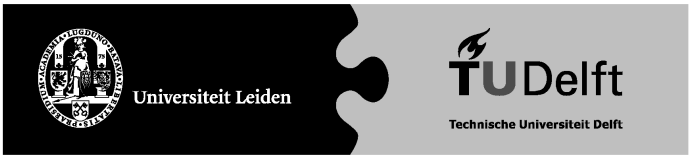
ALGEBRA II

P. Stevenhagen



2017

INHOUDSOPGAVE ALGEBRA II

Versie augustus 2017

De volgende versie bevat hopelijk minder typefouten en onnauwkeurigheden dan de huidige – stuur hiertoe alle op- en aanmerkingen naar psh@math.leidenuniv.nl.

Postadres van de auteur:

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

11 Ringen

In Algebra I hebben we verzamelingen bestudeerd voorzien van een enkele bewerking die tot een *groepsstructuur* aanleiding geeft. In deze syllabus[1] bekijken we de structuur van verzamelingen voorzien van zowel een optelling als een vermenigvuldiging. Dergelijke verzamelingen, waarvan gehele en reële getallen bekende voorbeelden zijn, heten *ringen*. We kwamen ze al tegen in 6.8.

11.1. Definitie. *Een ring is een additief geschreven abelse groep R voorzien van een multiplicatief geschreven bewerking $R \times R \to R$ die aan de volgende drie voorwaarden voldoet.*

(R1) *R bevat een eenheidselement 1 voor de vermenigvuldiging;*

(R2) *Voor elk drietal elementen $x, y, z \in R$ geldt de associatieve eigenschap*

$$x(yz) = (xy)z;$$

(R3) *Voor elk drietal elementen $x, y, z \in R$ gelden de distributieve eigenschappen*

$$x(y+z) = xy + xz \qquad \text{en} \qquad (x+y)z = xz + yz.$$

Geldt bovendien $xy = yx$ voor alle $x, y \in R$, dan heet R een commutatieve ring.

De onderliggende optelgroep van een ring R nemen we per definitie abels. Dit is geen beperking, want commutativiteit van de optelling is een *gevolg* van de overige axioma's. Immers, wegens de distributieve eigenschappen geldt

$$\begin{aligned}(x+y)(1+1) &= x(1+1) + y(1+1) = x + x + y + y\\ (x+y)(1+1) &= (x+y)\cdot 1 + (x+y)\cdot 1 = x + y + x + y,\end{aligned}$$

en hieruit volgt direct de identiteit $x + y = y + x$.

De multiplicatieve structuur van een ring is zelden die van een groep. Vermenigvuldiging is associatief en het eenheidselement $1 \in R$ is uniek, maar het standaardvoorbeeld $R = \mathbf{Z}$ laat zien dat ringelementen niet altijd een multiplicatieve inverse hebben, en dat links- of rechtsvermenigvuldiging met een ringelement niet in het algemeen een bijectie van de ring naar zichzelf geeft. De identiteit $0 \cdot x = (0+0)\cdot x = 0\cdot x + 0\cdot x$ laat zien dat het nulelement met ieder ringelement product 0 heeft.

De *nulring* is de ring die ontstaat door de triviale groep $R = \{0\}$ te voorzien van de vermenigvuldiging $0 \cdot 0 = 0$. Notatie: $R = 0$. In de nulring geldt $0 = 1$. Indien R een element $x \neq 0$ bevat, dan geldt $1 \cdot x = x \neq 0 = 0 \cdot x$, en dus $0 \neq 1$.

Opgave 1. Laat zien dat de nulring de enige ring is waarin vermenigvuldiging een groepsoperatie is.

Een *deelring* R' van een ring R is een deelverzameling $R' \subset R$ met $1 \in R'$ waarop een ringstructuur gedefinieerd is door beperking van de ringoperaties op R. Met andere woorden: R' is een additieve ondergroep van R die $1 \in R$ bevat, en gesloten is onder vermenigvuldiging binnen R.

▶ Eenheden

Een element $x \in R$ heet een *eenheid* als er een element $y \in R$ bestaat met $xy = yx = 1$. Als zo'n element y bestaat, is het uniek bepaald door x (opgave 11). Men schrijft $y = x^{-1}$ en noemt y de (multiplicatieve) *inverse* van x. De verzameling van eenheden in R is de *eenhedengroep* R^* van R.

11.2. Lemma. *De eenhedengroep R^* van R is een groep onder vermenigvuldiging.*

Bewijs. Het product xy van twee eenheden is weer een eenheid: $y^{-1}x^{-1}$ levert een tweezijdige inverse van xy. De vermenigvuldiging definieert dus een bewerking op R^*. Het element $1 \in R^*$ is het eenheidselement, associativiteit is precies axioma (R2), en inversen van eenheden – die ook weer eenheden zijn – bestaan per definitie van R^*. □

11.3. Definitie. *Een delingsring is een ring R met eenhedengroep $R^* = R \setminus \{0\}$. Een commutatieve delingsring heet een lichaam.*

De in 8.7 gedefinieerde *quaternionenalgebra van Hamilton* $\mathbf{H}$ is een voorbeeld van een niet-commutatieve delingsring (opgave 19). De bekendere delingsringen $\mathbf{Q}$, $\mathbf{R}$ en $\mathbf{C}$ van respectievelijk rationale, reële en complexe getallen zijn voorbeelden van lichamen.

De ring $\mathbf{Z}$ van gehele getallen is een commutatieve ring met eenhedengroep $\mathbf{Z}^* = \{\pm 1\}$. Het is een deelring van elk van de bovenstaande delingsringen.

Voor $n \neq 0$ geheel is $\mathbf{Z}/n\mathbf{Z}$ een *eindige* commutatieve ring met eenhedengroep

$$(\mathbf{Z}/n\mathbf{Z})^* = \{\bar{a} \in \mathbf{Z}/n\mathbf{Z} : \mathrm{ggd}(a, n) = 1\}.$$

Als in 6.12 concluderen we dat $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ voor ieder priemgetal p een lichaam is. Merk op dat $\mathbf{Z}/n\mathbf{Z}$ voor $n = 1$ de nulring is, en dat dit geen lichaam is.

▶ Voorbeelden van ringen

11.4. Functieringen. Zij X een willekeurige verzameling en R een ring. Dan heeft de verzameling $\mathrm{Map}(X, R)$ van R-waardige functies op X een ringstructuur indien we sommen en producten van functies puntsgewijs definiëren door

$$(f + g)(x) = f(x) + g(x) \quad \text{en} \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

Voor commutatieve R is de functiering $\mathrm{Map}(X, R)$ weer commutatief.

Ringen van functies komen zeer veel voor. Meestal heeft X een aanvullende structuur, en beschouwt men niet de ring van *alle* R-waardige functies, maar één of andere deelring van interessante functies. Men kan denken aan de ring $C(X) \subset \mathrm{Map}(X, \mathbf{R})$ van continue reëelwaardige functies op een topologische ruimte X of de ring $C^\infty(0, 1)$ van oneindig vaak differentieerbare functies op het open eenheidsinterval $(0, 1)$.

Opgave 2. Ga na dat $C(X)$ en $C^\infty(0, 1)$ inderdaad deel*ringen* zijn.

11.5. Polynoomringen. Voor iedere ring R kan men op de bekende wijze de polynoomring $R[X]$ in een variabele X over R definiëren. De elementen van $R[X]$ zijn

formele uitdrukkingen $\sum_{k\geq 0} r_k X^k$ met coëfficiënten $r_k \in R$ die slechts voor eindig veel gehele getallen $k \geq 0$ verschillen van 0. Deze uitdrukkingen, die men *polynomen* noemt, telt men coëfficiëntsgewijs op:

$$\textstyle\sum_{k\geq 0} r_k X^k + \sum_{k\geq 0} s_k X^k = \sum_{k\geq 0}(r_k + s_k)X^k.$$

In het bijzonder is ieder polynoom uniek te schrijven als som van polynomen met precies één coëfficiënt verschillend van 0, *monomen* genaamd. De vermenigvuldiging definiëren we voor monomen door $r_k X^k \cdot s_\ell X^\ell = r_k s_\ell X^{k+\ell}$. Uit de distributieve eigenschappen (R3) volgt dan dat de n-de coëfficiënt c_n van het productpolynoom

$$\textstyle\sum_{k\geq 0} c_k X^k = (\sum_{k\geq 0} r_k X^k) \cdot (\sum_{k\geq 0} s_k X^k)$$

gelijk is aan $c_n = \sum_{k=0}^{n} r_k s_{n-k}$. Een rechtstreekse verificatie laat zien dat $R[X]$ hiermee een ring wordt. In de meeste toepassingen is R commutatief, en dan is $R[X]$ dat ook. De polynoomring $R[X]$ bevat R als deelring van *constante polynomen*.

Een polynoom $f \in R[X]$ geeft voor ieder element $r \in R$ aanleiding tot een functiewaarde $f(r)$, door *evaluatie* van f in $X = r$. In sommige gevallen, bijvoorbeeld voor $R = \mathbf{R}$, kan men $R[X]$ zo opvatten als een deelring van de functiering $\mathrm{Map}(R, R)$. In het algemeen is dit echter niet mogelijk, want polynomen in $R[X]$ liggen niet voor alle R vast door hun waarden op R. Zo is bijvoorbeeld het polynoom $X^p - X \in \mathbf{F}_p[X]$ niet het nulpolynoom, maar de bijbehorende functie $\mathbf{F}_p \to \mathbf{F}_p$ wegens de kleine stelling van Fermat 6.18 toch de nulfunctie.

De constructie van de polynoomring $R[X]$ uit R kan op een aantal manieren gevarieerd worden. Laat men bijvoorbeeld uitdrukkingen $\sum_{k\geq 0} r_k X^k$ toe waarin oneindig veel coëfficiënten van 0 mogen verschillen, dan krijgt men met de boven aangegeven definities voor som en product de *machtreeksenring* $R[[X]]$ over R. De *Taylorreeksen* uit de analyse zijn bekende voorbeelden in het geval $R = \mathbf{R}$.

Laat men in de definitie van een polynoom ook negatieve machten van X toe, dan krijgt men de ring van *Laurentpolynomen*

$$R[X, X^{-1}] = \{\textstyle\sum_{k\in\mathbf{Z}} r_k X^k : \quad r_k = 0 \text{ voor bijna alle } k \in \mathbf{Z}\}.$$

De rekenregels zijn als voor gewone polynomen, maar $r_k X^k \cdot s_\ell X^\ell = r_k s_\ell X^{k+\ell}$ geldt nu voor alle $k, \ell \in \mathbf{Z}$. Tenslotte heeft men de ring $R((X))$ van *Laurentreeksen* over R; voor $R = \mathbf{C}$ wordt deze ring in de complexe analyse veel gebruikt. Men beschouwt hier uitdrukkingen $\sum_{k\in\mathbf{Z}} r_k X^k$ waarin slechts eindig veel coëfficiënten r_k met $k < 0$ van 0 verschillen. Merk op dat met deze definitie alle coëfficiënten van het product van twee Laurentreeksen nog steeds door *eindige* sommen gegeven worden. De ring $R((X))$ bevat zowel $R[X, X^{-1}]$ als $R[[X]]$ op natuurlijke wijze als deelring.

In een abstracte ring R, of zelfs in $R = \mathbf{Z}$, hebben 'oneindige sommen' geen betekenis. De boven gedefinieerde machtreeksen en Laurentreeksen zijn dan ook formele objecten, die geen functies $R \to R$ induceren. Om bekende begrippen uit de analyse als *limiet* en *convergentie* te definiëren is een aanvullende (topologische) structuur op R nodig.

Door iteratie van de polynoomconstructie in 1 variabele krijgt men polynomen in meer variabelen. De polynoomring $(R[X])[Y]$ in de variabelen X en Y, die men ook als de polynoomring $(R[Y])[X]$ op kan vatten (waarom?), noteert men als $R[X,Y]$. Algemener heeft men de polynoomring $R[X_1, X_2, \ldots, X_n]$ in n variabelen, en op soortgelijke wijze construeert men de machtreeksenring $R[[X_1, X_2, \ldots, X_n]]$ in n variabelen.

Bij Laurentreeksen in meer variabelen is de definitie problematischer (opgave 71).

11.6. Groepenringen. Voor R een ring en G een groep definieert men de *groepenring* $R[G]$ op een manier die enigszins aan de constructie van de polynoomring doet denken. Als verzameling bestaat $R[G]$ uit de uitdrukkingen $\sum_{g\in G} r_g g$, waarbij $r_g \in R$ voor bijna alle $g \in G$ gelijk aan 0 genomen wordt. De optelling geschiedt componentsgewijs:

$$(\textstyle\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G}(a_g + b_g)g.$$

Omdat alleen eindige sommen optreden krijgt men een vermenigvuldiging door de regel $a_g g \cdot b_h h = a_g b_h gh$ te combineren met de distributieve regels. Men gaat gemakkelijk na dat $R[G]$ hiermee een ring met eenheidselement $1 \cdot e$ wordt, en dat voor $R \neq 0$ de groepenring $R[G]$ commutatief is dan is en slechts dan als R commutatief is en G abels. De hier gebruikte multiplicatieve notatie voor G vermijdt verwarring tussen de optelling in $R[G]$ en de groepsoperatie in G. Wil men G toch additief noteren, dan is er de notatie $\sum_{g\in G} a_g[g]$ voor ringelementen die het onderscheid tussen $[g_1 + g_2]$ en $[g_1] + [g_2]$ duidelijk maakt.

Opgave 3. Laat zien dat $R[X]$ als deelring van de groepenring $R[\mathbf{Z}]$ kan worden opgevat, en dat $R[X, X^{-1}]$ met $R[\mathbf{Z}]$ geïdentificeerd kan worden.

11.7. Matrixringen. Een veel voorkomend type ring, dat meestal niet commutatief is, is de *matrixring* van dimensie $n \geq 0$ over een willekeurige grondring R. Voor $n \in \mathbf{Z}_{\geq 0}$ en matrices $A = (a_{ij})_{i,j=1}^n$ en $B = (b_{ij})_{i,j=1}^n$ in de verzameling $\mathrm{Mat}_n(R)$ van $n \times n$-matrices met coëfficiënten in R definieert men de som 'coëfficiëntsgewijs' door

$$A + B = (a_{ij} + b_{ij})_{i,j=1}^n.$$

Het *matrixproduct* $AB = (c_{ij})_{i,j=1}^n$ heeft coëfficiënten $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$ gegeven door wat wel de 'rij-maal-kolom-productregel' heet. Een rechtstreekse (maar licht vermoeiende) verificatie laat zien dat dit een ringstructuur op $\mathrm{Mat}_n(R)$ definieert. We hebben $\mathrm{Mat}_0(R) = 0$, en $\mathrm{Mat}_1(R)$ kan men met R identificeren. Voor $n \geq 2$ en $R \neq 0$ is $\mathrm{Mat}_n(R)$ niet-commutatief. De eenhedengroep van $\mathrm{Mat}_n(R)$ is de groep $\mathrm{GL}_n(R)$ van inverteerbare $n \times n$-matrices.

In de lineaire algebra is R een lichaam zoals $\mathbf{R}$, $\mathbf{C}$ of $\mathbf{F}_p$. De elementen van $\mathrm{Mat}_n(R)$ corresponderen dan met de R-lineaire afbeeldingen $R^n \to R^n$ van de n-dimensionale 'standaardvectorruimte' over R naar zichzelf. Onder deze identificatie is de definitie van het matrixproduct heel natuurlijk: het is de *samenstelling* van de bijbehorende afbeeldingen.

11.8. Endomorfismenringen. Voor iedere abelse groep A is de verzameling $\mathrm{End}(A)$ van groepshomomorfismen $A \to A$, meestal *endomorfismen* genoemd, op een natuurlijke manier een ring. De som en het product van twee endomorfismen $f, g \in \mathrm{End}(A)$ zijn gedefinieerd als

$$(f+g)(a) = f(a) + g(a)$$
$$(f \cdot g)(a) = (f \circ g)(a) = f(g(a)).$$

We weten al (opgave 4.41) dat voor abelse A de afbeelding $f+g$ inderdaad een homomorfisme is, en dat $\mathrm{End}(A)$ onder deze optelling een abelse groep is met het triviale homomorfisme $A \to 0 \subset A$ als nulelement. De identiteit $1 = \mathrm{id}_A$ is een eenheidselement voor de vermenigvuldiging, en een distributieve regel als $f(g+h) = fg + fh$ volgt door eenvoudig uitschrijven:

$$[f(g+h)](a) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = (fg)(a) + (fh)(a).$$

We concluderen dat $\mathrm{End}(A)$ een ring is. Deze is niet in het algemeen commutatief. De eenhedengroep $\mathrm{End}(A)^*$ van $\mathrm{End}(A)$ is niets anders dan de al in §4 gedefinieerde automorfismengroep $\mathrm{Aut}(A)$ van A.

Opgave 4. Laat zien dat $\mathrm{End}(\mathbf{Z}^n)$ geïdentificeerd kan worden met de matrixring $\mathrm{Mat}_n(\mathbf{Z})$.

Endomorfismenringen zijn van grote algemeenheid, want zoals we in 11.12 zullen zien kunnen de elementen van een ring R als endomorfismen van de onderliggende optelgroep worden opgevat.

▶ Nuldelers

In lichamen of in ringen zoals $\mathbf{Z}$ weten we dat het product van twee elementen verschillend van 0 nooit gelijk is aan 0. In willekeurige ringen kan dit verschijnsel echter wel optreden. Voor matrices is dit feit bekend uit de lineaire algebra, maar er zijn veel meer voorbeelden. Nemen we bijvoorbeeld twee niet-nul functies $f, g : [0,1] \to \mathbf{R}$ die op disjuncte stukken van $[0,1]$ van 0 verschillen, dan is fg de nulfunctie zonder dat f en g het zijn. Is g een element van orde n in een groep G, dan geldt in de groepenring $\mathbf{Z}[G]$ de identiteit $(1-g)(1+g+g^2+\ldots+g^{n-2}+g^{n-1}) = 1-g^n = 0$.

11.9. Definitie. *Een element $x \in R$ heet een nuldeler als er een element $y \neq 0$ in R bestaat waarvoor $xy = 0$ of $yx = 0$ geldt.*

In iedere ring $R \neq 0$ hebben we de *triviale nuldeler* $0 \in R$. Voor niet-commutatieve ringen maakt men in 11.9 wel onderscheid tussen *linkernuldelers* (het geval $xy = 0$) en *rechternuldelers* (het geval $yx = 0$). Een element $x \in R$ is een linkernuldeler dan en slechts dan als de afbeelding $\lambda_x : R \to R$ gegeven door $\lambda_x(r) = xr$, die een endomorfisme van de optelgroep van R is, *niet* injectief is. Voor rechternuldelers geldt dezelfde uitspraak met λ_x vervangen door de afbeelding $\rho_x : R \to R$ gegeven door $\rho_x(r) = rx$. Het is niet altijd waar dat linkernuldelers ook rechternuldelers zijn (opgave 28).

Opgave 5. Laat zien dat een eenheid in een ring nooit een nuldeler is.

Ringen met niet-triviale nuldelers gedragen zich in veel opzichten anders dan welbekende ringen als $\mathbf{Z}$ of $\mathbf{R}$. Zo hebben voor $R = \mathbf{Z}/8\mathbf{Z}$ het lineaire polynoom $\overline{4}X$ en het kwadratische polynoom $X^2 - \overline{1}$ elk *vier* nulpunten in R. Uit de gelijkheid $\overline{4} \cdot \overline{1} = \overline{4} \cdot \overline{3} \in \mathbf{Z}/8\mathbf{Z}$ kan men dan ook, anders dan in het geval van groepen, *niet* $\overline{1} = \overline{3}$ concluderen!

▶ Domeinen

Een commutatieve ring $R \neq 0$ zonder niet-triviale nuldelers heet een *domein*. In plaats van domein komt men ook wel het woord *integriteitsgebied* tegen, als nettere vertaling van het Engelse equivalent *integral domain*. In domeinen geldt de ons van de reële getallen bekende eigenschap

$$xy = 0 \quad \Longrightarrow \quad x = 0 \quad \text{of} \quad y = 0.$$

Door hierin y door $y - z$ te vervangen vinden we de implicatie

$$xy = xz \quad \Longrightarrow \quad x = 0 \quad \text{of} \quad y = z,$$

die suggereert dat we in domeinen elementen verschillend van 0 kunnen 'wegdelen'. In lichamen is dit letterlijk waar, en in alle deelringen van lichamen, die domeinen zijn, dus ook. In feite kan men *ieder* domein R opvatten als deelring van een lichaam, het quotiëntenlichaam $Q(R)$ van R. De constructie van $Q(R)$ uit R is het ringtheoretisch analogon van de constructie van $\mathbf{Q}$ uit $\mathbf{Z}$. Het 'niet-unieke' van breuk-representaties maakt de definitie – net als voor gewone breuken – enigszins subtiel.

11.10. Quotiëntenlichaam. Definieer voor een domein R op de productverzameling $R \times (R \setminus \{0\})$ een equivalentierelatie door

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

De transitiviteit van deze relatie vereist een verificatie: met $(a, b) \sim (c, d)$ en $(c, d) \sim (e, f)$ hebben we $adf = bcf = bde$, en wegens de commutativiteit van R geeft dit $d(af - be) = 0$. Omdat R geen niet-triviale nuldelers heeft en $d \neq 0$ geldt, volgt hieruit de relatie $af = be$, die $(a, b) \sim (e, f)$ geeft.

We noteren de equivalentieklasse van (a, b) suggestief als $\frac{a}{b}$. De verzameling $Q(R)$ van equivalentieklassen wordt nu een lichaam als we optelling en vermenigvuldiging van 'breuken' op de bekende wijze definiëren door

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{en} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Men gaat eerst na dat dit *welgedefinieerde* bewerkingen zijn: ze hangen niet van de keuze van de representant af. Weten we dit eenmaal, dan volgt gemakkelijk dat aan de ringaxioma's voldaan is. Omdat ieder element $\frac{a}{b} \in Q(R)$ verschillend van het nulelement $\frac{0}{b} = \frac{0}{1}$ een inverse $\frac{b}{a} \in Q(R)$ heeft is het quotiëntenlichaam $Q(R)$ een lichaam.

Door een element $r \in R$ te identificeren met de klasse $\frac{r}{1} \in Q(R)$ wordt R een deelring van $Q(R)$.

Neemt men in het voorafgaande voor R de polynoomring $K[X]$ over een lichaam K, dan is $Q(R)$ het lichaam $K(X)$ van *rationale functies* met coëfficiënten in K.

De vorming van het quotiëntenlichaam van een domein is een speciaal geval van het centrale concept van *localisatie* in de commutatieve algebra. Men kan andere deelverzamelingen van R dan alleen $S = R \setminus \{0\}$ als 'noemers' toelaten in de *gelocaliseerde ring* $S^{-1}R$, en met een geschikte aanpassing van de equivalentierelatie op de verzameling van 'breuken' $\frac{r}{s} = (r, s) \in R \times S$ werkt de constructie voor willekeurige commutatieve ringen R, niet alleen voor domeinen. Zie hiervoor de opgaven 72 en verder.

▶ Homomorfismen en idealen

Net als in de groepentheorie heten de afbeeldingen in de ringentheorie *homomorfismen*, en is er een soortgelijk isomorfiebegrip.

11.11. Definitie. *Een afbeelding $f : R \to R'$ tussen ringen heet een ringhomomorfisme als voor alle $x, y \in R$*

$$f(x + y) = f(x) + f(y) \qquad \text{en} \qquad f(xy) = f(x)f(y)$$

geldt, en tevens $f(1_R) = 1_{R'}$. Een bijectief ringhomomorfisme heet een ringisomorfisme.

Net als in de groepentheorie heten ringen R en R' isomorf als er een ringisomorfisme $R \xrightarrow{\sim} R'$ bestaat. Notatie: $R \cong R'$.

Met de identiteit $f(1_R) = 1_{R'}$ in (11.11) bedoelen we dat f het eenheidselement voor de vermenigvuldiging in R naar het eenheidselement voor de vermenigvuldiging in R' stuurt. Als R' niet de nulring is, sluit deze eis de 'nulafbeelding' $f : R \to 0 \subset R'$, die wel aan de eerste twee eisen voldoet, uit als homomorfisme. Onder een injectief homomorfisme $f : R \to R'$ kunnen we R als deelring opvatten van R'. Algemener is onder een ringhomomorfisme $f : R \to R'$ het beeld $f[R]$ een deelring van R'.

De in 5.8 verwoorde stelling van Cayley zegt dat elementen van een groep G opgevat kunnen worden permutaties van de verzameling G, en dat G hierdoor een ondergroep van $S(G)$ wordt. Het ringtheoretisch analogon hiervan verkrijgt men door ringelementen op te vatten als endomorfismen van de onderliggende optelgroep.

11.12. Stelling. *Zij R een ring en R^+ de onderliggende abelse optelgroep. Geef voor $x \in R$ met $\lambda_x : R^+ \to R^+$ de linksvermenigvuldiging $r \mapsto xr$ aan. Dan is*

$$\begin{aligned} f : R &\longrightarrow \mathrm{End}(R^+) \\ x &\longmapsto \lambda_x \end{aligned}$$

een injectief homomorfisme, en R is isomorf met een deelring van $\mathrm{End}(R^+)$.

Bewijs. Wegens de distributieve regel $x(r_1 + r_2) = xr_1 + xr_2$ is λ_r een endomorfisme van de optelgroep R^+. Distributiviteit geeft tevens

$$(\lambda_x + \lambda_y)(r) = xr + yr = (x + y)r = \lambda_{x+y}(r),$$

en associativiteit geeft $(\lambda_x \cdot \lambda_y)(r) = x(yr) = (xy)r = \lambda_{xy}(r)$. Wegens $\lambda_1 = \mathrm{id}_{R^+}$ is nu f een homomorfisme, en wegens $\lambda_x(1) = x$ zijn λ_x en λ_y verschillend voor $x \neq y$. We concluderen dat R isomorf is met de deelring $f[R] \subset \mathrm{End}(R^+)$. □

Opgave 6. Bewijs: R is isomorf met $\mathrm{End}_R(R^+) = \{f \in \mathrm{End}(R^+) : f(r_1 r_2) = f(r_1)r_2$ voor alle $r_1, r_2 \in R\}$.

In de groepentheorie hebben we gezien dat de ondergroepen $H \subset G$ die als kern van een homomorfisme optreden een welomschreven klasse vormen, namelijk de klasse van *normale* ondergroepen. Voor een ring R is de onderliggende optelgroep R^+ abels, dus alle ondergroepen van R^+ zijn normaal. Een ringhomomorfisme $f : R \to R'$ is in het bijzonder een homomorfisme van de onderliggende optelgroepen, dus de kern

$$\ker(f) = \{r \in R : f(r) = 0\}$$

is weer een ondergroep van R^+. De multiplicatieve eigenschap $f(xy) = f(x)f(y)$ impliceert echter dat niet alle ondergroepen van R^+ als kern van een ringhomomorfisme op kunnen treden, maar alleen de zogenaamde *idealen* van R.

11.13. Definitie. *Een ideaal I in een ring R is een ondergroep van de additieve groep R^+ met de volgende eigenschap:*

$$\textit{voor } r \in R \textit{ en } x \in I \textit{ geldt } rx \in I \textit{ en } xr \in I.$$

Het is niet moeilijk in te zien dat de kern van een ringhomomorfisme $f : R \to R'$ een ideaal is. Immers, voor $r \in R$ en $x \in \ker(f)$ geldt $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$, en dus $rx \in \ker(f)$. Evenzo geldt $xr \in \ker(f)$. Omgekeerd laat het volgende analogon van 4.12 voor ringen zien dat de idealen $I \subset R$ precies de ondergroepen van R^+ zijn waarvoor de factorgroep R/I, die zoals bekend de nevenklassen $x + I$ van I in R als elementen heeft, een ringstructuur van R erft.

11.14. Stelling. *Zij R een ring en $I \subset R$ een ideaal. Dan definieert de vermenigvuldiging*

$$(x + I)(y + I) = xy + I$$

een ringstructuur op de factorgroep R/I. Hiermee wordt de natuurlijke afbeelding $R \to R/I$ een ringhomomorfisme met kern I.

Bewijs. Het is voldoende om te laten zien dat de genoemde vermenigvuldiging op R/I welgedefinieerd is. Dit betekent dat voor elementen $x \equiv x' \bmod I$ en $y \equiv y' \bmod I$ de producten xy en $x'y'$ congruent moeten zijn modulo I. Schrijven we als in (6.10)

$$xy - x'y' = x(y - y') + (x - x')y',$$

dan volgt uit de hypothesen $y - y' \in I$ en $x - x' \in I$ en de ideaaleigenschap 11.13 dat $xy - x'y'$ inderdaad in I ligt.

De ringaxioma's voor R/I volgen nu onmiddellijk uit die voor R, en de natuurlijke afbeelding $R \to R/I$ is bijna per definitie een ringhomomorfisme met kern I. □

Iedere ring $R \neq 0$ heeft twee triviale idealen, het nulideaal $\{0\}$ en de ring R zelf. De corresponderende quotiëntringen zijn R zelf en de nulring. Als R een lichaam is, of algemener een delingsring, dan zijn er geen andere idealen. Immers ieder ideaal $I \subset R$ verschillend van $\{0\}$ bevat dan een eenheid $x \in R^*$, en dus ook $1 = xx^{-1}$. Wegens de ideaaleigenschap 11.13 geldt dan $r \cdot 1 = r \in I$ voor alle $r \in R$, en dus $I = R$.

Voor een ring R zonder niet-triviale idealen is ieder ringhomomorfisme $f : R \to R'$ naar een ring $R' \neq 0$ injectief, want $\ker(f)$ is het nulideaal en 4.4 blijft geldig in de context van ringen.

Een voorbeeld van een niet-triviaal ideaal is $n\mathbf{Z} \subset \mathbf{Z}$ voor een geheel getal $n > 1$. De bijbehorende quotiëntring is de ring $\mathbf{Z}/n\mathbf{Z}$ van restklassen modulo n uit 6.9. Algemener kunnen we voor een commutatieve ring R en $x \in R$ kijken naar het *hoofdideaal*

$$(x) = xR = \{xr : r \in R\}$$

voortgebracht door x. Dit is het kleinste ideaal dat x bevat (waarom?), en het is gelijk aan R dan en slechts dan als x een eenheid is. De elementen in (x) zijn de elementen van R die *deelbaar* zijn door x; het zijn de *veelvouden* van x. Wegens 6.2 zijn voor $R = \mathbf{Z}$ *alle* idealen hoofdidealen. Een domein met deze prettige eigenschap heet een *hoofdideaaldomein*, in het Engels soms met PID (*principal ideal domain*) afgekort. We bestuderen ze nader in de volgende paragraaf.

Opgave 7. Laat zien dat iedere commutatieve ring $R \neq 0$ zonder niet-triviale idealen een lichaam is.

Voor iedere eindige deelverzameling $S = \{s_1, s_2, \ldots s_n\}$ van een commutatieve ring R kan men het ideaal $(S) = (s_1, s_2, \ldots s_n) \subset R$ *voortgebracht door* S definiëren als

$$(S) = \{\textstyle\sum_{s\in S} r_s s : \quad r_s \in R \text{ voor alle } s\}.$$

Dit is een ondergroep van R^+ die aan de ideaaleigenschap 11.13 voldoet, en duidelijk het kleinste ideaal vormt dat S omvat. Idealen voortgebracht door een eindige verzameling heten *eindig voortgebracht*. Voor oneindige S definieert men (S) als boven, maar met de aanvullende eis dat in de sommen $\sum_{s\in S} r_s s$ bijna alle r_s gelijk zijn aan 0.

In niet-commutatieve ringen is het zinnig om naast idealen ook over links- en rechtsidealen te praten. Een *linksideaal* van R is een additieve ondergroep van R^+ die onder linksvermenigvuldiging met R in zichzelf overgaat. Evenzo heeft men het begrip *rechtsideaal*. Een ideaal van R in de zin van 11.13, dat zowel een linksideaal als een rechtsideaal is, wordt als R niet-commutatief is ook wel een *tweezijdig ideaal* genoemd. Alleen voor tweezijdige idealen I kan men een quotiëntring R/I construeren.

Opgave 8. Laat zien dat ieder element $x \in R$ een linksideaal Rx en een rechtsideaal xR voortbrengt. Bepaal Rx en xR voor $R = \mathrm{Mat}_2(\mathbf{R})$ en $x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

▶ Isomorfie- en homomorfiestellingen

De fundamentele isomorfiestelling 4.9 uit de groepentheorie geldt onverkort in ringtheoretische context.

11.15. Isomorfiestelling. *Zij $f : R \to R'$ een ringhomomorfisme met kern I. Dan is de afbeelding*

$$\overline{f} : R/I \xrightarrow{\sim} f[R]$$

gegeven door $x + I \mapsto f(x)$ een ringisomorfisme.

Bewijs. Wegens 4.9 is $\overline{f}$ een isomorfisme van additieve groepen. Omdat f een ringhomomorfisme is, is $\overline{f}$ ook een ringhomomorfisme, en dus een ringisomorfisme. □

11.16. Voorbeeld. Zij R een commutatieve ring en $a \in R$ een element. Dan is de *evaluatie-afbeelding* $\phi_a : R[X] \to R$ op de polynoomring $R[X]$ in het 'punt' $a \in R$ gedefinieerd door $\phi_a(f) = f(a)$. Men gaat gemakkelijk na (opgave 34) dat dit voor commutatieve R een ringhomomorfisme is. We laten zien dat de kern $\ker \phi_a$ van polynomen in $R[X]$ die a als *nulpunt* hebben gelijk is aan het hoofdideaal $(X - a)$.

Wegens $X - a \in \ker \phi_a$ hebben we $(X - a) \subset \ker \phi_a$. Omgekeerd is ieder polynoom $f = \sum c_i X^i$ met $f(a) = 0$ te schrijven als

$$f = f - f(a) = \textstyle\sum_i c_i X^i - \sum_i c_i a^i = \sum_i c_i (X^i - a^i).$$

Ieder van de termen $X^i - a^i$ is een veelvoud van $X - a$:

$$(*) \qquad X^i - a^i = (X^{i-1} + aX^{i-2} + a^2 X^{i-3} + \ldots + a^{i-2}X + a^{i-1})(X - a).$$

Er volgt dat f zelf ook in $(X - a)$ ligt, en we vinden $\ker \phi_a = (X - a)$. Passen we nu de isomorfiestelling toe voor ϕ_a, dan vinden we omdat ϕ_a surjectief is een isomorfisme

$$R[X]/(X - a) \xrightarrow{\sim} R$$
$$f + (X - a) \cdot R[X] \longmapsto f(a).$$

Kennelijk is ieder polynoom $f \in R[X]$ te schrijven als $f = q \cdot (X - a) + f(a)$ met $q \in R[X]$. Omdat voor de gelijkheid $(*)$ de commutativiteit van R niet vereist is, is dit laatste ook waar in niet-commutatieve ringen. Het is een speciaal geval van *deling met rest* in polynoomringen, waarop we in 12.1 nader in zullen gaan.

Opgave 9. Laat zien dat de afbeelding $\mathbf{Z}[X] \to \mathbf{Z}/3\mathbf{Z}$ gegeven door $f \mapsto (f(0) \bmod 3)$ een ringhomomorfisme is met kern $(3, X)$, en bewijs dat $(3, X)$ geen hoofdideaal is.

Veel van de in §8 bewezen stellingen laten zich moeiteloos generaliseren naar ringen. Het is in de meeste gevallen voldoende op te merken dat de geconstrueerde afbeeldingen niet alleen groepshomomorfismen zijn, maar tevens ringhomomorfismen. We noemen als voorbeeld het ringtheoretisch analogon van de homomorfiestelling 8.4. Voor de analoga van 8.1, 8.2 en 8.5 verwijzen we naar de opgaven 51–53.

11.17. Homomorfiestelling. *Zij $f : R \to R'$ een ringhomomorfisme en $I \subset \ker(f)$ een ideaal van R. Dan bestaat er een uniek ringhomomorfisme $\overline{f} : R/I \to R'$ zo dat f verkregen wordt als samenstelling*

$$R \xrightarrow{\pi} R/I \xrightarrow{\overline{f}} R'$$

van de quotiëntafbeelding $\pi : R \to R/I$ met $\overline{f}$. □

▶ Chinese reststelling

In een commutatieve ring R kan men net als in $\mathbf{Z}$ naar sommen, producten en doorsneden van idealen kijken. De *doorsnede* $I \cap J$ van idealen I en J van R is weer een ideaal, en hetzelfde geldt voor de *som* $I + J = \{i + j : i \in I \text{ en } j \in J\}$. Geldt $I + J = R$, dan noemen we naar analogie met het geval $R = \mathbf{Z}$ in 6.3.2 de idealen I en J *onderling ondeelbaar* of *copriem*. Het *product* $I \cdot J$ (of IJ) van twee idealen is gedefinieerd als het ideaal *voortgebracht* door de elementen $i \cdot j$ met $i \in I$ en $j \in J$. De verzameling $\{i \cdot j : i \in I \text{ en } j \in J\}$ is niet in het algemeen een ideaal van R (opgave 44). Omdat alle producten $i \cdot j$ bevat zijn in $I \cap J$ geldt altijd de inclusie

$$I \cdot J \subset I \cap J. \tag{11.18}$$

Voor $R = \mathbf{Z}$ betekent dit dat voor $a, b \in \mathbf{Z}$ het product ab deelbaar is door het kleinste gemene veelvoud $\mathrm{kgv}(a, b)$.

De Chinese reststelling 6.15 laat zich generaliseren voor willekeurige commutatieve ringen. We merken eerst op dat het cartesisch product $R_1 \times R_2$ van twee ringen met coëfficiëntsgewijze bewerkingen weer een ring is. De projectie $R_1 \times R_2 \to R_1$ op de eerste coördinaat is een surjectief ringhomomorfisme. Voor $R_2 \neq 0$ is echter de afbeelding $R_1 \to R_1 \times R_2$ gegeven door $r_1 \mapsto (r_1, 0)$ geen ringhomomorfisme in de zin van 11.11: het eenheidselement $1 \in R_1$ wordt niet op het eenheidselement $(1, 1) \in R_1 \times R_2$ afgebeeld. Men spreekt in zo'n geval wel van een *niet-unitair ringhomomorfisme*.

11.19. Chinese reststelling. *Laat I en J onderling ondeelbare idealen van een commutatieve ring R zijn. Dan geldt $I \cdot J = I \cap J$, en de natuurlijke afbeelding*

$$\begin{aligned} \psi : \quad R/(I \cdot J) \quad &\xrightarrow{\sim} \quad R/I \times R/J \\ (x + I \cdot J) \quad &\longmapsto (x + I, x + J) \end{aligned}$$

is een ringisomorfisme.

Bewijs. Na (11.18) is het voor de gelijkheid $I \cdot J = I \cap J$ voldoende de inclusie $I \cap J \subset I \cdot J$ te bewijzen. Wegens de aanname bestaan er elementen $i \in I$ en $j \in J$ met $i + j = 1$. Schrijven we nu $x = x(i + j) = ix + xj$ voor $x \in I \cap J$, dan liggen ix en xj elk in $I \cdot J$, en dus x zelf ook.

De natuurlijke afbeelding $f : R \to R/I \times R/J$ is een ringhomomorfisme met kern $I \cap J = I \cdot J$, dus we krijgen het isomorfisme ψ als direct gevolg van 11.15 indien we laten zien dat f surjectief is. Met $i = 1 - j$ als boven hebben we $f(i) = (0, 1)$, en evenzo $f(j) = (1, 0)$. Er volgt $f(r_1 j + r_2 i) = (r_1 + I, r_2 + J)$, dus f is surjectief. □

Het rekenen met idealen in een commutatieve ring R lijkt sterk op het rekenen met elementen in R. Er zijn de voor de hand liggende definities voor sommen en producten van meer dan twee idealen, en er gelden distributieve regels als $(I+J)\cdot K = I\cdot K + J\cdot K$ (ga na!). Voor het n-voudig product $I \cdot I \cdot \ldots \cdot I$ schrijft men ook wel I^n.

Opgave 10. Bewijs: $(I + J)^2 = I^2 + I \cdot J + J^2$.

Aan het einde van de volgende paragraaf zullen we zien dat het rekenen met idealen in sommige opzichten *makkelijker* is dan het rekenen met elementen. Zie ook opgave 42.

OPGAVEN.

In onderstaande opgaven is R steeds een ring.

11. Zij $x \in R$ gegeven, en laat $y, z \in R$ voldoen aan $xy = zx = 1$. Bewijs: $y = z$. Concludeer dat een ringelement ten hoogste één (multiplicatieve) inverse heeft.

12. Bewijs: $\mathrm{Map}(X, R)^* = \mathrm{Map}(X, R^*)$.

13. Zij R een domein. Bewijs: $R[X]^* = R^*$.

14. Zij $R = \mathbf{Z}/4\mathbf{Z}$. Bewijs: voor alle $r \in R[X]$ geldt $1 + 2r \in R[X]^*$. Is iedere eenheid $u \in R[X]^*$ van de vorm $u = 1 + 2r$?

15. Zij R een domein. Bewijs: $R[X, X^{-1}]^* = \{uX^k : u \in R^*, k \in \mathbf{Z}\} \cong R^* \times \mathbf{Z}$.

16. Bewijs: $\sum_{k\geq 0} r_k X^k \in R[[X]]^* \iff r_0 \in R^*$. Concludeer dat de ring $R((X))$ van Laurentreeksen over R een lichaam is dan en slechts dan als R een lichaam is.

17. Zij p een priemgetal en $R_p \subset \mathbf{Q}$ de verzameling van breuken $\frac{m}{n}$ met $p \nmid n$. Bewijs dat R_p een deelring van $\mathbf{Q}$ is, en bepaal R_p^*.

18. Laat zien dat ieder element in een eindige ring R een eenheid of een nuldeler is. Concludeer: ieder eindig domein is een lichaam.

19. Zij $\mathbf{H} = \mathbf{R} + \mathbf{R}\cdot i + \mathbf{R}\cdot j + \mathbf{R}\cdot k$ de in 8.7 gedefinieerde *quaternionenalgebra van Hamilton*. Bewijs dat $\mathbf{H}$ een niet-commutatieve delingsring is.
[Hint: $(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$.]

20. Bewijs dat de identiteit $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ voor $a, b \in R$ en $n > 0$ (het 'binomium van Newton') geldig is in iedere commutatieve ring R. Laat zien dat omgekeerd een ring waarin het binomium van Newton geldt commutatief is.

21. Laat zien dat het *centrum* $Z(R) = \{x \in R : \ rx = xr \text{ voor alle } r \in R\} \subset R$ van R een *deelring* is van R. Bewijs: $Z(R[X]) = (Z(R))[X]$.

