ALGEBRA 1, honoursvariant

Spelregels. De uiterste inlevertermijn is 1 augustus 2011. Na die datum is inleveren niet meer mogelijk. Wanneer je je werk inlevert, houd dan zelf een kopie. Je mag bij het maken van de opgaven overleggen met andere studenten, maar je dient je uitwerkingen zelfstandig op te schrijven. Je uitwerkingen dienen in goed Nederlands geschreven te zijn. Gebruik volledige zinnen; geen steno; geen reeksen formules zonder verdere uitleg.

De onderstaande opdrachten bevatten zowel theorie als opgaven. Het is uitdrukkelijk de bedoeling dat je zelf in de literatuur op zoek gaat naar definities en uitleg. Veel succes!

1. De struktuur van eindig voortgebrachte abelse groepen.

(i) Geef de definitie van een eindig voortgebrachte groep. Is $\mathbb{Q}$ eindig voortgebracht? Geef een voorbeeld van een eindig voortgebrachte abelse groep die niet eindig is.

(ii) Stel G is een eindige abelse groep. Gegeven zijn elementen x, $y \in G$ zo dat $\mathrm{orde}(x)$ en $\mathrm{orde}(y)$ onderling ondeelbaar zijn. Bewijs dat $\mathrm{orde}(xy) = \mathrm{orde}(x) \cdot \mathrm{orde}(y)$. Geef een voorbeeld waaruit blijkt dat de voorwaarde dat G abels is niet gemist kan worden.

(iii) Stel G is een eindige abelse groep. Kies een element $a \in G$ waarvan de orde zo groot mogelijk is, d.w.z., $\mathrm{orde}(a) = \max\bigl\{\mathrm{orde}(x) \bigm| x \in G\bigr\}$. (Merk op dat zo'n element bestaat.) Bewijs dat $\mathrm{orde}(x)$ een deler is van $\mathrm{orde}(a)$ voor elke $x \in G$.

(iv) Kies een element $a \in G$ als in (iii). Zij $H = \langle a \rangle$ de door a voortgebrachte ondergroep van G en zij $\varphi\colon G \to G/H$ de quotiëntafbeelding. Bewijs dat er voor elke $y \in G/H$ een element $\tilde{y} \in G$ bestaat zo dat $\varphi(\tilde{y}) = y$ en $\mathrm{orde}(\tilde{y}) = \mathrm{orde}(y)$.

(v) Bewijs het volgende resultaat:

Stelling. *Zij G een eindige abelse groep. Dan bestaan er positieve gehele getallen n_1, $n_2, \ldots, n_t$ met $n_i > 1$ voor alle i, zo dat $n_1 | n_2 | \cdots | n_t$ (dus: n_1 is een deler van n_2 en n_2 is een deler van n_3 en...) en*

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}) .$$

Bovendien zijn deze getallen n_i uniek bepaald.

(vi) Zij G een eindige abelse groep waarvan de orde kwadraatvrij is; d.w.z.: er is geen geheel getal $m > 1$ zo dat m^2 een deler is van $\#G$. Bewijs dat G cyklisch is.

(vii) Zij G een abelse groep. Bewijs dat

$$\mathrm{Tors}(G) := \bigl\{g \in G \bigm| \mathrm{orde}(g) < \infty\bigr\}$$

een ondergroep is van G. (Deze groep heet de torsie-ondergroep van G.) Als G eindig voortgebracht is, laat zien dat $\mathrm{Tors}(G)$ eindig is.

(viii) Zij G een eindig voortgebrachte abelse groep. Dan heet G *torsievrij* als $\mathrm{Tors}(G) = \{1\}$; dit betekent dus dat G geen elementen heeft van eindige orde, afgezien van he eenheidselement. Bewijs dat een dergelijke torsievrije groep G isomorf is met $\mathbb{Z}^r$ voor een uniek bepaalde $r \geqslant 0$.

(ix) Bewijs het volgende resultaat:

Stelling. *Zij G een eindig voortgebrachte abelse groep. Dan bestaan er positieve gehele getallen r, n_1, $n_2, \ldots, n_t$ met $n_i > 1$ voor alle i, zo dat $n_1 | n_2 | \cdots | n_t$ en*

$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}).$$

Bovendien zijn deze getallen r en n_i uniek bepaald.

Het getal r in deze stelling heet de *rang* van de groep G.

