Voorbeeldoplossingen Tussentijdse Toets

1. (a) We geven eerst de definitie van een deelgroep van een groep $G, *$.
Zij $G, *$ een groep en $H \subset G$. We zeggen dat H een deelgroep is van G als
(i) $e \in H$,
(ii) $\forall x, y \in H : x * y \in H$ *en*
(iii) $\forall x \in H : x^{-1} \in H$.
Uiteraard is het neutraal element in $\mathrm{GL}_2(\mathbb{R})$ de eenheidsmatrix

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Bovendien weten we dat het product van twee matrices en de inverse van een matrix in $\mathrm{GL}_2(\mathbb{R})$ gegeven wordt als volgt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{1}$$

Dat U, B en D deelgroepen zijn van $\mathrm{GL}_2(\mathbb{R})$ is nu duidelijk, immers I_2 behoort tot U, B en D per definitie van deze deelverzamelingen. De restrictie op de matrixelementen bij U, B en D, zal samen met (1) er voor zorgen dat zowel het product van twee elementen als de inverse van een element van één van de drie verzamelingen weer tot de respectievelijke verzameling zal horen.

(b) Stel dat

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

orde twee heeft, dan is dus met behulp van (1)

$$\begin{pmatrix} a^2 & ab + bd \\ 0 & d^2 \end{pmatrix} = I_2,$$

of met andere woorden we hebben volgende vergelijkingen

$$\begin{cases} 1 &= a^2 \\ 1 &= d^2 \\ 0 &= ab + bd \end{cases}$$

Met andere woorden $a = \pm 1$ en $d = \pm 1$. Stel $a = d = \pm 1$, dan is $2ab = 0$, dus $b = 0$. Stel dat $a = -d = \pm 1$, dan is de derde vergelijking steeds voldaan. Met andere woorden de elementen van orde twee zijn

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \left\{ \begin{pmatrix} \pm 1 & b \\ 0 & \mp 1 \end{pmatrix}, \middle| \, b \in \mathbb{R} \right\}.$$

(c) We geven eerst de definitie van een homo- en isomorfisme van groepen $G, *$ en $H, \square$.
Een groepshomomorfisme $f : G \to H$ is een afbeelding $f : G \to H$ zodat

$$\forall x, y \in G : f(x * y) = f(x) \square f(y).$$

Een groepshomomorfisme is een groepsisomorfisme als f een inverse heeft, dus een groepshomomorfisme $g : H \to G$ zodat $f \circ g$ de indentieke afbeelding op H is en zodat $g \circ f$ de identieke afbeelding op G is. In de cursus is bewezen dat deze voorwaarde equivalent is met het bijectief zijn van het groepsmorfisme f.
We definiëren dan een morfisme

$$\varphi : \mathbb{R}, + \to U : b \mapsto \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Dit is is inderdaad een groepsmorfisme omdat voor $b, b' \in \mathbb{R}$ geldt dat

$$\varphi(b + b') = \begin{pmatrix} 1 & b + b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \varphi(b)\varphi(b').$$

en aangezien dit groepsmorfisme overduidelijk injectief en surjectief is, hebben we dus een isomorfisme geconstrueerd tussen U en $\mathbb{R}, +$.

(d) *Zij $G_1, \ldots, G_n$ groepen met respectievelijke bewerkingen $*_1, \ldots, *_n$, dan is het direct product van deze groepen gegeven door*

$$G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i \text{ voor } i = 1, \ldots, n\}$$

met als bewerking $*$ gedefinieerd als

$$(g_1, \ldots, g_n) * (g_1', \ldots, g_n') = (g_1 *_1 g_1', \ldots, g_n * g_n'),$$

waarbij $g_i, g_i' \in G_i$ voor $i = 1, \ldots, n$.
We tonen dan aan dat $D \cong (\mathbb{R}_0, \cdot) \times (\mathbb{R}_0, \cdot)$. Immers we definieren

$$\psi : (\mathbb{R}_0, \cdot) \times (\mathbb{R}_0, \cdot) \to D : (a, d) \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Dit is een groepsmorfisme omdat voor $a, a', d, d' \in \mathbb{R}$ geldt dat

$$\begin{aligned} \psi((a, d) \cdot (a', d')) &= \psi((aa', dd')) = \begin{pmatrix} aa' & 0 \\ 0 & dd' \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ 0 & d' \end{pmatrix} \\ &= \psi((a, d))\psi((a', d')). \end{aligned}$$

Dit is duidelijk een injectief groepsmorfisme. Dat dit ook surjectief is, volgt omdat D enkel inverteerbare diagonaalmatrices bevat en die hebben geen nullen op de diagonaal, anders zou immers hun determinant 0 zijn en zouden ze niet inverteerbaar zijn.

