Uitwerkingen Lichamen en Galoistheorie, 10 november 2022

1. (**15 pt**) Als K/F een lichaamsuitbreiding is, definiëren we een echt tussenlichaam E van K/F als een tussenlichaam ongelijk aan F en ongelijk aan K.

   Hieronder staat ζ_n voor een primitieve n-de machts eenheidswortel.

   (a) Hoeveel echte tussenlichamen heeft $\mathbb{Q}(\zeta_5)/\mathbb{Q}$?

   (b) Hoeveel echte tussenlichamen heeft $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$?

   (c) Hoeveel echte tussenlichamen heeft $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$?

   Uitwerking. We weten dat $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ een Galoisuitbreiding is met groep $G = (\mathbb{Z}/n\mathbb{Z})^\times$, de eenhedengroep van $\mathbb{Z}/n\mathbb{Z}$, met orde $\phi(n)$. De Hoofdstelling zegt dat de tussenlichamen van $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ precies corresponderen met de ondergroepen van G (en de echte tussenlichamen met de echte ondergroepen (ongelijk $\{1\}$ en G)).

   (a) $\mathbb{Z}/5\mathbb{Z}$ is een eindig lichaam (want 5 is priem), dus $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclisch, van orde 4. De enige echte ondergroep is van orde 2. Er is dus precies één echt tussenlichaam.

   (b) $\mathbb{Z}/13\mathbb{Z}$ is een eindig lichaam (want 13 is priem), dus $(\mathbb{Z}/13\mathbb{Z})^\times$ is cyclisch, van orde 12. De echte ondergroepen van een cyclische groep van orde k corresponderen precies met de echte delers van k. Voor $k = 12$ zijn dit 2, 3, 4 en 6. Er zijn dus 4 echte tussenlichamen.

   (c) $\mathbb{Z}/15\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, daarom $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$, en dit is isomorf met $Z_2 \times Z_4$, het produkt van een cyclische groep van orde 2 en een van orde 4. Hoe vind je de (echte) ondergroepen in deze groep? Ze hebben orde 2 of orde 4 (de echte delers van 8). Die van orde 2 worden voortgebracht door een element van orde 2. De elementen van $Z_2 \times Z_4$ schrijf je als (a, b), waar $a \in \mathbb{Z}/2\mathbb{Z}$ en $b \in \mathbb{Z}/4\mathbb{Z}$. Dan is $(0, 0)$ van orde 1; $(1, 0)$, $(0, 2)$ en $(1, 2)$ hebben orde 2, en $(0, 1)$, $(0, 3)$, $(1, 1)$ en $(1, 3)$ hebben orde 4. Er zijn dus 3 elementen van orde 2, dus 3 ondergroepen van orde 2. Er zijn 4 elementen van orde 4, die geven 2(!) cyclische ondergroepen van orde 4. Tenslotte is er een ondergroep die bestaat uit het eenheidselement en de 3 elementen van orde 2; die is isomorf met $Z_2 \times Z_2$. Er zijn dus 6 echte ondergroepen, dus 6 echte tussenlichamen.

2. (**24 pt**) Laat $\mathbb{F}_4$ een eindig lichaam zijn met 4 elementen. Laat G de groep zijn van matrices van de vorm

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

   met $a \in \mathbb{F}_4^\times$ en $b \in \mathbb{F}_4$ (de groepsbewerking is vermenigvuldiging van matrices).

   (a) Hoeveel elementen heeft G ?

   (b) Bepaal de ordes van de (niet-triviale) Sylow-ondergroepen van G.

   (c) Definieer $\phi\colon G \to \mathbb{F}_4^\times$ door

$$\phi(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}) = a.$$

   Bewijs dat ϕ een groepshomomorfisme is en dat de kern van ϕ een Sylow-ondergroep van G is.

   (d) Bepaal het aantal Sylow-2-ondergroepen van G.

   (e) Bewijs dat de diagonale matrices in G een Sylow-ondergroep van G vormen die niet normaal is.

   (f) Bepaal het aantal Sylow-3-ondergroepen van G.

Uitwerking.

(a) Voor a zijn er 3 mogelijkheden en voor b zijn er 4, dus G heeft $3 \times 4 = 12$ elementen.

(b) $12 = 2^2 \cdot 3$, dus de Sylow-2-ondergroepen hebben orde $2^2 = 4$ en de Sylow-3-ondergroepen hebben orde 3. Andere niet-triviale Sylow-ondergroepen van G zijn er niet.

(c) Het produkt van $\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}$ en $\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} a_1a_2 & a_1b_2 + b_1 \\ 0 & 1 \end{pmatrix}$. Linksboven staat dus a_1a_2, dus ϕ is een groepshomomorfisme. Het is duidelijk dat ϕ surjectief is, dus het beeld van ϕ heeft orde 3. Dan heeft de kern van ϕ orde $12/3 = 4$. Dit is dus een Sylow-2-ondergroep van G.

