Uitwerkingen Ringen en Galoistheorie, 10 april 2019

1. Beschouw het polynoom $P(X) = X^4 - 2X^3 + 2X^2 + 1$.

   (a) Bewijs dat $P(X)$ irreducibel is in $\mathbb{Q}[X]$ (hint: vervang X door $X + 1$).

   (b) Ontbind $P(X)$ in irreducibele factoren in $(\mathbb{Z}/3\mathbb{Z})[X]$.

   Uitwerking.

   (a) We bekijken $P(X+1)$. Modulo 2 krijgen we $P(X+1) \equiv (X+1)^4 + 1 \equiv X^4$ (mod 2), dus de coëfficiënten van X^3, X^2 en X zijn deelbaar door 2. Ook de constante coëfficiënt is deelbaar door 2, maar voor de Eisensteineigenschap hebben we meer nodig. De constante coëfficiënt van $P(X+1)$ (gezien als polynoom in X) is $P(0+1) = P(1) = 1 - 2 + 2 + 1 = 2$, dus deze is niet deelbaar door 4. Dus $P(X+1)$ is Eisenstein bij 2, en ook primitief (want monisch), dus $P(X+1)$ is irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$. Ook $P(X)$ is dan irreducibel in die twee ringen (want een factorisatie $f(X)g(X)$ van $P(X)$ geeft de factorisatie $f(X+1)g(X+1)$ van $P(X+1)$).

   (b) Modulo 3 geldt $P(X) = X^4 + X^3 - X^2 + 1$. We zien dat -1 een nulpunt is, en $P(X) = (X+1)(X^3 - X + 1)$. De tweede factor is van graad 3 en heeft geen nulpunten (want elk element van $\mathbb{Z}/3\mathbb{Z}$ is nulpunt van $X^3 - X$) en is daarom irreducibel. Dus $(X+1)(X^3 - X + 1)$ is de ontbinding in irreducibele factoren in $(\mathbb{Z}/3\mathbb{Z})[X]$ (eventueel kan men beide factoren met -1 vermenigvuldigen en/of de volgorde veranderen).

2. Laat $f\colon R \to S$ een ringhomomorfisme zijn. Laat I een ideaal van S zijn en laat M een maximaal ideaal van S zijn.

   (a) Bewijs dat $f^{-1}(I)$ een ideaal van R is.

   (b) Bewijs dat $f^{-1}(M)$ een priemideaal van R is.

   (c) Geef een voorbeeld waaruit blijkt dat $f^{-1}(M)$ geen maximaal ideaal van R hoeft te zijn.

   (d) Bewijs: als f surjectief is, dan is $f^{-1}(M)$ wel een maximaal ideaal van R.

   Uitwerking.

   (a) Laat $g\colon S \to S/I$ het standaard quotiënthomomorfisme zijn. De kern van g is dus I. De samenstelling $g \circ f$ van g en f is een ringhomomorfisme van R naar S/I en de kern van $g \circ f$ is $f^{-1}(\ker g) = f^{-1}(I)$. De kern van elk ringhomomorfisme is een ideaal, dus $f^{-1}(I)$ is een ideaal van R. (Het is ook eenvoudig na te gaan dat $f^{-1}(I)$ aan alle definiërende eigenschappen van een ideaal voldoet.)

(b) We weten al dat $f^{-1}(M)$ een ideaal is. We weten ook dat S/M een lichaam is. En omdat de kern van het homomorfisme $g \circ f$ van R naar S/M gelijk is aan $f^{-1}(M)$ (zie hierboven), is $R/f^{-1}(M)$ isomorf met een deelring van S/M. Elke deelring van een lichaam is een domein, dus $R/f^{-1}(M)$ is een domein, dus $f^{-1}(M)$ is een priemideaal van R.

(c) We kunnen bijvoorbeeld $R = \mathbb{Z}$ en $S = \mathbb{Q}$ nemen. Dan is f noodzakelijk de inclusie van $\mathbb{Z}$ in $\mathbb{Q}$. In $\mathbb{Q}$ is (0) het enige maximale ideaal, en het inverse beeld is het ideaal (0) in $\mathbb{Z}$. Dit is natuurlijk niet maximaal, want $\mathbb{Z}$ is geen lichaam.

