Tentamen algebra 1

8 juni 2005, 13.30–16.30, zaal A.404

Schrijf je naam en collegekaartnummer of het werk dat je inlevert.
Het tentamen bestaat uit 5 opgaven.
Beargumenteer telkens je antwoord. Veel succes!

Opgave 1.
a. Bepaal alle oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ die voldoen aan de vergelijking $42x + 26y = 2$.
b. Bepaal de restklasse $u \pmod{273}$ die de congruenties

$$u \equiv 4 \pmod{21}, \quad u \equiv 5 \pmod{13}$$

oplost.
c. Toon aan dat $u^{13} \equiv u \pmod{273}$ voor alle $u \in \mathbb{Z}$.

Oplossing:
a. Na deling door de gemeenschappelijke factor 2, zoeken we de oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ van $21x + 13y = 1$. We passen Euclides' algorithme toe om een oplossing te vinden:

$$\begin{aligned}
21.1 + 13.0 &= 21\\
21.0 + 13.1 &= 13\\
21.1 - 13.1 &= 8\\
-21.1 + 13.2 &= 5\\
21.2 - 13.3 &= 3\\
-21.3 + 13.5 &= 2\\
21.5 - 13.8 &= 1,
\end{aligned}$$

waarbij we steeds twee opeenvolgende vergelijkingen van elkaar af hebben getrokken. We concluderen dat $(x, y) = (5, -8)$ een oplossing is van $21x+13y = 1$. Iedere andere oplossing is van de vorm $(x, y) = (5 + u, -8 + v)$ met $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ een oplossing van $21u + 13v = 0$. Omdat $\text{ggd}(21, 13) = 1$ geldt er voor zo'n (u, v) dat v deelbaar is door 21 en dat u deelbaar is door 13. We concluderen dat $\{(13k, -21k) \mid k \in \mathbb{Z}\}$ alle oplossingen van de vergelijking $21u + 13v = 0$ zijn. Dus alle oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ van $42x + 26y = 2$ zijn: $\{(5 + 13k, -8 - 21k) \mid k \in \mathbb{Z}\}$.
b. Bij onderdeel **a** hebben we gezien dat $1 = 21.5-13.8$. We nemen nu $u = 21.5.5-13.8.4 = 109$. Dan geldt

$$\begin{aligned}
u &\equiv (21.5 - 13.8).4 \equiv 4 \pmod{21},\\
u &\equiv (21.5 - 13.8).5 \equiv 5 \pmod{13}
\end{aligned}$$

dus $109 \pmod{273}$ is de gevraagde restklasse.
c. De priemontbinding van 273 is $273 = 3.7.13$. De Chinese reststelling geeft dan dat

$$\mathbb{Z}/273\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$$

als groepen via de afbeelding

$$x(\text{mod } 273) \mapsto \big(x(\text{mod } 3), x(\text{mod } 7), x(\text{mod } 13)\big).$$

Voor $u \in \mathbb{Z}$ geldt dan dat $u^{13} - u \equiv 0$ modulo 273 dan en slechts dan als

$$\begin{aligned} u^{13} - u &\equiv 0 \pmod 3, \\ u^{13} - u &\equiv 0 \pmod 7, \\ u^{13} - u &\equiv 0 \pmod{13}. \end{aligned} \tag{1}$$

We tonen nu eerst aan dat de tweede congruentie geldt. Als u deelbaar is door 7, dan is $u^{13} - u$ ook deelbaar door 7, dus $u^{13} - u \equiv 0 \pmod 7$. Als u niet delbaar is door 7, dan $u(\text{mod } 7) \in \big(\mathbb{Z}/7\mathbb{Z}\big)^*$. De kleine stelling van Fermat geeft dan dat $u^6 \equiv 1 \pmod 7$, en dus

$$u^{13} \equiv u(u^6)^2 \equiv u(\text{mod } 7).$$

De andere twee congruenties in (1) volgen op dezelfde manier.

Opgave 2. Noteer

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 6 & 1 & 2 & 5 & 7 \end{pmatrix} \in S_7.$$

a. Schrijf σ als produkt van disjunkte cykels.
b. Bepaal de orde en het teken van σ.
c. Is de ondergroep van S_7 voortgebracht door σ een normaaldeler? Motiveer je antwoord.