(x) Zij $f\colon \mathbb{Z}^3 \to \mathbb{Z}^4$ de afbeelding gegeven door de matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -2 & 4 \\ -1 & 7 & 0 \\ 2 & 15 & 5 \end{pmatrix}.$$

(Dus $f(x_1, x_2, x_3) = (x_1 + 2x_2 + 3x_3, -2x_2 + 4x_3, \ldots)$.) Dan is $\mathrm{Im}(f)$ een ondergroep van $\mathbb{Z}^4$. Bepaal getallen r en n_i voor de groep $G = \mathbb{Z}^4/\mathrm{Im}(f)$.

2. Sylow ondergroepen. In deze opdracht is p steeds een priemgetal. Het hoofddoel van de opgave is om drie stellingen van L. Sylow te bewijzen.

(i) Een eindige groep G heet een *p-groep* als de orde van G een macht is van p. Laat zien dat het centrum van een p-groep niet triviaal is.

(ii) Bewijs het volgende resultaat:

Stelling. *Zij G een eindige groep. Schrijf $\#G = p^k \cdot m$ met $p \nmid m$. Dan heeft G een ondergroep van orde p^k.*

Hints: Zij Z het centrum van G. Redeneer met inductie naar de orde van G. Als $\#Z$ deelbaar is door p, kies een element $z \in Z$ van orde p en kijk naar de quotiëntafbeelding $\pi\colon G \to G/\langle z \rangle$. Als $\#Z$ niet deelbaar is door p, kijk naar de werking van G op $G \setminus Z$ (het complement van Z in G) door conjugatie. Laat zien dat er een baan is waarvan de lengte niet deelbaar is door p en concludeer dat er een ondergroep $H \subset G$ is met $\#H = p^k \cdot n$ voor een $n < m$.

Een ondergroep $P \subset G$ met $\#P = p^k$ heet een *p-Sylow-ondergroep* van G.

(iii) Bewijs het volgende resultaat:

Stelling. *Zij G een eindige groep. Dan zijn alle p-Sylow-ondergroepen van G onderling geconjugeerd.*

(iv) Bewijs het volgende resultaat:

Stelling. *Zij G een eindige groep. Zij s_p het aantal p-Sylow-ondergroepen van G. Dan is $s_p \equiv 1 \bmod p$ en s_p is een deler van $\#G$. Verder geldt voor elke p-Sylow-ondergroep $P \subset G$ dat $s_p = \bigl[G : N_G(P)\bigr]$.*

(v) Beschrijf alle Sylow-ondergroepen (voor $p \in \{2, 3, 5\}$) van de groep S_6.

(vi) Zij N een normaaldeler van een eindige groep G en zij $\pi\colon G \to G/N$ de quotiëntafbeelding. Zij Q een p-Sylow-ondergroep van G/N. Bewijs dat er een p-Sylow-ondergroep $P \subset G$ bestaat zo dat $\pi(P) = Q$. Bewijs ook dat P uniek is als N een p-groep is.

3. Oplosbare, nilpotente en simpele groepen. Het is een natuurlijke vraag of een gegeven groep G is "op te bouwen" uit kleinere groepen, of uit groepen die gemakkelijker te begrijpen zijn. Stel bijvoorbeeld dat G een eindige groep is die een normaaldeler $N \triangleleft G$ heeft met $N \neq \{1\}$ en $N \neq G$. Dan zijn N en G/N groepen van kleinere orde, zodat je zou kunnen hopen dat ze gemakkelijker te begrijpen zijn, en je kunt de groep G opvatten als een groep die is verkregen door de "bouwstenen" N en G/N te combineren. Pogingen om een groep in eenvoudigere stukken uitelkaar te halen, hebben geleid tot een aantal begrippen die een belangrijke rol spelen in de groepentheorie en zijn toepassingen, en het doel van deze opgave is om op enkele van deze begrippen nader in te gaan.

Een groep G heet *nilpotent* als er een rij ondergroepen

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

is, zo dat elke G_i normaal is in G en zo dat G_i/G_{i-1} bevat is in het centrum van G/G_{i-1}.

Een groep G heet *oplosbaar* als er een rij ondergroepen

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

is, zo dat elke G_i normaal is in G_{i+1} en zo dat G_{i+1}/G_i abels is, voor elke i.

(i) Ga voor elk van de volgende groepen na of deze nilpotent is en of deze oplosbaar is: A_3, S_3, A_4, S_4, D_4, Q.

Zij G een groep. Definieer een dalende rij ondergroepen

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

door $G^{(i+1)} := \big[G^{(i)}, G^{(i)}\big]$, de commutatorondergroep van $G^{(i)}$. Deze rij heet de *afgeleide rij* van ondergroepen.

(ii) Bewijs dat G oplosbaar is dan en slechts dan als er een index $n \geqslant 0$ bestaat zo dat $G^{(n)} = \{1\}$.

