Gelieve elke vraag op een apart antwoordblad op te lossen. Succes!

Vraag 1 (10 punten). In deze vraag polsen we naar het inzicht in het bewijs van Stelling 2.1.8 en Gevolg 2.1.9 uit de cursus.

Stelling. *Voor elke $n \geq 5$ is de alternerende groep $\mathbf{A}_n$ enkelvoudig.*

Bewijs. We bewijzen dit per inductie op n, waarbij het geval $n = 5$ precies Lemma 2.1.6 is. Zij dus $n \geq 6$, stel $G = \mathbf{A}_n$, en veronderstel dat $1 \neq N \lhd G$ een echte niet-triviale normaaldeler is. Zij $H = \mathrm{Stab}_G(n)$; dan is $H \cong \mathbf{A}_{n-1}$, (i)
en door de inductiehypothese weten we dat H enkelvoudig is. Aangezien $N \cap H \trianglelefteq H$, volgt hieruit dat ofwel $N \cap H = 1$, ofwel $H \leq N$.

Veronderstel eerst dat $H \leq N$. Omdat N een normaaldeler is, volgt hieruit dat ook $H^g \leq N$ voor alle $g \in \mathbf{A}_n$, en omdat $\mathbf{A}_n$ uiteraard tran- (ii)
sitief werkt op $\{1, \ldots, n\}$, halen we hieruit dat $\mathrm{Stab}_G(i) \leq N$ voor alle (iii)
$i \in \{1, \ldots, n\}$. In het bijzonder bevat N dus alle elementen die het pro-
duct zijn van twee transposities, maar dan is $N = \mathbf{A}_n$, strijdig. (iv)

Veronderstel nu dat $N \cap H = 1$. Dan is ook $N \cap H^g = (N \cap H)^g = 1$, en dus $N \cap \mathrm{Stab}_G(i) = 1$ voor alle i, i.e. enkel het triviale element van N heeft fixpunten. Kies nu een $g \in N \setminus \{1\}$ willekeurig. De cykeldecompositie van g bevat ofwel een m-cykel met $m \geq 3$, ofwel bestaat het volledig uit (v)
2-cykels, maar dan zijn er ten minste twee 2-cykels. Door de elementen $\{1, \ldots, n\}$ te hernummeren ... □

Gevolg. *De enige normaaldelers van $\mathbf{S}_n$, $n \geq 5$, zijn 1, $\mathbf{A}_n$ en $\mathbf{S}_n$.*

Bewijs. Zij $N \trianglelefteq \mathbf{S}_n$. Dan is $\mathbf{A}_n \cap N \trianglelefteq \mathbf{A}_n$, en uit Stelling 1 volgt dan dat ofwel $\mathbf{A}_n \leq N$, ofwel $\mathbf{A}_n \cap N = 1$.

In het eerste geval moet ofwel $N = \mathbf{A}_n$, ofwel $N = \mathbf{S}_n$. Stel dus nu dat (vi)
$\mathbf{A}_n \cap N = 1$; dan is $|\mathbf{A}_n N| = |\mathbf{A}_n| \cdot |N|$, en bijgevolg $|N| \leq [\mathbf{S}_n : \mathbf{A}_n] = 2$. Er (vii)
rest ons enkel nog het geval $|N| = 2$ uit te sluiten. Een normaaldeler van orde 2 is echter steeds bevat in het centrum, en dus zou $N \leq Z(\mathbf{S}_n)$. Dit is (viii)
in strijd met Gevolg 2.1.4. □

(i) Waarom is $H \cong \mathbf{A}_{n-1}$?

(ii) Waarom werkt $\mathbf{A}_n$ transitief op $\{1, \ldots, n\}$?

(iii) Hoe volgt hieruit dat $\mathrm{Stab}_G(i) \leq N$?

(iv) Waarom geldt dan $N = \mathbf{A}_n$?

(v) Verklaar deze beschrijving in verband met de cykeldecompositie van g.

(vi) Hoe volgt uit $\mathbf{A}_n \leq N$ dat $N = \mathbf{A}_n$ of $N = \mathbf{S}_n$?

(vii) Verklaar deze "bijgevolg".

(viii) Waarom is elke normaaldeler van orde 2 bevat in het centrum?

Deze bijlage bevat de oplossing en opgave van oefeningen 51 en 57 en kan helpen bij vraag 3(vi)

Opmerking: Volgende opgave bestudeert in vrij grote algemeenheid hoe splijtvelden van vergelijkingen van graad 3 eruit zien. Merk daartoe op dat elke derdegraads vergelijking na een geschikte substitutie $x \mapsto x + a$ in de vorm $x^3 + px + q$ kan gebracht worden (zolang de karakteristiek niet 3 is), een zogenaamde 'depressed cubic'. De conclusie geldt eigenlijk zelfs indien we veronderstellen dat de karakteristiek copriem is met 6. Indien f een polynoom is in $F[x]$ van graad n met wortels $\alpha_1, \ldots, \alpha_n$, dan stellen we:

$$\Delta(f) = (\prod_{i<j}(\alpha_i - \alpha_j))^2.$$

Oefening 51. Beschouw een veld F met karakteristiek 0, $f(x) = x^3 + px + q \in F[x]$ een irreduciebel polynoom en noteer de wortels van f in $\bar{F}$ met $\alpha_1, \alpha_2, \alpha_3$. Dan is gegeven dat

$$\Delta(f) = \big((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)\big)^2 = -4p^3 - 27q^2.$$

(i) Toon aan dat $\alpha_3 \in F(\alpha_1, \alpha_2)$.

