UITWERKINGEN

1. Beantwoord de volgende korte vragen en geef een motivatie:

   (a) (5 pt) Waar of niet waar: Stel L/K is een Galoisuitbreiding en M een tussenlichaam, dat wil zeggen $K \subset M \subset L$. Dan is L/M een Galoisuitbreiding.
   Antwoord: Waar. Uit L/K Galois volgt dat L splijtlichaam is van een separabel polynoom $f \in K[X]$. Omdat ook geldt dat $f \in M[X]$ is L/M ook splijtlichaam van een separabel polynoom en dus Galois.

   (b) (5 pt) Waar of niet waar: Stel L/K is een Galoisuitbreiding en M een tussenlichaam, dus $K \subset M \subset L$. Dan is M/K een Galoisuitbreiding.
   Antwoord: Niet waar. Neem als voorbeeld $K = \mathbb{Q}, M = \mathbb{Q}(\sqrt[3]{2})$ en L splijtlichaam van $X^3 - 2$. Omdat M maar 1 nulpunt van $X^3 - 2$ bevat is M/K niet normaal in dit geval en dus niet Galois.

   (c) (4+4 pt) Welk van de volgende groepen kunnen voorkomen als Galoisgroep van het splijtlichaam van een vierde graads polynoom:

      i. $C(2) \times C(2) \times C(2)$ ($C(2)$ is de cyclische groep van 2 elementen).

      ii. De diedergroep van orde 8.

   Antwoord: De Galoisgroep G van het splijtlichaam van een vierde graadspolynoom is een ondergroep van S_4 omdat G de nulpunten van het polynoom permuteert.
   De groep $C(2)^3$ is geen ondergroep van S_4. Kijk naar de elementen van orde 2 in deze groepen. De eerste bevat er 7 en ze commuteren. De groep S_4 bevat de 6 2-cykels en de 3 producten van disjuncte 2-cykels. De groep $C(2)^3$ moet dus minstens $7 - 3 = 4$ 2-cykels bevatten. Omdat ze commuteren zouden ze disjunct moeten zijn. Dit is niet mogelijk, S_4 bevat geen 4 paarswijs disjuncte 2-cykels.
   De diedergroep D_4, ofwel de groep van het vierkant is een ondergroep van S_4 omdat deze de 4 hoekpunten van een vierkant permuteert. Een voorkomend geval is het splijtlichaam van $X^4 - 2$, dat gelijk is aan $\mathbb{Q}(\sqrt[4]{2}, i)$. De twee isomorfismen σ, τ gegeven door $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma(i) = i$ en $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$, $\tau(i) = -i$ voldoen aan de relaties $\tau^2 = \sigma^4 = id$ en $\sigma\tau = \tau\sigma^{-1}$. Precies de definierende relatie van D_4.

   (d) (5 pt) Bewijs dat $x^3 - x - 1$ irreducibel in $\mathbb{Q}[x]$ is.
   Antwoord: Stel $x^3 - x - 1$ is reducibel. Dan is hij ook reducibel in $\mathbb{Z}[x]$ met een ontbinding $x^3 - x - 1 = (x^2 + ax + b)(x - c)$ met $a, b, c \in \mathbb{Z}$. Hieruit volgt $ac = 1$ en dus $c = \pm 1$. Controleert dat noch 1, noch -1 een nulpunt is. Dus irreducibel.

   (e) (11 pt) Zij α een nulpunt van $x^3 - x - 1$. Bepaal het inverse element van $\alpha + 2$ in $\mathbb{Q}(\alpha)$.
   Antwoord: Los op: $(x+2)(ax^2+bx+c) \equiv 1 (\mathrm{mod}\, x^3-x-1)$ in $a, b, c \in \mathbb{Q}$.
   Product uitwerken: $(ax^2+bx+c)(x+2) = ax^3+(2a+b)x^2+(2b+c)x+2c$
   Modulo $x^3 - x - 1$: $(2a+b)x^2 + (a+2b+c)x + 2c + a$. Dit gelijk stellen aan 1 geeft

$$2a + b = 0, \quad a + 2b + c = 0, \quad 2c + a = 1.$$

Oplossen geeft $a = 1/7, b = -2/7, c = 3/7$. Dus $(x^2 - 2x + 3)/7$.

(f) (8 pt) Bepaal het aantal tussenlichamen van de uitbreiding $\mathbb{F}_{3^{10}}/\mathbb{F}_3$ (inclusief $\mathbb{F}_{3^{10}}$ en $\mathbb{F}_3$ zelf).
Antwoord: Elk deelichaam van $\mathbb{F}_{3^{10}}$ is tevens tussenlichaam. $\mathbb{F}_{3^n}$ is deellichaam van $\mathbb{F}_{3^{10}}$ precies dan als n een deler is van 10. Dus $n = 1, 2, 5, 10$ en we hebben 4 tussenlichamen.