(e) Deze uitspraak is vals, omdat het rechterlid eindig veel elementen van orde 2 bevat, namelijk $(\pm 1, \pm 1, 0), (\pm 1, \pm 1, 0)$, en D er oneindig veel heeft (zie (b)). Maar onder groepsisomorfisme wordt het aantal elementen van een gegeven orde steeds bewaard, dus kunnen deze groepen niet isomorf zijn. Dat de gegeven elementen de enige elementen van orde 2 zijn in $(\mathbb{R}_0, \cdot) \times (\mathbb{R}_0, \cdot) \times (\mathbb{R}, +)$, is omdat als we een element (a, b, c) hierin van orde twee hebben, dan moet $(a^2, b^2, 2c) = (1, 1, 0)$ (immers $(1, 1, 0)$ is het neutraal element in deze productgroep) en dus krijgen we de gestelde 4 mogelijkheden.

2. (a) *Zij X een verzameling met een rechteractie van de groep G. Zij $x \in X$. Dan is de baan van x onder G gedefinieerd als*

$$xG := \{xg \mid g \in G\}.$$

(b) We bewijzen dat

$$xG = \{x' \in X \mid x'G = xG\}.$$

Noem de rechterverzameling met A. We tonen dan eerst aan dat $xG \subset A$. Stel dus dat $y \in xG$, dan is $y = xg$ voor een zekere $g \in G$. Maar dan geldt voor elke $g' \in G$ dat $yg = (xg)g' = x(gg') \in xG$. Met andere woorden $yG \subset xG$. Omdat uit $y = xg$ volgt dat $yg^{-1} = (xg)g^{-1} = x(gg^{-1}) = x$, zal op analoge manier ook volgen dat $xG \subset yG$. **(Hier gebruiken we dat elk element in G een inverse heeft.)** Bijgevolg is dus $xG = yG$ en dus is $y \in A$. Daarom is dus $xG \subset A$.
Zij vervolgens $y \in A$, dan is dus $xG = yG$. Maar $y = ye \in yG = xG$, dus er is een $g \in G$ zodat $y = xg$. Bijgevolg is $y \in xG$ en dus is $A \subset xG$.
We besluiten dus dat $A = xG$.

(c) Uiteraard ligt elk element van X in een baan, namelijk zijn eigen baan. Bovendien is uiteraard geen enkele baan leeg, want een baan xG bevat zeker x. We gebruiken het lemma om aan te tonen dat twee verschillende banen elkaar niet snijden. Stel immers dat $y \in xG \cap x'G$ voor $x, x' \in G$. Dan volgt uit het lemma dat de baan van y gelijk aan de baan van x en van x', dus is $xG = yG = x'G$. Daarmee hebben we aangetoond dat twee verschillende banen disjunct zijn.

(d) Omdat $x + 0 = x$ en $x + (n + m) = (x + n) + m$ voor elke $x \in \mathbb{R}, +$ en $n, m \in \mathbb{N}$, voldoet deze afbeelding aan alle eigenschappen van groepsactie, behalve het feit dat $\mathbb{N}$ geen groep vormt met de optelling. Voor $x \in \mathbb{R}$ is dan de 'baan' van x onder $\mathbb{N}$

$$x + \mathbb{N} = \{x + n \mid n \in \mathbb{N}\} = \{x, x + 1, x + 2, \ldots\}. \tag{2}$$

In dit geval vormen de 'banen' geen partitie, immers bijvoorbeeld $0 + \mathbb{N} \neq 1 + \mathbb{N}$, want volgens (2) is $0 \in 0 + \mathbb{N}$, maar $0 \notin 1 + \mathbb{N}$. Maar

$$0 + \mathbb{N} \cap 1 + \mathbb{N} = 1 + \mathbb{N} \neq \emptyset.$$

(e) *Voor het modelantwoord hiervan verwijzen we naar de cursustekst p.22, waar dit helemaal uitgewerkt staat. We herhalen dit hier niet. Opmerking: Voorgaande zinnen zijn geen geldig antwoord op een examen.*

3. (a) We leiden dadelijk af dat $x = \bar{5}^{-1} \cdot \bar{3}$. We zoeken dus $\bar{5}^{-1} \in \mathbb{Z}/7\mathbb{Z}, \cdot$. Dit kunnen we doen door Bezout-Bachet te gebruiken of door te 'gokken'. We zien alleszins dat $\bar{5} \cdot \bar{3} = \bar{1}$, dus $\bar{5}^{-1} = \bar{3}$ en $x = \bar{9} = \bar{2}$.

