Syllabus Algebra IIa

voorlopige versie

Prof. Dr G. van der Geer

Faculteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam

Versie: 2002

1. Ringen

Ich denke mir den Leser wie einen Reisenden, die Hilfssätze sind Haltestellen, die Sätze sind grössere Stationen, im voraus bezeichnet, damit an Ihnen das Auffassungvermögen ausruhen kann.
Hilbert*, Zahlbericht, 1897

De verzameling van de gehele getallen $\mathbb{Z}$ laat twee bewerkingen toe, de optelling en de vermenigvuldiging en vormt een voorbeeld van een *ring*. Ook de verzameling $\mathbb{R}$ van de reële getallen bezit twee bewerkingen en het is gemakkelijk vele andere voorbeelden te geven die allemaal aan bepaalde axioma's voldoen. We formalizeren dit nu in de volgende definitie, die van Hilbert stamt.

(1.1) Definitie. Een *ring* is een verzameling R voorzien van twee bewerkingen, d.w.z. afbeeldingen $R \times R \to R$, de *optelling* '$+$' en de *vermenigvuldiging* '$\cdot$' , en voorzien van een element $0 \in R$, de *nul*, zodat aan de volgende axioma's is voldaan:

(R1) (*Additieve groep*) De verzameling R is een abelse groep met betrekking tot de optelling en het element 0;

(R2) (*Associativiteit*) Voor alle $x, y, z \in R$ geldt

$$(x \cdot y) \cdot z = x \cdot (y \cdot z);$$

(R3) (*Distributiviteit*) Voor alle $x, y, z \in R$ geldt

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

Voorbeelden zijn gemakkelijk te vinden: de gehele getallen $\mathbb{Z}$, de rationale getallen $\mathbb{Q}$, de reële getallen $\mathbb{R}$ en de complexe getallen $\mathbb{C}$ met de gebruikelijke optelling en vermenigvuldiging leveren voorbeelden van ringen. In deze gevallen is ook voldaan aan het volgende axioma:

(R4) (*Eenheidselement*) Er is een element $1 \in R$ met de eigenschap $1 \cdot x = x \cdot 1 = x$ voor alle $x \in R$.

Ringen die aan R4 voldoen heten *ringen met* 1 of ook wel *ringen met eenheidselement*. Wanneer voldaan is aan het axioma

(R5) (*Commutativiteit*) Voor alle $x, y \in R$ geldt $x \cdot y = y \cdot x$.

dan noemen we de ring *commutatief*.

(1.2) Definitie. Een *delingsring* is een ring met eenheidselement met $1 \neq 0$ waarin er voor ieder element $x \in R$ met $x \neq 0$ een element x^* bestaat zodat $x \cdot x^* = x^* \cdot x = 1$. Een *lichaam* is een commutatieve delingsring.

(1.3) Voorbeelden. De verzamelingen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ en de quaternionen $\mathbb{H}$ zijn voorbeelden van ringen met eenheidselement. Hiervan zijn $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ commutatief. De

* D. Hilbert, 1862-1943, was de belangrijkste Duitse wiskundige uit het begin van de twintigste eeuw. Hij maakte van Göttingen het centrum van de wiskunde en dat bleef het tot de nazi-tijd.

ringen $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ en $\mathbb{H}$ zijn delingsringen, terwijl $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ ook lichamen zijn. Ga dit zelf na.

(1.4) Voorbeeld. De triviale groep $R = \{0\}$ met als vermenigvuldiging $0 \cdot 0 = 0$ is een voorbeeld van een ring. Het is een ring met eenheidselement $1 = 0$. Deze ring heet wel de triviale ring.

In de praktijk zullen we in plaats van de notatie $x \cdot y$ voor het gemak vaak xy schrijven. Wegens de associativiteit mogen we xyz schrijven in plaats van $(xy)z$.

(1.5) Voorbeeld. (*De ring van gehele getallen van Gauss*) Laat $\mathbb{Z}[i]$ de volgende deelverzameling van de complexe getallen $\mathbb{C}$ zijn:

$$\mathbb{Z}[i] = \{a + b\,i \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

voorzien van de bewerkingen $+$ en $\cdot$ van $\mathbb{C}$. Dit is ook een voorbeeld van een commutatieve ring met eenheidselement.

(1.6) Voorbeeld. Laat n een geheel getal zijn en $\mathbb{Z}/n\mathbb{Z}$ de groep van de restklassen modulo n. Op de groep $\mathbb{Z}/n\mathbb{Z}$ kunnen we een vermenigvuldiging definiëren via

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

zoals we in Syllabus Algebra I, (3.10) gedaan hebben. Met deze vermenigvuldiging is aan alle axioma's voor een commutatieve ring met eenheidselement voldaan. Ga dit na.

(1.7) Voorbeeld. (*Polynoomringen of veeltermringen*) Laat R een ring zijn. De verzameling $R[X]$ bestaat per definitie uit de uitdrukkingen

$$a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

waarbij $n \in \mathbb{Z}_{\geq 0}$ en $a_0, a_1, \ldots, a_n \in R$. We schrijven ook wel

$$\sum_{i=0}^{n} a_i X^i$$

of ook wel

$$\sum_{i=0}^{\infty} a_i X^i,$$

waarbij alle $a_i \in R$ en slechts eindig veel a_i ongelijk 0 zijn. Zulke uitdrukkingen heten veeltermen of polynomen. We definiëren nu een optelling $+$ via

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

en een vermenigvuldiging $\cdot$ via

$$(\sum_{i=0}^{\infty} a_i X^i) \cdot (\sum_{i=0}^{\infty} b_i X^i) = \sum_{i=0}^{\infty} c_i X^i$$

met c_i bepaald door

$$c_i = \sum_{j,k\,:\,j+k=i} a_j b_k \tag{1}$$

Hierbij worden de optelling en vermenigvuldiging in R gebruikt. Het nulelement is de veelterm $0 = \sum_{i=0}^{\infty} 0X^i$. Met deze bewerkingen wordt $R[X]$ een ring, zoals direct is na te gaan. De regel voor de vermenigvuldiging volgt uit de distributiviteit en de regel

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

Met andere woorden, de vermenigvuldiging is de gebruikelijke vermenigvuldiging van veeltermen. Als voorbeeld geldt de identiteit

$$X^n - 1 = (-1 + X)(1 + X + X^2 + \ldots + X^{n-1})$$

in $\mathbb{Z}[X]$, de identiteit

$$1 + X^2 = (i + X)(-i + X)$$

in $\mathbb{C}[X]$ en de identiteit

$$1 + 3X^2 + X^4 = (1 + 2X + X^2)(1 + 3X + X^2)$$

in $\mathbb{Z}/5\mathbb{Z}[X]$. Ga dit na.

De variable X speelt alleen een boekhoudkundige rol. We kunnen in plaats van uitdrukkingen $\sum_{i=0}^{\infty} a_i X^i$ ook oneindige rijtjes $(a_0, a_1, \ldots)$ met $a_i \in R$ en nul voor bijna alle i beschouwen en de optelling coördinaatsgewijs en de vermenigvuldiging via (1) definiëren.

We voeren nog wat terminologie in. Als $f = \sum_{i=0}^{\infty} a_i X^i$ een polynoom of veelterm is in $R[X]$ dan heten de elementen a_i de coëfficiënten van f. Als $a_n \neq 0$ en $a_m = 0$ voor alle $m > n$ dan heet n de *graad* van f en wordt wel geschreven $\deg(f)$ ('degree') en a_n heet de *kopcoëfficiënt* van f.

We kunnen ook veeltermringen in meer variabelen invoeren door met inductie te definiëren:

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

Een element $f \in R[X_1, \ldots, X_n]$ laat zich schrijven als

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

waarbij slechts eindig veel coëfficiënten ongelijk 0 zijn. We schrijven ook wel

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

waarbij $I = (i_1, \ldots, i_n)$ en X^I staat voor $X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$.

(1.8) Definitie. Laat R een ring met eenheidselement zijn. Een element x waarvoor er een x^* in R bestaat met $x \cdot x^* = x^* \cdot x = 1$ heet een *eenheid* van R. Het element x^* is het enige element van R met $x \cdot x^* = x^* \cdot x = 1$ (zie Opgave 3) en heet de *inverse* van

x en wordt geschreven als x^{-1}. We schrijven R^* voor de verzameling van eenheden van R.

(1.9) Propositie. *Laat R een ring met eenheidselement zijn. Dan vormen de eenheden een groep R^* met betrekking tot de vermenigvuldiging en* 1.

Bewijs. Uit R2 volgt het axioma G1 van de associativiteit. Het element 1 is het eenheidselement van R^* en met $x \in R^*$ zit ook x^{-1} in R^*. We moeten nog laten zien dat als $x, y \in R^*$ dan ook $xy \in R^*$. Maar er geldt

$$(xy)(y^{-1}x^{-1}) = 1 = (y^{-1}x^{-1})(xy)$$

dus $xy \in R^*$. We zien dus dat R^* met de vermenigvuldiging een groep is.

(1.10) Voorbeelden. De groep $\mathbb{Z}^*$ is gelijk aan $\{1, -1\}$. Verder geldt

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

(zie Opgave 4). Verder weten we al wat $(\mathbb{Z}/n\mathbb{Z})^*$ is: een element $\bar{a}$ heeft een multiplicatieve inverse dan en slechts dan als $\text{ggd}(a, n) = 1$, want dan zijn er gehele getallen x en y zodat $xa + yn = 1$, dat wil zeggen $\bar{x}\bar{a} = \bar{1}$.

De schrijfwijze R^* is in overeenstemming met de al eerder gehanteerde notaties $\mathbb{R}^*$, $\mathbb{Q}^*$ en $\mathbb{C}^*$.

(1.11) Propositie. *Laat n een positief geheel getal zijn. De ring $\mathbb{Z}/n\mathbb{Z}$ is een lichaam dan en slechts dan als n een priemgetal is.*

Bewijs. De ring $\mathbb{Z}/n\mathbb{Z}$ is een lichaam als $\bar{1} \neq \bar{0}$ en ieder element $\bar{a}$ ongelijk $\bar{0}$ een multiplicatieve inverse heeft. Dus moet $n \geq 2$ zijn en iedere a met $0 < a < n$ moet onderling ondeelbaar zijn met n. Dat gebeurt precies wanneer n een priemgetal is.

(1.12) Definitie. Een deelverzameling R' van een ring R heet een *deelring* als voldaan is aan

(D1) (*Ondergroep*) R' is een ondergroep van R voor de optelling $+$;
(D2) (*Geslotenheid*) Voor alle $x, y \in R'$ geldt $xy \in R'$.

Merk op dat met de optelling en vermenigvuldiging van R de deelverzameling R' zelf een ring is. Het kan echter gebeuren dat R een eenheidselement heeft, terwijl R' dat niet heeft, bijv. $n\mathbb{Z} \subset \mathbb{Z}$ voor $n > 1$. (Zie ook Opgave 8.)

(1.13) Definitie. Laat R een ring zijn. Een element $x \in R$ met $x \neq 0$ heet *linkernuldeler* als er een element $y \neq 0$ in R is met $xy = 0$. Een element $x \in R$ met $x \neq 0$ heet *rechternuldeler* als er een $y \in R$ is met $y \neq 0$ zodat $yx = 0$. Een element $x \in R$ heet *nuldeler* als het linker- of rechternuldeler is.

De ringen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ bezitten geen nuldelers. Maar in $\mathbb{Z}/6\mathbb{Z}$ is $\bar{2}$ een nuldeler: $\bar{2} \cdot \bar{3} = \bar{0}$.

(1.14) Propositie. *Een nuldeler in een ring R is geen eenheid.*

Bewijs. Laat x een (linker)nuldeler zijn. Dan is er een $y \neq 0$ met $xy = 0$. Als x eenheid is, dan is er ook een z met $zx = 1$. Dus vinden we

$$0 = z \cdot xy = z(xy) = (zx)y = 1 \cdot y = y,$$

in tegenspraak met de aanname dat $y \neq 0$. Het geval van een rechternuldeler is analoog.

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

Vele van de ringen die we tegenkwamen zijn domeinen, zoals $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ en ook $\mathbb{Z}[i]$. Maar als n geen priem is dan is $\mathbb{Z}/n\mathbb{Z}$ geen domein. De ring $\mathbb{Z}[i]$ is geen lichaam, maar als we meer noemers toelaten wordt het dat wel: $\mathbb{Q}(i)$ gedefinieerd door

$$\{a + b\,i : a, b \in \mathbb{Q}\}$$

is een lichaam. (Zie opgave 2.) Dit is een voorbeeld van een algemene constructie die we nu geven.

(1.16) Voorbeeld. *Het Quotiëntenlichaam* of *Breukenlichaam.* Laat R een domein zijn. We construeren nu een lichaam $Q(R)$, het *quotiëntenlichaam* van R, door aan R ook de quotiënten xy^{-1} voor $y \neq 0$ toe te voegen als volgt.

We nemen de verzameling

$$D = \{(x, r) \in R \times R : r \neq 0\}$$

en we definiëren nu een equivalentierelatie op D via

$$(x, r) \sim (y, s) \iff xs = yr.$$

We moeten nagaan dat dit een equivalentierelatie is. Dat $(x, r) \sim (x, r)$ en dat uit $(x, r) \sim (y, s)$ ook $(y, s) \sim (x, r)$ volgt is duidelijk. De transitiviteit zien we als volgt. Stel dat $(x, r) \sim (y, s)$ en dat $(y, s) \sim (z, t)$, dan weten we dat

$$xts = xst = yrt = ryt = rzs = zrs$$

en dus geldt $(xt - zr)s = 0$. Omdat $s \neq 0$ en R geen nuldelers heeft, moet $xt = zr$, dat wil zeggen $(x, r) \sim (z, t)$, zoals gewenst.

Laat nu $Q(R)$ de verzameling equivalentieklassen zijn van $\sim$ op D. We schrijven eenvoudig $\frac{x}{r}$ (of x/r) voor de equivalentieklasse van (x, r). Er geldt dus:

$$\frac{x}{r} = \frac{y}{s} \quad \text{dan en slechts dan als} \quad xs = yr.$$

(Vergelijk de schrijfwijze voor elementen uit $\mathbb{Q}$.)

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

$$\frac{x}{r} + \frac{y}{s} = \frac{xs + yr}{rs},$$
$$\frac{x}{r} \cdot \frac{y}{s} = \frac{xy}{rs}.$$

Merk op dat de 'noemers' rs ongelijk nul zijn omdat r en s ongelijk nul zijn en R een domein is.

We moeten nu laten zien dat deze definitie gerechtvaardigd is, omdat we de definitie geven in termen van een representanten van de equivalentieklassen en deze representanten niet uniek zijn.

Stel dat we andere representanten kiezen, zeg

$$\frac{x}{r} = \frac{x'}{r'}, \quad \frac{y}{s} = \frac{y'}{s'}.$$

Dan geldt $xr' = x'r$ en $ys' = y's$ zodat

$$\begin{aligned}(x's' + y'r')rs &= x's'rs + y'r'rs = (x'r)s's + (y's)r'r \\ &= xr's's + ys'r'r = (xs + yr)r's'\end{aligned}$$

zodat volgens de definitie geldt

$$\frac{x's' + y'r'}{r's'} = \frac{xs + yr}{rs},$$

en dit betekent dat het resultaat van de optelling niet van de gekozen representanten afhangt. De berekening die dit ook voor de vermenigvuldiging controleert laten we aan de lezer over.

We beweren nu dat $Q(R)$ een lichaam is. De controle van de ringaxioma's is rechttoe rechtaan. Het nulelement is $\frac{0}{1}$. Ook de commutativiteit en het eenheidselement zijn duidelijk $1 = \frac{1}{1}$. Dat ieder element $\neq 0$ een multiplicatieve inverse heeft is direct te zien:

$$(\frac{x}{r})^{-1} = \frac{r}{x}.$$

We kunnen R opvatten als deelring van R via de afbeelding

$$R \longrightarrow Q(R), \quad x \mapsto \frac{x}{1}.$$

Ga na dat deze afbeelding injectief is.

(1.17) Voorbeelden. Als $R = \mathbb{Z}$ dan vinden we $Q(R) = \mathbb{Q}$. Als we voor R een polynoomring $k[X]$ nemen met k een lichaam, dan vinden we als quotiëntenlichaam het lichaam $k(X)$ van *rationale functies in een variabele*. De elementen van $k(X)$ laten zich schrijven als

$$\frac{f(X)}{g(X)} \quad \text{waarbij } f(X), g(X) \in k[X], \text{ en } g(X) \neq 0.$$

(1.18) Voorbeeld. *Ringen van functies.* Laat X een verzameling zijn en R een ring. De verzameling R^X van afbeeldingen $f : X \longrightarrow R$ wordt met de volgende optelling en vermenigvuldiging een ring:

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x),\end{aligned}$$

waarbij de optelling en vermenigvuldiging van de functiewaarden in R gebeurt.

Aan de afbeeldingen of functies die voorkomen kunnen nog verdere restricties worden opgelegd. Zo is de verzameling $C([0,1])$ van continue reëelwaardige functies $f : [0,1] \longrightarrow \mathbb{R}$ op het eenheidsinterval een deelring van $\mathbb{R}^{[0,1]}$. Analoog kunnen we de ring $C^1([0,1])$ (of $C^\infty([0,1])$) van differentieerbare (of oneindig vaak differentieerbare) functies op het eenheidsinterval nemen, etc.

(1.19) Voorbeeld *Endomorfismenringen.* Laat A een abelse (en additief geschreven) groep zijn en laat

$$\mathrm{End}(A) = \{f : A \to A : f \text{ is een groepshomomorfisme } \}$$

de verzameling van endomorfismen van A zijn. We definiëren nu een optelling $+$ en een vermenigvuldiging $\cdot$ van endomorfismen via

$$(f+g)(x) = f(x) + g(x), \quad f \cdot g(x) = f(g(x)).$$

Merk op dat $f + g$ weer een endomorfisme van A is (hier wordt gebruikt dat A abels is). Samenstelling van endomorfismen is een endomorfisme, dus $fg \in \mathrm{End}(A)$. We laten het aan de lezer over te controleren dat $\mathrm{End}(A)$ met deze bewerkingen een ring is. Deze ring heet de *endomorfismenring* van A. Deze ring heeft een eenheidselement, 1_A, de identieke afbeelding op A.

Een speciaal geval hiervan wordt verkregen door $A = \mathbb{R}^n$ te nemen. Een lineaire afbeelding $f : \mathbb{R}^n \to \mathbb{R}^n$ is een speciaal geval van een endomorfisme. Dus de lineaire afbeeldingen vormen een deelverzameling van $\mathrm{End}(A)$; in feite vormen ze een deelring. Omdat we een lineaire afbeelding kunnen identificeren met een matrix kunnen we de verzameling $\mathrm{Mat}(n, \mathbb{R})$ van $n \times n$-matrices opvatten als een deelring van $\mathrm{End}(A)$.

(1.20) Voorbeeld. Laat R_1 en R_2 ringen zijn. Dan voorzien we de productgroep $R_1 \times R_2$ van een ringstructuur door te definiëren: $(r_1, r_2) \cdot (s_1, s_2) = (r_1 s_1, r_2 s_2)$. Ga na dat dit inderdaad een ring is. Deze ring is commutatief als R_1 en R_2 het zijn. Als beide ringen een eenheidselement hebben, dan heeft $R_1 \times R_2$ dat ook. De lezer mag nagaan dat in dat geval geldt $R^* = R_1^* \times R_2^*$.

Opgaven

1) Laat R een ring zijn. Ga na dat de volgende identiteiten gelden in R:

$$x(y_1 + y_2 + \ldots + y_n) = xy_1 + xy_2 + \ldots + xy_n$$
$$(x_1 + x_2 + \ldots + x_n)y = x_1y + x_2y + \ldots x_ny,$$
$$x(y - z) = xy - xz.$$

Laat verder zien dat geldt $0x = x0 = 0$ voor alle $x \in R$.

2) Laat zien dat $\mathbb{Z}[i]$ een commutatieve ring met 1 is, maar geen lichaam. Laat verder zien dat

$$\mathbb{Q}(i) = \{a + b\,i \in \mathbb{C} : a, b \in \mathbb{Q}\}$$

met de optelling en vermenigvuldiging van $\mathbb{C}$ wel een lichaam is.

3) Laat zien dat een element van een ring met 1 maar een inverse kan hebben. Laat verder zien dat een ring maar een eenheidselement kan bezitten.

4) Bewijs dat $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

5) Definiëer voor een ring R het *centrum* van R als

$$Z(R) = \{x \in R : xy = yx \quad \text{voor alle } y \in R\}$$

Laat zien dat het centrum een deelring van R is.

6) Gegeven is dat k een lichaam is. Bewijs dat $k[X]$ een domein is.

7) Laat zien dat de ring $C([0,1])$ van continue reëelwaardige functies op het eenheidsinterval nuldelers bezit.

8) Laat $R = \mathbb{Z}/10\mathbb{Z}$. Laat zien dat $R' = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ een deelring van R is en dat R' een ring met eenheidselement is.

9) Gegeven zij een eindige ring R met $1 \neq 0$. Bewijs dat elke niet-nuldeler van R nul is of een eenheid. (Dit impliceert dat zo een R een delingsring is als er geen nuldelers zijn.)

10) Laat R een ring met 1 en zonder nuldelers zijn. Bewijs dat $R[X]^* = R^*$.

11) Laat X een verzameling zijn en $R = P(X)$ de machtsverzameling van X, dat wil zeggen, de elementen van R zijn de deelverzamelingen van X. We definiëren een optelling en vermenigvuldiging op R via:

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

Laat zien dat R hiermee een ring is. Laat verder zien dat voor alle $x \in R$ de relatie $x^2 = x$ en ook $2x = 0$ geldt.

13) Laat R een commutatieve ring zijn. Bewijs voor $n > 0$ geheel en $x, y \in R$ het "binomium van Newton"

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

en laat omgekeerd zien dat als in een ring het binomium van Newton geldt de ring commutatief is.

14) Laat A een abelse groep zijn. Bewijs dat $\mathrm{End}(A)^* = \mathrm{Aut}(A)$.

15) Gegeven zij een ring R. We definiëren nu een nieuwe vermenigvuldiging op R, geschreven $x * y$, door $x * y = y \cdot x$ voor alle $x, y \in R$ te stellen. Bewijs dat R met deze nieuwe vermenigvuldiging een ring is. We schrijven R^{opp}, de tegengestelde ring van R.

16) *De groepenring.** Laat G een (multiplicatief geschreven) groep zijn en R een ring. De verzameling $R[G]$ bestaat uit alle uitdrukkingen $\sum_{g \in G} r_g\, g$ met $r_g \in R$ en $r_g = 0$ voor bijna alle $g \in G$. We definiëren een optelling door

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$$

en een vermenigvuldiging via

$$r_g g \cdot s_h h = r_g s_h\, gh$$

* De groepenring is een uitvinding van A. Cayley uit 1854.

en de distributieve wet. Dus uitgeschreven

$$(\sum_{g\in G} r_g g)\cdot(\sum_{h\in G} s_h h) = \sum_{\gamma\in G}(\sum_{g,h:gh=\gamma} r_g s_h)\gamma.$$

Bewijs dat $R[G]$ op deze manier een ring wordt. Als R een eenheidselement bezit, dan is $1\,e$ het eenheidselement van $R[G]$ en kan G opgevat worden als ondergroep van $R[G]^*$ via $g \mapsto 1\,g$. Laat nu zien dat als g eindige orde in G heeft en $g \neq e$ en R niet de nulring is, het element $1-g$ nuldeler is van $R[G]$.

17) *Ring van de duale getallen over k.** Laat k een lichaam zijn en $R = k[\epsilon]$ de verzameling

$$\{a + b\epsilon : a, b \in k\}.$$

De optelling en vermenigvuldiging worden gedefinieerd door

$$(a+b\epsilon)+(c+d\epsilon) = (a+c)+(b+d)\epsilon, \qquad (a+b\epsilon)(c+d\epsilon) = ac+(bc+ad)\epsilon.$$

Er geldt dus $\epsilon^2 = 0$. Laat zien dat R met deze bewerkingen een ring met eenheidselement wordt. Wat zijn de eenheden van deze ring?

18) Laat d een geheel getal zijn met $d \equiv 1 \pmod 4$ dat geen kwadraat is. Laat

$$\alpha = \frac{1+\sqrt{d}}{2} \in \mathbb{C} \quad \text{en} \quad R = \{a + b\,\alpha : a, b \in \mathbb{Z}\}.$$

Bewijs dat R een deelring is van $\mathbb{C}$.

