Samenvatting

Algebra 1 - Collegejaar 2013-2014

Dictaat algebra 1

Disclaimer

ALGEBRA 1 - SAMENVATTING

1. Hoofdstuk 1 (+ opgaven)

1.1. **Commuteren.** Twee elementen a en b commuteren als de samenstellingen $a \circ b$ en $b \circ a$ gelijk zijn.

1.2. **Cykelnotatie.** Een permutatie kan worden weergegeven met de cykelnotatie, waarbij ieder punt wordt afgebeeld op het volgende punt in de cykel. De cykel $(ABCD)$ staat dus voor de permutatie $A \mapsto B \mapsto C \mapsto D \mapsto A$.

1.3. **Isomorfisme.** Een bijectie $f\colon A \to B$ is een isomorfisme als hij de bewerking in B hetzelfde houdt als in A. In dit geval zijn A en B isomorf.

1.4. **Kristallografische groepen.** Kristallografische groepen zijn symmetrieverzamelingen op ruimtelijke structuren.

1.5. **Orde.** De orde van een bewerking is het aantal keer dat je de bewerking met zichzelf moet vermenigvuldigen om de identiteit te krijgen.

1.6. **Pariteitsargument.** Methode om iets aan te tonen door twee gevallen te beschouwen: even en oneven getallen.

1.7. **Permutatie.** Een permutatie van een verzameling is een bijectieve afbeelding van een verzameling naar zichzelf. Voor een verzameling met n elementen, bestaan er $n!$ verschillende permutaties. De verzameling S_n is de verzameling van al deze permutaties.

1.8. **Permutatie opdelen in transposities.** Iedere permutatie σ van een eindige verzameling X is een product van transposities.

1.9. **Permutaties uit S_4.** Ieder element van S_4 kan als een product van niet meer dan 3 transposities worden geschreven.

1.10. **Samenstelling symmetrieën.** De samenstelling van 2 symmetrieën is weer een symmetrie.

1.11. **Symmetrieën.** Een symmetrie van een vlakke figuur is een afbeelding van het vlak naar zichzelf die onderlinge afstanden tussen punten bewaart en de gegeven figuur in zichzelf overvoert. Voorbeelden zijn:

- id = identiteit = triviale symmetrie waarbij niets verandert
- s_x = spiegeling in de x-as = $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- s_y = spiegeling in de y-as = $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
- h = draai van 180° om de oorsprong = $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
- r = rotatie van 90° om de oorsprong
- r^3 = rotatie van 270° om de oorsprong

- $s_{y=x}$ = spiegeling in de lijn $y = x$
- $s_{y=-x}$ = spiegeling in de lijn $y = -x$

Verzamelingen van symmetrieën zijn:

- $V_4 = \{\text{symmetrieën van de ruit}\} = \{\text{id}, s_x, s_y, h\}$
- $D_4 = \{\text{symmetrieën van het vierkant}\} = \{\text{id}, r, h, r^3, s_x, s_y, s_{y=x}, s_{y=-x}\}$
- $S_4 = \{\text{symmetrieën van de tetraëder}\} = \{\text{alle mogelijke permutaties op een verzameling van 4 elementen}\}$

1.12. **Symmetrisch verschil.** Het symmetrisch verschil van twee verzamelingen A en B is gedefinieerd als $A\Delta B = (A \cup B)\backslash(A \cap B)$

1.13. **Transpositie.** Een transpositie is een permutatie die twee elementen verwisselt (en alle andere op hun plaats laat).

1.14. **Viergroep van Klein.** Een viergroep van Klein is:
Een verzameling met daarin een triviaal element en 3 elementen van orde 2, waarvan de samenstelling van twee verschillende elementen steeds het derde is.

1.15. **Voortbrengen.** Als alle elementen van een groep gemaakt kunnen worden door samenstellingen van één of meerdere elementen uit een deelverzameling hiervan, dan wordt de groep voortgebracht door de elementen uit deze deelverzameling.

2. Hoofdstuk 2 (+ opgaven)

2.1. **Abelse groepen.** Een abelse groep is een groep G waarin alle elementen met elkaar commuteren (dus voor elke $a, b \in G$ geldt $ab = ba$).

2.2. **De alternerende groep.** De alternerende groep A_n is de ondergroep van S_n met alle even permutaties uit S_n. Deze groep A_n wordt voortgebracht door de 3-cykels uit S_n. De orde van A_n is $\frac{1}{2}n!$ voor alle $n \geq 2$.

2.3. **Bewerking/compositievoorschrift.** Een bewerking/compositievoorschrift op een verzameling G is een afbeelding $G \text{ x } G \to G$, $(a, b) \mapsto a \circ b$, ofwel een functie die aan elk geordend paar (a, b) van elementen uit G een compositie/samenstelling $a \circ b$ toekent. In plaats van $a \circ b$ wordt ook vaak gewoon ab geschreven, de samenstelling wordt dan vaak het product genoemd.

2.4. **Commutator.** De commutator van twee elementen $a, b \in G$ is het element $[a, b] = aba^{-1}b^{-1}$. Hierbij geldt $ab = [a, b]ba$. Daarnaast geldt: a en b commuteren $\iff [a, b] = e$.

2.5. **Conjugatieklassen.** De conjugatieklasse van $x \in G$ is de verzameling van alle elementen in G die geconjugeerd zijn met x.

2.6. **Conjugatieklassen abelse groep.** Voor een eindige groep G geldt:
Alle conjugatieklaasen van G hebben evenveel elementen $\iff G$ is abels

2.7. **Cyclische groep.** Een groep die wordt voortgebracht door 1 element $a \in G$ heet een cyclische groep. De cyclische groep $\langle a \rangle$ heeft dezelfde orde als het element a.

2.8. **Cykeltype.** Het cykeltype van $\sigma \in S_n$ is de reeks van de lengtes van alle cykels in de disjuncte cykelrepresentatie. De som van alle getallen uit deze reeks (dus de totale lengte van de cykels) is gelijk aan n.

2.9. **Dekpunt.** Een element in een baan van lengte 1 wordt door σ op zijn plaats gelaten en heet een dekpunt van de permutatie σ.

2.10. **Disjuncte cykels.** Twee cykels $(x_1\ x_2\ x_3\ \ldots\ x_{k-1}\ x_k)$ en $(x'_1\ x'_2\ x'_3\ \ldots\ x'_{m-1}\ x'_m)$ heten disjunct als $x_i \neq x'_j$ voor alle $1 \leq i \leq k$ en $1 \leq j \leq m$. Disjuncte cykels commuteren altijd.

2.11. **Disjuncte cykelrepresentatie.** Zij X een eindige verzameling. Dan is iedere permutatie $\sigma \in S(X)$ te schrijven als product van disjuncte cykels. Deze disjuncte cykelrepresentatie is uniek (behalve dat de volgorde van de cykels kan verschillen en de elementen binnen een cykel verschoven kunnen worden). De cykels in deze representatie corresponderen met de banen waarin de verzameling X uiteenvalt onder het herhaald toepassen van σ.

2.12. **Doorsnede ondergroepen.** Iedere doorsnede $\bigcap_i H_i$ van ondergroepen $H_i \subset G$ is een ondergroep van G.

