EXAMEN ALGEBRA II:
28 januari 2008
oplossingen

Opgelet: de oplossingen die hieronder staan, zijn soms nogal kort uitgeschreven. Een goed antwoord op het examen is best wat gedetailleerder.

---

1. *In de definitie van het radicaal Rad(J) van een ideaal J in een commutatieve ring R wordt beweerd dat Rad(J) een ideaal is van R. Geef hiervoor een bewijs.*

   - Stel $f, g \in \mathrm{Rad}(J)$. Neem $n, m \in \mathbb{N}_0$ zodanig dat $f^n, g^m \in J$. We kunnen dan aantonen dat $(f+g)^{n+m} \in J$, wat bewijst dat $f + g \in \mathrm{Rad}(J)$. Immers, in een commutatieve ring geldt dat

     $$(f+g)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} f^{n+m-k} g^k$$

     en elke term hiervan behoort tot J. (Als $k \leq m$, is dit zo omdat $f^{n+m-k} \in J$, anders omdat $g^k \in J$.)
   - Stel $h \in R$ en $f \in \mathrm{Rad}(J)$. Neem n weer zodanig dat $f^n \in J$. Dan zal $(hf)^n \in J$, wat bewijst dat $hf \in \mathrm{Rad}(J)$.

2. *Waar of niet waar?*

   (a) *Voor elk even geheel getal $n \geq 2$, bestaat er een polynoom van graad n over $\mathbb{Q}$ met n verschillende niet-rationale wortels, met Galoisgroep over $\mathbb{Q}$ isomorf met $\mathbb{Z}/2\mathbb{Z}$.*
   WAAR. Neem bijvoorbeeld $f(X) = \prod_{i=1}^{n/2}(X^2 - 2^{2i-1})$.

   (b) *Zij $F \subset E_1 \subset E_2$ eindige velduitbreidingen. Als $Gal(E_1, F) \cong Gal(E_2, F)$, dan is $E_1 = E_2$.*
   NIET WAAR. Neem bijvoorbeeld $F = \mathbb{Q} = E_1$, en $E_2 = \mathbb{Q}(\sqrt[3]{2})$.

3. *Zij $n \geq 1$ een geheel getal, ω een primitieve n-de eenheidswortel in $\mathbb{C}$. Zij K een deelveld van $\mathbb{C}$ dat ω bevat. Zij $a \in \mathbb{Z}$ en b een wortel van $X^n - a$ in $\mathbb{C}$. Toon volgende uitspraken aan.*

   (a) *De Galoisgroep $Gal(K(b), K)$ is isomorf met de cyclische groep $\mathbb{Z}_d$, waarbij d een deler is van n. Ook geldt dat $b^d \in K$.*
   Aangezien b een wortel is van $X^n - a$, bestaat er een $k \in \mathbb{N}$ zodanig dat $b = \sqrt[n]{a}\,\omega^k$. Aangezien $\omega \in K$, zal $K(b) = K(\sqrt[n]{a})$. De morfismen zijn dus bepaald door het beeld van $\sqrt[n]{a}$. Dit element moet weer worden afgebeeld op een wortel van $X^n - a$, dus de morfismen zijn van de vorm $\sigma_l(\sqrt[n]{a}) = \sqrt[n]{a}\,\omega^l$ voor $l \in \{0, \ldots, n-1\}$. (Maar opgelet, er hoeft niet noodzakelijk voor elke l uit deze verzameling zo een σ_l te zijn.) Bij samenstelling van deze morfismen, zien we dat we de Galoisgroep kunnen beschouwen als deelgroep van de cyclische groep $\mathbb{Z}_n$. Een deelgroep hiervan is steeds van de vorm $\mathbb{Z}_d$ voor d een deler van n.
   Om aan te tonen dat $b^d \in K$, kiezen we een willekeurige $\sigma_l \in Gal(K(b), K)$ en tonen we aan dat $\sigma_l(b^d) = b^d$. Immers, onze uitbreiding is Galois (ontbindingsveld), dus zegt Theorem 4.40 dat K het vasteveld is. We gebruiken dat $b = \sqrt[n]{a}\,\omega^k$ en schrijven

   $$\sigma_l(b^d) = (\sigma_l(b))^d = (\sigma_l(\sqrt[n]{a}\,\omega^k))^d = (\sqrt[n]{a}\,\omega^l\omega^k)^d = b^d\omega^{ld}.$$

Dus moeten we enkel nog aantonen dat $\omega^{ld} = 1$, wat volgt als je uitschrijft dat $\sigma_l^d = Id$.

