

Inhoudsopgave

1	Ringen	4
1.1	Definitie, voorbeelden, elementaire eigenschappen	4
1.2	Eenheden en nuldelers	8
1.3	Constructies van ringen	13
1.4	Opgaven	20
2	Ringhomomorfismen en idealen	26
2.1	Ringhomomorfismen	26
2.2	De factorring R/I	31
2.3	Rekenen met idealen	37
2.4	Opgaven	45
3	Polynoomringen	51
3.1	Polynomen	51
3.2	Evaluatiehomomorfismen	54
3.3	Delen met rest van polynomen	57
3.4	Polynoomringen over een lichaam	62
3.5	Polynoomringen over een domein	64
3.6	Differentiëren	65
3.7	Opgaven	68
4	Priemidealen en maximale idealen	73
4.1	Priemidealen	73
4.2	Maximale idealen	76
4.3	Het lemma van Zorn	77
4.4	Opgaven	83
5	Deling in ringen	88
5.1	Irreducibele elementen	88
5.2	Hoofdideaaldomeinen	90
5.3	Ontbindingsdomeinen	93
5.4	Deelbaarheid	97
5.5	Het factoriseren van polynomen	101
5.6	Opgaven	106
6	Modulen	110
6.1	Definities	110
6.2	R -moduulhomomorfismen	112
6.3	Direkte sommen	113
6.4	Een bovendriehoeksvorm voor matrices	121

6.5	Opgaven	129
7	Lichamen	133
7.1	Priemlichamen en karakteristiek	133
7.2	Algebraïsch en transcendent	134
7.3	Eindige en algebraïsche uitbreidingen	138
7.4	Het bepalen van het minimumpolynoom	143
7.5	Opgaven	146
8	Lichaamsautomorfismen en ontbindingslichamen	149
8.1	Lichaamshomomorfismen	149
8.2	Ontbindingslichamen	154
8.3	Opgaven	160
9	Eindige lichamen	161
9.1	Classificatie van eindige lichamen.	161
9.2	Structuur van eindige lichamen	164
9.3	Irreducibele polynomen in $\mathbb{F}_q[X]$	168
9.4	De vermenigvuldigingsgroep van een eindig lichaam.	170
9.5	Opgaven	173
10	Algebraïsch afgesloten lichamen	177
10.2	Opgaven	184
11	Symmetrische polynomen	185
11.2	Opgaven	194
12	De getallen van Gauss	196
12.1	Sommen van kwadraten	196
12.2	Euclidische ringen	200
12.3	Het Euclidische algoritme	204
12.4	Opgaven	208
13	Projectieve Modulen	211
13.1	Quotiënten van modulen	211
13.2	Homomorfismen van R -modulen	213
13.3	Hom en exactheid	216
13.4	Eigenschappen van projectieve modulen	219
13.5	Opgaven	224

14 Cyclotomische lichamen	225
14.1 De kwadratische reciprociteitswet	225
14.2 De p -de eenheidswortels over \mathbb{Q}	232
14.3 Opgaven	235
Index	236

1 Ringen

1.1 Definitie, voorbeelden, elementaire eigenschappen

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

$$+ : R \times R \rightarrow R, \quad (a, b) \mapsto a + b \quad \cdot : R \times R \rightarrow R, \quad (a, b) \mapsto ab,$$

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 $0 + 0 = 0 \cdot 0 = 0$.

Men komt ook definities tegen van ringen $(R, +, \cdot, 0)$ waarbij (R1) t/m (R3) moeten gelden; zulke ringen noemen we niet-unitaire ringen.

Een **delingsring** (of **scheeffichaam**) 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 ($\neq 0$), 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 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ met $\bar{i} = i + n\mathbb{Z} \subset \mathbb{Z}$, is een optelling gedefinieerd, omdat dit de nevenklassen zijn van de normale ondergroep $n\mathbb{Z}$ van \mathbb{Z} . De regel

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

waarbij de \cdot rechts de gewone vermenigvuldiging in \mathbb{Z} is, definieert een product (ga na dat als $\bar{a} = \bar{a}_1$ en $\bar{b} = \bar{b}_1$ 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 $\bar{1}$. In 1.18 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 $M(n, \mathbb{R})$ der $n \times n$ -matrices met reële coëfficiënten is, met de gebruikelijke matrix-optelling en matrixvermenigvuldiging, een ring met eenheidselement. 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 $M(n, R)$ definiëren.

Voorbeeld 1.5 Laat K een lichaam zijn (bv. \mathbb{R} of \mathbb{Q}) en laat $\alpha, \beta \in K - \{0\}$. De **quaternionenalgebra** $(\alpha, \beta)_K$ bestaat uit uitdrukkingen (quaternionen) van de vorm:

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

Twee quaternionen zijn gelijk als de componenten het zijn:

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

De quaternionenalgebra is een ring. 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 regeltjes:

$$ij = -ji = k, \quad i^2 = \alpha, \quad j^2 = \beta, \quad \text{en}$$

$$x(a + bi + cj + dk) = (a + bi + cj + dk)x = ax + bxi + cxj + dxk,$$

met $x = x + 0 \cdot i + 0 \cdot j + 0 \cdot k \in K$. Om een ring te verkrijgen moet dan zeker gelden:

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

Uitgewerkt levert dit

$$\begin{aligned} (a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) &= \\ &= (aa' + bb'\alpha + cc'\beta - dd'\alpha\beta) \\ &\quad + (ab' + ba' - cd'\beta + dc'\beta)i \\ &\quad + (ac' + bd'\alpha + ca' - db'\alpha)j \\ &\quad + (ad' + bc' - cb' + da')k \end{aligned}$$

Men kan nu rechtstreeks verifiëren dat de quaternionen een ring vormen.

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

$$\bar{q} := a - bi - cj - dk.$$

We definiëren

$$N(q) := q\bar{q} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2,$$

i.h.b. geldt $N(q) \in K$ voor elk quaternion q . Merk op dat

$$N(q) \neq 0 \Rightarrow (a + bi + cj + dk)^{-1} = \frac{1}{N(q)}\bar{q} = \frac{a}{N(q)} - \frac{b}{N(q)}i - \frac{c}{N(q)}j - \frac{d}{N(q)}k.$$

Dit impliceert:

$$(\alpha, \beta)_K \quad \text{is een } \textit{delingsring} \text{ precies dan als}$$

voor alle $a, b, c, d \in K$ geldt:

$$N(a + bi + cj + dk) = 0 \implies a = b = c = d = 0.$$

Als nl. geldt: $N(q) = 0 \Rightarrow q = 0$ dan heeft $q \neq 0$ als inverse $q^{-1} := \frac{1}{N(q)}\bar{q}$ en dus is $(\alpha, \beta)_K$ een delingsring. Omgekeerd, als er een $q \neq 0$ is met $N(q) = 0$ dan is $q\bar{q} = 0$. Zou deze q toch een inverse q^{-1} hebben, dan: $0 = q^{-1}q\bar{q} = 1 \cdot \bar{q} = \bar{q}$, maar dan is ook $q = 0$, een tegenspraak. Zo'n q kan dus geen inverse hebben en $(\alpha, \beta)_K$ is geen delingsring.

In geval $K = \mathbb{R}$ definieert men de quaternionen van Hamilton (1843; Sir William Rowan Hamilton, Engels-Iers wiskundige, 1805-1865) als zijnde de quaternionen algebra $(-1, -1)_{\mathbb{R}}$ en men schrijft:

$$\mathbb{H} := (-1, -1)_{\mathbb{R}}, \quad \text{dwz. in } \mathbb{H}: \quad i^2 = j^2 = k^2 = -1.$$

In het bijzonder is \mathbb{H} een delingsalgebra want $N(q) = a^2 + b^2 + c^2 + d^2 = 0$ met $a, b, c, d \in \mathbb{R}$ precies dan als $a = b = c = d = 0$.

Tenslotte een voorbeeld van een quaternionenalgebra die geen delingsalgebra is. In $M(2, \mathbb{R})$ vinden we de volgende matrices:

$$\mathbf{i} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{j} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{k} := \mathbf{ij} = -\mathbf{ji} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Voorts is iedere matrix in $M(2, \mathbb{R})$ te schrijven als $\begin{pmatrix} p & q \\ r & s \end{pmatrix} =$

$$= \frac{p+s}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{p-s}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \frac{q+r}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{q-r}{2} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Op deze wijze zien we dat $M(2, \mathbb{R})$ geïdentificeerd wordt met de quaternionenalgebra $(1, 1)_{\mathbb{R}}$. Het is geen delingsalgebra want bv. $\mathbf{j} + \mathbf{k} \neq 0$ maar $N(\mathbf{j} + \mathbf{k}) = 0$, dus $(\mathbf{j} + \mathbf{k})$ kan geen inverse hebben in de quaternionen algebra $(1, 1)_{\mathbb{R}}$.

Voor meer voorbeelden van ringen en methoden om ringen te construeren verwijzen we naar paragraaf 1.3.

Definitie 1.6 Een deelverzameling R' van een ring R heet een (unitaire) **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 , d.w.z. $a - b \in R'$ voor alle $a, b \in R'$;

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

1.1.1 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 $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ 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 met 1, maar geen lichaam. De verzameling $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ is ook een deelring van \mathbb{C} en is wèl 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

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

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

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 $a, b, b_1, \dots, b_n, c \in R$:*

$$a(b_1 + b_2 + \dots + b_n) = ab_1 + ab_2 + \dots + ab_n,$$

$$(b_1 + b_2 + \dots + b_n)a = b_1a + b_2a + \dots + b_na,$$

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

$$a \cdot 0 = 0 \cdot a = 0.$$

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. \square

1.2 Eenheden en nuldelers

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 (unitaire) 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 met 1. 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 1.11). Men vindt ook wel de notatie $U(R)$ (unit (Engels) = eenheid).

Een element $a \in R$ noemt men een **linkseenheid** als $\exists b \in R : ab = 1$, en een **rechtseenheid** als $\exists c \in R : ca = 1$.

1.2.1 Als $a \in R$ zowel een links- als rechtseenheid is, dan is a een eenheid, nl.

$$ab = 1, \quad ca = 1 \quad \implies \quad cab = c \implies b = c.$$

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 1.3.3.

Voorbeeld 1.10 $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$, $\mathbb{H}^* = \mathbb{H} - \{0\}$.

1.2.2 In het algemeen geldt, zie (R6):

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

Stelling 1.11 *De eenhedengroep R^* van een ring R met 1 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).

R^* heeft een neutraal element, 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 4 axioma's voor een groep geverifieerd en de stelling is bewezen. \square

1.2.3 Als R commutatief is, is R^* natuurlijk abels. De omkering geldt niet: men kan een niet-commutatieve (unitaire) ring R construeren waarvoor R^* abels is, zie opgave 18.

Voorbeeld 1.12 Indien $A \in M(n, \mathbb{R})$ inverteerbaar is met inverse B dan geldt $AB = BA = I$, met I de identiteitsmatrix. Bovendien geldt:

A is een linkseenheid $\iff A$ is een rechtseenheid $\iff \det(A) \neq 0$.

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

Voorbeeld 1.13 Zij $R = \mathbb{Z}[\sqrt{m}]$ als in 1.7, waar m een geheel getal is dat geen kwadraat is. We definiëren de **norm**

$$N : R \longrightarrow \mathbb{Z}, \quad N(a + b\sqrt{m}) = (a + b\sqrt{m}) \cdot (a - b\sqrt{m}) = a^2 - mb^2.$$

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

$$\alpha \in R^* \iff N(\alpha) = \pm 1;$$

\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 .

\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

$$a = \pm 1, \quad b = 0, \quad \text{en}$$

$$a = 0, \quad b = \pm 1, \quad |m| = 1.$$

Dus er geldt

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

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

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 $\dots, \pm\epsilon^{-2}, \pm\epsilon^{-1}, \pm 1, \pm\epsilon, \pm\epsilon^2, \dots$. 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: $x_{n+1} = 2x_n + x_{n-1}$, $y_{n+1} = 2y_n + y_{n-1}$.)

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

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

Definitie 1.14 Een element a van een ring R heet een **linkernuldeler** als: $a \neq 0$ en $\exists b \in R : b \neq 0 \wedge ab = 0$;

een **rechternuldeler** als $a \neq 0$ en $\exists c \in R : c \neq 0 \wedge ca = 0$;

en een **nuldeler** als het een linker- of rechternuldeler is.

Een **nilpotent element** is een $a \in R$, $a \neq 0$, en met $a^n = 0$ 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** als $a^2 = a$ en $0 \neq a \neq 1$. Een idempotent element is altijd 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 $a, a - 1 \neq 0$.

Voorbeeld 1.15 In $M(2, \mathbb{R})$ bekijken we de volgende elementen:

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

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 1.16 *Een element a van een commutatieve ring R met 1 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 1.16. \square

Opmerking 1.17 Het bewijs van 1.16 laat in feite zien dat in een willekeurige (niet noodzakelijk commutatieve) ring een linkernuldeler geen rechtseenheid (zie voor 1.2.1) kan zijn. Evenzo kan een rechternuldeler geen linkseenheid zijn. In 1.3.3 zullen we aan de hand van een voorbeeld zien dat een linkernuldeler wel een linkseenheid kan zijn.

Gevolg 1.2.5 *Een delingsring heeft geen nuldelers.*

Bewijs. Dit volgt uit 1.2.2, want alle elementen $\neq 0$ van een delingsring zijn eenheden. \square

Stelling 1.18 *Voor $n \in \mathbb{Z}_{>0}$ geldt:*

$\mathbb{Z}/n\mathbb{Z}$ is een lichaam $\iff n$ is een priemgetal.

Voor een priemgetal p noteren we het lichaam $\mathbb{Z}/p\mathbb{Z}$ met

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}.$$

Bewijs. Voor een commutatieve ring R met 1 geldt (zie 1.2.2):

R is een lichaam $\iff R^* = R - \{0\}$.

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

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

Het element $\bar{a} \in \mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}$ kan dus geen eenheid zijn (zie 1.16) en dus is $\mathbb{Z}/n\mathbb{Z}$ 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 $m\bar{a} := \bar{a} + \dots + \bar{a}$ (m keer) gelijk is aan $\bar{1}$. Dan is dus $m\bar{a} = \bar{a}m = \bar{1}$, en \bar{m} is de gezochte inverse van \bar{a} .

Hiermee is stelling 1.18 bewezen. \square

1.2.6 In hoofdstuk 9 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 1.19 Een **domein** (of **integriteitsgebied**) is een commutatieve ring met $1 \neq 0$ zonder nuldelers.

Voorbeeld 1.20 Voorbeelden van domeinen zijn lichamen (wegens 1.2.5), zoals

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_{59},$$

en ook (unitaire) deelringen van lichamen, zoals \mathbb{Z} , $\mathbb{Z}[i]$. In 1.3.2 zullen we zien dat ieder domein deelring van een lichaam is.

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

Stelling 1.21 *Zij R een ring zonder nuldelers (bijv. een domein), en $a, b, c \in R$. Dan geldt:*

$$a. \quad ab = 0 \iff a = 0 \text{ of } b = 0,$$

$$b. \quad ab = ac \iff a = 0 \text{ of } b = c.$$

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. $ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$ (wegens 1.8) $\Leftrightarrow a = 0$ of $b - c = 0$ (wegens onderdeel (a)) $\Leftrightarrow a = 0$ of $b = c$. Dit bewijst 1.21.

□

1.3 Constructies van ringen

We geven nog enkele belangrijke manieren om ringen te construeren.

1.3.1 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

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

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 al deze beweringen worden aan de lezer overgelaten.

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 $a \in R_1$, $b \in R_2$.

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

1.3.2 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 $R \times S = \{(a, s) : a, s \in R, s \neq 0\}$ definiëren we een equivalentierelatie \sim door

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

Dat dit inderdaad een equivalentierelatie is is gemakkelijk na te gaan: reflexiviteit $((a, s) \sim (a, s))$ en symmetrie $((a, s) \sim (b, t) \Rightarrow (b, t) \sim (a, s))$ zijn triviaal, en transitiviteit $((a, s) \sim (b, t) \wedge (b, t) \sim (c, u) \Rightarrow (a, s) \sim (c, u))$ wordt als volgt bewezen.

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

$$aut = cst \implies (au - cs)t = 0,$$

en $t \neq 0$, volgt uit 1.19 (b): $au = cs$. 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 $\frac{a}{s}$ in. Dus er geldt:

$$Q(R) = \left\{ \frac{a}{s} : a, s \in R, s \neq 0 \right\},$$

$$\frac{a}{s} = \frac{b}{t} \iff at = bs.$$

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

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

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

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 geldt:

$$\frac{a'}{s'} = \frac{a}{s} \quad \wedge \quad \frac{b'}{t'} = \frac{b}{t} \quad \implies \quad a's = as' \quad \wedge \quad b't = bt' \quad \implies$$

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

$$= (at + bs)s't' \quad \implies \quad \frac{a't' + b's'}{s't'} = \frac{at + bs}{st}$$

en voor het product is het 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 $\frac{a}{1} \in Q(R)$:

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

Merk hierbij op dat er zo geen twee verschillende elementen van R aan elkaar gelijk gemaakt worden, want $\frac{a}{1} = \frac{b}{1} \Leftrightarrow a \cdot 1 = b \cdot 1 \Leftrightarrow a = b$. 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 $\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$.

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 1.20 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

$$K(X) := Q(K[X])$$

(voor een precieze definitie van $K[X]$ zie verderop in 3.1). Elementen van $K(X)$ zijn bijvoorbeeld $\frac{1}{1+X} = \frac{X}{X+X^2}$, $\frac{1-X^2}{1-X+X^3}$.

Voor een in de theorie van de commutatieve ringen belangrijke generalisatie van de constructie van het quotiëntenlichaam verwijzen we naar opgave 29.

1.3.3 Endomorfismenringen. Zij A een additief geschreven abelse groep, en $End(A)$ de verzameling endomorfismen van A :

$$End(A) := \{f : A \rightarrow A : f(a+b) = f(a) + f(b) \quad \forall a, b \in A\}.$$

Voor $f, g \in End(A)$ definiëren we $f + g : A \rightarrow A$ en $fg : A \rightarrow A$ door

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

Omdat A abels is geldt $f + g \in End(A)$, en ook geldt $fg \in End(A)$. Het is gemakkelijk na te gaan dat $End(A)$ 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 $A = 0$.

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 matrix optelling en -vermenigvuldiging corresponderen met de boven gedefinieerde optelling en vermenigvuldiging van endomorfismen, zien we dat $M(n, \mathbb{R})$ te beschouwen is als deelring van $End(A)$.

Omdat $M(n, \mathbb{R})$ niet-commutatief is voor $n \geq 2$ zien we dat $End(A)$ 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 $f, g, x \in End(A)$ door

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

We schrijven verder $1 = id_A$, het eenheidslement van $End(A)$. Men rekent nu eenvoudig na, dat in $End(A)$ geldt:

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

Dus f is een linkseenheid en een linkernuldeler in $End(A)$. Wegens opmerking 1.17 kan f geen rechtseenheid of rechternuldeler zijn. Evenzo is x een rechtseenheid en een rechternuldeler, maar geen linkseenheid of linkernuldeler.

Differentiatie geeft een $d \in End(A)$:

$$d : a_0 + a_1X + \dots + a_nX^n \mapsto a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

Merk op dat geldt:

$$\begin{aligned} dx(a_0 + a_1X + \dots + a_nX^n) &= d(a_0X + a_1X^2 + \dots + a_nX^{n+1}) \\ &= a_0 + 2a_1X + \dots + (n+1)a_nX^n, \end{aligned}$$

en

$$\begin{aligned} xd(a_0 + a_1X + \dots + a_nX^n) &= x(a_1 + 2a_2X + \dots + na_nX^{n-1}) \\ &= a_1X + 2a_2X^2 + \dots + na_nX^n. \end{aligned}$$

Voor elke $f \in A$ is blijkbaar $(dx - xd)f = f$, dus in de ring $End(A)$ geldt:

$$dx - xd = id_A.$$

We beschouwen \mathbb{R} als deelring van $End(A)$ door:

$$a : a_0 + a_1X + \dots + a_nX^n \mapsto aa_0 + aa_1X + \dots + aa_nX^n.$$

Omdat $End(A)$ een ring is, zit ook elke eindige lineaire combinatie

$$D := \sum_{i,j}^{<\infty} a_{ij}x^i d^j, \quad a_{ij} \in \mathbb{R}$$

in $End(A)$. Door herhaald toepassen van de regel $dx - xd = 1$ zien we dat

$$W := \left\{ \sum_{i,j}^{<\infty} a_{ij}x^i d^j \in End(A) \right\}$$

een deelring van $End(A)$ is. We noemen W de **Weyl algebra**.

1.3.4 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 $f, g : V \rightarrow R$ som $f + g$ en product fg als volgt te definiëren:

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

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

voor $v \in V$. Geldt $V = \{v_1, v_2, \dots, v_n\}$, met $n \in \mathbb{Z}_{>0}$, dan zien we dat R^V ‘dezelfde’ ring is als $R \times R \times \dots \times R$ (product van ringen: zie 1.3.1) ziet men in dat R^V voor $\#V \geq 2$, $R \neq \{0\}$ 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

$$C([0, 1]) = \{f : [0, 1] \rightarrow \mathbb{R} : f \text{ is continu}\}.$$

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

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

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

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

1.3.5 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 $\forall g \in G : a_g = b_g$. 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:

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

dus uitgewerkt met de distributieve wet:

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

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

Als R en G beide commutatief zijn, is ook $R[G]$ commutatief. Heeft R een 1, dan heeft ook $R[G]$ een eenheidselement, nl. 1.e, waarbij e het neutrale element van G aangeeft; in het vervolg schrijven we hiervoor gewoon 1.

Als R een 1 heeft, kunnen we 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

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

een nuldeeler van $R[G]$, want

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

Het is een onopgelost probleem of $R[G]$ nuldelers kan hebben in het geval dat R een lichaam is en G een groep die geen elementen van eindige orde behalve e bevat.

1.4 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. Bewijs dat de verzameling $2\mathbb{Z}$ der even gehele getallen met de gebruikelijke optelling en vermenigvuldiging een commutatieve ring *zonder* eenheidselement is.
4. Laat $M(2, 2\mathbb{Z})$ de deelverzameling van $M(2, \mathbb{R})$ (zie 1.4) zijn bestaande uit die 2×2 -matrices waarvan de coëfficiënten tot $2\mathbb{Z}$ behoren. Bewijs: $M(2, 2\mathbb{Z})$ is met de gewone matrixoptelling en -vermenigvuldiging een *niet*-commutatieve ring *zonder* eenheidselement.
5. Zij A een *additief* geschreven abelse groep, en definieer op A een vermenigvuldiging door $a \cdot b = 0$ voor alle $a, b \in A$. Bewijs dat A hiermee een commutatieve ring wordt. Heeft deze ring een eenheidselement?
6. Laat R een niet-unitaire ring zijn met $R^+ \cong \mathbb{Q}/\mathbb{Z}$. Bewijs dat voor alle $a, b \in R$ geldt: $ab = 0$.
7. Zij m een geheel getal dat geen kwadraat is, en $\alpha := \frac{1+\sqrt{m}}{2} \in \mathbb{C}$.
 - a. Voor welke m is $\mathbb{Z}[\alpha] := \{a + b\alpha : a, b \in \mathbb{Z}\}$ een deelring van \mathbb{C} ?
 - b. Hoe ziet $\mathbb{Z}[\alpha]$ er als deelverzameling van het complexe vlak uit als $m = -3$?
8. Zij R een ring (niet noodzakelijk unitair), en 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

$$ns = s + s + \dots + s \quad (n \text{ keer})$$

voor $n > 0$, etc.).

- a. Bewijs dat $\mathbb{Z} \times R$ hiermee een ring met eenheidselement wordt.

- b. Bewijs dat iedere ring kan worden ingebed als deelring in een ring met eenheidselement.
9. Zij R een ring met 1, en H een additieve ondergroep van R . Laat $R_0 = \{x \in R : \forall h \in H : xh \in H\}$. Bewijs dat R_0 een deelring van R is, $R_0 \neq \{0\}$ als $R \neq \{0\}$.
10. Laat R een ring zijn, en $a \in R$. Definieer $\lambda_a, \phi_a : R \rightarrow R$ door $\lambda_a(x) = ax, \phi_a(x) = xa$. Bewijs dat λ_a en ϕ_a endomorfismen van de additieve groep R^+ van R zijn.
11. 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 vermenigvuldiging een ring is. Deze ring heet de **tegengestelde** ring van R , notatie: R^0 .
12. Zij R een ring. Het **centrum** van R is

$$Z(R) = \{a \in R : \forall x \in R : ax = xa\}.$$

Bewijs dat dit een deelring van R is.

13. 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 $x \in R$.
14. Stel dat R een ring is die uit 10 elementen bestaat. Bewijs dat R commutatief is.
15. (**Binomium** van Newton). Laat R een ring zijn. Voor $n \in \mathbb{Z}, r \in R$ definiëren we $nr \in R$ als in opgave 8.
- a. Stel R is commutatief. Bewijs dat

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

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

17. Zij R een commutatieve ring met 1 en $n \in \mathbb{Z}_{>0}$. Voor $A \in M(n, R)$ is $\det(A)$ volgens de uit de lineaire algebra bekende formule gedefinieerd:

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n a_{i\sigma(i)} \quad \text{als } A = [a_{ij}]_{1 \leq i, j \leq n}.$$

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

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

- Bewijs dat T een deelring van $M(2, R)$ is, en dat T niet commutatief is.
- Bewijs: $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in T^* \iff a \in R^*$ en $d \in R^*$.
- Bewijs: T^* is commutatief $\iff R^* = \{1\}$.
- Stel dat $R = \mathbb{Z}/2\mathbb{Z}$. Bewijs: T is een niet-commutatieve ring met een commutatieve eenhedengroep.

19. Laat $m \in \mathbb{Z}_{>0}$, $\sqrt{m} \notin \mathbb{Z}$.

- 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: $\epsilon > 1 \iff a > 0 \wedge b > 0$.
- 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 $\mathbb{Z}[\sqrt{m}]^* = \langle -1, \epsilon_1 \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.

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

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

- Bewijs dat S een deelring van R is.
 - Bewijs: $S^* = R^* \cap S$.
21. Laat $A \in M(n, \mathbb{R})$. Bewijs: A is een linkernuldeler $\iff A$ is een rechternuldeler $\iff A \neq 0$ en $\det(A) = 0$.
22. Geef een voorbeeld van een commutatieve ring R met 1, die een element a bevat met de eigenschappen: $a \neq 0$, a is geen eenheid van R , en a is geen nuldeler van R .
23. Geef een voorbeeld van een oneindige commutatieve ring die nuldelers bezit.

24. Zij K een lichaam, en definieer op $R = K \times K$ een optelling en een vermenigvuldiging door

$$(x, y) + (u, v) = (x + u, y + v),$$

$$(x, y) \cdot (u, v) = (xu, yv).$$

- a. Bewijs dat R een niet-commutatieve ring zonder eenheidselement is.
 - b. Bepaal de linkernuldelers van R en de rechternuldelers van R .
25. Zij R een commutatieve ring met 1, en R' een deelring van R met $1 \in R'$. 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.

26. Laten R_1 en R_2 ringen zijn. Bewijs: $R_1 \times R_2$ is een domein \Leftrightarrow 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'.

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

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

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

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

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: $f \in R^* \Leftrightarrow f(1) \neq 0$.
28. a. Zij R een domein en R' een deelring van R met $1 \in R'$. 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 $\mathbb{Q}[\sqrt{m}]$.

29. Zij R een commutatieve ring met 1, 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 met 1 wordt:

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

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

30. Zij A een abelse groep. Bewijs: $End(A)^* = Aut(A)$.

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

32. Zij R een ring met 1, en $a, b \in R$ zò, dat $ab = 0$. Dan geldt $(ba)^2 = 0$ en $1 + ba \in R^*$; bewijs dit.

33. (G. Higman, Proc. London Math. Soc. 46 (1940), 231-248).

a. Laat $R = \mathbb{Z}[S_3]$, $a = (13) \cdot \{1 - (12)\}$, $b = 1 + (12) \in R$. 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: $1 - g - g^{-1} \in \mathbb{Z}[G]^*$.

34. Een **Boolese ring** (naar de Engelse wiskundige George Boole, (1815-1864)) is een ring R waarin geldt $x^2 = x$ voor alle $x \in R$.
- Bewijs: $x + x = 0$ voor alle x in een Boolese ring R .
 - Bewijs dat elke Boolese ring commutatief is.
 - Stel dat de Boolese ring R een lichaam is. Bewijs: $R \cong \mathbb{F}_2$.

35. 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

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

Bewijs dat R hiermee een commutatieve ring met 1 wordt, en dat R een lichaam is dan en slechts dan als $\#X = 1$. Bewijs ook dat R een **Boolese ring** is (opgave 34).

36. Zij R een (unitaire) ring. Zij $v \in R$ een rechtsinversen van $u \in R$: $uv = 1$. Bewijs dat de volgende 3 beweringen equivalent zijn:
- u heeft meer dan één rechtsinversen;
 - u is geen eenheid;
 - u is een linksnuldeler, d.w.z. $\exists x \neq 0 : ux = 0$.

37. (Kaplansky) Zij R een (unitaire) ring. Bewijs: u heeft meer dan één rechtsinversen $\implies u$ heeft ∞ veel rechtsinversen. (Hint: als $uv = 1$ en $vu \neq 1$, beschouw dan de rechtsinversen $v + (1 - vu)u^n$.)

38. Zij R een eindige (unitaire) ring en zij $u \in R$ met $u \neq 0$. Bewijs dat de volgende uitspraken equivalent zijn:
- u heeft een rechtsinversen;
 - u heeft een linksinversen;
 - u is geen linksnuldeler;
 - u is geen rechtsnuldeler;
 - u is een eenheid.

39. Zij R een (unitaire) ring. Bewijs dat voor $a, b \in R$ geldt:

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

2 Ringhomomorfismen en idealen

2.1 Ringhomomorfismen

Definitie 2.1.1 Een afbeelding $f : R_1 \rightarrow R_2$ van een (unitaire) ring R_1 naar (unitaire) een ring R_2 heet een (unitair) **ringhomomorfisme** als geldt

$$f(1) = 1,$$

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

$$f(ab) = f(a) \cdot f(b)$$

voor alle $a, b \in R_1$. (Het '(unitair)' in de definitie van ringhomomorfisme correspondeert met de eerste eis.)

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

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

2.1.2 Voorbeelden.

- Is R' een deelring van een ring R , dan is de inclusie afbeelding $R' \rightarrow R$ een injectief ringhomomorfisme.
- Laat $n \in \mathbb{Z}_{>0}$. De kanonieke afbeelding

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad f(a) = \bar{a},$$

is een ringhomomorfisme, omdat $\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a} \cdot \bar{b} = \overline{ab}$.

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

$$\gamma_s : R \longrightarrow R, \quad r \mapsto sr s^{-1}$$

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

- Zijn R_1, R_2 ringen, dan is de projectie $f : R_1 \times R_2 \rightarrow R_1$, $f((a, b)) = a$, een ringhomomorfisme.

Definitie 2.1.3 Zij $f : R_1 \rightarrow R_2$ een ringhomomorfisme, dan is het **beeld** van f :

$$f(R_1) := \{y \in R_2 : \exists x \in R_1 \text{ met } y = f(x)\}.$$

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

$$\ker(f) := \{x \in R_1 : f(x) = 0\}.$$

2.1.4 Ringhomomorfismen hebben eigenschappen die in verscheidene opzichten analoog zijn aan die van groepshomomorfismen. Bijvoorbeeld: is $f : R_1 \rightarrow R_2$ 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.

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

$$\ker(f) = \{0\} \iff f \text{ is injectief.}$$

De kern van een (unitair) ringhomomorfisme f is een niet-unitaire deelring, immers $f(1)$ hoeft niet 0 te zijn.

In de groepentheorie bleek dat niet *alle* ondergroepen als kern kunnen optreden, maar alleen de *normaaldeleers*. Evenzo zullen we nu zien dat niet alle niet-unitaire deelringen als kern van een ringhomomorfisme optreden, maar alleen de *idealen*, die we nu definiëren.

Definitie 2.1.5 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.:

$$(H0) \quad 0 \in I;$$

$$(H1) \quad a - b \in I \text{ voor alle } a, b \in I;$$

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

Opmerking 2.1.6 In plaats van ‘ideaal’ zegt men ook wel ‘tweezijdig ideaal’. Vervangt men (I2) door de zwakkere eis

$$(I2') \quad \forall r \in R : \forall a \in I : ra \in I$$

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 men opgave 22. We zullen voornamelijk in commutatieve ringen geïnteresseerd zijn, en daar vallen de drie begrippen natuurlijk samen.

Voorbeeld 2.1.7 Triviale voorbeelden van idealen zijn $\{0\}$ en R zelf. Voor iedere $n \in \mathbb{Z}$ is de deelverzameling:

$$n\mathbb{Z} := \{nk \in \mathbb{Z} : k \in \mathbb{Z}\} \quad (\subseteq \mathbb{Z})$$

een ideaal van \mathbb{Z} (ga na).

Opmerking 2.1.8 Ieder ideaal is een deelring, in het algemeen niet-unitair, maar de omkering geldt bij lange na niet: \mathbb{Z} is wel een deelring van \mathbb{Q} , maar geen ideaal, want

$$r = \frac{1}{2} \in \mathbb{Q}, \quad a = 1 \in \mathbb{Z}, \quad \text{maar} \quad ra = \frac{1}{2} \notin \mathbb{Z}$$

waaruit blijkt dat niet aan (I2) voldaan is. 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 2.3.5 voor een generalisatie hiervan.

Stelling 2.1.9 *Zij $f : R_1 \rightarrow R_2$ een ringhomomorfisme.*

Dan is $\ker(f)$ een ideaal van R_1 .

Bewijs. We controleren (I1) en (I2) voor $I = \ker(f)$.

(I1) Dit volgt uit het feit dat f ook een groepshomomorfisme is

$$R_1^+ \longrightarrow R_2^+.$$

(I2) Voor $r \in R_1$, $a \in \ker(f)$ geldt $f(a) = 0$, dus

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

waaruit blijkt dat $ra, ar \in \ker(f)$, zoals verlangd. Dit bewijst 2.1.9. \square

2.1.10 Verderop (zie 2.2.6) zullen we zien dat ook de omkering van 2.1.9 geldt: elk ideaal I , $I \neq R$, is de kern van een geschikt gekozen ringhomomorfisme.

Voorbeeld 2.1.11 Voor $n > 1$ is de kern van het kanonieke ringhomomorfisme

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto \bar{a}$$

gelijk aan het ideaal $n\mathbb{Z}$ uit voorbeeld 2.1.7.

Voorbeeld 2.1.12 Men rekt eenvoudig na dat:

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

een (surjectief, unitair) ringhomomorfisme is. We beweren:

$$\ker(f) = \{2r + (1+i)s \in \mathbb{Z}[i] : r, s \in \mathbb{Z}[i]\} = \{(1+i)t \in \mathbb{Z}[i] : t \in \mathbb{Z}[i]\}.$$

(Als we hierboven overal $i = \sqrt{-1}$ vervangen door $\sqrt{-5}$, dan dan blijft het eerste '=' teken waar, maar het tweede niet, zie opgave 16.) Om te beginnen bewijzen we het eerste '=' teken:

' \supset ' omdat f een ringhomomorfisme is, geldt voor alle $r, s \in \mathbb{Z}[i]$:

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

' \subset ' Als $a + bi \in \ker(f)$ met $a, b \in \mathbb{Z}$, dan geldt $a + b \equiv 0 \pmod{2}$ 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 2.1.9 zijn beide verzamelingen idealen. Ga dit ook zelf na met de definitie van ideaal.

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

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

idealen in $\mathbb{Z}[i]$, ze bleken zelfs gelijk te zijn. Algemener:

Zij R een commutatieve (unitaire) ring en laat $a_1, a_2, \dots, a_n \in R$. Het door a_1, a_2, \dots, a_n **voortgebrachte** ideaal is gedefinieerd als:

$$Ra_1 + Ra_2 + \dots + Ra_n = \{r_1a_1 + r_2a_2 + \dots + r_na_n : r_1, r_2, \dots, r_n \in R\}.$$

Ga na, met definitie 2.1.5, 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:

$$(a_1, a_2, \dots, a_n) := Ra_1 + Ra_2 + \dots + Ra_n.$$

In geval $n = 1$, d.w.z. het ideaal is voortgebracht door één element a_1 , noemen we het door a_1 voortgebrachte ideaal een **hoofdideaal**:

$$(a_1) = a_1R = Ra_1 = \{ra_1 : r \in R\}.$$

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

In paragraaf 2.3 zullen we nader ingaan op voortbrengers van idealen.

2.1.14 Voor een willekeurige ring R kan men een polynoomring $R[X]$ definiëren, zie 3.1 verderop, die geheel analoog is aan polynoomringen zoals $\mathbb{Z}[X]$ en $\mathbb{R}[X]$. De volgende stelling formuleren we daarom alvast voor het algemenere geval.

Stelling 2.1.15 *Laat R een commutatieve ring met 1 zijn en $\alpha \in R$.*

Dan is

$$\Phi_\alpha : R[X] \longrightarrow R, \quad \Phi_\alpha \left(\sum_{i=0}^n a_i X^i \right) = \sum_{i=0}^n a_i \cdot \alpha^i$$

een (surjectief, unitair) ringhomomorfisme (merk op dat $\Phi_\alpha(f) = f(\alpha)$).

Bovendien geldt:

$$\ker(\Phi_\alpha) = (X - \alpha) = \{(X - \alpha)g : g \in R[X]\}.$$

Bewijs. Dat Φ_α een ringhomomorfisme is, is eenvoudig na te rekenen voor de u bekende $R[X]$, het algemene bewijs gaat net zo (zie ook 3.2.1). We bewijzen nu het tweede deel.

‘ \supset ’: Er geldt $\Phi_\alpha(X - \alpha) = \alpha - \alpha = 0$, dus $X - \alpha \in \ker(\Phi_\alpha)$, en omdat $\ker(\Phi_\alpha)$ een ideaal is geldt dan ook $R[X](X - \alpha) \subset \ker(\Phi_\alpha)$.

‘ \subset ’: Stel dat $\sum_{i=0}^n a_i X^i \in \ker(\Phi_\alpha)$, dan geldt $\sum_{i=0}^n a_i \alpha^i = 0$, dus

$$\begin{aligned} \sum_{i=0}^n a_i X^i &= \sum_{i=0}^n a_i X^i - \sum_{i=0}^n a_i \alpha^i \\ &= \sum_{i=0}^n a_i (X^i - \alpha^i) \\ &= \sum_{i=0}^n a_i (X^{i-1} + \alpha X^{i-2} + \dots + \alpha^{i-3} X^2 + \alpha^{i-2} X + \alpha^{i-1}) (X - \alpha) \\ &\in R[X](X - \alpha). \end{aligned}$$

Hiermee is stelling 2.1.15 bewezen. \square

Voorbeeld 2.1.16 Een eenvoudig voorbeeld is het ringhomomorfisme

$$\Phi_0 : \mathbb{R}[X] \longrightarrow \mathbb{R}, \quad f \mapsto f(0).$$

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

$$\ker(\Phi_0) = \{f \in \mathbb{R}[X] : f = \sum a_i X^i \text{ en } a_0 = 0\}.$$

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 $\ker(\Phi_0) = X\mathbb{R}[X]$.

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:

$$\Phi_f : \mathbb{R}[X, Y] = (\mathbb{R}[X])[Y] \longrightarrow \mathbb{R}[X], \quad F(X, Y) \mapsto F(X, f(X)).$$

De kern van dit ringhomomorfisme is volgens de stelling het ideaal

$$\ker(\Phi_f) = \{ (Y - f(X))G(X, Y) : G(X, Y) \in \mathbb{R}[X, Y] \}.$$

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

2.2 De factorring R/I .

2.2.1 Laat R een ring zijn en $I \subset R$ een ideaal. Dan is I een **normale ondergroep** van de additieve groep van R (wegens (I1) en het feit dat R^+ abels is). De verzameling van nevenklassen van I in R :

$$R/I := \{ \bar{a} := a + I \subset R : a \in R \}$$

is dus een (optel)groep. Twee elementen $\bar{a}, \bar{b} \in R/I$, d.w.z. twee deelverzamelingen van R als boven, zijn gelijk precies dan als $a - b \in I$:

$$\bar{a} = \bar{b} \iff a + I = b + I \iff a - b \in I,$$

immers \Rightarrow : $a + I = b + I$ en $0 \in I$ geeft dat $a + 0 = b + i$ voor zekere $i \in I$, dus $a - b = i \in I$;

\Leftarrow : Als $a = b + i$ met $i \in I$ dan geldt, omdat I een ondergroep van R^+ is, dat $i + I = I$ en dus dat $a + I = b + i + I = b + I$.

De groepsbewerking wordt gegeven door:

$$(a + I) + (b + I) := (a + b) + I, \quad \text{d.w.z.} \quad \bar{a} + \bar{b} = \overline{a + b}.$$

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

$$(a + I) \cdot (b + I) := ab + I, \quad \text{d.w.z.} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Om na te gaan dat dit goed gedefinieerd is, moeten we bewijzen: als

$$\bar{a} = \bar{a}_1, \quad \bar{b} = \bar{b}_1 \quad \text{dan geldt} \quad \overline{ab} = \overline{a_1 b_1}.$$

Welnu, uit $\bar{a} = \bar{a}_1$ volgt $a_1 = a + i$ met $i \in I$ en analoog is $b_1 = b + j$ voor een $j \in I$. Dan is:

$$a_1 b_1 = (a + i)(b + j) = ab + ib + aj + ij = ab + k \quad \text{met} \quad k \in I,$$

immers I is een ideaal zodat $ai, bj, ij \in I$ wegens (I2) en omdat I een optelgroep is, zit ook hun som k in I . Omdat $a_1 b_1 = ab + k$, $k \in I$, equivalent is met $\overline{a_1 b_1} = \overline{ab}$, is aangetoond dat de vermenigvuldiging op R/I goed gedefinieerd is.

Ga na dat de regel $\bar{a}\bar{b} = \overline{ab}$ niet goed gedefinieerd is in de groep \mathbb{Q}/\mathbb{Z} (probeer $a = \frac{1}{2}$, $b = 3$, $a_1 = \frac{1}{2}$, $b_1 = 2$). De ondergroep \mathbb{Z} van \mathbb{Q} is dan ook geen ideaal in \mathbb{Q} , zie 2.1.8.

2.2.2 We beweren dat R/I nu een **ring** is.

Bij wijze van voorbeeld controleren we één der distributieve wetten (R4):

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

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

Is R commutatief, dan is R/I het natuurlijk ook. Heeft R een 1, dan is $\bar{1}$ een eenheidselement van R/I .

Voorbeeld 2.2.3 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.

2.2.4 De afbeelding

$$\phi : R \longrightarrow R/I, \quad \phi(a) := \bar{a} = a + I,$$

heet de **natuurlijke** of **canonieke** afbeelding.

Stelling 2.2.5 *Laat R een ring zijn en I een ideaal van R .*

Dan is de natuurlijke afbeelding $\phi : R \rightarrow R/I$ een surjectief ringhomomorfisme met

$$\ker(\phi) = I.$$

Bewijs. Surjectiviteit van ϕ is duidelijk. Uit

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

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

blijkt dat ϕ een ringhomomorfisme is. Tenslotte geldt

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

dus $I = \ker(\phi)$. Dit bewijst stelling 2.2.5. □

Gevolg 2.2.6 *Zij R een ring en $I \subset R$ een deelverzameling. Dan geldt:*

I is een ideaal van R d.e.s.d.a.

er is een ringhomomorfisme $f : R \rightarrow R_1$ waarvoor geldt $\ker(f) = I$.

Bewijs. \Leftarrow : dit is 2.1.9. \Rightarrow : neem $R_1 = R/I$, $f = \phi$ als in 2.2.5. Dit bewijst 2.2.6. □

2.2.7 Bovenstaande twee resultaten zijn analoog aan resultaten uit de groentheorie. We zullen nu de resultaten die overeenkomen met de homomorfieën isomorfiestellingen formuleren. Wegens de verregerende analogie zal het niet nodig zijn lang stil te staan bij de bewijzen.

Stelling 2.2.8 *(De homomorfiestelling voor ringen). Laat $f : R_1 \rightarrow R_2$ een ringhomomorfisme zijn, en $I \subset R_1$ een ideaal waarvoor geldt $I \subset \ker(f)$. Zij $\phi : R_1 \rightarrow R_1/I$ het canonieke ringhomomorfisme.*

Dan is er precies één ringhomomorfisme $g : R_1/I \rightarrow R_2$ waarvoor geldt $f = g \circ \phi$. Bovendien geldt :

$$\ker(g) = \phi(\ker(f)). \quad \begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ \phi \downarrow & \nearrow g & \\ R_1/I & & \end{array}$$

Bewijs. Als g bestaat, dan moet gelden: $f(a) = g(\phi(a)) = g(a + I)$, voor elke $a \in R_1$. We zouden dus willen definiëren: $g(a + I) := f(a)$. Het (mogelijke) probleem van dit voorschrift is dat zou kunnen gelden: $a + I = b + I$ terwijl $f(a) \neq f(b)$. We kunnen dan niet het beeld van de nevenklasse definiëren, want de keuze van de representant van de nevenklasse speelt een rol. In dat geval definieert $g(a + I) := f(a)$ geen afbeelding $g : R_1/I \rightarrow R_2$.

Uit de aanname $I \subset \ker(f)$ volgt evenwel, dat het hier geschetste probleem niet optreedt:

$$a + I = b + I \quad \Rightarrow \quad a - b \in I \subset \ker(f) \quad \Rightarrow \quad f(a - b) = 0 \quad \Rightarrow \quad f(a) = f(b).$$

Aan een nevenklasse $a + I$ van I kunnen we dus wel een eenduidig bepaald element $f(a)$ in R_2 toevoegen en we hebben een goed gedefinieerde afbeelding

$$g : R_1/I \longrightarrow R_2, \quad a + I \mapsto f(a).$$

Reken zelf na dat g een ringhomomorfisme is met kern $\phi(\ker(f))$. □

Stelling 2.2.9 (De eerste isomorfstelling voor ringen). Laat $f : R_1 \rightarrow R_2$ een ringhomomorfisme zijn.

Dan is er een isomorfisme van ringen:

$$R_1/\ker(f) \xrightarrow{\cong} f(R_1), \quad \bar{a} = a + \ker(f) \mapsto f(a) \quad (a \in R_1).$$

Is in het bijzonder f surjectief, dan geldt

$$R_1/\ker(f) \cong R_2.$$

Bewijs. We passen de vorige stelling toe met $I = \ker(f)$. Dan geeft $g : R_1/\ker(f) \rightarrow R_2$ een ringhomomorfisme met $\ker(g) = \phi(\ker(f)) = \bar{0}$, d.w.z. g is injectief. Maar dan is $g : R_1/\ker(f) \rightarrow f(R_1) \subset R_2$ een bijjectief ringhomomorfisme, en is dus een isomorfisme van ringen. Dit bewijst 2.2.9. □

Voorbeeld 2.2.10 De voorbeelden uit de vorige paragraaf, gecombineerd met de eerste isomorfstelling, laten zien dat:

$$\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2, \quad R[X]/(X-\alpha) \cong R, \quad \mathbb{R}[X, Y]/(Y-f(X)) \cong \mathbb{R}[X].$$

Voorbeeld 2.2.11 We gebruiken de eerste isomorfstelling om te bewijzen:

$$\mathbb{Z}[X]/N\mathbb{Z}[X] \cong (\mathbb{Z}/N\mathbb{Z})[X], \quad (N \in \mathbb{Z}),$$

hierin is $(\mathbb{Z}/N\mathbb{Z})[X]$ de ring van polynomen met coëfficiënten in $\mathbb{Z}/N\mathbb{Z}$.

We definiëren een afbeelding:

$$\psi : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/N\mathbb{Z})[X], \quad \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \overline{a_i} X^i,$$

met $\overline{a_i} \in \mathbb{Z}/N\mathbb{Z}$. Ga zelf na dat ψ een surjectief ringhomomorfisme is.

$$\text{Stel } \sum_{i=0}^n \overline{a_i} X^i = 0 \quad \text{dan : } \overline{a_i} = \overline{0} \quad \forall i$$

wegens de definitie ($\sum a_i X^i = \sum b_i X^i$ precies dan als $a_i = b_i$). Als $\overline{a_i} = \overline{0}$ dan is $a_i = Nb_i$ voor zekere $b_i \in \mathbb{Z}$. Door N buiten haakje te halen zien we

$$\psi\left(\sum_{i=0}^n a_i X^i\right) = 0 \iff \sum_{i=0}^n a_i X^i = N\left(\sum_{i=0}^n b_i X^i\right),$$

oftewel

$$\ker(\psi) = N\mathbb{Z}[X] \subset \mathbb{Z}[X].$$

Uit de eerste isomorfiestelling volgt nu het gezochte isomorfisme.

2.2.12 Voor het ringentheoretische equivalent van de tweede isomorfiestelling verwijzen we naar opgave 27. Met de derde isomorfiestelling correspondeert de volgende stelling.

Stelling 2.2.13 *Zij R een ring, I een ideaal van R en $\phi : R \rightarrow R/I$ de natuurlijke afbeelding. Er is een bijectie tussen de idealen J' van R/I en de idealen J van R met $I \subset J$. Deze bijectie voegt aan het ideaal J' van R/I het ideaal J van R toe met:*

$$J := \{x \in R : \phi(x) \in J'\} \quad (\text{merk op } \phi(J) = J').$$

Voor elk ideaal J van R met $I \subset J$ geldt bovendien:

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

Bewijs. Dit is geheel analoog aan het bewijs van de analoge stelling in de groepentheorie, zie opgave 24 op blz. 48. Dit bewijst stelling 2.2.13. \square

Voorbeeld 2.2.14 Zij $(a, b) \in \mathbb{R}$ en laat

$$I := (Y - b) = (Y - b)\mathbb{R}[X, Y]$$

en

$$J := (X - a, Y - b) = (X - a)\mathbb{R}[X, Y] + (Y - b)\mathbb{R}[X, Y].$$

Dan zijn I en J idealen van $\mathbb{R}[X, Y]$ en er geldt $I \subset J$. We laten zien dat

$$\mathbb{R}[X, Y]/J \cong \mathbb{R}.$$

De ring $\mathbb{R}[X, Y]/I$ heeft een eenvoudige beschrijving, zie 2.2.10:

$$\Phi_b : \mathbb{R}[X, Y]/I \xrightarrow{\cong} \mathbb{R}[X], \quad F + I \mapsto F(X, b).$$

Gebruik makende van het ringisomorfisme Φ_b , zien we dat:

$$(\mathbb{R}[X, Y]/I) / \phi(J) \cong \mathbb{R}[X] / \Phi_b(\phi(J)), \quad \text{met } \phi : \mathbb{R}[X, Y] \rightarrow \mathbb{R}[X, Y]/I$$

de natuurlijke afbeelding.

Om stelling 2.2.13 toe te kunnen passen, bepalen we het ideaal $\Phi_b(\phi(J))$ van $\mathbb{R}[X]$. Definieer $\Psi_b := \Phi_b \circ \phi : \mathbb{R}[X, Y] \rightarrow \mathbb{R}[X]$, omdat $\Phi_b(\phi(F)) = \Phi_b(F + I) = F(X, b)$, geldt:

$$\Phi_b \circ \phi = \Psi_b : \mathbb{R}[X, Y] \longrightarrow \mathbb{R}[X], \quad F(X, Y) \mapsto F(X, b).$$

Het ideaal $\Psi_b(J) = \Phi_b(\phi(J))$ van $\mathbb{R}[X]$ is dan:

$$\begin{aligned} \Phi_b(\phi(J)) = \Psi_b(J) &= \Psi_b(Y - b)\Psi_b(\mathbb{R}[X, Y]) + \Psi_b(X - a)\Psi_b(\mathbb{R}[X, Y]) \\ &= 0 + (X - a)\mathbb{R}[X] \\ &= (X - a)\mathbb{R}[X]. \end{aligned}$$

We concluderen dat:

$$\mathbb{R}[X, Y]/J \cong \mathbb{R}[X]/(X - a) \cong \mathbb{R}, \quad F + J \mapsto F(X, b) + (X - a) \mapsto F(a, b),$$

waarbij we stelling 2.1.15 nogmaals gebruikten.

Omdat de kanonieke afbeelding $\psi : \mathbb{R}[X, Y] \rightarrow \mathbb{R}[X, Y]/J$ een surjectief homomorfisme is met $\ker(\psi) = J$ geldt blijkbaar dat

$$\psi : \mathbb{R}[X, Y] \longrightarrow \mathbb{R}, \quad F \mapsto F(a, b),$$

een (surjectief) ringhomomorfisme is met kern J . Ga dat zelf nog eens rechtstreeks na als $a = b = 0$.

2.3 Rekenen met idealen

2.3.1 In 2.1.13 definieerden we

$$(a_1, \dots, a_n) = \{r_1 a_1 + \dots + r_n a_n : r_i \in R\},$$

het ideaal voortgebracht door a_1, \dots, a_n in een commutatieve ring R . Verder is een **hoofdideaal** een ideaal dat door een enkel element kan worden voortgebracht.

We zeggen dat R een **hoofdideaalring** is als ieder ideaal in R een hoofdideaal is.

Stelling 2.3.2 *De ring \mathbb{Z} is een hoofdideaalring.*

Bewijs. Zij I een ideaal in \mathbb{Z} . Als $I = \{0\}$ dan is I zeker een hoofdideaal. Als $I \neq \{0\}$, dan is er een $n \in I$, $n \neq 0$. Zij nu

$$N := \min\{n \in I : n > 0\}.$$

We beweren dat $I = (N) = N\mathbb{Z}$, een hoofdideaal.

Omdat $N \in I$ geldt $N\mathbb{Z} \subset I$, wegens (I2). Omgekeerd, zij $n \in I$. Deling met rest in \mathbb{Z} geeft een $q \in \mathbb{Z}$ en een $r \in \mathbb{Z}_{>0}$ met:

$$n = qN + r \quad 0 \leq r < N.$$

Omdat I een optelgroep is en $n, qN \in I$ geldt $r = n - qN \in I$. Omdat N het kleinste, positieve element in I is, en $0 \leq r < N$ moet gelden $r = 0$. Maar dan is:

$$n = qN \in N\mathbb{Z} = (N),$$

dus ook $I \subset N\mathbb{Z}$ zodat $I = N\mathbb{Z}$, een hoofdideaal. Hiermee is stelling 2.3.2 bewezen. \square

Voorbeeld 2.3.3 We laten zien dat het ideaal

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

géén hoofdideaal is.

Bewijs van deze bewering. Stel dat (X, Y) wel een hoofdideaal was. Dan was er een $f \in \mathbb{R}[X, Y]$,

$$f = a_{00} + a_{10}X + a_{01}Y + \dots, \quad \text{met } f\mathbb{R}[X, Y] = (X, Y).$$

Uit $f\mathbb{R}[X, Y] \subset X\mathbb{R}[X, Y] + Y\mathbb{R}[X, Y]$ volgt $f = f \cdot 1 = Xh + Yk$ voor zekere $h, k \in \mathbb{R}[X, Y]$. Dit impliceert dat $a_{00} = 0$. Merk op dat

$$(f) \supset (X, Y) \implies \begin{cases} X &= fh \\ Y &= fk \end{cases}$$

voor zekere $h, k \in \mathbb{R}[X, Y]$. Uit $X = fh$ volgt dat $a_{10} \neq 0$ en $h(0, 0) = a_{10}^{-1} \neq 0$ en uit $Y = fk$ volgt $a_{01} \neq 0$ (hierbij gebruiken we $a_{00} = 0$). Dit geeft al een tegenspraak, want nu is:

$$fh = (a_{10}X + a_{01}Y + \dots)(a_{10}^{-1} + \dots) = X + a_{01}a_{10}^{-1}Y + \dots \neq X,$$

omdat $a_{01}a_{10}^{-1} \neq 0$.

De aanname dat (X, Y) een hoofdideaal is leidt dus tot een tegenspraak, en we concluderen dat (X, Y) géén hoofdideaal is.

2.3.4 We zullen verderop nog zien dat $\mathbb{R}[X]$ en $\mathbb{Z}[i]$ hoofdideaalringen zijn (het bewijs daarvan is analoog aan dat van stelling 2.3.2), maar dat $\mathbb{Z}[X]$ en $\mathbb{Z}[\sqrt{-5}]$ geen hoofdideaalringen zijn.

We laten nu zien dat elke delingsring een hoofdideaalring is, zie gevolg 2.3.6.

Stelling 2.3.5 *Zij R een ring met 1, 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 $\exists b \in R : ab = 1$. Uit (I2) (met $r = b$) volgt nu $1 \in I$. Weer met (I2) (met $a = 1$) volgt dat elke $r \in R$ tot I behoort, dus $R = I$. Dit bewijst stelling 2.3.5.

