Uitwerkingen Lichamen en Galoistheorie, 12 april 2021

Je mag alleen gebruik maken van eigen aantekeningen en van het boek of het pdf-bestand ervan. Als je voor het lezen van het pdf-bestand een computer of ander apparaat gebruikt, moet het geluid uitstaan en de wifi uitgeschakeld zijn. Het apparaat mag geen toegang hebben tot het internet. Alleen het pdf-bestand van het boek mag geopend zijn; je mag niet typen, alleen scrollen. De surveillanten mogen je scherm bekijken.

1. (**30 pt**) In deze opgave staat ζ_k steeds voor een primitieve k-de machts eenheidswortel in $\mathbb{C}$ (dus ζ_k heeft orde k in $\mathbb{C}^\times$). Bewijs de volgende beweringen:

   (a) (**4 pt**) $\sqrt{2} \in \mathbb{Q}(\zeta_8)$;

   (b) (**4 pt**) $\sqrt{3} \in \mathbb{Q}(\zeta_{12})$;

   (c) (**4 pt**) $\sqrt{5} \in \mathbb{Q}(\zeta_5)$;

   (d) (**4 pt**) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\zeta_{24})$;

   (e) (**6 pt**) als n oneven is, dan $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$;

   (f) (**8 pt**) $\sqrt{3} \notin \mathbb{Q}(\zeta_n)$ als $1 \leq n \leq 11$. (Hint: het volstaat om te bewijzen dat $\sqrt{3}$ niet in het maximale reële deellichaam $\mathbb{R} \cap \mathbb{Q}(\zeta_n)$ zit als $1 \leq n \leq 11$.)

   Uitwerking. Voor elke k geldt dat $\mathbb{Q}(\zeta_k)$ niet afhangt van welke primitieve k-de machts eenheidswortel in $\mathbb{C}$ gekozen is, want als ξ_k een andere is, dan is ξ_k een macht van ζ_k en ζ_k een macht van ξ_k.

   (a) We kunnen dus $\zeta_8 = \exp(\pi i/4) = \frac{1}{2}\sqrt{2}(1+i)$ nemen. Dan $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$.

   (b) We kunnen als hierboven redeneren met $\zeta_{12} = \exp(\pi i/6)$, dan $\sqrt{3} = \zeta_{12} + \zeta_{12}^{-1}$. We weten ook allemaal dat $\sqrt{-3} \in \mathbb{Q}(\zeta_3)$ en $\zeta_4 = \pm i$ en ζ_{12}^3 heeft orde 4 en ζ_{12}^4 heeft orde 3, dus $\sqrt{3} = \pm i\sqrt{-3}$ in $\mathbb{Q}(\zeta_{12})$.

   (c) Dit staat in Voorbeeld 1 op p. 597: $\alpha = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$, dus $\sqrt{5} \in \mathbb{Q}(\zeta_5)$.

   (d) We kunnen ζ_{24}^3 als ζ_8 nemen en ζ_{24}^2 als ζ_{12}, dus dit volgt uit (a) en (b), want $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is het kleinste lichaam in $\mathbb{C}$ dat $\sqrt{2}$ en $\sqrt{3}$ bevat.

   (e) ζ_{2n}^2 heeft orde n, dus de ene inclusie is duidelijk. Anderzijds, $(-\zeta_n)^n = (-1)^n = -1$, dus de orde van $-\zeta_n$ deelt $2n$, maar niet n. Als $-\zeta_n$ orde $2d$ heeft, met $d|n$, dan ook $\zeta_n^{2d} = 1$, dus $n|2d$, maar n is oneven, dus $n|d$. Dus $d = n$ en $-\zeta_n$ heeft orde $2n$, dus is een ζ_{2n}.

   (f) Op grond van (e) hoeven we alleen $n = 1, 3, 4, 5, 7, 8, 9, 11$ te bekijken. $n = 1$ valt direct af en $n = 3, 4$ ook want het maximale reële deellichaam is dan $\mathbb{Q}$. Voor $n = 7, 9, 11$ heeft het maximale reële deellichaam graad $3, 3, 5$ dus het bevat geen deellichaam van graad 2 over $\mathbb{Q}$. Over zijn $n = 5, 8$. In beide gevallen heeft het maximale reële deellichaam graad 2 over $\mathbb{Q}$. Maar het is $\mathbb{Q}(\sqrt{5})$ resp. $\mathbb{Q}(\sqrt{2})$, vgl. (a) en (c). We weten dat $a + b\sqrt{2}$ en $a + b\sqrt{5}$ niet kwadraat 3 hebben als $a, b \in \mathbb{Q}$, want direct volgt $ab = 0$, maar 3, $\frac{3}{2}$ en $\frac{3}{5}$ zijn geen kwadraten in $\mathbb{Q}$.

