

EXAMEN ALGEBRA II – 15 JANUARI 2010

Naam:

- Schrijf op elk blad je naam (ook onmiddellijk op dit opgaveblad).
- Als je een vraag blanco afgeeft, noteer dan op dit opgaveblad ‘blanco’ naast de vraag.
- Geef voldoende uitleg (vermeld de stellingen en eigenschappen die je gebruikt, argumenteer elke niet-triviale stap, geef uitleg bij je berekeningen, verzorg je taal en zorg ervoor dat de logische volgorde van de stappen die je volgt duidelijk is).
- Je moet enkel het net afgeven.

Veel succes!

- (3pt.) 1. (a) In het bewijs van de Tweede-Isomorfisme-stelling (Stelling 2.1.5): waarom heeft $p^\sigma(x)$ een wortel in E' ? In detail uitleggen!
- (b) In de Engelse tekst over Gröbnerbasisen, in het bewijs van Dicksons lemma (Theorem 21.18): leg in detail uit waarom er voor elke α in A een minimaal element β in B bestaat met $\beta \leq \alpha$.

- (5pt.) 2. Zij $a, b, c \in \mathbb{N}$ en beschouw het veld $E = \mathbb{Q}(\sqrt{a + b\sqrt{c}})$.

- (a) Bewijs dat E Galois is over $\mathbb{Q}$ als en slechts als
- (i) c een volkomen kwadraat is of
 - (ii) $a^2 - b^2c$ een kwadraat is in $\mathbb{Q}(\sqrt{c})$.
- (b) Geef voorbeelden van concrete a, b, c waarvoor $G(E/\mathbb{Q})$ respectievelijk de structuren $\mathbb{Z}_1$ (triviale groep), $\mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ en $\mathbb{Z}_4$ aanneemt.

Antwoord: (a) Merk eerst op dat $\sqrt{a + b\sqrt{c}}$ een nulpunt is van

$$f(X) = X^4 - 2aX^2 + a^2 - b^2c \in \mathbb{Q}[X].$$

De vier nulpunten van deze veelterm zijn te schrijven als

$$\pm\sqrt{a + b\sqrt{c}}, \quad \pm\sqrt{a - b\sqrt{c}}.$$

Merk ook op dat we in karakteristiek 0 werken, dus elke veelterm is separabel.

$\boxed{\Leftarrow}$ Als c een volkomen kwadraat is, dan is $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ een ontbindingsveld over $\mathbb{Q}$ van

$$X^2 - (a + b\sqrt{c}) \in \mathbb{Q}[X]$$

en bijgevolg Galois.

Als $a^2 - b^2c$ een kwadraat is in $\mathbb{Q}(\sqrt{c})$, dan beweren we dat $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ een ontbindingsveld over $\mathbb{Q}$ is van $f(X)$, en bijgevolg Galois. Daarvoor is het voldoende te bewijzen dat

$$\sqrt{a - b\sqrt{c}} \in \mathbb{Q}(\sqrt{a + b\sqrt{c}}).$$

Merk echter op dat

$$\sqrt{a - b\sqrt{c}} \cdot \sqrt{a + b\sqrt{c}} = \sqrt{a^2 - b^2c},$$

wat een element is van $\mathbb{Q}(\sqrt{c}) \subset \mathbb{Q}(\sqrt{a + b\sqrt{c}})$ omwille van het gegeven. Of nog:

$$\sqrt{a - b\sqrt{c}} = \frac{\sqrt{a^2 - b^2c}}{\sqrt{a + b\sqrt{c}}} \in \mathbb{Q}(\sqrt{a + b\sqrt{c}}).$$

$\boxed{\Rightarrow}$ Uit het ongerijmde. Veronderstel dat c geen volkomen kwadraat is, dat $a^2 - b^2c$ geen kwadraat is in $\mathbb{Q}(\sqrt{c})$, en dat $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ toch Galois is over $\mathbb{Q}$.

We kunnen dan gemakkelijk nagaan dat $f(X)$ irreducibel is. Inderdaad, $f(X)$ heeft geen lineaire factoren, want anders zou minstens één van de vier wortels $\pm\sqrt{a} \pm b\sqrt{c} \in \mathbb{Q}$ en dus $\sqrt{c} \in \mathbb{Q}$. Maar $f(X)$ kan evenmin splitsen in twee kwadratische factoren, omdat

$$X^4 - 2aX^2 + a^2 - b^2c = (X^2 + pX + q)(X^2 + rX + s)$$

impliceert dat $p + r = 0$ en $rq + ps = 0 \Rightarrow p = r = 0$ of $q = s$. Het eerste geval zou betekenen dat $(\sqrt{a + b\sqrt{c}})^2 + q = 0$ of $(\sqrt{a + b\sqrt{c}})^2 + s = 0$, in strijd met het feit dat c geen volkomen kwadraat is. Het tweede geval zou impliceren dat $q^2 = a^2 - b^2c$, in strijd met het feit dat $a^2 - b^2c$ geen kwadraat is in $\mathbb{Q}(\sqrt{c})$.

