2

Def Een afb. $S \times S \to S$ op verz. S heet een bewerking.

Def Een verz. G met daarop afb. $G \times G \to G$, aangegeven hier als $(x,y) \mapsto x \circ y$, $(x,y) \in G \times G$, heet een groep als

(G1) $\forall\, a,b,c \in G: \quad a \circ (b \circ c) = (a \circ b) \circ c$
(G2) $\exists\, e \in G : \forall x \in G: \quad e \circ x = x \circ e = x$
(G3) $\forall x \in G : \exists\, x^{-1} \in G: \quad x \circ x^{-1} = x^{-1} \circ x = e$

Opm (G1) & (G2) heet een monoïde, als ook

(G4) $\forall x,y \in G: \quad x \circ y = y \circ x$

geldt, heet G een abelse groep.

Vb $\mathbb{Z}$ met gewone optelling $+$, zo ook $\mathbb{R}$, $\mathbb{Q}$, met eenheid 0 en inverse $-x$
$\mathbb{Z}_{\geq 0}$ is een monoïde onder optelling, $\mathbb{R}$ en $\mathbb{Q}$ en $\mathbb{Z}$ zijn alle monoïde onder gewone vermenigvuldiging, omdat 0 geen inverse heeft en in $\mathbb{Z}$ heel veel elementen niet.
Echter $\mathbb{R} \setminus \{0\}$ en $\mathbb{Q} \setminus \{0\}$ zijn wél groepen onder gewone verm.

Vb $\mathbb{C} := \{a+bi \mid a,b \in \mathbb{R}\}$ vormt met $+ : (a+bi, c+di) \mapsto (a+c)+(b+d)i$ een groep en $\mathbb{C}^* := \{a+bi \mid a,b \in \mathbb{R},\ a \neq 0 \vee b \neq 0\}$ met $\cdot : (a+bi, c+di) \longmapsto ((ac-bd) + (ad+bc)i)$
De eenheid is 0, de inverse is $(-a)+(-b)i$ voor $a+bi$
De eenheid is 1, inverse is $\frac{a}{d} - \frac{b}{d} i$ voor $a+bi$, en daar $d = a^2+b^2$

We noteren ook de geconjugeerde van $\alpha \in \mathbb{C}$ als $\bar{\alpha} := a - bi$ voor $\alpha = a+bi$. We zien $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha \cdot \beta} = \bar{\alpha} \cdot \bar{\beta}$

St. 2.7 G zij een groep, $e \in G$ de eenheid die voldoet aan (G2) en voor $x \in G$ zij x^{-1} de inverse zoals gegeven door (G3). Dan geldt:
(a) $\exists!\, e \in G : \forall x \in G : \quad x \circ e = e \circ x = x$ de eenheid is <u>uniek</u>!

(b) $\forall x \in G : \exists! x^{-1} \in G : \quad x \circ x^{-1} = x^{-1} \circ x = e$ per x is x^{-1} uniek

(c) $\forall x \in G : (x^{-1})^{-1} = x$ de inverse van de inverse van x is x zelf.

Vb quaternionen : $\mathbb{H} := \{ a + bi + cj + dk \mid a,b,c,d \in \mathbb{R} \}$
met bewerking $+ : (a+bi+cj+dk,\ e+fi+gj+hk) \mapsto$
$(a+e)+(b+f)i+(c+g)j+(d+h)k$ is groep, evenals
$\mathbb{H}^* := \{ a+bi+cj+dk \in \mathbb{H} \mid a \neq 0 \vee b \neq 0 \vee c \neq 0 \vee d \neq 0 \}$
met bewerking $\cdot\ \mathbb{H}^* \times \mathbb{H}^* \to \mathbb{H}^*$ zdd de $+$ distribueert over $\cdot$
en $i \cdot j = k$ $\ jk = i$ en $ki = j$ elke $x \in \mathbb{R}$ commuteert met een $h \in \mathbb{H}$ en $i^2 = j^2 = k^2 = -1$
Daaruit volgt direct $k \cdot j = \cancel{\ } k^2 i = -i$, $j \cdot i = j^2 \cdot k = -k$ $\ ik = i^2 j = -j$.

Vb $GL_n(F)$ met F 'lichaam', is de verz. van $n \times n$-matrices A met determinant niet-0, die dus een inverse A^{-1} hebben waarvoor A^{-1} ook coëfficiënten in F heeft.