22. Laat zien dat er voor iedere ring R precies één homomorfisme $f : \mathbf{Z} \to R$ bestaat. De niet-negatieve voortbrenger van $\ker f$ heet de *karakteristiek* $\mathrm{char}(R)$ van R. Laat zien dat de karakteristiek van een domein 0 of een priemgetal is. Wat is de karakteristiek van de nulring?

23. Zij $R' \subset R$ een deelring. Geef een bewijs of een tegenvoorbeeld voor:
    a. R is een lichaam $\implies R'$ is een lichaam;
    b. R' is een lichaam $\implies R$ is een lichaam;
    c. R is een domein $\implies R'$ is een domein;
    d. R' is een domein $\implies R$ is een domein.

24. Voor welke waarden van $n \in \mathbf{Z}_{\geq 0}$ is de determinantafbeelding $\det : \mathrm{Mat}_n(\mathbf{R}) \to \mathbf{R}$ een ringhomomorfisme?

25. Zij $A \in \mathrm{Mat}_n(\mathbf{R}) \setminus \{0\}$ een niet-inverteerbare matrix. Bewijs: A is zowel een linker- als een rechternuldeler.

26. Laat zien dat de matrixring $\mathrm{Mat}_n(\mathbf{R})$ geen niet-triviale (tweezijdige) idealen heeft.

27. Bepaal het centrum van de matrixring $\mathrm{Mat}_n(\mathbf{R})$.

28. Zij $V = \{(a_i)_{i=0}^{\infty} : a_i \in \mathbf{R}\}$ de $\mathbf{R}$-vectorruimte van $\mathbf{R}$-waardige rijtjes met componentsgewijze optelling en scalaire vermenigvuldiging. Zij R de ring van $\mathbf{R}$-lineaire afbeeldingen $V \to V$. Definieer $s, t, u \in R$ door

$$\begin{aligned}(a_0, a_1, a_2, a_3, \ldots) &\overset{s}{\longmapsto} (0, a_0, a_1, a_2, \ldots)\\ (a_0, a_1, a_2, a_3, \ldots) &\overset{t}{\longmapsto} (a_1, a_2, a_3, a_4, \ldots)\\ (a_0, a_1, a_2, a_3, \ldots) &\overset{u}{\longmapsto} (a_0, 0, 0, 0, \ldots).\end{aligned}$$

Bewijs de volgende uitspraken:
   a. $st \neq 1 \in R$ en $ts = 1 \in R$;
   b. $us = 0 \in R$ en $tu = 0 \in R$;
   c. s is rechternuldeler in R maar geen linkernuldeler, t is linkernuldeler in R maar geen rechternuldeler.

29. Zij $R \neq 0$ een commutatieve ring met eenhedengroep $R^* = \{1\}$.
   a. Bewijs: R heeft karakteristiek 2.
   b. Bewijs dat $f : R \to R$ gegeven door $f(r) = r^2$ een ringhomomorfisme is.
   c. Bewijs dat de afbeelding f in onderdeel (b) injectief is. Is f noodzakelijk surjectief?

30. Een *Boolese ring* is een ring waarin voor ieder element x de identiteit $x^2 = x$ geldt. Bewijs dat iedere Boolese ring de nulring of een commutatieve ring van karakteristiek 2 is. Laat zien dat $\mathbf{F}_2$ de enige Boolese ring is die een lichaam is.
[George Boole (1815–1864) was een Engels wiskundige.]

31. Zij X een verzameling. Dan definieert het symmetrisch verschil $A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$ wegens opgave 4.41 een abelse groepsstructuur op de machtsverzameling $\mathcal{P}(X)$. Laat zien dat R met de multiplicatieve bewerking $A \cdot B = A \cap B$ een Boolese ring wordt, en dat hiermee het groepsisomorfisme $\mathcal{P}(X) \xrightarrow{\sim} \mathrm{Map}(X, \mathbf{Z}/2\mathbf{Z})$ uit 4.41 een ringisomorfisme met de functiering $\mathrm{Map}(X, \mathbf{Z}/2\mathbf{Z})$ wordt.

32. Laten X en Y verzamelingen zijn, en $f\colon X \to Y$ een afbeelding. Dan induceert f natuurlijke afbeeldingen $f_*\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ en $f^*\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ door

$$f_*(A) = f[A] = \{f(x) : x \in A\}, \qquad f^*(B) = f^{-1}[B] = \{x \in X : f(x) \in B\},$$

voor $A \subset X$ en $B \subset Y$.
   a. Bewijs: f_* is een ringhomomorfisme dan en slechts dan als f een bijectie is.
   b. Is f^* een ringhomomorfisme? Geef een bewijs of een tegenvoorbeeld.

33. Zij R de ring van differentieerbare functies $\mathbf{R} \to \mathbf{R}$. Welke van de volgende afbeeldingen $R \to \mathbf{R}$ zijn homomorfismen van additieve groepen? Zijn het ringhomomorfismen?

$$f \longmapsto f(0); \qquad f \longmapsto f'(0); \qquad f \longmapsto \textstyle\int_0^1 f(x)dx.$$

34. Laat zien dat een ringhomomorfisme $f : R_1 \to R_2$ door beperking een groepshomomorfisme $g = f|_{R_1^*} : R_1^* \to R_2^*$ op de eenhedengroepen induceert. Is g surjectief als f het is? Is f surjectief als g het is?

35. Laat zien dat de evaluatie-afbeelding $\phi_a : \sum c_i X^i \mapsto \sum c_i a^i$ een ringhomomorfisme $R[X] \to R$ geeft dan en slechts dan als a bevat is in het centrum $Z(R)$ van R.

36. Zij R een commutatieve ring. Laat zien dat voor $n \geq 1$ en $a = (a_1, a_2, \ldots, a_n) \in R^n$ de evaluatie-afbeelding $\phi_a : R[X_1, X_2, \ldots, X_n] \to R$ gegeven door $\phi_a(f) = f(a)$ een surjectief ringhomomorfisme is met kern $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$.

37. Definieer $T \subset \mathrm{Mat}_2(R)$ door $T = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) : a, b, d \in R\}$. Bewijs:
    a. T is een deelring van $\mathrm{Mat}_2(R)$, en voor $R \neq 0$ is T niet commutatief;
    b. $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in T^* \iff a \in R^*$ en $d \in R^*$;
    c. T^* is abels $\iff R^* = \{1\}$.

    Bestaat er een niet-commutatieve ring R waarvoor de eenhedengroep R^* abels is?

38. Zij K een lichaam.
    a. Kan men $K[X, X^{-1}]$ met het quotiëntenlichaam $Q(K[X])$ van $K[X]$ identificeren?
    b. Vat de machtreeksenring $K[[X]]$ op als deelring van de ring $K((X))$ van Laurentreeksen over K. Bewijs: $Q(K[[X]]) = K((X))$.

39. Een *ring zonder eenheidselement*, door sommigen wel *rng* genoemd, is een additief geschreven abelse groep R voorzien van een multiplicatieve bewerking $R \times R \to R$ die voldoet aan (R2) en (R3), maar niet aan (R1). In welke van de onderstaande gevallen hebben we met zo'n ring te doen?
    a. de deelverzameling $2\mathbf{Z} \subset \mathbf{Z}$ van even getallen;
    b. een ideaal $I \subset R$ dat niet gelijk is aan $\{0\}$ of R;
    c. de deelcollectie $R \subset C(\mathbf{R})$ van continue functies $\mathbf{R} \to \mathbf{R}$ met begrensde drager. (De *drager* van $f \in C(\mathbf{R})$ is de verzameling $\{x \in \mathbf{R} : f(x) \neq 0\}$.)
    d. een willekeurige abelse groep R voorzien van de 'nulvermenigvuldiging' $xy = 0$ voor alle $x, y \in R$.

40. Zij R' een ring zonder eenheidselement. Definieer op $R = \mathbf{Z} \times R'$ de bewerkingen

$$(n_1, r_1) + (n_2, r_2) = (n_1 + n_2, r_1 + r_2)$$
$$(n_1, r_1) \cdot (n_2, r_2) = (n_1 n_2, r_1 r_2 + n_1 r_2 + n_2 r_1).$$

    (Gebruik de voor de hand liggende definitie van nr voor $n \in \mathbf{Z}$ en $r \in R'$.) Laat zien dat R een ring is, en dat R' met een ideaal in R geïdentificeerd kan worden.

41. Laat I en J onderling ondeelbare idealen in een commutatieve ring R zijn, en $m, n \in \mathbf{Z}_{>0}$ positieve getallen. Bewijs dat I^m en J^n onderling ondeelbaar zijn.

42. Laat I en J als in de vorige opgave zijn, en stel dat $I \cdot J = K^n$ geldt, met K een ideaal en $n \in \mathbf{Z}_{>0}$. Bewijs dat er idealen I_0 en J_0 zijn met $I = I_0^n$ en $J = J_0^n$.
    [Hint: kijk naar $I_0 = I + K$, de 'ggd' van I en K.]

43. Laat i en j onderling ondeelbare gehele getallen zijn, en stel dat $i \cdot j = k^n$ geldt, met $k \in \mathbf{Z}$ en $n \in \mathbf{Z}_{>0}$. Bewijs: er bestaan $i_0, j_0 \in \mathbf{Z}$ en $\varepsilon \in \mathbf{Z}^* = \{\pm 1\}$ met $i = \varepsilon i_0^n$ en $j = \varepsilon j_0^n$.
    *Geef een voorbeeld van een commutatieve ring R waarin identiteiten $ai + bj = 1$ en $i \cdot j = k^n$ gelden $(a, b, i, j, k \in R)$, maar i en j niet het product zijn van een eenheid en een n-de macht in R.

44. Definieer $I, J \subset \mathbf{Z}[X]$ door $I = (2, X)$ en $J = (3, X)$. Laat zien dat $\{i \cdot j : i \in I \text{ en } j \in J\}$ geen ideaal is in $\mathbf{Z}[X]$, en in het bijzonder niet gelijk is aan $I \cdot J = (6, X)$.

45. Laat I en J idealen van een commutatieve ring R zijn. Laat zien dat $\{xy : x \in I, y \in J\}$ een ideaal van R is als I of J een hoofdideaal is.

46. Bewijs voor idealen I en J van een commutatieve ring R de inclusie $(I+J)\cdot(I\cap J)\subset IJ$, en laat zien dat voor $R=\mathbf{Z}$ gelijkheid geldt. *Geldt altijd gelijkheid?

47. Zij X een eindige verzameling, en neem $R=\mathrm{Map}(X,\mathbf{C})$. Definieer voor $x\in X$ het ideaal $I_x=\{f\in R: f(x)=0\}$. Bewijs:
    a. $R/I_x\cong\mathbf{C}$ voor iedere $x\in X$;
    b. er is een ringisomorfisme $R\cong\mathbf{C}^n$ voor zekere $n\in\mathbf{Z}_{\geq 0}$.

48. Formuleer en bewijs een generalisatie van 11.19 voor het geval van paarsgewijs coprieme idealen $I_1, I_2, \ldots, I_n$.

49. Zij $f: R_1\longrightarrow R_2$ een ringhomomorfisme en $I_2\subset R_2$ een ideaal van R_2. Bewijs dat $I_1=f^{-1}[I_2]$ een ideaal van R_1 is, en dat R_1/I_1 isomorf is met een deelring van R_2/I_2.

50. Zij $R=\mathrm{Map}(\mathbf{Z}_{>0},\mathbf{Q})$ de ring van $\mathbf{Q}$-waardige functies op $\mathbf{Z}_{>0}$. We noemen $f\in R$ een *Cauchy-functie* als er voor alle $\varepsilon\in\mathbf{Q}_{>0}$ een getal N bestaat zodat $|f(m)-f(n)|<\varepsilon$ geldt voor alle $m,n>N$. Een functie $f\in R$ heet een *nulfunctie* als $\lim_{n\to\infty} f(n)=0$ geldt. Bewijs:
    a. de verzameling C van Cauchy-functies vormt een deelring $C\subset R$;
    b. de verzameling I van nulfuncties is een ideaal van C, maar niet van R;
    c. er geldt $C/I\cong\mathbf{R}$.

51. Zij $I\subset R$ een ideaal. Bewijs: ieder ideaal van R/I is van de vorm J/I voor een ideaal $J\supset I$ van R, en voor dergelijke J is er een natuurlijk isomorfisme

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

    [Dit is het ringen-analogon van 8.1. Het stelt ons in staat R/J 'stapsgewijs' te berekenen: maak eerst R/I, en deel dan verder uit naar J/I.]

52. Zij $R'\subset R$ een deelring en $I\subset R$ een ideaal. Bewijs het ringen-analogon van 8.2:
    a. $R'\cap I$ is een ideaal van R', en $R'+I=\{r+s: r\in R', s\in I\}$ een deelring van R;
    b. er is een natuurlijk isomorfisme $R'/(R'\cap I)\xrightarrow{\sim}(R'+I)/I$.

53. Het *commutatorideaal* $[R,R]$ van een ring R is het linksideaal voortgebracht door de elementen van de vorm $yx-xy$ met $x,y\in R$. Bewijs dat $[R,R]$ een tweezijdig ideaal is, en $R_{\mathrm{comm}}=R/[R,R]$ een commutatieve ring met de eigenschap dat ieder homomorfisme $R\to R'$ naar een commutatieve ring R' factoriseert via R_{comm}, dat wil zeggen geschreven kan worden als een samenstelling van homomorfismen $R\to R_{\mathrm{comm}}\to R'$.
    [Dit is het ringen-analogon van 8.5.]

54. Het tweezijdige ideaal (S) voortgebracht door een deelverzameling $S\subset R$ is gedefinieerd als het kleinste tweezijdige ideaal van R dat S bevat. Laat zien dat zo'n ideaal altijd bestaat, en geef een 'expliciete beschrijving' van (S) zoals we die voor commutatieve R gaven.

*55. Bewijs dat ieder linksideaal in $\mathrm{Mat}_n(\mathbf{R})$ van de vorm $L_V=\{M:\ker(M)\supset V\}$ is, en ieder rechtsideaal van de vorm $R_V=\{M:\mathrm{im}(M)\subset V\}$, met $V\subset\mathbf{R}^n$ een deelruimte.

56. Een *idempotent* in een ring R is een element $e\in R$ waarvoor $e^2=e$ geldt. De triviale idempotenten in een ring zijn de elementen 0 en 1. Bewijs dat als e een idempotent van een commutatieve ring R is, dan is $1-e$ ook een idempotent en er is een isomorfisme

$$R\xrightarrow{\sim}R/eR\times R/(1-e)R.$$

Laat zien dat de idempotenten van een commutatieve ring R bijectief corresponderen met de 'decomposities' van R als een product $R = R_1 \times R_2$, en dat de verzameling van idempotenten in R een *ring* vormt onder de 'gewone' vermenigvuldiging en een 'idempotentenoptelling' gegeven door

$$x \oplus y = (x - y)^2.$$

57. Bepaal de idempotenten in de ring $\mathbf{Z}/1000\mathbf{Z}$.

58. Definieer recursief een rij van gehele getallen door $x_0 = 5$ en voor $k \geq 1$

$$x_k = [\text{rest van } x_{k-1}^2(3 - 2x_{k-1}) \text{ bij deling door } 10^{2^k}].$$

Hierbij worden alle resten in het interval $[0, 10^{2^k})$ genomen, dus: $x_1 = 25$, $x_2 = 625$, $x_3 = 12890625$, enz. Bewijs: $(x_k \bmod 10^{2^k})$ is voor alle $k \geq 1$ een idempotent in $\mathbf{Z}/10^{2^k}\mathbf{Z}$. Geldt hetzelfde als we met $x_0 = 6$ starten?

59. Zij G een groep. Definieer de *augmentatie-afbeelding* $f : \mathbf{Z}[G] \to \mathbf{Z}$ op de groepenring $\mathbf{Z}[G]$ door $f(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$. Laat zien dat f een surjectief ringhomomorfisme is, en dat het tweezijdige ideaal $I_G = \ker(f)$ wordt voortgebracht door de verzameling $\{g - 1 : g \in G\}$.
[Het ideaal I_G heet het *augmentatie-ideaal* van $\mathbf{Z}[G]$.]

60. Laat G en I_G als in de vorige opgave zijn. Bewijs dat de afbeelding

$$\begin{aligned} G_{\text{ab}} = G/[G,G] &\longrightarrow I_G/I_G^2 \\ g \bmod [G,G] &\longmapsto g - 1 \bmod I_G^2 \end{aligned}$$

een isomorfisme van abelse groepen is. Hier is G_{ab} de abels gemaakte groep uit 8.5.

61. Zij G een cyclische groep. Laat zien dat het augmentatie-ideaal I_G een hoofdideaal is.

62. Zij R een ring waarvoor de onderliggende optelgroep R^+ cyclisch is. Bewijs: $R \cong \mathbf{Z}/n\mathbf{Z}$ (als ring) voor zekere $n \in \mathbf{Z}_{\geq 0}$.

63. Bepaal alle (isomorfietypen van) ringen waarvoor R^+ een viergroep van Klein is.

64. De rij $(F_n)_{n=0}^{\infty}$ van *Fibonacci-getallen* is inductief gedefinieerd door $F_0 = 0$, $F_1 = 1$, en $F_{n+2} = F_{n+1} + F_n$ (voor $n \geq 0$).
    a. Construeer een ring R die $\mathbf{Z}$ als deelring omvat en een element ϑ bevat met de eigenschap dat voor alle positieve gehele getallen n geldt $\vartheta^n = F_{n-1} + F_n \cdot \vartheta$.
    b. Bestaat er een ring R als in (a) zodanig dat er maar één $\vartheta \in R$ met de genoemde eigenschap bestaat?

65. Zij R de verzameling van alle 2×2-matrices $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ met $a \in \mathbf{Z}/4\mathbf{Z}$, $b \in 2\mathbf{Z}/4\mathbf{Z}$, $c \in \mathbf{Z}/2\mathbf{Z}$. Twee elementen van R worden componentsgewijs opgeteld, en ze worden vermenigvuldigd als matrices, waarbij de nodige bewerkingen op de componenten van de matrices geïnduceerd zijn door de ringoperaties op $\mathbf{Z}$. Op deze manier wordt R een ring (ga na, geen deel van de opgave...). Schrijf $I = \{x \in R : x^2 = 0\}$.
    a. Bewijs dat I een tweezijdig ideaal van R is met $\#I = 4$, en dat de ring R/I isomorf is met de productring $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$.

b. Bewijs: er bestaat geen element $y \in R$ met $I = Ry$, maar er is wel een element $z \in R$ met $I = zR$.

66. Zij R een ring. De tegengestelde ring R^{opp} maakt men uit R door op de optelgroep van R een vermenigvuldiging '$\star$' te definiëren door $x \star y = yx$. Laat zien dat R^{opp} een ring is, en construeer een ring R waarvoor R *niet* isomorf is met R^{opp}.

67. *(Lemma van Goursat voor ringen)* Laat R_1 en R_2 ringen zijn, en $A \subset R_1 \times R_2$ een deelring. Bewijs dat er deelringen $A_1 \subset R_1$ en $A_2 \subset R_2$ bestaan, alsmede een ideaal I_1 van A_1, een ideaal I_2 van A_2 en een ringisomorfisme $\phi\colon A_1/I_1 \xrightarrow{\sim} A_2/I_2$, zodanig dat geldt
$$A = \{(a_1, a_2) \in A_1 \times A_2 : \phi(a_1 + I_1) = a_2 + I_2\}.$$
(Vergelijk met opgave 8.37.)

68. Bewijs dat de idealen van $R_1 \times R_2$ van de vorm $I_1 \times I_2$ zijn, met $I_i \subset R_i$ een ideaal. [Er is dus geen 'lemma van Goursat' voor idealen.]

69. Stel dat R een ring is met de eigenschap dat elk element van R eindige orde in de additieve groep van R heeft. Bewijs dat er een positief geheel getal m is zodat voor elke $a \in R$ geldt $m \cdot a = 0$. Construeer een abelse groep die niet optreedt als de additieve groep van een ring.

70. Zij $A_X = \mathbf{Z}((X))$ de ring van Laurentreeksen in X over $\mathbf{Z}$, en $A_X((Y)) = \mathbf{Z}((X))((Y))$ de ring van Laurentreeksen in Y over A_X. Bewijs: $X - Y \in A^*_{X,Y}$.

71. Definieer als in de vorige opgave nu ook $A_Y = \mathbf{Z}((Y))$ en $A_{Y,X} = \mathbf{Z}((Y))((X))$, en laat B de optelgroep zijn van van alle formele uitdrukkingen $\sum_{i,j\in\mathbf{Z}} a_{ij}X^iY^j$ met $a_{ij} \in \mathbf{Z}$, onder componentsgewijze optelling.
    a. Laat zien dat de optelgroepen van de ringen $A_{X,Y}$ en $A_{Y,X}$ als ondergroepen van B opgevat kunnen worden, dat de doorsnede $C = A_{X,Y} \cap A_{Y,X}$ binnen B een deelring is van zowel $A_{X,Y}$ als $A_{Y,X}$, en dat de beide aldus op C gedefinieerde vermenigvuldigingen samenvallen.
    b. Bewijs: $X - Y \in C$ en $X - Y \notin C^*$.
    c. Bestaat er een ondergroep D van B die zowel $A_{X,Y}$ als $A_{Y,X}$ omvat, waarop men een vermenigvuldiging kan definiëren zodanig dat D een ring is waarvan de ringen $A_{X,Y}$ en $A_{Y,X}$ deelringen zijn (met dezelfde vermenigvuldiging)?

72. *(Localisatie)* Zij R een commutatieve ring, en $S \subset R$ een deelverzameling die 1 bevat en gesloten is onder vermenigvuldiging. Definieer een equivalentierelatie op $R \times S$ door
$$\frac{r}{s} \sim \frac{r'}{s'} \iff (rs' - r's)s\text{"} = 0 \quad \text{voor een element } s\text{"} \in S.$$
    a. Laat zien dat dit een equivalentierelatie is.

    Noteer de equivalentieklasse van $(r, s) \in R \times S$ als $\frac{r}{s}$, en definieer een optelling en vermenigvuldiging op de verzameling $S^{-1}R$ van equivalentieklassen door de bekende 'breukenformules' uit 11.10.
    b. Laat zien dat $S^{-1}R$ hiermee een commutatieve ring wordt, en de afbeelding $R \to S^{-1}R$ gegeven door $r \mapsto \frac{r}{1}$ een ringhomomorfisme.
    c. Bewijs: $S^{-1}R = 0 \iff 0 \in S$.
    d. Geef een voorbeeld waarin $S^{-1}R$ niet de nulring is, en de afbeelding $R \to S^{-1}R$ *niet* injectief.

12 Hoofdideaaldomeinen

Hoofdideaaldomeinen zijn domeinen waarin alle idealen hoofdidealen zijn. De ring $\mathbf{Z}$ is er een voorbeeld van, en veel eigenschappen van $\mathbf{Z}$ blijken voor willekeurige hoofdideaaldomeinen te gelden. Hieronder is ook de fundamentele stelling 6.7 over de *eenduidige priemfactorontbinding* van gehele getallen.

▶ Deling met rest

In 6.2 bewezen we dat $\mathbf{Z}$ een hoofdideaaldomein is door gebruik te maken van de deling met rest 6.1. Dit procédé kan gebruikt worden in veel situaties waar een geschikte notie van 'grootte' van elementen bestaat. In de polynoomring $R[X]$ is de *graad* een dergelijke notie. De graad $\deg(f)$ van een polynoom $f = \sum a_k X^k \in R[X]$ is de grootste index $k \in \mathbf{Z}_{\geq 0}$ met $a_k \neq 0$. Alleen voor het nulpolynoom bestaat zo'n k niet; we nemen $\deg(0) = -1$. Voor f van graad $n \geq 0$ heet de coëfficiënt a_n de *kopcoëfficiënt* van f. Voor ringen R zonder niet-triviale nuldelers is de kopcoëfficiënt van een product fg in $R[X]$ het product van de kopcoëfficiënten van f en g, en geldt het bekende regeltje

$$\deg(fg) = \deg(f) + \deg(g)$$

voor de vermenigvuldiging van polynomen verschillend van 0.

12.1. Deling met rest voor polynomen. *Zij R een ring, en laat $f, g \in R[X]$ polynomen zijn. Stel dat $g \neq 0$ een kopcoëfficiënt in R^* heeft. Dan bestaan er polynomen $q, r \in R[X]$ met*

$$f = qg + r \qquad \text{en} \qquad \deg(r) < \deg(g).$$

Bewijs. We voeren het bewijs met inductie naar de graad van f. Voor $\deg(f) = -1$ hebben we $f = 0$ en voldoet de keus $q = r = 0$. Stel nu dat deling met rest mogelijk is voor polynomen f van graad $\deg(f) < n \in \mathbf{Z}_{\geq 0}$. Voor f van graad n schrijven we nu informeel $f = a_n X^n + \ldots$, en evenzo $g = b_m X^m + \ldots$, met $m = \deg(g)$ en $b_m \in R^*$. Voor $m > n$ kunnen we $q = 0$ en $r = f$ nemen en is er niets te bewijzen. Voor $m \leq n$ kijken we naar het verschil $f - a_n b_m^{-1} X^{n-m} g$. Omdat $a_n b_m^{-1} X^{n-m} g$ net als f graad n en kopcoëfficiënt a_n heeft is de graad van dit verschil kleiner dan n. Wegens de inductiehypothese hebben we dus

$$f - a_n b_m^{-1} X^{n-m} g = q_1 g + r \qquad \text{met} \qquad \deg(r) < \deg(g)$$

voor zekere $q_1, r \in R[X]$. Met $q = a_n b_m^{-1} X^{n-m} + q_1$ geldt nu $f = qg + r$, en dit is de deling met rest voor f zelf. □

Opgave 1. Laat zien dat q en r in 12.1 uniek bepaald zijn door f en g.

De ring R in 12.1 is volstrekt willekeurig, en mag niet-triviale nuldelers hebben of niet-commutatief zijn. In al deze gevallen zijn het *quotiënt* q en de *rest* r uniek bepaald door f en g, en het bewijs van 12.1 beschrijft de manier waarop men q en r met een *staartdeling* uit f en g berekent: trek steeds een veelvoud van g van f af waarvoor de 'kopterm' wegvalt, en ga zo door tot een rest van graad kleiner dan de graad van g overblijft.

Opgave 2. Bereken q en r in 12.1 voor $R = \mathbf{Z}$ en $f = 4X^4 + 3X^3 + 2X^2 + X$ en $g = X^2 + 2X + 3$.

Nemen we voor g in 12.1 een lineair polynoom $X - a$, dan is de rest r een constant polynoom met waarde $f(a)$. Voor commutatieve R volgt dit door $X = a$ in te vullen. Het argument in 11.16 laat echter zien dat het polynoom $f - f(a)$, als 'R-lineaire combinatie' van uitdrukkingen $X^i - a^i$, altijd van de vorm $q \cdot (X - a)$ is.

12.2. Gevolg. *Zij R een ring. Dan bestaat er voor iedere $f \in R[X]$ en $a \in R$ een polynoom $q \in R[X]$ met*

$$f = q \cdot (X - a) + f(a). \qquad \square$$

12.3. Gevolg. *Zij R een domein, en stel dat $f \in R[X]$ de n verschillende nulpunten $a_1, a_2, \ldots, a_n$ heeft in R. Dan geldt*

$$f = q \cdot (X - a_1)(X - a_2) \ldots (X - a_n) \qquad \text{met } q \in R[X].$$

Voor $f \neq 0$ is het aantal nulpunten van f in R niet groter dan $\deg(f)$.

Bewijs. We passen inductie toe naar n. Voor $n = 1$ hebben we een speciaal geval van 12.2. Voor $n > 1$ schrijven we $f = q_1 \cdot (X - a_n)$ met $q_1 \in R[X]$ met behulp van 12.2. Omdat R commutatief is, geeft invullen van een nulpunt a_i met $i \neq n$ de relatie $q_1(a_i) \cdot (a_i - a_n) = 0$. Omdat R geen niet-triviale nuldelers heeft volgt dat alle $n - 1$ nulpunten a_i met $i < n$ nulpunten zijn van het polynoom q_1. Met inductie hebben we nu $q_1 = q \cdot (X - a_1)(X - a_2) \ldots (X - a_{n-1})$, en dit laat zien dat $f = q_1 \cdot (X - a_n)$ de vereiste vorm heeft. In het bijzonder zien we dat voor een domein R een polynoom $f \in R[X] \setminus \{0\}$ met n verschillende nulpunten graad tenminste gelijk aan n heeft. $\square$

12.4. Gevolg. *Zij R een domein, en $H \subset R^*$ een eindige ondergroep van de eenhedengroep van R. Dan is H cyclisch.*

Bewijs. We brengen in herinnering dat een *cyclische* groep $C = \langle y \rangle$ van orde n voor iedere positieve deler $d|n$ precies één ondergroep van orde d bevat, voortgebracht door $x = y^{n/d}$, en dat de elementen van orde d in C de machten x^i van x zijn met exponent $i \in \{1, 2, \ldots d\}$ onderling ondeelbaar met d. In het bijzonder bevat C voor iedere $d|n$ precies $\varphi(d)$ elementen van orde d, met φ de Euler-φ-functie. Sommatie over alle $d|n$ geeft $\sum_{d|n} \varphi(d) = \#C = n$, de formule van Gauss.

Laat nu, voor $H \subset R^*$ in 12.4 van orde n en $d|n$ een positieve deler, $\psi(d)$ het aantal elementen van orde d in H zijn. Als $x \in H$ orde d heeft, dan zijn de d verschillende machten $x, x^2, x^3, \ldots, x^d = 1$ van x nulpunten van $X^d - 1$ in R. Wegens 12.3 zijn er dan geen andere nulpunten van $X^d - 1$ in R, dus de elementen van orde d in H zijn precies de $\varphi(d)$ machten x^i van x met exponent i copriem met d. We concluderen dat $\psi(d)$ gelijk is aan $\varphi(d)$ als H een element van orde d bevat, en gelijk aan 0 als dat niet het geval is. Nu geldt

$$n = \#H = \textstyle\sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n,$$

en er volgt $\psi(d) = \varphi(d)$ voor alle $d|n$. In het bijzonder geldt $\psi(n) = \varphi(n) > 0$, dus H bevat een element van orde n en is cyclisch. $\square$

12.5. Gevolg. *De eenhedengroep F^* van een eindig lichaam F is cyclisch.* □

De enige eindige lichamen die wij tegen zijn gekomen zijn de lichamen $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ behorende bij de priemgetallen $p \in \mathbf{Z}$. Een getal $x \in \mathbf{Z}$ waarvoor $(x \bmod p)$ een voortbrenger is van $\mathbf{F}_p^* = (\mathbf{Z}/p\mathbf{Z})^*$ heet een *primitieve wortel* modulo p. Het bestaan van zulke elementen noemden we al in §9 (in verband met de constructie van niet-abelse groepen van orde pq) en in §10 (in verband met de structuur van de groepen $(\mathbf{Z}/p^k\mathbf{Z})^*$).

Voor ieder geheel getal $n > 0$ vormen de complexe nulpunten van $X^n - 1$ de ondergroep van n-de *eenheidswortels* in $\mathbf{C}^*$. Dit is een cyclische groep van orde n voortgebracht door $e^{2\pi i/n}$. De enige niet-triviale eindige ondergroep van $\mathbf{R}^*$ (of $\mathbf{Z}^*$) is de cyclische tekengroep $\{\pm 1\}$ van orde 2.

12.6. Gevolg. *Zij K een lichaam. Dan is $K[X]$ een hoofdideaaldomein.*

Bewijs. We imiteren het bewijs van 6.2. Zij $I \subset K[X]$ een ideaal. Voor $I = 0$ is 0 een voortbrenger van I. Voor $I \neq 0$ kiezen we een niet-nul-polynoom $g \in I$ van minimale graad. Is nu $f \in I$ een willekeurig ander polynoom, dan bestaan er wegens 12.1 polynomen $q, r \in K[X]$ met $f = qg + r$ en $\deg(r) < \deg(g)$. Wegens $r = f - qg \in I$ en de minimaliteit van $\deg(g)$ geldt $r = 0$, dus $f = qg$. We vinden $I = (g)$. □

▶ Eenduidige ontbinding

We gaan in stelling 12.11 bewijzen dat in willekeurige hoofdideaaldomeinen R ieder element $x \neq 0$ te ontbinden is in een in essentie uniek product van priemelementen. Voor $R = \mathbf{Z}$ is dit een uit 6.7 bekende stelling. Voor $R = K[X]$ uit 12.6 betekent het dat ieder polynoom $f \neq 0$ in essentie eenduidig te ontbinden is in een product van *irreducibele polynomen* in $K[X]$.

We spreken van 'in essentie' eenduidige ontbindingen omdat de factoren in een ontbinding altijd met eenheden uit de ring vermenigvuldigd kunnen worden. Voor $R = \mathbf{Z}$ konden we de priemgetallen steeds *positief* kiezen, en hiermee krijgt ieder getal $x \neq 0$ een unieke ontbinding als product van een eenheid in $\mathbf{Z}^* = \{\pm 1\}$ en een eindig aantal priemgetallen. Voor $R = K[X]$ bestaat $R^* = K^*$ uit constante polynomen (opgave 11.13), zodat irreducibele polynomen in een ontbinding tot op vermenigvuldiging met een constante vastliggen.

Voor de goede orde vermelden we dat in een commutatieve ring R een element $x \in R$ een *deler* van $y \in R$ heet als $y = xz$ geldt voor zekere $z \in R$. Men zegt ook wel dat y een *veelvoud* van x is. De eenheden van R delen 1, en dus ieder ander element van R.

12.7. Definitie. *Een element p in een domein R heet irreducibel als het geen eenheid is en voldoet aan de eigenschap*

$$p = xy \quad \text{met} \quad x, y \in R \quad \Longrightarrow \quad x \in R^* \quad \text{of} \quad y \in R^*.$$

Merk op dat de irreducibele elementen in $\mathbf{Z}$ op teken na precies de priemgetallen zijn. In de polynoomring $K[X]$ (en in andere polynoomringen) spreken we van *irreducibele polynomen*.

12.8. Lemma. *Zij R een hoofdideaaldomein en $x \in R$ verschillend van 0. Dan bestaat er een ontbinding*

$$x = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t$$

van x als product van een eenheid $u \in R^*$ en eindig veel irreducibele elementen $p_i \in R$.

Bewijs. We geven een bewijs uit het ongerijmde. Stel dat er een element $x \neq 0$ in R bestaat dat *geen* ontbinding van de genoemde soort heeft. Dan is x geen eenheid, want $x = x$ zou in dat geval een ontbinding (met $t = 0$ irreducibele elementen) zijn. Ook is x niet irreducibel, omdat in dat geval $x = 1 \cdot x$ een ontbinding zou geven. Uit definitie 12.7 volgt nu dat er een identiteit $x = yz$ in R bestaat waarin y en z *geen* eenheden zijn. Als y en z beide een ontbinding van de verlangde soort hebben, dan geven die samen een ontbinding van x; immers, we hoeven slechts de eenheden uit beide ontbindingen te vermenigvuldigen tot een nieuwe eenheid in de ontbinding van x. We concluderen dat y of z, zeg y, óók geen ontbinding van de verlangde soort heeft.

Uit $x = yz$ zien we dat we een ideaalinclusie $(x) \subset (y)$ hebben, en deze inclusie is geen gelijkheid. Immers, uit $y \in (x)$, zeg $y = wx$, zou volgen $x = zwx$ en, omdat R een domein is, $zw = 1$ en $z \in R^*$.

Passen we het argument voor x nu toe op $x_1 = y$, dan vinden we een strikte ideaalinclusie $(x_1) \subsetneq (x_2)$ voor een element x_2 dat wederom geen ontbinding heeft. Zo doorgaande krijgen we een oneindig lange strikt stijgende keten

$$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq (x_4) \subsetneq \ldots$$

van hoofdidealen in R voortgebracht door elementen x_i zonder ontbinding in R.

We besluiten het bewijs door te laten zien dat zo'n keten niet kan bestaan. Zij namelijk $I = \bigcup_{k \geq 1}(x_k)$ de vereniging van de idealen (x_i). Dan is I weer een ideaal in R (waarom?), en er geldt $I = (x_\infty)$ voor zekere $x_\infty \in R$. Per definitie van I is er een waarde van k met $x_\infty \in (x_k)$, en dit geeft, in tegenspraak met de aanname, $I = (x_\infty) = (x_k)$ voor deze k. □

In concrete hoofdideaaldomeinen R is het vaak direct duidelijk dat men in eindig veel stappen een ontbinding als in 12.8 kan vinden. Immers, als x niet irreducibel en geen eenheid is schrijft men $x = yz$ met y en z geen eenheden, en gaat inductief verder met ontbinden van y en z. In veel gevallen is duidelijk dat dit proces eindigt omdat de elementen y en z in zo'n splitsing 'kleiner' zijn dan x. Zo wordt bijvoorbeeld in $\mathbf{Z}$ de absolute waarde kleiner, terwijl in $K[X]$ steeds de graad van de polynomen omlaag gaat. Opgave 34 geeft een axiomatisering van dit fenomeen.

We willen nu bewijzen dat de in 12.8 gevonden ontbindingen op vermenigvuldiging van de irreducibele elementen p_i met eenheden na eenduidig zijn. We hebben hiervoor de in 6.6 geformuleerde *priemeigenschap* van irreducibele elementen in een hoofdideaaldomein nodig.

12.9. Definitie. *Een priemelement in een domein R is een element $p \neq 0$ dat geen eenheid is en voldoet aan de priemeigenschap*

$$p|xy \qquad \Longrightarrow \qquad p|x \quad \textit{of} \quad p|y.$$

De priemelementen in een domein zijn altijd irreducibel. Immers, als voor een priemelement p de gelijkheid $p = yz$ geldt, dan is p een deler van y of z. Hebben we bijvoorbeeld $y = pw$, dan vinden we $p = yz = pwz$ en $wz = 1$, dus z is een eenheid en p is irreducibel.

Domeinen met de complicerende eigenschap dat ze irreducibele elementen bevatten die *niet* priem zijn komen we aan het einde van deze paragraaf tegen. Ze vormen de historische aanleiding tot het beschouwen van *idealen* in ringen.

12.10. Lemma. *Ieder irreducibel element in een hoofdideaaldomein is priem.*

Bewijs. We imiteren het bewijs van 6.6. Stel dat p een irreducibel element is in een hoofdideaaldomein R, en dat p een deler is van xy maar niet van x. We moeten laten zien dat p in dat geval y deelt.

Omdat p geen deler is van x geldt $x \notin (p)$, en dit betekent dat het ideaal $(p) + (x) = (p, x) \subset R$ strikt groter is dan (p). Omdat het een hoofdideaal is, heeft het een voortbrenger $z \in R$. Dan geldt $p = zw$ voor zekere $w \in R$, en omdat de inclusie $(p) \subsetneq (z)$ een strikte is, is w *geen* eenheid in R. Wegens de irreducibiliteit van p geldt nu $z \in R^*$, dus we hebben $(z) = (p, x) = R$. In het bijzonder is het element $1 \in (p, x) = (p)+(x)$ te schrijven als $1 = ap+bx$ met $a, b \in R$. Het element $y = (ap+bx)y = apy+bxy$ is nu een som van elementen apy en bxy die elk deelbaar zijn door p. Er volgt dat y zelf ook deelbaar is door p. □

Opgave 3. Bewijs: als p een irreducibel element in een hoofdideaaldomein R is, dan is R/pR een lichaam.

We kunnen nu ons belangrijkste resultaat voor hoofdideaaldomeinen bewijzen.

12.11. Stelling. *Zij R een hoofdideaaldomein. Dan is ieder element $x \neq 0$ in R te schrijven als een product*

$$x = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t$$

van een eenheid $u \in R^*$ en eindig veel irreducibele elementen $p_i \in R$; deze schrijfwijze is op volgorde en vermenigvuldiging met eenheden na eenduidig.

Bewijs. Het is na 12.8 voldoende om de eenduidigheid van de ontbinding te bewijzen. Stel dus dat we twee ontbindingen

$$up_1p_2 \ldots p_s = vq_1q_2 \ldots q_t$$

hebben, met $u, v \in R^*$ en alle p_i en q_j irreducibel. We willen bewijzen dat $s = t$ geldt, en dat de irreducibele elementen in beide ontbindingen op eenheden na aan elkaar gelijk zijn. We voeren het bewijs met inductie naar s. Voor $s = 0$ is $t = 0$ omdat geen enkel irreducibel element q_i de eenheid u deelt — dan zou immers q_i een eenheid zijn. In dat geval geldt $u = v$ en zijn we klaar.

Voor $s > 0$ merken we op dat wegens de in 12.10 bewezen priemeigenschap van p_s het element p_s één van de elementen q_i deelt, zeg $q_t = p_sw$. Omdat p_s geen eenheid is, is wegens de irreducibiliteit van q_t het element w een eenheid. Omdat we in een domein werken hebben we door 'wegstrepen' van p_s de gelijkheid $up_1p_2 \ldots p_{s-1} =$

$vwq_1q_2\ldots q_{t-1}$. Wegens inductie geldt nu $s-1=t-1$, en zijn de irreducibele elementen aan beide kanten op eenheden en volgorde na aan elkaar gelijk. Voor de oorspronkelijke ontbindingen gold dit dus ook. Dit bewijst de *uniciteit* van de ontbinding. □

Voor $R=\mathbf{Z}$ is de door de eenheden veroorzaakte meerduidigheid van de ontbinding beperkt tot een simpele tekenkwestie. Voor $R=K[X]$ is er de eenhedengroep K^* van constante polynomen. Een polynoom met kopcoëfficiënt gelijk aan 1 heet *monisch*. Elk irreducibel polynoom in $K[X]$ is na vermenigvuldiging met een geschikte constante monisch. We kunnen daarom stelling 12.11 voor $K[X]$ als volgt formuleren.

12.12. Gevolg. *Zij K een lichaam. Dan is ieder polynoom $f\neq 0$ in $K[X]$ op volgorde na uniek te schrijven als een product $f=c\cdot p_1\cdot p_2\cdot\ldots\cdot p_t$ van een constante $c\in K^*$ en eindig veel monische irreducibele polynomen $p_i\in K[X]$.* □

In de volgende paragraaf gaan we nader in op de expliciete *berekening* van de factorisatie in 12.12. Net als voor gehele getallen is dit in de praktijk een niet-triviaal probleem.

▶ Priemidealen

Het bewijs van de hoofdingrediënten 12.8 en 12.10 in het bewijs van 12.11 laat zien dat deelbaarheidskwesties in commutatieve ringen gemakkelijk geformuleerd kunnen worden in termen van *ideaalinclusies*. Immers, x deelt y dan en slechts dan als het hoofdideaal (x) het hoofdideaal (y) bevat. Het adagium 'delen is bevatten' voor idealen geeft soms wel aanleiding tot een conflicterende notie van 'groot' en 'klein'. Zo correspondeert in $\mathbf{Z}$ een 'klein' getal $n>0$ met een verzamelingstheoretisch 'groot' ideaal $n\mathbf{Z}$ waarvan de *index* n in $\mathbf{Z}$ juist klein is.

