Primitivt Algebra Brevkursus

Malte Kildelund Rosenkilde

27/02/23

Disclaimer

Jeg kommer nok til at lave en masse fejl så tag ikke alt som værende helt korrekt. Så stil endeligt spørgsmål hvis der er noget der ser forkert ud eller ikke giver mening. Stave fejl er nok også noget der kommer til at være meget af. Alt jeg ved er fra bogen Abstract Algebra, 3rd Edition af David S. Dummit og Richard M. Foote så læs i den hvis der er brug for bedre kilder.

Grupper 21/2

Det helt basele i abstract algebra er grupper hvilket er en struktur der ses overalt i matematikken.

Teori

Definition 1. *Lad G være en mængde, da er en function $* : G \times G \to G$ en binær operation.*
Som notation skrives $a * b$ istedet for $*(a, b)$.
En binær operation $*$ kaldes ascosiativ hvis $\forall a, b, c \in G : a * (b * c) = (a * b) * c$.
En binær operation $*$ kaldes kommutativ hvis $\forall a, b \in G : a * b = b * a$.

Definition 2. *En tupel $(G, *)$ med en mængde G og en binær operation $*$ kaldes en gruppe hvis:*
(1) $*$ er ascosiativ.
(2) Der eksistere et element $e \in G$ så $\forall a \in G : a * e = e * a = a$ kaldet det neutrale element.
(3) For alle elementer $a \in G$ eksistere $a^{-1} \in G$ så $a * a^{-1} = a^{-1} * a = e$ kaldet det inverse element til a.
En gruppe kaldes abelsk hvis $*$ er kommutativ.
Ofte kalder betegner man G for gruppen istedet for $(G, *)$ og da er operationen implicit.

Som notation bruges der ofte $\cdot$ som operation istedet for $*$ og $a \cdot b$ bliver ofte skrevet ab istedet. Det neutrale element bliver så betegnet 1. Dog er det normalt at bruge $+$ for opreationen i abelsek grupper og at bruge $-a$ istedet for a^{-1}. Dog er $-$ ikke en operation her men der skrives stadig $a - b$ istedet for $a + -b$.

Sætninger

Sætning 1. *Neutrale elementer er unikke. Altså givet en gruppe $(G, *)$ og to elementer $e_1, e_2 \in G$ hvor $\forall a \in G : e_1 * a = a * e_1 = a$ og $e_2 * a = a * e_2 = a$ da er $e_1 = e_2$.*

Proof.

$$e_1 = e_1 * e_2 = e_2$$

□

Vis selv

Sætning 2. *Invers elementer er unikke. Altså givet en gruppe $(G, *)$ og tre element $a, a_1^{-1}, a_2^{-1} \in G$ hvor $a * a_1^{-1} = a_1^{-1} * a = e$ og $a * a_2^{-1} = a_2^{-1} * a = e$ da er $a_1^{-1} = a_2^{-1}$.*

Sætning 3. *Givet en gruppe $(G, *)$ og et element $a \in G$ da er $(a^{-1})^{-1} = a$.*

Sætning 4. *Givet en gruppe $(G, *)$ og to elementer $a, b \in G$ da er $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Homomorphier 22/2

En vigtig del af abstract algebra er at se på relationer mellem forskellige strukture hvilket gøres ved hjælp af homomorphier og isomorphier.

Definitioner

Definition 3. *Lad $(G, *)$ og $(G, \diamond)$ være to grupper og $\varphi : G \to H$ være en function. Da kaldes φ en gruppe homomorphi hvis*

$$\forall a, b \in G : \varphi(a * b) = \varphi(a) \diamond \varphi(b)$$

En bijektiv homomorphi kaldes en isomorphi.
To grupper G og H kaldes isomorphe hvis der eksistere en isomorphi mellem dem. Dette skrives $G \cong H$.
En isomorphi $\varphi : G \to G$ mellem en gruppe G og den selv kaldes for en automorphi på G.

