), dan

$$p \nmid a_t\,, \qquad p | a_i \quad (0 \leq i < t)\,, \qquad p^2 \nmid a_0\,.$$

Duidelijk is dat f monisch is, dus $a_t = 1$ is niet deelbaar door p. Verder is $a_0 = f(0) = \Phi_{p^m}(1) = p$ (wegens (14.9.1)) en dit is wel deelbaar door p maar niet door p^2. Om te bewijzen dat de overige coëfficiënten van f door p deelbaar zijn, gaan we de gelijkheid

$$\big((X+1)^{p^{m-1}} - 1\big) \cdot f = (X+1)^{p^m} - 1$$

(die volgt uit (14.9.1)) modulo p bekijken. Aangezien in $\mathbb{F}_p[X]$ geldt $(X+1)^{p^k} = X^{p^k} + 1$, vinden we

$$X^{p^{m-1}} \cdot \bar{f} = X^{p^m} \,,$$

waarbij $\bar{f} = (f \bmod p) \in \mathbb{F}_p[X]$. Hieruit volgt

$$\bar{f} = X^{(p-1)p^{m-1}} = X^t$$

waaruit blijkt dat alle coëfficiënten van f, behalve de kopcoëfficiënt, deelbaar zijn door p.

Hiermee is aangetoond dat Φ_{p^m} irreducibel is in $\mathbb{Q}[X]$. De volgende stelling zegt dat Φ_n voor *alle* n irreducibel is in $\mathbb{Q}[X]$, zodat 14.6 in feite de ontbinding van $X^n - 1$ in $\mathbb{Q}[X]$ levert. In het algemeen is er echter geen eenvoudige formule voor Φ_n, en het bewijs zal dan ook van een heel andere aard zijn.

Stelling 14.10. *Voor elke $n \in \mathbb{Z}_{>0}$ is Φ_n irreducibel in $\mathbb{Q}[X]$.*

Lemma 14.11. *Laat ζ een n-de machts eenheidswortel in een uitbreiding van $\mathbb{Q}$ zijn, met $n \in \mathbb{Z}_{>0}$. Dan geldt $f_{\mathbb{Q}}^{\zeta} = f_{\mathbb{Q}}^{\zeta^p}$ voor elk priemgetal p dat n niet deelt.*

Bewijs van Lemma 14.11. Laat $f = f_{\mathbb{Q}}^{\zeta}$ en $g = f_{\mathbb{Q}}^{\zeta^p}$. We gaan een tegenspraak afleiden uit de aanname dat $f \neq g$. Eerst bewijzen we:

$$f \cdot g | X^n - 1 \,, \tag{14.11.1}$$

$$f | g(X^p) \,. \tag{14.11.2}$$

Omdat ζ en ζ^p allebei nulpunten zijn van $X^n - 1$, volgt uit 9.8(b) dat $f | X^n - 1$ en $g | X^n - 1$ in $\mathbb{Q}[X]$. Dus f en g zijn (aannemende dat $f \neq g$!) twee verschillende irreducibele factoren van $X^n - 1$ en daarom $f \cdot g | X^n - 1$. Dit bewijst (14.11.1). Uit $g(\zeta^p) = 0$ blijkt dat ζ een nulpunt van $g(X^p)$ is, dus 9.8(b) impliceert dat $f | g(X^p)$. Dit bewijst (14.11.2).

Het Lemma van Gauss (Gevolg 5.27) vertelt ons dat f en g tot $\mathbb{Z}[X]$ behoren en dat de relaties (14.11.1) en (14.11.2) ook in de ring $\mathbb{Z}[X]$ geldig zijn. Nemen we alle coëfficiënten modulo p, dan vinden we dat in $\mathbb{F}_p[X]$ geldt:

$$\bar{f} \cdot \bar{g} | X^n - 1 \,, \tag{14.11.3}$$

$$\bar{f} | \bar{g}(X^p) \,. \tag{14.11.4}$$

waarbij $\bar{f} = (f \bmod p)$ en $\bar{g} = (g \bmod p) \in \mathbb{F}_p[X]$. We beweren nu dat geldt $\bar{g}(X^p) = \bar{g}^p$. Bewijs hiervan: laat $\bar{g} = \sum a_i X^i$, met $a_i \in \mathbb{F}_p$, dan volgt uit Stelling 8.4 en de Kleine Stelling van Fermat dat

$$\bar{g}^p = \big(\sum a_i X^i\big)^p = \sum a_i^p X^{ip} = \sum a_i X^{ip} = \bar{g}(X^p) \,,$$

zoals verlangd. We kunnen (14.11.4) dus herschrijven in de vorm

$$\bar{f}|\bar{g}^p\,. \tag{14.11.5}$$

Uit (14.11.3) en (14.11.5) leiden we nu een tegenspraak af. Laat $h \in \mathbb{F}_p[X]$ een monische irreducibele factor van $\bar{f}$ in $\mathbb{F}_p[X]$ zijn. Uit (14.11.5) volgt dan dat $h|\bar{g}^p$, dus $h|\bar{g}$, en met (14.11.3) levert dit dat $h^2|X^n-1$ in $\mathbb{F}_p[X]$. Dan moet h een deler zijn van de afgeleide $n\cdot X^{n-1}$ van X^n-1. Maar omdat $n\neq 0$ in $\mathbb{F}_p$ (hier gebruiken we onze aanname dat $p\nmid n$) kan dit alleen als $h=X$, hetgeen absurd is, want $X^2\nmid X^n-1$. Deze tegenspraak bewijst 14.11. □

Bewijs van Stelling 14.10. Laat ζ een primitieve n-de machts eenheidswortel in een uitbreiding K van $\mathbb{Q}$ zijn, en $f=f_{\mathbb{Q}}^{\zeta}$. We gaan bewijzen dat $f=\Phi_n$. Aangezien f irreducibel is (Stelling 9.8(a)) is hiermee dan 14.10 bewezen.

Omdat $\Phi_n(\zeta)=0$, volgt uit Stelling 9.8(b) dat f een deler is van Φ_n. Om te bewijzen dat omgekeerd Φ_n een deler van f is, is het wegens

$$\Phi_n=\prod_{\substack{1\leq a\leq n,\\ \gcd(a,n)=1}}(X-\zeta^a)$$

voldoende te laten zien dat $f(\zeta^a)=0$ voor elke $a\in\mathbb{Z}_{\geq 1}$ met $\gcd(a,n)=1$. Schrijf $a=p_1p_2\cdots p_t$, waar $p_1,p_2,\ldots,p_t$ priemgetallen zijn die n niet delen. Door t maal Lemma 14.11 toe te passen vinden we

$$f_{\mathbb{Q}}^{\zeta}=f_{\mathbb{Q}}^{\zeta^{p_1}}=f_{\mathbb{Q}}^{\zeta^{p_1p_2}}=\cdots=f_{\mathbb{Q}}^{\zeta^{p_1p_2\cdots p_t}},$$

met andere woorden

$$f=f_{\mathbb{Q}}^{\zeta^a}$$

waaruit blijkt dat $f(\zeta^a)=0$.

We hebben nu bewezen dat f en Φ_n elkaar delen in $K[X]$. Bovendien zijn ze beide monisch, dus $f=\Phi_n$. Dit bewijst Stelling 14.10. □

Vervolgens gaan we onderzoeken hoe, voor een priemgetal p, de polynomen $\bar{\Phi}_n=(\Phi_n \bmod p)\in\mathbb{F}_p[X]$ in irreducibele factoren splitsen. We beperken ons tot het geval $p\nmid n$, daar het algemene geval hiertoe teruggevoerd kan worden, zie Opgave 11. Uit de voorbeelden

$$\begin{aligned}\bar{\Phi}_5&=X^4+X^3+X^2+X+1=(X-\bar{3})(X-\bar{4})(X-\bar{5})(X+\bar{2})\in\mathbb{F}_{11}[X],\\ \bar{\Phi}_{23}&=(X^{11}+X^9X^7+X^6+X^5+X+1)(X^{11}+X^{10}+X^6+X^5+X^4+X^2+1)\in\mathbb{F}_2[X]\end{aligned}$$

blijkt dat Φ_n helemaal niet irreducibel in $\mathbb{F}_p[X]$ hoeft te zijn. In Stelling 14.13 zullen we de graad van alle irreducibele factoren van $\bar{\Phi}_n$ in $\mathbb{F}_p[X]$ aangeven. Eerst gaan we de nulpunten van $\bar{\Phi}_n$ bestuderen.