(d) De kern van een homomorfisme is een normale ondergroep. Dus de kern van ϕ is een normale Sylow-2-ondergroep van G. Alle Sylow-2-ondergroepen van G zijn met elkaar geconjugeerd. Maar als er een normale ondergroep bij zit, is dat noodgedwongen de enige. Antwoord: 1.

(e) De diagonale matrices hebben $b = 0$; er zijn dus 3 diagonale matrices. Die vormen een ondergroep, van orde 3. Een Sylow-3-ondergroep dus. Maar het produkt van $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}$, en het produkt van die matrix met $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} a & a+1 \\ 0 & 1 \end{pmatrix}$. Dit is de geconjugeerde van $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ met $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, want deze laatste matrix is gelijk aan zijn eigen inverse. Maar als $a \neq 1$ (dit komt voor) is de geconjugeerde géén diagonaalmatrix (want $a+1 \neq 0$ dan). Dus de ondergroep van diagonaalmatrices is geen normale ondergroep van G.

(f) Het aantal is niet 1 (want dan zou die groep wel normaal zijn). Het is congruent met 1 modulo 3, en het deelt $4 = 12/3$. Het is dus 4.

3. (**20 pt**) Voor elk lichaam F kan $x^3 - 2$ als element van $F[x]$ beschouwd worden. Hieronder komen vier vragen. Geef niet alleen de antwoorden, maar ook een *korte* motivatie. (En let goed op!)

(a) Wat is de graad van het splijtlichaam van $x^3 - 2$ over $\mathbb{Q}$?

(b) De derdemachten in $\mathbb{F}_7$ zijn 0, 1 en -1. Wat is de graad van het splijtlichaam van $x^3 - 2$ over $\mathbb{F}_7$?

(c) De derdemachten in $\mathbb{F}_5$ zijn 0, 1, 2, 3 en 4. Wat is de graad van het splijtlichaam van $x^3 - 2$ over $\mathbb{F}_5$?

(d) 4 is een wortel van $x^3 - 2$ in $\mathbb{F}_{31}$. Wat is de graad van het splijtlichaam van $x^3 - 2$ over $\mathbb{F}_{31}$?

Uitwerking.

(a) Het splijtlichaam van $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, zoals bekend. Dit heeft graad 6 over $\mathbb{Q}$ (zoals ook bekend), want $\sqrt[3]{2}$ heeft graad 3 over $\mathbb{Q}$ en ζ_3 heeft graad 2 over $\mathbb{Q}$. (Deze graden zijn relatief priem en hun produkt is 6.)

(b) (Inderdaad, $2^3 = 8 = 1$, $3^3 = 27 = -1$, enz. Meer theoretisch gezien: $\mathbb{F}_7^\times$ is cyclisch van orde 6; de derdemacht van een voortbrenger heeft dan orde 2 en is gelijk aan -1, enz.) Gegeven is dus dat 2 géén derdemacht is in $\mathbb{F}_7$. Dan heeft $x^3 - 2$ geen wortels in $\mathbb{F}_7$. Een derdegraads polynoom zonder wortels over een lichaam is irreducibel. Dus $x^3 - 2$ is irreducibel in $\mathbb{F}_7[x]$. Het toevoegen van een wortel levert dan een uitbreiding van graad 3. Maar $\mathbb{F}_7$ bevat al 3 derdemachts eenheidswortels, namelijk 1, 2 en 4. Dus de overige

wortels van x^3-2 zitten ook in die uitbreiding van graad 3. Die is dus het splijtlichaam van x^3-2 over $\mathbb{F}_7$. (Alternatief: elke eindige uitbreiding van een eindig lichaam is Galois, dus met één wortel van een irreducibel polynoom zitten alle wortels erin.) Antwoord: 3.

(c) x^3-2 heeft kennelijk één wortel in $\mathbb{F}_5$, want één derdemacht is gelijk aan 2. Om de overige wortels te vinden hebben we dan nog een uitbreiding van graad 2 nodig. Antwoord: 2.

(d) 4 is inderdaad een wortel. En $\mathbb{F}_{31}^\times$ is cyclisch van orde 30. De 10e macht van een voortbrenger heeft dan orde 3 en is een primitieve derdemachts eenheidswortel in $\mathbb{F}_{31}$. Dus met één wortel van x^3-2 (namelijk 4) krijgen we alle wortels (de andere twee zijn 7 en 20, maar dit terzijde). Het splijtlichaam is dus $\mathbb{F}_{31}$ zelf. Antwoord: 1.

4. (**31 pt**)

(a) Laat zien dat elke lichaamsuitbreiding L/F van graad 2 normaal is.

(b) Laat $\alpha = (1+i)\sqrt[4]{7}$. Bereken α^2 en laat zien dat $\mathbb{Q}(\alpha)$ een normale uitbreiding is van $\mathbb{Q}(i\sqrt{7})$.