2. (**10 pt**) Laat $F = \mathbb{F}_q$ een eindig lichaam met q elementen zijn. Laat K een uitbreiding van F zijn met $[K : F] = k$ en laat L een uitbreiding van F zijn met $[L : F] = \ell$. Neem aan dat K en L bevat zijn in een uitbreiding M van F.

   Laat KL het compositum van K en L zijn. Bewijs dat

   $$[KL : F] = \text{kgv}(k, \ell)$$

(het kleinste gemene veelvoud (least common multiple)) en dat

$$[(K \cap L) : F] = \text{ggd}(k, \ell)$$

(de grootste gemene deler (greatest common divisor)).

Uitwerking. KL is een eindige uitbreiding van F in M. Voor elke eindige uitbreiding N van F van graad n geldt dat N een uniek deellichaam heeft van graad d over F voor elke deler d van n; en er zijn geen andere deellichamen. (Want F is eindig en N is Galois over F met cyclische Galoisgroep van orde n.)

Schrijf $v = \text{kgv}(k, \ell)$ en $d = \text{ggd}(k, \ell)$. Dan zijn k en ℓ delers van $[KL : F]$, dus $v|[KL : F]$. Laat V de unieke uitbreiding van graad v over F in KL zijn en D de unieke uitbreiding van graad d over F in KL. Dan bevat V zowel K als L, dus $V = KL$. En $[(K \cap L) : F]$ deelt d, dus $(K \cap L) \subseteq D$; maar ook $D \subseteq K$ en $D \subseteq L$, dus $D \subseteq K \cap L$, dus $D = K \cap L$.

3. (**40 pt**) Laat $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}, i)$.

   (a) (**5 pt**) Bewijs: K is het splijtlichaam van $f(x) = (x^3 - 2)(x^4 - 3)$ over $\mathbb{Q}$.
   Uitwerking. Omdat K zowel i als $\sqrt{3}$ bevat, bevat K ook $\sqrt{-3}$, dus een primitieve derdemachts eenheidswortel $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. Dus K bevat alle wortels van $f(x)$, dus het splijtlichaam van $f(x)$ over $\mathbb{Q}$. Maar de drie elementen die K voortbrengen zitten in het splijtlichaam, dus gelijkheid geldt.

   (b) (**5 pt**) Bewijs: $[K : \mathbb{Q}] = 24$.
   Uitwerking. De graad van $\sqrt[3]{2}$ over $\mathbb{Q}$ is 3 en de graad van $\sqrt[4]{3}$ over $\mathbb{Q}$ is 4, want $x^3 - 2$ is Eisenstein bij 2 en $x^4 - 3$ bij 3. Dus de graad van $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$ over $\mathbb{Q}$ is 12, want ten hoogste dat, maar deelbaar door 3 en 4. Dit is een lichaam bevat in $\mathbb{R}$, dus K heeft graad 24 over $\mathbb{Q}$.

   Noteer $\text{Gal}(K/\mathbb{Q})$ met G en laat ρ een primitieve derdemachts eenheidswortel zijn.

   (c) (**5 pt**) Bewijs dat G elementen α, β en γ bevat met
   $$\alpha(\sqrt[3]{2}) = \rho\sqrt[3]{2}, \qquad \beta(\sqrt[3]{2}) = \sqrt[3]{2}, \qquad \gamma(\sqrt[3]{2}) = \sqrt[3]{2},$$
   $$\alpha(\sqrt[4]{3}) = \sqrt[4]{3}, \qquad \beta(\sqrt[4]{3}) = i\sqrt[4]{3}, \qquad \gamma(\sqrt[4]{3}) = \sqrt[4]{3},$$
   $$\alpha(i) = i, \qquad \beta(i) = i, \qquad \gamma(i) = -i.$$
   Bewijs ook dat α, β en γ de groep G voortbrengen.
   Uitwerking. Voor het beeld van $\sqrt[3]{2}$ zijn er ten hoogste 3 mogelijkheden; voor dat van $\sqrt[4]{3}$ ten hoogste 4; voor dat van i ten hoogste 2. Maar G heeft orde 24, want K is Galois over $\mathbb{Q}$, omdat het een splijtlichaam is. Dus alle mogelijkheden komen voor. (Een automorfisme ligt vast door de beelden van de elementen die K voortbrengen.) Dus α, β en γ zijn elementen van G. De groep $\langle \alpha, \beta \rangle$ is van orde 12 of 24, want de orde is deelbaar door 3 en 4. Maar deze groep bevat γ niet, dus $\langle \alpha, \beta, \gamma \rangle$ heeft orde 24 en is gelijk aan G.