19) Laat $d \in \mathbb{Z}_{>0}$ een geheel getal zijn dat geen kwadraat is. Stel dat $\epsilon = a + b\sqrt{d}$ een eenheid is van $R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. Bewijs dat $\pm a \pm b\sqrt{d}$ allemaal eenheden zijn. Laat zien dat $\mathbb{Z}[\sqrt{5}]$ oneindig veel eenheden bezit.

20) Laat $R = \{f : \mathbb{R} \to \mathbb{R}\}$ met optelling en vermenigvuldiging gegeven door

$$(f+g)(x) = f(x)+g(x), \quad (f\cdot g)(x) = f(x)g(x).$$

Laat zien dat R een ring met 1 is en dat ieder element $f \neq 0$ van R een eenheid of nuldeler is.

21) Zij R een ring met 1 zonder nuldelers en laat $x, y \in R$ elementen zijn. Bewijs dat uit $xy = 1$ volgt $yx = 1$.

22) Is de productring $\mathbb{Z} \times \mathbb{Z}$ een domein?

23) Laat $R = \{a + bi : a, b \in \mathbb{Z}/3\mathbb{Z}\}$ met optelling en vermenigvuldiging gegeven door:

$$(a+bi)+(c+di) = (a+c)+(b+d)i, \qquad (a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

Dus i is een symbool met $i^2 = -1$. Bewijs dat R een lichaam met 9 elementen is.

---

* Deze ring werd ingevoerd door door E. Study, een Duits wiskundige, 1862-1930

2. Ringhomomorfismen en Idealen

It was she who taught us to think in terms of simple and general algebraic concepts– homomorphic mappings, groups and rings with operators, ideals– and not in terms of cumbersome algebraic computations.
(P.S. Alexandrov in zijn herdenkingsrede op Emmy Noether (1935))

Net als bij groepen kunnen we ringen vergelijken met behulp van struktuurbewarende afbeeldingen, de ringhomomorfismen.

(2.1) Definitie. Een afbeelding $f : R_1 \longrightarrow R_2$ van twee ringen heet een *ringhomomorfisme* als voor alle $x, y \in R_1$ geldt

i) $f(x + y) = f(x) + f(y)$,
ii) $f(xy) = f(x)f(y)$.

Een bijectief ringhomomorfisme heet een *isomorfisme*.

Nog wat terminologie: een ringhomomorfisme van ringen met een eenheidselement heet *unitair* als $f(1) = 1$. (Ga na dat voor een ringhomomorfisme altijd $f(0) = 0$ geldt.) Zijn R_1 en R_2 lichamen dan heet een unitair ringhomomorfisme $f : R_1 \longrightarrow R_2$ een *lichaamshomomorfisme*; een unitair isomorfisme van lichamen heet een lichaamsisomorfisme. Isomorfismen van een ring naar zichzelf heten *automorfismen*. Soms zeggen we kortweg homomorfisme in plaats van ringhomomorfisme als het duidelijk is wat we bedoelen.

(2.2) Voorbeelden

i) De kanonieke afbeelding $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ met $f(x) = \bar{x}$ is een ringhomomorfisme.
ii) De inclusieafbeelding $R' \to R$ van een deelring in een ring is een injectief ringhomorfisme.
iii) De afbeelding $R_1 \to R_1 \times R_2$ met $x \mapsto (x, 0)$ is een ringhomomorfisme. De *projectie* $p_1 : R_1 \times R_2 \longrightarrow R_1$ met $(x, y) \mapsto x$ is een ringhomomorfisme. Ook de projectie op de tweede factor is een ringhomomorfisme.
iv) Laat R een commutatieve ring zijn en $r \in R$ een ringelement. Dan is de "substitutieafbeelding" $s_r : R[X] \longrightarrow R$ gegeven door

$$f = \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i r^i$$

een ringhomomorfisme. We controleren hier ii) en laten de controle van i) aan de lezer over. Er geldt $s_r(fg) = \sum_{i=0}^{\infty} c_i r^i$ waarbij $c_i = \sum_{j,k:j+k=i} a_j b_k$; anderzijds geldt

$$s_r(f)s_r(g) = \sum_{j=0}^{\infty} a_j r^j \sum_{k=0}^{\infty} b_k r^k.$$

Omdat R commutatief is geldt $a_j r^j b_k r^k = a_j b_k r^{j+k}$ en daaruit volgt dat $s_r(fg) = s_r(f)s_r(g)$ zoals gewenst.
v) Laat R een ring met eenheidselement zijn. Dan is de afbeelding $\mathbb{Z} \longrightarrow R$ gegeven door $n \mapsto 1 + 1 + \ldots + 1$ (n maal) voor $n > 0$, $n \mapsto -1 - 1 \ldots - 1$ ($-n$ maal) als $n < 0$ en $0 \mapsto 0$ een ringhomomorfisme.

Het beeld $f(R_1) = \{f(x) : x \in R_1\}$ van een ring R_1 onder een ringhomomorfisme $f : R_1 \to R_2$ is een deelring van R_2. De kern $\ker(f)$ van een ringhomomorfisme

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

is een deelring van R_1. Analoog aan de groepentheorie nemen de kernen van homomorfismen een speciale plaats in onder de deelringen, het zijn idealen, een begrip dat geïntroduceerd werd door de Duitse wiskundige E.E. Kummer in 1845:

(2.3) Definitie. Laat R een ring zijn. Een *ideaal* van R is een deelverzameling $I \subset R$ die aan de volgende twee eisen voldoet:

i) I is een ondergroep van R;
ii) voor alle $x \in I$ en alle $r \in R$ geldt $rx \in I$ en $xr \in I$.

Als we in ii) de eis vervangen door: voor alle $x \in I$ en $r \in R$ geldt $rx \in I$ dan krijgen we het begrip *linksideaal*. Analoog is er het begrip *rechtsideaal*. Een ideaal is dus zowel links- als rechtsideaal.

(2.4) Voorbeelden.

i) In iedere ring zijn $\{0\}$ en R idealen.
ii) Laat $R = \mathbb{Z}$ en $m \in \mathbb{Z}$. Dan is $m\mathbb{Z}$ een ideaal en ieder ideaal is van deze vorm.
iii) Laat $R = \mathrm{Mat}(2, \mathbb{R})$. De verzameling

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

is een linksideaal, maar geen rechtsideaal.
iv) Laat $R = C([0, 1])$ de ring van continue functies op het interval $[0, 1]$ zijn. Als $p \in [0, 1]$ een willekeurig punt is dan is de verzameling $\{f \in R : f(p) = 0\}$ een ideaal.

(2.5) Propositie. *De kern* $\ker(f)$ *van een ringhomomorfisme* $f : R_1 \to R_2$ *is een ideaal van* R_1.

Bewijs. Omdat f ook een groepshomomorfisme is, is de kern ook een ondergroep. We controleren nu ii). Laat $r \in R_1$ en $x \in \ker(f)$. Dan geldt

$$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0, \quad f(xr) = f(x)f(r) = 0 \cdot f(r) = 0.$$

(2.6) Definitie Laat R een commutatieve ring met 1 zijn. Als $x_1, \ldots, x_n$ elementen van R zijn dan heet de verzameling

$$\{r_1x_1 + r_2x_2 + \ldots + r_nx_n : r_1, \ldots, r_n \in R\}$$

het door $x_1, \ldots, x_n$ *voortgebracht ideaal*. Notatie $(x_1, \ldots, x_n)$. De elementen $x_1, \ldots, x_n$ heten de *voortbrengers*. (Ga na dat dit inderdaad een ideaal is.) Een ideaal (x) voortgebracht door één element x heet een *hoofdideaal*. Een element $y \in R$ heet *deelbaar* door x als $y \in (x)$.

Niet ieder ideaal is een hoofdideaal. Bijvoorbeeld: in de ring $\mathbb{Z}[X]$ is het ideaal $(2, X)$ geen hoofdideaal. Immers, als f een voortbrenger van $(2, X)$ is (dus $(f) = (2, X)$) dan kunnen we schrijven

$$2 = fg \quad \text{voor zekere } g.$$

Omdat $0 = \deg(2) = \deg(fg) = \deg(f) + \deg(g)$ volgt dat f en g constanten zijn, dus $f \in \{\pm 1, \pm 2\}$. Verder geldt ook $X = fh$, waaruit volgt dat $f \neq \pm 2$, dus $f = \pm 1$. We beweren nu dat 1 en -1 niet in het ideaal $(2, X)$ liggen; immers, dit ideaal bestaat uit polynomen waarvan de constante term even is. Dus I is geen hoofdideaal.

(2.7) Definitie. Laat R een ring met eenheidselement zijn en beschouw het homomorfisme $f : \mathbb{Z} \longrightarrow R$ met $f(n) = n$ uit voorbeeld (2.2.v)). Dan is de kern van f een ideaal in $\mathbb{Z}$, dus van de vorm $\mathbb{Z}n$ met $n \geq 0$. Het getal n heet de *karakteristiek* van R.

De ringen $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ hebben karakteristiek 0; de ring $\mathbb{Z}/n\mathbb{Z}$ heeft karakteristiek n voor $n \geq 0$.

(2.8) Propositie. *Zij R een ring met eenheidselement en I een ideaal van R. Als I een eenheid bevat dan geldt $I = R$.*

Bewijs. Laat $x \in I$ een eenheid zijn. Dan behoort $1 = x \cdot x^{-1}$ tot I, en dan ook ieder element $r = r \cdot 1$ van R.

(2.9) Propositie. *Laat R een delingsring zijn. Dan is ieder ideaal van R gelijk aan (0) of aan R. Een unitair homomorfisme $f : R \to R'$ met R' ook een ring met $1 \neq 0$, is injectief.*

Bewijs. Een element $x \neq 0$ is een eenheid. Als zo een element in een ideaal I ligt dan volgt $I = R$. Dus of $I = (0)$ of $I = R$. Omdat voor een unitair ringhomomorfisme $\ker(f) \neq R$ volgt $\ker(f) = \{0\}$.

We voeren nu nog een aantal operaties met idealen uit.
Als R een ring is en I en J zijn idealen van R dan is

$$I \cap J$$

een ideaal. Het is het grootste ideaal van R dat zowel in I als in J bevat is. We definiëren nu de *som* $I + J$ van I en J via

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

Dit is weer een ideaal; het is het kleinste ideaal dat zowel I als J bevat. We zeggen dat I en J *onderling ondeelbaar* zijn als $I + J = R$.

Het *product* IJ van I en J wordt gedefinieerd als

$$IJ = \{\sum_{k=1}^{m} x_k y_k : m \in \mathbb{Z}_{\geq 1}, x_k \in I,\ y_k \in J\}.$$

dit is een ideaal; het is het ideaal voortgebracht door de verzameling $\{xy : x \in I, y \in J\}$ (die in het algemeen geen ideaal is). We hebben de volgende inclusies:

$$\begin{array}{ccccc} & & I & & \\ & \nearrow & & \searrow & \\ IJ \subseteq I \cap J & & & & I + J \\ & \searrow & & \nearrow & \\ & & J & & \end{array}$$

In het geval van $R = \mathbb{Z}$ is de betekenis van deze idealen als volgt: laat $I = (m)$, $J = (n)$. Dan $IJ = mn\mathbb{Z}$, $I \cap J = \text{kgv}(m, n)\mathbb{Z}$ en $I + J = \text{ggd}(m, n)\mathbb{Z}$. Ga dit na.

Opgaven

1) Laat R een ring met eenheidselement zijn. Bewijs dat er precies één unitair ringhomomorfisme $\mathbb{Z} \longrightarrow R$ is.

2) Bewijs de volgende uitspraken: een unitair ringhomomorfisme $f : \mathbb{Q} \to \mathbb{Q}$ is de identiteit. Een unitair ringhomomorfisme $f : \mathbb{R} \longrightarrow \mathbb{R}$ voldoet aan $f(x) > 0$ als $x > 0$. Een unitair ringhomomorfisme $f : \mathbb{R} \to \mathbb{R}$ is de identiteit.

3) Bewijs of weerleg de uitspraak: ieder unitair ringhomomorfisme $f : \mathbb{C} \to \mathbb{C}$ is de identiteit.

4) Laat R een ring met 1 zijn zonder nuldelers. Laat zien dat de karakteristiek van R gelijk is aan 0 of een priemgetal is.

5) Laat $f : R_1 \longrightarrow R_2$ een unitair ringhomomorfisme zijn. Bewijs dat $f^* = f|R_1^*$ de verzameling R_1^* afbeeldt naar R_2^*. Bewijs verder: f^* is een groepshomomorfisme. Bewijs ook: f^* is injectief als f dat is. Is f^* surjectief als f surjectief is?

6) Laat I en J idealen van R zijn. Laat zien dat $IJ \subseteq I \cap J$. Bewijs: $I \cup J$ is een ideaal dan en slechts dan als $I \subseteq J$ of $J \subseteq I$.

7) Laat R een ring zijn en $r \in Z(R)$ een element uit het centrum. Laat zien dat de substitutie $X \mapsto r$ een homomorfisme $R[X] \to R$ definiëert.

8) Laat A een abelse groep zijn. Bewijs dat de verzameling

$$\{f \in \text{End}(A) : f(a) = 0 \quad \text{voor alle } a \in A \text{ van eindige orde}\}$$

een ideaal van $\text{End}(A)$ is.

9) Is de afbeelding $\text{Mat}(n, \mathbb{R}) \to \mathbb{R}$ gegeven door $M \mapsto \det(M)$ een ringhomomorfisme?

10) Laat R een ring zijn. Bewijs het ringisomorfisme $R[X, Y] \cong R[Y, X]$.

11) Laat R_1 en R_2 ringen zijn met eenheidselement. Bewijs: ieder ideaal van $R_1 \times R_2$ is van de vorm $I_1 \times I_2$ met I_1 (resp. I_2) een ideaal van R_1 (resp. R_2).

12) Laat R een oneindige commutatieve ring zijn die een nuldeler bezit. Bewijs dat R oneindig veel nuldelers bezit.

13) Hoeveel idealen heeft een lichaam?

14) Bepaal de idealen van de ring $k[\epsilon]$ van de duale getallen.

15) Laat R een commutatieve ring met 1 zijn en I en J twee onderling ondeelbare idealen van R. Laat zien dat $I^2 = II$ en $J^2 = JJ$ twee onderling ondeelbare idealen zijn.

16) Laat R de ring van continue reëelwaardige functies op het eenheidsinterval $[0,1]$ zijn. Laat $D \subset [0,1]$ een deelverzameling zijn. Bewijs dat

$$I = \{f \in R; f(x) = 0 \quad \text{voor alle } x \in D\}$$

een ideaal van R is. Wat zijn de eenheden van R?

17) Laat k een lichaam zijn van karakteristiek p, een priemgetal. Bewijs dat voor alle $x, y \in k$ geldt: $(x+y)^p = x^p + y^p$. Bewijs verder dat de afbeelding $k \to k$ met $x \mapsto x^p$ een endomorfisme van k is.

18) Laat S een commutatieve ring met 1 zijn en laat

$$R = \{f : \mathbb{Z}_{>0} \longrightarrow S\}.$$

We definiëren een optelling op R via $(f+g)(x) = f(x) + g(x)$ en een vermenigvuldiging via

$$(f * g)(x) = \sum_{yz=x} f(y)g(z),$$

waarbij de som loopt over alle paren $y, z \in \mathbb{Z}_{>0}$ met $yz = x$. Bewijs dat R een commutatieve ring is met eenheidselement. Wat is het eenheidselement? (Het product $f * g$ heet het *convolutieproduct* van f en g.)

19) Laat R_1 en R_2 ringen zijn. Bewijs het isomorfisme: $R_1[X] \times R_2[X] \cong (R_1 \times R_2)[X]$.

20) Laat $G = \{1, g\}$ een groep van orde 2 zijn. Bewijs dat de afbeelding $\mathbb{R}[G] \longrightarrow \mathbb{R} \times \mathbb{R}$ gegeven door $a + bg \mapsto (a+b, a-b)$ een isomorfisme van ringen is.

21) Bepaal alle idealen van $\mathbb{Z}/24\mathbb{Z}$.

22) Bepaal de kleinste deelring van $\mathbb{Q}$ die het element $1/2$ bevat.

23) Laat zien dat $\mathbb{Z}$ wel een deelring, maar geen ideaal van $\mathbb{Z}[X]$ is.

24) Laat R een commutatieve ring met 1 zijn en I een ideaal van R. Definieer het *radicaal* van I door

$$\sqrt{I} = \{x \in R : \text{ er is een } n \in \mathbb{Z}_{>0} \text{ met } x^n \in I\}.$$

Bewijs dat dit een ideaal van R is. Bewijs verder dat $\sqrt{\sqrt{I}} = \sqrt{I}$.

25) Laat $R = \mathbb{Z}/36\mathbb{Z}$. Bereken $\sqrt{(0)}$, $\sqrt{(4)}$, $\sqrt{(6)}$ en $\sqrt{(18)}$.

26) Laat R een commutatieve ring met 1 zijn en $D \subset R$ een deelverzameling. Bewijs dat de *annihilator* van D

$$\mathrm{Ann}(D) := \{r \in R : rx = 0 \text{ voor alle } x \in D\}$$

een ideaal van R is.

27) Bepaal de automorfismen van de ring $\mathbb{Z}[X]$.

28) Bepaal alle idealen van de ring $\mathbb{R}[[X]]$ van formele machtreeksen met reële coëfficiënten. (De elementen van $\mathbb{R}[[X]]$ zijn uitdrukkingen $\sum_{i=0}^{\infty} a_i X^i$ met de $a_i \in \mathbb{R}$ en met optelling en vermenigvuldiging als in (1.7).)

29) Bepaal alle ringhomomorfismen van $\mathbb{Z}/12\mathbb{Z}$ naar $\mathbb{Z}/42\mathbb{Z}$.

30) Laat zien dat (X, Y) geen hoofdideaal is in $\mathbb{Q}[X, Y]$.

3. Quotienten van Ringen

These theorems have found important applications
in all branches of mathematics.
E. Artin*

In dit hoofdstuk introduceren we quotiëntringen analoog aan de constructie van quotiënt- of factorgroepen.

(3.1) Afspraak. In het vervolg van deze syllabus zullen we (stilzwijgend) aannemen dat alle ringen een eenheidselement 1 bezitten en dat alle ringhomomorfismen unitair zijn (d.w.z. $f(1) = 1$).

(3.2) Definitie. *Quotiëntring.* Laat R een ring zijn en I een ideaal. Omdat I een ondergroep is van de abelse groep R kunnen we de quotiëntgroep R/I vormen. We definiëren nu een vermenigvuldiging op de groep R/I via

$$\bar{x} \cdot \bar{y} := \overline{xy}$$

waarbij we $\bar{x}$ schrijven voor de nevenklasse $x + I$. We controleren dat deze definitie niet afhangt van de gekozen representanten x en y: laat x' en y' elementen zijn met $\bar{x'} = \bar{x}$, $\bar{y'} = \bar{y}$. Dan hebben we

$$x' = x + i, \quad y' = y + j, \quad \text{met } i, j \in I.$$

en vinden

$$x'y' = (x + i)(y + j) = xy + iy + xj + ij$$

en omdat I een ideaal is liggen ix, jy en ij in I, dus we zien

$$\overline{x'y'} = \overline{xy}.$$

De bewering is nu dat R/I met deze vermenigvuldiging een ring is, de *quotiëntring* van R naar I. De controle van de ringaxioma's is nu weer rechttoe rechtaan en wordt aan de lezer overgelaten. Het eenheidselement van R/I is $\bar{1}$.

(3.3) Propositie. *Laat R een ring zijn en I een ideaal van R. Dan is het kanonieke homomorfisme*

$$\phi : R \longrightarrow R/I \quad \text{gegeven door } x \mapsto \bar{x}$$

een surjectief ringhomomorfisme met kern I.

Bewijs. De surjectiviteit van ϕ is duidelijk uit de definitie $\phi(x) = \bar{x}$. Verder is $\bar{x} = \bar{0}$ dan en slechts dan als $x \in I$. Verder is ook direct duidelijk dat ϕ een homomorfisme is.

De homomorfiestelling voor groepen heeft een pendant voor ringen die we nu formuleren.

* Emil Artin, 1898-1962, geboren in Wenen en werkzaam in Duitsland tot 1937 toen hij naar Amerika emigreerde.

(3.4) Stelling. (Homomorfiestelling) *Laat $f : R \longrightarrow R'$ een ringhomomorfisme zijn en I een ideaal van R met $I \subseteq \ker(f)$. Dan bestaat er een eenduidig bepaald ringhomomorfisme $h : R/I \longrightarrow R'$ zodat $h \cdot \phi = f$, of anders geformuleerd, het volgende diagram commuteert.*

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ & \phi \searrow \quad h \nearrow & \\ & R/I & \end{array}$$

Bewijs. Net zoals bij de groepen definiëren we h via $h(\bar{x}) = f(x)$. Deze h is dan een welgedefinieerd groepshomomorfisme en het enige groepshomomorfisme met de eigenschap dat $h \cdot \phi = f$. Men gaat gemakkelijk na dat h een ringhomomorfisme is. Daarmee is de stelling bewezen.

Ook de isomorfiestelling heeft een analogon:

(3.5) Stelling. *(Isomorfiestelling) Laat $f : R \longrightarrow R'$ een ringhomomorfisme zijn. Dan is er een isomorfisme*

$$R/\ker(f) \cong f(R).$$

Bewijs. Analoog aan het geval voor groepen. Met behulp van de homomorfiestelling voor $f : R \to f(R)$ vinden we een uniek ringhomomorfisme

$$h : R/\ker(f) \longrightarrow f(R),$$

met $h(\bar{x}) = f(x)$ en h is duidelijk surjectief. Stel $\bar{x} \in \ker(h)$. Dan geldt $f(x) = 0$, dus $x \in \ker(f)$, m.a.w. $\bar{x} = \bar{0}$.

Het analogon van de tweede isomorfiestelling is de volgende stelling.

(3.6) Stelling. *(Tweede isomorfiestelling) Laat R een ring zijn, R' een deelring van R en I een ideaal van R zijn. Dan is $R' \cap I$ een ideaal van R', en $R' + I = \{r + x : r \in R', x \in I\}$ een deelring van R en er geldt het isomorfisme*

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

Het bewijs hiervan wordt aan de lezer overgelaten. (Zie opgave 1.)

Tenslotte heeft ook de Derde Isomorfiestelling een analogon. Het luidt als volgt.

(3.7) Stelling. *(Derde Isomorfiestelling) Laat R een ring zijn en I een ideaal.*

i) Ieder ideaal van de ring R/I heeft de gedaante J/I, waar J een ideaal van R is dat I bevat.

ii) Laat J een ideaal van R zijn dat I bevat. Dan is J/I een ideaal van R/I en er geldt het isomorfisme

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

Bewijs. Het bewijs is volstrekt analoog aan het bewijs voor het geval van groepen en wordt aan de lezer overgelaten.

De voorgaande stelling kan gebruikt worden voor het stapsgewijs uitdelen van een ring naar een ideaal. Zie bijvoorbeeld 3.8 iii). We geven nu een aantal voorbeelden en toepassingen van het gebruik van de verschillende isomorfiestellingen.

(3.8) Voorbeelden.

i) Laat R een commutatieve ring zijn en laat $a \in R$ een element van R zijn. We beschouwen de afbeelding

$$\rho : R[X] \longrightarrow (R/aR)[X], \quad f = \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a}_i X^i,$$

waarbij $\overline{a}_i$ de restklasse van a_i in R/aR is. Dit is een ringhomomorfisme. Een element f dat in de kern van ρ zit heeft alle coefficiënten in aR, m.a.w. de coëfficiënten zijn deelbaar door a. Schrijven we nu $a_i = aa_i'$ dan is f van de vorm

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

Dus de kern van ρ is precies $aR[X]$. De isomorfiestelling vertelt ons nu dat

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

ii) Laat R een ring zijn en laat $\nu : R[X] \longrightarrow R$ de afbeelding zijn gegeven door $f \mapsto f(0)$, m.a.w. $\sum_{i=0}^{n} a_i X^n \mapsto a_0$. De lezer mag nagaan dat dit een surjectief ringhomomorfisme is. De kern van ν bestaat uit alle polynomen met $a_0 = 0$. Deze polynomen zijn deelbaar door X en we concluderen dat $\ker(\nu) = XR[X]$. De isomorfiestelling zegt nu dat

$$R[X]/XR[X] \cong R.$$

iii) Laat p een priemgetal zijn en laat $I = (p, X)$ het door p en X voortgebrachte ideaal van $\mathbb{Z}[X]$ zijn. We passen nu de Derde Isomorfiestelling toe met $I = (p)$, $J = (p, X)$. Deze zegt dat

$$\mathbb{Z}[X]/(p, X) \cong (\mathbb{Z}[X]/p\mathbb{Z}[X])/((p, X)/(p\mathbb{Z}[X])$$

Uit het eerste voorbeeld weten we nu dat $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$ en het beeld van het ideaal (p, X) in deze ring is het ideaal (X). We zien dus dat

$$(\mathbb{Z}[X]/p\mathbb{Z}[X])/((p, X)/(p\mathbb{Z}[X]) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(X),$$

en met voorbeeld ii) zien we dat deze laatste ring isomorf is met $\mathbb{Z}/p\mathbb{Z}$. Een alternatieve methode bestaat erin te bewijzen dat de kern van het surjectieve homomorfisme

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad \text{gegeven door } f \mapsto f(0)$$

gelijk is aan (p, X). Met behulp van de Eerste Isomorfiestelling volgt het resultaat dan ook.