Definition 4. *Lad G og H være to grupper med identiterter e_G og e_H og $\varphi : G \to H$ være en homomorphi. Da betegner kernen af φ mængde af elementer som bliver afbilledet til e_H.*

$$\ker(\varphi) = \{g \in G | \varphi(g) = e_H\}$$

Sætninger

Sætning 5. *For to grupper $(G, *)$ og $(H, \diamond)$ med neutrale elementer e_G og e_H og en homomorphi $\varphi : G \to H$ da er $\varphi(e_1) = e_2$.*

Proof.

$$\varphi(e_G) = \varphi(e_G) \diamond e_H = \varphi(e_G) \diamond \varphi(e_G) \diamond \varphi(e_G)^{-1} = \varphi(e_G * e_G) \diamond \varphi(e_G)^{-1} = \varphi(e_G) \diamond \varphi(e_G)^{-1} = e_H$$

□

Vis selv

Sætning 6. *For to grupper G og H, en homomorphi $\varphi : G \to H$ og et element $a \in G$ da er $\varphi(a)^{-1} = \varphi(a^{-1})$.*

Sætning 7. *For to grupper G og H eksistere der altid en homomoprhi mellem dem.*

At to grupper er isomorphe betyder at deres struktur er meget ens og isomorphier fungere næsten som en ekvilens relation hvilket ses i følgene opgave.

Sætning 8. *Isomorphier opfylder kravende for en ekvivilens relation:*
$\cong$ *er refleksiv altså $G \cong G$ for alle grupper G.*
$\cong$ *er symmetrisk altså $G \cong H \Leftrightarrow H \cong G$ for alle grupper G og H.*
$\cong$ *er transitiv altså $G \cong H \wedge H \cong K \Rightarrow G \cong K$ for alle grupper G, H og K.*

Årsagen til at det ikke er en ekvivilens relations skyldes at mængde lærer ikke kan lide at konstruere en mængde af alle grupper og der dermed ikke er en mængde ekvivilens relationen kan være over.

Sætning 9 ($\star$)**.** *Lad G og H være to grupper med identiterter e_G og e_H og $\varphi : G \to H$ være en homomorphi. Da er φ injektiv hvis og kun hvis $\ker(\varphi) = \{e_G\}$.*

Denne sætninger ret relevant så jeg skriver beviset i næste opdatering, det er dog stadig en ret god øvelse at vise.

Undergrupper 23/2

Opsamling

Her er beviset for sætning 9.

Proof. Lad $a, b \in G$. Hvis $\ker(\varphi) = e_G$ da ses det at

$$\varphi(a) = \varphi(b) \Rightarrow \varphi(a * b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H \Rightarrow a * b^{-1} \in \ker(\varphi) \Rightarrow a * b^{-1} = e_G \Rightarrow a = b$$

Hvis $\ker(\varphi)$ ikke er triviel er functionen åbenlyst ikke injektiv. □

Definitioner

Fra nu af vil noten skifte over til multiplikativ notation så operationer er underforstået i forhold til hvor de sker og der bliver brugt. 1 bliver også brugt som enhed. $a \cdot b$ eller bare ab.

Definition 5. *Lad G være en gruppe og $H \neq \emptyset \subseteq G$ være en delmængde. Da er H en undergruppe af G noteret $H \leq G$ hvis*
(1) $x \in H \Rightarrow x^{-1} \in H$
(2) $x, y \in H \Rightarrow xy \in H$

Notation 1. *Lad G være en gruppe, $H \leq G$ og $g \in G$. Da er der følgende notation*
$gH = \{gh | \forall h \in H\}$ Kaldet en venstrsideklasse.
$Hg = \{hg | \forall h \in H\}$ Kaldet en højresideklasse.
$gHg^{-1} = \{ghg^{-1} | \forall h \in H\}$ Kaldet H konjugeret med g ligesom ghg^{-1} er h konjugeret med g.