Oplossing:
a. De permutatie σ doet het volgende: $1 \to 4 \to 1$, $2 \to 3 \to 6 \to 5 \to 2$ en $7 \to 7$. Dus in cykel-notatie,

$$\sigma = (14)(2365).$$

b. De cykel-type van σ is $(4, 2)$. De orde van σ is dan $\text{kgv}(4, 2) = 4$, en voor het teken $\epsilon(\sigma)$ van σ geldt

$$\epsilon(\sigma) = \epsilon((14))\epsilon((2365)) = (-1)(-1)^3 = 1$$

aangezien het teken van een k-cykel gelijk is aan $(-1)^{k-1}$.
c. De ondergroep

$$\begin{aligned} \langle\sigma\rangle &= \{(1), \sigma, \sigma^2, \sigma^3\} \\ &= \{(1), (14)(2365), (26)(35), (14)(2563)\} \end{aligned}$$

van S_7 voortgebracht door σ is geen normaaldeler van S_7. Om deze bewering te bewijzen is het voldoende om een $\tau \in S_7$ te vinden zodat $\tau\sigma\tau^{-1} \notin \langle\sigma\rangle$. Hiervoor kunnen we bijvoorbeeld gebruik maken van het feit dat $7 \to 7$ voor ieder element van $\langle\sigma\rangle$. Neem dan bijvoorbeeld $\tau = (17) = \tau^{-1}$, dan $\tau\sigma\tau^{-1}(7) = 4$ dus $\tau\sigma\tau^{-1} \notin \langle\sigma\rangle$. We concluderen dus dat $\langle\sigma\rangle$ geen normaaldeler van S_7 is.

Opgave 3.
a. Toon aan dat

$$\{\overline{d} \in \mathbb{Z}/8\mathbb{Z} \mid \langle \overline{d} \rangle = \mathbb{Z}/8\mathbb{Z}\} = \big(\mathbb{Z}/8\mathbb{Z}\big)^*,$$

waarbij $\langle \overline{d} \rangle$ de ondergroep van $\mathbb{Z}/8\mathbb{Z}$ is die voortgebracht wordt door $\overline{d} \in \mathbb{Z}/8\mathbb{Z}$.
b. Bewijs dat

$$\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) := \{\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \mid \phi \text{ groepsisomorfisme}\}$$

een ondergroep is van de groep $S(\mathbb{Z}/8\mathbb{Z})$ van alle bijecties $\mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$.
c. Laat zien dat de groepen $\mathrm{Aut}\big(\mathbb{Z}/8\mathbb{Z}\big)$ en $\big(\mathbb{Z}/8\mathbb{Z}\big)^*$ isomorf zijn.

Oplossing:
a. Er geldt $(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Directe berekening geeft $\langle \overline{d} \rangle = \mathbb{Z}/8\mathbb{Z}$ voor $\overline{d} \in (\mathbb{Z}/8\mathbb{Z})^*$. Bijvoorbeeld,

$$\begin{aligned}\langle \overline{3} \rangle &= \{m\overline{3} = \overline{3m} \mid m \in \mathbb{Z}\} \\ &= \{\overline{3}, \overline{6}, \overline{9} = \overline{1}, \overline{12} = \overline{4}, \overline{15} = \overline{7}, \overline{18} = \overline{2}, \overline{21} = \overline{5}, \overline{24} = \overline{0}\} = \mathbb{Z}/8\mathbb{Z}.\end{aligned}$$

Voor een restklasse $\overline{d} \notin (\mathbb{Z}/8\mathbb{Z})^*$ geldt dat d even is, dus de ondergroep $\langle \overline{d} \rangle$ voortgebracht door $\overline{d}$ bevat slechts restklassen $\overline{d'} \in \mathbb{Z}/8\mathbb{Z}$ met d' even. In dit geval is dus $\langle d \rangle \neq \mathbb{Z}/8\mathbb{Z}$.

Een ander argument toont aan dat het gevraagde waar is voor restklassen modulo k met $k \in \mathbb{N}$ willekeurig. Noteer $X = \{\overline{d} \in \mathbb{Z}/k\mathbb{Z} \mid \langle \overline{d} \rangle = \mathbb{Z}/k\mathbb{Z}\}$. Als $\overline{d} \in X$, dan bestaat er een $m \in \mathbb{Z}$ zodat $m\overline{d} = \overline{md} = \overline{1}$. Met andere woorden, er bestaan $n, m \in \mathbb{Z}$ zodat $m.d + n.k = 1$. Hieruit volgt dat $\mathrm{ggd}(d, k) = 1$, dus $\overline{d} \in (\mathbb{Z}/k\mathbb{Z})^*$. We concluderen dat $X \subseteq (\mathbb{Z}/k\mathbb{Z})^*$.

