Groepen en Ringen

8078254

May 6, 2025

Talky talky

In which Wooclap and technical issues waste our time.

Ondergroepen

Definitie. Zij G een groep (met een operatie $\cdot$).
Een ondergroep van G is een deelverzameling $H \subset G$ zodat H (met operatie $\cdot$) ook een groep is.
Notatie: $H \leq G$
Daarvoor geldt:

1. H is gesloten onder $\cdot$, d.w.z. $x, y \in H \Rightarrow x \cdot y \in H$
2. $\cdot$ is nog steeds associatief op H
3. H heeft een eenheid (Dezelfde als G)
4. Alle inverses x^{-1} voor $x \in H$ zitten ook in H

Voorbeelden: $(\mathbb{Q}, +) \geq (\mathbb{Z}, +) \geq (\mathbb{Z}_{\text{even}}, +)$
Opmerkingen:

- Een groep is altijd een ondergroep van zichzelf
- De lege verzameling mag niet, want die kan geen eenheid hebben
- De triviale ondergroep bestaat uit alleen de eenheid. $1_G \leq G$

Hoe check je voor een willekeurige $H \subset G$ of het een ondergroep is?
Het ondergroepcriterium:

1. $H \neq \emptyset$
2. $\forall x, y \in H$ geldt $xy^{-1} \in H$

Criterium 2. vat eigenlijk de 4 criteria van de ondergroep samen, dus zo kun je snel checken of iets een ondergroep is.

Voorbeeld. In de diëdergroep $D_{2n} = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$ zit de niet-lege deelverzameling $H = \{1, r, \dots, r^{n-1}\}$ van rotaties.
Check het criterium: Kies twee elementen $r^m, r^k \in H, (0 \leq m \leq k < n)$ (zonder verlies van algemeenheid)
Dan $r^m(r^k)^{-1} = r^m r^{-k} = r^{m-k} \in H$

Opmerking. Als G eindig is, dan geldt voor $H \subset G$:
"gesloten onder operatie" $\Rightarrow$ "bevat alle inverses"

Voor een vaste groep G kunnen we al haar ondergroepen bekijken.

$$H_1, H_2, \dots,$$

Teken een *ondergroepdiagram.* Zie aantekeningen docent (!!) voor tekening.
Hierin komt bovenaan G te staan, en onderaan $\{1_G\}$

- Ondergroepen geordend "naar grootte"
- "H_1–H_2" H_2 een ondergroep van H_1

Voorbeeld. De *Klein-4 groep* V_4 heeft 4 elementen $\{1, a, b, c\}$ en a, b, c alle drie orde 2. Het diagram is te zien in de aantekeningen van de docent.

Opmerkingen.

- Als twee groepen isomorf zijn, hebben ze hetzelfde diagram. Andersom hoeft niet!
- Ondergroepen kunnen alleen een rang hebben die de vorige deelt.

Cyclische groepen

Definitie. Een groep H is cyclisch als als ze één voortbrenger heeft, zeg x. Dat wil zeggen dat ieder element van H van de vorm x^n is voor een n.
Ofwel, dat $H = \{\dots, x^{-2}, x^{-1}, 1, x, x^1, x^2, \dots\}$.
Notatie: $H = \langle x \rangle$

Lemma. Als H cyclisch is, dan is H abels.
Bewijs. Stel dat $H = \langle x \rangle$ en kies $a = x^m, b = x^n \in H$
Dan $ab = x^m x^n = x^{m+n} = x^{n+m} = x^n x^m = ba$
□

Propositie. Als $H = \langle x \rangle$ dan $|H| = |x|$ "orde van x = orde van H"
Bewijs. Als $|x| = \infty$ dan zijn $\{1, x, x^2, x^3, \dots\}$ allemaal verschillend, want als $x^m = x^n (m > n)$ dan $x^{m-n} = 1$, dus dan heeft x eindig orde.
Maar $\{1, x, x^2, \dots\} \subset H$, dus $|H| = \infty$. ($|H| = \infty \Rightarrow |x| = \infty$ is een opgave voor de lezer)

Als $|x| = n < \infty$ dan zijn tenminste $\{1, x, \dots, x^{n-1}\}$ allemaal verschillend, anders zou x een kleinere orde dan n hebben. Daaruit volgt dat $|H| \geq n$.
Stel dat H nog een ander element heeft: x^t. Schrijf $t = kn + b$ voor $0 \leq b < n$
Dan $x^t = x^{kn+b} = x^{kn} x^b = (\underbrace{x^n}_{=1})^k x^b = x^b \in \{1, \dots, x^{n-1}\}$
Dus x^t "hadden we al" dus $|H| = n = |x|$

In het bijzonder is $\mathbb{Z} \setminus n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ cyclisch, met voortbrenger $\overline{1}$ *of* voortbrenger $\overline{a}$ met $\text{ggd}(a, n) = 1$.
Dus cyclische groepen hebben niet altijd een unieke voortbrenger. Maar …

Stelling Als $H_1 = \langle x \rangle$ en $H_2 = \langle x \rangle$ en $|H_1| = n = |H_2|$ dan is er een isomorfisme $H_1 \tilde{\to} H_2$

Bewijs. Een homomorfisme φ vanaf een cyclische groep is volledig bepaald door waar ze de voortbrenger heenstuurt.
Dat is omdat ieder element van de vorm x^k is, x een voortbrenger en $\varphi(x^k) = \varphi(x) \dots \varphi(x) = \varphi(x)^k$

Dus kies nu $\varphi : x \mapsto y$ en $\varphi(x^k) = \varphi(x)^k$.
φ is surjectief: elk element van H_2 heeft de vorm y^k, dus geldt $y^k = \varphi(x)^k = \varphi(x^k)$. Voor verzamelingen van dezelfde kardinaliteit voldoet het voor bijectiviteit om alleen sur- of injectiviteit te bewijzen.

Opmerking. Voor $\mathbb{Z}$ kunnen we geen andere voortbrenger kiezen; stel dat we kijken naar $\langle b \rangle \subset \mathbb{Z}$ met $b \neq 1$, dan zit 1 er nooit in.