RINGEN EN LICHAMEN

Uitwerking van het tentamen van dinsdag 24 januari 2017.

Opgave 1. Zij R een commutatieve ring met $1 \neq 0$.

(i) (Theorievraag) Geef de definities van de begrippen *priemideaal* en *maximaal ideaal*.

(ii) (Theorievraag) Zij $I \subset R$ een ideaal. Bewijs dat I een priemideaal is dan en slechts dan als de ring R/I een domein is.

(iii) Geef een expliciet voorbeeld van een priemideaal in de ring $R = \mathbb{C}[X,Y]/(X^2-Y^2)$ dat niet een maximaal ideaal is. Bewijs dat het voorbeeld dat je geeft voldoet aan het gevraagde.

Uitwerking. (i)+(ii) Zie de syllabus. (iii) Zij $I \subset R$ het ideaal voortgebracht door de klasse van het element $X-Y$. Omdat $(X^2-Y^2) \subset (X-Y) \subset \mathbb{C}[X,Y]$ geldt (stapsgewijs uitdelen) $R/I \cong \mathbb{C}[X,Y]/(X-Y) \cong \mathbb{C}[X]$. Dit is een domein maar niet een lichaam; dus I is een priemideaal maar niet een maximaal ideaal.

Opgave 2. Zij $M_2(\mathbb{Z})$ de ring van 2×2 matrices met gehele coëfficiënten. Laat $A = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)$ en $I = A^0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, en zij $\varphi\colon \mathbb{Z}[X] \to M_2(\mathbb{Z})$ het homomorfisme gegeven door

$$\varphi(a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) = a_0 \cdot I + a_1 \cdot A + a_2 \cdot A^2 + \cdots + a_n \cdot A^n \,.$$

Je hoeft niet na te gaan dat φ inderdaad een homomorfisme van ringen is. Definieer de deelverzameling $R \subset M_2(\mathbb{Z})$ door

$$R = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\} .$$

(i) Laat zien dat R een commutatieve deelring is van $M_2(\mathbb{Z})$.

(ii) Bewijs dat $R \cong \mathbb{Z}[X]/(X^2-2)$.

(iii) Zij $J \subset R$ het ideaal dat wordt voortgebracht door het element $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. Bewijs dat J een maximaal ideaal is. Hoeveel elementen heeft R/J ?

Uitwerking. (i)+(ii) Er geldt $A^2 = 2 \cdot I$. Dus $A^{2k} = 2^k \cdot I$ en $A^{2k+1} = 2^k \cdot A$ voor alle $k \geqslant 0$. Dus het beeld van φ is precies de verzameling R, en dus is R een deelring van $M_2(\mathbb{Z})$. Duidelijk is dat $X^2-2 \in \mathrm{Ker}(\varphi)$. Omgekeerd, stel $f \in \mathrm{Ker}(\varphi)$. Deling met rest geeft $f = q \cdot (X^2-2) + r$, waarbij $r = aX + b$ voor gehele a en b. Dan is $r \in \mathrm{Ker}(\varphi)$, maar omdat $\varphi(r) = \left(\begin{smallmatrix} a & b \\ 2b & a \end{smallmatrix}\right)$ volgt dat $a = b = 0$; dus f is een veelvoud van X^2-2. De conclusie is dat $\mathrm{Ker}(\varphi) = (X^2-2)$. De uitspraak in (ii) volgt nu uit de isomorfiestelling, en ook is duidelijk dat R commutatief is.

(iii) Het ideaal J is het beeld in R van het ideaal (3) in $\mathbb{Z}[X]$. Daarmee vinden we dat $R/J \cong \mathbb{Z}[X]/(3, X^2-2) \cong \mathbb{F}_3[X]/(X^2-2)$. Omdat X^2-2 geen nulpunten heeft in $\mathbb{F}_3$, is het een irreducibel kwadratisch polynoom in de hoofdideaalring $\mathbb{F}_3[X]$. Dus R/J is een lichaam met 9 elementen, en J is een maximaal ideaal.

Opgave 3. Laat $f = 20X^3 - 120X^2 - 160X + 140$ en $g = X^4 + 3X + 3$.

(i) Ontbind f en g in irreducibele factoren in $\mathbb{Z}[X]$ en ook in $\mathbb{F}_7[X]$.

(ii) Laat zien dat g in $\mathbb{F}_{49}[X]$ ontbindt als een product van lineaire factoren.

Uitwerking. (i) In $\mathbb{Z}[X]$ geldt

$$f = 20 \cdot (X^3 - 6X^2 - 8X + 7) = 2 \cdot 2 \cdot 5 \cdot (X - 7) \cdot (X^2 + X - 1)\,. \tag{1}$$

Omdat $X^2 + X - 1$ monisch kwadratisch is en geen nulpunten heeft in $\mathbb{Q}$ (zelfs niet in $\mathbb{R}$), is dit polynoom irreducibel in $\mathbb{Z}[X]$, dus (1) is de gevraagde factorisatie. In $\mathbb{F}_7[X]$ vinden we dan dat

$$f = -X \cdot (X^2 + X - 1)\,. \tag{2}$$

We gaan gemakkelijk na dat $X^2 + X - 1$ geen nulpunten heeft in $\mathbb{F}_7$; dus (2) is de gevraagde factorisatie in $\mathbb{F}_7[X]$.

In $\mathbb{Z}[X]$ is g irreducibel, want het is Eisenstein bij $p = 3$. In $\mathbb{F}_7[X]$ is

$$g = (X - 1)^2 \cdot (X^2 + 2X + 3) \tag{3}$$

en $X^2 + 2X + 3$ is irreducibel want het is kwadratisch en heeft geen nulpunten in $\mathbb{F}_7$; dus (3) is de gevraagde factorisatie in $\mathbb{F}_7[X]$.