Stelling 14.12. *Laat K een lichaam van karakteristiek $p>0$ zijn, n een positief geheel getal dat niet deelbaar is door p, en $\zeta\in K$ een nulpunt van $\bar{\Phi}_n=(\Phi_n \bmod p)\in\mathbb{F}_p[X]\subset K[X]$. Dan is ζ een primitieve n-de machts eenheidswortel.*

Bewijs. Uit $\bar{\Phi}_n(\zeta) = 0$ en $\bar{\Phi}_n \mid X^n - 1$ volgt dat $\zeta^n - 1 = 0$, dus orde(ζ) i s een deler van n. Als orde$(\zeta) = e$ een *echte* deler van n is, d.w.z. $e < n$, dan is ζ zowel een nulpunt van $X^e - 1$ als van $\bar{\Phi}_n$. Maar $(X^e - 1) \cdot \bar{\Phi}_n \mid X^n - 1$ (dit volgt uit 14.6), dus ζ is dan een *dubbel* nulpunt van $X^n - 1$. Dit is wegens 14.3(a) echter uitgesloten. We concluderen dat orde$(\zeta) = n$. Hiermee is 14.12 bewezen. □

Stelling 14.13. *Laat $\mathbb{F}_q$ een eindig lichaam zijn, en n een positief geheel getal dat onderling ondeelbaar is met q. Zij t de orde van $q \pmod n$ in de groep $(\mathbb{Z}/n\mathbb{Z})^*$. Dan is de graad van elke irreducible factor van $\bar{\Phi}_n$ in $\mathbb{F}_q[X]$ gelijk aan t.*

Bewijs. Zij K een algebraïsche afsluiting van $\mathbb{F}_q$. Laat f een irreducibele factor van $\bar{\Phi}_n$ in $\mathbb{F}_q[X]$ zijn, $\zeta \in K$ een nulpunt van f, en $d = \mathrm{gr}(f)$. Dan $[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = d$ (zie 10.3), dus $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^d}$. Voor willekeurige $m \in \mathbb{Z}_{\geq 0}$ gelden nu wegens 12.9 de volgende equivalenties:

$$\zeta \in \mathbb{F}_{q^m} \iff \mathbb{F}_q(\zeta) \subset \mathbb{F}_{q^m} \iff \mathbb{F}_{q^d} \subset \mathbb{F}_{q^m} \iff d \mid m.$$

Anderzijds:

$$\begin{aligned}
\zeta \in \mathbb{F}_{q^m} &\iff \zeta^{q^m} = \zeta \\
&\iff \zeta^{q^m-1} = 1 && \text{(want } \zeta \neq 0\text{)} \\
&\iff n \mid q^m - 1 && \text{(want orde}(\zeta) = n \text{ wegens 14.12)} \\
&\iff q^m \equiv 1 \mod n \\
&\iff (q \bmod n)^m = (1 \bmod n) \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \\
&\iff t \mid m && \text{(want } (q \bmod n) \text{ heeft orde } t\text{).}
\end{aligned}$$

Al met al vinden we $d \mid m \iff t \mid m$ voor alle $m \in \mathbb{Z}_{>0}$, dus d en t hebben precies dezelfde veelvouden. Omdat d en t positief zijn volgt hieruit $d = t$. Hiermee is 14.13 bewezen. □

De rest van deze paragraaf is gewijd aan enkele toepassingen van cyclotomische polynomen.

De eerste toepassing betreft een speciaal geval van de *stelling van Dirichlet* over priemgetallen in rekenkundige rijen (Peter Gustav Lejeune Dirichlet, Duits wiskundige, 1805–1859) die uitspreekt dat er voor elk tweetal positieve gehele getallen a en b met ggd$(a, b) = 1$ oneindig veel priemgetallen van de vorm $a + bx$ bestaan, met $x \in \mathbb{Z}_{\geq 0}$. Voor $b = 10$ zegt deze stelling dat dus elk van de cijfers 1, 3, 7, 9 oneindig vaak als eindcijfer van een priemgetal optreedt. Het bewijs van de stelling van Dirichlet maakt gebruik van analyse en zal hier niet gegeven worden; zie J.-P. Serre, Cours d'arithmétique, P.U.F. 1970, Ch. VI (ook in het Engels vertaald). Het speciale geval $a = 1$ kan echter bijzonder eenvoudig met behulp van cyclotomische polynomen bewezen worden. Voor een aantal andere eenvoudige speciale gevallen zie Opgave 14 en Stelling 15.12.

Stelling 14.14. *Voor elke $n \in \mathbb{Z}_{>0}$ zijn er oneindig veel priemgetallen p met $p \equiv 1 \mod n$.*

Bewijs. We merken eerst op dat het voldoende is aan te tonen dat er minstens één priemgetal p met $p \equiv 1 \mod n$ bestaat. Want als men dit dan toepast op $n, 2n, 3n, \ldots$ vindt men dat er voor elke $k \in \mathbb{Z}_{>0}$ een priemgetal $p \equiv 1 \mod kn$ bestaat, en dat levert oneindig veel priemgetallen die $1 \mod n$ zijn.

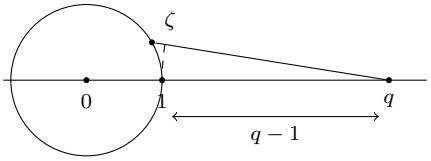
Omdat Φ_n een monisch polynoom van graad ≥ 1 is, geldt $\lim_{x\to\infty} \Phi_n(x) = \infty$, dus er is zeker een positief geheel getal m met $\Phi_n(mn) > 1$. Laat p een priemgetal zijn dat $\Phi_n(mn)$ deelt. Dan geldt $\Phi_n(mn) \equiv 0 \mod p$, dus het element $\overline{mn} = (mn \bmod p)$ van $\mathbb{F}_p$ is een nulpunt van $\bar{\Phi}_n = (\Phi_n \bmod p)$. Uit $\Phi_n \mid X^n - 1$ (in $\mathbb{Z}[X]$) blijkt dat $p \mid \Phi_n(mn) \mid (mn)^n - 1$, dus p is geen deler van n. We zijn dus in de situatie van Stelling 14.12, met $K = \mathbb{F}_p$ en $\zeta = \overline{mn}$. Passen we deze stelling toe dan vinden we dat $\overline{mn}$ orde n in $\mathbb{F}_p^*$ heeft. Maar de orde van een element is een deler van de orde van de groep, dus $n \mid p - 1$, met andere worden $p \equiv 1 \mod n$. Hiermee is 14.14 bewezen. □

De tweede toepassing van cyclotomische polynomen is de stelling van Wedderburn (Joseph Henry Maclagan Wedderburn, Schots-Amerikaans wiskundige, 1882–1948) die zegt dat in de definitie van "eindig lichaam" het axioma voor de commutativiteit van de vermenigvuldiging weggelaten kan worden. Met andere woorden:

Stelling 14.15 (Stelling van Wedderburn)**.** *Elke eindige delingsring is commutatief.*

Lemma 14.16. *Voor elke $q \in \mathbb{Z}_{>1}$ en elke $n \in \mathbb{Z}_{>1}$ geldt $|\Phi_n(q)| > q - 1$.*

Bewijs van 14.16. Er geldt $|\Phi_n(q)| = \prod_\zeta |q - \zeta|$, waarbij het product loopt over alle $\zeta \in \mathbb{C}^*$ van orde n. Al deze ζ liggen op de eenheidscirkel en zijn $\neq 1$ (want $n > 1$), dus $|q - \zeta| > q - 1$ (zie illustratie),



en we vinden $|\Phi_n(q)| > (q-1)^{\phi(n)} \geq q - 1$. Dit bewijst 14.16. □

Bewijs van 14.15. Laat K een eindige delingsring zijn, en zij

$$Z(K) = \big\{a \in K \;\big|\; ax = xa \text{ voor alle } x \in K\big\} \qquad \text{(het } \textit{centrum} \text{ van } K\text{)}.$$

Dit is een deel-delingsring van K, d.w.z. $1 \in Z(K)$, en

$$a, b \in Z(K), b \neq 0 \implies a - b, ab^{-1} \in Z(K).$$

Voorts is $Z(K)$ commutatief, dus het is een lichaam. Laat $q = \#Z(K)$. We kunnen K als vectorruimte over $Z(K)$ opvatten, dus $\#K = q^n$ waarbij $n = \dim_{Z(K)}(K)$ (vgl. het bewijs van 12.1(a)).

Laat nu $x \in K$, en definieer

$$Z_K(x) = \big\{a \in K \;\big|\; ax = xa\big\} \qquad \text{(de } \textit{centralisator} \text{ van } x \text{ in } K\text{)}.$$

Dit is een deel-delingsring van K die $Z(K)$ omvat, dus er geldt $\#Z_K(X) = q^{d(x)}$, waarbij $d(x) = \dim_{Z(K)}(Z_K(x))$. We beweren dat $d(x)$ een *deler* van n is. Eén manier om dit te bewijzen berust op een generalisatie van 10.6 voor delingsringen, hetgeen vereist dat men lineaire algebra over delingsringen in plaats van lichamen beoefent. Een andere, wat eenvoudigere, manier gaat uit van de opmerking dat

$Z_K(x)^*$ een ondergroep van K^* is, en dat dus $\#Z_K(x)^* = q^{d(x)} - 1$ een deler is van $\#K^* = q^n - 1$. Met behulp van Opgave 16 leidt men hieruit af dat $d(x)$ een deler is van n, zoals beweerd.

We merken op: $d(x) = n$ dan en slechts dan als $Z_K(x) = K$, dan en slechts dan als $x \in Z(K)$. Op de multiplicatieve groep van K^* gaan we nu de klassenformule uit de groepentheorie toepassen. We vinden

$$q^n - 1 = \#K^* = \sum_{x \in Y} \text{index}[K^* : Z_K(x)^*] = \sum_{x \in Y} \frac{q^n - 1}{q^{d(x)} - 1},$$

waarbij $Y \subset K^*$ een deelverzameling is die uit elke conjugatieklasse van K^* precies één element bevat. Nemen we de elementen van het centrum apart dan krijgen we

$$q^n - 1 = q - 1 + \sum_{x \in Y - Z(K^*)} \frac{q^n - 1}{q^{d(x)} - 1} \tag{14.16.1}$$

waarbij de nog optredende $d(x)$ allemaal delers van n *kleiner* dan n zijn. Aangezien $\Phi_n(q)$ een deler is van $q^n - 1$, en ook van $\frac{q^n-1}{q^d-1}$ voor elke deler d van n met $d < n$ (want $(X^d - 1) \cdot \Phi_n$ deelt $X^n - 1$ in $\mathbb{Z}[X]$), zien we uit (14.16.1) dat $\Phi_n(q)$ eveneens een deler is van $q - 1$, dus $|\Phi_n(q)| \leq q - 1$. In het geval $n > 1$ leidt dit tot een tegenspraak met 14.16. We concluderen dat $n = 1$, dus $K = Z(K)$, en K is commutatief. Hiermee is 14.15 bewezen. □

Het hier gegeven bewijs van de stelling van Wedderburn is afkomstig van Ernst Witt (Über die Kommutativität endlicher Schiefkörper, Abh. Math. Sem. Hamburg 8 (1931), 413). Voor een ander bewijs zie Herstein, Topics in Algebra, §7.2.