Een eerste manier om de oefening dan af te werken is door op te merken dat $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ normaal is over $\mathbb{Q}$ (want Galois) en dat dus

$$\sqrt{a - b\sqrt{c}} \in \mathbb{Q}(\sqrt{a + b\sqrt{c}}).$$

Bijgevolg bestaan er $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ waarvoor

$$\sqrt{a - b\sqrt{c}} = \alpha + \beta\sqrt{a + \gamma\sqrt{c}} + \gamma\left(\sqrt{a + b\sqrt{c}}\right)^2 + \delta\left(\sqrt{a + b\sqrt{c}}\right)^3.$$

Dus bestaan er $\alpha, \beta \in \mathbb{Q}(\sqrt{c})$ waarvoor

$$\sqrt{a - b\sqrt{c}} = \alpha + \beta\sqrt{a + b\sqrt{c}},$$

waarbij $\beta \neq 0$ omdat anders $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{c})$ anders uitbreidingsgraad 4 over $\mathbb{Q}$ zou hebben (want de minimale veelterm van het linkerlid is $f(X)$). Door beide leden van

$$\sqrt{a - b\sqrt{c}} - \beta\sqrt{a + b\sqrt{c}} = \alpha$$

te kwadrateren en alles door 2β te delen, besluiten we dat $\sqrt{a^2 - b^2c} \in \mathbb{Q}(\sqrt{c})$. *Contradictie.*

Alternatieve oplossing: omdat $f(X)$ irreducibel is, geldt $[\mathbb{Q}(\sqrt{a + b\sqrt{c}}) : \mathbb{Q}] = 4$ en bijgevolg

$$\#G(\mathbb{Q}(\sqrt{a + b\sqrt{c}})/\mathbb{Q}) = 4.$$

Omdat $\mathbb{Q}(\sqrt{a^2 - b^2c})$ en $\mathbb{Q}(\sqrt{c})$ twee verschillende tussenvelden zijn van graad 2 over $\mathbb{Q}$, moet wegens de Galois-correspondentie

$$\#G(\mathbb{Q}(\sqrt{a + b\sqrt{c}})/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

(want $\mathbb{Z}_4$ heeft slechts één deelgroep van orde 2). Omdat een Galois-morfisme volledig bepaald wordt door zijn actie op $\sqrt{a + b\sqrt{c}}$ en omdat wortels van $f(X)$ op wortels van $f(X)$ moeten worden afgebeeld, moeten dit de vier Galois-morfismen zijn:

$$\begin{aligned} \text{id} = \sigma_1 : \quad & \sqrt{a + b\sqrt{c}} \mapsto \sqrt{a + b\sqrt{c}} \\ \sigma_2 : \quad & \sqrt{a + b\sqrt{c}} \mapsto -\sqrt{a + b\sqrt{c}} \\ \sigma_3 : \quad & \sqrt{a + b\sqrt{c}} \mapsto \sqrt{a - b\sqrt{c}} \\ \sigma_4 : \quad & \sqrt{a + b\sqrt{c}} \mapsto -\sqrt{a - b\sqrt{c}}. \end{aligned}$$

Omdat $\sigma_2, \sigma_3, \sigma_4$ orde 2 hebben, permuteren ze twee wortels van $f(X)$. Bijgevolg worden ook de andere twee wortels van $f(X)$ gepermuteerd. Maar dat betekent dat

$$\sqrt{a^2 - b^2c} = \sqrt{a + b\sqrt{c}}\sqrt{a - b\sqrt{c}}$$

invariant is onder elke σ_i . Het Galois zijn impliceert dan dat $\sqrt{a^2 - b^2c} \in \mathbb{Q}$. *Contradictie.*

(b) Voor $\mathbb{Z}_1$ kunnen we bijvoorbeeld $a = b = c = 0$ kiezen.

Voor $\mathbb{Z}_2$ kunnen we bijvoorbeeld $a = 2, b = c = 0$ kiezen.

