RINGEN EN LICHAMEN

Aanvullende opgaven met uitwerkingen

Hierna volgen een aantal aanvullende opgaven die gaan over kernbegrippen uit de eerste hoofdstukken van Ringen en Lichamen. Probeer deze opgaven te maken zonder hulp van de syllabus. Kijk niet naar de antwoorden voordat je deze opgaven echt hebt gemaakt.

Het accent ligt bij deze opgaven op enkele *basis*technieken; deze opgaven zijn vooral bedoeld voor degenen die nog veel moeite hebben met de opgaven die de afgelopen weken bij het werkcollege aan bod zijn gekomen.

Opgave 1. (i) Bepaal of het polynoom $X^2 - 2$ reducibel of irreducibel is in elk van de volgende ringen:

$$\mathbb{Q}[X]\,, \qquad \mathbb{F}_2[X]\,, \qquad \mathbb{F}_3[X]\,, \qquad \mathbb{F}_{11}[X]\,, \qquad \mathbb{F}_{17}[X]\,.$$

Licht je antwoorden zorgvuldig toe.

(ii) Idem in elk van de volgende ringen:

$$\mathbb{Q}(i)[X]\,, \qquad \mathbb{R}[X]\,, \qquad \mathbb{Q}(T)[X]\,, \qquad \mathbb{R}(T)[X]\,.$$

(N.B.: $\mathbb{Q}(T)$ is het lichaam van rationale functies in de variabele T; dit is dus het breukenlichaam van $\mathbb{Q}[T]$. Analoog voor $\mathbb{R}(T)$.)

Opgave 2. (i) Zij K een lichaam en $0 \neq f \in K[X]$. Bewijs:

$$f \text{ is irreducibel in } K[X] \quad \Leftrightarrow \quad K[X]/(f) \text{ is een domein} \quad \Leftrightarrow \quad K[X]/(f) \text{ is een lichaam.}$$

(ii) Zij $f \in \mathbb{Q}[X]$ een niet-constant polynoom zo dat $\text{ggd}(f, f') = 1$. Bewijs dat $\mathbb{Q}[X]/(f)$ isomorf is met een product van een eindig aantal domeinen.

Opgave 3. (i) Is $\mathbb{Q}(T)[X]/(X^2 - 2)$ een domein? Is het een lichaam?

(ii) Is $\mathbb{Q}[T, X]/(X^2 - 2)$ een domein? Is het een lichaam?

Opgave 4. Bepaal of het polynoom $X^2 - T$ reducibel of irreducibel is in elk van de volgende ringen:

$$\mathbb{Q}(T)[X]\,, \qquad \mathbb{R}(T)[X]\,, \qquad \mathbb{F}_3(T)[X]\,.$$

Opgave 5. (i) Is $(3) \subset \mathbb{Z}\big[\sqrt{2}\,\big]$ een priemideaal? Is het een maximaal ideaal?

(ii) Dezelfde vragen voor de idealen $(11) \subset \mathbb{Z}\big[\sqrt{2}\,\big]$ en $(17) \subset \mathbb{Z}\big[\sqrt{2}\,\big]$.

Opgave 6. Bepaal of het polynoom $3X^3 - 8X^2 + 19X - 10$ reducibel of irreducibel is in elk van de volgende ringen:

$$\mathbb{Z}[X]\,, \qquad \mathbb{Q}[X]\,, \qquad \mathbb{F}_3[X]\,.$$

Opgave 7. Is de ring

$$\mathbb{Z}[X, Y]/(X - Y + 1, XY - X - 2, Y - X + 16)$$

een domein? Is het een lichaam?