Zij G een groep. Definieer een dalende rij ondergroepen

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq \gamma_3(G) \supseteq \cdots$$

door $\gamma_{(i+1)} := \big[G, \gamma_i(G)\big]$. Deze rij heet de *onderste centrale rij* van ondergroepen. Definieer ook een stijgende rij van ondergroepen van G,

$$\{1\} = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots ,$$

door de eigenschap dat $\zeta_{i+1}(G)/\zeta_i(G)$ het centrum is van de groep $G/\zeta_i(G)$. Deze rij heet de *bovenste centrale rij* van ondergroepen.

(iii) Ga na dat de ondergroepen $\gamma_i(G)$ en $\zeta_j(G)$ normaaldelers zijn van G.

(iv) Bewijs dat de volgende drie eigenschappen equivalent zijn: (a) G is nilpotent, (b) er is een $n \geqslant 1$ zo dat $\gamma_n(G) = \{1\}$, (c) er is een $n \geqslant 0$ zo dat $\zeta_n(G) = G$.

(v) Bewijs dat een nilpotente groep oplosbaar is en geef een voorbeeld waaruit blijkt dat het omgekeerde in het algemeen niet geldt.

(vi) Als G_1 en G_2 nilpotent zijn, toon aan dat ook $G_1 \times G_2$ nilpotent is. Als G een nilpotente groep is, laat dan zien dat elke ondergroep van G en elke quotiëntgroep van G ook nilpotent is. Idem met "nilpotent" overal vervangen door "oplosbaar".

(vii) Toon aan dat elke p-groep nilpotent is.

(viii) Zij G een eindige groep. Bewijs dat G nilpotent is dan en slechts dan als G isomorf is met een produkt van p-groepen. [*Hints voor de "slechts dan" implicatie:* Laat zien dat het volstaat te bewijzen dat er voor elk priemgetal p een unieke p-Sylow-ondergroep is. Kijk naar het centrum Z van G en naar G/Z en gebruik inductie naar $\#G$.]

(ix) Zij N een normaaldeler van een groep G en stel dat N en G/N allebei oplosbaar zijn. Laat zien dat G ook oplosbaar is. Geef een voorbeeld waaruit blijkt dat iets dergelijks niet geldt voor nilpotente groepen.

(x) Zij G een groep met $\#G < 60$. Bewijs dat G oplosbaar is. [*Hints:* Werk met inductie naar $\#G$. Vanwege het vorige onderdeel ben je klaar als je kunt aantonen dat G een niet-triviale normaaldeler heeft. Gebruik daartoe de stellingen die zijn behandeld en de resultaten over Sylow-ondergroepen uit deel 2, in het bijzonder de stelling in punt 2(iv). Je kunt het beste eerst bewijzen dat groepen van orde $2p^m$ met p een priemgetal $\geqslant 3$ en groepen van orde $3p^m$ met p een priemgetal $\geqslant 5$ oplosbaar zijn. De lastige ordes zijn 12, 24, 30, 36, 48 en 56. Kijk in die gevallen naar doorsnedes van (handig gekozen) Sylow-ondergroepen, en kijk steeds goed naar wat je kunt zeggen over de normalisator. Als je een niet-triviale ondergroep vindt waarvan de normalisator de hele G is dan ben je klaar!]

Een groep G heet *simpel* als G geen enkele niet-triviale normaaldeler heeft.

(xi) Bewijs dat de alternerende groep A_n simpel is als $n \geqslant 5$. Concludeer dat A_5 de kleinste niet-oplosbare groep is.

De eindige simpele groepen kunnen beschouwd worden als de "bouwstenen" van de theorie van eindige groepen. Er is een volledige classificatie van alle simpele eindige groepen, maar het bewijs dat deze classificatie correct en volledig is, grenst aan wat een mens nog kan bevatten: het originele bewijs uit de jaren 1980 besloeg vele duizenden pagina's. Er wordt door experts gewerkt aan een beter bewijs, waarvan een deel inmiddels is gepubliceerd in een zestal boeken.

Sommige simpele eindige groepen vormen "families". Zo zijn de alternerende groepen A_n voor $n \geqslant 5$ allemaal simpel. Maar er zijn ook 26 zogenaamde "sporadische" eindige simpele groepen. De grootste daarvan, het monster genaamd, heeft orde

$$808017424794512875886459904961710757005754368000000000\,.$$

Een van de belangrijkste stellingen in deze classificatie is de Feit-Thompson stelling die zegt dat elke eindige groep van oneven orde oplosbaar is.