Vraag 2 (8 punten)**.** Waar of vals? Verklaar. (Een antwoord zonder verklaring levert geen punten op.)

(a) Elke groep van orde 2020 is nilpotent.

(b) Beschouw de vrije groep $F = F(\{a,b\})$ van rang 2. Als g en h twee elementen zijn van F die niet met elkaar commuteren, dan is $F = \langle g,h \rangle$.

(c) Zij E/F een Galoisuitbreiding van graad 2020. Er bestaat een irreducibel polynoom van graad 20 over F zodat E het splijtveld is van dit polynoom.

(d) Elke algebraïsche velduitbreiding van een perfect veld is een perfect veld.

Oplossing. (a) VALS. We weten dat een nilpotente groep van orde 2020 isomorf is met het direct product van een Sylow 2-, 5-, en 101-groep. Gezien elke groep van orde 4, 5 en 101 abels is, is elke nilpotente groep van orde 2020 abels. Bijgevolg is $\mathbf{D}_{2020}$ een tegenvoorbeeld.

(b) VALS. Beschouw $g = a^2$ en $h = b^2$. Men gaat na dat

$$\langle g,h \rangle = \{a^{2i_1} b^{2j_1} \dots a^{2i_n} b^{2j_n} \mid i_l, j_l \in \mathbb{Z}, n \in \mathbb{N}\} \neq F.$$

(c) VALS. Door Gevolg 4.1.15 zou de Galoisgroep dan een deelgroep van $\mathbf{S}_{20}$ zijn. Gezien E/F Galois is, heeft deze Galoisgroep orde 2020. Merk nu op dat $2020 = 2^2 \cdot 5 \cdot 101$ geen deler is van $20! = |\mathbf{S}_{20}|$, gezien $101 > 20$.

(d) WAAR. Zij F een perfect veld, en E/F een algebraïsche velduitbreiding. Door Gevolg 4.8.8 en 4.8.12 is een veld perfect als en slechts als elke algebraïsche uitbreiding ervan separabel is. Zij dus L/E een willekeurige algebraïsche uitbreiding. Door Stelling 3.2.11 is L/F algebraïsch. Omdat F perfect is volgt dan dat L/F separabel is. Door Lemma 4.3.11 is L/E dan separabel. Bijgevolg is E perfect.

$\square$

Vraag 3 (8 punten)**.** Beschouw de groep $\mathbf{T}$ van orde 12 met onderliggende verzameling $\mathbb{Z}/3 \times \mathbb{Z}/4$, en met bewerking gegeven door

$$(x,y) \cdot (z,w) := \begin{cases} (x+z, y+w) & \text{als } y \in \{0,2\}, \\ (x+2z, y+w) & \text{als } y \in \{1,3\}. \end{cases}$$

In Algebra I werd opgemerkt dat $g := (1,2)$ orde 6 heeft, $h := (0,1)$ orde 4 heeft en dat $g^3 = h^2 = (hg)^2$ en $gh = hg^{-1}$. (Dit hoef je *niet* na te gaan, je mag er eveneens van uitgaan dat $\mathbf{T}$ een groep is.)

(i) Toon aan dat $\mathbf{T} \cong \mathbf{C}_3 \rtimes \mathbf{C}_4$. Wat is de actie?

(ii) Bepaal alle deelgroepen van $\mathbf{T}$. Welke deelgroepen zijn normaaldelers? Teken een deelgroepentralie, d.w.z., een figuur zoals we gemaakt hebben in Figuur 4.2 op p. 80 van de cursus.

Veronderstel nu dat $E/\mathbb{Q}$ een Galoisuitbreiding is met Galoisgroep $\mathbf{T}$.

(iii) Toon aan dat er een uniek tussenveld M van E bestaat zodat $M/\mathbb{Q}$ een Galoisuitbreiding is met Galoisgroep $\mathbf{S}_3$.

(iv) Toon aan dat er een uniek tussenveld L van E bestaat zodat $L/\mathbb{Q}$ een Galoisuitbreiding is met Galoisgroep $\mathbf{C}_4$.