Sætninger

Sætning 10. *Lad G være en gruppe og $H \leq G$. For elementer $a, b \in G$ da er $aH = bH$ eller $aH \cap bH = \emptyset$.*

Proof. Antag at der eksister $c \in aH \cap bH$. Da ligger c både i aH og i bH så der må eksistere h_1, h_2 så $c = ah_1$ og $c = bh_2$. Da ses det at

$$ah_1 = bh_2 \Rightarrow a = bh_2h_1^{-1}$$

Lad nu d være et element i aH. Da ses det at

$$d = ah_3 = bh_2h_1^{-1}h_3$$

Men da h_1, h_2 og h_3 ligger i H må $h_2h_1^{-1}h_3$ ligge i H da H er en undegruppe. Altså må d ligge i bH og dermed er $aH \subseteq bH$. Det ses symmetrisk at $bH \subseteq aH$ hvilket medføre $aH = bH$. □

Vis selv

Sætning 11. *Lad G være en gruppe og $H \leq G$. Da gælder det at $1 \in H$.*

Sætning 12. *Lad G og H være to grupper og $\varphi : G \to H$ være en homomorphi. Da er både $\ker(\varphi)$ og $\varphi(G)$ undergrupper af H.*
(Note: $\varphi(G)$ er billedet af φ ofte skrevet $im(\varphi)$.)

Sætning 13. *Lad G være en gruppe, $H \leq G$ og $a, b \in G$. Da er $|aH| = |bH|$. Hvilket er ekvivilent med at der eksistere en bijektion mellem $|aH|$ og $|bH|$.*

Sætning 14 (Lagrange ⋆)**.** *Lad G være en endelig gruppe og $H \leq G$. Da gælder det at*

$$|H| \,\Big|\, |G|$$

Læses $|H|$ deler $|G|$.

(Hint: Benyt sætning 13 og 10.)

Normale undergrupper 24/2

Idag bliver lidt kortere.

Opsamling

Her er beviset for 14.

Proof. For et givent element $g \in G$ må $g \in gH$ da $1 \in H$. Fra sætning 10 ses det så at H sideklasserne er en partition af G. Lad K betgne mægnden af H sideklasser da må

$$|G| = \sum_{S \in K} |S|$$

Fra 13 fåes det at alle H sideklasser har samme størelser og da H er en H sideklasse har de alle størelse $|H|$. Det ses så at

$$|G| = \sum_{S \in K} |S| = \sum_{S \in K} |H| = |H| \cdot |K|$$

Da G er endelig må både H og K være endelige og $|G|$, $|H|$ og $|K|$ må da være hele tal og derfor må $|H| \Big| |G|$. □

Definitioner

Det giver nu mening at tale om mængden af sideklasser.

Definition 6. *Lad G være en gruppe og $H \leq G$. Da betegner $|G : H|$ antallet af H sideklasser. $|G : H|$ kan godt være uendelig.*

Definition 7. *Lad G være en gruppe og $H \leq G$. Da er H en normal undergruppe hvis*

$$\forall g \in G : gHg^{-1} = H$$

Hvilket skrives $H \trianglelefteq G$.

Vis selv

Sætning 15. *Lad G og H være grupper og $\varphi : G \to H$ være en homomorphi. Da er $\ker(\varphi) \trianglelefteq H$.*

Kvotientgrupper 25/2

Definitioner

Definition 8. *Lad G være en gruppe og $H \trianglelefteq G$ da betegner G/H gruppen af H sideklasserne hvor for to side klasser aH og bH hvor a og b er to vilkårlige representanter er $aH \cdot bH = abH$. Denne gruppe er kaldet en kvotientgruppe. Homomorphien $\pi : G \to G/H$ defineret ved $\pi(g) = gH$ er kaldet den kanoniske afbildning.*

Definition 9. *Lad G være en gruppe og $H \leq G$. Da er der følgende undergrupper:*

$$N_G(H) = \{g \in G | gHg^{-1} = H\}$$

Kaldet normalisatoren til H.

$$C_G(H) = \{g \in G | \forall h \in H : gh = hg\}$$

Kaldet centralisatoren til H. $Z(G) = C_G(G)$ kaldet centeret i G.