De laatste toepassing van cyclotomische polynomen die we geven betreft een probleem uit de vlakke meetkunde. De waarde ervan moet voornamelijk in de amusementssfeer gezocht worden.

Stelling 14.17. *Laat n een oneven getal groter dan 1 zijn. Dan zijn er in een regelmatige n-hoek geen drie diagonalen te vinden die door één punt gaan, tenzij dit een hoekpunt van de n-hoek is.*

Voor *even* n groter dan 4 is de stelling kennelijk fout, want van een regelmatige $2k$-hoek gaan er k diagonalen door het middelpunt; en men kan ook andere voorbeelden geven. De situatie is uitgezocht door Gerrit Bol (Beantwoording van prijsvraag no. 17, Nieuw Arch. Wisk (2), 18 (1936), 14–66). Het bewijs van 14.17 dat we beneden geven is afkomstig van Hermann Heineken (Regelmässige Vielecke und ihre Diagonalen, Enseignement Math., II Sér. 8 (1962), 275–278).

Lemma 14.18. *Laat n een* oneven *positief geheel getal zijn, en laten $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{C}$ n-de machts eenheidswortels zijn. Stel dat $F \in \mathbb{Q}[X_1, X_2, \ldots, X_t]$ de eigenschap heeft dat*

$$F(\alpha_1, \alpha_2, \ldots, \alpha_t) = 0.$$

Dan geldt ook

$$F(\alpha_1^2, \alpha_2^2, \ldots, \alpha_t^2) = 0.$$

Bewijs van 14.18. Laat $\zeta \in \mathbb{C}$ een primitieve n-de eenheidswortel zijn, en kies $a_i \in \mathbb{Z}$ met $\alpha_i = \zeta^{a_i}$. Dan geldt

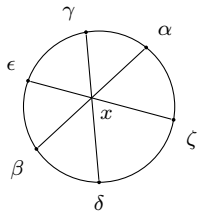
$$F(\zeta^{a_i}, \zeta^{a_2}, \ldots, \zeta^{a_t}) = 0$$

waaruit volgt dat het polynoom $g = F(X^{a_1}, X^{a_2}, \ldots, X^{a_t}) \in \mathbb{Q}[X]$ deelbaar is door $f_{\mathbb{Q}}^{\zeta} = \Phi_n$. Maar omdat n oneven is, is ook ζ^2 een primitieve n-de machts eenheidswortel, dus een nulpunt van Φ_n. We concluderen dat $g(\zeta^2) = 0$, d.w.z.

$$F(\zeta^{2a_1}, \zeta^{2a_2}, \ldots, \zeta^{2a_t}) = 0,$$

en dat is precies wat we moesten bewijzen. Hiermee is 14.18 bewezen. □

Bewijs van 14.17. We identificeren het platte vlak zodanig met het vlak der complexe getallen, dat de n hoekpunten van de regelmatige n-hoek juist samenvallen met de n-de machts eenheidswortels.



Stel dat de diagonalen $\alpha\beta$, $\gamma\delta$, $\epsilon\zeta$ door één punt x gaan. Omdat x op de lijn door α en β gaat, is $\frac{x-\alpha}{\beta-\alpha}$ reëel, d.w.z. gelijk aan zijn complex geconjugeerde:

$$\frac{x-\alpha}{\beta-\alpha} = \frac{\bar{x}-\bar{\alpha}}{\bar{\beta}-\bar{\alpha}}.$$

Omdat α en β absolute waarde 1 hebben geldt $\bar{\alpha} = \alpha^{-1}$, $\bar{\beta} = \beta^{-1}$, dus $\frac{\bar{x}-\bar{\alpha}}{\bar{\beta}-\bar{\alpha}} = \frac{\alpha\beta\bar{x}-\beta}{\alpha-\beta}$. We vinden

$$x + \alpha\beta\bar{x} - (\alpha + \beta) = 0$$

en evenzo

$$x + \gamma\delta\bar{x} - (\gamma + \delta) = 0$$
$$x + \epsilon\zeta\bar{x} - (\epsilon + \zeta) = 0.$$

De kolommen van de matrix

$$\begin{pmatrix} 1 & \alpha\beta & \alpha+\beta \\ 1 & \gamma\delta & \gamma+\delta \\ 1 & \epsilon\zeta & \epsilon+\zeta \end{pmatrix}$$

zijn dus afhankelijk, waaruit volgt dat de determinant nul is. Trekken we de eerste rij van de beide andere af en vermenigvuldigen we de laatste kolom met $-\alpha$ dan zien we

$$\det \begin{pmatrix} \gamma\delta - \alpha\beta & \alpha^2 + \alpha\beta - \alpha\gamma - \alpha\delta \\ \epsilon\zeta - \alpha\beta & \alpha^2 + \alpha\beta - \alpha\epsilon - \alpha\zeta \end{pmatrix} = 0.$$

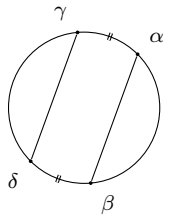
Tel de eerste kolom bij de tweede op:

$$\det \begin{pmatrix} \gamma\delta - \alpha\beta & (\alpha-\gamma)(\alpha-\delta) \\ \epsilon\zeta - \alpha\beta & (\alpha-\epsilon)(\alpha-\zeta) \end{pmatrix} = 0$$

d.w.z.

$$(\gamma\delta - \alpha\beta)(\alpha - \epsilon)(\alpha - \zeta) = (\epsilon\zeta - \alpha\beta)(\alpha - \gamma)(\alpha - \delta). \tag{14.18.1}$$

We beweren dat deze uitdrukking niet nul is. Immers, $\alpha - \epsilon = 0$ of $\alpha - \zeta = 0$ zou in tegenspraak zijn met de aanname dat x niet één der hoekpunten is; en als $\gamma\delta - \alpha\beta = 0$ dan $\gamma\alpha^{-1} = \beta\delta^{-1}$, d.w.z. de afstand van α tot γ langs de cirkel is gelijk aan die van δ tot β, maar dan zijn de diagonalen $\alpha\beta$ en $\gamma\delta$ evenwijdig en hebben dus geen snijpunt x (vgl. illustratie).



Pas op het verschil van linkerlid en rechterlid in (14.18.1) nu Lemma 14.18 toe, met $\alpha_1, \alpha_2, \ldots, \alpha_t$ gelijk aan $\alpha, \beta, \ldots, \zeta$. Dan vinden we

$$(\gamma^2\delta^2 - \alpha^2\beta^2)(\alpha^2 - \epsilon^2)(\alpha^2 - \zeta^2) = (\epsilon^2\zeta^2 - \alpha^2\beta^2)(\alpha^2 - \gamma^2)(\alpha^2 - \delta^2).$$

Omdat de uitdrukking in (14.18.1) niet nul is mogen we erdoor delen, en dat levert

$$(\gamma\delta + \alpha\beta)(\alpha + \epsilon)(\alpha + \zeta) = (\epsilon\zeta + \alpha\beta)(\alpha + \gamma)(\alpha + \delta). \tag{14.18.2}$$

Werken we in (14.18.2) en (14.18.1) alle producten uit, dan vinden we afgezien van de min-tekens in (14.18.1) dezelfde termen. Tellen we (14.18.2) en (14.18.1) op dan houden we (na deling door 2) alleen de plustermen in (14.18.1) over:

$$\gamma\delta\alpha^2 + \gamma\delta\epsilon\zeta + \alpha^2\beta\zeta + \alpha^2\beta\epsilon = \epsilon\zeta\alpha^2 + \epsilon\zeta\gamma\delta + \alpha^2\beta\delta + \alpha^2\beta\gamma$$

d.w.z. $\gamma\delta + \beta\zeta + \beta\epsilon = \epsilon\zeta + \beta\delta + \beta\gamma$, hetgeen men ook kan schrijven als

$$(\beta - \gamma)(\beta - \delta) = (\beta - \epsilon)(\beta - \zeta).$$

Weer is deze uitdrukking niet nul, en precies als boven vindt men

$$(\beta + \gamma)(\beta + \delta) = (\beta + \epsilon)(\beta + \zeta).$$

Nu leveren de plustermen: $\beta^2 + \gamma\delta = \beta^2 + \epsilon\zeta$, dus $\gamma\delta = \epsilon\zeta$, hetgeen betekent dat de diagonalen $\gamma\delta$ en $\epsilon\zeta$ evenwijdig zijn, een tegenspraak. Hiermee is 14.17 bewezen. □

Opgaven

1. Laat $n \in \mathbb{Z}_{>0}$. Bewijs:

$$\Phi_n(0) = \begin{cases} 1 & \text{voor } n > 1, \\ -1 & \text{voor } n = 1, \end{cases}$$

$$\Phi_n(1) = \begin{cases} 0 & \text{voor } n = 1, \\ p & \text{voor } n = p^m, \text{ met } p \text{ priem}, m \in \mathbb{Z}_{>0}, \\ 1 & \text{anders;} \end{cases}$$

   de coëfficiënt van Φ_n bij $X^{\phi(n)-1}$ is $-\mu(n)$ (zie na 12.13.1).