2.13. **Eindig voortgebracht.** Een groep die door een eindige verzameling van elementen wordt voortgebracht, heet eindig voortgebracht.
Voor een abelse groep G geldt:
G is eindig voortgebracht en elke $a \in G$ heeft eindige orde $\Longrightarrow G$ is eindig.
Voor een oneindige groep G geldt:
G is eindig voortgebracht $\Longrightarrow G$ is aftelbaar oneindig

2.14. **Geconjugeerd.** Twee elementen $x, y \in G$ heten geconjugeerd als er een $g \in G$ bestaat zodat $y = gxg^{-1}$. Als twee elementen in een groep geconjugeerd zijn, hebben ze dezelfde orde.
Verder geldt: $\sigma, \tau \in S_n$ zijn geconjugeerd $\Longleftrightarrow \sigma$ en τ hebben hetzelfde cykeltype.

2.15. **Geconjugeerde ondergroep.** Als $H \subset G$ een ondergroep van G is, dan is de met H geconjugeerde ondergroep $gHg^{-1} = \{ghg^{-1}\colon\ h \in H\}$ weer een ondergroep van G.

2.16. **Groep.** Een verzameling G, voorzien van een bewerking $\circ$, heet een groep als:

(G1) G bevat een (uniek) eenheidselement/identiteit e. Zo'n eenheidselement heeft de eigenschap dat voor elke $a \in G$ geldt dat $e \circ a = a \circ e = a$.
(G2) Voor elk drietal elementen $a, b, c \in G$ geldt de associatieve eigenschap: $a \circ (b \circ c) = (a \circ b) \circ c$
(G3) Voor elk element $a \in G$ bestaat er een (unieke) inverse $a^{-1} \in G$, met de eigenschap dat $a \circ a^{-1} = a^{-1} \circ a = e$.

2.17. **Groep van orde 4.** Als een groep G orde 4 heeft, dan is G óf cyclisch, óf de viergroep van Klein.

2.18. **Inversies.** Een inversie is een paar (i, j) van indices in $\{1, 2, \ldots, n\}$ waarvoor geldt $i < j$ en $\sigma(i) > \sigma(j)$. Als $\sigma \in S_n$ een even aantal inversies induceert, is de pariteit van σ ook even, als σ een oneven aantal inversies induceert, is de pariteit van σ oneven.

2.19. **k-cykel.** Een k-cykel/cyclische permutatie van lengte k is een element $\sigma \in S(X)$ dat k elementen $(x_1, x_2, \ldots, x_k)$ in X cyclisch verschuift en de andere elementen van X op hun plek laat. Notatie: $\sigma = (x_1\ x_2\ x_3\ \ldots\ x_{k-1}\ x_k) = (x_2\ x_3\ \ldots\ x_{k-1}\ x_k\ x_1)$.

2.20. **Keten van ondergroepen.** Een keten van ondergroepen in G is een collectie $\{H_i\}_{i\in I}$ van ondergroepen $H_i \subset G$, met de eigenschap dat voor ieder tweetal ondergroepen H_i, H_j geldt dat $H_i \subset H_j$ of $H_j \subset H_i$.

2.21. **Linksvermenigvuldiging.** De afbeelding λ_a: $G \to G$, gegeven door $x \mapsto ax$, zorgt voor linksvermenigvuldiging met $a \in G$. Deze afbeelding is bijectief (voor elke $b \in G$ is er een uniek element $x \in G$ dat door linksvermenigvuldiging met a op b wordt afgebeeld). Aangezien geldt $\lambda_a \circ \lambda_b = \lambda_{ab}$, wordt duidelijk dat de inverse van λ_a de afbeelding $\lambda_{a^{-1}}$ is.

2.22. **Machtsverzameling.** De collectie $P(X)$ van deelverzamelingen van de verzameling X heet de machtsverzameling van X. Onder de bewerking Δ (het symmetrisch verschil) is $P(X)$ een abelse groep.

2.23. **Ondergroepen.** Een deelverzameling H van een groep G heet een ondergroep van G als hij aan de volgende voorwaarden voldoet:

(H1) H bevat het eenheidselement van G
(H2) Voor elk tweetal elementen $a, b \in H$ geldt $ab \in H$
(H3) Voor ieder element $a \in H$ geldt $a^{-1} \in H$

In plaats van deze voorwaarden kunnen ook de volgende voorwaarden worden gebruikt om aan te tonen dat een deelverzameling $H \subset G$ een ondergroep van G is:

(H1') H is niet leeg
(H2') Voor elk tweetal elementen $a, b \in H$ geldt $ab^{-1} \in H$

2.24. **Orde van een element.** De orde van een element $a \in G$ is het kleinste positieve getal n waarvoor $a^n = e$. Als zo'n n niet bestaat, is de orde van a oneindig. In een eindige groep is de orde van een element altijd een deler van de orde van de groep.

2.25. **Orde van een groep.** $\#G$ = de orde van een groep G = aantal elementen van G (kan zowel eindig als oneindig zijn).

2.26. **Ordes groepen en elementen.** Voor een groep G geldt:

- $\#G$ is eindig $\implies$ ieder element $a \in G$ heeft eindige orde
- $a \in G$ heeft oneindige orde $\implies$ alle machten van a (dus alle elementen in de rij $(a^k)_{k\in\mathbb{Z}}$) zijn verschillend.
- $a \in g$ heeft (eindige) orde $n \implies$ er zijn precies n verschillende machten van a, dus de rij $(a^k)_{k\in\mathbb{Z}}$ is periodiek met periode n.

2.27. **De permutatiegroep/symmetrische groep.** De verzameling $S(X)$ is de verzameling van alle bijecties van een verzameling X naar zichzelf ($X \to X$). Met als bewerking de samenstelling van afbeeldingen vormt deze verzameling een groep, genaamd de permutatiegroep/symmetrische groep $S(X)$ op X.
Als X een eindige verzameling is met n elementen, geven we $S(X)$ aan met S_n. Deze groep heeft orde $n!$.

2.28. **Rechtsaxioma's.** G is een groep met de bewerking $\circ$, als G voldoet aan $(G2)$ en de rechtsaxioma's:

(G1') Voor alle $a \in G$ geldt $a \circ e = a$
(G2') Elk element $a \in G$ heeft een rechtsinverse $a^\dagger \in G$ met de eigenschap $a \circ a^\dagger = e$

2.29. **Rechtsvermenigvuldiging.** De afbeelding ρ_a: $G \to G$, gegeven door $x \mapsto xa$, zorgt voor rechtsvermenigvuldiging met $a \in G$. Deze afbeelding is bijectief (voor elke $b \in G$ is er een uniek element $x \in G$ dat door rechtsvermenigvuldiging met a op b wordt afgebeeld). Aangezien geldt $\rho_a \circ \rho_b = \rho_{ba}$, wordt duidelijk dat de inverse van ρ_a de afbeelding $\rho_{a^{-1}}$ is.