Uitwerking van de opgaven

Opgave 1. (i) Uit Stelling 5.3 weten we dat X^2-2 reducibel is in $K[X]$ dan en slechts dan als X^2-2 een nulpunt heeft in K. Dit geeft: X^2-2 is
— irreducibel in $\mathbb{Q}[X]$, want $\mathbb{Q}$ bevat geen wortel van 2;
— reducibel in $\mathbb{F}_2[X]$, want in $\mathbb{F}_2[X]$ is het gelijk aan $X \cdot X$;
— irreducibel in $\mathbb{F}_3[X]$, want 2 is geen kwadraat in $\mathbb{F}_3$;
— irreducibel in $\mathbb{F}_{11}[X]$, want 2 is geen kwadraat in $\mathbb{F}_{11}$;
— reducibel in $\mathbb{F}_{17}[X]$, want $6^2 \equiv 2$ modulo 17, dus 2 is een kwadraat in $\mathbb{F}_{17}$.

(ii) In $\mathbb{Q}(i)$ is 2 niet een kwadraat. Stel maar dat $2=(a+bi)^2$ met a, $b \in \mathbb{Q}$. Uitwerken geeft dat $ab=0$ (kijk naar het imaginaire deel). Maar $b=0$ leidt tot $2=a^2$, terwijl $a=0$ leidt tot $2=-b^2$. In beide gevallen vinden we geen rationale oplossingen. Dus x^2-2 is irreducibel in $\mathbb{Q}(i)[X]$. In $\mathbb{R}[X]$ geldt $X^2-2=\left(X-\sqrt{2}\right)\cdot\left(X+\sqrt{2}\right)$; reducibel dus. Hetzelfde gaat op in $\mathbb{R}(T)[X]$.

In $\mathbb{Q}(T)[X]$ is X^2-2 irreducibel: als 2 een kwadraat was in $\mathbb{Q}(T)$ dan waren er polynomen f, $g \in \mathbb{Q}[T]$ met $g \neq 0$ zo dat $(f/g)^2=2$. Dit geeft $f^2=2g^2$. Omdat $\mathbb{Q}[T]$ een ontbindingsring is, volgt hieruit dat 2 een kwadraat is in $\mathbb{Q}[T]$, zeg $2=h^2$. Maar dan moet h een constant polynoom zijn, en dat geeft een tegenspraak met het feit dat 2 geen kwadraat is in $\mathbb{Q}$. Merk op dat het hier gegeven argument neerkomt op een eenvoudig speciaal geval van Gevolg 5.27, toegepast met $R=\mathbb{Q}[T]$.

Opgave 2. (i) Dit is niets anders dan Stelling 5.8, waarbij we natuurlijk de equivalenties uit Stellingen 4.5 en 4.10 gebruiken.

(ii) Omdat $\mathbb{Q}[X]$ een ontbindingsring is, kunnen we f in $\mathbb{Q}[X]$ ontbinden als

$$f = g_1^{m_1} \cdot g_2^{m_r} \cdots g_r^{m_r} \,,$$

waarbij $r \geqslant 1$ en $m_i \geqslant 1$ voor alle i, en waarbij $g_1, \ldots, g_r$ irreducibele polynomen zijn die onderling ondeelbaar zijn. De aanname dat $\mathrm{ggd}(f, f') = 1$ impliceert dat $m_i = 1$ voor alle i. (Als $m_i > 1$ dan is g_i een gemeenschappelijke factor van f en f'.) Omdat de idealen $(g_i) \subset \mathbb{Q}[X]$ paarsgewijs onderling ondeelbaar zijn, volgt uit de Chinese reststelling dat

$$\mathbb{Q}[X]/(f) \cong \mathbb{Q}[X]/(g_1) \times \cdots \times \mathbb{Q}[X]/(g_r)$$

en wegens Stelling 5.12 is dit een product van domeinen. (We gebruiken hier de versie van de Chinese reststelling die gegeven wordt in Opgave 42 van Hoofdstuk 2.)

Merk op dat een deel van dit argument overlapt met het bewijs van Stelling 5.15.