In feite is het zo dat ook stelling 12.11 er in termen van idealen transparanter uitziet. De reden hiervoor is dat vermenigvuldiging met eenheden onzichtbaar wordt als we van elementen op idealen overgaan. In domeinen geldt ook een omkering van deze mededeling.

12.13. Lemma. *Voor elementen x,y in een domein R geldt*

$$(x)=(y) \qquad\Longleftrightarrow\qquad x=uy \quad \text{voor zekere} \quad u\in R^*.$$

Bewijs. Als er een eenheid u bestaat met $x=uy$, dan geldt ook $y=u^{-1}x$ en hebben we naast $(x)\subset(y)$ ook $(y)\subset(x)$, dus $(x)=(y)$.

Als $(x)=(y)$ geldt, bestaan er $u,v\in R$ met $x=uy$ en $y=vx$. Dit geeft $x=uvx$ en $(1-uv)x=0$. Voor $x=0$ geldt $y=0$ en kunnen we in het bovenstaande $u=1$ nemen. Voor $x\neq 0$ vinden we $uv=1$ omdat R een domein is, en dus $u\in R^*$. □

De voorwaarde in 12.13 dat R een domein is kan niet worden weggelaten (opgave 36). Elementen die hetzelfde ideaal voortbrengen in een domein R heten *geassocieerd* in R.

12.14. Definitie. *Een ideaal I in een commutatieve ring R heet een priemideaal als het niet gelijk is aan R en voor alle $x,y\in R$ geldt*

$$xy\in I \qquad\Longrightarrow\qquad x\in I \quad \text{of} \quad y\in I.$$

Een compactere versie van definitie 12.14 krijgen we door bovenstaande implicatie in de factorring R/I te schrijven als ($\overline{xy} = 0 \Rightarrow \overline{x} = 0$ of $\overline{y} = 0$). Dit leidt tot de equivalentie

(12.15) $\qquad I \subset R$ is een priemideaal $\iff R/I$ is een domein.

voor een ideaal I in een commutatieve ring R. In het bijzonder is het nulideaal (0) priem dan en slechts dan als R een domein is. Nemen we in 12.14 voor I het hoofdideaal (p) voortgebracht door een element $p \neq 0$ in een domein R, dan geldt wegens 12.9

(12.16) $\qquad (p)$ is een priemideaal $\iff p$ is een priemelement.

Combineren we 12.13 en 12.16, dan zien we dat stelling 12.11 in termen van idealen de volgende compacte formulering krijgt.

12.17. Stelling. *Ieder ideaal $I \neq 0$ in een hoofdideaaldomein R is te schrijven als een op volgorde na uniek product van priemidealen.* □

In een hoofdideaaldomein R noemt men elementen $a, b \in R$ *copriem* als $(a) + (b) = R$ geldt. Algemener kunnen we, net als we dat in 6.3.3 voor $R = \mathbf{Z}$ deden, een *grootste gemene deler* $d = \mathrm{ggd}(a, b)$ en een *kleinste gemene veelvoud* $k = \mathrm{kgv}(a, b)$ van elementen $a, b \in R$ definiëren door de gelijkheden

(12.18) $\qquad (a) + (b) = (d) \qquad$ en $\qquad (a) \cap (b) = (k).$

Dit legt d en k wegens 12.13 slechts vast tot op vermenigvuldiging met eenheden. Voor $R = \mathbf{Z}$ en $R = K[X]$ kan men unieke voortbrengers van idealen kiezen door te eisen dat deze respectievelijk *niet-negatief* en *monisch* (of 0) zijn.

▶ Gehele getallen van Gauss

We geven een klassieke getaltheoretische toepassing van de theorie in deze paragraaf. Hiertoe nemen we voor de ring R in 12.11 de ring $\mathbf{Z}[i]$ van *gehele getallen van Gauss*. Dit is de deelring van het lichaam $\mathbf{C}$ van complexe getallen gedefinieerd door $\mathbf{Z}[i] = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Z}\}$. Men ziet gemakkelijk in dat dit een deelring van $\mathbf{C}$ is. Hij kan gevisualiseerd worden als de verzameling van 'standaardroosterpunten' in het complexe vlak. We definiëren de *norm* $N : \mathbf{Z}[i] \to \mathbf{Z}$ door

$$N(\alpha) = \alpha\overline{\alpha}, \qquad \text{oftewel} \qquad N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

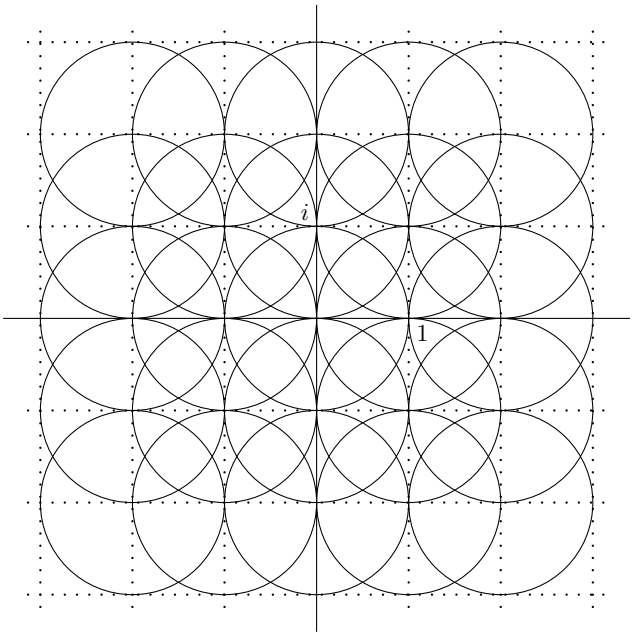
Deze norm is het *kwadraat* van de gewone absolute waarde op $\mathbf{C}$, en hij voldoet net als de gewone absolute waarde aan de multiplicatieve eigenschap $N(xy) = N(x)N(y)$. We kunnen hem voortzetten tot een multiplicatieve afbeelding $N : \mathbf{Q}(i) \to \mathbf{Q}$ op het quotiëntenlichaam $\mathbf{Q}(i) = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Q}\}$ van $\mathbf{Z}[i]$.

12.19. Stelling. *De ring* $\mathbf{Z}[i]$ *is een hoofdideaaldomein; de eenhedengroep* $\mathbf{Z}[i]^*$ *is cyclisch van orde* 4 *en wordt voortgebracht door* i*.*

Bewijs. We laten zien dat voor ieder tweetal getallen α en $\beta \neq 0$ in $\mathbf{Z}[i]$ er getallen $q, r \in \mathbf{Z}[i]$ zijn die voldoen aan $\alpha = q\beta + r$ en $N(r) < N(\beta)$. Schrijven we deze identiteit als

$$\frac{\alpha}{\beta} - q = \frac{r}{\beta} \qquad \text{met} \quad N(\frac{r}{\beta}) < 1,$$

dan zien we dat we de breuk $\frac{\alpha}{\beta} \in \mathbf{Q}(i)$ zó goed met een getal $q \in \mathbf{Z}[i]$ moeten benaderen dat het verschil $\frac{\alpha}{\beta} - q$, dat inderdaad van de vorm $\frac{r}{\beta}$ met $r \in \mathbf{Z}[i]$ is, een complex getal van absolute waarde kleiner dan 1 is. Tekenen we de elementen van $\mathbf{Z}[i]$ als roosterpunten in het vlak, dan betekent dit dat de open cirkelschijfjes met straal 1 om deze roosterpunten het hele complexe vlak moeten overdekken. Dit zien we eenvoudig in aan de hand van een plaatje.



Wie bewijzen met plaatjes niet overtuigend vindt kan opmerken dat voor ieder getal $z = x + yi \in \mathbf{C}$ er gehele getallen x_0 en y_0 bestaan met $|x - x_0| \leq 1/2$ en $|y - y_0| \leq 1/2$. Dan is $q = x_0 + y_0 i$ een element van $\mathbf{Z}[i]$, en er geldt

$$|z - q|^2 = |(x - x_0) + (y - y_0)i|^2 = |x - x_0|^2 + |y - y_0|^2 \leq (1/2)^2 + (1/2)^2 < 1.$$

Nu we eenmaal weten dat $\mathbf{Z}[i]$ net als $\mathbf{Z}$ of $K[X]$ een deling met rest toelaat, volgt net als in 12.6 of opgave 38 dat $\mathbf{Z}[i]$ een hoofdideaaldomein is.

Een element $\alpha = a + bi \in \mathbf{Z}[i]$ dat 1 deelt heeft een norm $N(\alpha) = a^2 + b^2$ die $N(1) = 1$ deelt. De vier geheeltallige oplossingen van $N(a + bi) = a^2 + b^2 = 1$ geven de elementen van de eenhedengroep $\mathbf{Z}[i]^* = \{\pm 1, \pm i\}$. In overeenstemming met 12.4 is deze groep cyclisch, met voortbrenger i. □

Opgave 4. Bepaal een quotiënt q en een rest r voor $\alpha = 10 + 3i$ en $\beta = 3 + 4i$. Zijn q en r uniek?

Opgave 5. Bewijs: $N(\alpha)$ is priem in $\mathbf{Z} \Rightarrow \alpha$ is priem in $\mathbf{Z}[i]$. Geldt de omkering?

Uit 12.11 en 12.19 volgt dat ieder element $\alpha \in \mathbf{Z}[i]$ ontbonden kan worden in een product van priemelementen. Omdat ieder getal $\alpha \in \mathbf{Z}[i]$ het gehele getal $N(\alpha) = \alpha\overline{\alpha}$ deelt, is ieder priemelement van $\mathbf{Z}[i]$ een deler van een positief geheel getal. Schrijven we dit gehele getal als product van priemgetallen, dan volgt dat ieder priemelement van $\mathbf{Z}[i]$ een priemgetal in $\mathbf{Z}$ deelt. Om ze allemaal te vinden is het dus voldoende de priemgetallen uit $\mathbf{Z}$ te ontbinden in $\mathbf{Z}[i]$.

12.20. Stelling. *Zij $p \in \mathbf{Z}$ een priemgetal. Dan is p als volgt te ontbinden in $\mathbf{Z}[i]$:*

1. *voor $p = 2$ geldt $2 = -i \cdot (1 + i)^2$;*
2. *voor $p \equiv 1 \bmod 4$ geldt $p = \pi\overline{\pi}$, met π en $\overline{\pi}$ niet-geassocieerd en priem in $\mathbf{Z}[i]$;*
3. *voor $p \equiv 3 \bmod 4$ is p een priemelement in $\mathbf{Z}[i]$.*

Bewijs. De identiteit voor $p = 2$, het enige priemgetal in $\mathbf{Z}$ dat kennelijk door het *kwadraat* van een priemelement in $\mathbf{Z}[i]$ deelbaar is, is direct te verifiëren.

Als p een priemgetal is dat niet irreducibel is in $\mathbf{Z}[i]$, dan kan het geschreven worden als $p = \alpha\beta$ met $\alpha, \beta \notin \mathbf{Z}[i]^*$. Uit $N(\alpha)N(\beta) = N(p) = p^2$ zien we dan dat $N(\alpha) = N(\beta) = p$ moet gelden. De vraag is dus voor welke p er een element $\pi \in \mathbf{Z}[i]$ bestaat van norm $N(\pi) = \pi\overline{\pi} = p$.

Voor priemen $p \equiv 3 \bmod 4$ heeft de vergelijking $N(a + bi) = a^2 + b^2 = p$ geen geheeltallige oplossingen. Immers, kwadraten in $\mathbf{Z}$ liggen in de restklassen $0 \bmod 4$ en $1 \bmod 4$, dus een som van twee kwadraten is niet congruent met $3 \bmod 4$. We concluderen dat een priemgetal $p \equiv 3 \bmod 4$ irreducibel is in $\mathbf{Z}[i]$, en dus wegens 12.10 een priemelement is in $\mathbf{Z}[i]$.

Voor priemen $p \equiv 1 \bmod 4$ is de groep $\mathbf{F}_p^* = (\mathbf{Z}/p\mathbf{Z})^*$ wegens 12.5 cyclisch, en zijn orde $p-1$ is deelbaar door 4. Zoals we al in het bewijs van 12.4 memoreerden, betekent dit dat er een element $\overline{x} \in \mathbf{F}_p^*$ bestaat waarvan de orde gelijk is aan 4. Het kwadraat $\overline{x}^2$ is dan het element van orde 2 in $\mathbf{F}_p^*$, en dat is $-\overline{1}$. Voor een element $x \in \mathbf{Z}$ in de restklasse $\overline{x} \in \mathbf{F}_p^*$ geldt nu $x^2 + 1 \equiv 0 \bmod p$, dus

$$p \mid x^2 + 1 = (x + i)(x - i) \in \mathbf{Z}[i].$$

Het is echter duidelijk dat p geen deler is van $x + i$ of $x - i$ in $\mathbf{Z}[i]$. We zien dat p *geen* priemelement is in $\mathbf{Z}[i]$, en wegens 12.10 is p dan ook niet irreducibel in $\mathbf{Z}[i]$. Zoals we zagen bestaat er dan een element $\pi = a + bi \in \mathbf{Z}[i]$ van norm $N(\pi) = \pi\overline{\pi} = a^2 + b^2 = p$. Omdat de norm van π en $\overline{\pi}$ gelijk is aan p, geldt voor een ontbinding $\alpha\beta$ van π of $\overline{\pi}$ de gelijkheid $N(\alpha\beta) = N(\alpha)N(\beta) = p$, dus $N(\alpha) = 1$ of $N(\beta) = 1$. We concluderen dat π en $\overline{\pi}$ beide irreducibel zijn in $\mathbf{Z}[i]$, en dus priem.

Als $\pi = a + bi$ en $\overline{\pi} = a - bi$ geassocieerd zijn, dan geldt wegens 12.13 voor een eenheid $u \in \mathbf{Z}[i]^*$ de gelijkheid $a + bi = u(a - bi)$. De vier mogelijke keuzen $u = \pm 1$ en $u = \pm i$ leiden tot de evident onjuiste conclusies $b = 0$ en $a = 0$ en $a = \pm b$. □

Opgave 6. Laat zien: voor $p \equiv 1 \bmod 4$ en $x \in \mathbf{Z}$ als boven is $\gcd(p, x - i)$ een element van norm p.

Fermat schreef al in 1640 in een brief aan Mersenne dat hij kon bewijzen dat ieder priemgetal $p \equiv 1 \bmod 4$ als som van twee kwadraten te schrijven is – een mededeling equivalent met 12.20.2. Het eerste complete overgeleverde bewijs werd in 1749 door Euler gegeven.[2]

Opgave 7. Laat zien dat de schrijfwijze $p = a^2+b^2$ voor een priemgetal $p \equiv 1 \bmod 4$ tot op tekenkeuzes voor a en b en verwisseling van a en b na uniek bepaald is.

Algemener is het zo dat een positief geheel getal n een som van twee kwadraten is dan en slechts dan als de exponent $\mathrm{ord}_p(n)$ van p in de factorisatie van n *even* is voor ieder priemgetal $p \equiv 3 \bmod 4$ (opgave 54).

Stelling 12.20 geeft ons voldoende informatie om een willekeurig element $x \in \mathbf{Z}[i]$ te ontbinden. We illustreren dit door $x = 174 - 582\,i$ expliciet te factoriseren.

Allereerst berekenen we $\mathrm{ggd}(174, 582) = 6$, bijvoorbeeld als in 6.14 door toepassing van de Euclidische algoritme, en schrijven $174 - 582i = 6(29 - 97i)$. Het ontbinden van $6 = 2 \cdot 3$ geschiedt door toepassing van 12.20, voor de factor $\alpha = 29 - 97i$, die geen rationale priemdelers meer heeft in $\mathbf{Z}[i]$, kijken we eerst naar de norm

$$N(\alpha) = N(29 - 97i) = 29^2 + 97^2 = 841 + 9409 = 10250 = 2 \cdot 5^3 \cdot 41.$$

We lezen hieruit af dat α het product is van priemelementen van norm 2, 5 en 41. Op vermenigvuldiging met machten van i na zijn deze priemelementen gelijk aan $1+i$, $2 \pm i$ en $5 \pm 4i$. Om bijvoorbeeld te besluiten welk van beide priemelementen $5 \pm 4i$ van norm 41 als deler optreedt, kunnen we uitrekenen welk van beide quotiënten $\frac{29-97i}{5\pm 4i} \in \mathbf{Q}(i)$ in $\mathbf{Z}[i]$ ligt.

Opgave 8. Voer deze berekening uit.

Instructiever is het om deelbaarheid van α door de priemelementen $5 \pm 4i$ op te vatten als het al dan niet bevat zijn van α in de hoofdidealen $(5 \pm 4i)$. Idealen zijn kernen van homomorfismen, en in het onderhavige geval zijn dit de beide homomorfismen $\varphi_{1,2} : \mathbf{Z}[i] \to \mathbf{F}_{41}$ die $\mathbf{Z}[i]$ toelaat. Corresponderende met de beide wortels $\pm 9 \bmod 41$ van $-1 \bmod 41$ hebben we $\varphi_1 : a+bi \mapsto a+9b \bmod 41$ en $\varphi_2 : a+bi \mapsto a-9b \bmod 41$ met kernen $\ker \varphi_1 = (5+4i)$ en $\ker \varphi_2 = (5-4i)$. Er geldt $\varphi_1(\alpha) = (29 + 9 \cdot -97 \bmod 41) = 17 \bmod 41$, dus $5 + 4i$ is *geen* deler van α. Kennelijk is $5 - 4i$ de factor die we zoeken. Inderdaad geldt $\varphi_2(\alpha) = (29 - 9 \cdot -97 \bmod 41) = 0 \bmod 41$.

Omdat α niet deelbaar is door 5, treedt van de priemelementen $2 \pm i$ van norm 5 er slechts één op als deler van α, en wel met multipliciteit 3. Voor het homomorfisme $\psi_1 : a+bi \mapsto (a+2b \bmod 5)$ met kern $(2-i)$ geldt $\psi_1(\alpha) = (29-2\cdot 97 \bmod 5) = 0 \bmod 5$, dus $2 - i$ is de gezochte factor. Omdat er op eenheden na slechts één priemelement van norm 2 is krijgen we

$$\alpha = 29 - 97\,i = i^k \cdot (1 + i) \cdot (2 - i)^3 \cdot (5 - 4i).$$

Voor de bepaling van de noodzakelijke macht i^k van i is het niet nodig om het rechterlid door vermenigvuldiging uit te rekenen. Passen we het homomorfisme $\psi_2 : a + bi \mapsto$

$a-2b \bmod 5$ toe behorende bij het priemelement $2+i$ dat α *niet* deelt, dan vinden we dat $\psi_2(\alpha) = (29+2\cdot 97 \bmod 5) = 3 \bmod 5$ gelijk moet zijn aan $(-2)^k \cdot -1 \cdot (-1)^3 \cdot 3 \bmod 5$. Er volgt $(-2)^k \equiv 1 \bmod 5$, dus $k \equiv 0 \bmod 4$ en de 'eenhedenbijdrage' i^k in bovenstaande factorisatie is 1.

Opgave 9. Controleer dit resultaat door k nogmaals te bepalen via $\varphi_1 : \mathbf{Z}[i] \to \mathbf{F}_{41}$ of een zelf te kiezen homomorfisme $\mathbf{Z}[i] \to \mathbf{F}_{13}$.

We geven een toepassing van 12.19 op het oplossen van een *Diophantische vergelijking*. Hiermee bedoelen we een algebraïsche vergelijking met rationale coëfficiënten waarvan we niet de reële of complexe oplossingen zoeken, maar alleen de rationale of geheeltallige oplossingen. Meer meetkundig geformuleerd komt onderstaand probleem neer op het bepalen van de punten met geheeltallige coördinaten op een algebraïsche kromme.

12.21. Stelling. *De enige geheeltallige oplossing van* $X^2+1 = Y^3$ *is* $(X,Y) = (0,1)$.

Bewijs. Laat (x,y) een oplossing van de vergelijking zijn, en schrijf

$$x^2+1 = (x+i)(x-i) = y^3.$$

We gaan bewijzen dat $x+i$ en $x-i$ copriem zijn in $\mathbf{Z}[i]$. Hiertoe merken we eerst op dat x *even* is. Immers voor oneven x moet y even zijn en vinden we modulo 4 een tegenspraak: $x^2+1 \equiv 2 \bmod 4$ en $y^3 \equiv 0 \bmod 4$. Een voortbrenger d van het ideaal $(x+i, x-i) \subset \mathbf{Z}[i]$ deelt nu zowel $x+i$ als $x-i$, dus ook $(x+i)-(x-i) = 2i$. Omdat $2i$ het even getal x deelt, deelt d nu zowel x als $x+i$, dus ook de eenheid i. We vinden dat d zelf een eenheid is in $\mathbf{Z}[i]$, dus $x+i$ en $x-i$ zijn copriem in $\mathbf{Z}[i]$.

We bewijzen vervolgens dat een product van twee coprieme elementen in $\mathbf{Z}[i]$ alleen een derde macht kan zijn als *elk* van deze beide elementen een derde macht is in $\mathbf{Z}[i]$. Zij π namelijk een irreducibele factor van $x+i$. Dan is π geen deler van $x-i$, en het aantal factoren π in $x+i$ is gelijk aan het aantal factoren π in $(x+i)(x-i) = y^3$, *dus* een drievoud. Door nu naar de ontbinding van $x+i$ te kijken zien we dat $x+i$ het product is van een eenheid $u \in \mathbf{Z}[i]^*$ en een derde macht. Wegens $u^4 = 1$ is $u = u^{-3}$ zelf ook een derde macht. We concluderen dat $x+i$ te schrijven is als een derde macht

$$x+i = (a+bi)^3 = a(a^2-3b^2) + (3a^2-b^2)bi \qquad \text{met } a,b \in \mathbf{Z}.$$

Vergelijken we de imaginaire delen, dan volgt uit $(3a^2-b^2)b = 1$ gemakkelijk $b = \pm 1$ en $3a^2 - 1 = \pm 1$. De enige oplossing hiervan is $a = 0$ en $b = -1$, en we vinden hieruit de unieke oplossing $(x,y) = (0,1)$. □

▶ Priemideaalfactorisatie

Bovenstaand voorbeeld laat zien dat het bij het vinden van de gehele oplossingen van een vergelijking met coëfficiënten in $\mathbf{Z}$ nuttig kan zijn om te werken in een *grotere* ring dan $\mathbf{Z}$ zelf, zoals $\mathbf{Z}[i]$. Nu blijkt dat de ringen die men hierbij tegenkomt *niet* altijd hoofdideaaldomeinen zijn. Zo is de deelring $\mathbf{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbf{Z}\}$ van $\mathbf{C}$ een domein dat enigszins lijkt op $\mathbf{Z}[i]$, maar *geen* hoofdideaaldomein is. Hierin heeft

$$21 = 3 \cdot 7 = (4+\sqrt{-5})(4-\sqrt{-5}) = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

drie totaal verschillende ontbindingen in irreducibele elementen (opgave 61). Kennelijk is niet ieder irreducibel element in $\mathbf{Z}[\sqrt{-5}]$ een priemelement. Door werk van de Duitser Ernst Eduard Kummer (1810–1893) en andere grondleggers van de *algebraïsche getaltheorie*[3] werd duidelijk dat men in dit soort getallenringen *niet* altijd unieke factorisatie in priemelementen heeft als in 12.11, maar *wel* unieke factorisatie in *priemidealen* als in 12.17. In het gegeven voorbeeld bestaan er priemidealen

$$P_3 = (3, 1+\sqrt{-5}), \quad Q_3 = (3, 1-\sqrt{-5}), \quad P_7 = (7, 4+\sqrt{-5}), \quad Q_7 = (7, 4-\sqrt{-5})$$

die *geen* hoofdidealen zijn, en waarmee het ideaal (21) ontbonden kan worden als

$$(21) = P_3 \cdot Q_3 \cdot P_7 \cdot Q_7.$$

Ieder product van twee 'ideale priemfactoren' van (21) is een hoofdideaal, en dit 'verklaart' de bovengenoemde elementfactorisaties — zie de opgaven 61–63.

Opgave 10. Laat I_1 en I_2 idealen in een commutatieve ring R zijn. Bewijs de *priemideaaleigenschap*

$$P \supset I_1 I_2 \quad \Longrightarrow \quad P \supset I_1 \ \text{ of } \ P \supset I_2$$

voor priemidealen P in de zin van 12.14.

Het door Kummer ingevoerde woord *ideaal*, dat nu een basisbegrip in de algebra is, werd rond 1850 nog als tamelijk mysterieus ervaren. Kummer zelf benadrukte de analogie met de chemie, die op enigszins vergelijkbare wijze de moleculen van een stof beschrijft in termen van niet los voorkomende constituenten, 'atomen' genaamd.[4]

Opgaven

11. Laat zien dat ieder ideaal in een product $R = R_1 \times R_2 \times \ldots \times R_n$ van hoofdideaaldomeinen R_i een hoofdideaal is. Is R weer een hoofdideaaldomein?

12. Laat zien dat de polynoomring $K[X, Y]$ over een lichaam K geen hoofdideaaldomein is.

13. Is de ring $K[X, X^{-1}]$ van Laurentpolynomen over een lichaam K een hoofdideaaldomein?

14. Is de ring $K[[X]]$ van machtreeksen over een lichaam K een hoofdideaaldomein?

15. Zij R een ring. Laat zien dat het regeltje $\deg(fg) = \deg(f) + \deg(g)$ voor alle $f, g \in R[X]$ geldt dan en slechts dan als R geen niet-triviale nuldelers heeft.

16. Bewijs dat voor niet-negatieve gehele getallen a en b de volgende uitspraken equivalent zijn:
(i) er bestaan f, $g \in (\mathbf{Z}/15\mathbf{Z})[X]$ met

$$\deg(f) = a, \qquad \deg(g) = b, \qquad f \cdot g = X^{10};$$

(ii) er geldt $0 \leq a \leq 10$, $0 \leq b \leq 10$, $a + b \geq 10$.
[Hint: gebruik het isomorfisme $(\mathbf{Z}/15\mathbf{Z})[X] \cong (\mathbf{Z}/3\mathbf{Z})[X] \times (\mathbf{Z}/5\mathbf{Z})[X]$.]

17. Voor welke paren niet-negatieve gehele getallen (a, b) bestaan er f, $g \in (\mathbf{Z}/8\mathbf{Z})[X]$ met

$$\deg(f) = a, \qquad \deg(g) = b, \qquad f \cdot g = 1?$$

18. Zij $\mathbf{H}$ de quaternionenalgebra van Hamilton. Bewijs dat het polynoom $X^2 + 1 \in \mathbf{H}[X]$ *oneindig* veel verschillende nulpunten heeft in de delingsring $\mathbf{H}$. Waarom is dit niet in tegenspraak met 12.3? [Hint: kwadrateer $xi + yj + zk$.]

19. Zij R een commutatieve ring en $f \in R[X]$ een polynoom met $f \neq 0$. Stel dat $a_1, \ldots, a_n \in R$ nulpunten van f zijn met de eigenschap $a_i - a_j \in R^*$ voor alle i, j met $1 \leq i < j \leq n$. Bewijs: $n \leq \deg f$.

20. Laat H een eindige ondergroep van de eenhedengroep van een domein R zijn, en beschouw het polynoom $f = \prod_{a \in H}(X - a) \in R[X]$. Bewijs: $f = X^{\#H} - 1$.

21. Zij $\phi : R[X] \to \mathrm{Map}(R, R)$ de afbeelding die aan een polynoom $f \in R[X]$ de bijbehorende afbeelding $r \mapsto f(r)$ in de functiering $\mathrm{Map}(R, R)$ toevoegt. Bewijs:
    a. ϕ is een ringhomomorfisme dan en slechts dan als R commutatief is;
    b. ϕ is injectief maar niet surjectief als R een oneindig domein is;
    c. ϕ is surjectief maar niet injectief als R een eindig domein is.

22. De *afgeleide* van een polynoom $f = \sum_k a_k X^k$ met coëfficiënten in een commutatieve ring R is het polynoom $f' = \sum_k k a_k X^{k-1}$. Is f van de vorm $f = (X-a)^2 q$ met $q \in R[X]$ en $a \in R$, dan heet a een *dubbel nulpunt* van f.
    a. Bewijs de differentiatieregels $(f+g)' = f' + g'$ en $(fg)' = f'g + fg'$ voor $f, g \in R[X]$.
    b. Zij $a \in R$ een nulpunt van f. Bewijs: a is een dubbel nulpunt van $f \iff f'(a) = 0$.
    c. Ga na welke nulpunten van $f = X^2 - \overline{1}$ en $f = X^2$ in $\mathbf{Z}/8\mathbf{Z}$ dubbel zijn.

23. Laat zien dat het polynoom $X^7 + 7X + 1 \in \mathbf{C}[X]$ geen dubbele nulpunten heeft in $\mathbf{C}$.

24. Laat R een commutatieve ring zijn. We zeggen dat R *samenhangend* is als het aantal nulpunten van $X^2 - X$ in R gelijk is aan 2.
    a. Bewijs: R is samenhangend dan en slechts dan als R niet de nulring is en er geen ringen $R_1 \neq \{0\}$ en $R_2 \neq \{0\}$ bestaan waarvoor er een ringisomorfisme $R \cong R_1 \times R_2$ is.
    b. Stel dat R samenhangend is en dat I, J idealen zijn met $IJ = \{0\}$ en $I + J = R$. Bewijs: $\{I, J\} = \{\{0\}, R\}$.

25. Laat R een commutatieve ring zijn, en $f \in R[X]$. We noemen f *separabel* als geldt $R[X]f + R[X]f' = R[X]$ geldt, met f' de afgeleide van f.
    a. Stel dat $a \in R$ een nulpunt van f is, en schrijf $f = (X - a) \cdot g$ met $g \in R[X]$. Bewijs: $g(a) = f'(a)$, en als f separabel is dan geldt $g(a) \in R^*$.
    b. Stel dat f separabel is, laten a, $b \in R$ nulpunten van f zijn, en schrijf $f = (X - a) \cdot g$ met $g \in R[X]$. Bewijs: de idealen $I = R \cdot (b - a)$ en $J = R \cdot g(b)$ voldoen aan $IJ = \{0\}$ en $I + J = R$.
    c. Stel dat R samenhangend is en f separabel. Bewijs: $f \neq 0$, en het aantal nulpunten van f in R is ten hoogste $\deg f$.

26. Laat $x_0, x_1, x_2, \ldots, x_n$ een $(n+1)$-tal *verschillende* elementen uit een lichaam K zijn, en $y_0, y_1, y_2, \ldots, y_n$ een $(n+1)$-tal willekeurige elementen in K. Bewijs dat er precies één polynoom $f \in K[X]$ van graad $\deg(f) \leq n$ bestaat met $f(x_i) = y_i$ voor $i = 0, 1, 2, \ldots, n$, en dat het gegeven wordt door de *interpolatieformule van Lagrange*:

$$f = \sum_{i=0}^{n} \left(\prod_{j=0, j\neq i}^{n} \frac{X - x_j}{x_i - x_j} \right) y_i.$$

27. Laat zien dat er geen polynoom $f \in (\mathbf{Z}/100\mathbf{Z})[X]$ bestaat met $f(\overline{1}) = \overline{1}$ en $f(\overline{11}) = \overline{17}$.

28. Zij R een commutatieve ring en $U \subset R^*$ een eindige deelverzameling. Bewijs dat er $f \in R[X]$ bestaat met $f(u) = u^{-1}$ voor alle $u \in U$.

29. Bepaal primitieve wortels modulo de priemgetallen 11, 31, 41 en 71.

30. Bepaal de kleinste 6 priemgetallen $p > 2$ waarvoor 5 mod p een primitieve wortel is. Wat valt je op aan de eindcijfers van deze priemgetallen[5]? *Zijn er oneindig veel priemgetallen p met de genoemde eigenschap[6]?

31. Laat F een eindig lichaam zijn. Een *primitieve wortel* van F is een element $a \in F^*$ met $F^* = \langle a \rangle$. Stel dat het product van alle primitieve wortels van F *niet* gelijk is aan 1. Bewijs dat F isomorf is met $\mathbf{Z}/3\mathbf{Z}$.

*32. Voor een priemgetal p geven we met $s(p) \in \mathbf{F}_p$ de som van alle primitieve wortels van $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ aan. Vind, door (eventueel met een rekenmachine) een aantal waarden van $s(p)$ te berekenen, een vermoedelijke formule voor $s(p)$, en bewijs vervolgens de correctheid daarvan.

33. Een commutatieve ring R heet *noethers* als er geen oneindige stijgende keten

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq I_4 \subsetneq \ldots$$

van idealen in R bestaat. Bewijs dat R noethers is dan en slechts dan als ieder ideaal in R door een eindige verzameling $S \subset R$ wordt voortgebracht.
[Amalie Emmy Noether (1882–1935) is een van de grondleggers van de moderne algebra.]

34. Bewijs dat ieder element $x \neq 0$ in een noethers domein R te schrijven is als een product van een eenheid en een eindig aantal irreducibele elementen.

35. Definieer op de additieve groep $R = \mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ een productbewerking door

$$(a_1, \overline{b}_1) \cdot (a_2, \overline{b}_2) = (a_1 a_2, \overline{a_1 b_2 + a_2 b_1}).$$

Laat zien dat R hiermee een commutatieve ring isomorf met $\mathbf{Z}[X]/(5X, X^2)$ wordt. Bewijs dat R^* een cyclische groep van orde 10 is. Is R een domein?

36. Laat zien dat de elementen $x = (0, \overline{1})$ en $y = (0, \overline{2})$ hetzelfde ideaal voortbrengen in de ring R uit de vorige opgave, maar dat er geen eenheid $u \in R^*$ is met $y = ux$.

37. Zij K een lichaam. Bewijs dat iedere rationale functie $f \in K(X)^*$ uniek geschreven kan worden als $f = c \cdot \prod_p p^{n_p}$. Hier is $c \in K^*$ een constante, loopt p over alle monische irreducibele polynomen in $K[X]$ en zijn de exponenten $n_p \in \mathbf{Z}$ gehele getallen die bijna allemaal gelijk zijn aan 0.

38. Een *Euclidische ring* is een domein R voorzien van een functie $g : R\backslash\{0\} \to \mathbf{Z}_{\geq 0}$ waarvoor de volgende eigenschap geldt:
(∗) voor $a, b \in R$ met $b \neq 0$ bestaan er $q, r \in R$ met $a = qb + r$ en r een element dat voldoet aan $r = 0$ of $g(r) < g(b)$.
Bewijs dat iedere Euclidische ring een hoofdideaaldomein is.

39. Laat zien dat $\mathbf{Z}$ en de polynoomring $K[X]$ over een lichaam K Euclidische ringen zijn, en dat in iedere Euclidische ring een analogon van de in 6.13 gegeven *Euclidische algoritme* gebruikt kan worden om ggd's te berekenen.

40. Bewijs dat de ring $\mathbf{Z}((X))$ een Euclidische ring is.

41. Zij K een lichaam. Bewijs dat de ringen $K((X))[Y]$ en $K[Y]((X))$ allebei Euclidisch zijn, dat de eerste ring isomorf is met een deelring van de tweede, en dat beide ringen niet isomorf zijn.

42. Ontbind $63 + 75i$ en $217 - 35i$ in factoren in $\mathbf{Z}[i]$.

43. Bereken $\gcd(135 - 14i, 155 + 34i)$ zowel via de Euclidische algoritme als via expliciete priemfactorisaties in $\mathbf{Z}[i]$.

44. Laat zien dat $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$ het quotiëntenlichaam is van $\mathbf{Z}[i]$, en dat er isomorfismen $\mathbf{Q}(i) \cong \mathbf{Q}[X]/(X^2 + 1)$ en $\mathbf{Z}[i] \cong \mathbf{Z}[X]/(X^2 + 1)$ zijn.

45. Zij $q \in \mathbf{Q}^*$. Bewijs: er bestaat $\alpha \in \mathbf{Q}(i)$ met $\alpha^2 = q$ dan en slechts dan als er $r \in \mathbf{Q}$ bestaat met $q = r^2$ of $q = -r^2$.

46. Zij $q \in \mathbf{Q}^*$. Bewijs: er bestaat $\alpha \in \mathbf{Q}(i)$ met $\alpha^4 = q$ dan en slechts dan als er $r \in \mathbf{Q}$ bestaat met $q = r^4$ of $q = -4 \cdot r^4$.

47. Bestaan er drie verschillende punten P, Q, $R \in \mathbf{Q} \times \mathbf{Q}$ waarvoor de lijn PQ een hoek van 60° met de lijn RQ maakt? Geef dergelijke punten aan, of bewijs dat ze niet bestaan.

48. Laat zien dat $\mathbf{Z}[i]/p\mathbf{Z}[i]$ voor $p \equiv 3 \bmod 4$ een lichaam van p^2 elementen is, en voor $p \equiv 1 \bmod 4$ een product $\mathbf{F}_p \times \mathbf{F}_p$ van twee lichamen. Welk van de ringen uit opgave 11.63 krijgen we voor $p = 2$?

49. In deze opgave wordt bewezen dat voor elk element $\alpha = a + bi \in \mathbf{Z}[i]$ ongelijk aan 0 de norm $N(\alpha) = a^2 + b^2$ van α gelijk is aan het aantal elementen van de ring $\mathbf{Z}[i]/\mathbf{Z}[i]\alpha$.
    a. Bewijs: voor elke $n \in \mathbf{Z} \setminus \{0\}$ is de ring $\mathbf{Z}[i]/n\mathbf{Z}[i]$ eindig van orde n^2. Leid hieruit af dat $\mathbf{Z}[i]/\mathbf{Z}[i]\alpha$ eindig is voor elke $\alpha \in \mathbf{Z}[i]$, $\alpha \neq 0$.
    b. Definieer $\mathcal{N}\colon \mathbf{Z}[i]\backslash\{0\} \to \mathbf{Z}_{>0}$ door $\mathcal{N}(\alpha) = \#(\mathbf{Z}[i]/\mathbf{Z}[i]\alpha)$. Bewijs: $\mathcal{N}(\alpha) = \mathcal{N}(\bar{\alpha})$ en $\mathcal{N}(\alpha \cdot \beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$ voor alle α, $\beta \in \mathbf{Z}[i]\backslash\{0\}$.
    c. Bewijs: $\mathcal{N}(\alpha) = N(\alpha)$ voor alle $\alpha \in \mathbf{Z}[i]\backslash\{0\}$.

50. Bepaal alle geheeltallige oplossingen van de vergelijking $X^2 + 4 = Y^3$.

51. Bepaal alle geheeltallige oplossingen van de vergelijking $X^2 + 1 = Y^5$.

52. Een *Pythagoreïsch tripel* is een tripel (a, b, c) van gehele getallen dat voldoet aan de identiteit
$$a^2 + b^2 = c^2.$$
Het heet *primitief* als a, b en c geen gemeenschappelijke factoren hebben. Bewijs: voor ieder primitief Pythagoreïsch tripel (a, b, c) bestaan er coprieme gehele getallen m en n zo dat, na eventuele verwisseling van a en b, de volgende identiteiten gelden:
$$a = m^2 - n^2 \qquad b = 2mn \qquad c = \pm(m^2 + n^2).$$
[Hint: schrijf $(a + bi)(a - bi) = c^2$, en leid $a + bi = (m + ni)^2$ af als in 12.21.]

53. Leid de beschrijving van Pythagoreïsche tripels uit de vorige opgave 'binnen $\mathbf{Z}$' af door de vergelijking voor even b te herschrijven als $(\frac{b}{2})^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}$.

54. Bewijs dat voor een geheel getal $n > 0$ met priemfactorisatie $\prod_p p^{e(p)}$ het aantal paren $(a, b) \in \mathbf{Z}^2$ met $n = a^2 + b^2$ gelijk is aan
$$r(n) = \begin{cases} 0 & \text{als er een priem } p \equiv 3 \bmod 4 \text{ is met } e(p) \textit{ oneven}; \\ 4 \prod_{p \equiv 1 \bmod 4} (e(p) + 1) & \text{anders.} \end{cases}$$
*Hoeveel paren zijn er als we bovendien de ongelijkheden $a \geq b \geq 0$ eisen?

55. Definieer $r(n)$ als in de vorige opgave. Bewijs: $\lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} r(n) = \pi$.

56. Laten we een paar (a, b) van *positieve* getallen van ieder niet meer dan k decimale cijfers *normvast* van orde k noemen als het voldoet aan de merkwaardige identiteit
$$N(a + bi) = a^2 + b^2 = a \cdot 10^k + b.$$
Voorbeelden van zulke paren worden gegeven door identiteiten als
$$12^2 + 33^2 = 1233, \qquad 990^2 + 100^2 = 990100, \qquad 123288^2 + 328768^2 = 123288328768.$$
Laat zien dat er normvaste paren van orde k bestaan dan en slechts dan als $10^{2k} + 1$ *geen* priemgetal is, en dat het aantal van zulke paren gelijk is aan $[r(10^{2k} + 1) - 8]/4$.
[Hint: kijk naar $(2a - 10^k, 2b - 1)$.]

57. Bepaal alle normvaste paren van orde $k \leq 10$.
[Hint: Sage kan zowel getallen ontbinden als modulo n rekenen.]

58. Zij $\rho = \frac{-1+\sqrt{-3}}{2} \in \mathbf{C}$ een nulpunt van het polynoom $X^2 + X + 1$. De *gehele getallen van Eisenstein* zijn de complexe getallen van de vorm $a + b\rho$ met $a, b \in \mathbf{Z}$. Bewijs:
    a. $\mathbf{Z}[\rho] = \{a + b\rho : a, b \in \mathbf{Z}\}$ is een deelring van $\mathbf{C}$, en de normafbeelding $N : \mathbf{Z}[\rho] \to \mathbf{Z}$ gegeven door $a + b\rho \mapsto |a + b\rho|^2 = a^2 - ab + b^2$ is multiplicatief;
    b. $\mathbf{Z}[\rho]^* = \langle -\rho \rangle$ is cyclisch van orde 6;
    c. $\mathbf{Z}[\rho]$ is een hoofdideaaldomein.
[Ferdinand Gotthold Max Eisenstein[7] (1823–1852) was een Duits getaltheoreticus.]

59. Bewijs dat de priemgetallen $p \equiv 2 \bmod 3$ irreducibel zijn in $\mathbf{Z}[\rho]$, dat de priemgetallen $p \equiv 1 \bmod 3$ ontbinden als $p = \pi\overline{\pi}$, en dat $3 = -(2\rho + 1)^2$ geldt. Leid hieruit af dat ieder priemgetal $p \not\equiv 2 \bmod 3$ te schrijven is als $p = x^2 + 3y^2$ met $x, y \in \mathbf{Z}$, en dat deze representatie op het teken van x en y na uniek is.