2.30. **Sokken-en-schoenenregel.** $(ab)^{-1} = b^{-1}a^{-1}$

2.31. **Tekenafbeelding.** De afbeelding ε: $S_n \to \{\pm 1\}$ kent aan iedere permutatie $\sigma \in S_n$ een teken toe, volgens de volgende regels:

- Als σ een transpositie is, dan geldt $\varepsilon(\sigma) = -1$
- Voor alle elementen $\sigma, \tau \in S_n$ geldt $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$

In plaats van het teken $+$ of $-$ wordt ook wel gezegd dat een permutatie even (teken $+$) of oneven (teken $-$) is. Dit slaat op het aantal transposities waarin de permutatie op te delen is.
Een k-cykel $\sigma \in S_n$ heeft altijd pariteit $\varepsilon(\sigma) = (-1)^{k-1}$. Voor $\sigma \in S_n$ met cykeltype $(k_1, k_2, \ldots, k_t)$ geldt dus:

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{t}(k_i-1)} = (-1)^{n-t}$$

2.32. **Torsie-element.** Een torsie-element is een element $a \in G$ met eindige orde. In een abelse groep G geldt: a en b zijn torsie-elementen $\Longrightarrow$ ab is een torsie-element.

2.33. **De triviale groep.** De triviale groep, genoteerd als $G = 1$, bestaat alleen uit het eenheidselement (en heeft dus orde 1). Het is de kleinste groep die er bestaat.

2.34. **Triviale ondergroepen.** Een groep G bevat altijd de triviale ondergroep $H = \{e\}$ (ook wel genoteerd als $H = 1$) en de ondergroep $H = G$.

2.35. **Vereniging ondergroepen.** De vereniging $H_1 \cup H_2$ van twee ondergroepen H_1 en H_2 van G is een ondergroep van $G \Longleftrightarrow H_1 \subset H_2$ of $H_2 \subset H_1$

2.36. **Vermenigvuldigtafel.** Van iedere groep G kan een vermenigvuldigtafel worden gemaakt, waarbij de producten/samenstellingen van alle mogelijke geordende paren in G worden weergegeven. In de vermenigvuldigtafel van een eindige groep komt ieder element precies één keer voor in iedere rij en één keer in iedere kolom.

2.37. **Voortbrengen.** De ondergroep $\langle S \rangle$ is de ondergroep van G voortgebracht door S. Deze ondergroep $\langle S \rangle$ bestaat uit alle eindige producten van elementen $s \in S \cup S^{-1}$, waarbij $S^{-1} = \{s^{-1} \colon s \in S\}$. $\langle S \rangle$ is de kleinste ondergroep van G die S bevat.
Als geldt dat $\langle S \rangle = G$, dan wordt G voortgebracht door S, ofwel S is een verzameling voortbrengers van G.
Als geldt dat $\#S > \frac{1}{2}\#G$, dan geldt $G = \langle S \rangle$.

3. Hoofdstuk 3 (+ opgaven)

3.1. **Affiene afbeeldingen.** De groep $\mathrm{Aff}_2(\mathbb{R})$ is de groep van vlakke affiene afbeeldingen, deze groep ontstaat door translaties samen te stellen met willekeurige elementen uit $GL_2(\mathbb{R})$. De afbeeldingen die dan ontstaan voeren rechte lijnen over in rechte lijnen.
Er gelden natuurlijke inclusies: $I_2(\mathbb{R}) \subset \mathrm{Sim}_2(\mathbb{R}) \subset \mathrm{Aff}_2(\mathbb{R})$.

3.2. **Collineaire punten.** Punten in het vlak zijn collineair als er een lijn in het vlak bestaat waarop al deze punten liggen.

3.3. **Complexe vlak.** In het complexe vlak worden isometrieën als volgt weergegeven:

- Oriëntatie bewarende isometrieën: $\varphi^+_{a,b}$: $z \mapsto az + b$ met $a, b \in \mathbb{C}$ en $|a| = 1$
- Oriëntatie omkerende isometrieën: $\varphi^-_{a,b}$: $z \mapsto a\overline{z} + b$ met $a, b \in \mathbb{C}$ en $|a| = 1$

Hierbij is $z \mapsto \overline{z}$ gelijk aan een spiegeling in de x_1-as, $z \mapsto az$ met $a = e^{i\alpha}$ gelijk aan een rotatie over een hoek α om O en $z \mapsto z + b$ gelijk aan de translatie over een punt b.

3.4. **Cyclische ondergroep.** De groep $C_n \subset O_2(\mathbb{R})$ bestaat uit de n rotaties om O over hoeken $\frac{2\pi}{n} \cdot k$, met k geheel. Dit zijn alle rotaties in de groep D_n.

3.5. **Dekpunt.** Het punt x is een dekpunt van φ (of φ laat het punt x invariant) als geldt $\varphi(x) = x$ voor $x \in \mathbb{R}^2$ en φ: $\mathbb{R}^2 \to \mathbb{R}^2$.

3.6. **Twee dekpunten.** Als een isometrie 2 verschillende punten invariant laat, is deze isometrie de identiteit of de spiegeling in de lijn door deze twee punten.

3.7. **Drie dekpunten.** Als een isometrie 3 niet-collineaire punten invariant laat, is deze isometrie de identiteit.

3.8. **Gelijkvormigheid.** Een gelijkvormigheid is een niet-constante afbeelding φ: $\mathbb{R}^2 \to \mathbb{R}^2$ die verhoudingen van afstanden invariant laat, dus voor $a, b, c, d \in \mathbb{R}^2$ met $a \neq b$ en $c \neq d$ geldt: $\frac{|\varphi(a)-\varphi(b)|}{|a-b|} = \frac{|\varphi(c)-\varphi(d)|}{|c-d|}$.
De verzameling van gelijkvormigheden is $\mathrm{Sim}_2(\mathbb{R})$, dit is een ondergroep van $S(\mathbb{R}^2)$ die $I_2(\mathbb{R})$ bevat.

3.9. **Gelijkvormigheidstransformaties.** De groep $\mathrm{Sim}_2(\mathbb{R})$ is de groep van vlakke gelijkvormigheidstransformaties, dit zijn de afbeeldingen die niet de afstanden tussen punten behouden, maar de verhoudingen van afstanden tussen punten. Deze afbeeldingen voeren dus rechte lijnen over in rechte lijnen, en bewaren de hoeken daartussen.
Er gelden natuurlijke inclusies: $I_2(\mathbb{R}) \subset \mathrm{Sim}_2(\mathbb{R}) \subset \mathrm{Aff}_2(\mathbb{R})$.

3.10. **Isometrie/vlakke symmetrie.** Een vlakke symmetrie of isometrie is een afbeelding φ: $\mathbb{R}^2 \to \mathbb{R}^2$ die afstanden onveranderd laat, dus waarvoor geldt:
$\forall x, y \in \mathbb{R}^2$: $|\varphi(x) - \varphi(y)| = |x - y|$.
Uit deze definitie volgt dat φ een bijectie is, en dat φ hoeken tussen lijnen invariant laat.
De verzameling van isometrieën van het vlak is $I_2(\mathbb{R})$, dit is een ondergroep van de

permutatiegroep $S(\mathbb{R}^2)$.
Voor een isometrie φ en punten $x_1, x_2 \ldots, x_n \in \mathbb{R}^2$ geldt:

$$\varphi\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right) = \frac{\varphi(x_1) + \varphi(x_2) + \ldots + \varphi(x_n)}{n}$$

3.11. **Lineaire bijecties.** De verzameling $GL_2(\mathbb{R})$ is de groep bijecties van het vlak die lineair zijn. Dit komt overeen met de groep van inverteerbare 2x2-matrices (ofwel de 2x2-matrices met determinant ongelijk aan 0) met reële coëfficiënten. Voor deze groep geldt: $GL_2(\mathbb{R}) \cap I_2(\mathbb{R}) = O_2(\mathbb{R})$.

