Ringen en Galoistheorie, 11 april 2018, 13:30-16:30 uur

UITWERKINGEN

1. Zijn de volgende uitspraken goed of fout? Geef een tegenvoorbeeld of een bewijs.

   (a) (1/2 pt) Het product van twee hoofdidealen in een ring is weer een hoofdideaal.
   Uitwerking: Gegeven de idealen (a) en (b). Bewering: $(a)(b) = (ab)$. Omdat $ab \in (a)(b)$ geldt ook $(ab) \subset (a)(b)$. Het ideaal $(a)(b)$ bestaat uit sommen van termen van van de vorm xy met $x \in (a)$ en $y \in (b)$. Dus er zijn ξ, η zo dat $x = \xi a$ en $y = \eta b$. Dus $xy = \xi\eta ab \in (ab)$. Alle sommen van dergelijke producten zitten ook in (ab). Conclusie $(a)(b) \subset (ab)$.

   (b) (1/2 pt) Het polynoom $10X^6 - 15X^2 + 7$ is irreducibel in $\mathbb{Q}[X]$.
   Uitwerking Het polynoom $P(X) = 10X^6 - 15X^2 + 7$ is irreducibel dan en slechts dan als $X^6 * P(1/X) = 7X^6 - 15X^4 + 10$ dat is. Merk op dat het laatste polynoom Eisenstein is t.a.v. 5, en dus irreducibel.

   (c) (1/2 pt) In $\mathbb{Z}[X, Y]$ is $(X - 2, Y - X^2)$ een maximaal ideaal.
   Uitwerking: Het is geen maximaal ideaal want strict bevat in $J = (2, X - 2, Y - X^2) = (2, X, Y)$. Dit laatste ideaal $\neq \mathbb{Z}[X, Y]$.

   (d) (1/2 pt) De graad $[L : K]$ van het splijtlichaam van een irreducibel polynoom $f \in K[X]$ is altijd deelbaar door de graad van f.
   Uitwerking: Waar, stel $\alpha \in L$ nulpunt van f. Dan geldt $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. Omdat de graad van f gelijk is aan $[K(\alpha) : K]$ (per definitie), is de graad van f een deler van $[L : K]$.

   (e) (1/2 pt) Als $K \subset M \subset L$ lichamen zijn, en L/K is Galois, dan is M/K Galois.
   Uitwerking: Niet waar, neem $K = \mathbb{Q}$ en L splitlichaam van $X^3 - 2$. Dan is $M = K(\sqrt[3]{2})$ niet Galois.

2. Beschouw het polynoom $P(X) = X^4 + 3X^3 + X^2 - 5$

   (a) (1 pt) Ontbindt $P(X)$ in $\mathbb{Q}[X]$.
   Uitwerking: Als P een lineaire factor heeft dan is deze van de vorm $X - a$ met a een deler van 5. Proberen geeft dat $a = 1$ voldoet. Ontbinden geeft

   $$X^4 + 3X^3 + X^2 - 5 = (X - 1)(X^3 + 4X^2 + 5X + 5).$$

   Als de derde graads factor reducibel zou zijn, zou hij deelbaar moeten zijn door een polynoom van de vorm $X - b$ met b een deler van 5. Proberen van $b = \pm 1, \pm 5$ geeft geen oplossing.

(b) (1/2 pt) Ontbindt $P(X)$ in $(\mathbb{Z}/3\mathbb{Z})[X]$.
Uitwerking: Op grond van voorgaande ontbinding weten we dat