60. Definieer $\mathbf{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbf{Z}\} \subset \mathbf{C}$.
    a. Laat zien dat $\mathbf{Z}[\sqrt{-3}]$ een deelring van index 2 is in $\mathbf{Z}[\rho]$.
    b. Bewijs: ieder ideaal $I \subset \mathbf{Z}[\sqrt{-3}]$ is van de vorm $x\mathbf{Z}[\sqrt{-3}]$ of $x\mathbf{Z}[\rho]$, met $x \in \mathbf{Z}[\sqrt{-3}]$.
    c. Is $\mathbf{Z}[\sqrt{-3}]$ een hoofdideaaldomein?

61. Laat zien dat $\mathbf{Z}[\sqrt{-5}]$ eenhedengroep $\{\pm 1\}$ heeft, en dat de elementen 3, 7, $4 + \sqrt{-5}$ en $1 + 2\sqrt{-5}$ irreducibel zijn in $\mathbf{Z}[\sqrt{-5}]$.
[Hint: gebruik de norm $N : a + b\sqrt{-5} \mapsto a^2 + 5b^2$.]

62. Laat zien dat de afbeelding $\mathbf{Z}[\sqrt{-5}] \to \mathbf{Z}/7\mathbf{Z}$ gegeven door $a + b\sqrt{-5} \mapsto (a + 3b \bmod 7)$ een surjectief homomorfisme is met kern $P_7 = (7, 4 + \sqrt{-5})$, en dat P_7 geen hoofdideaal is in $\mathbf{Z}[\sqrt{-5}]$.

63. Laat zien dat (21) priemideaalfactorisatie $P_3 \cdot Q_3 \cdot P_7 \cdot Q_7$ heeft in $\mathbf{Z}[\sqrt{-5}]$, en dat ieder tweetal priemideaalfactoren van (21) als product een hoofdideaal geeft.

64. Zij $p \neq 5$ een priemgetal. Bewijs:

$$p = x^2 + 5y^2 \quad \text{voor } x, y \in \mathbf{Z} \quad \Longrightarrow \quad p \equiv 1, 9 \bmod 20.$$

    *Geldt de omkering?

*65. Zij p een oneven priemgetal. Bewijs:

$$p = x^2 + 2y^2 \quad \text{voor } x, y \in \mathbf{Z} \quad \Longleftrightarrow \; p \equiv 1, 3 \bmod 8.$$

[Hint voor $\Longleftarrow$: bewijs eerst dat $\mathbf{Z}[\sqrt{-2}]$ een hoofdideaaldomein is; laat vervolgens zien dat $\overline{-2}$ een kwadraat is in $\mathbf{F}_p^*$ voor $p \equiv 1, 3 \bmod 8$. Nuttig: voor $p \equiv 1 \bmod 8$ en $x \in \mathbf{F}_p^*$ van orde 8 geldt $(x + x^3)^2 = \overline{-2}$. Voor $p \equiv 3 \bmod 8$ bestaat zo'n x van orde 8 pas in $\mathbf{Z}[i]/p\mathbf{Z}[i]$, maar er geldt $x + x^3 \in \mathbf{F}_p \subset \mathbf{Z}[i]/p\mathbf{Z}[i]$.]

66. Bepaal de ontbinding van $5 + i$ en $239 + i$ in $\mathbf{Z}[i]$, en leid de klassieke formule

$$\pi = 16 \arctan \frac{1}{5} - 4 \arctan \frac{1}{239} \qquad \text{met} \quad \arctan x = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1}$$

af waarmee John Machin (1680–1752) in 1706 honderd decimalen van π berekende.[8]

13 Ontbinding van polynomen

Polynoomringen in één of meer variabelen met coëfficiënten in domeinen als $\mathbf{Z}$, $\mathbf{R}$ of $\mathbf{F}_p$ komt men in de wiskunde veelvuldig tegen. In het eenvoudigste geval van de polynoomring $K[X]$ in één variabele X over een lichaam K krijgen we wegens 12.6 een hoofdideaaldomein en is de theorie uit de vorige paragraaf van toepassing. Is de ring van coëfficiënten geen lichaam of het aantal variabelen groter dan 1, dan is dit niet langer het geval. In de ring $\mathbf{Z}[X]$ is bijvoorbeeld het ideaal $(3, X)$ geen hoofdideaal (opgave 11.8), en in de ring $K[X, Y]$ het ideaal (X, Y) ook niet. We gaan bewijzen dat voor dergelijke ringen toch eenduidige ontbinding mogelijk is in de zin van 12.11.

▶ Ontbindingsringen

We definiëren eerst formeel de ringen 'met eenduidige ontbinding' als die domeinen waarvoor de uitspraak van stelling 12.11 geldt. Uit 13.2 en 13.3 zal blijken dat dat niet alleen de hoofdideaaldomeinen zijn.

13.1. Definitie. *Een ontbindingsring is een domein R waarin ieder element $x \neq 0$ te schrijven is als een product*

$$x = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t$$

van een eenheid $u \in R^*$ en een eindig aantal irreducibele elementen $p_i \in R$, en bovendien deze schrijfwijze op volgorde en vermenigvuldiging met eenheden na eenduidig is.

In het Engels komt men ontbindingsring tegen als *factorial ring* of *unique factorization domain* (UFD).

Kiest men in een ontbindingsring R een verzameling $\mathcal{P}$ van irreducibele elementen met de eigenschap dat ieder irreducibel element van R met precies één element van $\mathcal{P}$ geassocieerd is, dan kan ieder element $x \neq 0$ in R eenduidig ontbonden worden als

$$x = u \cdot \prod_{p \in \mathcal{P}} p^{n_p}$$

met $u \in R^*$ en $n_p \in \mathbf{Z}_{\geq 0}$ voor bijna alle $p \in \mathcal{P}$ gelijk aan 0. Als in het uit 6.7 bekende geval $R = \mathbf{Z}$ heet de exponent $n_p = \mathrm{ord}_p(x)$ wel de *orde* van x bij p. Er geldt de multiplicatieve eigenschap $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$. In het bijzonder zien we hieruit dat de irreducibele elementen in een ontbindingsring priemelementen zijn:

$$\mathrm{ord}_p(xy) > 0 \quad \Longrightarrow \quad \mathrm{ord}_p(x) > 0 \ \text{ of } \ \mathrm{ord}_p(y) > 0$$

is een implicatie die de priemeigenschap uit 12.9 voor $p \in \mathcal{P}$ verwoordt.

Opgave 1. Laat zien dat ord_p voortgezet kan worden tot een homomorfisme $\mathrm{ord}_p : K^* \to \mathbf{Z}$ op de eenhedengroep van het quotiëntenlichaam K van R.

In ontbindingsringen kan men de *grootste gemene deler* $\mathrm{ggd}(a, b)$ en het *kleinste gemene veelvoud* $\mathrm{kgv}(a, b)$ van elementen $a, b \in R \setminus \{0\}$ definiëren in termen van hun ontbinding:

$$\mathrm{ggd}(a, b) = \textstyle\prod_{p \in \mathcal{P}} p^{\min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}}$$
$$\mathrm{kgv}(a, b) = \textstyle\prod_{p \in \mathcal{P}} p^{\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}}$$

Met de conventie $\mathrm{ord}_p(0) = \infty$ kan men deze definitie ook gebruiken als a of b gelijk is aan 0. In het geval $\mathrm{ggd}(a, b) = 1$ noemt men a en b weer *onderling ondeelbaar* of *copriem*.

Opgave 2. Geef analoge definities voor $\mathrm{ggd}(a_1, a_2, \ldots, a_n)$ en $\mathrm{kgv}(a_1, a_2, \ldots, a_n)$.

Voor hoofdideaaldomeinen zijn de gegeven definities van ggd en kgv equivalent met die in 12.18 (opgave 11). In willekeurige ontbindingsringen is $(a) + (b)$ echter niet noodzakelijk een hoofdideaal, en voldoet $d = \mathrm{ggd}(a, b)$ aan een inclusie $(d) \supset (a) + (b)$ die geen gelijkheid hoeft te zijn. In het bijzonder geldt voor coprieme elementen a en b niet noodzakelijk dat $1 \in R$ als lineaire combinatie van a en b geschreven kan worden. Zo zijn de voortbrengers van de al genoemde idealen $(3, X) \subset \mathbf{Z}[X]$ en $(X, Y) \subset K[X, Y]$ weliswaar copriem, maar brengen zij als ideaal *niet* de hele ring voort.

▶ Polynomen over een ontbindingsring

Zoals gezegd zijn hoofdideaaldomeinen voorbeelden van ontbindingsringen. De volgende stelling laat zien dat er veel meer voorbeelden zijn.

13.2. Stelling. *Zij R een ontbindingsring. Dan is de polynoomring $R[X]$ over R ook een ontbindingsring.*

Door 13.2 herhaald toe te passen zien we dat voor alle $n \geq 1$ de polynoomring $R[X_1, X_2, \ldots, X_n]$ in n variabelen over een ontbindingsring R weer een ontbindingsring is. In het bijzonder hebben we, door R gelijk te nemen aan $\mathbf{Z}$ of aan een lichaam, het volgende nuttige resultaat.

13.3. Gevolg. *Zij $n \geq 1$ een geheel getal en K een lichaam. Dan zijn de polynoomringen $\mathbf{Z}[X_1, X_2, \ldots, X_n]$ en $K[X_1, X_2, \ldots, X_n]$ met coëfficiënten in respectievelijk $\mathbf{Z}$ en K ontbindingsringen.* □

Het bewijs van 13.2 maakt gebruik van het feit dat $R[X]$ een deelring is van $K[X]$, met K het quotiëntenlichaam van R. We gaan de ontbindingen in het hoofdideaaldomein $K[X]$ gebruiken om ook in $R[X]$ ontbindingen te maken.

Zij nu verder R een ontbindingsring. De eerste stap in de factorisatie van een niet-nul polynoom $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ is het 'buiten haakjes halen' van de factor $a = \mathrm{ggd}(a_0, a_1, \ldots, a_n) \in R$. We krijgen dan $f = a \cdot f_0 \in R[X]$ voor een polynoom $f_0 \in R[X]$ waarvoor geen enkel priemelement $p \in \mathcal{P}$ alle coëfficiënten van f_0 deelt. Een dergelijk polynoom heet een *primitief polynoom* in $R[X]$. Merk op dat de schrijfwijze $f = a \cdot f_0$ op vermenigvuldiging met eenheden uit R na eenduidig is.

13.4. Lemma. *Het product van twee primitieve polynomen in $R[X]$ is weer primitief.*

Bewijs. Stel dat een priemelement $p \in \mathcal{P}$ alle coëfficiënten van het product fg van twee primitieve polynomen in $R[X]$ deelt. In de quotiëntring $(R/pR)[X]$ geldt dan de identiteit $\overline{f} \cdot \overline{g} = \overline{0}$. Omdat p echter een priemelement is, is R/pR wegens 12.15 en 12.16 een domein. Dan is $(R/pR)[X]$ ook een domein, dus $\overline{f}$ of $\overline{g}$ is het nulelement in $(R/pR)[X]$. Maar dan zijn alle coëfficiënten van f of g deelbaar door p, in tegenspraak met de primitiviteit van f en g. □

Ieder niet-nul polynoom $f \in K[X]$ kan men schrijven in de vorm $f = c \cdot f_0$ voor een primitief polynoom $f_0 \in R[X]$ en een constante $c \in K^*$. Immers, door f met het product b van alle noemers van de coëfficiënten van f te vermenigvuldigen heeft men $bf \in R[X]$. Schrijf nu als boven $bf = a \cdot f_0$ met $a \in R$ en $f_0 \in R[X]$ primitief, dan geldt $f = c \cdot f_0$ voor $c = ab^{-1} \in K^*$.

Opgave 3. Laat zien dat c en f_0 op vermenigvuldiging met eenheden in R na uniek bepaald zijn.

Bewijs van 13.2. Zij $f \in R[X]$ een niet-nul polynoom. We ontbinden f eerst in $K[X]$ als $f = a \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_t$ met $a \in K^*$ en $g_i \in K[X]$ irreducibel. Door alle g_i zo nodig met een element $c_i \in K^*$ te wijzigen (en vervolgens a aan te passen) kunnen we bereiken dat steeds g_i een primitief polynoom is in $R[X]$. Deze schrijfwijze is bovendien op vermenigvuldiging met eenheden uit R^* na uniek. Omdat $g_1 \cdot g_2 \cdot \ldots \cdot g_t \in R[X]$ wegens 13.4 primitief is, geldt $a \in R$: het is de ggd van de coëfficiënten van f in R.

Omdat R een ontbindingsring is, kunnen we het element $a \in R$ ontbinden als $a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s$, met $u \in R^*$ en alle p_i irreducibel in R. Dit geeft een schrijfwijze

$$(*) \qquad f = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_t$$

voor f in $R[X]$ die op volgorde en vermenigvuldiging met eenheden in $R^* = R[X]^*$ na uniek is.

We beweren dat $(*)$ de verlangde factorisatie van f in $R[X]$ geeft. Uniciteit hebben we al, dus het is voldoende te laten zien dat de irreducibele elementen van $R[X]$ precies de priemelementen van R en de primitieve, in $K[X]$ irreducibele polynomen van $R[X]$ zijn. Enerzijds is uit de schrijfwijze $(*)$ van elementen uit $R[X]$ duidelijk dat ieder irreducibel element in $R[X]$ een priemelement van R of een primitief, in $K[X]$ irreducibel polynoom is. Anderzijds is duidelijk dat een schrijfwijze van een dergelijk element als product van twee niet-eenheden in $R[X]$ in tegenspraak is met de uniciteit van de in $(*)$ gevonden schrijfwijze. □

Enigszins slordig kan men uit het bewijs van 13.2 concluderen dat het ontbinden van een (primitief) polynoom f in $R[X]$ en in $K[X] = (Q(R))[X]$ op hetzelfde neerkomt: iedere irreducibele factor van f in $R[X]$ is ook irreducibel in $K[X]$. Een klassiek gevolg hiervan is het volgende lemma, dat voor $R = \mathbf{Z}$ al door Gauss bewezen werd.

13.5. Lemma van Gauss. *Zij R een ontbindingsring met quotiëntenlichaam K, en $f \in R[X]$ een monisch polynoom. Stel dat er monische polynomen $g_1, g_2 \in K[X]$ bestaan waarvoor $f = g_1 g_2$ geldt. Dan hebben g_1 en g_2 coëfficiënten in R.*

Bewijs. Er bestaan elementen $c_i \in K^*$ zodat $c_i g_i$ primitief is in $R[X]$. Omdat c_i de kopcoëfficiënt van $c_i g_i$ is, geldt $c_i \in R$. Het polynoom $c_1 c_2 \cdot f = (c_1 g_1) \cdot (c_2 g_2)$ is wegens 13.4 weer primitief, dus $c_1 c_2 \in R$ is een eenheid. Er volgt dat c_1 en c_2 eenheden zijn in R, dus g_1 en g_2 zijn polynomen in $R[X]$. □

▶ Ontbinding in $\mathbf{Z}[X]$

Passen we het lemma van Gauss toe op een lineaire factor $g_1 = X - q \in \mathbf{Q}[X]$ van een monisch polynoom $f \in \mathbf{Z}[X]$, dan volgt dat ieder rationaal nulpunt van een monisch polynoom in $\mathbf{Z}[X]$ geheel is. Algemener geldt het volgende.

13.6. Lemma. *Zij $f = \sum_{i=0}^{n} a_i X^i \in \mathbf{Z}[X]$ een polynoom van graad $n \geq 1$ en $q \in \mathbf{Q}$ een nulpunt van f. Schrijven we $q = \frac{b}{c}$ met $b, c \in \mathbf{Z}$ copriem, dan geldt $b|a_0$ en $c|a_n$.*

Bewijs. Is $q = \frac{b}{c}$ een nulpunt van f, dan is $cX - b$ een irreducibel polynoom in $\mathbf{Z}[X]$ dat f deelt in $\mathbf{Q}[X]$, en *dus* ook in $\mathbf{Z}[X]$. Er volgt dat c de kopcoëfficiënt a_n van f deelt, en b de constante coëfficiënt a_0. □

Opgave 4. Wat zijn de rationale nulpunten van $f = 10X^5 + 23X^4 - 30X^3 - 20X^2 + 20X - 3$?

Lemma 13.6 geeft een manier om alle rationale nulpunten van een polynoom $f \in \mathbf{Z}[X]$ te bepalen. Algemener is er de vraag hoe men in eindig veel stappen de ontbinding van een polynoom $f \in \mathbf{Z}[X]$ van graad $n > 0$ bepaalt. Om te onderzoeken of f een factor $g \in \mathbf{Z}[X]$ van graad niet meer dan d heeft, met $1 \leq d \leq n$, kan men $d+1$ verschillende waarden $x_0, x_1, \ldots, x_d \in \mathbf{Z}$ kiezen die geen nulpunten van f zijn. Omdat f ten hoogste n nulpunten in $\mathbf{Z}$ heeft is dit niet moeilijk; treft men per ongeluk een nulpunt dan kan dit bovendien direct gebruikt worden om een lineaire factor uit f te verwijderen. Is nu g een deler van f, dan is $g(x_i)$ een deler van $f(x_i)$ voor $i = 0, 1, \ldots, d$. Ieder van de getallen $f(x_i)$ heeft maar eindig veel delers in $\mathbf{Z}$, dus dit geeft eindig veel mogelijkheden voor elk van de getallen $g(x_i)$. Bij ieder $(d+1)$-tupel van mogelijke waarden voor $(g(x_i))_{i=0}^{d}$ behoort een *uniek* polynoom $g \in \mathbf{Q}[X]$ van graad ten hoogste d dat deze waarden aanneemt in de punten x_i. De *interpolatieformule van Lagrange* uit opgave 12.26 geeft er een formule voor. Dit geeft een eindige lijst van mogelijkheden voor g, en in deze lijst staan alle delers van f van graad ten hoogste d. Men kan vervolgens met de methode van 12.1 nagaan wat de daadwerkelijke delers van $f \in \mathbf{Z}[X]$ zijn.

Opgave 5. Laat zien dat we voor $d \geq n/2$ alle priemfactoren van f vinden.

Bovenstaande methode is al snel zeer tijdrovend, maar laat zien dat het factorisatieprobleem in $\mathbf{Z}[X]$ in eindig veel stappen oplosbaar is. (Zie opgave 40 voor een ander argument.) Door de eenvoud van de onderliggende gedachte doet hij enigszins denken aan de methode van *trial division* die we in §6 noemden om gehele getallen te factoriseren: door domweg proberen van delers $d = 2, 3, \ldots$ tot aan $\sqrt{n}$ kan men ieder getal $n > 1$ ontbinden in $\mathbf{Z}$.

▶ Reductie modulo priemen

Veel factorisatietechnieken in $\mathbf{Z}[X]$ maken gebruik van de reductie-afbeelding $\mathbf{Z}[X] \to (\mathbf{Z}/n\mathbf{Z})[X]$, waarbij n een priemgetal of een macht van een priemgetal is.

13.7. Stelling. *Zij p een priemgetal en $f = \sum_{i=0}^{n} a_i X^i \in \mathbf{Z}[X]$ een primitief polynoom waarvan de kopcoëfficiënt niet deelbaar is door p. Dan geldt*

$$(f \bmod p) \text{ is irreducibel in } \mathbf{F}_p[X] \quad \Longrightarrow \quad f \text{ is irreducibel in } \mathbf{Z}[X].$$

Bewijs. Als f reducibel is in $\mathbf{Z}[X]$, dan volgt uit de primitiviteit van f dat er niet-constante polynomen $g, h \in \mathbf{Z}[X]$ bestaan met $f = g \cdot h$. Door deze identiteit modulo p te nemen krijgen we $\overline{f} = \overline{g} \cdot \overline{h} \in \mathbf{F}_p[X]$. Wegens de aanname op de kopcoëfficiënt van f zijn ook de kopcoëfficiënten van g en h niet deelbaar door p. Er volgt dat $\overline{g}$ en $\overline{h}$ niet

constant zijn in $\mathbf{F}_p[X]$, dus $\overline{f} = (f \bmod p)$ is reducibel in $\mathbf{F}_p[X]$. De bewezen implicatie is wegens elementaire logica equivalent met de uitspraak van de stelling. □

Opgave 6. Laat zien dat de voorwaarde op de kopcoëfficiënt van f in 13.7 niet weggelaten kan worden.

Opgave 7. Generaliseer 13.7 voor het geval van een priemelement p in een ontbindingsring R.

Stel dat we het primitieve polynoom $f = 143X^3 - 8X^2 + X + 105 \in \mathbf{Z}[X]$ willen ontbinden. Omdat f van graad 3 is, is f irreducibel in $\mathbf{Z}[X]$ indien f geen nulpunt heeft in $\mathbf{Q}$. Testen van alle door 13.6 toegestane nulpunten (64 stuks!) is hier enig werk. Merken we echter op dat $(f \bmod 2) = X^3 + X + 1 \in \mathbf{F}_2[X]$ geen nulpunten heeft in $\mathbf{F}_2$ en dus irreducibel is, dan volgt direct dat f irreducibel is in $\mathbf{Z}[X]$.

Opgave 8. Is $7X^3 - 51X^2 + 5X + 70$ irreducibel in $\mathbf{Z}[X]$?

Voor kleine priemgetallen p zijn de nulpunten van een polynoom in $\mathbf{F}_p[X]$ te vinden door eenvoudig alle elementen van $\mathbf{F}_p$ te proberen. Iets soortgelijks geldt voor factoren van lage graad. Voor grotere p gebruikt men ggd-berekeningen als in opgave 22.

Ook als $f \in \mathbf{Z}[X]$ een polynoom is waarvoor $(f \bmod p)$ reducibel is, geeft de factorisatie van $(f \bmod p)$ in $\mathbf{F}_p[X]$ nuttige informatie over de ontbinding van f. Zo heeft het polynoom $f = X^4 + 13X^3 - 9X^2 - 2X + 65$ modulo de priemen 2 en 3 de respectievelijke factorisaties

$$(f \bmod 2) = X^4 + X^3 + X^2 + 1 = (X\ \ + 1)(X^3 + X + 1) \in \mathbf{F}_2[X]$$
$$(f \bmod 3) = X^4 + X^3 + X\ \ - 1 = (X^2 + 1)(X^2 + X - 1) \in \mathbf{F}_3[X].$$

Uit de tweede factorisatie zien we dat f geen lineaire factoren heeft in $\mathbf{Z}[X]$, uit de eerste dat f geen irreducibele kwadratische factoren heeft in $\mathbf{Z}[X]$. We concluderen dat f irreducibel is.

Soms kan men irreducibiliteit van f in $\mathbf{Z}[X]$ bewijzen met een variatie op het *bewijs* van 13.7. Als in opgave 7 geldt het resultaat voor polynomen over een willekeurige ontbindingsring R.

13.8. Criterium van Eisenstein. *Zij R een ontbindingsring en $p \in R$ een priemelement. Laat $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ een primitief polynoom zijn dat voldoet aan*

$$p \nmid a_n, \qquad p \mid a_i \text{ voor } i = 0, 1, \ldots, n-1 \qquad \text{en} \qquad p^2 \nmid a_0.$$

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

Bewijs. Als f reducibel is in $R[X]$, dan volgt weer uit de primitiviteit van f dat er niet-constante polynomen $g, h \in R[X]$ bestaan met $f = g \cdot h$. Modulo p vinden we $\overline{g} \cdot \overline{h} = \overline{f} = \overline{a}_n X^n \in K[X]$, met K het quotiëntenlichaam van de restklassenring R/pR. Dit geeft $\overline{g} = \overline{c}_g X^k$ en $\overline{h} = \overline{c}_h X^{n-k}$ voor zekere kopcoëfficiënten c_g en c_h van g en h in R en $k \in \{0, 1, 2, \ldots, n\}$. Wegens de aanname op de kopcoëfficiënt van f hebben $\overline{g}$ en $\overline{h}$ positieve graad, dus k is niet gelijk aan 0 of n. Er volgt dat de constante coëfficiënt van zowel g als h deelbaar is door p. De constante coëfficiënt van f, die hiervan het product is, wordt daarmee deelbaar door p^2, in tegenspraak met de aanname. □

Een polynoom dat aan de voorwaarden van het criterium voldoet heet een *Eisenstein-polynoom bij* p in $R[X]$.

13.9. Voorbeelden. 1. Zij $n \geq 1$ willekeurig. Het polynoom $X^n - 2$ is voor alle $n \geq 1$ Eisenstein bij $p = 2$, en dus irreducibel in $\mathbf{Z}[X]$. Evenzo is voor $a \neq \pm 1$ kwadraatvrij $X^n - a$ Eisenstein bij iedere priemdeler van a, en dus irreducibel in $\mathbf{Z}[X]$.

2. Zij p een priemgetal. Het *p-de cyclotomische polynoom*, in zuiver Nederlands ook wel *p-de cirkeldelingsveelterm* genoemd, is het polynoom

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + X^{p-3} + \ldots + X + 1 \in \mathbf{Z}[X].$$

De complexe nulpunten van Φ_p zijn de p-de eenheidswortels in $\mathbf{C}^*$ verschillend van 1. Om in te zien dat dit polynoom irreducibel is in $\mathbf{Z}[X]$ passen we een automorfisme van de polynoomring $\mathbf{Z}[X]$ toe geïnduceerd door $X \mapsto X + 1$. Onder dit 'opschuiven van polynomen' gaat Φ_p over in het polynoom

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + pX^{p-2} + \binom{p}{2} X^{p-3} + \ldots + \binom{p}{p-2} X + p.$$

Omdat alle binomiaalcoëfficiënten $\binom{p}{i}$ met $1 < i < p$ deelbaar zijn door p is dit een Eisensteinpolynoom bij p. Met $\Phi_p(X+1)$ is Φ_p zelf ook irreducibel in $\mathbf{Z}[X]$ – zie de opgaven 26 en 27.

3. Zij $f \in \mathbf{Z}[X, Y]$ het polynoom gegeven door

$$f = X^3 + Y^3 + X^2Y + XY^2 + X^2 + Y^2 - Y.$$

Vat f op als kubisch polynoom in Y met coëfficiënten in $\mathbf{Z}[X]$ en schrijf

$$f = Y^3 + (X+1)Y^2 + (X^2 - 1)Y + (X^3 + X^2).$$

Dit is een primitief polynoom in Y, en behalve de kopcoëfficiënt zijn alle coëfficiënten deelbaar door het priemelement $X + 1 \in \mathbf{Z}[X]$. De constante coëfficiënt $X^2(X+1)$ heeft slechts een enkele factor $X + 1$, dus f is een Eisensteinpolynoom in Y bij $X + 1$. Er volgt dat f irreducibel is in $\mathbf{Z}[X, Y]$.

Opgave 9. Laat zien dat $X^3 + Y^3 + X^2Y + XY^2 + Y^2 - Y$ irreducibel is in $\mathbf{Z}[X, Y]$.

▶ Numerieke methoden

Moderne computeralgebra-pakketten als Maple, Mathematica of Pari hebben standaardroutines voor het ontbinden van polynomen in 1 of meer variabelen. Dit maakt de moderne wiskundige minder afhankelijk van allerlei 'handigheidjes' van het in 13.9 voorkomende type. Aan de andere kant creëren dergelijke pakketten een sterke behoefte aan *efficiënte* methoden voor polynoomfactorisatie, en hierbij is meer nodig dan 'slim programmeren'. Net als in het in §6 besproken geval van getallenfactorisatie berusten

praktische methoden op enigszins geavanceerde wiskunde, en dit maakt de zogenaamde *algoritmische algebra* tot een actief onderzoeksgebied.[9]

Voor een polynoom $f \in \mathbf{Z}[X]$ in één variabele heeft men allereerst een *bovengrens* nodig op de grootte van de coëfficiënten van mogelijke delers $g \in \mathbf{Z}[X]$ van f. Dergelijke bovengrenzen leidt men af met gebruikmaking van het fundamentele feit dat een polynoom van graad n met complexe coëfficiënten precies n complexe nulpunten heeft. Deze stelling, die vroeger wel de *hoofdstelling van de algebra* genoemd werd, wordt bewezen in 26.3. De complexe nulpunten van een deler $g|f$ in $\mathbf{Z}[X]$ vormen een deelverzameling van deze nulpunten, en door de absolute waarde van de complexe nulpunten van f af te schatten (en op te merken dat de kopcoëfficiënt van g die van f deelt) krijgt men een bovengrens B op de absolute waarde van de coëfficiënten van g (opgave 40).

Men berekent nu de factorisatie van f modulo een *priemmacht* $p^k > 2B$. Dit geschiedt door f eerst modulo p te factoriseren – hiervoor bestaan redelijk snelle methodes – en vervolgens de factorisatie met een Newton-achtig iteratie-proces modulo steeds hogere priemmachten te bepalen. Weliswaar is $\mathbf{Z}/p^k\mathbf{Z}$ geen ontbindingsring, maar voor voldoend grote k blijkt dit geen rol te spelen.[10] Voor iedere factor $(g \bmod p^k)$ die men zo krijgt, is er een uniek polynoom $g \in \mathbf{Z}[X]$ met deze reductie en coëfficiënten niet groter dan B. Men test vervolgens of dit een factor van f is. Deze algoritme, die bekend staat als de Hensel-Berlekamp-algoritme, werkt goed als $(g \bmod p^k)$ niet al te veel factoren heeft. In het ongelukkige geval dat dit wel zo is, kan men met succes zijn toevlucht nemen tot in de jaren tachtig ontwikkelde technieken die berusten op methodes om korte vectoren in roosters in $\mathbf{R}^n$ te vinden. Deze technieken kunnen ook voor factorisatie van polynomen in meer variabelen worden toegepast.

Factorisatie van polynomen in $\mathbf{R}[X]$ of $\mathbf{C}[X]$ rekent men tot het vakgebied van de *numerieke wiskunde*. Omdat reële en complexe getallen slechts met eindige precisie gerepresenteerd kunnen worden, moet men zich anders dan in het geval van $\mathbf{Q}[X]$ tevreden stellen met *benaderingen* van nulpunten en factoren. Er zijn diverse methoden, waarvan met name *Newtoniteratie* veel gebruikt wordt. Ook hier zijn er weer talloze algoritmische verfijningen mogelijk.

OPGAVEN.

10. Bewijs dat in een ontbindingsring R het element $\mathrm{kgv}(a,b)$ een voortbrenger is van $(a)\cap(b)$.

11. Zij R een domein. We noemen $d \in R$ een *grootste gemene deler* van $a, b \in R$ als geldt:

    $(a) + (b) \subset (d)$;

    voor alle $x \in R$ geldt: $(a) + (b) \subset (x) \implies (d) \subset (x)$.

    a. Bewijs: a en b hebben een ggd dan en slechts dan als de doorsnede van alle hoofdidealen die $(a) + (b)$ omvatten weer een hoofdideaal is.
    b. Bewijs: als R een hoofdideaaldomein of ontbindingsring is, is deze definitie equivalent met de eerder gegeven definities.

12. Laat zien dat de ggd van $1 + \sqrt{-5}$ en $1 - \sqrt{-5}$ in $\mathbf{Z}[\sqrt{-5}]$ gelijk is aan 1. Laat ook zien dat 6 en $3 + 3\sqrt{-5}$ *geen* ggd hebben in de zin van de vorige opgave.

13. Bepaal de ggd van $X^4 + 2X$ en $X^2 + 5$ in $\mathbf{C}[X]$ en in $\mathbf{F}_3[X]$.

14. Bepaal de ggd van $X^{12} - 1$ en $X^4 + X$ in $\mathbf{C}[X]$, $\mathbf{R}[X]$, $\mathbf{F}_3[X]$ en $\mathbf{F}_2[X]$.

15. Bewijs: als R een ontbindingsring is, dan is de polynoomring $\Omega = \bigcup_{n>0} R[X_1, X_2, \ldots, X_n]$ in aftelbaar veel variabelen over R ook een ontbindingsring. Is Ω een hoofdideaaldomein? Is Ω noethers?

16. Is de ring $R[X, X^{-1}]$ van Laurentpolynomen over een ontbindingsring R weer een ontbindingsring?

17. Een *trigonometrisch polynoom* is een functie $f : \mathbf{R} \to \mathbf{R}$ van de vorm

$$f(x) = a_0 + \textstyle\sum_{k=1}^{n}(a_k \cos kx + b_k \sin kx)$$

    met $n \in \mathbf{Z}_{\geq 0}$ en $a_k, b_k \in \mathbf{R}$. Als a_n en b_n niet beide 0 zijn heet n de *graad* $\deg(f)$ van f.

    a. Laat zien dat de verzameling $\mathcal{T}$ van trigonometrische polynomen een deelring vormt van de ring van reëelwaardige functies op $\mathbf{R}$.
    [Hint: schrijf $f(x) = \sum_{k=0}^{n}(c_k e^{ikx} + \overline{c}_k e^{-ikx})$ met $c_k \in \mathbf{C}$.]
    b. Laat zien dat de graad op $\mathcal{T}$ voldoet aan $\deg(fg) = \deg(f) + \deg(g)$. Concludeer dat $\mathcal{T}$ een domein is.
    c. Laat zien dat de elementen $\sin x$, $1 + \cos x$ en $1 - \cos x$ irreducibel zijn in $\mathcal{T}$, maar niet priem. Concludeer dat $\mathcal{T}$ geen ontbindingsring is.
    [Hint: $\sin^2 x = 1 - \cos^2 x$.]

18. Laat zien dat de verzameling van afbeeldingen $f : \mathbf{C} \to \mathbf{C}$ van de vorm

$$f(z) = a_0 + \textstyle\sum_{k=1}^{n}(a_k \cos kz + b_k \sin kz)$$

    met $n \in \mathbf{Z}_{\geq 0}$ en $a_k, b_k \in \mathbf{C}$ een deelring vormt van de ring van complexwaardige functies op $\mathbf{C}$, en dat deze ring een hoofdideaaldomein is.

19. Zij K een lichaam en $f \in K[X]$ een polynoom van graad n. Laat zien dat er polynomen $f_0, f_1, \ldots, f_n \in K[X]$ bestaan met $f(X + Y) = \sum_{k=0}^{n} f_k Y^k$. Bewijs: $f_0 = f$, en f_1 is de *afgeleide* van f uit opgave 12.22.

20. Zij $f \in \mathbf{F}_p[X]$ een polynoom met afgeleide $f' = 0$. Bewijs: $f(X) = g(X^p)$ voor zekere $g \in \mathbf{F}_p[X]$.

21. Laat zien dat de natuurlijke afbeelding $\mathbf{F}_p[X] \to \mathrm{Map}(\mathbf{F}_p, \mathbf{F}_p)$, die een polynoom als functie op $\mathbf{F}_p$ opvat, een ringisomorfisme $\mathbf{F}_p[X]/(X^p - X) \xrightarrow{\sim} \mathrm{Map}(\mathbf{F}_p, \mathbf{F}_p)$ induceert.

22. Zij $f \in \mathbf{F}_p[X]$ een niet-nul polynoom, en $S \subset \mathbf{F}_p$ de verzameling nulpunten van f in $\mathbf{F}_p$. Bewijs: $\mathrm{ggd}(f, X^p - X) = \prod_{x \in S}(X - x)$.

23. Zij $f \in \mathbf{Z}[X]$ een monisch polynoom met $f(4) = 17$. Bewijs dat f ten hoogste drie rationale nulpunten heeft.

24. Zij $f \in \mathbf{Z}[X]$ een irreducibel polynoom.
    a. Bewijs dat f geen dubbele nulpunten heeft in $\mathbf{C}$.
    b. Bewijs dat er maar eindig veel priemgetallen p zijn waarvoor f mod p meervoudige priemfactoren heeft in $\mathbf{F}_p[X]$. [Een priemfactor $q|f$ heet *meervoudig* als $q^2|f$ geldt.]

25. Definieer het *reciproke polynoom* van een polynoom $f = \sum_{i=0}^{n} a_i X^i \in \mathbf{Q}[X]$ met $a_n a_0 \neq 0$ als $f^* = \sum_{i=0}^{n} a_i X^{n-i}$. Bewijs: f is irreducibel $\iff f^*$ is irreducibel.

26. Zij K een lichaam en $\sigma : K[X] \xrightarrow{\sim} K[X]$ een automorfisme van de polynoomring dat de identiteit is op K. Bewijs: $\sigma(X) = aX + b$ voor zekere $a \in K^*$ en $b \in K$. Concludeer dat de groep $\mathrm{Aut}_K(K[X])$ van automorfismen van $K[X]$ die op K de identiteit zijn isomorf is met de affiene groep $\mathrm{Aff}(K) \cong K \rtimes K^*$ over K uit 8.14.1 en 8.14.4.

27. Zij R een ontbindingsring en $\sigma \in \mathrm{Aut}(R)$ een automorfisme. Bewijs: r is irreducibel in R $\iff \sigma(r)$ is irreducibel in R.

28. Ontbind de volgende polynomen in $\mathbf{Z}[X]$ en in $\mathbf{Q}[X]$:
    $$4X^2 + 8, \qquad 3X^4 + 6X + 6, \qquad X^4 - 7X^2 + 5X - 3, \qquad X^3 + 2X + 3.$$

29. Ontbind de volgende polynomen in $\mathbf{Z}[X]$:
    $$3X^{12}+9X^4+7, \quad X^4+3X^3+2X^2+8X+6, \quad (X+1)^7-X^7-1, \quad X^4+2X^3+4X^2+8X+16.$$

30. Ontbind de volgende polynomen in $\mathbf{Z}[X]$:
    $$X^{120} - 5X^{65} + 3X^{55} - 15, \qquad X^6 - X^2 + 20X - 100, \qquad X^4 - 4X^3 + 4X^2 - 25.$$

31. Ontbind de volgende polynomen in $\mathbf{Q}[X, Y]$ en $\mathbf{C}[X, Y]$;
    $$Y^5 + X^2 - 2, \quad X^{12} + Y^3 + Y, \quad X^4 + 4Y^4, \quad Y^3 - (X + 2)Y^2 + Y + X(X + 1).$$

32. Zij p een priemgetal. Laat zien dat het p^k-de cyclotomische polynoom
    $$\Phi_{p^k}(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + X^{(p-3)p^{k-1}} + \ldots + X^{p^{k-1}} + 1 \in \mathbf{Z}[X]$$
    voor alle $k \in \mathbf{Z}_{\geq 1}$ irreducibel is in $\mathbf{Z}[X]$.

33. Bepaal de factorisatie van $f = X^4 + 1$ in $\mathbf{F}_p[X]$ voor alle priemgetallen $p \leq 41$. Voor welke $p \in \mathbf{Z}$ splitst f in lineaire factoren in $\mathbf{F}_p[X]$?

34. Laat zien dat $X^4 + 1$ reducibel is in $\mathbf{F}_p[X]$ voor alle p, maar irreducibel in $\mathbf{Z}[X]$.
[Hint: tenminste één van de elementen $-1, 2, -2$ is een kwadraat in $\mathbf{F}_p^*$.]

35. Laat zien dat een polynoom $f = X^2 + aX + b \in \mathbf{Z}[X]$ irreducibel is modulo een priemgetal $p > 2$ dan en slechts dan als $a^2 - 4b$ geen kwadraat is modulo p. *Stel dat f reducibel is modulo alle priemgetallen p. Is f reducibel in $\mathbf{Z}[X]$?

36. Neem $f = X^2 - X + 41 \in \mathbf{Z}[X]$. Bepaal het kleinste positieve gehele getal x waarvoor $f(x)$ *geen* priemgetal is. Laat zien dat er een niet-constant polynoom $f \in \mathbf{Q}[X]$ bestaat met de eigenschap dat $f(x)$ priem is voor alle positieve gehele getallen $x < 1000$. *Bestaat er ook zo'n polynoom in $\mathbf{Z}[X]$?

37. Zij $f \in \mathbf{Z}[X]$ een polynoom met de eigenschap dat $f(x)$ voor *alle* $x \in \mathbf{Z}$ een priemgetal is. Is f noodzakelijk een constant polynoom?

*38. Zij $f \in \mathbf{Z}[X]$ een polynoom met de eigenschap dat $f(x)$ voor alle $x \in \mathbf{Z}$ een kwadraat is. Is f noodzakelijk het kwadraat van een polynoom in $\mathbf{Z}[X]$?

39. Zij $V = \{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\}$ de eenheidscirkel in $\mathbf{R}^2$ en $\phi : \mathbf{R}[X, Y] \to \mathrm{Cont}(V, \mathbf{R})$ de afbeelding die polynomen als continue functies op V opvat. Bewijs: ϕ is een homomorfisme met kern $(X^2 + Y^2 - 1)$. Is $\mathrm{im}[\phi]$ een domein? Is ϕ surjectief?
[Hint: schrijf $F \in \mathbf{R}[X, Y]$ als $f(X) + Yg(X) + (X^2 + Y^2 - 1)h(X, Y)$.]

40. Zij $f \in \mathbf{Z}[X]$ een monisch polynoom van graad n, en stel dat de coëfficiënten van f in absolute waarde begrensd worden door A.
    a. Bewijs: voor ieder nulpunt $\alpha \in \mathbf{C}$ van f geldt $|\alpha| \leq nA$.
    b. Bewijs: iedere monische deler $\sum_{j=0}^{d} b_j X^j$ van f in $\mathbf{C}[X]$ van graad d voldoet aan $|b_j| \leq \binom{d}{j} n^{d-j} A^{d-j}$.
    c. Leid uit (b) af dat de factorisatie van f in $\mathbf{Z}[X]$ in eindig veel stappen gevonden kan worden.

14 Symmetrische polynomen

In deze paragraaf beschouwen we een speciaal type van polynomen in meer variabelen, de zogenaamde *symmetrische polynomen*. Dit is een zeer klassiek algebraïsch onderwerp, dat we later in de Galoistheorie nog in grote algemeenheid tegen zullen komen.

In 12.3 zagen we dat voor een domein R een niet-nul polynoom $f \in R[X]$ niet meer dan $n = \deg(f)$ nulpunten heeft. Voor $R = \mathbf{Z}$ vertelt de hoofdstelling van de algebra 26.3 ons dat f *precies* $n = \deg(f)$ nulpunten heeft, mits we deze met multipliciteit tellen en bereid zijn nulpunten te beschouwen in een grotere ring dan $\mathbf{Z}$ zelf, zoals $\mathbf{C}$. Voor willekeurige domeinen is dit ook waar, en we zullen in §21 de benodigde 'uitbreidingslichamen' construeren.

