

EXAMEN ALGEBRA II – 5 JUNI 2021

- Leg je antwoorden helder uit en geef duidelijk aan welke resultaten je gebruikt.
- Dit examen bestaat uit **drie vragen**, genummerd van (1) tot en met (3), die elk bestaan uit verschillende deelvragen. **Elk van de drie vragen** moet op een apart blad worden beantwoord. Vergeet niet om op elk antwoordblad je naam te schrijven, en de bladen te nummeren. Je kladpapier hoeft je **niet** in te dienen.
- Zelfs als je een onderdeel van een oefening niet kan oplossen, mag je het resultaat gebruiken in het vervolg van de oefening.
- Het examen is open boek, je mag gebruik maken van de cursustekst en persoonlijke notities. Het is ook toegestaan om de cursustekst van Algebra 1 te gebruiken.
- Je hebt voor dit examen **3 uur** de tijd (4 uur voor studenten met faciliteiten).

- (1) Zij $K \subset E$ een eindige uitbreiding van velden. Beschouw twee deelvelden L en M van E die K bevatten. We noteren met LM het kleinste deelveld van E dat L en M bevat. Veronderstel dat L een Galoisuitbreiding is van K .

- (a) **(2 punten)** Toon aan dat LM een Galoisuitbreiding is van M .

Oplossing: Omdat L Galois is over K , is L een splitsingsveld van een separebele veelterm $f(x) \in K[x]$ over K . Dan is LM ook een splitsingsveld van $f(x)$ over M . De veelterm $f(x)$ is nog steeds separebel over M , omdat elke irreducibele factor van $f(x)$ over M een deler is van een irreducibele factor van $f(x)$ over K , en dus geen meervoudige wortels heeft wegens de separabiliteit van $f(x)$ over K .

- (b) **(2 punten)** Toon aan dat de Galoisgroep $\text{Gal}(LM/M)$ een deelgroep is van de Galoisgroep $\text{Gal}(L/K)$.

Oplossing: Voor elk automorfisme σ van LM over M geldt dat $\sigma(L) \subset L$, aangezien L wordt voortgebracht over K door de wortels van de veelterm $f(x)$, die splitst in lineaire factoren over L , en σ elke wortel van $f(x)$ afbeeldt op een wortel van $f(x)$. Omdat dit ook geldt voor σ^{-1} , is $\sigma|_L$ een automorfisme van L over K . Op deze manier bekomen we een afbeelding

$$\varphi: \text{Gal}(LM/M) \rightarrow \text{Gal}(L/K)$$

en dit is een groepsmorphisme omdat de samenstelling van automorfismen wordt gerespecteerd onder de beperking tot L . Dit groepsmorphisme is injectief: als $\sigma|_L$ de identieke afbeelding is, dan moet het vasteveld van σ zowel L als M bevatten, en dus gelijk zijn aan LM .

- (c) **(2 punten)** Toon aan dat de Galoisgroepen $\text{Gal}(LM/M)$ en $\text{Gal}(L/K)$ isomorf zijn als en slechts als $L \cap M = K$.

Oplossing: Noteer met H het beeld van φ ; deze groep is isomorf met $\text{Gal}(LM/M)$. Als H en $\text{Gal}(L/K)$ dezelfde orde hebben, dan geldt $H = \text{Gal}(L/K)$ en $L^H = K$.

Omdat elk automorfisme in H elk element van $L \cap M$ op zichzelf afbeeldt, geldt ook dat $L \cap M \subset L^H$. Hieruit volgt dat $L \cap M = K$ wanneer $\text{Gal}(LM/M)$ en $\text{Gal}(L/K)$ isomorf zijn.

Veronderstel omgekeerd dat $L \cap M = K$. Omdat L separabel is over K , kunnen we L schrijven als $L = K(\alpha)$ wegens de stelling van het primitieve element. Dan is $LM = M(\alpha)$. Noteer met $p(x)$ de minimale veelterm van α over K . We gaan bewijzen dat $p(x)$ nog steeds irreducibel is over M . Hieruit volgt dan dat $[LM:M] = \deg p(x) = [L:K]$ zodat $\text{Gal}(LM/M)$ en $\text{Gal}(L/K)$ dezelfde orde hebben en φ een isomorfisme is.

Omdat L Galois is over K , splitst de veelterm $p(x)$ in lineaire factoren over L . Hieruit volgt dat elke monische factor van $p(x)$ in $M[x]$ coëfficiënten heeft in $L \cap M = K$, want zo'n factor is een product van factoren $x - \beta$ met β een wortel van $p(x)$ in L . Dus $p(x)$ is nog steeds irreducibel over M .