We 'nummeren' de wortels van $f(x)$ als volgt: $\pi_1 = \sqrt[3]{2}$, $\pi_2 = \rho\sqrt[3]{2}$, $\pi_3 = \rho^2\sqrt[3]{2}$, $\pi_4 = \sqrt[4]{3}$, $\pi_5 = i\sqrt[4]{3}$, $\pi_6 = -\sqrt[4]{3}$ en $\pi_7 = -i\sqrt[4]{3}$. Gebruik deze nummering om G als ondergroep van S_7 te zien.

   (d) (**5 pt**) Bewijs dat dan $\alpha = (123)$, $\beta = (23)(4567)$ en $\gamma = (23)(57)$.
   Uitwerking. α laat ρ invariant en is in S_7 gelijk aan (123). Bij β en γ moet je opletten: die sturen ρ naar $\rho^2 = \overline{\rho}$, want $\beta(\sqrt{3}) = -\sqrt{3}$ en $\gamma(i) = -i$ (terwijl $\beta(i) = i$ en $\gamma(\sqrt{3}) = \sqrt{3}$). Dus op de eerste drie wortels geven β en γ de transpositie (23). Op de laatste vier geven ze (4567) resp. (57).

(e) (**5 pt**) Bewijs dat de discriminant van $f(x)$ een kwadraat is in $\mathbb{Q}$.

Uitwerking. De drie voortbrengers van G geven *even* elementen van S_7 (zie (d)), dus G is bevat in A_7. Dit betekent dat de discriminant van $f(x)$ een kwadraat is in $\mathbb{Q}$ (in feite in $\mathbb{Z}$).

(f) (**5 pt**) Bewijs dat G een unieke normale ondergroep van orde 3 bevat. Wat is het bijbehorende tussenlichaam?

Uitwerking. $\langle\alpha\rangle$ is een groep van orde 3, dus een 3-Sylow-ondergroep van G. Maar

$$\beta\alpha\beta^{-1} = (132) = \alpha^{-1} = \gamma\alpha\gamma^{-1},$$

dus deze ondergroep is normaal. Alle 3-Sylow-ondergroepen zijn geconjugeerd met elkaar, dus er is precies één. Het bijbehorende tussenlichaam is van graad 8 over $\mathbb{Q}$ en Galois over $\mathbb{Q}$. Het bevat in elk geval $\sqrt[4]{3}$ en i, maar deze twee brengen een lichaam van graad 8 voort, dus het bijbehorende tussenlichaam is $\mathbb{Q}(\sqrt[4]{3}, i)$ (het splijtlichaam van $x^4 - 3$ over $\mathbb{Q}$).

(g) (**5 pt**) Bewijs dat G een unieke normale ondergroep van orde 4 bevat. Wat is het bijbehorende tussenlichaam?

Uitwerking. (Het lastigste onderdeel van deze opgave.) Kennelijk is er een unieke normale ondergroep van orde 4. Kennelijk is er dan ook een uniek tussenlichaam van graad 6 over $\mathbb{Q}$ dat Galois is over $\mathbb{Q}$. Dat is makkelijk te vinden: het splijtlichaam van $x^3 - 2$ over $\mathbb{Q}$, dus $\mathbb{Q}(\sqrt[3]{2}, \rho)$. Omgekeerd kunnen we dan in elk geval een normale ondergroep van orde 4 vinden: β en γ laten $\sqrt[3]{2}$ invariant, maar ρ niet; maar β^2 en $\beta\gamma$ laten ρ wel invariant. Dit zijn de elementen (46)(57) en (45)(67) en de ze brengen de normale viergroep van Klein in de S_4 op $\{4, 5, 6, 7\}$ voort. Deze groep hoort bij $\mathbb{Q}(\sqrt[3]{2}, \rho)$ en is dus normaal in G (wat ook rechtstreeks is in te zien). Ten slotte de uniciteit: een normale ondergroep van orde 4 kan aan de S_3-kant (permutaties van $\{1, 2, 3\}$) geen transpositie bevatten, want conjugatie met α levert dan een andere transpositie in S_3 op; samen brengen ze S_3 voort. Merk op dat β en γ aan de S_4-kant een 2-Sylow-ondergroep H (isomorf met D_8) voortbrengen, want (4567) heeft orde 4, (57) orde 2, en $\gamma\beta\gamma^{-1}$ geeft daar (4765), de inverse van (4567). Dus G is bevat in $S_3 \times H$ (van orde 48) en is gelijk aan de *even* ondergroep van die groep. Een normale ondergroep van G van orde 4 is dus bevat in H en in A_4, dus in $A_4 \cap H$; dit is de al genoemde groep $\langle\beta^2, \beta\gamma\rangle$ van orde 4.

