RINGEN EN LICHAMEN

Uitwerking van het proeftentamen

Opgave 1.

(i) Ontbind de volgende polynomen in irreducibele factoren in $\mathbb{Z}[X]$ en ook in $\mathbb{Q}[X]$:

$$2X^5 - 12X^3 + 64X^2 - 12$$
$$X^3 - 4X^2 - 4X - 5$$

Licht je antwoorden zorgvuldig toe.

(ii) Ontbind het polynoom $2X^5Y^5 - Y^5 + 3X^2Y^3 + 8X^2 - X$ in irreducibele factoren in $\mathbb{Q}[X, Y]$.

Uitwerking. (i) In $\mathbb{Z}[X]$ is $X^5 - 6X^3 + 32X^2 - 6$ irreducibel, want het is een Eisensteinpolynoom bij $p = 2$. (De coëfficiënten -6, 32 en -6 zijn deelbaar door 2, en de constante coëfficiënt -6 is niet deelbaar door 2^2.) Uit Gevolg 5.26 volgt dat dit polynoom ook irreducibel is in $\mathbb{Q}[X]$. Omdat $2 \in \mathbb{Z}[X]$ irreducibel is, is $2X^5 - 12X^3 + 64X^2 - 12 = 2 \cdot (X^5 - 6X^3 + 32X^2 - 6)$ de gezochte factorisatie in $\mathbb{Z}[X]$. Omdat 2 een eenheid is in $\mathbb{Q}[X]$, is het oorspronkelijke polynoom $2X^5 - 12X^3 + 64X^2 - 12$ irreducibel in $\mathbb{Q}[X]$.

Er geldt $X^3 - 4X^2 - 4X - 5 = (X - 5)(X^2 + X + 1)$. Het polynoom $X^2 + X + 1$ heeft geen rationale nulpunten en is dus (Stelling 5.3) irreducibel in $\mathbb{Q}[X]$. Uit Gevolg 5.26 volgt dat $X^2 + X + 1$ ook irreducibel is in $\mathbb{Z}[X]$. Dus $X^3 - 4X^2 - 4X - 5 = (X - 5)(X^2 + X + 1)$ is de gevraagde factorisatie in zowel $\mathbb{Z}[X]$ als $\mathbb{Q}[X]$.

(ii) Het polynoom $2X^5Y^5 - Y^5 + 3X^2Y^3 + 8X^2 - X = (2X^5 - 1) \cdot Y^5 + 3X^2 \cdot Y^3 + (8X^2 - X)$ is een Eisensteinpolynoom in $\mathbb{Q}[X]\big[Y\big]$ bij het irreducibele element $X \in \mathbb{Q}[X]$, en is dus irreducibel. (De kopcoëfficiënt is niet deelbaar door X, de overige coëfficiënten wel, en de constante coëfficiënt $8X^2 - X$ is niet deelbaar door X^2.)

Opgave 2. Zij R een commutatieve ring met $1 \neq 0$. Gegeven zijn verder twee idealen I en J van R.

(i) Als $I \cup J$ een ideaal is, bewijs dat $I \subseteq J$ of $J \subseteq I$.

(ii) Als $I \cap J$ een priemideaal is, bewijs dat $I \subseteq J$ of $J \subseteq I$.

Uitwerking. Stel $I \not\subseteq J$ en $J \not\subseteq I$. Dan zijn er $x \in I \setminus J$ en $y \in J \setminus I$. Stel $I \cup J$ was een ideaal. Dan is $x + y$ een element van I of van J. In het eerste geval volgt dat $y = (x + y) - x \in I$, in het tweede geval $x = (x + y) - y \in J$. In beide gevallen is dit in tegenspraak met hoe we x en y hebben gekozen. Als $I \cap J$ een priemideaal was dan moest, wegens $xy \in IJ \subset I \cap J$, ofwel $x \in I \cap J$, ofwel $y \in I \cap J$, wat weer in tegenspraak is met hoe we x en y hebben gekozen.