(ii) Definieer $K = F(\alpha_1)$ en $L = F(\alpha_1, \alpha_2)$. Over K kunnen we $f(x) = (x - \alpha_1)h(x)$ schrijven, voor zekere $h(x) \in K[x]$. Toon dat $K \neq L$ als en slechts als h irreduciebel is over K.

(iii) Bepaal de graad $[L : F]$ in het geval $K = L$ en in het geval $K \neq L$.

(iv) Schrijf $\Delta(f)$ in functie van $\Delta(h)$ en $h(\alpha_1)$.

(v) Toon aan dat $\Delta(f)$ een kwadraat is in F als en slechts als $K = L$. (*Hint:* bewijs eerst dat $\Delta(f)$ een kwadraat is in K als en slechts als $K = L$.)

Oplossing. (i) We hebben dat $x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Gelijkstellen van de coëfficiënt van x^2 levert dat $\alpha_1 + \alpha_2 + \alpha_3 = 0$, zodat $\alpha_3 = -\alpha_1 - \alpha_2 \in F(\alpha_1, \alpha_2)$.

(ii) Merk op dat h in L factoriseert als $(x - \alpha_2)(x - \alpha_3)$. Dus h factoriseert reeds in K als en slechts als $\alpha_2 \in K$ (en dan ook $\alpha_3 \in K$). In dat geval is $\alpha_2 \in F(\alpha_1)$, zodat $K = L$.

(iii) Het is duidelijk dat $K \cong F[X]/f(X)$ een uitbreiding is van graad 3. Indien $L = K$, is uiteraard $[L : F] = 3$. Indien $L \neq K$, is $L \cong K[X]/h(X)$ zodat $[L : K] = 2$ en $[L : F] = 6$.

(iv) Vermits de twee wortels van h in L gegeven zijn door α_2 en α_3, is $\Delta(h) = (\alpha_2 - \alpha_3)^2$. Daarnaast is $h(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$, zodat $\Delta(f) = \Delta(h) \cdot h(\alpha_1)^2$.

(v) Vermits de karakteristiek niet 2 is, is een polynoom van graad 2 reduciebel als en slechts als de discriminant een kwadraat is. Dus indien

in $\mathbb{Q}$. Veronderstel dus $d \neq 0$, dan geldt $2c = ad$. Indien we dit in de eerste vergelijking invullen bekomen we

$$d^2 = \frac{4b}{a^2 - 4b}.$$

Merk nu op dat $a^2 - 4b$ de discriminant is van de vergelijking $y^2 + ay + b = 0$, die oplossingen α^2 en β^2 heeft. Gezien de discriminant van een vergelijking met coëfficiënt van x^2 gelijk aan 1 gelijk is aan het kwadraat van het verschil van de oplossingen bekomen we $(\alpha^2 - \beta^2)^2 = a^2 - 4b^2$. Merk ook op dat $4b = (2\alpha\beta)^2$. Bijgevolg is het eerste stelsel vergelijkingen oplosbaar (onder de voorwaarde $d \neq 0$) als en slechts als $\frac{2\alpha\beta}{\alpha^2-\beta^2} \in \mathbb{Q}$. Gezien $\frac{\alpha^2-\beta^2}{\alpha\beta} = \frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ is dit equivalent met $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$. Merk ook nog op dat $b = \alpha^2\beta^2$, dus b is een kwadraat in $\mathbb{Q}$ als en slechts als $\alpha\beta \in \mathbb{Q}$.

We bekomen dus dat het splijtveld van f graad 4 heeft als en slechts als $\alpha\beta \in \mathbb{Q}$ of $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$. Indien het splijtveld graad 8 heeft, weten we door (de oplossing van) oefening 56 dat $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbf{D}_8$. Indien het splijtveld graad 4 heeft, is $\mathrm{Aut}_{\mathbb{Q}}(L)$ een groep van orde 4 gezien het beeld van α het automorfisme vastlegt en α naar een wortel van f gestuurd moet worden. Zij σ het (unieke) automorfisme met $\sigma(\alpha) = -\beta$. In het geval $\alpha\beta \in \mathbb{Q}$ bekomen we $\alpha\beta = \sigma(\alpha)\sigma(\beta) = -\beta\sigma(\beta)$ en dus $\sigma(\beta) = -\alpha$, dus moet σ overeenkomen met de permutatie $(\alpha\ -\beta)(-\alpha\ \beta)$. Ook de automorfismen die α naar β en α naar $-\alpha$ sturen hebben orde 2 en dus $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbf{C}_2 \times \mathbf{C}_2$. In het geval $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$ geldt

$$\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = \sigma\Big(\frac{\alpha}{\beta} - \frac{\beta}{\alpha}\Big) = \frac{-\beta}{\sigma(\beta)} - \frac{\sigma(\beta)}{-\beta}.$$

Bijgevolg geldt $\sigma(\beta) = \alpha$ en dus moet σ overeenkomen met de permutatie $(\alpha\ -\beta\ -\alpha\ \beta)$. Gezien $\mathrm{Aut}_{\mathbb{Q}}(L)$ een element van orde 4 bevat, geldt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbf{C}_4$. □