Ringen en Galoistheorie Uitwerkingen, 21 april 2016

1. Stel $P(x) = x^4 - 2x^3 + 2x^2 - 2x - 1$.

   (a) (1 pt) Bewijs dat $P(x)$ irreducibel is in $\mathbb{Q}[x]$ (hint: vervang x door $x+1$).
   Antwoord: Berekening leert dat $P(x+1) = x^4+2x^3+2x^2-2$. Dit is een Eisensteinpolynoom voor $p = 2$ en dus irreducibel in $\mathbb{Q}[x]$. Daarmee is $P(x)$ ook irreducibel.

   Iets minder rekenwerk, bekijk $P(x+1)$ modulo 2, $P(x+1) \equiv (x+1)^4 - 1 \equiv x^4 (\text{mod } 2)$. Alle coefficienten van $P(x+1)$ zijn dus deelbaar door 2. De constante term van $P(x+1)$ is $P(1) = -2$, dus 2^2 deelt de constante term niet.

   (b) (1 pt) Ontbind $P(x)$ in irreducibele factoren in $(\mathbb{Z}/3\mathbb{Z})[x]$.
   Antwoord: Proberen van $x = 0, 1, 2$ leert dat 2 een nulpunt van $P(x) (\text{mod } 3)$ is. Staartdeling geeft $P(x) \equiv (x-2)(x^3+2x+2) (\text{mod } 3)$. Als $x^3 + 2x + 2 (\text{mod } 3)$ reducibel zou zijn dan heeft het een lineaire factor en dus een nulpunt in $\mathbb{Z}/3\mathbb{Z}$. Controle voor $x = 0, 1, 2$ leert dat dat niet het geval is.

   (c) (1/2 pt) Bewijs dat voor elke $n, m \in \mathbb{Z}_{\geq 1}$ het polynoom $x^n + y^m - 1$ irreducibel is in $\mathbb{C}[x, y]$.
   Antwoord: Beschouw het polynoom als polynoom in x met coefficienten in $\mathbb{C}[y]$. Deze laatste ring is een uniek ontbindingsdomein en kunnen we het Eisensteincriterium toepassen. We doen dit met het irreducibele element $y - 1$. Deze deelt alle coefficienten behalve de kopcoefficient x^n. Bovendien is $(y-1)^2$ geen deler van $y^m - 1$. Dit laatste polynoom heeft geen meervoudige nulpunten.

2. Zij R de deelring van $\mathbb{Q}(x)$ die bestaat uit de rationale functies $P(x)/Q(x)$ met de eigenschap dat $Q(0) \neq 0$ en $Q(1) \neq 0$.

   (a) (1/2 pt) Bepaal de eenheden in R.
   Antwoord: Zij $P(x)/Q(x) \in R$ waarbij we aannemen dat $P(x)$ en $Q(x)$ ggd 1 hebben. Dan geldt: $P(x)/Q(x) \in R^\times \iff Q(x)/P(x) \in R \iff P(0)P(1) \neq 0$. De eenheden in R worden dus gegeven door alle $P(x)/Q(x)$ met $P(0), P(1) \neq 0$ (en natuurlijk $Q(0), Q(1) \neq 0$).

   (b) (1/2 pt) Bepaal de irreducibele elementen in R.
   Antwoord: Stel $P(x)/Q(x) \in R$. We kunnen $P(x)$ schrijven als $P(x) = x^m(x-1)^n P^*(x)$ waarin $P^*(0) \neq 0$ en $P^*(1) \neq 0$. Dus $P^*(x)/Q(x)$ is een éénheid in R. Met andere woorden, elke element in R kan worden geschreven als $x^m(x-1)^n$ maal een éénheid voor zekere $m, n \in \mathbb{Z}_{\geq 0}$. Als $m + n \geq 2$ dan is dit element reducibel, want product van minstens twee factoren. De enige irreducibele elementen zijn dus van de vorm x of $x - 1$ (op vermenigvuldiging met eenheden na).

(c) (1 pt) Bepaal de maximale idealen in R.
Antwoord: Zij I een maximaal ideaal. De elemnten van I kunnen geen éénheid zijn, anders zou gelden dat $I = R$. Voor elk element $A(x) \in I$ geldt dus $A(0) = 0$ of $A(1) = 0$. Als voor alle $A(x) \in I$ zou gelden dat $A(0) = 0$ dan is x een deler voor alle elementen, dus $(x) \subset I$. Maar (x) is een maximaal ideaal, want $R/(x)$ is isomorf met $\mathbb{Q}$ via het evaluatie-isomorfisme gegeven door $A(x) \mapsto A(0)$. Conclusie, $I = (x)$. Op dezelfde manier handelen we het geval af dat voor alle elementen $A(x) \in I$ geldt $A(1) = 0$. In dat geval geldt $I = (x - 1)$.