(d) Als f surjectief is, dan is $g \circ f$ ook surjectief, en dan is $R/f^{-1}(M)$ isomorf met het lichaam S/M. Dus dan is $R/f^{-1}(M)$ een lichaam, dus $f^{-1}(M)$ is een maximaal ideaal van R.

3. Welke van de volgende beweringen zijn waar? In elk van de gevallen: geef een bewijs of laat zien dat de bewering onwaar is.

(a) Als x een nilpotent element is van een ring R, dan is $1 - x$ een eenheid van R.

(b) $\mathbb{F}_2[X]/(X^2 + 1) \cong \mathbb{F}_2 \times \mathbb{F}_2$.

(c) Laat L een Galoisuitbreiding zijn van $\mathbb{Q}$ van graad n. Dan is het aantal tussenlichamen van L over $\mathbb{Q}$ gelijk aan het aantal positieve delers van n.

Uitwerking.

(a) Deze bewering is waar. Er bestaat een $n \in \mathbb{Z}_{\geq 1}$ met $x^n = 0$, dus $1 - x^n = 1$, maar $1 - x^n$ is natuurlijk deelbaar door $1 - x$: $1 = 1 - x^n = (1 - x)(1 + x + x^2 + \cdots + x^{n-1})$, dus $1 - x$ is een eenheid.

(b) We zien eerst dat aan beide kanten ringen staan met 4 elementen, dus er is een kans. Als *abelse groep* zijn ze ook allebei isomorf met $\mathbb{F}_2 \times \mathbb{F}_2$. Merk echter op dat $X^2 + 1 = (X + 1)^2$ in $\mathbb{F}_2[X]$, dus $X + 1$ is nilpotent in $\mathbb{F}_2[X]/(X^2 + 1)$ (niet nul, maar het kwadraat is nul). Maar de elementen van $\mathbb{F}_2 \times \mathbb{F}_2$ zijn $(0, 0)$, $(1, 0)$, $(0, 1)$ en $(1, 1)$; geen daarvan is nilpotent. Dus $\mathbb{F}_2[X]/(X^2 + 1)$ en $\mathbb{F}_2 \times \mathbb{F}_2$ zijn niet isomorf als ringen, dus de bewering is onwaar.

(c) Laat G de Galoisgroep zijn van L over $\mathbb{Q}$. We weten dat de tussenlichamen van L over $\mathbb{Q}$ precies corresponderen met de ondergroepen van G. De orde van een ondergroep van G is een deler van n, de orde van G. Maar we zouden een voorbeeld moeten kunnen vinden waar het aantal ondergroepen verschilt van het aantal positieve delers. Inderdaad: als L het splijtlichaam is van $X^3 - 2$ over $\mathbb{Q}$, dan is $G \cong S_3$ zoals bekend; voor elk van de delers 1, 3 en 6 is er precies één ondergroep van die orde, maar er zijn drie ondergroepen van orde 2. De bewering is dus onwaar. (Ook $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ met Galoisgroep isomorf met $C_2 \times C_2$ levert een tegenvoorbeeld.)

4. Bepaal voor elk van de volgende idealen of het een priemideaal is en of het een maximaal ideaal is.

   (a) $(3, X^3 + 4X^2 + 4X + 10)$ in $\mathbb{Z}[X]$.

   (b) $(X^2 + 2Y^2)$ in $\mathbb{Q}(\sqrt{2})[X, Y]$.

   (c) $(X^2 + 1, Y^2 + 2, Z^2 - 2)$ in $\mathbb{Q}[X, Y, Z]$.

   Uitwerking.

   (a) Noem het ideaal I. Dan is $\mathbb{Z}[X]/I$ isomorf met $\mathbb{F}_3[X]/(X^3 + X^2 + X + 1)$. Maar $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$, dus $X^3 + X^2 + X + 1$ is niet irreducibel in $\mathbb{F}_3[X]$, dus $(X^3 + X^2 + X + 1)$ is geen priemideaal in $\mathbb{F}_3[X]$, dus het quotiënt is geen domein, dus $\mathbb{Z}[X]/I$ is geen domein, dus I is geen priemideaal van $\mathbb{Z}[X]$, dus ook geen maximaal ideaal.