De Chinese Reststelling voor de groepen $\mathbb{Z}/n\mathbb{Z}$ laat zich ook generalizeren tot de volgende stelling.

(3.9) Stelling. *(Chinese Reststelling) Laat R een commutatieve ring met 1 zijn en I en J twee idealen die onderling ondeelbaar zijn: $I + J = R$. Dan geldt $IJ = I \cap J$ en er is een ringisomorfisme*

$$R/(IJ) \cong (R/I) \times (R/J).$$

Bewijs. Er geldt vanwege de definitie van IJ dat $IJ \subseteq I \cap J$. Wegens de aanname $I + J = R$ zijn er elementen $x \in I$ en $y \in J$ zodat $1 = x + y$. Laat nu $z \in I \cap J$. Uit $z = z \cdot 1 = zx + zy$ volgt dat $z \in IJ$. Verder geeft de afbeelding

$$\phi : R \longrightarrow (R/I) \times (R/J), \quad x \mapsto (x \bmod I, x \bmod J),$$

een ringhomomorfisme met kern $I \cap J = IJ$. We laten nu zien dat ϕ surjectief is. Laat $(a \bmod I, b \bmod J)$ een element van $(R/I) \times (R/J)$ zijn. Neem dan het element $z = ay + bx \in R$ met $x \in I$ en $y \in J$ zodat $1 = x + y$. Een kleine berekening leert nu

$$z = ay + bx \equiv a \,(\mathrm{mod} I)$$

en evenzo

$$z = ay + bx \equiv b \,(\mathrm{mod} J).$$

Dus volgt $\phi(z) = (a \bmod I, b \bmod J)$. (Opmerking: als we IJ vervangen door $(IJ + JI)$ in de stelling geldt het isomorfisme ook voor niet-commutatieve ringen.)

(3.10) Gevolg. *Laat m en n twee onderling ondeelbare getallen zijn (*$\mathrm{ggd}(m, n) = 1$*).*

i) Er is een isomorfisme van ringen

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

ii) Er is een isomorfisme van groepen

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

Merk op dat ii) uit (1.20) volgt.

Nu heeft (3.10) tot gevolg dat de Euler phi-functie *multiplicatief* is, d.w.z., zijn m en n twee positieve onderling ondeelbare getallen dan

$$\phi(mn) = \phi(m)\phi(n).$$

Immers, $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. We verwijzen naar Opgave 10 voor een expliciete formule voor de Euler phi-functie.

(3.11) Voorbeeld. Laat $R = \mathbb{C}[X]$ en $I = (X + i)$ en $J = (X - i)$. Er geldt

$$1 = \frac{i}{2}(X - i) + \frac{-i}{2}(X + i).$$

Dus I en J zijn ondeelbaar en we vinden zo $IJ = (X^2 + 1)$ en een isomorfisme

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

In het volgende hoofdstuk zullen we zien dat $\mathbb{C}[X]/(X - i) \cong \mathbb{C}[X]/(X + i) \cong \mathbb{C}$, zodat $\mathbb{C}[X]/(X^2 + 1) \cong \mathbb{C} \times \mathbb{C}$.

Opgaven

1) Bewijs Stelling (3.6).

2) Laat $f : R \to R'$ een ringhomomorfisme zijn en I' een ideaal van R'. Laat zien dat $f^{-1}(I')$ een ideaal van R is en dat $R/f^{-1}(I')$ isomorf is met een deelring van R'/I'.

3) Bewijs dat de quotiëntring $k[X]/(X^2)$ isomorf is met de ring van de duale getallen.

4) Laat R een commutatieve ring met 1 zijn. Een idempotent van R is een element $e \in R$ met $e^2 = e$. Triviale voorbeelden zijn 0 en 1. Laat nu zien dat als e een idempotent is, dat ook $1 - e$ een idempotent is. Laat verder zien dat

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

5) Bepaal de idempotenten van de ring $\mathbb{Z}/350\mathbb{Z}$.

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

7) Laat zien dat $\mathbb{Z}[X]/(X^2 - 1)$ niet isomorf is met $\mathbb{Z} \times \mathbb{Z}$.

8) Laat R de deelring $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y(\mathrm{mod}2)\}$ van $\mathbb{Z} \times \mathbb{Z}$ zijn. Bewijs het ringisomorfisme $\mathbb{Z}[X]/(X^2 - 1) \cong R$.

9) Laat R een commutatieve ring zijn. Een element $x \in R$ heet *nilpotent* als $x^n = 0$ voor een positief geheel getal n. Laat zien dat als x en y nilpotent zijn, ook $x + y$ nilpotent is. Laat verder zien dat de nilpotente elementen een ideaal vormen.

10) Laat R een ring zijn met 1. Laat voor $[R, R]$ het ideaal zijn van R voortgebracht door alle uitdrukkingen $(xy - yx)$ met $x, y \in R$. Bewijs dat $R/[R, R]$ een commutatieve ring is. Bewijs verder de volgende *universele eigenschap* van $R/[R, R]$. Als R' een commutatieve ring is en $f : R \to R'$ een homomorfisme dan is er een eenduidig bepaald homomorfisme $h : R/[R, R] \to R'$ met $h(x + [R, R]) = f(x)$.

11) Bewijs de volgende formule voor de Euler phi-functie:

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

waar het product over alle priemdelers van n loopt.

12) Bewijs dat de ring $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ isomorf is met de volgende deelring R van $\mathrm{Mat}(2, \mathbb{Z})$:

$$R = \{\begin{pmatrix} a & 5b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}\}.$$

13) Laat zien dat de quotiëntring $(\mathbb{Z}/5\mathbb{Z})[X]/(X^2 + 2X + 2)$ geen lichaam is.

14) Bepaal het aantal elementen van de volgende ringen: $\mathbb{Z}[i]/(1 + i)$, $\mathbb{Z}[i]/(2 + i)$ en $\mathbb{Z}[X]/(X^2 - 3, 2X + 4)$. Beschrijf de structuur van de laatste ring.

15) Bereken $\phi(2000)$, $\phi(2001)$ en $\phi(2002)$.

16) Laat R een commutatieve ring met 1 zijn en I een ideaal van R. Laat $J = IR[X]$ het door I voortgebrachte ideaal in $R[X]$ zijn. Bewijs het isomorfisme $R[X]/J \cong (R/I)[X]$.

17) Laat R een ring en $I = (x, y)$ een ideaal van R. Laat zien dat $R/I \cong R/(x, y + rx)$ voor alle $r \in R$.

4. Veeltermringen

On peut dire que l'origine historique et un des buts essentiels de l'Algèbre, depuis les Babyloniens, les Hindous et Diophante jusqu'à nos jours, est l'étude des solutions de systèmes d'équations polynomiales.

A. Grothendieck* en J. Dieudonné**

In dit hoofdstuk zullen we ons bezighouden met polynomen en hun nulpunten. We zullen er, zoals aan het begin van het vorige hoofdstuk is opgemerkt, in het vervolg van uitgaan dat al onze ringen een eenheidselement bezitten.

Het fundamentele resultaat over polynoomringen is de *deling met rest* analoog aan de deling met rest in $\mathbb{Z}$.

(4.1) Stelling. (Deling met rest) *Laat R een ring zijn en f en g veeltermen uit $R[X]$. Neem aan dat de kopcoëfficiënt van g een eenheid in R is. Dan bestaan er eenduidig bepaalde veeltermen q en r in $R[X]$ zodat*

$$f = qg + r \quad \text{met } r = 0 \text{ of } \deg(r) < \deg(g).$$

Bewijs. We moeten zowel de existentie als ook de eenduidigheid van q en r laten zien. We beginnen met de existentie. We schrijven $g = b_m X^m + b_{m-1}X^{m-1} + \ldots + b_1 X + b_0$ met $b_m \in R^*$. Als $f = 0$ kunnen we $q = r = 0$ nemen. We mogen dan aannemen dat $f \neq 0$ en voeren inductie naar de graad van f. Als $\deg(f) < \deg(g)$ kunnen we $q = 0$ en $r = f$ nemen. Als we de existentie hebben laten zien in het geval dat $\deg(f) < n$ en we nemen nu een $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ met $a_n \neq 0$ en $n \geq m = \deg(g)$ dan heeft

$$f' = f - a_n b_m^{-1} X^{n-m} g = (a_{n-1} - a_n b_m^{-1} a_{n-1})X^{n-1} + \ldots$$

een lagere graad dan f en met inductie kunnen we schrijven

$$f' = q'g + r' \quad \text{met } r' = 0 \quad \text{of} \quad \deg(r') < \deg(g).$$

Dus vinden we

$$f = f' + a_n b_m^{-1} X^{n-m} g = (q' + a_n b_m^{-1} X^{n-m})g + r'.$$

met $r' = 0$ of $\deg(r') < \deg(g)$ zoals gewenst. Hiermee is de existentie van q en r aangetoond.

Stel nu dat $f = qg + r = q_1 g + r_1$, waarbij $\deg(r) < \deg(g)$ (resp. $\deg(r_1) < \deg(g)$ of $r = 0$ (resp. $r_1 = 0$). Er geldt dan

$$(q - q_1)g = r - r_1$$

---

* A. Grothendieck, geboren in Berlijn in 1928, statenloos wiskundige, een revolutionair vernieuwer van de wiskunde, wellicht de belangrijkste wiskundige van de twintigste eeuw

** J.A. Dieudonné, Frans wiskundige, 1906-1992. Hij schreef samen met Grothendieck 'Eléments de Géométrie Algebrique.'

en omdat de kopcoëfficiënt van g een eenheid is (en dus geen nuldeler) is de graad van $(q-q_1)g$ groter of gelijk aan $\deg(g)$ als $q-q_1 \neq 0$. Anderzijds is ofwel $r-r_1=0$ of $\deg(r-r_1) < \deg(g)$. We zien dus dat $r=r_1$ en $q=q_1$ en daarmee is de eenduidigheid bewezen.

(4.2) Voorbeeld. Als $R=\mathbb{Z}$ en $g=X^2+X+1$ dan vinden we voor $f=X^6+6X^5+6X^4+5X^3+7X^2+1$ met een 'staartdeling'

$$\begin{array}{rl} X^2+X+1/ & X^6+6X^5+6X^4+5X^3+7X^2+1 \backslash X^4+5X^3+7 \\ & X^6+X^5+X^4 \\ & \quad ------ \\ & \quad 5X^5+5X^4+5X^3+7X^2+1 \\ & \quad 5X^5+5X^4+5X^3 \\ & \quad ---------- \\ & \qquad\qquad 7X^2+1 \\ & \qquad\qquad 7X^2+7X+7 \\ & \qquad\qquad ------- \\ & \qquad\qquad\quad -7X-6 \end{array}$$

zodat $q=X^4+5X^3+7$ en $r=-7X-6$.

We kunnen hiermee voor polynoomringen over lichamen informatie krijgen zoals we met deling met rest voor de ring van de gehele getallen deden.

(4.3) Stelling. *Als k een lichaam is dan is ieder ideaal van $k[X]$ een hoofdideaal.*

Bewijs. Omdat k een lichaam is, is iedere kopcoëfficiënt van een polynoom $f \neq 0$ een eenheid. Laat I een ideaal van $k[X]$ zijn. Als $I=\{0\}$ dan is I ten duidelijkste een hoofdideaal. Laat nu $I \neq \{0\}$ en neem een element $g \neq 0$ van minimale graad in I. We beweren dat dit element het ideaal I voortbrengt. Laat $f \in I$ een willekeurig element zijn. Dan kunnen we schrijven $f=qg+r$ met $r=0$ of $\deg(r) < \deg(g)$. Nu ligt het element $r=f-qg$ in I en kan geen graad kleiner dan $\deg(g)$ hebben, dus moet $r=0$ gelden, d.w.z. $f=qg$. Hieruit volgt $I=(g)$.

(4.4) Propositie. *Laat R een commutatieve ring zijn en $a \in R$ een element van R.*

i) Voor ieder polynoom $f \in R[X]$ is er een $q \in R[X]$ zodat

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

ii) De substitutieafbeelding $R[X] \longrightarrow R$ gegeven door $f \mapsto f(a)$ definieert een isomorfisme

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

Bewijs. Volgens de Deling met Rest kunnen we schrijven $f=q(X-a)+r$, waar $r=0$ of $\deg(r) < \deg(X-a)=1$. Dus is r een constante in R en om r te berekenen substitueren we $X=a$. Dan vinden we

$$f(a) = q\,0 + r, \quad \text{dus } r=f(a).$$

De substitutieafbeelding is een surjectief ringhomomorfisme $R[X] \longrightarrow R$ zoals we hiervoor al zagen. (Hier wordt de commutativiteit van R gebruikt.) Volgens i) is de kern hiervan precies het ideaal $(X - a)$. Dus de Eerste Isomorfiestelling bewijst nu ii).

We zien dus dat uitdelen van $R[X]$ naar een ideaal voortgebracht door een lineair polynoom $X - a$ de ring R oplevert. Uitdelen naar hoofdidealen voortgebracht door hogere-graads polynomen kan veel interessante ringen opleveren zoals we later uitgebreid zullen zien. We geven hier nu een speciaal voorbeeld.

(4.5) Propositie. *Laat $i = \sqrt{-1} \in \mathbb{C}$. Dan levert de substitutieafbeelding*

$$\psi : \mathbb{R}[X] \longrightarrow \mathbb{C}, \qquad f \mapsto f(i)$$

een isomorfisme

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

Bewijs. De lezer kan gemakkelijk nagaan dat ψ een surjectief homomorfisme is. We gaan bewijzen dat de kern van ψ gelijk is aan het hoofdideaal (X^2+1). Duidelijk is dat $X^2 + 1 \in \ker(\psi)$. Laat nu f een willekeurig element van $\ker(\psi)$ zijn. Volgens Deling met Rest kunnen we schrijven

$$f = q(X^2 + 1) + r \qquad \text{met } r = 0 \text{ of } \deg(r) < 2 = \deg(X^2 + 1)$$

Substitutie van i levert $r(i) = 0$. Als r een lineair polynoom is, zeg $r = r_0 + r_1 X$ dan $r(i) = r_0 + r_1 i$ en omdat $r_0, r_1 \in \mathbb{R}$ betekent dit dat $i = -r_0/r_1 \in \mathbb{R}$ als $r_1 \neq 0$. Dat kan niet. Hieruit volgt $r_0 = r_1 = 0$ en dus $f \in (X^2 + 1)$. Volgens de Eerste Isomorfiestelling volgt nu de bewering.

Bovenstaande propositie maakt het mogelijk op een puur algebraïsche manier het lichaam van de complexe getallen in te voeren door te stellen

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

Het element i is dan de restklasse van X in deze quotiëntring.

(4.6) Definitie. Laat R een ring zijn en $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ een polynoom. We zeggen dat $a \in R$ een nulpunt is van f als

$$f(a) = a_0 + a_1 a + a_2 a^2 + \ldots + a_n a^n = 0.$$

(4.7) Stelling. *Laat R een domein zijn en $f \in R[X]$. Als $a_1, \ldots, a_m$ verschillende nulpunten van f zijn dan is er een polynoom $q \in R[X]$ zodat*

$$f = q \cdot (X - a_1)(X - a_2) \ldots (X - a_m).$$

Bewijs. We voeren inductie naar m. Als $m = 0$ dan is de stelling waar (met $q = f$). Veronderstel nu dat de stelling bewezen is voor $< m$ verschillende nulpunten en veronderstel dat ons polynoom m verschillende nulpunten a_i $(i = 1, \ldots, m)$ heeft. Vanwege Propositie (4.4) kunnen we schrijven

$$f = f_1 \cdot (X - a_m). \tag{1}$$

met $f_1 \in R[X]$. Voor $i = 1, \ldots, m-1$ levert substitutie van a_i in (1) dat

$$(a_i - a_m) f_1(a_i) = 0$$

en omdat R een domein is en dus geen nuldelers heeft volgt $f_1(a_i) = 0$. Toepassen van de inductieveronderstelling op f_1 levert

$$f_1 = q \cdot (X - a_1)(X - a_2) \ldots (X - a_{m-1})$$

met $q \in R[X]$. Dus we zien dat $f = f_1(X - a_m)$ de gevraagde schrijfwijze heeft.

(4.8) Gevolg. *Laat $f \in R[X]$ een polynoom zijn van graad d en $f \neq 0 \in R[X]$. Als R een domein is dan heeft f hoogstens d verschillende nulpunten.*

Bewijs. Als $a_1, \ldots, a_m$ verschillende nulpunten van f zijn kunnen we schrijven

$$f = q \cdot (X - a_1)(X - a_2) \ldots (X - a_m)$$

met $q \in R[X]$ en hieruit volgt dat de graad $\deg(f)$ groter of gelijk aan m is. Dit bewijst de bewering.

Als voorbeeld nemen we het polynoom $X^n - 1 \in \mathbb{C}[X]$. De n complexe getallen $e^{2\pi i a/n} = \cos(2a\pi/n) + i \sin(2a\pi/n)$ voor $a = 1, \ldots, n$ zijn n verschillende nulpunten. Er zijn dus geen andere nulpunten. Deze nulpunten heten de n-de machts eenheidswortels.

Een polynoom van graad d met coëfficiënten in een domein R kan dus hoogstens d verschillende nulpunten hebben, maar in het algemeen zullen het er minder zijn. Zo heeft het polynoom $X^2 + 1 \in \mathbb{Z}[X]$ geen nulpunten in $\mathbb{Z}$. Of eenvoudiger nog, het polynoom $5X - 7 \in \mathbb{Z}[X]$ heeft geen nulpunt in $\mathbb{Z}$. Ook het polynoom $X^2 - 2 \in \mathbb{Q}[X]$ heeft geen nulpunt in $\mathbb{Q}$. Verder heeft $X^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ maar één nulpunt in $\mathbb{Z}/2\mathbb{Z}$ (er geldt $X^2 + 1 = (X + 1)^2$ in deze ring).

Als R geen domein is kan een polynoom van graad d meer dan d nulpunten hebben; bijvoorbeeld heeft het polynoom $X^2 + 1$ in $\mathbb{H}[X]$ met $\mathbb{H}$ de quaternionen *oneindig veel* nulpunten, zie Opgave 10. Ga na dat het polynoom $X^2 - 1 \in (\mathbb{Z}/12\mathbb{Z})[X]$ precies vier nulpunten heeft, nl. $\bar{1}, \bar{5}, \bar{7}, \bar{11}$.

Om meervoudige nulpunten (of wortels) van polynomen te detecteren maken we gebruik van de *afgeleide* van een polynoom.

(4.9) Definitie. Laat R een commutatieve ring zijn en $f \in R[X]$ een polynoom, zeg van de vorm

$$f = a_0 + a_1 X + \ldots + a_n X^n.$$

De *afgeleide* van f is het polynoom

$$f' := \sum_{i=0}^{n} i a_i X^{i-1} = a_1 + 2a_2 X + \ldots + (n-1) a_{n-1} X^{n-2} + n a_n X^{n-1} \quad \in R[X].$$

Deze puur algebraïsche definitie van het nemen van de afgeleide voldoet weer aan de bekende regels van Leibniz die we kennen uit de analyse.

(4.10) Lemma. *Laat R een commutatieve ring zijn en $f, g \in R[X]$. Dan gelden de volgende rekenregels.*
i) $(f+g)' = f' + g'$.
ii) $(cf)' = cf'$ *voor alle* $c \in R$.
iii) $(fg)' = f'g + fg'$.

Bewijs. De controle van i) en ii) is eenvoudig en wordt aan de lezer overgelaten. We controleren nu iii) en schrijven

$$f = a + 0 + a_1X + \ldots + a_nX^n \quad \text{en} \quad g = b_0 + b_1X + \ldots + b_mX^m.$$

We voeren inductie naar de graad van f. Als f constant is hebben we $f' = 0$ en iii) volgt dan uit ii). Veronderstel nu dat $\deg(f) = n > 0$. Als we schrijven $f = f_1 + a_nX^n$ met $\deg(f_1) < n$ dan geldt

$$(fg)' = (a_nX^ng)' + (f_1g)'$$

vanwege i). Met de inductieaanname volgt $(f_1g)' = f_1'g + f_1g'$. We doen een eenvoudige berekening

$$\begin{aligned}(X^ng)' &= (b_0X^n + b_1X^{n+1} + \ldots + b_mX^{n+m})' \\ &= \sum_{i=0}^{m}(n+i)b_iX^{n-1+i} \\ &= nX^{n-1}g + X^ng'\end{aligned}$$

en zien dus door nu i) te gebruiken

$$\begin{aligned}(fg)' &= a_n(nX^{n-1}g + X^ng') + (f_1'g + f_1g') \\ &= f'g + fg'.\end{aligned}$$

Dit bewijst het lemma.

(4.11) Definitie. Laat R een domein zijn, $f \in R[X]$ een polynoom en $a \in R$ een nulpunt van f. We zeggen dat a een dubbel nulpunt van f is als in de schrijfwijze $f = f_1 \cdot (X - a)$ van (4.4) geldt $f_1(a) = 0$.

(4.12) Propositie. *Laat R een domein zijn en $f \in R[X]$. Het element $a \in R$ is een dubbel nulpunt van f dan en slechts dan als $f(a) = 0$ en $f'(a) = 0$.*

Bewijs. Als a een nulpunt is van f geldt $f = f_1(X - a)$ met $f_1 \in R[X]$. Differentiëren met gebruik van (4.10) iii) geeft

$$f' = f_1'(X - a) + f_1$$

Substitutie van a hierin levert $f'(a) = f_1(a)$. Dit laat zien dat een nulpunt a precies dan een dubbel nulpunt is als $f'(a) = 0$.

Als voorbeeld nemen we het polynoom $f = X^p - a \in (\mathbb{Z}/p\mathbb{Z})[X]$. Omdat $a^p = a$ in $\mathbb{Z}/p\mathbb{Z}$ (Fermat) is a een nulpunt. Volgens Propositie (4.12) is dit een dubbel nulpunt want de afgeleide is $pX^{p-1} = 0$. Er geldt zelfs $X^p - a = (X - a)^p$ (Ga na), met andere woorden, a is een p-voudig nulpunt.

Laat nu p een priemgetal in $\mathbb{Z}$ zijn en beschouw $\mathbb{Z}/p\mathbb{Z}$. We hebben al gezien dat dit een lichaam is en we schrijven

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

Als verdere illustratie van het thema nulpunten bekijken we nu de factorisatie van $X^p - X$ in $\mathbb{F}_p[X]$.

(4.13) Stelling. *In de polynoomring $\mathbb{F}_p[X]$ geldt de identiteit*

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

Bewijs. Volgens de stelling van Fermat geldt voor ieder geheel getal a dat $a^p \equiv a \pmod{p}$. Dus alle p restklassen $\bar{x}$ modulo p zijn een nulpunt. Omdat $\mathbb{F}_p$ een domein is volgt

$$X^p - X = q \cdot (X - \bar{0})(X - \bar{1}) \ldots (X - \overline{p-1})$$

met $q \in \mathbb{F}_p[X]$. Vergelijken van de graad levert dat q een constant polynoom is en vergelijken van de kopcoëfficiënten levert $q = 1$.

(4.14) Gevolg. *(Stelling van Wilson)* Laat p een priemgetal zijn. Dan geldt*

$$(p-1)! \equiv -1 \pmod{p}.$$

Bewijs. Analoog aan het voorgaande ziet men gemakkelijk in dat

$$X^{p-1} - 1 = \prod_{i=1}^{p-1} (X - \bar{i}) \text{ in } \quad \mathbb{F}_p[X].$$

Substitutie van $X = \bar{0}$ levert

$$(-\bar{1})(-\bar{2}) \cdot \ldots \cdot (-\overline{p-1}) = -\bar{1}.$$

Als p een oneven priemgetal is dan staat er links een even aantal mintekens en het resultaat volgt. Voor $p = 2$ is het ook evident.