3.12. **Lineaire component.** De productrepresentatie van een isometrie φ is van de vorm $\varphi = \tau\psi$. Hierbij wodt ψ de lineaire component van φ genoemd, geschreven als $\psi = L(\varphi)$. Hiervoor geldt $L(\varphi_1\varphi_2) = L(\varphi_1)L(\varphi_2)$.

3.13. **Lineaire isometrie.** Voor een lineaire isometrie φ: $\mathbb{R}^2 \to \mathbb{R}^2$ geldt:

- $|\varphi(x)| = |x|$ voor elke $x \in \mathbb{R}^2$
- $\langle\varphi(x), \varphi(y)\rangle = \langle x, y\rangle$ voor alle $x, y \in \mathbb{R}^2$

3.14. **Oriëntatie behoudende afbeeldingen.** Alle orthogonale afbeeldingen die door de tekenafbeelding naar 1 worden gestuurd, dus de oriëntatie behoudende afbeeldingen, vormen de ondergroep $O_2^+(\mathbb{R}) \subset O_2(\mathbb{R})$ van alle rotaties om O.

3.15. **Orthogonale afbeelding.** Een orthogonale afbeelding is een isometrie φ waarvoor geldt $\varphi(O) = O$ (dus een isometrie die de oorsprong naar zichzelf stuurt). Dit is altijd óf een rotatie om de oorsprong, óf het product van een rotatie om de oorsprong met een spiegeling in de x_1-as.
De verzameling van orthogonale afbeeldingen van het vlak is de orthogonale groep $O_2(\mathbb{R})$. Dit is de ondergroep van lineaire afbeeldingen in $I_2(\mathbb{R})$. De groep $O_2(\mathbb{R})$ is de symmetriegroep vn de eenheidscirkel in het vlak.

3.16. **Productrepresentatie.** Iedere isometrie φ is op een unieke manier te schrijven als een product $\varphi = \tau\psi$ van een translatie τ en een orthogonale afbeelding ψ, dit is de productrepresentatie van de isometrie.

3.17. **Puntgroep.** De puntgroep van G is de groep $\overline{G} = \{L(\varphi)\colon\ \varphi \in G\}$, dit is een ondergroep van $O_2(\mathbb{R})$.

3.18. **Rotatie om de oorsprong.** Rotaties om O in $O_2(\mathbb{R})$ zien er in matrixvorm als volgt uit: $\rho_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$. Hierbij is α de hoek waarover geroteerd wordt. Voor twee rotaties van α en β geldt: $\rho_\alpha\rho_\beta = \rho_\beta\rho_\alpha$.

3.19. **Rotatie en spiegeling.** Afbeeldingen in $O_2(\mathbb{R})$ waarbij ook een spiegeling wordt gebruikt, zien er als volgt uit: $\rho_\alpha\sigma = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$. Deze afbeelding is de spiegeling in de lijn l die een hoek van $\alpha/2$ met de positieve x_1-as maakt.
De afbeelding $\rho\sigma$ heeft orde 2, dus $(\rho\sigma)^{-1} = \rho\sigma$. Omdat ook geldt $(\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \sigma\rho^{-1}$, volgt hieruit $\rho\sigma = \sigma\rho^{-1}$. De spiegeling σ commuteert dus niet met alle rotaties.

3.20. **Symmetriegroep.** De symmetriegroep van een figuur $F \subset \mathbb{R}^2$ is de ondergroep $\mathrm{Sym}(F) = \{\varphi \in I_2(\mathbb{R})\colon\ \varphi[F] = F\}$ van $I_2(\mathbb{R})$. De enige eindige symmetriegroepen zijn de groepen C_n en D_n (dus iedere eindige ondergroep van $I_2(\mathbb{R})$ is voor een geschikte keuze van de coördinaten gelijk aan C_n of D_n).

3.21. **Symmetriegroep D_n.** De symmetriegroep D_n is de symmetriegroep van de regelmatige n-hoek, ook wel de dihedrale groep of de diëdergroep van orde $2n$ genoemd. Voor een n-hoek met middelpunt O geldt $D_n \subset O_2(\mathbb{R})$.

3.22. **Tekenafbeelding isometrieën.** De tekenafbeelding voor isometrieën $(I_2(\mathbb{R}) \to \{\pm 1\})$ is gedefinieerd door $\varphi \mapsto \det L(\varphi)$. De ondergroep $I_2^+(\mathbb{R})$, met isometrieën met teken 1, is dan de ondergroep van oriëntatie bewarende isometrieën.

3.23. **Tekenafbeelding orthogonale groep.** Voor de orthogonale groep bestaat er ook een tekenafbeelding $O_2(\mathbb{R}) \to \{\pm 1\}$ die iedere afbeelding naar de determinant van de bijbehorende matrix stuurt. Afbeeldingen met determinant 1 zijn rotaties, deze afbeeldingen worden oriëntatie behoudend genoemd. Afbeeldingen met determinant -1 zijn spiegelingen, ofwel oriëntatie omkerende afbeeldingen.

3.24. **Translatieondergroep.** De translatieondergroep is de ondergroep van G die alle translaties in G bevat: $G_T = \{\varphi \in G\colon\ L(\varphi) = \mathrm{id}\}$.

3.25. **Type van een isometrie.** Aan het teken en het wel/niet hebben van een dekpunt kun je afleiden van welk type een isometrie is:

	met dekpunt	zonder dekpunt
det=+1	rotatie	translatie
det=-1	spiegeling	glijspiegeling

Hierbij is een translatie een 'echte' translatie, dat wil zeggen dat er getransleerd wordt over een vector ongelijk aan 0. De glijspiegeling is een spiegeling, gevolgd door een 'echte' translatie evenwijdig aan de spiegelas.
Een isometrie met een dekpunt is orthogonaal als het dekpunt de oorsprong is. Voor een isometrie zonder dekpunt geldt dat de vergelijking $z = az + b$ (of $z = a\overline{z} + b$) geen oplossing heeft.

3.26. **Type isometrie na samenstelling.** De volgende stellingen gelden:

- De samenstelling van de spiegelingen in 2 evenwijdige lijnen is een translatie.
- De samenstelling van de spiegelingen in 2 snijdende lijnen is een rotatie.
- Het kwadraat van een glijspiegeling is een translatie.
- De samenstelling van 2 rotaties over hoeken α en $-\alpha$ is een translatie.
- De samenstelling van 2 rotaties over hoeken α en $\beta \neq -\alpha$ is een rotatie over $\alpha + \beta$.

3.27. **Verzameling matrices.** De verzameling $\mathrm{Mat}_2(\mathbb{R})$ is de verzameling van alle reële 2x2-matrices.

3.28. **Vlakke kristallografische groep.** De translatieondergroep van een vlakke kristallografische groep $G \subset I_2(\mathbb{R})$ wordt voortgebracht door 2 onafhankelijke translaties (translaties over 2 onafhankelijke vectoren). De puntgroep van zo'n groep is gelijk aan C_n of D_n met $n \in \{1, 2, 3, 4, 6\}$.

3.29. **Vlakke affiene afbeelding.** Een vlakke affiene afbeelding $\mathbb{R}^2 \to \mathbb{R}^2$ wordt verkregen door een inverteerbare lineaire afbeelding met een translatie samen te stellen. De verzameling van affiene afbeeldingen $\mathrm{Aff}_2(\mathbb{R})$ is een ondergroep van $S(\mathbb{R}^2)$ die $\mathrm{Sim}_2(\mathbb{R})$ bevat.