$$P(X) \equiv (X-1)(X^3+X^2+2X+2) (\text{mod } 3).$$

We zien meteen al de factor $X+1$ in het derde graads polynoom. Dus

$$P(X) \equiv (X-1)(X+1)(X^2-1) \equiv (X-1)^2(X+1)^2 (\text{mod } 3).$$

3. Bewijs de volgende twee beweringen:

(a) (1 pt) Elk ideaal in de productring $R_1 \times R_2$ kan geschreven worden als $I_1 \times I_2$, met I_1, I_2 idealen in respectievelijk R_1 en R_2.
Uitwerking: Zij π_1 het homomorfisme $R_1 \times R_2 \to R_1$ gegeven door $\pi_1(r_1, r_2) = r_1$. Evenzo definieren we π_2 als projectie van $R_1 \times R_2$ op R_2. Zij I een ideaal in $R = R_1 \times R_2$. Stel I_1 het beeld van I onder π_1 en I_2 het beeld van I onder π_2. Het is duidelijk dat $I \subset I_1 \times I_2$. Kies nu $(i_1, i_2) \in I_1 \times I_2$. Omdat I_1 het beeld is van I onder π_1 bestaat er een paar $(i_1, b) \in I$. Vermenigvuldig dit met $(1, 0)$. Omdat I een ideaal is zit het product $(1, 0)(i_1, b) = (i_1, 0)$ ook in I. Evenzo geldt dat $(0, i_2) \in I$. En dus zit hun som (i_1, i_2) in I. We concluderen dat $I_1 \times I_2 \subset I$.

(b) (1/2 pt) Zij R een ring en $R_1 \subset R$ een deelring. Zij $I \subset R$ een priemideaal. Dan is $I \cap R_1$ een priemideaal in R_1.
Uitwerking: Stel $a, b \in R_1$ and $ab \in I \cap R_1$. Omdat I een priemideaal is geldt $a \in I$ of $b \in I$ (of beide). Omdat a, b ook element van R_1 zijn geldt $a \in I \cap R_1$ of $b \in I \cap R_1$.

4. (a) (1 pt) Bepaal de éénheden van de polynoomring $(\mathbb{Z}/4\mathbb{Z})[X]$.
Uitwerking: Zij $A \in (\mathbb{Z}/4\mathbb{Z})[X]$ een éénheid. dan is er een polynoom B zó dat $AB \equiv 1 (\text{mod } 4)$. In het bijzonder geldt dat $AB \equiv 1 (\text{mod } 2)$. Omdat $(\mathbb{Z}/2\mathbb{Z})[X]$ een polynoomring is met coefficienten in een lichaam $(\mathbb{Z}/2\mathbb{Z})$, hebben we unieke ontbinding en volgt uit $AB \equiv 1 (\text{mod } 2)$ dat $A \equiv B \equiv \pm 1 (\text{mod } 2)$. Stel omgekeerd dat $A(X) \equiv \epsilon (\text{mod } 2)$ met $\epsilon \equiv \pm 1$. Dat wil zeggen, $A(X) = \epsilon + 2A_1(X)$ met $A_1(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$. Dan zien we dat

$$(\epsilon + 2A_1(X))(\epsilon - 22A_1(X)) = 1 - 4A_1(X)^2 \equiv 1 (\text{mod } 4).$$

Met andere woorden, de éénheden in $(\mathbb{Z}/4\mathbb{Z})[X]$ worden gegeven door de polynomen $\epsilon + 2A_1(X)$.

(b) (1 pt) Zij R een ring en $a \in R$ een nilpotent element (dat wil zeggen: er is een $n \geq 1$ zó dat $a^n = 0$). Zij $x \in R^*$ een éénheid. Bewijs dat $x - a$ een éénheid in R is (hint: begin met $x = 1$ en $n = 2$).
Uitwerking: We bewijzen eerst onze bewering met $x = 1$. Merk op dat $(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1 - a^n = 1$. Dus is $1 - a$ een éénheid. Nu voor een willekeurige eenheid x. Merk op dat $(a/x)^n = 0$. Uit het voorgaande volgt dat $1 - a/x$ een éénheid is, en dus ook $x - a = x(1 - x/a)$.

5. Beschouw het polynoom $f = X^6 + 3X^3 + 3 \in \mathbb{Q}[X]$. Zij L het splijtlichaam van f over het grondlichaam $\mathbb{Q}$. Zij ω een primitieve derde éénheidswortel (dat wil zeggen, $\omega^3 = 1$ en $\omega \neq 1$).

   (a) (1/2 pt) Bewijs dat f irreducibel in $\mathbb{Q}[X]$ is.
   Uitwerking: f is Eisenstein t.a.v $p = 3$.