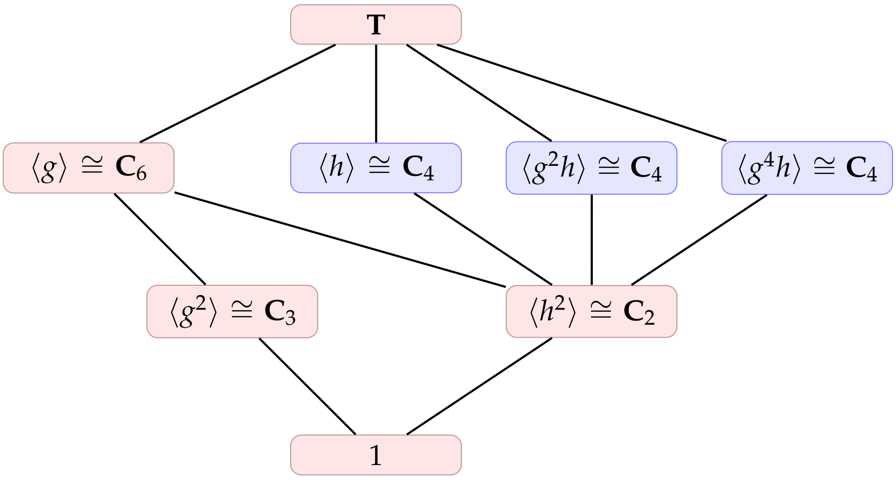
(v) Bepaal $[L \cap M : \mathbb{Q}]$.

Door de voorgaande delen hebben we enkele voorwaarden bepaald waaraan een Galoisuitbreiding moet voldoen om $\mathbf{T}$ als Galoisgroep te hebben.

(vi) Gebruik nu (de oplossing van) oefeningen 51 en 57 om aan te tonen dat er effectief een Galoisuitbreiding $E/\mathbb{Q}$ bestaat met Galoisgroep $\mathbf{T}$. (*Hint:* In een mogelijke oplossing staan de getallen 37 en 148 centraal.) Je kan de oplossing en opgave van deze oefeningen vinden in de bijlage van dit examen.

Oplossing. (i) Er geldt $\langle g^2 \rangle \cong \mathbf{C}_3$ en $\langle h \rangle \cong \mathbf{C}_4$. Door het vergelijken van de ordes volgt al $\langle g^2 \rangle \langle h \rangle = \mathbf{T}$. Merk op dat $gh = hg^{-1}$ impliceert dat $g^h = g^{-1}$ en dus $(g^2)^h = (g^2)^{-1} = g^4$. In het bijzonder is de actie van h^2 triviaal, en valt de actie van h^3 samen met die van h. We bekomen dus ook dat $\langle g^2 \rangle$ een normaaldeler is en dat $\mathbf{T} \cong \mathbf{C}_3 \rtimes \mathbf{C}_4$. Expliciet is de actie van $i \in \mathbf{C}_4$ gegeven door: $j \mapsto (-1)^i j$, met $j \in \mathbf{C}_3$.

(ii) Door stelling van Sylow en het feit dat $\langle g^2 \rangle \cong \mathbf{C}_3$ een normaaldeler is, volgt dat dit de enige groep is van orde 3. Omdat de actie van h op $\langle g^2 \rangle$ niet triviaal is, is $\langle h \rangle \cong \mathbf{C}_4$ geen normaaldeler en de stelling van Sylow levert dan dat er exact 3 deelgroepen zijn van orde 4, allen isomorf met $\mathbf{C}_4$. Meer specifiek zijn dit $\langle h \rangle$, $\langle g^2 h \rangle$ en $\langle g^4 h \rangle$, en deze bevatten allen de deelgroep $\langle h^2 \rangle$ van orde 2. Merk ook op dat $\langle g \rangle \cong \mathbf{C}_6$ een deelgroep is van index 2, en dus een normaaldeler. We zijn dus reeds 12 elementen van de groep $\mathbf{T}$ tegengekomen, 2 elementen van orde 6, 6 van orde 4, 2 van orde 3, 1 van orde 2 en 1 van orde 1. Bijgevolg is er een uniek element van orde 2 en is $\langle h^2 \rangle$ een normaaldeler, en gezien er maar 2 elementen van orde 3 en 1 van orde 2 zijn, is er een unieke deelgroep van orde 6. We bekomen dus volgend deelgroepentralie:



Figuur 1: *De deelgroepen van T. Normaaldelers staan in het rood.*

(iii) Via de hoofdstelling komt de normaaldeler van orde 2 overeen met een tussenveld M zodat $M/\mathbb{Q}$ Galois is en $[E : M] = 2$. Bovendien geldt er $\operatorname{Gal}(M/\mathbb{Q}) \cong \operatorname{Gal}(E/\mathbb{Q}) / \operatorname{Gal}(E/M) \cong \mathbf{T}/\langle h^2 \rangle \cong \langle g^2 \langle h^2 \rangle \rangle \rtimes \langle h \langle h^2 \rangle \rangle \cong \mathbf{C}_3 \rtimes \mathbf{C}_2$. Gezien de actie van h niet-triviaal is, is deze groep isomorf met $\mathbf{D}_6 \cong \mathbf{S}_3$. De uniciteit volgt omdat $\mathbf{T}$ een unieke deelgroep van orde 2 heeft.

(iv) Via de hoofdstelling komt de normaaldeler van orde 3 overeen met een tussenveld L zodat $L/\mathbb{Q}$ Galois is en $[E : L] = 3$. Bovendien geldt er $\operatorname{Gal}(L/\mathbb{Q}) \cong \operatorname{Gal}(E/\mathbb{Q}) / \operatorname{Gal}(E/L) \cong \mathbf{T}/\langle g^2 \rangle \cong \langle h \langle g^2 \rangle \rangle \cong \mathbf{C}_4$, door (i). De uniciteit volgt omdat $\mathbf{T}$ een unieke deelgroep van orde 3 heeft.

(v) Door de hoofdstelling komt het tussenveld $L \cap M$ overeen met de kleinste deelgroep die $\mathbf{C}_2$ en $\mathbf{C}_3$ bevat, $\langle g \rangle \cong \mathbf{C}_6$ dus. Er volgt $[L \cap M : \mathbb{Q}] = 12/6 = 2$.

(vi) We moeten dus een Galoisuitbreiding M van $\mathbb{Q}$ vinden met Galoisgroep $\mathbf{S}_3$, en een Galoisuitbreiding L van $\mathbb{Q}$ met Galoisgroep $\mathbf{C}_4$ zodat $M \cap L = \mathbb{Q}(\sqrt{d})$, voor een zeker niet-kwadraat $d \in \mathbb{Q}$. Vanwege de hint lijkt $d = 37$ aannemelijk. We beginnen met het construeren van M. Zij M het splijtveld van een irreducibele kubische veelterm $f(x) = x^3 + px + q$. Gezien $\sqrt{\Delta(f)}$ het product is van wortels van

f, is het bevat in M. Door oefening 51(ii) is $[M : \mathbb{Q}]$ gelijk aan 3 of aan 6, in dit laatste geval is de Galoisgroep duidelijk isomorf met $\mathbf{S}_3$ gezien deze getrouw werkt op de 3 wortels van f. Dan is door oefening 51(v) de Galoisgroep isomorf met $\mathbf{S}_3$ als en slechts $\sqrt{\Delta(f)}$ geen kwadraat is in $\mathbb{Q}$. Door het voorgaande houdt het nu steek om p en q zo te kiezen dat $\Delta(f) = -4p^3 - 27q^2$ gelijk is aan 37 of 148. Na een aantal kleine getallen te proberen vind je dat $-4(-4)^3 - 27 \cdot 2^2 = 148 = 4 \cdot 37$. Bijgevolg bevat het splijtveld M van het irreducibel polynoom $x^3 - 4x + 2$ (door Eisenstein) de kwadratische velduitbreiding $\mathbb{Q}(\sqrt{37})$, en heeft het $\mathbf{S}_3$ als Galoisgroep.