Gevolg 2.3.6 *De enige idealen van een delingsring R zijn $\{0\}$ en $R = R \cdot 1$.*

Bewijs. Zij $I \subset R$ een ideaal. Bevat I een element $a \neq 0$, dan $a \in R^*$ dus $I = R$ wegens 2.3.5. Bevat I geen element $\neq 0$, dan $I = \{0\}$. Dit bewijst gevolg 2.3.6. \square

Gevolg 2.3.7 *Elk (unitair) ringhomomorfisme $f : K \rightarrow R$ van een lichaam K naar een ring $R \neq \{0\}$ is injectief. In het bijzonder is elk lichaamshomomorfisme injectief.*

Bewijs. De kern $\ker(f)$ van f is een ideaal van K , dus $\ker(f) = \{0\}$ of K (wegens 2.3.6). Maar $f(1) = 1 \neq 0$, dus $1 \notin \ker(f)$ en $\ker(f) \neq K$. Daarom geldt: $\ker(f) = \{0\}$, d.w.z. f is injectief. De laatste bewering volgt direct uit de eerste. \square

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

$$I + J = \{x + y : x \in I, y \in J\}.$$

Aan de hand van definitie 2.1.5 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 $R = \mathbb{Z}$. Omdat R een 1 heeft, geldt

$$\begin{aligned} I + J = R &\iff 1 \in I + J && \text{(wegens 2.3.5)} \\ &\iff \exists x \in I, y \in J : x + y = 1. \end{aligned}$$

De **doorsnede** $I \cap J$ van twee idealen I en J is ook een ideaal van R , zoals men aan de hand van 2.1.5 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

$$I \cdot J = \left\{ \sum_{i=1}^n x_i y_i : n \in \mathbb{Z}_{\geq 0}, x_i \in I, y_i \in J \right\}.$$

Hiervan is ook weer makkelijk na te gaan dat het een ideaal van R is; uit opgave 30 blijkt dat $\{xy : x \in I, y \in J\}$ 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 $I \cdot J \subset I \cap J$.

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

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 2.3.9 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 2.3.2).

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: volgens stelling 2.3.2 geldt: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}N$, d.w.z. $(a, b) = (N)$, voor zekere $N \in \mathbb{Z}_{>0}$ zodat we alleen nog moeten bewijzen: $d = N$. Omdat a en b deelbaar zijn door d , en er $k, l \in \mathbb{Z}$ zijn met $ak + bl = N$ geldt $d|N$. Anderzijds, $(a, b) = (N)$ impliceert dat $a = a \cdot 1 + b \cdot 0 = r_1N$ en ook $b = r_2N$ voor zekere $r_1, r_2 \in \mathbb{Z}$. Dan geldt blijkbaar $N|a$ en $N|b$, dus N is een gemeenschappelijke deler van a, b . Omdat d de *grootste* gemeenschappelijke deler is, geldt $N|d$. Uit $d, N \in \mathbb{Z}_{>0}$, $d|N$, $N|d$ volgt $d = N$ waarmee het bewijs geleverd is.

In het bijzonder zien we dat

$$\text{ggd}(a, b) = d \implies ka + lb = d \quad \text{voor zekere } k, l \in \mathbb{Z}.$$

De idealen $\mathbb{Z}a$ en $\mathbb{Z}b$ zijn dus onderling ondeelbaar 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:

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

Bewijs: $x \in \mathbb{Z}a \cap \mathbb{Z}b \Leftrightarrow x$ is een veelvoud van zowel a als $b \Leftrightarrow x$ is een veelvoud van $c \Leftrightarrow x \in \mathbb{Z}c$; einde bewijs.

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 2.3.10 Als R een commutatieve ring is, dan geldt:

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

zoals je eenvoudig nagaat met de definities. Verder geldt:

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

voor alle $a, b, r \in R$ (ga na), je mag dus ‘vegen’ met de voortbrengers. In de ring $\mathbb{Z}[\sqrt{-5}]$ geldt bijvoorbeeld:

$$\begin{aligned} & (2, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}) = \\ & = (6, 2 - 2\sqrt{-5}, 3 + 3\sqrt{-5}, 6) \\ & = (6, 2 - 2\sqrt{-5}, 1 + 5\sqrt{-5}) \\ & = (6, 6\sqrt{-5}, 2 - 2\sqrt{-5}, 1 + 5\sqrt{-5}) \\ & = (6, 2 - 2\sqrt{-5}, 1 - \sqrt{-5}) \\ & = ((1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}), 2(1 - \sqrt{-5}), 1 - \sqrt{-5}) \\ & = (1 - \sqrt{-5}). \end{aligned}$$

De idealen $(2, 1 + \sqrt{-5})$ en $(3, 1 - \sqrt{-5})$ zijn geen van beide hoofdidealen (zie opgave 16), we zien dat desalniettemin hun product wél een hoofdideaal is. Het vermenigvuldigen van idealen speelt een belangrijke rol in de getaltheorie.

Stelling 2.3.11 (*Chinese reststelling voor ringen*). *Laat R een commutatieve ring met 1 zijn, en laat I, J onderling ondeelbare idealen van R zijn:*

$$I + J = R.$$

Dan is er een ringisomorfisme

$$R/(I \cdot J) \cong (R/I) \times (R/J), \quad a + (I \cdot J) \mapsto (a + I, a + J)$$

en bovendien geldt: $I \cap J = I \cdot J$.

Bewijs. We bewijzen eerst $I + J = R$ impliceert dat $I \cap J = I \cdot J$.

De inclusie $I \cap J \supset I \cdot J$ is algemeen geldig. Omgekeerd, omdat $I + J = R$ zijn er $x \in I$, $y \in J$ met $x + y = 1$. Voor iedere $z \in I \cap J$ geldt dan:

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

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

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

$$\phi : R \rightarrow (R/I) \times (R/J) \quad \phi(a) := (\phi_1(a), \phi_2(a)).$$

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 2.2.9.

i. ϕ is een ringhomomorfisme:

$$\phi(ab) = (\phi_1(ab), \phi_2(ab)) = (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b))$$

(want ϕ_1, ϕ_2 zijn ringhomomorfismen). Verder geldt:

$$\begin{aligned}\phi(ab) &= (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)) \\ &= (\phi_1(a), \phi_2(a)) \cdot (\phi_1(b), \phi_2(b)) \\ &= \phi(a)\phi(b)\end{aligned}$$

(zo is de vermenigvuldiging op een product van twee ringen immers gedefinieerd). Evenzo $\phi(a + b) = \phi(a) + \phi(b)$. Dus ϕ is een ringhomomorfisme.

ii. $\ker(\phi) = I \cdot J$. Er geldt $a \in \ker(\phi) \Leftrightarrow (\phi_1(a), \phi_2(a)) = (0, 0) \Leftrightarrow a \in \ker(\phi_1) \wedge a \in \ker(\phi_2) \Leftrightarrow a \in I \cap J \Leftrightarrow a \in I \cdot J$ (want we weten al dat $I \cdot J = I \cap J$).

iii. ϕ is surjectief. Laat $x + y = 1$ als boven, met $x \in I, y \in J$. Dan

$$\phi_1(x) = 0, \quad \phi_2(y) = 0$$

en uit $x = 1 - y$ volgt

$$\begin{aligned}\phi_2(x) &= \phi_2(1) - \phi_2(y) = 1 - 0 = 1 \in R/J, \\ \phi_1(y) &= \phi_1(1 - x) = 1 \in R/I.\end{aligned}$$

Al met al hebben we

$$\phi(x) = (0, 1), \quad \phi(y) = (1, 0).$$

Laat nu $(\phi_1(a), \phi_2(b))$ 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

$$\begin{aligned}\phi_1(c) &= \phi_1(b)\phi_1(x) + \phi_1(a)\phi_1(y) \\ &= \phi_1(b) \cdot 0 + \phi_1(a) \cdot 1 \\ &= \phi_1(a)\end{aligned}$$

en evenzo

$$\phi_2(c) = \phi_2(b) \quad \text{dus :} \quad \phi(c) = (\phi_1(a), \phi_2(b))$$

waarmee de surjectiviteit van ϕ bewezen is.

Dit bewijst de chinese reststelling. \square

Gevolg 2.3.12 *Laten $n, m \in \mathbb{Z}$ onderling ondeelbaar zijn.*

Dan is er een ringisomorfisme

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \quad a + nm\mathbb{Z} \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z}).$$

Bewijs. Dit volgt uit 2.3.11 want $\mathbb{Z}n + \mathbb{Z}m = \mathbb{Z}ggd(n, m) = \mathbb{Z}$. Dit bewijst gevolg 2.3.12.

2.3.13 Merk op dat de eis van de ondeelbaarheid van n, m niet gemist kan worden. Bijvoorbeeld $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, immers de optelgroepen zijn niet isomorf.

Voorbeeld 2.3.14 Laat $R = \mathbb{Q}[X]$ en laat

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

Er geldt

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

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 2.3.11 volgt dan:

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

Blijkens 2.1.15 geldt $\mathbb{Q}[X]/I \cong \mathbb{Q}$, $f \mapsto f(1)$ en $\mathbb{Q}[X]/J \cong \mathbb{Q}$, $f \mapsto f(-1)$, dus

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

Voorbeeld 2.3.15 Als $R = R_1 \times R_2$, waarbij R_1, R_2 ringen met 1 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 (met 1) zijn, en $e \in R$ een idempotent. We passen 2.3.11 toe op

$$I = R \cdot e, \quad J = R \cdot (1 - e).$$

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 2.3.11 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 met 1, 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 $R = \mathbb{Z}/6\mathbb{Z}$, $e = \bar{4}$, vindt men de isomorfie $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ (zie ook 2.3.12).

2.4 Opgaven

1. Zij R een ring. Bewijs dat er precies één unitair ringhomomorfisme $f : \mathbb{Z} \rightarrow R$ bestaat.

N.B. De niet-negatieve voortbrenger van $\ker(f)$ noemt men wel de **karakteristiek** van R , notatie: $\text{kar}(R)$.

2. Bewijs dat de karakteristiek van een domein 0 of een priemgetal is.
3. Bewijs dat de volgende ringen geen ringautomorfisme behalve de identiteit hebben:

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

4. Zij σ een ringautomorfisme van \mathbb{R} .

a. Bewijs: $x > 0 \Rightarrow \sigma(x) > 0$.

b. Bewijs: $\sigma = \text{id}_{\mathbb{R}}$.

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

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

7. Is $\det : M(n, \mathbb{R}) \rightarrow \mathbb{R}$ een ringhomomorfisme?

8. Laat $f : R_1 \rightarrow R_2$ een (unitair) ringhomomorfisme zijn. Bewijs dat $g = f|_{R_1^*}$ een groephomomorfisme $R_1^* \rightarrow R_2^*$ is, en laat aan de hand van een voorbeeld zien dat g niet surjectief hoeft te zijn als f het is.

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

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

11. Zij A een additief geschreven abelse groep, en $B = \{a \in A : a \text{ heeft eindige orde}\}$. Definieer $I \subset \text{End}(A)$ door

$$I = \{\sigma \in \text{End}(A) : \sigma(x) = 0 \text{ voor alle } x \in B\}.$$

Bewijs dat I een ideaal van $\text{End}(A)$ is, en dat $\text{End}(A)/I$ isomorf is met een deelring van $\text{End}(B)$.

12. Zij R een ring. Voor $a \in R$ definiëren we $\lambda_a, \rho_a : R \rightarrow R$ door $\lambda_a(x) = ax, \rho_a(x) = xa$.

- Bewijs: $\lambda_a, \rho_a \in \text{End}(R^+)$ voor alle $a \in R$.
- Bewijs dat de afbeelding $f : R \rightarrow \text{End}(R^+)$, $f(a) = \lambda_a$, een ringhomomorfisme is. Bewijs voorts dat f unitair en injectief is als R een 1 heeft.
- Bewijs dat de afbeelding $g : R^0 \rightarrow \text{End}(R^+)$, $g(a) = \rho_a$, een ringhomomorfisme is, met R^0 de ‘teggengestelde ring’ gedefinieerd in opgave 11.

13. Een **Cauchyrij** over \mathbb{Q} is een rij $(a_n)_{n=1}^\infty$, met $a_n \in \mathbb{Q}$, waarvoor geldt:

$$\forall \epsilon \in \mathbb{Q}_{>0} : \exists n_0 : \forall n, m > n_0 : |a_n - a_m| < \epsilon.$$

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: $\lim_{n \rightarrow \infty} a_n = 0$. 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.

14. Laat R een ring met 1 zijn en G een groep. Definieer $f : R[G] \rightarrow R$ door $f(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g$. Bewijs dat f een ringhomomorfisme is, en dat $\ker(f)$ wordt voortgebracht door $\{g - 1 : g \in G\}$.

15. Zij $R = \mathbb{Z}[X]$ en definieer:

$$\phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}/2\mathbb{Z}, \quad f \mapsto f(0) + 2\mathbb{Z}.$$

- Bewijs dat ϕ een surjectief homomorfisme is en dat

$$\ker(\phi) = (2, X).$$

- Bewijs dat $(2, X)$ geen hoofdideaal is.

16. Zij $R = \mathbb{Z}[\sqrt{-5}]$ en zij

$$\phi : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}/3\mathbb{Z}, \quad a + b\sqrt{-5} \mapsto \overline{a + b} \quad (a, b \in \mathbb{Z}).$$

- Bewijs dat ϕ een surjectief ringhomomorfisme is.
- Bewijs dat $\ker(\phi) = (3, 1 - \sqrt{-5})$

- c. Bewijs dat $\ker(\phi)$ geen hoofdideaal is. (Aanwijzing: stel $\ker(\phi) = (x)$, met $3 = xy$ en $1 - \sqrt{-5} = xz$, bekijk dan $N(xy)$ en $N(xz)$ met N uit 1.13.)
- d. Bewijs ook dat $(2, 1 + \sqrt{-5})$ geen hoofdideaal is.
- e. Is het ideaal $(3, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5})$ een hoofdideaal?
17. Definieer $\varphi : \mathbb{Z}[i] \rightarrow \mathbb{F}_{13}$ door $\varphi(a + bi) = a + 5b \pmod{13}$.
Bewijs dat φ een homomorfisme is, en dat $\ker(\varphi)$ wordt voortgebracht door 13 en $i - 5$. Vind één voortbrenger voor $\ker(\varphi)$.
18. Zij R een ring en $I \subset R$ een linksideaal dat een rechtseenheid bevat.
Bewijs: $I = R$.
19. Laten R_1 en R_2 ringen zijn, en $I = \{0\} \times R_2 \subset R_1 \times R_2$.
- a. Bewijs dat I een ideaal van $R_1 \times R_2$ is.
- b. Stel dat R_1 en R_2 commutatief zijn. Bewijs dat I een hoofdideaal is.
20. 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 ($i = 1, 2$).
21. Zij R een ring met 1, met de eigenschap dat $f : R \rightarrow R$, $f(x) = x^2$, een ringhomomorfisme van R naar zichzelf is. Bewijs: R is commutatief, en $\text{kar}(R) = 1$ of 2 (zie opgave 1); bewijs ook:

$$\forall x \in \ker(f) : 1 + x \in R^*.$$

22. a. Bewijs dat

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R}) : b = d = 0 \right\}$$

een linksideaal maar geen rechtsideaal van $M(2, \mathbb{R})$ is.

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

23. Laat $n \in \mathbb{Z}_{>0}$. In deze opgave vatten we de elementen van $M(n, \mathbb{R})$ 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 $\{A \in M(n, \mathbb{R}) : \forall w \in W : Aw = 0\}$ een linksideaal van $M(n, \mathbb{R})$ is.

- b. Bewijs dat $\{A \in M(n, \mathbb{R}) : \forall v \in \mathbb{R}^n : Av \in W\}$ een rechtsideaal van $M(n, \mathbb{R})$ is.
- c. Bewijs: elk linksideaal van $M(n, \mathbb{R})$ is van de onder a. aangegeven vorm, en elk rechtsideaal van $M(n, \mathbb{R})$ is van de onder b. aangegeven vorm.
- d. Bewijs dat $\{0\}$ en $M(n, \mathbb{R})$ de enige tweezijdige idealen van $M(n, \mathbb{R})$ zijn.

24. Zij $I \subset R$ een ideaal in een ring en zij $\phi : R \rightarrow R/I$ de natuurlijke afbeelding.

- a. Zij $J' \subset R/I$ een ideaal. Bewijs dat

$$\phi^{-1}(J') := \{x \in R : \phi(x) \in J'\}$$

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: $(R/I)/\phi(J) \cong R/J$.

25. 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).

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

27. . 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. $R' + I = \{r + s : r \in R', s \in I\}$ is een deelring van R ;
 c. $R'/(R' \cap I) \cong (R' + I)/I$.

28. Zij R een ring met 1, en definieer

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

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

29. Laat

$$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R}) : c = 0 \right\}$$

en

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M(2, \mathbb{R}) : b \in \mathbb{R} \right\}.$$

Bewijs de volgende uitspraken:

- a. R is een deelring van $M(2, \mathbb{R})$;
 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.
30. 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 $\{xy : x, y \in I\}$ geen ideaal van R is.
31. 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 $R = \mathbb{Z}$.

32. Bewijs dat 2.3.11 ook geldig is voor niet-commutatieve ringen, als men op beide plaatsen $I \cdot J$ door $I \cdot J + J \cdot I$ vervangt.
33. Laat R een ring met 1 zijn, en I_1, I_2, I_3 idealen van R .
 Bewijs: $I_1 + I_3 = R \wedge I_2 + I_3 = R \Rightarrow (I_1 \cdot I_2) + I_3 = R$.
34. (Chinese reststelling voor meer idealen). Zij R een commutatieve ring met 1, en laten I_1, I_2, \dots, 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 $(I_1 \cdot I_2 \cdot \dots \cdot I_{t-1}) + I_t = R$ als in opgave 33, en pas inductie naar t toe.)

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

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

36. Laat $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \pmod{2}\}$.

- Bewijs dat R een deelring van $\mathbb{Z} \times \mathbb{Z}$ is.
- Bewijs: $\mathbb{Z}[X]/\mathbb{Z}[X] \cdot (X^2 - 1) \cong R$.
- 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 $\mathbb{Z} \times \mathbb{Z}$).
- 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?)

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

38. Bewijs:

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

en

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

39. Zij R een commutatieve ring met 1, en $Id(R)$ de verzameling idempotenten van R (inclusief de triviale idempotenten 0, 1). Bewijs:

$$e_1, e_2 \in Id(R) \Rightarrow e_1 + e_2 - 2e_1e_2 \in Id(R), e_1e_2 \in Id(R).$$

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

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

Onder welke omstandigheden is $Id(R)$ een deelring van R ?

3 Polynoomringen

3.1 Polynomen

3.1.1 Laat R een ring zijn. We gaan een ring $R[X]$ definiëren, de polynoomring in een veranderlijke X . Een **polynoom** (of veelterm) met coëfficiënten in R is een uitdrukking

$$\sum_{i=0}^{<\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 \dots, \quad a_i \in R$$

en bijna alle a_i gelijk aan nul (d.w.z. $\exists n : \forall i > n : a_i = 0$). 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 $\forall i \geq 0 : a_i = b_i$. In plaats van het symbool X gebruikt men ook wel andere letters, zoals $Y, Z, U, T, X_0, X_1, \dots$. Als $a_i = 0$ voor $i > n$ dan schrijft men het polynoom $\sum_{i=0}^{\infty} a_i X^i$ ook wel als

$$a_0 + a_1 X + \dots + a_n X^n.$$

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:

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

Men duidt een polynoom $\sum a_i X^i$ vaak aan met een letter als f , of als $f(X)$.

De **graad** $gr(f)$ (of $graad(f)$ 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 $gr(1 - 2X + X^3) = 3$. Voor het **nulpolynoom** $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$ definiëren we $gr(0) = -\infty$ (men komt ook andere definities voor $gr(0)$ tegen).

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 $gr(f) \leq 0$, dwz met $a_n = 0$ voor $n \geq 1$. Als $f \neq 0$ en $n = gr(f)$, dan heet a_n de **kopcoëfficiënt** van f . Een polynoom met kopcoëfficiënt 1 heet **monisch** (of **moniek**).

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

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

Vermenigvuldigen 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:

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

Voorbeeld 3.1.3

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

De verzameling van alle polynomen met coëfficiënten in R wordt aangegeven met $R[X]$.

Stelling 3.1.4 *De verzameling $R[X]$ is met de zojuist gedefinieerde optelling en vermenigvuldiging een ring, de polynoomring in één veranderlijke over R .*

De ring R kan opgevat worden als de deelring van $R[X]$ van de constante polynomen:

$$R \hookrightarrow R[X], \quad r \mapsto r + 0 \cdot X + \dots + 0 \cdot X^i + \dots$$

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

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

en analoog laat men zien dat ook

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

hieraan gelijk is. Dit bewijst (R3). We laten (R1), (R2) en (R4) aan de lezer over.

In de laatste uitspraak is het eenvoudig na te gaan dat de gegeven afbeelding een injectief ringhomomorfisme is. \square

Als R commutatief is, dan is $R[X]$ het ook. Heeft R een 1, dan is deze 1 ook een eenheidselement van $R[X]$. Als R geen nuldelers heeft, dan heeft $R[X]$ evenmin nuldelers (zie opgave 1), en er geldt dan

$$gr(f \cdot g) = gr(f) + gr(g) \quad \text{voor } f, g \in R[X],$$

waarbij we $-\infty + n = n + (-\infty) = -\infty + (-\infty) = -\infty$ nemen.

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

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

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

Elementen van $R[X_1, X_2, \dots, X_n]$ zijn dus uitdrukkingen:

$$f = g_0 + g_1 X_n + g_2 X_n^2 + \dots, \quad g_i \in R[X_1, \dots, X_{n-1}],$$

met slechts eindig veel $g_i \neq 0$. Men schrijft ook wel:

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

met coëfficiënten $a_{i_1 i_2 \dots i_n} \in R$ waarvan er slechts eindig veel ongelijk nul zijn. Men gebruikt ook wel de "multi-index-notatie

$$f = \sum_I a_I X^I$$

waarbij de 'multi-index' $I = (i_1, i_2, \dots, i_n)$ loopt over $(\mathbb{Z}_{\geq 0})^n$ en X^I een afkorting is voor $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$.

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

$$gr_j(f) := \max \{ m \in \mathbb{Z}_{\geq 0} : \exists i_1, \dots, i_n : a_{i_1 \dots i_n} \neq 0 \text{ en } i_j = m \}$$

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

$$totgr(f) = \max \left\{ m \in \mathbb{Z}_{\geq 0} : \exists i_1, \dots, i_n : a_{i_1 \dots i_n} \neq 0 \text{ en } \sum_{j=1}^n i_j = m \right\}$$

Voor het nulpolynoom zullen we deze graden als $-\infty$ definiëren.

Voorbeeld 3.1.7 Voor $f = X_1 X_2^4 - X_1^2 X_2^2$ geldt $gr_1(f) = 2$, $gr_2(f) = 4$, $totgr(f) = 5$.

3.2 Evaluatiehomomorfismen

Zoals bekend kan men in een polynoom $f \in \mathbb{R}[X]$ een reëel of zelfs een complex getal z invullen. Bij vaste z krijgen we zo een afbeelding $\mathbb{R}[X] \rightarrow \mathbb{C}$. Als $f \in \mathbb{Z}[X]$ dan kunnen we een $a \in \mathbb{Z}$ invullen en vervolgens $f(a) \in \mathbb{Z}/(n)$ nemen. Dit is hetzelfde als eerst de coëfficiënten van f modulo n nemen en vervolgens \bar{a} in te vullen (ga na). De volgende stelling geeft een generalisatie van deze operaties.

Stelling 3.2.1 (Het evaluatiehomomorfisme) *Laat R en S twee ringen zijn.*

a. *Een ringhomomorfisme*

$$\phi : R \longrightarrow S$$

induceert een ringhomomorfisme

$$\Phi : R[X] \rightarrow S[X], \quad \Phi : a_0 + \dots + a_n X^n \mapsto \phi(a_0) + \dots + \phi(a_n) X^n.$$

b. *Voor iedere $s \in S$ die voldoet aan $st = ts$ voor alle $t \in S$ is de afbeelding*

$$\Psi_s : S[X] \rightarrow S, \quad \Psi_s : a_0 + a_1 X + \dots + a_n X^n \mapsto a_0 + a_1 s + \dots + a_n s^n$$

een ringhomomorfisme. We schrijven vaak $f(s)$ voor $\Psi_s(f)$.

c. *Voor ieder $s \in S$ die voldoet aan $s\phi(r) = \phi(r)s$ voor alle $r \in R$ is de samenstelling:*

$$\Phi_s : R[X] \xrightarrow{\Phi} S[X] \xrightarrow{\Psi_s} S$$

*een ringhomomorfisme. Het ringhomomorfisme Φ_s heet het **evaluatiehomomorfisme** in s .*

Bewijs. Voor het eerste onderdeel moeten we laten zien dat voor alle polynomen $f = a_0 + a_1 X + \dots$, $g = b_0 + b_1 X + \dots \in R[X]$ geldt:

$$\Phi(f + g) = \Phi(f) + \Phi(g), \quad \text{en} \quad \Phi(fg) = \Phi(f)\Phi(g).$$

Omdat $f + g = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 \dots$ geldt:

$$\begin{aligned} \Phi(f + g) &= \phi(a_0 + b_0) + \phi(a_1 + b_1)X + \phi(a_2 + b_2)X^2 + \dots \\ &= \phi(a_0) + \phi(a_1)X + \phi(a_2)X^2 + \dots + \phi(b_0) + \phi(b_1)X + \dots \\ &= \Phi(f) + \Phi(g) \end{aligned}$$

Voor de tweede eis schrijven we $fg = c_0 + c_1X + c_2X^2 + \dots$, dwz $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$. Dan is $\phi(c_k) = \phi(a_0)\phi(b_k) + \dots + \phi(a_k)\phi(b_0)$, waaruit volgt dat $\Phi(fg) \stackrel{def}{=} \phi(c_0) + \phi(c_1)X + \phi(c_2)X^2 + \dots = \Phi(f)\Phi(g)$. Hiermee is het eerste onderdeel bewezen.

Voor het tweede onderdeel moeten we laten zien dat:

$$\Psi_s(f+g) = \Psi_s(f) + \Psi_s(g), \quad \Psi_s(fg) = \Psi_s(f)\Psi_s(g) \quad \forall f, g \in S[X].$$

Het bewijs van de eerste eis is rechttoe rechtaan. Voor de tweede eis merken we op dat wegens $st = ts$ voor alle $t \in S$ geldt dat

$$(a_i s^i)(b_j s^j) = a_i b_j s^{i+j} \quad \forall a_i, b_j \in S.$$

Schrijven we $f = a_0 + a_1X + \dots$ en $g = b_0 + b_1X + \dots$ dan is:

$$\begin{aligned} \Psi_s(f)\Psi_s(g) &= (a_0 + a_1s + \dots)(b_0 + b_1s + \dots) \\ &= a_0b_0 + (a_0b_1 + b_0a_1)s + \dots + \left(\sum_{i+j=k} a_i b_j\right)s^k + \dots \\ &= \Psi_s(fg). \end{aligned}$$

Het laatste onderdeel volgt uit het eenvoudig te bewijzen feit dat de samenstelling van twee ringhomomorfismes weer een ringhomomorfisme is. Hierbij dient opgemerkt te worden dat $\Psi_s : S[X] \rightarrow S$ niet noodzakelijk een ringhomomorfisme is (immers s commuteert a priori alleen met elementen in $\phi(R)$), maar Ψ_s beperkt tot $\Phi(R[X])$ is wel een homomorfisme. \square

Opmerking 3.2.2 Voor $r := (r_1, \dots, r_n) \in R^n$ kunnen we ook een evaluatiehomomorfisme

$$\Phi_r : R[X_1, \dots, X_n] \longrightarrow R, \quad \Phi_r(f) := f(r_1, \dots, r_n)$$

definiëren mits $r_i s = s r_i$ voor alle $s \in R$.

Voorbeeld 3.2.3 Zij K een (commutatief) lichaam, zij V een lineaire ruimte over K en zij $End_K(V)$ de ring van K -lineaire afbeeldingen van V naar V . Bij een lineaire afbeelding $A \in End_K(V)$ definiëren we een evaluatiehomomorfisme $\Phi_A : K[X] \rightarrow End_K(V)$, d.w.z. we willen $X := A$ substitueren in elk polynoom $f \in K[X]$. Tevens bestuderen we de kern van Φ_A .

Voordat Φ_A gedefinieerd kan worden, moeten we een homomorfisme $\phi : K \rightarrow End_K(V)$ definiëren dat voldoet aan $\phi(\lambda)A = A\phi(\lambda)$ voor alle $\lambda \in K$, $A \in End_K(V)$. Zij

$$\phi : K \longrightarrow End_K(V), \quad \phi : \lambda \mapsto \lambda I$$

met I de identiteit op V (d.w.z. $(\lambda I)v := \lambda \cdot v$ voor alle $v \in V$). Dan is voor elke $A \in \text{End}_K(V)$ en elke $v \in V$:

$$(\phi(\lambda)A)v = \phi(\lambda)(Av) = \lambda(Av) = A(\lambda v) = (A\phi(\lambda))v,$$

dus $\phi(\lambda)A = A\phi(\lambda)$ voor elke $\lambda \in K$ en elke $A \in \text{End}_K(V)$.

We schrijven λA i.p.v. $(\lambda I) \cdot A$. (Als $V = K^n$ dan is $\text{End}_K(V) = M(n, K)$, ring van $n \times n$ matrices met coëfficiënten in K , en λA is de matrix waarin alle coëfficiënten van A met λ vermenigvuldigd zijn.)

Neem $A \in \text{End}_K(V)$ en zij Φ_A het evaluatiehomorfisme in A :

$$\Phi_A : K[X] \longrightarrow \text{End}_K(V), \quad \Phi_A(f) := f(A),$$

waarin we in plaats van $\Phi_A(f) = \phi(a_0) + \phi(a_1)A + \phi(a_2)A^2 + \dots$ gewoon schrijven

$$f(A) := a_0 + a_1A + a_2A^2 + \dots$$

Het beeld van Φ_A noteren we met $K[A]$. Dit is dus een deelring van $\text{End}_K(V)$. Merk op, dat deze deelring commutatief is (omdat ook $K[X]$ dat is). Als de dimensie van de lineaire ruimte V minstens 2 is, dan is $\text{End}_K(V)$ niet commutatief. Hieruit concluderen we dat als $\dim_K(V) \geq 2$, dan is Φ_A *niet* surjectief.

We laten nu zien dat Φ_A ook niet injectief is als voor V een eindig dimensionale lineaire ruimte wordt genomen. Zij $\dim_K V = n$, dan geldt $\dim_K \text{End}_K(V) = n^2$ (kies een basis van V , dat geeft $\text{End}_K(V) \cong M(n, K)$). De $n^2 + 1$ elementen $I, A, A^2, \dots, A^{n^2} \in \text{End}_K(V)$ zijn dus zeker lineair afhankelijk. Daarom zijn er $c_i \in K$, niet allemaal nul, zodat:

$$c_0 + c_1A + c_2A^2 + \dots + c_{n^2}A^{n^2} = 0.$$

Dan is dus $g(A) = 0$ met $g = c_0 + c_1X + \dots + c_{n^2}X^{n^2} \in K[X]$, dwz $g \in \ker \Phi_A$.

Voor het geval $K = \mathbb{R}$ of $K = \mathbb{C}$ herinnert u zich wellicht nog dat het eigenwaardepolynoom P_A van A ook in de kern van Φ_A zit,

$$P_A(X) := \det(A - X \cdot I) \in K[X].$$

De graad van P_A is n . We zullen de kern van Φ_A later nog uitvoeriger bestuderen, zie voorbeeld 3.4.4.

Opmerking 3.2.4 Laat R een ring zijn, dan geeft elk polynoom $f = a_0 + a_1X + a_2X^2 + \dots \in R[X]$ een functie

$$\rho f : R \longrightarrow R, \quad r \mapsto \rho f(r) := a_0 + a_1r + a_2r^2 + \dots$$

Het kan best zijn dat $f \neq g$ maar dat toch $\rho f(r) = \rho g(r)$ voor alle $r \in R$. De afbeelding

$$\rho : R[X] \rightarrow \text{Afb}(R, R), \quad f \mapsto \rho f,$$

is dus niet altijd injectief.

Bijvoorbeeld als $R = \mathbb{Z}/(2)$, dan hebben de polynomen X en X^2 dezelfde functiewaarden ($\bar{0} = \bar{0}^2$, $\bar{1} = \bar{1}^2$), maar zijn wel verschillend.

Men dient zich dus te realiseren dat er een verschil is tussen polynomen (zoals f) en de afbeeldingen die ze geven (zoals ρf).

3.3 Delen met rest van polynomen

We geven nu een techniek waarmee het bepalen van de kern van een evaluatie homomorfisme vereenvoudigd wordt. Deze **deling met rest** voor polynomen is analoog aan de deling met rest voor gehele getallen.

Stelling 3.3.1 *Zij R een ring met 1, 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

$$f = qg + r, \quad \text{en} \quad gr(r) < gr(g).$$

Men noemt q en r het quotiënt en de rest bij de deling door g .

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

Als $n < m$ dan kunnen we $q = 0$, $r = f$ 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:

$$f_1 = q_1g + r_1, \quad gr(r_1) < gr(g).$$

Er geldt dus:

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

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

$$f = qg + r, \quad \text{en} \quad gr(r) < gr(g),$$

zoals verlangd.

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

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

De graad van de rechterkant is kleiner dan $gr(g)$. Zou nu $q \neq q'$, dan was de graad van de linkerkant groter dan of gelijk aan $gr(g)$, aangezien de kopcoëfficiënt van g een eenheid is. Maar dan hebben we

$$gr(g) \leq gr((q - q')g) = gr(r' - r) < gr(g).$$

Dit levert een tegenspraak, dus moet wel $q = q'$, en dan ook $r' - r = 0$ dus $r = r'$.

Hiermee is Stelling 3.3.1 bewezen. Merk op dat we niet verondersteld hebben dat R commutatief is. \square

Voorbeeld 3.3.2 Het delen van polynomen gaat in de praktijk met een staartdeling. Zij $R = \mathbb{Z}$ en laat $f, g \in \mathbb{Z}[X]$:

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

het quotiënt q en de rest r worden als volgt bepaald:

$$\begin{array}{r} X^2 - 1 \mid X^4 - X^3 - 2X^2 + 3X - 4 \\ \underline{X^4} - X^2 - 4 \\ - X^3 - X^2 - 4 \\ - X^2 - 4 \\ + 3X - 4 \\ + 2X - 4 \\ + 1 \\ 2X - 5 \end{array}$$

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

3.3.3 De stelling over deling met rest stelt ons in staat om eenvoudige representanten van nevenklassen van een hoofdideaal $(g) \subset R[X]$ te vinden. Deze zijn analoog aan de representanten $0, 1, \dots, n-1$ van het hoofdideaal $(n) \subset \mathbb{Z}$.

Stelling 3.3.4 *Zij R een ring met 1 en zij $g \in R[X]$, $gr(g) > 0$. Neem aan dat de kopcoëfficiënt van g een eenheid van R is.*

Dan is er een bijectie tussen de verzamelingen:

$$\{h \in R[X] : gr(h) < gr(g)\} \longrightarrow R[X]/(g) \quad h \mapsto h + (g).$$

D.w.z. dat iedere nevenklasse van het ideaal (g) een unieke representant $h \in R[X]$ heeft met $gr(h) < n$.

Bewijs. We bewijzen eerst dat de afbeelding surjectief is. Zij $f + (g)$, met $f \in R[X]$, een nevenklasse van het ideaal (g) . We mogen Stelling 3.3.1 toepassen met deze f en g en we vinden $q, r \in R[X]$ met $gr(r) < gr(g)$:

$$f = qg + r \implies f + (g) = r + qg + (g) = r + (g),$$

immers $qg \in (g)$. Om de injectiviteit te bewijzen merken we op:

$$h_1 + (g) = h_2 + (g) \iff h_1 - h_2 \in (g) \iff h_1 - h_2 = fg,$$

voor zekere $f \in R[X]$. Omdat de kopcoëfficiënt van g een eenheid is, is $gr(fg) = gr(f) + gr(g)$. Als $gr(h_1), gr(h_2) < gr(g)$ kan de gelijkheid alleen gelden als $f = 0$, dus als $h_1 = h_2$.

Uit surjectief en injectief volgt bijectief en de stelling is bewezen. \square

Opmerking 3.3.5 Zowel de linker als de rechter verzameling in de stelling zijn optelgroepen, de linker omdat $gr(h_1 + h_2) \leq \max(gr(h_1), gr(h_2)) < gr(g)$ als $gr(h_1), gr(h_2) < gr(g)$ en de rechterzijde is zelfs een ring. Omdat $h_1 + (g) + h_2 + (g) = h_1 + h_2 + (g)$ is de bijectie zelfs een isomorfisme van de optelgroepen. In het bijzonder hangt de optelgroep van $R/(g)$ alleen maar af van de graad van g . In feite is de optelgroep van $R/(g)$ isomorf met R^m als $m = gr(g)$, via

$$a_0 + a_1X + \dots + a_{m-1}X^{m-1} \longmapsto (a_0, a_1, \dots, a_{m-1}).$$

Het product op de ring rechts hangt daarentegen wel sterk af van g , zoals we in de voorbeelden hieronder zullen zien.

Voorbeeld 3.3.6 Zij $g = X^2 + X + 1 \in \mathbb{F}_2[X]$, waarbij we $0 := \bar{0}$, $1 := \bar{1}$ schrijven voor de elementen van $\mathbb{F}_2 = \mathbb{Z}/(2)$. Aangezien een polynoom in $\mathbb{F}_2[X]$ coëfficiënten uit $\{0, 1\}$ heeft, zijn er volgens Stelling 3.3.4 slechts 4 nevenklassen van (g) , representanten zijn:

$$0, \quad 1, \quad X, \quad X + 1.$$

Schrijven we, als gebruikelijk,

$$x := X + (g) \quad \text{dan is} \quad \mathbb{F}_2[X]/(g) = \{0, 1, x, x + 1\}.$$

De optelgroep van $\mathbb{F}_2[X]/(g)$ is isomorf met $(\mathbb{Z}/(2))^2$ door $ax + b \mapsto (a, b)$. Het product is iets ingewikkelder. Bij vermenigvuldigen geldt de regel: $x^2 + x + 1 = 0$ omdat $X^2 + X + 1 = g \in 0 + (g)$. Zo is bv:

$$x(x + 1) = x^2 + x = 1 \cdot (x^2 + x + 1) + 1 = 1.$$

(bij het tweede = teken hebben we de deling met rest gebruikt (!)). In de ring $\mathbb{F}_2[X]/(g)$ zijn dus $x + 1$ en x elkaars inverse! Verder is $1 \cdot 1 = 1$, dus elk element ongelijk aan nul heeft een inverse. We concluderen dat $\mathbb{F}_2[X]/(X^2 + X + 1)$ een lichaam met 4 elementen is!

De ring $\mathbb{F}_2[X]/(X^2 + X)$ is daarentegen geen lichaam. De representanten voor de nevenklassen zijn hetzelfde, maar nu is $X(X + 1) \in 0 + (X^2 + X)$, de nevenklassen $X + (X^2 + X)$ en $X + 1 + (X^2 + X)$ zijn dus nuldelers.

In de ring $\mathbb{F}_2[X]/(X^2)$ is het element $X + (X^2)$ zelfs een nilpotent want $(X + (X^2))^2 = X^2 + (X^2) = 0 + (X^2)$. Deze ring is dus niet isomorf met $\mathbb{F}_2[X]/(g)$ en ook niet met $\mathbb{F}_2[X]/(X^2 + X)$, want deze ring heeft geen nilpotenten (in $\mathbb{F}_2[X]/(X^2 + X)$ geldt zelfs $r^2 = r$ voor elke r (ga na)).

Voorbeeld 3.3.7 Zij

$$S^1 := \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\},$$

de cirkel met straal 1 en midden $(0, 0)$ in \mathbb{R}^2 . De ring van continue functies van S^1 naar \mathbb{R} geven we aan met $C(S^1, \mathbb{R})$.

Een polynoom $f \in \mathbb{R}[X, Y]$ geeft een functie $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ (eigenlijk zouden we ρf moeten schrijven). Deze functie kunnen we beperken tot $S^1 \subset \mathbb{R}^2$. Op deze wijze verkrijgen we een ringhomomorfisme:

$$\Phi : \mathbb{R}[X, Y] \longrightarrow C(S^1, \mathbb{R}), \quad f \mapsto f|_{S^1}.$$

De afbeelding Φ is niet injectief, bijvoorbeeld $X^2 + Y^2 - 1 \in \ker(\Phi)$ want $a^2 + b^2 - 1 = 0$ voor alle $(a, b) \in S^1$.

We bewijzen:

$$\ker(\Phi) = (X^2 + Y^2 - 1) = (X^2 + Y^2 - 1)\mathbb{R}[X, Y].$$

Bewijs. ‘ \supset ’ Elk element in $(X^2 + Y^2 - 1)$ is te schrijven als $(X^2 + Y^2 - 1)f$, en $\Phi((X^2 + Y^2 - 1)f) = \Phi(X^2 + Y^2 - 1)\Phi(f) = 0 \cdot \Phi(f) = 0$.

‘ \subset ’ Zij $f \in \ker(\Phi)$ d.w.z. $f(a, b) = 0$ voor alle $(a, b) \in S^1$. We delen f door

$X^2 + Y^2 - 1$ in de ring $(\mathbb{R}[X])[Y] = \mathbb{R}[X, Y]$. Omdat $gr_Y(X^2 + Y^2 - 1) = 2$ zijn er $q, r \in \mathbb{R}[X, Y]$ met:

$$f = q(X^2 + Y^2 - 1) + r, \quad r = r_0 + r_1Y,$$

met $r_0, r_1 \in \mathbb{R}[X]$. De aanname $f \in \ker(\Phi)$ impliceert:

$$r(a, b) = r_0(a) + r_1(a)b = 0, \quad \forall (a, b) \in S^1.$$

Merk op dat als $(a, b) \in S^1$ dat dan ook $(a, -b) \in S^1$, dus er geldt ook:

$$r(a, -b) = r_0(a) - r_1(a)b = 0 \quad \forall (a, b) \in S^1.$$

Door optellen en aftrekken van de twee vergelijkingen volgt (ga na):

$$r_0(a) = r_1(a) = 0 \quad \forall a \in (-1, 1) \subset \mathbb{R}.$$

De polynomen $r_0, r_1 \in \mathbb{R}[X]$ hebben dus ieder oneindig veel nulpunten, en daaruit volgt $r_0 = r_1 = 0$ (zie ook stelling 3.5.2). Maar dan is $f = q(X^2 + Y^2 - 1) \in (X^2 + Y^2 - 1)$. Hiermee is bewezen dat $\ker(\Phi) = (X^2 + Y^2 - 1)$.

Uit de eerste isomorfiestelling 2.2.9 volgt nu dat

$$\mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \cong \Phi(\mathbb{R}[X, Y]) \quad (\subset C(S^1, \mathbb{R})),$$

het beeld $\Phi(\mathbb{R}[X, Y])$ noemen we ook wel de ring van polynoomfuncties op de cirkel.

Met behulp van stelling 3.3.4 (toegepast op $R[Y]$, met $R = \mathbb{R}[X]$ en $g = Y^2 + X^2 - 1 \in R[Y]$) kunnen we deze ring expliciet beschrijven. De representanten voor het ideaal $I := (X^2 + Y^2 - 1)$ van $\mathbb{R}[X, Y]$ zijn:

$$f + gY \quad f, g \in \mathbb{R}[X].$$

In $\mathbb{R}[X, Y]/I$ definiëren we de volgende elementen:

$$x := \bar{X} = X + I, \quad y := \bar{Y} = Y + I.$$

Omdat $X^2 + Y^2 - 1 \in I$ geldt $x^2 + y^2 - 1 = 0$, oftewel $y^2 = 1 - x^2$. Samenvattend:

$$\mathbb{R}[X, Y]/I = \{f + gy : f, g \in \mathbb{R}[x]\}$$

en zulke elementen worden vermenigvuldigd volgens de regel

$$(f + gy)(h + ky) = (fh + gk(1 - x^2)) + (fk + gh)y.$$

3.4 Polynoomringen over een lichaam

We bewijzen in deze paragraaf dat een polynoomring $K[X]$ in een variabele X over een lichaam K een hoofdideaalring is. In het bijzonder is de kern van een evaluatiehomomorfisme $\Phi_s : K[X] \rightarrow S$ van de vorm (g) voor zekere $g \in K[X]$.

Stelling 3.4.1 *Zij K een lichaam. Dan is ieder ideaal van $K[X]$ een hoofdideaal.*

Als het ideaal $I \neq 0$ is, dan is iedere polynoom $g \in I$, $g \neq 0$ met minimale graad een voortbrenger van I , d.w.z. $I = (g)$.

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 $gr(g)$ zo klein mogelijk is. We beweren dat geldt:

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

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 3.3.1 toepassen. Dit levert $q, r \in K[X]$ met

$$f = qg + r, \quad gr(r) < gr(g).$$

Omdat $f, qg \in I$ en I een optelgroep is, zit ook $r = f - qg \in I$. 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 minimale 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 Stelling 3.4.1 bewezen. \square

Opmerking 3.4.2 De voorwaarde in Stelling 3.4.1 dat K een lichaam is, kan niet gemist worden. Het ideaal $(2, X) \subset \mathbb{Z}[X]$ is bijvoorbeeld geen hoofdideaal, zie opgave 15, blz. 46.

Ook in de polynoomring $\mathbb{R}[X, Y]$ zijn er idealen die geen hoofdideaal zijn, bijvoorbeeld (X, Y) , zie voorbeeld 2.3.3.

Voorbeeld 3.4.3 Zij Φ_i het evaluatiehomomorfisme (we gebruiken $\mathbb{R} \subset \mathbb{C}$):

$$\Phi_i : \mathbb{R}[X] \longrightarrow \mathbb{C}, \quad f \mapsto f(i).$$

Merk op dat Φ_i surjectief is. Aangezien $i \notin \mathbb{R}$, zitten er geen polynomen $\neq 0$ van graad ≤ 1 in $\ker(\Phi_i)$. Omdat $i^2 = -1$ zit het tweede graads polynoom

$g := X^2 + 1$ in $\ker(\Phi_i)$. Dan is g een polynoom met minimale graad in $\ker(\Phi_i)$ dus, met stelling 3.4.1, $\ker(\Phi_i) = (g)$. Uit de eerste isomorfiestelling 2.2.9 volgt verder nog:

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

Voor generalisaties zie opgave 12.

Voorbeeld 3.4.4 Zij V een lineaire ruimte over een lichaam K , en zij $A \in \text{End}_K(V)$. Dan is de kern van het evaluatiehomorfisme

$$\Phi_A : K[X] \longrightarrow \text{End}_K(V), \quad f \mapsto f(A),$$

(zie ook 3.2.3) waarbij we $\lambda \in K$ identificeren met het endomorfisme λI van V , een hoofdideaal (g) in $K[X]$. Als $a_n \in K - \{0\}$ de kopcoëfficiënt van g is, dan is $(a_n^{-1}g) = (g)$ en $a_n^{-1}g$ is een monisch polynoom. Het **minimumpolynoom** van A is het *monische* polynoom $m_A \in K[X]$ dat de kern van Φ_A voortbrengt:

$$\ker(\Phi_A) = (m_A) := m_A K[X].$$

Als bijvoorbeeld $A = \lambda I$, en $\lambda \in K - \{0\}$, dan is $m_A = X - \lambda$. Laat $\lambda, \mu \in K$ en zij

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad f := (X - \lambda)(X - \mu).$$

Als $\lambda = \mu$ dan is $A = \lambda I$ en dus $m_A = X - \lambda$. Als $\lambda \neq \mu$ dan geldt $A - \tau I \neq 0$ voor elke $\tau \in K$, dus het minimumpolynoom heeft graad ≥ 2 . We berekenen: $f(A) = (A - \lambda)(A - \mu) =$

$$\begin{aligned} & \left(\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right) \cdot \left(\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} - \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \right) \\ & \quad = \\ & \begin{pmatrix} 0 & 0 \\ 0 & \mu - \lambda \end{pmatrix} \begin{pmatrix} \lambda - \mu & 0 \\ 0 & 0 \end{pmatrix} = 0. \end{aligned}$$

Omdat $f(A) = 0$ en $gr(f) = 2$ is f het polynoom met de laagste, positieve, graad in $\ker(\Phi_A)$, dus $\ker(\Phi_A) = (f)$. Omdat f bovendien monisch is, concluderen we dat $f = m_A$.

Algemener, zij

$$A = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n), \quad \text{met } \lambda_i \neq \lambda_j \text{ als } i \neq j,$$

d.w.z. A is een diagonaalmatrix met coëfficiënten $A_{ii} = \lambda_i$, $A_{ij} = 0$ als $i \neq j$. Laat dan

$$f = (X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_n).$$

Omdat $\Phi_A(f) = f(A) = 0$ (ga na) geldt $f \in (m_A)$. Dus geldt: $f = gm_A$ voor zekere $g \in K[X]$. Als $f \neq m_A$ dan ontbreekt minstens een van de factoren $(X - \lambda_i)$ van f in m_A . Dit is echter in tegenspraak met $m_A(A) = 0$, zoals je makkelijk narekent. De conclusie is dat $f = m_A$. Bepaal zelf m_A als de λ_i ook gelijk mogen zijn.

3.5 Polynoomringen over een domein

Stelling 3.5.1 *Laat R een domein zijn, laat $f \in R[X]$, en laat $\alpha_1, \alpha_2, \dots, \alpha_n \in R$ onderling verschillende nulpunten van f zijn. Dan is er een $q \in R[X]$ met*

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

Bewijs. We gebruiken inductie naar n . Voor $n = 1$ passen we Stelling 3.3.1 toe:

$$f = q(X - \alpha_1) + r \quad \text{met} \quad gr(r) \leq 0,$$

d.w.z. r is een constante. Vul nu $X = \alpha_1$ in (preciezer gezegd, gebruik het evaluatiehomomorfisme in α_1 ; dat kan omdat R een domein, dus in het bijzonder commutatief, is), dan komt er: $0 = 0 + r$ dus $r = 0$, hetgeen de uitspraak voor $n = 1$ bewijst.

Laat nu $n > 1$. Uit $f(\alpha_n) = 0$ en deling met rest (als bij $n = 1$) volgt:

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

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

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

(want alle α_i zijn verschillend) en omdat R geen nuldelers heeft volgt hieruit:

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

De inductiehypothese, toegepast op f_1 , laat zien dat

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

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

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

zoals verlangd. Hiermee is Stelling 3.5.1 bewezen. \square

Stelling 3.5.2 *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 $gr(f)$.*

Bewijs. Dit volgt uit Stelling 3.5.1, want als $\alpha_1, \dots, \alpha_n$ verschillende nulpunten zijn van f dan is $f = q \cdot (X - \alpha_1) \dots (X - \alpha_n)$. Vergelijken we de graad links en rechts dan volgt $gr(f) = gr(q) + n$, dus $gr(f) \geq n$. \square

Opmerking 3.5.3 De eis dat R een domein is, is essentieel. Het polynoom $X^2 - \bar{1}$ in $\mathbb{Z}/(8)[X]$ heeft graad 2 maar heeft vier nulpunten in $\mathbb{Z}/(8)$, nl $\bar{1}, \bar{3}, \bar{5}, \bar{7}$.

In het niet-commutatieve lichaam van de quaternionen \mathbb{H} , zie 1.5, heeft het polynoom $X^2 + 1$ van graad 2 bijvoorbeeld de nulpunten $\pm i, \pm j, \pm k$ (het heeft zelfs oneindig veel nulpunten in de quaternionen, zie opgave 4 op blz. 68).

3.6 Differentiëren

3.6.1 Laat in het vervolg van deze paragraaf R een commutatieve ring met 1 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 2.1.15 (toegepast op $\alpha = 0$, en met als grondring $R[X]$) heeft $f(X + Y) - f(X)$ nu een factor Y :

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

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

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

wat we ook kunnen schrijven als

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

(èerst 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 3.6.2 *Zij R een commutatieve ring met 1.*

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

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

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

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

(Met $ka_k = a_k + a_k + \dots + a_k$ (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

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

en

$$\begin{aligned} f(X + Y) \cdot g(X + Y) - f(X) \cdot g(X) \\ = \\ Y \cdot (f(X) \cdot H_2 + g(X) \cdot H_1 + Y \cdot H_1 \cdot H_2). \end{aligned}$$

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

$$(f + g)' = H_1(X, 0) + H_2(X, 0) = f' + g',$$

$$(fg)' = f \cdot H_2(X, 0) + g \cdot H_1(X, 0) + 0 = fg' + gf'.$$

b. We bewijzen eerst met inductie naar k dat

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

Voor $k = 1$ rekt 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 $(zX^0)' = 0$, en met a. vinden we nu

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

zoals verlangd.

Dit bewijst stelling 3.6.2. □

3.6.3 Met de formule uit 3.6.2b hadden we f' natuurlijk ook kunnen definiëren. Dan moet a. wel anders bewezen worden.

3.6.4 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 3.5.1 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 3.6.5 *Zij R een commutatieve ring met 1, en $f \in R[X]$. Stel dat $\alpha \in R$ een nulpunt van f is. Dan geldt:*

α is een dubbel nulpunt van $f \iff \alpha$ is een nulpunt van f' .

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

α is een dubbel nulpunt van $f \iff$ er is een $q_1 \in R[X]$

met $q = (X - \alpha)q_1 \iff q(\alpha) = 0$.

Uit $f = (X - \alpha) \cdot q$ en 3.6.2(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: $q(\alpha) = 0 \iff f'(\alpha) = 0$. Hiermee is stelling 3.6.5 bewezen. \square

3.7 Opgaven

1. Laat R een ring zonder nuldelers zijn, en $f, g \in R[X]$.

Bewijs: $gr(f \cdot g) = gr(f) + gr(g)$. Bewijs dat $R[X]$ geen nuldelers heeft.

2. Laat aan de hand van een voorbeeld zien dat de voorwaarde dat de kopcoëfficiënt van g een eenheid van R is in 3.3.1 niet gemist kan worden.
3. Zij K een lichaam, $f \in K[X]$ een polynoom, en $\alpha_0, \alpha_1, \dots, \alpha_n$ een $n+1$ -tal verschillende elementen van K , met $n \geq gr(f)$. 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.

4. Zij $x = a + bi + cj + dk \in \mathbb{H}$, met $a, b, c, d \in \mathbb{R}$. Bewijs: x is een nulpunt van $X^2 + 1 \Leftrightarrow x\bar{x} = 1$ en $\bar{x} = -x \Leftrightarrow a = 0$ en $b^2 + c^2 + d^2 = 1$. Concludeer dat $X^2 + 1$ oneindig veel nulpunten in \mathbb{H} heeft.
5. Laat $f, g \in R[X]$ (R een comm. ring met 1) 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 $f \in R[X] \cdot g^k$.
6. 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: $(f')' = 0$.

7. Voor $f \in R[X]$ en $k \in \mathbb{Z}_{\geq 0}$ definiëren we $f^{(k)}$ inductief door $f^{(0)} = f$, $f^{(k)} = (f^{(k-1)})'$. 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).

8. Zij R een eindige ring. Bewijs: $\exists n, m \in \mathbb{Z} : n > m > 0$, zodat $x^n = x^m$ voor alle $x \in R$.
9. Laat R een domein zijn, en $f, g \in R[X]$ polynomen met $\max\{gr(f), gr(g)\} < \#R$ (dat geldt bijvoorbeeld als R oneindig is). Bewijs: $(\forall x \in R : f(x) = g(x)) \Leftrightarrow f = g$.
10. Zij p een priemgetal, en $f, g \in \mathbb{F}_p[X]$. Bewijs:

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

11. We definiëren een evaluatiehomomorfisme:

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

Bewijs dat $\ker(\Phi) = (X^3 - Y^2)$ en dat $\Phi(\mathbb{R}[X, Y]) = \{\sum a_i T^i : a_1 = 0\}$.

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

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

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

- b. Zij $g = X^2 - 2aX + a^2 + b^2$. Bewijs dat:

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

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

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

hierin is $\mathbb{R}[\epsilon]$ de ring van duale getallen (zie opgave 25 op blz. 48). Probeer ook expliciete isomorfismen aan te geven.