Let op: Als we in (ii) van deze opgave $\mathbb{Q}[X]$ vervangen door $K[X]$ met K een willekeurig lichaam, dan is de uitspraak wel waar maar moet je een beetje voorzichtig zijn bij het bewijs dat $m_i = 1$ voor alle i. Bijvoorbeeld: neem $f = X^2$ in de ring $\mathbb{F}_2[X]$. Dan is $f' = 2X = 0$ (!), omdat $2 = 0$ in $\mathbb{F}_2$. Nu moet je bedenken dat $\mathrm{ggd}(f, 0) = f$; dus aan de voorwaarde dat $\mathrm{ggd}(f, f') = 1$ is in dit geval niet voldaan.

Opgave 3. (i) Uit Opgave 2, samen met wat we gezien hebben in (ii) van Opgave 1, volgt dat $\mathbb{Q}(T)[X]/(X^2-2)$ een lichaam is, en dus ook een domein.

(ii) De ring $\mathbb{Q}[T,X]/(X^2-2)$ is een domein, want $\mathbb{Q}[T,X]$ is een ontbindingsring (zie Gevolg 5.17) en X^2-2 is irreducibel in deze ring (zie de uitwerking van Opgave 1); pas nu Stelling 5.12 toe. Deze ring is echter geen lichaam, want $(X^2-2) \subset \mathbb{Q}[T,X]$ is niet een maximaal ideaal; een voorbeeld van een (strict) groter niet-triviaal ideaal is (T, X^2-2).

Opgave 4. Dit gaat op precies dezelfde manier als bij Opgave 1. Omdat T geen kwadraat is in $K(T)$, voor K een willekeurig lichaam, geldt dat X^2-T in alle drie de genoemde ringen irreducibel is.

Opgave 5. Het is handig om gebruik te maken van het isomorfisme $\mathbb{Z}[X]/(X^2-2) \xrightarrow{\sim} \mathbb{Z}\big[\sqrt{2}\,\big]$ dat gegeven wordt door $X \mapsto \sqrt{2}$. Eerst even de details hiervan: begin met het homomorfisme $\phi\colon \mathbb{Z}[X] \to \mathbb{Z}\big[\sqrt{2}\,\big]$ dat gegeven wordt door een polynoom $P = \sum a_i X^i$ te sturen naar $P\big(\sqrt{2}\big) = \sum a_i (\sqrt{2})^i$. (Dus $X \mapsto \sqrt{2}$.) Dit homomorfisme is surjectief, per definitie van de ring $\mathbb{Z}\big[\sqrt{2}\,\big]$. Het is duidelijk dat X^2-2 in de kern zit, en we beweren dat X^2-2 een voortbrenger is voor de kern. Om dat in te zien: stel P zit in de kern. Stelling 3.1 geeft ons q en r in $\mathbb{Z}[X]$ met $P = q\cdot(X^2-2)+r$ en $r = aX+b$ voor zekere gehele getallen a en b. Dan zit ook r in de kern van ϕ (want $r = P - q\cdot(X^2-2)$ en P en X^2-2 zitten allebei in de kern), en omdat $\sqrt{2} \notin \mathbb{Q}$ volgt dat $a=b=0$, dus $r=0$, dus P is een veelvoud van X^2-2. De isomorfiestelling geeft nu dat ϕ een isomorfisme $\mathbb{Z}[X]/(X^2-2) \xrightarrow{\sim} \mathbb{Z}\big[\sqrt{2}\,\big]$ induceert.

Als p een priemgetal is, dan is

$$\mathbb{Z}\big[\sqrt{2}\,\big]/(p) \cong \mathbb{Z}[X]/(X^2-2,p) \cong \mathbb{F}_p[X]/(X^2-2)$$

en we kunnen toepassen wat we gezien hebben in Opgaven 1 en 2(i). Conclusie: (3) en (11) zijn maximale idealen (en dus ook priemidealen), en (17) is niet een priemideaal (en dus ook geen maximaal ideaal).