Als $\overline{d} \in (\mathbb{Z}/k\mathbb{Z})^*$ dan bestaat er een $\overline{m} \in (\mathbb{Z}/k\mathbb{Z})^*$ zodat $\overline{m}\,\overline{d} = \overline{1}$. Met andere woorden, $\overline{1} = m\overline{d} \in \langle \overline{d} \rangle$, dus ook $\overline{n} = n\overline{1} = nm\overline{d} \in \langle \overline{d} \rangle$ voor alle $n \in \mathbb{Z}$. We concluderen dat $(\mathbb{Z}/k\mathbb{Z})^* \subseteq X$. Combineren van beide inclusies geeft $X = (\mathbb{Z}/k\mathbb{Z})^*$.
b. We beargumenteren dat voor willekeurige eindige groep G, $\mathrm{Aut}(G) \subseteq S(G)$ een ondergroep is, waarbij $\mathrm{Aut}(G)$ de verzameling van groepsisomorfismen $\phi : G \to G$ is. Het gevraagde is dan het speciale geval dat $G = \mathbb{Z}/8\mathbb{Z}$.

Het is voldoende aan te tonen dat $\mathrm{Aut}(G) \subseteq S(G)$ een niet-lege deelverzameling is waarvoor geldt dat $\phi^{-1}, \phi\psi \in \mathrm{Aut}(G)$ voor alle $\phi, \psi \in \mathrm{Aut}(G)$. Hierbij zijn ϕ^{-1} en $\phi\psi$ de inverse, respectievelijk het produkt, van de funkties ten opzichte van de groepsbewerking van $S(G)$: dus de bewerking is samenstelling van funkties, met eenheidselement de funktie $\mathrm{Id}(g) = g$ voor alle $g \in G$. Er geldt dat $\mathrm{Id} \in \mathrm{Aut}(G)$, dus $\mathrm{Aut}(G)$ is niet leeg. We weten bovendien dat samenstellingen en inversen van groepsisomorfismen weer groepsisomorfismen zijn. Dus $\mathrm{Aut}(G) \subseteq S(G)$ is een ondergroep.
c. Voor gegeven $\phi \in \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$, noteren we $\overline{d} = \phi(\overline{1}) \in \mathbb{Z}/8\mathbb{Z}$. Dan

$$\phi(\overline{m}) = \phi(m\overline{1}) = m\phi(\overline{1}) = m\overline{d}, \qquad \forall m \in \mathbb{Z},$$

dus het beeld van ϕ is $\langle \overline{d} \rangle$. Maar ϕ is ook surjectief, dus $\langle \overline{d} \rangle = \mathbb{Z}/8\mathbb{Z}$. Vanwege **a** concluderen we dat $\overline{d} \in (\mathbb{Z}/8\mathbb{Z})^*$. We definieren nu een afbeelding

$$\psi : \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \to (\mathbb{Z}/8\mathbb{Z})^*$$

door $\psi(\phi) := \phi(\overline{1})$. Dit is een homomorfisme: neem $\phi, \phi' \in \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ en schrijf $\overline{d} = \phi(\overline{1})$ en $\overline{d'} = \phi'(\overline{1})$. Dan

$$\psi(\phi\phi') = \overline{dd'} = \overline{d} \cdot \overline{d'} = \psi(\phi)\psi(\phi').$$

Het homomorfisme ψ is injectief: als $\phi \in \mathrm{Ker}(\psi)$, dan $\phi(\overline{1}) = \overline{1}$ en

$$\phi(\overline{m}) = \phi(m\overline{1}) = m\phi(\overline{1}) = m\overline{1} = \overline{m}, \qquad \forall m \in \mathbb{Z},$$

dus $\phi = \mathrm{Id}$. Voor $\overline{d} \in (\mathbb{Z}/8\mathbb{Z})^*$ is het eenvoudig in te zien dat $\overline{m} \mapsto \overline{md}$ een groepsisomorfisme $\phi_{\overline{d}} \in \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ definieert, die voldoet aan $\psi(\phi_{\overline{d}}) = \phi_{\overline{d}}(\overline{1}) = \overline{d}$. Dus ψ is ook surjectief. Dus ψ realiseert een groepsisomorfisme $(\mathbb{Z}/8\mathbb{Z})^* \simeq \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$.

Opgave 4. Noteer $D_n = \{r^k \mid k = 0, \ldots, n-1\} \cup \{sr^k \mid k = 0, \ldots, n-1\}$ voor de dihedrale groep (diëdergroep) van orde $2n$. Hierbij is s een spiegeling en r een rotatie over een hoek van $2\pi/n$ zodanig dat $rs = sr^{-1}$.
a. Bepaal het centrum van D_4 en van D_5.
b. Toon aan dat $D_4/Z(D_4)$ isomorf is met de Viergroep V_4 van Klein.
c. Laat zien dat $[D_4, D_4] = Z(D_4)$.
d. Bepaal de commutator ondergroep $[D_5, D_5]$ van D_5.