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

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

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

14. a. Ga na dat de raaklijn aan de cirkel

$$S^1 := \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}$$

in het punt $(a, b) \in S^1$ gegeven wordt door

$$l_{(a,b)}(X, Y) = 0,$$

waarbij

$$l_{(a,b)} = a(X - a) + b(Y - b) \in \mathbb{R}[X, Y].$$

- b. Zij $\mathbb{R}[\epsilon]$ de ring van de duale getallen (d.w.z. $\epsilon^2 = 0$, zie opgave 25 op blz. 48). Definieer

$$S^1(\mathbb{R}[\epsilon]) := \{(a + s\epsilon, b + t\epsilon) \in \mathbb{R}[\epsilon]^2 : (a + s\epsilon)^2 + (b + t\epsilon)^2 = 1\},$$

‘de punten van S^1 met coördinaten in $\mathbb{R}[\epsilon]$ ’. Laat zien dat:

$$(a + s\epsilon, b + t\epsilon) \in S^1(\mathbb{R}[\epsilon]) \iff l_{(a,b)}(a + s, b + t) = 0.$$

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

$$r = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \quad a_i \in K.$$

- 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 nuldeeler in R nilpotent is. Wat is de kleinste k met $r^k = 0$ voor elke nuldeeler r in R ?
 c. Geef voor elke $a \in K$ een ringisomorfisme:

$$K[X]/((X - a)^n) \cong K[X]/(X^n).$$

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

16. Zij $R = \mathbb{R}[X, Y]/(Y^2)$ en zij $h := Y + (Y^2) \in R$.

- a. Ga na dat iedere $r \in R$ op unieke wijze te schrijven is als $r = r_0 + r_1h$, met $r_0, r_1 \in \mathbb{R}[X]$. Laat zien dat

$$R_0 := \{r \in R : r_1 = 0\}$$

een deelring vormt van R die isomorf is $\mathbb{R}[X]$.

b. Zij

$$\Phi_h : \mathbb{R}[X] \longrightarrow R, \quad \Phi_h(f) := f(X + h)$$

het evaluatiehomomorfisme (hierbij wordt $\phi : \mathbb{R} \rightarrow R$ gegeven door $\phi(a) = a + 0 \cdot h$). Laat zien dat:

$$\Phi_h(f) = f + f'h$$

met $f' \in \mathbb{R}[X]$ de afgeleide van f .

c. Ga na dat uit $\Phi_h(fg) = \Phi_h(f)\Phi_h(g)$ volgt dat de produktregel voor differentiëren geldt.

17. Zij V een eindig dimensionale lineaire ruimte over een lichaam K en zij $A \in \text{End}_K(V)$. Zij $\lambda \in K$ een eigenwaarde van A , dwz er is een $v \in V$, $v \neq 0$ met $Av = \lambda v$, of, equivalent, $A - \lambda$ is niet inverteerbaar in $\text{End}_K(V)$.

- Bewijs dat λ een nulpunt van m_A is. (Hint: bekijk $m_A(A)v$).
- Bewijs dat ieder nulpunt μ van m_A een eigenwaarde van A is. (Hint: schrijf $m_A = (X - \mu) \cdot g$ en bekijk $0 = (A - \mu) \cdot g(A)$).
- Bewijs dat als alle eigenwaarden van A in K zitten en verschillend zijn, dat dan m_A , op teken na, het eigenwaarde polynoom $\det(A - XI)$ van A is.

18. Bereken de minimumpolynomen van de volgende matrices in $M_3(K)$ met K een lichaam. Onderscheidt de gevallen $\lambda = \mu$ en $\lambda \neq \mu$.

$$A := \begin{pmatrix} \lambda & 0 & 1 \\ 0 & \mu & 1 \\ 0 & 0 & \mu \end{pmatrix}, \quad B := \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \mu & 1 \\ 0 & 0 & \mu \end{pmatrix}.$$

19. Zij R de ring van polynoomfuncties op de cirkel:

$$R = \mathbb{R}[X, Y]/I, \quad \text{met } I = (X^2 + Y^2 - 1).$$

Definieer $x, y \in R$ door:

$$x := X + I, \quad y := Y + I, \quad \text{en zij } M := (x - 1, y),$$

een ideaal in R . Merk op dat elke $r \in R$ op unieke wijze geschreven kan worden als $r = f + gy$ met $f, g \in \mathbb{R}[x]$.

a. Bewijs dat

$$\Psi_{(1,0)} : R \longrightarrow \mathbb{R}, \quad f + gy \mapsto f(1)$$

een surjectief ringhomomorfisme is met $\ker(\Psi_{(1,0)}) = M$.

b. Definieer

$$N : R \longrightarrow \mathbb{R}[x]$$

door

$$N(f + gy) := (f + gy)(f - gy) = f^2 - g^2(1 - x^2).$$

Bewijs: Als $N(r) \in \mathbb{R}[x]$ een constant polynoom is, dan geldt $r = f + gy$ met f constant en $g = 0$.

c. Bewijs dat M géén hoofdideaal is. (Aanwijzing: stel $1 - x = \alpha \cdot r$, $y = \alpha \cdot s$, bekijk dan $N(1 - x)$, $N(y)$.)

20. We definiëren de n -sfeer door:

$$S^n := \{(x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} : x_0^2 + x_1^2 + \dots + x_n^2 = 1\},$$

zij $C(S^n, \mathbb{R})$ de ring van continue functies van S^n naar \mathbb{R} . Zij Φ_n de restrictie afbeelding:

$$\mathbb{R}[X_0, X_1, \dots, X_n] \longrightarrow C(S^n, \mathbb{R}), \quad f \mapsto f|_{S^n}.$$

Bewijs dat

$$\ker(\Phi_n) = (X_0^2 + X_1^2 + \dots + X_n^2 - 1).$$

4 Priemidealen en maximale idealen

4.1 Priemidealen

In dit hoofdstuk is R steeds een **commutatieve** (unitaire) ring.

4.1.1 Een belangrijke eigenschap van priemgetallen p is, dat

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

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 4.1.2 Laat R een commutatieve ring met 1 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 4.1.3 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 4.1.4 *Het ideaal $\{0\} \subset R$ is een priemideaal d.e.s.d.a. R is een domein.*

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. Omdat R ook unitair is, is R dan een domein. Dit bewijst 4.1.4. \square

Voorbeeld 4.1.5 Het ideaal $\mathbb{R}[X].(X^2 - 1) \subset \mathbb{R}[X]$ is geen priemideaal, want het bevat wèl $(X + 1)(X - 1)$, 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 evaluatiehomomorfisme (zie 3.4.3):

$$\Psi_i : \mathbb{R}[X] \longrightarrow \mathbb{C}, \quad f \mapsto f(i).$$

We weten al dat:

$$\ker \Psi_i = \mathbb{R}[X] \cdot (X^2 + 1).$$

Voor $f, g \in \mathbb{R}[X]$ geldt nu:

$$\begin{aligned} fg \in \mathbb{R}[X] \cdot (X^2 + 1) &\Rightarrow (fg)(i) = f(i)g(i) = 0 \Rightarrow f(i) = 0 \text{ of } g(i) = 0 \\ &\Rightarrow f \in \mathbb{R}[X] \cdot (X^2 + 1) \text{ of } g \in \mathbb{R}[X] \cdot (X^2 + 1). \end{aligned}$$

Hiermee is (P2) gecontroleerd; we laten (P1) aan de lezer over.

4.1.6 De volgende stelling, die een generalisatie is van 4.1.4, zegt dat men kan zien of een ideaal I priem is door naar de restklassenring R/I te kijken.

Stelling 4.1.7 *Zij R een commutatieve ring met 1, 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 1.19 een domein dan en slechts dan als $\bar{1} \neq \bar{0}$ en R/I geen nuldelers heeft. Nu geldt:

$$\bar{1} \neq \bar{0} \iff 1 \notin I \iff I \neq R \iff (P1) \text{ geldt,}$$

en

$$\begin{aligned} &R/I \text{ heeft geen nuldelers} \\ \iff &(\forall \bar{a}, \bar{b} \in R/I : \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0} \text{ of } \bar{b} = \bar{0}) \\ \iff &(\forall a, b \in R : ab \in I \Rightarrow a \in I \text{ of } b \in I) \\ \iff &(P2) \text{ geldt.} \end{aligned}$$

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 4.1.7. \square

Voorbeeld 4.1.8 Er geldt $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$, en dit is een domein. Met stelling 4.1.7 zien we nu direct dat $(X^2 + 1)$ een priemideaal is van $\mathbb{R}[X]$.

4.1.9 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 4.1.7 toepassen. Voor speciale ringen bestaan er ook andere manieren: zie bijvoorbeeld stelling 5.2.3 verderop.

4.1.10 Voorbeelden.

- a. Laat $J = (X + Y, X^2 + X + Y + 1) \subset R = \mathbb{R}[X, Y]$ en zij $I = (X + Y) = (Y - (-X)) \subset R$. Dan is (zie 2.2.10)

$$R/I \cong \mathbb{R}[X], \quad F(X, Y) \mapsto F(X, -X).$$

Zij $\phi : R \rightarrow R/I$ de canonieke afbeelding, dan is $\phi(J) = (0, X^2 + X + (-X) + 1) = (X^2 + 1) \subset \mathbb{R}[X]$ en met 2.2.13:

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

Dus J is een priemideaal van R .

- b. Laat $J = (5, X^2 + Y + 1) \subset R = \mathbb{Z}[X, Y]$ en zij $I = (Y - (-X^2 - 1)) \subset J$. Dan is:

$$R/I \cong \mathbb{Z}[X], \quad F(X, Y) \mapsto F(X, -X^2 - 1),$$

en $J/I = (5, 0) = (5)$. Men rekent eenvoudig na dat:

$$\phi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_5[X], \quad \sum_i a_i X^i \mapsto \sum_i \bar{a}_i X^i,$$

dus met $\bar{a}_i \in \mathbb{F}_5$) een surjectief ringhomomorfisme is met $\ker(\phi) = (5) = 5\mathbb{Z}[X]$ (zie ook 2.2.11). Met 2.2.9 en 2.2.13 volgt dan

$$R/J \cong \mathbb{F}_5[X],$$

een domein is omdat \mathbb{F}_5 een domein (zelfs een lichaam) is. Daarom is J een priemideaal.

- 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 .

4.2 Maximale idealen

Definitie 4.2.1 Zij R een commutatieve ring met 1. 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 $J = R$.

4.2.2 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 4.1.7 voor maximale idealen bewezen hebben. We beginnen met het analogon van 4.1.4:

Stelling 4.2.3 *Het ideaal $\{0\} \subset R$ is maximaal d.e.s.d.a. R is een lichaam.*

Bewijs. \Leftarrow . 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 2.3.6, dus ook aan (M2) is voldaan. Dit bewijst \Leftarrow .

\Rightarrow . 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. Omdat R unitair is, is volgt dat R een lichaam is. Dit bewijst \Rightarrow . Hiermee is 4.2.3 bewezen. \square

Stelling 4.2.4 *Zij R een commutatieve ring met 1, en $M \subset R$ een ideaal. Dan geldt:*

M is een maximaal ideaal van $R \iff R/M$ is een lichaam.

Bewijs. Het idee van het bewijs bestaat er uit de bewering terug te voeren tot het speciale geval 4.2.3, door gebruik te maken van 2.2.13.

Schrijf $\bar{R} = R/M$. Volgens 2.2.13 corresponderen de idealen J in R met $M \subset J \subset R$ éénéénduidig 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:

$$\begin{array}{c} M \text{ is een maximaal ideaal van } R \\ \iff \\ \{\bar{0}\} \text{ is een maximaal ideaal van } \bar{R} = R/M. \end{array}$$

Volgens 4.2.3 is dit weer hetzelfde als: $\bar{R} = R/M$ is een lichaam. Hiermee is 4.2.4 bewezen. \square

4.2.5 Men gebruikt stelling 4.2.4 op dezelfde manier om te zien of een ideaal maximaal is als men stelling 4.1.7 gebruikt om te zien of een ideaal priem is.

4.2.6 Voorbeelden. Laat $n \in \mathbb{Z}_{>0}$. Dan is $\mathbb{Z}/n\mathbb{Z}$ een lichaam, precies dan als n priem is (zie 1.18), dus

$$p\mathbb{Z} \subset \mathbb{Z} \text{ is maximaal, voor } p \text{ priem}$$

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 2.2.14)

$$\mathbb{R}[X, Y]/(X - a, Y - b) \cong \mathbb{R}[X]/(X - a) \cong \mathbb{R},$$

en \mathbb{R} is een lichaam.

Gevolg 4.2.7 *Elk maximaal ideaal is priem.*

Bewijs. Dit volgt direct uit 4.2.4, 4.1.7, en de opmerking dat elk lichaam een domein is. \square

Opmerking 4.2.8 Zoals uit het bovengegeven voorbeeld $(5, X^2 + Y + 1) \subset \mathbb{Z}[X, Y]$ blijkt, is de omkering van 4.2.7 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.

4.3 Het lemma van Zorn

4.3.1 Stelling Elke commutatieve ring R met $1 \neq 0$ bezit een maximaal ideaal.

4.3.2 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).

4.3.3 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, \dots . Definieer inductief de rij idealen

$$I_0 \subseteq I_1 \subseteq \dots \quad \text{door: } I_0 = (0);$$

$$I_n = \begin{cases} I_{n-1} + (r_n) & \text{als } I_{n-1} + (r_n) \neq R \\ I_{n-1} & \text{anders.} \end{cases}$$

Zet 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 $ra \in I_n \subseteq M$.

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 4.3.3 bewezen. \square

4.3.4 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 transfinitie 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 tamelijk evidente uitspraak dat je bij elke surjectieve afbeelding ten minste één rechtsinverse hebt.)

Lemma van Zorn. Zij P een **partieel geordende** verzameling. Dan bezit P tenminste één **maximale keten**.

4.3.5 Verklaringen van de vetgedrukte woorden: een **partieel geordende verzameling** is een verzameling P die voorzien is van een binaire relatie \leq met de volgende twee eigenschappen:

$$\begin{aligned} \forall x, y, z \in P : (x \leq y \wedge y \leq z) &\Rightarrow x \leq z, \\ \forall x, y \in P : (x \leq y \wedge y \leq x) &\Leftrightarrow x = y; \end{aligned}$$

een **keten** in een partieel geordende verzameling P is een deelverzameling $K \subset P$ met de eigenschap

$$\forall x, y \in K : x \leq y \vee y \leq x.$$

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 Van der Waerden, Algebra I, §69, of naar de syllabus Inleiding in de wiskunde (H.C. Doets & A.S. Troelstra, Mathematisch Instituut, Universiteit van Amsterdam, 1979/80).

Bewijs. (van stelling 4.3.1) Neem als partieel geordende verzameling P de verzameling van alle idealen in R verschillend van R :

$$P = \{I : I \text{ is een ideaal van } R, \text{ en } 1 \notin I\}.$$

met als partieële ordening de *inclusierelatie*. Dus $I \leq J$ in P als $I \subseteq J$.

Merk op dat in het bewijs van 4.3.3 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 $\forall I, J \in K: I \subset J \vee J \subset I$.

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 4.3.3. 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 4.3.3). We concluderen dat M inderdaad een maximaal ideaal is. \square

Gevolg 4.3.6 *Zij R een commutatieve ring (met 1), en $I \subset R$ een ideaal, $I \neq R$. Dan bezit R een maximaal ideaal M met $I \subset M$.*

Bewijs. Wegens 4.3.1 heeft de ring R/I een maximaal ideaal, en dit moet wegens 2.2.13 van de vorm M/I zijn, waar M een ideaal van R is met $M \supset I$. Voorts zegt 2.2.13 dat $R/M \cong (R/I)/(M/I)$ en dit is een lichaam; dus M is maximaal in R (stelling 4.2.4). Hiermee is 4.3.6 bewezen.

(Alternatief bewijs: pas het lemma van Zorn toe op de verzameling idealen $\neq R$ van R die I omvatten.) \square

Gevolg 4.3.7 *Zij R een commutatieve ring met 1. 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 2.3.5 en 4.2.1(M1). Dus $\bigcup_M M \subset R - R^*$.

\supset : Als $a \in R - R^*$ dan $Ra \neq R$, en Ra is een ideaal van R .

Wegens 4.3.6 is er dus een maximaal ideaal M van R met $Ra \subset M$. Dus $a \in \bigcup_M M$ voor alle $a \in R - R^*$.

Hiermee is 4.3.7 bewezen. \square

Voorbeeld 4.3.8 Laat $R = C([0, 1])$ de ring van continue functies $f : [0, 1] \rightarrow \mathbb{R}$ zijn. Voor $x \in [0, 1]$ zij

$$M_x = \{f \in R : f(x) = 0\}.$$

Dit is de kern van het surjectieve ringhomomorfisme

$$R \rightarrow \mathbb{R}, \quad f \mapsto f(x), \quad \text{dus} \quad R/M_x \cong \mathbb{R}$$

en dus is $M_x \subset R$ maximaal. Uit opgave 18 blijkt dat elk maximaal ideaal van R van deze vorm is. Er geldt

$$R - \bigcup_{x \in [0,1]} M_x = \{f \in R : \forall x \in [0,1] : f(x) \neq 0\}.$$

Dit is juist de eenhedengroep R^* van R , in overeenstemming met 4.3.7.

4.3.9 Een typische toepassing van stelling 4.3.1 is het volgende resultaat, dat iets zegt over de oplosbaarheid van een stelsel vergelijkingen over een lichaam.

Gevolg 4.3.10 *Laat K een lichaam zijn, $n, t \in \mathbb{Z}_{>0}$, en $f_1, f_2, \dots, f_t \in K[X_1, X_2, \dots, X_n]$. Dan zijn de volgende twee beweringen equivalent.*

a. *Er bestaan geen $g_1, g_2, \dots, g_t \in K[X_1, X_2, \dots, X_n]$ met $g_1 f_1 + g_2 f_2 + \dots + g_t f_t = 1$.*

b. *Er bestaat een lichaam L , met $K \hookrightarrow L$, en er zijn $x_1, x_2, \dots, x_n \in L$ met*

$$\begin{aligned} f_1(x_1, x_2, \dots, x_n) &= f_2(x_1, x_2, \dots, x_n) = \dots = \\ f_t(x_1, x_2, \dots, x_n) &= 0. \end{aligned}$$

Bewijs.

(b) \Rightarrow (a). Laten L, x_1, \dots, x_n als in (b) zijn, en stel dat toch

$$g_1 f_1 + \dots + g_t f_t = 1, \quad \text{met } g_1, \dots, g_t \in K[X_1, \dots, X_n].$$

Substitueer x_1, x_2, \dots, x_n voor X_1, X_2, \dots, X_n in deze relatie, dan vinden we $0 = 1$, een tegenspraak.

(a) \Rightarrow (b). Laat $I \subset K[X_1, \dots, X_n]$ het door f_1, f_2, \dots, f_t voortgebrachte ideaal van $K[X_1, \dots, X_n]$ zijn. Dan wil (a) precies zeggen dat $1 \notin I$, dus $I \neq K[X_1, \dots, X_n]$. Volgens 4.3.1 is er nu een maximaal ideaal M van $K[X_1, \dots, X_n]$ met $I \subset M$. Neem $L = K[X_1, \dots, X_n]/M$. Dit is volgens 4.2.4 een lichaam. Stellen we de ringhomomorfismen

$$K \hookrightarrow K[X_1, \dots, X_n] \longrightarrow L = K[X_1, \dots, X_n]/M,$$

samen, dan vinden we een ringhomomorfisme $K \rightarrow L$, dat volgens 2.3.7 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

$$f_j(x_1, \dots, x_n) = f_j(X_1, \dots, X_n) + M \in 0 + M$$

aangezien $f_j(X_1, \dots, X_n) = f_j \in I \subset M$, voor $1 \leq j \leq t$, zoals verlangd. Hiermee is 4.3.10 bewezen. \square

Voorbeeld 4.3.11 Neem

$$K = \mathbb{R}, \quad n = t = 1, \quad f_1 = X^2 + 1 \in \mathbb{R}[X].$$

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 $L = \mathbb{C}$, $x = i$. Aan dit voorbeeld zien we ook dat het niet steeds mogelijk is $L = K$ te nemen.

Opmerking 4.3.12 Men kan bewijzen dat elk maximaal ideaal van $\mathbb{C}[X_1, \dots, X_n]$ van de vorm:

$$M = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n) \quad (a_i \in \mathbb{C})$$

is. De maximale idealen corresponderen dus met de punten van \mathbb{C}^n (het ideaal M correspondeert uiteraard met het punt $(a_1, a_2, \dots, a_n) \in \mathbb{C}^n$).

Stelling 4.3.10 impliceert dan: Als een stel polynomen $f_1, \dots, f_k \in \mathbb{C}[X_1, \dots, X_n]$ geen gemeenschappelijk nulpunt in \mathbb{C}^n heeft, dan bestaat er een relatie $g_1 f_1 + g_2 f_2 + \dots + g_t f_t = 1$ tussen de f_i .

4.4 Opgaven

1. Laat R een domein zijn. Bewijs: het door X en Y voortgebrachte ideaal van $R[X, Y]$ is gelijk aan

$$\{f \in R[X, Y] : f(0, 0) = 0\}$$

en dit is een priemideaal van $R[X, Y]$.

2. Laat K een lichaam zijn, $n \in \mathbb{Z}_{>0}$, en $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. Bewijs: het door $X_1 - \alpha_1, X_2 - \alpha_2, \dots, X_n - \alpha_n$ voortgebrachte ideaal van $K[X_1, X_2, \dots, X_n]$ 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 $f \in M \Leftrightarrow f(a, b) = 0$ 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 met 1 en $I \subset R$ een ideaal. Bewijs: I is een priemideaal van $R \Leftrightarrow$ er is een lichaam K en een ringhomomorfisme $f : R \rightarrow K$ met $f(1) = 1$ en $I = \ker(f)$.
9. Laat R een commutatieve ring met 1 zijn, $I \subset R$ een ideaal en $\phi : R \rightarrow R/I$ 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 4.1.7 en 2.2.13).

10. Als opgave 9, met overal ‘priemideaal’ vervangen door ‘maximaal ideaal’.

11. Zij $f : R_1 \rightarrow R_2$ een (unitair) homomorfisme van commutatieve ringen, $I_2 \subset R_2$ een ideaal, en $I_1 = f^{-1}(I_2) \subset R_1$.
- Bewijs: I_1 is een ideaal in R_1 , en R_1/I_1 is isomorf met een deelring van R_2/I_2 .
 - Bewijs: als I_2 priem is in R_2 dan is I_1 priem in R_1 .
 - 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 34 op blz. 25) met 1.
- Bewijs: R is een domein $\Leftrightarrow R$ is een lichaam $\Leftrightarrow R \cong \mathbb{F}_2$.
 - Zij $I \subset R$ een ideaal. Bewijs: I is een priemideaal $\Leftrightarrow I$ is een maximaal ideaal $\Leftrightarrow R/I \cong \mathbb{F}_2$.
13. Zij R een commutatieve ring met 1, en $I \subset R$ een ideaal, $I \neq R$. Gegeven is, dat voor elke $x \in R, x \notin I$, geldt dat $x^2 - 1 \in I$.
- Bewijs: $R/I \cong \mathbb{F}_2$ of $R/I \cong \mathbb{F}_3$.
 - Is I een priemideaal van R ?
14. Zij R een commutatieve ring met 1, en $I \subset R$ een ideaal van *eindige* index.
Bewijs: I is een priemideaal $\Leftrightarrow I$ 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 1, met de eigenschap dat $I \cap J \neq \{0\}$ voor elk tweetal idealen $I \neq \{0\}, J \neq \{0\}$ van R .
Bewijs dat $\{a \in R : a \text{ is een nuldeeler}\} \cup \{0\}$ een priemideaal van R is.
17. Zij R de ring waarvan de additieve groep die van \mathbb{Q} is, maar met als vermenigvuldiging $\forall x, y \in R : xy = 0$. Bewijs: R heeft geen ideaal M dat aan de voorwaarden (M1) en (M2) uit 4.2.1 voldoet. Waarom is dit niet in tegenspraak met 4.3.1 ?
18. Laat $R = C([0, 1])$, en zij $M_x \subset R$ voor $x \in [0, 1]$ gedefinieerd als in voorbeeld 4.3.8.
- Zij $I \subset R$ een ideaal met $\forall x \in [0, 1] : I \not\subset M_x$.
Bewijs: $\forall x \in [0, 1] : \exists f_x \in I : f_x(x) \neq 0$.
Laat de f_x zo gekozen zijn. Bewijs dat er $x_1, x_2, \dots, x_n \in [0, 1]$

zijn met $\forall x \in [0, 1] : \sum_{i=1}^n f_{x_i}(x)^2 > 0$. (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: $\exists x \in [0, 1] : M = M_x$. Laat ook zien dat deze x eenduidig bepaald is door M .

19. Zij $R = \mathbb{R}[X, Y]/I$ met $I = (X^2 + Y^2 - 1)$ de ring van polynoomfuncties op de cirkel. Zij $x := X + I$, $y = Y + I \in R$.

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 ?

20. Zij R een commutatieve ring met 1, en $a \in R$ een element met $\forall n \in \mathbb{Z}_{>0} : a^n \neq 0$. 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.)

21. Het **radicaal** $\sqrt{0}$ van een commutatieve ring R met 1 is gedefinieerd door

$$\sqrt{0} = \{a \in R : \exists n \in \mathbb{Z}_{>0} : a^n = 0\}.$$

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 opg. 20).

22. Het **Jacobson-radicaal** $J(R)$ van een commutatieve ring R met 1 is gedefinieerd door

$$J(R) = \{x \in R : \forall r \in R : 1 + rx \in R^*\}.$$

a. Zij $x \in J(R)$, zij $M \subset R$ een maximaal ideaal en definieer 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.

23. Zij R een commutatieve ring met 1, en $S \subset R$ een niet-lege deelverzameling met de eigenschap $0 \notin S$ en $\forall s, t \in S: st \in S$.
Laat zien dat er een priemideaal I van R is met $I \cap S = \emptyset$. (Aanwijzing: gebruik de ring $S^{-1}R$ uit opgave 29 op blz. 24, en pas 4.3.1 en opgave 11(b) toe). Wat is de relatie met opgave 20?
24. Zij R een commutatieve ring met 1. We noemen R **locaal** als $R - R^*$ een ideaal van R is.
- Bewijs: R is lokaal $\Leftrightarrow R$ heeft precies één maximaal ideaal.
 - Zij R lokaal, $x \in R$, en stel dat $x^2 = x$. Bewijs: $x = 0$ of $x = 1$.
25. Zij R een commutatieve ring met 1 en $I \subset R$ een priemideaal. Laat $S = R - I$.
- Bewijs: $\forall s, t \in S: st \in S$.
 - Bewijs dat de ring $S^{-1}R$ uit opgave 29 op blz. 24 een lokale ring is (zie opgave 24).
26. Zij $R = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z}, b \not\equiv 0 \pmod{5}\}$. Bewijs dat R een lokale ring is. Wat is het maximale ideaal M van R ?
Bewijs: $R/M \cong \mathbb{F}_5$.
27. Zij X een verzameling. Een **filter** op X is een collectie \mathcal{F} van deelverzamelingen van X met de volgende eigenschappen:

$$X \in \mathcal{F}; \quad \emptyset \notin \mathcal{F}; \quad A, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F};$$

$$\text{als } A \subset B \subset X \text{ en } A \in \mathcal{F}, \text{ dan } B \in \mathcal{F}.$$

Een **ultrafilter** is een filter \mathcal{F} met de eigenschap:

$$\forall A, B \subset X: (A \cup B \in \mathcal{F} \Rightarrow A \in \mathcal{F} \vee B \in \mathcal{F}).$$

Laat R de ring $P(X)$ uit opgave 35 op blz. 25 zijn.

- Zij \mathcal{F} een collectie deelverzamelingen van X . Bewijs:

$$\mathcal{F} \text{ is een filter op } X \iff$$

$$\{A \subset X : X - A \in \mathcal{F}\} \text{ is een ideaal } \neq R \text{ van } R,$$

en

$$\mathcal{F} \text{ is een ultrafilter op } X \iff$$

$$\{A \subset X : X - A \in \mathcal{F}\} \text{ is een maximaal ideaal van } R.$$

(Aanwijzing: 12(b) op blz. 84.)

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: 4.3.6).

28. 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 met 1. Voor een ultrafilter \mathcal{F} op X definiëren we $I_{\mathcal{F}} \subset R$ door

$$(\alpha_x)_{x \in X} \in I_{\mathcal{F}} \Leftrightarrow \{x \in X : \alpha_x = 0\} \in \mathcal{F}.$$

Bewijs dat $I_{\mathcal{F}}$ een maximaal ideaal van R is, en dat alle maximale idealen van R van deze vorm zijn.

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 1.19).

5.1 Irreducibele elementen

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. $\mathbb{Z}p := \{np : n \in \mathbb{Z}\} \subset \mathbb{Z}$ is een priemideaal.

We gaan de eerste eigenschap generaliseren, maar we zullen zien dat de tweede eigenschap in sommige gevallen verloren gaat, zie bv. 5.1.5 en de opgaven 1 en 2.

Definitie 5.1.1 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 juist de priemgetallen p en hun tegengestelde $-p$.

5.1.2 Als R een domein is, en $f, g \in R[X]$, dan geldt $gr(fg) = gr(f) + gr(g)$. Omdat $gr(1) = 0$ 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 een is in het algemeen *niet* irreducibel: $2X - 2 = 2 \cdot (X - 1)$ is reducibel in $\mathbb{Z}[X]$ (!), het 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 van graad 0 een eenheid, en dus is ieder polynoom van graad 1 irreducibel. Voor polynomen van hogere graad is het in het algemeen een subtiële zaak om te bepalen of ze irreducibel zijn of niet, zie paragraaf 5.5 verderop.

Stelling 5.1.3 *Zij K een lichaam en zij $f \in K[X]$ een polynoom met $gr(f) = 2$ of $gr(f) = 3$.*

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 3.5.1) en dus is f reducibel.

Stel nu dat f geen nulpunt in K heeft. Omdat $gr(f) > 0$ is f geen eenheid. Stel $f = gh$, met $gr(g) \leq gr(h)$. Als $gr(g) \neq 0$ dan moet gelden $gr(g) = 1$ want $gr(f) = gr(g) + gr(h)$. Maar dan heeft g een nulpunt in K en f dus ook, in tegenspraak met de aanname. Daarom geldt $gr(g) = 0$ en dus is g een eenheid in $K[X]$. We concluderen dat f irreducibel is. \square

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 5.1.4 *Zij $a \in R$, $a \neq 0$ 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 4.1.2 blijkt dat $Ra \neq R$, dus a is geen eenheid (zie 2.3.5). Met (P2) volgt uit

$$bc = a \in Ra \quad \text{dat :} \quad b \in Ra \quad \text{of} \quad c \in Ra,$$

laten we zeggen $b \in Ra$. Dan geldt $b = ra$ voor zekere $r \in R$. Uit:

$$bc = a \quad \text{en} \quad b = ra \quad \text{volgt :} \quad (rc - 1)a = 0 \quad \text{en dus} \quad rc = 1,$$

waarbij we gebruikten dat R commutatief is en dat R een domein is ($(rc - 1)a = 0$, $a \neq 0 \Rightarrow rc - 1 = 0$). 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 5.1.4 bewezen. \square

Voorbeeld 5.1.5 Laat R de ring

$$R = \left\{ \sum_{i=0}^n a_i X^i \in \mathbb{Q}[X] : a_1 = 0, \quad n \in \mathbb{Z}_{\geq 0} \right\}$$

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

$$X^2 = f \cdot g, \quad \text{met } f, g \in R, \quad \text{dan } f \in R^* \text{ of } g \in R^*.$$

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 4.1.2 (met $a = b = X^3$) volgen dat $X^3 \in RX^2$, dus $X \in R$, tegenspraak.

5.2 Hoofdideaaldomeinen

We gaan nu een belangrijke klasse ringen definiëren waarin ieder irreducibel element wél een priemideaal, en zelfs een maximaal ideaal voortbrengt.

Definitie 5.2.1 Een **hoofdideaaldomein** (Engels: PID, principal ideal domain) is een domein R waarin elk ideaal een hoofdideaal is (een hoofdideaal is een ideaal van de vorm Ra , zie 2.1.13).

(N.B. In de literatuur wordt dit soms hoofdideaalring genoemd, die naam wordt overigens ook wel eens gebruikt voor ringen (evt. met nuldelers) waarin elk ideaal hoofdideaal is.)

Voorbeeld 5.2.2 We bewezen eerder, zie stelling 2.3.2, dat \mathbb{Z} een hoofdideaaldomein is. Uit voorbeeld 2.3.3 blijkt dat $\mathbb{R}[X, Y]$ geen hoofdideaaldomein is. Alle lichamen zijn hoofdideaaldomeinen; dit volgt op triviale wijze uit 2.3.6. Volgens 3.4.1 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 5.2.3 *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 4.2.7.

(ii) \Rightarrow (iii): dit is precies stelling 5.1.4.

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 4.2.1.

(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. \square

In het bijzonder zien we dat in hoofdideaaldomeinen de omkering van 4.2.7 geldt, voor idealen $\neq \{0\}$:

Gevolg 5.2.4 *In een hoofdideaaldomein is elk priemideaal $\neq \{0\}$ maximaal.*

Bewijs. Dit volgt uit 5.2.3, (ii) \Rightarrow (i), aangezien elk ideaal $\neq \{0\}$ van de vorm Ra is, met $a \neq 0$. Dit bewijst 5.2.4. \square

Voorbeeld 5.2.5 Uit stelling 5.2.3 volgt dus dat de ring R uit voorbeeld 5.1.5 geen hoofdideaaldomein is (R is overigens wel een domein). In feite is het ideaal voortgebracht door X^2 en X^3 geen hoofdideaal, zie opgave 4.

Een belangrijke toepassing van stelling 5.2.3 is het ‘vinden’ (beter: construeren) van een lichaam waarin een polynoom een nulpunt heeft.

Stelling 5.2.6 *Zij K een lichaam en zij $f \in K[X]$ een irreducibel polynoom. Laat*

$$\alpha := X + (f) \in K[X]/(f).$$

Dan is $L := K[X]/(f)$ een lichaam, $K \subset L$ is een deelring en α is een nulpunt van f in L .

Bewijs. Omdat $K[X]$ een hoofdideaaldomein en f irreducibel is, is het ideaal (f) maximaal en dus is $L = K[X]/(f)$ een lichaam. De inclusie $K \subset L$ wordt gegeven door $a \mapsto a + (f)$ ($a \in K$), we schrijven gewoon a i.p.v. $a + (f)$ of \bar{a} .

Omdat $K \subset L$ kunnen we f opvatten als een element van $L[X]$. In L geldt:

$$\alpha^i = (X + (f))^i := X^i + (f) \quad \text{en} \quad a_i(X^i + (f)) = a_i X^i + (f) \quad (a_i \in K).$$

Als $f = a_0 + a_1 X + \dots + a_n X^n$ dan is dus:

$$f(\alpha) = a_0 + a_1 X + \dots + a_n X^n + (f) = f + (f) = 0 + (f),$$

en we zien dat $\alpha \in L$ een nulpunt is van f .

Hiermee is de stelling bewezen. \square

Voorbeeld 5.2.7 Laat $K = \mathbb{R}$, $f = X^2 + 1 \in \mathbb{R}[X]$, $L = \mathbb{R}[X]/(X^2 + 1)$ en $\alpha := X + (X^2 + 1)$. Dan is \mathbb{R} op te vatten als deelring van L . Ieder element van L is op unieke wijze te schrijven als $a + bX + (X^2 + 1) = a + b\alpha$. Dan geldt:

$$\begin{aligned} \alpha^2 &= (X + (X^2 + 1))^2 := X^2 + (X^2 + 1) \\ &= -1 + 1 \cdot (X^2 + 1) + (X^2 + 1) \\ &= -1 + (X^2 + 1), \end{aligned}$$

dus $\alpha^2 = -1 \in L$. Dan is α inderdaad een nulpunt van f . Merk ook op dat we al aangetoond hebben dat $L \cong \mathbb{C}$ (zie 3.4.3), onder dit isomorfisme ging $\alpha = X + (f)$ naar $i \in \mathbb{C}$ en i is een nulpunt van $X^2 + 1$ in \mathbb{C} .

Algemener, zie opgave 12 op blz. 69, als $g = X^2 + bX + c \in \mathbb{R}[X]$ geen nulpunt in \mathbb{R} heeft, dan is $\mathbb{R}[X]/(X^2 + bX + c) \cong \mathbb{C}$ en $X + (X^2 + bX + c)$ correspondeert met een nulpunt $z \in \mathbb{C}$ van g .

Voorbeeld 5.2.8 Zij \mathbb{F}_p het lichaam $\mathbb{Z}/p\mathbb{Z}$, met p een priemgetal (zie 1.18). Als $p > 2$, dan is er een $a \in \mathbb{F}_p$ zodat $X^2 - a \in \mathbb{F}_p[X]$ irreducibel is, d.w.z. geen nulpunt in \mathbb{F}_p heeft. Bekijken we nl. de verzameling $\{x^2 : x \in \mathbb{F}_p\}$, dan heeft deze hoogstens $1 + \frac{p-1}{2}$ (verschillende) elementen, want $x^2 = (-x)^2$ (in feite heeft de verzameling precies $1 + (p-1)/2$ elementen). Er is dus een $a \in \mathbb{F}_p$ die geen kwadraat is en dan heeft het polynoom $X^2 - a$ inderdaad geen nulpunt in \mathbb{F}_p . Voor $p = 3, 5, 7$ kun je resp. $a = 2, 2, 3$ nemen.

Voor iedere $p > 2$ bestaat er dus een lichaam met p^2 elementen, nl. $\mathbb{F}_p[X]/(X^2 - a)$ met a als boven, en hierin is elk element r op unieke wijze te schrijven als $r := a + b\alpha$ met $a, b \in \mathbb{F}_p$ en $\alpha := X + (X^2 - a)$. Voor $p = 2$ kennen we ook al een lichaam met p^2 elementen, zie 3.3.6. We zullen later zien, 9.1.1, dat er, op isomorfie na, slechts één lichaam met p^2 elementen bestaat.

5.3 Ontbindingsdomeinen

We gaan ons nu bezighouden met een algemene methode om aan te tonen dat in bepaalde ringen irreducibele elementen priemidealen voortbrengen.

Definitie 5.3.1 Een **factorontbindingsdomein** of **ontbindingsdomein** 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:

$$a = u \cdot p_1 \cdot p_2 \cdots p_t, \quad u \in R^*, \quad t \in \mathbb{Z}_{\geq 0}, \quad p_i \in R \text{ irreducibel}$$

en een dergelijke ontbinding bovendien eenduidig bepaald is op volgorde en eenheden na, d.w.z. als ook

$$a = v \cdot q_1 \cdot q_2 \cdots q_s, \quad v \in R^*, \quad s \in \mathbb{Z}_{\geq 0}, \quad q_i \in R \text{ irreducibel},$$

dan geldt $s = t$ en er is een permutatie σ van $\{1, 2, \dots, t\}$ zodat

$$p_i = v_i \cdot q_{\sigma(i)} \quad \text{voor zekere eenheden } v_i \in R^*, \quad i = 1, 2, \dots, t.$$

(Kennelijk geldt dan $v = uv_1v_2 \cdots v_t$.)

We noemen zo'n schrijfwijze voor a de **priemontbinding** van a , naar de analogie met de priemontbinding in \mathbb{Z} . (De idealen Rp_i zijn inderdaad priemidealen, zie stelling 5.3.3.)

Ruw gesproken: een ontbindingsdomein is een ring waarin de stelling van de eenduidige priemfactorenontbinding geldt.

In het engels schrijft men UFD, unique factorization domain, voor ontbindingsdomein. Men schrijft ook wel factorontbindingsring voor ontbindingsdomein.

5.3.2 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 5.3.3 *Zij R een ontbindingsdomein, en $a \in R$.*

Dan geldt: a is irreducibel $\iff Ra$ is een priemideaal $\neq (0)$.

Bewijs. \Leftarrow : dit is algemeen waar, zie 5.1.4.

\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 5.3.3 bewezen. \square

In een ontbindingsdomein geldt de omkering van stelling 5.1.4 dus *wel*. Om te verifiëren of een ring een ontbindingsdomein is, is het volgende lemma van belang.

Lemma 5.3.4 *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:*

$$a = u \cdot p_1 \cdot p_2 \cdots p_t, \quad u \in R^*, \quad t \in \mathbb{Z}_{\geq 0}, \quad p_i \in R$$

met de eigenschap dat voor iedere $i = 1, 2, \dots, t$ geldt dat:

$$p_i R \text{ is een priemideaal.}$$

Dan is R een ontbindingsdomein.

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 5.1.4 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 $q_1 q_2 \dots q_s = v^{-1} \cdot u p_1 p_2 \dots p_t \in R p_t$, en $R p_t$ is een priemideaal. Als $s = 0$ zou dit leveren $1 \in R p_t$, hetgeen voor een priemideaal onmogelijk is ((P1) van 4.1.2). Dus $s > 0$. Het product van de s factoren q_1, q_2, \dots, q_s kan volgens (P2) van 4.1.2 alleen tot het priemideaal $R p_t$ 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:

$$u p_1 p_2 \dots p_{t-1} = (r v) q_1 q_2 \dots q_{s-1}, \quad r v \in R^*.$$

Dit is een dergelijke gelijkheid, met t één kleiner. De inductiehypothese zegt dus dat $t - 1 = s - 1$, en dat p_1, p_2, \dots, p_{t-1} op volgorde en eenheden na samenvallen met q_1, q_2, \dots, 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, \dots, p_t op volgorde en eenheden na samenvallen met q_1, q_2, \dots, q_s .

Hiermee is lemma 5.3.4 bewezen. \square

We bewijzen nu dat hoofdideaaldomeinen ontbindingsdomeinen zijn.

Stelling 5.3.5 *Ieder hoofdideaaldomein is een ontbindingsdomein.*

Bewijs. Zij R een hoofdideaaldomein. We hoeven alleen maar te bewijzen dat elke $r \in R$ met $r \neq 0$ een ontbinding $r = u p_1 \dots p_t$, met $R p_i$ priemidealen) heeft, de eenduidigheid volgt dan uit lemma 5.3.4.

Stel dat $a_1 \in R$, $a_1 \neq 0$, niet zo'n ontbinding heeft. Het ideaal $R a_1$ 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 $R a_1 \subset M$. Vanwege onze aanname dat R een hoofdideaalring is, geldt $M = R p_1$ voor een $p_1 \in R$. Wegens $a_1 \in R a_1 \subset M = R p_1$ kunnen we schrijven $a_1 = a_2 p_1$ voor een $a_2 \in R$. Dan is $R a_1 \subset R a_2$, en, omdat p_1 geen eenheid is, ook $R a_1 \neq R a_2$.

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 $R p_2 \supset R a_2$, enz. Zo verder gaande met a_2 vindt men een $a_3 \in R$ met $R a_2 \subset R a_3$, maar $R a_2 \neq R a_3$, en a_3 is geen eenheid, etcetera. Dit leidt nu tot een keten van idealen $(R a_n)_{n=1}^{\infty}$ met $R a_n \subset R a_{n+1}$ maar $R a_n \neq R a_{n+1}$. Zij

$$I := \bigcup_{n \geq 1} R a_n \quad (\subset R).$$

Er geldt dat I een ideaal in R is. Als nl. $a, b \in I$ dan is $a \in R a_k$ en $b \in R a_l$ voor zekere $k, l \in \mathbb{N}$ en wegens de inclusies van de $R a_i$ geldt $a, b \in R a_m$ 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. \square

5.3.6 Als K een lichaam is, dan is $K[X]$ een hoofdideaaldomein, zie 3.4.1, en dus is $K[X]$ een ontbindingsdomein. 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 5.3.7 *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, en zij $k \geq 1$ (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

$$f = (u h_1^{n_1} \dots h_{k-1}^{n_{k-1}}) h_k^{n_k} := f_{k-1} h_k^{n_k}.$$

We definiëren idealen I, J in $K[X]$ door

$$I = (f_{k-1}) \quad \text{en} \quad J = (h_k^{n_k}),$$

en we zullen laten zien dat $I + J = K[X]$, zodat we de chinese reststelling 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 $m \leq n_k$, en 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:

$$uh_1^{n_1} \dots h_{k-1}^{n_{k-1}} = svh_k^m.$$

Omdat de h_i monisch, irreducibel zijn en $K[X]$ een ontbindingsdomein 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 $I + J = (g) = K[X]$.

Met de chinese reststelling, 2.3.11, 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

$$K[X]/(f) \cong K[X]/(h_1^{n_1}) \times K[X]/(h_2^{n_2}) \dots \times K[X]/(h_k^{n_k}),$$

zoals verlangd. Hiermee is 5.3.7 bewezen. \square

5.4 Deelbaarheid

Als K een lichaam is, dan is $K[X]$ een hoofdideaaldomein en dus in het bijzonder een ontbindingsdomein (stelling 5.3.5). We gaan nu de volgende algemenere stelling bewijzen.

Stelling 5.4.1 *Als R een ontbindingsdomein is, dan is $R[X]$ ook een ontbindingsdomein.*

Gevolg 5.4.2 Voor elke $n \in \mathbb{Z}_{>0}$ en elk ontbindingsdomein R is ook de polynoomring $R[X_1, X_2, \dots, X_n]$ een ontbindingsdomein. 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) ontbindingsdomeinen.

Bewijs. (van gevolg 5.4.2.) Dit volgt onmiddellijk met volledige inductie naar n uit stelling 5.4.1. \square

Voor het bewijs van stelling 5.4.1 hebben we enige voorbereidingen nodig. We nemen steeds aan dat R een ontbindingsdomein is, en we geven het quotiëntenlichaam $Q(R)$ van R aan met K , zie 1.3.2. Aangezien K een lichaam is, weten we al dat $K[X]$ een ontbindingsdomein 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 bewijs lemma 5.4.8.

5.4.3 Twee elementen $a, b \in R$ noemt men wel **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 5.4.4 Zij R een ontbindingsdomein. Laat $a, b \in R$ met priemontbinding:

$$a = u \cdot \prod_{p \in P} p^{n(p)}, \quad b = v \cdot \prod_{p \in P} p^{m(p)},$$

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:

$$ggd(a, b) := \prod_{p \in P} p^{\min\{n(p), m(p)\}} \quad (\in R),$$

de *ggd* is slechts op eenheden na (keuze van P (!)) bepaald. Zie opgave 7 voor een verklaring van de terminologie.

5.4.5 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 coëfficiënten a_0, a_1, \dots, a_n van f zijn. We noemen d de **inhoud** van f , notatie:

$$inh(f) := ggd(a_0, a_1, \dots, a_n),$$

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 coëfficiënten uit K .

Lemma 5.4.6 *Elk polynoom $f \neq 0$ uit $K[X]$ kan worden geschreven als:*

$$f = d \cdot f_0, \quad \text{met } d \in K^* \text{ en } f_0 \in R[X] \text{ een primitief polynoom.}$$

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

$$cf \in R[X], \quad \text{en } cf = \text{inh}(cf) \cdot f_0 \quad \text{met } f_0 \in R[X]$$

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 5.4.6 bewezen. \square

Uit het volgende lemma zien we, hoe de in 5.4.6 aangegeven schrijfwijze zich gedraagt als we producten van polynomen gaan vormen.

Lemma 5.4.7 *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 coëfficiënten c_k van $f \cdot g$ deelt: $c_k \in Rp$ voor alle k . Laat nu $\bar{f} = \sum \bar{a}_i X^i \in (R/pR)[X]$ en $\bar{g} = \sum \bar{b}_j X^j \in (R/pR)[X]$ (hier $\bar{a} = (a \bmod pR) \in R/pR$, voor $a \in R$). Dan geldt in $(R/pR)[X]$:

$$\bar{f} \cdot \bar{g} = \left(\sum \bar{a}_i X^i \right) \cdot \left(\sum \bar{b}_j X^j \right) = \sum \bar{c}_k X^k = \sum \bar{0} \cdot X^k = \bar{0}.$$

Omdat Rp een priemideaal van R is (stelling 5.3.3), is R/pR een domein, en dan is ook $(R/pR)[X]$ een domein. Maar een domein heeft geen nuldelers, dus het product $\bar{f} \cdot \bar{g}$ kan alleen nul zijn als een der factoren \bar{f} of \bar{g} nul is; laten we zeggen \bar{f} . Dan zijn alle \bar{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 5.4.7 bewezen. \square

Lemma 5.4.8 *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, \dots, p_s irreducibele elementen uit R zijn, en g_1, g_2, \dots, 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 ontbindingsdomein 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 $g_1, g_2, \dots, g_t \in K[X]$ irreducibel. Verder is deze schrijfwijze op volgorde en elementen van K^* na eenduidig bepaald. Schrijf nu elke g_i in de door lemma 5.4.6 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 $f = d g_1 g_2 \cdots g_t$ geldt hetzelfde voor d .

Merk op dat, met de g_i , ook het product $g_1 g_2 \cdots g_t$ primitief is, wegens 5.4.7. Dus $f = d \cdot (g_1 g_2 \cdots g_t)$ is de eenduidig bepaalde schrijfwijze uit 5.4.6. 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 :

$$d = u \cdot p_1 p_2 \cdots p_s \quad (u \in R^*, \quad s \in \mathbb{Z}_{\geq 0}, \quad p_i \in R \text{ irreducibel})$$

(dit is weer uniek, op volgorde en R^* na), dan vinden we de verlangde schrijfwijze $f = u p_1 p_2 \cdots p_s g_1 g_2 \cdots g_t$. De eenduidigheid hebben we in de loop van het bewijs gezien. Hiermee is 5.4.8 bewezen. \square

5.4.9 Bewijs van stelling 5.4.1

Zij $f \in R[X]$, $f \neq 0$. We gaan bewijzen dat de ontbinding van f die door lemma 5.4.8 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 5.4.8. 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 5.4.8 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 5.4.1 bewezen. \square

Aan dit bewijs verbinden we nog diverse conclusies.

Gevolg 5.4.10 *Zij R een ontbindingsdomein met quotiëntenlichaam K , en $f \in R[X]$ een primitief polynoom. Dan geldt:*

f is irreducibel in $K[X]$ \iff f is irreducibel in $R[X]$.

Bewijs. \Leftarrow : We hebben net gezien dat elke irreducibele $f \in R[X]$ óf irreducibel in $K[X]$ is, óf een irreducibel element uit R is; maar het laatste geval valt uit 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 5.4.10 bewezen. \square

Gevolg 5.4.11 (Lemma van Gauss) *Zij R een ontbindingsdomein 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 5.4.6 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 5.4.7. 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: $g = u^{-1} \cdot ug \in R[X]$, $h = v^{-1} \cdot vh \in R[X]$. Dit bewijst 5.4.11. \square

5.5 Het factoriseren van polynomen

We bespreken enkele praktische methoden om polynomen in factoren te ontbinden.

5.5.1 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 3.5.2 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: $K = \mathbb{F}_3$, $f = X^3 + X + \bar{1}$; dan $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{0}$, $f(\bar{2}) = \bar{1}\bar{1} = \bar{2}$, dus $\bar{1}$ is het enige nulpunt van f in K .
- c. als $K = \mathbb{Q}$, dan mogen we aannemen dat f primitief is:

$$f = a_n X^n + \dots + a_1 X + a_0, \quad a_i \in \mathbb{Z}, \quad a_n \neq 0, \quad a_0 \neq 0.$$

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 $b, c \in \mathbb{Z}$, $c > 0$, $\text{ggd}(b, c) = 1$. 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.

5.5.2 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 $\mathbb{Q}[X]$.

Bewijs: een ontbinding $f = g \cdot h$ in $\mathbb{Z}[X]$ zou een ontbinding $\bar{f} = \bar{g} \cdot \bar{h}$ van $\bar{f} = (f \bmod p)$ in $\mathbb{F}_p[X]$ geven, tegenspraak. Dus f is irreducibel in $\mathbb{Z}[X]$, en wegens het lemma van Gauss dan ook in $\mathbb{Q}[X]$.

Voorbeeld: $f = X^4 + 3X^3 - X^2 - X + 27$. Kies $p = 2$. Het polynoom $\bar{f} = X^4 + X^3 + X^2 + X + \bar{1}$ 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. $X^2 + X + \bar{1}$. Er volgt dat f irreducibel is in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

Ook als \bar{f} niet irreducibel is levert deze methode informatie. Voorbeeld: $f = X^4 - X^2 + X + 2$. Met methode 5.5.1(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 $\bar{f} = \bar{g} \cdot \bar{h}$ in $\mathbb{F}_2[X]$. Maar in $\mathbb{F}_2[X]$ splitst \bar{f} in de irreducibele factoren X en $X^3 + X + \bar{1}$, dus \bar{f} kan niet ontbonden worden in tweedegraads factoren. Conclusie: f is irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

5.5.3 Het kenmerk van Eisenstein (Gotthold Eisenstein, Duits wiskundige, 1823-1852). Laat R een ontbindingsdomein zijn, p een irreducibel element van R , en

$$f = a_n X^n + \dots + a_1 X + a_0 \in R[X], \quad n > 0.$$

We zeggen dat f een **Eisensteinpolynoom** (bij p) is als geldt:

$$\begin{aligned} p \nmid a_n, \\ p \mid a_i \quad & \text{voor } i = 0, 1, \dots, n-1, \\ p^2 \nmid a_0 \quad & \text{(maar } p \mid a_0). \end{aligned}$$

5.5.4 Belangrijke eigenschap: een Eisensteinpolynoom f is irreducibel in $K[X]$ (met $K = \text{quotiëntenlichaam van } R$) en, als f primitief is, ook in $R[X]$.

Bewijs. Omdat $\text{inh}(f)$ niet door p deelbaar is, is ook het primitieve polynoom $f/\text{inh}(f)$ een Eisensteinpolynoom. Zonder beperking der algemeenheid

mogen we dus aannemen dat f primitief is. Stel nu

$$f = g \cdot h, \quad g, h \in R[X], \quad \text{graad}(g) > 0, \quad \text{graad}(h) > 0.$$

In $(R/pR)[X]$ geldt wegens $p \nmid a_n$, $p \mid a_i$ ($i = 0, 1, \dots, n-1$):

$$\bar{f} = (f \bmod p) = \bar{a}_n X^n \quad \text{met} \quad \bar{a}_n = (a_n \bmod p) \neq 0,$$

en bovendien

$$\bar{f} = \bar{g} \cdot \bar{h}, \quad \text{graad}(\bar{g}) > 0, \quad \text{graad}(\bar{h}) > 0.$$

Dit kan alleen als

$$\bar{g} = \bar{b}X^k, \quad \bar{h} = \bar{c}X^\ell$$

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 5.4.10). Einde bewijs.

Voorbeeld 5.5.5 $R = \mathbb{Z}$, $f = X^5 + 2X^3 - 6$; dit is een Eisensteinpolynoom bij $p = 2$, dus irreducibel.

$R = \mathbb{R}[Y]$, $f = X^3 + (Y^4 - 1)X - (Y^2 + 1)$: dit is 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 $p = Y - 1$.

5.5.6 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 5.5.1(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

- i. $b_2 c_2 = a_4$
- ii. $b_2 c_1 + b_1 c_2 = a_3$
- iii. $b_2 c_0 + b_1 c_1 + b_0 c_2 = a_2$
- iv. $b_1 c_0 + b_0 c_1 = a_1$
- v. $b_0 c_0 = a_0$.

Voor b_2, c_2, b_0, c_0 zijn er wegens i. en v. slechts eindig veel mogelijkheden: voor vaste b_2, c_2, b_0, c_0 kan men $b_1 c_1$ uit iii. 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 5.5.7 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.

5.6 Opgaven

1. We beschouwen de ring:

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

- a. Bewijs dat $2, 3 \in R$ irreducibel zijn.

Aanwijzing: gebruik, zie 1.13, de afbeelding

$$N : R \rightarrow \mathbb{Z}, \quad N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Deze heeft de eigenschap

$$r \in R^* \Leftrightarrow N(r) = \pm 1.$$

- b. Bewijs dat R_2 en R_3 geen priemidealen zijn. Is R een ontbindingsdomein?
- c. Is dit niet in tegenspraak met stelling 5.2.3 ?
- 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. Zij R de ring van polynoomfuncties op de cirkel:

$$R = \mathbb{R}[X, Y]/I, \quad I = (X^2 + Y^2 - 1),$$

en zij $x := X + I$, $y := Y + I \in R$.

- a. Bewijs dat $x - 1$ en $y - 1$ irreducibel zijn in R . (Aanwijzing: gebruik de afbeelding $N : R \rightarrow \mathbb{R}[X]$ uit opgave 19 op blz. 71.)
- b. Bewijs dat $(x - 1)$ en $(y - 1)$ geen priemidealen zijn en dat R geen ontbindingsring is.
- c. Laat zien dat $a = (x + y - 1)^2 = 2(x - 1)(y - 1)$ twee verschillende ontbindingen van a als product van irreducibele elementen (en een eenheid 2) zijn.
- d. Teken een plaatje met de cirkel en de lijnen $X + Y - 1 = 0$, $X - 1 = 0$ en $Y - 1 = 0$. Probeer zelf elementen in R te vinden die twee verschillende ontbindingen in irreducibele elementen toelaten.