Zelfs als de nulpunten van $f \in R[X]$ pas in een grotere ring $R' \supset R$ te vinden zijn, blijken toch alle 'symmetrische uitdrukkingen' in de nulpunten van f in R zelf te liggen. We zullen zien hoe we ze kunnen berekenen *zonder* ooit buiten de grondring R te treden. De gegeven methodes worden door alle computeralgebra-pakketten gebruikt.

▶ Algemeen polynoom van graad n

We definiëren een 'algemeen' polynoom van graad n door te werken in de ring $R = \mathbf{Z}[T_1, T_2, \ldots, T_n]$ van polynomen in de n variabelen $T_1, T_2, \ldots, T_n$. Als coëfficiëntenring kan men in plaats van $\mathbf{Z}$ ook andere ringen toelaten, maar wij zullen dat voor de eenvoud niet doen. De *(totale) graad* van het monoom $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ is gelijk aan $e_1 + e_2 + e_3 + \ldots + e_n$, en men definieert de *graad* $\deg(f)$ van een niet-nul polynoom $f \in R$ als het maximum van de graden van de in f voorkomende monomen. Indien alle monomen in f van dezelfde graad d zijn, dan heet f *homogeen* van graad d. Een willekeurig polynoom $f \in R$ van graad d kan men door de monomen van vaste graad bij elkaar te nemen schrijven als $f = f_0 + f_1 + f_2 + \ldots + f_d$, met f_k homogeen van graad k.

Het *algemene* of *universele polynoom* F_n van graad n is het monische polynoom in $R[X]$ dat de variabelen $T_1, T_2, \ldots, T_n$ als nulpunten heeft:

$$F_n = (X - T_1)(X - T_2)\ldots(X - T_n) = X^n + \sum_{k=1}^{n} (-1)^k s_k X^{n-k} \in R[X].$$

De coëfficiënten $s_k \in R$ heten de *elementaire symmetrische polynomen* in de nulpunten T_i van f, en de Fransman François Viète (1540–1603) wist al dat s_k voor $k = 1, 2, \ldots n$ gelijk is aan

$$s_k = \sum_{1 \le i_1 < i_2 < \ldots i_k \le n} T_{i_1} T_{i_2} \ldots T_{i_k},$$

de som van alle producten van precies k verschillende nulpunten van F. Het polynoom $s_k \in R$ is homogeen van graad k, en we hebben

$$s_1 = T_1 + T_2 + \ldots + T_n,$$
$$s_2 = T_1T_2 + T_1T_3 + \ldots + T_1T_n + T_2T_3 + T_2T_4 + \ldots + T_{n-1}T_n,$$

en

$$s_n = T_1T_2T_3 \ldots T_n.$$

Merk op dat het algemene polynoom van graad n per definitie coëfficiënten heeft in het domein $R_0 = \mathbf{Z}[s_1, s_2, \ldots, s_n]$, en dat zijn n nulpunten de variabelen van de uitbreidingsring $R = \mathbf{Z}[T_1, T_2, \ldots, T_n] \supset R_0$ zijn.

▶ Symmetrische polynomen

Een polynoom in $R = \mathbf{Z}[T_1, T_2, \ldots, T_n]$ (of, algemener, in $A[T_1, T_2, \ldots, T_n]$ voor een commutatieve ring A) heet *symmetrisch* (in de variabelen T_i) als het invariant is onder alle permutaties van de variabelen T_i. Iets formeler kunnen we de natuurlijke werking van de symmetrische groep S_n op R beschouwen, die gegeven wordt door

$$(\sigma f)(T_1, T_2, \ldots, T_n) = f(T_{\sigma(1)}, T_{\sigma(2)}, \ldots, T_{\sigma(n)}) \qquad \text{voor } f \in R, \sigma \in S_n.$$

De symmetrische polynomen in R zijn dan de polynomen in R die invariant zijn onder de werking van S_n. De afbeelding $f \mapsto \sigma f$ is voor iedere $\sigma \in S_n$ een *automorfisme* van R, zodat we een inclusie $S_n \subset \mathrm{Aut}(R)$ hebben. Hieruit volgt gemakkelijk dat de symmetrische polynomen een *deelring* $R_0 \subset R$ vormen.

Opgave 1. Ga dit na.

Omdat het k-de elementaire symmetrische polynoom $s_k \in R$ symmetrisch is, geldt $\mathbf{Z}[s_1, s_2, \ldots, s_n] \subset R_0$. De hoofdstelling voor symmetrische polynomen is dat deze inclusie een gelijkheid is: *ieder* symmetrisch polynoom is een veelterm in de elementaire symmetrische polynomen. In de Galoistheorie wordt dit thema verder uitgewerkt: uitdrukkingen met 'veel' symmetrieën zijn bevat in 'kleine' deelringen.

14.1. Hoofdstelling. *Zij $P \in R = \mathbf{Z}[T_1, T_2, \ldots, T_n]$ een symmetrisch polynoom. Dan is P uniek te schrijven als een veelterm in de elementaire symmetrische polynomen s_k.*

We geven een bewijs dat in feite een *algoritme* geeft om een P als element van $\mathbf{Z}[s_1, s_2, \ldots, s_n]$ te schrijven.

Bewijs. We ordenen de in P voorkomende monomen *lexicografisch*, als in een woordenboek. Dus: monomen $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ met de hoogste exponent e_1 komen voorop, bij gelijke e_1 ordenen we op e_2, enzovoort.

Laat nu $c \cdot T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ met $c \in \mathbf{Z} \setminus \{0\}$ de lexicografisch eerste term in P zijn, en $d = e_1 + e_2 + e_3 + \ldots + e_n$ de graad van deze term. Dan geldt $e_1 \geq e_2 \geq e_3 \geq \ldots \geq e_n$. Immers, indien dit niet het geval is kunnen we door een geschikte permutatie van de T_i hieruit een term maken die lexicografisch nog eerder komt, en die wegens de symmetrie van P óók in P voorkomt: tegenspraak. Vorm nu het monoom

$$\Sigma = s_1^{e_1 - e_2} s_2^{e_2 - e_3} s_3^{e_3 - e_4} \ldots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n} \in R$$

van graad

$$\begin{aligned} &e_1 - e_2 + 2(e_2 - e_3) + 3(e_3 - e_4) + \ldots + (n-1)(e_{n-1} - e_n) + n e_n \\ &= e_1 + e_2 + e_3 + \ldots + e_n = d \leq \deg(P), \end{aligned}$$

met lexicografisch eerste term $T_1^{e_1}T_2^{e_2}\dots T_n^{e_n}$, en beschouw $P_1 = P - c\Sigma \in R$. Wegens $\deg(\Sigma) \leq \deg(P)$ hebben we $\deg(P_1) \leq \deg(P)$, en alle monomen in P_1 komen lexicografisch *later* dan $T_1^{e_1}T_2^{e_2}\dots T_n^{e_n}$. Omdat bij begrensde graad maar eindig veel verschillende monomen mogelijk zijn, zien we dat we door herhaald aftrekken van een element uit $\mathbf{Z}[s_1, s_2, \dots, s_n]$ het polynoom P gelijk wordt aan 0. Met andere woorden: P is zelf bevat in $\mathbf{Z}[s_1, s_2, \dots, s_n]$.

Om te bewijzen dat een polynoom niet op twee verschillende manieren als veelterm in $\mathbf{Z}[s_1, s_2, \dots, s_n]$ geschreven kan worden, moeten we laten zien dat er geen niet-nul polynoom $g \in \mathbf{Z}[X_1, X_2, \dots, X_n]$ bestaat met $g(s_1, s_2, \dots, s_n) = 0$. Schrijf hiertoe ieder in g voorkomend monoom in de vorm

$$cX_1^{e_1-e_2}X_2^{e_2-e_3}X_3^{e_3-e_4}\dots X_{n-1}^{e_{n-1}-e_n}X_n^{e_n},$$

en bekijk het monoom M in g waarvoor het corresponderende n-tupel $(e_1, e_2, \dots, e_n)$ lexicografisch als eerste komt. Bij uitschrijven van $g(s_1, s_2, \dots, s_n)$ als polynoom in $\mathbf{Z}[T_1, T_2, \dots, T_n]$ zien we dat M aanleiding geeft tot een term $cT_1^{e_1}T_2^{e_2}\dots T_n^{e_n}$ die niet verdwijnt: tegenspraak. □

Uit de uniciteit van representaties in termen van de elementaire symmetrische polynomen s_k volgt dat $\mathbf{Z}[s_1, s_2, \dots, s_n]$ weer als polynoomring in de variabelen s_k op te vatten is: de elementaire symmetrische polynomen zijn *algebraïsch onafhankelijk*.

Een monoom $s_1^{a_1}s_2^{a_2}\dots s_n^{a_n}$ noemt men van *gewicht* $a_1 + 2a_2 + 3a_3 + \dots + na_n$, en algemener is het gewicht van $g \in \mathbf{Z}[s_1, s_2, \dots, s_n]$ het maximum van de gewichten van de in g voorkomende monomen. Hebben alle monomen in g hetzelfde gewicht d, dan heet g *isobarisch* van gewicht d. Merk op dat het gewicht van $g \in \mathbf{Z}[s_1, s_2, \dots, s_n]$ niets anders is dan de *graad* van g als element van $R = \mathbf{Z}[T_1, T_2, \dots, T_n]$. Het bewijs van 14.1 laat het volgende zien.

14.2. Gevolg. *Een homogeen symmetrisch polynoom in $\mathbf{Z}[T_1, T_2, \dots, T_n]$ van graad d is uniek te schrijven als isobarisch polynoom van gewicht d in $\mathbf{Z}[s_1, s_2, \dots, s_n]$.* □

Een willekeurig symmetrisch polynoom P kan men schrijven als som van homogene polynomen P_k van graad k, en de polynomen P_k zijn dan symmetrisch omdat de werking van S_n op $\mathbf{Z}[T_1, T_2, \dots, T_n]$ de graad invariant laat. Wegens 14.2 is P_k te schrijven als isobarisch polynoom van gewicht k in de elementaire symmetrische polynomen s_k .

▶ Rekenen met symmetrische polynomen

Voor een symmetrisch polynoom P heeft men een verkorte notatie die eruit bestaat dat men uit elke S_n-baan van monomen in P een enkele representant opschrijft, voorafgegaan door het symbool $\sum_n$ om aan te geven dat men de som over de monomen in de S_n-baan van de representant neemt. Het k-de elementaire symmetrische polynoom $s_k \in R$ is in deze notatie gelijk aan

$$s_k = \sum_n T_1T_2T_3\dots T_k.$$

Algemener staat $\sum_n f$ met $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ voor de som van de polynomen in de S_n-baan van f. Voorbeelden:

$$\sum_3 T_1^2 T_2 = T_1^2T_2 + T_1^2T_3 + T_2^2T_3 + T_1T_2^2 + T_1T_3^2 + T_2T_3^2$$
$$\sum_4 T_1T_2T_3 = T_1T_2T_3 + T_1T_2T_4 + T_1T_3T_4 + T_2T_3T_4$$
$$\sum_4 T_1T_2 = T_1T_2 + T_1T_3 + T_1T_4 + T_2T_3 + T_2T_4 + T_3T_4$$

Wil men een gegeven symmetrisch polynoom met de methode uit het bewijs van 14.1 schrijven als veelterm in de s_k's, dan is de korte notatie vaak nuttig. Immers, als in een symmetrisch polynoom $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ een monoom $rT_1^{e_1}T_2^{e_2}\ldots T_n^{e_n}$ voorkomt, dan komt ook $\sum_n rT_1^{e_1}T_2^{e_2}\ldots T_n^{e_n}$ voor.

14.3. Voorbeelden. 1. Neem $n \geq 2$ en $P = T_1^2 + T_2^2 + \ldots + T_n^2 = \sum_n T_1^2$. Dan is T_1^2 de lexicografisch hoogste term in P, dus we vormen

$$s_1^2 = (T_1 + T_2 + \ldots + T_n)^2 = \sum_n T_1^2 + 2\sum_n T_1T_2$$

en berekenen $P_1 = P - s_1^2 = -2\sum_n T_1T_2 = -2s_2$. In dit geval zijn we na 1 stap klaar, en vinden we $P = s_1^2 - 2s_2$. Merk op dat P homogeen van graad 2 is, en $s_1^2 - 2s_2$ isobarisch van gewicht 2.

2. Neem nu $n \geq 3$ en $P = T_1^3 + T_2^3 + \ldots + T_n^3 = \sum_n T_1^3$. Dan is T_1^3 de lexicografisch hoogste term in P, dus we vormen

$$s_1^3 = (T_1 + T_2 + \ldots + T_n)^3 = \sum_n T_1^3 + 3\sum_n T_1^2T_2 + 6\sum_n T_1T_2T_3.$$

De coëfficiënten 3 en 6 die hierbij optreden geven aan hoe vaak een term bij het uitwerken van s_1^3 optreedt. We vinden $P_1 = P - s_1^3 = -3\sum_n T_1^2T_2 - 6\sum_n T_1T_2T_3$. De lexicografisch hoogste term in P_1 is $-3T_1^2T_2$, dus we trekken -3 maal

$$s_1s_2 = \sum_n T_1 \cdot \sum_n T_1T_2 = \sum_n T_1^2T_2 + 3\sum_n T_1T_2T_3$$

af en krijgen

$$P_2 = P_1 + 3s_1s_2 = P - s_1^3 + 3s_1s_2 = 3\sum_n T_1T_2T_3 = 3s_3.$$

Conclusie: $P = T_1^3 + T_2^3 + \ldots + T_n^3 = s_1^3 - 3s_1s_2 + 3s_3$. Merk weer op dat P homogeen van graad 3 is, en $s_1^3 - 3s_1s_2 + 3s_3$ isobarisch van gewicht 3.

Opgave 2. Wat gebeurt er in de gevallen $n < 2$ (in 1) en $n < 3$ (in 2)?

Zie opgave 23 voor de representatie van de *machtssom* $\sigma_k = T_1^k + T_2^k + \ldots + T_n^k$ in termen van de elementaire symmetrische polynomen met behulp van de *Newtonidentiteiten*.

▶ Discriminant

Een veel voorkomend symmetrisch polynoom in $\mathbf{Z}[T_1, T_2, \ldots, T_n]$ is de *discriminant*

$$\Delta_n = \prod_{1 \le i < j \le n} (T_i - T_j)^2 \tag{14.4}$$

van het algemene polynoom F_n van graad n. Het polynoom Δ_n is homogeen van graad $n(n-1)$, dus wegens 14.2 is Δ_n een universele isobarische uitdrukking van gewicht $n(n-1)$ in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. In andere woorden: de discriminant van het algemene polynoom F_n van graad n is een veelterm in de coëfficiënten $(-1)^{n-k}s_k$ van F_n.

Na het oninteressante geval $\Delta_1 = 1$ hebben we

$$\Delta_2 = (T_1 - T_2)^2 = (T_1 + T_2)^2 - 4T_1T_2 = s_1^2 - 4s_2,$$

een resultaat dat ook wel genoteerd wordt als $\Delta(X^2 + AX + B) = A^2 - 4B$. Met de methode van 14.1 kan men in principe Δ_n uitdrukken in de elementaire symmetrische polynomen, en met enige vlijt vindt men zo

$$\Delta_3 = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2 + 18s_1s_2s_3$$
$$\Delta_4 = \frac{1}{27}\left(4(s_2^2 - 3s_1s_3 + 12s_4)^3 - (2s_2^3 - 72s_2s_4 + 27s_1^2s_4 - 9s_1s_2s_3 + 27s_3^2)^2\right),$$

formules die te onaantrekkelijk zijn om te onthouden. Voor grotere waarden van n zijn ze ook nog eens te onaantrekkelijk om op te schrijven.

Opgave 3. Ga na dat Δ_4 in $\mathbf{Z}[s_1, s_2, s_3, s_4]$ ligt.

Zij nu A een willekeurig domein en $f \in A[X]$ een monisch polynoom van graad n. Dan heeft n wegens 12.3 ten hoogste n nulpunten in A, en we zullen in 21.13 bewijzen dat het aantal nulpunten van f in een voldoende groot domein $A' \supset A$ *precies* n is in de zin dat

$$f = \prod_{i=1}^{n}(X - \alpha_i)$$

geldt met $\alpha_i \in A'$. Is A een deelring van $\mathbf{C}$, zoals $\mathbf{Z}$, $\mathbf{Q}$ of $\mathbf{R}$, dan kan men wegens de hoofdstelling van de algebra 26.3 altijd $A' = \mathbf{C}$ nemen. De discriminant van f is nu gedefinieerd als

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2. \tag{14.5}$$

Omdat A' een domein is hebben we $\Delta(f) = 0$ dan en slechts dan als f een dubbel nulpunt heeft in A'.

Het homomorfisme $\mathbf{Z}[T_1, T_2, \ldots, T_n] \to A'$ dat T_i naar α_i stuurt, beeldt Δ_n op $\Delta(f)$ af. Omdat de beelden van de elementaire symmetrische polynomen s_k, die naar (plus of min) de coëfficiënten van f gaan, in A bevat zijn, zien we dat $\Delta(f)$ óók een

element van A is. Met andere woorden: de discriminant van een polynoom $f \in A[X]$ is een element van A, en wordt gegeven door een universeel polynoom in de coëfficiënten van f.

Voorbeeld. De algemene formule voor de discriminant van een cubisch polynoom is lastig te onthouden, maar de bekende formule

$$\Delta(X^3 + pX + q) = -4p^3 - 27q^2 \tag{14.6}$$

die ontstaat door $(s_1, s_2, s_3) = (0, p, -q)$ in de algemene uitdrukking voor Δ_3 te substitueren is zowel onthoudbaar als gemakkelijk afleidbaar. Immers, door $A = \mathbf{Z}[p, q]$ te nemen weten we dat de discriminant een universeel polynoom in p en q is. Omdat er maar twee monomen in $\mathbf{Z}[s_2, s_3]$ van gewicht $3(3-1) = 6$ zijn, namelijk s_2^3 en s_3^2, bestaan er in feite constanten $c_1, c_2 \in \mathbf{Z}$ zodat $\Delta(X^3 + pX + q) = c_1 p^3 + c_2 q^2$ geldt. Men berekent c_1 en c_2 gemakkelijk door voor p en q een paar geschikte waarden te kiezen. Er geldt namelijk $c_1 = -\Delta(X^3 - X) = -4$ en $c_2 = \Delta(X^3 - 1) = -27$.

Opgave 4. Ga dit na.

▶ Resultante

Om discriminanten van polynomen van hogere graad in $A[X]$ te berekenen maakt men meestal geen gebruik van de algemene formules voor Δ_n, maar van de *resultante*. Om onbeperkt te kunnen delen vervangen we het domein A zo nodig door zijn quotiëntenlichaam, en nemen verder aan dat $A = K$ een *lichaam* is. Voor polynomen

$$f = a\prod_{i=1}^{n}(X - \alpha_i) \qquad \text{en} \qquad g = b\prod_{j=1}^{m}(X - \beta_j)$$

in $K[X]$ van graad respectievelijk n en m is de resultante $R(f, g)$ gedefinieerd door

$$R(f, g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j). \tag{14.7}$$

Uit deze definitie volgen direct de volgende eigenschappen:

(R1) $R(f, g) = (-1)^{mn} R(g, f)$;
(R2) $R(f, g) = a^m \prod_{i=1}^{n} g(\alpha_i)$;
(R3) is $g_1 \in K[X]$ van graad m_1 met $g \equiv g_1 \bmod (f)$, dan geldt $R(f, g) = a^{m-m_1} R(f, g_1)$.

Met behulp van deze eigenschappen en de deling met rest in $K[X]$ kan men resultantes berekenen *zonder* ooit gebruik te maken van enige expliciete kennis van de nulpunten α_i en β_j die in de definitie voorkomen. Men kan door zo nodig (R1) te gebruiken bereiken dat $\deg(g) \geq \deg(f)$ geldt, en vervolgens g vervangen met behulp van (R3) door de rest $g_1 \in A[X]$ bij deling van g door f. Herhalen van deze stappen leidt tot verlaging

van de graad van de polynomen, en zodra f graad 0 of 1 heeft en men de nulpunten $\alpha_i \in A$ kent, geeft (R2) de waarde van de resultante.

Voor een monisch polynoom $f = \prod_{i=1}^{n}(X - \alpha_i)$ is de afgeleide in een nulpunt α_i gelijk aan

$$f'(\alpha_i) = (\alpha_i - \alpha_1)(\alpha_i - \alpha_2)\dots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\dots(\alpha_i - \alpha_n).$$

Neemt men het product van deze uitdrukkingen voor $i = 1, 2, \dots, n$ dan volgt na telling van een aantal factoren -1

$$\Delta(f) = (-1)^{n(n-1)/2} R(f, f'). \tag{14.8}$$

Met behulp van de resultante kan men zo discriminanten van polynomen in $K[X]$ berekenen.

14.9. Voorbeeld. 1. Neem $K = \mathbf{Q}(p, q)$ en $f = X^3 + pX + q$. Dan geldt

$$\Delta(X^3 + pX + q) = -R(X^3 + pX + q, 3X^2 + p).$$

Passen we hierop (R1) en vervolgens (R3) toe voor $f = 3X^2 + p$, $g = X^3 + pX + q$ en $g_1 = g - (X/3)f = (2p/3)X + q$, dan wordt dit $-3^2 \cdot R(3X^2 + p, (2p/3)X + q)$. Passen we nogmaals (R1) toe en bedenken we dat g_1 een enkel nulpunt $\alpha = -3q/(2p)$ heeft, dan geeft (R2) in overeenstemming met (14.6)

$$\Delta(X^3 + pX + q) = -3^2 \cdot \left(\frac{2p}{3}\right)^2 \left[3\left(\frac{-3q}{2p}\right)^2 + p\right] = -4p^3 - 27q^2.$$

2. Neem $K = \mathbf{Q}$ en $f = X^5 + X + 1$. Dan geldt

$$\begin{aligned}\Delta(X^5 + X + 1) &= R(X^5 + X + 1, 5X^4 + 1) = R(5X^4 + 1, X^5 + X + 1)\\ &= 5^4 \cdot R(5X^4 + 1, \frac{4}{5}X + 1)\\ &= 5^4 \cdot (\frac{4}{5})^4 \cdot [5 \cdot (\frac{-5}{4})^4 + 1] = 5^5 + 4^4 = 3381.\end{aligned}$$

Omdat f irreducibel is in $\mathbf{Z}[X]$ liggen de complexe nulpunten van f niet in $\mathbf{Z}$ of $\mathbf{Q}$, en het is dan ook niet gemakkelijk om ze 'expliciet' aan te geven. Voor de berekening van de discriminant is dit ook in het geheel niet nodig.

OPGAVEN.

5. Stel dat $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ invariant is onder iedere verwisseling $T_i \leftrightarrow T_j$ van twee variabelen. Is f noodzakelijkerwijs symmetrisch?

6. Laat α_1, α_2 en α_3 de nulpunten van $X^3 - X - 1$ in $\mathbf{C}$ zijn, en definieer $p_k = \alpha_1^k + \alpha_2^k + \alpha_3^k$ voor alle $k \in \mathbf{Z}$. Bewijs: de rij $\{p_k\}_{k \in \mathbf{Z}}$ bestaat uit gehele getallen die voldoen aan $p_{-1} = -1$, $p_0 = 3$, $p_1 = 0$ en de recurrentie $p_k = p_{k-2} + p_{k-3}$ voor $k \in \mathbf{Z}$.

7. Laat zien: voor $f \in \mathbf{Z}[T_1, T_2, \ldots, T_n]$ homogeen van graad d en $r \in \mathbf{Z}$ geldt

$$f(rT_1, rT_2, \ldots, rT_n) = r^d f(T_1, T_2, \ldots, T_n).$$

   Is omgekeerd f homogeen van graad d als deze identiteit geldt voor alle $r \in \mathbf{Z}$?

8. Geef een voorbeeld van een ring A en een niet-homogeen polynoom $f \in A[T_1, T_2, \ldots, T_n]$ dat voor zekere $d \geq 1$ voldoet aan $f(rT_1, rT_2, \ldots, rT_n) = r^d f(T_1, T_2, \ldots, T_n)$ voor alle $r \in A$.

9. Laat zien dat er precies $\binom{n+d-1}{n-1}$ verschillende monomen $T_1^{e_1} T_2^{e_2} \ldots T_n^{e_n}$ van graad d bestaan.

10. Druk de symmetrische polynomen $\sum_n T_1^2 T_2$ en $\sum_n T_1^3 T_2$ uit in de elementaire symmetrische polynomen.

11. Laat zien dat de baan van het polynoom $B = T_1T_2 + T_3T_4 \in \mathbf{Z}[T_1, T_2, T_3, T_4]$ onder de actie van S_4 uit 3 elementen B, B' en B'' bestaat, en bepaal het cubische polynoom in $\mathbf{Z}[s_1, s_2, s_3, s_4][X]$ met deze drie nulpunten.

12. Laat zien dat de discriminant van het cubische polynoom uit de vorige opgave gelijk is aan de discriminant Δ_4 van het algemene polynoom van graad 4, en gebruik dit om $\Delta_4 \in \mathbf{Z}[s_1, s_2, s_3, s_4]$ te bepalen.

13. Laat zien dat de resultante van de polynomen $f = \sum_{i=0}^{n} a_i X^i$ en $g = \sum_{j=0}^{m} b_j X^j$ van graad n en m in $K[X]$ gelijk is aan de $(m+n) \times (m+n)$-determinant

$$\begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} m \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \end{array} \left|\begin{array}{cccccc} a_n & a_{n-1} & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & a_0 & \\ & & & \ddots & & \\ & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & \\ & b_m & b_{m-1} & \cdots & b_0 & \\ & & & \ddots & & \\ & & b_m & b_{m-1} & \cdots & b_0 \end{array}\right| \quad \overbrace{\qquad\qquad}^{m+n}$$

   in termen van de coëfficiënten van f en g. (Neem alle niet ingevulde coëfficiënten gelijk aan 0.)
   [Hint: laat zien dat deze determinant ook de eigenschappen (R1) en (R3) heeft.]

14. Bewijs: voor $n \in \mathbf{Z}_{>0}$ geldt $\Delta(X^n + a) = (-1)^{\frac{1}{2}n(n-1)} n^n a^{n-1}$.

15. Bereken de discriminant van het polynoom $X^4 + pX + q \in \mathbf{Q}(p, q)[X]$.

16. Vind voor elke $n > 1$ een uitdrukking voor de discriminant van het polynoom $X^n + pX + q \in \mathbf{Q}(p, q)[X]$.

17. Zij $f \in \mathbf{Z}[X]$ een monisch polynoom. Bewijs dat equivalent zijn:
    a. $\Delta(f) \neq 0$;
    b. f heeft geen dubbele nulpunten in $\mathbf{C}$;
    c. de ontbinding van f in $\mathbf{Q}[X]$ heeft geen meervoudige priemfactoren;
    d. f en zijn afgeleide f' zijn copriem in $\mathbf{Q}[X]$;
    e. $f \bmod p$ en $f' \bmod p$ zijn copriem in $\mathbf{F}_p[X]$ voor bijna alle priemen p.

18. Bepaal de 'uitzonderingspriemen' in onderdeel (e) van de vorige opgave voor $f = X^3 + X + 1$ en voor het polynoom $X^7 + 7X + 1$ uit opgave 12.17.

19. Zij $f \in \mathbf{Q}[X]$ een monisch polynoom met $n = \deg(f)$ verschillende complexe nulpunten. Bewijs: het *teken* van $\Delta(f)$ is gelijk aan $(-1)^s$, met $2s$ het aantal niet-reële nulpunten van f.

20. Bewijs: $X^3 + pX + q \in \mathbf{R}[X]$ heeft drie (met multipliciteit getelde) reële nulpunten $\iff 4p^3 + 27q^2 \leq 0$.

21. Druk de machtssom $\sum_n T_1^4$ uit in de elementaire symmetrische polynomen. Is de waarde van n hierbij van belang?

22. Een rationale functie $f \in \mathbf{Q}(T_1, T_2, \ldots, T_n)$ heet symmetrisch als hij invariant is onder permutaties van de variabelen T_i. Bewijs dat iedere symmetrische rationale functie een rationale functie in de elementaire symmetrische functies is.

23. Schrijf $\sum_n T_1^{-1}$ en $\sum_n T_1^{-2}$ als rationale functies in $\mathbf{Q}(s_1, s_2, \ldots, s_n)$.

24. *(Newtonidentiteiten)* Laat zien dat de machtssommen $\sigma_k = \sum_n T_1^k$ voldoen aan

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \ldots + (-1)^{k-1} s_{k-1}\sigma_1 + (-1)^k k s_k = 0 \quad \text{voor } 1 \leq k \leq n,$$

    en dat hiermee de machtssommen σ_k voor $1 \leq k \leq n$ inductief als polynomen in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$ geschreven kunnen worden. Laat ook zien dat voor $k > n$ de machtssom σ_k als polynoom in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$ gevonden kan worden uit de relatie

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \ldots + (-1)^n s_n\sigma_{k-n} = 0.$$

    [Hint: bepaal de logaritmische afgeleide $f'/f \in R[[X]]$ van $f = \prod_{i=1}^n (1 - T_i X) \in R[X]$.]

25. Kan men met de methode van de vorige opgave ook de machtssommen σ_k voor $k < 0$ vinden als elementen van $\mathbf{Q}(s_1, s_2, \ldots, s_n)$?

26. Laat zien dat de discriminant Δ_n in termen van de machtssommen σ_k uitgedrukt wordt door

$$\Delta_n = \det(\sigma_{i+j-2})_{i,j=1}^n.$$

    Gebruik deze relatie om $\Delta_3 \in \mathbf{Z}[s_1, s_2, s_3]$ te berekenen.
    [Hint: ga uit van de Vandermonde-determinant $\det(T_i^{j-1})_{i,j=1}^n$.]

27. Laat zien dat de discriminant $\Delta_n \in \mathbf{Z}[s_1, s_2, \ldots, s_n]$ van het algemene polynoom van graad n een irreducibel polynoom is in $\mathbf{Z}[s_1, s_2, \ldots, s_n]$. Is Δ_n ook irreducibel in de ring $\mathbf{C}[s_1, s_2, \ldots, s_n]$?

15 De meetkunde van commutatieve ringen

In de *algebraïsche meetkunde*, waar men oplossingsverzamelingen van stelsels polynoomvergelijkingen bestudeert, spelen de polynoomringen $R = K[X_1, X_2, \ldots, X_n]$ over een lichaam K uit paragraaf 13 een hoofdrol. Ieder polynoom in R geeft aanleiding tot een functie $K^n \to K$, en gegeven een k-tal elementen $f_1, f_2, \ldots, f_k \in R$ zijn we geïnteresseerd in hun gemeenschappelijke nulverzameling ('zero locus')

$$Z(f_1, f_2, \ldots, f_k) = \{x \in K^n : f_1(x) = f_2(x) = \ldots = f_k(x) = 0\}.$$

Zo'n verzameling heet een *algebraïsche verzameling* in K^n. Merk op dat de punten $x \in K^n$ in de definitie n-tupels $x = (x_1, x_2, \ldots, x_n)$ met coördinaten in K zijn. Is $I = (f_1, f_2, \ldots, f_k) \subset R$ het ideaal voortgebracht door de polynomen f_i, dan geldt

$$Z(f_1, f_2, \ldots, f_k) = Z(I) = \{x \in K^n : \quad f(x) = 0 \quad \text{voor alle } f \in I\},$$

want ieder element van de vorm $g_1 f_1 + g_2 f_2 + \ldots + g_n f_n \in I$ met $g_i \in R$ neemt in $x \in Z(f_1, f_2, \ldots, f_k)$ de waarde 0 aan. Kennelijk hangt $Z(I)$ slechts van het ideaal $I \subset R$ af, en niet van de gekozen voortbrengers. Omdat polynomen uit R die een element van I verschillen dezelfde waarden aannemen op $Z(I)$, kunnen we de quotiëntring R/I opvatten als de *ring van polynomiale functies* op de algebraïsche verzameling $Z(I)$.

Opgave 1. Laat zien dat eindige doorsnedes van algebraïsche verzamelingen weer algebraïsch zijn.

15.1. Voorbeelden. We nemen $K = \mathbf{R}$ en kiezen $f_1 = X^2 + Y^2 - 1$ en $f_2 = XY - 1$ in $R = \mathbf{R}[X, Y]$. Dan is $Z(f_1)$ de *eenheidscirkel* in het platte vlak, en $R/(f_1)$ de ring van polynomiale functies op de eenheidscirkel. Op soortgelijke manier is $R/(f_2)$ de ring van polynomiale functies op de 'eenheidshyperbool'. Ringtheoretisch zijn dit domeinen die in diverse opzichten van $\mathbf{R}[X, Y]$ en van elkaar verschillen: zie de opgaven 18–20.

Opgave 2. Zij K een *oneindig* lichaam. Bewijs dat verschillende polynomen in $R = K[X_1, X_2, \ldots, X_n]$ niet tot dezelfde functie $K^n \to K$ aanleiding geven. Vind $I \subset R$ en verschillende elementen in R/I die dezelfde waarden op $Z(I)$ aannemen.

Naast de zojuist voor $R = K[X_1, X_2, \ldots, X_n]$ gedefinieerde afbeelding

$$\begin{aligned} \{\text{idealen van } R\} &\longrightarrow \{\text{algebraïsche verzamelingen in } K^n\} \\ I &\longmapsto Z(I) \end{aligned}$$

is er ook een afbeelding in de omgekeerde richting, die aan $V \subset K^n$ een ideaal

$$I(V) = \{f \in R : \quad f(x) = 0 \quad \text{voor alle } x \in V\} \subset R$$

toevoegt. Deze beide fundamentele afbeeldingen worden in de algebraïsche meetkunde gebruikt om een compleet woordenboek tussen meetkunde en algebra op te zetten, waarbij de *meetkundige* eigenschappen van $Z(I)$ verband houden met de *algebraïsche* eigenschappen van de ring R/I. Dit is het eenvoudigst als K een *algebraïsch afgesloten*

lichaam is; dit betekent dat ieder niet-constant polynoom in de polynoomring $K[X]$ in één variabele over K in een product van lineaire factoren ontbindt. Wegens de al genoemde hoofdstelling van de algebra 26.3 is $K = \mathbf{C}$ zo'n lichaam.

Opgave 3. Bewijs de implicaties $I_1 \subset I_2 \Rightarrow Z(I_1) \supset Z(I_2)$ en $V_1 \subset V_2 \Rightarrow I(V_1) \supset I(V_2)$.

Van de zee van resultaten die de algebraïsche meetkunde ons geeft kunnen wij hier slechts een klein slokje nemen. We gaan, in het geval van het algebraisch afgesloten grondlichaam $K = \mathbf{C}$, aan de hand van laag-dimensionale voorbeelden in op het verband tussen *punten* van Z en *maximale idealen* van R/I, en definiëren een *dimensie* voor willekeurige commutatieve ringen. Hierop voortbordurende komen we tot het moderne inzicht dat *iedere* commutatieve ring R als een 'functiering' op een bijbehorende ruimte kan worden opgevat, het *spectrum* $\mathrm{Spec}(R)$ van de ring.

▶ Het affiene vlak

Deze sectie moet eigenlijk *Het complexe affiene vlak* heten, maar omdat we overal in deze sectie aannemen dat $\mathbf{C}$ ons grondlichaam is, zullen we niet alle objecten voortdurend van het adjectief 'complex' voorzien.

De polynoomring in n variabelen over $\mathbf{C}$ is de ring van polynomiale functies op de *affiene n-dimensionale ruimte* $\mathbf{A}^n(\mathbf{C}) = \mathbf{C}^n$ *over* $\mathbf{C}$. De toevoeging 'affien' onderscheidt deze ruimte van de hier niet beschouwde *projectieve n-dimensionale ruimte* $\mathbf{P}^n(\mathbf{C})$ *over* $\mathbf{C}$, die door 'completering' uit $\mathbf{C}^n$ verkregen kan worden.[11]

De *affiene lijn* $\mathbf{A}^1(\mathbf{C}) = \mathbf{C}$ heeft als functiering de polynoomring $\mathbf{C}[X]$ in één variabele, die wegens 12.6 een hoofdideaaldomein is. Ieder ideaal $I \subset \mathbf{C}[X]$ is van de vorm $I = (f)$, en de nulverzameling $Z(I)$ is de verzameling van nulpunten van f. Voor de triviale idealen $I = 0$ en $I = \mathbf{C}[X]$ hebben we $f = 0$ en $f = 1$, en de algebraïsche verzameling $Z(I)$ is dan respectievelijk gelijk aan $\mathbf{C}$ en leeg. In de andere gevallen is I wegens de keuze $K = \mathbf{C}$ het product van een eindig aantal priemidealen van de vorm $(X - a) \subset \mathbf{C}[X]$ met $a \in \mathbf{C}$. Ieder priemideaal $(X - a)$ dat f deelt, draagt een punt a bij aan de verzameling $Z(I)$. In het 'irreducibele geval' dat $I = (X - a)$ zelf priem is hebben we $Z(I) = \{a\}$, en de quotiëntafbeelding $\mathbf{C}[X] \to \mathbf{C}[X]/I \cong \mathbf{C}$ is de evaluatie-afbeelding uit 11.16 die een polynoom $f \in \mathbf{C}[X]$ naar zijn waarde in a stuurt.

15.2. Definitie. *Een irreducibele algebraïsche verzameling of affiene algebraïsche variëteit over* $\mathbf{C}$ *is een niet-lege algebraïsche verzameling* $Z \subset \mathbf{A}^n(\mathbf{C})$ *die niet te schrijven is als een vereniging* $Z = Z_1 \cup Z_2$ *van algebraïsche verzamelingen* $Z_i \subsetneq Z$.

Kortheidshalve zullen wij in deze paragraaf verder over variëteiten praten als we complexe affiene algebraïsche variëteiten bedoelen. Variëteiten in $\mathbf{A}^1(\mathbf{C})$ zijn niet erg opwindend.

Opgave 4. Bewijs: een variëteit in $\mathbf{A}^1(\mathbf{C})$ is een punt of $\mathbf{A}^1(\mathbf{C})$ zelf.

Het geval van variëteiten in het complexe affiene vlak $\mathbf{A}^2(\mathbf{C})$, ook wel *vlakke variëteiten* genoemd, is minder triviaal. We hebben hier te maken met de polynoomring $\mathbf{C}[X, Y]$ in twee variabelen. Dit is geen hoofdideaaldomein, maar wegens 13.3 wel een ontbindingsring.

Ieder punt $(a,b) \in \mathbf{A}^2(\mathbf{C})$ is een variëteit; de bijbehorende evaluatie-afbeelding $f \mapsto f(a,b)$ is (opgave 11.35) een surjectie $\mathbf{C}[X,Y] \to \mathbf{C}$ met kern $(X-a, Y-b)$, en de ring $\mathbf{C}[X,Y]/(X-a,Y-b)$ van polynomiale functies in (a,b) is isomorf met $\mathbf{C}$.

Beduidend interessanter zijn de nulverzamelingen $Z(f)$ van een niet-constant polynoom $f \in \mathbf{C}[X,Y]$, die *vlakke algebraïsche krommen* heten en in deze sectie verder kortweg krommen worden genoemd. Is f irreducibel, dan spreken we van een *irreducibele kromme*. Ieder niet-constant polynoom in de ontbindingsring $\mathbf{C}[X,Y]$ is te schrijven als een product $\prod_{i=1}^{t} p_i^{e(i)}$ met paarsgewijs niet-geassocieerde irreducibele polynomen p_i, dus iedere kromme is een eindige vereniging $\bigcup_{i=1}^{t} Z(p_i)$ van irreducibele krommen.

Opgave 5. Laat zien dat een vlakke kromme in $\mathbf{A}^2(\mathbf{C})$ oneindig veel punten heeft, en dat $\mathbf{A}^2(\mathbf{C})$ geen eindige vereniging van vlakke krommen is.

We gaan bewijzen dat irreducibele krommen variëteiten zijn. Eerst laten we zien dat verschillende irreducibele krommen elkaar in slechts eindig veel punten doorsnijden.

15.3. Lemma. *Laat f en g onderling ondeelbare polynomen in $\mathbf{C}[X,Y]$ zijn. Dan is $Z(f,g)$ een eindige verzameling.*

Bewijs. Vatten we f en g op als polynomen in Y met coëfficiënten in $\mathbf{C}[X]$, dan zijn f en g wegens de voor 13.5 gemaakte opmerking ook onderling ondeelbaar als polynomen in het hoofdideaaldomein $\mathbf{C}(X)[Y]$ van polynomen in Y over het lichaam $\mathbf{C}(X)$ van rationale functies in X. In deze laatste ring hebben we $r_1 f + r_2 g = 1$ voor $r_i \in \mathbf{C}(X)[Y]$. Door met een veelvoud van de noemers van de coëfficiënten van r_1 en r_2 te vermenigvuldigen zien we dat het ideaal $(f,g) \subset \mathbf{C}[X,Y]$ een polynoom $h \in \mathbf{C}[X]$ bevat verschillend van nul. Voor ieder punt $(x,y) \in Z(f,g)$ geldt $h(x) = 0$, en dit laat zien dat er maar eindig veel mogelijkheden voor x zijn. Op symmetriegronden zijn er ook maar eindig veel mogelijkheden voor y, dus $Z(f,g)$ is eindig. □

15.4. Stelling. *Iedere algebraïsche verzameling in $\mathbf{C}^2$ is een eindige vereniging van variëteiten; deze variëteiten zijn de punten, de irreducibele krommen en het vlak $\mathbf{C}^2$ zelf. De afbeelding $I \mapsto Z(I)$ induceert een bijectie tussen de priemidealen van $\mathbf{C}[X,Y]$ en de irreducibele algebraïsche verzamelingen in $\mathbf{A}^2(\mathbf{C})$.*

Bewijs. Zij $Z(I)$ een vlakke algebraïsche verzameling. Voor $I = (0)$ geldt $Z(I) = \mathbf{C}^2$. Voor $I \neq 0$ bestaat er $f \neq 0$ in I, en geldt $Z(I) \subset Z(f)$. Schrijven we de kromme $Z(f)$ als een eindige vereniging $\bigcup_{i=1}^{n} Z(p_i)$ van irreducibele krommen, dan vinden we

$$Z(I) = \bigcup_{i=1}^{n} \left(Z(I) \cap Z(p_i) \right).$$

Voor ieder van de algebraïsche verzamelingen $Z(I) \cap Z(p_i)$ zijn er twee mogelijkheden. Zijn alle elementen van I deelbaar door p_i, dan is $Z(I) \cap Z(p_i) = Z(p_i)$ een irreducibele kromme. Is dit niet zo, dan bevat I een element dat onderling ondeelbaar is met p_i en is $Z(I) \cap Z(p_i)$ een eindige verzameling wegens 15.3. We concluderen dat iedere vlakke algebraïsche verzameling een eindige vereniging is van verzamelingen die gelijk zijn aan $\mathbf{C}^2$, een irreducibele kromme of een punt.