Stel tenslotte dat er $A(x), B(x) \in I$ zijn zo dat $A(0) = 0, A(1) \neq 0$ en $B(0) \neq 0, B(1) = 0$. Dan geldt dat $A(x) + B(x)$ niet nul is in $x = 0$ en $x = 1$. Dus is het een eenheid, en dat kan niet.

3. Zij R_1, R_2 een tweetal ringen. Onder de productring $R_1 \times R_2$ verstaan we de ring bestaande uit geordende paren (r_1, r_2) met $r_1 \in R_1, r_2 \in R_2$ en de componentsgewijze optelling en vermenigvuldiging. Dus $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ en $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$.

Beschouw nu de polynoomring $\mathbb{R}[x, y]$ in twee variabelen x, y en het ringhomomorfisme $\phi : \mathbb{R}[x, y] \to \mathbb{R}[x] \times \mathbb{R}[y]$ gegeven door $\phi : p(x, y) \mapsto (p(x, 0), p(0, y))$.

(a) (1/2 pt) Bewijs dat de kern van ϕ gegeven wordt door (xy).
Antwoord:

$$p(x, y) \in \ker(\phi) \iff p(x, 0) = 0 \text{ en } p(0, y) = 0 \iff$$

$$\iff y | p(x, y) \text{ en } x | p(x, y) \iff xy | p(x, y) \iff p(x, y) \in (xy).$$

(b) (1 pt) Bewijs dat er geen isomorfisme bestaat tussen $\mathbb{R}[x, y]/(xy)$ en $\mathbb{R}[x] \times \mathbb{R}[y]$. (hint: bepaal de oplossingen voor $a^2 = 1$ in elk van de ringen).
Antwoord: We lossen eerst $a^2 = 1$ op in $\mathbb{R}[x] \times \mathbb{R}[y]$. Stel $a = (p(x), q(y))$. Dan impliceert $a^2 = 1$ dat $(p(x)^2, q(y)^2) = (1, 1)$, het 1-element in $\mathbb{R}[x] \times \mathbb{R}[y]$. Dus $p(x)^2 = 1$ en $q(y)^2 = 1$, waaruit volgt dat $p(x) = \pm 1$ en $q(y) = \pm 1$. De oplossingen zijn dus $(1, 1), (1, -1), (-1, 1), (-1, -1)$.

We lossen nu $a^2 = 1$ in $\mathbb{R}[x, y]/(xy)$ op. Zij $f = f(x, y)$ een polynoom zó dat $f^2 - 1 \equiv 0 (\text{mod } xy)$. Hieruit volgt dat $xy | (f^2 - 1)$ en dat impliceert $xy | (f - 1)(f + 1)$. Als xy een deler is van $f + 1$ of $f - 1$, dan krijgen we $f \equiv 1 (\text{mod } xy)$ of $f \equiv -1 (\text{mod } xy)$. Maar het kan ook gebeuren dat $x | (f - 1)$ en $y | (f + 1)$. Schrijf nu $f - 1 = x f_1(x, y)$ en $f + 1 = y f_2(x, y)$. Neem het verschil van de twee, $2 = x f_1(x, y) + y f_2(x, y)$. Rechts zien we een polynoom dat constante term 0 heeft, terwijl er links een 2 staat. Dat kan dus niet. Evenzo kan $y | (f - 1)$ en $x | (f + 1)$ niet optreden. We hebben dus twee oplossingen gevonden, $f \equiv \pm 1 (\text{mod } xy)$.

Als $\mathbb{R}[x] \times \mathbb{R}[y]$ en $\mathbb{R}[x, y]/(xy)$ isomorf zouden zijn, dan zou de vergelijking $a^2 = 1$ in beide ringen hetzelfde aantal oplossingen moeten hebben, en dat is niet het geval.

(c) (1/2 pt) Geef een element van $\mathbb{R}[x] \times \mathbb{R}[y]$ dat niet in het beeld van ϕ zit.
Antwoord: Stel dat $(a(x), b(y))$ in het beeld van ϕ zit.Dan is er $p(x, y) \in \mathbb{R}[x, y]$ zó dat $p(x, 0) = a(x)$ en $p(0, y) = b(y)$. Gevolg $a(0) = p(0, 0) = b(0)$. Conclusie, als we $a(x), b(y)$ kiezen zó dat $a(0) \neq b(0)$ dan zit $(a(x), b(y))$ niet in het beeld. Voorbeeld, $(1, -1)$.

