UITWERKINGEN

1. Zijn de volgende uitspraken goed of fout? Verklaar je antwoord.

   (a) (5 pt) 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: Ja, een Galoisuitbreiding L/K is splijtlichaam van een separabel polynoom $f \in K[X]$. Omdat tevens $f \in M[X]$, is L ook Galois over M.

   (b) (5 pt) Stel L/K is een Galoisuitbreiding en M een tussenlichaam, dus $K \subset M \subset L$. Dan is M/K een Galoisuitbreiding.
   Antwoord: Nee, tegenvoorbeeld, splijtlichaam L van X^3-2 over $K = \mathbb{Q}$. Deze bevat $M = \mathbb{Q}(\sqrt[3]{2})$, dat niet Galois over $\mathbb{Q}$ is.

   (c) (5 pt) Stel L is het splijtlichaam van een irreducibel polynoom $f \in K[X]$ van graad n. Zij M een tussenlichaam, Galois over K, zó dat $L = M(\alpha)$ voor een nulpunt α van f. Dan is $[L : M]$ een deler van n.
   Antwoord: Ja, stel f ontbindt in $M[X]$ als $g = g_1 \cdots g_r$ en stel dat $g_1 \in M[x]$ het minimaalpolynoom van α over M is. Dan zijn de overige factoren g_i Galoisgeconjugeerden van g_1 (deze zitten ook in $M[X]$ omdat M Galois is) en hebben dus graad r. Gevolg, f is het product van polynomen van graad r en dus is $r = [L : M]$ is een deler van n.

   (d) (7 pt) Het aantal tussenlichamen van de uitbreiding $\mathbb{F}_{64}/\mathbb{F}_2$ (inclusief $\mathbb{F}_{64}$ en $\mathbb{F}_2$ zelf) is gelijk aan 6.
   Antwoord: Nee, $\mathbb{F}_{2^d}$ is een deellichaam van $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ precies dan als $d|6$. Dus $d = 1, 2, 3, 6$.

   (e) (5 pt) Elke eindige uitbreiding van $\mathbb{F}_p$ (p priem) is een Galois uitbreiding met cyclische Galoisgroep.
   Antwoord: Ja, elke eindige uitbreiding van $\mathbb{F}_p$ is van de vorm $\mathbb{F}_{p^f}$, en deze is Galois over $\mathbb{F}_p$.

2. Beschouw het polynoom $f = X^6 - tX^3 + t \in \mathbb{Q}(t)[X]$ in de variabelen X, t en zij L het splijtlichaam van f over het grondlichaam $\mathbb{Q}(t)$.

   (a) (5 pt) Bewijs dat f irreducibel in $\mathbb{Q}(t)[X]$ is.
   Antwoord: f is Eisenstein polynoom mbt het irreducibele element t in $\mathbb{Q}[t]$.

   (b) (5 pt) Stel dat $\alpha \in L$ een nulpunt is van f, dat wil zeggen: $\alpha^6 - t\alpha^3 + t = 0$. Laat zien dat $\omega\alpha$ en $t^{1/3}/\alpha$ ook nulpunten van f zijn (hierin is $\omega^3 = 1, \omega \neq 1$.
   Antwoord: Controle:

   $$(\omega\alpha)^6 - t(\omega\alpha)^3 + t = \alpha^6 - t\alpha^3 + t = 0$$
   $$(t^{1/3}/\alpha)^6 - t(t^{1/3}/\alpha)^3 + t = (t/\alpha^6)(t - t\alpha^3 + \alpha^6 = 0.$$

   (c) (5 pt) Bewijs dat $L = \mathbb{Q}(\alpha, \omega, t^{1/3})$.
   Antwoord: Uit voorgaande onderdeel volgt dat de nulpunten van f gegeven worden door $\omega^k\alpha$ en $\omega^l t^{1/3}/\alpha$ met $k, l = 0, 1, 2$. Dus L bevat $(\omega\alpha)/\alpha = \omega$ en $(t^{1/3}\alpha)\alpha = t^{1/3}$, en natuurlijk α Omgekeerd is elk nulpunt bevat in $\mathbb{Q}(\alpha, \omega, t^{1/3})$.

(d) (7 pt) Bepaal de Galois groep en de deellichamen van de uitbreiding $\mathbb{Q}(\omega, t^{1/3})/\mathbb{Q}(t)$.

Antwoord: $M = \mathbb{Q}(\omega, t^{1/3})$ is het splijtlichaam van $X^3 - t$ over $\mathbb{Q}(t)$. Omdat $t^{1/3} \notin \mathbb{Q}(\omega)$ is $M : \mathbb{Q}] = 6$ en de Galoisgroep gelijk aan S_3 (dit is de enige ondergroep van S_3 met 6 elementen. De echte deellichamen zijn $\mathbb{Q}(t, \omega)$ en $\mathbb{Q}(t^{1/3}), \mathbb{Q}(\omega t^{1/3}), \mathbb{Q}(\omega^2 t^{1/3})$.