Punten in het vlak zijn duidelijk irreducibele algebraïsche verzamelingen, en hetzelfde geldt voor het vlak $\mathbf{C}^2$ zelf (opgave 5). Om in te zien dat een irreducibele kromme $Z(p)$ behorende bij een irreducibel polynoom p ook een irreducibele algebraïsche verzameling is, merken we op dat ieder polynoom dat identiek 0 is op $Z(p)$ wegens 15.3 (en opgave 5) deelbaar is door p. Bovendien is het irreducibele element p in de ontbindingsring $\mathbf{C}[X,Y]$ een priemelement. Geldt nu $Z(p) = Z(I_1) \cup Z(I_2)$, dan zijn alle elementen van $I_1 I_2$ deelbaar door p. Er volgt dat I_1 en I_2 niet beide een element kunnen bevatten dat niet door p deelbaar is – het product van deze elementen is namelijk wel deelbaar door het priemelement p – en we vinden zoals gewenst dat $Z(I_1)$ of $Z(I_2)$ gelijk is aan $Z(p)$. Hiermee zijn de twee eerste uitspraken van 15.4 bewezen.

Het vlak $\mathbf{C}^2$ is de nulverzameling van het nulideaal (0), dat priem is in het domein $\mathbf{C}[X,Y]$. Een irreducibele kromme is per definitie de nulverzameling van een priemideaal (p) voortgebracht door een irreducibel polynoom p. Een punt (a,b) is de nulverzameling van het ideaal $(X-a, Y-b)$ dat, als kern van de evaluatie-afbeelding $\mathbf{C}[X,Y] \to \mathbf{C}$ in het punt (a,b), eveneens priem is.

Zij omgekeerd $P \subset \mathbf{C}[X,Y]$ een priemideaal. Geldt $P \neq (0)$, dan bevat P een polynoom $f \neq 0$, en wegens $P \neq \mathbf{C}[X,Y]$ is f niet constant. Als we f als product van irreducibele elementen schrijven, dan volgt uit de priemideaal-eigenschap 12.14 dat P een irreducibel polynoom p bevat. Is p een voortbrenger van P, dan hoort P bij de irreducibele kromme $Z(p)$. Is p geen voortbrenger van P, dan bevat P een element dat copriem is met p en volgt als in het bewijs van 15.3 dat P niet-constante polynomen in zowel X als Y bevat. Ontbinden we deze over $\mathbf{C}$ in lineaire factoren, dan volgt, weer wegens de priemeigenschap, dat P een ideaal van de vorm $(X-a, Y-b)$ bevat. Omdat $\mathbf{C}[X,Y]/(X-a,Y-b) \cong \mathbf{C}$ geen niet-triviale idealen bevat, is P niet strikt groter dan $(X-a,Y-b)$ (opgave 11.51), dus $P = (X-a,Y-b)$ hoort bij het punt (a,b). □

Opgave 6. Bewijs: iedere vlakke algebraïsche verzameling is *uniek* te schrijven als eindige vereniging van vlakke variëteiten die elkaar niet bevatten.

De algebraïsche stelling 15.4 verwoordt het meetkundige feit dat er 3 types van vlakke variëteiten zijn: punten, krommen en het vlak zelf. De basisstellingen uit de algebraïsche meetkunde laten zien dat het analogon van 15.4 voor willekeurige dimensie $n \geq 1$ geldt: iedere algebraïsche verzameling in $\mathbf{A}^n(\mathbf{C})$ is een eindige vereniging van algebraïsche variëteiten, en iedere algebraïsche variëteit $V \subset \mathbf{A}^n(\mathbf{C})$ is de nulverzameling van een corresponderend *priemideaal* $P = I(V) \subset R = \mathbf{C}[X_1, X_2, \ldots, X_n]$. De bewijzen van deze stellingen vereisen meer ringtheorie dan wij hier behandelen.[12]

Voor een variëteit V is de bijbehorende ring $R/I(V)$ van polynomiale functies op V een domein, de *coördinatenring* R_V van V. Alle 'meetkundige' eigenschappen van V, zoals de dimensie van V of het 'glad' zijn van de punten van V, laten zich formuleren in termen van de coördinatenring R_V.

Opgave 7. Laat zien dat er een natuurlijke correspondentie is tussen de punten van de 'eenheidscirkel' $V = Z(X^2+Y^2-1) \subset \mathbf{A}^2(\mathbf{C})$ en de priemidealen $P \neq 0$ van $R_V = \mathbf{C}[X,Y]/(X^2+Y^2-1)$.

Algebraïsch-meetkundige karakteriseringen laten zich vaak generaliseren naar andere grondlichamen dan $\mathbf{C}$, en men kan in 15.4 voor $\mathbf{C}$ een willekeurig algebraïsch afgesloten

lichaam nemen. De meetkunde over niet algebraïsch afgesloten lichamen als $\mathbf{Q}$ of $\mathbf{F}_p$, die wel *aritmetische algebraïsche meetkunde*[13] wordt genoemd, is vaak aanzienlijk gecompliceerder. Deze meetkunde vormt een grensgebied tussen getaltheorie en meetkunde dat tegenwoordig erg in de belangstelling staat. Anders dan in de klassieke meetkunde kan men hier veel moeilijker bewijzen aan 'plaatjes' ontlenen.

▶ Dimensie

We geven een voorbeeld van een algebraïsche karakterisering van een meetkundig begrip aan de hand van het begrip *dimensie*. Intuïtief is duidelijk dat variëteiten in het affiene vlak, die wegens 15.4 het hele vlak, een vlakke irreducibele kromme of een punt in het vlak zijn, dimensie respectievelijk 2, 1 en 0 hebben. Omdat bij inclusies van variëteiten van het type punt–kromme–vlak de dimensie steeds stijgt, ligt het voor de hand de dimensie van een variëteit V 'meetkundig' te definiëren in termen van maximale lengtes van rijtjes van 'geschakelde deelvariëteiten' van V. Met andere woorden: $V \subset \mathbf{A}^n(\mathbf{C})$ heeft dimensie $\dim(V) = d$ als er een strikt stijgend rijtje $V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_d = V$ van variëteiten $V_i \subset V$ van *lengte* d bestaat, maar geen rijtje van lengte groter dan d.

Interpreteren we bovenstaand rijtje in termen van inclusies van priemidealen in de ring $R = \mathbf{C}[X_1, X_2, \ldots, X_n]$, dan zien we dat $\dim(V)$ de maximale lengte is van een dalend rijtje $P_0 \supsetneq P_1 \supsetneq \ldots \supsetneq P_d = I(V)$ van priemidealen $P_i \subset R$ die $I(V)$ omvatten. Vatten we de priemidealen P_i onder de correspondentie van opgave 11.51 op als priemidealen van de coördinatenring $R_V = R/I(V)$ van V, dan is de dimensie van V niets anders dan de maximale lengte van een *keten* van priemidealen in R_V. Een keten van idealen van lengte d in een ring is per definitie een collectie $\{I_k\}_{k=0}^{d}$ van idealen waarvoor strikte inclusies $I_0 \subsetneq I_1 \subsetneq \ldots \subsetneq I_d$ gelden.

15.5. Definitie. *De dimensie* $\dim(R)$ *van een commutatieve ring* R *is het supremum van de lengtes van de ketens van priemidealen in* R*.*

Met deze definitie is de dimensie van een affiene variëteit gelijk aan de dimensie van zijn coördinatenring R_V. De dimensie in 15.5, die naar de Duitse algebraïcus Wolfgang Krull (1899–1971) wel de *Krull-dimensie* van R heet, is echter van een *veel* algemenere aard dan onze 'meetkundige' dimensie, die alleen in de context van variëteiten over algebraïsch afgesloten lichamen betekenis heeft. Immers, *iedere* commutatieve ring die een priemideaal bezit krijgt met 15.5 een dimensie. Dat iedere commutatieve ring $R \neq 0$ een priemideaal bezit zullen we in 15.10 bewijzen.

15.6. Voorbeelden. Een *nul-dimensionale ring* is een ring waarin geen inclusies tussen priemidealen bestaan. Een voorbeeld hiervan is de coördinatenring $\mathbf{C}$ van een punt in $\mathbf{A}^n(\mathbf{C})$, of algemener een willekeurig lichaam K. Immers, in een lichaam is (0) het enige priemideaal.

Iedere *eindige* ring R, zoals $\mathbf{Z}/n\mathbf{Z}$, is nul-dimensionaal. Immers, voor een priemideaal P in een eindige ring R is R/P een eindig domein, en dus wegens opgave 11.18 een lichaam. Dit betekent dat er geen inclusies tussen priemidealen bestaan in R, en we vinden $\dim(R) = 0$.

Voor $R = \mathbf{Z}$ zijn de priemidealen het nulideaal (0) en de idealen $p\mathbf{Z}$ voor de priemgetallen p. Er is een keten $(0) \subset p\mathbf{Z}$ van lengte 1, en omdat verschillende priemgetallen elkaar niet delen hebben we $\dim(\mathbf{Z}) = 1$. Algemener laat het bewijs van 12.10 zien dat ieder priemideaal $(p) \neq (0)$ in een hoofdideaaldomein R een 'maximaal' ideaal is: voor $x \notin (p)$ willekeurig geldt $(p, x) = R$. Een hoofdideaaldomein R dat geen lichaam is, bevat wegens 12.11 priemidealen $(p) \neq (0)$; we vinden $\dim(R) = 1$.

Opgave 8. Bewijs: $\dim(\mathbf{Z}[\sqrt{-5}]) = 1$.

Het zal niet als een verrassing komen dat de coördinatenring $R = \mathbf{C}[X_1, X_2, \ldots, X_n]$ van de affiene n-dimensionale ruimte $\mathbf{A}^n(\mathbf{C})$ dimensie n heeft. Voor $n \leq 2$ zagen we dit al. Voor $n \geq 3$ is het niet moeilijk in te zien dat de keten $\{P_k\}_{k=0}^n$, met $P_0 = (0)$ en $P_k = (X_1, X_2, \ldots, X_k)$ voor $k \geq 1$ het ideaal voortgebracht door de eerste $k \leq n$ variabelen, een keten van priemidealen van lengte n is. Dat er geen langere ketens bestaan bewijzen we hier niet![14]

▶ Maximale idealen

Als grootste idealen in de ketens van priemidealen van maximale lengte in een ring komt men zogenaamde *maximale idealen* van de ring tegen: idealen die men niet groter kan maken zonder direct de hele ring te krijgen. Dergelijke idealen hebben in de meetkunde te maken met de 'punten' van variëteiten.

15.7. Definitie. *Een ideaal $I \subset R$ in een commutatieve ring R heet maximaal als het niet gelijk is aan R, en er geen idealen $J \subset R$ bestaan met $I \subsetneq J \subsetneq R$.*

Omdat de idealen J die voldoen aan de inclusies $I \subset J \subset R$ corresponderen met de idealen van de factorring R/I, zegt 15.7 dat I maximaal is in R dan en slechts dan als R/I niet de nulring is en alleen triviale idealen heeft. In een commutatieve ring brengt ieder element $x \neq 0$ dat geen eenheid is een niet-triviaal ideaal (x) voort, dus lichamen zijn de enige commutatieve ringen $R \neq 0$ zonder niet-triviale idealen. Dit geeft het volgende analogon van (12.15):

$$(15.8) \qquad I \subset R \text{ is een maximaal ideaal } \iff R/I \text{ is een lichaam.}$$

In het bijzonder is het nulideaal $(0) \subset R$ maximaal dan en slechts dan als R een lichaam is. Omdat ieder lichaam een domein is, geven (12.15) en (15.8) de volgende implicatie.

15.9. Lemma. *Ieder maximaal ideaal in een commutatieve ring R is priem.* □

Ieder punt $a = (a_1, a_2, \ldots, a_n)$ van een affiene variëteit $V \subset \mathbf{A}^n(\mathbf{C})$ geeft aanleiding tot een evaluatie-afbeelding $R_V \to \mathbf{C}$, met als kern (opgave 11.35) het priemideaal

$$M_a = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subset R_V.$$

De isomorfiestelling geeft $R_V/M_a \cong \mathbf{C}$, dus wegens (15.8) is M_a maximaal in R_V. Voor $n \leq 2$ volgt uit 15.4 dat *alle* maximale idealen van de vorm M_a zijn voor een punt $a \in V$. Voor willekeurige n is dit ook waar, maar het bewijs is moeilijker. Het is één

van de formuleringen van de zogenaamde *Hilbert Nullstellensatz* uit de algebraïsche meetkunde. Het bewijs geven we niet in deze syllabus.[15]

Voor willekeurige commutatieve ringen $R \neq 0$ is het niet a priori duidelijk dat er maximale idealen in R bestaan. In theorie lijkt het heel eenvoudig om ze te construeren. Men begint namelijk met het nulideaal (0) en kijkt of dit maximaal is. Is dit niet zo, dan bestaat er wegens 15.7 een ideaal I_1 met $(0) \subsetneq I_1 \subsetneq R$. Is I_1 nog niet maximaal, dan nemen we een ideaal I_2 met $I_1 \subsetneq I_2 \subsetneq R$ en kijken of dit maximaal is. Zolang we met een niet-maximaal ideaal te doen hebben kunnen we dit vergroten, en we gaan hiermee door 'tot het niet langer kan zonder de hele ring te krijgen'. Het verkregen ideaal is dan maximaal. De volgende stelling klinkt dus zeer plausibel.

15.10. Stelling. *Iedere commutatieve ring $R \neq 0$ bezit een maximaal ideaal.*

Om een bewijs van stelling 15.10 te geven moeten we laten zien dat het zojuist beschreven proces van 'ideaalvergroting' $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ uiteindelijk tot een maximaal ideaal leidt. In *noetherse* ringen, die per definitie geen oneindige stijgende ketens van idealen hebben (opgave 12.23), is duidelijk dat het beschreven proces na eindig veel stappen een maximaal ideaal levert. In willekeurige ringen kunnen echter overaftelbaar veel stappen nodig zijn, en in dergelijke situaties is het niet altijd mogelijk het verkregen ideaal 'expliciet' aan te geven (opgaven 40–42). Onvrede met deze situatie speelde een belangrijke rol in het ontstaan van het *intuïtionisme* in de wiskunde.[16]

▶ Het lemma van Zorn

Alle bewijzen van 15.10 maken gebruik van het *keuzeaxioma* uit de verzamelingentheorie. Dit axioma, dat niet uit de 'basisaxioma's' van de verzamelingentheorie afgeleid kan worden, gebruiken we in de volgende vorm.[17]

15.11. Lemma van Zorn. *Laat X een partieel geordende verzameling zijn waarvoor iedere keten een bovengrens in X bezit. Dan bevat X een maximaal element.*

Allereerst enige uitleg voor wie dit lemma niet kent. Een *partiële ordening* op een verzameling X is per definitie een relatie $\leq$ op X die aan de volgende eigenschappen voldoet:

(P1) voor $x \in X$ geldt $x \leq x$;
(P2) als $x \leq y$ en $y \leq z$ geldt, dan ook $x \leq z$;
(P3) als $x \leq y$ en $y \leq x$ geldt, dan geldt $x = y$.

Een standaardvoorbeeld van een partieel geordende verzameling is de machtsverzameling $\mathcal{P}(A)$ van een verzameling A, de collectie van alle deelverzamelingen van A, met als partiële ordening de *inclusierelatie*. Partiële ordeningen op de verzameling $\mathbf{Z}_{\geq 0}$ van natuurlijke getallen zijn de 'gewone' ordening $\leq$ die we van $\mathbf{R}$ kennen, maar ook de *deelbaarheidsrelatie* $x|y$. Voor een abstracte partiële ordening op X zeggen we meestal 'x kleiner gelijk y' voor $x \leq y$.

Een *keten* in een partieel geordende verzameling is een *totaal geordende* deelverzameling $K \subset X$. Dit betekent dat voor ieder tweetal elementen $x, y \in K$ de relatie $x \leq y$

of $y \leq x$ geldt. Voor ieder n-tal elementen in een keten geldt bij geschikte nummering

$$x_1 \leq x_2 \leq x_3 \leq \ldots \leq x_{n-1} \leq x_n.$$

Voor de inclusie-ordening van ondergroepen in een groep kwamen we dit al in opgave 2.29 tegen.

Een *bovengrens* voor een deelverzameling $Y \subset X$ in X is een element $x \in X$ dat voldoet aan $y \leq x$ voor alle $y \in Y$. Ieder element $x \in X$ is een bovengrens voor de lege deelverzameling $\emptyset \subset X$, die bij gebrek aan eisen tevens een keten in X is, de *lege keten*. Een *maximaal element* in X is een element $x \in X$ met de eigenschap dat het enige element $z \in X$ dat voldoet aan $x \leq z$ het element x zelf is: er zijn geen elementen in X die 'echt groter' zijn dan x.

Opgave 9. Wat zijn de maximale elementen van $\mathcal{P}(A)$ en $\mathbf{Z}_{\geq 0}$ ten opzichte van de boven aangegeven partiële ordeningen?

Bewijs van 15.10. De existentie van maximale idealen in een commutatieve ring $R \neq 0$ is een directe toepassing van 15.11 op de collectie idealen

$$X = \{I \subset R : I \text{ is een ideaal verschillend van } R\}$$

met de inclusierelatie als partiële ordening. Het nulideaal $(0) \in X$ is een bovengrens voor de lege keten in X. Voor een niet-lege keten $K = \{I_k\}_k$ in X is de vereniging $I = \bigcup_k I_k$ weer een ideaal in R (ga na!). Omdat $1 \in R$ in geen enkel ideaal I_k bevat is, geldt $1 \notin I$ en $I \neq R$, dus I is een bovengrens voor K die in X ligt. Wegens 15.11 bestaan er maximale elementen in X, en dit zijn maximale idealen van R. □

15.12. Gevolg. *Ieder ideaal $I \subsetneq R$ is bevat in een maximaal ideaal van R. De vereniging van alle maximale idealen van R is gelijk aan*

$$\textstyle\bigcup_{M \subset R \text{ maximaal}} M = R \setminus R^*.$$

Bewijs. De maximale idealen M/I van de quotiëntring $R/I \neq 0$ corresponderen met de maximale idealen $M \subset R$ die I omvatten, en wegens 15.10 bestaan zulke idealen. Nemen we voor I het hoofdideaal (x) voortgebracht door een niet-eenheid $x \in R$, dan volgt dat iedere niet-eenheid van R bevat is in een maximaal ideaal van R. Omdat eenheden in geen enkel maximaal ideaal van R bevat zijn, volgt $\bigcup_M M = R \setminus R^*$. □

Voor een hoofdideaaldomein R komt 15.12 neer op de eenvoudige bewering dat ieder element dat geen eenheid is, deelbaar is door een priemelement.

15.13. Voorbeeld. Zij $R = \mathrm{Map}(X, \mathbf{R})$ de ring van reëelwaardige functies op een eindige verzameling X. Voor ieder punt $x \in X$ is de kern van de evaluatie-afbeelding $f \mapsto f(x)$ in het punt x gelijk aan $M_x = \{f \in R : f(x) = 0\}$ van R. De isomorfiestelling geeft een isomorfisme $R/M_x \cong \mathbf{R}$, dus wegens 15.8 is M_x maximaal. Het complement van $\bigcup_{x \in X} M_x$ in R bestaat uit de functies op X zonder nulpunten, en dit zijn precies de eenheden van R.

Om te bewijzen dat de maximale idealen van R precies de idealen M_x zijn, is het voldoende te laten zien dat ieder ideaal $I \subsetneq R$ bevat is in een ideaal M_x. Is I namelijk niet in enig ideaal van de vorm M_x bevat, dan is er voor ieder element $x \in X$ een functie $f_x \in I$ met $f_x(x) \neq 0$. De functie $f = \sum_{x \in X} f_x^2 \in I$ is nu strikt positief op X, dus een eenheid in R. Er volgt $I = R$.

Opgave 10. Gebruik de isomorfie $R \cong \prod_{x \in X} \mathbf{R}$ en opgave 11.47 om te bewijzen dat de maximale idealen van R de idealen M_x zijn.

Voor *iedere* ring R van functies op een verzameling X met waarden in een lichaam geven, indien R alle constante functies bevat, de punten van X als in 15.13 via de puntevaluaties aanleiding tot maximale idealen. In vele (maar niet alle) gevallen is dit een bijectie, zodat men X kan 'reconstrueren' uit de verzameling van maximale idealen van R. Zie opgave 29 voor een voorbeeld.

▶ Nilradicaal

Het lemma van Zorn is nuttig in allerlei andere situaties waarbij maximale verzamelingen met een gegeven eigenschap geconstrueerd moeten worden. We geven een toepassing op de beschrijving van het *nilradicaal* $\mathrm{nil}(R)$ van een commutatieve ring R. Dit is per definitie de deelverzameling van R bestaande uit elementen x waarvoor een positieve macht x^k gelijk is aan 0. Dergelijke elementen in R heten *nilpotent*. Het nulelement van R is duidelijk nilpotent, en als R een domein is, is dit het enige element met deze eigenschap. Voor een ring als $R = \mathbf{Z}/p^2\mathbf{Z}$ hebben we echter $\mathrm{nil}(R) = p\mathbf{Z}/p^2\mathbf{Z}$.

15.14. Stelling. *Het nilradicaal* $\mathrm{nil}(R)$ *is een ideaal van* R*, en het is gelijk aan*

$$\mathrm{nil}(R) = \bigcap_{P \subset R \text{ priem}} P.$$

Bewijs. Als $x \in \mathrm{nil}(R)$ een nilpotent element is en $P \subset R$ een priemideaal, dan geldt $x^k = 0 \in P$ voor geschikte k, en uit de priemeigenschap volgt $x \in P$. Dus $\mathrm{nil}(R)$ is bevat in de doorsnede van alle priemidealen.

Laat nu $f \in R$ een element zijn dat niet nilpotent is. We willen laten zien dat er een priemideaal P is dat f niet bevat. Deze keer nemen we de collectie van idealen

$$X = \{I \subset R : I \text{ is een ideaal dat geen enkele macht van } f \text{ bevat}\}$$

met de inclusierelatie als partiële ordening op X. Omdat f niet nilpotent is geldt $(0) \in X$, dus de lege keten heeft een bovengrens in X. Voor niet-lege ketens krijgen we bovengrenzen door de vereniging van de keten te nemen. Passen we weer 15.10 toe, dan volgt dat X een maximaal element P bevat. Dit is een ideaal van R dat geen machten van f bevat, en we beweren dat P een *priemideaal* van R is.

Stel namelijk dat $x, y \in R$ product $xy \in P$ hebben, maar dat P geen van beide elementen bevat. Dan bevatten de idealen $P + (x)$ en $P + (y)$, die elk strikt groter zijn dan P, wegens de maximaliteitseigenschap van P elk wel een macht van f. Het productideaal $(P + (x)) \cdot (P + (y))$ bevat dan ook een macht van f. Wegens

$$(P + (x)) \cdot (P + (y)) \subset P + (xy) \subset P$$

bevat P dan ook een macht van f: tegenspraak. We concluderen dat P een priemideaal is dat f niet bevat, en dit bewijst zoals gewenst $f \notin \bigcap_{P \subset R \text{ priem}} P$. In het bijzonder zien we uit de zojuist bewezen identiteit dat $\mathrm{nil}(R)$, als doorsnede van idealen, een ideaal van R is. □

Opgave 11. Bewijs dat $\mathrm{nil}(R)$ een ideaal van R is *zonder* de beschrijving uit 15.14 te gebruiken.

▶ Spectrum van een ring

Voor coördinatenringen en veel andere functieringen uit de meetkunde zijn de elementen van de ring op te vatten als functies op de verzameling van maximale idealen van de ring. Ook in niet-meetkundige situaties is een dergelijke beschrijving vaak mogelijk: een element $x \in \mathbf{Z}$ heeft voor elk maximaal ideaal $p\mathbf{Z}$ een 'functiewaarde' $x \bmod p$ in het restklassenlichaam $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ behorende bij het 'punt' $p\mathbf{Z}$ van $\mathbf{Z}$. Het is bovendien duidelijk dat een element $x \in \mathbf{Z}$ uniek bepaald is door zijn functiewaarden $x \bmod p$.

Opgave 12. Geef een voorbeeld van een commutatieve ring R en verschillende elementen $x, y \in R$ met de eigenschap dat $x \equiv y \bmod M$ geldt voor alle maximale idealen $M \subset R$.

De gedachte om elementen van een ring R als functies op de verzameling van maximale idealen van R te beschouwen, blijkt uiterst suggestief. Nog beter is het om het *spectrum* $\mathrm{Spec}(R)$ van R te nemen, de verzameling die uit *alle* priemidealen van R bestaat. Deze heeft de prettige eigenschap dat er voor ieder homomorfisme $f : R_1 \to R_2$ van commutatieve ringen een geïnduceerde afbeelding

$$\begin{aligned} f^* : \mathrm{Spec}(R_2) &\longrightarrow \mathrm{Spec}(R_1) \\ P_2 &\longmapsto f^{-1}[P_2] \end{aligned} \tag{15.15}$$

is. Immers, de kern $f^{-1}[P_2]$ van de samengestelde afbeelding $R_1 \xrightarrow{f} R_2 \to R_2/P_2$ is een priemideaal wegens 12.15 en het simpele feit dat een deelring van een domein weer een domein is.

Opgave 13. Laat zien dat het inverse beeld van een maximaal ideaal niet altijd maximaal is.

De Franse wiskundige Grothendieck[18] liet in de vroege jaren zestig zien hoe de interpretatie van ringen als functieruimtes op spectra gebruikt kan worden om de hele theorie van commutatieve ringen in algebraïsch-meetkundige termen te formuleren. De tot Bernhard Riemann (1826–1866) teruggaande methode uit de meetkunde om variëteiten uit 'lokale stukjes' (*kaarten*) aan elkaar te plakken leidt voor spectra tot de definitie van *schema's*. In omgekeerde richting kan men de gehele algebraïsche meetkunde opzetten in termen van schema's. De verkregen flexibiliteit maakt het mogelijk niet alleen over $\mathbf{C}$ of $\mathbf{R}$, maar over willekeurige grondlichamen of zelfs commutatieve grondringen meetkunde te ontwikkelen. In de al genoemde aritmetische algebraïsche meetkunde is deze aanpak zeer productief gebleken.

De algebraïsche abstractie die de theorie met zich meebrengt heeft Grothendieck's schema's lang een ongenaakbaar aureool gegeven. Door de succesvolle toepassingen van de theorie in de afgelopen veertig jaar is het onderliggend meetkundig gedachtengoed echter tot de fundamenten van de algebra gaan behoren.

▶ Topologie van spectra

Het spectrum van een ring is niet alleen een *verzameling* van priemidealen; het blijkt op natuurlijke wijze een *topologische ruimte* te zijn, zij het dan van een iets andere soort dan de vertrouwde *metrische* topologische ruimtes. Ten opzichte van de natuurlijke topologie op spectra, de naar de meetkundige Oscar Zariski (1899–1986) genoemde Zariski-topologie, zijn de door ringhomomorfismen geïnduceerde afbeeldingen f^* uit (15.15) *continue* afbeeldingen (opgave 49).

We brengen in herinnering dat een collectie $\mathcal{U}$ van deelverzamelingen van een verzameling X een *topologie* op X heet als $\emptyset$ en X in $\mathcal{U}$ bevat zijn, en $\mathcal{U}$ gesloten is onder het nemen van *willekeurige* verenigingen en doorsneden van *eindig* veel elementen van $\mathcal{U}$. De elementen van $\mathcal{U}$ heten de *open* deelverzamelingen van X. Een complement van een open deelverzameling van X heet een *gesloten* deelverzameling van X.

De Zariski-topologie is de topologie uit onderstaande stelling.

15.16. Stelling. *De verzameling* $\mathrm{Spec}(R)$ *van priemidealen van een commutatieve ring* R *heeft een topologie waarin de gesloten verzamelingen de verzamelingen van de vorm*

$$Z(I) = \{P \text{ priem} : P \supset I\} \subset \mathrm{Spec}(R)$$

zijn, met I *een ideaal van* R*. De topologische ruimte* $\mathrm{Spec}(R)$ *is compact.*

Bewijs. De deelverzamelingen $Z(I) \subset \mathrm{Spec}(R)$ vormen de gesloten verzamelingen van een topologie als hun complementen aan de axioma's voor een topologie op $\mathrm{Spec}(R)$ voldoen. De verzamelingen $Z(R) = \emptyset$ en $Z(0) = \mathrm{Spec}(R)$ zijn zowel open als gesloten.

De identiteit $Z(I_1) \cup Z(I_2) = Z(I_1 I_2)$, die gemakkelijk uit de priemideaaleigenschap volgt, laat zien dat eindige verenigingen van gesloten verzamelingen weer gesloten zijn, en dus eindige doorsnijdingen van open verzamelingen open.

Een willekeurige doorsnede $\bigcap_\alpha Z(I_\alpha)$ van gesloten verzamelingen $Z(I_\alpha)$ is weer gesloten, want gelijk aan $Z(I)$, met I het ideaal *voortgebracht* door de idealen I_α. Dit laat zien dat verenigingen van open verzamelingen open zijn, dus de Zariski-topologie is inderdaad een topologie. Ook volgt dat de gesloten verzamelingen in $\mathrm{Spec}(R)$ de 'eindige-doorsnijdingseigenschap' hebben, hetgeen equivalent is met de compactheid van $\mathrm{Spec}(R)$. Immers, als $\bigcap_\alpha Z(I_\alpha) = Z(I)$ leeg is, dan is I in geen enkel priemideaal bevat, en dus wegens 15.12 gelijk aan R. Schrijven we $1 \in I$ als R-lineaire combinatie van elementen uit de idealen I_α, dan zijn hiervoor slechts eindig veel idealen I_α nodig, en de eindige doorsnijding van de bijbehorende verzamelingen $Z(I_\alpha)$ is dan leeg. □

Opgave 14. Bewijs: $Z(I_1) \cup Z(I_2) = Z(I_1 \cap I_2) = Z(I_1 I_2)$.

15.17. Voorbeelden. 1. Het spectrum van de nulring is de lege verzameling. Het spectrum $\mathrm{Spec}(K) = \{(0)\}$ van een lichaam K is een eenpuntsverzameling.

2. Het spectrum $\mathrm{Spec}(R)$ van een hoofdideaaldomein R bestaat uit de idealen (p) voortgebracht door de irreducibele elementen van R, die immers wegens 12.10 priem zijn, en het nulideaal (0). In het bijzonder hebben we

$$\mathrm{Spec}(\mathbf{Z}) = \{(0)\} \cup \{p\mathbf{Z} : p \text{ een priemgetal}\}$$
$$\mathrm{Spec}(\mathbf{C}[X]) = \{(0)\} \cup \{(X - \alpha) : \alpha \in \mathbf{C}\}.$$

Voor $I = (x) \subset R$ bestaat de gesloten verzameling $Z(I) = Z(x)$ uit de priemidealen (p) die (x) delen. Voor $x \neq 0$ is dit een *eindige* verzameling, voor $x = 0$ is het $\mathrm{Spec}(R)$ zelf. Het nulideaal is in geen enkele gesloten verzameling verschillend van $\mathrm{Spec}(R)$ bevat. We concluderen dat de open verzamelingen $U \neq \emptyset$ in $\mathrm{Spec}(R)$ de verzamelingen zijn die $\{(0)\}$ bevatten en een eindig complement hebben. Deze topologie heeft de eigenschap dat voor ieder tweetal niet-lege open verzamelingen U_1, U_2 de doorsnede $U_1 \cap U_2$ niet-leeg is. Merk op dat dit fenomeen in de klassieke (metrische) topologische ruimtes, die altijd Haussdorffruimtes zijn, niet optreedt.

3. Uit 15.4 volgt dat $\mathrm{Spec}(\mathbf{C}[X,Y])$ uit drie soorten priemidealen bestaat: het nulideaal, de priemidealen (p) behorende bij de irreducibele krommen in $\mathbf{A}^2(\mathbf{C})$, en de maximale idealen $(X-a, Y-b)$ behorende bij de punten $(a,b) \in \mathbf{C}^2$. Voor $I \neq (0)$ bestaat de gesloten verzameling $Z(I) \subset \mathrm{Spec}(\mathbf{C}[X,Y])$ uit de priemidealen behorende bij de punten en de irreducibele krommen bevat in de *algebraïsche verzameling* $Z(I) \subset \mathbf{A}^2(\mathbf{C})$. We zien dat vlakke algebraïsche verzamelingen en gesloten delen van $\mathrm{Spec}(\mathbf{C}[X,Y])$ in essentie dezelfde dingen zijn: de topologische ruimte $\mathrm{Spec}(\mathbf{C}[X,Y])$ is een 'algebraïsch model' voor het affiene vlak. De corresponderende *Zariski-topologie* op het affiene vlak is *niet* de bekende metrische topologie op $\mathbf{C}^2$ (opgave 45).

Iedere gesloten verzameling $Z(I)$ die een punt $P \in \mathrm{Spec}(R)$ bevat, bevat tevens alle priemidealen van R die P omvatten. Er volgt dat de *afsluiting* van $\{P\}$ gelijk is aan $Z(P)$. In het bijzonder zijn de 'gesloten punten' van $\mathrm{Spec}(R)$ precies de *maximale idealen* van R. In domeinen R is het nulideaal (0) een punt met als afsluiting de hele ruimte $\mathrm{Spec}(R)$. Het wordt wel het *generieke punt* van $\mathrm{Spec}(R)$ genoemd.

Opgaven.

Alle ringen R in de onderstaande opgaven zijn commutatief.

15. Laat zien dat de nulverzameling $Z(f_1, f_2)$ in voorbeeld 15.1 de lege verzameling is, maar dat $R/(f_1, f_2)$ niet de nulring is. [Hint: evalueer $f \in R$ in een geschikt punt van $\mathbf{A}^2(\mathbf{C})$.]

16. Laat zien dat een eindig lichaam niet algebraïsch afgesloten is.

17. Bepaal welke van de volgende deelverzamelingen van $\mathbf{C}^2$ algebraïsche verzamelingen zijn:
    a. $\{(t^2, t^3) : t \in \mathbf{C}\}$;
    b. $\{(t, \sin t) : t \in \mathbf{C}\}$;
    c. $\{(\cos t, \sin t) : t \in \mathbf{C}\}$;
    d. $\{(e^t, \sin t) : t \in \mathbf{C}\}$;
    e. $\{(e^t + e^{-t}, e^t - e^{-t}) : t \in \mathbf{C}\}$;
    f. $\{(e^{2t}, e^{3t}) : t \in \mathbf{C}\}$.

18. Zij $R = \mathbf{R}[X,Y]/(X^2+Y^2-1)$ de ring van reële polynomiale functies op de eenheidscirkel.
    a. Laat zien dat $\mathbf{R}^*$ de eenhedengroep van R is.
    [Hint: gebruik, net als voor de ring $\mathbf{Z}[i]$ in 12.19, een normfunctie $f(X) + Yg(X) \mapsto f(X)^2 - (1-X^2)g(X)^2$.]
    b. Laat zien dat $M = (X-1, Y) \subset R$ de kern van de puntevaluatie in $(1,0)$ is.
    c. Laat zien dat M geen hoofdideaal is.
    [Hint: wat kan de norm zijn van een element dat zowel $X-1$ als Y deelt?]

d. Laat zien dat $X-1$ en $Y-1$ irreducibele elementen in R zijn die niet priem zijn. Concludeer: R is geen ontbindingsring.
[Hint: er geldt $(X+Y-1)^2 = 2(X-1)(Y-1) \in R$ – maak een plaatje!]

19. Laat zien dat de ring van trigonometrische polynomen uit opgave 13.17 isomorf is met de ring van polynomiale functies op de eenheidscirkel uit de vorige opgave.

20. Zij $R = \mathbf{R}[X,Y]/(XY-1)$ de ring van polynomiale functies op de 'eenheidshyperbool'.
    a. Laat zien dat R isomorf is met de ring $\mathbf{R}[T,T^{-1}] \subset \mathbf{R}(T)$ van Laurentpolynomen.
    b. Bewijs: R is een hoofdideaaldomein met eenhedengroep

$$R^* = \{cX^i \bmod (XY-1) : c \in \mathbf{R}^*, i \in \mathbf{Z}\} \cong \mathbf{R}^* \times \langle X \rangle.$$

21. Bewijs dat de ringen $R = \mathbf{C}[X,Y]/(X^2+Y^2-1)$ en $\mathbf{C}[U,V]/(UV-1)$ isomorf zijn, en bepaal een voortbrenger van het ideaal $(X-1,Y) \subset R$.

22. Zijn de ringen $K[X,Y]/(X^2+Y^2-1)$ en $K[U,V]/(UV-1)$ isomorf voor K respectievelijk gelijk aan $\mathbf{R}$, $\mathbf{F}_5$ en $\mathbf{F}_3$?

23. Laat zien dat de ring Ω uit opgave 13.15 oneindige Krull-dimensie heeft.

24. Laat $P \subset \mathbf{Z}[X]$ een priemideaal zijn.
    a. Bewijs: $P \cap \mathbf{Z} = p\mathbf{Z}$ met $p = 0$ of p een priemgetal.
    b. Bewijs: de priemidealen $P \subset \mathbf{Z}[X]$ met $P \cap \mathbf{Z} = 0$ zijn de hoofdidealen $P = (f)$, met $f \in \mathbf{Z}[X]$ irreducibel of gelijk aan 0.
    c. Bewijs: de priemidealen $P \subset \mathbf{Z}[X]$ met $P \cap \mathbf{Z} = p\mathbf{Z}$ en p priem zijn de idealen van de vorm $P = (p, f_p)$, met $f_p \in \mathbf{Z}[X]$ een polynoom dat irreducibel is modulo p of gelijk aan 0.
    d. Concludeer dat $\mathbf{Z}[X]$ een 2-dimensionale ring is.

25. Ga voor elk van de volgende idealen in $\mathbf{Z}[X]$ na of het priem is en of het maximaal is:

$$(X-7,3), \qquad (X^2-7), \qquad (X^2-7,3), \qquad (X^2-7,5).$$

    Zelfde vragen met $\mathbf{Q}[X]$ in plaats van $\mathbf{Z}[X]$.

26. Een commutatieve ring R met precies één maximaal ideaal heet een *locale ring*. Bewijs dat R locaal is dan en slechts dan als $R \setminus R^*$ een ideaal is in R.

27. Laat zien dat de ring $R_p \subset \mathbf{Q}$ uit opgave 11.17 een locale ring is. Bewijs algemener dat voor een priemelement p in een hoofdideaaldomein R de ring $R_p = \{\frac{a}{b} : \mathrm{ord}_p(b) = 0\}$ een deelring van $K = Q(R)$ is, en dat deze ring locaal is.

28. Een *discrete valuatie* op een lichaam K is een surjectief groepshomomorfisme $v : K^* \to \mathbf{Z}$ dat voldoet aan $v(x+y) \geq \min\{v(x), v(y)\}$ voor $y \neq -x$. De bijbehorende *discrete valuatiering* is gedefinieerd als $R_v = \{0\} \cup \{x \in K^* : v(x) \geq 0\}$.
    a. Laat zien dat voor ieder priemgetal p de uit §6 bekende functie $\mathrm{ord}_p : \mathbf{Q}^* \to \mathbf{Z}$ een discrete valuatie op $\mathbf{Q}$ is, en de deelring $R_p \subset \mathbf{Q}$ uit de vorige opgave de bijbehorende discrete valuatiering.
    b. Laat zien dat een discrete valuatiering R_v een locale ring is, en dat ieder element $\pi \in R$ met $v(\pi) = 1$ het maximale ideaal van R_v voortbrengt.
    c. Bewijs: als R_v en π als in (b) zijn, dan is ieder element $x \in K^*$ uniek te schrijven als $x = u\pi^k$ met $u \in R^*$ en $k \in \mathbf{Z}$.

29. Zij $R = C([0,1])$ de ring van continue reëelwaardige functies op $[0,1]$. Bewijs dat de maximale idealen van R de kernen M_x van de puntevaluaties zijn.
[Hint: gebruik compactheid.]

30. Bepaal alle priemidealen en het nilradicaal van $\mathbf{Z}/300\mathbf{Z}$.

31. Laat zien dat equivalent zijn:
    a. $R/\mathrm{nil}(R)$ is een lichaam;
    b. $R \neq 0$, en ieder element van R is nilpotent of een eenheid;
    c. R heeft precies één priemideaal.

32. Het *Jacobson-radicaal* $J(R)$ van R is de verzameling van elementen $x \in R$ waarvoor $1 + xR = \{1 + xr : r \in R\} \subset R^*$ geldt. Bewijs: $J(R)$ is een ideaal van R, en het is gelijk aan de doorsnede van alle maximale idealen $M \subset R$.

33. Een ring R heet *gereduceerd* als $\mathrm{nil}(R) = 0$ geldt. Laat zien dat $R/\mathrm{nil}(R)$ een gereduceerde ring is, en dat de afbeelding $P \mapsto P/\mathrm{nil}(R)$ de priemen van R bijectief naar die van $R/\mathrm{nil}(R)$ afbeeldt.

34. Laat zien dat R gereduceerd is dan en slechts dan als R in een product van lichamen ingebed kan worden.

35. Bewijs dat voor ieder ideaal $I \subset R$ het radicaal $\sqrt{I} = \{x \in R : x^k \in I \text{ voor zekere } k \geq 1\}$ van I een ideaal van R is, en dat het de doorsnede is van alle priemidealen die I omvatten. Is $R/\sqrt{I}$ een gereduceerde ring?

36. Bewijs: een polynoom $f \in R[X]$ is nilpotent dan en slechts dan alle coëfficiënten van f nilpotent zijn in R.

37. Laat zien dat voor $x \in \mathrm{nil}(R)$ het element $1 + x$ een eenheid is, en dat algemener de som van een eenheid en een nilpotent element een eenheid is.

38. Laat zien dat $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ een eenheid is in $R[X]$ dan en slechts dan als a_0 een eenheid is in R en de coëfficiënten a_i met $i > 0$ nilpotent zijn.
[Hint: reduceer modulo priemen van R.]

39. Laat zien dat $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ een nuldeler is in $R[X]$ dan en slechts dan als er een element $a \in R \setminus \{0\}$ bestaat met $af = 0$.
[Hint: stel $gf = 0$ met $g = \sum_{j=0}^{m} b_j X^j$ van minimale graad; gebruik $a_n fg = 0$ om inductief $a_{n-k} g = 0$ te krijgen voor $k = 0, 1, \ldots, n$.]

40. Noem een $\mathbf{F}_2$-waardige functie $f \in R = \mathrm{Map}(\mathbf{Z}, \mathbf{F}_2)$ op $\mathbf{Z}$ *klein* als hij slechts in eindig veel punten van $\mathbf{Z}$ de waarde $1 \in \mathbf{F}_2$ aanneemt. Bewijs dat er een ringhomomorfisme $\phi : R \to \mathbf{F}_2$ bestaat dat op alle kleine functies de waarde 0 aanneemt.