De echte oefening zit hem in de laatste twee gevallen. Alleszins moeten a, b, c aan voorwaarden (i) en (ii) voldoen, anders is de uitbreiding niet Galois en zal de Galoisgroep sowieso te klein zijn. De vier Galoisvormismen zijn dan:

$$\begin{aligned}\text{id} = \sigma_1 : \quad & \sqrt{a + b\sqrt{c}} \mapsto \sqrt{a + b\sqrt{c}} \\ \sigma_2 : \quad & \sqrt{a + b\sqrt{c}} \mapsto -\sqrt{a + b\sqrt{c}} \\ \sigma_3 : \quad & \sqrt{a + b\sqrt{c}} \mapsto \sqrt{a - b\sqrt{c}} \\ \sigma_4 : \quad & \sqrt{a + b\sqrt{c}} \mapsto -\sqrt{a - b\sqrt{c}}.\end{aligned}$$

Het morfisme σ_2 heeft zeker orde 2. Als σ_3 ook orde 2 heeft, dan is de structuur $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, zoniet is de structuur $\mathbb{Z}_4$. Het volstaat dus a, b, c te vinden waarvoor wel resp. niet geldt dat

$$\sigma_3 \left(\sqrt{a - b\sqrt{c}} \right) = \sqrt{a + b\sqrt{c}}.$$

Dit zal bijvoorbeeld wel zo zijn als $a = 2, b = 1, c = 3$ omdat

$$\sqrt{2 + \sqrt{3}} \sqrt{2 - \sqrt{3}} = 1,$$

dus zal

$$\sigma_3 \left(\sqrt{2 - \sqrt{3}} \right) = \sigma_3 \left(\sqrt{2 + \sqrt{3}} \right)^{-1} = \left(\sqrt{2 - \sqrt{3}} \right)^{-1} = \sqrt{2 + \sqrt{3}}$$

(dit komt trouwens letterlijk uit de oefenzittingen). Het zal foutlopen als bijvoorbeeld $a = 2, b = 1, c = 2$ omdat

$$\sqrt{2 + \sqrt{2}} \sqrt{2 - \sqrt{2}} = \sqrt{2},$$

waardoor

$$\begin{aligned}\sigma_3 \left(\sqrt{2 - \sqrt{2}} \right) &= \sigma_3(\sqrt{2}) \cdot \sigma_3 \left(\sqrt{2 + \sqrt{2}} \right)^{-1} = \sigma_3 \left(\left(\sqrt{2 + \sqrt{2}} \right)^2 - 2 \right) \cdot \sigma_3 \left(\sqrt{2 + \sqrt{2}} \right)^{-1} \\ &= \left(\left(\sqrt{2 - \sqrt{2}} \right)^2 - 2 \right) \cdot \left(\sqrt{2 - \sqrt{2}} \right)^{-1} = -\sqrt{2} \left(\sqrt{2 - \sqrt{2}} \right)^{-1} = -\sqrt{2 + \sqrt{2}}.\end{aligned}$$

(4pt.) 3. Zij $E_1, E_2 \subset F$ velden met $[F : E_1 \cap E_2] < \infty$. Noteer met $E_1 E_2$ het kleinste deelveld van F dat zowel E_1 als E_2 omvat. Veronderstel dat E_2 Galois is over $E_1 \cap E_2$. Toon aan:

- (a) $E_1 E_2$ is Galois over E_1 .
- (b) Het beperkingsmorfisme

$$\varphi : G(E_1 E_2, E_1) \rightarrow G(E_2, E_1 \cap E_2) : \sigma \mapsto \sigma|_{E_2}$$

is goed gedefinieerd en bijectief. Hint: toon eerst de injectiviteit aan en beschouw dan het vasteveld van E_2 onder het beeld van φ .

Antwoord: (a) Omdat E_2 Galois is over $E_1 \cap E_2$, is E_2 een ontbindingsveld van een separabele veelterm

$$f(X) \in (E_1 \cap E_2)[X],$$

i.e. $E_2 = (E_1 \cap E_2)(\alpha_1, \dots, \alpha_r)$ waarbij $f(X) = \prod_{i=1}^r (X - \alpha_i)$ over E_2 . Maar dan geldt

$$E_1 E_2 = E_1(\alpha_1, \dots, \alpha_r).$$

Inderdaad, duidelijk geldt $E_1, E_2 \subset E_1(\alpha_1, \dots, \alpha_r)$, en anderzijds moet elk veld dat E_1 en E_2 omvat ook E_1 en $\{\alpha_1, \dots, \alpha_r\}$ omvatten. Met andere woorden: $E_1 E_2$ is een ontbindingsveld van $f(X)$ over E_1 . Bijgevolg is $E_1 E_2$ Galois over E_1 , op voorwaarde dat we kunnen inzien dat de veelterm $f(X)$ nog steeds separabel is wanneer we ze over E_1 beschouwen. Maar dat is eenvoudig: elke irreducibele factor van $f(X)$ als veelterm over E_1 is een deler van een irreducibele factor van $f(X)$ als veelterm over $E_1 \cap E_2$ en kan dus geen meervoudige wortels bevatten.