Oplossing:
a. Het centrum $Z(G)$ van een groep G is

$$Z(G) = \{g \in G \mid gg' = g'g \quad \forall g' \in G\}.$$

In D_n geldt

$$r(sr^k) = sr^{k-1}, \qquad (sr^k)r = sr^{k+1},$$

dus sr^k commuteert met r in D_n als $r^2 = 1$. Maar $r \in D_n$ heeft orde n, dus $sr^k \notin Z(D_n)$ als $n \geq 3$. Er geldt dat $r^k \in Z(D_n) \Leftrightarrow r^k$ commuteert met s. Aangezien $sr^k = r^{-k}s$, geldt dat r^k commuteert met $s \Leftrightarrow r^{2k} = 1 \Leftrightarrow 2k$ is een veelvoud van n. We concluderen in het bijzonder dat $Z(D_4) = \{e, r^2\}$ en $Z(D_5) = \{e\}$.
b. Het centrum van een groep G is een normaaldeler van G. Voor $g \in D_4$ noteren we $\overline{g} = gZ(D_4) = \{g, gr^2\}$ voor de (linker=rechter) nevenklasse van g. Dan $D_4/Z(D_4) = \{\overline{e}, \overline{r}, \overline{s}, \overline{sr}\}$. Het is eenvoudig om de vermenigvuldigingstabel van $D_4/Z(D_4)$ te bepalen. Alle elementen $\neq \overline{e}$ hebben orde 2,

$$\overline{r} \cdot \overline{r} = \overline{r^2} = \overline{e}, \quad \overline{s} \cdot \overline{s} = \overline{s^2} = \overline{e}, \quad \overline{sr} \cdot \overline{sr} = \overline{srsr} = \overline{e}.$$

Verder geldt,

$$\overline{r} \cdot \overline{s} = \overline{rs} = \overline{sr^{-1}} = \overline{sr} = \overline{s} \cdot \overline{r},$$

en analoog $\overline{r} \cdot \overline{sr} = \overline{s} = \overline{sr} \cdot \overline{r}$, $\overline{s} \cdot \overline{r} = \overline{sr} = \overline{r} \cdot \overline{s}$. Dus $D_4/Z(D_4)$ is een abelse groep van orde 4 met dezelfde vermenigvuldigingstabel als die van de Viergroep $V_4 = \{e, a, b, c\}$ van

Klein: een expliciete groepsisomorfisme $D_4/Z(D_4) \simeq V_4$ is bijvoorbeeld: $\overline{e} \mapsto e$, $\overline{r} \mapsto a$, $\overline{s} \mapsto b$ en $\overline{sr} \mapsto c$.

c. Voor een groep G is de commutator ondergroep $[G, G]$ van G de ondergroep voortgebracht door alle commutatoren $[g, h] = ghg^{-1}h^{-1}$ $(g, h \in G)$. We kunnen nu door een directe berekening van alle commutatoren in D_4 inzien dat $[D_4, D_4] = \{e, r^2\}$ (vergelijk met de uitwerking van onderdeel **d**), dus $[D_4, D_4] = Z(D_4)$. We kunnen ook een bewijs geven zonder berekeningen door gebruik te maken van het volgende feit: als N een normaaldeler is van G zodat de quotientgroep G/N abels is, dan $[G, G] \subseteq N$. We weten dat $D_4/Z(D_4)$ abels is (want isomorf met de abelse Viergroep V_4 van Klein), dus $[D_4, D_4] \subseteq Z(D_4) = \{e, r^2\}$. Aangezien D_4 niet abels is, geldt $[D_4, D_4] \neq \{e\}$. De enige resterende mogelijkheid is dus $[D_4, D_4] = \{e, r^2\} = Z(D_4)$.

d. We merken of dat $r^2 \in [D_5, D_5]$, want

$$[r, s] = rsr^{-1}s^{-1} = r^2.$$

Dan $\langle r^2 \rangle = \{e, r^2, r^4, r^6 = r, r^8 = r^3\} = \langle r \rangle \subseteq [D_5, D_5]$. Nu iedere commutator $[g, h]$ $(g, h \in D_5)$ zit bevat in $\langle r \rangle$:

$$[r^k, r^l] = e, \qquad [sr^k, sr^l] = sr^k sr^l r^{-k} sr^{-l} s = r^{2l-2k},$$
$$[r^k, sr^l] = r^k sr^l r^{-k} r^{-l} s = r^{2k}, \qquad [sr^k, r^l] = r^{-2l}.$$

Dus $[D_5, D_5] \subseteq \langle r \rangle$. We concluderen dat $[D_5, D_5] = \langle r \rangle = \{e, r, r^2, r^3, r^4\}$.