Sætninger

Sætning 16. *Kvotientgruppe operationen er veldefineret.*

Proof. Lad $a, a', b, b' \in G$ så $aH = a'H$ og $bH = b'H$. Da eksistere $h_1, h_2 \in H$ så $a' = ah_1$ og $b' = bh_2$. Betragt nu

$$a'b'H = ah_1bh_2H = abb^{-1}h_1bH$$

Men da H er en normal under gruppe ligger $b^{-1}h_1b = h_3 \in H$.

$$a'b'H = abb^{-1}h_1bH = abh_3H = abH$$

Ergo er valget af representatner for gruppe operationen ligegyldig og operationen er dermed veldefineret. □

Sætning 17. *Kvotientgrupper er grupper.*

Proof. Det ses at der både er inverser, et neutralt element og at operationen er asosiativ:
$1H \cdot aH = aH$,
$aH \cdot a^{-1}H = 1H$,
$aH(bH \cdot cH) = aH \cdot bcH = abcH = abH \cdot cH = (aH \cdot bH)cH$. □

Sætning 18. *Lad G være en gruppe og $H \leq G$. Da gælder det at*

$$H \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$$

Proof.

$$aH = bH \Leftrightarrow \exists h \in H : b = ah \Leftrightarrow \exists h \in H : a^{-1}b = h \Leftrightarrow a^{-1}b \in H$$

Første biimplikation fåes fra sætning 10. □

Vis selv

Sætning 19. *Lad G væren en gruppe og $H \leq G$, da er både $C_G(H)$ og $N_G(H)$ undergrupper af G.*

Sætning 20. *Lad G være en gruppe og $H \trianglelefteq G$ da er den kanoniske afbildning en homomorphi.*

Opgave 1. *Vis at $(3\mathbb{Z}, +)$ er en gruppe og bestem $\mathbb{Z}/3\mathbb{Z}$.*
Bestem $\mathbb{Z}/n\mathbb{Z}$ for et naturligt tal n.
(Bemærkning: $n\mathbb{Z} = \{n \cdot a | \forall a \in \mathbb{Z}\}$.)

Sætning 21 (Første isomorphi sætning $\star$)**.** *Lad G og H være grupper og lad $\varphi : G \to H$ være en gruppe homomorphi. Da er $G/\ker(\varphi) \cong \varphi(G)$.*

Isomorphi sætninger del 1 26/2

Opsamling

Her er beviset for sætning 21.

Proof. Betragt functionen $\pi : G/\ker(\varphi) \to \phi(G)$ defineret ved

$$\pi(g\ker(\varphi)) = \varphi(g)$$

Først ses det at π er veldefineret. Så antag $g\ker(\varphi) = g'\ker(\varphi)$. Der eksistere $k \in \ker(\varphi)$ så

$$\pi(g\ker(\varphi)) = \varphi(g) = \varphi(g'k) = \varphi(g')\varphi(k) = \varphi(g') = \pi(g'\ker(\varphi))$$

Det ses nu at π er en homomorphi:

$$\pi(a\ker(\varphi)b\ker(\varphi)) = \pi(ab\ker(\varphi)) = \varphi(ab) = \varphi(a)\varphi(b) = \pi(a\ker(\varphi))\pi(b\ker(\varphi))$$

Det ses let at π er surjektiv da hvis $h \in \varphi(G)$ eksistere g så $\varphi(g) = h$ og da er $\pi(g\ker(\varphi)) = \varphi(g) = h$. Det ses også at π er injektiv da

$$\pi(g\ker(\varphi)) = 1 \Rightarrow \varphi(g) = 1 \Rightarrow g \in \ker(\varphi) \Rightarrow g\ker(\varphi) = 1\ker(\varphi)$$

Da er kernen af π triviel og fra sætning 9 må π være injektiv. Ergo er π en isomorphi. □