   (b) (1/2 pt) Stel dat $\alpha \in L$ een nulpunt is van f. Laat zien dat $\omega^k\alpha$ voor $k = 1, 2$ ook een nulpunt van f is, evenals $\sqrt[3]{3}/\alpha$.
   Uitwerking: $(\omega^k\alpha)^6 + 3(\omega^k\alpha)^3 + 3 = \alpha^6 + 3\alpha^3 + 3 = 0$. Verder,

$$(\sqrt[3]{3}/\alpha)^6 + 3(\sqrt[3]{3}/\alpha)^3 + 3 = (3/\alpha^6)(3 + 3\alpha^3 + \alpha^6) = 0.$$

   (c) (1/2 pt) Bewijs dat $\alpha^3 \in \mathbb{Q}(\omega)$.
   Uitwerking: α^3 is nulpunt van het polynoom $Y^2 + 3Y + 3$. De nulpunten daarvaan zijn $-3/2 \pm \sqrt{-3}/2$. Dus $\alpha^3 \in \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$.

   (d) (1/2 pt) Bewijs dat $L = \mathbb{Q}(\alpha, \sqrt[3]{3})$.
   Uitwerking Uit het tweede onderdeel volgt dat L wordt voortgebracht over $\mathbb{Q}$ door $\omega^k\alpha$ en $\omega^l\sqrt[3]{3}$ met $k, l = 0, 1, 2$. Dus $L = \mathbb{Q}(\alpha, \omega, \sqrt[3]{3})$. Maar uit het derde onderdeel weten we dat $\omega \in \mathbb{Q}(\alpha)$. Dus kunnen we ω weglaten en krijgen we het gevraagde resultaat.

   (e) (1/2 pt) Er is gegeven dat $\sqrt[3]{3} \notin \mathbb{Q}(\alpha)$. Bepaal $[L : \mathbb{Q}]$.
   Uitwerking: Er geldt dat $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. We weten dat $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. We willen nu aantonen dat $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha, \sqrt[3]{3} : \mathbb{Q}(\alpha)] = 3$. Met andere woorden $\sqrt[3]{3}$ heeft graad 3 over $\mathbb{Q}(\alpha)$, ofwel $X^3 - 3$ is irreducibel in $\mathbb{Q}(\alpha)[X]$. Stel dat $X^3 - 3$ reducibel is. Dan heeft $X^3 - 3$ een nulpunt in $\mathbb{Q}(\alpha)$. Stel dat dit $\omega^k\sqrt[3]{3}$ is (met $k = 0, 1$ of 2). Omdat $\omega \in \mathbb{Q}(\alpha)$ zou dus ook $\sqrt[3]{3}$ in $\mathbb{Q}(\alpha)$ moeten liggen. Maar er is gegeven dat dat niet kan. We concluderen dat $[L : \mathbb{Q}] = 18$.

   (f) (1 pt) Laat zien dat $\mathrm{Gal}(L/\mathbb{Q}(\omega))$ isomorf is met $C_3 \times C_3$ (direct product van twee cyclische groepen van orde 3).
   Uitwerking: Zij $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(\omega))$. Dan zijn er $k, l \in \{0, 1, 2\}$ zó dat $\sigma(\sqrt[3]{3}) = \omega^k\sqrt[3]{3}$ en $\sigma(\alpha) = \omega^l\alpha$ (omdat $\alpha^3 \in \mathbb{Q}(\omega)$, NB: $\sigma(\omega) = \omega$). Dit zijn 9 mogelijkheden. Omdat $[L : \mathbb{Q}(\omega)] = 9$ komt elke mogelijkheid ook voor. Kies nu de Galoisgroep elementen ρ, τ gegeven door

$$\rho(\sqrt[3]{3}) = \omega\sqrt[3]{3}, \qquad \rho(\alpha) = \alpha$$

   en

$$\rho(\sqrt[3]{3}) = \sqrt[3]{3}, \qquad \rho(\alpha) = \omega\alpha.$$

   Dan leert een eenvoudige berekening dat ρ en τ orde 3 hebben, en $\rho \circ \tau = \tau \circ \rho$. Ze brengen dus het product van twee cyclische groepen van orde 3 voort.