(4.15) Propositie. *Laat R een domein zijn en G een eindige ondergroep van R^*. Dan is G cyklisch.*

Bewijs. Omdat R een domein is, is R commutatief en R^* dus een abelse groep. Laat x nu een element van maximale orde in G zijn, zeg zijn orde is m. We beweren nu dat ieder element van G aan de identiteit $y^m = 1$ voldoet. Zie Opgave 16. Dus alle elementen van G zijn nulpunten van het polynoom $X^m - 1 \in R[X]$. Wegens (4.8) volgt dat

$$m = \deg(X^m - 1) \geq \#G.$$

Maar anderzijds bevat G de ondergroep $\langle x \rangle$ en die heeft m elementen. Dus $\#G = m$ en $G = \langle x \rangle$, met andere woorden x is een voortbrenger van G.

* John Wilson, Engels wiskundige, 1741-1793, aan wie deze bewering wordt toegeschreven, maar die waarschijnlijk geen bewijs voor deze stelling kende.

(4.16) Gevolg. *Laat p een priemgetal zijn. De groep $(\mathbb{Z}/p\mathbb{Z})^*$ is cyklisch.*

We leiden nu een gevolg af.

(4.17) Propositie. *Laat $p > 2$ een priemgetal zijn. Dan zijn de twee volgende beweringen equivalent:*

i) Er bestaat een $a \in \mathbb{Z}$ met $a^2 \equiv -1 \pmod{p}$;

ii) $p \equiv 1 \pmod{4}$.

Bewijs. Uit i) volgt dat $\bar{a}$ orde 4 in $(\mathbb{Z}/p\mathbb{Z})^*$ heeft. Dus moet 4 de orde $p-1$ van $(\mathbb{Z}/p\mathbb{Z})^*$ delen. Dus volgt ii). Omgekeerd, als $p \equiv 1 (\mathrm{mod} 4)$ dan deelt 4 de orde van $(\mathbb{Z}/p\mathbb{Z})^*$. Omdat $(\mathbb{Z}/p\mathbb{Z})^* \cong \langle g \rangle$ een cyklische groep is, is er dan ook een element $\bar{a}$ van orde 4, namelijk $g^{(p-1)/4}$. Er geldt $\bar{a}^4 - \bar{1} = (\bar{a}^2 - 1)(\bar{a}^2 + 1) \equiv 0 (\mathrm{mod}\, p)$. Omdat $\bar{a}^2 \not\equiv 1 (\mathrm{mod}\, p)$ en omdat $\mathbb{Z}/p\mathbb{Z}$ een domein is volgt $\bar{a}^2 = -1$.

Een geheel getal x zodat $\bar{x}$ een voortbrenger van de cyklische groep $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ is heet een *primitieve wortel* modulo p. Het aantal restklassen modulo p dat een voortbrenger van $\mathbb{F}_p^*$ is is gelijk aan $\phi(p-1)$ met ϕ de Euler-phi functie. Het is in het algemeen niet gemakkelijk om een primitieve wortel modulo p te vinden.

Hebben we een primitieve wortel g modulo p gevonden dan geeft dit een isomorfisme van groepen

$$\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}, \quad g^i \mapsto i (\mathrm{mod}\, (p-1))$$

wat de vermenigvuldiging in een optelling vertaalt en dit isomorfisme functioneert als een soort logaritme.

Opgaven

1) Bepaal de nulpunten van $X^2 - 1$ in $(\mathbb{Z}/36\mathbb{Z})[X]$.

2) Laat $f = 3X^2 + 1 \in (\mathbb{Z}/6\mathbb{Z})[X]$ en $g = 2X + 1 \in (\mathbb{Z}/6\mathbb{Z})[X]$. Bewijs dat er geen polynomen q en r in $(\mathbb{Z}/6\mathbb{Z})[X]$ als in (4.1) bestaan met $f = qg + r$.

3) Geef een $n \in \mathbb{Z}_{>1}$ aan zodat $(\mathbb{Z}/n\mathbb{Z})^*$ niet cyklisch is.

4) Bereken voor ieder positief geheel getal n en priemgetal p de uitdrukking

$$1^n + 2^n + \ldots + (p-1)^n \pmod{p}.$$

5) Laat R een domein zijn en f en g polynomen met $\deg(f) < \#R$ en $\deg(g) < \#R$. Laat zien dat $f = g$ dan en slechts dan als $f(x) = g(x)$ voor alle $x \in R$.

6) Laat p een priemgetal zijn en $f, g \in (\mathbb{Z}/p\mathbb{Z})[X]$. Laat zien dat $f(x) = g(x)$ voor alle $x \in \mathbb{Z}/p\mathbb{Z}$ dan en slechts dan als $f - g \in (X^p - X)$.

7) Bewijs het lichaamsisomorfisme $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2 + 1)$.

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

9) Bepaal voor alle priemgetallen p met $19 \leq p \leq 47$ de kleinste $x > 0$ die een primitieve wortel is modulo p.

10) Laat $x = a + bi + cj + dk \in \mathbb{H}$ met $a, b, c, d \in \mathbb{R}$. Laat zien dat de volgende uitspraken equivalent zijn.

i) $x\bar{x} = 1$ en $\bar{x} = -x$.

ii) $a = 0$ en $b^2 + c^2 + d^2 = 1$.
iii) x is een nulpunt van het polynoom $X^2 + 1 \in \mathbb{H}[X]$.

11) Bewijs dat de volgende uitspraken voor een polynoom $f \in \mathbb{F}_2[X]$ equivalent zijn.
i) Er is een $g \in \mathbb{F}_2[X]$ met $g^2 = f$
ii) De afgeleide van f voldoet aan $f' = 0$
iii) f is van de vorm $\sum_{i=0}^{n} a_i X^{2i}$.

12) Bewijs dat $\mathbb{F}_p[X]/(X^2+1)$ geen lichaam is als $p \equiv 1 (\mathrm{mod} 4)$. Laat verder zien dat $\mathbb{F}_3[X]/(X^2+1)$ wel een lichaam is.

13) *De structuur van $(\mathbb{Z}/p^n\mathbb{Z})^*$ voor p een oneven priem.*
i) Laat $i \in \mathbb{Z}_{\geq 0}$. Laat zien dat geldt

$$(1+p)^{p^i} \equiv 1 + p^{i+1} \,(\mathrm{mod}\, p^{i+2}).$$

ii) Bewijs dat de orde van $1 + p \in (\mathbb{Z}/p^n\mathbb{Z})^*$ gelijk is aan p^{n-1}.
iii) Laat x een primitieve wortel modulo p zijn (d.w.z. $\langle \bar{x} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$). Laat zien dat de orde van $\bar{x} \in (\mathbb{Z}/p^n\mathbb{Z})^*$ deelbaar is door $p - 1$.
iv) Laat zien dat $(\mathbb{Z}/p^n\mathbb{Z})^*$ een element u van orde $p - 1$ bezit.
v) Laat zien dat $(p+1)u$ orde $(p-1)p^{n-1}$ heeft in $(\mathbb{Z}/p^n\mathbb{Z})^*$.
vi) Bewijs dat $(\mathbb{Z}/p^n\mathbb{Z})^*$ een cyklische groep is en isomorf met $\mathbb{Z}/(p-1)p^{n-1}\mathbb{Z}$.

14) *De structuur van $(\mathbb{Z}/2^n\mathbb{Z})^*$.*
i) Bewijs $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ en $(\mathbb{Z}/8\mathbb{Z})^* \cong V_4$, de Viergroep van Klein.
ii) Bereken het element $(1+4)^{2^{n-3}} \in (\mathbb{Z}/2^n\mathbb{Z})^*$ en laat zien dat 5 orde 2^{n-2} heeft voor $n \geq 2$.
iii) Laat zien dat 5 en -1 de groep $(\mathbb{Z}/2^n\mathbb{Z})^*$ voortbrengen.
iv) Laat zien dat $-1 \notin \langle 5 \rangle$.
v) Bewijs het isomorfisme

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

15) Laat $n \in \mathbb{Z}_{>1}$ een oneven getal zijn. Bewijs dat $X^2 - 1 \in (\mathbb{Z}/n\mathbb{Z})[X]$ precies 2^t verschillende nulpunten heeft in $(\mathbb{Z}/n\mathbb{Z})$, waarbij t het aantal verschillende priemdelers van n is.

16) Laat G een eindige abelse groep zijn en laat m de maximale orde van een element van G zijn. Bewijs dat de orde van ieder element van G een deler van m is.

17) Laat n een geheel getal > 1 zijn. Bewijs dat $(\mathbb{Z}/n\mathbb{Z})^*$ cyklisch is dan en slechts dan als $n \in \{2, 4, p^k, 2p^k : p \quad \text{oneven priem}, k \geq 1\}$.

18) Laat n een positief geheel getal zijn en d een deler van n. Bewijs: de afbeelding $\alpha : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ gegeven door $x \bmod n \mapsto x \bmod d$ is een surjectief groepshomomorfisme.

5. Priemidealen en Maximale Idealen

Dieser letzter Satz rechtfertigt die Benennung idealer Primfactor *volkommen, denn man kann mit ihnen nun wie mit numerischen ganzzahligen Primfactoren rechnen.*

(E.E. Kummer *, in een brief van 18 oktober 1845 aan Kronecker)

(5.1) Afspraak. In dit hoofdstuk zijn de ringen steeds commutatief met eenheidselement.

We gaan nu het begrip *priemgetal* dat we kennen voor de ring van gehele getallen $\mathbb{Z}$ generalizeren. Dit doen we door niet zozeer naar een element p zelf, als wel naar het ideaal (p) dat door dit element wordt voortgebracht te kijken.

(5.2) Definitie. Laat R een commutatieve ring met 1 zijn. Een *priemideaal* van R is een ideaal I van R dat voldoet aan

i) $I \neq R$;
ii) voor alle $x, y \in R$ met $xy \in I$ geldt $x \in I$ of $y \in I$.

Merk op dat dit een generalisatie is van de regel dat als $p \in \mathbb{Z}$ een priemgetal is en p deelt xy dan deelt p of x of y. Vertaald in idealen betekent dit immers

$$xy \in (p) \quad \Rightarrow \quad x \in (p) \quad \text{of} \quad y \in (p).$$

(5.3) Voorbeelden.

i) In de ring $\mathbb{Z}$ is ieder ideaal een hoofdideaal. Het ideaal (0) is een priemideaal, want als $xy = 0$ dan is $x = 0$ of $y = 0$. Verder is ieder ideaal (p) met p een priemgetal een priemideaal zoals zojuist werd uitgelegd. Een ideaal (n) met n niet priem (samengesteld) is geen priemideaal: als $n = ab$ met $1 < a, b < n$ dan $a \notin (n)$ en $b \notin (n)$.
ii) In de ring $\mathbb{Q}[X]$ is het ideaal $(X^2 + 1)$ een priemideaal. Laat f, g polynomen zijn in $\mathbb{Q}[X]$ met $fg \in I$. Volgens het bewijs van (4.5) is I precies de kern van het homomorfisme $f \mapsto f(i)$. Het gegeven $fg \in I$ betekent dus $fg(i) = 0$, dus $f(i)g(i) = 0$. Maar daaruit volgt dat $f(i) = 0$ of $g(i) = 0$ en dus $f \in I$ of $g \in I$.
iii) In de ring $\mathbb{Q}[X]$ is het ideaal $I = (X^2-1)$ geen priemideaal. Immers $(X+1)(X-1) \in I$, maar $X - 1 \notin I$ zoals we zien door naar de graad te kijken.

We geven nu een handig criterium om te beslissen of een ideaal een priemideaal is.

---

* Ernst Eduard Kummer, Duits wiskundige, 1810-1893

(5.4) Stelling. *Laat I een ideaal van een commutatieve ring R met eenheidselement zijn. Dan geldt:*

$$I \quad \text{is een priemideaal} \iff \quad R/I \quad \text{is een domein.}$$

Bewijs. Om te controleren of R/I een domein is moeten we nagaan dat $\bar{1} \neq \bar{0}$ en dat R/I geen nuldelers heeft. Merk op: $\bar{x} = 0$ in R/I dan en slechts dan als $x \in I$. Hier schrijven we $\bar{x}$ voor de nevenklasse $x + I$ in R/I. Maar nu geldt

$$\bar{1} \neq \bar{0} \iff 1 \notin I \iff I \neq R$$

en dit is precies conditie i) van definitie (5.2). Verder geldt:

$$\begin{aligned} R/I \text{ is nuldelervrij} &\iff \text{als } \bar{x}, \bar{y} \in R/I \text{ met } \bar{x}\bar{y} = 0 \text{ dan } \bar{x} = 0 \text{ of } \bar{y} = 0 \\ &\iff \text{als } x, y \in R \text{ met } xy \in I \text{ dan } x \in I \text{ of } y \in I \end{aligned}$$

en dit is precies conditie ii) van (5.2). Dus we zien dat I een priemideaal is dan en slechts dan als R/I een domein is.

(5.5) Gevolg. *R is een domein dan en slechts dan als (0) een priemideaal is.*

Bewijs. Pas de stelling toe met $I = (0)$.

(5.6) Voorbeelden.

i) Laat $R = \mathbb{Q}[X, Y]$ en laat $I = (X^2 - Y)$. Dan zien we dat $R/I \cong (\mathbb{Q}[X])[Y]/(Y - X^2)$ en toepassen van Propositie (4.4) (met $R = \mathbb{Q}[X]$ en $a = X^2$) levert $R/I \cong \mathbb{Q}[X]$. Dit is een domein, dus I is een priemideaal.

ii) Laat $R = \mathbb{Z}[X]$ en $I = (p, X)$ met p een priemgetal. We hebben al gezien dat R/I isomorf is met $\mathbb{Z}/p\mathbb{Z}$ en dit is een lichaam, dus zeker een domein. Daarmee zien we dat (p, X) een priemideaal is.

iii) Laat $R = \mathbb{C}[X, Y]$ en $I = (X^2 - Y, X^2 + Y)$. Dan vinden we $R/I \cong \mathbb{C}[X]/(X^2)$. Omdat $X \cdot X \in (X^2)$, maar $X \notin (X^2)$ zien we in dat I geen priemideaal is.

iv) Laat $R = \mathbb{Z}[i]$ en (5) het ideaal voortgebracht door 5. Dit is geen priemideaal want er geldt

$$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[X]/(X^2 + 1, 5) \cong (\mathbb{Z}/5\mathbb{Z})[X]/(X^2 + 1)$$

en er geldt $X^2 + 1 \equiv (X + 2)(X + 3) \bmod 5$. Dus $(X + \bar{2})(X + \bar{3}) \in (X^2 + \bar{1}) \subset \mathbb{Z}/5\mathbb{Z}[X]$, maar $X + \bar{2} \notin (X^2 + \bar{1})$ en $X + \bar{3} \notin (X^2 + \bar{1})$. (Of gebruik dat de idealen $J_1 = (X + \bar{2})$ en $J_2 = (X + \bar{3})$ onderling ondeelbaar zijn in $(\mathbb{Z}/5\mathbb{Z})[X]$ en dus $R/J_1J_2 \cong R/J_1 \times R/J_2 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ en deze ring heeft nuldelers.) We kunnen ook gebruiken dat $5 = (1 + 2i)(1 - 2i)$ en $1 \pm 2i \notin (5)$ om in te zien dat (5) geen priemideaal is.

We komen nu aan de tweede generalisatie van het begrip priem.

(5.7) Definitie. Laat R een commutatieve ring met 1 zijn. Een ideaal I van R heet *maximaal* als

i) $I \neq R$;

ii) als J een ideaal is van R met $I \subseteq J \subseteq R$ dan geldt $J = I$ of $J = R$.

Voor een priemgetal $p \in \mathbb{Z}$ is het ideaal (p) van $\mathbb{Z}$ een maximaal ideaal: als $I \supsetneq (p)$ een ideaal is en $a \in I$ en $a \notin (p)$ dan geldt $\gcd(a, p) = 1$ en er zijn $x, y \in \mathbb{Z}$ met

$xa + yp = 1$, dus $1 \in I$. Voordat we verdere voorbeelden geven bewijzen we eerste het analogon van Stelling (5.4).

(5.8) Stelling. *Laat I een ideaal van een commutatieve ring R met eenheidselement zijn. Dan geldt:*

$$I \quad \text{is een maximaal ideaal} \iff \quad R/I \text{ is een lichaam.}$$

Bewijs. De idealen van R/I corresponderen 1-1 met de idealen van R die I omvatten. Laat nu J een ideaal van R zijn dat I omvat. We schrijven $\bar{J}$ voor het corresponderende ideaal van R/I.

Stel nu dat I een maximaal ideaal is. We gaan bewijzen dat R/I een lichaam is. Uit $I \neq R$ volgt dat $\bar{1} \neq \bar{0}$, dus R/I heeft een eenheidselement ongelijk 0. Als $\bar{x}$ (met $x \in R$) een element van R/I is met $\bar{x} \neq 0$, dan weten we dat $x \notin I$. Maar dan is het ideaal (I, x) echt groter dan I, dus wegens ii) gelijk aan R. Dit betekent dat $1 = r + sx$ voor zekere $r \in I$ en $s \in R$. Maar dit zegt

$$\bar{1} = \bar{s}\bar{x},$$

dus $\bar{x}$ is een eenheid zoals te bewijzen was.

Omgekeerd, als R/I een lichaam is dan geldt $\bar{1} \neq \bar{0}$, ofwel $1 \notin I$, d.w.z. i) is juist. Als J een ideaal is van R dat I omvat en $J \neq I$, dan bevat J een element x dat niet in I ligt. Maar dan is $\bar{x}$ een eenheid in R/I, dus er is een $\bar{s}$ met $\bar{s}\bar{x} = \bar{1}$. Met andere woorden er is een element $r \in I$ zodat $1 = r + sx$. Omdat $sx \in J$ en $r \in I \subset J$ volgt $1 \in J$, dus $J = R$ zoals te bewijzen was.

Ook (5.5) heeft een analogon:

(5.9) Gevolg. *R is een lichaam dan en slechts dan als (0) een maximaal ideaal is.*

Bewijs. Pas de stelling toe met $I = (0)$.

(5.10) Propositie. *Een maximaal ideaal van een commutatieve ring R met 1 is een priemideaal.*

Bewijs. Ieder lichaam is een domein. Het resultaat volgt dus onmiddellijk met (5.4) en (5.8).

(5.11) Voorbeelden.

i) In de ring $\mathbb{Z}$ is voor een priemgetal p het ideaal (p) een maximaal ideaal, want $\mathbb{Z}/p\mathbb{Z}$ is een lichaam. Het ideaal (0) is wel een priemideaal, maar niet maximaal, want $\mathbb{Z}$ is geen lichaam (of merk op $(0) \subsetneq (p)$).

ii) Het ideaal $(X^2 + 1)$ is maximaal in $\mathbb{R}[X]$. In $\mathbb{C}[X]$ is dit ideaal niet maximaal. Het ideaal $(X^2 + \bar{1})$ is niet maximaal in $(\mathbb{Z}/5\mathbb{Z})[X]$, vgl. (5.6) iv.

iii) Het ideaal $(X^2 + Y)$ is niet maximaal in $\mathbb{C}[X, Y]$, want bevat in het grotere ideaal (X, Y).

iv) Laat $R = \mathbb{Z}[\sqrt{-5}]$ de deelring van $\mathbb{C}$ zijn met

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Het ideaal $(3, 1+\sqrt{-5})$ is een maximaal ideaal van R. Immers met behulp van het isomorfisme

$$\mathbb{Z}[X]/(X^2+5) \cong \mathbb{Z}[\sqrt{-5}], \quad \text{gegeven door } X \mapsto \sqrt{-5}$$

zien we dat

$$\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \cong \mathbb{Z}[X]/(X^2+5, 3, 1+X) = \mathbb{Z}[X]/(3, 1+X),$$

waarbij de gelijkheid komt van het feit dat

$$X^2 + 5 = (X+5)(1+X) - 6X \in (3, 1+X).$$

Nu geldt $\mathbb{Z}[X]/(3, 1+X) \cong (\mathbb{Z}/3\mathbb{Z})[X]/(1+X) \cong \mathbb{Z}/3\mathbb{Z}$, en dit is een lichaam zoals gewenst.

We hebben nu twee generalisaties van het begrip 'priem' gezien, en geven nu een derde. Daarvoor nemen we echter aan dat R geen nuldelers heeft.

(5.12) Definitie. Laat R een domein zijn. Een element $x \in R$ met $x \neq 0$ heet *irreducibel* als x geen eenheid is en als voor elke $y, z \in R$ met $x = yz$ geldt dat $y \in R^*$ of $z \in R^*$.

De irreducibele elementen van $\mathbb{Z}$ zijn de getallen $\pm p$ met p priem.

(5.13) Propositie. *Laat R een domein zijn en $x \in R$ met $x \neq 0$. Als (x) een priemideaal is, dan is x een irreducibel element.*

Bewijs. Omdat (x) een priemideaal is volgt $(x) \neq R$, dus x is geen eenheid. Als we een schrijfwijze $x = yz$ hebben met $y, z \in R$ dan geldt $yz \in (x)$, dus omdat (x) een priemideaal is volgt $y \in (x)$ of $z \in (x)$. Als $y \in (x)$, dan geldt

$$y = rx = ryz \qquad \text{voor een } r \in R.$$

We zien dus $y(1-rz) = 0$. Omdat R een domein is en $x \neq 0$ volgt $y \neq 0$ en dus $1 - rz = 0$. Maar dan is z een eenheid. Het geval dat $z \in (x)$ levert analoog dat dan y een eenheid is. Dit bewijst de propositie.

(5.14) Gevolg. Voor een element $x \neq 0$ van een domein R geldt dus:

$$(x) \quad \text{is een maximaal ideaal} \Longrightarrow (x) \quad \text{is een priemideaal} \Longrightarrow x \quad \text{is irreducibel.}$$

(5.15) Voorbeeld. We laten zien dat er domeinen zijn en irreducibele elementen $x \in R$ zodat (x) geen priemideaal is. We nemen hiervoor de ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

We laten nu eerst zien dat het ideaal (2) geen priemideaal is. Beschouw het element $1+\sqrt{-5}$. Er geldt

$$(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5} = 2\,(-2+\sqrt{-5}) \in (2).$$

Anderzijds ligt $1+\sqrt{-5}$ niet in het ideaal (2). Dus (2) is niet een priemideaal.

We beweren nu dat 2 wel een irreducibel element is. Daarvoor gebruiken we de *norm* op R gedefiniëerd door

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Er geldt dan

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

(Ga dit na.) Stel nu dat $2 = yz$ voor zekere $y, z \in R$. Dan geldt

$$4 = N(2) = N(y)N(z).$$

Maar het getal 2 laat zich niet schrijven als $a^2 + 5b^2$ (ga na), dus volgt $N(y) = 4$ en $N(z) = 1$ of $N(y) = 1$ en $N(z) = 4$. Als $N(y) = 1$, en $y = c + d\sqrt{-5}$ dan volgt $1 = c^2 + 5d^2$, waaruit volgt dat $c = \pm 1$, $d = 0$. Maar dan is y een eenheid. Het geval $N(z) = 1$ impliceert dat z een eenheid is. Daarmee is bewezen dat 2 irreducibel is.

We komen nu nog even terug op het begrip maximaal ideaal. Allereerst laten we zien dat met behulp van het Lemma van Zorn (of het Keuze-Axioma) het bestaan van maximale idealen is gegarandeerd in de volgende zin.

(5.16) Propositie. *Laat R een commutatieve ring met 1 zijn. Als $I \neq R$ een ideaal is van R dan is er een maximaal ideaal J van R dat I bevat.*

Bewijs. We nemen eerst het geval $I = (0)$ en dus $1 \neq 0$. Laat Ω de verzameling van idealen van R zijn die ongelijk aan R zijn. Deze verzameling is partieel geordend ($\leq$) met inclusie. We moeten laten zien dat iedere keten een bovengrens heeft. (Een keten is een deelverzameling K van Ω met de eigenschap dat voor elk paar $x, y \in K$ geldt $x \leq y$ of $y \leq x$.) Gegeven zij nu een keten $\{I_a; a \in A\}$ van idealen van R. Laat J dan de vereniging zijn:

$$J = \cup_{a \in A} I_a.$$

We beweren dat J een ideaal van R is. Immers, als $x, y \in J$ dan zijn er indices $a, b \in A$ zodat $x \in I_a$ en $y \in I_b$. Omdat nu geldt $I_a \subseteq I_b$ of $I_b \subseteq I_a$ zien we $x, y \in I_a$ of $x, y \in I_b$. Omdat I_a en I_b idealen van R zijn en bevat in J volgt $x - y \in J$. Verder gaat men ook snel na dat $rx \in J$ voor iedere $r \in R$ en $x \in J$. Dus is J een ideaal. Merk op dat $1 \notin I_a$ voor alle $a \in A$, dus $1 \notin J$. Dus J is een ideaal ongelijk aan R. Kortom, onze keten K heeft in Ω een bovengrens: J. Het Lemma van Zorn vertelt ons nu dat Ω een maximaal element (met betrekking tot inclusie) bezit. Dit is dan een maximaal ideaal van R.