(e) (5 pt) Bewijs dat $\mathbb{Q}(t, \alpha^3) = \mathbb{Q}(t, \sqrt{t^2 - 4t})$ door $f = 0$ op te lossen in X^3. Waarom geldt nu dat $\alpha \notin \mathbb{Q}(\omega, t^{1/3})$?

Antwoord: Merk op dat $f^(\alpha) = 0$ een kwadratische vergelijking in α^3 is. Oplossing geeft, $(t \pm \sqrt{t^2 - 4t})/2$. Dus $\mathbb{Q}(t, \alpha^3) = \mathbb{Q}(t, \sqrt{t^2 - 4t})$. Stel $\alpha \in \mathbb{Q}(\omega, t^{1/3}$. Dan geldt $\alpha^3 \in \mathbb{Q}(\omega, t^{1/3})$ en dus $\sqrt{t^2 - 4t} \in \mathbb{Q}(\omega, t^{1/3})$. Echter, het enige kwadratische deellichaam van $\mathbb{Q}(\omega, t^{1/3})$ is $\mathbb{Q}(\omega, t)$. En deze bevat niet $\sqrt{t^2 - 4t}$. Conclusie, $\alpha \notin \mathbb{Q}(\omega, t^{1/3})$.

(f) (7 pt) Bewijs dat $[L : \mathbb{Q}(t)]$ gelijk is aan $12, 18$ of 36.

Antwoord: Definieer $M = \mathbb{Q}(\omega, t^{1/3})$. Onder $\mathrm{Gal}(L/\mathbb{Q}(t))$ vormen de zes nulpunten 1 baan van lengte 6. Omdat $\mathrm{Gal}(L/M)$ normaaldeler van de totale Galoisgroep is, splitsen de nulpunten in banen van lengte $1, 2, 3$ of 6 op onder $\mathrm{Gal}(L/M)$. Lengte 6 kan niet, want dan zou $\alpha \in M$. Dus blijven baanlengten $1, 2, 3$ over en dit correspondeert met $[L : M] = 6, 3, 2$. Samen met $[M : \mathbb{Q}(t)] = 6$ geeft dit onze bewering.

(g) (5 pt) Er is nu gegeven dat $[L : \mathbb{Q}(t)] = 36$. Laat zien dat er elementen $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q}(\omega, t^{1/3})$ bestaan, zó dat $\tau(\alpha) = t^{1/3}/\alpha$ en $\sigma(\alpha) = \omega\alpha$.

Antwoord: Stel $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(t))$. Dan geldt in elk geval dat $\sigma(\alpha)$ weer een nulpunt van f is, $\sigma(t^{1/3}) = \omega^k t^{1/3}$ voor $k = 0, 1$ of 2 en $\sigma(\omega) = \omega^{\pm 1}$. Hiervoor zijn $6 \cdot 3 \cdot 2 = 36$ mogelijkheden en omdat de graad 36 is, komt elke mogelijkheid voor. In het bijzonder zijn er Galois elementen die α naar $t^{1/3}/\alpha$ of α naar $\omega\alpha$.

Sterker nog, ook zonder graad 36 geldt dit, de Galois groep werkt immers transitief op de nulpunten van een irreducibel polynoom.

3. In de volgende onderdelen mag je gebruiken dat elke kwadratische uitbreiding van een lichaam K (van karakteristiek $\neq 2$) van de vorm $K(\sqrt{\alpha})$ is met $\alpha \in K$.

(a) (7 pt) Zij K een lichaam van karakteristiek $\neq 2$ en $\alpha, \beta \in K^*$. Bewijs dat $K(\sqrt{\alpha}) \cong K(\sqrt{\beta})$ precies dan als er $\gamma \in K$ bestaat zó dat $\alpha = \beta\gamma^2$.
Antwoord: Stel eerst $\alpha = \beta\gamma^2$. Dan geldt $\sqrt{\alpha} = \gamma\sqrt{\beta}$, dus $K(\sqrt{\alpha}) \cong K(\sqrt{\beta})$.

Stel nu $K(\sqrt{\alpha}) \cong K(\sqrt{\beta})$. Dan geldt $\sqrt{\alpha} = a + b\sqrt{\beta}$ voor zekere $a, b \in K$. Neem kwadraat $\alpha = a^2 + b^2\beta + 2ab\sqrt{\beta}$. Vergelijken van linker- en rechetrzijde geeft $\alpha = a^2 + b^2\beta$ en $2ab = 0$. Dus $ab = 0$ (karakteristiek is $\neq 2$). Als $b = 0$ dan $\sqrt{\alpha} = a \in K$. Maar lichamen zijn isomorf, dus ook $\sqrt{\beta} \in K$ en de uitspraak volgt. Stel nu $a = 0$. Dan geldt $\sqrt{\alpha} = b\sqrt{\beta}$ en we zijn klaar.

In de volgende onderdelen nemen we $K = \mathbb{Q}(i)$ met $i = \sqrt{-1}$. Kies $a, b \in \mathbb{Q}$, stel dat $a + bi$ geen kwadraat is $\mathbb{Q}(i)$ is, en definieer $L = \mathbb{Q}(i, \sqrt{a + bi})$.