(g) (8 pt) Zij $f(x) \in \mathbb{F}_p[x]$ een irreducibel polynoom van graad r. Zij α een nulpunt van f en $K = \mathbb{F}_p(\alpha)$. Zij $\phi : K \to K$ het automorfisme gegeven door $\phi : \beta \mapsto \beta^p$ voor alle $\beta \in \mathbb{F}_p(\alpha)$. Bewijs dat de verzameling nulpunten van f gegeven wordt door $\alpha, \phi(\alpha), \ldots, \phi^{r-1}(\alpha)$.
Antwoord: Het lichaam K is isomorf met $\mathbb{F}_{p^r}$. Er geldt $0 = \phi(f(\alpha) = f(\phi(\alpha))$ en dus is $\phi(\alpha)$ ook nulpunt van f. Op dezelfde manier is $\phi^k(\alpha)$ nulpunt van f voor elke k. Om onze bewering te bewijzen moeten we aantonen dat $\alpha, \phi(\alpha), \ldots, \phi^{r-1}(\alpha)$ verschillend zijn. Dan hebben we alle r nulpunten van f te pakken. Stel dat $\phi^(\alpha) = \phi^j(\alpha)$ voor $0 \le i < j < r$. Dan geldt $\phi^{j-i}(\alpha) = \alpha$. En omdat α voortbrenger is van K geldt ook $\phi^{j-i}(\beta) = \beta$ voor alle $\beta \in K$. Dus alle elementen van K zijn nulpunt van $X^{j-i} - 1$. Gevolg: $p^r = |K| \le p^{j-i} \le p^{r-1}$. Tegenspraak. Dus alle $\phi^i(\alpha)$ met $i = 0, 1 \ldots, r-1$ zijn verschillend.

2. NB: Als je in de volgende vragen een onderdeel gemist heb dan kun je het resultaat ervan toch gebruiken in de daaropvolgende onderdelen.

We bekijken de uitbreiding $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ van $\mathbb{Q}$.

(a) (5 pt) Bewijs dat $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$.
Antwoord: Omdat $\sqrt{3}$ irrationaal geldt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Stel dat $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$. Dan zijn er $a, b \in \mathbb{Q}$ zó dat $\sqrt{5} = a + b\sqrt{3}$. Kwadrateren geeft $5 = a^2 + 3b^2 + 2ab\sqrt{3}$. Hieruit volgt dat $ab = 0$ en $a^2 + 3b^2 = 5$. Stel $a = 0$, dan $3b^2 = 5 \Rightarrow b = \sqrt{5/3}$ in tegenspraak met $b \in \mathbb{Q}$. Op dezelfde manier geeft $b = 0$ aanleiding tot $a^2 = 5 \Rightarrow a = \sqrt{5}$ in tegenspraak met $a \in \mathbb{Q}$. Conclusie, $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$ en heeft dus graad 2 over $\mathbb{Q}(\sqrt{3})$. De torenstelling voor graden levert dus $[\mathbb{Q}(\sqrt{3}, \mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

(b) (5 pt) Bewijs dat $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ een Galois uitbreiding is en laat zien dat er elementen $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ zijn met de eigenschap

$$\sigma(\sqrt{3}) = \sqrt{3},\ \sigma(\sqrt{5}) = -\sqrt{5}, \quad \tau(\sqrt{3}) = -\sqrt{3},\ \tau(\sqrt{5}) = \sqrt{5}.$$

Antwoord: Het element $\sqrt{3} + \sqrt{5}$ is een voortbrenger van ons lichaam en voldoet aan vierde graadsvergelijking. De Galoisgroep heeft orde vier. Voor een willekeurig element ρ van de Galoisgroep moet gelden dat $\rho(\sqrt{3}) = \pm\sqrt{3}$ en $\rho(\sqrt{5}) = \pm\sqrt{5}$. Dit zijn vier mogelijkheden, en dus komt iedere mogelijkheid aan bod in de Galoisgroep. In het bijzonder komen de elementen σ, τ voor.

(c) (5 pt) Met welke groep van vier elementen is $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ isomorf?
Antwoord: De elementen σ, τ hebben beide orde 2. De enige groepen van orde 4 zijn de cyclische $C(4)$ en de Viergroep van Klein $C(2) \times C(2)$. Het aantal elementen van orde 2 in $C(4)$ is 1. Dus hebben we de Viergroep.

Stel $\alpha = \sqrt{(2-\sqrt{3})(5-2\sqrt{5})}$. We gaan allereerst laten zien dat α graad 8 over $\mathbb{Q}$ heeft.