(c) Laat zien dat $\mathbb{Q}(\alpha)$ géén normale uitbreiding is van $\mathbb{Q}$.

(d) Bepaal de normale afsluiting K van $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Leg uit waarom dit een Galoisuitbreiding van $\mathbb{Q}$ is.

(e) Bepaal $G := \mathrm{Gal}(K/\mathbb{Q})$ en $H := \mathrm{Gal}(K/\mathbb{Q}(i\sqrt{7}))$.

(f) Welke ondergroep van G hoort bij $\mathbb{Q}(\alpha)$?

Uitwerking.

(a) $L = F(\alpha)$ voor een $\alpha \notin F$. Het minimumpolynoom van α over F is dan $x^2+ax+b \in F[x]$, voor zekere a en b in F. De twee wortels hebben dan som $-a$, dus $\beta = -a-\alpha$ is de andere wortel, die zit ook in L. Dus L is het splijtlichaam van x^2+ax+b over F, dus L is normaal over F.

(b) $\alpha^2 = (1+i)^2\sqrt{7} = 2i\sqrt{7}$. Dit zit in $\mathbb{Q}(i\sqrt{7})$ en $\mathbb{Q}(\alpha)$ is dus een uitbreiding van $\mathbb{Q}(i\sqrt{7})$ van graad ten hoogste 2. Het is dus zeker een normale uitbreiding.

(c) $\alpha^4 = -28$, dus α is een wortel van x^4+28. Dit polynoom is monisch en Eisenstein bij 7 (niet bij 2 !), dus irreducibel. Dus $\mathbb{Q}(\alpha)$ heeft graad 4 over $\mathbb{Q}$. Als dit een normale uitbreiding zou zijn, moeten alle wortels van x^4+28 in $\mathbb{Q}(\alpha)$ zitten; dan volgt $i \in \mathbb{Q}(\alpha)$. Maar dan zou $\beta = \sqrt[4]{7}$ ook in $\mathbb{Q}(\alpha)$ zitten. Maar $\mathbb{Q}(\beta)$ is ook van graad 4 over $\mathbb{Q}$ (polynoom x^4-7) en is bevat in $\mathbb{R}$; dit levert een tegenspraak, want $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ zou dan in $\mathbb{R}$ zitten. Dus het is géén normale uitbreiding van $\mathbb{Q}$.

(d) Die normale afsluiting krijgen we dan door i erbij te stoppen: $K = \mathbb{Q}(\alpha, i)$. Dit is een uitbreiding van $\mathbb{Q}(\alpha)$ van graad 2, dus K heeft graad 8 over $\mathbb{Q}$. Het is het splijtlichaam van x^4+28 over $\mathbb{Q}$, dus Galois over $\mathbb{Q}$.

(e) G heeft orde 8 en H heeft orde 4. Schrijf K als $\mathbb{Q}(\beta, i)$, dan zijn er 4 mogelijkheden voor het beeld van β en 2 voor het beeld van i. En alle 8 mogelijkheden komen voor. Definieer σ door $\sigma(\beta) = i\beta$ en $\sigma(i) = i$. Definieer τ door $\tau(\beta) = \beta$ en $\tau(i) = -i$. Dan zitten σ en τ in G en σ heeft orde 4 en τ heeft orde 2. En τ zit niet in $\langle\sigma\rangle$, dus σ en τ brengen G voort. We zien dat $\tau\sigma\tau = \tau\sigma\tau^{-1} = \sigma^3$; er volgt dat G isomorf is met D_8, de dihedrale groep van orde 8. De elementen van G zijn 1, σ, σ^2, σ^3, τ, $\sigma\tau$, $\sigma^2\tau$ en $\sigma^3\tau$.

Welke elementen zitten in H? De elementen die $i\sqrt{7}$ invariant laten. Dit is $i\beta^2$. Dus σ en τ zitten niet in H, maar σ^2 en $\sigma\tau$ wel, en $\sigma^3\tau$ en 1 dus ook. We zien dat H isomorf is met $Z_2 \times Z_2$.

(f) $\mathbb{Q}(\alpha)$ bevat $\mathbb{Q}(i\sqrt{7})$, dus de bijbehorende ondergroep van G is een ondergroep van H, van orde 2. Drie mogelijkheden. Merk op $\sigma(\alpha) = (1+i)i\beta = i\alpha$, dus $\sigma^2(\alpha) = \sigma(i\alpha) = -\alpha$, dus σ^2 is het niet. Verder, $\tau(\alpha) = (1-i)\beta = -i\alpha$. Dus $\sigma\tau(\alpha) = \sigma(-i\alpha) = (-i)i\alpha = \alpha$, dus $\sigma\tau$ is het gezochte element en $\langle\sigma\tau\rangle$, van orde 2, is de gezochte ondergroep.