(b) *In het bijzonder, als $X^n - a$ irreducibel is over K, is $Gal(K(b), K) \cong \mathbb{Z}_n$.*

Dit is een eenvoudig gevolg, aangezien $X^n - a$ nu de minimale polynoom is van b over K, dus moet de uitbreidingsgraad gelijk zijn aan n en de Galoisgroep heeft orde n. (We gebruiken weer dat de uitbreiding $K \subset K(b)$ Galois is. Dit is zo omdat na toevoegen van $\sqrt[n]{a}$ elke wortel van $X^n - a$ tot $K(b)$ behoort.)

4. *Bepaal de Galoisgroep van $X^3 - 5$ over $\mathbb{Q}$, over $\mathbb{Q}(\sqrt[3]{5})$ en over $\mathbb{Q}(\sqrt{3}i)$.*

Ontbindingsveld $E = \mathbb{Q}(\sqrt[3]{5}, e^{2\pi i/3})$. De uitbreiding is Galois en de uitbreidingsgraad van $\mathbb{Q} \subset E$ is 6. (Uitleg nodig!) Dus we zoeken 6 Galoismorfismen. De $\mathbb{Q}$-morfismen zijn volledig bepaald door de beelden van $\sqrt[3]{5}$ en $e^{2\pi i/3}$, welke respectievelijk moeten worden afgebeeld op wortels van $X^3 - 5$ en $X^2 + X + 1$. Dit geeft slechts 6 kandidaten en aangezien er 6 Galoismorfismen zijn, zijn deze kandidaten inderdaad morfismen. De groepsstructuur wordt gegeven door de samenstelling van deze morfismen. We kunnen inzien dat de Galoisgroep isomorf is met S_3.

De uitbreidingsgraad van $E = \mathbb{Q}(\sqrt[3]{5}, e^{2\pi i/3})$ over $\mathbb{Q}(\sqrt[3]{5})$ is 2. De uitbreiding is Galois. De morfismen worden gegeven door het beeld van $e^{2\pi i/3}$ vast te leggen, wat enkel $e^{2\pi i/3}$ of $e^{4\pi i/3}$ kan zijn.

De uitbreidingsgraad van $E = \mathbb{Q}(\sqrt{3}i, \sqrt[3]{5}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt{3}i, \sqrt[3]{5})$ over $\mathbb{Q}(\sqrt{3}i)$ is 3. (We gebruiken dat $e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.) De morfismen worden nu bepaald door het beeld van $\sqrt[3]{5}$. Hiervoor zijn drie mogelijkheden.

5. (a) *Zij $I = < xy + y, xy + 2y - x > \subset \mathbb{C}[x, y]$. Bereken een Gröbner-basis voor I, gebruik makend van de gegradeerde lexicografische orde. Geef nu een basis van $\frac{\mathbb{C}[x,y]}{I}$ als vectorruimte over $\mathbb{C}$.*

Een Gröbner-basis voor I is $\{x - y, y^2 + y\}$, deze is te berekenen via het Buchberger-algoritme. Een basis voor de vectorruimte is $\{1, y\}$.

(b) *Zij nu een Gröbner-basis G van een ideaal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ gegeven. Hoe construeer je hieruit een basis van de $\mathbb{C}$-vectorruimte $\frac{\mathbb{C}[x_1,\ldots,x_n]}{I}$? Leg in detail uit waarom dit een basis is.*

Neem als basis alle monomen die niet deelbaar zijn door de leidende term van een van de veeltermen uit G. Deze zijn voortbrengend: als je vertrekt van de klasse van een willekeurige polynoom uit $\mathbb{C}[x_1, \ldots, x_n]$, kan je met behulp van het delingsalgoritme steeds een representant vinden waarvan geen enkele monoom deelbaar is door een leidende term van een element van G. Via eigenschappen van een Gröbnerbasis is ook aan te tonen dat deze lineair onafhankelijk zijn (voor een Gröbnerbasis geldt dat de rest na het delingsalgoritme nul is als en slechts als de polynoom tot het ideaal behoort).