Uitwerkingen tussentoets Algebra 1

- Datum: 24 maart, 2009.
- Tijd: 09:00-12:00.
- Vergeet niet je naam en studentnummer te noteren op het werk dat je inlevert.
- Formuleer zorgvuldig alle resultaten die je gebruikt.
- Beargumenteer zorgvuldig hoe je tot de oplossingen van de opgaven bent gekomen. Slechts het geven van het correcte antwoord is niet voldoende.
- De tussentoets bestaat uit vier opgaven.
- Veel succes!

Opgave 1. **(a)** Laat zien dat $\text{ggd}(42, 55) = 1$.

(b) Noteer $\overline{42}$ voor de restklasse van 42 modulo 55. Bepaal de inverse van $\overline{42}$ in de multiplicatieve groep $\left(\mathbb{Z}/55\mathbb{Z}\right)^*$ van restklassen modulo 55.

(c) Bepaal een $x \in \mathbb{Z}$ die voldoet aan

(i) de congruenties

$$\begin{aligned} x &\equiv 0 \pmod{42}, \\ x &\equiv 110 \pmod{55}. \end{aligned}$$

(ii) de congruenties

$$\begin{aligned} x &\equiv 2 \pmod{42}, \\ x &\equiv 1 \pmod{55}. \end{aligned}$$

(d) Bepaal de orde van $\overline{2}$ in $\left(\mathbb{Z}/55\mathbb{Z}\right)^*$.

Oplossing. **(a)** De priemontbindingen zijn $42 = 2 \cdot 3 \cdot 7$ en $55 = 5 \cdot 11$. Aangezien 42 en 55 geen priemfactoren gemeen hebben, geldt $\text{ggd}(42, 55) = 1$.

(b) Hiervoor bepalen we met het algorithme van Euclides eerst getallen $x, y \in \mathbb{Z}$ zodat $1 = x \cdot 42 + y \cdot 55$:

$$\begin{aligned} 55 &= 0 \cdot 42 + 1 \cdot 55 \\ 42 &= 1 \cdot 42 + 0 \cdot 55 \\ 13 &= -1 \cdot 42 + 1 \cdot 55 \\ 3 &= 4 \cdot 42 - 3 \cdot 55 \\ 1 &= -17 \cdot 42 + 13 \cdot 55, \end{aligned}$$

dus bijvoorbeeld $x = -17$ en $y = 13$. Dan geldt $\overline{42}^{-1} = \overline{-17} = \overline{38}$.

(c) **(i)** De congruenties die we moeten oplossen kunnen geschreven worden als $x \equiv 0 (\text{mod } 42)$ en $x \equiv 0 (\text{mod } 55)$, aangezien 110 een 55-voud is. Dus $x = 0$ is een oplossing.

(ii) We hebben eerder al gezien dat $1 = -17 \cdot 42 + 13 \cdot 55$. De congruenties $x \equiv 2 (\text{mod } 42)$ en $x \equiv 1 (\text{mod } 55)$ worden dan dus opgelost door $x = 1 \cdot (-17) \cdot 42 + 2 \cdot 13 \cdot 55 = 1 + 13 \cdot 55 = 716$.

(d) De Chinese reststelling (in multiplicatieve vorm) zegt dat de toekenning

$$x(\text{mod } 55) \mapsto \big(x(\text{mod } 5), x(\text{mod } 11)\big)$$

een isomorfisme $\big(\mathbb{Z}/55\mathbb{Z}\big)^* \to \big(\mathbb{Z}/5\mathbb{Z}\big)^* \times \big(\mathbb{Z}/11\mathbb{Z}\big)^*$ definieert. De orde van $2(\text{mod } 5) \in \big(\mathbb{Z}/5\mathbb{Z}\big)^*$ is 4 (door direct na te gaan dat $m = 4$ het kleinste natuurlijke getal is zodat $2^m(\text{mod } 5) = 1(\text{mod } 5)$). De orde van $2(\text{mod } 11) \in \big(\mathbb{Z}/11\mathbb{Z}\big)^*$ is 10. Met behulp van de Chinese reststelling concluderen we dan dat de orde van $2(\text{mod } 55) \in \big(\mathbb{Z}/55\mathbb{Z}\big)^*$ gelijk is aan $\text{kgv}(4, 10) = 20$.