(d) (5+5 pt) Zij $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})$ als boven en stel dat $\alpha \in \mathbb{Q}(\sqrt{5},\sqrt{3})$. We gaan een tegenspraak afleiden.

i. Laat zien dat $\sigma(\alpha) = \epsilon\sqrt{5}(2-\sqrt{3})/\alpha$ met $\epsilon \in \{-1,1\}$ (Hint: bepaal $\sigma(\alpha^2)$).
Antwoord: Er geldt:

$$\sigma(\alpha^2) = \sigma((2-\sqrt{3})(5-2\sqrt{5})) = (2-\sqrt{3})(5+2\sqrt{5}) = \frac{5(2-\sqrt{3})^2}{(2-\sqrt{3})(5-2\sqrt{5})} = \frac{5(2-\sqrt{3})^2}{\alpha^2}.$$

Ons resultaat volgt door worteltrekking.

ii. Laat vervolgens zien dat $\sigma^2(\alpha) = -\alpha$.
Antwoord: Gebruikmakend van het resultaat van het vorige onderdeel leiden we af,

$$\sigma^2(\alpha) = \epsilon\sigma\left(\frac{\sqrt{5}(2-\sqrt{3})}{\alpha}\right) = \epsilon^2\frac{-\sqrt{5}(2-\sqrt{3})}{\sqrt{5}(2-\sqrt{3})}\alpha = -\alpha.$$

(e) (5 pt) Laat zien dat uit voorgaand onderdeel volgt dat $\alpha \notin \mathbb{Q}(\sqrt{3},\sqrt{5})$ en concludeer dat α graad 8 over $\mathbb{Q}$ heeft.
Antwoord: Stel dat $\alpha \in \mathbb{Q}(\sqrt{3},\sqrt{5})$. Dan zou moeten gelden dat $\sigma^2(\alpha) = \alpha$. Dit is in tegenspraak met voorgaande onderdeel. Dus heeft α graad 2 over $\mathbb{Q}(\sqrt{3},\sqrt{5})$. Verder is α^2 voortbrenger van $\mathbb{Q}(\sqrt{3},\sqrt{5})$. Dus,

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^2)][\mathbb{Q}(\alpha^2):\mathbb{Q}] = 2 \times [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = 8.$$

(f) (5 pt) Laat zien dat de nulpunten van het minimaalpolynoom van α geschreven kunnen worden als

$$\pm\alpha,\ \pm\sqrt{5}/\alpha,\ \pm\sqrt{5}(2-\sqrt{3})/\alpha,\ \pm(5-2\sqrt{5})/\alpha.$$

(Hint: ze komen van $\pm\sqrt{(2\pm\sqrt{3})(5\pm2\sqrt{5})}$).
Antwoord: We maken herhaald gebruik van $1/(2-\sqrt{3}) = 2+\sqrt{3}$ en $5/(5-2\sqrt{5} = 5+2\sqrt{5}$.

(g) (5+10 pt) Laat zien dat $\mathbb{Q}(\alpha)$ een Galois uitbreiding van $\mathbb{Q}$ is en bepaal de Galoisgroep.
Antwoord: Het lichaam $\mathbb{Q}(\alpha)$ bevat $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Uit deze opmerking en voorgaand onderdeel volgt dat $\mathbb{Q}(\alpha)$ naast α ook de andere nulpunten van het minimaalpolynoom bevat. Dus is $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois.
Een element uit de Galoisgroep wordt vastgelegd door zijn beeld van α. Elk beeld komt in aanmerking. Kies twee elementen r, s in de Galoisgroep met de eigenschap

$$r(\alpha) = (5-2\sqrt{5})/\alpha, \quad s(\alpha) = \sqrt{5}/\alpha.$$

Kwadrateren we de eerste:

$$r((2-\sqrt{3})(5-2\sqrt{5})) = \frac{5-2\sqrt{5})^2}{(2-\sqrt{3})(5-2\sqrt{5})} = (2+\sqrt{3}(5-2\sqrt{5}).$$

Dus $r(\sqrt{5}) = \sqrt{5}$ en $r(\sqrt{3}) = -\sqrt{3}$. Kwadrateren van de tweede,

$$s((2-\sqrt{3})(5-2\sqrt{5})) = s(\alpha^2) = 5/\alpha^2 = \frac{5}{(2-\sqrt{3})(5-2\sqrt{5})} = (2+\sqrt{3})(5+2\sqrt{5}).$$

Dus $s(\sqrt{3}) = -\sqrt{3}, s(\sqrt{5}) = -\sqrt{5}$. Hiermee gewapend vinden we

$$r^2(\alpha) = r((5-2\sqrt{5})/\alpha) = \alpha$$

en

$$s^2(\alpha) = s(\sqrt{5}/\alpha) = -\alpha.$$

Hieruit volgt dat s orde vier heeft. Verder,

$$rs(\alpha) = r(\sqrt{5}/\alpha) = \frac{\sqrt{5}}{5-2\sqrt{5}}\alpha$$

en

$$sr(\alpha) = s((5-2\sqrt{5})/\alpha) = \frac{5+2\sqrt{5}}{\sqrt{5}}\alpha.$$

Merk op dat $\sqrt{5}/(5-2\sqrt{5}) = (5+2\sqrt{5})/\sqrt{5}$. De elementen r, s commuteren dus. Gevolg: de Galoisgroep is isomorf met $C(2) \times C(4)$.