Opgave 5. G is een groep met ondergroep H.

a. Bewijs dat de linkernevenklassen van H in G een partitie van G geven.

Voor een deelverzameling $X \subseteq G$ noteren we $\phi_X : X \times H \to G$ voor de afbeelding

$$\phi_X(x, h) := xh, \qquad x \in X,\ h \in H.$$

b. Bewijs dat er deelverzamelingen $X \subset G$ bestaan zodat de bijbehorende afbeelding ϕ_X een bijectie is.

Voor het vervolg van de opgave kiezen we een deelverzameling $X \subset G$ waarvoor ϕ_X een bijectie is.

c. Voor gegeven $h \in H$ en $x \in X$ bestaan er unieke $x' \in X$ en $h' \in H$ zodanig dat $hx = x'h'$. Toon dit aan.

Voor gegeven $h \in H$ en $x \in X$ noteren we $h \circ x \in X$ voor het bijbehorende element $x' \in X$ uit onderdeel **b.**

d. Laat zien dat de afbeelding

$$H \times X \to X, \qquad (h, x) \mapsto h \circ x$$

een linksactie van H op X definieert.
e. Bewijs: $h \circ x = x$ voor alle $h \in H$ en $x \in X \Leftrightarrow H \trianglelefteq G$ is een normaaldeler.

Oplossing:
a. Voor een verzameling X met equivalentie-relatie $\sim$ geldt dat de bijbehorende equivalentie-klassen een partitie van X geven. Dit passen we toe op de equivalentie-relatie $g \sim g' \Leftrightarrow g^{-1}g' \in H$ op G. Het gewenste resultaat volgt dan uit het feit dat de equivalentie-klassen de linkernevenklassen van H in G zijn.
b. Neem voor X een volledige set representanten van de linkernevenklassen van H in G. Per definitie geldt dan dat iedere $g \in G$ een unieke schrijfwijze $g = xh$ heeft met $x \in X$ en $h \in H$. Met andere woorden, de afbeelding $\phi_X : X \times H \to G$, $\phi_X(x, h) := xh$ is bijectief.
c. Neem $x \in X$ en $h \in H$, dan $hx \in G$. Dan $(x', h') = \phi_X^{-1}(hx) \in X \times H$ is het unieke paar zodat $x'h' = \phi_X(x', h') = hx$.
d. We moeten aantonen dat $e \circ x = x$ voor alle $x \in X$ en dat $(gh) \circ x = g \circ (h \circ x)$ voor alle $g, h \in H$ en $x \in X$. Aangezien $ex = x = xe$ in G geldt dat $e \circ x = x$ voor alle $x \in X$. Voor $g, h \in H$ en $x \in X$ geldt aan de ene kant dat$(gh)x = ((gh) \circ x)v$ voor een unieke $v \in H$. We noteren $g', h' \in H$ zodat $hx = (h \circ x)h'$ en $g(h \circ x) = (g \circ (h \circ x))g'$. Dan geldt aan de andere kant dat

$$g(hx) = (g \circ (h \circ x))g'h'.$$

Aangezien ϕ_X een bijectie is, volgt uit

$$\phi_X(g \circ (h \circ x), g'h') = g(hx) = (gh)x = \phi_X((gh) \circ x, v)$$

dat $(gh) \circ x = g \circ (h \circ x)$.
e. Er geldt: $h \circ x = x$ voor alle $h \in H$ en $x \in X \Leftrightarrow x^{-1}hx \in H$ voor alle $x \in X$ en $h \in H$ $\Leftrightarrow g^{-1}hg \in H$ voor alle $g \in G$ en $h \in H$. Voor de laatste equivalentie volgt "$\Rightarrow$" door op te merken dat iedere $g \in G$ geschreven kan worden als $g = xh'$ met $x \in X$ en $h' \in H$, dus

$$g^{-1}hg = (h')^{-1}x^{-1}hxh' \in (h')^{-1}Hh' = H.$$

We concluderen dus dat $h \circ x = x$ voor alle $h \in H$ en $x \in X \Leftrightarrow ghg^{-1} \in H$ voor alle $g \in G$ en $h \in H \Leftrightarrow H$ is een normaaldeler van G.