Opgave 2. **(a)** Schrijf

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 4 & 5 & 3 & 2 & 8 & 6 \end{pmatrix} \in S_8$$

als produkt van disjunkte cykels.

(b) Bepaal de orde van σ.

(c) Vind een $\tau \in S_8$ zodat $\sigma\tau \neq \tau\sigma$.

(d) Bepaal het teken $\epsilon(\sigma)$ van σ.

(e) Kan σ geschreven worden als produkt van 3-cykels? Zo ja, geef dan een expliciete schrijfwijze van σ als produkt van 3-cykels.

Oplossing. **(a)** $\sigma = (1\,7\,8\,6\,2)(3\,4\,5)$.

(b) De orde van een k-cykel is k. De permutatie σ kan geschreven worden als een produkt van een (onderling disjunkte) 5-cykel en een 3-cykel (zie **(a)**), dus de orde van σ is $\text{kgv}(5, 3) = 15$.

(c) Neem bijvoorbeeld $\tau = (1\,3)$. Dan $(\sigma\tau)(1) = \sigma(3) = 4$ en $(\tau\sigma)(1) = \tau(7) = 7$, dus $\sigma\tau \neq \tau\sigma$.

(d) Het teken van een k-cykel is $(-1)^{k-1}$. Omdat de tekenafbeelding een groephomomorfisme is, volgt dan dat $\epsilon(\sigma) = \epsilon((1\,7\,8\,6\,2))\epsilon((3\,4\,5)) = (-1)^4(-1)^2 = 1$.

(e) Vanwege **(d)** geldt dat $\sigma \in A_8$ (de alternerende groep), dus σ kan geschreven worden als produkt van 3-cykels. Zo een schrijfwijze kunnen we makkelijk krijgen door de 5-cykel $(1\,7\,8\,6\,2)$ te schrijven als produkt van 3-cykels,

$$(1\,7\,8\,6\,2) = (1\,7\,8)(8\,6\,2),$$

waarmee (vanwege onderdeel **(a)**) we de schrijfwijze $\sigma = (1\,7\,8)(8\,6\,2)(3\,4\,5)$ van σ krijgen als produkt van 3-cykels.

Opgave 3. In deze opgave noteren we $x(\text{mod } m)$ voor de restklasse van $x \in \mathbb{Z}$ modulo $m \in \mathbb{N}$.

(a) Laat zien dat er geen afbeelding $\mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ bestaat die $x(\text{mod } 8)$ stuurt naar $x(\text{mod } 3)$ voor alle $x \in \mathbb{Z}$.

(b) Toon aan dat de volgende afbeeldingen goedgedefinieerd zijn.

(i) $\mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, gedefinieerd door $x(\text{mod } 8) \mapsto 0(\text{mod } 3)$ als x even is, en $x(\text{mod } 8) \mapsto 1(\text{mod } 3)$ als x oneven is.

(ii) $\mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, gegeven door $x(\text{mod } 24) \mapsto x(\text{mod } 3)$.

(iii) $\left(\mathbb{Z}/24\mathbb{Z}\right)^* \to \left(\mathbb{Z}/3\mathbb{Z}\right)^*$, gegeven door $x(\text{mod } 24) \mapsto x(\text{mod } 3)$.

(c) Ga na welke van de afbeeldingen uit onderdeel **(b)** groepshomomorfismen zijn.

(d) Bepaal de kern van deze groepshomomorfismen.

Oplossing. **(a)** Het voldoet om een voorbeeld te geven van een restklasse $x(\text{mod } 3) \in \mathbb{Z}/3\mathbb{Z}$ die afhankelijk is van een keuze van representant x van de bijbehorende restklasse $x(\text{mod } 8)$. Bijvoorbeeld: 0 en 8 zijn beiden representanten van de restklasse $0(\text{mod } 8)$, maar

$$0(\text{mod } 3) \neq 8(\text{mod } 3)$$

want 8 is niet deelbaar door 3.