(b) Uit $x^{23} = \bar{6}$ halen we dadelijk dat $x \neq \bar{0}$ omdat $\mathbb{Z}/7\mathbb{Z}$ een veld is en dus geen nuldelers bevat.
Nu is $23 \equiv -1 \mod 6$ met $6 = \varphi(7)$, dus de congruentie van Euler geeft ons dat $x^{23} = x^{-1}$ in $\mathbb{Z}/7\mathbb{Z}$. We kunnen de congruentie van Euler toepassen omdat $\gcd(7, x) = 1$, immers $\bar{x} \neq 0$. We zoeken dus x zodat $x^{-1} = \bar{6}$ ofnog $x = \bar{6}^{-1}$ We zoeken dus $\bar{6}^{-1} \in \mathbb{Z}/7\mathbb{Z}, \cdot$. Maar $\bar{6} = \overline{-1}$, dus $\bar{6}^{-1} = \bar{6}$ en dus $x = \bar{6}$.

4. (a) $15x + 24y = 3$ is in $\mathbb{Z} \times \mathbb{Z}$ equivalent met $5x + 8y = 1$. Een resultaat (gevolg 2.4) uit de cursus leert ons dat dit een oplossing heeft omdat $\gcd(5, 8) = 1$. Bovendien

kunnen we aantonen dat als (x_0, y_0) één oplossing is, dat dan alle oplossingen gegeven zijn door

$$V := \{(x_0 + 8k, y_0 - 5k) \mid k \in \mathbb{Z}\}.$$

Immers voor een $k \in \mathbb{Z}$ is dan inderdaad $(x_0 + 8k, y_0 - 5k)$ ook een oplossing want

$$5(x_0 + 8k) + 8(y_0 - 5k) = 5x_0 + 8y_0 = 1.$$

Dus alle elementen van V zijn oplossingen. Omgekeerd, gesteld dat we een oplossing $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ hebben, weten we dat

$$0 = (5x_0 + 8y_0) - (5x_1 + 8y_1) = 5(x_0 - x_1) + 8(y_0 + y_1).$$

Dus $5(x_0 - x_1) = -8(y_0 - y_1)$, bijgevolg $5|8(y_0 - y_1)$, maar dan is $5|(y_0 - y_1)$. Bijgevolg is er een $k \in \mathbb{Z}$ zodat $5k = y_0 - y_1$. We verkrijgen dus dat $5(x_0 - x_1) = -40k$, of $x_0 - x_1 = -8k$. Bijgevolg is $(x_1, y_1) = (x_0 + 8k, y_0 - 5k)$ en dus inderdaad een element van V.
We zoeken dus nog één oplossing van deze vergelijking en die vinden we met het algoritme van Euclides of door te 'gokken'. We zien immers met een beetje combineren dat $5 \cdot (-3) + 8 \cdot 2 = 1$. Bijgevolg worden alle oplossingen gegeven door

$$\{(-3 + 8k, 2 - 5k) \mid k \in \mathbb{Z}\}.$$

(b) Dit valt op te lossen met de Chinese reststelling. We zoeken dan eerst gehele b_1 en b_2 zodat $8b_1 \equiv 1 \mod 3$ en $3b_2 \equiv 1 \mod 8$. We kunnen deze vinden met Bezout-Bachet maar ook op het zicht. Neem namelijk $b_1 = 2$ en $b_2 = 3$. Het bewijs van de Chinese reststelling geeft dan dat $x = 2 \cdot 2 \cdot 8 + 7 \cdot 3 \cdot 3 = 95$ een oplossing is. Alle oplossingen zijn dan (volgens de Chinese reststelling) gegeven door

$$\{95 + 24k \mid k \in \mathbb{Z}\} = \{23 + 24k \mid k \in \mathbb{Z}\}.$$