Als I een willekeurig ideaal $\neq R$ is beschouwen we de ring R/I. Toepassen van bovenstaande levert een maximaal ideaal M van R/I. Maar ieder ideaal van R/I is van de vorm J/I met J een ideaal van R dat I omvat. Omdat $R/J \cong (R/I)/(J/I)$ en de laatste ring een lichaam is volgt dat J een maximaal ideaal van R is dat I bevat. Dit bewijst de propositie.

(5.17) Gevolg. *Laat R een commutatieve ring met 1 zijn. Dan is de vereniging $\cup_m m$ van alle maximale idealen van R gelijk aan $R - R^*$.*

Bewijs. Als $x \in R$ geen eenheid is dan is het ideaal (x) verschillend van R en dus bevat in een maximaal ideaal. Dit bewijst de inclusie $R - R^* \subseteq \cup_m m$. Omgekeerd, als x bevat

is in een maximaal ideaal dan is x geen eenheid (want $m \neq R$). Dus $\cup_m m \subseteq R - R^*$. Dit bewijst het gevolg.

Als k een lichaam is dan is voor ieder element $a \in k$ het ideaal $(X - a)$ een maximaal ideaal. Immers we kennen het isomorfisme $k[X]/(X - a) \cong k$. Meer algemeen is ieder ideaal van de vorm $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subset k[X_1, \ldots, X_n]$ een maximaal ideaal, zoals men inziet door de substitutieafbeelding $k[X_1, X_2, \ldots, X_n] \to k$ met $f \mapsto f(a_1, \ldots, a_n)$ te gebruiken. De punten van de 'ruimte' k^n definiëren dus maximale idealen. Als $k = \mathbb{C}$ dan geldt ook de omkering: alle maximale idealen van $\mathbb{C}[X_1, \ldots, X_n]$ zijn van deze vorm. (Wordt hier niet bewezen.) We zien dat in dit geval de maximale idealen in 1-1 correspondentie staan met de punten van de verzameling k^n. De maximale idealen krijgen zo een meetkundige betekenis. Dit geldt dan ook voor geschikte quotiëntringen, bijvoorbeeld voor de ring $\mathbb{C}[X, Y]/(X - Y^2)$. Deze laatste ring kunnen we opvatten als de ring van polynomiale functies op de parabool gegeven door $X = Y^2$ in $\mathbb{C}^2$ en de maximale idealen van deze ring corresponderen 1-1 met de punten van $\mathbb{C}^2$ op deze parabool. Deze meetkundige interpretatie van idealen vormt de basis van de *algebraïsche meetkunde*, die de nulpuntsverzamelingen van polynomen in meer variabelen bestudeert. In de algebraïsche meetkunde wordt iedere commutatieve ring met 1 opgevat als de ring van functies op een meetkundige ruimte. Zie ook de opgaven 11 en 12.

Opgaven

1) Laat R de deelring $\mathbb{Z}[\sqrt{-3}]$ van $\mathbb{C}$ zijn. Bepaal de eenheden van R. Bewijs dat 2 irreducibel is in R, en dat (2) geen priemideaal is.

2) Laat zien dat het polynoom $X^2 + X + 1$ irreducibel is in $\mathbb{Z}[\sqrt{-3}][X]$, maar niet irreducibel in $k[X]$ met $k = Q(\mathbb{Z}[\sqrt{-3}])$ het quotiëntenlichaam van $\mathbb{Z}[\sqrt{-3}]$.

3) Laat $f : R \longrightarrow R'$ een unitair ringhomomorfisme van commutatieve ringen met 1 zijn. Laat I een priemideaal van R' zijn. Bewijs dat $f^{-1}(I)$ een priemideaal van R is. Geldt iets dergelijks ook voor maximale idealen? Bewijs of weerleg.

4) Ga na of de volgende idealen van $\mathbb{Z}[X]$ priem of maximaal zijn. $(X, 5)$, $(X^2 - 7)$, $(7, X^2 - 2)$.

5) Ga van de volgende idealen van $\mathbb{Q}[X, Y]$ na of ze priem zijn. Welke zijn maximaal?
i) $(X^2 + 3)$.
ii) $(X^2 + 3, Y^2 + 3)$.
iii) $(X^2 + 1, Y^2 - 3)$.

6) Laat R een commutatieve ring zijn en I een ideaal van R. Laat J een priemideaal van R zijn dat I bevat. Laat zien dat J/I een priemideaal is van R/I. Laat verder zien dat ieder priemideaal van R/I van deze vorm is. Zelfde opgave met priemideaal vervangen door maximaal ideaal.

7) Bewijs dat $I = \{a + bi \in \mathbb{Z}[i] : a \equiv b \,(\mathrm{mod}\, 2)\}$ een maximaal ideaal van $\mathbb{Z}[i]$ is.

8) Laat R een commutatieve ring zijn en I een ideaal van eindige index. (Dus $\#R/I < \infty$.) Laat zien dat I maximaal is dan en slechts dan als I priem is.

9) Laat R de ring (zonder 1) zijn bestaande uit de optelgroep van de rationale getallen $\mathbb{Q}$ met als vermenigvuldiging $ab = 0$ voor alle $a, b \in \mathbb{Q}$. Laat zien dat deze ring geen maximale idealen bezit.

10) Bewijs: een ideaal I van een commutatieve ring R met 1 is een priemideaal dan en slechts dan als I de kern is van een homomorfisme $f : R \to k$ met k een lichaam.

11) Laat R een commutatieve ring met 1 zijn. Definieer het *maximale spectrum*

$$\mathrm{Specm}(R) = \{m \subset R;\ m \text{ is een maximaal ideaal}\}$$

Deze verzameling wordt voorzien van een topologie door als gesloten verzamelingen te nemen:

$$V(a) = \{m \in \mathrm{Specm}(R) : m \supseteq a\},$$

waarbij a een ideaal van R. Ga na dat dit een topologie op $\mathrm{Specm}(R)$ definieert.

12) Laat R een commutatieve ring met 1 zijn. Definieer het *spectrum*

$$\mathrm{Spec}(R) = \{p \subset R;\ p \text{ is een priemideaal}\}$$

Deze verzameling wordt voorzien van een topologie door als gesloten verzamelingen te nemen:

$$V(a) = \{p \in \mathrm{Spec}(R) : p \supseteq a\},$$

waarbij a een ideaal van R. Ga na dat dit een topologie op $\mathrm{Spec}(R)$ definieert. Laat verder $f : R \longrightarrow R'$ een ringhomomorfisme zijn. Bewijs dat dit een continue afbeelding $f^* : \mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R)$ geeft door $p \mapsto f^{-1}(p)$.

13) Laat R een commutatieve ring met 1 zijn. Bewijs dat het *nilradicaal* $\sqrt{(0)}$ gelijk is aan de doorsnede $\cap_p p$ van alle priemidealen van R.

14) Laat R een commutatieve ring met $1 \neq 0$ zijn met de eigenschap dat elk ideaal $I \neq R$ een priemideaal is. Bewijs dat R een lichaam is.

15) Een commutatieve ring met 1 heet *locaal* als R precies één maximaal ideaal bezit. Bewijs: een commutatieve ring met 1 is locaal dan en slechts dan als $R - R^*$ een ideaal van R is.

16) Laat R een locale ring zijn en $x \in R$ een element van R met $x^2 = x$. Bewijs dat $x = 0$ of $x = 1$.

17) Laat $R = \{x/y \in \mathbb{Q} : x, y \in \mathbb{Z}, y \not\equiv 0 (\mathrm{mod} 3)\}$. Bewijs dat de deelring R van $\mathbb{Q}$ een locale ring is. Wat is het maximale ideaal m van R? Bewijs verder dat $R/m \cong \mathbb{F}_3$.

18) Laat k een lichaam zijn. Laat zien dat de ring van de duale getallen $k[\epsilon]$ een locale ring is.

19) Laat R de ring $\mathbb{Z}[\sqrt{-5}]$ zijn en laat $I = (3, 1 + \sqrt{-5})$ en $J = (3, 1 - \sqrt{-5})$ twee idealen van R zijn. Bewijs $I\,J = (3)$.

20) Zij R een commutatieve ring met $1 \neq 0$. Stel dat voor iedere rij idealen $I_1 \supseteq I_2 \supseteq \ldots$ geldt: er is een N zodat $I_n = I_m$ als $n, m \geq N$. Bewijs dat ieder priemideaal van R een maximaal ideaal is. Bewijs verder dat R een lichaam is als R nuldelervrij is.

6. Ontbindingsringen

In art as in science there is no delight without the detail,...
Vladimir Nabokov

De ring van gehele getallen kent een eenduidige ontbinding in priemfactoren, zie Syllabus Algebra 1, (1.13). In dit hoofdstuk bestuderen we deelbaarheid in ringen en in het bijzonder analoga van deze eenduidige ontbinding.

In de ring $\mathbb{Z}$ is ieder ideaal een hoofdideaal, dat wil zeggen voortgebracht door één element. Ringen met deze eigenschap zijn heel speciaal.

(6.1) Definitie. Een domein R heet een *hoofdideaalring* als ieder ideaal van R een hoofdideaal is.

(6.2) Stelling. *Laat R een hoofdideaalring zijn en $x \in R$ met $x \neq 0$. Dan zijn de volgende uitspraken equivalent.*

i) (x) *is een maximaal ideaal.*
ii) (x) *is een priemideaal.*
iii) x *is een irreducibel element.*

Bewijs. Wegens (5.14) geldt algemeen i) $\Rightarrow$ ii) $\Rightarrow$ iii). We laten nu zien dat iii) de uitspraak i) impliceert in hoofdideaalringen. Wegens onze aanname is x geen eenheid, dus $(x) \neq R$. Stel nu dat J een ideaal is met $(x) \subsetneq J \subset R$. Omdat R een hoofdideaalring is geldt $J = (y)$ en $x = ry$ voor een $r \in R$. Omdat x irreducibel is volgt $r \in R^*$, dus $(x) = J$, wat we uitgesloten hebben, of $y \in R^*$, dus $J = R$. Dit bewijst de bewering.

(6.3) Gevolg. *In een hoofdideaalring is ieder priemideaal $I \neq (0)$ een maximaal ideaal.*

Bewijs. Omdat $I \neq (0)$ is I van de vorm (x) met $x \neq 0$ en kunnen we Stelling (6.2) toepassen.

We hebben al eerder bewezen dat $\mathbb{Z}$ een hoofideaalring was. Bij het bewijs speelde de deling met rest een hoofdrol. Als k een lichaam is dan heeft de polynoomring $k[X]$ ook een deling met rest, zie (4.1). Met een analoge redenering concluderen we dan ook dat ook $k[X]$ een hoofdideaalring is. Het bewijsprincipe laat zich verder uitbuiten als volgt.

(6.4) Definitie. Een domein R heet een *Euclidische ring* als er een functie

$$N : R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

bestaat met de eigenschap dat er voor alle $x, y \in R$ met $y \neq 0$ elementen $q, r \in R$ bestaan zodat

$$x = q\,y + r \quad \text{met } r = 0 \text{ of } N(r) < N(y).$$

We merken op dat de functie N (zo er al een bestaat) niet uniek hoeft te zijn.

(6.5) Voorbeelden.

i) De ring $\mathbb{Z}$ is Euclidisch voor de functie $N(x) = |x|$.
ii) Laat k een lichaam zijn. De ring $k[X]$ is Euclidisch voor de functie $N(f) = \deg(f)$. Dit volgt uit Deling met Rest (4.1).
iii) De ring $\mathbb{Z}[i]$ is Euclidisch voor de functie $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. Om dit in te zien breiden we eerst de functie N uit tot $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$,

het quotiëntenlichaam van $\mathbb{Z}[i]$ via $N(x/y) = N(x)/N(y)$ voor $x, y \in \mathbb{Z}[i]$ met $y \neq 0$. Omdat de functie N op $\mathbb{Z}[i]$ voldoet aan $N(xy) = N(x)N(y)$, is N op $\mathbb{Q}(i)$ welgedefinieerd. Als nu twee elementen $x, y \in \mathbb{Z}[i]$ gegeven zijn met $y \neq 0$, moeten we laten zien dat er een q in $\mathbb{Z}[i]$ is zodat $N(x - qy) < N(y)$. Delen we nu door $N(y)$ dan vinden we de conditie dat er voor ieder element $x/y \in \mathbb{Q}(i)$ een $q \in \mathbb{Z}[i]$ moet bestaan zodat

$$N(\frac{x}{y} - q) < 1.$$

Als we $\mathbb{Z}[i]$ nu opvatten als deelring van $\mathbb{C}$ dan zien we dat de norm niets anders is dan het kwadraat van de absolute waarde $|a+bi|$. Om in te zien dat $\mathbb{Z}[i]$ Euclidisch is, moeten we dus laten zien dat voor iedere $z \in \mathbb{Q}(i)$ er een $q \in \mathbb{Z}[i]$ is met $|z - q| < 1$. Ofwel dat de cirkelschijven met als middelpunten de punten van $\mathbb{Z}[i]$ en straal 1 het gehele complexe vlak overdekken. Maar dat is duidelijk (maak een plaatje).

(6.6) Stelling. *Iedere Euclidische ring R is een hoofdideaalring.*

Bewijs. De ring R is een domein gezien de aanname. Laat I een ideaal van R zijn. Als $I = \{0\}$ dan is I een hoofdideaal. Neem daarom nu aan dat $I \neq \{0\}$. Dat betekent dat de verzameling $\{N(x) : x \in I - \{0\}\}$ een niet-lege deelverzameling van $\mathbb{Z}_{\geq 0}$ is. Laat x_0 een element van $I - \{0\}$ zijn met minimale norm. We beweren dat x_0 een voortbrenger is van I. Laat x een willekeurig element van I zijn. Dan zijn er q en r in R zodat $x = q\,x_0 + r$ met $r = 0$ of $N(r) < N(x_0)$. Omdat $r = x - qx_0 \in I$ kan de norm van r niet kleiner zijn dan $N(x_0)$, dus moet $r = 0$. Dit bewijst dat $x = qx_0$, met andere woorden x_0 is een voortbrenger van I. Daarmee is (6.6) bewezen.

Zoals we bij Algebra 1 gezien hebben kent de ring $\mathbb{Z}$ eenduidige ontbinding (factorisatie). Bij het bewijs hiervan werd het Euclidisch algoritme gebruikt. Het ligt voor de hand dat Euclidische ringen een vorm van eenduidige ontbinding kennen. We gaan dit nu precies maken.

(6.7) Definitie. Laat R een commutatieve ring met 1 zijn. We noemen twee elementen $x, y \in R$ *geassocieerd* als er een eenheid $r \in R^*$ is met $x = ry$.

De lezer gaat gemakkelijk na dat geassocieerd zijn een equivalentierelatie op R is. Merk op dat geassocieerde elementen dezelfde deelbaarheidseigenschappen hebben. Zijn x en y geassocieerd dan deelt z het element x dan en slechts dan als z het element y deelt.

(6.8) Definitie. Een domein R heet een *ontbindingsring* als ieder element $x \in R$ met $x \neq 0$ zich laat schrijven als product van een eenheid en eindig veel irreducibele elementen

$$x = u \cdot p_1 \cdot \ldots \cdot p_n$$

(waar $u \in R^*$ en de p_i irreducibel zijn) en deze schrijfwijze bovendien uniek is op volgorde en vermenigvuldiging met eenheden na.

Dus als we x ook kunnen schrijven als $x = v \cdot q_1 \cdot \ldots \cdot q_m$ met $v \in R^*$ en q_i irreducibel dan geldt $n = m$ en er is een permutatie σ van $\{1, 2, \ldots n\}$ zodat p_i en $q_{\sigma(i)}$ geassocieerd zijn.

(6.9) Lemma. *Laat R een ontbindingsring zijn en $x \in R$ een element $\neq 0$. Dan geldt*

$$x \in R \quad \textit{is irreducibel} \Longleftrightarrow (x) \quad \textit{is een priemideaal.}$$

Bewijs. We weten al (zie (5.3)) dat als (x) een priemideaal is het element x irreducibel is. Stel nu dat x irreducibel is en $y, z \in R$ met $yz \in (x)$. Op grond van de unieke ontbinding komt de factor x voor in y of in z. Maar dat betekent $y \in (x)$ of $z \in (x)$. Dit bewijst het lemma.

We noemen een element $p \neq 0$ van een domein een *priemelement* als (p) een priemideaal is. In een ontbindingsring vallen de begrippen *priem* en *irreducibel* samen.

(6.10) Opmerking. We zien dus in dat in een ontbindingsring geldt:

als p een irreducibel element is en $p|xy$ dan volgt $p|x$ of $p|y$.

Immers, (p) is een priemideaal, en $xy \in (p)$ impliceert $x \in (p)$ of $y \in (p)$.

Een nuttig resultaat is de volgende stelling waarmee we ook inzien dat Euclidische ringen ontbindingsringen zijn.

(6.11) Stelling. *Een hoofdideaalring is een ontbindingsring.*

Bewijs. Stel dat R een hoofdideaalring is. We gaan eerst laten zien dat een element $x \neq 0$ te schrijven is als product van een eenheid en eindig veel irreducibele elementen. Daarna bewijzen we de eenduidigheid van de schrijfwijze (op eenheden en volgorde na).

Als x een eenheid is of irreducibel is zijn we klaar. Stel x is dat niet; dan kunnen we schrijven $x = x_1y_1$ met x_1 en y_1 geen eenheid. Dan zijn de idealen (x) en (x_1) verschillend. Immers, anders geldt $x_1 = rx$ en dus $x = rxy_1$, dus $x(1 - ry_1) = 0$, waaruit volgt dat y_1 een eenheid is, tegen onze aanname. Dus we zien

$$(x) \subsetneq (x_1).$$

Als x_1 en y_1 irreducibel zijn, dan zijn we klaar. Zo niet, dan is een van beiden reducibel, zeg x_1. We kunnen we het argument nu herhalen voor x_1 en vinden we $x_1 = x_2y_2$ met x_2 en y_2 geen eenheden. Zo vinden we idealen $(x_1) \subsetneq (x_2)$. Herhalen van het argument levert een rij idealen

$$(x_1) \subsetneq (x_2) \subsetneq \ldots \subsetneq (x_n) \subsetneq \ldots$$

We beweren nu dat deze rij moet stabilizeren. Immers, neem

$$I = \cup_{n=1}^{\infty}(x_n).$$

Het is gemakkelijk te zien dat I een ideaal van R is en dit moet een hoofdideaal zijn, zeg $I = (\xi)$ met $\xi \in I$. Maar dan ligt ξ in een (x_n) en we vinden dan

$$(x_n) \subseteq (\xi) \subseteq (x_n).$$

Dus $(x_n) = (\xi)$. Dus $(x_n) = (x_{n+1}) = \ldots$ en dat betekent dat onze aanname dat x_n niet irreducibel was fout is. Dus x_n is irreducibel voor zekere n. Maar dan is x te schrijven als product van irreducibele elementen.

We moeten nu de eenduidigheid nog inzien. We voeren inductie naar het aantal irreducibele factoren. Als x een schrijfwijze met 0 irreducibele factoren toelaat dan is x een eenheid. Als x nu ook een schrijfwijze

$$x = v \cdot q_1 \cdots q_m$$

toelaat met $v \in R^*$ en q_i irreducibel dan volgt $m = 0$ en $v = u$. De eenduidigheid in dat geval is dus duidelijk. Nemen we dan aan dat x geen eenheid is en twee ontbindingen toelaat:

$$u \cdot p_1 \cdots p_n = x = v \cdot q_1 \cdots q_m$$

met $n > 0$. Maar dan deelt p_1 het element x, dus met Stelling (6.2) een van de factoren q_i (vgl Opm. (6.10). Na hernummeren, mogen we aannemen dat dit q_1 is. Dus $q_1 = wp_1$ met $w \in R^*$. Dus we zien

$$p_1(u \cdot p_2 \cdots p_n - vw \cdot q_2 \cdots q_m) = 0$$

Met inductie heeft $x' = u \cdot p_2 \cdots p_n$ een eenduidige ontbinding op eenheden en volgorde na en daarmee ook x. Dit bewijst de stelling.

(6.12) Voorbeeld. Laat k een lichaam zijn en $R = k[X]$. Dan is R een Euclidische ring, dus ook een hoofdideaalring, en dan ook een ontbindingsring.

(6.13) Definitie. Laat R een ontbindingsring zijn en p een irreducibel element van R. Voor een element $x \neq 0$ van R definiëren we $\mathrm{ord}_p(x)$ als het aantal factoren in de ontbinding van x die geassocieerd zijn met p.

In een ontbindingsring kunnen we ook de *grootste gemene deler* $\mathrm{ggd}(x, y)$ van twee elementen $x, y \in R - \{0\}$ definiëren:

$$\mathrm{ggd}(x, y) = \prod_p p^{\min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))},$$

waarbij het product genomen wordt over de irreducibele elementen modulo eenheden (meer precies over een volledige verzameling representanten van de irreducibele elementen voor de equivalentierelatie 'geassocieerd zijn'). Merk op dat de grootste gemene deler afhangt van de keuze van de irreducibele elementen. Dus de ggd is welgedefinieerd op vermenigvuldiging met een eenheid van R na. Voor deze ggd gaat men snel de analoga van rekenregeltjes voor de gewone ggd in $\mathbb{Z}$ na. Zo geldt het volgende lemma.

(6.14) Lemma.

i) De grootste gemene deler $\mathrm{ggd}(x, y)$ *deelt zowel* x *als* y.
ii) Iedere gemeenschappelijke deler van x *en* y *deelt* $\mathrm{ggd}(x, y)$.
iii) Er geldt $\mathrm{ggd}(zx, zy) = z\,\mathrm{ggd}(x, y)$ *voor alle* $x, y, z \in R - \{0\}$.

De verificatie hiervan wordt aan de lezer overgelaten.

Opgaven

1) Laat zien dat in een commutatieve ring R met 1 de relatie 'geassocieerd zijn' (d.w.z. $x \sim y \iff$ er is een $u \in R^*$ met $x = uy$) een equivalentierelatie is.

2) Laat $R = \mathbb{Z}[\sqrt{-5}]$. Bewijs dat het ideaal $(2, 1+\sqrt{-5})$ een maximaal ideaal van R is. Laat verder zien dat het geen hoofdideaal is.

3) Laat $R = \mathbb{Q}[X,Y]/(Y^2 - X^3)$. Bewijs dat de restklassen van X en Y irreducibele elementen zijn in R. Bewijs dat R een domein is, maar geen ontbindingsring.

4) Laat k een lichaam zijn. Bepaal de priemidealen van $k[X]$. Welke zijn maximaal?

5) Laat p een priemgetal zijn. Bepaal het aantal irreducibele kwadratische polynomen in $\mathbb{F}_p[X]$.

6) Bepaal de ggd van $X^5 + X^2$ en $X^{12} - 1$ in $\mathbb{R}[X]$, $\mathbb{C}[X]$ en $\mathbb{F}_2[X]$.

7) Laat zien dat in $\mathbb{Z}[i]$ het element $a + bi$ irreducibel is als $a^2 + b^2$ een priemgetal is. Geldt het omgekeerde ook? Bewijs of weerleg.

8) Gegeven is een priemgetal $p \in \mathbb{Z}$. Laat zien dat $X^2 + p$ irreducibel is in $\mathbb{Q}[X]$. Laat zien dat $\mathbb{Q}[X]/(X^2+p)$ een lichaam is.

9) Laat k een lichaam zijn en laat

$$k[[X]] = \{\sum_{i=0}^{\infty} a_i X^i : a_i \in k\}$$

met de gebruikelijke optelling en vermenigvuldiging; dit is een commutatieve ring. Deze ring heet de ring van *formele machtreeksen* met coëfficiënten uit k.

i) Bewijs dat $k[[X]]^* = \{f \in k[[X]] : a_0 \neq 0\}$.

ii) Definieer de functie $N : k[[X]] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ via

$$N(\sum_{i=0}^{\infty} a_i X^i) = \min\{i : a_i \neq 0\}.$$

Laat zien dat $k[[X]]$ een Euclidische ring is met betrekking tot N.

10) Bewijs Lemma (6.15).

11) Ga van de volgende elementen in $\mathbb{Z}[\sqrt{-5}]$ na of ze irreducibel zijn en of ze priem zijn: 1, 2, 3, 4, 5, $1+\sqrt{-5}$, $2+\sqrt{-5}$.