(b) **(i)** De elementen in de restklasse $x(\text{mod } 8)$ zijn allemaal even als x even is, en allemaal oneven als x oneven is. Hieruit volgt dat de toekenningen $x(\text{mod } 8) \mapsto 0(\text{mod } 3)$ als x even is, en $x(\text{mod } 8) \mapsto 1(\text{mod } 3)$ als x oneven is, niet van de keuze van de representant van de restklasse $x(\text{mod } 8)$ afhangen. De afbeelding is dus goedgedefinieerd.

(ii) We moeten in dit geval aantonen dat de restklasse $x(\text{mod } 3)$ niet afhangt van de keuze van representant x van de bijbehorende restklasse $x(\text{mod } 24)$. Als $x(\text{mod } 24) = y(\text{mod } 24)$ dan deelt 24 het verschil $x - y$. Dan deelt ook 3 het verschil $x - y$, immers 3 deelt 24. Dus $x(\text{mod } 3) = y(\text{mod } 3)$.

(iii) Vanwege onderdeel **(ii)** weten we al dat het een goedgedefinieerde afbeelding $\left(\mathbb{Z}/24\mathbb{Z}\right)^* \to \mathbb{Z}/3\mathbb{Z}$ oplevert. We moeten alleen nog aantonen dat het beeld bevat is in $\left(\mathbb{Z}/3\mathbb{Z}\right)^*$. Als $x(\text{mod } 24) \in \left(\mathbb{Z}/24\mathbb{Z}\right)^*$ dan geldt $\text{ggd}(24, x) = 1$. Aangezien 3 een deler is van 24 volgt dat $\text{ggd}(3, x) = 1$, dus $x(\text{mod } 3) \in \left(\mathbb{Z}/3\mathbb{Z}\right)^*$.

(c) We noteren de afbeelding in elk van de 3 onderdelen van de opgave met ϕ.

(i) Dit is geen groepshomorfisme. Bijvoorbeeld

$$\phi(1(\text{mod } 8) + 1(\text{mod } 8)) = \phi(2(\text{mod } 8)) = 0(\text{mod } 3),$$

want niet gelijk is aan

$$\phi(1(\text{mod } 8)) + \phi(1(\text{mod } 8)) = 1(\text{mod } 3) + 1(\text{mod } 3) = 2(\text{mod } 3).$$

(ii) Dit is een groepshomomorfisme, want voor $x, y \in \mathbb{Z}$ geldt,

$$\begin{aligned}\phi(x(\text{mod } 24) + y(\text{mod } 24)) &= \phi((x + y)(\text{mod } 24)) \\ &= (x + y)(\text{mod } 3) \\ &= x(\text{mod } 3) + y(\text{mod } 3) \\ &= \phi(x(\text{mod } 24)) + \phi(y(\text{mod } 24)).\end{aligned}$$

(iii) Dit is een groepshomomorfisme, want voor $x, y \in \mathbb{Z}$ met $\text{ggd}(x, 24) = 1 = \text{ggd}(y, 24)$ geldt,

$$\begin{aligned}\phi(x(\text{mod } 24) \cdot y(\text{mod } 24)) &= \phi(xy(\text{mod } 24)) \\ &= xy(\text{mod } 3) \\ &= x(\text{mod } 3) \cdot y(\text{mod } 3) \\ &= \phi(x(\text{mod } 24)) \cdot \phi(y(\text{mod } 24)).\end{aligned}$$

(d) We houden de notatie ϕ aan voor de afbeelding in onderdeel **(ii)** en **(iii)** van onderdeel **(b)**.

(ii) De kern $\text{Ker}(\phi)$ van de groepshomomorfisme ϕ is

$$\begin{aligned}\text{Ker}(\phi) &= \{x(\text{mod } 24) \mid x(\text{mod } 3) = 0(\text{mod } 3)\} \\ &= \{x(\text{mod } 24) \mid x = 0, 3, 6, 9, 12, 15, 18, 21\}.\end{aligned}$$

(iii) De kern $\text{Ker}(\phi)$ van de groepshomomorfisme ϕ is in dit geval

$$\begin{aligned}\text{Ker}(\phi) &= \{x(\text{mod } 24) \mid \text{ggd}(x, 24) = 1 \ \& \ x(\text{mod } 3) = 1(\text{mod } 3)\} \\ &= \{x(\text{mod } 24) \mid x = 1, 7, 13, 19\}.\end{aligned}$$

Ga na: $\text{Ker}(\phi)$ is isomorf met de Viergroep van Klein.