   (b) In $\mathbb{C}[X, Y]$ splitst $X^2 + 2Y^2$ als $(X + i\sqrt{2}Y)(X - i\sqrt{2}Y)$. Maar deze factorisatie is niet mogelijk in $\mathbb{Q}(\sqrt{2})[X, Y]$, dus $X^2 + 2Y^2$ is irreducibel in de ontbindingsring (UFD) $\mathbb{Q}(\sqrt{2})[X, Y]$, dus $(X^2 + 2Y^2)$ is een priemideaal in die ring. Het is echter duidelijk strikt bevat in het ideaal (X, Y), en dat is een maximaal ideaal, dus is het zelf geen maximaal ideaal.

   (c) Noem het ideaal J. Dan is $\mathbb{Q}[X, Y, Z]/J$ isomorf met $\mathbb{Q}(\sqrt{2})[X, Y]/(X^2 + 1, Y^2+2)$, en dit is weer isomorf met $\mathbb{Q}(\sqrt{2}, i)[Y]/(Y^2+2)$. Maar in $\mathbb{Q}(\sqrt{2}, i)[Y]$ splitst $Y^2 + 2$ als $(Y + i\sqrt{2})(Y - i\sqrt{2})$, dus $(Y^2 + 2)$ is geen priemideaal in $\mathbb{Q}(\sqrt{2}, i)[Y]$, dus het quotiënt is geen domein, dus J is geen priemideaal in $\mathbb{Q}[X, Y, Z]$, dus ook geen maximaal ideaal.

5. Beschouw het polynoom $f = X^4 + 6X^2 - 3 \in \mathbb{Q}[X]$ en laat L het splijtlichaam van f over $\mathbb{Q}$ zijn.

   (a) Bewijs dat f irreducibel is in $\mathbb{Q}[X]$.

   (b) Bewijs dat f minstens één reëel nulpunt heeft.

   (c) Zij α een reëel nulpunt van f. Toon aan dat $\sqrt{-3}/\alpha$ en $-\alpha$ ook nulpunten van f zijn. Bepaal alle nulpunten van f in termen van α en $\sqrt{-3}$.

   (d) Toon aan dat $\sqrt{-3} \in L$ en dat $L = \mathbb{Q}(\alpha, \sqrt{-3})$.

   (e) Bepaal de graad $[L : \mathbb{Q}]$.

   (f) Toon aan dat er een $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ bestaat zó dat

   $$\sigma(\alpha) = \sqrt{-3}/\alpha, \quad \sigma(\sqrt{-3}) = -\sqrt{-3}.$$

   Laat zien dat σ orde 4 heeft.

   (g) Bepaal het deellichaam van L dat via de Galoiscorrespondentie met de ondergroep voortgebracht door σ^2 correspondeert.

(h) Zij M het deellichaam van L dat via de Galoiscorrespondentie met de ondergroep voortgebracht door σ correspondeert. Bewijs dat M een primitieve vierde eenheidswortel bevat.

Uitwerking.

(a) f is primitief en Eisenstein bij 3, dus irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

(b) Omdat $f(0) < 0$ en $f(100) > 0$ volgt uit de tussenwaardestelling dat f minstens één reëel nulpunt heeft (f is continu op $\mathbb{R}$).

(c) Het is direct duidelijk dat $-\alpha$ ook een nulpunt is, want $f(X)$ is een polynoom in X^2. Verder

$$f(\sqrt{-3}/\alpha) = 9/\alpha^4 - 18/\alpha^2 - 3 = -3(\alpha^4 + 6\alpha^2 - 3)/\alpha^4 = -3(f(\alpha))/\alpha^4 = 0,$$

dus $\sqrt{-3}/\alpha$ is ook een nulpunt. Ook $-\sqrt{-3}/\alpha$ is dus een nulpunt. Geen van deze nulpunten is 0. Ze zijn alle vier verschillend, want α en $-\alpha$ zijn reëel, met verschillend teken, en de andere twee zijn zuiver imaginair, met positief resp. negatief imaginair deel. We hebben dus alle 4 nulpunten van f gevonden.