Nu willen we oefening 57 gebruiken om een bikwadratisch polynoom $x^4 + bx^2 + c$ te vinden die irreducibel is, waarvan het splijtveld L de velduitbreiding $\mathbb{Q}(\sqrt{37})$ bevat en zodat de Galoisgroep isomorf is met $\mathbf{C}_4$. Zij α een wortel van deze vergelijking, dan is $\alpha^2 = \frac{-b\pm\sqrt{b^2-4c}}{2}$. Bijgevolg geldt best $b^2 - 4c = 37$. Nu werken we de voorwaarde opdat de Galoisgroep $\mathbf{C}_4$ is verder uit (zie oefening 57). Zonder verlies van algemeenheid geldt $\alpha = \sqrt{\frac{-b+\sqrt{b^2-4c}}{2}}$ en $\beta = \sqrt{\frac{-b-\sqrt{b^2-4c}}{2}}$. Er geldt dus $\alpha\beta = \sqrt{\frac{b^2-(b^2-4c)}{4}}$. Bijgevolg geldt $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = \frac{2}{\sqrt{b^2-(b^2-4c)}}(\alpha^2 - \beta^2) = \frac{2\sqrt{b^2-4c}}{\sqrt{b^2-(b^2-4c)}}$. Dit getal moet dus in $\mathbb{Q}$ bevat zijn. Er nu even vanuit gaande dat $b^2 - 4c = 37$ bekomen we dat we λ en b in $\mathbb{Q}$ moeten vinden zodat $37\lambda^2 = b^2 - 37$. Het is duidelijk dat $b = 37$ en $\lambda = 6$ voldoen. Bovendien kunnen we $c = 9 \cdot 37$ kiezen zodat $b^2 - 4c = 37$.

Zij dus E het splijtveld van $(x^3 - 4x + 2)(x^4 + 37x^2 + 333)$, M het splijtveld van $x^3 - 4x + 2$, L het splijtveld van $x^4 + 37x + 333$ (irreducibel door Eisenstein, $p = 37$). Zij α_1, α_2 en α_3 de wortels van het graad 3 polynoom, en α een wortel van de bikwadratische vergelijking. Dan is $\mathbb{Q}(\alpha_1)$ een velduitbreiding van graad 3 die niet Galois is, want het splijtveld M bevat de kwadratische uitbreiding $\mathbb{Q}(\sqrt{37})$. Gezien $\mathbb{Q}(\alpha_1,\sqrt{37})$ een velduitbreiding is van graad 6, bevat in de velduitbreiding M van graad 6, vallen ze samen. Vanwege de graad van het minimaalpolynoom heeft $\mathbb{Q}(\alpha)$ graad 4 over $\mathbb{Q}$ en valt het dus samen met L. Merk op dat $\mathbb{Q}(\alpha)$ dus $\mathbb{Q}(\sqrt{37})$ bevat. Bijgevolg geldt $E = \mathbb{Q}(\alpha_1,\beta)$, door de torenformule nu op twee verschillende manieren toe te passen bekomen we dat $[E : \mathbb{Q}]$ het getal $4 \cdot 3$ deelt en kleiner of gelijk is aan 12. Bijgevolg is $E/\mathbb{Q}$ een Galoisuitbreiding van graad 12. Deze heeft corresponderende Galoisgroep van orde 12, die een normaaldeler van orde 3 bevat (corresponderend met de Galoisuitbreiding $L/\mathbb{Q}$) en een deelgroep van orde 4 die geen normaaldeler is (corresponderend met de uitbreiding $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ die niet Galois is). Deze deelgroep van orde 4 is isomorf met $\mathbf{C}_4$ gezien het quotient van de Galoisgroep en $\mathbf{C}_3$ isomorf is met $\mathbf{C}_4$. Bijgevolg is de Galoisgroep een semidirect product van $\mathbf{C}_3$ en $\mathbf{C}_4$ dat geen direct product is. Gezien er maar één niet-triviale actie van $\mathbf{C}_4$ op $\mathbf{C}_3$ bestaat, is de Galoisgroep isomorf met $\mathbf{T}$.

$\square$