(ii) Het volstaat om te bewijzen dat $h = X^2 + 2X + 3$ een nulpunt heeft in $\mathbb{F}_{49}$, want dan valt h, en dus ook g, uiteen als een product van lineaire factoren. Maar $\mathbb{F}_{49} \cong \mathbb{F}_7[X]/(h)$ en de klasse ($X \bmod h$) is een nulpunt van h.

Opgave 4. Zij $\alpha \in \mathbb{R}$ een *reëel* nulpunt van het polynoom $X^5 + 7X^4 + X^3 + 14X^2 + 7$.

(i) Bewijs dat het minimumpolynoom van α over $\mathbb{Q}$ gegeven is door $f^{\alpha}_{\min} = X^3 + 7X^2 + 7$.

(ii) Bepaal rationale getallen c_0, c_1, c_2 zo dat

$$(1 + \alpha^2)^{-1} = c_0 + c_1 \cdot \alpha + c_2 \cdot \alpha^2\,.$$

(iii) Zij $0 \neq \beta \in \mathbb{R}$ een reëel getal dat transcendent is over $\mathbb{Q}$. Is $1 + \alpha\beta^{-1}$ algebraïsch over $\mathbb{Q}$ of transcendent? Motiveer je antwoord.

Uitwerking. (i) Er geldt

$$X^5 + 7X^4 + X^3 + 14X^2 + 7 = \left(X^2 + 1\right)\left(X^3 + 7X^2 + 7\right)$$

en omdat $X^2 + 1$ geen reële nulpunten heeft, volgt dat α een nulpunt is van het polynoom $f = X^3 + 7X^2 + 7$. Bovendien is f irreducibel in $\mathbb{Q}[X]$ omdat het een Eisensteinpolynoom is bij $p = 7$ (de kopcoëfficiënt is 1, dus niet deelbaar door 7, de overige coëfficiënten zijn deelbaar door 7 en de constante coëfficënt is 7 en is dus niet deelbaar door 7^2). Dus $f = f^{\alpha}_{\mathbb{Q}}$.

(ii) Uit (i) volgt dat $\alpha^3 = -7\alpha^2 - 7$ en $\alpha^4 = -7\alpha^3 - 7\alpha = 49\alpha^2 - 7\alpha + 49$. Voor c_0, c_1, $c_2 \in \mathbb{Q}$ geldt daarom dat

$$\begin{aligned}(1 + \alpha^2) \cdot (c_0 + c_1\alpha + c_2\alpha^2) &= c_0 + c_1\alpha + (c_0 + c_2)\alpha^2 + c_1\alpha^3 + c_2\alpha^4 \\ &= (c_0 - 7c_1 + 49c_2) + (c_1 - 7c_2)\alpha + (c_0 - 7c_1 + 50c_2)\alpha^2\,.\end{aligned}$$

Dit voert tot het lineaire stelsel

$$\begin{aligned} c_0 - 7c_1 + 49c_2 &= 1 \\ c_1 - 7c_2 &= 0 \\ c_0 - 7c_1 + 50c_2 &= 0 \end{aligned}$$

met als oplossing $c_0 = 1$, $c_1 = -7$ en $c_2 = -1$. Dus $(1+\alpha^2)^{-1} = 1 - 7\alpha - \alpha^2$.

(iii) Het getal $\gamma = 1 + \alpha\beta^{-1}$ is transcendent over $\mathbb{Q}$. Als namelijk γ algebraïsch was over $\mathbb{Q}$ dan was ook $\beta = \alpha(\gamma - 1)^{-1}$ algebraïsch over $\mathbb{Q}$; tegenspraak.

Opgave 5. Bewijs dat $K = \mathbb{Q}\big(i\sqrt{3}, \sqrt[3]{5}\big)$ een ontbindingslichaam is van het polynoom $X^3 - 5$ over $\mathbb{Q}$, en bepaal $[K : \mathbb{Q}]$.

Uitwerking. Laat $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2} \cdot i\sqrt{3}$. Dan is ζ een primitieve derde eenheidswortel in $\mathbb{C}$, en het is duidelijk dat $K = \mathbb{Q}\big(\zeta, \sqrt[3]{5}\big)$. In $K[X]$ geldt

$$X^3 - 5 = (X - \sqrt[3]{5}) \cdot (X - \zeta\sqrt[3]{5}) \cdot (X - \zeta^2\sqrt[3]{5}),$$

dus $X^3 - 5$ factoriseert in $K[X]$ als een product van lineaire factoren. Anderzijds is duidelijk dat $K = \mathbb{Q}\big(\sqrt[3]{5}, \zeta\sqrt[3]{5}, \zeta^2\sqrt[3]{5}\big)$. Dus K is inderdaad het ontbindingslichaam.

Laat $L = \mathbb{Q}\big(\sqrt[3]{5}\big)$. Het polynoom $X^3 - 5$ is irreducibel over $\mathbb{Q}$ (want monisch en Eisenstein bij $p = 5$), dus het is het minimumpolynoom van $\sqrt[3]{5}$ over $\mathbb{Q}$, zodat $[L : \mathbb{Q}] = 3$. Omdat $L \subset \mathbb{R}$, is de uitbreiding $L \subset K = L\big(i\sqrt{3}\big)$ niet triviaal. Anderzijds is $i\sqrt{3}$ nulpunt van het kwadratische polynoom $X^2 + 3 \in L[X]$. Dus $[K : L] = 2$, en daarmee vinden we dat $[K : \mathbb{Q}] = [K : L] \cdot [L : \mathbb{Q}] = 6$.