12) Bepaal $\text{ggd}(5, 10+8i)$ en $\text{ggd}(7-4i, 8-i)$ in $\mathbb{Z}[i]$. Ontbind 15 en $9+7i$ in $\mathbb{Z}[i]$ in irreducibele factoren.

13) Laat p een priemgetal zijn en laat

$$R = \{\frac{x}{y} \in \mathbb{Q} : x, y \in \mathbb{Z},\ p \text{ deelt niet } y\}.$$

Dit is een deelring van $\mathbb{Q}$.

i) Bepaal de eenheden van R.

ii) Laat zien dat $\{\frac{x}{y} \in R : x, y \in \mathbb{Z},\ p \text{ deelt } x\}$ een maximaal ideaal van R is.

iii) Laat zien dat ieder element $a \in R$ met $a \neq 0$ eenduidig te schrijven is als $a = u \cdot p^k$ met u een eenheid van R en $k \in \mathbb{Z}_{\geq 0}$.

iv) Laat nu zien dat R een Euclidische ring is met normfunctie $N(a) = k$ als $a = u \cdot p^k$.

v) Bepaal de irreducibele elementen van R.

14) Bewijs dat $\mathbb{F}_5[X]/(X^2+3)$ een lichaam met 25 elementen is.

15) Laat $R = \mathbb{Z}[\sqrt{-5}]$. Dit is een deelring van $\mathbb{C}$.
i) Laat zien dat 3 en $2 \pm \sqrt{-5}$ irreducibel zijn.
ii) Ga na: $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.
iii) Bewijs: R is geen ontbindingsring.

16) Laat zien dat ieder lichaam een Euclidische ring is.

17) Bepaal de eenheden van $\mathbb{Z}[X]$.

18) Laat R een Euclidische ring zijn met functie $N : R - 0 \to \mathbb{Z}_{\geq 0}$. Definieer een nieuwe functie $N' : R - \{0\} \to \mathbb{Z}_{\geq 0}$ via

$$N'(x) = \min\{N(rx) : r \in R - \{0\}\}.$$

Laat zien dat R een Euclidische ring is voor de functie N' en dat N' voldoet aan $N'(xy) \geq N'(x)$ voor alle $x, y \in R - \{0\}$. (Dit verklaart waarom men vaak de extra eis $N(xy) \geq N(x)$ voor alle $x, y \in R - \{0\}$ voor Euclidische ringen in leerboeken vindt.)

19) Is de ring $\mathbb{R}[X, Y]$ een Euclidische ring?

20) Bewijs dat de ring $\mathbb{Z}[\sqrt{-2}]$ een Euclidische ring is.

21) Laat k een lichaam zijn en $a, b \in k$ elementen van k met $a \neq 0$. Bewijs: een polynoom $f(X) \in k[X]$ is irreducibel dan en slechts dan als $f(aX + b)$ irreducibel is.

22) Ontbind het polynoom $X^3 + X + 1$ in $\mathbb{F}_p[X]$ voor $p = 2, 3, 5, 7$.

23) Bewijs dat $\mathbb{F}_2[X]/(X^3+X+1)$ een lichaam is. Hoeveel elementen heeft dit lichaam?

7. Ontbinding van Polynomen

Dass dem Forscher, solange er sucht, jeder Weg
gestattet ist, versteht sich von selbst.
K. Weierstrass*

In dit hoofdstuk bestuderen we het ontbinden van polynomen. Gezien de resultaten van het vorige hoofdstuk weten we dat voor een lichaam k de polynoomring $k[X]$ een ontbindingsring is. Maar ook voor een grotere klasse van coëfficiëntenringen R zijn de polynoomringen $R[X]$ ontbindingsringen; bijvoorbeeld zal blijken dat dit het geval is wanneer R zelf een ontbindingsring is, zoals $R = \mathbb{Z}$.

Laat nu R een *ontbindingsring* zijn en $R[X]$ de bijbehorende polynoomring.

(7.1) Definitie Als $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ een polynoom is dan heet de grootste gemene deler $\text{ggd}(a_0, a_1, \ldots, a_n)$ van de coëfficiënten de *inhoud* van f. We noemen een polynoom met inhoud 1 een *primitief* polynoom.

(7.2) Voorbeeld. Ieder monisch polynoom is primitief. Het polynoom $21X^7 - 10X^2 + 5X + 4 \in \mathbb{Z}[X]$ is ook primitief. De inhoud van $20X^3 - 8X + 2 \in \mathbb{Z}[X]$ is gelijk aan 2.

Laat nu $K = Q(R)$ het quotiëntenlichaam van R zijn. Dan is de ring $K[X]$ een ontbindingsring en de ontbinding daar kunnen we gebruiken om een ontbinding in $R[X]$ te vinden.

(7.3) Lemma. *Ieder polynoom in $f \in K[X]$ met $f \neq 0$ laat zich schrijven als $f = c\, f_0$ met $f_0 \in R[X]$ primitief en $c \in K^*$. Deze schrijfwijze is eenduidig op vermenigvuldiging met eenheden van R na.*

Bewijs. Door vermenigvuldiging met een geschikt element $a \in R$ met $a \neq 0$ kunnen we bereiken dat $af \in R[X]$. Laat nu b de inhoud van af zijn. Dan deelt b alle coëfficiënten van af en we kunnen schrijven

$$af = b \cdot f_0,$$

waarbij f_0 een primitief polynoom uit $R[X]$ is. En dus ook

$$f = \frac{b}{a}\, f_0,$$

zoals gewenst. Om de eenduidigheid van deze schrijfwijze in te zien veronderstellen we dat

$$cf_0 = f = c'\, f_0'$$

twee zulke schrijfwijzen zijn. Er is een $d \in R$ met $d \neq 0$ zodat dc en dc' beide in R liggen. Dan vinden we dus op eenheden na

$$dc = \text{inhoud}(dcf_0) = \text{inhoud}(dc'\, f_0') = dc'.$$

en dus ook $f_0 = f_0'$. Dit bewijst het lemma.

---

* Karl Weierstrass, Duits wiskundige, 1815-1897.

(7.4) Propositie. *Als R een ontbindingsring is en f en $g \in R[X]$ zijn primitieve polynomen, dan is ook fg primitief.*

Bewijs. Als fg niet primitief is, is er een irreducibel element $p \in R$ zodat p alle coëfficiënten van fg deelt. Dit betekent dat

$$\bar{f}\bar{g} \equiv 0 \quad \text{in de ring} \quad (R/pR)[X].$$

Nu is (p) een priemideaal van R en dus is $R/(p)$ een domein en kent dus geen nuldelers. Dan is ook $(R/(p))[X]$ nuldelervrij en we zien dat uit $\bar{f}\bar{g} = 0$ in deze ring volgt dat $\bar{f} = 0$ of $\bar{g} = 0$. Maar dan deelt p alle coëfficiënten van f of van g, in tegenspraak met de aanname dat f en g primitief zijn.

Gevolg. *Als $f = gh$ in $R[X]$ dan geldt* $\text{inhoud}(f) = \text{inhoud}(g)\text{inhoud}(h)$.

(7.5) Stelling. *Als R een ontbindingsring is, dan is $R[X]$ dat ook.*

Bewijs. We schrijven $K = Q(R)$ voor het quotiëntenlichaam van R. We beweren nu eerst dat een polynoom $f \in R[X]$ met $f \neq 0$ zich laat schrijven als

$$f = u \cdot p_1 \cdot p_2 \cdots p_m \cdot g_1 \cdots g_n, \tag{1}$$

waarbij $u \in R^*$, de elementen p_i irreducibele elementen van R zijn en de polynomen g_j primitieve polynomen van $R[X]$ zijn die irreducibel in $K[X]$ zijn. Immers, omdat $K[X]$ een ontbindingsring is kunnen we f schrijven als

$$f = a \cdot g_1 \cdots g_n$$

met $a \in K^*$ en de g_j ireducibele polynomen van $K[X]$. Met behulp van (7.3) kunnen we na verandering van a aannemen dat de g_i primitieve polynomen van $R[X]$ zijn die irreducibel in $K[X]$ zijn. Maar volgens (7.4) is dan het product $g_1 \cdots g_n$ ook primitief en a ligt in R en is dan gelijk aan de inhoud van f.

Als we nu gebruiken dat R een ontbindingsring is mogen we schrijven

$$a = u \cdot p_1 \cdots p_2 \cdots p_m$$

met u een eenheid van R en de p_i irreducibel in R. Dit bewijst de mogelijkheid om f te schrijven als in (1). De lezer mag nagaan dat op volgorde en vermenigvuldiging met eenheden van R na deze schrijfwijze eenduidig is.

Om het bewijs te kunnen afsluiten moeten we nog inzien dat de irreducibele elementen van $R[X]$ precies de irreducibele elementen van R zijn en de primitieve polynomen van $R[X]$ die irreducibel in $k[X]$ zijn.

Laat nu f een irreducibel element van $R[X]$ zijn. Uit de schrijfwijze (1) volgt dat omdat f geen eenheid is f ofwel gelijk is aan een enkele factor p of of enkele factor g.

Omgekeerd, als p een irreducibel element is van R, maar niet irreducibel in $R[X]$ dan weerspreekt dit de schrijfwijze (1). Evenzo, als g een primitief polynoom van $R[X]$ is dat irreducibel is in $K[X]$, en als g reducibel in $R[X]$ was, dan zou dat weer de eenduidigheid van de schrijfwijze (1) weerspreken. Daarmee is het bewijs voltooid.

(7.6) Toepassing. *De ring $\mathbb{Z}[X_1, \ldots, X_n]$ is een ontbindingsring. Voor een lichaam k is de ring $k[X_1, \ldots, X_n]$ een ontbindingsring.*

Bewijs. De ring $\mathbb{Z}$ is een ontbindingsring en $k[X_1]$ is dat ook want beide ringen zijn Euklidische ringen. Met inductie volgen beide uitspraken uit de voorgaande stelling.

In de rest van dit hoofdstuk houden we ons nog in meer praktische zin met de ontbinding van polynomen bezig. Hoe vinden we factoren of irreducibele factoren van een polynoom?

Als R een domein is dan volgt uit Propositie (4.4) dat een polynoom $f \in R[X]$ een lineaire factor $X - a$ heeft dan en slechts dan als a een nulpunt is van f; dat laatste valt te controleren door substitutie. Soms kunnen we nulpunten a priori beperken, zoals de volgende propositie ons leert.

(7.7) Propositie. *Laat R een ontbindingsring zijn met quotiëntenlichaam K. Laat $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ met $a_0 \neq 0$, $a_n \neq 0$.*

i) Ieder nulpunt van f in K heeft de gedaante $x = a/b$, waarbij a en b elementen van R zijn met a deelt a_0 en b deelt a_n.

ii) Als f ook monisch is, dan ligt ieder nulpunt in K van f ook in R en deelt a_0.

Bewijs. Laat $x = a/b$ met $\gcd(a, b) = 1$ een nulpunt van f in K zijn. Deling met rest in $K[X]$ leert ons dan dat

$$f = (bX - a)g$$

met $g = \sum_{i=0}^{n-1} b_i X^i \in K[X]$. Schrijf g als $g = cg_0$ met g_0 primitief in $R[X]$ en $c \in K^*$. Maar $f = (bX - a)g$ ligt in $R[X]$, dus de inhoud van f ligt in R en is gelijk aan de inhoud van $g = cg_0$. Daaruit volgt nu dat ook g in $R[X]$ ligt (Ga na dat $\text{inhoud}(f) = \text{inhoud}(g)$.) Vergelijken van coëfficiënten geeft dan

$$a_0 = -ab_0, \quad a_n = bb_{n-1}.$$

Daaruit volgt nu de deelbaarheid zoals in i) beweerd wordt.

Nemen we nu $a_n = 1$ dan volgt ook direkt ii).

De irreducibiliteit van tweede- of derdegraads polynomen in $K[X]$ is eenvoudig na te gaan:

(7.8) Lemma. *Een polynoom $f \in K[X]$ van graad 2 of 3 is reducibel dan en slechts dan als f een nulpunt heeft in K.*

Bewijs. Als $f = gh$ met g, h geen eenheden, d.w.z. $g, h \notin k$, dan heeft g of h graad 1.

Dit geldt niet voor polynomen van hogere graad, bijv. heeft het polynoom $X^4 + 1 \in \mathbb{F}_3[X]$ geen nulpunten in $\mathbb{F}_3$, maar is toch reducibel:

$$(X^2 + 2X + 2)(X^2 + X + 2) = X^4 + 1.$$

Of ook $X^4 + 9X^2 + 25 = (X^2 + X + 5)(X^2 - X + 5) \in \mathbb{Q}[X]$ terwijl men met Prop. (7.7) of door naar het tekenverloop op $\mathbb{R}$ te kijken eenvoudig inziet dat dit polynoom geen nulpunten heeft.

Als we in $R[X]$ willen ontbinden waarbij R een ontbindingsring is, dan ligt het voor de hand eerst in $K[X]$ te ontbinden met $K = Q(R)$, het quotiëntenlichaam van R en dan te zien wat dit voor $R[X]$ betekent. Het cruciale hulpmiddel is het volgende lemma van Gauss.

(7.9) Lemma van Gauss. *Laat R een ontbindingsring zijn met quotiëntenlichaam $K = Q(R)$.*

i) Als $f \in R[X]$ een monisch polynoom is en $f = gh$ met $g, h \in K[X]$ monisch dan liggen g en h in $R[X]$.

ii) Stel $f \in R[X]$ is primitief. Dan is f irreducibel in $R[X]$ dan en slechts dan als f irreducibel in $K[X]$ is.

Bewijs. Door vermenigvuldiging met geschikte constanten c en d uit K^* krijgen we primitieve polynomen cg en dh uit $R[X]$ Omdat g en h monisch zijn volgt dat c en d elementen van R zijn. Er geldt dan $cdf = (cg)(dh)$. Nu is f monisch en dus primitief. Maar het product $(cg)(dh)$ van twee primitieve polynomen is volgens (7.4) ook weer primitief. Wegens de eenduidigheid zoals uitgesproken in Stelling (7.5) volgt dan dat $cd \in R^*$, en daaruit volgt weer dat c en d ook eenheden in R zijn. We zien dus in dat g en h in $R[X]$ liggen. Dit bewijst i).

ii) Stel dat f reducibel is in $R[X]$, zeg $f = gh$ met $g, h \in R[X]$ met $g, h \notin R[X]^*$. Omdat f primitief is zijn g en h geen constanten. Dus dit geeft een niet-triviale ontbinding in $K[X]$.

Omgekeerd, laat f reducibel zijn in $K[X]$, zeg, $f = gh$ met $g, h \in K[X]$ beiden niet constant. Dan bestaan er eenduidig bepaalde constanten $c, d \in K^*$ zodat $g = cg_0$ en $h = dh_0$ met g_0 en h_0 primitieve polynomen uit $R[X]$. De ontbinding $f = cdg_0h_0$ levert volgens het gevolg van Propositie (7.4) dat $cd \in R^*$. Dus f is reducibel in $R[X]$. Dit bewijst het Lemma.

Een handig middel om polynomen uit $\mathbb{Z}[X]$ te testen op irreducibiliteit is reductie modulo een priemgetal.

(7.10) Gevolg. *Laat $f \in \mathbb{Z}[X]$een monisch polynoom zijn en $p \in \mathbb{Z}$ een priemgetal zodat $f \pmod p \in \mathbb{F}_p[X]$ irreducibel is. Dan is f irreducibel in $\mathbb{Z}[X]$ en $\mathbb{Q}[X]$.*

Bewijs. Stel dat $f = gh$ reducibel is in $\mathbb{Z}[X]$ met $\deg(g) > 0$, $\deg(h) > 0$, dan vinden we na reductie modulo p een ontbinding $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[X]$. Omdat $\bar{g}$ en $\bar{h}$ geen constanten zijn spreekt dit de irreducibiliteit van $\bar{f}$ tegen. Dit bewijst het gevolg.

Ook als de reductie van f modulo een priem p niet irreducibel is, levert dit toch nuttige informatie op. Bijvoorbeeld, als $f \in \mathbb{Z}[X]$ een polynoom van graad 5 is dat modulo een priemgetal p een product van twee irreducibele factoren van graad 2 en 3 is, maar modulo een andere priem q het product is van twee irreducibele factoren van graad 1 en 4, dan moet f wel irreducibel zijn.

(7.11) Voorbeeld. Laat $f = X^5+X^2-X+4 \in \mathbb{Z}[X]$. Modulo 3 kunnen we f ontbinden in irreducibele factoren als $(X^2+1)(X^3-X+1)$ en modulo 2 als $X(X^4+X+1)$. Hieruit volgt dat f irreducibel is in $\mathbb{Z}[X]$.

We geven nu een nuttig kriterium om irreducibiliteit vast te stellen.

(7.12) Stelling. (Kriterium van Eisenstein.*) *Laat R een ontbindingsring zijn en p een irreducibel element van R. Stel dat*

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

een primitief polynoom uit $R[X]$ is zodat

i) p deelt niet a_n;
ii) p deelt a_i voor $i = 0, 1, \ldots, n-1$;
iii) p^2 deelt niet a_0.

Dan is f irreducibel in $R[X]$.

Bewijs. Stel dat f reducibel is en $f = gh$ is een niet-triviale ontbinding. Dan zijn g en h geen constanten omdat f primitief is. Reductie modulo p geeft

$$\bar{f} = \bar{a}_n X^n = \bar{g}\bar{h}.$$

Merk op dat $\bar{a}_n \neq \bar{0}$. Omdat de quotiëntring $R/(p)$ een domein is moeten we hebben

$$g \equiv \gamma X^k (\mathrm{mod} p), \quad h \equiv \eta X^{n-k} (\mathrm{mod} p)$$

met $\gamma, \eta \in R$ en $k \in \mathbb{Z}_{>0}$. Hieruit volgt dat de constante termen van g en h deelbaar zijn door p en dus dat a_0 deelbaar is door p^2. Maar dit weerspreekt onze aanname. Dit bewijst het Kriterium van Eisenstein.

Een polynoom dat aan de voorwaarden van Stelling (7.12) voldoet heet een *Eisenstein-polynoom*.

(7.13) Voorbeeld. Laat $R = \mathbb{Z}$ en $f = X^6 + 3X^4 - 12X^2 + 6$. Dit is een Eisensteinpolynoom en is dus irreducibel.

Of neem $R = \mathbb{Q}[X, Y]$ en $f = X^5 - (Y^4 - 9)X^3 + (Y^2 - 3)$. Dit is een Eisensteinpolynoom met $p = Y^2 - 3$.

(7.14) Voorbeeld. Laat p een priemgetal zijn en

$$f = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Q}[X].$$

We beweren dat dit polynoom irreducibel is. Merk eerst op dat $f = (X^p - 1)/(X - 1)$. We definiëren nu een nieuw polynoom g via

$$g(X) = f(X + 1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + pX^{p-2} + \ldots + p.$$

Dit is een Eisensteinpolynoom in $\mathbb{Z}[X]$ en dus is g irreducibel. Was f nu reducibel, zeg $f = f_1 f_2$ dan was $g = f_1(X + 1) f_2(X + 1)$ een ontbinding van g, in tegenspraak met de irreducibiliteit. Dus is f ook irreducibel in $\mathbb{Z}[X]$, en met het Lemma van Gauss dan ook in $\mathbb{Q}[X]$.

---

* *G. Eisenstein, Duits wiskundige, 1823-1852. Hij leverde een belangrijke bijdrage aan de ontwikkeling van de theorie van elliptische functies.*

Opgaven

1) Laat R een domein zijn en $f = \sum_{i=0}^{n} a_i X^i$ een polynoom met $a_0 \neq 0$ en $a_n \neq 0$. We definiëren het 'omgekeerde' polynoom $f^* = \sum_{i=0}^{n} a_{n-i} X^i$. Bewijs dat voor $f, g \in R[X]$ geldt $(fg)^* = f^* \cdot g^*$. Ga na: f is irreducibel dan en slechts dan als f^* irreducibel is.

2) Ontbind de volgende polynomen in $\mathbb{Q}[X]$ en in $\mathbb{Z}[X]$:

$$4X^2 + 8X + 4, \quad 3X^8 + 6X^4 + 2, \quad X^5 - 2X^4 + X^3 - 2X^2 - 2,$$
$$X^6 + X^3 + 1, \quad X^4 + 1, \quad X^3 + 3X^2 + 4X + 5.$$

3) Ontbind de volgende polynomen in $\mathbb{Q}[X]$ en in $\mathbb{Z}[X]$:

$$X^5 - X^4 + x^3 - X^2 + X - 1, \quad X^{12} - 1, \quad X^3 + 3X^2 + 6X + 9, \quad X^5 - 5X^3 + 15.$$

4) Laat $f = X^4 - 8X^2 + 36 \in \mathbb{Z}[X]$. Is f irreducibel? Ga na of $f \pmod p$ irreducibel is in $\mathbb{F}_p[X]$ voor $p = 2, 3, 5, 7, 11, 13$.

5) Bepaal het aantal monische irreducibele polynomen van graad 2 in $\mathbb{F}_p[X]$.

6) Laat f een Eisensteinpolynoom zijn in $\mathbb{Z}[X]$. Bewijs dat $f(X^2)$ irreducibel is.

7) Ga na of het door $X^2 - 7$ voortgebrachte ideaal een priemideaal en ook of het een maximaal ideaal is in $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, en in $\mathbb{F}_5[X]$.

8) Laat $f \in \mathbb{Z}[X]$ een monisch polynoom zijn. Stel $f(0)$ is een priemgetal. Bewijs: het aantal nulpunten van f in $\mathbb{Q}$ is ten hoogste 3.

9) Is $X^2 + Y^2 - 1$ irreducibel in $\mathbb{Q}[X, Y]$? En in $\mathbb{C}[X, Y]$?

10) Is $X^5 + X^4 + X^3 + X^2 + X + 1$ irreducibel in $\mathbb{Q}[X]$?

11) Laat p een priemgetal zijn. Bepaal $\gcd(p, X)$ in $\mathbb{Z}[X]$. Bewijs dat $\gcd(p, X)$ niet bevat is in het ideaal (p, X) van $\mathbb{Z}[X]$.

8. Lichamen

. . . les racines ne sont pas toujours réelles, mais quelquefois seulement imaginaires, c'est-à-dire qu'on peut bien toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine.
Rene Descartes*: Discours de la Méthode

Een homomorfisme van lichamen $f : K \to L$ is een unitair ringhomomorfisme. De kern van zo een homomorfisme is een ideaal I van K dat 1 niet bevat, dus $I = \{0\}$ en dus is ieder homomorfisme van lichamen injectief. Het beeld $f(K)$ is een deellichaam van L, dat wil zeggen, een deelring die zelf weer een lichaam is. We kunnen dan K via het isomorfisme $f : K \xrightarrow{\sim} f(K)$ opvatten als deellichaam van L. Het lichaam L heet dan een *uitbreidingslichaam* van K.

(8.1) Lemma-Definitie. *De doorsnede K_0 van alle deellichamen van een lichaam K is een deellichaam van K. Dit lichaam heet het* priemlichaam *van K.*

Bewijs. De verificatie dat K_0 een lichaam is wordt aan de lezer overgelaten.

(8.2) Propositie. *Een priemlichaam is isomorf met het lichaam van de rationale getallen $\mathbb{Q}$ of met een eindig lichaam $\mathbb{Z}/p\mathbb{Z}$ voor een priemgetal p.*

Bewijs. Laat K een lichaam zijn. Dan is er een homomorfisme

$$\phi : \mathbb{Z} \longrightarrow K, \quad n \mapsto n \cdot 1.$$

Het beeld van ϕ is bevat in ieder deellichaam van K omdat ieder deellichaam het element 1 bevat. Nu zijn er twee mogelijkheden:

i) ϕ is niet injectief. Dan is de kern van ϕ een echt ideaal van $\mathbb{Z}$, zeg $\ker(\phi) = (m)$ met $m > 0$. Volgens de isomorfiestelling geldt dan $\mathbb{Z}/m\mathbb{Z} \cong \phi(\mathbb{Z}) \subset K_0$. Omdat K_0 een lichaam is en dus geen nuldelers bezit, moet (m) een priemideaal zijn. Maar dan is $m = p$, een priemgetal. We zien dat K_0 het lichaam $\mathbb{Z}/p\mathbb{Z}$ bevat, dus omdat K_0 het kleinste deellichaam is, moet K_0 gelijk zijn aan $\mathbb{Z}/p\mathbb{Z}$.

ii) ϕ is injectief. Dan bevat K_0 een deelring isomorf met $\mathbb{Z}$. Maar dan bevat K_0 ook het quotiëntenlichaam van deze deelring, en dat quotientenlichaam is isomorf met $\mathbb{Q}$. Dus K_0 bevat een deellichaam isomorf met $\mathbb{Q}$ en dan moet K_0 gelijk zijn aan dit deellichaam. Dit bewijst de propositie.