- (d) **(4 punten)** We schrappen nu de veronderstelling dat L Galois is over K . Geef een voorbeeld van eindige uitbreidingsvelden L en M van $\mathbb{Q}$ in $\mathbb{C}$ zodat $L \cap M = \mathbb{Q}$ maar $[LM:M] < [L:\mathbb{Q}]$. Bewijs je antwoord.

Oplossing: Neem $L = \mathbb{Q}(\sqrt[3]{2})$ en $M = \mathbb{Q}(\sqrt[3]{2}\zeta)$ met $\zeta = \exp(2\pi i/3)$. Dit zijn allebei uitbreidingen van graad 3: de minimale veelterm van de voortbrenger is telkens gelijk aan $x^3 - 2$. De doorsnede $L \cap M$ is een veld tussen $\mathbb{Q}$ en M , en wegens de productformule moet het dus gelijk zijn aan $\mathbb{Q}$ of M . Het is niet gelijk aan M omdat L enkel reële elementen bevat, zodat $L \cap M = \mathbb{Q}$. Het veld LM is gelijk aan $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ en dit is een uitbreiding van graad 2 van M , omdat de minimale veelterm van ζ over M gelijk is aan $x^2 + x + 1$.

- (2) Zij G een eindige groep, H een deelgroep van G , en p een priemgetal. We noteren met $n_p(G)$ en $n_p(H)$ het aantal Sylow p -deelgroepen van G en H .

- (a) **(2 punten)** Zij P een Sylow p -deelgroep van G . Toon aan dat er een element g in G bestaat zodat $gPg^{-1} \cap H$ een Sylow p -deelgroep is van H .

Oplossing: Zij Q een Sylow p -deelgroep van H . Dit is een p -deelgroep van G en dus bevat in een Sylow p -deelgroep P' van G . We hebben $P' \cap H = Q$ omdat $P \cap H$ een p -deelgroep is van H die Q bevat, en Q een maximale p -deelgroep is van H . Wegens de stelling van Sylow zijn P en P' geconjugeerd: er bestaat een g in G zodat $P' = gPg^{-1}$.

- (b) **(2 punten)** Toon aan dat elke Sylow p -deelgroep van G ten hoogste één Sylow p -deelgroep van H bevat. Besluit dat $n_p(H) \leq n_p(G)$.

Oplossing: Als Q een Sylow p -deelgroep is van H en P een Sylow p -deelgroep van G die Q bevat, dan hebben we in (a) al gezien dat $Q = P \cap H$. Dus Q is uniek bepaald door P . Uit (a) volgt ook dat elke Sylow p -deelgroep van H bevat is in een Sylow p -deelgroep van G . Daarom geldt $n_p(H) \leq n_p(G)$.

- (c) **(2 punten)** Veronderstel nu dat H een normale deelgroep is van G . Toon aan dat, voor elke Sylow p -deelgroep P van G , de doorsnede $P \cap H$ een Sylow p -deelgroep is van H , en dat elke Sylow p -deelgroep van H van deze vorm is.

Oplossing: De doorsnede $P \cap H$ is een p -deelgroep van H , en dus bevat in een Sylow p -deelgroep Q van H . Zij P' een Sylow p -deelgroep van G die Q bevat. Dan geldt

$P' = gPg^{-1}$ met g in G . Omdat $gHg^{-1} = H$ volgt nu dat $Q = P' \cap H = g(P \cap H)g^{-1}$ zodat $P \cap H$ evenveel elementen heeft als Q , en dus $P \cap H = Q$. We hebben in (a) al gezien dat we elke Sylow p -deelgroep van H kunnen schrijven als $P \cap H$ met P een Sylow p -deelgroep van G .

- (d) **(4 punten)** Stel dat de orde van G gelijk is aan 24. Toon aan dat G een normale deelgroep heeft van orde 4 of 8. *Hint: kies een Sylow 2-deelgroep P in G en beschouw de actie van G op G/P door linkse translatie.*

Oplossing: De orde van P is gelijk aan 8. Als P een normale deelgroep is van G dan valt er niets meer te bewijzen. Veronderstel dus dat dit niet het geval is, en beschouw de actie van G op G/P door linkse translatie:

$$G \times (G/P), (g, hP) \mapsto ghP.$$

Deze actie komt overeen met een groepsmorphisme φ van G naar de permutatiegroep van G/P , die isomorf is met $\mathcal{S}_3$. We gaan aantonen dat φ surjectief is. De kern van φ is dus een normale deelgroep van G van orde $\#G/\#\mathcal{S}_3 = 4$.