3. Geef van elk van de volgende elementen van $\mathbb{Z}[\sqrt{-3}]$ aan of ze irreducibel zijn en of ze een priemideaal voortbrengen :

$$\sqrt{-3}, 1, 2, 1 + \sqrt{-3}, 5.$$

4. Zij $R = \{\sum a_i X^i \in \mathbb{Q}[X] : a_1 = 0\}$, zie voorbeeld 5.1.5.

- a. Zij

$$\Phi_0 : R \longrightarrow \mathbb{R}, \quad f \mapsto f(0)$$

het evaluatiehomomorfisme in 0. Bewijs dat

$$\ker(\Phi_0) = (X^2, X^3) = \{f = X^2g + X^3h \in R : g, h \in R\}.$$

- b. Bewijs dat $\ker(\Phi_0)$ geen hoofdideaal is, maar wel een maximaal ideaal is.

5. Laat $R = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z}, b \text{ oneven}\}$. 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 2, op eenheden na, het enige irreducibele element van R is. Is $2R$ een priemideaal?

6. Zij $R = \mathbb{Z}[X]/(5X, X^2)$.

- a. Bewijs dat elk element van R op eenduidige wijze geschreven kan worden als

$$\bar{a} + \bar{b} \cdot \bar{X} \quad \text{met} \quad a \in \mathbb{Z}, b \in \mathbb{Z}, 0 \leq b < 5.$$

waarbij $\bar{}$ de restklasse modulo $(5X, X^2)$ aangeeft.

- b. Bewijs: $\bar{a} + \bar{b}\bar{X} \in R^* \iff a \in \{\pm 1\}$.

- c. Bewijs: als $\alpha = \bar{X}$, $\beta = \bar{2} \cdot \bar{X}$, dan geldt

$$R \cdot \alpha = R \cdot \beta \quad \text{en} \quad \alpha \notin R^* \cdot \beta.$$

7. Zij R een ontbindingsdomein en zij $d \in R$ de ggd van $a, b \in R$: $d = ggd(a, b)$. 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.

8. Ontbind $X^8 - 16$ en $X^6 + 27$ in irreducibele factoren in $\mathbb{Q}[X]$.

9. Is $5X^4 + 10X + 10$ een Eisensteinpolynoom in $\mathbb{Z}[X]$? Is het irreducibel in $\mathbb{Z}[X]$? en in $\mathbb{Q}[X]$?
10. 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 $n \in \mathbb{Z}_{\geq 0}$.
11. 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.
12. Zij R een ontbindingsdomein. Bewijs dat

$$\cup_{n \geq 0} R[X_1, X_2, \dots, X_n]$$

een ontbindingsdomein is.

13. Ontbind de volgende polynomen in irreducibel factoren in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$:

$$\begin{aligned} &4X^2 + 4, \\ &2X^{10} + 4X^5 + 3, \\ &X^4 - 7X^2 + 5X - 3, \\ &X^{111} + 9X^{74} + 27X^{37} + 27, \\ &X^3 + X + 3. \end{aligned}$$

14. Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$:

$$\begin{aligned} &\frac{1}{7}((X+1)^7 - X^7 - 1), \\ &X^3 + 3X^2 + 6X + 9, \\ &X^4 + 2X^3 + 3X^2 + 9X + 6, \\ &X^{12} - 1, \\ &X^4 - X^3 + X^2 - X + 1. \end{aligned}$$

15. Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Q}[X, Y]$:

$$\begin{aligned} &Y^4 + X^2 + 1, \\ &Y^3 - (X+1)Y^2 + Y + X(X-1), \\ &X^n + Y^3 + Y \quad (n \geq 1), \\ &X^4 + 4Y^4, \\ &X^4 + 2X^3 + X^2 - Y^2 - 2Y - 1, \\ &Y^n - 13X^4 \quad (n \geq 1). \end{aligned}$$

16. Zij $I \subset \mathbb{Z}[X]$ een priemideaal.
- Bewijs dat $I \cap \mathbb{Z}$ een priemideaal in \mathbb{Z} is.
 - 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.
 - Bepaal alle maximale idealen van $\mathbb{Z}[X]$.
17. Stel dat n een positief geheel getal is waarvoor $n^4 + 4^n$ een priemgetal is. Bewijs dat $n = 1$.
18. 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.
19. Bepaal alle irreducibele polynomen $f \in \mathbb{F}_2[X]$ met graad $(f) \leq 3$.
20. Zij $R = \mathbb{C}[U, V]/(UV - 1)$.

- Bewijs dat

$$\mathbb{C}[T, T^{-1}] := \left\{ \frac{f(T)}{T^i} \in \mathbb{C}(T) : f(T) \in \mathbb{C}[T], i \in \mathbb{Z} \right\}$$

een deelring van het lichaam $\mathbb{C}(T)$ is.

- Bewijs dat $R \cong \mathbb{C}[T, T^{-1}]$.
- Bewijs dat R een hoofdideaaldomein is.
- Bewijs dat $R \cong \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ (hint: $X^2 + Y^2 = (X + iY)(X - iY)$).
- Bepaal een $r \in \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ met $(r) = (x - 1, y)$ waarin $x := X + (X^2 + Y^2 - 1)$ en $y = Y + (X^2 + Y^2 - 1)$. (vergelijk opgave 19 op blz. 71).

6 Modulen

6.1 Definities

Het analogon van lineaire ruimten over een lichaam zijn modulen over een ring.

Definitie 6.1.1 Zij R een (unitaire) ring. Een **links- R -moduul** M is een abelse (optel)groep (we schrijven ‘+’ voor de groepsoperatie), met een **actie** van een ring R , d.w.z. er is een afbeelding:

$$R \times M \longrightarrow M, \quad (a, m) \mapsto am,$$

zodanig dat voor alle $a, b \in R$ en alle $m, n \in M$ geldt:

$$\text{(RM1)} \quad a(m + n) = am + an,$$

$$\text{(RM2)} \quad (a + b)m = am + bm,$$

$$\text{(RM3)} \quad a(bm) = (ab)m,$$

$$\text{(RM4)} \quad 1m = m.$$

Een **rechts- R -moduul** wordt analoog gedefinieerd, maar dan met een actie $M \times R \rightarrow M$ et cetera.

Opmerking 6.1.2 Tenzij anders vermeld zijn alle modulen die we beschouwen links- R -modulen en we schrijven gewoon R -modulen.

6.1.3 Voorbeelden.

- a. Zij $R = K$, een lichaam. Dan zijn de axioma’s voor een links- R -moduul precies de axioma’s voor een lineaire ruimte over K .
- b. Zij K een lichaam. De ring R van $n \times n$ matrices met coëfficiënten in K werkt op de optelgroep $(K^n)^+$ van de lineaire ruimte K^n :

$$R = M(n, K), \quad M = (K^n)^+ \quad \text{met actie} \quad (A, \vec{v}) \mapsto A\vec{v},$$

het gebruikelijke product van een matrix met een vector. Hiermee is K^n een links- $M(n, K)$ -moduul.

- c. Zij $R = \mathbb{Z}$ en zij $M = G$ een abelse groep. Definieer $0g := 0$, $(-1)g := -g$ met $0 \in G$ het eenheidselement en met $-g$ de inverse van g in G . Definieer vervolgens $ng := g + g + \dots + g$ (n keer) en $(-n)g = (-g) + (-g) + \dots + (-g)$ ($n \times$) als $n \geq 1$. Ga na dat G op deze wijze een \mathbb{Z} -moduul is.

- d. Zij R een ring en zij $I \subset R$ een ideaal. Dan is I een R -moduul. Bovendien is R/I ook een R -moduul, met actie:

$$R \times R/I \longrightarrow R/I \quad (r, a + I) \mapsto ra + I.$$

Merk op dat dus geldt: $r\bar{a} := ra + I = \overline{ra}$.

Opmerking 6.1.4 Uit de axioma's van links- R -moduul volgt:

$$0m = (0 + 0)m = 0m + 0m \quad \text{dus} \quad 0m = 0.$$

Verder geldt:

$$0 = (a + (-a))m = am + (-a)m \quad \text{dus} \quad (-a)m = -(am),$$

i.h.b. geldt $(-1)m = -(1m) = -m$, dus $a(-m) = a((-1)m) = (a(-1))m = (-a)m$, hetgeen de notatie $-am$ voor $(-a)m = -(am) = a(-m)$ rechtvaardigt.

Definitie 6.1.5 Een **deelmoduul** N van een links- R -moduul M is een ondergroep van M die gesloten is onder de actie van R . Precieser, een $N \subset M$ met voor alle $a, b \in N$ en alle $r \in R$:

$$\text{(DM1)} \quad 0 \in N, \quad a - b \in N,$$

$$\text{(DM2)} \quad ra \in N, \quad \text{we schrijven hiervoor ook wel } rN \subseteq N.$$

Een deelmoduul N van een R -moduul M is zelf ook een R -moduul.

6.1.6 Voorbeelden.

- Zij $R = K$, een lichaam, en zij M een lineaire ruimte over K . De deelmodulen van M zijn precies de lineaire deelruimten van M .
- De enige deelmodulen van het $M(n, K)$ -moduul K^n zijn $\{\vec{0}\}$ en K^n . Als immers $\vec{x}, \vec{y} \in K^n - \{\vec{0}\}$ dan is er een $A \in M(n, K)$ met $A\vec{x} = \vec{y}$ (ga na).
- De deelmodulen van het \mathbb{Z} -moduul G , met G een abelse groep, zijn precies de ondergroepen van G (ga na).
- De ring R is zelf een R -moduul, en de R -deelmodulen van R zijn precies de idealen van R (ga na).
- Zij $A \in M(n, K)$, K een lichaam en zij $R = K[A] = \{\sum_{i < \infty} a_i A^i : a_i \in K\}$. Zij $\vec{v} \in K^n$ een eigenvector van A met eigenwaarde $\lambda \in K$. Dan is de (één dimensionale) deelruimte $K\vec{v} = \langle \vec{v} \rangle$ een deelmoduul van het R -moduul K^n . Immers, een deelruimte is een optelgroep en omdat \vec{v} een eigenvector is, geldt $A\vec{v} = \lambda\vec{v} \in \langle \vec{v} \rangle$ zodat ook $(\sum_{i < \infty} a_i A^i)\langle \vec{v} \rangle \subset \langle \vec{v} \rangle$.

6.2 R -moduulhomomorfismen

De R -moduulhomomorfismen zijn de generalisatie van de lineaire afbeeldingen.

Definitie 6.2.1 Zij R een ring en laat M, N (links)- R -modulen zijn. Een **R -moduulhomomorfisme** is een afbeelding

$$f : M \longrightarrow N,$$

die een homomorfisme van abelse groepen is en die R -lineair is, preciezer, voor alle $x, y \in M$ en alle $r \in R$ voldoet f aan:

$$(H1) \quad f(x + y) = f(x) + f(y),$$

$$(H2) \quad f(rx) = rf(x).$$

In het bijzonder geldt: $f(0) = 0$.

Een **R -moduulisomorfisme** is een bijectief R -moduulhomomorfisme. (Gana dat de inverse van een R -moduulisomorfisme weer een (bijectief) R -moduulhomomorfisme is, d.w.z. de inverse is ook een R -moduul isomorfisme.) De **kern** van een R -moduulhomomorfisme $f : M \rightarrow N$ is gedefinieerd door:

$$\ker(f) := \{m \in M : f(m) = 0 (\in N)\}.$$

Het **beeld** van een R -moduulhomomorfisme is gedefinieerd door

$$\text{beeld}(f) = \text{im}(f) = f[M] = \{f(m) \in N : m \in M\}.$$

6.2.2 Voorbeelden.

- a. Omdat $0 = \{0\} \subset R$ een R -moduul is (het is immers een ideaal van R) zijn de afbeeldingen

$$0 \longrightarrow M, \quad M \longrightarrow 0$$

R -moduulhomomorfismen (de eerste afbeelding stuurt ten gevolge van de definitie van R -moduulhomomorfisme 0 naar $0 \in M$, de tweede stuurt uiteraard elke $m \in M$ naar 0).

- b. Voor een commutatieve ring R en een R -moduul M en een $a \in R$ definieert

$$\phi_a : M \longrightarrow M, \quad m \mapsto am,$$

een R -moduulhomomorfisme.

- c. Een homomorfisme $f : G \rightarrow H$ van abelse groepen is een \mathbb{Z} -moduulhomomorfisme, immers $f(2g) = f(g+g) = f(g) + f(g) = 2f(g)$ etc.
- d. Zij R een ring en zij I een ideaal, dan zijn R en R/I beide R -modulen. De kanonieke afbeelding (een ringhomomorfisme):

$$\phi : R \longrightarrow R/I, \quad m \mapsto \bar{m} = m + I,$$

is een R -moduulhomomorfisme. Aan eis (H1) is voldaan omdat ϕ een ringhomomorfisme en dus een homomorfisme van optelgroepen is. Verder geldt (zie 6.1.3):

$$\phi(rm) := rm + I = r\phi(m), \quad (r, m \in R)$$

zodat ook aan (H2) voldaan is.

Stelling 6.2.3 *Zij $f : M \rightarrow N$ een R -moduulhomomorfisme. Dan geldt:*

- a. $\ker(f)$ is een deelmoduul van M .
- b. $\text{im}(f)$ is een deelmoduul van N .

Bewijs. De bewijzen van de twee uitspraken volgen direct uit de definities (ga na). □

6.3 Direkte sommen

In deze paragraaf zijn alle modulen links-modulen.

6.3.1 Zij R een ring en zij M_i een R -moduul voor iedere $i \in I$, waarbij I een index verzameling is (bv. $I = \{1, 2, \dots, n\}$ of $I = \mathbb{Z}$). De **direkte som** M van de M_i is gedefinieerd door:

$$M = \bigoplus_{i \in I} M_i := \left\{ (\dots, x_i, \dots)_{i \in I} : \text{slechts eindig veel } x_i \neq 0 \right\}.$$

Op deze verzameling definiëren we de structuur van een R -moduul door:

$$\begin{aligned} (\dots, x_i, \dots) + (\dots, y_i, \dots) &= (\dots, z_i, \dots), & \text{met } z_i &= x_i + y_i \quad \forall i \in I \\ 0 &= (\dots, 0, \dots), & \text{d.w.z. } x_i &= 0 \quad \forall i \in I \\ r \cdot (\dots, x_i, \dots) &= (\dots, z_i, \dots) & \text{met } z_i &= rx_i \quad \forall i \in I. \end{aligned}$$

Ga na dat deze regels inderdaad een R -moduul definiëren.

Definitie 6.3.2 Een R -moduul F heet **vrij** (ook wel een vrij R -moduul) indien er een verzameling I bestaat en een isomorfisme van R -modulen:

$$F \xrightarrow{\cong} \bigoplus_{i \in I} R.$$

Hierbij namen we voor de M_i uit 6.3.1 steeds R .

In het bijzonder is $\bigoplus_{i \in I} R$ voor iedere niet-lege I een vrij R -moduul. We definiëren voor elke $i \in I$:

$$e_i = (\dots, x_j, \dots)_{j \in I} \in \bigoplus_{i \in I} R \quad \text{door: } x_i = 1, \quad x_j = 0 \text{ als } i \neq j.$$

Iedere $x \in F$ is dan, op unieke wijze, te schrijven als:

$$x = \sum_{i \in I} x_i e_i, \quad (x, e_i \in F, \quad x_i \in R),$$

waarbij slechts eindig veel $x_i \neq 0$ zijn.

Voor $n \in \mathbb{Z}_{\geq 1}$ definieert men een vrij R -moduul:

$$R^n := \bigoplus_{i \in \{1, 2, \dots, n\}} R.$$

6.3.3 Voorbeelden. Als K een lichaam is, dan is K^n de bekende lineaire ruimte over K .

De polynoomring $R[X]$ kan gezien worden als een R -moduul (gebruikelijke optelling en scalaire vermenigvuldiging). De afbeelding:

$$\phi : R[X] \longrightarrow F := \bigoplus_{i \in \mathbb{Z}_{\geq 0}} R, \quad \sum_{i=0}^n a_i X^i \mapsto (a_0, a_1, \dots, a_n, 0, 0, \dots),$$

geeft een isomorfisme van R -modulen; ϕ is surjectief omdat slechts eindig veel x_i ongelijk nul zijn in een element $(\dots, x_i, \dots) \in F$.

6.3.4 Als R *niet-commutatief* is, dan blijkt het mogelijk te zijn (zie opgave 7), dat:

$$R \cong R^2 \quad (!).$$

Als R commutatief is, dan kan zoiets niet gebeuren:

Stelling 6.3.5 *Zij R een commutatieve (unitaire) ring; $R \neq (0)$. Dan geldt:*

$$R^m \cong R^n \quad \implies \quad m = n.$$

Men noemt m ($= n$) dan wel de rang van het R -moduul R^m . Algemener geldt:

$$R^m \cong \bigoplus_{i \in I} R \quad \implies \quad m = \#I.$$

Bewijs. Een bewijs van deze stelling dat gebaseerd is op de bekende regel $\det(AB) = \det(A)\det(B)$ voor determinanten van $n \times n$ matrices, is te vinden in Section 3.4 van het boek N. Jacobson, Basic Algebra I. Het voordeel van dat bewijs is dat het geen gebruik maakt van het Lemma van Zorn, wat we in het onderstaande bewijs wel doen (we gebruiken namelijk het bestaan van een maximaal ideaal in een commutatieve ring).

Neem aan dat $\phi : R^m \rightarrow R^n$ een R -moduulisomorfisme is. Zij M een maximaal ideaal in R . Dan is $M^m = \bigoplus_{i=1}^m M$ een deelmoduul van R^m . De factorgroep R^m/M^m is op een natuurlijke manier een $K = R/M$ -moduul, en dus, omdat K een lichaam is, een lineaire ruimte over K . Men gaat eenvoudig na dat de afbeelding

$$(r_1, \dots, r_m) + M^m \mapsto (r_1 + M, \dots, r_m + M)$$

een welgedefinieerd isomorfisme tussen de lineaire ruimten R^m/M^m en K^m over K geeft. Er volgt dus dat $\dim_K(R^m/M^m) = m$.

Het beeld $\phi(M^m)$ is een deelmoduul van R^n . De factorgroep $R^n/\phi(M^m)$ is dan een R -moduul, en zelfs een K -moduul: immers, is $m \in M$ en $v \in R^n$, dan is $mv = \phi\phi^{-1}(mv) = \phi(m\phi^{-1}(v)) \in \phi(M^m)$. Met andere woorden, de vermenigvuldiging van een klasse $v + \phi(M^m) \in R^n/\phi(M^m)$ met een element $r \in R$ hangt alleen van de klasse van r in $R/M = K$ af, oftewel anders gezegd, $R^n/\phi(M^m)$ is een K -moduul. Het isomorfisme ϕ induceert een isomorfisme $R^m/M^m \cong R^n/\phi(M^m)$ van lineaire ruimten over K , dus in het bijzonder $\dim_K(R^n/\phi(M^m)) = m$.

Iedere $x \in R^n$ is op unieke wijze te schrijven als:

$$\begin{aligned} x &= (x_1, x_2, \dots, x_n) \\ &= x_1 \cdot (1, 0, \dots, 0) + x_2 \cdot (0, 1, 0, \dots, 0) + \dots + x_n \cdot (0, 0, \dots, 1) \\ &= x_1 e_1 + x_2 e_2 + \dots + x_n e_n, \end{aligned}$$

analoog aan de schrijfwijze in een lineaire ruimte. Bijgevolg wordt de lineaire ruimte $R^n/\phi(M^m)$ over K opgespannen door de klassen $e_1 + \phi(M^m), \dots, e_n + \phi(M^m)$. We concluderen hieruit dat $n \geq \dim_K(R^n/\phi(M^m)) = m$.

Als we in het hierboven gegeven bewijs de rol van R^n en R^m verwisselen en ϕ door ϕ^{-1} vervangen, volgt geheel analoog dat ook $m \geq n$. Met andere woorden, $n = m$. De algemenere uitspraak in de stelling volgt geheel analoog. Hiermee is de stelling 6.3.5 is bewezen. \square

6.3.6 We hebben al gezien dat modulen over een lichaam K lineaire ruimten zijn. I.h.b. geldt: als K^n de direkte som is van twee modulen:

$$K^n \cong V \oplus W \implies V \cong K^a, \quad W \cong K^{n-a},$$

voor zekere a omdat V en W immers ook (eindig dimensionale) lineaire ruimten zijn. Bij modulen over een ring is de situatie veel interessanter. Een eenvoudig voorbeeld daarvan is:

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad n + 6\mathbb{Z} \mapsto (n + 2\mathbb{Z}, n + 3\mathbb{Z})$$

hierbij nemen we $R = \mathbb{Z}/6\mathbb{Z}$ (zie 2.3.12). Met de chinese reststelling kunnen we, geheel analoog, nog meer voorbeelden construeren. Een interessanter voorbeeld is het volgende.

Voorbeeld 6.3.7 We beschouwen de deelring R van de ring van C^∞ -functies op \mathbb{R} bestaande uit de periodieke functies met periode 2π :

$$R := \{f \in C^\infty(\mathbb{R}) : f(x + 2\pi) = f(x) \quad \forall x \in \mathbb{R}\}.$$

Merk op dat R geïdentificeerd kan worden met de ring van C^∞ functies op de cirkel S^1 . Zij M het R -moduul gedefinieerd door:

$$M := \{m \in C^\infty(\mathbb{R}) : m(x + 2\pi) = -m(x) \quad \forall x \in \mathbb{R}\},$$

dan is M een (optel)groep (het is een ondergroep van $C^\infty(\mathbb{R})^+$) en de actie van R wordt gegeven door de vermenigvuldiging in de ring $C^\infty(\mathbb{R})$:

$$\begin{aligned} (m + n)(x) &:= m(x) + n(x), & m, n \in M, \quad x \in \mathbb{R}, \\ (fm)(x) &:= f(x)m(x), & f \in R, m \in M, \quad x \in \mathbb{R}, \end{aligned}$$

merk op dat $fm \in M$ (!) en ga na dat M inderdaad een R -moduul is. De bekende formules voor sinus en cosinus laten zien dat de volgende functies in het moduul M zitten:

$$\forall a \in \mathbb{R} : C_a, S_a \in M, \quad \text{met} \quad \begin{cases} C_a : \mathbb{R} \rightarrow \mathbb{R}, & x \mapsto \cos \frac{x-a}{2}, \\ S_a : \mathbb{R} \rightarrow \mathbb{R}, & x \mapsto \sin \frac{x-a}{2}. \end{cases}$$

We laten nu zien dat:

$$M \not\cong R, \quad \text{maar wel : } M \oplus M \cong R^2,$$

en we bewijzen ook dat M niet vrij is.

Stel er bestaat een R -moduulisomorfisme:

$$\phi : R \longrightarrow M, \quad \text{dan} \quad \phi(f) = f \cdot \phi(1),$$

met $1 \in R$ de functie die overal de waarde 1 heeft. We schrijven $g := \phi(1) \in M$. Omdat g continu is en $g(2\pi) = -g(0)$ heeft g tenminste één nulpunt in het interval $[0, 2\pi]$. Zij $a \in [0, 2\pi]$ zo'n nulpunt.

Omdat ϕ ook surjectief is, is iedere $m \in M$ dan te schrijven als $m = \phi(f)$ dus:

$$m = fg, \quad \text{i.h.b.} \quad m(a) = f(a)g(a) = 0.$$

Iedere $m \in M$ moet dus een nulpunt in a hebben. Nemen we $m = C_a \in M$ dan is echter $C_a(a) = \cos \frac{a-a}{2} = 1 \neq 0$, een tegenspraak. We concluderen dat er géén isomorfisme $\phi : R \rightarrow M$ bestaat, waarmee de eerste uitspraak bewezen is.

We definiëren een R -moduulhomomorfisme:

$$\psi : R^2 \longrightarrow M \oplus M, \quad (f, g) \mapsto (fC_0 + gS_0, -fS_0 + gC_0)$$

(ga na dat ψ inderdaad een R -moduulhomomorfisme is). In termen van matrices (met coëfficiënten in het R -moduul M) wordt ψ gegeven door:

$$A := \begin{pmatrix} C_0 & S_0 \\ -S_0 & C_0 \end{pmatrix}, \quad \text{i.h.b.} \quad A^{-1} = \begin{pmatrix} C_0 & -S_0 \\ S_0 & C_0 \end{pmatrix},$$

waarbij we gebruiken dat $C_0^2 + S_0^2 = 1$, immers $(\cos \frac{x}{2})^2 + (\sin \frac{x}{2})^2 = 1$ voor alle $x \in \mathbb{R}$. (De berekening van de determinant kan eigenlijk niet plaats vinden in M , omdat er immers geen product van elementen van M gedefinieerd is. Het resultaat 1 zit ook niet in M (!). We gebruiken echter dat $M \subset C^\infty(\mathbb{R})$, een ring.)

De inverse van ψ wordt dan hopelijk gegeven door:

$$\psi^{-1} : M \oplus M \longrightarrow R^2, \quad (m, n) \mapsto (C_0m - S_0n, S_0m + C_0n)$$

(merk op dat $C_0m \in R$ (!) etc.). Ga na dat inderdaad $\psi^{-1}\psi = \text{id}_{R^2}$ en $\psi\psi^{-1} = \text{id}_{M \oplus M}$ (dit moet men echt nagaan; onze argumenten waren immers heuristisch).

Tenslotte bewijzen we dat M niet vrij is.

$$\text{Als } F := \bigoplus_{i \in I} R \xrightarrow{\cong} M, \quad \text{dan } F \oplus F \cong M \oplus M \cong R^2.$$

Omdat $F \oplus F$ vrij is, met indexverzameling $I \amalg I$, volgt uit stelling 6.3.5 dat $\# I \amalg I = 2$, dus $\# I = 1$ en $F = R$. Maar we hebben al gezien dat $R \not\cong M$, dus is M niet vrij. Hiermee is de laatste uitspraak bewezen.

Opmerking 6.3.8 We proberen een ‘meetkundige’ verklaring voor het voorbeeld hierboven te geven. Om te beginnen kunnen we de ring R , wegens de periodiciteit van de functies in R , opvatten als de ring van C^∞ functies op de cirkel

$$S^1 := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}, \quad R = C^\infty(S^1, \mathbb{R}) = C^\infty(S^1).$$

Maar we willen er anders tegenaan kijken. Een functie g in het R -moduul R zullen we opvatten als een afbeelding

$$\tilde{g} : S^1 \mapsto \mathcal{C} := S^1 \times \mathbb{R}, \quad t \mapsto (t, g(t)).$$

merk op dat $\tilde{g}(S^1)$ nu de ‘grafiek’ van de functie g is. We kunnen

$$\mathcal{C} = S^1 \times \mathbb{R} \subset \mathbb{R}^2 \times \mathbb{R} = \mathbb{R}^3$$

zien als een cylinder in \mathbb{R}^3 , (de lijnen door $(x, y, 0)$ met $x^2 + y^2 = 1$ evenwijdig aan de z -as). Er is een projectie:

$$\pi_{\mathcal{C}} : \mathcal{C} \longrightarrow S^1, \quad (t, u) \mapsto t, \quad t \in S^1, u \in \mathbb{R}.$$

Voor iedere $t \in S^1$ noemen we $\pi_{\mathcal{C}}^{-1}(t)$ de **vezel** van $\pi_{\mathcal{C}}$ boven t , de vezel boven t is dus de lijn evenwijdig aan de z -as door het punt $(t, 0)$. Men noemt \mathcal{C} wel een vezelbundel over S^1 . Voor iedere $t \in S^1$ en $g \in R$ geldt:

$$\pi_{\mathcal{C}}\tilde{g}(t) = \pi_{\mathcal{C}}(t, g(t)) = t, \quad \text{dus} \quad \pi_{\mathcal{C}}\tilde{g} = \text{id}_{S^1}.$$

Men noemt algemener een $\tilde{g} : S^1 \rightarrow \mathcal{C}$ een **sectie** van de vezelbundel \mathcal{C} als aan de eis $\pi_{\mathcal{C}}\tilde{g} = \text{id}_{S^1}$ voldaan is (\tilde{g} voegt dan aan iedere $t \in S^1$ een punt $(t, g(t))$ in $\pi_{\mathcal{C}}^{-1}(t)$ toe).

Deze secties vormen een moduul over R : de som $\tilde{g} + \tilde{h}$ van twee secties van \mathcal{C} en ook het vermenigvuldigen met een $f \in R$ definiëren we vezelsgewijs, dwz. $(\tilde{g} + \tilde{h})(t) := (t, g(t) + h(t))$ en $f\tilde{g}(t) = f \cdot (t, g(t)) := (t, f(t)g(t))$. Al met al zien we dat:

$$R \cong \Gamma(S^1, \mathcal{C}) := \{ \tilde{g} : S^1 \rightarrow \mathcal{C}, \tilde{g} \text{ is } C^\infty, \text{ en } \pi_{\mathcal{C}}\tilde{g} = \text{id}_{S^1} \},$$

waar $g \mapsto \tilde{g}$ een isomorfisme van R -modulen is. We noemen $\Gamma(S^1, \mathcal{C})$ het moduul van C^∞ sneden van de vezelbundel \mathcal{C} . Deze vezelbundel (een cylinder) is nu ons meetkundig beeld van het R -moduul R .

We bekijken nu het moduul M . Omdat $m(x + 2\pi) = -m(x)$ kunnen we m niet opvatten als een functie op S^1 . Merk op dat m geheel bepaald is door zijn restrictie tot het interval $[0, 2\pi]$ (verschuif x over gehele veelvouden van 2π en gebruik $m(x + 2k\pi) = (-1)^k m(x)$). De functie m is dus bepaald door de afbeelding

$$m : [0, 2\pi] \rightarrow [0, 2\pi] \times \mathbb{R}, \quad x \mapsto (x, m(x)).$$

Als we $\{0\} \times \mathbb{R}$ met $\{2\pi\} \times \mathbb{R}$ willen identificeren door $(0, u) = (2\pi, u)$ te eisen (zodat we \mathcal{C} krijgen) dan geeft m , als $m(0) \neq m(2\pi)$ d.w.z. als $m(0) \neq 0$, geen sectie meer van \mathcal{C} . Merk echter op dat dit probleem opgelost wordt door

$(0, u)$ met $(2\pi, -u)$ te identificeren, de verzameling die zo ontstaat noemen we

$$\mathcal{M} := ([0, 2\pi] \times \mathbb{R}) / \sim \quad \text{met} \quad (x, u) \sim (y, v) \Leftrightarrow (|x - y| = 2\pi \text{ en } u = -v).$$

Ook \mathcal{M} kunnen we zien als een vezelbundel, met projectie:

$$\pi_{\mathcal{M}} : \mathcal{M} \longrightarrow S^1, \quad (x, u) \mapsto x,$$

merk op dat we de laatste x interpreteren als een punt van S^1 , en dat $(0, u)$ en $(2\pi, -u)$ hetzelfde beeld in de cirkel hebben, zodat $\pi_{\mathcal{M}}$ goed gedefinieerd is. De vezels van $\pi_{\mathcal{M}}$ zijn steeds reële rechten (wegens de identificatie is ook de vezel boven het punt corresponderende met 0 én 2π ook één reële rechte). Iedere $m \in M$ geeft dan een C^∞ sectie

$$\tilde{m} : S^1 \rightarrow \mathcal{M}, \quad t \mapsto (t, m(t)).$$

Door vezelsgewijs optellen en vezelsgewijs vermenigvuldigen met een $f \in R$ vormen de C^∞ sneden van \mathcal{M} een moduul over R . Op deze wijze krijgen we een isomorfisme van R -modulen:

$$M \cong \Gamma(S^1, \mathcal{M}) := \{ \tilde{m} : S^1 \rightarrow \mathcal{M}, \tilde{m} \text{ is } C^\infty, \text{ en } \pi_{\mathcal{M}} \tilde{m} = \text{id}_{S^1} \},$$

met $m \mapsto \tilde{m}$. De vezelbundel \mathcal{M} is ons meetkundig beeld van het R -moduul M .

Om \mathcal{M} te visualiseren kun je beter eerst \mathbb{R} herschalen, m.b.v. een veelvoud van de bv. de arctangens, tot een interval $(-\epsilon, \epsilon)$, met $0 < \epsilon < 1$. Je moet dan van de ‘rechthoek’ $[0, 2\pi] \times (-\epsilon, \epsilon)$ de zijden $\{0\} \times (-\epsilon, \epsilon)$ en $\{2\pi\} \times (-\epsilon, \epsilon)$ zo aan elkaar plakken dat $(0, u)$ op $(2\pi, -u)$ komt. De zo ontstane figuur heet de **Möbiusband**.

Zoals je ziet zijn de Möbiusband en de cylinder inderdaad verschillend. Het is dan ook niet verbazend dat de R -modulen R en M , bestaande uit de (C^∞) secties van \mathcal{C} en \mathcal{M} respectievelijk, niet isomorf zijn.

We proberen te zien dat R^2 en $M^2 = M \oplus M$ isomorf zijn. We kunnen R^2 identificeren met de C^∞ afbeeldingen:

$$(\tilde{g}, \tilde{h}) : S^1 \longrightarrow \mathcal{T} := S^1 \times \mathbb{R} \times \mathbb{R}, \quad t \mapsto (t, g(t), h(t)) \quad g, h \in R.$$

Wederom is \mathcal{T} een vezelbundel met projectie $\pi_{\mathcal{T}} : \mathcal{T} \rightarrow S^1$ en de vezels zijn nu isomorf met \mathbb{R}^2 . De afbeelding $s := (g, h) \mapsto \tilde{s} := (\tilde{g}, \tilde{h})$ geeft dan een R -moduulisomorfisme:

$$R^2 \cong \Gamma(S^1, \mathcal{T}) := \{ \tilde{s} : S^1 \rightarrow \mathcal{T}, \tilde{s} \text{ is } C^\infty, \text{ en } \pi_{\mathcal{T}} \tilde{s} = \text{id}_{S^1} \},$$

de R -moduulstructuur op $\Gamma(S^1, \mathcal{T})$ is weer via vezelsgewijs optellen en vezelsgewijs vermenigvuldigen met een $f \in R$. De vezelbundel \mathcal{T} is ons meetkundig beeld van het R -moduul R^2 .

We laten zien dat $M \oplus M$ hetzelfde beeld oplevert. Allereerst merken we op dat we \mathcal{M} als ‘deelvezelbundel’ van \mathcal{T} kunnen zien. Daartoe definiëren we:

$$\alpha : \mathcal{M} \longrightarrow \mathcal{T}, \quad (x, u) \mapsto \left(x, u \cos \frac{x}{2}, u \sin \frac{x}{2}\right) = (x, u \vec{f}_1(x))$$

merk op dat $\alpha(0, u) = \alpha(2\pi, -u)$, dus dat α inderdaad welgedefinieerd is. Bovendien reken je makkelijk na dat

$$\alpha_* : M = \Gamma(S^1, \mathcal{M}) \longrightarrow \Gamma(S^1, \mathcal{T}), \quad \tilde{m} \mapsto \alpha_* \tilde{m}$$

een R -moduulhomomorfisme is. Merk op dat geldt:

$$\alpha_* \tilde{m} : x \mapsto (x, m(x) \vec{f}_1(x)), \quad (x \in S^1), \quad \text{en dat} \quad \vec{f}_1(x) = (C_0(x), S_0(x)),$$

met de notatie van het voorbeeld.

Als we in iedere vezel het loodrechte complement van de vezel van $\alpha(\mathcal{M})$ nemen, dan vinden we een tweede deelvezelbundel van \mathcal{T} die ook isomorf is met \mathcal{M} . Precieser, definieer:

$$\beta : \mathcal{M} \longrightarrow \mathcal{T}, \quad (x, v) \mapsto \left(x, -v \sin \frac{x}{2}, v \cos \frac{x}{2}\right) = (x, v \vec{f}_2(x)),$$

dan is het beeld van β ook isomorf met \mathcal{M} . Geheel analoog aan α_* kan men ook β_* definiëren. (Merk op dat: $\vec{f}_2(x) = (-S_0(x), C_0(x))$.)

Voor iedere $x \in S^1$ geldt:

$$\vec{f}_1(x) \perp \vec{f}_2(x), \quad \text{dus} \quad \{x\} \times \mathbb{R} \times \mathbb{R} = \{x\} \times (\langle \vec{f}_1(x) \rangle \oplus \langle \vec{f}_2(x) \rangle),$$

d.w.z. dat elke vezel van \mathcal{T} wordt opgespannen door vectoren uit het beeld van α en het beeld van β . De afbeelding:

$$M \oplus M \longrightarrow \Gamma(S^1, \mathcal{T}), \quad (m, n) \mapsto \alpha_* \tilde{m} + \beta_* \tilde{n},$$

is dan een injectief R -moduulhomomorfisme. Het is zelfs surjectief, want de inverse wordt gegeven door een sectie \tilde{s} van \mathcal{T} (vezelsgewijs) te projecteren op $\alpha(\mathcal{M})$ resp. $\beta(\mathcal{M})$. (Merk op dat de ‘matrix’ van de afbeelding $M \oplus M \longrightarrow \Gamma(S^1, \mathcal{T})$ gegeven wordt door de matrix A^{-1} uit het voorbeeld.)

Hiermee hebben we dan uiteindelijk:

$$R^2 \cong \Gamma(S^1, \mathcal{T}) \cong M \oplus M,$$

hetgeen we zochten.

Om dit te visualiseren, schalen we $\mathbb{R} \times \mathbb{R}$ tot een schijfje

$$D := \{(u, v) \in \mathbb{R}^2 : u^2 + v^2 < \epsilon\} \quad (\epsilon \in (0, 1)).$$

We kunnen dan \mathcal{T} zien als een ‘massieve’ fietsband: voor iedere $t \in S^1$ nemen we een schijfje $D_t \subset \mathbb{R}^3$ met midden t en D_t ligt in het vlak opgespannen door de lijn van $(0, 0, 0)$ naar $t = (x, y, 0) \in S^1$ en de z -as

$$D_t = \{t + u\vec{e}(t) + v\vec{e}_3 \in \mathbb{R}^3 : u^2 + v^2 < \epsilon\}, \quad \text{met} \begin{cases} \vec{e}(t) = (x, y, 0), \\ \vec{e}_3 = (0, 0, 1). \end{cases}$$

De vereniging van deze schijven, over alle $t \in S^1$, is dan isomorf met (de geschaalde) \mathcal{T} :

$$\mathcal{T} := \cup_{t \in S^1} D_t.$$

Anderzijds kunnen we in D ook de twee möbiusbanden $\alpha(\mathcal{M})$ en $\beta(\mathcal{M})$ zien, deze zijn nl. het beeld van de afbeeldingen:

$$[0, 2\pi] \times (-\epsilon, \epsilon) \longrightarrow \mathbb{R}^3, \quad (x, u) \mapsto t_x + u(C_0(x)\vec{e}(t_x) + S_0(x)\vec{e}_3)$$

$$[0, 2\pi] \times (-\epsilon, \epsilon) \longrightarrow \mathbb{R}^3, \quad (x, v) \mapsto t_x + v(-S_0(x)\vec{e}(t_x) + C_0(x)\vec{e}_3)$$

met $t_x = (\cos x, \sin x, 0) \in S^1$. Zowel R^2 als $M \oplus M$ zien er dus uit als een massieve fietsband, hetgeen overeenstemt met het feit dat de modulen isomorf zijn.

Tenslotte merken we nog op dat het moduul M isomorf blijkt te zijn (als R -moduul) met een (niet-hoofd)ideaal in R (zie opgave 3):

$$M \cong I := \ker(\Phi_{(1,0)} : R \longrightarrow \mathbb{R}), \quad \Phi_{(1,0)} : f(x, y) \mapsto f(1, 0).$$

De moraal is dat niet-hoofdidealen te maken hebben met interessante meetkundige verschijnselen.

6.4 Een bovendriehoeksvorm voor matrices

6.4.1 Zij K een lichaam, zij V een eindig dimensionale lineaire ruimte over K en zij $\alpha : V \rightarrow V$ een K -lineaire afbeelding. Indien alle eigenwaarden van α in K zitten, dan construeren we een basis van V zodat de matrix A van α , t.o.v. die basis, een bovendriehoeksmatrix is (d.w.z. $A_{ij} = 0$ als $i > j$).

6.4.2 Zij α als boven en zij

$$K[\alpha] := \text{beeld}(\Phi_\alpha) = \left\{ \sum_{i < \infty} a_i \alpha^i : a_i \in K \right\},$$

het beeld van het evaluatiehomomorfisme:

$$\Phi_\alpha : K[X] \longrightarrow \text{End}_K(V), \quad f \mapsto f(\alpha),$$

zie voorbeeld 3.2.3. De ring $K[\alpha]$ is een commutatieve deelring van $\text{End}_K(V)$ (commutatief omdat $\alpha^i \alpha^j = \alpha^{i+j} = \alpha^j \alpha^i$ en $a\alpha = \alpha a$). Omdat $\text{beeld}(\Phi_\alpha) = K[\alpha]$ geeft de eerste isomorfie stelling, zie 2.2.9, dat:

$$K[\alpha] \cong K[X]/(m_\alpha), \quad \alpha \mapsto X + (m_\alpha),$$

hierin is $m_\alpha \in K[X]$ het minimumpolynoom van α (zie 3.4.4), d.w.z. het unieke monische polynoom dat $\ker(\Phi_\alpha)$ voortbrengt

$$(m_\alpha) = \ker(\Phi_\alpha).$$

6.4.3 We kunnen de lineaire ruimte V de structuur van $K[\alpha]$ -moduul geven, met de optelling als in de lineaire ruimte, en met actie van $K[\alpha]$ gegeven door:

$$K[\alpha] \times V \longrightarrow V, \quad \left(\sum_{i=0}^n a_i \alpha^i, \vec{v} \right) \mapsto \sum_{i=0}^n a_i \alpha^i \vec{v},$$

hierbij is $\alpha \vec{v}$ het beeld van \vec{v} onder de lineaire afbeelding $\alpha : V \rightarrow V$.

Omdat $K \hookrightarrow K[\alpha]$ (de constante polynomen), is een $K[\alpha]$ -deelmoduul ook een K -deelmoduul, d.w.z. een lineaire ruimte. We gaan hieronder V als direkte som van $K[\alpha]$ -deelmodulen van V schrijven. In elk van deze deelmodulen kunnen we de actie van α op eenvoudige wijze beschrijven.

6.4.4 Omdat de hoofdideaalring $K[X]$ een ontbindingsring is, kunnen we elk monisch polynoom (op unieke wijze) als product van monische, irreducibele polynomen schrijven. In het bijzonder kunnen we schrijven:

$$m_\alpha = h_1^{n_1} h_2^{n_2} \dots h_k^{n_k},$$

met de h_i monisch en irreducibel en met $h_i \neq h_j$ als $i \neq j$. Deze schrijfwijze is uniek op verwisseling van de indices $1, 2, \dots, k$ na.

Dan geldt dat (zie 5.3.7):

$$K[\alpha] \cong K[X]/(h_1^{n_1}) \times K[X]/(h_2^{n_2}) \times \dots \times K[X]/(h_k^{n_k}).$$

We laten zien dat dit een direkte som splitsing van het $K[\alpha]$ -moduul V geeft.

Stelling 6.4.5 *Zij K een lichaam, zij $V \neq (0)$ een eindig dimensionale lineaire ruimte over K en zij*

$$\alpha : V \longrightarrow V$$

een lineaire afbeelding met minimumpolynoom

$$m_\alpha = h_1^{n_1} h_2^{n_2} \dots h_k^{n_k},$$

met irreducibele, monische h_i en met $h_i \neq h_j$ als $i \neq j$.

Definieer $K[\alpha]$ -deelmodulen van het $K[\alpha]$ -moduul V door:

$$V_i := \{v \in V : h_i^{n_i}(\alpha)v = 0\}.$$

*Merk op dat de V_i inderdaad $K[\alpha]$ -modulen zijn; men noemt de V_i wel de **gegeneraliseerde eigenruimten** van α .*

Dan geldt dat $V_i \neq 0$ voor iedere $i = 1, 2, \dots, k$ en bovendien:

$$V \cong \bigoplus_{i \in \{1, 2, \dots, k\}} V_i.$$

Bewijs. We voeren het bewijs met inductie naar k . Als $k = 1$ geldt $h_1^{n_1}(\alpha) = m_\alpha(\alpha) = 0$. Dan is per definitie $V = V_1$ hetgeen het geval $k = 1$ bewijst.

Zij nu $k > 1$. We definiëren:

$$h := h_k^{n_k}, \quad f := h_1^{n_1} h_2^{n_2} \dots h_{k-1}^{n_{k-1}}, \quad \text{en} \quad N := \ker(f(\alpha) : V \rightarrow V).$$

De polynomen h en f zijn onderling ondeelbaar, dus (zie het bewijs van stelling 5.3.7) geldt $(f) + (h) = K[X]$, en daarom zijn er $g_1, g_2 \in K[X]$ met

$$g_1 f + g_2 h = 1, \quad \text{i.h.b.} \quad g_1(\alpha) f(\alpha) + g_2(\alpha) h(\alpha) = 1.$$

We bewijzen nu eerst dat het $K[\alpha]$ -moduulhomorfisme:

$$\psi : N \oplus V_k \longrightarrow V \quad (n, v_k) \mapsto n + v_k,$$

een $K[\alpha]$ -moduulisomorfisme is.

Elke $v \in V$ is te schrijven als:

$$v = 1v = f(\alpha)g_1(\alpha)v + h(\alpha)g_2(\alpha)v = v_k + n.$$

Omdat $m_\alpha(\alpha) = f(\alpha)h(\alpha) = 0$ geldt:

$$\begin{aligned} h(\alpha)v_k &= m_\alpha(\alpha)g_1(\alpha)v = 0 &\implies v_k &\in V_k \\ f(\alpha)n &= m_\alpha(\alpha)g_2(\alpha)v = 0 &\implies n &\in N, \end{aligned}$$

Dus ψ is surjectief.

Verder geldt voor $n \in N$ en $v_k \in V_k$:

$$n + v_k = 0 \implies x := n = -v_k \in N \cap V_k.$$

Dan is dus $f(\alpha)x = 0$ en $h(\alpha)x = 0$. Uit $x = 1x$ en $1 = f(\alpha)g_1(\alpha) + h(\alpha)g_2(\alpha)$ volgt dan $x = 0$. Dus ψ is ook injectief en we concluderen dat $V \cong N \oplus V_k$.

Noem β de beperking van α tot N , dus $\beta : N \rightarrow N$. Dan is (vergelijk opgave 9) $m_\beta = f$. Uit de inductiehypothese volgt dat:

$$N \cong \bigoplus_{i=1}^{k-1} V_i, \quad \text{dus : } V \cong N \oplus V_k \cong V_1 \oplus V_2 \oplus \dots \oplus V_k.$$

Tenslotte zijn de $V_i \neq \{0\}$ omdat anders $h_i(\alpha)^{n_i}$ een injectieve, en dus ($\dim_K(V)$ is eindig) een inverteerbare afbeelding is. Uit $m_\alpha(\alpha) = 0$ volgt dan $m_\alpha(\alpha)h_i(\alpha)^{-n_i} = 0$, dus het polynoom $m_\alpha h_i^{-n_i}$ zit in de kern van het evaluatiehomomorfisme Φ_α en heeft lagere graad dan m_α , een tegenspraak.

Hiermee is de stelling bewezen. \square

Voorbeeld 6.4.6 Zij $\alpha : K^n \rightarrow K^n$ een lineaire afbeelding met n onderling verschillende eigenwaarden $\lambda_1, \dots, \lambda_n \in K$. Dan is

$$m_\alpha = (X - \lambda_1) \dots (X - \lambda_n)$$

(zie 3.4.4) en in dit geval is m_α gelijk aan het eigenwaarden polynoom van α . Definiëren we dan $V = K^n$ (gezien als $K[\alpha]$ -moduul), dan geldt:

$$V_i := \ker(\alpha - \lambda_i), \quad \text{dus } V_i := \{\vec{v} \in V : \alpha\vec{v} = \lambda_i\vec{v}\}$$

m.a.w. V_i is precies de eigenruimte van α bij de eigenwaarde λ_i .

Omdat iedere $V_i \neq \{0\}$ en $\sum_i \dim_K V_i = n$ is iedere V_i één dimensionaal. Kies nu voor $i = 1, 2, \dots, n$ een $\vec{f}_i \in V_i - \{0\}$, d.w.z. \vec{f}_i is een eigenvector voor α met eigenwaarde λ_i . Dan is $V_i = \langle \vec{f}_i \rangle$ en uit:

$$V = \bigoplus_{i=1}^n V_i = \langle \vec{f}_1 \rangle \oplus \dots \oplus \langle \vec{f}_n \rangle$$

volgt dat de \vec{f}_i onafhankelijk zijn over K en dus een basis van K^n vormen. Omdat $\alpha\vec{f}_i = \lambda_i\vec{f}_i$ is de matrix A van α t.a.v. deze basis dus de diagonaal-matrix $\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$.

6.4.7 We beschouwen in de rest van deze paragraaf het speciale geval dat:

$$m_\alpha = (X - \lambda_1)^{n_1} (X - \lambda_2)^{n_2} \dots (X - \lambda_k)^{n_k},$$

met $\lambda_i \in K$.

In het bijzonder zijn de λ_i dan de eigenwaarden van α (zie opgave 17 op blz. 71), maar m_α is niet noodzakelijkerwijs het eigenwaarde polynoom $P_\alpha(X) = \det(\alpha - XI)$. Wel geldt dat m_α een deler van P_α is (immers $P_\alpha(\alpha) = 0$ impliceert $P_\alpha \in (m_\alpha)$).

Omdat we volgens de stelling de lineaire ruimte V kunnen schrijven als een direkte som van de $K[\alpha]$ -modulen V_{λ_i} :

$$V_{\lambda_i} := \ker((\alpha - \lambda_i)^{n_i}) \neq \{\vec{0}\},$$

geldt voor $\vec{v}_i \in V_{\lambda_i}$ dat ook $\alpha\vec{v}_i \in V_{\lambda_i}$. Daarom kunnen we een matrix van α in een blokvorm schrijven:

$$V = \bigoplus_{i=1}^k V_{\lambda_i} \xrightarrow{\alpha} \bigoplus_{i=1}^k V_{\lambda_i}, \quad \alpha(V_{\lambda_i}) \subset V_{\lambda_i}.$$

We bekijken nu hoe ieder blok eruit ziet, d.w.z. hoe de restrictie van α tot V_{λ_i} er uit ziet. Merk op dat de restrictie van α tot V_{λ_i} minimum polynoom $(X - \lambda_i)^{n_i}$ heeft.

Voorbeeld 6.4.8 Zij $V = \mathbb{R}^3$ en zij

$$A := \begin{pmatrix} 4 & -4 & 4 \\ 1 & -1 & 4 \\ 0 & -1 & 4 \end{pmatrix}.$$

We bepalen het minimumpolynoom van A en de (beter: een) blokvorm van A . Omdat de nulpunten van het minimumpolynoom de eigenwaarden van A zijn, berekenen we eerst:

$$\det(A - XI) = -(X^3 - 7X^2 + 16X - 12) = -(X - 2)^2(X - 3).$$

Het minimumpolynoom van A is dan $(X - 2)(X - 3)$ of $(X - 2)^2(X - 3)$. Omdat $(A - 2)(A - 3) \neq 0$ (ga na) volgt:

$$m_A = (X - 2)^2(X - 3).$$

De gegeneraliseerde eigenruimten zijn de kernen van:

$$(A - 2)^2 = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}, \quad A - 3 = \begin{pmatrix} 1 & -4 & 4 \\ 1 & -4 & 4 \\ 0 & -1 & 1 \end{pmatrix}.$$

Hieruit volgt dan (met V_λ de gegeneraliseerde eigenruimte bij de eigenwaarde λ):

$$V_2 = \langle (1, 1, 0), (1, 1, 1) \rangle, \quad V_3 = \langle (0, 1, 1) \rangle.$$

Beperken we A tot V_2 dan geldt:

$$\left. \begin{aligned} A(1, 1, 0) &= (0, 0, -1) = 1 \cdot (1, 1, 0) + (-1) \cdot (1, 1, 1) \\ A(1, 1, 1) &= (4, 4, 3) = 1 \cdot (1, 1, 0) + 3 \cdot (1, 1, 1) \end{aligned} \right\}, \quad \text{dus} \quad \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$$

is de matrix van A beperkt tot V_2 (tov. de basis $(1, 1, 0)$, $(1, 1, 1)$ van V_2). De beperking van A tot V_3 is de 1×1 matrix 3 . De matrix van A tov. deze basis van V is dan inderdaad in blokvorm:

$$\begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Stelling 6.4.9 *Zij W een eindig dimensionale lineaire ruimte over K en zij gegeven een lineaire afbeelding*

$$B : W \longrightarrow W, \quad \text{met} \quad m_B = (X - \lambda)^m.$$

Dan geldt:

$$B = \lambda + N, \quad \text{met} \quad N^m = 0,$$

hierbij is, zoals gebruikelijk, λ de diagonaalmatrix $\text{diag}(\lambda, \dots, \lambda)$. Merk op dat N een nilpotente lineaire afbeelding is, d.w.z. een nilpotent in $\text{End}_K(W)$ is.

Er is een basis van W zodat de matrix van N t.o.v. die basis in de bovendriehoeksvorm staat, en bovendien zijn alle diagonaalcoëfficiënten van deze matrix 0 . De matrix van B ziet er, t.o.v. van die basis dus uit als:

$$\begin{pmatrix} \lambda & * & \dots & \dots & * \\ 0 & \lambda & * & \dots & * \\ 0 & 0 & & & * \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Bewijs. De eerste bewering volgt door te definiëren:

$$N := B - \lambda \quad \text{dan geldt nl. :} \quad N^m = (B - \lambda)^m = 0.$$

Voor iedere $i = 1, 2, \dots, m$ definiëren we een lineaire deelruimte W_i van W door:

$$W_1 = \ker(N), \dots, W_i = \ker(N^i), \dots, W_m = \ker(N^m) = \ker(0) = W.$$

Merk op dat geldt:

$$W_i \subset W_{i+1}, \quad \text{want} \quad N^i \vec{v} = \vec{0} \implies N^{i+1} \vec{v} = \vec{0}.$$

Kies nu een basis van W door eerst een basis van W_1 te kiezen, en vervolgens deze basis aan te vullen tot een basis van W_2 . Zo voortgaande kies je basis van W_{i+1} door de basis van $W_i \subset W_{i+1}$ aan te vullen tot een basis van W_{i+1} , totdat je uiteindelijk een basis $\{\vec{f}_i\}$ van $W = W_m$ hebt. Merk nu op:

$$NW_i \subset W_{i-1}, \quad \text{immers} \quad N^i \vec{v} = \vec{0} \implies N^{i-1}(N\vec{v}) = \vec{0},$$

en hier staat dat $N\vec{v} \in W_{i-1}$.

Zij \vec{f}_l een van deze basisvectoren met

$$\vec{f}_l \in W_i, \quad \vec{f}_l \notin W_{i-1}.$$

De basis van W_{i-1} bestaat dan uit \vec{f}_k 's met $1 \leq k \leq \dim W_{i-1} < l$. Omdat $NW_i \subset W_{i-1}$ geldt:

$$N\vec{f}_l \in W_{i-1}, \quad \text{dus:} \quad N\vec{f}_l = \sum_i x_{il} \vec{f}_i \quad \text{en} \quad x_{il} = 0 \quad \text{als} \quad i > \dim W_{i-1}.$$

Omdat $l > \dim W_{i-1}$ geldt i.h.b. dat $x_{il} = 0$ als $i \geq l$.

De matrix van N t.o.v. deze basis wordt gegeven door de x_{ij} 's en is dus inderdaad een boven driehoeksmatrix, zoals gewenst, met nullen op de diagonaal (want $x_{il} = 0$, voor elke l). Omdat de diagonaalmatrix $\text{diag}(\lambda, \dots, \lambda)$ op elke basis dezelfde is, heeft de matrix $B = \lambda + N$ λ 's op de diagonaal en nullen daaronder. Hiermee is de stelling bewezen. \square

Voorbeeld 6.4.10 We beschouwen de lineaire afbeelding

$$B : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad \text{met matrix} \quad \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}.$$

Het minimumpolynoom m_B is een deler van het eigenwaardepolynoom van van B . Dit gebruiken we om m_B te berekenen. Het eigenwaarde polynoom is:

$$\det(B - XI) = X^2 - 4X + 4 = (X - 2)^2.$$

Omdat $B - 2 \neq 0$ (immers $B \neq \text{diag}(2, 2)$), geldt $m_B \neq X - 2$. Dan is:

$$m_B = (X - 2)^2, \quad \text{en} \quad N := B - 2 = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Ga zelf na dat inderdaad $N^2 = 0$. We bepalen nu de W_i 's:

$$W_1 = \ker(N) = \langle (1, 1) \rangle, \quad W_2 = \mathbb{R}^2; \quad \text{kies:} \quad f_1 := (1, 1), \quad f_2 := (0, 1),$$

merk op dat je voor f_1 elke vector van vorm (a, a) met $a \neq 0$ mag nemen en voor f_2 mag je elke vector in \mathbb{R}^2 nemen, mits deze niet in van de vorm (a, a) is. Er geldt:

$$Nf_1 = 0, \quad Nf_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = f_1, \quad \text{dus} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is de matrix van N t.o.v. de basis f_1, f_2 . (Bij andere keuze van f_1 en f_2 kan er een ander getal dan 1 rechtsboven staan, de drie nullen staan er altijd zoals het bewijs van de stelling laat zien.) Op de basis f_1, f_2 is de matrix van B dan inderdaad in bovendriehoeks vorm:

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

6.5 Opgaven

1. Zij $R = \mathbb{R}[X]$, voor $a \in \mathbb{R}$ definiëren we:

$$I_a := (X - a) = \mathbb{R}[X](X - a),$$

een ideaal van R (en dus een R -moduul).