We zien dat in het eerste geval de *karakteristiek* van K gelijk is aan p, terwijl in het tweede geval de karakteristiek gelijk is aan 0. Als K een eindig lichaam is dan is de karakteristiek van K ongelijk 0.

---

* René Descartes, Frans wiskundige, 1596-1650, die gedurende de periode 1628-1649 in Amsterdam verbleef. Hij introduceerde coördinaten in de meetkunde en maakte die daarmee toegankelijk voor een algebraïsche behandeling.

(8.3) Propositie. *Laat K een lichaam van karakteristiek $p > 0$ zijn. Dan is de afbeelding $F : K \longrightarrow K$, $x \mapsto x^p$ een injectief lichaamshomomorfisme.*

Bewijs. Er geldt

$$F(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

Maar voor $1 \leq i \leq p-1$ zijn de binomiaalcoëfficiënten $\binom{p}{i}$ deelbaar door p in $\mathbb{Z}$ en dus 0 in ons lichaam. Dus vinden we $(x+y)^p = x^p + y^p$. Verder geldt ook $F(xy) = F(x)F(y)$ en $F(1) = 1$. Daarmee is bewezen dat F een lichaamshomomorfisme is. Aangezien ieder lichaamshomomorfisme injectief is volgt nu de bewering.

Het zojuist beschreven lichaamshomomorfisme heet het *Frobenius-homomorfisme**

(8.4) Definitie. Een vectorruimte over K is een (additief geschreven) commutatieve groep V tezamen met een bewerking $K \times V \longrightarrow V$, dat wil zeggen, voor ieder paar $(\lambda \in K, v \in V)$ is een element $\lambda v \in V$ gedefinieerd, met de volgende regels:

i) Voor iedere $\lambda \in V$ en ieder $v_1, v_2 \in V$ geldt

$$\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2.$$

ii) Voor elke $\lambda_1, \lambda_2 \in K$ en $v \in V$ geldt

$$(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v.$$

iii) Voor elke $\lambda_1, \lambda_2 \in K$ en $v \in V$ geldt

$$(\lambda_1 \lambda_2)v = \lambda_1(\lambda_2 v).$$

iv) Voor elke $v \in V$ geldt

$$1\, v = v.$$

We kunnen met vectorruimten over willekeurige lichamen werken zoals we in de lineaire algebra gewend zijn.

(8.5) Lemma. *Laat $K \subset L$ een lichaamsuitbreiding zijn. Dan is L door middels de vermenigvuldiging in L op te vatten als vectorruimte over K.*

Bewijs. De axiomas i) tot en met iv) volgen direct uit de associativiteit en de distributiviteit van de vermenigvuldiging in L.

Een vectorruimte over een lichaam K heet eindig-dimensionaal als V een basis heeft die uit eindig veel elementen bestaat. Het aantal elementen van een basis heet de dimensie van V, genoteerd als $\dim_K V$ en hangt niet af van de gekozen basis. De bewijzen hiervan verlopen als die in de lineaire algebra waar $K = \mathbb{R}$ of $K = \mathbb{C}$. Als V niet een basis heeft bestaande uit eindig veel elementen zeggen we dat $\dim_K V = \infty$.

* F.G. Frobenius, Duits wiskundige, 1849-1917.

(8.6) Definitie. Laat $K \subset L$ een lichaamsuitbreiding zijn. Dan heet de dimensie $\dim_K L$ van L als K-vectorruimte de *graad* van L over K. Notatie:

$$[L : K] = \dim_K L.$$

De lichaamsuitbreiding heet *eindig* als $\dim_K L < \infty$.

(8.7) Voorbeelden. i) De lichaamsuitbreiding $\mathbb{R} \subset \mathbb{C}$ heeft graad 2 want $\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i$ als $\mathbb{R}$-vectorruimte.

ii) De ring $\mathbb{F}_3[X]/(X^2+1)$ is een lichaam met 9 elementen. Omdat een $\mathbb{F}_3$-vectorruimte van dimensie n cardinaliteit 3^n heeft volgt dat de lichaamsuitbreiding

$$\mathbb{F}_3 \subset \mathbb{F}_3[X]/(X^2+1)$$

graad 2 heeft.

iii) Laat k een lichaam zijn. De lichaamsuitbreiding $k \subset k(X)$ met $k(X) = Q(k[X])$ het quotiëntenlichaam van de polynoomring $k[X]$, heeft graad ∞. Immers, de monomen X^i voor $i = 0, 1, 2, \ldots$ zijn lineair onafhankelijk over k.

(8.8) Propositie. *Laat $K \subset L \subset M$ lichaamsuitbreidingen zijn. Dan geldt de identiteit*

$$[M : K] = [M : L][L : K].$$

Bewijs. Laat $\{e_\alpha : \alpha \in A\}$ een basis van de K-vectorruimte L zijn en laat $\{e_\beta : \beta \in B\}$ een basis van de L vectorruimte M zijn. Dan vormen de elementen

$$\{e_\alpha f_\beta : \alpha \in A, \beta \in B\}$$

een basis van de K-vectorruimte M. Immers, laat $x \in M$, dan kunnen we x schrijven als lineaire combinatie $x = \sum_{j=1}^{r} \xi_j f_{\beta_j}$. Ieder van de coëfficiënten $\xi_j \in L$ laat zich weer uitdrukken als een lineaire combinatie $\xi_j = \sum_{k=1}^{s_j} \eta_k e_{\alpha_k}$ met $\eta_k \in K$. Substitueren we dit in de uitdrukking voor x dan krijgen we een schrijfwijze van x als (eindige) lineaire combinatie $\sum c_{\alpha\beta} e_\alpha f_\beta$ van elementen $e_\alpha f_\beta$. Dit bewijst dat de $e_\alpha f_\beta$ de K-vectorruimte M voortbrengen. Om in te zien dat deze elementen lineair onafhankelijk zijn, merken we op dat de coëfficiënten ξ_j eenduidig bepaald zijn door x omdat de e_α een basis vormen. Zo zijn ook de coëfficiënten η_k eenduidig bepaald. Dus de coëfficiënten $c_{\alpha\beta}$ zijn eenduidig bepaald en dus vormen de $e_\alpha f_\beta$ een basis. Dit bewijst de propositie.

Laat nu K een lichaam zijn en L een lichaamsuitbreiding van K. Als $\alpha \in L$ een element van L is kunnen we kijken naar het *kleinste deellichaam* van L dat α bevat.

(8.9) Definitie. Het lichaam $K(\alpha)$ is de doorsnede van alle deellichamen van L die K en α bevatten.

Het heeft ook zin de *kleinste deelring* van L te bekijken die α bevat. Deze ring moet alle veeltermen van de vorm $\sum_{i=1}^{n} a_i \alpha^i$ met $n \in \mathbb{Z}_{\geq 0}$ en $a_i \in K$ bevatten. We definiëren daarom

$$K[\alpha] = \{\sum_{i=1}^{n} a_i \alpha^i : n \in \mathbb{Z}_{\geq 0},\ a_i \in K\}.$$

Het is niet moeilijk na te gaan dat dit inderdaad een deelring van L is. Algemener, als $\alpha_1, \ldots, \alpha_m \in L$ dan is $K(\alpha_1, \ldots, \alpha_m)$ per definitie het kleinste deellichaam van L dat $\alpha_1, \ldots, \alpha_m$ bevat. Er geldt

$$K(\alpha_1, \ldots, \alpha_m) = K(\alpha_1, \ldots, \alpha_{m-1})(\alpha_m).$$

We zeggen dat het lichaam $K(\alpha)$ uit K is verkregen door *adjunctie van het element* α.

We maken nu een belangrijk onderscheid in twee gevallen.

(8.10) Definitie. Laat $K \subset L$ een lichaamsuitbreiding zijn en $\alpha \in L$. Dan heet α *algebraïsch* over K als er een polynoom $f \in K[X]$ is met $f \neq 0$ zodat $f(\alpha) = 0$. Een lichaamsuitbreiding $K \subset L$ heet *algebraïsch* als ieder element $\alpha \in L$ algebraïsch over K is. Een element $\alpha \in L$ heet *transcendent* over K als α niet algebraïsch over K is.

Merk op dat we in de definitie van algebraïsch net zo goed hadden kunnen eisen dat er een *irreducibel* polynoom in $K[X]$ is waarvan α een nulpunt is. Immers, als $f \in K[X]$ een polynoom $\neq 0$ is met $f(\alpha) = 0$ dan kunnen we f ontbinden als product van irreducibele polynomen

$$f = f_1 \cdot f_2 \cdots f_r$$

en uit $f(\alpha) = 0$ volgt dat minstens een van de $f_i(\alpha) = 0$.

(8.11) Voorbeelden.

i) Laat $i = \sqrt{-1} \in \mathbb{C}$. Dit element i is algebraïsch over $\mathbb{R}$ en $\mathbb{C} = \mathbb{R}(i)$. Het element i is ook algebraïsch over $\mathbb{Q}$ en de ring $\mathbb{Q}[i]$ bestaat uit alle elementen van de vorm $a + bi$ met $a, b \in \mathbb{Q}$. Een quotiënt $(a + bi)/(c + di)$ laat zich schrijven als $(a + bi(c - di)/(c^2 + d^2)$ en ligt ook in $\mathbb{Q}[i]$, dus $\mathbb{Q}(i) = \mathbb{Q}[i]$.

ii) Laat K een lichaam zijn en $K[X]$ de polynoomring over K. Zij verder $L = Q(K[X])$ het quotiëntenlichaam van $K[X]$. Dan is X een transcendent element en er geldt $K(X) = L$.

(8.12) Stelling. *Laat $K \subset L$ een lichaamsuitbreiding zijn en $\alpha \in L$ een element van L. Dan zijn de volgende uitspraken equivalent:*

i) Het element α is algebraïsch.
ii) $K(\alpha) = K[\alpha]$.
iii) De graad $[K(\alpha) : K]$ is eindig.

Bewijs. i) $\Rightarrow$ ii). Laat f een irreducibel polynoom zijn in $K[X]$ met $f(\alpha) = 0$. Beschouw dan het homomorfisme

$$\psi : K[X] \longrightarrow K[\alpha] \subset L, \quad \text{gegeven door} \quad X \mapsto \alpha.$$

Deze afbeelding is surjectief. Omdat $f(\alpha) = 0$ (en dus $(f) \subset \ker(\psi)$) factoriseert deze afbeelding via een homomorfisme

$$\psi' : K[X]/(f) \longrightarrow K[\alpha].$$

Omdat f irreducibel is, is (f) een maximaal ideaal (zie (6.2)) en dus is $K[X]/(f)$ een lichaam, en ψ' is dan een surjectief lichaamshomomorfisme, dus een isomorfisme $K[X]/(f) \cong K[\alpha]$. Dus $K[\alpha]$ is een lichaam, zodat $K[\alpha] = K(\alpha)$.

ii) $\Rightarrow$ iii). Omdat $K[\alpha] = K(\alpha)$ is $K[\alpha]$ een lichaam. Laat I de kern zijn van het homomorfisme

$$\psi : K[X] \longrightarrow K[\alpha] \subset L, \quad \text{gegeven door} \quad X \mapsto \alpha.$$

Omdat $K[X]$ geen lichaam is, volgt $I \neq (0)$. Maar dan is $I = (f)$ voor een polynoom $\neq 0$ in $K[X]$. Omdat $K[\alpha]$ een lichaam moet I een maximaal ideaal zijn en dus is f een irreducibel element. Laat $d = \deg(f)$. We mogen na vermenigvuldiging met een geschikte constante aannemen dat f monisch is, zeg $f = X^d + a_1X^{d-1} + \ldots + a_d$. Dan geldt

$$\alpha^d = -a_1\alpha^{d-1} + \ldots - a_d. \tag{1}$$

We beweren nu dat ieder element van $K[\alpha]$ geschreven kan worden als lineaire combinatie

$$\sum_{i=0}^{d-1} r_i\,\alpha^i \quad \text{met } r_i \in K \tag{2}$$

Immers, we kunnen (1) gebruiken om hogere machten te verwijderen; meer precies, als $g \in K[X]$ en $\beta = g(\alpha)$ is een element van $K[\alpha]$, dan passen we deling met rest toe op g en vinden q en $r \in K[X]$ zodat

$$g = qf + r$$

met $r = 0$ of $\deg(r) < \deg(f) = d$. Substitueren we nu α dan vinden we $g(\alpha) = r(\alpha)$ en dit is van de vorm (2). Daarmee hebben we een basis $1, \alpha, \ldots, \alpha^{d-1}$ van $K[\alpha]$ gevonden.

iii) $\Rightarrow$ i). Laat de dimensie van $K(\alpha)$ als K-vectorruimte gelijk zijn aan d. Dan zijn de vectoren

$$1, \alpha, \alpha^2, \ldots, \alpha^d$$

noodzakelijkerwijs lineair afhankelijk. Maar dat betekent dat er elementen $a_i \in K$, niet allemaal 0, zijn zodat $\sum_{i=0}^{d} a_i\alpha^i = 0$, met andere woorden, α is een nulpunt van het polynoom $f = \sum_{i=0}^{d} a_iX^i$. Dit bewijst de stelling.

(8.13) Gevolg. *Laat $K \subset L$ een lichaamsuitbreiding van eindige graad zijn. Dan is ieder element van L algebraïsch over K.*

Bewijs. Voor ieder element $\alpha \in L$ is $K(\alpha)$ een deellichaam van L. Omdat $K(\alpha)$ een lineaire deelruimte van L is, is $K(\alpha)$ een lichaamsuitbreiding van eindige graad over K. Maar dan is volgens Stelling (8.12) het element α algebraïsch.

Het geval dat α transcendent is laat zich nu ook als volgt karakterizeren.

(8.14) Gevolg. *Laat $K \subset L$ een lichaamsuitbreiding zijn en $\alpha \in L$ een element van L. Dan zijn de volgende uitspraken equivalent:*

i) Het element α is transcendent over K.
ii) $K[\alpha]$ is isomorf met de polynoomring $K[X]$.
iii) $K(\alpha)$ is een oneindig-dimensionale K-vectorruimte.

Bewijs. i) $\Rightarrow$ ii). Het surjectieve ringhomomorfisme $\psi : K[X] \longrightarrow K[\alpha]$ heeft kern (0) omdat α transcendent is. Dit bewijst ii). ii)$\rightarrow$ iii). Omdat de machten α^i met

$i \in \mathbb{Z}$ lineair onafhankelijk zijn over K volgt dat $\dim_K(K(\alpha)) = \infty$. iii) $\Rightarrow$ i). Was α algebraïsch, dan zou $\dim_K(K(\alpha) < \infty$ gelden, in tegenspraak met iii).

(8.15) Definitie. Laat $K \subset L$ een lichaamsuitbreiding zijn en $\alpha \in L$ een algebraïsch element en $\psi : K[X] \to K[\alpha]$ het homomorfisme met $X \mapsto \alpha$. Dan heet het monisch polynoom $f \in K[X]$ met $(f) = \ker(\psi)$ het *minimumpolynoom* van α over K. Notatie: $f^{\alpha}_{\min}$ of ook wel $f^{\alpha}_{\min,K}$.

Met andere woorden, $f^{\alpha}_{\min}$ is het monische polynoom van minimale graad in $K[X]$ waarvan α een nulpunt is.

(8.16) Propositie. *Laat $K \subset L$ een lichaamsuitbreiding zijn en $\alpha \in L$ een algebraïsch element van L. Dan geldt*
i) $K(\alpha) \cong K[X]/(f^{\alpha}_{\min})$.
ii) $[K(\alpha) : K] = \deg(f^{\alpha}_{\min})$.

Bewijs. De isomorfiestelling impliceert direct i). Laat $\beta = g(\alpha)$ met $g \in K[X]$. Deling van g door $f = f^{\alpha}_{\min}$ in $K[X]$ levert $g = qf + r$ met $r = 0$ of $\deg(r) < \deg(f)$, dus $g(\alpha) = r(\alpha)$. Dit laat zien dat de elementen $1, \alpha, \ldots, \alpha^{d-1}$ voortbrengers van de K-vectorruimte $K(\alpha)$ zijn. Deze elementen zijn lineair onafhankelijk want anders is er een polynoom $0 \neq h \in K[X]$ met graad $< d = \deg(f)$ zodat $h(\alpha) = 0$, in tegenspraak met de minimaliteit van $f^{\alpha}_{\min}$. Dit bewijst ii).

Laat K een lichaam zijn en $f \in K[X]$ een polynoom met $f \notin K$. Zoals we gezien hebben heeft f niet altijd een nulpunt in K. Maar we kunnen altijd een lichaamsuitbreiding L van K construeren waarin f wel een nulpunt heeft als volgt.

Het is geen beperking van de algemeenheid als we veronderstellen dat f irreducibel is in $K[X]$. Dan is (f) een maximaal ideaal omdat $K[X]$ een hoofdideaalring is, zie (6.2). Dus

$$L = K[X]/(f)$$

is een lichaam dat K als deellichaam bevat omdat $(f) \cap K = (0)$. In dit lichaam heeft f een nulpunt, namelijk de restklasse van X:

$$\overline{f(X)} = f(\overline{X}) = 0 \quad \text{in} \quad K[X]/(f).$$

(8.17) Conclusie. *Laat $f \in K[X]$ een niet-constant polynoom zijn. Dan is er een lichaamsuitbreiding L van K waarin f een nulpunt heeft.*

Bewijs. Laat $f = f_1 \cdots f_r$ een ontbinding zijn van f in irreducibele factoren. Dan is $K[X]/(f_1)$ een lichaam waarin f_1 een nulpunt $\alpha = \bar{X}$ heeft. Maar dan is α ook nulpunt van f.

Als $f \in K[X]$ een nulpunt $\alpha \in L$ heeft in L dan kunnen we f schrijven als $f = (X - \alpha)f_1$ met $f_1 \in L[X]$. We kunnen nu ook verdergaan en proberen een lichaam te vinden waarin een gegeven polynoom in lineaire factoren uiteenvalt. Zo een lichaam bestaat en is op isomorfisme na eenduidig.

(8.18) Definitie. Laat K een lichaam zijn en $f \in K[X]$ een polynoom $\neq 0$. Een lichaamsuitbreiding L van K heet *ontbindingslichaam* van f over K als er elementen $c \in K$ en $\alpha_1, \ldots, \alpha_d \in L$ zijn zodat

i) $f = c(X - \alpha_1)\dots(X - \alpha_d)$ in $L[X]$;
ii) $L = K(\alpha_1, \dots, \alpha_d)$.

Als voorbeeld: het lichaam $\mathbb{C}$ is het ontbindingslichaam van $X^2 + 1 \in \mathbb{R}[X]$ over $\mathbb{R}$.

(8.19) Stelling. *Laat K een lichaam zijn en $f \in K[X]$ een niet-constant polynoom. Dan bestaat er een ontbindingslichaam van f over K. Als L en L' twee ontbindingslichamen van f over K zijn, dan is er een lichaamsisomorfisme $\phi : L \to L'$ waarvan de beperking tot K de identiteit op K is.*

Bewijs. We moeten zowel de existentie als de eenduidigheid op isomorfie na van het ontbindingslichaam aantonen. We beginnen met de existentie, en bewijzen dit door middel van inductie naar de graad $\deg(f)$. Als f graad ≤ 1 heeft dan is de existentie duidelijk. (Er geldt $f = c$ of $f = c(X - \alpha)$ met $\alpha \in K$. Dus $L = K$.)

Nemen we aan dat de existentie bewezen is voor f met $\deg(f) < d$. Stel dat $f \in K[X]$ graad d heeft. We onderscheiden nu twee gevallen:

i) f is reducibel, zeg $f = gh$ met $\deg(g) = \gamma < d$ en $\deg(h) < d$. Dan is er een lichaam L_g en elementen $\alpha_1, \dots, \alpha_\gamma$ in L_g zodat

$$g = c_g(X - \alpha_1)\dots(X - \alpha_\gamma) \qquad \text{met} \quad c_g \in K.$$

Evenzo is er een lichaam L_h en elementen $\alpha_{\gamma+1}, \dots, \alpha_d \in L_h$ met

$$h = c_h(X - \alpha_{\gamma+1})\dots(X - \alpha_d) \qquad \text{met} \quad c_h \in K.$$

Dan geldt

$$f = c_g c_h(X - \alpha_1)\dots(X - \alpha_d)$$

en $L = L_g(\alpha_{\gamma+1}, \dots, \alpha_d) = K(\alpha_1, \dots, \alpha_d)$ is een ontbindingslichaam van f.

ii) f is irreducibel. Maar dan heeft f in $K[X]/(f)$ een nulpunt, dus

$$f = c(X - \alpha_1)f_1 \quad \in K[X]/(f).$$

Met inductie weten we dan dat f_1 een ontbindingslichaam $L_1 = K(\alpha_2, \dots, \alpha_d)$ heeft. Dan is $L = L_1(\alpha) = K(\alpha_1, \dots, \alpha_d)$ een ontbindingslichaam van f. Daarmee is de existentie bewezen. Om de eenduidigheid in te zien bewijzen we een iets algemener feit in de volgende propositie.

(8.20) Propositie. *Gegeven zijn twee lichamen K en K' en een lichaamsisomorfisme $\sigma : K \to K'$. Laat $f = \sum_{i=0}^{d} a_i X^i \in K[X]$ en laat L een ontbindingslichaam van f over K zijn. Laat verder L' het ontbindingslichaam van $f' = \sum_{i=0}^{n} \sigma(a_i)X^i \in K'[X]$ over K' zijn. Dan is er een lichaamsisomorfisme $\tau : L \longrightarrow L'$ dat beperkt tot K gelijk is aan σ.*

Bewijs van de Propositie. Het bewijs wordt gevoerd met inductie naar de graad van f. Als $g = \sum b_i X^i \in K[X]$ schrijven we $\sigma(g)$ voor het polynoom $\sum \sigma(b_i)X^i \in K'[X]$.

Als f graad 1 heeft, dan heeft $f' = \sigma(f)$ dat ook en we vinden $L = K$ en $L' = K'$. Wanneer we $\tau = \sigma$ kiezen, zijn we klaar.

Laat nu f een polynoom van graad > 1 zijn en laat g een irreducibele factor van f zijn in $K[X]$. Toepassen van σ levert een irreducibele factor $\sigma(g)$ van $f' = \sigma(f)$ en als α een nulpunt van g in L is en α' een nulpunt van $\sigma(g)$ in L', dan geeft de rij isomorfismen

$$K(\alpha) \cong K[X]/(g) \xrightarrow{\sigma} K'[X]/(\sigma(g)) \cong K(\alpha')$$

een isomorfisme $\sigma_1 : K_1 = K(\alpha) \cong K_1' = K'(\alpha')$ dat beperkt tot K gelijk is aan σ. We kunnen nu de inductiehypothese toepassen op de lichamen K_1, K_1' en het isomorfisme σ_1 en de ontbindingslichamen van $f_1 = f/(X-\alpha)$ en van $f_1' = \sigma(f)/(X-\alpha')$. Merk op dat het ontbindingslichaam van $f/(X-\alpha)$ gelijk is aan L en dat van $f'/(X-\alpha')$ is gelijk aan L'. We vinden dan een isomorfisme $L \cong L'$ dat beperkt tot K gelijk is aan σ. Dit bewijst de propositie.

Toepassen van de propositie op het geval $K = K'$ en σ de identieke afbeelding van K levert de gewenste eenduidigheid van het ontbindingslichaam. Dit bewijst de stelling.

Als $K \subset L$ een uitbreiding van lichamen is, kunnen we in L de verzameling van alle elementen die algebraïsch zijn over K beschouwen:

$$\{x \in L : x \text{ is algebraïsch over } K\}$$

We beweren dat dit een deellichaam van L is: immers, zijn x en y algebraïsch over K dan is $K(x,y)$ een eindige uitbreiding van K en met (8.13) volgt dan dat ook $x \pm y$ en xy en x^{-1} algebraïsch zijn.

We kunnen in het bizonder het deellichaam

$$\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ is algebraïsch over } \mathbb{Q}\}$$

bekijken. Dit heet het lichaam van de algebraïsche getallen.