2. Bewijs de volgende symmetrie-eigenschap van Φ_n:

$$X^{\phi(n)} \cdot \Phi_n(1/X) = \begin{cases} \Phi_n & (n > 1) \\ -\Phi_n & (n = 1) \end{cases}$$

3. Laat $n \in \mathbb{Z}_{>0}$, en laat p een priemgetal zijn. Bewijs:

$$\begin{aligned} \Phi_{np} &= \Phi_n(X^p) && \text{als } p \mid n, \\ \Phi_{np} &= \Phi_n(X^p)/\Phi_n && \text{als } p \nmid n, \\ \Phi_{2n} &= (-1)^{\phi(n)} \cdot \Phi_n(-X) && \text{als } 2 \nmid n. \end{aligned}$$

4. Bewijs: $\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$. Bereken Φ_{30}.

5. Laten p en q verschillende priemgetallen zijn.

   (a) Zij $V = \{ap+bq \mid a, b \in \mathbb{Z}_{\geq 0}\}$. Bewijs $\Phi_{pq} = (1-X)\cdot\sum_{v\in V} X^v$ (product van machtreeksen).

   (b) Bewijs dat de coëfficiënten van Φ_{pq} die niet nul zijn afwisselend $+1$ en -1 zijn.

   (c) Laat $\lambda, \mu \in \mathbb{Z}$ bepaald zijn door $0 < \lambda \leq q$, $0 < \mu \leq p$, $\lambda p \equiv 1 \mod q$, $\mu q \equiv 1 \mod p$. Bewijs dat $\lambda p + \mu q = 1 + pq$, en dat

$$\Phi_{pq} = \sum_{i=0}^{\lambda-1}\sum_{j=0}^{\mu-1} X^{ip+jq} - \sum_{i=\lambda}^{q-1}\sum_{j=\mu}^{p-1} X^{ip+jq-pq}.$$

6. (a) Stel dat n door ten hoogste 2 verschillende oneven priemgetallen deelbaar is. Bewijs dat dan alle coëfficiënten van Φ_n in absolute waarde ≤ 1 zijn.

   (b) Bewijs dat Φ_{105} twee coëfficiënten -2 heeft.

7. Bewijs dat $[\Omega_{\mathbb{Q}}^{X^n-1} : \mathbb{Q}] = \phi(n)$, voor alle $n \in \mathbb{Z}_{\geq 1}$.

8. Met ζ_k geven we een primitieve k-de eenheidswortel aan.

(a) Laat $n, m \in \mathbb{Z}_{\geq 1}$, $\text{ggd}(n, m) = 1$. Bewijs:

$$\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm}), \qquad \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

(b) Bewijs voor willekeurige $n, m \in \mathbb{Z}_{\geq 1}$:

$$\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{\text{kgv}(n,m)}), \qquad \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\text{ggd}(n,m)}).$$

9. Laat $n \in \mathbb{Z}_{\geq 1}$, en zij $K = \mathbb{Q}(\zeta)$, waar ζ een primitieve n-de machts eenheidswortel aangeeft. Bewijs: het aantal eenheidswortels in K is n als n even is, en $2n$ als n oneven is.

10. (a) Laat $\alpha \in \mathbb{Q}(i)^*$, en stel dat de hoek die de lijn van 0 naar α met de reële as maakt een rationaal veelvoud van π is. Bewijs: $\alpha/\bar{\alpha} \in \{1, i, -1, -i\}$.

(b) Stel dat $P, Q, R \in \mathbb{R}^2$ drie verschillende punten zijn, waarvan de zes coördinaten alle *geheel* zijn, en stel dat de hoek $\angle PQR$ een rationaal veelvoud van π is. Bewijs dat deze hoek een veelvoud van $\pi/4$ is.

11. Zij p een priemgetal, $n \in \mathbb{Z}_{>0}$, en schrijf $n = n_0 \cdot p^m$, met $m \in \mathbb{Z}_{\geq 0}$ en $p \nmid n_0$. Bewijs dat in $\mathbb{F}_p[X]$ geldt:

$$(\Phi_n \bmod p) = (\Phi_{n_0} \bmod p)^{\phi(p^m)}.$$

(Aanwijzing: Opgave 3.)

12. Bewijs, in de situatie van 14.13, dat het aantal irreducibele factoren van Φ_n in $\mathbb{F}_q[X]$ gelijk is aan de index van de ondergroep $\langle q \mod n \rangle$ van $(\mathbb{Z}/n\mathbb{Z})^*$.

13. (a) Bewijs dat $\Phi_9 \in \mathbb{F}_2[X]$ irreducibel is.

(b) Ontbind Φ_7 in $\mathbb{F}_{13}[X]$ in irreducibele factoren.

(c) Bewijs: $\Phi_5 \in \mathbb{F}_q[X]$ is irreducibel dan en slechts dan als $q \equiv 2$ of $3 \mod 5$.

(d) Bewijs dat $\Phi_{24} \in \mathbb{F}_p[X]$ reducibel is voor elke priemgetal p.

14. (a) Bewijs dat er oneindig veel priemgetallen p zijn met $p \equiv -1 \mod 4$. (Aanwijzing: elk getal van de vorm $4n - 1$ heeft minstens één priemfactor die $-1 \mod 4$ is.)

(b) Bewijs dat er oneindig veel priemgetallen p zijn met $p \equiv -1 \mod 3$.

15. Zij K een eindige ring zonder nuldelers. Bewijs: K is een lichaam of $K = \{0\}$.

16. Laat a, $b \in \mathbb{Z}$ en zij q een geheel getal met $q \geq 2$.

(a) Zij r de rest van a bij deling door b. Bewijs dat $q^r - 1$ de rest is van $q^a - 1$ bij deling door $q^b - 1$.

(b) Bewijs dat $q^b - 1$ een deler is van $q^a - 1$ dan en slechts dan als b een deler is van a.

(c) Bewijs dat $\text{ggd}(q^a - 1, q^b - 1) = q^{\text{ggd}(a,b)} - 1$.

Hoofdstuk 15

Kwadratische resten

Laat $p = 2k + 1$ een oneven priemgetal zijn, en a een geheel getal dat niet deelbaar door p is. Uit

$$(a^k - 1) \cdot (a^k + 1) = a^{2k} - 1 = a^{p-1} - 1 \equiv 0 \mod p$$

(wegens de kleine stelling van Fermat) volgt dat $a^k - 1$ of $a^k + 1$ deelbaar door p is, dus

$$a^k \equiv 1 \mod p \qquad \text{of} \qquad a^k \equiv -1 \mod p$$

(en natuurlijk niet allebei, want $1 \not\equiv -1 \mod p$). Is a wel deelbaar door p, dan geldt natuurlijk $a^k \equiv 0 \mod p$. Wegens $k = \frac{p-1}{2}$ is hiermee de volgende definitie gerechtvaardigd.

Definitie 15.1. Laat p een oneven priemgetal zijn en zij $a \in \mathbb{Z}$. Dan is het *Legendre-symbool* $\left(\frac{a}{p}\right)$ gedefinieerd door

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p, \qquad \left(\frac{a}{p}\right) \in \{-1, 0, 1\}.$$

(Adrien Marie Legendre, Frans astronoom en wiskundige, 17520–1833.)

Stelling 15.2. *Zij p een oneven priemgetal. Dan hangt het Legendre-symbool $\left(\frac{a}{p}\right)$ alleen van de restklasse $(a \bmod p)$ af, en de afbeelding $\mathbb{F}_p^* \to \{\pm 1\}$ gegeven door $(a \bmod p) \mapsto \left(\frac{a}{p}\right)$ is een* surjectief groepshomomorfisme.

Bewijs. Uit $a \equiv a' \mod p$ volgt $a^{\frac{p-1}{2}} \equiv a'^{\frac{p-1}{2}} \mod p$, dus $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$. Hieruit blijkt dat $\left(\frac{a}{p}\right)$ alleen van $(a \bmod p)$ afhangt. Uit $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}}$ blijkt dat de afbeelding $\mathbb{F}_p^* \to \{\pm 1\}$ gegeven door $(a \bmod p) \mapsto \left(\frac{a}{p}\right)$ een groepshomomorfisme is. Stel dat dit groepshomomorfisme niet surjectief is. Dan is het beeld ervan gelijk aan $\{1\}$, dus $a^{\frac{p-1}{2}} \equiv 1 \mod p$ voor alle $(a \bmod p) \in \mathbb{F}_p^*$. Maar dit is onmogelijk, want het polynoom $X^{\frac{p-1}{2}} - 1$ kan in $\mathbb{F}_p$ niet meer dan $\frac{p-1}{2}$ nulpunten hebben. Hiermee is 15.2 bewezen. □

Stelling 15.3 (criterium van Euler)**.** *Laat p een oneven priemgetal zijn, en $a \in \mathbb{Z}$. Dan geldt:*

$$\left(\frac{a}{p}\right) = 0 \iff a \text{ is deelbaar door } p,$$
$$\left(\frac{a}{p}\right) = 1 \iff \text{er is een } x \in \mathbb{Z} \text{ met } x \not\equiv 0 \bmod p \text{ en } x^2 \equiv a \bmod p,$$
$$\left(\frac{a}{p}\right) = -1 \iff a \text{ is niet congruent met een kwadraat modulo } p$$

Bewijs. Het is duidelijk dat $\left(\frac{a}{p}\right) = 0 \iff p \mid a$. Uit 15.2 blijkt dat de kern van de afbeelding $\mathbb{F}_p^* \to \{\pm 1\}, (a \bmod p) \mapsto \left(\frac{a}{p}\right)$, index twee in $\mathbb{F}_p^*$ heeft. Maar $\mathbb{F}_p^*$ is een cyclische groep van orde $p-1$ (zie 3.16), en dus heeft $\mathbb{F}_p^*$ slechts één ondergroep van index twee, namelijk $(\mathbb{F}_p^*)^2 = \left\{x^2 \;\middle|\; x \in \mathbb{F}_p^*\right\}$. Dus

$$\left(\frac{a}{p}\right) = 1 \iff (a \bmod p) \in (\mathbb{F}_p^*)^2$$

en daarom

$$\left(\frac{a}{p}\right) = -1 \iff (a \bmod p) \notin (\mathbb{F}_p^*)^2 \qquad (\text{voor } p \nmid a).$$

Hiermee is 15.3 bewezen. □

Naar aanleiding van 15.3 noemt men het Legendre-symbool ook wel het *kwadratische restsymbool*. Gehele getallen a met $\left(\frac{a}{p}\right) = 1$ heten *kwadratische resten* modulo p, gehele getallen a met $\left(\frac{a}{p}\right) = -1$ *kwadratische niet-resten* modulo p. Modulo p beschouwd, vormt de verzameling kwadratische resten een ondergroep van orde $\frac{p-1}{2}$ van $\mathbb{F}_p^*$, en de verzameling kwadratische niet-resten het complement hiervan, eveneens bestaande uit $\frac{p-1}{2}$ elementen.

