Departement Wiskunde, Faculteit Bètawetenschappen, UU.
In elektronische vorm beschikbaar gemaakt door de TBC van A−Eskwadraat.
Het college WISB222 werd in 2005/2006 gegeven door Wilberd van der Kallen.
De uitwerking is samengesteld/gemaakt door Andor Lukacs.

Uitwerking[1] Ringen en Galoistheorie (WISB222) 3 juli 2006

Opgave 1

Zij τ het reële getal $\sqrt{1+\sqrt{2}}$ en zij $i \in \mathbb{C}$ de gebruikelijke wortel uit -1.
Zij $f(X) = (X^2-1)^2 - 2 \in \mathbb{Q}[X]$.
Zij L het lichaam dat over $\mathbb{Q}$ wordt voortgebracht door de nulpunten in $\mathbb{C}$ van $f(X)$.

a) Laat zien dat $f(\tau) = 0$.

b) Laat zien dat $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ en $\mathbb{Q}(\tau)/\mathbb{Q}(\sqrt{2})$ Galois uitbreidingen zijn.

c) Laat zien dat er een $\beta \in \mathrm{Gal}(L/\mathbb{Q})$ is met $\beta(\sqrt{2}) = -\sqrt{2}$.

d) Laat zien dat $\beta(\mathbb{Q}(\sqrt{2})) \subset \mathbb{R}$.

e) Laat zien dat $(\tau\beta(\tau))^2 = \tau^2\beta(\tau^2) = -1$.

f) Laat zien dat $\mathbb{Q}(i, \sqrt{2}) \subset L$.

g) Laat zien dat τ, $-\tau$, i/τ, $-i/\tau$ de wortels van f zijn.

h) Laat zien dat $L = \mathbb{Q}(\tau, i)$ en bepaal $[L : \mathbb{Q}]$.

i) Laat zien dat $\mathbb{Q}(\tau)/\mathbb{Q}$ niet Galois is.

j) Laat zien dat er α, γ in $\mathrm{Gal}(L/\mathbb{Q})$ zijn met $\alpha(\tau) = \tau$, $\alpha(i) = -i$, $\gamma(\tau) = i/\tau$, $\gamma(i) = -i$. Men kan narekenen dat α, γ een diëdergroep D_4 voortbrengen.

Oplossingen

b) Merk op dat beide uitbreidingen karakteristiek nul en graad twee hebben: het minimaalpolynoom van $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$ en dat van τ over $\mathbb{Q}(\sqrt{2})$ is $X^2 - (1+\sqrt{2})$. Dus zijn deze uitbreidingen separabel en normaal, dus zijn ze Galois.

c) De identiteitsafbeelding van $\mathbb{Q}$ kan op twee manieren worden uitgebreid tot een $\mathbb{Q}$-inbedding $\mathbb{Q}(\sqrt{2}) \longrightarrow L$: de wortels van $X^2 - 2$ zijn $\pm\sqrt{2}$ en een van deze uitbreidingen moet $\sqrt{2}$ naar $-\sqrt{2}$ afbeelden. Deze afbeelding kan weer op verschillende manieren uitgebreid worden tot $\mathbb{Q}$-automorfismen $L \longrightarrow L$, dus we kunnen er daar een willekeurige van nemen: β zodat $\beta(\sqrt{2}) = -\sqrt{2}$.

d) $\{1, \sqrt{2}\}$ is een basis van $\mathbb{Q}(\sqrt{2})$, β is $\mathbb{Q}$-lineair en beeldt $\sqrt{2}$ af op $-\sqrt{2}$, dus $\beta(\mathbb{Q}(\sqrt{2})) = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Merk op dat dit feit niet afhangt van de gekozen β.

e) De eerste gelijkheid geldt aangezien β een morfisme van lichamen is. De tweede is slechts een berekening.

f) In opgave a) gebruikten we al dat $\sqrt{2} = \tau^2 - 1 \in L$. Nu volgt uit opgave e) dat $i = \pm\tau\beta(\tau)$, wat elementen zijn van L.

[1] Deze uitwerkingen zijn met de grootste zorg gemaakt. In geval van fouten kan de TBC niet verantwoordelijk worden gesteld, maar wordt zij wel graag op de hoogte gesteld: `tbc@a-eskwadraat.nl`

h) Het eerste deel volgt direct uit opgave g). Merk voor het tweede deel op dat $[\mathbb{Q}(\tau) : \mathbb{Q}] = 4$, want opgaven d) en e) impliceren dat $\tau \notin \mathbb{Q}(\sqrt{2})$ (hieruit volgt dat f inderdaad het minimaalpolynoom van τ is), en dat $[\mathbb{Q}(\tau, i) : \mathbb{Q}(\tau)] = 2$, aangezien $X^2 + 1$ irreducibel is over $\mathbb{Q}(\tau)$. Dus het antwoord is $[L : \mathbb{Q}] = 8$.

i) f splijt niet over $\mathbb{Q}(\tau)$ aangezien $i \notin \mathbb{Q}(\tau)$. Dus is de uitbreiding $\mathbb{Q}(\tau)/\mathbb{Q}$ niet normaal, dus niet Galois.