- a. Voor $a, b \in \mathbb{R}$ definiëren we:

$$\phi : I_a \longrightarrow \mathbb{R}(X) = Q(R), \quad f \mapsto f \cdot \frac{X - b}{X - a}.$$

Ga na dat ϕ een injectief R -moduulhomomorfisme is met beeld $\text{im}(\phi) = I_b$. Concludeer dat I_a en I_b isomorfe R -modulen zijn.

- b. Bewijs dat de R -modulen $\mathbb{R}_a := R/I_a$ en $\mathbb{R}_b := R/I_b$ *niet* isomorf zijn als $a \neq b$.

2. Bepaal, met de methodes uit het dictaat, een bovendriehoeksvorm voor de volgende matrices:

$$A = \begin{pmatrix} 3 & -1 & 0 \\ 4 & -2 & 1 \\ 4 & -4 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -2 & 3 \\ -1 & -3 & 4 \end{pmatrix}.$$

3. Zij R de ring van C^∞ functies met periode 2π en zij:

$$M := \{ g \in C^\infty(\mathbb{R}) : g(x+2\pi) = -g(x) \}, \quad I := \{ f \in R : f(0) = 0 \},$$

dan zijn M en I beide R -modulen (voor M zie 6.3.7 en I is een ideaal van R).

- a. Bewijs dat

$$\phi : M \longrightarrow I, \quad g \mapsto gS_0,$$

met $S_0(x) := \sin \frac{x}{2}$, een injectief R -moduulhomomorfisme is.

- b. Zij $f \in I$. Bewijs dat de functie g gedefinieerd door:

$$\begin{cases} g(x) := f(x)/S_0(x), & \text{als } x \not\equiv 0 \pmod{2\pi} \\ g(x) := 2f'(x) & \text{als } x \equiv 0 \pmod{2\pi} \end{cases}$$

een C^∞ functie is (hint: $f(x) = \int_0^1 \frac{\partial f}{\partial t}(tx) dt = x \int_0^1 f'(tx) dt$), en ga na dat $g \in M$.

c. Bewijs dat de R -modulen M en I isomorf zijn.

4. Zij R een commutatieve ring en laat $I, J \subset R$ idealen zijn met

$$I + J = R \quad \text{en laat} \quad i_1 + j_1 = 1 \quad (i_1 \in I, j_1 \in J).$$

a. Bewijs dat

$$\phi : I \oplus J \longrightarrow R, \quad (i, j) \mapsto i + j$$

een surjectief R -moduulhomomorfisme is met $\ker(\phi) \cong I \cap J \cong IJ$ (iso van R -modulen).

b. Bewijs dat

$$\psi : I \oplus J \longrightarrow R \oplus IJ, \quad (i, j) \mapsto (i + j, ij_1 - ji_1)$$

een R -moduulisomorfisme is.

5. We geven een algebraïsch analogon van de möbiusband, vergelijk opgave 3. Zij R de ring van polynoomfuncties op de cirkel:

$$R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$$

en definieer

$$x := X + (X^2 + Y^2 - 1), \quad y := Y + (X^2 + Y^2 - 1) \in R.$$

Omdat $X^2 + Y^2 - 1$ irreducibel is (Eisenstein bij $p = Y - 1$ in de ontbindingsring $(\mathbb{R}[X])[Y]$), is $(X^2 + Y^2 - 1)$ een priemideaal en dus is R een domein. Het breukenlichaam van R noteren we met $Q(R)$. We definiëren idealen

$$I := (x - 1, y) \quad \text{en} \quad J := (x, y - 1),$$

zoals bekend is I geen hoofdideaal (zie opgave 19 op blz. 71).

a. Bewijs dat in R geldt:

$$(x+y-1)^2 = 2(x-1)(y-1), \quad (x+y-1)(x-y+1) = -2y(y-1).$$

(Tekenen een plaatje met de cirkel en deze lijnen, waar zijn de snijpunten en wat zijn de 'snijmultipliciteiten'?)

b. Definieer een R -moduulhomomorfisme

$$\psi : I \longrightarrow Q(R), \quad i \mapsto i \cdot \frac{2(y-1)}{x+y-1},$$

waarbij $Q(R)$ het quotiëntenlichaam van R is. Ga na dat ψ een injectief R -moduulhomomorfisme is en dat $\text{im}(\psi) = J \subset R \subset Q(R)$.

- c. Bewijs dat $I + J = R$ en dat $IJ = (x + y - 1)R \cong R$ (iso van R -modulen).
 d. Concludeer (gebruik opgave 4): $I \not\cong R$, maar $I \oplus I \cong R^2$.

6. Zij $R = \mathbb{Z}[\sqrt{-5}]$, zij $I := (2, 1 + \sqrt{-5})$ en zij $J := (3, 1 - \sqrt{-5})$ (I en J zijn dus idealen van R).

a. Ga na dat:

$$\psi : I \longrightarrow \mathbb{Q}[\sqrt{-5}], \quad i \mapsto i \cdot \frac{3}{1 + \sqrt{-5}},$$

een injectief R -moduulhomomorfisme is met $\text{im}(\psi) = J \subset R = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{Q}(\sqrt{-5})$.

- b. Bewijs dat $I + J = R$ en dat $IJ = (1 - \sqrt{-5})R$.
 c. Bewijs dat $I \not\cong R$, maar dat $I \oplus I \cong R^2$ (gebruik opgave 4).

7. We geven een voorbeeld van een ring R met $R \cong R^2$. We definiëren R als zijnde de ring van rij-eindige matrices met coëfficiënten in een lichaam K . Dat wil zeggen, iedere $r \in R$ is een oneindig grote matrix $r = (r_{ij})$ met $i, j \in \mathbb{Z}_{>0}$, waarbij voor elke i geldt, dat $r_{ij} \neq 0$ voor slechts eindig veel j .

Optelling en product zijn analoog aan de gebruikelijke matrixoperaties:

$$r + s = t, \quad \text{met } t_{ij} := r_{ij} + s_{ij}, \quad rs = u, \quad \text{met } u_{ij} := \sum_{k=0}^{\infty} r_{ik}s_{kj},$$

merk op dat dit in feite een eindige som is, omdat slechts eindig veel r_{ik} 's ongelijk nul zijn.

- a. Bewijs dat R een ring is.
 b. Definieer $b, c \in R$ door:

$$b := (b_{ij}), \quad b_{ij} = 1 \text{ als } j = 2(i-1) + 1 \text{ en } b_{ij} = 0 \text{ anders,}$$

$c := (c_{ij})$, $c_{ij} = 1$ als $j = 2(i - 1) + 2$ en $c_{ij} = 0$ anders, hierbij is $i \in \mathbb{Z}_{>0}$. Bewijs dat de volgende R -modulen isomorf zijn:

$$R \cong Rb \oplus Rc \cong R \oplus R.$$

8. Een R -moduul $M \neq 0$ heet **enkelvoudig** als $M \neq 0$ en als elk deelmoduul van M gelijk is aan ofwel $\{0\}$ ofwel M . Laat nu M een enkelvoudig R -moduul zijn.

Bewijs dat voor elk R -moduulhomomorfisme $f : M \rightarrow M$ geldt: $f = 0$ of f is een R -moduulisomorfisme. Concludeer dat $End_R(M)$ een delingsring is.

Bepaal $End_R(M)$ in geval $R = M(n, K)$ en $M = K^n$ met K een (commutatief) lichaam (zie voorbeeld 6.1.3).

9. Gegeven eindig dimensionale lineaire ruimten V, W over een lichaam K . Laat $\alpha : V \rightarrow V$ en $\beta : W \rightarrow W$ lineaire afbeeldingen over K zijn, met minimum polynomen m_α en m_β . Definieer

$$\alpha \oplus \beta : V \oplus W \rightarrow V \oplus W : (v, w) \mapsto (\alpha(v), \beta(w)).$$

Bewijs dat als m_α en m_β onderling ondeelbaar zijn, dan is $m_{\alpha \oplus \beta} = m_\alpha m_\beta$.

7 Lichamen

7.1 Priemlichamen en karakteristiek

7.1.1 Laat K een lichaam zijn. Een deelverzameling $K' \subset K$ heet een **deellichaam** als aan de volgende drie voorwaarden voldaan is:

- 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 inclusie relatie). Merk op dat $0, 1 \in K_0$.

Stelling 7.1.2 *Laat K een lichaam zijn. Dan is het priemlichaam van K isomorf met*

- òfwel het lichaam \mathbb{Q} der rationale getallen
- òfwel één 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

$$\kappa : \mathbb{Z} \longrightarrow K_0$$

door:

$$\begin{aligned} \kappa(n) &= 1 + 1 + \dots + 1 \in K_0 && (n \text{ termen}) \\ \kappa(0) &= 0 \in K_0 \\ \kappa(-n) &= -(1 + 1 + \dots + 1) \in K_0 && (n \text{ termen}) \end{aligned}$$

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 , en 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 $\kappa(\mathbb{Z}) \cong \mathbb{Z}/\ker(\kappa)$ (Stelling 2.2.9), is $\ker(\kappa)$ een priemideaal van \mathbb{Z} , dus $\ker(\kappa) = \{0\}$ of $\ker(\kappa) = p\mathbb{Z}$, waarbij p een priemgetal is.

Laat eerst $\ker(\kappa) = 0$. Dan is κ injectief, en $\kappa(\mathbb{Z}) \cong \mathbb{Z}$. We kunnen κ voortzetten tot een functie

$$\kappa_1 : \mathbb{Q} \rightarrow K_0, \quad \kappa_1(a/b) := \kappa(a) \cdot (\kappa(b))^{-1}, \quad (a, b \in \mathbb{Z}, b \neq 0).$$

Men gaat gemakkelijk na dat dit een goed gedefinieerde afbeelding is, en dat $\kappa_1 : \mathbb{Q} \rightarrow K_0$ een lichaamshomomorfisme is. Omdat $\{0\}$ en \mathbb{Q} de enige idealen van \mathbb{Q} zijn, 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 $\ker(\kappa) = p\mathbb{Z}$, waarbij p een priemgetal is. Dan is $\kappa(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, hetgeen volgens Stelling 1.18 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 $K_0 \cong \mathbb{Z}/p\mathbb{Z}$. \square

Definitie 7.1.3 Laat K een lichaam zijn met priemlichaam K_0 .

Als $K_0 \cong \mathbb{Q}$ zeggen we dat K **karacteristiek nul** heeft, notatie: $\text{kar}(K) = 0$.

Als $K_0 \cong \mathbb{F}_p$ zeggen we dat K **karacteristiek p** heeft, notatie: $\text{kar}(K) = p$.

We zien dat in beide gevallen $\text{kar}(K)$ de niet-negatieve voortbrenger van het ideaal $\ker(\kappa) \subset \mathbb{Z}$ is, waarin $\kappa : \mathbb{Z} \rightarrow K$ het unieke ringhomomorfisme met $\kappa(1) = 1$ is.

7.2 Algebraïsch en transcendent

7.2.1 Als L een lichaam is en $K \subset L$ is een deellichaam van L , dan noemen we L een **uitbreiding** of **lichaamsuitbreiding** van K . Voor iedere $\alpha \in L$ is er dan een evaluatiehomomorfisme:

$$\Phi_\alpha : K[X] \longrightarrow L, \quad f \mapsto f(\alpha).$$

De kern van Φ_α is een ideaal in $K[X]$, en is dus een hoofdideaal, zie 3.4.1. Dan is ofwel $\ker(\Phi_\alpha) = (0)$ (dus Φ_α is injectief) ofwel

$$\ker(\Phi_\alpha) = (f_K^\alpha), \quad \text{met } f_K^\alpha \in K[X],$$

een (uniek) monisch polynoom, dat we het **minimumpolynoom** van α over K noemen.

In geval Φ_α injectief is, noemen we α **transcendent** over K . Er is dan geen enkel polynoom $f \in K[X]$, $f \neq 0$ met $f(\alpha) = 0$. De ring $K[X]$ is, via Φ_α , isomorf met z'n beeld $\Phi_\alpha(K[X])$.

In geval Φ_α niet injectief is, dan voldoet α aan een algebraïsche vergelijking (een polynoom vergelijking) en noemen we α **algebraïsch** over K . Merk op: als

$$g \in K[X], \quad g(\alpha) = 0, \quad \text{dan} \quad g \in \ker(\Phi_\alpha) = (f_K^\alpha) \implies g = qf_K^\alpha$$

voor zekere $q \in K[X]$.

In beide gevallen is

$$K[\alpha] := \text{beeld}(\Phi_\alpha) \subseteq L$$

een domein, en heeft dus een quotiëntenlichaam $Q(K[\alpha])$ (zie 1.3.2) dat isomorf is met het deellichaam $K(\alpha)$ van L gedefinieerd door:

$$K(\alpha) := \left\{ \frac{x}{y} \in L : x, y \in K[\alpha], y \neq 0 \right\}.$$

Een uitbreiding L van K noemt men **enkelvoudig** indien er een $\alpha \in L$ is met $L = K(\alpha)$.

In geval α transcendent is over K , is $K(\alpha) \cong K(X)$, het lichaam van rationale functies in een variabele met coëfficiënten in K . In het bijzonder is $\alpha^{-1} \notin K[\alpha]$ en $K(\alpha) \not\cong K[\alpha]$.

In het geval α algebraïsch is over K , geldt daarentegen $K[\alpha] = K(\alpha)$ en dus $\alpha^{-1} \in K[\alpha]$ als $\alpha \neq 0$, zoals we in 7.2.5 zullen zien.

Opmerking 7.2.2 Merk op dat het onderscheid transcendent/algebraïsch in deze paragraaf analoog is aan het onderscheid karakteristiek nul/karakteristiek $p > 0$ in 7.1.3. In deze analogie correspondeert het evaluatiehomomorfisme

$$\Phi_\alpha : K[X] \rightarrow K[\alpha], \quad \Phi_\alpha(X) := \alpha$$

met het ringhomomorfisme

$$\kappa : \mathbb{Z} \rightarrow K, \quad \kappa(1) := 1$$

in het bewijs van 7.1.2, en f_K^α correspondeert met p .

Voorbeeld 7.2.3 Nemen we $L = K(X)$, en $\alpha = X \in K(X)$ dan hebben we een heel eenvoudig voorbeeld van een enkelvoudige uitbreiding L van K met een transcendente α .

Lastiger is het bestaan van getallen in \mathbb{R} of \mathbb{C} die transcendent zijn over \mathbb{Q} , deze noemt men **transcendent** (zonder meer). Zo'n getal is dus niet een nulpunt van een polynoom ($\neq 0$) met coëfficiënten in \mathbb{Q} . Met een telargument (zie opg 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 $0,12345678910111213\dots$ transcendent is. In 1873 werd door Hermite (Charles Hermite, Frans wiskundige, 1822-1901) bewezen dat het getal e , de basis der natuurlijke logaritmen, transcendent is, en in 1882 deed Lindemann (Carl Louis Ferdinand von Lindemann, Duits wiskundige) hetzelfde voor π , de halve omtrek van een cirkel met straal 1. Literatuur hierover: I. Steward, Galois Theory Ch.6.

Voorbeeld 7.2.4 Het complexe getal $i \in \mathbb{C}$ is algebraïsch over \mathbb{R} , met $f_{\mathbb{R}}^i := X^2 + 1$, en is ook algebraïsch over \mathbb{Q} met $f_{\mathbb{Q}}^i = X^2 + 1$. Als $a \in \mathbb{R}$ transcendent is, dan is $ia \in \mathbb{C}$ wel algebraïsch over \mathbb{R} , met $f_{\mathbb{R}}^{ia} = X^2 + a^2$ maar ia is niet algebraïsch over \mathbb{Q} (ga na).

In het algemeen geldt: als $\alpha \in L$ dan is $f_L^\alpha = X - \alpha$, het minimumpolynoom van α over een deellichaam K van L hangt dus i.h.a. van de keuze van K af.

Voor elke $k, n \in \mathbb{Z}_{>0}$ is het getal $\alpha = \sqrt[n]{k} \in \mathbb{R}$ algebraïsch over \mathbb{Q} , het is immers nulpunt van het polynoom $X^n - k$. Ook zijn de complexe getallen:

$$e^{\frac{2\pi ik}{n}} := \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \quad (k \in \mathbb{Z})$$

algebraïsch over \mathbb{Q} , ze zijn immers nulpunt van $X^n - 1$. Deze laatste getallen noemt men **eenheidswortels**. Het minimumpolynoom is i.h.a. niet zo eenvoudig te bepalen, zie 7.4 en 14.2.1.

Stelling 7.2.5 Laat L een uitbreiding van een lichaam K zijn, en zij $\alpha \in L$ algebraïsch over K .

Dan is f_K^α , het minimumpolynoom van α over K , irreducibel in $K[X]$. Verder is $K[\alpha] \cong K[X]/(f_K^\alpha)$ en $K[\alpha]$ is een lichaam, i.h.b.:

$$K(\alpha) = K[\alpha].$$

Bewijs. Het evaluatiehomorfisme $\Phi_\alpha : K[X] \rightarrow K[\alpha] \subset L$ geeft volgens de eerste isomorfiestelling een isomorfisme $K[X]/\ker(\Phi_\alpha) \cong K[\alpha]$. Omdat L een lichaam is, is $K[\alpha]$ een domein en dus is $\ker(\Phi_\alpha) = (f_K^\alpha)$ een priemideaal in $K[X]$. Omdat $K[X]$ een hoofdideaalring is, is f_K^α dan irreducibel, zie

Stelling 5.2.3. Volgens dezelfde stelling is dan (f_K^α) ook een maximaal ideaal, dus is $K[\alpha]$ een lichaam. Omdat $K(\alpha) := Q(K[\alpha])$ het kleinste deellichaam van L is waar $K[\alpha]$ in zit, geldt $K(\alpha) = K[\alpha]$. \square

Voorbeeld 7.2.6 Zij $d \in \mathbb{Q}$ met $\alpha := \sqrt{d} \notin \mathbb{Q}$. Dan is $f_{\mathbb{Q}}^\alpha = X^2 - d$. Dit polynoom is irreducibel want het heeft (wegens de keuze van d) geen nulpunt in \mathbb{Q} . Verder geldt:

$$\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \in \mathbb{C} : a, b \in \mathbb{Q} \right\}.$$

We laten zien dat $\mathbb{Q}[\sqrt{d}]$ inderdaad een lichaam is door de inverse van een $x = a + b\sqrt{d} \neq 0$ aan te geven. Definieer

$$\bar{x} := a - b\sqrt{d} \quad \text{en} \quad N(x) = x\bar{x} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d \quad (\in \mathbb{Q}).$$

Omdat d in \mathbb{Q} geen kwadraat is, en $x \neq 0$, geldt $N(x) \neq 0$ (ga na). Daarom geldt voor $x \neq 0$:

$$x^{-1} := \frac{\bar{x}}{N(x)} = \frac{a}{a^2 - b^2d} - \frac{b}{a^2 - b^2d}\sqrt{d} \in \mathbb{Q}[\sqrt{d}].$$

Voorbeeld 7.2.7 Zij $\alpha \in \mathbb{C} = L$ een nulpunt van het polynoom $f = X^3 + X^2 - 1$. Dan is α algebraïsch over $\mathbb{Q} = K$ (immers $f \in \ker(\Phi_\alpha)$). Het polynoom f is irreducibel in $\mathbb{Q}[X]$, want f heeft geen nulpunt in \mathbb{Z} en dus ook niet in \mathbb{Q} (zie 5.4.11). Daarom geldt $f_{\mathbb{Q}}^\alpha = f$ en $\mathbb{Q}[\alpha] \cong \mathbb{Q}[X]/(f)$ is een lichaam. We geven een methode om de inverse van een $a \in \mathbb{Q}[\alpha]$ met $a \neq 0$ te bepalen. (Voor een andere methode die het Euclidisch algoritme gebruikt, zie 12.3.6).

Uit stelling 3.3.4 weten we dat iedere $a \in \mathbb{Q}[\alpha]$ op unieke wijze te schrijven is als

$$a = a_0 + a_1\alpha + a_2\alpha^2 \quad \text{met} \quad a_0, a_1, a_2 \in \mathbb{Q}.$$

Om de inverse te bepalen moeten we de vergelijking:

$$ax = 1 \quad \text{dwz} \quad (a_0 + a_1\alpha + a_2\alpha^2)(x_0 + x_1\alpha + x_2\alpha^2) = 1$$

oplossen met $x_i \in \mathbb{Q}$. Omdat $1, \alpha, \alpha^2$ onafhankelijk zijn over \mathbb{Q} (dit volgt uit de uniciteit van de schrijfwijze) en

$$\alpha^3 = -\alpha^2 + 1, \quad \alpha^4 = \alpha \cdot \alpha^3 = -\alpha^3 + \alpha = \alpha^2 + \alpha - 1$$

moeten we (voor gegeven a_i) het volgende stelsel lineaire vergelijkingen oplossen:

$$\begin{cases} a_0x_0 + a_2x_1 + (a_1 - a_2)x_2 = 1 \\ a_1x_0 + a_0x_1 + a_2x_2 = 0 \\ a_2x_0 + (a_1 - a_2)x_1 + (a_0 - a_1 + a_2)x_2 = 0 \end{cases}$$

Dit stelsel kan in matrixvorm met een matrix M worden geschreven:

$$\begin{pmatrix} a_0 & a_2 & a_1 - a_2 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 - a_2 & a_0 - a_1 + a_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Het probleem is dus opgelost als we de 3×3 matrix M inverteren. Men kan dit (zonder eerst speciale waarden voor de a_i te kiezen) doen met de regel van Cramer uit de lineaire algebra.

In geval

$$a = 1 + \alpha^2, \quad \text{dus } (a_0, a_1, a_2) = (1, 0, 1),$$

is de inverse eenvoudig te bepalen met Gauss-eliminatie, er geldt:

$$M = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & -1 & 2 \end{pmatrix} \quad \text{dus} \quad M^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -1 & 2 \\ 1 & 3 & -1 \\ -1 & 2 & 1 \end{pmatrix}.$$

Dan is $M^{-1}(1, 0, 0) = \frac{1}{5}(3, 1, -1)$ en:

$$a = 1 + \alpha^2 \quad \implies \quad a^{-1} = \frac{3}{5} + \frac{1}{5}\alpha - \frac{1}{5}\alpha^2.$$

7.3 Eindige en algebraïsche uitbreidingen

Laat L een uitbreiding van een lichaam K zijn. Dan kunnen we L opvatten als een *lineaire ruimte* (=vectorruimte) over K . Dat wil zeggen, de elementen van K zien we als *scalair*en (met de gebruikelijke regels voor een lichaam), de elementen van L zien we als *vectoren* (een optelgroep) en de vectoren kunnen met scalairen vermenigvuldigd worden (hierbij gebruiken we dat K een deellichaam van L is).

Zo kunnen we bv. de complexe getallen zien als vectoren over \mathbb{R} , via het reële en imaginaire deel van een complex getal is er zelfs een isomorfisme van lineaire ruimtes over \mathbb{R} : $\mathbb{C} \cong \mathbb{R}^2$.

Definitie 7.3.1 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 7.2.1).

Voorbeeld 7.3.2 $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Immers, het minimumpolynoom van $\sqrt[3]{2}$ over \mathbb{Q} is $X^3 - 2$. Dus weten we dat $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3 - 2)$ en met behulp van stelling 3.3.4 ziet men gemakkelijk in dat dit een vectorruimte van dimensie 3 over \mathbb{Q} definieert. Zie ook stelling 7.3.3 hieronder voor een generalisatie van dit argument. Omdat een eindigdimensionale vectorruimte over \mathbb{Q} aftelbaar is (als S en T aftelbaar zijn, dan is $S \times T$ ook aftelbaar), is \mathbb{R} niet eindig over \mathbb{Q} .

Stelling 7.3.3 *Laat L een uitbreiding van het lichaam K zijn, en $\alpha \in L$.*

Dan geldt: α is algebraïsch over $K \iff K(\alpha)$ is eindig over K .

Voorts geldt: als α algebraïsch over K is, dan is

$$n := [K(\alpha) : K] = \text{gr}(f_K^\alpha) \quad \text{en} \quad 1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

is een K -basis van $K(\alpha)$.

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 $1, \alpha, \alpha^2, \dots, \alpha^n \in K(\alpha)$ een relatie

$$a_0 \cdot 1 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n = 0$$

bestaan, met $a_0, a_1, \dots, a_n \in K$, niet alle nul. Dat wil zeggen dat α een nulpunt is van het polynoom $a_0 + a_1X + \dots + a_nX^n \in K[X]$, dus α is algebraïsch over K .

\Rightarrow : Stel, omgekeerd, dat α algebraïsch over K is. Dan is $K(\alpha) = K[\alpha] \cong K[X]/(f_K^\alpha)$ (zie stelling 7.2.5). Omdat ieder element van $K[X]/(f_K^\alpha)$ wegens stelling 3.3.4 op unieke wijze te schrijven is als $a_0 + a_1X + \dots + a_{n-1}X^{n-1} + (f_K^\alpha)$ met $a_i \in K$ en $n := \text{gr}(f_K^\alpha)$ geldt $\dim_K(K[X]/(f_K^\alpha)) = n$. De lineaire ruimte $K[X]/(f_K^\alpha)$ wordt immers opgespannen door de nevenklassen van $1, X, \dots, X^{n-1}$ en uit de uniciteit van representanten van graad $< n$ voor elementen van $K[X]/(f_K^\alpha)$ volgt dat de nevenklassen van $1, X, \dots, X^{n-1}$ onafhankelijk zijn. Ze vormen dus een basis van $K[X]/(f_K^\alpha)$.

Het isomorfisme $K[X]/(f_K^\alpha) \cong K[\alpha]$ wordt gegeven door het evaluatiehomorfisme Φ_α ; het stuurt de nevenklasse $X^i + (f_K^\alpha)$ naar α^i en is ook K -lineair. Dus is $n = \text{gr}(f_K^\alpha) = \dim_K(K[X]/(f_K^\alpha)) = \dim_K(K[\alpha])$ en $1, \alpha, \dots, \alpha^{n-1}$ is een K -basis van $K[\alpha] = K(\alpha)$. Hiermee is 7.3.3 bewezen. \square

Stelling 7.3.4 *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 7.3.3 volgt nu dat α algebraïsch over K is. Aangezien α willekeurig gekozen was concluderen we dat L algebraïsch over K is. Dit bewijst 7.3.4. \square

7.3.5 Uit 7.3.3 en 7.3.4 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 deze paragraaf zullen we methoden aangeven om in zulke gevallen het minimumpolynoom van β over K te berekenen, zie 7.4. Zoals uit opgave 9 blijkt is de omkering van 7.3.4 fout: er bestaat voor sommige lichamen een algebraïsche uitbreiding die niet eindig is.

Stelling 7.3.6 *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 is eindig over $K \iff M$ is eindig over L en L is eindig over K .

Voorts geldt, als M eindig over K is:

$$[M : K] = [M : L] \cdot [L : K].$$

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 $\alpha_1, \dots, \alpha_n$ 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 $\alpha_1, \dots, \alpha_n$, 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 $\alpha_1, \alpha_2, \dots, \alpha_m$ van L over K en een basis $\beta_1, \beta_2, \dots, \beta_n$ 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

$$x = \sum_{j=1}^n y_j \beta_j \quad \text{met } y_1, \dots, y_n \in L.$$

Omdat $\alpha_1, \dots, \alpha_m$ een basis van L over K is, kan elke y_j geschreven worden als

$$y_j = \sum_{i=1}^m a_{ij} \alpha_i \quad \text{met } a_{ij} \in K \quad (1 \leq i \leq m, 1 \leq j \leq n).$$

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

$$\sum_{1 \leq i \leq m, 1 \leq j \leq n} c_{ij} \alpha_i \beta_j = 0, \quad \text{met } c_{ij} \in K.$$

Dan geldt

$$\sum_{j=1}^n \left(\sum_{i=1}^m c_{ij} \alpha_i \right) \beta_j = 0 \quad \text{met} \quad \sum_{i=1}^m c_{ij} \alpha_i \in L$$

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 $j = 1, 2, \dots, n$. 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 7.3.6 bewezen. □

7.3.7 Is L een uitbreiding van een lichaam K , en $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, dan definiëren we inductief

$$K(\alpha_1, \alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})(\alpha_n).$$

Gevolg 7.3.8 Laat L een lichaamsuitbreiding van K zijn, en stel dat $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ algebraïsch over K zijn. Dan is $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ eindig over K .

Bewijs. Met inductie naar n . Voor $n = 1$ kan men 7.3.3 toepassen. Laat vervolgens $n > 1$, en $K' = K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$. Uit de inductiehypothese volgt dan: K' is **eindig** 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 7.3.6 (met $L = K'$, $M = K'(\alpha_n)$) volgt nu dat $K'(\alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ eindig over K is, zoals verlangd. Dit bewijst 7.3.8. □

Stelling 7.3.9 Laat L een uitbreiding van een lichaam K zijn. Dan geldt:

a. als $\alpha, \beta \in L$ algebraïsch over K zijn, dan zijn ook

$$\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad \alpha/\beta \quad (\beta \neq 0)$$

algebraïsch over K .

b. de verzameling $\{\alpha \in L : \alpha \text{ is algebraïsch over } K\}$ is een deellichaam van L dat K omvat.

Bewijs.

- a. Wegens 7.3.8 is $K(\alpha, \beta)$ eindig over K , dus ook algebraïsch (zie 7.3.4). Volgens definitie 7.3.1 betekent dit dat alle elementen van $K(\alpha, \beta)$, in het bijzonder $\alpha \pm \beta$, $\alpha\beta$, α/β ($\beta \neq 0$), 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 7.3.9 bewezen.

□

7.3.10 De verzameling in 7.3.9 b. noemt men wel de **algebraïsche afsluiting van K in L** .

De laatste stelling van deze paragraaf is het analogon van 7.3.6, met ‘eindig’ vervangen door ‘algebraïsch’.

Stelling 7.3.11 *Laat K een lichaam zijn, L een uitbreiding van K , en M een uitbreiding van L . Dan geldt:*

$$M \text{ is algebraïsch over } K \iff \begin{array}{l} M \text{ is algebraïsch over } L \text{ en} \\ L \text{ is algebraïsch over } K. \end{array}$$

Bewijs. \Rightarrow : Deze implicatie volgt onmiddellijk 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 $\beta_1, \beta_2, \dots, \beta_n \in L$ zodanig dat

$$\alpha^n + \beta_1\alpha^{n-1} + \dots + \beta_{n-1}\alpha + \beta_n = 0.$$

Kennelijk is α ook algebraïsch over het deellichaam $K' = K(\beta_1, \beta_2, \dots, \beta_n)$ van L , dus $K'(\alpha)$ is eindig over K' . Omdat L algebraïsch is over K , zijn alle β_i algebraïsch over K , dus volgens 7.3.8 is $K' = K(\beta_1, \beta_2, \dots, \beta_n)$ eindig over K . Passen we nu 7.3.6 toe op $K \subset K' \subset K'(\alpha)$ dan vinden we dat $K'(\alpha)$ eindig is over K . Wegens 7.3.4 is $K'(\alpha)$ dan algebraïsch over K , en in het bijzonder is α algebraïsch over K , zoals verlangd. Hiermee is 7.3.11 aangetoond. □

7.4 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 7.3.4 weten we dat het *bestaat*.) Drie methoden hiervoor zullen we illustreren aan de hand van het geval $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (vgl. opgave 11), $\beta = 1 + \sqrt{2} + \sqrt{3}$.

- 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 7.3.6 en opgave 11). 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 $\beta^0, \beta^1, \beta^2, \dots$ van β als rijvectoren:

$$\begin{aligned}\beta^0 &= 1 &= (1, 0, 0, 0) \\ \beta^1 &= \beta &= (1, 1, 1, 0) \\ \beta^2 &= &= (6, 2, 2, 2) \\ \beta^3 &= &= (16, 14, 12, 6) \\ \beta^4 &= &= (80, 48, 40, 32).\end{aligned}$$

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 β^0, β^1, \dots eerder lineair afhankelijk worden.

Bij het bepalen wanneer precies de vectoren β^0, β^1, \dots afhankelijk worden kan in het algemene geval opgave 12 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 dat deze vier nulpunten bezit:

$$\begin{aligned} & (X - (1 + \sqrt{2} + \sqrt{3})) \\ & \quad \times \\ & (X - (1 + \sqrt{2} - \sqrt{3})) \\ & \quad \times \\ & (X - (1 - \sqrt{2} + \sqrt{3})) \\ & \quad \times \\ & (X - (1 - \sqrt{2} - \sqrt{3})) \end{aligned}$$

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 11.1.5 verderop, 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 13. Wel is het zo verkregen polynoom steeds *deelbaar* door het minimumpolynoom, het zit immers in $(f_{\mathbb{Q}}^{\beta}) = \ker(\Phi_{\beta})$ met

$$\Phi_{\beta} : \mathbb{Q}[X] \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad \Phi_{\beta}(f) := f(\beta) = f(1 + \sqrt{2} + \sqrt{3}).$$

- 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:

$$\begin{aligned} \beta - 1 &= \sqrt{2} + \sqrt{3} \\ (\beta - 1)^2 &= (\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{2} \cdot \sqrt{3} + 3 \\ &= 5 + 2\sqrt{2} \cdot \sqrt{3} \\ ((\beta - 1)^2 - 5)^2 &= (2\sqrt{2} \cdot \sqrt{3})^2 = 24 \end{aligned}$$

en als men de gevonden relatie uitwerkt ontdekt men weer dat β een nulpunt is van het polynoom

$$((X - 1)^2 - 5)^2 - 24 = X^4 - 4X^3 - 4X^2 + 16X - 8.$$

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 7.3.3 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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ bevat zijn in $\mathbb{Q}(\beta)$. Uiteraard ook $\mathbb{Q}(\beta) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, dus $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ en wegens opgave 11 heeft dit lichaam graad 4 over \mathbb{Q} , zoals verlangd.

7.5 Opgaven

1. Bewijs dat elke $\alpha \in \mathbb{Q}(\sqrt{2})$ algebraïsch over \mathbb{Q} is.
2. Bewijs dat de verzameling $\{\alpha \in \mathbb{C} : \alpha \text{ is algebraïsch over } \mathbb{Q}\}$ aftelbaar is (aanwijzing: $\mathbb{Q}[X]$ is aftelbaar, en elke $f \in \mathbb{Q}[X]$, $f \neq 0$, 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 's:
 $2 - \sqrt{3}$, $\sqrt[3]{2} + \sqrt[3]{4}$, $\sqrt{3 + 2\sqrt{2}}$; β^{-1} , $\beta + 1$ met $\beta^3 + 3\beta - 3 = 0$.
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 $\alpha \in \mathbb{R}$, $\alpha^3 - \alpha - 1 = 0$. Schrijf elk van de volgende elementen in de vorm $a + b\alpha + c\alpha^2$, met $a, b, c \in \mathbb{Q}$:

$$\alpha^{10}, \quad \alpha^{-10}, \quad (\alpha^2 + \alpha + 1)^2, \quad (\alpha^2 + 1)^{-1}.$$

9. Laat $L = \cup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$. Bewijs:
 - a. L is een lichaam (aanw.: $\mathbb{Q}(\sqrt[n]{2}) \cup \mathbb{Q}(\sqrt[m]{2}) \subset \mathbb{Q}(\sqrt[nm]{2})$);
 - 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} .
10. 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.

11. 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: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
12. Laat L een *eindige* uitbreiding van een lichaam K zijn, en $\alpha \in L$. Bewijs dat $\text{graad}(f_K^\alpha)$ een *deler* van $[L : K]$ is.
13. 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 $\mathbb{Q}[X]$.
14. 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 $\mathbb{Q}(\beta)$.
15. 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 $\alpha = \sqrt{2} + \sqrt[3]{5}$.
16. a. Ga na dat $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1) =: (X - 1)\Phi_5$ en dat Φ_5 irreducibel is in $\mathbb{Q}[X]$ (hint: substitueer $X := X + 1$ in Φ_5).
 b. Zij

$$M := \mathbb{Q}[X]/(\Phi_5), \quad \zeta := X + (\Phi_5),$$

$$\text{en zij } \beta := X + X^4 + (\Phi_5) \in M, \quad L := \mathbb{Q}[\beta] \subset M.$$

Bepaal $a, b \in \mathbb{Q}$ zodat $\beta^2 = a\beta + b$ 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.

17. Laat $\alpha \in \mathbb{R}$, $\alpha^3 - \alpha - 1 = 0$. Bereken van elk van de volgende elementen het minimumpolynoom over \mathbb{Q} :

$$\alpha - 1, \quad \alpha^2 + \alpha + 1, \quad (\alpha^2 + 1)^{-1}.$$

18. Laat α algebraïsch over een lichaam K zijn, en stel dat $[K(\alpha) : K]$ *oneven* is. Bewijs: $K(\alpha) = K(\alpha^2)$.
19. Laat L een uitbreiding van een lichaam K zijn, en laten $\alpha, \beta \in L$ algebraïsch over K zijn. Veronderstel dat $[K(\alpha) : K]$ en $[K(\beta) : K]$ *onderling ondeelbaar* zijn.

$$\text{Bewijs: } [K(\alpha, \beta) : K] = [K(\alpha) : K] \cdot [K(\beta) : K]$$

20. Laat L een uitbreiding van K zijn, en zij K_0 de algebraïsche afsluiting van K in L (zie 7.3.10).

Bewijs: elke $\alpha \in L, \alpha \notin K_0$ is transcendent over K_0 .

21. Laat α transcendent over een lichaam K zijn, en $\beta \in K(\alpha), \beta \notin K$.

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 .

22. Laat K een lichaam zijn.

a. ('breuk-splitsen'). Bewijs dat de volgende collectie een basis van $K(X)$ over K is:

$$\{X^n : n \in \mathbb{Z}_{\geq 0}\} \cup \{X^i \cdot f^{-m} : f \in K[X]\},$$

met in de tweede verzameling alleen irreducibele en monische $f \in K[X]$ en $m \in \mathbb{Z}_{>0}, 0 \leq i < \text{gr}(f)$.

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.

23. 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

$$L := K[T]/(f), \quad t := T + (f) \in L.$$

b. Zij $g = S^2 + Y \in L[S]$. Bewijs dat g irreducibel is en zij

$$M := L[S]/(g), \quad s := S + (g) \in M.$$

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: $\text{gr}(f_K^\alpha) = 2$. Concludeer dat de uitbreiding M van K niet enkelvoudig is.

8 Lichaamsautomorfismen en ontbindingslichamen

8.1 Lichaamshomomorfismen

8.1.1 Ter herinnering: Als K en L lichamen zijn, dan is $\phi : K \rightarrow L$ een **lichaamshomomorfisme** als ϕ een (unitair) homomorfisme van ringen is (zie 2.1.1), i.h.b. geldt $\phi(1) = 1$.

In het bijzonder is

$$\phi\left(\frac{1}{a}\right) = \phi(a)^{-1}, \quad \phi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)},$$

want uit $\phi(a) \cdot \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(1) = 1$ volgt $\phi(a^{-1}) = (\phi(a))^{-1}$.

Omdat $\phi(1 + 1 + \dots + 1) = 1 + 1 + \dots + 1$, is het beeld van het priemlichaam K_0 van K (zie 7.1.1) het priemlichaam L_0 van L . I.h.b. geeft ϕ een isomorfisme van K_0 naar L_0 . Als $K \subset L$ dan is $K_0 = L_0$ en ϕ beperkt tot K_0 is de identiteit.

8.1.2 Het beeld $\phi(K)$ van een lichaamshomomorfisme is weer een lichaam. Een lichaamshomomorfisme is injectief (omdat K alleen (0) en K als ideaal heeft en $1 \notin \ker(\phi)$). Het hoeft niet surjectief te zijn (bv. $\mathbb{R} \hookrightarrow \mathbb{C}$), zelfs niet als $K = L$ (zie voorbeeld 8.1.4 hieronder).

De samenstelling van lichaamshomomorfismen

$$K \xrightarrow{\phi} L \xrightarrow{\psi} M$$

is weer een lichaamshomomorfisme, zoals je makkelijk narekent.

In geval $\text{kar}(K) = p$ is er het volgende interessante lichaamshomomorfisme.

Stelling 8.1.3 *Zij K een lichaam met $\text{kar}(K) = p > 0$. Zij*

$$F : K \longrightarrow K, \quad F : x \mapsto x^p.$$

*Dan is F een lichaamshomomorfisme, en F heet het **Frobenius-homomorfisme**.*

Indien K eindig is, is F zelfs een lichaamsautomorfisme.

Bewijs. Merk op dat $F(1) = 1$ en dat $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$ (want K is commutatief). We moeten nog bewijzen dat $F(a+b) := (a+b)^p$ gelijk is aan $F(a) + F(b) := a^p + b^p$.

Volgens het binomium van Newton, dat geldig is in iedere commutatieve ring, hebben we:

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}, \quad \text{met} \quad \binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}.$$

De teller van $\binom{p}{k}$ is deelbaar door p , maar de noemer niet als $0 < k < p$ omdat p een priemgetal is. Dan is

$$(a + b)^p = a^p + b^p + p \cdot c,$$

voor zekere $c \in K$. Omdat $p = 1 + 1 + \dots + 1$ ($p \times$) en $\text{kar}(K) = p$ volgt dat $p = 0 \in K$. We concluderen dat $(a + b)^p = a^p + b^p$.

Als K eindig is, is iedere injectieve afbeelding van K naar zichzelf (dus i.h.b. F) ook surjectief, dus F is bijectief. Dat F^{-1} ook een lichaamshomomorfisme is, is eenvoudig na te rekenen. Hiermee is Stelling 8.1.3 bewezen. \square

Voorbeeld 8.1.4 Zij $K = \mathbb{F}_p(T)$, het lichaam van rationale functies (= quotiënten van polynomen) met coëfficiënten in \mathbb{F}_p . Zij $f(T) = \frac{a_0 + a_1 T + \dots + a_n T^n}{b_0 + b_1 T + \dots + b_m T^m} \in \mathbb{F}_p(T)$, dan is

$$\begin{aligned} F(f(T)) &= F\left(\frac{a_0 + a_1 T + \dots + a_n T^n}{b_0 + b_1 T + \dots + b_m T^m}\right) \\ &= \frac{F(a_0 + a_1 T + \dots + a_n T^n)}{F(b_0 + b_1 T + \dots + b_m T^m)} \\ &= \frac{F(a_0) + F(a_1)F(T) + \dots + F(a_n)F(T^n)}{F(b_0) + F(b_1)F(T) + \dots + F(b_m)F(T^m)} \\ &= \frac{a_0 + a_1 T^p + \dots + a_n T^{pn}}{b_0 + b_1 T^p + \dots + b_m T^{pm}} = f(T^p), \end{aligned}$$

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 $T \notin \text{beeld}(F)$ (ga na).

8.1.5 Als L en L' twee uitbreidingen van een lichaam K zijn, dan is een K -**homomorfisme** $L \rightarrow L'$ een ringhomomorfisme

$$\phi : L \rightarrow L' \quad \text{met} \quad \phi|_K = \text{id}_K,$$

de identiteit op K , en een K -**isomorfisme** is een bijectief K -homomorfisme. De lichamen L en L' heten K -**isomorf** als er een K -isomorfisme $L \rightarrow L'$ bestaat, notatie $L \cong_K L'$

Een K -**automorfisme** is een K -isomorfisme met $L = L'$.

8.1.6 In het bijzonder is elk homomorfisme $K \rightarrow L$ een K_0 -homomorfisme met K_0 het priemlichaam van K , zie 8.1.1. Voor een uitbreiding L van K schrijven we $\text{Aut}_K(L)$ voor de groep van K -automorfismen van L (voor $\phi, \psi \in \text{Aut}_K(L)$ is het produkt $\phi\psi \in \text{Aut}_K(L)$ gedefinieerd door samenstelling: $(\phi\psi)(x) = \phi(\psi(x))$).

Stelling 8.1.7 *Zij L een eindige uitbreiding van het lichaam K en zij $\alpha \in L$ met minimumpolynoom $f_K^\alpha \in K[X]$.*

- a. *Voor elke $\phi \in \text{Aut}_K(L)$ geldt dat $\phi(\alpha)$ weer een nulpunt van f_K^α is.*
- b. *Zij m het aantal nulpunten van f_K^α in het lichaam $K[\alpha] \subset L$.
Dan is $\#\text{Aut}_K(K[\alpha]) = m$, waarbij $\#$ het aantal elementen in de groep aangeeft.
In het bijzonder is het aantal K -automorfismen van $K[\alpha] \leq \text{gr}(f_K^\alpha)$.*

Bewijs. We schrijven

$$f_K^\alpha = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \quad \text{met } a_i \in K.$$

Passen we $\phi \in \text{Aut}_K(L)$ toe op de identiteit $0 = f_K^\alpha(\alpha)$ dan komt er:

$$\begin{aligned} 0 &= \phi(\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) \\ &= \phi(\alpha)^n + \phi(a_{n-1})\phi(\alpha)^{n-1} + \dots + \phi(a_1)\phi(\alpha) + \phi(a_0) \\ &= \phi(\alpha)^n + a_{n-1}\phi(\alpha)^{n-1} + \dots + a_1\phi(\alpha) + a_0 \\ &= f_K^\alpha(\phi(\alpha)), \end{aligned}$$

waarbij we gebruikten dat $\phi(a_i) = a_i$ (immers $a_i \in K$ en $\phi|_K = \text{id}_K$). We concluderen dat $\phi(\alpha)$ inderdaad ook een nulpunt van f_K^α is.

Voor het tweede onderdeel bewijzen we dat de afbeelding:

$$\Delta : \text{Aut}_K(K[\alpha]) \longrightarrow \{\alpha_1, \alpha_2, \dots, \alpha_m\}, \quad \Delta(\phi) := \phi(\alpha)$$

een bijectie is, hierin is $\{\alpha_1, \dots, \alpha_m\} \subset K[\alpha]$ de verzameling van nulpunten van f_K^α in $K[\alpha]$, met $\alpha_1 = \alpha$.

Dat Δ goed gedefinieerd is volgt uit het eerste onderdeel. We laten nu zien dat Δ injectief is. Iedere $x \in K[\alpha]$ is op unieke wijze te schrijven als $x = x_0 + x_1\alpha + \dots + x_{n-1}\alpha^{n-1}$ met $x_i \in K$. Dan is

$$\begin{aligned} \phi(x) &= \phi(x_0) + \phi(x_1)\phi(\alpha) + \dots + \phi(x_{n-1})\phi(\alpha)^{n-1} \\ &= x_0 + x_1\phi(\alpha) + \dots + x_{n-1}\phi(\alpha)^{n-1}, \end{aligned}$$

dus $\phi(x)$ is volledig bepaald door $\phi(\alpha) = \Delta(\phi)$. Als $\Delta(\phi) = \Delta(\psi)$ dan geldt dus: $\phi(x) = \psi(x)$ voor iedere $x \in K[\alpha]$ oftewel $\phi = \psi$.

Om surjectiviteit te bewijzen, moeten we voor elke nulpunt $\beta \in K[\alpha]$ van f_K^α een K -automorfisme ϕ construeren met $\phi(\alpha) = \beta$. Dat gaat als volgt. Zij

$$\Phi_\beta : K[X] \longrightarrow K[\alpha], \quad \Phi_\beta(f) := f(\beta),$$

het evaluatiehomorfisme. Aangezien β een nulpunt is van $f_K^\alpha \in K[X]$ geldt $f_K^\alpha \in \ker(\Phi_\beta)$. Omdat f_K^α irreducibel is in $K[X]$ geldt dan $\ker(\Phi_\beta) = (f_K^\alpha)$. Dus induceert Φ_β een injectief K -homorfisme $\overline{\Phi}_\beta : K[X]/(f_K^\alpha) \rightarrow K[\alpha]$ met als beeld $K[\beta] \subset K[\alpha]$. De eerste isomorfiestelling voor ringen 2.2.9 levert dan dat $K[\beta] \cong K[X]/(f_K^\alpha)$; in het bijzonder is dit isomorfisme K -lineair. Dus is $K[\beta]$ een lineaire deelruimte van $K[\alpha]$ van dimensie $\dim_K(K[X]/(f_K^\alpha)) = \dim_K(K[\alpha])$. Deze dimensie is eindig en dus volgt $K[\beta] = K[\alpha]$; met andere woorden $\overline{\Phi}_\beta$ is een isomorfisme. Schrijf $\overline{\Phi}_\alpha$ voor het isomorfisme $K[X]/(f_K^\alpha) \xrightarrow{\cong} K[\alpha]$ dat door het evaluatiehomorfisme Φ_α wordt geïnduceerd. We hebben dan isomorfismen:

$$\begin{array}{ccc} & & K[\alpha] \\ & \nearrow \overline{\Phi}_\alpha & \\ K[X]/(f_K^\alpha) & & \\ & \searrow \overline{\Phi}_\beta & \\ & & K[\beta] = K[\alpha] \end{array}$$

Dit geeft een K -automorfisme

$$\phi := \overline{\Phi}_\beta \circ \overline{\Phi}_\alpha^{-1} : K[\alpha] \xrightarrow{\cong} K[\alpha].$$

Uit de definitie van evaluatiehomorfisme volgt:

$$\overline{\Phi}_\alpha^{-1}(\alpha) = X + (f_K^\alpha) \quad \text{en} \quad \overline{\Phi}_\beta(X + (f_K^\alpha)) = \beta,$$

en dus: $\phi(\alpha) = \beta$. Hiermee is de stelling bewezen. \square

Voorbeeld 8.1.8 Zij $f \in K[X]$ een monisch irreducibel polynoom van graad 2 en zij $L = K[X]/(f)$. We schrijven $\alpha := X + (f) \in L$ dan is α een nulpunt van f in $L = K[\alpha]$. We kunnen f schrijven als $f = X^2 + aX + b$ en zoals je makkelijk narekent met het delingsalgoritme, geldt in $L[X]$:

$$X^2 + aX + b = (X - \alpha)(X - (-a - \alpha)).$$

Er zijn nu twee gevallen:

$$(i) \quad \alpha = -a - \alpha, \quad (ii) \quad \alpha \neq -a - \alpha.$$

In het eerste geval volgt $2\alpha = -a$. Als $2 \neq 0$ in K , dan is $\alpha = -a/2 \in K$ in tegenspraak met de irreducibiliteit van f . Het eerste geval treed dus alleen op als $\text{kar}(K) = 2$ en $a = 0$. Een voorbeeld van zo'n irreducibele f is het polynoom $f = X^2 + T$ in de polynoomring $K[X]$ met $K = \mathbb{F}_2(T)$, het lichaam van de rationale functies in de variabele T met coëfficiënten in \mathbb{F}_2 . (Als f reducibel was, dan was $(g/h)^2 = T$ ofwel $g^2 = Th^2$ voor zekere $g, h \in \mathbb{F}_2[T]$ maar vergelijken van de graden laat zien dat dit onmogelijk is.)

In het tweede geval zijn er twee verschillende nulpunten in L en dus is $\#Aut_K(L) = 2$. Omdat er maar één groep is met twee elementen geldt:

$$Aut_K(L) = \{id_L, \phi\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Dan is $\phi(\alpha) = -a - \alpha$ en dus is $\phi(x + y\alpha) = \phi(x) + \phi(y)\phi(\alpha) = x + y(-a - \alpha)$ zodat:

$$\phi : L \rightarrow L, \quad x + y\alpha \mapsto (x - ay) - y\alpha \quad (x, y \in K).$$

Een zeer bekend voorbeeld is natuurlijk $K = \mathbb{R}$ en $f = X^2 + 1$. In dit geval is ϕ de complexe conjugatie.

Een ander voorbeeld wordt gegeven door de eindige lichamen $L = \mathbb{F}_p[X]/(X^2 - d)$ met d een niet-kwadraat in \mathbb{F}_p (zie 5.2.8), i.h.b. is $p > 2$. In dat geval is

$$\phi : L \rightarrow L, \quad \phi : x + y\alpha \mapsto x - y\alpha, \quad x, y \in \mathbb{F}_p$$

het lichaamsautomorfisme.

Anderzijds geeft stelling 8.1.3 ook het Frobeniusautomorfisme F . Er geldt:

$$F(x + y\alpha) = F(x) + F(y)F(\alpha) = x + y\alpha^p,$$

want $x, y \in \mathbb{F}_p$, het priemlichaam van L . We zullen laten zien:

$$F = \phi.$$

Omdat $\#Aut_{\mathbb{F}_p}(L) = 2$ is het voldoende te bewijzen dat $F \neq id_L$. Welnu, als wel $F = id_L$, dan zou $x^p = x$ voor elke $x \in L$, dus het polynoom $X^p - X$ zou minstens $\#L > p$ nulpunten hebben. Maar dat is in tegenspraak met stelling 3.5.2. Dus concluderen we $F \neq id_L$ en daarom $F = \phi$.

Uit $F = \phi$ volgt $\alpha^p = F(\alpha) = \phi(\alpha) = -\alpha$. Omdat $p > 2$ priem en dus oneven is, kunnen we schrijven: $p = 2\left(\frac{p-1}{2}\right) + 1$ met $\frac{p-1}{2} \in \mathbb{Z}$. Dan is:

$$\alpha^p = (\alpha^2)^{\frac{p-1}{2}} \alpha = d^{\frac{p-1}{2}} \alpha.$$

Kennelijk is dus $d^{\frac{p-1}{2}} = -1$ in $\mathbb{F}_p \subset L$. We komen hier in stelling 14.1.4 nog op terug.

8.2 Ontbindingslichamen

We hebben al gezien dat er voor ieder irreducibel polynoom $f \in K[X]$ een eindige uitbreiding M van K bestaat waarin f een nulpunt heeft, we kunnen nl. $M = K[X]/(f)$ nemen, zie 5.2.6. In $M[X]$ kan f dan geschreven worden als $f = (X - \alpha)g$, maar we weten i.h.a. niet of g nulpunten heeft in M . Om een lichaam te vinden waarin f precies $gr(f)$ nulpunten heeft (geteld met multipliciteit), ontbinden we f (in feite g) in irreducibele factoren in $M[X]$. Indien er nog een irreducibele factor van graad ≥ 2 is, kunnen we opnieuw een eindige uitbreiding maken (van M en dus ook van K) waarin deze factor een nulpunt heeft. Na een eindig aantal stappen verkrijgen we zo een lichaam L , een eindige uitbreiding van K , zodat f in $L[X]$ in lineaire factoren ontbonden kan worden:

$$f = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n), \quad \alpha_i \in L.$$

We werken dit uit in (het bewijs van) stelling 8.2.4

Definitie 8.2.1 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 $\alpha_1, \dots, \alpha_n \in L$ zijn zodanig dat

- a. $f = \prod_{i=1}^n (X - \alpha_i)$ in $L[X]$,
- b. $L = K(\alpha_1, \dots, \alpha_n)$.

8.2.2 Onnauwkeurig kan men dit uitdrukken door te zeggen: een ontbindingslichaam van f over K ontstaat door ‘alle’ nulpunten van f aan K te adjungeren (maar ja, nulpunten in wat?). Merk op dat een ontbindingslichaam van f *eindig* over K is, wegens b) van de definitie en gevolg 7.3.8.

Voorbeeld 8.2.3 Zij $f = X^3 - n$ met $n \in \mathbb{Q}$ en $n \neq k^3$ voor alle $k \in \mathbb{Q}$. We bepalen een ontbindingslichaam M voor f en we bepalen $Aut(M) = Aut_{\mathbb{Q}}(M)$.

Het polynoom f is irreducibel in $\mathbb{Q}[X]$, want het heeft graad 3 en geen nulpunt in \mathbb{Q} wegens de keuze van n . Zij

$$L := \mathbb{Q}[X]/(f), \quad \alpha_1 := X + (f) \in L,$$

dan is L een lichaam en α_1 is een nulpunt van f in L . Dus $\alpha_1 \in L$ en $\alpha_1^3 = n$ en $[L : \mathbb{Q}] = 3$.