Voorbeeld 15.4. In $\mathbb{F}_{11}$ geldt:

$$(\pm 1)^2 = 1, \quad (\pm 2)^2 = 4, \quad (\pm 3)^3 = 9, \quad (\pm 4)^2 = 5, \quad (\pm 5)^2 = 3,$$

waaruit blijkt dat

$$\left(\frac{a}{11}\right) = 1 \text{ als } a \equiv 1, 3, 4, 5, \text{ of } 9 \mod 11.$$

De andere $10/2 = 5$ elementen van $\mathbb{F}_{11}^*$ zijn geen kwadraat:

$$\left(\frac{a}{11}\right) = -1 \text{ als } a \equiv 2, 6, 7, 8, \text{ of } 10 \mod 11.$$

Stelling 15.5 (Kwadratische reciprociteitswet, (Gauss, 1801))**.** *Als p en q verschillende oneven priemgetallen zijn, dan geldt:*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \qquad \text{als } p \equiv 1 \bmod 4 \text{ of } q \equiv 1 \bmod 4,$$
$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \qquad \text{als } p \equiv q \equiv 3 \bmod 4.$$

Anders geformuleerd:

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

Dit verrassende verband tussen $\left(\frac{p}{q}\right)$ en $\left(\frac{q}{p}\right)$ zou men geheel niet vermoeden als men alleen naar de definitie van het Legendre-symbool $\left(\frac{a}{p}\right)$ keek, waarin immers geen enkele symmetrie tussen a en p te bespeuren valt. De eerste die dit verband ontdekte was Euler (1746), die aan de hand van uitgebreid getallenmateriaal tot de conclusie kwam dat de kwadratische reciprociteitswet (of preciezer: de daarmee equivalente stelling 15.9) moest gelden, zonder er evenwel een algemeen bewijs voor te vinden. Het eerste bewijs werd gevonden door Gauss, die in de loop van zijn leven in totaal acht verschillende bewijzen gegeven heeft. In deze paragraaf zullen we twee bewijzen van 15.5 geven: één, dat volledig elementair is en dat teruggaat op Gauss' derde bewijs, en één, dat berust op berekeningen in eindige lichamen en dat teruggaat op Gauss' zesde bewijs. Voor meer informatie, zie: H. Pieper, Variationen über ein zahlentheoretisches Thema von C.F. Gauss, Birkhäuser Verlag, 1978. Aan het eind van deze paragraaf zullen we zien hoe men de kwadratische reciprociteitswet kan gebruiken om voor gegeven a en p het Legendre-symbool op een efficiënte manier te berekenen. Deze methode maakt ook gebruik van de twee volgende stellingen, die dienovereenkomstig 'aanvullingswetten' genoemd worden.

Stelling 15.6 (Eerste aanvullingswet)**.** *Voor een oneven priemgetal p geldt*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{als } p \equiv 1 \mod 4 \\ -1 & \text{als } p \equiv -1 \mod 4, \end{cases}$$

met andere woorden:

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

Stelling 15.7 (Tweede aanvullingswet)**.** *Voor een oneven priemgetal p geldt*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{als } p \equiv \pm 1 \mod 8 \\ -1 & \text{als } p \equiv \pm 3 \mod 8, \end{cases}$$

met andere woorden:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In elk van de stellingen 15.5, 15.6, 15.7 is het gemakkelijk in te zien dat de beide gegeven formuleringen equivalent zijn.

We merken op dat $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ een direct gevolg is van Definitie 15.1. Hiermee is 15.6 bewezen.

Het bewijs van 15.7 geven we na het bewijs van 15.8; zie ook Opgave 13.

Het eerste bewijs van 15.5 dat we geven berust op een formule voor $\left(\frac{a}{p}\right)$ die voornamelijk theoretische waarde heeft. Laat $p = 2k + 1$ een oneven priemgetal zijn. Dan vormt de verzameling getallen

$$-k, -(k-1), \ldots, -2, -1, 0, 1, 2, \ldots, k-1, k$$

een volledig representantensysteem modulo p. Een geheel getal zullen we *positief* modulo p noemen als het congruent is met een van de getallen $1, 2, \ldots, k \pmod{p}$, en *negatief* als het congruent is met een van de getallen $-k, -(k-1), \ldots, -2, -1$. Van de getallen $1, 2, \ldots, p-1$ is dus de eerste helft positief modulo p, de tweede helft negatief modulo p.

Lemma 15.8 (Gauss, 1808)**.** *Laat $p = 2k + 1$ een oneven priemgetal zijn, en a een geheel getal dat niet deelbaar is door p. Dan geldt*

$$\left(\frac{a}{p}\right) = (-1)^\nu,$$

waarbij ν het aantal getallen uit de rij

$$a, 2a, 3a, \ldots, ka$$

is, dat negatief modulo p is.

Bewijs. Kies voor elke $i \in \{1, 2, \ldots, k\}$ een $\epsilon_i \in \{\pm 1\}$ en $r_i \in \{1, 2, \ldots, k\}$ met

$$ia \equiv \epsilon_i r_i \mod p. \tag{15.8.1}$$

Er geldt $\epsilon_i = -1$ dan en slechts dan als ia negatief modulo p is, dus $\prod_{i=1}^k \epsilon_i = (-1)^\nu$.

Stel dat geldt $r_i = r_j$, waarbij $i, j \in \{1, 2, \ldots, k\}$. Dan geldt $ia \equiv \epsilon_i r_i = \pm\epsilon_j r_j \equiv \pm ja \mod p$, dus wegens $\gcd(a, p) = 1$ ook $i \equiv \pm j \mod p$. Maar dit is voor $i, j \in \{1, 2, \ldots, k\}$ alleen mogelijk als $i = j$. Hieruit zien we: de getallen $r_1, r_2, \ldots, r_k \in \{1, 2, \ldots, k\}$ zijn alle k verschillend, dus op volgorde na zijn ze gelijk aan $1, 2, \ldots, k$. Dus: $\prod_{i=1}^k r_i = \prod_{i=1}^k i$.

Vermenigvuldig nu de congruenties 15.8.1 voor $i = 1, 2, \ldots, k$ met elkaar. Dan vinden we

$$a^k \prod_{i=1}^k i \equiv \prod_{i=1}^k \epsilon_i \cdot \prod_{i=1}^k r_i = (-1)^\nu \cdot \prod_{i=1}^k i \mod p.$$

Omdat $\prod_{i=1}^k i$ geen factor p bevat, volgt hieruit

$$a^k \equiv (-1)^\nu \mod p.$$

Wegens de definitie van $\left(\frac{a}{p}\right)$ is hiermee 15.8 bewezen. □

Bewijs van 15.7. Schrijf weer $p = 2k+1$. Volgens 15.8 geldt $\left(\frac{2}{p}\right) = (-1)^\nu$ waarbij ν het aantal getallen uit de rij $2, 4, 6, \ldots, 2k = p - 1$ aangeeft dat negatief modulo p is. Elk van deze getallen is kleiner dan p, en is dus positief modulo p als het $\leq k$ is en negatief anders. Aan gezien er $\lfloor \frac{k}{2} \rfloor$ getallen in de rij $\leq k$ zijn, vinden we voor het aantal negatieve:

$$\nu = k - \left\lfloor \frac{k}{2} \right\rfloor.$$

Schrijf nu $k = 4 \cdot h + r$, met $0 \leq r \leq 3$. Dan geldt

$$\begin{aligned}
\nu &= 2h && \text{als } r = 0 \text{ (d.w.z. } p \equiv 1 \bmod 8), \\
\nu &= 2h + 1 && \text{als } r = 1 \text{ (d.w.z. } p \equiv 3 \bmod 8), \\
\nu &= 2h + 1 && \text{als } r = 2 \text{ (d.w.z. } p \equiv -3 \bmod 8), \\
\nu &= 2h + 2 && \text{als } r = 3 \text{ (d.w.z. } p \equiv -1 \bmod 8).
\end{aligned}$$

Dus we vinden

$$\left(\frac{2}{p}\right) = (-1)^\nu = \begin{cases} 1 & \text{als } p \equiv \pm 1 \bmod 8, \\ -1 & \text{als } p \equiv \pm 3 \bmod 8. \end{cases}$$

Hiermee is 15.7 bewezen. □

Hetzelfde idee passen we toe om voor $\left(\frac{3}{p}\right)$ een dergelijke regel af te leiden. De getallen $3, 6, 9, \ldots, 3k$ uit Lemma 15.8 zijn nu allemaal kleiner dan $\frac{3}{2}p$, en een getal uit de rij is dus negatief mod p dan en slechts dan als het tussen $\frac{1}{2}p$ en p ligt. Dit levert:

$$\begin{aligned}\nu &= (\text{aantal 3-vouden tussen } \frac{1}{2}p \text{ en } p)\\ &= (\text{aantal 3-vouden} < p) - (\text{aantal 3-vouden} < \frac{1}{2}p)\\ &= \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor.\end{aligned}$$

Door de gevallen $p = 12h + 1, +5, +7, +11$ te onderscheiden vindt men

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{als } p \equiv \pm 1 \mod 12 \\ -1 & \text{als } p \equiv \pm 5 \mod 12. \end{cases}$$

Verder geldt

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{als } p \equiv 1 \mod 3 \\ -1 & \text{als } p \equiv -1 \mod 3. \end{cases}$$

Met deze formules is het gemakkelijk om Stelling 15.5 in het geval $q = 3$ te controleren.