St. als M met bewerking $\circ\ M \times M \to M$ een monoïde vormt, dan kan met $G := \{ x \in M \mid x \text{ heeft inverse in } M \}$ de bewerking $\circ$ tot G beperkt worden, dwz $x,y \in G \Rightarrow x \circ y \in G$. En G vormt met $\circ|_G$ een groep.
vaak noteert men M^*, zoals $\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Q}^*$

Vb Dit passen we toe wanneer we alle $n \times n$ matrices met coëfficiënten in F bekijken. Dat is namelijk een monoïde (associatief en met eenheid $\begin{pmatrix} e & \varepsilon & \varepsilon \\ & e & \\ \varepsilon & & e \end{pmatrix}$ met e eenheid op F en ε de nul op F), en
met de eis dat $A \in M_{n \times n}(F)$ ook een inverse heeft, definiëren we $GL_n(F)$
waar matrixvermenigvuldiging op beperkt.

Vb beschouw op $\mathbb{Z}$ de relatie $\sim_n$: $a \sim_n b \Leftrightarrow a + (-b) \in n\mathbb{Z}$ met
$n\mathbb{Z} := \{ n \cdot z \in \mathbb{Z} \mid z \in \mathbb{Z} \}$, dit is een equivalentierelatie en de quotiënt verzameling schrijven we als $\mathbb{Z}/n\mathbb{Z}$. Definiëren we hierop $+, \cdot$
$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ door $\bar{a} \cdot \bar{b} := \overline{ab}$, $\bar{a} + \bar{b} = \overline{a+b}$, dan
zien we dat de keuze van representant niet uitmaakt (welgedefinieerdheid)
en dat $\mathbb{Z}/n\mathbb{Z}$ onder $+$ een groep, onder $\cdot$ een monoïde is.
met eenheid $\bar{0}$, inverse $\overline{-a}$ $\quad$ met eenheid $\bar{1}$

We zien overigens dat $\bar{1}, \dots, \bar{n}$ de n verschillende equivalentieklassen in $(\mathbb{Z}/n\mathbb{Z})$ zijn, omdat er bij deling door n precies deze resten 0, $1, \dots, n-1$ kunnen ontstaan.

dan definiëren we $(\mathbb{Z}/n\mathbb{Z})^* := \{ x \in \mathbb{Z}/n\mathbb{Z} \mid \exists y \in \mathbb{Z}/n\mathbb{Z} : \bar{x} \cdot \bar{y} = \bar{1} \}$
En uit de stelling volgt dat $\cdot$ beperkt tot $(\mathbb{Z}/n\mathbb{Z})^*$ en dus $(\mathbb{Z}/n\mathbb{Z})$ een groep is.

Met technieken uit H1 zien we: $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ heeft inverse desda $\exists y \in \mathbb{Z} : \overline{xy} = 1$, dus $xy = 1 + k \cdot n$, $\exists k \in \mathbb{Z}$, dus desda (1.9): $\exists y, k \in \mathbb{Z}$: $xy + (-k)n = 1$, desda (1.9) $ggd(a, n) = 1$

dus $(\mathbb{Z}/n\mathbb{Z})^* = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid x$ en n zijn relatief priem $\}$

Def $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^* = \# \{ m \in \{1, \dots, n\} \mid ggd(m, n) = 1 \}$
we noemen $\varphi : \mathbb{Z} \to \mathbb{Z}$ de φ-functie van Euler.

Vb als $a \equiv b \mod n$ (dat is andere notatie voor $a \sim_n b$)
dan geldt, omdat $\bar{a} + \bar{b} := \overline{a+b}$ en $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$ welgedefinieerd zijn, dat als ook $c \equiv d \mod n$, dat $ac \equiv db \mod n$,
$a + c \equiv (b+d) \mod n$. Ihb. omdat $n \equiv 0 \mod n$, geldt voor $a = qb + r$, r de rest bij deling door b, dat $a \equiv r \mod n$
Ook volgen dingen als $a \equiv b \mod n \Rightarrow a - b \equiv 0 \mod n$.

Vb een congruentie of isometrie is een afb $f : \mathbb{R}^2 \to \mathbb{R}$ zdd
voor een gegeven metriek $d : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$
$\forall p, q \in \mathbb{R}^2 : d(f(p), f(q)) = d(p, q)$