In $L[X]$ bezit f de ontbinding

$$f(X) = X^3 - n = (X - \alpha_1)(X^2 + \alpha_1 X + \alpha_1^2) =: (X - \alpha_1)g(X).$$

We laten nu zien dat $g(X)$ irreducibel is in $L[X]$. Voldoende hiervoor is om aan te tonen dat g geen nulpunt heeft in L . Welnu, zou $\beta \in L$ een nulpunt van g zijn, dan zou $0 = \beta^2 + \alpha_1 \beta + \alpha_1^2 = \alpha_1^2 \left(\left(\frac{\beta}{\alpha_1}\right)^2 + \left(\frac{\beta}{\alpha_1}\right) + 1 \right)$ en dus zou $\frac{\beta}{\alpha_1} \in L$ een nulpunt van $X^2 + X + 1$ zijn. Het polynoom $X^2 + X + 1 \in \mathbb{Q}[X]$ is monisch en irreducibel, dus het zou dan het minimumpolynoom van $\frac{\beta}{\alpha_1}$ over \mathbb{Q} moeten zijn. Maar dit is onmogelijk wegens $[L : \mathbb{Q}] = 3$; vergelijk opgave 12 in hoofdstuk 7. We concluderen dus dat $g(X)$ irreducibel in $L[X]$ is.

Vervolgens adjungeren we een nulpunt van g aan L . Zij

$$M := L[Y]/(g) \quad \text{en} \quad \alpha_2 := Y + (g) \in M.$$

(We schrijven Y in plaats van X om verwarring te voorkomen(!)) Dan is M een tweedegraadsuitbreiding van L en dus een uitbreiding van graad 6 van \mathbb{Q} (stelling 7.3.6). $\alpha_2 \in M$ is een nulpunt van g en dus ook van f . In $M[Z]$ geldt $g(Z) = Z^2 + \alpha_1 Z + \alpha_1^2 = (Z - \alpha_2)(Z - \alpha_3)$ met $\alpha_3 = -\alpha_1 - \alpha_2$. Merk op dat $\alpha_2 \neq \alpha_3$, want anders zou $\alpha_2 \in M$ ook een nulpunt van de afgeleide van f zijn. Dus concluderen we dat f precies drie verschillende nulpunten $\alpha_1, \alpha_2, \alpha_3$ in M heeft, en in $M[X]$ geldt $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$.

Omdat $M = L(\alpha_2) = L(\alpha_2, \alpha_3)$ en $L = \mathbb{Q}(\alpha_1)$ geldt:

$$M = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3),$$

zodat M een ontbindingslichaam voor f over \mathbb{Q} is.

In feite geldt zelfs dat $M = \mathbb{Q}[\alpha_1, \alpha_2]$ en elke $m \in M$ is te schrijven als:

$$m = a_0 + a_1 \alpha_1 + a_2 \alpha_1^2 + (b_0 + b_1 \alpha_1 + b_2 \alpha_1^2) \alpha_2,$$

met $a_i, b_i \in \mathbb{Q}$ (ga na).

We bewijzen nu dat:

$$\text{Aut}_{\mathbb{Q}}(M) \cong S_3,$$

waar S_3 de groep van permutaties van $\{1, 2, 3\}$ is. Merk op dat $Aut(M) = Aut_{\mathbb{Q}}(M)$ want \mathbb{Q} is het priemlichaam. Iedere $\phi \in Aut_{\mathbb{Q}}(M)$ permuteert de drie wortels van f in M . Dit geeft een homomorfisme

$$\pi : Aut_{\mathbb{Q}}(M) \longrightarrow S_3, \quad \pi : \phi \mapsto \sigma,$$

waarbij $\sigma \in S_3$ gedefinieerd wordt door: $\phi(\alpha_i) = \alpha_{\sigma(i)}$. We laten zien dat π injectief en surjectief is, waarmee $Aut_{\mathbb{Q}}(M)$ bepaald is.

Laat $\phi \in \ker(\pi)$, dan is dus $\phi(\alpha_i) = \alpha_i$ voor elke i . Passen we ϕ toe op $m \in M$ dan laat de schrijfwijze voor m hierboven zien dat $\phi(m) = m$, dus ϕ is de identiteit op M . We concluderen dat π injectief is.

Om de surjectiviteit van π te bewijzen, construeren we lichaamsautomorfismen van M . Omdat $\mathbb{Q} \subset L \subset M$, is $Aut_L(M) \subset Aut_{\mathbb{Q}}(M)$ een ondergroep. Omdat $M = L[Y]/(g)$, met g een tweedegraads polynoom met verschillende nulpunten, heeft $Aut_L(M)$ precies één element ϕ_1 ongelijk aan de identiteit. Omdat ϕ_1 de identiteit is op L geldt $\phi_1(\alpha_1) = \alpha_1$. Omdat ϕ_1 niet de identiteit is op M verwisselt ϕ_1 de nulpunten α_2 en α_3 van g , dus:

$$\phi_1(\alpha_1) = \alpha_1, \quad \phi_1(\alpha_2) = \alpha_3, \quad \phi_1(\alpha_3) = \alpha_2 \quad \implies \quad \pi(\phi_1) = (2\ 3),$$

een paarwisseling in S_3 . Laat $L_2 := \mathbb{Q}(\alpha_2) \subset M$. Omdat α_2 een nulpunt is van het irreducibele polynoom f volgt dat $L_2 \cong \mathbb{Q}[X]/(f)$, en we kunnen bovenstaande redering herhalen met L_2 i.p.v. L . I.h.b. vinden we een $\phi_2 \in Aut_{L_2}(M) \subset Aut_{\mathbb{Q}}(M)$ met:

$$\phi_2(\alpha_1) = \alpha_3, \quad \phi_2(\alpha_2) = \alpha_2, \quad \phi_2(\alpha_3) = \alpha_1 \quad \implies \quad \pi(\phi_2) = (1\ 3).$$

Omdat S_3 wordt voortgebracht door de twee paarwisselingen (1 3) en (2 3) is het homomorfisme π surjectief.

Hiermee is bewezen dat $Aut(M) \cong S_3$.

Stelling 8.2.4 *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 $n = \text{gr}(f)$.

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 $E = K(\beta_1, \beta_2, \dots, \beta_m)$ 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 grondlichaam, dat er een ontbindingslichaam $L = E(\gamma_1, \gamma_2, \dots, \gamma_k)$ 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 $L = E(\gamma_1, \gamma_2, \dots, \gamma_k) = K(\beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_k)$.

Neem vervolgens aan dat f irreducibel is in $K[X]$. Dan is er wegens 5.2.6 een uitbreiding $K(\alpha)$ met $f(\alpha) = 0$. Volgens 3.5.1 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 $L = K(\alpha)(\alpha_1, \dots, \alpha_{n-1})$ 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 $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ en $f = \prod_{i=1}^n (X - \alpha_i)$ in $L[X]$, dus L is een ontbindingslichaam van f over K . Dit bewijst 8.2.4. \square

We gaan vervolgens de *uniciteit* van het ontbindingslichaam bewijzen. Eerst bewijzen we iets algemeners.

Stelling 8.2.5 *Laat $\phi : K_0 \rightarrow K_1$ een isomorfisme van een lichaam K_0 naar een lichaam K_1 zijn, en zij*

$$\Phi : K_0[X] \longrightarrow K_1[X], \quad \sum_i a_i X^i \mapsto \sum_i \phi(a_i) X^i$$

het door ϕ geïnduceerde isomorfisme van polynoomringen. Zij $f_0 \in K_0[X]$ een monisch polynoom en zij L_0 een ontbindingslichaam van f_0 over K_0 .

Zij L_1 een ontbindingslichaam van $f_1 := \Phi(f_0) \in K_1[X]$ over K_1 .

Dan is er een isomorfisme

$$\begin{array}{ccc} & & K_0 \hookrightarrow L_0 \\ \psi : L_0 \rightarrow L_1 & \psi|_{K_0} = \phi : & \phi \downarrow \qquad \downarrow \psi \\ & & K_1 \hookrightarrow L_1 \end{array}$$

Bewijs. Uit 8.2.1(b) en 7.3.8 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 $\beta_1, \dots, \beta_n \in K_0$. Dan is $f_1 = \Phi(f_0) = \prod_{i=1}^n \Phi(X - \beta_i) = \prod_{i=1}^n (X - \Phi(\beta_i)) \in K_1[X]$. 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 $\chi : K_0(\alpha_0) \rightarrow K_1(\alpha_1)$ 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 $h_0 \in K_0[X]$ het minimumpolynoom van α_0 over K_0 :

$$h_0 := f_{K_0}^{\alpha_0}, \quad \text{en zij } h_1 := \Phi(h_0).$$

Omdat $f_0(\alpha_0) = 0$ is h_0 een deler van f_0 in $K_0[X]$:

$$f_0 = h_0 q_0 \in K_0[X] \quad \text{dus} \quad f_1 = h_1 \Phi(q_0) \in K_1[X].$$

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. We bewijzen nu dat $K_0(\alpha_0) \cong K_1(\alpha_1)$.

Wegens 7.2.5 is er een isomorfisme

$$K_0[X]/(h_0) \xrightarrow{\cong} K_0(\alpha_0), \quad X + (h_0) \mapsto \alpha_0. \quad (1)$$

Omdat h_0 irreducibel is in $K_0[X]$ en Φ een isomorfisme is, is $h_1 = \Phi(h_0)$ irreducibel in $K_1[X]$. Omdat $h_1(\alpha_1) = 0$ moet dus h_1 het minimumpolynoom van α_1 over K_1 zijn. Opnieuw wegens 7.2.5 is er dus een isomorfisme

$$K_1[X]/(h_1) \xrightarrow{\cong} K_1(\alpha_1), \quad X + (h_1) \mapsto \alpha_1. \quad (2)$$

Tenslotte beeldt het isomorfisme $\Phi : K_0[X] \xrightarrow{\cong} K_1[X]$ het ideaal voortgebracht door h_0 af op het ideaal voortgebracht door $h_1 = \Phi(h_0)$, en induceert dus een isomorfisme

$$\bar{\Phi} : K_0[X]/(h_0) \xrightarrow{\cong} K_1[X]/(h_1), \quad X + (h_0) \mapsto X + (h_1), \quad (3)$$

dat beperkt tot K_0 gelijk is aan ϕ . Combineren we de isomorfismen (1), (2) en (3) dan vinden we een isomorfisme

$$\chi : K_0(\alpha_0) \xrightarrow{\cong} K_1(\alpha_1), \quad \alpha_0 \mapsto \alpha_1, \quad \chi|_{K_0} = \phi.$$

Om ψ te verkrijgen passen we nu de inductiehypothese toe op de rechter helft van het diagram:

$$\begin{array}{ccccc} K_0 & \hookrightarrow & K_0(\alpha_0) & \hookrightarrow & L_0 \\ \phi \downarrow & & \chi \downarrow & & \downarrow \psi \\ K_1 & \hookrightarrow & K_1(\alpha_1) & \hookrightarrow & L_1 \end{array}$$

We hadden α_0 buiten K_0 gekozen, dus $[K_0(\alpha_0) : K_0] > 1$ en daarom is

$$[L_0 : K_0(\alpha_0)] = \frac{[L_0 : K_0]}{[K_0(\alpha_0) : K_0]} < [L_0 : K_0],$$

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 $\psi : L_0 \rightarrow L_1$ met $\psi|_{K_0(\alpha_0)} = \chi$, dus $\psi|_{K_0} = \phi$. Hiermee is het bewijs van 8.2.5 geleverd. \square

We kunnen nu de belangrijkste stelling betreffende ontbindingslichamen uitspreken en bewijzen.

Stelling 8.2.6 *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.

In het vervolg kunnen we dus 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 8.2.4. Stel nu dat L en L' twee ontbindingslichamen van f over K zijn; we moeten bewijzen dat er een K -isomorfisme $\psi : L \rightarrow L'$ bestaat. Maar dit volgt direct door 8.2.5 toe te passen op $K_0 = K_1 = K$, $f_0 = f_1 = f$, $\phi = id_K$, $L_0 = L$, $L_1 = L'$. Hiermee is 8.2.6 bewezen. \square

8.2.7 Opmerking. Het K -isomorfisme $\psi : L \rightarrow L'$ tussen twee ontbindingslichamen van f over K hoeft niet eenduidig bepaald te zijn. Als σ een K -automorfisme van L is, is ook $\psi' = \psi \circ \sigma : L \rightarrow L'$ een K -isomorfisme, en men ziet gemakkelijk in dat zo uit één vaste ψ alle mogelijke K -isomorfismen $\psi' : L \rightarrow L'$ verkregen worden.

Voorbeeld 8.2.8 We keren terug naar voorbeeld 8.2.3. Dan is $f = X^3 - n$ en in $\mathbb{C}[X]$ geldt:

$$f(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3) \quad \text{met :}$$

$$\beta_1 = \sqrt[3]{n}, \quad \beta_2 = \sqrt[3]{n} \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \right), \quad \beta_3 = \sqrt[3]{n} \left(\cos \frac{2\pi}{3} - i \sin \frac{2\pi}{3} \right).$$

Dan is $\mathbb{Q}(\beta_1, \beta_2, \beta_3) \subset \mathbb{C}$ ook een splijtlichaam van f . Daarom is het isomorf met het in 8.2.3 onderzochte splijtlichaam $M = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. I.h.b. geldt:

$$[\mathbb{Q}(\beta_1, \beta_2, \beta_3) : \mathbb{Q}] = 6 \quad \text{en} \quad \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\beta_1, \beta_2, \beta_3)) \cong S_3.$$

8.3 Opgaven

1. Laat L een ontbindingslichaam van f over K zijn, en $f = \prod_{i=1}^n (X - \alpha_i)$ in $L[X]$. Bewijs: $L = K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ (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 8.2.4.)
3. Bewijs dat $L = \mathbb{Q}(\sqrt[4]{2}, i)$ een ontbindingslichaam van $X^4 - 2$ over \mathbb{Q} is. Bepaal ook $[L : \mathbb{Q}]$ en $\#Aut(L)$.
Probeer te bewijzen dat $Aut_{\mathbb{Q}(i)}(L) \cong \mathbb{Z}/4\mathbb{Z}$.
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 $\zeta^2, \zeta^3, \zeta^4$ de andere nulpunten van f in \mathbb{C} zijn. Bewijs dat $\mathbb{Q}(\zeta)$ een ontbindingslichaam van f over \mathbb{Q} is. Bepaal ook $Aut(\mathbb{Q}(\zeta))$.
6. Bewijs: $\Omega_{\mathbb{Q}}^{X^2-2} \not\cong \Omega_{\mathbb{Q}}^{X^2-3}$, maar $\Omega_K^{X^2-2} \simeq \Omega_K^{X^2-3}$ voor $K = \mathbb{F}_5$.
7. Bewijs dat $\mathbb{Q}(i, \sqrt{2})$ een ontbindingslichaam van $f_{\mathbb{Q}}^{i+\sqrt{2}}$ over \mathbb{Q} is. Bewijs: $Aut(\mathbb{Q}(i, \sqrt{2})) \simeq V_4$, de viergroep van Klein.
8. Laat L een ontbindingslichaam van f over K zijn, met $gr(f) = n$.
 - a. Bewijs: elke K -automorfisme van L permuteert de nulpunten van f in L ,
 - b. de groep $Aut_K(L)$ is isomorf met een ondergroep van S_n ;
 - c. $\#Aut_K(L)$ is een deler van $n!$.
9. Bewijs: $Aut(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})) \simeq S_3$.
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 $\mathbb{Q}(\alpha) = \Omega_{\mathbb{Q}}^f$. Bewijs ook dat $Aut(\Omega_{\mathbb{Q}}^f) \cong \mathbb{Z}/3\mathbb{Z}$.
11. Zij K een lichaam. Bewijs dat de afbeelding

$$\phi : K(X) \longrightarrow K(X), \quad f \mapsto f(X + 1)$$

een lichaamsautomorfisme is. Bepaal de orde van ϕ in $Aut(K(X))$.

9 Eindige lichamen

Een lichaam K heet **eindig** als het aantal elementen van K eindig is. We hebben al enige voorbeelden van eindige lichamen gezien: $\mathbb{Z}/p\mathbb{Z}$ met p priem, zie 1.18; een lichaam met 4 elementen, zie 3.3.6; en lichamen met p^2 elementen voor $p > 2$, zie 5.2.8.

9.1 Classificatie van eindige lichamen.

De volgende stelling classificeert de eindige lichamen.

Stelling 9.1.1

a. *Zij 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.*

Het eenduidig bepaalde lichaam met $q = p^n$ elementen wordt aangegeven met \mathbb{F}_q en het is het ontbindingslichaam van $X^q - X$ over \mathbb{F}_p :

$$\mathbb{F}_q \cong \Omega_{\mathbb{F}_p}^{X^q - X}.$$

Bewijs.

a. Laat K een eindig lichaam zijn. Dan kan K niet het lichaam \mathbb{Q} als deellichaam hebben, dus $\text{kar}(K) \neq 0$ (zie 7.1.2). 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, \dots, e_n voor K over \mathbb{F}_p . Elk element $x \in K$ kan dan eenduidig geschreven worden als

$$x = a_1 e_1 + a_2 e_2 + \dots + a_n e_n \quad \text{met} \quad a_i \in \mathbb{F}_p, \quad 1 \leq i \leq n.$$

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 $p \cdot p \cdot \dots \cdot p = p^n$. 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 $\alpha_1, \alpha_2, \dots, \alpha_q \in K$ met $X^q - X = \prod_{i=1}^q (X - \alpha_i)$ in $K[X]$. De verzameling van nulpunten:

$$A = \{\alpha_1, \alpha_2, \dots, \alpha_q\} \quad (\subset K)$$

gaan we nu nader onderzoeken.

- (i) $\#A = q$.

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 3.6.5 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 $\#A = q$.

- (ii) A is een *deellichaam* van K .

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:

$$\alpha, \beta \in A, \beta \neq 0 \implies (\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1} \implies \alpha\beta^{-1} \in A$$

en gebruik makende van 8.1.3 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 $-1 = 1 + 1 + \dots + 1 \in A$ ($p-1$) termen. Hieruit volgt dat A een deellichaam van K is.

- (iii) $A = K$ ($:= \Omega_{\mathbb{F}_p}^{X^q - X}$).

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 $\alpha_1, \dots, \alpha_q$ voortgebrachte lichaam in A bevat zijn:

$$\mathbb{F}_p(\alpha_1, \alpha_2, \dots, \alpha_q) \subset A.$$

Maar uit de definitie van ontbindingslichaam 8.2.1(b) volgt dat $K = \mathbb{F}_p(\alpha_1, \alpha_2, \dots, \alpha_q)$. We concluderen dat $K \subset A$, en omdat, per definitie, 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 9.1.1(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 8.2.1 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 8.2.6 voor ontbindingslichamen impliceert dus dat L en K isomorf zijn. De laatste uitspraak hebben we in de loop van het bewijs al gezien. Hiermee is stelling 9.1.1 bewezen. \square

Opmerking 9.1.2 In plaats van \mathbb{F}_q vindt men in de literatuur wel de notatie $GF(q)$, voor ‘Galois field’, genoemd 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 1.18, merk op: als $q = p^n$ met $n > 1$ dan $\bar{p} \neq \bar{0} \neq p^{n-1}$, maar $\bar{p} \cdot p^{n-1} = \bar{p}^n = \bar{0}$), dus dan $\mathbb{F}_q \not\cong \mathbb{Z}/q\mathbb{Z}$.

Voorbeeld 9.1.3 De polynomen $f, g \in \mathbb{F}_2[X]$:

$$f := X^3 + X^2 + 1 \quad \text{en} \quad g := X^3 + X + 1$$

zijn irreducibel omdat ze graad drie en geen nulpunten hebben. De lichamen

$$K := \mathbb{F}_2[X]/(f) \quad \text{en} \quad L := \mathbb{F}_2[X]/(g)$$

hebben dan beiden 8 elementen (van de vorm $a_0 + a_1\bar{X} + a_2\bar{X}^2$ met $a_i \in \mathbb{F}_2$), en zijn volgens de stelling isomorf. We geven een expliciet isomorfisme.

Merk op dat $\alpha := X + (f)$ 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

$$\beta := X + (g) \in L, \quad \text{dan} \quad \beta^3 = \beta + 1.$$

Merk op dat:

$$\begin{aligned} f(\beta + 1) &= (\beta + 1)^3 + (\beta + 1)^2 + 1 \\ &= (\beta^3 + \beta^2 + \beta + 1) + (\beta^2 + 1) + 1 \\ &= \beta^2 + (\beta^2 + 1) + 1 \\ &= 0, \end{aligned}$$

(we rekenen mod 2 met de coëfficiënten), waarmee het nulpunt gevonden is. Omdat het nogal lastig is rechtstreeks een lichaamsisomorfisme tussen K en L aan te geven definiëren we eerst een evaluatiehomomorfisme:

$$\Phi_{\beta+1} : \mathbb{F}_2[X] \longrightarrow L, \quad X \mapsto \beta + 1.$$

Ga na dat $\Phi_{\beta+1}$ surjectief is. De kern van $\Phi_{\beta+1}$ wordt voortgebracht door f want dat is het polynoom van de laagste graad in de kern. Met de eerste isomorfiestelling 2.2.9 volgt dan:

$$K = \mathbb{F}_2[X]/(f) \cong \text{beeld}(\Phi_{\beta+1}) = L,$$

het isomorfisme wordt dus expliciet gegeven door:

$$a_0 + a_1\alpha + a_2\alpha^2 \mapsto a_0 + a_1(\beta + 1) + a_2(\beta + 1)^2 = (a_0 + a_1 + a_2) + a_1\beta + a_2\beta^2.$$

9.2 Structuur van eindige lichamen

Uit het feit dat een eindig lichaam \mathbb{F}_{p^n} een n -dimensionale vectorruimte over \mathbb{F}_p is, volgt dat de optelgroep van \mathbb{F}_{p^n} isomorf is met $(\mathbb{Z}/p\mathbb{Z})^n$. De productstructuur is uiteraard niet componentsgewijs (dat geeft nl. nuldelers).

De volgende stelling laat zien dat ieder eindig lichaam een enkelvoudige uitbreiding van \mathbb{F}_p is, zodat we de rekenmethodes uit b.v. 7.2.7 kunnen toepassen.

Stelling 9.2.1 *Zij \mathbb{F}_q een eindig lichaam met $q = p^n$. Dan is er een $\alpha \in \mathbb{F}_q$ met:*

$$\mathbb{F}_q = \mathbb{F}_p[\alpha].$$

In het bijzonder is $\mathbb{F}_q \cong \mathbb{F}_p[X]/(f_{\mathbb{F}_p}^\alpha)$ en $gr(f_{\mathbb{F}_p}^\alpha) = n$.

Bovendien is er voor elke $n > 0$ een irreducibel polynoom van graad n in $\mathbb{F}_p[X]$.

Bewijs. Voor iedere $\beta \in \mathbb{F}_q$ is $\mathbb{F}_p(\beta)$ een eindig lichaam en dus $\mathbb{F}_p(\beta) \cong \mathbb{F}_{p^k}$ voor zekere $k \leq n$. Dan is β een nulpunt van $X^{p^k} - X$, en dat polynoom heeft hoogstens p^k verschillende nulpunten in het lichaam \mathbb{F}_{p^n} . Bekijken we alle mogelijke k , dan zien we dat het aantal elementen $\beta \in \mathbb{F}_{p^n}$ met $\mathbb{F}_p(\beta) \neq \mathbb{F}_{p^n}$ dus hoogstens $p + p^2 + \dots + p^{n-1} < p^n$ is. We concluderen dat er een $\alpha \in \mathbb{F}_{p^n}$ moet zijn met $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. (We zullen later een volledige beschrijving van de deellichamen van \mathbb{F}_q geven, zie 9.2.8.)

Omdat α algebraïsch is over \mathbb{F}_p (immers \mathbb{F}_{p^n} is eindig over \mathbb{F}_p) geldt $\mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$. Verder is $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = gr(f_{\mathbb{F}_p}^\alpha)$ en dus is $f_{\mathbb{F}_p}^\alpha$ een irreducibel polynoom van graad n . Hiermee is de stelling bewezen. \square

Voorbeeld 9.2.2 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 (ga na) en is dus reducibel. Zij $f = X^3 + X - 1 \in \mathbb{F}_5[X]$, deze f is irreducibel want f 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 $\#L = 5^3$ want ieder element van L is op unieke wijze te schrijven als:

$$x = a_0 + a_1\alpha + a_2\alpha^2, \quad \text{met } \alpha := X + (f) \in L,$$

en met $a_i \in \mathbb{F}_5$. Omdat er maar één lichaam is met 5^3 elementen, geldt $L \cong \mathbb{F}_{5^3}$. Omdat α een nulpunt is van f , geldt $\alpha^3 = -\alpha + 1$. Zo is b.v.:

$$\begin{aligned} (3\alpha + 1)(4\alpha^2 + 2) &= 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 2(-\alpha + 1) + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 4\alpha + 4, \\ &= -(\alpha^2 + \alpha + 1). \end{aligned}$$

waarbij de coëfficiënten modulo 5 genomen worden.

9.2.3 Zij $f \in \mathbb{F}_q[X]$ een irreducibel polynoom. Dan heeft f een nulpunt α in het lichaam $L = \mathbb{F}_q[X]/(f)$, merk op dat $\#L = q^m$ met $m = \text{gr}(f)$, dus $L \cong \mathbb{F}_{q^m}$ als $q = p^n$. In $L[X]$ is f dan te schrijven als $(X - \alpha)g$ met $g \in L[X]$ en we hebben gezien, zie voorbeeld 8.2.3, dat g i.h.a. geen nulpunt in L hoeft te hebben. Voor *eindige* lichamen blijkt echter dat f al zijn nulpunten in L heeft, d.w.z. f is te schrijven als een product van lineaire factoren in $L[X]$. Dit resultaat stelt ons ook in staat om $\text{Aut}(\mathbb{F}_q)$ te bepalen.

9.2.4 Hierbij maken we uiteraard gebruik van het Frobenius-homomorfisme (zie 8.1.3)

$$F : L \longrightarrow L \quad x \mapsto x^p.$$

Omdat L eindig is, is F zelfs een lichaamsautomorfisme, $F \in \text{Aut}(L)$. Dan wordt voor iedere $k \in \mathbb{N}$ de samenstelling van k Frobenius-homomorfismen gegeven door:

$$F^k : L \longrightarrow L, \quad x \mapsto x^{p^k}, \quad \text{en ook } F^k \in \text{Aut}(L).$$

Stelling 9.2.5 Zij $f \in \mathbb{F}_q[X]$, met $q = p^n$, een monisch en irreducibel polynoom van graad m . Zij $L := \mathbb{F}_q[X]/(f)$, en zij $\alpha \in L$ een nulpunt van f .

Dan is:

$$f = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{m-1}}) \in L[X].$$

Bovendien zijn de m nulpunten van f onderling verschillend.

Bewijs. Omdat $F^n(a) := a^{p^n} = a^q$ en iedere $a \in \mathbb{F}_q$ een nulpunt is van $X^q - X$, geldt: $F^n(a) = a$, dus $F^n \in \text{Aut}_{\mathbb{F}_q}(L)$, want F^n is immers de identiteit op \mathbb{F}_q .

Voor iedere $k \in \mathbb{N}$ is dan ook $(F^n)^k \in \text{Aut}_{\mathbb{F}_q}(L)$. Volgens stelling 8.1.7 is dan $(F^n)^k(\alpha) = \alpha^{q^k} \in L$ ook een nulpunt van f . We laten zien dat we zo m verschillende nulpunten van f krijgen. Als $\alpha^{q^k} = \alpha^{q^l}$ met $0 \leq k < l \leq m-1$, dan is, omdat $\text{kar}(L) = p$:

$$0 = \alpha^{q^l} - \alpha^{q^k} = (\alpha^{q^{l-k}} - \alpha)^{q^k}.$$

D.w.z. dat α een nulpunt is van $X^{q^a} - X$ met $a = l - k < m$ oftewel $\alpha \in \mathbb{F}_{q^a}$, in tegenspraak met $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. We concluderen dat de m nulpunten $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}} \in L$ van f onderling verschillend zijn en dus kan f in lineaire factoren ontbonden worden in $L[X]$. Hiermee is de stelling bewezen. \square

Voorbeeld 9.2.6 Zoals we zagen in voorbeeld 9.1.3 heeft het polynoom $f := X^3 + X^2 + 1$ het nulpunt $\beta + 1 \in L := \mathbb{F}_2[\beta] \cong \mathbb{F}_8$ met $\beta^3 = \beta + 1$. Reken zelf na dat:

$$(\beta + 1)^2 = \beta^2 + 1 \quad \text{en} \quad (\beta + 1)^4 = \beta^4 + 1 = \beta^2 + \beta + 1$$

ook nulpunten zijn van f en dat inderdaad

$$X^3 + X^2 + 1 = (X - (\beta + 1))(X - (\beta^2 + 1))(X - (\beta^2 + \beta + 1)).$$

Stelling 9.2.7 *Zij $q = p^n$ met p een priemgetal. Dan is:*

$$\text{Aut}(\mathbb{F}_q) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

d.w.z. $\text{Aut}(\mathbb{F}_q)$ is een cyclische groep van orde n en wordt voortgebracht door het Frobenius-homomorfisme.

Bewijs. We weten al dat er een $\alpha \in \mathbb{F}_q$ is met $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ en dat het minimumpolynoom van α precies n onderling verschillende nulpunten in \mathbb{F}_q heeft. Uit Stelling 8.1.7 volgt dan dat $\#\text{Aut}(\mathbb{F}_q) = \#\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) = n$ (\mathbb{F}_p is immers het priemlichaam van \mathbb{F}_q).

Merk op dat de n lichaamsautomorfismen $id, F, F^2, \dots, F^{n-1}$ alle verschillend zijn, immers in het bewijs van de vorige stelling zagen we (neem $p = q$) dat $F^k(\alpha) = \alpha^{p^k} \neq \alpha^{p^l} = F^l(\alpha)$ als $0 \leq k < l < n-1$. We concluderen dat elk element van $\text{Aut}(\mathbb{F}_q)$ een product van Frobenius automorfismen is. Hiermee is de stelling bewezen. \square

Stelling 9.2.8 *Laat $q = p^k$ en $r = p^m$. Er geldt:*

\mathbb{F}_q is isomorf met een deellichaam van \mathbb{F}_r precies dan als r een macht van q is (d.w.z. als $k|m$).

Als \mathbb{F}_q isomorf is met een deellichaam van \mathbb{F}_r dan is dat deellichaam uniek en het bestaat uit de nulpunten van het polynoom $X^q - X$. We mogen dus schrijven:

$$\mathbb{F}_{p^k} \subset \mathbb{F}_{p^m} \iff k|m.$$

Bewijs. 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 $\dim_{\mathbb{F}_q} \mathbb{F}_r = [\mathbb{F}_r : \mathbb{F}_q]$ dus:

$$p^m = \#\mathbb{F}_r = \#(\mathbb{F}_q)^{[\mathbb{F}_r : \mathbb{F}_q]} = p^{k[\mathbb{F}_r : \mathbb{F}_q]}, \quad \text{dus } k|m.$$

Neem nu aan dat $m = kn$ voor zekere $n \in \mathbb{Z}_{>0}$, dan geldt $r = q^n$. We willen laten zien dat het polynoom $X^q - X$ al zijn nulpunten (die het lichaam \mathbb{F}_q vormen) in \mathbb{F}_r heeft. Omdat ieder element van \mathbb{F}_r een nulpunt van $X^r - X$ is, moeten we dus laten zien dat:

$$X^q - X \mid X^r - X \quad (\text{in } \mathbb{F}_p[X]).$$

Omdat beide polynomen deelbaar zijn door X en omdat $r = q^n$ moeten we laten zien dat:

$$X^{q-1} - 1 \mid X^{q^n-1} - 1.$$

Aangezien in \mathbb{Z} geldt:

$$q^n - 1 = (q - 1)(q^{n-1} + q^{n-2} + \dots + q + 1) = (q - 1)b,$$

met $b \in \mathbb{Z}$, volgt de deelbaarheid van de polynomen uit:

$$X^{ab} - 1 = (X^a - 1)(X^{a(b-1)} + X^{a(b-2)} + \dots + X^a + 1),$$

met $a = q - 1$, $b = q^{n-1} + q^{n-2} + \dots + q + 1$.

Dit bewijst het eerste deel van de stelling. Als \mathbb{F}_r een deellichaam K heeft met q elementen, dan geldt $x^q - x = 0$ voor elke $x \in K$, en dus is K precies de verzameling van nulpunten van $X^q - X$. I.h.b. is er hoogstens één deellichaam met q elementen in \mathbb{F}_r . Hiermee is de stelling bewezen. \square

Opmerking 9.2.9 We merken op dat \mathbb{F}_4 geen deellichaam van \mathbb{F}_8 is, maar dat b.v. \mathbb{F}_4 en \mathbb{F}_8 beiden deellichamen zijn van \mathbb{F}_{64} , dit is ook het kleinste lichaam waarvan zowel \mathbb{F}_4 als \mathbb{F}_8 deellichamen zijn.

9.3 Irreducibele polynomen in $\mathbb{F}_q[X]$

Met behulp van de classificatie van de eindige lichamen kan men een aantal resultaten bewijzen over irreducibele polynomen in $\mathbb{F}_q[X]$.

Voorbeeld 9.3.1 Zij K een uitbreiding van \mathbb{F}_p met $[K : \mathbb{F}_p] = 2$. Omdat $\#K = p^2$ en $\#\mathbb{F}_p = p$, zijn er precies $p^2 - p$ elementen in K die niet in \mathbb{F}_p zitten.

Zij $\alpha \in K$, maar $\alpha \notin \mathbb{F}_p$. Dan is $\mathbb{F}_p(\alpha) = K$ en dus is $gr(f_{\mathbb{F}_p}^\alpha) = 2$. Het polynoom $f_{\mathbb{F}_p}^\alpha$ heeft dan precies twee verschillende nulpunten α en α^p (zie 9.2.5) in $\mathbb{F}_{p^2} - \mathbb{F}_p$. Gegeven K vinden we dus $\frac{1}{2}(p^2 - p)$ irreducibele, monische 2-de graads polynomen in $\mathbb{F}_p[X]$, en

$$K \cong \mathbb{F}_p[X]/(f)$$

voor elk van deze f .

Zij nu $g \in \mathbb{F}_p[X]$ een monisch, irreducibel polynoom van graad 2. Dan is, wegens de classificatie, $\mathbb{F}_p[X]/(g) \cong K$. Omdat g het minimum polynoom van $\alpha := X + (g)$ is, is g dus één van de $\frac{1}{2}(p^2 - p)$ polynomen die we eerder vonden. We concluderen: Er zijn precies $\frac{1}{2}(p^2 - p)$ monische, irreducibele polynomen van graad 2 in $\mathbb{F}_p[X]$.

We kunnen ook een rechtstreeks bewijs van dit feit geven. Een monisch, 2-de graads polynoom in $\mathbb{F}_p[X]$ is van de vorm $X^2 + aX + b$ met $a, b \in \mathbb{F}_p$, daarvan zijn er dus p^2 . De reducibele zijn van de vorm $(X - r)^2$ of $(X - r)(X - s)$ met $r \neq s$ en $r, s \in \mathbb{F}_p$. Er zijn dus $p + \binom{p}{2} = p + \frac{1}{2}(p^2 - p) = \frac{1}{2}(p^2 + p)$ reducibele monische 2-de graads polynomen in $\mathbb{F}_p[X]$. We concluderen dat het aantal monische, irreducibele 2-de graads polynomen in $\mathbb{F}_p[X]$ gelijk is aan $p^2 - \frac{1}{2}(p^2 + p) = \frac{1}{2}(p^2 - p)$.

Stelling 9.3.2 Laat $q > 1$ een priemmacht zijn en laat $n \in \mathbb{Z}_{\geq 1}$.

Dan geldt:

$$X^{q^n} - X = \prod f \quad \text{in } \mathbb{F}_q[X]$$

waarbij het product wordt uitgestrekt over de verzameling monische irreducibele polynomen $f \in \mathbb{F}_q[X]$ met $gr(f)$ een deler van n .

Bewijs. Omdat $\mathbb{F}_q[X]$ een factorontbindingsring 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 de afgeleide $(X^{q^n} - X)' = q^n X^{q^n - 1} - 1 = -1$ heeft geen nulpunt.

We weten nu al dat $X^{q^n} - X = \prod f$, met (verschillende) irreducibele f die bovendien monisch gekozen kunnen worden omdat $X^{q^n} - X$ monisch is. De stelling volgt als we kunnen aantonen:

$$f \mid X^{q^n} - X \iff gr(f) \mid n,$$

voor monische irreducibele $f \in \mathbb{F}_q[X]$.

Zij $d = \text{gr}(f)$. Aangezien $X^{q^n} - X = \prod_{\alpha \in \mathbb{F}_{q^n}} (X - \alpha) \in \mathbb{F}_{q^n}[X]$, geldt:

$$f \mid X^{q^n} - X \iff f = (X - \alpha_1) \cdots (X - \alpha_d) \in \mathbb{F}_{q^n}[X]. \iff \Omega_{\mathbb{F}_q}^f \subseteq \mathbb{F}_{q^n}.$$

Omdat voor een eindig lichaam geldt: $\Omega_{\mathbb{F}_q}^f = \mathbb{F}_q[\alpha_i] = \mathbb{F}_q[X]/(f)$ met α_i een nulpunt van f (zie 9.2.5), zien we:

$$f \mid X^{q^n} - X \iff \mathbb{F}_q[X]/(f) \subseteq \mathbb{F}_{q^n}.$$

Uit $[\mathbb{F}_q[X]/(f) : \mathbb{F}_q] = d$ volgt $\mathbb{F}_q[X]/(f) \cong \mathbb{F}_{q^d}$ en dus, met stelling 9.2.8

$$f \mid X^{q^n} - X \iff \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n} \iff d \mid n.$$

Hiermee is de stelling bewezen. \square

Voorbeeld 9.3.3 Merk op:

$$X^4 - X = X(X^3 - 1) = X(X - 1)(X^2 + X + 1) \quad \text{in } \mathbb{F}_2[X],$$

en ga na dat X , $X + 1$, $X^2 + X + 1$ inderdaad de enige monische, irreducibele polynomen van graad ≤ 2 in $\mathbb{F}_2[X]$ zijn. Algemener, omdat de elementen van \mathbb{F}_{p^2} precies de nulpunten zijn van $X^{p^2} - X$, geldt:

$$X^{p^2} - X = \prod_{\alpha \in \mathbb{F}_{p^2}} (X - \alpha).$$

Als $\alpha \in \mathbb{F}_p$, dan is $X - \alpha \in \mathbb{F}_p[X]$ monisch en irreducibel. Als $\alpha \notin \mathbb{F}_p$ dan heeft $f_{\mathbb{F}_p}^\alpha$ graad 2 en heeft 2 nulpunten in \mathbb{F}_{p^2} . Ieder monisch, irreducibel polynoom van graad 2 is volgens voorbeeld 9.3.1 van deze vorm. Daaruit volgt dan ook:

$$X^{p^2} - X = \prod f, \quad \text{in } \mathbb{F}_p[X]$$

waarbij we het product over de monische irreducibele polynomen van graad ≤ 2 nemen.

Gevolg 9.3.4 Zij x_d het aantal monische irreducibele d -de graads polynomen in $\mathbb{F}_q[X]$. Dan geldt voor alle $n \in \mathbb{Z}_{\geq 1}$:

$$\sum_{d \mid n} dx_d = q^n.$$

Bewijs. Merk op dat $q^n = gr(X^{q^n} - X)$. Volgens de stelling is dit polynoom gelijk aan het product van alle monische irreducibele polynomen met graad $d|n$, en de linkerzijde in de te bewijzen formule is precies de graad van dit product. \square

Voorbeeld 9.3.5 Met 9.3.4 kan men x_n , het aantal irreducibele polynomen van graad n , recursief bepalen. Voor $n = 1, 2, 3, 6$ vindt men:

$$\begin{aligned} 1 \cdot x_1 &= q^1 \Rightarrow x_1 = q \\ 1 \cdot x_1 + 2 \cdot x_2 &= q^2 \Rightarrow x_2 = \frac{1}{2}(q^2 - q) \\ 1 \cdot x_1 + 3 \cdot x_3 &= q^3 \Rightarrow x_3 = \frac{1}{3}(q^3 - q) \\ 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 6 \cdot x_6 &= q^6 \Rightarrow x_6 = \frac{1}{6}(q^6 - q^3 - q^2 + q). \end{aligned}$$

9.3.6 In het algemeen vindt men met behulp van de **Moebius-inversieformule** (zie opgave 11):

$$x_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}, \quad \text{met}$$

$$\begin{cases} \mu(n) = 0 & \text{als er een priemgetal } p \text{ is met } p^2|n \\ \mu(p_1 p_2 \dots p_r) = (-1)^r, \end{cases}$$

waarbij de p_i onderling verschillende priemgetallen zijn met $r \in \mathbb{Z}_{\geq 0}$, dus i.h.b. $\mu(1) = 1$ (dan is nl. $r = 0$).

9.4 De vermenigvuldigingsgroep van een eindig lichaam.

We zullen het volgende resultaat uit de groepentheorie gebruiken, waarvan we volledigheidshalve ook het bewijs geven.

Stelling 9.4.1 *Zij G een eindige commutatieve groep, en zij $a \in G$ een element waarvan de orde $m = \text{orde}(a)$ zo groot mogelijk is.*

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

Bewijs. We gebruiken de structuurstelling van de eindige abelse groepen:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}, \quad \text{met } n_1|n_2|n_3|\dots|n_k,$$

d.w.z. dat n_i een deler van n_{i+1} is. In het bijzonder is $\bar{n}_k = \bar{0} \in \mathbb{Z}/n_i\mathbb{Z}$ voor elke i . Als $b = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_k) \in G$, dan is $b + b + \dots + b$ (n_k keer) gelijk aan

$$n_k b = (n_k \bar{b}_1, n_k \bar{b}_2, \dots, n_k \bar{b}_k) = (\bar{0}, \bar{0}, \dots, \bar{0}) = 0 \quad (\in G).$$

Dus elke $b \in G$ heeft een orde die een deler van n_k is. Verder heeft het element $a = (\bar{0}, \bar{0}, \dots, \bar{1})$ orde n_k (omdat $\bar{1} \in \mathbb{Z}/n_k\mathbb{Z}$ orde n_k heeft). We concluderen dat voor elke $b \in G$ geldt: $orde(b)|n_k = orde(a)$. \square

Stelling 9.4.2 *Zij R een domein en G een eindige ondergroep van de eenhedengroep R^* van R .*

Dan is G cyclisch.

In het bijzonder is \mathbb{F}_q^ een cyclische groep.*

Bewijs. Omdat R commutatief is, is G abels. Volgens voorgaande stelling is er een $a \in G$ met $orde(a) = m$ zodanig dat $orde(b)|m$ voor alle $b \in G$. Dus alle $b \in G$ zijn nulpunten van het polynoom $X^m - 1$ (immers 1 is het eenheidselement van R^*). Omdat $X^m - 1$ niet meer dan m nulpunten in R heeft (zie 3.5.2), volgt hieruit dat de orde van G , $\#G$, hoogstens m is (er geldt zelfs dat $\#G$ een deler van m is). In G zit een element van orde m , nl. a , en de ondergroep die door a wordt voortgebracht heeft dus al m elementen. We concluderen dat G een cyclische groep is, met voortbrenger a .

Door dit toe te passen op het domein \mathbb{F}_q en $G = \mathbb{F}_q^*$ volgt de laatste uitspraak. Hiermee is stelling 9.4.2 bewezen. \square

9.4.3 Een element $\alpha \in \mathbb{F}_q^*$ dat de multiplicatieve groep \mathbb{F}_q^* voortbrengt heet een **primitieve wortel** van \mathbb{F}_q . Volgens de stelling is $\alpha \in \mathbb{F}_q^*$ een primitieve wortel precies dan als de multiplicatieve orde van α gelijk is aan $\#\mathbb{F}_q^* = q - 1$.

Als α een primitieve wortel van \mathbb{F}_q is, dan kan iedere $x \in \mathbb{F}_q^*$ geschreven worden als:

$$x = \alpha^k, \quad \text{en} \quad \Lambda : \mathbb{F}_q^* \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}, \quad x \mapsto \bar{k}$$

is een isomorfisme van (abelse) groepen. In het bijzonder is k uniek bepaald modulo $q - 1$ (door x en door α).

Voorbeeld 9.4.4 Het element $3 \in \mathbb{F}_7$ is een primitieve wortel van \mathbb{F}_7 want:

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1,$$

dus $orde(3) = 6 = \#\mathbb{F}_7^*$.

We bepalen een primitieve wortel van \mathbb{F}_9 , d.w.z. een element van orde 8 in de groep \mathbb{F}_9^* . Aangezien de orde van een element de orde van de groep deelt, hoeven we alleen maar een $\alpha \in \mathbb{F}_9^*$ te vinden met $\alpha^4 \neq 1$.

Omdat $X^2 + 1$ geen nulpunt heeft in \mathbb{F}_3 , geldt:

$$\mathbb{F}_9 \cong \mathbb{F}_3[i] := \mathbb{F}_3[X]/(X^2 + 1), \quad \text{met} \quad i := X + (X^2 + 1).$$

Ieder element van \mathbb{F}_9 is dus op unieke wijze te schrijven als $a+bi$ met $a, b \in \mathbb{F}_3$ en er geldt $i^2 = -1$. Zij nu $\alpha = 1 + i$, dan is:

$$\alpha^2 = (1 + i)^2 = 2i, \quad \alpha^4 = (2i)^2 = -1,$$

dus de orde van α is 8 en α is een primitieve wortel. Bereken zelf α^k voor $1 \leq k \leq 8$ en ga na dat je zo inderdaad alle elementen van \mathbb{F}_9^* vindt.

9.5 Opgaven

1. Bepaal alle primitieve wortels van \mathbb{F}_7 , \mathbb{F}_8 en \mathbb{F}_9 .
2. Zij p een priemgetal met $p \equiv 3 \pmod{4}$. Bewijs: $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{F}_{p^2}$.
3. Bepaal $f_{\mathbb{F}_3}^\alpha$ voor alle $\alpha \in \mathbb{F}_9$, en ontbind $X^8 - 1$ in irreducibele factoren in $\mathbb{F}_3[X]$.
4. Bewijs dat $\bar{2} + \sqrt{2} \in \mathbb{F}_{25}$ een primitieve wortel is (met $\sqrt{2}^2 = \bar{2}$).
5. Bewijs dat $X^4 + \bar{2}$ irreducibel is in $\mathbb{F}_{125}[X]$.
6. Bewijs, met een telargument, dat het aantal monische irreducibele polynomen in $\mathbb{F}_q[X]$ van graad 3 gelijk is aan $\frac{1}{3}(q^3 - q)$.
7. Ontbind de polynomen $X^2 - X$, $X^4 - X$, $X^8 - X$ en $X^{64} - X$ in $\mathbb{F}_2[X]$ in irreducibele factoren.
8. Leid uit gevolg 9.3.4 af:

$$\frac{1}{n}q^n \geq x_n \geq \frac{1}{n}\left(q^n - \frac{q}{q-1}q^{\frac{1}{2}n}\right).$$

9. Stel dat $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Bewijs rechtstreeks dat het in 9.2.5 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 $c^p = c$.
10. 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 òf irreducibel in $K[X]$ is, òf in p lineaire factoren splitst in $K[X]$. (Aanwijzing: als $f = gh$ bekijk dan de gelijkheid $f(X-j) = g(X-j)h(X-j)$ ($j \in \mathbb{F}_p$) en concludeer dat de irreducibele factoren van f dezelfde graad hebben.)
 - c. Bewijs dat $X^p - X - a$ irreducibel in $\mathbb{F}_p[X]$ is, voor alle $a \in \mathbb{F}_p^*$.

11. Zij R de in opgave 27 op blz. 23 gedefinieerde ring van alle arithmetische functies. Een element van R is een functie $f : \mathbb{Z}_{>0} \rightarrow \mathbb{C}$, 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

$$e(n) = \begin{cases} 1 & \text{als } n = 1 \\ 0 & \text{als } n > 1, \end{cases}$$

$$E(n) = 1 \text{ voor alle } n \in \mathbb{Z}_{>0}.$$

Laat verder $\mu \in R$ gedefinieerd zijn als in 9.3.6.

- Bewijs dat e het eenheidselement van de ring R is.
- Bewijs dat $\mu * E = e$ (dus μ is de *inverse* van E in R).
- 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 $f = \mu * g$).

- Bewijs 9.3.6.

12. (vgl. opgave 11 op blz. 147)

- Bewijs dat de lichamen $\mathbb{Q}[X]/(X^2 - 2)$ en $\mathbb{Q}[Y]/(Y^2 - 3)$ niet isomorf zijn.
- Bij gegeven priemgetal p is

$$R_2 := \mathbb{F}_p[X]/(X^2 - \bar{2}) \text{ en } R_3 := \mathbb{F}_p[Y]/(Y^2 - \bar{3}).$$

Bepaal voor alle priemgetallen p vanaf 2 tot en met 23 de structuur van deze twee ringen, en beslis of ze isomorf zijn.

13. Als q een priemgetal is dan schrijven we $\Phi_q = X^{q-1} + \dots + X^2 + X + 1 = (X^q - 1)/(X - 1) \in \mathbb{Z}[X]$; 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

$$f_{11,p} = g_p := X^{10} + \dots + X^2 + X + \bar{1} \in \mathbb{F}_p[X].$$

Bewijs dat alle irreducibele factoren van g_p dezelfde graad hebben. Zij G een irreducibele factor van g_p . Bewijs:

- graad(G) = 1 desda ($p = 11$ of $p \equiv 1 \pmod{11}$)
 graad(G) = 2 desda $p \equiv -1 \pmod{11}$
 graad(G) = 5 desda $p \equiv 3, 4, 5, \text{ of } 9 \pmod{11}$,
 graad(G) = 10 desda $p \equiv 2, 6, 7, \text{ of } 8 \pmod{11}$.

14. Zij $g = f_{11,3}$ (notatie van opgave 13), m.a.w. $g = X^{10} + \dots + X + \bar{1} \in \mathbb{F}_3[X]$. 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 coëfficiënten van G zijn ook nog gemakkelijk te berekenen?).

15. We gebruiken de notatie uit opgave 13.

- a. Factoriseer $f_{11,5} \in \mathbb{F}_5[X]$
- b. idem $f_{7,13} \in \mathbb{F}_{13}[X]$.
- c. idem $f_{13,5} \in \mathbb{F}_5[X]$.

16.
 - a. Zij K een lichaam, $x \in K$, $x^4 \neq 1$, $x^8 = 1$. 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 $(3 \pmod{41})$ in \mathbb{F}_{41}^* . Vind een $y \in \mathbb{Z}$ met $y^2 \equiv 2 \pmod{41}$.
 - c. Gegeven is een priemgetal p met $p \equiv 1 \pmod{8}$. Bewijs dat er een $z \in \mathbb{Z}$ bestaat met $z^2 \equiv 2 \pmod{p}$.

17. (in opgave 16 losten we de vergelijking ' $z^2 \equiv 2 \pmod{p}$ ' op voor $p \equiv 1 \pmod{8}$. Nu bestuderen we ' $x^2 \equiv 3 \pmod{p}$ ') voor p een priemgetal met $p \equiv 1 \pmod{12}$).

- 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 (1), 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 $(a^5 + a^7)^2 = \bar{3} \in \mathbb{F}_p$.
- d. Bewijs dat er een $x \in \mathbb{Z}$ is met $x^2 \equiv 3 \pmod{p}$. (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.).

18. Bepaal het aantal irreducibele polynomen van graad 4 in $\mathbb{F}_q[X]$.
19. Zij $a, b \in \mathbb{F}_p$ ($p > 2$) zodanig dat $X^2 - a$ en $X^2 - b$ irreducibel zijn in $\mathbb{F}_p[X]$.

- a. Bewijs dat er een $r \in \mathbb{F}_p$ is met $a = r^2b$. (Hint: het groeps-homomorfisme $k : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$ met $k(x) = x^2$ heeft kern $\{\pm 1\}$.)
- b. Zij $\beta := X + (X^2 - b) \in \mathbb{F}_p[X]/(X^2 - b)$. Laat zien dat:

$$\Phi_{r\beta} : \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]/(X^2 - b), \quad f \mapsto f(r\beta),$$

een surjectief ringhomomorfisme is met kern $(X^2 - a)$.

- c. Geef een expliciet lichaamshomomorfisme:

$$\phi : \mathbb{F}_p[X]/(X^2 - a) \longrightarrow \mathbb{F}_p[X]/(X^2 - b).$$

- d. Zij $X^2 + tX + s \in \mathbb{F}_p[X]$ een irreducibel polynoom. Geef aan hoe een lichaamsisomorfisme

$$\psi : \mathbb{F}_p[X]/(X^2 + tX + s) \longrightarrow \mathbb{F}_p[X]/(X^2 - b)$$

geconstrueerd kan worden.

20. (Uit een wiskunde olympiade)

- a. Vind $a, b \in \mathbb{Z}$ met:

(a) $ab(a + b) \not\equiv 0 \pmod{7}$,

(b) $(a + b)^7 \equiv a^7 + b^7 \pmod{7^7}$.

Hoeveel oplossingen zijn er voor a en b in $(\mathbb{Z}/7^7) \times (\mathbb{Z}/7^7)$?

- b. (een suggestie voor oplossingen) Zij $p \equiv 1 \pmod{3}$ 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 $p \equiv 1 \pmod{3}$ een priemgetal, en $f := \frac{1}{p}((X + 1)^p - X^p - 1) \in \mathbb{Z}[X]$ (waarom heeft dat polynoom gehele coëfficiënten?). 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 $p = 7$.

10 Algebraïsch afgesloten lichamen

Definitie 10.1.1 Een lichaam K heet **algebraïsch afgesloten** als er voor elke $f \in K[X]$, $f \notin K$, een $\alpha \in K$ is met $f(\alpha) = 0$.

10.1.2 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 10.1.3 *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 $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ 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 lineair is (vgl. 5.1.2).

(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 $[K(\alpha) : K] = \text{graad}(f_K^\alpha)$ 7.3.3, 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 10.1.3 bewezen. \square

Stelling 10.1.4 *Elk algebraïsch afgesloten lichaam K is oneindig.*

Bewijs. Als K eindig is, $K = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, 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 10.1.4. \square

De volgende stelling stond vroeger bekend als de ‘hoofdstelling van de algebra’.

Stelling 10.1.5 *Het lichaam \mathbb{C} der complexe getallen is algebraïsch afgesloten.*

10.1.6 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 10.1.7 *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. (van 10.1.7) Dit is een speciaal geval van de tussenwaardestelling uit de analyse, want polynomen zijn continue functies. Dit bewijst lemma 10.1.7. \square

10.1.8 Merk op dat we, in 10.1.7, α tussen β en γ kunnen kiezen; maar dit zullen we niet nodig hebben.

Voor we het volledige bewijs van stelling 10.1.5 geven leiden we enkele hulpresultaten af.

Lemma 10.1.9 *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

$$f = \left(X + \frac{1}{2}\beta\right)^2 - \left(\frac{1}{4}\beta^2 - \gamma\right)$$

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 10.1.7 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

$$c^2 - d^2 = a, \quad 2cd = b.$$

Omdat $b \neq 0$ zijn ook $c, d \neq 0$, en dus kunnen we schrijven:

$$c = \frac{b}{2d}, \quad \text{dus} \quad \frac{b^2}{4d^2} - d^2 = a.$$

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 10.1.7 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 lemma 10.1.9. \square

Lemma 10.1.10 *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 10.1.7 volgt nu dat f een nulpunt in \mathbb{R} heeft. Hiermee is 10.1.10 bewezen. \square

Lemma 10.1.11 *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 $gr(f) = 2 \cdot gr(g)$, 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 10.1.11 bewezen. \square

Bewijs. (van 10.1.5) Zij $f \in \mathbb{R}[X]$ een niet-constant polynoom. Volgens lemma 10.1.11 is het voldoende aan te tonen dat f een nulpunt in \mathbb{C} heeft. We mogen, en zullen, aannemen dat f monisch is. Laat $n = gr(f)$. 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 10.1.10 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 lemma 10.1.11 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:

$$f = \prod_{i=1}^n (X - \alpha_i), \quad \alpha_i \in L \quad (1 \leq i \leq n).$$

Zij c een willekeurig reëel getal, en beschouw het polynoom

$$g_c = \prod_{1 \leq i < j \leq n} (X - (\alpha_i + \alpha_j + c\alpha_i\alpha_j)) \quad (\in L[X]).$$

We zullen nu in het bewijs gebruik maken van een resultaat uit hoofdstuk 11. Elk van de coëfficiënten van g_c is een symmetrische uitdrukking

in $\alpha_1, \alpha_2, \dots, \alpha_n$, dus behoort wegens stelling 11.1.9 (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 $gr(g_c)$ 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

$$\alpha_i + \alpha_j + c\alpha_i\alpha_j \in \mathbb{C}, \quad \alpha_i + \alpha_j + c'\alpha_i\alpha_j \in \mathbb{C}.$$

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 10.1.9 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 10.1.5. Het hier gegeven bewijs van 10.1.5 gaat terug op C.F. Gauss (1777-1855). \square

Gevolg 10.1.12 *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 7.3.3 vinden we

$$gr(f) = [\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$$

waarbij we gebruiken dat $\mathbb{R}(\alpha) \subset \mathbb{C}$. Dit bewijst de eerste bewering van 10.1.12. De tweede bewering volgt uit

$$X^2 + bX + c = \left(X + \frac{1}{2}b\right)^2 - \frac{1}{4}(b^2 - 4c)$$

en het feit dat $X^2 - a$ irreducibel in \mathbb{R} is dan en slechts dan als $a < 0$. Hiermee is 10.1.12 bewezen. \square

Definitie 10.1.13 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 bij 7.3.10 gedefinieerde algebraïsche afsluiting van K in een uitbreidingslichaam L .