41. Laat zien dat er een manier is om de deelverzamelingen van $\mathbf{Z}$ zo onder te verdelen in 'kleine' en 'grote' verzamelingen dat het volgende geldt:
    1. eindige verzamelingen zijn klein;
    2. deelverzamelingen van kleine verzamelingen zijn klein;
    3. een doorsnijding van twee grote verzamelingen is groot;
    4. een vereniging van twee kleine verzamelingen is klein;
    5. de verzameling van priemgetallen is groot.

*42. Zij X een verzameling, $\mathcal{F}$ een collectie deelverzamelingen van X en $\mathcal{P}(X) \cong \mathrm{Map}(X, \mathbf{F}_2)$ de Boolese ring uit opgave 11.31. We noemen $\mathcal{F}$ een *filter* op X als geldt:

$$\begin{aligned} &X \in \mathcal{F}, \qquad \emptyset \notin \mathcal{F}; \\ &A, B \in \mathcal{F} \implies A \cap B \in \mathcal{F}; \\ &A \in \mathcal{F} \;\&\; A \subset B \implies B \in \mathcal{F}. \end{aligned}$$

Geldt bovendien ($A \cup B \in \mathcal{F} \implies A \in \mathcal{F}$ of $B \in \mathcal{F}$), dan heet $\mathcal{F}$ een *ultrafilter* op X. Bewijs de volgende uitspraken:

a. $\mathcal{F}$ is een filter $\Leftrightarrow \{A \subset X : (X \setminus A) \in \mathcal{F}\}$ is een ideaal $\neq \mathcal{P}(X)$ van $\mathcal{P}(X)$;
b. $\mathcal{F}$ is een ultrafilter $\Leftrightarrow \{A \subset X : (X \setminus A) \in \mathcal{F}\}$ is een maximaal ideaal van $\mathcal{P}(X)$;
c. voor $x \in X$ is $\mathcal{F}_x = \{A \subset X : x \in A\}$ een ultrafilter op X;
d. voor oneindige X bestaan er ultrafilters op X die *niet* van de vorm $\mathcal{F}_x$ zijn.
[De ultrafilters in (d) heten *vrije ultrafilters*[19] op X.

*43. Zij K_n een lichaam voor $n \geq 0$, en $R = \prod_{n \geq 0} K_n$ de productring. Voor $x = (x_n)_n \in R$ schrijven we $V(x) = \{n \geq 0 : x_n = 0\}$. Laat zien dat de maximale idealen van R bijectief corresponderen met de ultrafilters op $\mathbf{Z}_{\geq 0}$ onder de afbeelding $I \longmapsto \{V(x) : x \in I\}$.

44. Zij K een lichaam. Laat zien dat de algebraïsche verzamelingen in de affiene ruimte $\mathbf{A}^n(K)$ de gesloten verzamelingen zijn van een *topologie* op K^n, de *Zariski-topologie* op K^n. [Je mag aannemen dat $K[X_1, X_2, \ldots, X_n]$ noethers is.]

45. De *Zariski-afsluiting* van $V \subset \mathbf{C}^n$ is de afsluiting van V in de Zariski-topologie.
a. Bepaal de Zariski-afsluiting van $\mathbf{Z} \subset \mathbf{C}$.
b. Bepaal de Zariski-afsluiting van $\{(x, y) : |x| \leq 1 \text{ en } |y| < 1\} \subset \mathbf{C}^2$.
c. Laat zien dat de klassieke (metrische) topologie op $\mathbf{C}^n$ (strikt) fijner is dan de Zariski-topologie op $\mathbf{C}^n$.

46. Een topologische ruimte X heet *irreducibel* als hij niet leeg is en niet de vereniging $X = Z_1 \cup Z_2$ is van gesloten verzamelingen $Z_i \subsetneq X$.
a. Bewijs dat twee niet-lege open deelverzamelingen van een irreducibele topologische ruimte een niet-lege doorsnede hebben.
b. Bewijs dat het spectrum van een domein irreducibel is.

47. Een topologische ruimte $X \neq \emptyset$ heet *samenhangend* als $\emptyset$ en X zelf de enige deelverzamelingen van X zijn die zowel open als gesloten zijn. Bewijs dat voor een gereduceerde ring $R \neq 0$ equivalent zijn:
1. $\mathrm{Spec}(R)$ is niet samenhangend;
2. er bestaan niet-nul-ringen R_1 en R_2 en een isomorfisme $R \cong R_1 \times R_2$;
3. R bevat een idempotent element verschillend van 0 of 1.

*Is de eis dat R gereduceerd is noodzakelijk?

48. Definieer voor $f \in R$ de verzameling $D(f) = \{P \in \mathrm{Spec}(R) : f \notin P\} \subset \mathrm{Spec}(R)$. Bewijs de volgende uitspraken:
a. $D(f)$ is open in $\mathrm{Spec}(R)$; er geldt $D(f) \cap D(g) = D(fg)$
b. $D(f) = \emptyset \Leftrightarrow f$ is nilpotent;
c. $D(f) = \mathrm{Spec}(R) \Leftrightarrow f \in R^*$;
d. $U \subset \mathrm{Spec}(R)$ is open $\Leftrightarrow U$ is een vereniging van verzamelingen van de vorm $D(f)$.
[De verzamelingen $D(f)$ vormen een *basis* voor de Zariski-topologie op $\mathrm{Spec}(R)$.]

49. Zij $f : A \to B$ een homomorfisme van commutatieve ringen en $f^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ de geïnduceerde afbeelding op de spectra. Bewijs de volgende uitspraken:
    a. f^* is een continue afbeelding;
    b. is f surjectief met kern I, dan is $f^* : \mathrm{Spec}(B) \to \mathrm{im}\, f^* = Z(I)$ een homeomorfisme;
    c. voor de natuurlijke afbeelding $f : A \to B = A/\mathrm{nil}(A)$ is f^* een homeomorfisme.

50. Zij $f : \mathbf{C}[X] \to \mathbf{C}[X, Y]$ de natuurlijke inclusie-afbeelding. Beschrijf de geïnduceerde afbeelding op de spectra en de vezels van deze afbeelding. Wat is het bijbehorende 'meetkundige plaatje'?

51. Zelfde vragen voor de afbeelding $f : \mathbf{C}[X] \to \mathbf{C}[X]$ gegeven door $f(X) \mapsto f(X^2)$.

52. Zij $f : \mathbf{Z} \to \mathbf{Z}[i]$ de natuurlijke inclusie-afbeelding. Beschrijf de geïnduceerde afbeelding op de spectra en de vezels van deze afbeelding.

16 Modulen

Het komt vaak voor dat de elementen van een abelse groep 'vermenigvuldigd' kunnen worden met de elementen uit een ring. Men kan hierbij denken aan de in §9 veel gebruikte vermenigvuldiging van elementen uit een abelse groep met getallen uit $\mathbf{Z}$ of aan de vermenigvuldiging in de lineaire algebra van vectoren uit een vectorruimte met matrices. Zo'n vermenigvuldiging respecteert de groepsoperatie en is daarmee een *endomorfisme* van de abelse groep. In dergelijke situaties spreekt men van *modulen* over een ring. De formele definitie doet sterk denken aan de in 5.1 gegeven definitie voor werkingen. In plaats van de permutatie*groep* op een verzameling gebruiken we nu de in 11.8 gedefinieerde endomorfismen*ring* van een abelse groep.

16.1. Definitie. *Zij R een ring. Een R-moduul is een abelse groep M voorzien van een ringhomomorfisme $\phi : R \to \mathrm{End}(M)$.*

Noteren we M additief en schrijven we kortweg rm voor $\phi(r)(m)$, dan kunnen we de eis '$\phi(r) \in \mathrm{End}(M)$' en de voorwaarden uit 11.11 voor 'ϕ is een homomorfisme' vertalen in termen van de volgende identiteiten, geldig voor alle $r, s \in R$ en $m, n \in M$:

(M1) $r(m+n) = rm + rn$;
(M2) $(r+s)m = rm + sm$;
(M3) $(rs)m = r(sm)$;
(M4) $1 \cdot m = m$.

Definitie 16.1 beschrijft in feite een *linksmoduul* M over R. Net als in het geval van werkingen, waar met iedere linkswerking van een groep G op een verzameling X een rechtswerking van G op X correspondeert (opgave 5.20), kan men uit ieder linksmoduul over R een rechtsmoduul maken over de *tegengestelde ring* R^{opp} uit opgave 11.66, die voor commutatieve R met R zelf geïdentificeerd kan worden.

Opgave 1. Een *rechtsmoduul* M over een ring R is een abelse groep voorzien van een ringhomomorfisme $\phi : R^{\mathrm{opp}} \to \mathrm{End}(M)$. Schrijf $\phi(r)(m)$ als mr en geef de eisen corresponderend met (M1)–(M4).

Het geeft zelden aanleiding tot verwarring dat de nulelementen van R en van M elk met 0 worden aangegeven, zoals in de voor alle $m \in M$ geldende identiteit $0 \cdot m = 0$, en dat men $M = 0$ schrijft voor het *nulmoduul*. De direct uit 16.1 volgende identiteiten als $(-r)m = -(rm) = r(-m)$ laten zien dat men zonder problemen $-rm$ kan schrijven voor $r \in R$ en $m \in M$.

Opgave 2. Leid deze identiteiten af uit 16.1.

Voorbeelden. Voor iedere abelse groep M is er een uniek ringhomomorfisme $\phi : \mathbf{Z} \to \mathrm{End}(M)$, en daarmee wordt M op natuurlijke wijze een $\mathbf{Z}$-moduul. De '$\mathbf{Z}$-moduul-notatie' km voor $k \in \mathbf{Z}$ en $m \in M$ gebruiken we voor abelse groepen reeds lang.

Nemen we $R = \mathrm{End}(M)$ en ϕ de identiteit in 16.1, dan zien we dat iedere abelse groep tevens op natuurlijke wijze een moduul is over zijn endomorfismenring $\mathrm{End}(M)$. Merk op dat $\mathrm{End}(M)$ in veel gevallen niet-commutatief is.

Is $f : R_1 \to R_2$ een ringhomomorfisme, dan kan men ieder R_2-moduul 'via f' opvatten als R_1-moduul. De moduulstructuur over R_1 wordt verkregen uit de samengestelde

afbeelding $R_1 \xrightarrow{f} R_2 \xrightarrow{\phi} \mathrm{End}(M)$. Men spreekt hierbij wel van *restrictie van scalairen*. Deze situatie is in het bijzonder van toepassing op iedere deelring $R_1 \subset R_2$. Voor de unieke afbeelding $R_1 = \mathbf{Z} \to R_2$ zien we nogmaals dat ieder moduul in het bijzonder een $\mathbf{Z}$-moduul (d.w.z. een abelse groep) is.

Net als groepen en ringen komen modulen met 'bijbehorende' afbeeldingen, de moduulhomomorfismen.

16.2. Definitie. *Een homomorfisme $M \to N$ van R-modulen is een groepshomomorfisme $f : M \to N$ dat voldoet aan $f(rm) = rf(m)$ voor alle $r \in R$ en $m \in M$.*

Men spreekt ook wel van *R-homomorfismen* of *R-lineaire afbeeldingen*. Is de ring R een lichaam, dan vindt men de bekende definitie uit de lineaire algebra terug. Voor $R = \mathbf{Z}$ krijgt men een homomorfisme van abelse groepen.

Zoals bekend (opgave 4.41) is de verzameling $\mathrm{Hom}(M, N)$ van homomorfismen $M \to N$ van abelse groepen zelf ook weer een abelse groep, met som gedefinieerd door $(f_1+f_2)(m) = f_1(m)+f_2(m)$. De deelverzameling $\mathrm{Hom}_R(M, N)$ van R-homomorfismen $M \to N$ is hiervan een *ondergroep*.

Opgave 3. Laat zien dat de groep $\mathrm{Hom}_R(M, N)$ voor *commutatieve* R een R-moduul wordt indien we $(rf)(m) = rf(m)$ definiëren voor $r \in R$ en $f \in \mathrm{Hom}_R(M, N)$.

Nemen we $M = N$, dan is op soortgelijke wijze de verzameling $\mathrm{End}_R(M)$ van R-endomorfismen $M \to M$ een *deelring* van de endomorfismenring $\mathrm{End}(M) = \mathrm{End}_{\mathbf{Z}}(M)$ uit 11.8.

▶ Voorbeelden

De 'Cayley-afbeelding' $R \to \mathrm{End}(R^+) = \mathrm{End}_{\mathbf{Z}}(R)$ uit 11.12 laat zien dat iedere ring R een moduul over zichzelf is onder linksvermenigvuldiging. Algemener is ieder linksideaal $I \subset R$ een R-moduul, en dit maakt het begrip 'moduul' tot een generalisatie van het begrip 'ideaal'.

Is K een lichaam, dan is een K-moduul V niets anders dan een *K-vectorruimte*. De K-lineaire endomorfismen van V vormen een deelring $\mathrm{End}_K(V) \subset \mathrm{End}(V)$, en V is hierover een moduul door restrictie van scalairen. Heeft V een eindige basis $e_1, e_2, \ldots, e_n$ over K, dan kan men de elementen van V representeren als elementen van de n-dimensionale K-vectorruimte K^n, en $\mathrm{End}_K(V)$ identificeren met de matrixring $\mathrm{Mat}_n(K)$. De moduulstructuur van V over $\mathrm{End}_K(V)$ is dan de vertrouwde vermenigvuldiging van vectoren in K^n met matrices uit $\mathrm{Mat}_n(K)$. Merk op dat $\mathrm{End}_K(V)$ zelf ook weer een K-vectorruimte is.

Opgave 4. Is evenzo de productring R^n een moduul over de matrixring $\mathrm{Mat}_n(R)$?

Is R een ring, dan is een moduul over de polynoomring $R[X]$ een R-moduul M voorzien van een R-lineair endomorfisme $f \in \mathrm{End}_R(M)$. De structuurafbeelding $\phi : R[X] \to \mathrm{End}(M)$ ligt immers vast door de beperking $\phi|_R$ en het beeld $f = \phi(X) \in \mathrm{End}(M)$ van X onder ϕ. De beperking $\phi|_R$ maakt van M een R-moduul, en de commutatierelatie $Xr = rX$ in $R[X]$ impliceert dat $f = \phi(X)$ de vermenigvuldiging met $r \in R$ respecteert:

$f(rm) = rf(m)$ voor $m \in M$. In het bijzonder zien we dat voor een lichaam K een moduul over $K[X]$ een K-vectorruimte V is voorzien van een K-lineaire afbeelding $\phi(X) : V \to V$. Dit gezichtspunt is verhelderend in de lineaire algebra.

Opgave 5. Geef eenzelfde beschrijving van een moduul over de ring $K[X, X^{-1}]$ van Laurentpolynomen over een lichaam K.

Neemt men R een ring en G een groep, dan is een moduul over de groepenring $R[G]$ een R-moduul M voorzien van een werking van G op M als een groep van R-lineaire automorfismen. Immers, omdat iedere $g \in G$ een *eenheid* is in $R[G]$, ligt de structuurafbeelding $\phi : R[G] \to \mathrm{End}(M)$ vast door de beperking $\phi|_R$ die M tot een R-moduul maakt en het geïnduceerde homomorfisme $G \subset R[G]^* \to \mathrm{End}(M)^* = \mathrm{Aut}(M)$ van eenhedengroepen. Uit de commutatierelatie $gr = rg$ voor $r \in R$ en $g \in G$ zien we weer dat $\phi(g)$ in de groep $\mathrm{Aut}_R(M) = (\mathrm{End}_R(M))^*$ van R-lineaire automorfismen ligt. Is M een willekeurige abelse groep en G een ondergroep van $\mathrm{Aut}(M)$, dan is M op natuurlijke wijze een $\mathbf{Z}[G]$-moduul. Dergelijke modulen komen veelvuldig voor in de Galoistheorie.

Neemt men G een willekeurige groep en K een lichaam, dan is een $K[G]$-moduul een K-vectorruimte waarop G werkt als een groep van K-lineaire automorfismen. We zagen in de groepentheorie dat men een groep G met vrucht kan bestuderen middels zijn *werkingen* op diverse al dan niet voor de hand liggende verzamelingen. Hetzelfde geldt voor de *lineaire* werkingen van G op welgekozen K-vectorruimtes. Deze lineaire werkingen vormen het onderwerp van de *representatietheorie* van groepen.

Is $f : R_1 \to R_2$ een ringhomomorfisme, dan is R_2 niet alleen een moduul over zichzelf onder linksvermenigvuldiging, maar door restrictie van scalairen tevens een R_1-moduul. De vermenigvuldiging van $r_1 \in R_1$ met $r_2 \in R_2$ is gedefinieerd door $r_1 r_2 = f(r_1)r_2$. Het geval waarin R_1 commutatief is en $f[R_1]$ bevat is in het centrum van R_2 komt veel voor en draagt een aparte naam.

16.3. Definitie. *Een (centrale) algebra over een commutatieve ring R is een ring A voorzien van een ringhomomorfisme $R \to A$ dat R binnen het centrum $Z(A)$ afbeeldt.*

Omdat iedere ring A een uniek homomorfisme $\mathbf{Z} \to A$ toelaat met beeld in het centrum van A is iedere ring een $\mathbf{Z}$-algebra.

Het lichaam $\mathbf{C}$ van complexe getallen en de polynoomring $\mathbf{R}[X]$ zijn commutatieve $\mathbf{R}$-algebra's. De *quaternionenalgebra* $\mathbf{H} = \mathbf{R} + \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$ van Hamilton is een niet-commutatieve $\mathbf{R}$-algebra. Het is geen algebra over de deelring $\mathbf{R} + \mathbf{R}i \cong \mathbf{C}$ van $\mathbf{H}$.

Voor een commutatieve ring R zijn de polynoomring $R[X]$ en de groepenring $R[G]$ algebra's over R. De ring $R[X]$ is commutatief, de ring $R[G]$ is het voor $R \neq 0$ alleen als G abels is.

Voor iedere n-dimensionale vectorruimte V over een lichaam K is de ring $\mathrm{End}_K(V)$ van K-lineaire endomorfismen van V een K-algebra. Voor $n > 1$ is deze niet commutatief.

▶ Standaardconstructies

Veel begrippen die ons reeds bekend zijn uit de theorie van (abelse) groepen en de lineaire algebra laten zich zonder problemen generaliseren tot het geval van modulen over ringen die niet $\mathbf{Z}$ of een lichaam zijn.

Is M een R-moduul en $M' \subset M$ een ondergroep die onder vermenigvuldiging met R in zichzelf overgaat, dan heet M' een *deelmoduul* van M. Voor R gelijk aan $\mathbf{Z}$, een lichaam K of de groepenring $K[G]$ over K krijgt men de respectievelijke definities van ondergroep, deelruimte en deelrepresentatie.

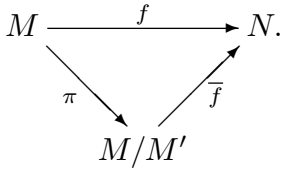
Voor een R-moduulhomomorfisme $f : M \to N$ zijn de kern $\ker f \subset M$ en het beeld $\operatorname{im} f = f[M] \subset N$ van f deelmodulen van respectievelijk M en N. Omdat f in het bijzonder een groepshomomorfisme is, is f wegens 4.4 injectief dan en slechts dan als $\ker f$ het nulmoduul is. Is $f : M \to N$ zowel injectief als surjectief, dan heeft f een tweezijdige inverse $f^{-1} \in \operatorname{Hom}_R(N, M)$ en is f een R-moduulisomorfisme. Isomorfie van R-modulen, wel aangegeven met $M \cong_R N$, is net als voor groepen een equivalentierelatie. Merk op dat twee R-modulen die isomorf zijn als abelse groepen dat niet als R-modulen hoeven te zijn: de werking van R op beide modulen kan verschillen.

Opgave 6. Geef een voorbeeld van twee niet-isomorfe modulen over een ring R die als abelse groepen isomorf zijn.

Is M een R-moduul en $M' \subset M$ een deelmoduul, dan heeft de factorgroep M/M' (die altijd bestaat omdat M abels is!) een natuurlijke R-moduulstructuur gegeven door

$$r(m + M') = rm + M' \in M/M'.$$

De homomorfie- en isomorfiestellingen uit de groepentheorie laten zich direct generaliseren naar R-modulen. Is $f : M \to N$ een homomorfisme van R-modulen en $M' \subset M$ een deelmoduul bevat in $\ker f$, dan zegt de *homomorfiestelling* voor modulen dat f via de natuurlijke afbeelding $\pi : M \to M/M'$ naar het quotiëntmoduul M/M' factoriseert als $f = \overline{f} \circ \pi$:



Voor $M' = \ker f$ is er de *isomorfiestelling* voor modulen: $\overline{f}$ geeft een isomorfisme

$$\overline{f} : M/\ker f \xrightarrow{\sim} f[M] \subset N.$$

Men kan de bewijzen hiervoor direct overnemen uit de groepentheorie, zie 4.9 en 8.4. Waar nodig dient men op te merken dat de optredende ondergroepen en homomorfismen nu deelmodulen en moduulhomomorfismen zijn.

Opgave 7. Formuleer en bewijs analoga voor modulen van de homomorfiestellingen 8.1 en 8.2 voor groepen.

Zij S een deelverzameling van een R-moduul M. De deelverzameling

$$RS = \{\textstyle\sum_{k=1}^{n} r_k s_k : r_k \in R, s_k \in S, n \in \mathbf{Z}_{\geq 1}\} \subset M$$

is het kleinste deelmoduul van M dat S bevat, en heet het deelmoduul *voortgebracht door* S. Hebben we $RS = M$, dan heet M voortgebracht door S, en S een stel voortbrengers van M. Het moduul M heet *eindig voortgebracht* als er een eindige deelverzameling $S \subset M$ bestaat met $RS = M$. Een moduul voortgebracht door een enkel element heet *cyclisch*. Voor $\mathbf{Z}$-modulen krijgen we de bekende definities voor abelse groepen terug. Een moduul dat eindig voortgebracht of cyclisch is *als moduul* is dat niet noodzakelijk als abelse groep. Zo is bijvoorbeeld iedere ring eindig voortgebracht als moduul over zichzelf, en zelfs cyclisch met voortbrenger 1, maar er zijn veel ringen waarvan de onderliggende abelse groep niet eindig voortgebracht is.

Opgave 8. Laat zien dat $\mathbf{R}^n$ een cyclisch $\mathrm{Mat}_n(\mathbf{R})$-moduul is.

Een deelverzameling $S \subset M$ van een R-moduul heet *lineair onafhankelijk* over R als voor $s_1, s_2, \ldots, s_n \in S$ verschillend en $r_i \in R$ slechts $r_1 s_1 + r_2 s_2 + \ldots + r_n s_n = 0$ kan gelden met $r_i = 0$ voor alle i. Een R-moduul M dat wordt voortgebracht door een lineair onafhankelijke deelverzameling $S \subset M$ heet *vrij* met basis S. Ieder element $m \in M$ heeft dan een *unieke* representatie als *eindige* som $m = \sum_{s \in S} r_s s$.

16.4. Voorbeeld. In de polynoomring $R[X]$ vormt de verzameling $\{X^k\}_{k=0}^{\infty}$ van machten van X een R-basis voor de polynoomring $R[X]$. Iets soortgelijks geldt voor de verzameling van 'monische monomen' $X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n}$ in $R[X_1, X_2, \ldots, X_n]$. In de machtreeksenring $R[[X]]$, die ook een R-moduul is, is $\{X^k\}_{k=0}^{\infty}$ wel lineair onafhankelijk, maar geen basis.

Gegeven een verzameling S kan men een vrij R-moduul $R^{(S)}$ met basis S construeren als de verzameling van eindige formele sommen

$$R^{(S)} = \{\textstyle\sum_{s \in S} r_s s : r_s \in R \text{ en } r_s \neq 0 \text{ voor slechts eindig veel } s\}$$

met componentsgewijze optelling en R-vermenigvuldiging. Dit laatste betekent dat men per definitie gelijkheden

$$\textstyle\sum_{s \in S} r_s s + \sum_{s \in S} r'_s s = \sum_{s \in S} (r_s + r'_s) s \qquad \text{en} \qquad r \sum_{s \in S} r_s s = \sum_{s \in S} (r r_s) s$$

heeft. Er is een natuurlijke inclusie $S \to R^{(S)}$ gegeven door $s \mapsto 1 \cdot s$. Voor $R = \mathbf{Z}$ herkennen we in het bovenstaande de vrije abelse groep met basis S, voor $R = K$ een lichaam krijgen we de K-vectorruimte met basis S.

Gegeven een familie $\{M_i\}_{i \in I}$ van R-modulen is hun *direct product* $\prod_{i \in I} M_i$ gedefinieerd als de productgroep

$$\textstyle\prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i\}$$

met componentsgewijze R-vermenigvuldiging: $r \cdot (m_i)_{i \in I} = (r m_i)_{i \in I}$. Voor iedere $i_0 \in I$ is de projectie $p_{i_0} : \prod_{i \in I} M_i \to M_{i_0}$ een surjectief R-homomorfisme.

De *directe som* $\bigoplus_{i\in I} M_i$ van de familie $\{M_i\}_{i\in I}$ is het deelmoduul van $\prod_{i\in I} M_i$ bestaande uit die elementen $(m_i)_{i\in I}$ die voor slechts eindig veel $i \in I$ een component $m_i \neq 0$ hebben. Voor iedere $i_0 \in I$ is er een injectief R-homomorfisme $\varepsilon_{i_0} : M_{i_0} \to \bigoplus_{i\in I} M_i$ dat op alle coördinaten buiten i_0 de waarde 0 aanneemt. Men kan $\bigoplus_{i\in I} M_i$ zien als het deelmoduul van $\prod_{i\in I} M_i$ voortgebracht door alle beelden $\varepsilon_i[M_i]$. Merk op dat voor *eindige* families de directe som en het directe product samenvallen. Bekijken we echter de in voorbeeld 16.4 optredende ringen $R[X]$ en $R[[X]]$ als R-modulen, dan is $R[X]$ een directe *som* van aftelbaar oneindig veel modulen R, terwijl $R[[X]]$ een direct *product* is van aftelbaar oneindig veel modulen R.

Opgave 9. Laat zien dat $R[X]$ en $R[[X]]$ voor een commutatieve ring $R \neq 0$ niet isomorf zijn als R-modulen. (Het algemene geval is moeilijker: zie opgaven 58 en 59.)

Net als in het geval van abelse groepen kunnen R-modulen vaak als sommen of producten van 'eenvoudiger' modulen geschreven worden. Om zo'n 'ontbinding' in kleinere bouwstenen te vinden is ook hier het taalgebruik van exacte rijtjes bijzonder nuttig.

Een rijtje $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ van modulen en moduulhomomorfismen heet *exact* als het exact is als rijtje van abelse groepen, dus als $\mathrm{im}(f) = \ker(g)$ geldt. Wegens de isomorfiestelling induceert een kort exact rijtje

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

van R-modulen een R-moduulisomorfisme $\overline{g} : M_2/M_1 \xrightarrow{\sim} M_3$. Het heet *gesplitst* als er een R-isomorfisme $\phi : M_2 \xrightarrow{\sim} M_1 \oplus M_3$ bestaat zodat $\phi \circ f$ de inbedding op de eerste coördinaat is en g uit ϕ verkregen wordt door samenstelling van ϕ met de projectie op de tweede coördinaat. Deze definitie is een directe generalisatie van 9.2, en als in 9.3 laat men zien dat het rijtje gesplitst is precies wanneer f of g een *sectie* toestaat.

Opgave 10. Laat zien dat g een sectie toelaat als M_3 een vrij R-moduul is.

▶ Modulen over hoofdideaaldomeinen

Vrijwel alles wat we in §9 bewezen hebben over de structuur van $\mathbf{Z}$-modulen laat zich probleemloos generaliseren tot het geval van modulen over een *hoofdideaaldomein* R. Bij wijze van illustratie geven we het analogon van 9.11: de structuurstelling voor eindig voortgebrachte modulen over een hoofdideaaldomein R.

We generaliseren eerst een aantal begrippen voor $\mathbf{Z}$-modulen tot R-modulen. Voor een R-moduul M heeft ieder element $m \in M$ een *annihilator*

$$\mathrm{Ann}_R(m) = \{r \in R : rm = 0\}.$$

Dit is een linksideaal van R, en $m \in M$ heet een *torsie-element* als zijn annihilator $\mathrm{Ann}_R(m) \subset R$ niet het nulideaal is. Voor een domein R vormen de torsie-elementen het *torsiedeelmoduul* $T(M) \subset M$ van M. Een moduul M over een domein R heet *torsievrij* als $T(M)$ het nulmoduul is, en een *torsiemoduul* over R als $T(M) = M$ geldt.

Opgave 11. Laat zien dat als R geen domein is de som van twee torsie-elementen niet altijd torsie is.

We nemen nu verder aan dat M een moduul is over een *hoofdideaaldomein* R. De *orde* van een torsie-element $m \in M$ is dan gedefinieerd als een voortbrenger van de annihilator $\mathrm{Ann}_R(m)$ van m. Deze is, zoals iedere voortbrenger van een ideaal, bepaald tot op vermenigvuldiging met eenheden in R. Het ideaal

$$\mathrm{Ann}_R(M) = \bigcap_{m \in M} \mathrm{Ann}_R(m)$$

is de *annihilator* van M in R. Geldt $\mathrm{Ann}_R(M) \neq 0$, dan is M een torsiemoduul en noemen we een voortbrenger van $\mathrm{Ann}_R(M)$ de *exponent* van M. Wegens 12.17 is in dit geval $\mathrm{Ann}_R(M)$ een product van priemidealen $(p) \neq 0$ in R.

Opgave 12. Ga na dat we voor $R = \mathbf{Z}$ de bekende definities van orde en exponent voor abelse groepen terugkrijgen.

Voor een priemideaal $(p) \subset R$ verschillend van 0 definiëren we het *p-macht-torsiemoduul* $M(p) \subset M$ als de ondergroep van M bestaande uit elementen waarvan de orde een p-macht is. Wegens de commutativiteit van R is dit een deelmoduul van M.

16.5. Stelling. *Zij R een hoofdideaaldomein en M een eindig voortgebracht moduul over R. Dan is M een directe som van een eindig aantal cyclische R-modulen.*
Er bestaan $r \in \mathbf{Z}_{\geq 0}$, de vrije rang van R, en een isomorfisme

$$M \cong_R T(M) \oplus R^r.$$

Het torsiedeelmoduul $T(M)$ van M is de directe som van eindig veel p-macht-torsiemodulen $M(p)$, één voor ieder priemideaal (p) dat de exponent van $T(M)$ deelt. Voor ieder priemideaal (p) is er een R-isomorfisme

$$M(p) \xrightarrow{\sim} R/(p^{k_1}) \oplus R/(p^{k_2}) \oplus \ldots \oplus R/(p^{k_m})$$

voor uniek bepaalde gehele getallen $k_1 \geq k_2 \geq \ldots \geq k_m > 0$.

Bewijs. Het bewijs is een directe generalisatie van het geval $R = \mathbf{Z}$. Men bewijst eerst als in 9.7 dat ieder deelmoduul van R^n vrij is van rang $k \leq n$, en leidt hieruit als in 9.9 af dat een eindig voortgebracht torsievrij R-moduul een vrij R-moduul is. Voor ons eindig voortgebrachte R-moduul M is $M/T(M)$ eindig voortgebracht en torsievrij, dus isomorf met R^r voor zekere $r \geq 0$. De exacte rij $0 \to T(M) \to M \to M/T(M) \to 0$ splitst (opgave 10), en dit geeft het eerste deel van de stelling.

Omdat $T(M)$ eindig voortgebracht en torsie is, is de exponent van $T(M)$ verschillend van 0, en dus wegens 12.17 te schrijven als een eindig product $E = \prod_{(p)} p^{e_p}$ van priemidealen (p). Neem een priemelement $p|E$, en schrijf $E = p^{e_p}E'$. Omdat p^{e_p} en E' onderling ondeelbaar zijn, kunnen we $xp^{e_p} + yE' = 1$ schrijven in R, en ieder element $m \in M$ is dan te schrijven als $m = xp^{e_p}m + yE'm$. De eerste term wordt geannihileerd door E', de tweede door p^{e_p}. Dit geeft een decompositie $T(M) = M' \oplus M(p)$ van R-modulen, en met inductie vindt men een isomorfisme $T(M) \cong_R \bigoplus_{(p)|E} M(p)$.

Voor het p-macht-torsiemoduul $M(p)$ tenslotte kopieert men het bewijs van 9.11. Is $m \in M(p)$ van maximale orde $p^{k_1} = p^{e_p}$ in $M(p)$, dan geldt $M(p) = Rm \oplus M'$ door constructie van een geschikte splitsing, en met inductie geeft dit een representatie van de gewenste vorm. Voor de uniciteit van de k_i en de vrije rang r verwijzen we naar de opgaven 32 en 55. □

▶ Lineaire algebra

Ter afsluiting van deze paragraaf laten we zien hoe in de lineaire algebra de theorie van modulen toegepast kan worden. We nemen hier als grondring een *lichaam* K. Zoals reeds opgemerkt is een K-moduul niets anders dan een K-vectorruimte, en een K-moduulhomomorfisme een K-lineaire afbeelding. Anders dan modulen over willekeurige ringen zijn modulen over lichamen altijd vrij. De existentie van bases voor vectorruimtes is echter in het oneindig-dimensionale geval niet evident: probeer maar eens een basis voor $\mathbf{R}$ als $\mathbf{Q}$-vectorruimte aan te geven!

16.6. Stelling. *Zij K een lichaam en V een K-vectorruimte. Dan is V vrij over K. Gegeven een verzameling voortbrengers $T \subset V$ van V en een lineair onafhankelijke verzameling $S \subset T$ bestaat er een K-basis B van V met $S \subset B \subset T$.*

Bewijs. De eerste uitspraak volgt uit de tweede door $S = \emptyset$ en $T = V$ te nemen. Voor de tweede uitspraak passen we het lemma van Zorn 15.11 toe op de collectie $\mathcal{C}$ van lineair onafhankelijke deelverzamelingen van T die S bevatten. De collectie $\mathcal{C}$ is niet leeg omdat hij S bevat, en onder de partiële ordening gegeven door inclusie heeft iedere keten in $\mathcal{C}$ een bovengrens bestaande uit de vereniging van zijn elementen. Wegens Zorn is er nu een maximaal element $B \in \mathcal{C}$. We moeten laten zien dat V door B wordt voortgebracht. Omdat V voortgebracht wordt door T is het voldoende te laten zien dat ieder element $t \in T$ bevat is in het deelmoduul $K \cdot B$ voortgebracht door B. Voor $t \in B$ is dit duidelijk, dus neem $t \in T \setminus B$. Dan is $B \cup \{t\}$ wegens de maximaliteit van B niet lineair onafhankelijk, dus er is een niet-triviale relatie $at + \sum_{x \in B} a_x x = 0$. Omdat B lineair onafhankelijk geldt $a \neq 0$, en omdat K een lichaam is vinden we zoals verlangd $t = -\sum_{x \in B} a^{-1} a_x x \in K \cdot B$. □

Stelling 16.6 laat zien dat we een basis van V kunnen opvatten als een maximale lineair onafhankelijke verzameling in V of als een minimale verzameling van voortbrengers van V. De cardinaliteit van een K-basis van V heet de *dimensie* $\dim(V) = \dim_K(V)$ van V over K. We laten zien dat deze niet van de keuze van de basis afhangt.

16.7. Stelling. *Ieder tweetal bases van een vectorruimte V heeft dezelfde cardinaliteit.*

Bewijs. Stel eerst dat V een basis B van eindige cardinaliteit n heeft. We bewijzen dan met inductie naar n dat iedere andere basis B' van V *ten hoogste* n elementen heeft – wegens symmetrie in B en B' is dit voldoende. Voor $n = 0$ hebben we $V = 0$ en is er niets te bewijzen. Voor $n \geq 1$ heeft B' een element $x \neq 0$, en toepassing van 16.6 met $S = \{x\}$ en $T = \{x\} \cup B$ geeft een deelverzameling $B_0 \subset B$ met $x \notin B_0$ waarvoor $\{x\} \cup B_0$ een basis voor V is. Er geldt $B_0 \neq B$ wegens de maximaliteit van B, dus B_0 heeft ten hoogste $n - 1$ elementen. Omdat B_0 en $B' \setminus \{x\}$ beiden een basis geven voor de quotiëntruimte V/Kx zegt de inductiehypothese dat $B' \setminus \{x\}$ ten hoogste $n-1$ elementen heeft, dus B' heeft ten hoogste n elementen en we zijn klaar.

Stel nu dat V geen basis van eindige cardinaliteit heeft. Gegeven twee bases B en B' van V kiezen we voor iedere $x \in B$ een eindige deelverzameling $C_x \subset B'$ met $x \in K \cdot C_x$. Men kan bijvoorbeeld voor C_x de verzameling van elementen $x' \in B'$ nemen

die voorkomen in de representatie van x op de basis B'. Er geldt $\bigcup_{x\in B} C_x = B'$, want $\cup_{x\in B} C_x$ brengt V voort. Omdat iedere C_x eindig is en B oneindig, is de cardinaliteit van $B' = \cup_{x\in B} C_x$ niet groter dan die van B. Wegens symmetrie hebben B en B' nu dezelfde cardinaliteit. □

Omdat K-vectorruimtes vrij zijn, splitst *ieder* kort exact rijtje $0 \to U \to V \to W \to 0$ van K-vectorruimtes (opgave 10) en hebben we $V \cong U \oplus W$. In het bijzonder hebben we voor zo'n rijtje de dimensierelatie $\dim(V) = \dim(U) + \dim(W)$. Passen we dit toe op het korte exacte rijtje $0 \to \ker f \to V \xrightarrow{f} f[V] \to 0$ behorende bij een K-lineaire afbeelding $f : V \to W$, dan krijgen we de bekende *dimensiestelling*

$$\dim \ker f + \dim f[V] = \dim(V)$$

uit de lineaire algebra.

Lineaire afbeeldingen tussen eindig-dimensionale vectorruimtes hebben een *matrixrepresentatie* met betrekking tot gekozen bases van de vectorruimtes. Zijn V en W vectorruimtes met bases $\{x_1, x_2, \ldots, x_n\}$ en $\{y_1, y_2, \ldots, y_m\}$, dan noteert men de lineaire afbeelding $A : V \to W$ gegeven door $Ax_j = \sum_{i=1}^{m} a_{ij} y_i$ voor $j = 1, 2, \ldots, n$ als een $m \times n$-matrix

$$A = (a_{ij})_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Hieruit ziet men dat de verzameling $\mathrm{Hom}_K(V, W)$ van K-lineaire afbeeldingen $V \to W$, die op natuurlijke wijze zelf weer een K-vectorruimte is, dimensie mn heeft. Samenstelling van lineaire afbeeldingen tussen vectorruimtes in termen van matrices geeft aanleiding tot de bekende *matrixvermenigvuldiging* van $m \times n$- en $n \times r$-matrices ('rijtje maal kolommetje') die de lezer zelf met meervoudige somtekens mag uitschrijven.

▶ Normaalvormen voor matrices

Veel expliciete berekeningen in de lineaire algebra maken gebruik van de matrixrepresentatie van lineaire afbeeldingen, maar 'lineaire afbeelding' en 'matrix' zijn niet synoniem: pas na een *keuze* van bases wordt een lineaire afbeelding door een matrix beschreven. Voor een n-dimensionale K-vectorruimte V leidt de keuze van een basis tot een identificatie $\mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{Mat}_n(K)$ van de endomorfismenring van V met de ring van $n \times n$-matrices met coëfficienten in K. Gegeven een endomorfisme $A \in \mathrm{End}_K(V)$ probeert men de basis van V vaak zo te kiezen dat A een eenvoudige vorm krijgt. Heeft V bijvoorbeeld een basis bestaande uit *eigenvectoren* van A, dan heeft A ten opzichte hiervan een representatie als *diagonaalmatrix*. Dergelijke matrices zijn in berekeningen bijzonder efficiënt.

Het schrijven van een endomorfisme $A \in \mathrm{End}_K(V)$ in diagonaalvorm betekent dat men de vectorruimte V als directe som van 1-dimensionale deelruimten schrijft, die

elk door A in zichzelf worden overgevoerd. Dit is niet altijd mogelijk, maar men kan algemener proberen V als som te schrijven van deelruimtes die elk door A in zichzelf worden overgevoerd. Een *ontbinding* of *decompositie* $V = V_1 \oplus V_2$ als som van twee A-invariante deelruimtes van dimensie k en $n-k$ leidt tot een matrixrepresentatie van A als een 'blokmatrix'

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

waarbij A_i een matrix is die de werking van A op de deelruimte V_i beschrijft.

Het ontbinden van V in A-invariante deelruimtes van kleinere dimensie betekent dat men V opvat als moduul over de polynoomring $K[T]$ door T te laten werken als de transformatie A, en V schrijft als een directe som van $K[T]$-deelmodulen. Omdat $K[T]$ een hoofdideaaldomein is, is 16.5 direct van toepassing. De resulterende normaalvorm voor matrices heet de *rationale kanonieke vorm*, zie opgave 42. Voor algebraïsch afgesloten grondlichamen K, zoals $K = \mathbf{C}$, is deze vorm bijzonder eenvoudig.

16.8. Jordan-normaalvorm van matrices. *Zij A een endomorfisme van een eindigdimensionale vectorruimte V over een algebraïsch afgesloten lichaam K. Dan bestaat er een decompositie $V = V_1 \oplus V_2 \oplus \ldots \oplus V_d$ van V als som van A-invariante deelruimtes, en voor ieder van de deelruimtes V_i is er een basis waarop A een matrixrepresentatie*

$$A|_{V_i} = \begin{pmatrix} \lambda_i & 1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_i & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \lambda_i & 1 \\ 0 & 0 & \ldots & 0 & 0 & \lambda_i \end{pmatrix}$$

heeft met coëfficiënten $\lambda_i \in K$ op de diagonaal, coëfficiënten 1 op een nevendiagonaal en coëfficiënten 0 elders.