Opgave 3. In $\mathbb{Z}[X]$ bekijken we de polynomen

$$f = X^2 + 4\,, \qquad g = X^3 - X^2 + 4X - 1\,, \qquad h = X^2 + 6\,.$$

Zij $I = (f, g) \subset \mathbb{Z}[X]$ het door f en g voortgebrachte ideaal, en laat $R = \mathbb{Z}[X]/\big(I \cap (h)\big)$.

(i) Bewijs dat $R \cong \mathbb{Z}[X]/I \times \mathbb{Z}[X]/(h)$.

(ii) Bepaal hoeveel verschillende homomorfismen $f\colon R \to \mathbb{F}_7$ er zijn. Licht je antwoord zorgvuldig toe.

Uitwerking. (i) Dit volgt uit de Chinese reststelling; we hoeven enkel te controleren dat $I+(h) = \mathbb{Z}[X]$. Nu bevat $I + (h) = (f, g, h)$ zeker het element $h - f = 2$, dus ook $X^2 = f - 2 \cdot 2$, dus ook $g + (-X + 1) \cdot X^2 - 2X \cdot 2 = -1$ en dus is $I + (h)$ inderdaad de hele ring.

(ii) Omdat $7 \in \mathrm{Ker}(f)$, factoriseert f via $\mathbb{F}_7[X]/(f, g) \times \mathbb{F}_7[X]/(h)$. Echter, $g = (X-1) \cdot f + 3$ en 3 is een eenheid in $\mathbb{F}_7[X]$, dus $\mathbb{F}_7[X]/(f, g)$ is de nulring. Verder geldt in $\mathbb{F}_7[X]$ dat $X^2 + 6 = (X - 1)(X + 1)$ en de factoren $X - 1$ en $X + 1$ zijn onderling ondeelbaar, dus met de Chinese reststelling vinden we dat $\mathbb{F}_7[X]/(h) \cong \mathbb{F}_7[X]/(X - 1) \times \mathbb{F}_7[X]/(X + 1) \cong \mathbb{F}_7 \times \mathbb{F}_7$. De twee projecties $\mathbb{F}_7 \times \mathbb{F}_7 \to \mathbb{F}_7$ zijn de enige twee homomorfismen, want in $\mathbb{F}_7 \times \mathbb{F}_7$ geldt $(1, 0) \cdot (0, 1) = 0$ en omdat $\mathbb{F}_7$ een domein is, moet $f(1, 0) = 0$ of $f(0, 1) = 0$, en dan blijven enkel de projecties als mogelijkheid over. De conclusie is dus dat er precies *twee* homomorfismen $f\colon R \to \mathbb{F}_7$ zijn.

Opgave 4.

(i) Bewijs dat $\sqrt{5} \notin \mathbb{Q}\big(\sqrt{2}\big)$.

(ii) Bepaal het minimumpolynoom van het complexe getal $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$ en bepaal de uitbreidingsgraad $\big[\mathbb{Q}(\sqrt{2} + \sqrt{5}) : \mathbb{Q}\big]$. Licht je antwoorden zorgvuldig toe.

(iii) Zij β een complex getal dat voldoet aan de relatie $\beta^3 + 3\beta^2 - 3 = 0$. Bepaal c_0, c_1, $c_2 \in \mathbb{Q}$ zo dat $\beta^4 - (1 + \beta)^{-1} = c_0 + c_1\beta + c_2\beta^2$.

Uitwerking. (i) Als $\sqrt{5} \in \mathbb{Q}\big(\sqrt{2}\big)$ dan zijn er a, $b \in \mathbb{Q}$ met $\big(a + b\sqrt{2}\big)^2 = 5$, want $\big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\big] = 2$ en $\{1, \sqrt{2}\}$ is een $\mathbb{Q}$-basis voor $\mathbb{Q}\big(\sqrt{2}\big)$. Maar $\big(a + b\sqrt{2}\big)^2 = a^2 + 2b^2 + 2ab\sqrt{2}$ en als dit een element van $\mathbb{Q}$ is dan moet $a = 0$ of $b = 0$. Omdat 5 en $5/2$ geen kwadraten zijn in $\mathbb{Q}$ geeft dit een tegenspraak.