Voorbeeld 10.1.14 \mathbb{C} is een algebraïsche afsluiting van \mathbb{R} .

Stelling 10.1.15 *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} :

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraïsch over } \mathbb{Q}\}.$$

Dit is volgens 7.3.9(b) een lichaamsuitbreiding van \mathbb{Q} , die kennelijk voldoet aan voorwaarde (a) uit definitie 10.1.13. 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 10.1.5 heeft f in ieder geval een nulpunt α in \mathbb{C} . Voor deze α geldt dan, dat $\bar{\mathbb{Q}}(\alpha)$ algebraïsch over $\bar{\mathbb{Q}}$ is. Omdat $\bar{\mathbb{Q}}$ op zijn beurt algebraïsch over \mathbb{Q} is, volgt uit 7.3.11 dat $\bar{\mathbb{Q}}(\alpha)$ 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 10.1.15. \square

Opmerking 10.1.16 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 7.2.3.

Algemener hebben we:

Stelling 10.1.17 *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’ Een volledig uitgewerkt bewijs van zowel de existentie als de uniciteit kan men vinden in het boek John B. Fraleigh, ‘A first course in abstract algebra’, pp. 396–397. (Addison-Wesley, 1989.)

Voor de eenvoud schetsen we alleen een bewijs van de existentie, en dit bewijs is niet eens geheel verantwoord. Neem de partieel geordende verzameling P van alle algebraïsche lichaamsuitbreidingen van K , met als partiële ordening dat $L \leq M$ betekent dat M een algebraïsche lichaamsuitbreiding van L is. Pas nu het lemma van Zorn toe en kies een maximale keten $\{L_i\}_{i \in I}$ in P . Ga nu na dat $\bigcup_{i \in I} L_i$ een algebraïsche lichaamsuitbreiding van K is die algebraïsch afgesloten is. (Als hij niet algebraïsch afgesloten was, dan kon de keten vergroot worden. Hoe?)

Wat is er mis met dit bewijs? Logici verbieden (op goede gronden) om het te hebben over de verzameling van *alle* algebraïsche lichaamsuitbreidingen van K . Dit heeft immers te veel weg van de ‘de verzameling van alle verzamelingen’, die tot bekende paradoxen leidt. Om de situatie te redden moet de algebraïcus veel specifiekker zijn over de collectie P van lichaamsuitbreidingen die beschouwd gaan worden. Dit leidt dan tot een lang en technisch verhaal dat alleen maar aantoonst ‘dat het bewijs toch goed was’.

□

10.2 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 10.1.4. 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: $[\bar{\mathbb{Q}} : \bar{\mathbb{Q}} \cap \mathbb{R}] = 2$.

11 Symmetrische polynomen

Laat R een commutatieve ring met 1 zijn, en n een geheel getal ≥ 1 .

Een polynoom $f \in R[X_1, X_2, \dots, X_n]$ heet **symmetrisch** als f in zichzelf overgaat bij *elke* permutatie van X_1, X_2, \dots, X_n .

11.1.1 Voorbeelden.

$$\sum_{i=1}^n X_i, \quad \prod_{i=1}^n X_i, \quad \sum_{i=1}^n X_i^k \quad (\text{met } k \in \mathbb{Z}_{\geq 0}).$$

Het polynoom $X_1X_2 + X_2X_3 + X_3X_4 + X_4X_1$ is *niet* symmetrisch: het gaat niet in zichzelf over bij verwisseling van X_1 en X_2 (hier $n = 4$).

11.1.2 Werken we, met een nieuwe variabele Z , het polynoom

$$(Z - X_1)(Z - X_2) \cdots (Z - X_n) \in R[X_1, X_2, \dots, X_n][Z]$$

uit, dan vinden we dat dit gelijk is aan

$$Z^n - \sigma_1 Z^{n-1} + \sigma_2 Z^{n-2} - \dots + (-1)^{n-1} \sigma_{n-1} Z + (-1)^n \sigma_n$$

waarbij

$$\begin{aligned} \sigma_1 &= X_1 + X_2 + \dots + X_n \\ \sigma_2 &= X_1X_2 + X_1X_3 + \dots + X_1X_n + X_2X_3 + \dots + X_{n-1}X_n, \\ \sigma_3 &= X_1X_2X_3 + \dots = \sum_{1 \leq i < j < k \leq n} X_iX_jX_k, \\ &\vdots \\ \sigma_t &= \sum_{1 \leq i_1 < i_2 < \dots < i_t \leq n} X_{i_1}X_{i_2} \cdots X_{i_t}, \\ &\vdots \\ \sigma_n &= X_1X_2 \cdots X_n. \end{aligned}$$

De coëfficiënten $\sigma_1, \sigma_2, \dots, \sigma_n$ zijn allemaal symmetrische polynomen, de zogenaamde **elementaire symmetrische polynomen**. Uit $\sigma_1, \sigma_2, \dots, \sigma_n$ kan men andere symmetrische polynomen krijgen door optellen, vermenigvuldigen en het vermenigvuldigen met elementen van R .

11.1.3 Voorbeelden. met $n = 2$;

$$\begin{aligned} \sigma_1 &= X_1 + X_2, & \sigma_2 &= X_1X_2, & \sigma_1^2 &= X_1^2 + 2X_1X_2 + X_2^2, \\ \sigma_1^2 - 2\sigma_2 &= X_1^2 + X_2^2, & \sigma_1^3 - 3\sigma_1\sigma_2 &= X_1^3 + X_2^3, & \text{etcetera.} \end{aligned}$$

11.1.4 In het algemeen zien we dat elk polynoom in $\sigma_1, \sigma_2, \dots, \sigma_n$, met coëfficiënten uit R , d.w.z. elke $g(\sigma_1, \sigma_2, \dots, \sigma_n)$ met $g \in R[X_1, \dots, X_n]$, een symmetrische polynoom is. De omkering hiervan is ook waar:

Stelling 11.1.5 (*Hoofdstelling over symmetrische polynomen*) *Elk symmetrisch polynoom $f \in R[X_1, X_2, \dots, X_n]$ is te schrijven als polynoom in $\sigma_1, \sigma_2, \dots, \sigma_n$ met coëfficiënten uit R (d.w.z. $f(X_1, \dots, X_n) = g(\sigma_1, \dots, \sigma_n)$ voor zekere $g \in R[X_1, \dots, X_n]$).*

Deze schrijfwijze is bovendien eenduidig (het polynoom g is dus uniek bepaald door f).

Bewijs. Zij $f \neq 0$. Orden de termen $rX_1^{a_1}X_2^{a_2}\cdots X_n^{a_n}$ die in f voorkomen zó, 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'

$$rX_1^{c_1}X_2^{c_2}\cdots X_n^{c_n} \quad (r \in R, r \neq 0)$$

van f heeft dus

$$\begin{aligned} c_1 &= (\text{grootste } a_1 \text{ die in } f \text{ als exponent bij } X_1 \text{ voorkomt}), \\ c_2 &= (\text{grootste } a_2 \text{ die bij gegeven } a_1 = c_1 \text{ voorkomt}), \end{aligned}$$

etcetera. We noemen r de **kopcoëfficiënt** van f .

Omdat f symmetrisch is, geldt $c_1 \geq c_2 \geq \dots \geq c_n$; 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,

$$\begin{aligned} \sigma_1 &\text{ heeft kopterm } X_1, \\ \sigma_2 &\text{ heeft kopterm } X_1X_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ \sigma_n &\text{ heeft kopterm } X_1X_2\cdots X_n \end{aligned}$$

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

$$\begin{aligned} \text{kopterm } (\sigma_1^{c_1-c_2} \sigma_2^{c_2-c_3} \dots \sigma_n^{c_n}) &= X_1^{c_1-c_2} \cdot (X_1 X_2)^{c_2-c_3} \dots (X_1 X_2 \dots X_n)^{c_n} \\ &= X_1^{c_1} X_2^{c_2} \dots X_n^{c_n}, \end{aligned}$$

zoals beweerd.

De polynomen f en $r\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n}$ hebben dezelfde kopterm. Deze valt bij aftrekken weg, dus in

$$f_1 = f - r\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n}$$

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:

$$f = r\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n}.$$

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

$$f_2 = f_1 - r'\sigma_1^{c'_1-c'_2} \dots \sigma_n^{c'_n}$$

waarbij alle termen van f_2 lexicografisch later komen dan de kopterm $r'X_1^{c'_1} \dots X_n^{c'_n}$ van f_1 . Als $f_2 = 0$ dan zijn we weer klaar:

$$f = r\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n} + r'\sigma_1^{c'_1-c'_2} \dots \sigma_n^{c'_n}$$

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, \dots op een gegeven ogenblik $f_k = 0$ vinden.

Hiertoe beschouwen we de *totale graad* $\text{totgr}(f)$ van f , d.w.z. de grootste waarde van $a_1 + a_2 + \dots + a_n$ die er bij de termen $r \cdot X_1^{a_1} \dots X_n^{a_n}$ ($\neq 0$) van f optreedt (vgl. 3.1.6). Kennelijk geldt: $\text{totgr}(\sigma_i) = i$, en dus

$$\begin{aligned} \text{totgr}(\sigma_1^{c_1-c_2} \dots \sigma_n^{c_n}) &= 1 \cdot (c_1 - c_2) + 2 \cdot (c_2 - c_3) + \dots + n \cdot c_n \\ &= c_1 + c_2 + \dots + c_n \\ &\leq \text{totgr}(f). \end{aligned}$$

Hieruit volgt

$$\text{totgr}(f_1) \leq \text{totgr}(f)$$

en algemeen

$$\dots \leq \text{totgr}(f_m) \leq \text{totgr}(f_{m-1}) \leq \dots \leq \text{totgr}(f)$$

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 lexicografische latere over. Op een gegeven ogenblik zijn dus alle termen uitgeput, en dan hebben we $f_k = 0$.

Hiermee is de eerste bewering van 11.1.5 aangetoond. We moeten nog aantonen: als g_1 en g_2 twee *verschillende* polynomen in n variabelen over R zijn, dan zijn ook $g_1(\sigma_1, \sigma_2, \dots, \sigma_n)$ en $g_2(\sigma_1, \sigma_2, \dots, \sigma_n)$ verschillend. Schrijven we $g = g_1 - g_2$ dan zien we dat het voldoende is om aan te tonen:

$$\text{als } g \in R[Y_1, \dots, Y_n], g \neq 0, \quad \text{dan } g(\sigma_1, \sigma_2, \dots, \sigma_n) \neq 0.$$

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, \dots, 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, \dots, X_n met als kopterm

$$(*) \quad rX_1^{a_1}X_2^{a_2} \cdots X_n^{a_n}$$

en de andere termen $r'\sigma_1^{a'_1-a'_2} \cdots \sigma_n^{a'_n}$ geven polynomen in X_1, \dots, X_n met een later komende kopterm. Dus (*) kan niet wegvallen, en inderdaad $g(\sigma_1, \sigma_2, \dots, \sigma_n) \neq 0$. Hiermee is 11.1.5 bewezen. \square

Voorbeeld 11.1.6 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 $c_1 = 3$, $c_2 = 1$, $c_3 = 0$. Volgens het bovenstaande bewijs moeten we nu van f aftrekken

$$\begin{aligned} \sigma_1^{c_1-c_2} \sigma_2^{c_2-c_3} \sigma_3^{c_3} &= \sigma_1^2 \sigma_2 = (X_1 + X_2 + X_3)^2 \cdot (X_1X_2 + X_1X_3 + X_2X_3) \\ &= X_1^3X_2 + X_1^3X_3 + 2X_1^2X_2^2 + 5X_1^2X_2X_3 + 2X_1^2X_3^2 + X_1X_2^3 \\ &\quad + 5X_1X_2^2X_3 + 5X_1X_2X_3^2 + X_1X_3^3 + X_2^3X_3 + 2X_2^2X_3^2 + X_2X_3^3, \end{aligned}$$

het 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

$$f = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3.$$

Het polynoom g uit de stelling is dus $X_1^2X_2 - 2X_2^2 - X_1X_3$.

11.1.7 Stelling 11.1.5 wordt meestal in de volgende situatie toegepast.

Zij $f \in R[X_1, \dots, X_n]$ een symmetrisch polynoom, en laat $\alpha_1, \alpha_2, \dots, \alpha_n \in R$. Omdat f volgens 11.1.5 is uit te drukken in $\sigma_1, \sigma_2, \dots, \sigma_n$, is $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ uit te drukken in

$$\begin{aligned} \sigma_1(\alpha_1, \dots, \alpha_n) &= \alpha_1 + \dots + \alpha_n, \\ \sigma_2(\alpha_1, \dots, \alpha_n) &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n \\ &\dots \\ &\dots \\ &\dots \\ \sigma_n(\alpha_1, \dots, \alpha_n) &= \alpha_1\alpha_2 \dots \alpha_n, \end{aligned}$$

en dat zijn juist \pm de coëfficiënten van

$$(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n).$$

Ruw gesproken 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 belangrijk 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 11.1.8 Laat $h = X^3 - X - 1 \in \mathbb{Z}[X]$. In \mathbb{Z} , of zelfs in \mathbb{Q} , heeft h geen nulpunten (gebruik methode 5.5.1(c)), maar zoals blijkt uit stelling 10.1.5 zijn er $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ waarvoor geldt

$$X^3 - X - 1 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

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 11.1.5 volgt nu:

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 11.1.6

$$f = X_1^3 X_2 + X_1^3 X_3 + \dots + X_2 X_3^3 = \sigma_1^2 \sigma_2 - 2\sigma_2^2 - \sigma_1 \sigma_3$$

dan vinden we, door te substitueren $X_i := \alpha_i$:

$$\alpha_1^3 \alpha_2 + \alpha_1^3 \alpha_3 + \dots + \alpha_2 \alpha_3^3 = 0^2 \cdot (-1) - 2 \cdot (-1)^2 - 0 \cdot 1 = -2.$$

Stelling 11.1.9 *Laat R' een commutatieve ring (met 1) 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 $\alpha_1, \alpha_2, \dots, \alpha_n \in R'$ zijn met*

$$h = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n).$$

Dan geldt voor elk symmetrisch polynoom $f \in R[X_1, X_2, \dots, X_n]$ dat

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) \in R.$$

Bewijs. Het bewijs van 11.1.9 is duidelijk uit het voorgaande. Immers, voor elke i geldt:

$$\sigma_i(\alpha_1, \dots, \alpha_n) \in R$$

omdat het \pm de coëfficiënten van $h \in R[X]$ zijn. Verder is het symmetrisch polynoom $f \in R[X_1, \dots, X_n]$ te schrijven als $f = g(\sigma_1, \dots, \sigma_n)$ voor zekere $g \in R[X_1, \dots, X_n]$ (zie 11.1.5). Invullen van de α_i in $g(\sigma_1, \dots, \sigma_n)$ geeft dus een element in R , zoals gewenst. \square

Voorbeeld 11.1.10 Een belangrijk symmetrisch polynoom is

$$D = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

De **discriminant** van een polynoom

$$h = X^n + a_1 X^{n-1} + \dots + a_n = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

is gedefinieerd als

$$\Delta(h) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = D(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Deze kan in a_1, a_2, \dots, a_n uitgedrukt worden. Zo heeft men voor $n = 2, 3, 4$ de volgende formules:

$$\begin{aligned}\Delta(X^2 + aX + b) &= a^2 - 4b, \\ \Delta(X^3 + aX^2 + bX + c) &= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc, \\ \Delta(X^4 + aX^3 + bX^2 + cX + d) &= \\ \frac{1}{27} \{ &4(b^2 - 3ac + 12d)^3 - (2b^3 - 72bd + 27a^2d - 9abc + 27c^2)^2 \}\end{aligned}$$

(bij uitwerken blijkt de 27 in de noemer weg te vallen).

Door deze formules kan men de discriminant van een monisch polynoom $h = X^n + a_1X^{n-1} + \dots + a_n \in R[X]$ 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 in het geval er geen nuldelers zijn geldt

$$\Delta(h) = 0 \iff \exists i, j \quad i \neq j : \quad \alpha_i = \alpha_j,$$

dus: de discriminant is nul dan en slechts dan als het polynoom een dubbel nulpunt heeft. Het geval $n = 2$ kennen we al van het VWO. Een andere toepassing van de discriminant wordt in opgave 5 gegeven.

Als K een lichaam is met $\text{kar}(K) \neq 3$ (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 11.1.11 We gebruiken de symmetrische polynomen om de nulpunten van een derdegraads polynoom te vinden.

Zij $f \in K[X]$, met K een lichaam met $\text{kar}(K) \neq 2, 3$, en $\text{gr}(f) = 3$ 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 8.2.1). 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 gepermuteed worden. Zij $\rho := (123) \in S_3$, dan:

$$\begin{aligned} \rho = (123) : \quad A_1 &\mapsto \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega^2 A_1, \\ A_2 &\mapsto \alpha_2 + \omega^2\alpha_3 + \omega\alpha_1 = \omega A_2 \end{aligned}$$

Verder geldt:

$$\tau = (23) : A_1 \mapsto A_2, \quad (23) : A_2 \mapsto A_1.$$

Omdat de groep S_3 wordt voortgebracht door ρ en τ zijn

$$A_1^3 + A_2^3, \quad A_1 A_2$$

symmetrische polynomen in $\alpha_1, \alpha_2, \alpha_3$.

Volgens stelling 11.1.5 zijn ze dan uit te drukken in elementair symmetrische functies σ_i en deze zijn weer, op teken na, gelijk aan de coëfficiënten van f (zie boven). Na enig rekenwerk vindt men:

$$\begin{aligned} 2B &:= A_1^3 + A_2^3 = -2a^3 + 9ab - 27c, \\ A &:= A_1 A_2 = a^2 - 3b. \end{aligned}$$

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 ‘ $\sqrt[3]{}$ ’). Tenslotte bepalen we α_1 door op te merken:

$$\begin{aligned} 3\alpha_1 &= (\alpha_1 + \alpha_2 + \alpha_3) + (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) + (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) \\ &= -a + A_1 + A_2, \end{aligned}$$

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:

$$B = 10, \quad A = 7,$$

$$A_1 = \sqrt[3]{10 + \sqrt{10^2 - 7^3}} = \sqrt[3]{10 + 9i\sqrt{3}}$$

(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:

$$A_1 = -2 + i\sqrt{3} \quad \text{of} \quad A_1 = \frac{1}{2}(-1 + 3i\sqrt{3}) \quad \text{of} \quad A_1 = \frac{1}{2}(5 + i\sqrt{3}).$$

Omdat $A_1 A_2 = A$ zijn de corresponderende A_2 's dan:

$$A_2 = -2 - i\sqrt{3}, \quad A_2 = \frac{1}{2}(-1 + 3i\sqrt{3}), \quad A_2 = \frac{1}{2}(5 - i\sqrt{3}).$$

Tenslotte vinden we de drie nulpunten van f uit $\alpha = \frac{1}{3}(-a + A_1 + A_2)$, ze zijn:

$$-2, \quad -1, \quad 1 \quad \text{resp.}$$

Deze formules werden, langs een andere weg, gevonden door Cardano en Tartaglia rond 1540. Ze worden de Cardano formules genoemd.

Opmerking 11.1.12 We komen nog even terug op de oplossingsmethode. Het oplossen van de van de algemene derde graads vergelijking wordt terug gebracht op het oplossen van de vergelijking $A_i^3 = W$, waarbij de A_i^3 invariant zijn onder de (normale) ondergroep $A_3 = \{e, \rho, \rho^2\}$ van S_3 en waarbij W zelf de oplossing is van een vergelijking van graad 2. In opgave 4 geven we een methode aan om de algemene vergelijking f van graad 4 op te lossen door eerst 3 combinaties C_i van de nulpunten van f in te voeren. Deze C_i zijn invariant onder de normale ondergroep

$$H := \{e, (12)(34), (13)(24), (14)(23)\} \subset S_4.$$

Omdat $S_4/H \cong S_3$ worden de C_i in feite gepermuteerd door S_3 . Dan heeft het polynoom $(X - C_1)(X - C_2)(X - C_3)$ dus coëfficiënten die invariant zijn onder de hele S_4 , d.w.z. het heeft coëfficiënten die uit te drukken zijn in de coëfficiënten van f . Hiermee wordt het vinden van de nulpunten van een vierde graads polynoom teruggebracht tot het vinden van nulpunten van een derde graads polynomen.

Helaas is voor $n > 4$ A_n de enige, niet-triviale, normale ondergroep van S_n . Het oplossen van een vergelijking van graad $n > 4$ is inderdaad, om deze reden, ook wezenlijk veel moeilijker dan het oplossen van een vergelijking van graad ≤ 4 . In het college Galoistheorie wordt hier verder op ingegaan.

11.2 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 11.1.5 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 kopcoëfficiënten 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:

$$\begin{aligned} s_{-1} &= -1, \quad s_0 = 3, \quad s_1 = 0 \\ s_k &= s_{k-2} + s_{k-3} \quad \text{voor alle } k \in \mathbb{Z}, \\ s_k &\in \mathbb{Z} \quad \text{voor alle } k \in \mathbb{Z} \text{ (ook negatief!)}. \end{aligned}$$

4. Zij $f = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ met K een lichaam met $\text{kar}(K) \neq 2, 3$ en laat $\alpha_1, \dots, \alpha_4$ de nulpunten van f (in een uitbreiding van K) zijn.

- a. Definieer:

$$\begin{aligned} C_1 &= (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2 \\ C_2 &= (\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4)^2 \\ C_3 &= (\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4)^2. \end{aligned}$$

Geef een uitdrukking voor α_1 in termen van $\sqrt{C_i}$ en de coëfficiënt a van f .

- b. Ga na dat de S_4 actie (permutatie van de α_i) de C_i 's permuteert. Ga ook na dat de ondergroep H uit opmerking 11.1.12 de C_i invariant laat.

- c. Laat zien dat geldt:

$$\begin{aligned} C_1 + C_2 + C_3 &= 3a^2 - 8b \\ C_1C_2 + C_1C_3 + C_2C_3 &= 3a^4 - 16a^2b + 16b^2 + 16ac - 64d \\ C_1C_2C_3 &= (a^3 - 4ab + 8c)^2. \end{aligned}$$

- d. Ga na dat je met deze informatie de algemene vergelijking van graad 4 kunt oplossen.

5. Zij $f = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ een irreducibel polynoom met nulpunten $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. Dan is dus $\Omega_{\mathbb{Q}}^f \cong \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, i.h.b.:

$$\sqrt{\Delta} := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in \Omega_{\mathbb{Q}}^f, \quad \text{en} \quad \Delta \in \mathbb{Q},$$

met Δ de discriminant van f , zie voorbeeld 11.1.10.

- a. Bewijs dat $[\Omega_{\mathbb{Q}}^f : \mathbb{Q}] = 3$ of 6 .
- b. Bewijs dat $\sqrt{\Delta} \notin \mathbb{Q} \Rightarrow [\Omega_{\mathbb{Q}}^f : \mathbb{Q}] = 6$.
- c. Stel nu dat $\sqrt{\Delta} \in \mathbb{Q}$. Schrijf $f = (X - \alpha_1)(X^2 + rX + s) \in \mathbb{Q}(\alpha_1)[X]$. Bewijs dat $\alpha_2 \in \mathbb{Q}(\alpha_1)$ door een uitdrukking voor α_2 in termen van $\sqrt{\Delta}, a, b, c, r, s, \alpha_1 \in \mathbb{Q}(\alpha_1)$ te geven. Concludeer $[\Omega_{\mathbb{Q}}^f : \mathbb{Q}] = 3 \Leftrightarrow \sqrt{\Delta} \in \mathbb{Q}$.

12 De getallen van Gauss

12.1 Sommen van kwadraten

12.1.1 In deze paragraaf zullen we de vraag beantwoorden, welke gehele getallen als som van twee kwadraten geschreven kunnen worden. We gebruiken hierbij de theorie van ontbindingsringen en een stelling over de vermenigvuldigingsgroep van een domein, stelling 9.4.2.

12.1.2 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 $\mathbb{Z}[i]$:

$$n = a^2 + b^2 \iff n = (a + bi)(a - bi).$$

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**.

12.1.3 In de volgende paragraaf laten we zien dat $\mathbb{Z}[i]$ een hoofdideaaldomein en dus ook een ontbindingsdomein is. Iedere $n \in \mathbb{Z}_{>0}$ heeft dus ook 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 op dat 5 irreducibel is in \mathbb{Z} maar er geldt:

$$5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i),$$

en $1 + 2i$, $1 - 2i$ zijn geen van beide eenheid in $\mathbb{Z}[i]$, dus 5 is *niet* irreducibel in $\mathbb{Z}[i]$ (!).) We kunnen dan alle α 's in $\mathbb{Z}[i]$ met $\alpha\bar{\alpha} = n$ vinden omdat de irreducibele elementen in de priemontbinding van α een deelverzameling vormen van de irreducibele elementen in de priemontbinding van n .

12.1.4 Zij

$$n = p_1^{n_1} \dots p_t^{n_t}, \quad n_j \in \mathbb{Z}_{>0}$$

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 12.1.5 a. De eenheden van $\mathbb{Z}[i]$ zijn:

$$(\mathbb{Z}[i])^* = \{1, i, -1, -i\}.$$

b. Er geldt

$$2 = (-i)(1+i)^2,$$

met $-i \in (\mathbb{Z}[i])^*$ en $(1+i)$ is irreducibel in $\mathbb{Z}[i]$.

c. Als q een priemgetal is en $q \equiv 3 \pmod{4}$ dan is q irreducibel in $\mathbb{Z}[i]$.

d. Als p een priemgetal is en $p \equiv 1 \pmod{4}$ dan

$$p = \pi \cdot \bar{\pi}, \quad \text{en} \quad \pi \neq u\bar{\pi}$$

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 1.13 zagen we al:

$$a + bi \in (\mathbb{Z}[i])^* \iff N(a + bi) := a^2 + b^2 = \pm 1,$$

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:

$$N(\alpha)N(\beta) = q^2, \quad N(\alpha) > 1, \quad N(\beta) > 1.$$

Omdat q priem is in \mathbb{Z} , kan dat alleen als $N(\alpha) = N(\beta) = q$. Schrijf

$$\alpha = a + bi, \quad \text{dan is} \quad N(\alpha) = a^2 + b^2 = q.$$

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 bv. a oneven is dan kunnen we schrijven:

$$a = 2k + 1 \quad \text{dus} \quad a^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$

We zien dat $a^2 + b^2 \equiv 1 \pmod{4}$ als a óf b oneven is, en dat $a^2 + b^2 \equiv 2 \pmod{4}$ als a én b oneven zijn. Er is dus geen $\alpha \in \mathbb{Z}[i]$ met $N(\alpha) = q \equiv 3 \pmod{4}$ en we concluderen dat q irreducibel is.

d) Als $p \equiv 1 \pmod{4}$ dan is de groep $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ een cyclische groep van orde

$p - 1$, zie stelling 9.4.2. Als α een voortbrenger van deze groep is, definieer dan

$$x = \alpha^{\frac{p-1}{4}} \quad (\in \mathbb{F}_p).$$

De orde van x is dan 4, dus $x^2 = -1$. Men rekent eenvoudig na dat de afbeelding:

$$\phi : \mathbb{Z}[i] \longrightarrow \mathbb{F}_p, \quad a + bi \mapsto \bar{a} + \bar{b}x,$$

een (surjectief) ringhomomorfisme is. Omdat de ring $\mathbb{Z}[i]$ een hoofdideaalring is, zie 12.2.6 verderop, is er een $\pi \in \mathbb{Z}[i]$ met

$$(\pi) := \pi\mathbb{Z}[i] = \ker(\phi), \quad \text{i.h.b.} \quad \mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p.$$

Omdat $p \in \ker(\phi)$, 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 (representanten van de nevenklassen worden gegeven door $a + bi$ met $a, b \in \{0, 1, \dots, p-1\}$) 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 blijktbaar 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

$$a + bi = u(a - bi) \quad \text{met} \quad u \in \mathbb{Z}[i]^* = \{1, i, -1, -i\}.$$

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 12.1.5 bewezen. \square

Opmerking 12.1.6 Het moeilijkste deel van deze stelling, het ontbinden van een priem $p \equiv 1 \pmod{4}$ in $\mathbb{Z}[i]$, kan ook op elementaire wijze bewezen worden. In het bijzonder kan het gebruik van stelling 9.4.2 in dit bewijs vermeden worden. het elementaire bewijs is niet erg lang, zie D. Zagier: A one-sentence proof that every prime $\equiv 1 \pmod{4}$ is a sum of two squares, The American Mathematical Monthly, Vol. 97, p.144.

Gevolg 12.1.7 Zij $n \in \mathbb{Z}_{>0}$, met priemontbinding:

$$n = 2^k p_1^{n_1} \dots p_r^{n_r} q_1^{m_1} \dots q_s^{m_s}, \quad n_j, m_j \in \mathbb{Z}_{>0},$$

hierin zijn p_j, q_j onderling verschillende priemgetallen met $p_j \equiv 1 \pmod{4}$ en $q_j \equiv 3 \pmod{4}$.

Dan is n te schrijven als som van twee kwadraten precies dan als:

$$m_j \equiv 0 \pmod{2}, \quad \text{voor alle } j \in \{1, \dots, s\}.$$

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:

$$n = 2^k (\pi_1^{n_1} \bar{\pi}_1^{n_1}) \dots (\pi_r^{n_r} \bar{\pi}_r^{n_r}) q_1^{m_1} \dots q_s^{m_s}.$$

Als $n = \alpha \bar{\alpha}$ is de priemontbinding van α van de vorm:

$$\alpha = u(1+i)^l (\pi_1^{a_1} \bar{\pi}_1^{b_1}) \dots (\pi_r^{a_r} \bar{\pi}_r^{b_r}) q_1^{c_1} \dots q_s^{c_s},$$

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:

$$m_j = 2c_j, \quad \text{dus } m_j \equiv 0 \pmod{2} \quad \forall j.$$

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

$$c_j := \frac{m_j}{2}, \quad l := k.$$

Voor a_j kiezen we een geheel getal tussen 0 en n_j :

$$a_j \in \{0, 1, \dots, n_j\} \quad \text{en} \quad b_j := n_j - a_j,$$

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 $4 \cdot \prod_{i=1}^r (n_i + 1)$ mogelijke α 's vinden, dit is dus ook precies het aantal elementen van de verzameling:

$$\{ (a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n \}.$$

Hiermee is 12.1.7 bewezen. □

Voorbeeld 12.1.8 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

$$\alpha = (1 + 2i)3 = 3 + 6i, \quad \text{dan} \quad 45 = \alpha\bar{\alpha} = 3^2 + 6^2.$$

Zij $n = 65 = 5 \cdot 13$. Omdat $5 = (1 + 2i)(1 - 2i)$ en $13 = (2 + 3i)(2 - 3i)$ is de priemontbinding van 65 in $\mathbb{Z}[i]$:

$$65 = \pi_1\bar{\pi}_1\pi_2\bar{\pi}_2, \quad \text{met} \quad \pi_1 = 1 + 2i, \quad \pi_2 = 2 + 3i.$$

Nemen we

$$\alpha = \pi_1\pi_2 \quad \text{dan} \quad \alpha = -4 + 7i \quad \text{en} \quad 65 = (-4)^2 + 7^2.$$

Nemen we

$$\alpha = \pi_1\bar{\pi}_2 \quad \text{dan} \quad \alpha = 8 + i \quad \text{en} \quad 65 = 8^2 + 1^2.$$

Dit zijn, op tekens en volgorde van a, b na, de enige twee schrijfwijzes van 65 als som van twee kwadraten.

12.2 Euclidische ringen

12.2.1 We gaan ons nu bezighouden met een algemene methode om aan te tonen dat bepaalde ringen hoofdideaalringen 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*: stelling 2.3.2 in het geval \mathbb{Z} , en stelling 3.4.1 in het geval $K[X]$. Ringen waarin zo'n deling met rest mogelijk is heten **Euclidisch**. De precieze definitie luidt als volgt.

Definitie 12.2.2 Een domein R heet een **Euclidische ring** als er een functie

$$g : R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

bestaat met de volgende eigenschap:

(**) voor alle $a, b \in R$ met $b \neq 0$ bestaan er $q, r \in R$ met

$$a = qb + r \quad r = 0 \quad \text{of} \quad g(r) < g(b).$$

Opmerking 12.2.3 Eigenschap (**) 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 $g(f) = \text{graad}(f)$. We zien dat we in het algemeen bij $g(a)$ aan iets als de ‘grootte’ van a moeten denken.

Een lichaam K is op triviale wijze een Euclidische ring, als we $g(a) = 0$ zetten, voor alle $a \in K - \{0\}$.

Stelling 12.2.4 *Elke Euclidische ring R is een hoofdideaalring.*

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

$$g(b) = \min \{g(x) : x \in I - \{0\}\}.$$

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 12.2.4 bewezen. \square

12.2.5 Merk op dat het bewijs van deze stelling geheel analoog verloopt aan de bewijzen van 2.3.2 (voor $R = \mathbb{Z}$) en 3.4.1 (voor $R = K[X]$).

De omkering van 12.2.4 geldt niet: er bestaan hoofdideaalringen die niet Euclidisch zijn. Een dergelijk voorbeeld wordt gegeven door de ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$, zie opgaven 2 en 3.

Stelling 12.2.6 *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 hoofdideaalring.

Bewijs. We verifiëren de voorwaarden.

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

$$\alpha = \gamma\beta + \rho \quad \text{en} \quad N(\rho) < N(\beta)$$

(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

$$\frac{\alpha}{\beta} = u + vi, \quad \text{met} \quad u, v \in \mathbb{R}$$

(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:

$$\gamma = u' + v'i \in \mathbb{Z}[i].$$

Definieer vervolgens de ‘rest’ ρ door:

$$\rho := \alpha - \gamma\beta \in \mathbb{Z}[i], \quad \text{dan} \quad \alpha = \gamma\beta + \rho.$$

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 $N(\rho/\beta) < 1$:

$$\begin{aligned} N\left(\frac{\rho}{\beta}\right) &= N\left(\frac{\alpha}{\beta} - \gamma\right) \\ &= N((u - u') + (v - v')i) \\ &= (u - u')^2 + (v - v')^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \\ &= \frac{1}{2} \\ &< 1 \end{aligned}$$

Hiermee is bewezen dat $\mathbb{Z}[i]$ een Euclidische ring is, en uit stelling 12.2.4 volgt dat $\mathbb{Z}[i]$ een hoofdideaalring is. \square

Voorbeeld 12.2.7 We voeren de deling met rest uit voor:

$$\alpha = 5 + 6i, \quad \beta = 2 + i.$$

Om te beginnen delen we deze getallen in \mathbb{C} :

$$\frac{\alpha}{\beta} = \frac{(5 + 6i)(2 - i)}{(2 + i)(2 - i)} = \frac{16 + 7i}{5} = 3\frac{1}{5} + i \cdot 1\frac{2}{5}.$$

Als ‘goede benadering’ γ nemen we:

$$\gamma := 3 + i \quad \implies \quad \rho := \alpha - \gamma\beta = 5 + 6i - (3 + i)(2 + i) = i.$$

De deling met rest is dus:

$$5 + 6i = (3 + i)(2 + i) + i, \quad \text{en inderdaad} \quad N(i) = 1 < 5 = N(2 + i).$$

12.2.8 Het gegeven bewijs van stelling 12.2.6 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 $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})] = \{a + \frac{1}{2}(1 + \sqrt{-3})b : a, b \in \mathbb{Z}\}$. Deze laatste ring vormt in het complexe vlak de verzameling hoekpunten van een regelmatig 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 fors probleem te zitten, maar ruim een jaar later wist Wiles dit samen met Richard Taylor te omzeilen. Het nu alom geaccepteerde bewijs is verschenen in *Annals of Mathematics* **142** (1995).

12.2.9 De ring $\mathbb{Z}[\sqrt{-5}]$ is geen hoofdideaalring, zie opgave 16 op blz. 46, 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 hoofdideaalring is, dus ook niet Euclidisch. In dit geval blijkt het niet overdekte gedeelte van het complexe vlak uit een stel losse punten te bestaan.

12.2.10 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

$$(*) \quad g(\alpha) = |N(\alpha)|, \quad N \text{ als in 1.13.}$$

Voor meer voorbeelden zie men de opgaven. De bewijzen zijn steeds analoog aan het bewijs voor $\mathbb{Z}[i]$.

Een interessante ring is $\mathbb{Z}[\sqrt{14}]$: in dit geval voldoet de door (*) gedefinieerde functie niet aan de eis, maar men vermoedt dat er wel een andere functie g is die aan de eis voldoet. Dit vermoeden is evenwel onbewezen. Het is dus onbekend of $\mathbb{Z}[\sqrt{14}]$ Euclidisch is. Wel weet men dat $\mathbb{Z}[\sqrt{14}]$ een hoofdideaalring is.

12.3 Het Euclidische algoritme

In deze paragraaf is R steeds een Euclidische ring.

12.3.1 In een hoofdideaaldomein (zoals bv. R , zie stelling 12.2.4) 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:

$$(a, b) = (d), \quad \text{i.h.b. geldt:} \quad ar + bs = d,$$

voor zekere r, s in R . We noemen d 'de' **grootste gemene deler** van a en b , we schrijven $ggd(a, b) = d$. 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 12.3.2 Een hoofdideaaldomein is ook een ontbindingsdomein, zie 5.3.5. In factorontbindingsdomeinen hebben we eerder al een ggd gedefinieerd, zie 5.4.4. Opgave 11 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.

12.3.3 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:

$$a = q_0b + r_1 \quad \text{met} \quad r_1 = 0 \quad \text{of} \quad g(r_1) < g(b).$$

Als $r_1 = 0$, dan is $(a, b) = (q_0b, b) = (b)$, waarmee de ggd bepaald is, $ggd(a, b) = b$. I.h.a. geldt, omdat $a, b \in (a, b)$, dat ook $r_1 = a - q_0b \in (a, b)$. Er geldt zelfs:

$$(a, b) = (q_0b + r_1, b) = (b, r_1), \quad \text{met} \quad g(r_1) < g(b) \leq g(a).$$

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 :

$$b = q_1r_1 + r_2, \quad \text{met} \quad r_2 = 0 \quad \text{of} \quad g(r_2) < g(r_1).$$

Bovendien geldt:

$$(a, b) = (b, r_1) = (q_1r_1 + r_2, r_1) = (r_1, r_2).$$

Als $r_2 \neq 0$, dan delen we r_2 op r_1 :

$$r_1 = q_2r_2 + r_3 \quad \text{met} \quad r_3 = 0 \quad \text{of} \quad g(r_3) < g(r_2)$$

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

$$r_{n-2} = q_{n-1}r_{n-1} + r_n \quad \text{en} \quad r_n = 0.$$

Dan geldt:

$$(a, b) = (r_{n-1}, r_n) = (r_{n-1}), \quad \text{dus} \quad ggd(a, b) = r_{n-1},$$

waarmee we de ggd van a en b gevonden hebben.

12.3.4 De elementen $r, s \in R$ met $ar + bs = d$ zijn nu eenvoudig te bepalen.

$$\left. \begin{array}{l} a - q_0b = r_1 \\ b - q_1r_1 = r_2 \end{array} \right\} \implies b - q_1(a - q_0b) = r_2, \quad \text{ofwel} \quad (-q_1)a + (1 + q_0q_1)b = r_2,$$

waarbij we de eerste vergelijking in de tweede gesubstitueerd hebben. Algemeener, als

$$\left. \begin{array}{l} h_{i-1}a + k_{i-1}b = r_{i-1} \\ h_i a + k_i b = r_i \end{array} \right\} \quad \text{en} \quad r_{i-1} - q_i r_i = r_{i+1},$$

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:

$$r_{-1} := a, \quad r_0 := b.$$

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 12.3.5 We bepalen met het algoritme de *ggd* van 84 en 30 in de euclidische ring \mathbb{Z} (dus $g(n) = |n|$). Merk op:

$$84 = 2 \cdot 30 + 24, \quad 30 = 1 \cdot 24 + 6, \quad 24 = 4 \cdot 6 + 0,$$

dus $(84, 30) = (30, 24) = (24, 6) = (6)$ en $ggd(84, 30) = 6$. Verder geldt:

$$24 = 84 - 2 \cdot 30, \quad 30 - 1 \cdot 24 = 6 \quad \implies \quad 30 - 1 \cdot (84 - 2 \cdot 30) = (-1) \cdot 84 + 3 \cdot 30 = 6,$$

zodat we $r = -1$ en $s = 3$ kunnen nemen.

Voorbeeld 12.3.6 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, zie ook 7.2.7.

Zij

$$f = X^3 + X^2 - 1 \in \mathbb{Q}[X],$$

dan is f irreducibel omdat hij geen nulpunt in \mathbb{Z} en dus ook niet in \mathbb{Q} heeft.

Zij

$$K := \mathbb{Q}[X]/(f), \quad \alpha := X + (f).$$

Dan is $K = \mathbb{Q}[\alpha]$ een lichaam en elk element van K kan op unieke wijze geschreven worden als

$$a_0 + a_1\alpha + a_2\alpha^2, \quad a_i \in \mathbb{Q}.$$

We bepalen de inverse van

$$b(\alpha) = 1 + \alpha^2, \quad \text{met } b = X^2 + 1 \quad (\in \mathbb{Q}[X]).$$

Omdat $\mathbb{Q}[X]$ een hoofdideaalring is en f irreducibel is met $gr(f) > gr(b)$, is $ggd(f, b) = 1$. Er zijn dus $r, s \in \mathbb{Q}[X]$ met

$$fr + sb = 1 \quad (\in \mathbb{Q}[X]) \quad \text{dus} \quad s(\alpha)(\alpha^2 + 1) = 1 \quad (\in K = \mathbb{Q}[X]/(f)),$$

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 $g(f) = gr(f)$) kunnen we s met het Euclidische algoritme bepalen. Er geldt:

$$X^3 + X^2 - 1 = (X+1)(X^2+1) + (-X-2), \quad \text{dus } q_0 = X+1, \quad r_1 = -(X+2).$$

Verder is:

$$X^2 + 1 = (-X + 2)(-X - 2) + 5, \quad \text{dus } q_1 = -X + 2, \quad r_2 = 5.$$

Omdat 5 een eenheid in $\mathbb{Q}[X]$ is, geldt inderdaad dat $ggd(f, b) = 1$.

Deze vergelijkingen kunnen we herschrijven als:

$$-X - 2 = f - (X + 1)b, \quad 5 = b + (X - 2)(-X - 2).$$

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:

$$rf + sb = 1 \quad \text{met} \quad r = \frac{1}{5}(X - 2), \quad s = \frac{1}{5}(3 + X - X^2).$$

Substitueren we $X := \alpha$ in deze vergelijking dan zien we dat:

$$(\alpha^2 + 1)^{-1} = \frac{1}{5}(3 + \alpha - \alpha^2).$$

12.4 Opgaven

1. Zij $\gamma = \frac{1}{2}(1 + \sqrt{-19})$, en $R = \mathbb{Z}[\gamma] = \{a + b\gamma : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Definieer

$$N : R \longrightarrow \mathbb{Z}_{\geq 0}, \quad N(a + b\gamma) := a^2 + ab + 5b^2.$$

- Bewijs dat $\gamma^2 = \gamma - 5$, en dat R een deelring van \mathbb{C} is.
- Bewijs: $N(\alpha\beta) = N(\alpha)N(\beta)$ voor alle $\alpha, \beta \in R$.
- Laat $\alpha \in R$. Bewijs:

$$\alpha \in R^* \iff N(\alpha) = 1 \iff \alpha \in \{\pm 1\},$$

$$\text{dus } R^* = \{1, -1\}.$$

- Bewijs dat er geen surjectieve ringhomomorfismen

$$\varphi : R \longrightarrow \mathbb{F}_2 \quad \text{of} \quad \varphi : R \longrightarrow \mathbb{F}_3$$

bestaan (aanwijzing: gebruik $\gamma^2 = \gamma - 5$, en kijk waar $\varphi(\gamma)$ aan gelijk zou kunnen zijn).

2. Laat $R = \mathbb{Z}[\gamma]$ zijn als in de vorige opgave. Stel dat $g : R - \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ voldoet aan de voorwaarde uit 12.2.2, en kies $b \in R - \{0, 1, -1\}$ met $g(b)$ zo klein mogelijk.

- Bewijs dat b geen eenheid is, en dat geldt:

$$\forall a \in R : \exists r \in \{0, 1, -1\} : a \equiv r \pmod{Rb}.$$

- Bewijs: $R/Rb = \{\bar{0}, \bar{1}, \overline{-1}\}$, met $\bar{r} = (r + Rb)$. Leid hieruit af, dat $R/Rb \cong \mathbb{F}_2$ of \mathbb{F}_3 .
- Leid met behulp van opgave 1 (d) een tegenspraak af.

Conclusie van dit vraagstuk: zo'n g bestaat niet, dus R is *niet* Euclidisch.

3. Laten R en N als in opgave 1 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

$$a = qb + r \quad \text{en} \quad N(r) < N(b).$$

- 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 hoofdideaalring is (aanwijzing: imiteer het bewijs van 12.2.4, gebruik makend van a. i.p.v. de eis van 12.2.2).
4. Definieer $\varphi : \mathbb{Z}[i] \rightarrow \mathbb{F}_{13}$ 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 $\ker(\varphi)$.
5. 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.
6. 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 $5n = r^2 + s^2$.
7. Bewijs dat de ringen $\mathbb{Z}[\sqrt{m}]$, $m = -2, 2, 3$, Euclidisch zijn, met $g(\alpha) = |N(\alpha)|$.
8. 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 $x, y \in \mathbb{Q}$.)

9. Laat $R = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z}, b \text{ oneven}\}$. 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
- $$g : R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}, \quad g(x) = k \quad \text{als} \quad x = 2^k \cdot u,$$
- 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 ?
10. 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 $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$, en stel dat R een 1 heeft. Bewijs:

$$f \in R[[X]]^* \iff a_0 \in R^*.$$

b. Stel dat R een *lichaam* is. Definieer

$$g : R[[X]] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

door

$$g\left(\sum_{i=0}^{\infty} a_i X^i\right) = \min \{i : a_i \neq 0\}.$$

Bewijs dat deze functie de ring $R[[X]]$ tot een Euclidische ring maakt.

11. Zij R een hoofdideaaldomein, zij $a, b \in R$ met priemontbinding:

$$a = up_1^{n_1} \dots p_r^{n_r}, \quad b = vp_1^{m_1} \dots p_r^{m_r}, \quad n_i, m_i \in \mathbb{Z}_{\geq 0}.$$

Definieer $d \in R$ als in definitie 5.4.4:

$$d := p_1^{k_1} \dots p_r^{k_r}, \quad \text{met } k_i := \min \{n_i, m_i\}.$$

Bewijs dat $(a, b) = (d)$ (hint: bekijk het bewijs van stelling 5.3.7).

13 Projectieve Modulen

13.1 Quotiënten van modulen

13.1.1 Zoals bekend is iedere ondergroep N van een abelse groep M een normale ondergroep, en dus bestaat er een quotientgroep M/N . Als M, N bovendien modulen over een ring R zijn, dan is er in het algemeen geen ‘natuurlijke’ manier (d.w.z. een manier die R -moduul structuur van M en N gebruikt) om een R -moduulstructuur op M/N te zetten. In geval N een deelmoduul van M is kan dat echter wel, zoals we nu zullen zien.

13.1.2 Zij N een deelmoduul van een R -moduul M . We definiëren een actie van R op de abelse groep

$$M/N = \{\bar{m} = m + N \subset M : m \in M\}$$

door het volgende voorschrift:

$$R \times M/N \longrightarrow M/N, \quad (r, m + N) \mapsto rm + N.$$

We moeten uiteraard eerst laten zien dat dit een goed gedefinieerde afbeelding $R \times M/N \rightarrow M/N$ is, d.w.z. :

$$\text{als } m_1 + N = m_2 + N \quad \text{dan } rm_1 + N = rm_2 + N.$$

Welnu, omdat geldt:

$$m_1 + N = m_2 + N \implies m_1 - m_2 \in N, \quad \text{en } rN \subset N$$

(N is immers een deelmoduul van M) volgt:

$$m_1 - m_2 \in N \implies r(m_1 - m_2) = rm_1 - rm_2 \in N,$$

en dit is equivalent met $rm_1 + N = rm_2 + N$. We concluderen dat $m_1 + N = m_2 + N \implies rm_1 + N = rm_2 + N$.

Men rekent eenvoudig na dat de gegeven afbeelding inderdaad aan de axioma's voor een actie voldoet. We schrijven overigens gewoon M/N voor het R -moduul bestaande uit de abelse groep M/N en bovenstaande actie. Men noemt het R -moduul M/N het **quotient** van M door N .

13.1.3 Voorbeelden.

- a. Zij $R = K$, een lichaam en zij $V \subset K^n$ een lineaire deelruimte. Dan heeft de abelse groep K^n/V dus op natuurlijke wijze de structuur van een lineaire ruimte over K . We kunnen dit explicieter maken door een (nieuwe) basis $\vec{f}_1, \dots, \vec{f}_n$ van K^n te kiezen zodat:

$$V := \langle \vec{f}_1, \vec{f}_2, \dots, \vec{f}_k \rangle \quad \text{d.w.z.}$$

$$V = \left\{ \sum_{i=1}^n x_i \vec{f}_i \in K^n : x_i = 0 \text{ als } k < i \leq n \right\}.$$

(dat kan door eerst een basis van V te kiezen en deze dan uit te breiden tot een basis van K^n). Definieer:

$$W := \langle \vec{f}_{k+1}, \dots, \vec{f}_n \rangle, \quad \text{dan is } K^n = V \oplus W.$$

Iedere $\vec{x} \in K^n$ is dus op unieke wijze te schrijven als $\vec{x} = \vec{v} + \vec{w}$ met $\vec{v} \in V$, $\vec{w} \in W$. I.h.b. geldt $\vec{x} \in V$ precies dan dan als $\vec{w} = \vec{0}$. Zij dan:

$$\vec{x}_1 = \vec{v}_1 + \vec{w}_1, \quad \vec{x}_2 = \vec{v}_2 + \vec{w}_2 \quad \text{dan geldt :}$$

$$\vec{x}_1 + V = \vec{x}_2 + V \iff \vec{x}_1 - \vec{x}_2 \in V \iff \vec{w}_1 = \vec{w}_2.$$

Er geldt dus:

$$K^n/V = \{ \vec{w} + V \subset K^n : \vec{w} \in W \},$$

en

$$\vec{w}_1 + V = \vec{w}_2 + V \iff \vec{w}_1 = \vec{w}_2.$$

Iedere nevenklasse $\vec{x} + V$ met $\vec{x} = \vec{v} + \vec{w}$ kan dan, op unieke wijze, geschreven worden als: $\vec{x} + V = \vec{w} + V$ met $\vec{w} \in W$. De lineaire ruimte K^n/V wordt op deze wijze geïdentificeerd met de lineaire ruimte W , precieser, de afbeelding

$$f : K^n/V \longrightarrow W, \quad \vec{w} + V \mapsto \vec{w}$$

is een isomorfisme van lineaire ruimten over K . Merk op dat er vele keuzes voor W zijn, maar elke keuze geeft een lineaire ruimte die isomorf is met K^{n-k} .

- b. Als G een abelse groep is en H een ondergroep van G is, dan is G/H weer een abelse groep en is dus ook een \mathbb{Z} -moduul. De actie van \mathbb{Z} die we op de abelse groep G/H definieerden is inderdaad precies de actie van \mathbb{Z} die we op het quotiënt G/H definieerden.

- c. Als R een ring is en $I \subset R$ is een ideaal, dan is I een deelmoduul van het R -moduul R . De R -moduul structuur op het quotient R/I is dezelfde als die uit 6.1.3 (ga na).

Stelling 13.1.4 *Zij $f : M \rightarrow N$ een R -moduulhomomorfisme. Dan geldt:*

- a. *Het R -moduulhomomorfisme f induceert een R -moduulisomorfisme*

$$M/\ker(f) \xrightarrow{\cong} \text{im}(f), \quad m + \ker(f) \mapsto f(m).$$

- b. *Zij $K \subset M$ een deelmoduul, dan is de **kanonieke** afbeelding*

$$\phi : M \longrightarrow M/K, \quad m \mapsto m + K$$

een (surjectief) R -moduulhomomorfisme met $\ker(\phi) = K$.

- c. *Als $g : N \rightarrow P$ een R -moduulhomomorfisme is, dan is ook de samenstelling $g \circ f : M \rightarrow P$ een R -moduulhomomorfisme:*

$$g \circ f : M \xrightarrow{f} N \xrightarrow{g} P.$$

We schrijven meestal gf voor de samenstelling $g \circ f$.

Bewijs. De eerste twee uitspraken zijn al bewezen voor het speciale geval $M = R$ en $\ker(f) = K = I$, een ideaal in R , in het hoofdstuk over ringen en de voorbeelden hierboven. Het algemene bewijs wordt aan de lezer overgelaten. De laatste uitspraak volgt direkt uit de definitie. \square

13.2 Homomorfismen van R -modulen

13.2.1 De volgende terminologie wordt veel gebruikt voor R -moduulhomomorfismen (niet alleen in de algebra, maar ook bv. ook in de topologie).

Een rij van R -moduulhomomorfismen

$$\dots \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow \dots$$

heet **exact in N** als geldt:

$$\text{im}(f) = \ker(g).$$

13.2.2 Speciale gevallen zijn:

$$0 \longrightarrow N \xrightarrow{g} P \quad \text{is exact} \quad \text{dan en slechts dan als } g \text{ injectief is,}$$

immers, het beeld van de linkerpijl is $0 \in N$, dus de rij is exact (in N) precies dan als $0 = \ker(g)$ d.w.z. als g injectief is. De rij

$$M \xrightarrow{f} N \longrightarrow 0 \quad \text{is exact} \quad \text{dan en slechts dan als } f \text{ surjectief is,}$$

immers, de kern van de rechterpijl is het hele moduul N , dus de rij is exact (in N) precies dan als $\text{im}(f) = N$ d.w.z. als f surjectief is.

Tenslotte bekijken we de rij:

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0.$$

Deze noemen we **exact** als hij bij elk van de drie modulen M, N, P exact is. In dat geval is dus f injectief, we kunnen dan M identificeren met het deelmoduul $\text{im}(f)$ van N . Verder is g surjectief en er geldt $\ker(g) = \text{im}(f) \cong M$, dus (zie 6.2.3),

$$f : M \xrightarrow{\cong} \text{im}(f) \subset N, \quad \text{im}(f) = \ker(g), \quad N/\text{im}(f) \cong P.$$

Op identificaties (d.w.z. R -moduulisomorfismen) na is zo'n exact rijtje dus altijd van de vorm:

$$0 \longrightarrow \ker(g) \hookrightarrow N \xrightarrow{g} N/\ker(g) \longrightarrow 0.$$

13.2.3 De verzameling van de (links-) R -moduulhomomorfismen van M naar N wordt aangegeven met:

$$\text{Hom}(M, N) = \{f : M \rightarrow N : f \text{ is een } R\text{-moduulhomomorfisme}\}.$$

Als men de ring R wil benadrukken schrijft men ook wel $\text{Hom}_R(M, N)$. Deze verzameling is op natuurlijke wijze een abelse groep, met de regel:

$$(f + g)(m) := f(m) + g(m) \quad (f, g \in \text{Hom}(M, N), \quad m \in M).$$

Men schrijft vaak $\text{Hom}(M, M) = \text{End}(M)$, de ring van de R -moduulendomorfismen van M . (Het product in deze ring is het samenstellen van afbeeldingen: $fg = f \circ g$.)

