

# Primitivt Algebra Brevkursus

Malte Kildelund Rosenkilde

24/02/23

## 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  $*$  :  $G \times G \rightarrow G$  en binær operation.

Som notation skrives  $a * b$  istedet for  $*(a, b)$ .

En binær operation  $*$  kaldes asociativ 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 asociativ.

(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 operationen i abelske 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 strukturer hvilket gøres ved hjælp af homomorphier og isomorphier.

### Definitioner

**Definition 3.** Lad  $(G, *)$  og  $(G, \diamond)$  være to grupper og  $\varphi : G \rightarrow H$  være en function. Da kaldes  $\varphi$  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 isomorfe hvis der eksisterer en isomorphi mellem dem. Dette skrives  $G \cong H$ .

En isomorphi  $\varphi : G \rightarrow G$  mellem en gruppe  $G$  og den selv kaldes for en automorphi på  $G$ .

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

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

### Sætninger

**Sætning 5.** For to grupper  $(G, *)$  og  $(H, \diamond)$  med neutrale elementer  $e_G$  og  $e_H$  og en homomorphi  $\varphi : G \rightarrow H$  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  $\varphi : G \rightarrow H$  og et element  $a \in G$  da er  $\varphi(a)^{-1} = \varphi(a^{-1})$ .

**Sætning 7.** For to grupper  $G$  og  $H$  eksisterer der altid en homomorphi mellem dem.

At to grupper er isomorfe betyder at deres struktur er meget ens og isomorphier fungerer næsten som en ekvivalens relation hvilket ses i følgende opgave.

**Sætning 8.** Isomorphier opfylder kravene for en ekvivalens 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 ekvivalens relations skyldes at mængde lærer ikke kan lide at konstruere en mængde af alle grupper og der dermed ikke er en mængde ekvivalens relationen kan være over.

**Sætning 9**  $(*)$ . Lad  $G$  og  $H$  være to grupper med identiteter  $e_G$  og  $e_H$  og  $\varphi : G \rightarrow H$  være en homomorphi.

Da er  $\varphi$  injektiv hvis og kun hvis  $\ker(\varphi) = \{e_G\}$ .

Denne sætning er 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 trivial er funktionen 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 venstresideklasse.

$Hg = \{hg | \forall h \in H\}$  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 undergruppe. Altså må  $d$  ligge i  $bH$  og dermed er  $aH \subseteq bH$ . Det ses symmetrisk at  $bH \subseteq aH$  hvilket medfører  $aH = bH$ . □

### 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  $\varphi : G \rightarrow H$  være en homomorphi. Da er både  $\ker(\varphi)$  og  $\varphi(G)$  undergrupper af  $H$ .

(Note:  $\varphi(G)$  er billedet af  $\varphi$  ofte skrevet  $\text{im}(\varphi)$ .)

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

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

$$|H| \mid |G|$$

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  $K$  betegne mængden af  $H$  sideklasser da må

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

Fra 13 fås det at alle  $H$  sideklasser har samme størrelse og da  $H$  er en  $H$  sideklasse har de alle størrelse  $|H|$ . 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  $|H| \mid |G|$ .  $\square$

### 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  $\varphi : G \rightarrow H$  være en homomorphi. Da er  $\ker(\varphi) \trianglelefteq G$ .