4. Hoofdstuk 4 (zonder opgaven)

4.1. **Additieve en multiplicatieve notatie.** Een groepsbewerking kan op 2 manieren worden genoteerd:

Multiplicatieve notatie	**Additieve notatie**
Bewerking xy	Bewerking $x + y$
Inverse x^{-1}	Tegengestelde $-x$
Machten x^n	Product nx
Eenheidselement e of 1	Nulelement 0
Restklasse gN	Restklasse $g + N$

Onder optelling zijn $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ groepen, onder vermenigvuldiging zijn $\mathbb{Q}^*$, $\mathbb{R}^*$ en $\mathbb{C}^*$ dit.

4.2. **Automorfisme.** Een bijectief endomorfisme $G \to G$ heet een automorfisme van G. De verzameling $\mathrm{Aut}(G)$ van alle automorfismen van G vormt een groep onder samenstelling (de automorfismengroep).

4.3. **Beeld.** Voor een homomorfisme $f\colon G \to G'$ geldt dat het beeld $f[G] = \{f(x)\colon x \in G\}$ van f een ondergroep van G is.

4.4. **Centrum.** Het centrum van een groep G bestaat uit alle elementen uit de groep die met alle elementen commuteren: $Z(G) = \{g \in G\colon \forall x \in G,\ gx = xg\}$. Voor abelse groepen geldt dus $Z(G) = G$. Voor $G = S_n$ met $n \neq 2$ geldt $Z(G) = 1$.

4.5. **Endomorfisme.** De homomorfismen van een groep G naar zichzelf heten endomorfismen. Hiervoor geldt $\mathrm{Hom}(G, G) = \mathrm{End}(G)$. De groep $\mathrm{End}(G)$ vormt alleen een groep onder samenstelling voor $G = 1$.
Voor abelse groepen G is de afbeelding $x \mapsto x^n$ voor iedere $n \in \mathbb{N}$ een endomorfisme.

4.6. **Homomorfisme.** Een homomorfisme van een groep G naar een groep G' is een afbeelding $f\colon G \to G'$, met de eigenschap dat voor ieder tweetal elementen $x, y \in G$ geldt: $f(xy) = f(x)f(y)$.
De verzameling van alle homomorfismen van G naar G' is $\mathrm{Hom}(G, G')$. Deze verzameling bevat altijd het triviale homomorfisme.
Een samenstelling van een homomorfisme $G \to G'$ en een homomorfisme $G' \to G''$ geeft een homomorfisme $G \to G''$.
Voor een homomorfisme $f\colon G \to G'$ geldt altijd:

- $f(e) = e'$ met $e \in G$ en $e' \in G'$ de eenheidselementen
- $f(x^{-1}) = f(x)^{-1}$ voor alle $x \in G$

4.7. **Index.** De index van H in G is $[G : H] = \#(G/H)$, dit is het aantal verschillende nevenklassen van H in G.

4.8. **Inwendig automorfisme.** Een inwendig automorfisme is een automorfisme $f\colon G \to G$ van de vorm: $f(x) = axa^{-1}$ met $a \in G$. De verzameling van alle inwendige automorfismen van G is de verzameling $\mathrm{Inn}(G)$.

4.9. **Isomorfiestelling.** Zij $f\colon G \to G'$ een homomorfisme met kern N, en definieer een bewerking op ${}^{G}/_{N}$ door $g_1N \cdot g_2N = g_1g_2N$. Dan wordt ${}^{G}/_{N}$ hiermee een groep, en de afbeelding $\overline{f}\colon {}^{G}/_{N} \to f[G]$ gegeven door $gN \mapsto f(g)$ een groepsisomorfisme.

4.10. **Isomorfisme.** Een bijectief homomorfisme $f\colon G \to G'$ heet een isomorfisme. Dit wordt genoteerd door een $\sim$ boven de pijl te zetten. Als zo'n isomorfisme bestaat, hebben G en G' dezelfde groepsstructuur, ze zijn dan isomorf (notatie $G \cong G'$).

4.11. **Kern.** Voor een homomorfisme $f\colon G \to G'$ geldt dat de kern $\mathrm{Ker}(f) = \{x \in G\colon f(x) = e'\}$ van f een ondergroep van G is.
Hierbij hoort de stelling: f is injectief $\iff \ker(f) = \{e\}$ (de kern is triviaal).
Een andere stelling is: de ondergroep $H \subset G$ treedt op als de kern van een homomorfisme $f \implies {}^{G}/_{H}$ bezit een natuurlijke groepsstructuur. Dit betekent dat normaaldelers van G precies de ondergroepen van G zijn die als kernen van homomorfismen op kunnen treden.

4.12. **Stelling van Lagrange.** Zij G een eindige groep en $H \subset G$ een ondergroep. Dan geldt: $\#G = [G : H] \cdot \#H$. Hieruit volgt:

- De orde $\#H$ van een ondergroep $H \subset G$ deelt $\#G$
- De orde van een element $x \in G$ deelt $\#G$

4.13. **Linkernevenklassen.** Voor een ondergroep $H \subset G$ geldt dat de linkernevenklasse van $g \in G$ van de vorm $gH = \{gh\colon h \in H\}$ is. Alle linkernevenklassen van H in G vormen de collectie ${}^{G}/_{H}$, die een partitie van G is (dus alle linkernevenklassen in ${}^{G}/_{H}$ zijn disjunct en de vereniging hiervan is G).
Er geldt: $g_1H = g_2H \iff g_1^{-1}g_2 \in H$.

4.14. **Natuurlijke/kanonieke afbeelding.** De natuurlijke/kanonieke afbeelding is de afbeelding $G \to {}^{G}/_{H}$.

4.15. **Normaaldeler.** Een normaaldeler/normale ondergroep van G is een ondergroep $H \subset G$ waarvoor geldt:
$\forall g \in G\colon gH = Hg$, ofwel: $\forall g \in G\colon gHg^{-1} = \{ghg^{-1}\colon h \in H\} = H$. Deze 2^e formulering maakt duidelijk dat normaaldelers ondergroep zijn die onder alle inwendige automorfismen $\sigma_g \in \mathrm{Inn}(G)$ in zichzelf overgaan.
Als een ondergroep $H \subset G$ normaal is, wordt dit aangegeven met $H \lhd G$.
In een abelse groep is iedere ondergroep een normaaldeler.
Gevolgen als H een normaaldeler is van G:

- ${}^{G}/_{H}$ is een groep met de bewerking $g_1H \cdot g_2H = g_1g_2H$. Hiermee wordt de natuurlijke afbeelding $G \to {}^{G}/_{H}$ een groepshomomorfisme met kern H.
- $\overline{h} \in H\colon \overline{h} = \overline{1}$
- $\overline{g}, \overline{h} \in H\colon \overline{g} \cdot \overline{h} = \overline{gh}$

4.16. **Quotiëntgroep.** De vorming van de quotiëntgroep/factorgroep G/N uit G en N gebeurt door G uit te delen naar N (met als quotiëntafbeelding het natuurlijke homomorfisme $G \to G/N$).
In G/N wordt vervolgens gerekend met de representanten van restklassen. De restklasse van een representant g kan worden geschreven als $\overline{g}$, als gN of als g mod N. Een afbeelding op G/N is welgedefinieerd als de definitie van de afbeelding onafhankelijk is van de keuze van de representanten.