13.2.4 Als R commutatief is, dan vormt $\text{Hom}(M, N)$ zelfs een R -moduul, de actie van R wordt gegeven door:

$$(rf)(m) := rf(m), \quad (f \in \text{Hom}(M, N), m \in M, r \in R).$$

De commutativiteit van R is essentieel, er moet namelijk gelden dat $rf \in \text{Hom}(M, N)$ dus i.h.b. moet rf R -lineair zijn. Merk op:

$$(rf)(sm) := rf(sm) = rsf(m),$$

de laatste stap wegens het R -lineair zijn van $f \in \text{Hom}(M, N)$. Als R commutatief is, dan kunnen we hiervoor schrijven $sr f(m)$, d.w.z. dan geldt $(rf)(sm) = s(rf)(m)$ zodat (rf) inderdaad R -lineair is. Ga zelf na dat $\text{Hom}(M, N)$ een R moduul is als R commutatief is.

13.2.5 In de rest van deze paragraaf nemen we steeds aan dat R commutatief is.

(De meeste resultaten die we bewijzen zijn ook juist voor niet-commutatieve ringen als je $\text{Hom}(M, N)$ alleen als abelse groep beschouwt.)

13.2.6 Voorbeelden

a. Zij K een lichaam, en neem $M = N = K^n$. Dan geldt:

$$\text{End}(K^n) := \text{Hom}(K^n, K^n) \cong M(n, K),$$

hierbij beschouwen we $M(n, K)$ als een K -moduul door matrices op de gebruikelijke wijze op te tellen (d.w.z. componentsgewijs) en met een scalar te vermenigvuldigen. Een $\alpha \in \text{Hom}(K^n, K^n)$ is nl., per definitie, een K -lineaire afbeelding.

b. Zij R een ring en zij M een R -moduul. Dan geldt dat

$$\Phi_1 : \text{Hom}(R, M) \xrightarrow{\cong} M, \quad f \mapsto f(1),$$

een isomorfismen van R -modulen is. De injectiviteit van Φ_1 volgt uit $f(r) = rf(1)$. Als nl. $\Phi_1(f) := f(1) = 0$ dan geldt $f(r) = rf(1) = r0 = 0$ voor elke $r \in R$ zodat $f = 0$. Voor de surjectiviteit merken we op dat voor elke $m \in M$:

$$f_m : R \longrightarrow M \quad f_m(r) := rm,$$

een R -moduulhomomorfisme is (ga na), en er geldt $\Phi_1(f_m) = m$.
Rest ons nog te bewijzen dat Φ_1 een R -moduulhomomorfisme is.
Welnu,

$$\begin{aligned}\Phi_1(f+g) &:= (f+g)(1) := f(1) + g(1) = \Phi_1(f) + \Phi_1(g), \\ \Phi_1(rf) &:= rf(1) = r\Phi_1(f),\end{aligned}$$

waarmee de uitspraak bewezen is.

c. Voor elke $n \in \mathbb{Z}_{>1}$ geldt:

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0.$$

Als $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$ namelijk \mathbb{Z} -lineair is dan geldt:

$$0 = f(\bar{0}) = f(\bar{n}) = f(n\bar{1}) = nf(\bar{1}),$$

en in \mathbb{Z} geldt dat $n \neq 0$ en $nf(\bar{1}) = 0$ impliceert dat $f(\bar{1}) = 0$.
Maar dan geldt $f(\bar{a}) = af(\bar{1}) = a0 = 0$ voor elke $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$
waarmee bewezen is dat $f = 0$. In woorden: elk element in $\mathbb{Z}/n\mathbb{Z}$
heeft eindige orde en het beeld onder f heeft dus eindige orde.
Maar dan is het beeld 0 omdat 0 het enige element van eindige
orde in \mathbb{Z} is.

13.3 Hom en exactheid

In deze paragraaf is R steeds een commutatieve ring.

13.3.1 Als A een R -moduul is, en $f \in \text{Hom}(M, N)$, dan kunnen we ieder R -moduulhomomorfisme $\phi : A \rightarrow M$ samenstellen met $f : M \rightarrow N$ tot een R -moduulhomomorfisme: $f_*(\phi) = f \circ \phi : A \rightarrow N$:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \phi \swarrow & \nearrow_{f_*(\phi)} & \\ & A & \end{array} \quad \text{met} \quad f_* : \text{Hom}(A, M) \longrightarrow \text{Hom}(A, N), \quad \phi \mapsto f \circ \phi.$$

Een andere, suggestieve, schrijfwijze voor f_* is $\text{Hom}(A, f)$.

Men rekent met de definities eenvoudig na dat f_* een R -moduulhomomorfisme is, d.w.z. ga na dat geldt:

$$f_*(\phi + \psi) = f_*(\phi) + f_*(\psi), \quad f_*(r\phi) = rf_*(\phi),$$

voor alle $\phi, \psi \in \text{Hom}(A, M)$ en alle $r \in R$.

13.3.2 Een interessant probleem is het volgende. Stel dat $f : M \rightarrow N$ surjectief is, is dan ook $f_* : \text{Hom}(A, M) \rightarrow \text{Hom}(A, N)$ surjectief? (Dezelfde vraag met injectief i.p.v. surjectief kan positief beantwoord worden, zie stelling 13.3.5. Als f niet surjectief is, dan is f_* niet surjectief als $A = R$, zie opgave 1).

We laten eerst zien dat f_* niet noodzakelijk surjectief is als f surjectief is. De R -modulen A met de eigenschap:

$$f : M \longrightarrow N \quad \text{surjectief} \quad \implies \quad f_* : \text{Hom}(A, M) \longrightarrow \text{Hom}(A, N) \quad \text{surjectief}$$

blijken nog vele andere interessante eigenschappen te hebben, zie ook 13.4.1.

13.3.3 Voorbeeld. We beschouwen:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/n\mathbb{Z} \\ \tilde{h} \swarrow & \nearrow \text{id}_{\mathbb{Z}/n\mathbb{Z}} & \\ & \mathbb{Z}/n\mathbb{Z} & \end{array} \quad \text{met} \quad f : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto a + n\mathbb{Z}.$$

Als de afbeelding f_* surjectief is, dan moeten we $\tilde{h} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$ kunnen vinden met $f \circ \tilde{h} = \text{id}_{\mathbb{Z}/n\mathbb{Z}}$.

Er geldt echter: $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$, zie 13.2.6, dus moet gelden $\tilde{h} = 0$. Omdat $f_*(0) = 0 \neq \text{id}_{\mathbb{Z}/n\mathbb{Z}}$ is f_* niet surjectief.

13.3.4 Voorbeeld. We laten zien: als $A = R$ en $f : M \rightarrow N$ is een surjectief R -moduulhomomorfisme, dan is ook $f_* : \text{Hom}(R, M) \rightarrow \text{Hom}(R, N)$ surjectief.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \tilde{h} \swarrow & \nearrow h & \\ & R & \end{array}$$

Zij dan $h \in \text{Hom}(R, N)$, we zoeken een $\tilde{h} \in \text{Hom}(R, M)$ met $f_*(\tilde{h}) = f \circ \tilde{h} = h$. Omdat f surjectief is, is er een $m \in M$ met

$$f(m) = h(1), \quad \text{definieer dan} \quad \tilde{h} : R \rightarrow M, \quad \tilde{h}(r) := rm.$$

Dan geldt: $\tilde{h} \in \text{Hom}(R, M)$ (zie 13.2.6) en bovendien:

$$(f_*\tilde{h})(r) := f\tilde{h}(r) = f(rm) = rf(m) = rh(1) = h(r),$$

voor elke $r \in R$, zodat inderdaad $f_*\tilde{h} = h$.

Stelling 13.3.5 *Zij R een ring en zij*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P$$

een exacte rij van R -modulen.

Dan geldt voor ieder R -moduul A dat:

$$0 \longrightarrow \text{Hom}(A, M) \xrightarrow{f_*} \text{Hom}(A, N) \xrightarrow{g_*} \text{Hom}(A, P)$$

een exacte rij van R -modulen is (men zegt wel dat $\text{Hom}(A, -)$ links-exact is).

In het bijzonder geldt: als $f : M \rightarrow N$ injectief is, dan is ook $f_ : \text{Hom}(A, M) \rightarrow \text{Hom}(A, N)$ injectief.*

Bewijs. Zij een exact rijtje en een R -moduul A gegeven.

We bewijzen eerst dat f_* injectief is, d.w.z. dat het tweede rijtje exact is in $\text{Hom}(A, M)$. Zij $\phi \in \text{Hom}(A, M)$, $\phi \neq 0$ gegeven. Dan is er een $a \in A$ met $\phi(a) \neq 0$. Omdat $\phi(a) \in M$ en $f : M \rightarrow N$ injectief is, geldt dan $(f_*\phi)(a) := f(\phi(a)) \neq 0$, d.w.z. dat $f_*\phi \neq 0$. Hiermee is bewezen dat f_* injectief is.

Om de exactheid in $\text{Hom}(A, N)$ te bewijzen, moeten we laten zien dat $\text{im}(f_*) = \text{ker}(g_*)$.

‘ \subset ’ Elk element $\psi \in \text{im}(f_*)$ is te schrijven als $\psi = f_*\phi$ voor zekere $\phi \in \text{Hom}(A, M)$. Voor elke $a \in A$ geldt dan dat $\psi(a) = f\phi(a) \in \text{im}(f)$. Er geldt $\text{im}(f) = \text{Ker}(g)$, wegens exactheid van de eerste rij. Maar dan is $g\psi(a) = 0$ voor alle $a \in A$ dus $g_*\psi = 0$. Hiermee is aangetoond dat $\text{im}(f_*) \subset \text{ker}(g_*)$.

‘ \supset ’ Zij $\psi \in \text{Hom}(A, N)$ met $g_*\psi = 0$, dan moeten we een $\phi \in \text{Hom}(A, M)$ construeren met $f_*\phi = \psi$. Omdat $g_*\psi = 0$ geldt voor elke $a \in A$ dat $g\psi(a) = 0$, d.w.z. dat $\psi(a) \in \text{ker}(g)$ voor elke $a \in A$. Omdat de eerste rij exact is, geldt $\text{ker}(g) = \text{im}(f)$. Omdat f bovendien injectief is, geldt $f : M \xrightarrow{\cong} \text{im}(f)$, dus bestaat er een R -moduulisomorfisme:

$$M \xleftarrow{h} \text{im}(f) \quad (\subset N), \quad \text{en} \quad fh = \text{id}_{\text{im}(f)}.$$

Definieer nu $\phi := h \circ \psi : A \rightarrow M$, dus $\phi \in \text{Hom}(A, M)$. Omdat $\text{im}(\psi) \subset \text{im}(f)$, het domein van h , is de samenstelling $h \circ \psi$ goed gedefinieerd. Dan geldt voor alle $a \in A$:

$$(f_*\phi)(a) := f\phi(a) = fh\psi(a) = \psi(a), \quad \text{dus} \quad f_*\phi = \psi,$$

waarbij we gebruikten dat $\psi(a) \in \text{ker}(g) = \text{im}(f)$ en $fh = \text{id}_{\text{im}(h)}$. Hiermee is aangetoond dat $\text{ker}(g_*) \subset \text{im}(f_*)$.

We hebben nu de exactheid van de tweede rij bewezen en daarmee is ook de stelling bewezen. \square

13.4 Eigenschappen van projectieve modulen

13.4.1 In 13.3.3 hebben gezien dat $\text{Hom}(A, -)$ in het algemeen niet exact is, d.w.z. exacte rijtjes gaan niet altijd over in exacte rijtjes. In paragraaf 6.3 hebben we modulen M, N gezien die niet vrij zijn, maar waarvoor toch $M \oplus N$ een vrij moduul is (in voorbeeld 6.3.7 was zelfs $M = N$).

In deze paragraaf definiëren we het begrip ‘projectief moduul’ (definitie 13.4.2) en we bewijzen dat $\text{Hom}(P, -)$ exact is precies dan als P projectief is (zie stelling 13.4.6). Vervolgens bewijzen we dat P projectief is precies dan als een Q bestaat met $P \oplus Q = F$ met F een vrij moduul (zie stelling 13.4.7) (!). Overigens hebben projectieve modulen nog meer fraaie eigenschappen, maar daar kunnen hier helaas niet op in gaan.

Definitie 13.4.2 Een R moduul P heet **projectief** als voor elk surjectief R -moduulhomomorfisme $M \xrightarrow{f} N \rightarrow 0$ en voor elk R -moduulhomomorfisme $h : P \rightarrow N$:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \rightarrow 0 \\ & \nearrow_h & \\ & P & \end{array}$$

er een R -moduul homomorfisme $\tilde{h} : P \rightarrow M$ bestaat

$$\begin{array}{ccc} M & \xrightarrow{f} & N \rightarrow 0 \\ \tilde{h} \uparrow & \nearrow_h & \\ & P & \end{array} \quad \text{zodat} \quad f\tilde{h} = h.$$

We beginnen met drie lemma's, 13.4.3, 13.4.4 en 13.4.5, die in de bewijzen van de stellingen gebruikt zullen worden.

Lemma 13.4.3 *Zij F een vrij R -moduul. Dan is F een projectief R -moduul.*

Bewijs. Volgens de definitie van vrij moduul geldt:

$$F \cong \bigoplus_{i \in I} R.$$

Zij nu $M \xrightarrow{f} N \rightarrow 0$ en $h : F \rightarrow N$ gegeven, dan moeten we een \tilde{h} construeren. Zij

$$n_i := h(e_i), \quad \text{kies nu } m_i \in M \quad \text{met} \quad f(m_i) = n_i,$$

deze m_i bestaan omdat f surjectief is. Omdat h een R -moduulhomomorfisme is, geldt $h(\sum x_i e_i) = \sum x_i h(e_i) = \sum x_i n_i$.

Vervolgens definiëren we:

$$\tilde{h} : F \longrightarrow M, \quad \sum_{i \in I} x_i e_i \mapsto \sum_{i \in I} x_i m_i,$$

men rekent eenvoudig na dat \tilde{h} een R -moduulhomomorfisme is en dat inderdaad geldt: $f\tilde{h} = h$. Hiermee is het lemma bewezen. \square

Lemma 13.4.4 *Zij R een ring en laat M, N twee R -modulen zijn. Stel er zijn R -moduulhomomorfismen:*

$$M \xrightarrow{f} N, \quad \text{en} \quad M \xleftarrow{g} N \quad \text{z.d.d.} \quad f \circ g = id_N$$

merk op dat f surjectief moet zijn (men zegt dan wel dat g het rijtje $M \xrightarrow{f} N \rightarrow 0$ splijt). Dan geldt:

$$M \cong im(g) \oplus ker(f), \quad \text{en} \quad im(g) \cong N.$$

Bewijs. We bewijzen dat $im(g) \cap ker(f) = \{0\}$ en dat $im(g) + ker(f) = M$. Hieruit volgt direkt dat de afbeelding

$$im(g) \oplus ker(f) \longrightarrow M, \quad (a, b) \mapsto a + b$$

een isomorfisme van R -modulen is (ga na).

We bewijzen eerst $im(g) \cap ker(f) = \{0\}$. Zij $x \in im(g) \cap ker(f)$, dan:

$$\left. \begin{array}{l} \exists n \in N : g(n) = x \\ f(x) = 0 \end{array} \right\} \implies n = fg(n) = f(x) = 0,$$

en dus $x = g(n) = g(0) = 0$.

Zij nu $m \in M$, dan is:

$$gf(m) \in im(g) \quad \text{en} \quad m = gf(m) + (m - gf(m)),$$

bovendien geldt:

$$f(m - gf(m)) = f(m) - fgf(m) = f(m) - f(m) = 0$$

dus $m - gf(m) \in ker(f)$. Elke $m \in M$ is dus als som van een element $gf(m) \in im(g)$ en een element $m - gf(m) \in ker(f)$ te schrijven. Hiermee is het lemma bewezen. \square

Lemma 13.4.5 *Zij P een projectief R -moduul en zij*

$$M \xrightarrow{f} P \longrightarrow 0$$

een surjectief homomorfisme van R -modulen. Dan geldt:

$$M \cong P \oplus \ker(f).$$

Bewijs. We gebruiken de definitie van projectief R -moduul, met $N = P$ en $h = id_P : P \rightarrow P = N$ om een $\tilde{h} : P \rightarrow M$ te vinden:

$$\begin{array}{ccc} M & \xrightarrow{f} & P \longrightarrow 0 \\ \tilde{h} \uparrow & \nearrow_{\cong} & \\ P & & \end{array} \quad \text{en er geldt} \quad f\tilde{h} = h = id_P,$$

(de existentie van \tilde{h} volgt uit de het projectief zijn van P . In het bijzonder splijt \tilde{h} het exacte rijtje $N \xrightarrow{f} P \rightarrow 0$. Dit lemma volgt dan uit lemma 13.4.4. \square)

Stelling 13.4.6 *Zij P een projectief R -moduul dan is $\text{Hom}(P, -)$ rechtsexact: d.w.z. als*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

een exacte rij van R -modulen is, dan is

$$\text{Hom}(P, A) \xrightarrow{f_*} \text{Hom}(P, B) \xrightarrow{g_*} \text{Hom}(P, C) \longrightarrow 0$$

ook een exacte rij van R modulen.

Bovendien geldt: als een R -moduul A niet projectief is, dan is $\text{Hom}(A, -)$ niet rechtsexact.

Een R -moduul is dus projectief precies dan als $\text{Hom}(P, -)$ rechtsexact is.

Bewijs. Zij een exact rijtje en een projectief moduul P gegeven.

We bewijzen eerst dat g_* surjectief is, d.w.z. dat het tweede rijtje exact is in $\text{Hom}(P, C)$. Dit volgt onmiddellijk uit de definitie van projectief, zij immers $h \in \text{Hom}(P, C)$ gegeven. Dan is er een $\tilde{h} \in \text{Hom}(P, C)$ met $f\tilde{h} = h$. Hier staat precies dat $f_*\tilde{h} = h$, waarmee de surjectiviteit bewezen is.

Om de exactheid in $\text{Hom}(P, B)$ te bewijzen, moeten we laten zien dat $\text{im}(f_*) = \ker(g_*)$.

‘ \subset ’ Elk element in $\psi \in \text{im}(f_*)$ is te schrijven als $\psi = f_*\phi$ voor zekere $\phi \in \text{Hom}(P, A)$. Voor elke $x \in P$ geldt dan $\psi(x) = f\phi(x) \in \text{im}(f)$. Omdat de eerste rij exact is geldt $\text{im}(f) = \ker(g)$. Dan is $g\psi(x) = 0$ voor elke $x \in P$, dus $g_*\psi = 0$. Hiermee is aangetoond dat $\text{im}(f_*) \subset \ker(g_*)$.

‘ \supset ’ Zij $\psi \in \text{Hom}(P, B)$, met $g_*\psi = 0$. Dan moeten we een $\phi \in \text{Hom}(P, A)$ construeren met $f_*\phi = \psi$. De conditie $g_*\psi = 0$ is equivalent met:

$$\text{im}(\psi) \subset \ker(g) = \text{im}(f), \quad \text{en} \quad A \xrightarrow{f} \text{im}(f) \longrightarrow 0$$

is een exacte rij. We kunnen ψ dus zien als een R -moduulhomomorfisme $\psi : P \rightarrow \text{im}(f)$. De definitie van projectief (met $h := \psi$, en $M := A$, $N := \text{im}(f)$) impliceert dat er een $\phi : P \rightarrow A$ bestaat ($\phi := \tilde{h}$) met $f\phi = \psi$, dus er geldt $f_*\phi = \psi$. Hiermee is $\ker(g_*) \subset \text{im}(f_*)$ bewezen.

Tenslotte bewijzen we de laatste uitspraak. Als A niet projectief is, dan is er een exact rijtje R -modulen $M \xrightarrow{f} N \rightarrow 0$ en een $h \in \text{Hom}(A, M)$ zodat er géén $\tilde{h} \in \text{Hom}(A, N)$ bestaat met $f\tilde{h} = h$. Dat betekent dat $\text{Hom}(A, -)$, toegepast op de exacte rij:

$$\ker(f) \hookrightarrow M \xrightarrow{f} N \longrightarrow 0$$

een rijtje geeft met $f_* : \text{Hom}(A, M) \rightarrow \text{Hom}(A, N)$ *niet* surjectief. Dan is dus $\text{Hom}(A, -)$ niet rechts-exact. \square

Stelling 13.4.7 *Zij R een ring en zij P een R -moduul. Dan geldt:*

P is een projectief R -moduul dan en slechts dan als er is een R -moduul Q met $P \oplus Q = F$, met F een vrij R -moduul.

Bewijs. ‘ \Leftarrow ’ Stel $F = P \oplus Q$ met F een vrij R -moduul. Zij gegeven

$$\begin{array}{ccc} M & \xrightarrow{f} & N \rightarrow 0 \\ \uparrow \nearrow h & & \\ P & & \end{array} .$$

We moeten een \tilde{h} construeren met $f\tilde{h} = h$. Definieer eerst

$$g : F = P \oplus Q \longrightarrow N, \quad g(p, q) := h(p) \quad (p \in P, q \in Q).$$

Dan is $g|_P = h$. Omdat F projectief is, zie 13.4.3, is er een \tilde{g} met

$$\begin{array}{ccc} M & \xrightarrow{f} & N \rightarrow 0 \\ \tilde{g} \uparrow \nearrow g & & \text{zodat } f\tilde{g} = g. \\ P \oplus Q = F & & \end{array}$$

Definieer nu $\tilde{h} := \tilde{g}|_P$. Dan volgt $f\tilde{h} = h$ uit $f\tilde{g} = g$ door restrictie tot P .

‘ \Leftarrow ’ Zij P een projectief R -moduul. We construeren eerst een vrij R -moduul F door P als indexverzameling te nemen:

$$F := \bigoplus_{p \in P} R.$$

Definieer nu:

$$f : F \rightarrow P, \quad \sum_{p \in P} x_p e_p \mapsto \sum_{p \in P} x_p \cdot p.$$

Dan is f een R -moduulhomomorfisme en f is uiteraard surjectief want $f(e_p) = p$ bij constructie (!). Uit stelling 13.4.5 volgt dan dat $F = P \oplus \ker(f)$, dus voor Q kunnen we $\ker(f)$ nemen. Hiermee is stelling 13.4.7 bewezen. \square

13.5 Opgaven

1. Zij R een commutatieve (unitaire) ring en zij $f : M \rightarrow N$ een *niet* surjectief R -moduulhomomorfisme.

Bewijs dat $f_* : \text{Hom}(R, M) \rightarrow \text{Hom}(R, N)$ niet surjectief is.

2. Zij R een commutatieve ring en laat M, N, P, Q R -modulen zijn. Geef R -moduulisomorfismen:

$$\text{Hom}(M \oplus N, P) \cong \text{Hom}(M, P) \oplus \text{Hom}(N, P),$$

$$\text{Hom}(M, P \oplus Q) \cong \text{Hom}(M, P) \oplus \text{Hom}(M, Q).$$

3. Zij R een commutatieve ring en laat I, J idealen in R zijn met $I + J = R$.

Bewijs dat het R -moduul $\text{Hom}(R/I, R/J) = 0$.

Concludeer dat de $R = \mathbb{R}[X]$ -modulen $R/(X - a)$ en $R/(X - b)$ niet isomorf zijn als $a \neq b$.

4. Zij R een commutatieve ring en zij $I \subset R$ een ideaal.

Bewijs: R/I is een projectief R -moduul dan en slechts dan als er is een ideaal $J \subset R$ is met $R \cong R/I \times R/J$.

(Aanwijzing: stel g splijt de kanonieke afbeelding $R \rightarrow R/I$, bekijk $g(R/I) \subset R$.)

5. Bewijs dat het ideaal $I = (X, Y) \subset \mathbb{R}[X, Y]$ geen projectief R -moduul is. (Aanwijzing: stel ϕ splijt de surjectie

$$R \oplus R \rightarrow I, \quad (f, g) \mapsto fX + gY,$$

bekijk dan $\phi(XY) \in R \oplus R$.

6. Zij M een projectief moduul over de commutatieve ring R .

Bewijs dat $\text{Hom}(M, R)$ ook een projectief R -moduul is. (Men noemt dit R -moduul wel de duale van M).

14 Cyclotomische lichamen

14.1 De kwadratische reciprociteitswet

In deze paragraaf zijn $p, q \in \mathbb{Z}_{>0}$ steeds priemgetallen.

14.1.1 De kwadratische reciprociteitswet stelt ons in staat om snel te bepalen of het polynoom $X^2 - a$ een nulpunt in \mathbb{F}_p heeft. Om de reciprociteitswet te bewijzen gebruiken we eenheidswortels, waarmee we handig kunnen rekenen en die via Gauss-sommen in verband staan met nulpunten van de vergelijking $X^2 - a$.

Definitie 14.1.2 Laat p een oneven priemgetal zijn en zij $a \in \mathbb{Z}$.

Dan is het **Legendre-symbool** $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ gedefinieerd door:

$$\left(\frac{a}{p}\right) = 0 \Leftrightarrow a \text{ is deelbaar door } p,$$

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \exists x \in \mathbb{Z} : x \not\equiv 0 \pmod{p} \text{ en } x^2 \equiv a \pmod{p},$$

$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow \nexists x \in \mathbb{Z} : x^2 \equiv a \pmod{p}.$$

In het bijzonder geldt:

het polynoom $X^2 - a$ heeft een nulpunt in \mathbb{F}_p d.e.s.d.a. $\left(\frac{a}{p}\right) = +1$ of 0 .

Voorbeeld 14.1.3 In \mathbb{F}_{11} geldt:

$$(\pm 1)^2 = 1, \quad (\pm 2)^2 = 4, \quad (\pm 3)^2 = 9, \quad (\pm 4)^2 = 5, \quad (\pm 5)^2 = 3,$$

en met de definitie van het Legendre-symbool volgt dan:

$$\left(\frac{a}{11}\right) = 1 \quad \text{als } a \equiv 1, 3, 4, 5, 9 \pmod{11}.$$

De andere $10/2 = 5$ elementen van \mathbb{F}_{11}^* zijn geen kwadraat:

$$\left(\frac{a}{11}\right) = -1 \quad \text{als } a \equiv 2, 6, 7, 8, 10 \pmod{11}.$$

Stelling 14.1.4 Zij $a \in \mathbb{Z}$. Identificeren we $-1, 0, 1 \in \mathbb{Z}$ met $-\bar{1}, \bar{0}, \bar{1} \in \mathbb{F}_p$ dan geldt:

$$\left(\frac{a}{p}\right) = \bar{a}^{\frac{p-1}{2}} \quad (\in \mathbb{F}_p).$$

Verder geldt voor alle $n, m \in \mathbb{Z}$:

$$\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{m}{p}\right).$$

Bewijs. Als $\bar{a} = \bar{0} \in \mathbb{F}_p$, dan is $\left(\frac{a}{p}\right) = 0$ en $\bar{a}^{\frac{p-1}{2}} = \bar{0}$, zodat de eerste uitspraak dan juist is.

Als $\bar{a} \neq \bar{0}$ dan geldt $\bar{a}^{p-1} = 1$ omdat \mathbb{F}_p^* een groep met $p-1$ elementen is. Daarom is $\bar{a}^{\frac{p-1}{2}}$ een nulpunt van de vergelijking $X^2 - 1 = 0$ en dus $\bar{a}^{\frac{p-1}{2}} \in \{\bar{1}, -\bar{1}\}$, omdat dit enige nulpunten van $X^2 - 1$ in het lichaam \mathbb{F}_p zijn. Daarom kunnen we definiëren:

$$\epsilon : \mathbb{F}_p^* \longrightarrow \{\bar{1}, -\bar{1}\} \quad x \mapsto x^{\frac{p-1}{2}}.$$

Merk op dat ϵ een homomorfisme van (vermenigvuldigings)groepen is. Omdat \mathbb{F}_p^* een cyclische groep is, zie 9.4.2, is er een $y \in \mathbb{F}_p^*$ met $y^{\frac{p-1}{2}} \neq \bar{1}$. Dus is ϵ surjectief en i.h.b. geldt $\#ker(\epsilon) = \frac{p-1}{2}$.

Als $\bar{a} = x^2$ voor zekere $x \in \mathbb{F}_p$, $x \neq 0$, dan geldt $\bar{a}^{\frac{p-1}{2}} = x^{p-1} = 1$, dus $\bar{a} \in ker(\epsilon)$. Omdat $\bar{a}^2 = \bar{b}^2$ equivalent is met $\bar{a} = \pm\bar{b}$, vinden we zo $\frac{p-1}{2}$ elementen in $ker(\epsilon)$. Omdat $\#ker(\epsilon) = \frac{p-1}{2}$ geldt dus:

$$ker(\epsilon) = \{\bar{a} \in \mathbb{F}_p^* : \bar{a} = x^2 \text{ voor zekere } x \in \mathbb{F}_p^*\}.$$

Hieruit volgt dan dat $\epsilon(\bar{b}) = -\bar{1}$ als b niet een kwadraat modulo p is, dus:

$$\left(\frac{a}{p}\right) = \epsilon(\bar{a}),$$

voor alle $a \in \mathbb{Z}$ met $\bar{a} \neq \bar{0} \in \mathbb{F}_p$. Hiermee is de eerste bewering bewezen.

De tweede bewering is gemakkelijk te bewijzen als $\bar{n} = \bar{0}$ of $\bar{m} = \bar{0}$, beide zijden zijn dan immers 0. In de andere gevallen gebruiken we dat het Legendre-symbool met het homomorfisme ϵ overeenstemt, zoals we zojuist opmerkten. Hiermee is de stelling bewezen. \square

Voorbeeld 14.1.5 In \mathbb{F}_{11} geldt:

$$2^5 = 32 = -1, \quad 3^5 = 27 \cdot 9 = 5 \cdot 9 = 1, \quad 5^5 = 125 \cdot 25 = 4 \cdot 3 = 1,$$

waaruit volgt dat 2 géén kwadraat modulo 11 is, en dat 3 en 5 wél kwadraten modulo 11 zijn, zie ook het vorige voorbeeld.

Het is niet moeilijk om $(-1)^{\frac{p-1}{2}}$ te berekenen voor oneven priemgetallen p . (als $p = 2$, dan is $-1 = 1 = 1^2$ in \mathbb{F}_2). We kunnen p schrijven als $p = 4k+1$ of als $p = 4k+3$. Dan geldt:

$$(-1)^{\frac{p-1}{2}} = 1 \quad \text{als } p = 4k+1, \quad (-1)^{\frac{p-1}{2}} = -1 \quad \text{als } p = 4k+3.$$

De vergelijking $X^2 + 1$ heeft dus een oplossing in \mathbb{F}_p , met p oneven precies dan als $p \equiv 1 \pmod{4}$ (als $p = 2$, dan is $X^2 + 1 = (X+1)^2$ in \mathbb{F}_2 , dus 1 is een nulpunt).

14.1.6 Een element $\zeta \in K$, met K een lichaam, noemen we een **primitieve p -de eenheidswortel** als geldt:

$$\zeta^p = 1, \quad \zeta \neq 1.$$

De primitieve p -de eenheidswortels zijn dus nulpunten van $\Phi_p := (X^p - 1)/(X - 1) \in K[X]$. Omdat K i.h.b. een domein is, zijn er hoogstens $p - 1$ verschillende primitieve p -de eenheidswortels in K . Pas overigens op: het is zeker mogelijk dat 1 een nulpunt is van Φ_p ; bijvoorbeeld voor $K = \mathbb{F}_p$ is dit het geval.

Als $\text{kar}(K) \neq p$, dan is $(X^p - 1)' = pX^{p-1} \neq 0$, dus zijn alle nulpunten van $X^p - 1$ en van Φ_p onderling verschillend. In het bijzonder is dan ook *ieder* nulpunt van Φ_p een primitieve p -de eenheidswortel. Er is dan een eindige uitbreiding L van K met een primitieve p -de eenheidswortel $\zeta \in L$, neem bijvoorbeeld $L = \Omega_K^{X^p - 1}$.

Als $\text{kar}(K) = p$, dan is $X^p - 1 = (X - 1)^p$, dus zijn er geen primitieve p -de eenheidswortels in K en ook niet in een uitbreiding van K .

Voorbeeld 14.1.7 Als $\text{kar}(K) \neq 2$ dan is -1 de enige primitieve 2-de eenheidswortel.

Als $K = \mathbb{C}$ dan zijn de primitieve p -de eenheidswortels precies de $p - 1$ (verschillende) complexe getallen:

$$\zeta_p^k \quad (1 \leq k \leq p - 1), \quad \text{met} \quad \zeta_p := \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}.$$

I.h.b. zijn $\frac{-1 \pm i\sqrt{3}}{2}$ de twee primitieve 3-de eenheidswortels.

Voorbeeld 14.1.8 De primitieve 3-de eenheidswortels in \mathbb{F}_7 zijn 2 en 4 want $2^3 = 8 = 1$, $4^3 = 64 = 1$.

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 , zie bijvoorbeeld opgave 19 in het hoofdstuk over eindige lichamen. Ieder element van \mathbb{F}_{25} is dan te schrijven als $a + b\alpha$ met $a, b \in \mathbb{F}_5$ en $\alpha^2 = 2$. De primitieve 3-de eenheidswortels zijn dan $3(-1 \pm \alpha)$, immers:

$$(3(-1 + \alpha))^3 = 2(-1 + 3\alpha - 3\alpha^2 + \alpha^3) = 2(-1 + 3\alpha - 1 + 2\alpha) = 1,$$

en analoog voor $3(-1 - \alpha)$.

14.1.9 We zullen primitieve p -de eenheidswortels later nog uitvoeriger onderzoeken. We geven nu een verband tussen eenheidswortels en oplossingen van kwadratische vergelijkingen door de Gauss-som in te voeren. Omdat het rekenen met eenheidswortels betrekkelijk eenvoudig is, verkrijgen we zo informatie over kwadratische vergelijkingen.

Definitie 14.1.10 Zij K een lichaam met $\text{kar}(K) \neq p$ en zij $\zeta \in K$ een primitieve p -de eenheidswortel. Voor $x \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ definiëren we:

$$\zeta^x := \zeta^n, \quad \left(\frac{x}{p}\right) := \left(\frac{n}{p}\right) \quad \text{als } x = n + p\mathbb{Z}, \quad n \in \mathbb{Z}.$$

(Dit hangt niet van de keuze van $n \in \mathbb{Z}$ met $\bar{n} = x$ af want $\zeta^p = 1$ en $\left(\frac{n}{p}\right)$ hangt alleen van $n \bmod p$ af.)

De **Gauss-som** $\tau \in K$ is gedefinieerd door:

$$\tau := \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \cdot \zeta^x.$$

(De Gauss-som hangt af van de keuze van ζ , maar dat is voor onze toepassing niet van belang.)

Voorbeeld 14.1.11 We nemen $p = 3$. Als $K = \mathbb{C}$ en $\zeta = \frac{-1+i\sqrt{3}}{2}$, dan is

$$\tau = \left(\frac{0}{3}\right) \cdot \zeta^0 + \left(\frac{1}{3}\right) \cdot \zeta^1 + \left(\frac{2}{3}\right) \cdot \zeta^2 = 0 + \zeta - \zeta^2 = i\sqrt{3}.$$

Als $K = \mathbb{F}_7$ en $\zeta = 2$ dan is:

$$\tau = \left(\frac{0}{3}\right) \cdot 2^0 + \left(\frac{1}{3}\right) \cdot 2^1 + \left(\frac{2}{3}\right) \cdot 2^2 = 2 - 4 = 5.$$

Merk op dat geldt: $\tau^2 = 5^2 = -3$ in \mathbb{F}_7 , analoog aan het geval $K = \mathbb{C}$, en dat $\left(\frac{-1}{3}\right) = -1$.

Stelling 14.1.12 Zij K een lichaam met $\text{kar}(K) \neq p$ en zij $\zeta \in K$ een primitieve p -de eenheidswortel. Dan geldt:

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

Bewijs. Er geldt

$$\begin{aligned} \tau^2 &= \left(\sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \cdot \zeta^x \right) \cdot \left(\sum_{y \in \mathbb{F}_p} \left(\frac{y}{p}\right) \cdot \zeta^y \right) \\ &= \sum_{x, y \in \mathbb{F}_p} \left(\frac{xy}{p}\right) \cdot \zeta^{x+y} \\ &= \sum_{z \in \mathbb{F}_p} \left(\sum_{x \in \mathbb{F}_p} \left(\frac{x(z-x)}{p}\right) \right) \cdot \zeta^z \quad (\text{met } z = x + y). \end{aligned}$$

Voor $x = 0$ geldt $\left(\frac{x(z-x)}{p}\right) = 0$, voor $x \neq 0$ geldt:

$$\begin{aligned}\left(\frac{x(z-x)}{p}\right) &= \left(\frac{-x^2}{p}\right) \cdot \left(\frac{1-zx^{-1}}{p}\right) \\ &= \left(\frac{-1}{p}\right) \left(\frac{x^2}{p}\right) \cdot \left(\frac{1-zx^{-1}}{p}\right) \\ &= \left(\frac{-1}{p}\right) \cdot \left(\frac{1-zx^{-1}}{p}\right),\end{aligned}$$

dus we vinden:

$$\tau^2 = \left(\frac{-1}{p}\right) \cdot \sum_{z \in \mathbb{F}_p} c_z \zeta^z \quad \text{met} \quad c_z = \sum_{x \in \mathbb{F}_p^*} \left(\frac{1-zx^{-1}}{p}\right).$$

Als $z = 0$ dan vinden we:

$$c_0 = \sum_{x \in \mathbb{F}_p^*} \left(\frac{1}{p}\right) = \sum_{x \in \mathbb{F}_p^*} 1 = p - 1.$$

Als $z \neq 0$, en x doorloopt \mathbb{F}_p^* , dan doorloopt zx^{-1} ook \mathbb{F}_p^* , en $w := 1 - zx^{-1}$ doorloopt $\mathbb{F}_p - \{1\}$, dus:

$$c_z = \left(\sum_{w \in \mathbb{F}_p} \left(\frac{w}{p}\right)\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1 \quad (\text{met } z \in \mathbb{F}_p^*),$$

want er zijn in \mathbb{F}_p evenveel elementen w met $\left(\frac{w}{p}\right) = 1$ als met $\left(\frac{w}{p}\right) = -1$. Al met al vinden we:

$$\begin{aligned}\tau^2 &= \left(\frac{-1}{p}\right) \cdot \left(p - 1 + \sum_{z \in \mathbb{F}_p^*} (-1) \zeta^z\right) \\ &= \left(\frac{-1}{p}\right) \cdot \left(p - 1 - \sum_{z \in \mathbb{F}_p^*} \zeta^z\right) \\ &= \left(\frac{-1}{p}\right) \cdot \left(p - \sum_{z=0}^{p-1} \zeta^z\right) \\ &= \left(\frac{-1}{p}\right) \cdot p,\end{aligned}$$

waarbij we gebruikten dat:

$$\sum_{z=0}^{p-1} \zeta^z = \frac{\zeta^p - 1}{\zeta - 1} = 0.$$

Hiermee is stelling 14.1.12 bewezen. □

14.1.13 Deze stelling geeft ons dus een nulpunt $\tau \in K$, als $\text{kar}(K) \neq p$, van het polynoom $X^2 - \left(\frac{-1}{p}\right)p$. Voor K kunnen we bijvoorbeeld het lichaam $\Omega_{\mathbb{F}_q}^{X^{p-1}}$ nemen, met $p \neq q$. We willen dan nog wel weten of het nulpunt τ in het lichaam \mathbb{F}_q zit.

Lemma 14.1.14 *Stel $\text{kar}(K) = q$ en q is een oneven priemgetal met $q \neq p$. Dan geldt:*

$$\tau^q = \left(\frac{q}{p}\right) \cdot \tau, \quad \text{i.h.b. :} \quad \tau \in \mathbb{F}_q \iff \left(\frac{q}{p}\right) = 1.$$

Bewijs. Uit de definitie van Gauss-som en uit het feit dat $x \mapsto x^q$ een lichaamshomomorfisme van K is volgt:

$$\begin{aligned} \tau^q &= \left(\sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \cdot \zeta^x \right)^q \\ &= \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right)^q \cdot \zeta^{qx} \\ &= \sum_{y \in \mathbb{F}_p} \left(\frac{yq^{-1}}{p}\right)^q \cdot \zeta^y \quad (\text{met } y = x\bar{q} \in \mathbb{F}_p) \\ &= \left(\frac{q^{-1}}{p}\right) \cdot \sum_{y \in \mathbb{F}_p} \left(\frac{y}{p}\right) \cdot \zeta^y \\ &= \left(\frac{q}{p}\right) \cdot \tau, \end{aligned}$$

immers als $\bar{q} = x^2$ dan is $\bar{q}^{-1} = (x^{-1})^2$.

Tenslotte merken we nog op: als $x \in K$ dan geldt: $x \in \mathbb{F}_q$ precies dan als $x^q = x$. Hiermee is de stelling bewezen. \square

Stelling 14.1.15 (*kwadratische reciprociteitswet*) (Gauss, 1801).

Als p en q verschillende oneven priemgetallen zijn, dan geldt:

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right) && \text{als } p \equiv 1 \pmod{4} \text{ of } q \equiv 1 \pmod{4}, \\ \left(\frac{q}{p}\right) &= -\left(\frac{p}{q}\right) && \text{als } p \equiv q \equiv 3 \pmod{4}. \end{aligned}$$

Anders geformuleerd:

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

Verder geldt:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Bewijs. Om te beginnen merken we op dat $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ direkt volgt uit stelling 14.1.4.

We bewijzen nu de kwadratische reciprociteitswet. Zij $K = \Omega_{\mathbb{F}_q}^{X^{p-1}}$ en zij τ de Gauss-som als boven. Volgens 14.1.14 geldt:

$$\tau^{q-1} = \left(\frac{q}{p}\right).$$

Anderzijds vinden we, door 14.1.12 te gebruiken,

$$\tau^{q-1} = (\tau^2)^{\frac{q-1}{2}} = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} p^{\frac{q-1}{2}}.$$

Uit stelling 14.1.4 volgt:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) \quad (\in \mathbb{F}_q).$$

Invullen geeft dan:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right),$$

hetgeen op evidente wijze equivalent is met de kwadratische reciprociteitswet.

Tenslotte bewijzen we nog:

$$(\exists x \in \mathbb{F}_p : x^2 = 2) \iff p \equiv \pm 1 \pmod{8}.$$

Zij p een oneven priemgetal, dan heeft de vergelijking $X^4 + 1$ een nulpunt ζ in een eindige uitbreiding K van \mathbb{F}_p . Dan is $\zeta^4 = -1$ en $\zeta^8 = 1$. Zij $x := \zeta + \zeta^7 \in K$, dan geldt

$$x^2 = (\zeta + \zeta^7)^2 = \zeta^2 + \zeta^6 + 2 = 2,$$

immers $\zeta^6 = \zeta^4 \zeta^2 = -\zeta^2$.

Als $p = 8k + 1$ of $p = 8k + 7$ dan zien we:

$$\left. \begin{array}{l} \zeta^p = \zeta, \quad \zeta^{7p} = \zeta^7 \quad \text{als } p \equiv 1 \pmod{8} \\ \zeta^p = \zeta^7, \quad \zeta^{7p} = \zeta \quad \text{als } p \equiv 7 \pmod{8} \end{array} \right\} \implies x^p = (\zeta + \zeta^7)^p = \zeta + \zeta^7 = x,$$

immers $x \mapsto x^p$ is een lichaamshomomorfisme. Omdat $x^p = x$ geldt $x \in \mathbb{F}_p$. Voor $p \equiv \pm 1 \pmod{8}$ is er dus een $x \in \mathbb{F}_p$ met $x^2 = 2$ en daarom is $\left(\frac{2}{p}\right) = 1$.

Als $p = 8k + 3$ of $p = 8k + 5$ dan geldt (gebruik $\zeta^4 = -1$):

$$\left. \begin{array}{ll} \zeta^p = \zeta^3 = -\zeta^7 & \text{als } p \equiv 3 \pmod{8} \\ \zeta^p = \zeta^5 = -\zeta & \text{als } p \equiv 5 \pmod{8} \end{array} \right\} \implies x^p = (\zeta + \zeta^7)^p = -(\zeta + \zeta^7) = -x,$$

dus het nulpunt x van de vergelijking $X^2 - 2$ ligt niet in \mathbb{F}_p . Het andere nulpunt, $-x$, ligt dan ook niet in \mathbb{F}_p dus $\left(\frac{2}{p}\right) = -1$.

Hiermee is stelling 14.1.15 bewezen. \square

Voorbeeld 14.1.16 We geven enige eenvoudige voorbeelden van stelling 14.1.15.

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1,$$

want $4 = 2^2$, dus 7 is geen kwadraat modulo 11. Verder geldt:

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

dus 5 is wel een kwadraat modulo 11, er geldt inderdaad $4^2 = 16 = 5$ in \mathbb{F}_{11} . Door te gebruiken dat het Legendre-symbool multiplicatief is (zie 14.1.4), vinden we:

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right) = (-1)^{\frac{11^2-1}{8}} \cdot -\left(\frac{11}{3}\right) = (-1) \cdot -\left(\frac{2}{3}\right) = -1.$$

14.2 De p -de eenheidswortels over \mathbb{Q}

Zij K een lichaam. Merk op dat in $K[X]$ geldt:

$$\Phi_p = (X^p - 1)/(X - 1), \quad \text{met } \Phi_p := X^{p-1} + X^{p-2} + \dots + X + 1 \in K[X].$$

De primitieve p -de eenheidswortels zijn dus de nulpunten van het polynoom Φ_p . We bestuderen nu de situatie als $K = \mathbb{Q}$.

Stelling 14.2.1 In $\mathbb{Q}[X]$ is het polynoom Φ_p irreducibel. Zij

$$\mathbb{Q}[\zeta] := \mathbb{Q}[X]/(\Phi_p), \quad \zeta := X + (\Phi_p).$$

Dan is $\mathbb{Q}[\zeta] = \mathbb{Q}(\zeta)$ een lichaam met $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ en er geldt:

$$\Phi_p = (X - \zeta)(X - \zeta^2) \dots (X - \zeta^{p-1}) \in \mathbb{Q}[X].$$

In het bijzonder is $\mathbb{Q}(\zeta)$ een splijtlichaam van Φ_p .

Bewijs. Merk op dat $\Phi_p(X)$ irreducibel is precies dan als $\Phi_p(X+1)$ irreducibel is (substitueer $X := X \pm 1$ in een ontbinding). Uit $\Phi_p(X) = (X^p - 1)/(X - 1)$ volgt dat:

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1}X^{p-2} + \dots + \binom{p}{p-2}X + \binom{p}{p-1}.$$

Omdat $\binom{p}{i}$ deelbaar is door p voor $1 \leq i \leq p-1$ en omdat $\binom{p}{p-1} = \binom{p}{1} = p$ is $\Phi_p(X+1)$ een Eisensteinpolynoom (zie 5.5.3) bij p en is dus irreducibel.

Zoals bekend is $\mathbb{Q}(\zeta)$ dan een lichaam en $[\mathbb{Q}(\zeta) : \mathbb{Q}] = gr(\Phi_p) = p-1$.

Als $\zeta^p = 1$ en $\zeta \neq 1$, dan geldt ook $(\zeta^k)^p = (\zeta^p)^k = 1$. Als $1 \leq k \leq p-1$ dan is $\zeta^k \neq 1$, anders was immers ζ een nulpunt van $(X^k - 1)/(X - 1) \in \mathbb{Q}[X]$, maar dit polynoom heeft lagere graad dan het irreducibele polynoom Φ_p en dat kan dus niet. Verder is ook $\zeta^k \neq \zeta^l$ als $1 \leq k < l \leq p-1$ anders was nl. $\zeta^{l-k} = 1$. We vinden zo dus $p-1 = gr(\Phi_p)$ verschillende nulpunten van het polynoom Φ_p in $\mathbb{Q}(\zeta)$ en daaruit volgt de ontbinding. \square

14.2.2 Met de stelling 8.1.1 kunnen we op eenvoudige wijze $Aut(\mathbb{Q}(\zeta))$ bepalen. Merk op dat iedere $x \in \mathbb{Q}(\zeta)$ op unieke wijze te schrijven is als:

$$x = a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{p-2}\zeta^{p-2}, \quad \text{i.h.b. : } \zeta^{p-1} = -1 - \zeta - \zeta^2 - \dots - \zeta^{p-2}.$$

Voor iedere $k \in \mathbb{Z}_{>0}$ definiëren we een afbeelding:

$$\phi_k : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$$

door

$$a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{p-2}\zeta^{p-2} \mapsto a_0 + a_1\zeta^k + a_2\zeta^{2k} + \dots + a_{p-2}\zeta^{(p-2)k}.$$

Omdat $\zeta^p = 1$ geldt:

$$\phi_k = \phi_l \quad \text{als} \quad \bar{k} = \bar{l} \in \mathbb{Z}/p\mathbb{Z},$$

dan is immers $l = k + np$ voor zekere $n \in \mathbb{Z}$.

Stelling 14.2.3 *Zij ζ een primitieve p -de eenheidswortel.*

Dan geldt $\sharp Aut(\mathbb{Q}(\zeta)) = p-1$ en er is een isomorfisme van groepen:

$$\phi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow Aut(\mathbb{Q}(\zeta)), \quad \bar{k} \mapsto \phi_k.$$

In het bijzonder is $Aut(\mathbb{Q}(\zeta))$ een cyclische groep van orde $p-1$.

Bewijs. Uit stelling 8.1.1 volgt meteen dat $\sharp Aut(\mathbb{Q}(\zeta)) = p - 1$ want het minimumpolynoom Φ_p van ζ over \mathbb{Q} heeft precies $p - 1$ nulpunten in $\mathbb{Q}(\zeta)$.

Uit het bewijs van die stelling blijkt dat de nulpunten van Φ_p corresponderen met automorfismen: bij ieder nulpunt β van Φ_p is er een uniek automorfisme ϕ met $\phi(\zeta) = \beta$. Daar $\beta = \zeta^k$, voor zekere k met $1 \leq k \leq p-1$, is er voor elk van deze k 's dus een automorfisme ϕ met

$$\phi(\zeta^i) = \phi(\zeta)^i = (\zeta^k)^i = \zeta^{ki}.$$

Omdat $\phi(a) = a$ voor $a \in \mathbb{Q}$, het priemlichaam, geldt dan:

$$\begin{aligned} \phi(a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{p-2}\zeta^{p-2}) &= \\ &= a_0 + a_1\phi(\zeta) + a_2\phi(\zeta)^2 + \dots + a_{p-2}\phi(\zeta)^{p-2} \\ &= a_0 + a_1\zeta^k + a_2\zeta^{2k} + \dots + a_{p-2}\zeta^{(p-2)k} \\ &= \phi_k(a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{p-2}\zeta^{p-2}). \end{aligned}$$

Het automorfisme ϕ is dus volledig bepaald door $\phi(\zeta) = \zeta^k$ en er geldt $\phi = \phi_k$.

Ieder element van $(\mathbb{Z}/p\mathbb{Z})^*$ is op unieke wijze te schrijven als \bar{k} met $1 \leq k \leq p-1$ zodat we al een bijectieve afbeelding $(\mathbb{Z}/p\mathbb{Z})^* \rightarrow Aut(\mathbb{Q}(\zeta))$, $\bar{k} \mapsto \phi_k$ gevonden hebben. We moeten alleen nog bewijzen dat deze afbeelding een homomorfisme is, d.w.z. dat $\phi_k\phi_l = \phi_{kl}$. Dit volgt uit:

$$\phi_k(\phi_l(\zeta)) = \phi_k(\zeta^l) = \zeta^{kl},$$

dus het automorfisme $\phi_k\phi_l$ stuurt ζ naar ζ^{kl} en moet dus hetzelfde zijn als ϕ_{kl} .

Tenslotte merken we op dat volgens stelling 9.4.2 de vermenigvuldigingsgroep $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ cyclisch is. \square

14.3 Opgaven

1. Bewijs dat geldt:

3 is een kwadraat modulo p d.e.s.d.a. $p \equiv 1, -1 \pmod{12}$.

2. Bewijs dat -3 een kwadraat is in \mathbb{F}_p precies dan als $p \equiv 1 \pmod{3}$.

3. Zij $p > 3$ een priemgetal dat $n^2 - 2$ deelt, ($n \in \mathbb{Z}$). Bewijs dat $p \equiv \pm 1 \pmod{8}$.

4. Bepaal de volgende Legendre-symbolen:

$$\left(\frac{5}{101}\right), \quad \left(\frac{6}{101}\right), \quad \left(\frac{7}{101}\right), \quad \left(\frac{11}{101}\right).$$

5. In deze opgave is K steeds een deellichaam van $\mathbb{Q}(\zeta)$, met ζ een primitieve p -de eenheids wortel en met $[K : \mathbb{Q}] = 2$.

We bewijzen dat er precies één zo'n deellichaam is.

a. Bewijs dat $K(\zeta) = \mathbb{Q}(\zeta)$ en dat:

$$gr(f_K^\zeta) = [K(\zeta) : K] = \frac{p-1}{2}.$$

b. Bewijs dat:

$$\#Aut_K(\mathbb{Q}(\zeta)) = \frac{p-1}{2}.$$

c. Bewijs dat een cyclische groep van orde $p-1 \in 2\mathbb{Z}$ (zoals bv. $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta))$) precies één ondergroep van orde $(p-1)/2$ heeft.

d. Zij $H \subset Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta))$ de unieke ondergroep van orde $(p-1)/2$. Laat zien dat:

$$H = \{x^2 : x \in (\mathbb{Z}/p\mathbb{Z})^*\} \subset Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = (\mathbb{Z}/p\mathbb{Z})^*.$$

e. Definieer een deellichaam van $\mathbb{Q}(\zeta)$ door:

$$\mathbb{Q}(\zeta)^H := \{\alpha \in \mathbb{Q}(\zeta) : h(\alpha) = \alpha \ \forall h \in H\}.$$

Zij $\tau \in \mathbb{Q}(\zeta)$ de Gauss-som. Bewijs:

$$\mathbb{Q}(\zeta)^H = \mathbb{Q}(\tau).$$

f. Merk op dat $H = Aut_{\mathbb{Q}(\tau)}(\mathbb{Q}(\zeta))$. Concludeer dat $K = \mathbb{Q}(\tau)$.

Index

A

- afbeelding natuurlijk 33
- afgeleide 65
- algebraïsch 135, 138
- algoritme Euclidisch 204
- automorfisme K - 150
- ring 26

B

- beeld 27

C

- chinese reststelling 41
- commutatief 4

D

- deellichaam 133
- deelmoduul 111
- deelring 7
- delingsring 4
- domein hoofdideaal- 90
- ontbindings- 93
- 13

E

- eenheid 9
- eenheidswortels 136
- eindig 138
- Eisenstein kenmerk van 103
- Eisensteinpolynoom 103
- Euclidisch algoritme 204
- Euclidische ring 200
- evaluatiehomomorfisme 54

F

- factorontbindingsdomein 93
- factorring 31
- Frobenius-homomorfisme 149

G

- graad 51, 53, 138

H

- homomorfisme evaluatie 54
- K - 150
- lichaams- 26
- R -moduul 112
- ring- 26
- hoofdideaal 37
- hoofdideaaldomein 90
- hoofdideaalring 37

I

- ideaal hoofd- 37
- maximaal 76
- priem 73
- product 39
- som 39
- voortbrengers 29
- 27
- irreducibel 88
- isomorfisme K - 150
- R -moduul- 112
- ring- 26

K

- karakteristiek 134
- kern 27

L

- lemma van Zorn 79
- lichaam deel- 133
- homomorfisme 149
- ontbindings- 154
- priem- 133
- quotiënten- 14
- scheef- 4
- slijt- 154
- uitbreidings- 134
- 5
- lichaamshomomorfisme 26, 149

M

maximaal ideaal 76
minimumpolynoom 63, 134
moduul deel- 111
— projectief 219
— vrij 114
— 110
moduulhomomorfisme 112
monisch 51

N

natuurlijke afbeelding 33
nilpotent 11
nuldeler 11

O

ontbindingsdomein 93
ontbindingslichaam 154

P

polynoom Eisenstein 103
— minimum- 63, 134
— symmetrisch 185
— 51
polynoomring 52
priemideaal 73
priemlichaam 133
priemontbinding 93
product van idealen 39
— van ringen 13
projectief moduul 219

Q

quaternionen 5
quotiëntenlichaam 14

R

rechtsexact 221
ring automorfisme 26
— commutatief 4
— deel- 7
— delings- 4
— endomorfismen- 16
— Euclidische 200

— factor- 31
— groepen- 18
— homomorfisme 26
— hoofdideaal 37
— isomorfisme 26
— polynoom- 52
— product van 13
— 4

S

scheeffichaam 4
som van idealen 39
splitslichaam 154
symmetrisch polynoom 185

T

transcendent 135

U

uitbreiding enkelvoudig 135
— 134

V

veelterm 51

W

Weylgebra 17

Z

Zorn, lemma van 79