Opgave 4. In deze opgave is G een eindige groep, en $g \in G$ is een willekeurig groepselement.

(a) Wat is de groepsbewerking en eenheidselement van de groep $S(G)$ van bijecties $G \to G$?

(b) Laat zien dat

$$\text{Aut}(G) := \{\phi \in S(G) \mid \phi \ \text{ automorfisme van } G\}$$

een ondergroep is van $S(G)$.

(c) Als $\phi \in \text{Aut}(G)$ dan is de orde van $\phi(g)$ gelijk aan de orde van g. Toon dit aan.

(d) Geef een voorbeeld van een groep G, een groepselement $g \in G$, en een $\phi \in S(G)$ zodat de orde van $\phi(g)$ **niet** gelijk is aan de orde van g.

Oplossing. **(a)** Het eenheidselement is Id_G, de afbeelding die g naar g stuurt voor alle $g \in G$. De groepsbewerking is samenstelling van afbeeldingen: als $\phi, \psi \in S(G)$, dan is $\phi \circ \psi$ de afbeelding van G naar G gedefinieerd door

$$(\phi \circ \psi)(g) := \phi(\psi(g)), \qquad \forall\, g \in G.$$

(b) $\text{Id}_G \in \text{Aut}(G)$, dus $\text{Aut}(G)$ is niet leeg. Het voldoet dan om aan te tonen dat $\phi \circ \psi \in \text{Aut}(G)$ en $\phi^{-1} \in \text{Aut}(G)$ als zowel $\phi \in \text{Aut}(G)$ en $\psi \in \text{Aut}(G)$. We weten dat $\phi \circ \psi \in S(G)$ en $\phi^{-1} \in S(G)$, dus het voldoet aan te tonen dat beide

afbeeldingen groepshomomorfismen zijn. Voor $g, h \in G$ geldt

$$\begin{aligned}(\phi \circ \psi)(gh) &= \phi(\psi(gh)) \\ &= \phi(\psi(g)\psi(h)) \\ &= \phi(\psi(g))\phi(\psi(h)) \\ &= (\phi \circ \psi)(g)(\phi \circ \psi)(h),\end{aligned}$$

dus $\phi \circ \psi \in \mathrm{Aut}(G)$. Noteer $x, y \in G$ zodat $\phi(x) = g$ en $\phi(y) = h$. Dan geldt

$$\begin{aligned}\phi^{-1}(gh) &= \phi^{-1}(\phi(x)\phi(y)) \\ &= \phi^{-1}(\phi(xy)) \\ &= xy = \phi^{-1}(g)\phi^{-1}(h),\end{aligned}$$

dus $\phi^{-1} \in \mathrm{Aut}(G)$.

(c) Laat e het eenheidselement van G zijn. Noteer m voor de orde van $g \in G$ en n voor de orde van $x := \phi(g) \in G$. Dan

$$x^m = (\phi(g))^m = \phi(g^m) = \phi(e) = e,$$

dus $n \leq m$. Aan de andere kant

$$g^n = (\phi^{-1}(x))^n = \phi^{-1}(x^n) = \phi^{-1}(e) = e,$$

dus $m \leq n$. Combineren van de twee ongelijkheden geeft $m = n$.

(d) Bijvoorbeeld $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ gedefinieerd door $\phi(0 (\mathrm{mod}\ 3)) = 2 (\mathrm{mod}\ 3)$, $\phi(1 (\mathrm{mod}\ 3)) = 1 (\mathrm{mod}\ 3)$ en $\phi(2 (\mathrm{mod}\ 3)) = 0 (\mathrm{mod}\ 3)$ is een bijectie maar geen groepsisomorfisme. $2 (\mathrm{mod}\ 3) \in \mathbb{Z}/3\mathbb{Z}$ heeft orde 3 maar $\phi(2 (\mathrm{mod}\ 3)) = 0 (\mathrm{mod}\ 2)$ heeft orde 1.