(d) Omdat α en $\sqrt{-3}/\alpha$ beide in L zitten, zit ook $\sqrt{-3}$ in L. We hebben net alle nulpunten uitgedrukt in α en $\sqrt{-3}$, dus $L = \mathbb{Q}(\alpha, \sqrt{-3})$.

(e) Omdat f irreducibel en monisch is, is het het minimumpolynoom van α over $\mathbb{Q}$. Dus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$. Maar $\mathbb{Q}(\alpha)$ is bevat in $\mathbb{R}$, dus bevat niet $\sqrt{-3}$. Dus L heeft graad 2 over $\mathbb{Q}(\alpha)$. De graad $[L : \mathbb{Q}]$ is dus gelijk aan $4 \cdot 2 = 8$.

(f) Elementen van $G := \mathrm{Gal}(L/\mathbb{Q})$ moeten α naar een wortel van f sturen, en $\sqrt{-3}$ naar $\pm\sqrt{-3}$, en liggen daardoor vast. Er zijn dus ten hoogste 8 mogelijkheden. Maar L is Galois over $\mathbb{Q}$, dus G heeft 8 elementen. Alle 8 mogelijkheden komen dus voor. I.h.b. is σ een element van G. We zien dat $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\sqrt{-3}/\alpha) = -\sqrt{-3}/(\sqrt{-3}/\alpha) = -\alpha$ en $\sigma^2(\sqrt{-3}) = \sqrt{-3}$. Dus σ^2 is niet de identiteit, maar σ^4 wel, want $\sigma^4(\alpha) = \sigma^2(\sigma^2(\alpha)) = \sigma^2(-\alpha) = -\sigma^2(\alpha) = -(-\alpha) = \alpha$ (en $\sigma^4(\sqrt{-3}) = \sqrt{-3}$). Dus σ heeft orde 4.

(g) Noem dit deellichaam N. Net hebben we gezien dat $\sqrt{-3} \in N$. Ook $\alpha^2 \in N$, want $\sigma^2(\alpha^2) = (\sigma^2(\alpha))^2 = (-\alpha)^2 = \alpha^2$. Nu is α^2 een nulpunt van X^2+6X-3 (ook irreducibel, natuurlijk), dus α^2 heeft graad 2 over $\mathbb{Q}$. Dus $\mathbb{Q}(\alpha^2, \sqrt{-3})$ heeft graad 4 over $\mathbb{Q}$. Anderzijds weten we via de Galoiscorrespondentie dat N graad 4 over $\mathbb{Q}$ heeft, want $\langle\sigma^2\rangle$ heeft orde 2. Dus $N = \mathbb{Q}(\alpha^2, \sqrt{-3})$.

(h) M is bevat in N en M heeft graad 2 over $\mathbb{Q}$. We weten dat $\sigma(\alpha^2) = (\sqrt{-3}/\alpha)^2 = -3/\alpha^2$ en dat $\sigma(\sqrt{-3}) = -\sqrt{-3}$. We zoeken een σ-invariant element dat niet in $\mathbb{Q}$ zit. Natuurlijk is $\alpha^2 - 3/\alpha^2$ invariant, maar dit is gelijk aan -6 ! Anderzijds wordt $\alpha^2 + 3/\alpha^2 = \alpha^2 - \sigma(\alpha^2)$ door σ naar zijn tegengestelde gestuurd. Dus $\beta := (\alpha^2 + 3/\alpha^2)\sqrt{-3}$ is σ-invariant. We weten ook dat $3/\alpha^2 = \alpha^2 + 6$, dus $\beta = (2\alpha^2 + 6)\sqrt{-3}$. Dus β is niet 0, en is zuiver

imaginair, dus $M = \mathbb{Q}(\beta)$. Tenslotte kunnen we α^2 expliciet bepalen: de nulpunten van $X^2 + 6X - 3$ zijn $(-6 \pm \sqrt{48})/2 = -3 \pm 2\sqrt{3}$. Omdat $\alpha \in \mathbb{R}$ geldt $\alpha^2 \geq 0$, dus $\alpha^2 = -3 + 2\sqrt{3}$. Dus $\beta = 4\sqrt{3}\sqrt{-3} = 12i$, dus M bevat een primitieve vierde eenheidswortel.