(b) Het goed gedefinieerd zijn komt er op neer dat als $\sigma \in G(E_1 E_2, E_1)$, dat dan $\sigma|_{E_2} \in G(E_2, E_1 \cap E_2)$. We tonen dus aan dat $\sigma|_{E_2}$ een veldautomorfisme van E_2 is dat $E_1 \cap E_2$ invariant laat.

Duidelijk laat $\sigma|_{E_2}$ $E_1 \cap E_2$ invariant, want het laat E_1 invariant.

Ten tweede is $\sigma|_{E_2}$ injectief omdat σ het is.

Ten derde neemt $\sigma|_{E_2}$ waarden in E_2 aan. Inderdaad, elk element van $E_2 = (E_1 \cap E_2)(\alpha_1, \dots, \alpha_r)$ is een rationale uitdrukking in de α_i 's met coëfficiënten in $E_1 \cap E_2$. Onder σ wordt dit afgestuurd op de overeenkomstige rationale uitdrukking in de $\sigma(\alpha_i)$'s. Maar voor elke i is $\sigma(\alpha_i) = \alpha_j$ voor een zekere j , omdat wortels van $f(X)$ op wortels van $f(X)$ worden afgebeeld. Bijgevolg zijn de beeldwaarden terug rationale uitdrukkingen in de α_i 's met coëfficiënten in $E_1 \cap E_2$, dus elementen van E_2 .

Ten vierde en laatste is $\sigma|_{E_2}$ surjectief. Dat kan worden aangetoond door het voorgaande argument te verfijnen, of door op te merken dat een injectief endomorfisme van een eindigdimensionale $(E_1 \cap E_2)$ -vectorruimte automatisch surjectief is wegens de dimensiestelling.

Om de injectiviteit (van φ) aan te tonen volstaat het te bewijzen dat als $\sigma|_{E_2} = \text{id}_{E_2}$, dat dan $\sigma = \text{id}_{E_1 E_2}$. Maar $\sigma|_{E_2} = \text{id}_{E_2}$ impliceert dat σ gans E_2 invariant laat. Nu laat $\sigma \in G(E_1 E_2, E_1)$ natuurlijk ook E_1 invariant. Bijgevolg moet σ ook $E_1 E_2$ invariant laten, i.e. $\sigma = \text{id}_{E_1 E_2}$.

Voor de surjectiviteit tenslotte merken we op dat

$$E_{2, \varphi(G(E_1 E_2, E_1))} \subset E_1.$$

Inderdaad, kies een $x \in E_2$ zodat $\sigma|_{E_2}(x) = x$ voor alle $\sigma \in G(E_1 E_2, E_1)$. Maar dan is $\sigma(x) = x$ voor alle $\sigma \in G(E_1 E_2, E_1)$. Dus

$$x \in (E_1 E_2)_{G(E_1 E_2, E_1)} = E_1$$

waarbij de laatste gelijkheid geldt wegens (a). Maar per definitie geldt ook dat

$$E_{2, \varphi(G(E_1 E_2, E_1))} \subset E_2 \quad \text{en dat} \quad E_{2, \varphi(G(E_1 E_2, E_1))} \supset E_1 \cap E_2,$$

waaruit we besluiten:

$$E_{2, \varphi(G(E_1 E_2, E_1))} = E_1 \cap E_2.$$

Maar omdat E_2 Galois is over $E_1 \cap E_2$ geldt er ook dat

$$E_{2, G(E_2, E_1 \cap E_2)} = E_1 \cap E_2.$$

Wegens de Galoiscorrespondentie kunnen geen twee verschillende deelgroepen met hetzelfde tussenveld overeenkomen. Dus moet

$$\varphi(G(E_1 E_2, E_1)) = G(E_2, E_1 \cap E_2)$$

wat de surjectiviteit bewijst.

(6pt.) 4. Zijn de volgende uitspraken waar of niet? Bewijs telkens je antwoord.

