

Groepen en Ringen 1

8078254

April 28, 2025

Talky talky

We gebruiken Brightspace (!!)

De werkcolleges:

Ma: om aan de inleveropgaven te werken. Er zijn geen TA's aanwezig.

Elke week is er een quiz om zelf te maken. Deze zijn niet verplicht.

Er zijn in totaal drie inleveropgaven. Groepjes van 4. Deze zijn wél verplicht.

Ook moet je twee opgaven presenteren aan een werk-collegebegeleider.

Tijd voor de wiskunde

(“We gaan iets leren over groepen, en dan gaan we iets leren over ringen.”)

Groepen

Het concept groep beschrijft een algebraïsche structuur, vaak symmetrieën.

Het gaat uit van een verzameling met een operatie op de elementen van de verzameling.

Voorbeeld: De verzameling $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ met optelling. Wat zijn handige eigenschappen hiervan?

- Als $a, b \in \mathbb{Z}$ dan $a + b \in \mathbb{Z}$ (“gesloten”)
- Als $a, b, c \in \mathbb{Z}$ dan $(a + b) + c = a + (b + c)$ (“associatief”)
- 0 is cool. $\forall a \in \mathbb{Z}, 0 + a = a + 0 = a$ (“eenheid”)
- Voor elke $a \in \mathbb{Z}$ hebben we ook een $-a \in \mathbb{Z}$
Bovendien: $a + (-a) = (-a) + a = 0$ (“inversen”)
- Als $a, b \in \mathbb{Z}$ dan $a + b = b + a$ (“commutatief”)

Nu wat formeler

Begin met een verzameling G (Eindig of oneindig).

Kies nu een **binaire operatie** op G . Dwz een functie $\star : G \times G \rightarrow G, \underbrace{(a, b)}_{\text{binair}} \mapsto a \star b$.

Definitie $(G, \star)$ is een groep als voldaan wordt aan deze voorwaarden:

1. Associativiteit: als $a, b, c \in G$ dan $(a \star b) \star c = a \star (b \star c)$

2. Eenheid: er bestaat $e = 1_G = 1 \in G$ zodat $e \star g = g \star e = g, \forall g \in G$

3. Inversen: voor elke $a \in G$ bestaat $a^{-1} \in G$ zodat $a \star a^{-1} = a^{-1} \star a = e$

4. **Als** ook nog geldt dat commutativiteit: $a \star b = b \star a, \forall a, b \in G$, **dan** heet de groep **abels** (of commutatief)

Voorbeeld Begin met $\mathbb{Z}$ en kies $n \in \mathbb{Z}_{>0}$.

(DF 0.3) Voor iedere $a \in \mathbb{Z}$ bekijken we de rest nadeling door n dwz $a = kn + b, k \in \mathbb{Z}$ en $b \in \{0, 1, \dots, n-1\}$
Ook wel $\bar{a} = b$.

Equivalentierelatie: $a_1 \sim a_2$ als a_1 en a_2 dezelfde rest hebben nadeling door n als $\bar{a}_1 = \bar{a}_2 \Leftrightarrow n | (a_1 - a_2) \Leftrightarrow a_1 \equiv a_2 \pmod{n}$

Dit is een echte equivalentierelatie: reflexiviteit, symmetrie en transitiviteit gelden.

Schrijf $\bar{a} = \{a, a \pm n, a \pm 2n, \dots\}$ voor de equivalentieklasse van $a \in \mathbb{Z}$.

Omdat $a = kn + b$ met $b \in \{0, \dots, n-1\}$, schrijven we alle equivalentieklassen als $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Nu is onze verzameling $G = \{\bar{0}, \dots, \overline{n-1}\} = \mathbb{Z} \setminus n\mathbb{Z}$.

Voor $\bar{a}_1, \bar{a}_2 \in \mathbb{Z} \setminus n\mathbb{Z}$ definiëren we $\bar{a}_1 + \bar{a}_2 = \overline{a_1 + a_2}$
Dat is welgedefinieerd. Dat wil zeggen, onafhankelijk van gemaakte keuzes.

Als $\bar{a}_1 = \bar{c}_1, \bar{a}_2 = \bar{c}_2$ dan $a_1 \equiv c_1 \pmod{n}, a_2 \equiv c_2 \pmod{n}$

Deze optelling is een binaire operatie, en

1. modularekenen is associatief
2. de eenheid is $\bar{0}$
3. de inverse van $\bar{a}$ is $-\bar{a} = \overline{-a}$

Voorbeeld Een opteltabel van $\mathbb{Z} \setminus 6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	0	1	2	3	4	5
$\bar{1}$	1	2	3	4	5	0
$\bar{2}$	2	3	4	5	0	1
$\bar{3}$	3	4	5	0	1	2
$\bar{4}$	4	5	0	1	2	3
$\bar{5}$	5	0	1	2	3	4

En nu, een vermenigvuldigingstabel!

¹Hoeft niet letterlijk 1 te zijn. Alleen maar notatie.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	0	0	0	0	0	0
$\bar{1}$	0	1	2	3	4	5
$\bar{2}$	0	2	4	0	2	4
$\bar{3}$	0	3	0	3	0	3
$\bar{4}$	0	4	2	0	4	2
$\bar{5}$	0	5	4	3	2	1

Stel dat we daar nu een groep van willen maken:

De eenheid wordt $\bar{1}$. Maar we hebben ook nog inverses nodig.

De enige elementen in $\mathbb{Z} \setminus n\mathbb{Z}$ met inverses zijn $(\mathbb{Z} \setminus n\mathbb{Z})^x = \{\bar{a} \in \mathbb{Z} \setminus n\mathbb{Z} \mid \text{a copriem met } n\}$. Dus $(\mathbb{Z} \setminus 6\mathbb{Z})^x = \{\bar{1}, \bar{5} = -\bar{1}\}$

Dus $(\mathbb{Z} \setminus n\mathbb{Z})^x$ is een groep onder vermenigvuldiging.

And now, for something completely different

Kies groep $(G, \star)$ **Lemma 1** De eenheid $1 = 1_G$ is uniek.

Bewijs Stel dat er twee eenheden zijn, e en f . Dan geldt $e = e \star f = f \square$

Lemma 2 De inverse a^{-1} van $a \in G$ is uniek.

Bewijs Neem het maar even aan.

Lemma 3 $(a \star b)^{-1} = b^{-1} \star a^{-1}$

Bewijs Door Lemma 2 hoeven we alleen te bewijzen dat

$$(b^{-1} \star a^{-1}) = (a \star b) = 1$$

$$b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star 1 \star b = b^{-1} \star b = 1 \square$$

Lemma 4 Als $a \star u = a \star v$ dan $u = v$

Bewijs Neem aan