4.17. **Rechternevenklassen.** Rechternevenklassen van H in G zijn van de vorm $Hg = \{hg\colon\ h \in H\}$. Alle rechternevenklassen van H in G vormen de collectie $H\backslash G$.

4.18. **Triviaal homomorfisme.** Het triviale homomorfisme stuurt alle elementen van G naar het eenheidselement $e' \in G'$.

4.19. **Vezel.** De vezel van f boven y is het volledig origineel $f^{-1}(y) = \{x \in G\colon\ f(x) = y\}$.
Niet-lege vezels van een homomorfisme zijn altijd even groot als de kern.
De vezel van een homomorfisme f boven een punt $f(g)$ is gelijk aan de linkernevenklasse gN van de kern N.

5. Hoofdstuk 5 (zonder opgaven)

5.1. **Baan.** De baan van x onder G is de deelverzameling $Gx = \{gx\colon\ g \in G\} \subset X$. Het aantal elementen in deze verzameling is de lengte van de baan. Hiervoor geldt: $\#Gx = [G : G_x] = \frac{\#G}{\#G_x}$. Dit volgt uit de stelling:
Voor een G-verzameling X en $x \in X$ geldt dat de afbeelding $g \mapsto gx$ een bijectie $G/G_x \longleftrightarrow Gx$ induceert tussen de verzameling van linkernevenklassen van G_x in G en de baan van x.
Andere formules waarbij de lengtes van de banen worden gebruikt, staan op blz 65 van het dictaat.

5.2. **Banenformule.** Voor een eindige groep G en een eindige verzameling X kan het aantal G-banen in X worden berekend met de banenformule:
$\#(G\backslash X) = \frac{1}{\#G} \sum_{g \in G} \chi(g)$.
In woorden betekent dit dat het aantal banen gelijk is aan het gemiddelde aantal dekpunten per element $g \in G$.

5.3. **Banenruimte.** De verzameling van banen van X onder de werking van G heet de banenruimte/quotiëntruimte van X onder de werking van G en wordt genoteerd met $G\backslash X$. De verzameling $G\backslash X$ bestaat uit disjuncte banen, waarvan de vereniging gelijk is aan G.

5.4. **Stelling van Cauchy.** Zij G een eindige groep en p een priemdeler van $\#G$. Dan bevat G een element van orde p.

5.5. **Stelling van Cayley.** Voor de groep G en permutatiegroep $S(G)$, met λ_g: $G \to G$ de linksvermenigvuldiging $x \mapsto gx$ voor $g \in G$, geldt dat $f\colon\ G \to S(G)$, gedefinieerd door $g \mapsto \lambda_g$ een inbedding is en dat G isomorf is met een ondergroep van $S(G)$.

5.6. **Conjugatiewerking.** De conjugatiewerking is de werking van een groep op zichzelf door conjugatie. Voor de groep G met σ_g: $x \mapsto gxg^{-1}$ voor $g \in G$ geldt dat f: $G \to Aut(G) \subset S(G)$, gedefinieerd door $g \mapsto \sigma_g$ een homomorfisme is met als kern $Z(G)$, het centrum van G, dit zijn ook de dekpunten voor de conjugatie-actie. De banen die ontstaan onder conjugatie in G heten de conjugatieklassen van G.

5.7. **Conjugatiewerking op H $\subset$ G.** Een groep werkt ook door conjugatie op de verzameling van zijn ondergroepen. De baan van een ondergroep $H \subset G$ bestaat dan uit de verzameling met H geconjugeerde ondergroepen $\{gHg^{-1}\colon\ g \in G\}$. Al deze ondergroepen zijn isomorf met H en hebben dezelfde index in G.
De dekpunten voor deze conjugatie-actie zijn de normaaldelers van G.

5.8. **Dekpunten.** Het punt $x \in X$ is een dekpunt van $g \in G$ als geldt $gx = x$. Als x een dekpunt is van alle $g \in G$, dan heet x een dekpunt voor de werking van G op X. Dit is het geval wanneer de baan $Gx = \{x\}$, dus wanneer $\#Gx = 1$. De verzameling van al deze dekpunten is X^G. Als $X^G = \emptyset$, dan werkt G dekpuntsvrij op X.

5.9. **Inbedding.** Een inbedding van K in S_8 is een isomorfisme van K met een ondergroep van S_8.

5.10. **Kleuringen.** Als het aantal echt verschillende kleuringen van een vorm bepaald moet worden, kan dit worden bepaald door het aantal banen voor de werking van de symmetriegroep op de vorm uit te rekenen met de banenformule (dit is gelijk aan het aantal echt verschillende kleuringen). Een voorbeeld hiervan staat in het dictaat op blz 61/62.

5.11. **Symmetrieën van een kubus.** De groep K is de groep van symmetrieën van een kubus.

5.12. **Normaaldelers en priemdelers.** Voor een eindige groep $G \neq 1$ en p de kleinste priemdeler van $\#G$ geldt dat iedere ondergroep $H \subset G$ met index p normaal is in G.

5.13. **Normalisator.** De stabilisator van $x \in G$ onder conjugatie heet de normalisator $N_x = \{g \in G\colon\ gxg^{-1} = x\}$ van het element x.
De stabilisator van een ondergroep $H \subset G$ onder conjugatie heet de normalisator $N_G(H) = \{g \in G\colon\ gHg^{-1} = H\}$ van H in G. Hiervoor geldt dat H normaal is in $N_G(H)$ en dat $N_G(H)$ de grootste ondergroep van G is waarin H normaal is.

5.14. **p-groep.** Een p-groep is een eindige groep G waarvan de orde een macht van een priemgetal p is. Voor een p-groep G geldt voor iedere G-verzameling X de congruentie $\#X \equiv \#X^G \bmod p$.

5.15. **Permutatiekarakter.** Het permutatiekarakter van een element $g \in G$ kan worden berekend met de functie χ: $G \to \mathbb{Z}$, gegeven door $\chi(g) = \#\{x \in X\colon\ gx = x\}$. Het permutatiekarakter is dus gelijk aan het aantal dekpunten van g in X.

5.16. **Rechtswerking.** Soms is het logischer om een groep G van rechts op een verzameling X te laten werken, dus om een afbeelding X x $G \to X$ te beschouwen die voldoet aan $x \circ (g_1 g_2) = (x \circ g_1) \circ g_2$. Zo'n rechtswerking correspondeert niet met een homomorfisme, maar met een anti-homomorfisme $G \to S(X)$.

5.17. **Reguliere werking.** De reguliere werking is de werking van een groep op zichzelf door linksvermenigvuldiging. Hierbij hoort de stelling van Cayley.

5.18. **Reguliere werking op G/H.** De reguliere werking van G op de verzameling G/H van linkernevenklassen van een ondergroep $H \subset G$ is gegeven door $g \circ xH = gxH$. Deze werking is het homomorfisme $G \to S(G/H)$ met kern $\bigcap_{x \in G} xHx^{-1}$.
De reguliere werking van G op G/H is transitief. De stabilisator van $H \in G/H$ is H zelf en de stabilisator van een nevenklasse $xH \in G/H$ is de geconjugeerde ondergroep xHx^{-1}.