Voor elke vaste a kunnen we volgens deze methode een regel voor $\left(\frac{a}{p}\right)$ afleiden. De volgende stelling zegt, dat we dan vinden dat $\left(\frac{a}{p}\right)$ alleen afhangt van de restklasse van p modulo $4a$ afhangt, en bovendien hetzelfde is voor de tegengestelde restklasse $\pmod{4a}$. Hierbij nemen we a positief (voor negatieve a geldt een analoge stelling: zie Opgave 5).

Stelling 15.9. *Laat a een* positief *geheel getal zijn, en p en q oneven priemgetallen die a niet delen, waarvoor geldt $p \equiv q \mod 4a$ of $p \equiv -q \mod 4a$. Dan geldt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Bewijs. Om $\left(\frac{a}{p}\right)$ volgens 15.8 te berekenen, moeten we kijken hoeveel van de getallen

$$a, 2a, 3a, \ldots, ka, \qquad \text{met } k = \frac{1}{2}(p-1)$$

tussen $\frac{1}{2}p$ en p liggen, of tussen $\frac{3}{2}p$ en $2p$, etcetera. Omdat ka het grootste a-voud kleiner dan $\frac{1}{2}pa$ is, is het laatste interval dat we moeten bekijken dat van $(b - \frac{1}{2})p$ tot bp, waarbij $b = \frac{1}{2}a$ als a even is en $b = \frac{1}{2}a - \frac{1}{2}$ als a oneven is. We zijn dus geïnteresseerd in het aantal a-vouden in de intervallen

$$\left(\frac{1}{2}p, p\right), \left(\frac{3}{2}p, 2p\right), \ldots, \left((b - \frac{1}{2})p, bp\right).$$

Op de eindpunten van deze intervallen hoeven we niet te letten, want dat zijn geen a-vouden.

Delen we alles door a, dan zien we dat we geïnteresseerd zijn in het aantal *gehele getallen* in de intervallen

$$\left(\frac{p}{2a}, \frac{p}{a}\right), \left(\frac{3p}{2a}, \frac{2p}{a}\right), \ldots, \left(\frac{(2b-1)p}{2a}, \frac{bp}{a}\right). \tag{15.9.1}$$

Gaan we nu bij p een veelvoud van $4a$ optellen, dan wordt bij elk van de eindpunten van deze intervallen een veelvoud van $\frac{4a}{2a} = 2$ opgeteld. Dit kan voor het aantal gehele getallen in deze intervallen natuurlijk verschil maken, maar voor dit aantal *modulo* 2 maakt het niet uit.

Is nu q een priemgetal met $q \equiv p \mod 4a$, dan ontstaat q uit p door er een veelvoud van $4a$ bij te tellen. Uit het voorgaande concluderen we dus dat het aantal (zeg ν') der gehele getallen in de intervallen

$$\left(\frac{q}{2a}, \frac{q}{a}\right), \left(\frac{3q}{2a}, \frac{2q}{a}\right), \ldots \left(\frac{(2b-1)q}{2a}, \frac{bq}{a}\right)$$

modulo 2 gelijk is aan het aantal ν der gehele getallen in de intervallen (15.9.1). Dus $\left(\frac{a}{q}\right) = (-1)^{\nu'} = (-1)^{\nu} = \left(\frac{a}{p}\right)$, waarmee 15.9 bewezen is in het geval $p \equiv q \mod 4a$.

Het geval $p \equiv -q \mod 4a$ is een klein beetje ingewikkelder. Laat $p = 4am - q$, dan is de serie intervallen (15.9.1) gelijk aan

$$\left(2m - \frac{q}{2a}, 4m - \frac{q}{a}\right), \left(6m - \frac{3q}{2a}, 8m - \frac{2q}{a}\right), \ldots, \left((4b-2)m - \frac{2b-1)q}{2a}, 4bm - \frac{bq}{a}\right).$$

Trek de getallen in het eerste interval van $4m$ af. Dan vindt men dat het aantal gehele getallen in dat interval gelijk is aan het aantal gehele getallen in het interval $(\frac{q}{a}, \frac{q}{2a} + 2m)$. Samen met het interval $(\frac{q}{2a}, \frac{q}{a})$ geeft dit juist een interval van lengte $2m$, waarin zich een even aantal, nl. $2m$, gehele getallen bevindt. We concluderen dat het aantal gehele getallen in $(2m - \frac{q}{2a}, 4m - \frac{q}{a})$ modulo 2 gelijk is aan het aantal gehele getallen in $(\frac{q}{2a}, \frac{q}{a})$. Door een analoge redenering op de overige intervallen toe te passen zien we, dat we bovenstaande serie mogen vervangen door

$$\left(\frac{q}{2a}, \frac{q}{a}\right), \left(\frac{3q}{2a}, \frac{2q}{a}\right), \ldots, \left(\frac{(2b-1)q}{2a}, \frac{bq}{a}\right)$$

zonder het aantal gehele getallen in deze intervallen van pariteit te veranderen. Hieruit blijkt opnieuw dat $\nu' \equiv \nu \mod 2$, dus als te voren $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$. Dit bewijst 15.9. □

Bewijs van 15.5. Laten p en q verschillende oneven priemgetallen zijn. We beschouwen eerst het geval dat $p \not\equiv q \mod 4$. Dan $p \equiv -q \mod 4$, dus $p + q = 4a$ voor een positief geheel getal a dat niet door p of q deelbaar is.

Uit $p + q \equiv p \mod q$ volgt

$$\left(\frac{p}{q}\right) = \left(\frac{p+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{2}{q}\right)^2 \cdot \left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$$

en evenzo

$$\left(\frac{q}{p}\right) = \left(\frac{a}{p}\right).$$

Uit $p \equiv -q \mod 4a$ en 15.9 blijkt dat $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, zoals verlangd.

Vervolgens beschouwen we het geval $p \equiv q \mod 4$. We concluderen dat

$$\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{als } p \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right) & \text{als } p \equiv 3 \mod 4 \end{cases}$$

waarbij we gebruik maken van 15.6.

Hiermee is 15.5 volledig bewezen. □

Het tweede bewijs van 15.5 dat we geven berust op de beschouwing van *Gauss-sommen*. Zij q een oneven priemgetal en ζ een primitieve q-de machts eenheidswortel in een lichaam van K waarvan de karakteristiek niet gelijk aan q is. Voor $x = (n \bmod q) \in \mathbb{F}_q$ definiëren we $\zeta^x = \zeta^n$; dit hangt neit van de keuze van n af, want $\zeta^q = 1$. Verder zetten we $\left(\frac{x}{q}\right) = \left(\frac{n}{q}\right)$ (vgl. 15.2). De *Gauss-som* τ is nu gedefinieerd door:

$$\tau = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \cdot \zeta^x$$

Dit is een element van K. Neemt men bijvoorbeeld $q = 3$, $K = \mathbb{C}$, $\zeta = \frac{-1+i\sqrt{3}}{2}$ dan geldt

$$\tau = \left(\frac{0}{3}\right) \cdot \zeta^0 + \left(\frac{1}{3}\right) \cdot \zeta^1 + \left(\frac{2}{3}\right) \cdot \zeta^2 = \zeta - \zeta^2 = i\sqrt{3}.$$

Algemeen geldt:

Lemma 15.10. $\tau^2 = \left(\frac{-1}{q}\right) \cdot q$.