4. Zij $L \subset \mathbb{C}$ het splijtlichaam van $f(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ en zij $\alpha \in L$ een reëel nulpunt van $f(x)$.

(a) (1/2 pt) Bewijs dat de volledige nulpuntenverzameling van f gegeven wordt door $\pm\alpha, \pm\sqrt{-2}/\alpha$.
Antwoord: f is een polynoom in x^2. Dus zowel α als $-\alpha$ zijn nulpunten. Verder, $f(\sqrt{-2}/\alpha) = 4/\alpha^4 + 4/\alpha^2 - 2 = (-2/\alpha^4)(-2 - 2\alpha^2 + \alpha^4) = (-2/\alpha^4)f(\alpha) = 0$. Dus $\sqrt{-2}/\alpha$ (en ook $-\sqrt{-2}/\alpha$) zijn nulpunten. Hiermee hebben we alle vier nulpunten te pakken.

(b) (1/2 pt) Bewijs dat $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
Antwoord: α is een nulpunt van $f(x)$ en dat is een Eisensteinpolynoom ten aanzien van $p = 2$. Dus f is irreducibel in $\mathbb{Q}[x]$ en het minimaalpolynoom van α. Gevolg: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{graad}(f) = 4$.

(c) (1/2 pt) Merk op dat $L = \mathbb{Q}(\alpha, \sqrt{-2})$ en bewijs dat $[L : \mathbb{Q}] = 8$.
Antwoord: Er geldt dat $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Verder $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha, \sqrt{-2}) : \mathbb{Q}(\alpha)] \leq 2$ omdat $\sqrt{-2}$ nulpunt van $x^2 + 2$ is. Omdat we $\alpha \in \mathbb{R}$ kunnen kiezen en $\sqrt{-2} \notin \mathbb{Q}(\alpha)$ geldt $[\mathbb{Q}(\alpha, \sqrt{-2}) : \mathbb{Q}(\alpha)] = 2$. In totaal vinden we daarmee $[L : \mathbb{Q}] = 2 \cdot 4 = 8$.

(d) (1 pt) Geef expliciete voortbrengers van $\text{Gal}(L/\mathbb{Q})$ en hun relaties.
Antwoord: Omdat L splijtlichaam is en $[L : \mathbb{Q}] = 8$ geldt $|G| = |\text{Gal}(L/\mathbb{Q})| = 8$. Voor elke $\rho \in G$ geldt dat $\rho : \alpha \mapsto \pm\alpha, \pm\sqrt{-2}/\alpha$ en $\rho : \sqrt{-2} \mapsto \pm\sqrt{-2}$. Omdat $|G| = 8$ komt elke mogelijkheid voor. We kiezen

$$\sigma : \alpha \mapsto \sqrt{-2}/\alpha, \qquad \sigma : \sqrt{-2} \to -\sqrt{-2}$$

en

$$\tau : \alpha \mapsto \alpha, \qquad \tau : \sqrt{-2} \mapsto -\sqrt{-2}.$$

Controleer dat $\sigma^2 : \alpha \mapsto -\alpha, \sqrt{-2} \mapsto \sqrt{-2}$. Hieruit zien we dat σ orde 4 heeft. Verder heeft τ orde 2 en geldt dat $\sigma\tau = \tau^3\sigma$. Dit zijn de definierende relaties voor de groep van het vierkant D_4.

(e) (1 pt) Bepaal alle ondergroepen van orde 4 van $\text{Gal}(L/\mathbb{Q})$ en de bijbehorende invariante lichamen van graad 2 over $\mathbb{Q}$.
Antwoord: Er zijn drie ondergroepen van orde 4 van D_4. Dat zijn $\langle\sigma\rangle, \langle\tau, \sigma^2\rangle, \langle\tau\sigma, \sigma^2\rangle$.
Eenvoudige controle leert dat α^2 een invariant is voor σ^2 en τ. Merk op dat α^2 als minimaal polynoom $x^2 - x - 2$ heeft. De abc-formule geeft als nulpunten $1 \pm \sqrt{3}$. Dus het invariante lichaam van $\langle\sigma^2, \tau\rangle$ is $\mathbb{Q}(\sqrt{3})$.

We weten ook dat $\sqrt{-2} \in L$. Deze is invaraint onder zowel σ^2 als $\sigma\tau$. Dus het invariantenlichaam van $\langle \sigma\tau, \sigma^2 \rangle$ is $\mathbb{Q}(\sqrt{-2})$.
Omdat $\sqrt{3}, \sqrt{-2} \in L$ moet ook $\sqrt{-6} \in L$ en dit geeft onze derde kwadratische uitbreiding, invariant onder $\langle \sigma \rangle$.