5.19. **Stabilisator.** De stabilisator/isotropiegroep van een punt $x \in X$ in G is de ondergroep $G_x = \{g \in G\colon\ gx = x\} \subset G$.

5.20. **Symmetrieën van een tetraëder.** De groep T is de groep van symmetrieën van een tetraëder.

5.21. **Transitief.** Als er een $x \in X$ bestaat met $Gx = X$, dan heet de werking van G op X transitief.

5.22. **Trouwe werking.** Een trouwe werking is een injectief homomorfisme φ: $G \to S(X)$.

5.23. **Werking.** Een werking/actie van een groep G op een verzameling X is een homomorfisme φ: $G \to S(X)$. In dit geval wordt X een G-verzameling genoemd. Voor $\varphi(g)(x)$ wordt ook wel $g \circ x$, $g(x)$ of gx geschreven.
Eigenschappen werking:

- Het eenheidselement $e \in G$ werkt als de identiteit op X.
- $g_1 g_2 \circ x = g_1 \circ (g_2 \circ x)$ voor $g_1, g_2 \in G$

De nu beschreven werking heet ook wel een linkswerking.

6. Hoofdstuk 6 (zonder opgaven)

6.1. **φ-functie van Euler.** De orde van de groep $(\mathbb{Z}/n\mathbb{Z})^*$ wordt aangegeven met $\varphi(n)$.

6.2. **Chinese reststelling.** Neem m en n met $\gcd(m,n) = 1$. Dan is de natuurlijke afbeelding ψ: $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ x $\mathbb{Z}/n\mathbb{Z}$ gedefinieerd door $(x \bmod mn) \mapsto (x \bmod m, x \bmod n)$ een ringisomorfisme. Dit isomorfisme induceert ook een isomorfisme van eenhedengroepen: ψ_*: $(\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ x $(\mathbb{Z}/n\mathbb{Z})^*$.
De Euler-φ-functie voldoet hierbij aan $\varphi(mn) = \varphi(m)\varphi(n)$.
Door de Chinese reststelling herhaald toe te passen, kan iedere ring $\mathbb{Z}/n\mathbb{Z}$ ontbonden worden in ringen van de vorm $\mathbb{Z}/p^k\mathbb{Z}$ met p^k de priemgetallen uit de factorisatie. Voor de Euler-φ-functie geldt dan $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

6.3. **Copriem.** Als $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, dan heten a en b onderling ondeelbaar of copriem. Dit is dus het geval wanneer $\gcd(a,b) = 1$, dus wanneer $xa + yb = 1$ een oplossing in gehele getallen heeft.

6.4. **Deler/veelvoud.** Als $b\mathbb{Z} \subset a\mathbb{Z}$, dan heet a een deler van b ($a|b$) en b een veelvoud van a. Dit betekent dat er een $x \in \mathbb{Z}$ bestaat waarvoor geldt $ax = b$.
Voor iedere deler $a|b$ geldt $|a| \leq |b|$.

6.5. **Eenhedengroep.** De verzameling $A^* = \{a \in A$: er bestaat een inverse $a^{-1}\}$ is de verzameling van eenheden in A, ook wel de eenhedengroep. Voor $\mathbb{Z}$ geldt $\mathbb{Z}^* = \{\pm 1\}$.

6.6. **Euclidisch algoritme.** Definieer voor gehele getallen a en b de rij van niet-negatieve gehele getallen r_0, r_1, r_2, ... door $r_0 = |a|$, $r_1 = |b|$ en $r_{i+1} =$ (rest van r_{i-1} bij deling door r_i) als $r_i \neq 0$. Dan bestaat er een index $k > 0$ met $r_k = 0$ en er geldt $\text{ggd}(a, b) = r_{k-1}$.
Het uitgebreide Euclidische algoritme geeft niet alleen de ggd, maar ook de oplossing van de vergelijking $xa + yb = \text{ggd}(a, b)$. Hiervoor wordt begonnen met de factoren $x_0 = \pm 1$ en $y_0 = 0$ en $x_1 = 0$ en $y_1 = \pm 1$.

6.7. **Stelling van Euler.** Voor a en $n \geq 1$ onderling ondeelbaar geldt $a^{\varphi(n)} \equiv 1 \bmod n$.

6.8. **Factorisatie.** Ieder positief getal n is uniek te ontbinden als een product van een eindig aantal priemgetallen $\left(n = \prod_{p \in \mathcal{P}} p^{n_p}\right)$. Hierbij heet de exponent n_p van p in de factorisatie de orde van n bij p, aangegeven met $\text{ord}_p(n)$. De functie ord_p: $\mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ voldoet aan de homomorfie-achtige eigenschap $\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$ voor $x, y \in \mathbb{Z}_{>0}$.

6.9. **Kleine stelling van Fermat.** Voor p een priemgetal en a een geheel getal geldt $a^p \equiv a \bmod p$.

6.10. **Groep $\mathbf{GL_n}(\mathbb{F}_\mathbf{p})$.** De groep $GL_n(\mathbb{F}_p)$ is de groep inverteerbare n x n-matrices met coëfficiënten in $\mathbb{F}_p$. Deze groep is eindig voor iedere n en iedere p.

6.11. **Grootste gemene deler.** De grootste gemene deler van a en b is $\text{ggd}(a, b)$. Dit is de niet-negatieve voortbrenger van $a\mathbb{Z} + b\mathbb{Z}$.
Uit deze definitie volgt dat er getallen $x, y \in \mathbb{Z}$ bestaan met $xa + yb = \text{ggd}(a, b)$.

6.12. **Kleinste gemene veelvoud.** Het kleinste gemene veelvoud van a en b is $\text{kgv}(a, b)$. Dit is de niet-negatieve voortbrenger van $a\mathbb{Z} \cap b\mathbb{Z}$.

6.13. **Lichamen.** Commutatieve ringen A waarvoor $A^* = A \backslash \{0\}$ heten lichamen.
Een ring $\mathbb{Z}/n\mathbb{Z}$ is een lichaam $\iff n$ is priem.

6.14. **Lichaam $\mathbb{F}_\mathbf{p}$.** Het eindige lichaam $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ voor p priem.

6.15. **Modulorekenen.** De cyclische groepen $\mathbb{Z}/n\mathbb{Z}$ van restklassen modulo n zijn de quotiënten van $\mathbb{Z}$. Deze groepen zijn handig bij deling met rest:
Laat x en $n > 0$ natuurlijke getallen zijn. Dan bestaan er natuurlijke getallen a en b waarvoor geldt: $x = an + b$. Er geldt dan $x \equiv b \bmod n$, dus als wordt gerekend in $\mathbb{Z}/n\mathbb{Z}$ zit x in restklasse b mod n ofwel $\overline{b}$. Er wordt ook wel gezegd dat $\overline{x}$ congruent is met $\overline{b}$.

6.16. **Ondergroepen $\mathbb{Z}$.** De cyclische groepen $\mathbb{Z}/n\mathbb{Z}$ zijn de enige quotiënten van $\mathbb{Z}$, dus iedere ondergroep van $\mathbb{Z}$ is van de vorm $n\mathbb{Z}$ voor een natuurlijk getal n.
De ondergroep van $\mathbb{Z}$ die wordt voortgebracht door a en b wordt geschreven als $a\mathbb{Z} + b\mathbb{Z}$. Deze ondergroep bestaat uit de elementen $xa + yb$ met $x, y \in \mathbb{Z}$.