j) De identiteitsafbeelding van $\mathbb{Q}(\tau)$ kan op twee manieren worden uitgebreid tot een $\mathbb{Q}(\tau)$-automorfisme van $L = \mathbb{Q}(\tau, i)$ (want $X^2 + 1$ heeft twee wortels). De ene, met $i \mapsto -i$, is de gevraagde α. Op eenzelfde manier kunnen we de identiteitsafbeelding van $\mathbb{Q}$ uitbreiden, eerst naar $\gamma_1 : \mathbb{Q}(i) \longrightarrow L$ zodat $\gamma_1(i) = -i$, en vervolgens kunnen we γ_1 weer uitbreiden naar $\gamma : L \longrightarrow L$ zodat $\tau \mapsto i/\tau$: merk op dat dit kan omdat f nog steeds irreducibel is over $\mathbb{Q}(i)$.

Opgave 2

Gegeven is in $\mathbb{Z}[X]$ het ideaal $I = (6, X^2 + 5)$.

a) Laat zien dat $\mathbb{Z}[X]/I \cong \mathbb{Z}[X]/(2, X^2 + 5) \times \mathbb{Z}[X]/(3, X^2 + 5)$.

b) Laat zien dat $\mathbb{Z}[X]/I \cong \mathbb{F}_2[X]/(X + 1)^2 \times \mathbb{F}_3 \times \mathbb{F}_3$.

c) Hoeveel elementen heeft $\mathbb{Z}[X]/I$?

d) Vind een priemideaal van $\mathbb{F}_2[X]$ dat $X^2 + 5$ bevat.

e) Vind een priemideaal van $\mathbb{Z}[X]$ dat I bevat.

f) Vind een maximaal ideaal van $\mathbb{Z}[X]$ dat I bevat.

Oplossingen

a) Zij $I_1 = (2, X^2 + 5)$ en $I_2 = (3, X^2 + 5)$. Aangezien $1 = 3 - 2 \in I_1 + I_2$, hebben we dat $I_1 + I_2 = \mathbb{Z}[X]$, dus kunnen we de Chinese reststelling toepassen, waaruit we kunnen concluderen dat $\mathbb{Z}[X]/I = \mathbb{Z}[X]/(I_1 \cdot I_2) \simeq \mathbb{Z}[X]/I_1 \times \mathbb{Z}[X]/I_2$.

b) Beschouw het ideaal $J_1 = (2) \subseteq I_1$. Volgens de derde isomorfismestelling geldt nu

$$\mathbb{Z}[X]/I_1 \simeq (\mathbb{Z}[X]/J_1)/\phi(I_1)$$

waarbij $\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/J_1$ de canonieke projectie is. Maar $\mathbb{Z}[X]/J_1 = \mathbb{F}_2[X]$ en $X^2 + 5 = X^2 + 1 = (X + 1)^2$ in $\mathbb{F}_2[X]$, dus $\mathbb{Z}[X]/I_1 \simeq \mathbb{F}_2[X]/(X + 1)^2$.

Analoog: beschouw het ideaal $J_2 = (3) \subseteq I_1$ en pas de derde isomorfismestelling toe, wat leidt tot $\mathbb{Z}[X]/I_2 \simeq \mathbb{F}_3[X]/((X + 1)(X - 1))$. De idealen $(X + 1)$ en $(X - 1)$ zijn relatief priem in $\mathbb{F}_3[X]$, aangezien $1 = (X - 1) - (X + 1)$, en toepassing van de Chinese reststelling leidt tot $\mathbb{Z}[X]/I_2 \simeq \mathbb{F}_3[X]/(X - 1) \times \mathbb{F}_3[X]/(X + 1) \simeq \mathbb{F}_3 \times \mathbb{F}_3$. Het resultaat uit opgave a) besluit vervolgens dit bewijs.

c) Zij $x = X + (g)$ in $\mathbb{F}_2[X]$ met $g = (X + 1)^2$. Dan geldt $x^2 + 1 = (X^2 + 1) + (g) = (g)$, en we zien dat we slechts vier elementen hebben: $\mathbb{F}_2[X]/(g) = \{0 + (g), 1 + (g), x, x + 1\}$. Het antwoord is dus $36 = 4 \times 3 \times 3$.

d) $X^2 + 5 = (X + 1) \cdot (X + 1)$, dus het ideaal $(X + 1)$ is een goede kandidaat. Aangezien $\mathbb{F}_2[X]/(X + 1) \simeq \mathbb{F}_2$ een domein is, is dit ideaal inderdaad een priemideaal.

e) We kunnen opgave d) gebruiken om een voorbeeld te construeren: $I \subseteq (2, X + 1)$ in $\mathbb{Z}[X]$, want $X^2 + 5 = (X + 1) \cdot (X - 1) + 2 \cdot 3$. Aan de andere kant geldt $\mathbb{Z}[X]/(2, X + 1) \simeq \mathbb{F}_2[X]/(X + 1) \simeq \mathbb{F}_2$ wat een domein is, dus $(2, X + 1)$ is een priemideaal van $\mathbb{Z}[X]$.

f) Het gegeven ideaal uit het vorige voorbeeld is ook maximaal: $\mathbb{F}_2$ is niet slechts een domein, maar ook een lichaam.