Omdat P geen normale deelgroep is van G , bestaan er een element g in G en een element p in P zodat $g^{-1}pg \notin P$. Dan ligt g zeker niet in P , zodat P en gP twee verschillende linkse nevenklassen zijn van P in G . We kiezen een representant h voor de derde linkse nevenklasse: $G/P = \{P, gP, hP\}$. De actie van p op G/P beeldt P af op zichzelf, en $pgP \neq gP$ omdat $g^{-1}pg$ niet in P ligt. Dus $pgP = hP$, en $\varphi(p)$ is een transpositie. De actie van g op G/P beeldt P af op gP , en daarom is $\varphi(g)$ ofwel een cyclische permutatie van orde 3, ofwel een transpositie verschillend van $\varphi(p)$. Dus $\varphi(g)$ of $\varphi(pg)$ is een element van orde 3 in $\varphi(G)$, en $\varphi(G)$ bevat zowel een element van orde 2 (namelijk $\varphi(p)$) als een element van orde 3. Hieruit volgt dat $\varphi(G)$ de ganse permutatiegroep van G/P moet zijn.

- (3) We definiëren een groep G door middel van de presentatie

$$G = \langle s, t \mid s^2, t^3, (st)^3 \rangle.$$

We noteren met $\mathcal{A}_4$ de alternerende groep op 4 elementen, dit wil zeggen de groep van even permutaties van $\{1, 2, 3, 4\}$. Herinner je dat een permutatie even wordt genoemd als hij een samenstelling is van een even aantal transposities, en dat de groep $\mathcal{A}_4$ wordt voortgebracht door de verzameling cykels van lengte 3.

- (a) **(3 punten)** Construeer een surjectief groepsmorphisme

$$f: G \rightarrow \mathcal{A}_4.$$

Bewijs je antwoord.

Oplossing: We stellen $s' = (12)(34)$ en $t' = (123)$ in $\mathcal{A}_4$. Dan geldt $(s')^2 = 1$, $(t')^3 = 1$ en $(s't')^3 = 1$. Er bestaat dus een uniek groepsmorphisme $f: G \rightarrow \mathcal{A}_4$ dat s afbeeldt op s' en t op t' .

Om te bewijzen dat f surjectief is, volstaat het om aan te tonen dat het beeld van f alle cykels van lengte 3 bevat, want deze brengen de hele groep $\mathcal{A}_4$ voort. Er zijn 8 verschillende cykels van lengte 3 in $\mathcal{A}_4$, en deze worden gegeven door t' , $s't'$, $s'(t')^2$, $s't's'$ en hun inversen. Ze liggen dus allemaal in het beeld van f .

- (b) **(3 punten)** Stel $u = tst^2$. Toon aan dat $H = \{1, s, u, su\}$ een normale deelgroep is van G . Met welke bekende groep is H isomorf?

Oplossing: We tonen eerst aan dat H een deelgroep is. De verzameling H bevat het element 1 en is gesloten onder producten, want $s^2 = u^2 = (su)^2 = 1$ en $us = su$. Hij is ook gesloten onder het nemen van inversen, omdat $s^{-1} = s$, $u^{-1} = u$ en $(su)^{-1} = su$. De deelgroep H is isomorf met de Viergroep van Klein, $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$, aangezien elk element orde 1 of 2 heeft. Een expliciet isomorfisme wordt gegeven door $s \mapsto ([1]_2, [0]_2)$, $u \mapsto ([0]_2, [1]_2)$.

Nu bewijzen we dat H een normale deelgroep is in G . Omdat elk element van $G \setminus \{1\}$ een product is van factoren s en t , hoeven we enkel aan te tonen dat $ghg^{-1} \in H$ voor $g \in \{s, t\}$ en $h \in \{s, u\}$. Dit is triviaal voor $g = s$ omdat $s \in H$. We hebben ook $tst^{-1} = tst^2 = u$ en $tut^{-1} = t^2st = su$ omdat $stst = (st)^{-1} = t^2s$ in G .

- (c) **(4 punten)** Toon aan dat de orde van G gelijk is aan 12, en besluit dat f een isomorfisme is.

Oplossing: Omdat f een surjectief morfisme is naar een groep van orde 12, hoeven we enkel aan te tonen dat G ten hoogste 12 elementen bevat. Het is voldoende te bewijzen dat de quotiëntgroep G/H ten hoogste 3 elementen bevat. Wegens de universele eigenschap van de presentatie bestaat er een uniek groepsmorfisme $G \rightarrow \mathbb{Z}/3\mathbb{Z}$ dat s afbeeldt op $[0]_3$ en t op $[1]_3$. De kern van dit groepsmorfisme bevat H . Dus G/H is isomorf met een quotiënt van $\mathbb{Z}/3\mathbb{Z}$ en heeft daarom ten hoogste 3 elementen.

Totaal: 30 punten