(a) In $\mathbb{Q}[x, y, z]$ geldt dat

$$x - yz \in \langle x^2 + 2xy^2 - 2y^3z - y^2z^2, xy + xz - y^2z - yz^2 \rangle.$$

Antwoord: NIET WAAR. De algoritmische manier om dit te doen was om een Gröbnerbasis voor dit ideaal te berekenen (je zou moeten hebben gevonden dat bovenstaande basis al een Gröbnerbasis was voor de gewone lexicografische ordening), en daarna lidmaatschap te testen via deling met rest. Het kan ook veel korter, uit het ongerijmde. Stel dat er $f(x, y, z)$ en $g(x, y, z)$ bestaan waarvoor

$$x - yz = f(x, y, z)(x^2 + 2xy^2 - 2y^3z - y^2z^2) + g(x, y, z)(xy + xz - y^2z - yz^2).$$

Beide leden evalueren in $(x, 0, 0)$ geeft

$$x = f(x, 0, 0) \cdot x^2$$

wat natuurlijk nooit kan.

- (b) Elk maximaal ideaal van $\mathbb{C}[x_1, \dots, x_n]$ is van de vorm $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ voor $a_1, \dots, a_n \in \mathbb{C}$.

Antwoord: WAAR. Dit staat eigenlijk letterlijk in het bewijs van de zwakke Nullstellensatz (4.11 in de cursusnota's). Het volgt ook onmiddellijk uit de zwakke Nullstellensatz. Zij M een maximaal ideaal, i.h.b. geldt $M \neq (1)$. Wegens de zwakke Nullstellensatz bestaat er een punt $(a_1, \dots, a_n) \in V(M)$. Maar dan is $I(V(M)) \subset I(\{(a_1, \dots, a_n)\})$ en bijgevolg

$$M \subset I(\{(a_1, \dots, a_n)\}).$$

Omdat M maximaal is en $I(\{(a_1, \dots, a_n)\})$ de veelterm 1 niet bevat, moet gelijkheid gelden. Anderzijds is ook duidelijk

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \subset I(\{(a_1, \dots, a_n)\})$$

en analoog moet gelijkheid gelden omdat het eerste ideaal maximaal is (quotiëntring is een veld, nl. $\mathbb{C}$). We besluiten dat $M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$.

- (c) Zij F een veld en zij $\prec_x$ een monomenordening in $F[x_1, \dots, x_n]$. Zij

$$\varphi : F[x_1, \dots, x_n] \rightarrow F[y_1, \dots, y_{n'}]$$

een ringmorfisme dat monomen op monomen afstuurt. Dan bestaat er altijd een monomenordening $\prec_y$ in $F[y_1, \dots, y_{n'}]$ zodat voor alle monomen $m, m' \in F[x_1, \dots, x_n]$ geldt dat $m \prec_x m'$ als en slechts als $\varphi(m) \prec_y \varphi(m')$.

Antwoord: NIET WAAR. Beschouw bijvoorbeeld het morfisme

$$F[x_1, x_2] \mapsto F[y_1]$$

bepaald door $x_1 \mapsto y_1$, $x_2 \mapsto y_1^2$. Neem voor $\prec_x$ de gewone lexicografische orde, i.h.b. $x_2 \prec_x x_1$. Voor geen enkele monomenordening $\prec_y$ kan echter gelden dat $y_1^2 \prec_y y_1$.

- (d) Zij F een veld en zij $I_1, I_2 \subset F[x_1, \dots, x_n]$ twee monomiale idealen. Dan is $I_1 \cap I_2$ ook een monomiaal ideaal.

Antwoord: WAAR. Zij $I_1 = \langle m_{1,1}, \dots, m_{1,r} \rangle$ en $I_2 = \langle m_{2,1}, \dots, m_{2,s} \rangle$, waarbij de $m_{i,j}$ monomen zijn. We zullen bewijzen dat

$$I_1 \cap I_2 = \langle \text{kgv}(m_{1,i}, m_{2,j}) \mid i = 1, \dots, r, j = 1, \dots, s \rangle =: J.$$

De inclusie $\supset$ volgt meteen. Om $\subset$ te bewijzen kiezen we een willekeurige veelterm $f \in I_1 \cap I_2$. Fixeer een term T van f . Omdat $f \in I_1$ bestaan er veeltermen $g_{1,i}$ zodat

$$f = g_{1,1}m_{1,1} + \dots + g_{1,r}m_{1,r}.$$

Wil T rechts voorkomen, dan moet er minstens één i bestaan zodat $m_{1,i} \mid T$. Analoog zal er een j bestaan zodat $m_{2,j} \mid T$. Dus $\text{kgv}(m_{1,i}, m_{2,j}) \mid T$ of nog: $T \in J$. Omdat dit geldt voor alle termen van f , moet ook $f \in J$.

(2pt.) Practicum.