Bewijs. Er geldt

$$\begin{aligned}
\tau^2 &= \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \cdot \zeta^x\right) \cdot \left(\sum_{y \in \mathbb{F}_q} \left(\frac{y}{q}\right) \cdot \zeta^y\right) \\
&= \sum_{x,y \in \mathbb{F}_q} \left(\frac{xy}{q}\right) \cdot \zeta^{x+y} \\
&= \sum_{z \in \mathbb{F}_q} \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x(z-x)}{q}\right)\right) \cdot \zeta^z \qquad \text{(met } z = x + y\text{)}
\end{aligned}$$

Voor $x = 0$ geldt $\left(\frac{x(z-x)}{q}\right) = 0$, voor $x \neq 0$ geldt

$$\left(\frac{x(z-x)}{q}\right) = \left(\frac{-x^2}{q}\right) \cdot \left(\frac{1 - zx^{-1}}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{1 - zx^{-1}}{q}\right).$$

Dus we vinden

$$\tau^2 = \left(\frac{-1}{q}\right) \cdot \sum_{z \in \mathbb{F}_q} c_z \zeta^z$$

waarbij

$$c_z = \sum_{x \in \mathbb{F}_q^*} \left(\frac{1 - zx^{-1}}{q}\right).$$

Als $z = 0$, dan $c_z = \sum_{x \in \mathbb{F}_q^*} \left(\frac{1}{q}\right) = q - 1$. Als $z \neq 0$, en x doorloopt $\mathbb{F}_q^*$, doorloopt $z \cdot x^{-1}$ ook $\mathbb{F}_q^*$, en $1 - zx^{-1}$ doorloopt $\mathbb{F}_q - \{1\}$, dus

$$c_z = \sum_{w \in \mathbb{F}_q} \left(\frac{w}{q}\right) - \left(\frac{1}{q}\right) = -1$$

want er zijn in $\mathbb{F}_q$ evenveel elementen w met $\left(\frac{w}{q}\right) = 1$ als met $\left(\frac{w}{q}\right) = -1$. Al met al vinden we:

$$\tau^2 = \left(\frac{-1}{q}\right)\left(q - 1 - \sum_{z \in \mathbb{F}_q^*} \zeta^z\right) = \left(\frac{-1}{q}\right) \cdot \left(q - \sum_{z=0}^{q-1} \zeta^z\right) = \left(\frac{-1}{q}\right) \cdot q$$

aangezien $\sum_{z=0}^{q-1} \zeta^z = \frac{\zeta^q - 1}{\zeta - 1} = 0$. Hiermee is 15.10 bewezen. □

Lemma 15.11. *Stel bovendien dat* $\mathrm{char}(K) = p$*, waarbij* p *een oneven priemgetal verschillend van* q *is. Dan geldt* $\tau^p = \left(\frac{p}{q}\right)\tau$.

Bewijs. Met 8.4 vinden we:

$$\begin{aligned}\tau^p &= \left(\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\zeta^x\right)^p = \sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)^p\cdot\zeta^{xp}\\ &= \sum_{y\in\mathbb{F}_q}\left(\frac{yp^{-1}}{q}\right)\cdot\zeta^y \qquad\qquad (\text{met } y = x\cdot(p \bmod q)\in\mathbb{F}_q)\\ &= \left(\frac{p}{q}\right)^{-1}\cdot\sum_{y\in\mathbb{F}_q}\left(\frac{y}{q}\right)\cdot\zeta^y = \left(\frac{p}{q}\right)\cdot\tau.\end{aligned}$$

Hiermee is 15.11 bewezen. □

Tweede bewijs van 15.5. Laten p en q twee verschillende priemgetallen zijn. Voor K kiezen we een uitbreiding van $\mathbb{F}_p$ waarin zich een primitieve q-de machts eenheidswortel bevindt, bijv. $K = \Omega_{\mathbb{F}_p}^{X^q-1}$ (vgl. 14.3), en we definiëren τ als boven.

Uit 15.10 blijkt dat $\tau \neq 0$, dus 15.11 levert

$$\tau^{p-1} = \left(\frac{p}{q}\right) \qquad (\text{in } K).$$

Wegens 15.10 geldt

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

Aangezien verder geldt

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}, \qquad q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) \qquad (\text{in } \mathbb{F}_p, \text{ dus ook in } K)$$

concluderen we

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

Hiermee is 15.5 opnieuw bewezen. □

Als toepassing van de kwadratische symbolen bewijzen we een aantal speciale gevallen van de voor 14.14 genoemde stelling van Dirichlet over priemgetallen in rekenkundige rijen.

Stelling 15.12. *Voor elke* $a \in \mathbb{Z}$ *met* $\mathrm{ggd}(a, 8) = 1$ *bestaan er oneindig veel priemgetallen* p *met* $p \equiv a \bmod 8$.

Voor elke $b \in \mathbb{Z}$ *met* $\mathrm{ggd}(b, 12) = 1$ *bestaan er oneindig veel priemgetallen* p *met* $p \equiv b \mod 12$.

Bewijs. Er zijn acht gevallen:

$$\begin{aligned}a &\equiv 1, 3, 5, \text{ of } 7 \mod 8,\\ b &\equiv 1, 5, 7, \text{ of } 11 \mod 12.\end{aligned}$$

De gevallen $a \equiv 1 \mod 8$, $b \equiv 1 \mod 12$ vallen onder 14.14. Van de overige behandelen we $a \equiv 7 \bmod 8$ in detail. De resterende vijf gevallen gaan analoog: zie Opgave 14.

Het geval $a \equiv 7 \mod 8$ berust op het volgende lemma.

Lemma 15.13. *Als n een oneven geheel getal is, dan geldt $n^2-2 \equiv -1 \mod 8$, en voor elke priemdeler p van n^2-2 geldt $p \equiv 1$ of $-1 \mod 8$.*

Bewijs van 15.13. Het is eenvoudig te controleren dat $n^2 \equiv 1 \mod 8$, dus $n^2-2 \equiv -1 \mod 8$. Als $p \mid n^2-2$, dan $n^2 \equiv 2 \mod p$ dus $\left(\frac{2}{p}\right) = 1$ wegens 15.3, en 15.7 levert nu $p \equiv \pm 1 \mod 8$. Dit bewijst 15.13. □

Is, in 15.13, n groter dan 1, dan $n^2-2 > 1$. Zouden alle priemfactoren van n^2-2 congruent met 1 (mod 8) zijn, dan zou n^2-2 ook $1 \mod 8$ zijn, een tegenspraak met 15.13. We concluderen dat n^2-2, voor elke oneven $n > 1$, een priemdeler p heeft die niet $1 \mod 8$ is, dus volgens 15.13 congruent met $-1 \equiv 7 \mod 8$ moet zijn.

Om te zien dat dit inderdaad oneindig veel priemgetallen $p \equiv -1 \mod 8$ oplevert merken we op dat we altijd n deelbaar door een willekeurig voorgegeven eindig aantal oneven priemgetallen $q_1, q_2, \ldots, q_t$ kunnen kiezen. Dan $q_i \nmid n^2-2$, dus p is verschillend van alle q_i, waaruit blijkt dat er oneindig veel p's moeten zijn. Hiermee is 15.12 bewezen. □

15.14 Het berekenen van $\left(\frac{a}{p}\right)$ Als voorbeeld bepalen we $\left(\frac{757}{3359}\right)$ (beide getallen zijn priem).

$$\begin{aligned}
\left(\frac{757}{3359}\right) &= \left(\frac{3359}{757}\right) && \text{(Stelling 15.5; } 757 \equiv 1 \mod 4) \\
&= \left(\frac{331}{757}\right) && \text{(want } 3359 \equiv 331 \mod 757) \\
&= \left(\frac{757}{331}\right) && \text{(weer 15.5; 331 is priem)} \\
&= \left(\frac{95}{331}\right) && \text{(} 757 \equiv 95 \mod 331) \\
&= \left(\frac{5}{331}\right) \cdot \left(\frac{19}{331}\right).
\end{aligned}$$

Nu geldt:

$$\begin{aligned}
\left(\frac{5}{331}\right) &= \left(\frac{331}{5}\right) = \left(\frac{1}{5}\right) = 1, \\
\left(\frac{19}{331}\right) &= -\left(\frac{331}{19}\right) = -\left(\frac{8}{19}\right) = -\left(\frac{2}{19}\right)^3 = -(-1)^3 = 1,
\end{aligned}$$

dus

$$\left(\frac{757}{3359}\right) = \left(\frac{95}{331}\right) = \left(\frac{5}{331}\right)\left(\frac{19}{331}\right) = 1.$$

Wegens 15.3 heeft de congruentie $x^2 \equiv 757 \mod 3359$ dus een oplossing. Inderdaad geldt $958^2 \equiv 757 \mod 3359$ (vgl. Opgave 21).

Om in het algemeen $\left(\frac{a}{p}\right)$ te berekenen, voor p een oneven priemgetal en $\gcd(a,p) = 1$, schrijft men

$$a = \pm 2^k \cdot q_1 q_2 \cdots q_t$$

waarbij de q_i oneven priemgetallen zijn. De factor $\left(\frac{\pm 2^k}{p}\right)$ laat zich met 15.6 en 15.7 berekenen, en de overblijvende factoren $\left(\frac{q_i}{p}\right)$ kan men met behulp van 15.5 uitdrukken als $\pm\left(\frac{p}{q_i}\right)$. Schrijf nu $p \equiv r_i \bmod q_i$, met $r_i \in \{0, 1, \ldots, q_i - 1\}$, dan geldt $\left(\frac{p}{q_i}\right) = \left(\frac{r_i}{q_i}\right)$, en de $\left(\frac{r_i}{q_i}\right)$ laten zich met inductie berekenen.

Voor grote getallen wordt deze methode aanzienlijk efficiënter als men het tijdrovende factorontbinden achterwege laat, en gewoon alle positieve oneven getallen als priem beschouwt. In bovenstaand voorbeeld vindt men dan bijvoorbeeld

$$\left(\frac{95}{331}\right) = -\left(\frac{331}{95}\right) = -\left(\frac{46}{95}\right) = -\left(\frac{2}{95}\right) \cdot \left(\frac{23}{95}\right) = \left(\frac{95}{23}\right) = \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

inderdaad het correcte antwoord. Dit moet natuurlijk theoretisch gerechtvaardigd worden; in het bijzonder moeten we een betekenis geven aan $\left(\frac{a}{n}\right)$ als n positief en oneven is, maar niet noodzakelijk priem. Dit gebeurt met behulp van het *Jacobi-symbool* $\left(\frac{a}{n}\right)$, dat voor $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, n oneven, als volgt gedefinieerd is:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right) \qquad \text{als } n = p_1 p_2 \cdots p_t, p_i \text{ priem.}$$

(Carl Gustav Jacob Jacobi, Duits wiskundige, 1804–1851.) In Opgaven 16, 17, 18, 19 vindt men de voornaamste eigenschappen van het Jacobi-symbool. In het bijzonder ziet men daar dat de analoga van 15.5, 15.6, 15.7 ook gelden, waarmee dan de boven aangeduide efficiëntere methode om $\left(\frac{a}{p}\right)$ te berekenen gerechtvaardigd is.