(ii) Voor $\alpha = \sqrt{2} + \sqrt{5}$ geldt dat $\alpha^2 = 7 + 2\sqrt{10}$ en dus $\alpha^4 - 14\alpha^2 + 9 = (\alpha^2 - 7)^2 - 40 = 0$. Verder is $\alpha^3 = 17\sqrt{2} + 11\sqrt{5}$; hieruit volgt dat $\alpha^3 - 11\alpha = 6\sqrt{2}$, dus $\sqrt{2} \in \mathbb{Q}(\alpha)$, en dus ook $\sqrt{5} \in \mathbb{Q}(\alpha)$. In het bijzonder heeft α graad 2 of 4 over $\mathbb{Q}$. Echter, als α graad 2 had, dan was $\mathbb{Q}(\alpha) = \mathbb{Q}\big(\sqrt{2}\big) = \mathbb{Q}\big(\sqrt{5}\big)$, maar dit geeft een tegenspraak met (i). Dus α heeft graad 4 en $X^4 - 14X^2 + 9$ is het minimumpolynoom.

(iii) Er geldt $\beta^3 = -3\beta^2 + 3$ en dus $\beta^4 = 9\beta^2 + 3\beta - 9$. We zoeken nu eerst d_0, d_1 en d_2 zo dat $(1 + \beta)^{-1} = d_0 + d_1\beta + d_2\beta^2$. Dit geeft

$$1 = (1 + \beta)(d_0 + d_1\beta + d_2\beta^2) = (d_0 + 3d_2) + (d_0 + d_1)\beta + (d_1 - 2d_2)\beta^2\,.$$

Oplossen van dit stelsel vergelijkingen geeft $(1 + \beta)^{-1} = -2 + 2\beta + \beta^2$, en dus

$$\beta^4 - (1 + \beta)^{-1} = 8\beta^2 + \beta - 7\,.$$

Opgave 5.

(i) (Theorievraag) Zij K een lichaam van karakteristiek $p > 0$. Bewijs dat de afbeelding $F\colon K \to K$ gegeven door $x \mapsto x^p$ een homomorfisme van lichamen is.

(ii) Zij $f \in \mathbb{F}_7[X]$ gegeven door $f = X^3+X+1$. Bewijs dat f irreducibel is en bepaal het aantal elementen van het ontbindingslichaam $\Omega^f_{\mathbb{F}_7}$ van f over $\mathbb{F}_7$. Licht je antwoord zorgvuldig toe.

(iii) Zij $\alpha \in \Omega^f_{\mathbb{F}_7}$ een nulpunt van het polynoom f uit onderdeel (ii). Bepaal het minimumpolynoom van $\alpha^{49} - 1$ over $\mathbb{F}_7$.

Uitwerking. Voor (i) zie de syllabus. (ii) Omdat f graad 3 heeft, volstaat het aan te tonen dat f geen nulpunten heeft in $\mathbb{F}_7$. Dit rekenen we gewoon na:

$$f(0) = 1\,, \quad f(1) = 3\,, \quad f(2) = 4\,, \quad f(3) = 3\,, \quad f(4) = -1\,, \quad f(5) = -2\,, \quad f(6) = -1\,.$$

Uit Gevolg 12.7 en Stelling 12.15 volgt dat het ontbindingslichaam $7^3 = 343$ elementen heeft.

(iii) Omdat $\alpha^{49} = F^2(\alpha)$ weer een nulpunt is van f (Gevolg 12.15), is $\alpha^{49} - 1$ een nulpunt van het polynoom $f(X+1) = (X+1)^3+(X+1)+1 = X^3+3X^2+4X+3$ en omdat f irreducibel is, is ook $f(X+1)$ irreducibel. Dus het gevraagde minimumpolynoom is $X^3 + 3X^2 + 4X + 3$.