Uitwerkingen Ringen en Galoistheorie, 3 juli 2019

1. Stel $f(X) = X^7 + 5X^6 - 6X^5 + 2X^4 - 2X^3 + 10X - 10$.

   (a) Ontbind $f(X)$ in irreducibele factoren in $\mathbb{Z}[X]$.

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

   (c) Ontbind $f(X)$ in irreducibele factoren in $(\mathbb{Z}/5\mathbb{Z})[X]$.

   Uitwerking.

   (a) We zien vrijwel direct dat $f(1) = 0$, dus $f(X)$ heeft een factor $X - 1$. Een staartdeling geeft dat $f(X) = (X-1)g(X)$ met $g(X) = X^6+6X^5+2X^3+10$. We zien dat $g(X)$ Eisenstein is bij 2, dus $g(X)$ is irreducibel in $\mathbb{Z}[X]$ (want monisch, dus primitief). De ontbinding van $f(X)$ in $\mathbb{Z}[X]$ is dus $(X-1)(X^6+6X^5+2X^3+10)$.

   (b) Modulo 3 geldt $g(X) = X^6+2X^3+1 = (X^3+1)^2$ en $X^3+1 = (X+1)^3$, dus $g(X) = (X+1)^6$ in $(\mathbb{Z}/3\mathbb{Z})[X]$, dus de ontbinding van $f(X)$ in $(\mathbb{Z}/3\mathbb{Z})[X]$ is $(X-1)(X+1)^6$.

   (c) Modulo 5 geldt $g(X) = X^6 + X^5 + 2X^3 = X^3(X^3 + X^2 + 2)$. Het polynoom $h(X) = X^3 + X^2 + 2$ heeft geen nulpunten in $\mathbb{Z}/5\mathbb{Z}$, want $h(0) = 2$, $h(1) = 4$, $h(2) = 4$, $h(3) = 3$ en $h(4) = 2$ (zoals uit berekeningen blijkt). Omdat h graad 3 heeft, is het dus irreducibel in $(\mathbb{Z}/5\mathbb{Z})[X]$. Dus de ontbinding van $f(X)$ in $(\mathbb{Z}/5\mathbb{Z})[X]$ is $(X-1)X^3(X^3+X^2+2)$.

2. Zij R een ring met $1 \neq 0$ zodat voor elk element $r \in R \setminus \{1\}$ er een geheel getal $n > 0$ bestaat zodat $r^n = 0$.

   (a) Neem $a \in R \setminus \{0\}$, laat zien dat a inverteerbaar is. *Hint: Gebruik dat* $1 + a \in R \setminus \{1\}$.

   (b) Laat zien dat R isomorf is aan $\mathbb{Z}/2\mathbb{Z}$.

   Uitwerking.

   (a) We gebruiken de hint: er bestaat een geheel getal $n > 0$ zodat $(1 + a)^n = 0$. Hogere machten van $1 + a$ zijn dan ook nul, dus laten we voor het gemak $n > 2$ nemen. Uitwerken met het binomium van Newton geeft $0 = 1 + na + \binom{n}{2}a^2 + \cdots + a^n$ dus $1 = -a(n + \binom{n}{2}a + \cdots + a^{n-1})$, dus a is inverteerbaar.

   (b) Als $x \in R$ en $x \neq 0$ en $x \neq 1$, dan is x zowel nilpotent als inverteerbaar. Dan zou $0 = 1$ volgen, dus dit kan niet. (Als $ax = 1$ en $x^n = 0$, dan $1 = a^n x^n = 0$.) Dus $R = \{0, 1\}$. We zien nu onmiddellijk dat $1 + 1 = 0$ en $1 \cdot 1 = 1$ en het volgt dat R isomorf is aan $\mathbb{Z}/2\mathbb{Z}$.

3. Laat R een ring zijn met slechts één ideaal I zodat $(0) \subsetneq I \subsetneq R$.

   (a) Laat zien dat I een priemideaal is.

   (b) Laat zien dat I een hoofdideaal is.

   (c) Bewijs dat I de verzameling is bestaande uit 0 en alle nuldelers van R. *Hint: Gebruik dat $I \cdot I$ gelijk is aan (0) of I.*

   Uitwerking.

   (a) I is een maximaal ideaal, dus een priemideaal.

   (b) Kies $x \in I$ met $x \neq 0$. Dan $(0) \subsetneq (x) \subseteq I$, dus $(x) = I$. Dus I is een hoofdideaal en elk niet-nul element van I is een voortbrenger.

   (c) $I \cdot I$ is een ideaal bevat in I, dus het is gelijk aan (0) of I. Kies x met $(x) = I$. Dan $I \cdot I = (x^2)$. Als $x^2 = 0$, dan is x een nuldeler. Als $(x^2) = I$ dan $x = ax^2$ voor een $a \in R$. Dus $x(1 - ax) = 0$. Natuurlijk $x \neq 0$. Maar ook $1 - ax \neq 0$, want als $ax = 1$, dan $(x) = R$. Dus x is ook nu een nuldeler. In beide gevallen is x dus een nuldeler, en I bestaat dan uit 0 en nuldelers. Als y een nuldeler is, dan is y geen eenheid, dus $(y) \subseteq I$, dus $y \in I$. Het gevraagde is bewezen.

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

   (a) $(5, X^3 + 6X^2 + 6X + 6)$ in $\mathbb{Z}[X]$.

   (b) $(3X^2 + Y^2)$ in $\mathbb{Q}(\sqrt{3})[X, Y]$.

   Uitwerking.