6.17. **Priemeigenschap.** De priemeigenschap zegt:
Laat a en b geheel zijn en p priem. Dan geldt: $p|ab \Longrightarrow p|a$ of $p|b$.

6.18. **Priemgetallen.** Een getal $a > 1$ met alleen triviale delers heet een priemgetal. Een getal $a > 1$ dat niet priem is heet samengesteld.
De verzameling priemgetallen is $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}$, deze verzameling is oneindig.

6.19. **Restklassenring.** Voor $n \neq 0$ is $\mathbb{Z}/n\mathbb{Z}$ een eindige ring met $|n|$ elementen. De eenhedengroep $(\mathbb{Z}/n\mathbb{Z})^*$ is de groep van inverteerbare restklassen modulo n. Een restklasse $\overline{a}$ is inverteerbaar als de vergelijking $ax = 1 + ny$ een oplossing in gehele getallen heeft. Dit is het geval wanneer a en n copriem zijn, dus $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z}$: $\text{ggd}(a, n) = 1\}$.

6.20. **Ringen.** Een ring is een additief geschreven abelse groep A, voorzien van een multiplicatief geschreven bewerking A x $A \to A$, die voldoet aan:

(R1) A bevat een eenheidselement 1 voor de vermenigvuldiging
(R2) Voor elk drietal elementen $a, b, c \in A$ geldt de associatieve eigenschap $a(bc) = (ab)c$.
(R3) Voor elk drietal elementen $a, b, c \in A$ gelden de distributieve eigenschappen $a(b + c) = ab + ac$ en $(a + b)c = ac + bc$.

Als daarbij ook geldt dat $ab = ba$ voor alle $a, b \in A$, dan heet A een commutatieve ring.
Belangrijke voorbeelden van ringen zijn $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ (de restklassenring), $\mathbb{R}[X]$ (polynomen met coëfficiënten in $\mathbb{R}$) en $\mathbb{C}[X]$ (polynomen met coëfficiënten in $\mathbb{C}$).

6.21. **Ringhomomorfisme.** Een ringhomomorfisme is een afbeelding f: $A \to A'$ tussen ringen die een homomorfisme van de additieve groepen is, en die voldoet aan:

- $f(1_A) = 1_{A'}$
- $f(xy) = f(x)f(y)$ voor $x, y \in A$

6.22. **Ringisomorfisme.** Een bijectief ringhomomorfisme heet een ringisomorfisme.

6.23. **Triviale delers.** De triviale delers van een getal $a \neq 0$ zijn de delers ± 1 en $\pm a$.

7. Hoofdstuk 7 (zonder opgaven)

7.1. **Cyclische groep.** Voor een priemgetal p is $(\mathbb{Z}/p\mathbb{Z})$ een cyclische groep van orde $p - 1$.

7.2. **Polynoom.** Zij $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ een polynoom van graad $n \geq 1$ met coëfficiënten in $\mathbb{Z}/p\mathbb{Z}$. Dan heeft f niet meer dan n nulpunten in $\mathbb{Z}/p\mathbb{Z}$.

8. Hoofdstuk 8 (zonder opgaven)

8.1. **Abels gemaakte groep.** Het quotiënt $G_{ab} = {}^{G}/_{[G,G]}$ heet de abels gemaakte G. Deze groep wordt ook wel het maximale abelse quotiënt van G genoemd.

8.2. **Automorfismen.** Voor de cyclische groep $G = {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ geldt $\mathrm{Aut}(G) = ({}^{\mathbb{Z}}/_{n\mathbb{Z}})^*$.

8.3. **Commutatorondergroep.** De commutatorondergroep $[G, G] \subset G$ is de ondergroep van G die wordt voortgebracht door alle commutatoren $[x, y] = xyx^{-1}y^{-1}$ van elementen $x, y \in G$. De commutatorondergroep is een normaaldeler van G.

8.4. **Homomorfiestelling.** Zij $f\colon G \to G'$ een homomorfisme en N een normaaldeler van G die in $\ker(f)$ bevat is. Dan bestaat er een uniek homomorfisme $\overline{f}\colon {}^{G}/_{N} \to G'$ zodat f verkregen wordt als samenstelling $G \to {}^{G}/_{N} \to G'$ van de quotiëntafbeelding $\pi\colon G \to {}^{G}/_{N}$ met $\overline{f}$.

8.5. **Homomorfismen.** Als $f\colon G \to A$ een homomorfisme naar een abelse groep A is, dan bestaat er een homomorfisme $f_{ab}\colon G_{ab} \to A$ zodat f verkregen wordt als samenstelling $G \to G_{ab} \to A$ van de natuurlijke afbeelding $\pi\colon G \to G_{ab}$ met f_{ab}. Hieruit volgt dat er een bijectie bestaat tussen $\mathrm{Hom}(G_{ab}, A)$ en $\mathrm{Hom}(G, A)$.

8.6. **Homomorfismen vanaf $\mathbf{S_n}$.** Ieder homomorfisme $f\colon S_n \to A$ naar een abelse groep A is de samenstelling $S_n \to \{\pm 1\} \to A$ van de tekenafbeelding ε met een homomorfisme $\overline{f}\colon \{\pm 1\} \to A$.

8.7. **Karakteristieke ondergroep.** Een karakteristieke ondergroep van G is een groep die op zijn plaats blijft onder automorfismen.

8.8. **Natuurlijk isomorfisme ondergroep.** Zij $N \lhd G$ een normaaldeler en $H \subset G$ een ondergroep. Dan is er een natuurlijk isomorfisme ${}^{H}/_{H\cap N} \to {}^{HN}/_{N}$.

8.9. **Product ggd en kgv.** Voor positieve getallen a en b geldt $\gcd(a, b) \cdot \mathrm{kgv}(a, b) = ab$.

8.10. **Quaternionengroep Q.** De quaternionengroep Q bestaat uit de 8 elementen ± 1, $\pm i$, $\pm j$ en $\pm k$. De groepsstructuur is vastgelegd door de identiteiten $i^2 = j^2 = k^2 = ijk = -1$ en $(-1)^2 = 1$.
Hieruit volgen de rekenregels:

- $jk = i$
- $ki = j$
- $ij = k$
- $kj = -i$
- $ik = -j$
- $ji = -k$

Eigenschappen Q:

- Q wordt voortgebracht door i en j (dus $Q = \langle i, j\rangle$)
- Het centrum is $Z(G) = \{\pm 1\}$
- De commutatorondergroep is $[Q, Q] = \{\pm 1\}$
- De abels gemaakte quaternionengroep Q_{ab} is isomorf met V_4

8.11. **Quotiëntgroep.** De ondergroepen van de quotiëntgroep $\overline{G} = {}^{G}\!/_{N}$ zijn van de vorm $\overline{H} = {}^{H}\!/_{N}$, waarbij $H \subset G$ een ondergroep van G is die N bevat. Voor dergelijke H geldt dat $f\colon {}^{G}\!/_{H} \to {}^{\overline{G}}\!/_{\overline{H}}$, gegeven door $gH \mapsto \overline{g}\overline{H}$, een bijectieve afbeelding tussen de verzamelingen van linkernevenklassen is.
Voor de index geldt $[G : H] = [\overline{G} : \overline{H}]$.
H is normaal in $G \iff \overline{H}$ is normaal in $\overline{G}$. In dit geval is f een groepsisomorfisme.