De transcendente getallen liggen niet in $\overline{\mathbb{Q}}$. De bekendste voorbeelden van transcendente getallen zijn:

$$\pi = 3.14159265358979323846264338 3...,$$

de halve omtrek van een cirkel met straal 1 en

$$e = \lim_{n\to\infty}(1+\frac{1}{n})^n = 2.71828182845904523536028747 1...,$$

de basis van de natuurlijke logaritme; ook de constante van Euler

$$\gamma = 0.57721566490153286060651209 00...$$

gedefinieerd door

$$\gamma = \lim_{n\to\infty}(1+\frac{1}{2}+\ldots+\frac{1}{n}-\log(n))$$

wordt geacht transcendent te zijn, maar dit is nog niet bewezen. Dat e transcendent was werd in 1873 bewezen door Hermite.* Het feit dat π transcendent is was een belangrijk

* Ch. Hermite, Frans wiskundige , 1822-1901

wapenfeit aan het eind van de 19de eeuw (1882) en staat op naam van Lindemann*. De transcendentie van π impliceert de onmogelijkheid van de kwadratuur van de cirkel; zie Algebra 2b.

(8.21) Definitie. Een lichaam K heet *algebraïsch afgesloten* als ieder niet-constant polynoom $f \in K[X]$ een nulpunt in K heeft.

Als K algebraïsch afgesloten is, dan valt ieder niet-constant polynoom $f \in K[X]$ uiteen in lineaire factoren.

(8.22) Stelling. *Het lichaam $\mathbb{C}$ van de complexe getallen is algebraïsch afgesloten.*

Het bewijs wordt gegeven in Algebra 2b.

Opgaven

1) Laat $f : K \to L$ een homomorfisme van lichamen zijn. Bewijs dat f een isomorfisme van de priemlichamen van K en L induceert.

2) Laat zien dat de karakteristiek van een eindig lichaam ongelijk 0 is.

3) Laat K een lichaam zijn en $\sigma : K \to K$ een lichaamshomomorfisme. Laat zien dat

$$K^\sigma = \{x \in K : \sigma(x) = x\}$$

een deellichaam van K is. Bewijs dat σ gelijk is aan de identiteit op het priemlichaam van K.

4) Laat zien dat complexe conjugatie $\sigma : \mathbb{C} \to \mathbb{C}$ met $z \mapsto \bar{z}$ een lichaamsautomorfisme is. Bepaal $\mathbb{C}^\sigma$.

5) Laat K een lichaam van karakteristiek $p > 0$ zijn.

i) Laat zien dat voor ieder positief geheel getal n de verzameling $\{x^{p^n} : x \in K\}$ een deellichaam van K is.

ii) Laat verder zien dat voor ieder positief geheel getal n de verzameling $\{x \in K : x^{p^n} = x\}$ een deellichaam met ten hoogste p^n elementen is.

6) Laat $\alpha = \sqrt{3} \in \mathbb{R}$ en stel $K = \mathbb{Q}(\sqrt{3})$. Bereken de graad $[K : \mathbb{Q}]$. Bewijs dat ieder element van K algebraïsch is over $\mathbb{Q}$.

7) Laat $n \in \mathbb{Z}_{\geq 1}$ en laat $\alpha = \sqrt[n]{5} \in \mathbb{C}$. Bewijs dat het minimumpolynoom $f^\alpha_{\min}$ van α over $\mathbb{Q}$ gelijk is aan $X^n - 5$.

8) Bereken de minimumpolynomen van de volgende algebraïsche getallen over $\mathbb{Q}$:

$$3 + \sqrt{2}, \sqrt{2} + \sqrt{3}, \sqrt[3]{2} + \sqrt[3]{4}, \sqrt{2 + 3\sqrt{3}}.$$

9) Laat $\alpha \in \bar{\mathbb{Q}}$ een nulpunt zijn van $X^3 + X + 1 \in \mathbb{Q}[X]$. Bereken de minimumpolynomen van α^{-1} en $\alpha - 1$. Schrijf verder de volgende elementen in de vorm $r_0 + r_1\alpha + r_2\alpha^2$ met $r_0, r_1, r_2 \in \mathbb{Q}$:

$$\alpha^4, \alpha^{-2}, (\alpha^4 + 1)^{-1}.$$

10) Laat $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Bewijs:

---

* C.L.F. von Lindemann, Duits wiskundige, 1852-1939.

i) $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
ii) Bewijs $[K : \mathbb{Q}] = 4$.
iii) Bereken het minimumpolynoom van $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
iv) Laat zien dat er geen $x, y \in \mathbb{Q}$ bestaan zodat $(x + y\sqrt{2})^2 = 3$.

11) Laat $\zeta \in \mathbb{C}$ een nulpunt van het polynoom $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ zijn.
i) Bewijs dat ζ een vijfdemachts eenheidswortel is.
ii) Laat zien dat ζ, ζ^2, ζ^3 en ζ^4 de wortels van f zijn.
iii) Bewijs dat het ontbindingslichaam van f over $\mathbb{Q}$ gelijk is aan $\mathbb{Q}(\zeta)$.

12) Laat $f = X^2 + 1 \in \mathbb{F}_3[X]$. Bewijs: het ontbindingslichaam van f heeft 9 elementen.

13) Laat α, β algebraïsche elementen in een uitbreidingslichaam L van een lichaam K zijn met hetzelfde minimumpolynoom. Bewijs dat $K(\alpha) \cong K(\beta)$.

14 Laat K een lichaam zijn en α, β twee algebraïsche elementen in een uitbreidingslichaam L van K.
i) Bewijs dat $[K(\alpha) : K]$ en $[K(\beta) : K]$ delers zijn van $[K(\alpha, \beta) : K]$.
ii) Bewijs dat $[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K]$.

15) Bewijs dat $\mathbb{Q}(\sqrt{2}, \sqrt{-1}) = \mathbb{Q}(\sqrt{2} + \sqrt{-2})$.

16) Ga na of de volgende idealen maximaal in $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ en $\mathbb{R}[X]$ zijn:

$$(2), \quad (X^2 + 1), \quad (X^3 + 1), \quad (X^4 + 1).$$

9. Eindige Lichamen

On voit ici cette conséquence remarquable, que toutes les quantités algébriques qui peuvent se présenter dans la théorie, sont racines d'equations de la forme $x^{p^\nu} = x$
E. Galois *

In dit hoofdstuk vormen eindige lichamen het onderwerp. Een lichaam K heet eindig als het aantal elementen van K eindig is. Voorbeelden kennen we al: de lichamen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ zijn eindige lichamen. Deze voorbeelden waren bekend aan Euler, Gauss en Legendre, maar het was Galois die eindige lichamen expliciet in de wiskunde heeft geïntroduceerd.

Laat K een eindig lichaam zijn. Dan is het priemlichaam K_0 van K ook eindig, en dus gelijk aan $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ voor een priemgetal p. We kunnen dan K opvatten als uitbreidingslichaam van $\mathbb{F}_p$ en K is dan ook een eindig-dimensionale $\mathbb{F}_p$-vectorruimte. Als de dimensie van deze vectorruimte gelijk is aan n, dan heeft K dus p^n elementen. We concluderen dat het aantal elementen van een eindig lichaam een macht van een priemgetal is.

(9.1) Propositie. *Laat K een eindig lichaam zijn van cardinaliteit $q = p^n$ met p een priemgetal. Dan voldoet elk element van K aan de vergelijking*

$$X^q - X = 0.$$

Bewijs. De multiplicatieve groep K^* is een eindige abelse groep van orde $q-1$ en deze groep is cyklisch, zoals elke eindige ondergroep van de multiplicatieve groep van een lichaam, zie (4.15). Dus ieder element $x \in K^*$ voldoet aan $x^{q-1} = 1$ en dus ook aan $x^q = x$. Omdat 0 hieraan ook voldoet is ieder element van K nulpunt van $X^q - X$. Dit bewijst de propositie.

Alhoewel Galois al in 1830 eindige lichamen invoerde, heeft het lang geduurd voordat eindige lichamen algemeen ingang hadden gevonden in de wiskunde. De Amerikaanse wiskundige Moore** was de eerste die de eindige lichamen geklassificeerd heeft.

(9.2) Stelling. *Een natuurlijk getal q is de cardinaliteit van een eindig lichaam dan en slechts dan als q een positieve macht van een priemgetal is. Een lichaam van cardinaliteit q is op isomorfie na eenduidig bepaald.*

Bewijs. We hebben al gezien dat een eindig lichaam een vectorruimte van eindige dimensie over zijn priemlichaam $\mathbb{F}_p$ is, en dat daarmee de cardinaliteit q een positieve macht van een priemgetal p is. Wat rest is in te zien dat er voor ieder priemgetal p en iedere $n \in \mathbb{Z}_{\geq 1}$ een lichaam van cardinaliteit $q = p^n$ bestaat en dat twee zulke lichamen

* E. Galois, Frans wiskundige, 1811-1832, wiens ideeen een cruciale rol in de ontwikkeling van de algebra gespeeld hebben.

** E.H. Moore, Amerikaans wiskundige, 1862-1932, die een prominente rol speelde in de opbouw van de wiskunde in de Verenigde Staten.

isomorf zijn. Gezien Propositie (9.1) nemen we het polynoom $f = X^q - X \in \mathbb{F}_p[X]$. We weten dat er een ontbindingslichaam K van $X^q - X$ over $\mathbb{F}_p$ bestaat. Laat

$$K' = \{x \in K : x^q = x\}$$

Volgens Opgave 3 van Hoofdstuk 7 is dit een deellichaam van K en bestaat uit de nulpunten van f. Omdat K het ontbindingslichaam van f is moet dan gelden $K' = K$. Verder is de afgeleide van f gelijk is aan $qX^{q-1} - 1 = -1 \in \mathbb{F}_p[X]$ en dus heeft f geen meervoudige nulpunten. Dus de q nulpunten van f vormen het lichaam K. Omdat K het ontbindingslichaam is van $X^q - X$ over $\mathbb{F}_p$ volgt dat K op isomorfie na eenduidig bepaald is. Dit bewijst de stelling.

(9.3) Notatie. We schrijven $\mathbb{F}_q$ voor een lichaam met q elementen.

(9.4) Gevolg. *Laat q een positieve macht van een priemgetal p zijn. Dan geldt de identiteit*

$$X^q - X = \prod_{a \in \mathbb{F}_q} (X - a) \qquad \text{in} \quad \mathbb{F}_q[X].$$

(9.5) Voorbeelden.

i) Laat $K = \mathbb{F}_2[X]/(X^2 + X + 1)$. Omdat $X^2 + X + 1 \in \mathbb{F}_2[X]$ een irreducibel polynoom is, is K een lichaam en vanwege (8.16) is de cardinaliteit van K gelijk aan 4. Dus $K \cong \mathbb{F}_4$ en $\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \mathbb{F}_2(\alpha)$ met α een nulpunt van $X^2 + X + 1$. Er geldt $\alpha^3 = 1$ en we kunnen α opvatten als een derde-machts eenheidswortel.

ii) Laat $K = \mathbb{F}_3[X]/(X^2 + 1)$. Dit is een lichaam omdat $X^2 + 1 \in \mathbb{F}_3[X]$ irreducibel is en heeft 9 elementen, dus $K \cong \mathbb{F}_9$. We kunnen schrijven $\mathbb{F}_9 = \mathbb{F}_3(i) = \mathbb{F}_3[i]$, waarbij i een element in $\mathbb{F}_9$ is met $i^2 = -1$. De cyklische groep $\mathbb{F}_9^*$ heeft orde 8 en wordt voortgebrcht door $1 + i$ (Ga na).

We hebben al opgemerkt dat de multiplicatieve groep $\mathbb{F}_q^*$ een cyklische groep is. We kunnen dit nu gebruiken om een andere beschrijving van $\mathbb{F}_q$ te geven.

(9.6) Stelling. *Laat p een priemgetal zijn en $q = p^n$ met $n \geq 1$. Dan is er een isomorfisme*

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha)$$

waarbij $f \in \mathbb{F}_p[X]$ een irreducibel polynoom van graad n is en α een nulpunt van f.

Bewijs. Laat $\alpha \in \mathbb{F}_q^*$ een voortbrenger van de cyklische groep $\mathbb{F}_q^*$ zijn en laat f het minimumpolynoom van α over $\mathbb{F}_p$ zijn. Dan geldt

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha) \subset \mathbb{F}_q$$

en omdat de orde van α in $\mathbb{F}_q^*$ gelijk is aan $q - 1$ bevat $\mathbb{F}_p(\alpha)$ tenminste q elementen. Dus volgt $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Dit bewijst de stelling.

Blijkbaar bestaat er voor iedere $n \geq 1$ een irreducibel polynoom van graad n in $\mathbb{F}_p[X]$.

Een voor de hand liggende vraag is die naar de deellichamen van een eindig lichaam $\mathbb{F}_q$. De volgende stelling beantwoordt deze vraag.

(9.7) Stelling. *Laat $q = p^n$ met $n \geq 1$ een macht van een priemgetal zijn. De deellichamen van $\mathbb{F}_q$ zijn de deellichamen $\mathbb{F}_{p^m}$ met m een deler van n en zijn gegeven door*

$$\{x \in \mathbb{F}_q : x^{p^m} = x\}.$$

Bewijs. Laat $K \subset \mathbb{F}_q$ een deellichaam van $\mathbb{F}_q$ zijn met p^m elementen. Dan is $\mathbb{F}_q$ een K-vectorruimte van dimensie d, dus $q = p^n = \#\mathbb{F}_q = (\#K)^d = p^{md}$, dat wil zeggen $n = dm$ en m is een deler van n.

Omgekeerd, neem aan dat m een deler is van n, zeg $n = dm$. Merk op dat als a een deler is van b dan deelt $X^a - 1$ het polynoom $X^b - 1$ in $\mathbb{Z}[X]$. (Ga na.) Er geldt

$$\frac{p^n - 1}{p^m - 1} = p^{(d-1)m} + p^{(d-2)m} + \ldots + p^m + 1,$$

zodat $X^{p^m-1} - 1$ het polynoom $X^{p^n-1} - 1$ deelt. Dus $X^{p^m} - X$ deelt $X^{p^n} - X$ in $\mathbb{F}_p[X]$ en we zien dat de nulpunten van $X^{p^m} - X$ een deellichaam van $\mathbb{F}_q$ vormen dat isomorf is met $\mathbb{F}_{p^m}$. Dit bewijst de stelling.

We kunnen uit deze stelling afleiden hoe het polynoom $X^{q^r} - X$ in irreducibele factoren uiteenvalt in $\mathbb{F}_{q^r}[X]$.

(9.8) Stelling. *In $\mathbb{F}_q[X]$ is er de ontbinding*

$$X^{q^r} - X = \prod_f f,$$

waarbij het product loopt over alle monische irreducibele polynomen van $\mathbb{F}_q[X]$ waarvan de graad een deler is van r.

Bewijs. Omdat de ring $\mathbb{F}_q[X]$ een ontbindingsring is, kunnen we $X^{q^r} - X$ eenduidig in irreducibele factoren ontbinden. We mogen verder aannemen dat deze factoren monisch zijn. We moeten nu laten zien dat een irreducibel monisch polynoom $f \in \mathbb{F}_q[X]$ een deler van $X^{q^r} - X$ is dan en slechts dan als de graad van f een deler is van r.

Laat $f \in \mathbb{F}_q[X]$ monisch en irreducibel zijn. Als α een nulpunt van f is in een ontbindingslichaam van f over $\mathbb{F}_q$ is, dan is $\mathbb{F}_q(\alpha)$ isomorf met $\mathbb{F}_q[X]/(f)$ en dus isomorf met $\mathbb{F}_{q^d}$ met d de graad van f. Er geldt nu op grond van Stelling (9.7)

$$d \quad \text{deelt} \quad r \iff \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^r} \iff \alpha \in \mathbb{F}_{q^r}$$

en ook

$$\alpha \in \mathbb{F}_{q^r} \iff \alpha \text{ is nulpunt van } X^{q^r} - X.$$

Maar de kern van de afbeelding $\mathbb{F}_q[X] \to \mathbb{F}_q(\alpha)$ met $X \mapsto \alpha$ is het ideaal voortgebracht door het minimumpolynoom f van α. Dus we vinden

$$d \quad \text{deelt} \quad r \iff f \quad \text{deelt} \quad X^{q^r} - X.$$

Dit bewijst de stelling.

Vergelijken van de graden geeft het volgende resultaat.

(9.9) Gevolg. *Laat i_d het aantal irreducibele monische polynomen in $\mathbb{F}_q[X]$ van graad d zijn. Dan geldt voor alle $n > 0$ de gelijkheid*

$$\sum_{d|n} i_d\, d = q^n,$$

waarbij de som loopt over alle positieve delers d van n.

We weten al dat de afbeelding $\mathbb{F}_q \to \mathbb{F}_q$ gegeven door $x \mapsto x^p$ een automorfisme van $\mathbb{F}_q$ definieert, het Frobenius-homomorfisme.

(9.10) Stelling. *Laat $q = p^n$. De automorfismengroep $\mathrm{Aut}(\mathbb{F}_q)$ is isomorf met $\mathbb{Z}/n\mathbb{Z}$ en wordt voortgebracht door het Frobenius-automorfisme F.*

Bewijs. Het is gemakkelijk na te gaan dat de lichaamsautomorfismen van $\mathbb{F}_q$ een groep vormen. Uit $F(x) = x^p$ volgt $F^n(x) = x^{p^n} = x$, dus de orde van F is een deler van n. Als F^r de identiteit is, dan is ieder element van $\mathbb{F}_q$ een nulpunt van $X^{p^r} - X$ en dat kan niet voor $r < n$. Dus is de orde van F gelijk aan n.

We moeten nog inzien dat ieder automorfisme σ van $\mathbb{F}_q$ een macht van F is. Daarvoor schrijven we $\mathbb{F}_q$ als $\mathbb{F}_p(\alpha)$ met α een nulpunt van een irreducibel polynoom $f \in \mathbb{F}_p[X]$. Dan is $\sigma(\alpha)$ ook een nulpunt van f; immers, als $f = \sum_{i=0}^n a_i X^i$ met $a_i \in \mathbb{F}_p$ dan $\sigma(a_i) = a_i$ en

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

Dus voor ieder nulpunt α van f is ook $\sigma(\alpha)$ een nulpunt van f. Maar omdat f hoogstens n nulpunten heeft in $\mathbb{F}_q$ betekent dit dat er maar n mogelijkheden voor $\sigma(\alpha)$ zijn. Omdat σ volledig vastligt door het beeld van α zijn er hoogstens n automorfismen van $\mathbb{F}_q$. Dit bewijst de stelling.

(9.11) Stelling. *Laat $f \in \mathbb{F}_q[X]$ een monisch en irreducibel polynoom van graad n zijn en α een nulpunt van f in een uitbreidingslichaam van $\mathbb{F}_q$. Dan kunnen we f ontbinden als*

$$f = \prod_{i=0}^{n-1} (X - \alpha^{q^i}) \qquad \text{in} \quad \mathbb{F}_q(\alpha)[X].$$

Bewijs. De afbeelding $\mathbb{F}_q(\alpha) \to \mathbb{F}_q(\alpha)$ gegeven door $x \mapsto x^q$ is een automorfisme van $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^n}$. Laat $f = \sum_{i=0}^n a_i X^i \in \mathbb{F}_q[X]$. We berekenen nu

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

Dus de elementen α^{q^i} zijn allemaal nulpunten van f in $\mathbb{F}_{q^n}$. We laten nu zien dat de elementen α^{q^i} met $i = 0, \ldots, n-1$ allemaal verschillend zijn en vinden zo n verschillende nulpunten en de gevraagde ontbinding. Stel dat $\alpha^{q^i} = \alpha^{q^j}$ voor $0 \le i < j \le n-1$. Dan vinden we

$$\alpha^{q^{n+j-i}} = (\alpha^{q^j})^{q^{n-i}} = (\alpha^{q^i})^{q^{n-i}} = \alpha^{q^n} = \alpha,$$

en dus ligt α in $\mathbb{F}_{q^{n+j-i}}$. Maar aangezien $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^n}$ moet n dan een deler van $n+j-i$ zijn. Maar uit $0 \leq i, j \leq n-1$ volgt dan $i = j$. Dit bewijst de stelling.

Eindige lichamen worden tegenwoordig veel toegepast bij data-transmissie zoals in de coderingstheorie en de cryptografie. In de coderingstheorie gaat het erom data zoveel mogelijk foutenvrij en efficient te versturen, terwijl het er in de cryptografie om gaat data veilig te versturen. Algebraïsche krommen over eindige lichamen zoals bijv. gedefinieerd door $f(x, y) = 0$ met $f \in \mathbb{F}_q[x, y]$ een irreducibel polynoom spelen hierbij een belangrijke rol.

Opgaven

1) Maak een tabel voor de optelling en vermenigvuldiging in $\mathbb{F}_4$. Doe dit ook voor $\mathbb{F}_9$.

2) Laat zien dat $\mathbb{F}_3[X]/(X^2+1)$ en $\mathbb{F}_3[X]/(X^2+X-1)$ isomorfe lichamen zijn.

3) Ontbind het polynoom $X^{16} - X$ in irreducibele factoren in $\mathbb{F}_2[X]$.

4) Laat p een priemgetal zijn en $\mathbb{F}_q$ een lichaam van cardinaliteit $q = p^n$. Voor $x \in \mathbb{F}_q$ definiëren we het *spoor* $\mathrm{Tr}(x) \in \mathbb{F}_q$ via

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}}.$$

Bewijs de volgende uitspraken:

i) Voor elke $x \in \mathbb{F}_q$ geldt $\mathrm{Tr}(x) \in \mathbb{F}_p$.
ii) De afbeelding $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is een lineaire afbeelding van $\mathbb{F}_p$-vectorruimten.
iii) De afbeelding $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is surjectief.

5) Laat $\mathbb{F}_q$ met $q = p^n$ een lichaam van karakteristiek p zijn met q elementen. Bewijs de volgende uitspraken:

i) De afbeelding $\phi : \mathbb{F}_q \to \mathbb{F}_q$ met $x \mapsto x^p - x$ is een lineaire afbeelding van $\mathbb{F}_p$-vectorruimten met kern $\mathbb{F}_p$.
ii) Er geldt $\mathrm{beeld}(\phi) \subset \ker(\mathrm{Tr})$.
iii) Voor $x \in \mathbb{F}_q$ is de vergelijking $y^p - y = x$ oplosbaar in $\mathbb{F}_q$ dan en slechts dan als $\mathrm{Tr}(x) = 0$.

6) Bepaal voor ieder element in $\mathbb{F}_9$ het minimumpolynoom over $\mathbb{F}_3$.

7) Laat f een irreducibel polynoom van graad m in $\mathbb{F}_p$ zijn dat $X^{p^n} - X$ deelt. Bewijs dat m een deler is van n.

8) Laat f een irreducibel monisch polynoom van graad 3 in $\mathbb{F}_5[X]$ en α een nulpunt van f in een uitbreidingslichaam $\mathbb{F}_q$ van $\mathbb{F}_5$. Bewijs dat de multiplicatieve orde van α in $\mathbb{F}_q^*$ deelbaar is door 31.

9) Laat i_r het aantal monische irreducibele polynomen van graad r in $\mathbb{F}_q[X]$ zijn. Bewijs de volgende formules voor i_r:

$$i_1 = q, \quad i_2 = \frac{1}{2}(q^2 - q), \quad i_3 = \frac{1}{3}(q^3 - q), \quad i_4 = \frac{1}{4}(q^4 - q^2), \quad i_6 = \frac{1}{6}(q^6 - q^3 - q^2 + q).$$

10) Laat $\mathbb{F}_q$ een eindig lichaam zijn van karakteristiek p en n een positief geheel getal niet deelbaar door p zijn. Bewijs dat het ontbindingslichaam van $X^n - 1$ over $\mathbb{F}_q$ een lichaam met q^r elementen is waarbij r de orde van q in de groep $(\mathbb{Z}/n\mathbb{Z})^*$ is.

11) Bereken het ontbindingslichaam van $X^{20} - 1$ over $\mathbb{F}_3$ en ontbind $X^{20} - 1$ in $\mathbb{F}_3[X]$ in irreducibele factoren.

12) Laat K een lichaam van karakteristiek $p > 0$ zijn. Voor $a \in K$ is $f = X^p - X - a \in K[X]$. Laat verder α een nulpunt van f in een uitbreidingslichaam van K zijn.

i) Laat zien dat $f = \prod_{i \in \mathbb{F}_p} (X - \alpha - i)$.
ii) Bewijs dat $K(\alpha)$ een ontbindingslichaam van f is.
iii) Laat zien dat de irreducibele factoren van f in $K[X]$ dezelfde graad hebben.
iv) Bewijs: f is irreducibel of splitst in lineaire factoren in $K[X]$.
v) Laat zien dat $X^p - X - a$ irreducibel is in $\mathbb{F}_p[X]$ voor elke $a \in \mathbb{F}_p^*$.