(h) (**5 pt**) Bepaal de tussenlichamen van $K/\mathbb{Q}$ die graad 2 over $\mathbb{Q}$ hebben en bepaal de bijbehorende ondergroepen van G.

Uitwerking. Drie zulke tussenlichamen zijn $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ en $\mathbb{Q}(\sqrt{-3})$. We zoeken ondergroepen van orde 12 (die dus normaal zijn); die moeten α bevatten. De tussenlichamen zijn dus bevat in $\mathbb{Q}(i, \sqrt[4]{3})$. Dat lichaam is Galois over $\mathbb{Q}$ met groep D_8, voortgebracht door $\delta = (4567)$ en $\epsilon = (57)$ als we dezelfde nummering gebruiken. We weten of zien snel in dat D_8 drie ondergroepen van orde 4 bevat: $\langle\delta\rangle$, $\langle\delta^2, \epsilon\rangle$ en $\langle\delta^2, \delta\epsilon\rangle$. Dus G heeft drie ondergroepen van orde 12, namelijk $\langle\alpha, \beta\rangle$, $\langle\alpha, \beta^2, \gamma\rangle$ en $\langle\alpha, \beta^2, \beta\gamma\rangle$. Die horen achtereenvolgens bij $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ en $\mathbb{Q}(\sqrt{-3})$.

4. (**10 pt**) Laat $f(x)$ een monisch irreducibel polynoom in $\mathbb{Z}[x]$ zijn.

(a) (**5 pt**) Leg uit waarom er oneindig veel priemgetallen p bestaan zó dat $f(x)$ modulo p volledig splitst in $\mathbb{F}_p[x]$ (d.w.z., een product is van eerstegraadspolynomen in $\mathbb{F}_p[x]$).

Uitwerking. Neem aan $f(x)$ heeft graad n. Laat G de Galoisgroep van $f(x)$ zijn (dus die van het splijtlichaam van $f(x)$ over $\mathbb{Q}$). We kunnen G als ondergroep van S_n zien. We weten uit §14.8: als p niet de discriminant D van $f(x)$ deelt (er zijn maar eindig veel p die D delen, want $f(x)$ is separabel (want irreducibel over $\mathbb{Q}$), dus $D \neq 0$ in $\mathbb{Z}$), en

als $f(x)$ mod p irreducibele factoren (in $\mathbb{F}_p[x]$) van graden n_1 tot en met n_k heeft (met $n_1 + \cdots + n_k = n$), dan bevat G een element met disjunkte-cykel-decompositie van type $(n_1, n_2, \ldots, n_k)$. En omgekeerd: als het aantal elementen in G van dit type gelijk is aan b, dan is de dichtheid van de priemen p met deze decompositie gelijk aan $b/|G|$, dus positief, dus zijn er oneindig veel zulke priemen. We zoeken type $(1, 1, \ldots, 1)$; alleen het eenheidselement van G heeft dit type. Er zijn dus oneindig veel priemen met het gewenste reductietype en ze hebben dichtheid $1/|G|$.

(b) (**5 pt**) Geef aan hoe dit tot een theoretische (maar niet noodzakelijk praktische) methode leidt om de **orde** van de Galoisgroep van $f(x)$ te **bepalen**.

Uitwerking. Dit is nu ook duidelijk: als we de dichtheid van deze priemen kunnen bepalen, vinden we $1/|G|$, dus weten we dan $|G|$. Omdat bewezen is dat de gezochte priemen deze dichtheid hebben, geldt dat de limiet

$$\lim_{N\to\infty} \frac{\#\{p \le N \text{ met dit type}\}}{\#\{p \le N\}}$$

gelijk is aan $1/|G|$. Dus voor elke $\epsilon > 0$ bestaat er een $M > 0$ zodat voor alle $N > M$ het quotiënt minder dan ϵ afwijkt van $1/|G|$. Neem $\epsilon = 1/(2n!)$. Neem $N > M$ en bereken het quotiënt Q; het zit in het open interval

$$(\frac{n!/|G|}{n!} - \frac{1}{2n!}, \frac{n!/|G|}{n!} + \frac{1}{2n!}).$$

Anderzijds is de dichtheid van de vorm $a/n!$ voor een $a \in \mathbb{N}$ en zit in het open interval van lengte $1/n!$ met middelpunt Q. Dan $a = n!/|G|$, dus $|G| = n!/a$.