Bewijs. Vat V op als moduul over $R = K[T]$ door T als A te laten werken. Dan is V eindig voortgebracht over R, en zelfs over K. Omdat R oneindige dimensie heeft als vectorruimte over K is ieder element $v \in V$ een R-torsie-element, en V een R-torsiemoduul. Omdat K algebraïsch afgesloten is, is ieder priemelement in $R = K[T]$ op een eenheid na gelijk aan $T - \lambda$ voor zekere $\lambda \in K$. Stelling 16.5 geeft ons een decompositie $V = \bigoplus_{i=1}^{d} V_i$ van V als som van cyclische R-modulen $V_i = R/(T-\lambda_i)^{n_i}$. Kiezen we als basis voor V_i de machten $(T-\lambda_i)^k$ voor $k = n_i - 1, , n_i - 2, \ldots, 2, 1, 0$, dan werkt vermenigvuldiging met $T - \lambda_i$ op deze basis door 'opschuiven':

$$0 \leftarrow (T-\lambda_i)^{n_i-1} \leftarrow (T-\lambda_i)^{n_i-2} \leftarrow (T-\lambda_i)^{n_i-3} \leftarrow \ldots \leftarrow T - \lambda_i \leftarrow 1.$$

Dit betekent dat $A - \lambda_i$ op V_i ten opzichte van deze basis een matrix is met coëfficiënten 1 op de nevendiagonaal boven de hoofddiagonaal en coëfficiënten 0 elders. Er volgt direct dat A op V_i de gewenste matrixrepresentatie heeft. □

Ten opzichte van de basis van V bestaande uit de vereniging van de in 16.8 aangegeven bases voor elk van de V_i heeft de matrix A de zogenaamde Jordan-normaalvorm: een blokmatrix bestaande uit de in de stelling aangegeven '*Jordanblokken*' langs de diagonaal. Omdat de Jordanblokken niets anders zijn dan een 'vertaling' van de structuur van V als $K[T]$-moduul in de zin van 16.5, is deze vorm op de volgorde van de blokken na uniek bepaald.

De waarden $\lambda_i \in K$ in 16.8 behorende bij de deelruimten V_i zijn de *eigenwaarden* van A, en in onze representatie is steeds de eerste basisvector van V_i een eigenvector met eigenwaarde λ_i. Merk op dat Jordanblokken voor verschillende componenten V_i *dezelfde* eigenwaarde λ_i kunnen hebben, en dat het *aantal* Jordanblokken met eigenwaarde λ gelijk is aan de dimensie van de eigenruimte $\ker[A-\lambda]$ behorende bij λ. Voor een eigenwaarde λ van A noemt men de deelruimte $V_\lambda = \bigoplus_{\lambda_i=\lambda} V_i$ van V de *gegeneraliseerde eigenruimte* behorende bij λ. Er geldt

$$V_\lambda = \ker[(A-\lambda)^n] \qquad \text{met} \quad n = \dim_K V.$$

In feite is het voldoende voor de exponent n het maximum van de dimensies n_i van de 'Jordan-deelruimtes' $V_i \subset V_\lambda$ te nemen. De matrix A is *diagonaliseerbaar* over K dan en slechts dan als alle deelruimtes V_i één-dimensionaal zijn. In dit geval is $V_\lambda = \ker[A-\lambda]$ de 'gewone' eigenruimte behorende bij λ.

Aan de Jordan-normaalvorm van een matrix kan men alle bekende invarianten van de bijbehorende lineaire afbeelding aflezen. Zo vindt men voor het *karakteristieke polynoom* $P_A = \det(T \cdot I - A) \in K[T]$ van de afbeelding A in 16.8 de uitdrukking

$$P_A = \prod_{i=1}^{d} (T-\lambda_i)^{n_i} \in K[T].$$

Hier is n_i de dimensie van de deelruimte $V_i \subset V$. Naar analogie met het geval van eindige abelse groepen zou men het polynoom P_A de 'orde' van het $K[T]$-moduul V kunnen noemen. Ieder element van V wordt geannihileerd door deze 'orde', net zoals voor eindige abelse groepen alle groepselementen door de orde van de groep geannihileerd worden. De klassieke formulering van dit resultaat in de lineaire algebra, dat voor willekeurige grondlichamen geldt (opgave 45), is als volgt.

16.9. Stelling (Cayley-Hamilton). *Zij $P_A \in K[T]$ het karakteristieke polynoom van $A \in \mathrm{End}_K(V)$. Dan geldt $P_A(A) = 0 \in \mathrm{End}_K(V)$.* □

Zoals het voorbeeld $A = \mathrm{id}_V$ voor $\dim_K(V) > 1$ al laat zien, is het karakteristieke polynoom P_A is niet in het algemeen het kleinste polynoom $f \in K[T]$ met $f(A) = 0$. Men definieert het *minimumpolynoom* $f_A \in K[T]$ van A als het monische polynoom van de kleinst mogelijke graad met deze eigenschap. Het is het analogon van de *exponent* van een eindige abelse groep. Zie opgave 46 voor enige eigenschappen van f_A.

Opgaven.

13. Zij K een lichaam. Laat zien dat een moduul over de polynoomring $K[X_1, X_2, \ldots, X_n]$ 'hetzelfde' is als een K-vectorruimte V voorzien van n commuterende K-lineaire afbeeldingen $V \to V$.

14. Zij M een moduul over een commutatieve ring R, en vat $\mathrm{Hom}_R(R, M)$ als in opgave 3 op als R-moduul. Bewijs dat de afbeelding $\mathrm{Hom}_R(R, M) \to M$ gegeven door $f \mapsto f(1)$ een isomorfisme van R-modulen is.

15. Zij I een linksideaal van een ring R en M een R-moduul. Laat zien dat
$$IM = \{\textstyle\sum_{k=1}^{n} i_k m_k : i_k \in I, m_k \in M, n \in \mathbf{Z}_{\geq 0}\}$$
een deelmoduul van M is, en dat in het geval I tweezijdig is het quotiëntmoduul M/IM een natuurlijke R/I-moduulstructuur heeft.

16. Een R-moduul M heet *simpel* als het precies twee deelmodulen heeft, 0 en M.
    a. Bewijs: een simpel R-moduul is cyclisch, en isomorf met R/I voor een maximaal linksideaal van R.
    b. Bewijs: ieder R-homomorfisme $f \neq 0$ tussen simpele R-modulen is een isomorfisme, en de endomorfismenring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ van een simpel R-moduul M is een delingsring.
    c. Waar komen a en b op neer voor $R = \mathbf{Z}$?

17. Zij K een lichaam en V een eindig-dimensionale K-vectorruimte. Ga na wanneer V een simpel R-moduul is voor $R = K$ en voor $R = \mathrm{End}_K(V)$. Bepaal in elk van beide gevallen voor simpele V de endomorfismenring $\mathrm{End}_R(V)$.

18. Zij M een R-moduul en $f \in \mathrm{End}_R(M)$ een *projectie*, i.e., een R-homomorfisme $f : M \to M$ met $f \circ f = f$. Bewijs dat er een isomorfisme $M \cong_R \ker f \oplus \mathrm{im}\, f$ is.

19. Zij R een ring en M een abelse groep met een R-vermenigvuldiging $R \times M \to M$ die voldoet aan de voorwaarden (M1)–(M3) gegeven na 16.1 ('een niet-unitair moduul').
    a. Laat zien dat er een ondergroep $M_1 \subset M$ bestaat die een R-moduul is, en een groepsisomorfisme $M \cong M_1 \oplus M_0$ zo dat de R-vermenigvuldiging op $M_1 \oplus M_0$ gegeven wordt door $r(m_1, m_0) = (rm_1, 0)$.
    b. Laat zien dat een R-homomorfisme $M = M_1 \oplus M_0 \to N = N_1 \oplus N_0$ van dergelijke objecten (definitie duidelijk) van de vorm $(m_1, m_0) \mapsto (f_1(m_1), f_0(m_0))$ is, met $f_1 \in \mathrm{Hom}_R(M_1, N_1)$ en $f_0 \in \mathrm{Hom}_{\mathbf{Z}}(M_0, N_0)$.

20. Laat zien dat voor iedere verzameling S het vrije R-moduul met basis S isomorf is met de directe som $\bigoplus_{s \in S} R$.

21. Zij R een ring en S een verzameling. Laat zien dat de verzameling R^S van functies $f : S \to R$ een natuurlijke R-moduulstructuur heeft, en dat er een isomorfisme $R^S \cong_R \prod_{s \in S} R$ van R-modulen is.

22. Zij R een commutatieve ring. Laat zien dat er R-isomorfismen $\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong_R \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$ en $\mathrm{Hom}_R(M, N_1 \oplus N_2) \cong_R \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2)$ zijn, en algemener
$$\mathrm{Hom}(\textstyle\bigoplus_{i \in I} M_i, N) \xrightarrow{\sim} \prod_{i \in I} \mathrm{Hom}(M_i, N)$$
$$\mathrm{Hom}(M, \textstyle\prod_{i \in I} N_i) \xrightarrow{\sim} \prod_{i \in I} \mathrm{Hom}(M, N_i).$$

23. Zij gegeven een exact rijtje $0 \to A \to B \to C \to 0$ van R-modulen.
    a. Bewijs dat B eindig voortgebracht is als A en C dat zijn.
    b. Laat zien dat de omkering van a niet algemeen geldt.
    c. Geldt de omkering van a voor een hoofdideaaldomein R?

24. Zij R een domein. Laat zien dat voor een exact rijtje $0 \to A \to B \to C$ van modulen over een domein R het geïnduceerde rijtje $0 \to T(A) \to T(B) \to T(C)$ van torsiedeelmodulen weer exact is. Is $T(B) \to T(C)$ surjectief als $B \to C$ het is?

25. Laat zien dat voor korte exacte rijtjes $0 \to A \to B \xrightarrow{f} C \to 0$ en $0 \to C \xrightarrow{g} D \to E \to 0$ van R-modulen de geïnduceerde rij $0 \to A \to B \xrightarrow{gf} D \to E \to 0$ weer exact is. Concludeer dat iedere lange exacte rij

$$0 \to A_1 \to A_2 \to A_3 \to \ldots \to A_{k-1} \to A_k \to 0$$

    van lengte k verkregen kan worden uit $k-2$ korte exacte rijtjes.

26. Formuleer en bewijs het analogon van 9.12 voor modulen over een hoofdideaaldomein.

27. Voor een moduul M over een commutatieve ring R definiëren we het *duale moduul* als $M^* = \mathrm{Hom}_R(M, R)$. Laat zien dat voor een exact rijtje $M_1 \to M_2 \to M_3 \to 0$ van R-modulen het geïnduceerde rijtje $0 \to M_3^* \to M_2^* \to M_1^*$ weer exact is. Is $M_2^* \to M_1^*$ surjectief als $M_1 \to M_2$ injectief is?

28. Bepaal M^* voor $M = \mathbf{Z}/m\mathbf{Z}$ als moduul over respectievelijk $R = \mathbf{Z}$ en $R = \mathbf{Z}/m\mathbf{Z}$. Bepaal ook de duale van een willekeurig eindig voortgebracht moduul over $\mathbf{Z}$.

29. Laat zien dat de duale van een vrij moduul $R^{(S)}$ met basis S isomorf is met het moduul R^S van R-waardige functies op S.

30. Laat zien dat er voor ieder moduul M over een commutatieve ring R een natuurlijk R-homomorfisme $M \to M^{**}$ is van M naar zijn dubbelduale moduul $M^{**} = (M^*)^*$. Beschrijf M^{**} voor $R = \mathbf{Z}$ en M eindig voortgebracht.

31. Een R-moduul M heet M *reflexief* als de natuurlijke afbeelding $M \to M^{**}$ een isomorfisme is. Laat zien dat eindig-dimensionale vectorruimten reflexief zijn, en dat een $\mathbf{Q}$-vectorruimte van oneindige dimensie *niet* reflexief is. *Is het grondlichaam $\mathbf{Q}$ essentieel voor deze bewering?

32. Laat zien dat voor een commutatieve ring $R \neq 0$ de vrije R-modulen $R^{(X)}$ en $R^{(Y)}$ isomorf zijn dan en slechts dan als X en Y dezelfde cardinaliteit hebben.
    [Hint: gebruik dat R een maximaal ideaal heeft om te reduceren tot 16.7.]

33. Zij A een ring.
    a. Laat zien dat er een A-moduul $M \neq 0$ bestaat met $M \oplus M \cong_A M$.
    b. Neem $R = \mathrm{End}_A(M)$, met M een A-moduul als in a. Bewijs dat voor willekeurige eindige verzamelingen X en Y de vrije modulen R^X en R^Y isomorf zijn.

34. Een *hypervlak* in een vectorruimte V is de kern van een niet-nul element $f \in V^*$. Laat zien dat iedere deelruimte $V' \subset V$ de doorsnijding is van de hypervlakken die V' bevatten.

35. Zij B een basis voor de vectorruimte V en $y \in V$ een element verschillend van 0. Laat zien dat er een element $x \in B$ bestaat waarvoor $\{y\} \cup (B \setminus \{x\})$ een basis is voor V. Leid uit dit *uitwisselingsprincipe van Steinitz* het eindig-dimensionale geval van 16.7 af.

36. Zij gegeven een dalende rij van verzamelingen $V \supset T_1 \supset T_2 \supset T_3 \supset \ldots$ in V, en stel dat iedere verzameling T_i de vectorruimte V voortbrengt. Is $\bigcap_{i=1}^{\infty} T_i$ noodzakelijk een voortbrengende verzameling voor V?

37. Zij R een hoofdideaaldomein. Bewijs: ieder deelmoduul van een vrij R-moduul is vrij. [Hint: Zij N vrij met basis B en $M \subset N$. Kijk nu naar de deelverzamelingen $C \subset B$ waarvoor $M \cap R \cdot C$ vrij is en pas het lemma van Zorn toe.]

38. Bewijs dat voor een exacte rij van eindig-dimensionale K-vectorruimtes

$$0 \to V_1 \to V_2 \to V_3 \to \ldots \to V_{n-1} \to V_n \to 0$$

de relatie $\sum_{i=1}^{n} (-1)^i \dim_K(V_i) = 0$ geldt.

39. Bepaal de Jordan-normaalvorm van de complexe matrix

$$A = \begin{pmatrix} 5 & 0 & -2 \\ 13 & 3 & 7 \\ 3 & 0 & 0 \end{pmatrix}.$$

40. Bepaal de Jordan-normaalvorm van de matrix

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

voor $K = \mathbf{C}$ en voor $K \supset \mathbf{F}_3$ algebraïsch afgesloten.

41. Vind de Jordan-normaalvorm van de matrix in $\mathrm{Mat}_n(K)$ waarvan alle coëfficiënten gelijk aan 1 zijn. Is de karakteristiek van K hierbij van belang?

De vectorruimtes V in alle verdere opgaven worden geacht *eindig-dimensionaal* te zijn.

42. (*Rationale kanonieke vorm*) Bewijs dat gegeven $A \in \mathrm{End}_K(V)$ er een decompositie $V = \bigoplus_i V_i$ van V als som van A-invariante deelruimtes bestaat zodat A ten opzichte van een geschikte basis van V_i werkt als

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & a_1 \\ 1 & 0 & 0 & \ldots & 0 & a_2 \\ 0 & 1 & 0 & \ldots & 0 & \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & a_{n-1} \\ 0 & 0 & 0 & \ldots & 1 & a_n \end{pmatrix}$$

43. Voor een complexe vectorruimte V en $A \in \mathrm{End}_{\mathbf{C}}(V)$ definieert men de *exponentiaal-afbeelding* $\exp(A) : V \to V$ door de identiteit $\exp(A) \cdot v = \sum_{k=0}^{\infty} \frac{1}{k!} A^k v$. Laat zien dat dit tot een welgedefinieerd endomorfisme $\exp(A) \in \mathrm{End}_{\mathbf{C}}(V)$ aanleiding geeft, en bereken $\exp(A)$ voor de matrices in de opgaven 39 en 40.

44. Zij V een complexe vectorruimte en $A \in \mathrm{End}_{\mathbf{C}}(V)$ een endomorfisme waarvoor $A^m = I$ geldt voor zekere $m \in \mathbf{Z}_{>0}$. Bewijs dat A diagonaliseerbaar is. *Is dit ook waar als we $\mathbf{C}$ door een willekeurig algebraïsch afgesloten lichaam vervangen?

45. Laat zien dat stelling 16.9 geldt voor willekeurige grondlichamen K.

46. Definieer voor $A \in \mathrm{End}_K(V)$ het minimumpolynoom $f_A \in K[T]$ als na 16.9. We vatten V op als $K[T]$-moduul door T als A te laten werken. Bewijs de de volgende uitspraken.
    1. f_A is een welgedefinieerd element van $K[T]$;
    2. V is een $K[T]$-torsiemoduul van exponent f_A;
    3. f_A is een deler van het karakteristieke polynoom P_A;
    4. P_A deelt een macht van f_A.

47. Laat het karakteristieke polynoom P_A en het minimumpolynoom f_A van $A \in \mathrm{End}_K(V)$, met K een algebraïsch afgesloten lichaam van karakteristiek ongelijk aan 2, voldoen aan

$$P_A = f_A \cdot (T^2+1)^2$$
$$f_A^3 = P_A \cdot (T-1)^4.$$

    Bepaal de Jordan-normaalvorm van A.

48. Bewijs dat een endomorfisme $A \in \mathrm{End}_K(V)$ diagonaliseerbaar is (over $\overline{K}$) dan en slechts dan als zijn minimumpolynoom geen meervoudige nulpunten heeft in $\overline{K}$.

49. Laat de vectorruimte V een $K[T]$-moduul zijn via $A \in \mathrm{End}_K(V)$. Bewijs dat de volgende uitspraken equivalent zijn.
    1. $f_A = P_A$;
    2. V is een cyclisch $K[T]$-moduul;
    3. er bestaat een basis $\{e_1, e_2, \ldots, e_n\}$ voor V waarop A werkt door opschuiven: $e_1 \mapsto e_2 \mapsto e_3 \mapsto \ldots \mapsto e_{n-1} \mapsto e_n$.

50. Laat $A, B \in \mathrm{End}_K(V)$ diagonaliseerbare endomorfismen zijn, en stel dat A en B commuteren. Bewijs dat er een basis van V is ten opzichte waarvan A en B beide diagonaalmatrices zijn.

51. Zij $f \in K[T]$ een polynoom en $A \in \mathrm{End}_K(V)$ een endomorfisme met karakteristiek polynoom $P_A = \prod_{i=1}^n (T-\lambda_i) \in K[T]$. Bewijs dat $B = f(A) \in \mathrm{End}_K(V)$ karakteristiek polynoom $P_B = \prod_{i=1}^n (T - f(\lambda_i))$ heeft.

52. Laat $A, B \in \mathrm{End}_K(V)$ diagonaliseerbare endomorfismen zijn. Zijn $A+B$ en AB noodzakelijk diagonaliseerbaar?

53. Geef voor elk van de volgende uitspraken over complexe matrices een bewijs of een tegenvoorbeeld.
    1. Als A^2 diagonaliseerbaar is, dan is A diagonaliseerbaar.
    2. Als $A^2 = A$ geldt, dan is A diagonaliseerbaar.
    3. Als A^5 diagonaliseerbaar is en A inverteerbaar, dan is A diagonaliseerbaar.

54. Zij $A \in \mathrm{End}_{\mathbf{R}}(V)$ een matrix die diagonaliseerbaar is over $\mathbf{C}$. Bewijs dat V geschreven kan worden als een som $\oplus_i V_i$ van A-invariante deelruimtes van dimensie $\dim V_i \leq 2$, waarbij de 2-dimensionale deelruimtes V_i een basis hebben waarop A de matrixrepresentatie $\begin{pmatrix} \lambda_i \cos\phi & -\lambda_i \sin\phi \\ \lambda_i \sin\phi & \lambda_i \cos\phi \end{pmatrix}$ heeft voor zekere $\lambda_i \in \mathbf{R}^*$ en $\phi \in (0, \pi)$.

55. Laat zien dat voor het p-macht-torsiemoduul $M(p)$ in stelling 16.5 het *aantal* k_i's groter dan $e \in \mathbf{Z}_{\geq 0}$ gelijk is aan de dimensie van $p^e M(p)/p^{e+1}M(p)$ als vectorruimte over $R/(p)$.

Concludeer dat de k_i's eenduidig bepaald zijn door het isomorfietype van het R-moduul $M(p)$.

56. Bepaal alle isomorfietypen van R-modulen met niet meer dan 16 elementen voor $R = \mathbf{Z}$ en voor $R = \mathbf{Z}[i]$.

57. Bepaal alle isomorfietypen van $\mathbf{F}_2[X]$-modulen M met $\dim_{\mathbf{F}_2}(M) \leq 3$. Geef voor ieder type de matrix waarmee X werkt op M (ten opzichte van een zelfgekozen basis).

*58. Zij R een ring. Bewijs dat er een rechts-R-moduul $M \neq 0$ is zodat M isomorf is met $\bigoplus_{n=1}^{\infty} M$, en dat voor elke dergelijke M de ring $A = \mathrm{End}_R M$ de eigenschap heeft dat A en $\prod_{n=1}^{\infty} A$ isomorf zijn als links-A-modulen.

*59. (G.M. Bergman). Laat R een ring zijn.
   a. Stel M_1, M_2, ... zijn R-modulen die geen van alle eindig voortgebracht zijn. Bewijs: $M = \prod_{n=1}^{\infty} M_n$ is niet aftelbaar voortgebracht, d.w.z. M heeft geen aftelbare deelverzameling die M als R-moduul voortbrengt.
   [Hint: gegeven x_1, x_2, ... $\in M$, construeer met een diagonaalmethode een element van M dat voor geen enkele i in $Rx_1 + \ldots + Rx_i$ ligt.]
   b. Bewijs: als het R-moduul $\prod_{n=1}^{\infty} R$ aftelbaar voortgebracht is, dan is het zelfs eindig voortgebracht.
   c. Bewijs dat voor $R \neq 0$ de R-modulen $\bigoplus_{n=1}^{\infty} R$ en $\prod_{n=1}^{\infty} R$ niet isomorf zijn.

60. Laat R een ring zijn, M een cyclisch R-moduul, en $N \subset M$ een deel-R-moduul.
   a. Bewijs: M/N is een cyclisch R-moduul.
   b. Is N automatisch cyclisch? Geef een bewijs of een tegenvoorbeeld.
   c. Als (b), maar nu met de aanname dat R een hoofdideaaldomein is.

Literatuurverwijzingen

1. De meeste algebraboeken behandelen niet alleen groepen, maar ook ringen en lichamen. In het bijzonder is dit het geval voor de in de vorige syllabus reeds genoemde boeken van Artin, Shafarevich, Lang, Gallian en Van der Waerden.

2. De representatie van priemen door kwadratische vormen als $x^2 + y^2$ is het startpunt van een zeer toegankelijk boek van Cox. Dit boek is tevens een goede inleiding tot de algebraïsche getaltheorie.

- D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, 1989. Second edition 2013.

3. Behalve het zojuist genoemde boek zijn er diverse boeken die min of meer elementaire inleidingen tot de algebraïsche getaltheorie geven. Het boek van Ireland en Rosen sluit goed aan op deze paragraaf. Kummer's ideaaltheorie is te vinden in het boekje van Stewart en Tall.

- K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84, 1982. Second edition 1990.
- I. Stewart, D. O. Tall, *Algebraic number theory and Fermat's last theorem*, Chapman & Hall, 1979, fourth edition 2015.

4. Het eerste van de twee delen van Kummer's verzameld werk, dat zijn getaltheoretisch werk bevat, heeft als 'Anmerkung' (pp. 243–245) bij een lang artikel uit 1847 over ideale priemfactoren een verhandeling over de analogie met de chemie. Of dergelijke analogieën meer dan 'Spiele des Witzes' zijn mag de moderne lezer zelf bepalen.

- E. E. Kummer, *Collected papers*, uitgegeven door A. Weil, Springer, 1975.

5. Er blijkt een onverwacht verband te bestaan tussen 5 mod p en p mod 5: de eerste is een kwadraat in $(\mathbf{Z}/p\mathbf{Z})^*$ dan en slechts dan als de tweede een kwadraat is in $(\mathbf{Z}/5\mathbf{Z})^*$. Dit is een speciaal geval van de kwadratische reciprociteitswet. Deze wet werd ontdekt door Euler en bewezen door de 19-jarige Gauss. Er zijn bewijzen door 'slim tellen', zoals in het boek van Hardy en Wright. Paragraaf 26 van de syllabus Algebra 3 geeft een meer conceptueel bewijs dat gebruik maakt van cyclotomische lichamen.

- G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1938. Er zijn diverse verbeterde herdrukken.

6. Het is niet bekend of 5 mod p een primitieve wortel is voor oneindig veel priemgetallen p. Een door de Duitser Emil Artin (1898–1962) uitgesproken vermoeden zegt dat dit wel zo is, en maakt precies hoeveel van zulke priemen $p < N$ men voor grote N kan verwachten. Onder aanname van een onbewezen vermoeden, de zogenaamde gegeneraliseerde Riemannhypothese voor de ligging van nulpunten van zeta-functies, kan men Artin's vermoeden bewijzen.

- M. Ram Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10, no. 4, 59–67 (1988).

7. André Weil's review van het verzameld werk van Eisenstein, dat in de jaren zeventig in drie delen bij Chelsea verscheen, is een klassiek geworden sprookje.

- A. Weil, *Review of 'Mathematische Werke' by Gotthold Eisenstein*, Bulletin of the AMS **VI**.82, pp. 658–663 (1976). Ook als pp. 398–403 in deel III van Weil's Œuvres scientifiques, Springer, 1979.

8. Over formules voor en benaderingen van π bestaat een enorme hoeveelheid literatuur. Het onderstaande boek, dat historisch materiaal van de meest uiteenlopende soort bevat, geeft een goede indruk.

- L. Berggren, J. Borwein, P. Borwein, *Pi, a source book*, Springer, 1997, 3rd edition 2004.

9. Voor informatie over de algoritmen die in de praktijk gebruikt worden om polynomen te factoriseren is er het boek van Cohen, dat op dit moment de standaardreferentie in de zogenaamde *algoritmische getaltheorie* is. Goede bovengrenzen op de coëfficiënten van een deler $g = \sum_{j=0}^{d} b_j X^j$ van een polynoom $f = \sum_{i=0}^{n} a_i X^i$ in $\mathbf{Z}[X]$, zoals

$$|b_j| \leq \tbinom{d-1}{j}(\textstyle\sum_{i=0}^{n} a_i^2)^{1/2} + \tbinom{d-1}{j-1}|a_n|,$$

zijn in 1974 gegeven door Mignotte. De uit 1982 stammende toepassing van roosterreductietechnieken op het factorisatieprobleem voor polynomen is een resultaat van de Nederlanders Arjen en Hendrik Lenstra (inderdaad, broers) en de Hongaar Lovász.

- H. Cohen, *A course in computational algebraic number theory*, Springer GTM, 1993.
- M. Mignotte, *An inequality about factors of polynomials*, Math. Comp. **28**, 1153–1157 (1974).
- A. K. Lenstra, H. W. Lenstra, Jr., L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261**, 515–534 (1982).

10. De opmerking dat de ringen $\mathbf{Z}/p^k\mathbf{Z}$ zich beter gedragen voor 'grote' k vindt zijn verklaring in het limietgeval $k = \infty$, dat aanleiding geeft tot de ring $\mathbf{Z}_p$ van p-adische getallen. Deze ring lijkt in veel opzichten meer op $\mathbf{R}$ dan op $\mathbf{Z}$. Zowel nuttig als leuk – zie de referenties.

- F. Q. Gouvêa, *p-adic Numbers*, Springer Universitext, 1993.
- N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-functions*, Springer GTM, 1977; second edition 1984.

11. De projectieve ruimte $\mathbf{P}^n(K)$ over een lichaam K maakt men door het toevoegen van 'punten in oneindig' aan de affiene ruimte K^n. Coxeter's boek geeft een klassieke benadering in de geest van Euclides, met veel aandacht voor het projectieve vlak (waarin elk tweetal lijnen een snijpunt heeft!) en de historie van het concept. De eenvoudige definitie van $\mathbf{P}^n(K)$ als verzameling van lijnen door de oorsprong in K^{n+1} komt men in veel teksten over lineaire algebra tegen, als ook in diverse boeken over (algebraïsche) meetkunde – zoals de bij volgende punten genoemde. Een aardige historische inleiding is hoofdstuk 7 in Stillwell's boek.

- H. S. M. Coxeter, *Projective geometry*, 1964. Second edition, Springer, 1987.
- J. Stillwell, *Mathematics and its history*, Springer UTM, 1989.

12. Een bewijs van de basisstellingen uit de algebraïsche meetkunde die 15.4 generaliseren vereist enige investering in de onderliggende commutatieve algebra. Van de hieronder genoemde boeken zijn dat van Fulton (dat zich tot krommen beperkt) en Reid het meest elementair. Het boek van Harris, dat veel 'echte meetkundige voorbeelden' bevat, noemt zich een inleiding tot het met name in zijn latere hoofdstukken nogal veeleisende boek van Hartshorne. Dit laatste boek werd direct na verschijnen in 1977 *het* tekstboek voor de moderne algebraïsch meetkundige.

- M. Reid, *Undergraduate algebraic geometry*, Cambridge University Press, 1988

- W. Fulton, *Algebraic curves*, Addison-Wesley, 1969.
- J. Harris, *Algebraic geometry*, Springer GTM 133, 1992.
- R. Hartshorne, *Algebraic geometry*, Springer GTM 52, 1977.

13. In de aritmetische algebraïsche meetkunde bestudeert men getaltheoretische problemen met meetkundige methoden. Behalve het directe verband tussen het oplossen van vergelijkingen en het vinden van punten – zoals in de zin voor stelling 12.21 – is er ook een sterke algebraïsche analogie tussen de ringen uit de getaltheorie (zoals $\mathbf{Z}$ of $\mathbf{Z}[i]$) en de coördinatenringen van algebraïsche krommen in (bijvoorbeeld) $\mathbf{A}^n(\mathbf{C})$.

- D. Lorenzini, *An invitation to arithmetic geometry*, American Mathematical Society, 1996.

14. De studie van dimensies van commutatieve ringen is een deelgebied van de commutatieve algebra dat *dimensietheorie* heet. Onderstaande boeken, die een boel nuttige informatie over ringen en idealen bevatten, hebben er hoofdstukken over. De genoemde identiteit $\dim(K[X_1, X_2, \ldots, X_n]) = n$ staat bij Matsumura op pagina 35.

- M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.
- H. Matsumura, *Commutative ring theory*, Cambridge, 1986.

15. Het hierboven genoemde boekje van Atiyah en Macdonald geeft twee bewijzen voor de Hilbert Nullstellensatz. Er is ook een bewijs in het relatief toegankelijke boekje van Reid. Eisenbud's recente, goed leesbare (maar nogal uitgebreide) boek over commutatieve algebra heeft er zelfs vijf, naast een aardige uiteenzetting over de Nullstellensatz in paragraaf 1.6.

- M. Reid, *Undergraduate commutative algebra*, Cambridge University Press, 1995.
- D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Springer GTM 150, 1995.

16. De grondlegger van het intuïtionisme is de Nederlandse wiskundige L. E. J. Brouwer (1881–1966), die in het buitenland vooral bekend is vanwege zijn bijdragen aan de topologie (zoals de *dekpuntsstelling van Brouwer*). Brouwer's *Grundlagenstreit* met de grote Duitse wiskundige Hilbert trok rond 1930 internationale aandacht, maar geldt tegenwoordig als weinig actueel.

- A. Heyting, *Intuitionism, an introduction*, Amsterdam, 1965.

17. Het lemma van Zorn is een veel gebruikte versie van het keuzeaxioma. Lang's *Algebra* bespreekt het in een nuttige appendix over verzamelingentheorie. Wie meer over de plaats van het keuzeaxioma en zijn varianten in de verzamelingentheorie wil weten kan bij Devlin terecht.

- K. Devlin, *The joy of sets*, 1979. Second edition, Springer UTM, 1993.

18. Het onder **12** al genoemde boekje van Reid over algebraïsche meetkunde heeft een slotparagraaf over 'history and sociology' waarin ook aan Grothendieck en zijn school aandacht wordt besteed. Wie iets meer over schema's wil weten kan, behalve in Hartshorne's boek, ook in het wat handzamere boekje van Eisenbud en Harris kijken.

- D. Eisenbud, J. Harris, *The geometry of schemes*, Springer GTM 197, 2000.

19. De 'constructie' van vrije ultrafilters kan men gebruiken om de zogenaamde *niet-standaard-analyse* op te zetten. Hierin werkt men formeel met 'oneindig kleine' en 'oneindig grote' objecten. Dit leidt soms tot snellere bewijzen van bepaalde uitspraken in de 'gewone' analyse, die zich meestal van ε-δ-argumenten bedient.

- M. Davis, Applied nonstandard analysis, Wiley, 1977.

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 2, vrijdag 19 december 2003, 10.00–13.00 uur

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt.

1. Zij $f = X^3 + 19X^2 + 12X + 3 \in \mathbf{C}[X]$ het polynoom van de dag.
   a. Laat zien dat de drie complexe nulpunten α_1, α_2 en α_3 van f verschillend zijn.
   b. Bereken $\alpha_1^4 + \alpha_2^4 + \alpha_3^4$.

2. Zij $f : R_1 \to R_2$ een ringhomomorfisme en $f_* : R_1^* \to R_2^*$ het geïnduceerde homomorfisme op de eenhedengroepen. Geef voor de volgende uitspraken een bewijs of een tegenvoorbeeld.
   a. Als f surjectief is, dan is f_* surjectief.
   b. Als f_* surjectief is, dan is f surjectief.
   c. Als f injectief is, dan is f_* injectief.
   d. Als f_* injectief is, dan is f injectief.

3. Bepaal voor elk van de volgende drie idealen of het priem is in respectievelijk $\mathbf{Z}[X]$, $\mathbf{Q}[X]$ en $\mathbf{F}_2[X]$:

$$(X^3 + 2X + 1), \qquad (X^3 + 2X + 1,\ 3), \qquad (X^3 + 2X + 1,\ X - 1).$$

4. Zij $H \subset \mathbf{Z}^3$ de ondergroep gegeven door

$$H = \{(x, y, z) \in \mathbf{Z}^3 : 6x + 3y + 2z \equiv 0 \bmod 12\}.$$

   a. Bepaal een basis voor H en schrijf het element $(0, 0, 6) \in H$ ten opzichte van deze basis.
   b. Bepaal de structuur van de abelse groep $\mathbf{Z}^3/H$.

5. Bepaal de Jordan-normaalvorm, het karakteristieke polynoom en het minimumpolynoom van de complexe matrix

$$A = \begin{pmatrix} 2 & 3 & -3 \\ 1 & 3 & -1 \\ 1 & 4 & -2 \end{pmatrix}.$$

Uitslagen vanavond op collegekaartnummer op de webpagina van het college.
Schrijf vooral je collegekaartnummer op je tentamen!

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 2, 17 december 2004, 10:00 – 13:00 uur

Geef steeds een volledige uitwerking, en noem de stellingen die je gebruikt.

1. Ontbind de volgende polynomen in irreducibele factoren in $\mathbf{Z}[X]$ en in $\mathbf{Q}[X]$:
(a) $3X - 12$;
(b) $X^5 - 5$;
(c) $X^7 - 1$;
(d) $X^4 - 20X^3 + 100X^2 - 4$.

2. Laat $\alpha_1, \alpha_2, \ldots, \alpha_8 \in \mathbf{C}$ zodat het polynoom $f = X^8 - 2X^5 + 3 \in \mathbf{C}[X]$ ontbindt als $f = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_8)$.
(a) Bewijs: $\alpha_1 + \alpha_2 + \cdots + \alpha_8 = 0$.
(b) Bereken

$$\alpha_1^2\alpha_2+\alpha_1^2\alpha_3+\cdots+\alpha_1^2\alpha_8+\alpha_2^2\alpha_1+\alpha_2^2\alpha_3+\cdots+\alpha_2^2\alpha_8+\alpha_3^2\alpha_1+\cdots+\alpha_8^2\alpha_1+\cdots+\alpha_8^2\alpha_7.$$

3. Bepaal in $\mathbf{Z}[i]$ de ggd van $7 + 100i$ en $100 + 6i$.

4. Zij R de verzameling $\{\frac{a}{2^k} \in \mathbf{Q} : a, k \in \mathbf{Z}, k \geq 0\}$.
(a) Bewijs dat R een ring is en dat $\mathbf{Z}$ een deelring is van R.
(b) Zij $I = (3)$ het hoofdideaal van R voortgebracht door 3 en $J = (2)$. Bepaal R/I en R/J.
(c) Bepaal de eenhedengroep R^* van R.

5. Bepaal de Jordan-normaalvorm, het karakteristieke polynoom en het minimumpolynoom van de complexe matrix

$$A = \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix}.$$

Uitslagen vanavond op collegekaartnummer op de webpagina van het college.

Schrijf vooral je collegekaartnummer op je tentamen!

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 2, 16 december 2005

Geef steeds een volledige uitwerking, eventueel met verwijzingen naar stellingen uit de syllabus.

1. Ontbind de volgende ring-elementen in irreducibelen:
(*a*) $X^3 - Y^3$ in de ring $\mathbf{Q}[X, Y]$;
(*b*) $X^3 - X^2 - 8X + 6$ in de ring $\mathbf{Z}[X]$;
(*c*) $X^4 - X^2 + 4X + 3$ in de ring $\mathbf{Q}[X]$;
(*d*) $2i + 9$ in de ring $\mathbf{Z}[i]$;

2. Definieer de ondergroepen $A, B \subset \mathbf{Z}^3$ door

$$A = \{(a, b, c) \in \mathbf{Z}^3 : a + b + c = 0\};$$
$$B = \{(a, b, c) \in \mathbf{Z}^3 : a + 2b + 3c \equiv 0 \bmod 6\}.$$

Geef een minimaal stel voortbrengers voor A, voor B, en voor $A \cap B$.

3. Laat $R = \{f \in \mathbf{C}[X] : f(0) \in \mathbf{Z}\}$.
(*a*) Laat zien dat R een deelring is van $\mathbf{C}[X]$.
(*b*) Laat zien dat $R/2R \cong \mathbf{F}_2$.

Definieer $I = \{f : f \in R \text{ met } f(\pi) = 0\}$. Hier is $\pi \in \mathbf{C}$ de halve omtrek van de eenheidscirkel.

(*c*) Laat zien dat I een maximaal ideaal is van R.
(*d*) Is I een hoofdideaal van R?
(*e*) Laat zien dat de ring $R/2I$ isomorf is met $\mathbf{F}_2 \times \mathbf{C}$.

4. Laat $\alpha_1, \ldots, \alpha_7 \in \mathbf{C}$ zodat $X^7 - 2X + 2 = (X - \alpha_1) \cdots (X - \alpha_7)$.
(*a*) Bepaal $\alpha_1 + \alpha_2 + \cdots + \alpha_7$.
(*b*) Laat zien dat $\alpha_1^3 + \alpha_2^3 + \cdots + \alpha_7^3 = 0$.
(*c*) Bepaal $\alpha_1^7 + \alpha_2^7 + \cdots + \alpha_7^7$.

— SUCCES —

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 2, vrijdag 15 december 2006, 10.00–13.00 uur

Motiveer steeds je antwoord (alleen ja/nee is niet voldoende!), en noem de stellingen die je gebruikt.

1. Laat $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbf{C}$ de complexe nulpunten zijn van het polynoom $f = X^4 + 15X + 12$. Bereken $\sum_{i=1}^{4} \alpha_i^4$ en de discriminant $\Delta(f)$ van f.

2. Bepaal voor elk van de volgende drie idealen in welke van de ringen $\mathbf{Z}[X]$, $\mathbf{Q}[X]$ en $\mathbf{F}_3[X]$ het priem is:

$$(X^3 - 18X + 12), \qquad (X^3 - 18X + 12,\ 5), \qquad (X^3 - 18X + 12,\ X - 1).$$

(Er worden dus $3 \times 3 = 9$ antwoorden verwacht....)

3. Definieer de deelverzameling $R \subset \mathbf{Q}$ als

$$R = \{\frac{a}{3^k} \in \mathbf{Q} : a \in \mathbf{Z}, k \in \mathbf{Z}_{\geq 0}\}.$$

a. Laat zien dat R een deelring is van $\mathbf{Q}$. Is het een hoofdideaaldomein?
b. Zijn de quotientringen $R/2R$ en $R/3R$ lichamen?
c. Ga na of de eenhedengroep R^* een vrije abelse groep is. Is R^* eindig voortgebracht?
d. Is de optelgroep van R vrij? Eindig voorgebracht?

4. Zij $A \subset \mathbf{Z}^3$ de ondergroep gegeven door

$$A = \{(x, y, z) \in \mathbf{Z}^3 : 3x + y + 4z \equiv 0 \bmod 6 \text{ en } x + 2z \equiv 0 \bmod 3\}.$$

a. Bepaal een basis voor de abelse groep A.
b. Bepaal de orde van de abelse groep $\mathbf{Z}^3/A$. Is $\mathbf{Z}^3/A$ cyclisch?

5. Zij $M = (a_{ij})_{i,j=1}^{2006}$ de complexe matrix met coëfficiënten $a_{ij} = (-1)^{i+j}$. Bepaal de Jordan-normaalvorm, het karakteristieke polynoom en het minimumpolynoom van M.

Uitslagen vanavond op collegekaartnummer op de webpagina van het college.
Schrijf vooral je collegekaartnummer op je tentamen!

Mathematisch Instituut
Universiteit Leiden

Tentamen Algebra 2, 14 december 2007, 10:00 – 13:00 uur

Motiveer steeds je antwoord, en noem de stellingen die je gebruikt. Je mag de syllabus, boeken en aantekeningen gebruiken, maar gebruik van een rekenmachine is niet toegestaan.

Opgave 1. Laat α, β en γ de complexe nulpunten van $f = X^3 + X^2 + 1$ zijn. Bepaal

$$\det \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{pmatrix}.$$

Opgave 2. Bepaal een voortbrenger van elk van de volgende idealen van $\mathbf{Z}[i]$.
(a) $(17, 12 + 3i)$
(b) $(19 + i) + (37 - 2i)$
(c) $(2007 + 2007i) \cap (2)$

Opgave 3.
(a) Bepaal alle monische, irreducibele polynomen van graad 2 in $\mathbf{F}_2[X]$ en in $\mathbf{F}_3[X]$.
(b) Ontbind $X^5 - X + 1$ in irreducibele factoren in $\mathbf{F}_2[X]$ en in $\mathbf{F}_3[X]$.
(c) Ontbind $X^5 - X + 1$ in irreducibele factoren in $\mathbf{Z}[X]$.

Opgave 4. Bepaal voor alle positieve $n \in \mathbf{Z}$ de Jordan-normaalvorm, het karakteristieke polynoom en het minimumpolynoom van de complexe $n \times n$ bovendriehoeksmatrix met enen op en boven de diagonaal (en nullen eronder).

Opgave 5. Zij a een reëel getal en definieer het $\mathbf{R}[X]$-moduul $M = \mathbf{R}[X]/(X^2 - a)$. Toon aan dat M precies twee deelmodulen heeft als a negatief is, precies drie als a nul is, en precies vier als a positief is. (Inclusief de "triviale" deelmodulen 0 en M.)

Index