   (a) Noem het ideaal I. Dan is $\mathbb{Z}[X]/I$ isomorf met $\mathbb{F}_5[X]/(X^3 + X^2 + X + 1)$. Maar $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$, dus $X^3 + X^2 + X + 1$ is niet irreducibel in $\mathbb{F}_5[X]$, dus $(X^3 + X^2 + X + 1)$ is geen priemideaal in $\mathbb{F}_5[X]$, 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 $3X^2 + Y^2$ als $(Y + i\sqrt{3}X)(Y - i\sqrt{3}X)$. Maar deze factorisatie is niet mogelijk in $\mathbb{Q}(\sqrt{3})[X, Y]$, dus $3X^2 + Y^2$ is irreducibel in de ontbindingsring (UFD) $\mathbb{Q}(\sqrt{3})[X, Y]$, dus $(3X^2 + Y^2)$ 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.

5. Zij $f = X^6 + 3$ en laat L een splijtlichaam zijn van f over $\mathbb{Q}$.

   (a) Laat zien dat f irreducibel is in $\mathbb{Z}[X]$.

   (b) Zij $\alpha \in L$ een nulpunt van f en ω een derdemachtseenheidswortel, laat zien dat $-\alpha$ en $\omega\alpha$ nulpunten zijn van f.

   (c) Bewijs dat $L = \mathbb{Q}(\alpha)$.

(d) Bepaal de groep $\mathrm{Gal}(L/\mathbb{Q})$.

(e) Bepaal een $\beta \in L$ zodat $\mathbb{Q}(\beta)$ een deellichaam is van L van graad 2 over $\mathbb{Q}$. Hoeveel zulke deellichamen zijn er?

(f) Bepaal een $\gamma \in L$ zodat $\mathbb{Q}(\gamma)$ een deellichaam is van L van graad 3 over $\mathbb{Q}$. Hoeveel zulke deellichamen zijn er?

Uitwerking.

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

(b) Omdat $f(X) = X^6 + 3$, geldt evident dat $f(-\alpha) = f(\alpha) = f(\omega\alpha)$, dus $-\alpha$ en $\omega\alpha$ zijn ook nulpunten van f.

(c) De wortels van f zijn $\pm\alpha$, $\pm\omega\alpha$ en $\pm\omega^2\alpha$ als ω een primitieve derdemachtseenheidswortel is. We moeten dus laten zien dat $\omega \in \mathbb{Q}(\alpha)$. We weten dat $\omega = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$, dus we hebben nodig dat $\sqrt{-3} \in \mathbb{Q}(\alpha)$. Welnu, $\alpha^6 = -3$, dus $\alpha^3 = \pm\sqrt{-3}$; dit geeft het gevraagde.

(d) L is Galois over $\mathbb{Q}$. Omdat $L = \mathbb{Q}(\alpha)$ weten we dat de elementen van $G = \mathrm{Gal}(L/\mathbb{Q})$ precies gegeven worden door α te sturen naar een wortel van het minimumpolynoom f van α over $\mathbb{Q}$. Dus G is een groep met 6 elementen en L heeft graad 6 over $\mathbb{Q}$.

We beginnen met σ gegeven door $\sigma(\alpha) = -\alpha$. Merk op dat $\sigma(\alpha^3) = -\alpha^3$, dus $\sigma(\sqrt{-3}) = -\sqrt{-3}$, dus $\sigma(\omega) = \omega^2$. Dus σ verwisselt $\omega\alpha$ en $-\omega^2\alpha$ en ook $-\omega\alpha$ en $\omega^2\alpha$. Natuurlijk is σ van orde 2.

Bekijk ook τ met $\tau(\alpha) = \omega\alpha$. Dan $\tau(\alpha^3) = \alpha^3$, dus $\tau(\omega) = \omega$. Dus τ geeft de cykels $\alpha \mapsto \omega\alpha \mapsto \omega^2\alpha \mapsto \alpha$ en $-\alpha \mapsto -\omega\alpha \mapsto -\omega^2\alpha \mapsto -\alpha$. Dus τ is van orde 3.

Op isomorfie na zijn er twee groepen van orde 6: de cyclische (dus abelse) groep C_6 en de niet-abelse permutatiegroep S_3. Het is duidelijk dat σ en τ de groep G voortbrengen, dus de vraag is of ze commuteren of niet.

Welnu, $\sigma\tau(\alpha) = \sigma(\omega\alpha) = -\omega^2\alpha$ en $\tau\sigma(\alpha) = \tau(-\alpha) = -\omega\alpha$. Dus σ en τ commuteren niet, en $G = \langle\sigma, \tau\rangle$ is isomorf met S_3.

(e) ω is van graad 2 over $\mathbb{Q}$, dus we kunnen $\beta = \omega$ nemen. Ook α^3 is van graad 2 over $\mathbb{Q}$; dit leidt tot hetzelfde deellichaam. Volgens de hoofdstelling van de Galoistheorie corresponderen de deellichamen van L van graad 2 over $\mathbb{Q}$ met de ondergroepen van G van orde 3. Elke groep van orde 6 heeft een unieke ondergroep van orde 3, zodat ook een fout antwoord bij (d) hier tot een goed antwoord kan leiden: er is precies één zo'n deellichaam.

(f) Natuurlijk is α^2 van graad 3 over $\mathbb{Q}$ en de keuze $\gamma = \alpha^2$ ligt wellicht het meest voor de hand. Deellichamen van L van graad 3 over $\mathbb{Q}$ corresponderen met ondergroepen van G van orde 2, dus met elementen van G van orde 2. Zoals bekend heeft S_3 drie elementen van orde 2, dus er zijn drie zulke deellichamen.