De verzameling $E(\mathbb{R}^2) := \{ f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f$ is isometrisch $\}$
is een groep onder samenstelling $\circ$ van functies:
waarbij $f \circ g$ de functie is gegeven door $(f \circ g)(x) = f(g(x))$
$\forall x \in \mathbb{R}^2$
Het blijkt na enige meetkunde (zie dictaat) dat elke $f \in E(\mathbb{R})$ geschreven kan worden als $t_p \circ \sigma_\varphi$ of $t_p \circ \rho_\varphi$
waarbij $t_p(x_1, x_2) := (x_1 + p_1, x_2 + p_2)$ voor zekere $(p_1, p_2) = p \in \mathbb{R}^2$
σ_φ spiegeling in lijn $L \subset \mathbb{R}^2$ met $0 \in L$ en L maakt hoek φ met x-as. ρ_φ rotatie rond 0 onder een hoek van φ graden.
de eenheid is $id_{\mathbb{R}^2}$, $t_p^{-1} = t_{-p}$, $\rho_\varphi^{-1} = \rho_{-\varphi}$, $\sigma_\varphi^{-1} = \sigma_\varphi$

$O_2(\mathbb{R}) : \{ f \in S(\mathbb{R}^2) \mid f \text{ lineair}, f \text{ orthogonaal} \}$

$\Downarrow$

$\|f(x)\| = \|x\|$

Vb als we verder nog eisen dat f lineair is, zien we dat de translaties afvallen en dus dat de groep die dan ontstaat, $O(\mathbb{R}^2)$ of $O_2(\mathbb{R})$ Deze bestaat alleen nog uit rotaties en spiegelingen. orthogonale groep. De speciale orthogonale groep $SO_2(\mathbb{R})$ heeft ook: voor alle $f \in SO_2(\mathbb{R})$ is $\det(f) = 0$.

Vb alle $f \in O(\mathbb{R}^2)$ die een regelmatige n-hoek met hoekpunten op de eenheidscirkel (of een cirkel met als middelpunt 0) in zichzelf overvoeren, vormen de groep D_n, de diedergroep.

Voor $r := \rho_{\frac{2\pi}{n}}$, $s = \sigma_0$ is deze groep te schrijven als:

$$D_n := \{ r^k \in O(\mathbb{R}^2) \mid k \in \{0, \dots n-1\} \} \cup \{ sr^k \in O(\mathbb{R}^2) \mid k \in \{0, \dots n-1\} \}$$

Ihb. waar $O(\mathbb{R}^2)$ oneindig veel elementen had, heeft D_n er $2n$.

Bovendien: $\underbrace{r^n = r^0}$ $= id$, $\underbrace{s^2 = id}$, $sr^k = r^{n-k}s = r^{-k}s$

hierom kan men exponenten van rotaties modulo n nemen en van spiegelingen modulo 2.

2.20 (Linksaxioma's) Neem de volgende 2 axioma's:

(G2') $\exists e^* \in G : \forall g \in G : \quad e^* \circ g = g$ links-eenheid

(G3') $\forall g \in G : \exists g^* \in G : \quad g^* \circ g = e^*$ links-inverse

het blijkt dat $((G1) \wedge (G2') \wedge (G3')) \Rightarrow ((G1) \wedge (G2) \wedge (G3))$

en het blijkt dan dat $e^* = e$, $g^* = g^{-1}$.

Evenzo zijn er rechts-axioma's

(G2'') $\exists e^\# \in G : \forall g \in G : g \circ e^\# = g$

(G3'') $\forall g \in G : \exists g^\# \in G : \quad g \circ g^\# = e^\#$

en $((G1) \wedge (G2'') \wedge (G3'')) \Rightarrow ((G1) \wedge (G2) \wedge (G3))$

Opm G2'' samen met G3' of G2' samen met G3'' impliceren onder G1 niet G2, G3. Gek genoeg. Er zijn tegenvoorbeelden, zie opgave 2.13 uit het dictaat.

St

2.21 G groep ; $\forall a, b \in G : \exists! \, x \in G : \quad ax = b$
namelijk $\quad x = a^{-1}b$.
evenzo $\quad \forall a, b \in G : \exists! \, x \in G : \quad xa = b$
namelijk $\quad ba^{-1}$

Bewijs: merk op dat $a^{-1}b$ voldoet, en dat als x' zodat $ax' = b$
dan $x' = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b = x$. met rechts-
vermenigvuldiging analoog bewijs $\square$

Opm zij $\lambda_a : G \to G$ voor gegeven $a \in G$ gegeven door $\lambda_a : x \mapsto ax, x \in G$
Dan volgt uit bovenstaande dat elke $b \in G$ geraakt wordt door (surjectief)
een $a^{-1}b \in G$, en tevens dat deze uniek is, dus $\lambda_a(x) = \lambda_a(y)$
$\Rightarrow \quad ax = ay \Rightarrow x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = y$
dus ook injectief. Dus $\lambda_a : G \to G$ is bijectie, in $S(G)$

Opm Waarbij $\quad S(G) := \{ f : G \to G \mid f \text{ bijectie} \}$