Opgave 6. Wegens Stelling 5.3 samen met Gevolg 5.27 hoeven we enkel na te gaan of $3X^3 - 8X^2 + 19X - 10$ een nulpunt heeft in $\mathbb{Q}$ en in $\mathbb{F}_3$. Om dit in $\mathbb{Q}$ te doen gebruiken we 5.29(c) om de mogelijkheden te beperken, en dan vinden we vrij snel dat $\frac{2}{3}$ een nulpunt is, zodat $3X^3 - 8X^2 + 19X - 10$ reducibel is in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$. (Het polynoom $3X-2$ is een niet-triviale factor.) In $\mathbb{F}_3[X]$ is ons polynoom gelijk aan X^2+X-1 en we gaan eenvoudig na (invullen van 0, 1 en -1) dat dit geen nulpunten heeft en dus irreducibel is.

Opgave 7. We gaan stapsgewijs uitdelen. De eerste stap is dat

$$\mathbb{Z}[X,Y]/(X-Y+1) \xrightarrow{\sim} \mathbb{Z}[X]$$

waarbij de klasse van Y gestuurd wordt naar $X+1$. Dat geeft:

$$\mathbb{Z}[X,Y]/(X-Y+1, XY-X-2, Y-X+16) \cong \mathbb{Z}[X]/(X^2-2,17) \cong \mathbb{F}_{17}[X]/(X^2-2)$$

en zoals we gezien hebben in Opgave 1 is dit niet een domein, en dus ook niet een lichaam.

Een veelgemaakte fout

Symbolen als $\sqrt{2}$ of i (het complexe getal) zijn gereserveerd voor specifieke elementen van $\mathbb{C}$. Dergelijke symbolen kun je dus *niet* gebruiken in andere getallensystemen. Bijvoorbeeld: als je werkt in de ring $\mathbb{F}_p[X]/(X^2+1)$, met p een priemgetal, dan kan je aan de klasse van X wel denken als "een soort van i ", maar je dient deze klasse niet i te noemen. Zou je dat wel doen, dan leidt dit tot verwarring, en dan maak je het alleen maar moeilijker om de structuur van deze ring te begrijpen. Hierbij zij opgemerkt dat $\mathbb{F}_p[X]/(X^2+1)$ een lichaam is als p een priemgetal is met $p \equiv 3$ modulo 4, dat deze ring isomorf is met $\mathbb{F}_p \times \mathbb{F}_p$ als $p \equiv 1$ modulo 4, en dat $\mathbb{F}_2[X]/(X^2+1) \cong \mathbb{F}_2[Y]/(Y^2)$. (Dit komt uitvoeriger aan bod in de tweede helft van dit vak.) We zien dus dat de structuur van deze ring sterk afhangt van wat p is en dat de notatie " i " voor de klasse van X alleen maar misleidend is.

Om dezelfde redenen gebruiken we meestal geen worteltekens in andere getallenstelsels dan $\mathbb{R}$ of $\mathbb{C}$. Zelfs in $\mathbb{C}$ is het al problematisch dat $\sqrt{a}$ in het algemeen meerduidig is: is $\sqrt{-1}$ nou gelijk aan i of aan -1 ? En is $\sqrt[3]{-1}$ gelijk aan -1 of ook aan $\frac{1}{2} + \frac{1}{2}\, i\sqrt{3}$? In andere lichamen is gewoon niet duidelijk wat we met een wortelteken bedoelen. Analoog aan het hierboven gegeven voorbeeld geldt dus dat je in een ring als $\mathbb{F}_p[X]/(X^2-2)$ aan de klasse van X wel mag denken als "een soort van $\sqrt{2}$ " maar dat we deze notatie *niet* gebruiken. Zoals we gezien hebben in Opgave 1 hangt de structuur van deze ring af van welk priemgetal p we kiezen.

Dit is overigens precies waarom we in de uitwerking van Opgave 5 overgaan van de ring $\mathbb{Z}\big[\sqrt{2}\,\big]$ op de isomorfe ring $\mathbb{Z}[X]/(X^2-2)$.