Opgaven

1. Bereken $\left(\frac{a}{p}\right)$ voor alle a en p met

$$p \text{ priem}, 2 < p \leq 23, \qquad a \in \mathbb{Z}, 0 \leq a < p.$$

2. Bereken $\left(\frac{5}{19}\right)$ met behulp van het lemma van Gauss 15.8.

3. Laat zien hoe de regel

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{als } p \equiv \pm 1 \mod 12 \\ -1 & \text{als } p \equiv \pm 5 \mod 12 \end{cases}$$

(voor p priem) uit 15.5 kan worden afgeleid.

4. Bewijs dat de volgende tabel voor elke a in de eerste kolom alle p aangeeft waarvoor $\left(\frac{a}{p}\right) = 1$.

a	p	a	p
2	$\pm 1 \mod 8$	-2	$1, 3 \mod 8$
3	$\pm 1 \mod 12$	-3	$1 \mod 3$
5	$\pm 1 \mod 5$	-5	$1, 3, 7, 9 \mod 20$
6	$\pm 1, \pm 5 \mod 24$	-6	$1, 5, 7, 11 \mod 24$

5. Laat a een *negatief* geheel getal zijn, en p en q oneven priemgetallen. Bewijs:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) \qquad \text{als } p \equiv q \mod 4|a|,$$
$$\left(\frac{a}{p}\right) = -\left(\frac{a}{q}\right) \qquad \text{als } p \equiv -q \mod 4|a|.$$

6. In deze paragraaf hebben we 15.5 bewezen met behulp van 15.9. Laat zien dat omgekeerd 15.9 uit 15.5 en 15.7 volgt.

7. Laat a een geheel getal zijn met $a \equiv 0$ of $1 \mod 4$, en p en q oneven priemgetallen met $p \equiv q \mod |a|$. Bewijs: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

8. Zij p priem, en $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$. Bewijs: als $a, b \in \mathbb{F}_p - \mathbb{F}_p^2$, dan $a \cdot b \in \mathbb{F}_p^2$.

9. Bewijs:

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{als } p \equiv 1 \text{ of } 3 \bmod 8, \\ -1 & \text{als } p \equiv -1 \text{ of } -3 \bmod 8. \end{cases}$$

10. Laat $f = X^2 + aX + b \in \mathbb{Z}[X]$ en zij p een oneven priemgetal. Bewijs:

$$\#\{x \in \mathbb{Z} \mid 0 \leq x < p, f(x) \equiv 0 \mod p\} = 1 + \left(\frac{a^2 - 4a}{p}\right).$$

11. Zoek een priemgetal p met
$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1.$$

12. Laat $a \in \mathbb{Z}$, en zij p een oneven priemgetal met $\left(\frac{a}{p}\right) = -1$. Bewijs: als $x, y, z, w \in \mathbb{Z}$ voldoen aan
$$x^2 - ay^2 = p(z^2 - aw^2)$$
dan geldt $x = y = z = w = 0$.

13. Zij p een oneven priemgetal, en $\zeta \in \Omega_{\mathbb{F}_p}^{X^8-1}$ een primitieve 8-ste machts eenheidswortel. Bewijs:
$$(\zeta + \zeta^{-1})^2 = 2, (\zeta + \zeta^{-1})^p = \begin{cases} \zeta + \zeta^{-1} & \text{als } p \equiv \pm 1 \mod 8, \\ -(\zeta + \zeta^{-1}) & \text{als } p \equiv \pm 3 \mod 8. \end{cases}$$
Leid hieruit een nieuw bewijs voor 15.7 af.

14. Maak het bewijs van 15.12 af door in plaats van $n^2 - 2$ de volgende uitdrukkingen te beschouwen:
$$\begin{array}{lll} n^2 + 2, & n \text{ oneven}, & \text{voor 3 mod 8;} \\ n^2 + 4, & n \text{ oneven}, & \text{voor 5 mod 8;} \\ n^2 + 4, & \gcd(n, 6) = 1, & \text{voor 5 mod 12;} \\ 4n^2 + 3, & \gcd(n, 6) = 1, & \text{voor 7 mod 12;} \\ 3n^2 - 4, & \gcd(n, 6) = 1, & \text{voor 11 mod 12.} \end{array}$$

15. Zij $f \in \mathbb{Z}[X] - \mathbb{Z}$. Bewijs: er zijn oneindig veel priemgetallen p waarvoor geldt: $\exists n \in \mathbb{Z} : f(n) \equiv 0 \mod p$. (Aanwijzing: zie voor $f = X^2 - 2$ het eind van het bewijs van 15.12.)

16. Voor $a, a_1, a_2 \in \mathbb{Z}$, $b, b_1, b_2 \in \mathbb{Z}_{>0}$, b, b_1, b_2 oneven, geldt:
    (a) $\left(\frac{a}{b}\right) \in \{-1, 0, 1\}$; en $\left(\frac{a}{b}\right) = 0 \iff \gcd(a, b) \neq 1$.
    (b) als $a_1 \equiv a_2 \mod b$ dan $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.
    (c) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right)$ en $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right)$.
    (d) als $\gcd(a, b) = 1$ en $\exists x \in \mathbb{Z} : x^2 \equiv a \mod b$, dan $\left(\frac{a}{b}\right) = 1$.

17. Voor oneven $b \in \mathbb{Z}_{>0}$ geldt:
$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{als } b \equiv 1 \mod 4 \\ -1 & \text{als } b \equiv -1 \mod 4. \end{cases}$$
$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{als } b \equiv \pm 1 \mod 8 \\ -1 & \text{als } b \equiv \pm 3 \mod 8. \end{cases}$$

18. Voor oneven $a, b \in \mathbb{Z}_{>0}$ geldt

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \qquad \text{als } a \equiv 1 \mod 4 \text{ of } b \equiv 1 \mod 4,$$
$$\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right) \qquad \text{als } a \equiv b \equiv 3 \mod 4.$$

19. Laat b_1, b_2 oneven positieve gehele getallen zijn, a een positief geheel getal, en stel dat $b_1 \equiv \pm b_2 \mod 4a$. Bewijs: $\left(\frac{a}{b_1}\right) = \left(\frac{a}{b_2}\right)$.

20. Laat $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$ zodat $\gcd(a, b) = 1$. Bewijs: $\left(\frac{a}{b}\right) = \epsilon(\sigma)$, waar $\sigma\colon (\mathbb{Z}/b\mathbb{Z}) \to (\mathbb{Z}/b\mathbb{Z})$ de permutatie is gedefinieerd door $\sigma(x) = x \cdot (a \bmod b)$.

21. Zij $p \equiv 3 \mod 4$ een priemgetal, en a een geheel getal met $\left(\frac{a}{p}\right) = 1$. Bewijs dat $x = a^{\frac{p+1}{4}}$ voldoet aan $x^2 \equiv a \mod p$.

    De voorgaande opgave levert een methode om de congruentie $x^2 \equiv a \mod p$ op te lossen als men weet dat er een oplossing bestaat, maar alleen voor het geval $p \equiv 3 \mod 4$, d.w.z.: $p - 1$ heeft precies één factor 2. Voor algemene p kan men Opgave 22 gebruiken, die al meer werk vereist naarmate $p - 1$ meer factoren 2 bevat.

22. Zij p een priemgetal, en schrijf $p - 1 = 2^k \cdot u$, met $k, u \in \mathbb{Z}$ en u oneven. Laat r een geheel getal zijn dat voldoet aan $r^{2^{k-1}} \equiv -1 \mod p$ (bijv. $r = s^u$, waar $\left(\frac{s}{p}\right) = -1$). Zij verder $a \in \mathbb{Z}$ zodanig dat $\left(\frac{a}{p}\right) = 1$. Bewijs dat het volgende algoritme om $x^2 \equiv a \mod p$ op te lossen correct is.

    (a) Laat $x = a^{\frac{u+1}{2}} \pmod p, c = a^u \pmod p$.

    (b) Als $c \equiv 1 \mod p$ dan geldt $x^2 \equiv a \mod p$, en het algoritme stopt.

    (c) Als $c \not\equiv 1$, bepaal dan de kleinste $m \in \mathbb{Z}_{>0}$ met $c^{2^m} \equiv 1 \mod p$, vervang x door $x \cdot r^{2^{k-1-m}} \pmod p$ en c door $c \cdot r^{2^{k-m}} \pmod p$, en ga terug naar stap (b).

    (Aanwijzing: bewijs dat steeds geldt $x^2 \equiv a \cdot c \mod p$, waarbij $c^{2^i} \equiv 1 \mod p$ voor een geheel getal $i \leq k - 1$ dat voortdurend kleiner wordt.)

23. Bereken $\left(\frac{a}{127}\right)$ voor $999 \leq a \leq 1004$.

24. Zij τ als in 15.11. Bewijs: $\tau^2 \in \mathbb{F}_p$, en $[\mathbb{F}_p(\tau) : \mathbb{F}_p] = 1$ of 2 al naar gelang $\left(\frac{p}{q}\right) = 1$ of -1.

25. Zij $\mathbb{F}_q$ een eindig lichaam met q oneven, en $a \in \mathbb{Z}$. Bewijs dat het Jacobi-symbool $\left(\frac{a}{q}\right)$ gelijk is aan 1 dan en slechts dan als er een $b \in \mathbb{F}_q^*$ is met $b^2 = a \cdot 1$.

Index