(b) (3+3 pt) Bewijs dat $L/\mathbb{Q}$ Galois is met Galoisgroep V_4 (Viergroep van Klein) precies dan als L een deellichaam van de vorm $\mathbb{Q}(\sqrt{d})$ bevat, met $d \in \mathbb{Z}$ en niet van de vorm $\pm m^2$ met $m \in \mathbb{Z}$.

Antwoord: Stel eerst dat L een deellichaam $\mathbb{Q}(\sqrt{d})$ bevat met $d/i \notin \mathbb{Q}$. dat betekent (zie voorgaand onderdeel) dat $\mathbb{Q}(i)$ niet isomorf is met $\mathbb{Q}(\sqrt{d})$ in het bijzonder $\sqrt{d} \notin \mathbb{Q}(i)$. Dus $\mathbb{Q}(i, \sqrt{d})$ heeft graad 4 over $\mathbb{Q}$ en is bovendien Galois, want splijtlichaam van $(X^2+1)(X^2-d)$. De Galoisgroep bevat de elementen σ, τ met $\sigma(i) = i, \sigma(\sqrt{d}) = -\sqrt{d}$ en $\tau(i) = -i, \tau(\sqrt{d}) = \sqrt{d}$. Ze hebben orde 2 en commuteren, dus Galois groep in V_4.

Stel nu dat $L/\mathbb{Q}$ Galois is met groep V_4. Deze groep bevat 3 ondergroepen van orde 2, dus bevat L drie kwadratische uitbreidingen van $\mathbb{Q}$. Eén ervan is $\mathbb{Q}(i)$, noem een van de anderen $\mathbb{Q}(\sqrt{d})$. Omdat deze niet gelijk is aan $\mathbb{Q}(i)$ moet gelden dat $d/i \notin \mathbb{Q}$. Door noemers uitvermenigvuldigen mogen we aannemen dat $d \in \mathbb{Z}$.

(c) (4+4 pt) Bewijs dat $L/\mathbb{Q}$ Galois is precies dan als er $c \in \mathbb{Q}$ bestaat, zó dat $a^2 + b^2 = c^2$.

Antwoord: Als $L/\mathbb{Q}$ Galois is dan bevat L ook $\sqrt{a-bi}$. In het bijzonder, $L = \mathbb{Q}(i, \sqrt{a-bi})$. Op grond van onderdeel a) volgt hieruit $(a+bi) = (a-bi)\gamma^2$ met $\gamma \in \mathbb{Q}(i)$. Na vermenigvuldigen met $a-bi$, $a^2+b^2 = (a-bi)^2\gamma^2$. Dus a^2+b^2 is een kwadraat in $\mathbb{Q}(i)$. Maar dit kan alleen als a^2+b^2 een kwadraat in $\mathbb{Q}$ is.

Stel $a^2+b^2 = c^2$. Het minimaalpolynoom van $a+bi$ is $X^4 - 2aX^2 + a^2 + b^2 = X^4 - 2aX^2 + c^2$. Als α een nulpunt is, dan zijn $-\alpha, c/\alpha$ en $-c\alpha$ dat ook. Dus $L = \mathbb{Q}(\alpha)$ is splitlichaam en daarmee Galois over $\mathbb{Q}$.

(d) (5 pt) Geef alle groepen van orde 4 (op isomorfie na).

Antwoord: V_4 en $C(4)$.

In de volgende opgaven mag je gebruiken dat als a^2+b^2 een kwadraat in $\mathbb{Q}$ is, er $r \in \mathbb{Q}, \gamma \in \mathbb{Q}(i)$ en $\mu \in \{\pm 1, \pm i\}$ bestaan, zó dat $a+bi = r\mu\gamma^2$.

(e) (5 pt) Bewijs dat er $r \in \mathbb{Q}$ en $\mu \in \{\pm 1, \pm i\}$ bestaan, zó dat $L = \mathbb{Q}(i, \sqrt{r\mu})$.

Antwoord: Vergeten te vermelden dat we $L/\mathbb{Q}$ Galois veronderstellen. Neem dit aan. Dan $a^2+b^2 = c^2$. Dus $a+bi = r\mu\gamma^2$ en $L = \mathbb{Q}(i, \sqrt{a+bi}) = \mathbb{Q}(i, \sqrt{r\mu})$.

(f) (5 pt) Bewijs dat er geen cyclische Galoisuitbreidingen van $\mathbb{Q}$ van graad 4 bestaan, die $\mathbb{Q}(i)$ als deellichaam bevatten.

Antwoord: Stel dat $L/\mathbb{Q}$ Galois is. Uit voorgaande, $L = \mathbb{Q}(i, \sqrt{r\mu})$. Als $\mu = \pm 1$ dan is L van de vorm $L = \mathbb{Q}(i, \sqrt{d})$ (met $r\mu = d$). Asl $\mu = i$, dan geldt $r\mu = (r/2)(1+i)^2$, en dus $L = \mathbb{Q}(i, \sqrt{r/2}(1+i)) = \mathbb{Q}(i, \sqrt{r/2}$. In beide gevallen is Galois groep V_4.