Definitioner

Definition 10. *Lad G være en gruppe og A og B være undergrupper af G. Da betegner*

$$AB = \{ab | \forall a \in A \forall b \in B\}$$

Sætninger

Sætning 22. *Lad G være en gruppe og $A \subseteq N_G(B)$ og B være undergrupper af G. Da er $AB \leq G$.*

Proof. Betragt $a \in A$ og $b \in B$ da $A \subseteq N_G(B)$ er $ab^{-1}a^{-1} = b' \in B$ og

$$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}ab^{-1}a^{-1} = a^{-1}b'$$

Da $a^{-1} \in A$ og $b' \in B$ ses det så at $(ab)^{-1} \in AB$. Betragt nu $a_1, a_2 \in A$ og $b_1, b_2\ inB$ da må $a_2^{-1}b_1a_2 = b' \in B$ det ses så at

$$a_1b_1a_2b_2 = a_1a_2a_2^{-1}b_1a_2b_2 = a_1a_2b'b_2$$

ergo ligger $(a_1b_1)(a_2b_2)$ i AB og AB må være en undergruppe. □

Sætning 23 (Den anden isomorphi sætning)**.** *Lad G være en gruppe og $A \subset N_G(B)$ og B være undergrupper af G. Da er $B \trianglelefteq AB$, $a \cap B \trianglelefteq A$ og $AB/B \cong A/A \cap B$.*

Proof. Beviset for at $B \trianglelefteq AB$ og $A \cap B \trianglelefteq A$ undlades til læseren(Dagens opgaver). Bestem $\varphi : A \to AB/B$ ved $\varphi(a) = aB$. Da ses det at φ er en homomorphi:

$$\varphi(aa') = aa'B = aBa'B = \varphi(a)\varphi(a')$$

Vi bestemmer nu $\ker(\varphi)$ så betragt $a \in A$ så $\varphi(a) = 1B$ Da må $aB = \varphi(a) = 1B$ ergo må $a \in B$ og kernen er dermed $A \cap B$. Det ses også at φ er surjectiv da $aB = \varphi(a')$ for enhver representant $a' \in aB$. Fra sætning 21 fåes det så at

$$A/A \cap B = A/\ker(\varphi) \cong \varphi(A) = AB/B$$

□

Isomorphi sætninger del 2 27/2

Vis selv

Sætning 24. *Lad G være en gruppe, $H \trianglelefteq G$, $K \trianglelefteq G$ og $H \leq K$.*
Da er $K/H \trianglelefteq G/H$ og

Sætninger

Sætning 25 (Tredje isomorphi sætning)**.** *Lad G være en gruppe, $H \trianglelefteq G$, $K \trianglelefteq G$ og $H \leq K$.*
Da er $(G/H)/(K/H) \cong G/K$

Proof. Definer $\varphi : G/H \to G/K$ ved $\varphi(gH) = gK$. Først ses det at φ er veldefineret. Lad $gH = g'H$ da eksister h så $g' = gh$. Da $H \leq K$ ses det at

$$\varphi(g'H) = g'K = ghK = gK$$

Vi bestemmer nu $\ker(\varphi)$.

$$\begin{aligned}\ker(\varphi) &= \{gH \in G/H | \varphi(gH) = 1K\} \\ &= \{gH \in G/H | gK = 1K\} \\ &= \{gH \in G/H | g \in K\} \\ &= K/H\end{aligned}$$

Det ses let at φ er surjektiv og fra sætning 21 ses det så at

$$(G/H)/(K/H) = (G/K)/\ker(\varphi) \cong= \varphi(G/K) = G/K$$

$\square$

Af isomorphi sætninger er det den første der er den stærkeste hvilket de to andre viser da beviserne falder ud ved at betragte den mest trivielle homomorphi og der efter bruge første isomorphi sætning.

Næste gang begynder vi på det sidste store resultat i gruppe teori vi vil se på før vi går videre til ringe og legmer.