

# Primitivt Algebra Brevkursus

Malte Kildelund Rosenkilde

29/03/23

## 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**  $(\star)$ . 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  $\ker(\varphi) \trianglelefteq G$ .

## 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 repræsentanter er  $aH \cdot bH = abH$ . Denne gruppe er kaldet en kvotientgruppe. Homomorphismen  $\pi : G \rightarrow G/H$  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:

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

Kaldet normalisatoren til  $H$ .

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

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 repræsentanter for gruppe operationen ligegyldig og operationen er dermed veldefineret.  $\square$

**Sætning 17.** Kvotientgrupper er grupper.

*Proof.* Det ses at der både er inverser, et neutralt element og at operationen er assosiativ:

$$1H \cdot aH = aH,$$

$$aH \cdot a^{-1}H = 1H,$$

$$aH(bH \cdot cH) = aH \cdot bcH = abcH = abH \cdot cH = (aH \cdot bH)cH. \quad \square$$

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

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

*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 fås fra sætning 10.  $\square$

### Vis selv

**Sætning 19.** Lad  $G$  være 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 homomorphism.

**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:  $n\mathbb{Z} = \{n \cdot a \mid \forall a \in \mathbb{Z}\}$ .)

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

# Isomorphi sætninger del 1 26/2

## Opsamling

Her er beviset for sætning 21.

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

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

Først ses det at  $\pi$  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  $\pi$  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  $\pi$  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  $\pi$  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  $\pi$  trivial og fra sætning 9 må  $\pi$  være injektiv. Ergo er  $\pi$  en isomorphi.  $\square$

## 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  $b_1, b_2 \in B$  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.  $\square$

**Sætning 23** (Den anden isomorphi sætning). Lad  $G$  være en gruppe og  $A \subseteq N_G(B)$  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  $\varphi : A \rightarrow AB/B$  ved  $\varphi(a) = aB$ . Da ses det at  $\varphi$  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  $\varphi$  er surjektiv da  $aB = \varphi(a')$  for enhver representant  $a' \in aB$ . Fra sætning 21 fås det så at

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

$\square$

## 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  $\varphi : G/H \rightarrow G/K$  ved  $\varphi(gH) = gK$ . Først ses det at  $\varphi$  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  $\ker(\varphi)$ .

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

Det ses let at  $\varphi$  er surjektiv og fra sætning 21 ses det så at

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

□

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.



## Start på Sylow

Vi kan nu begynd at gennemgå nogle sætninger der skal bruges til at vise Sylows sætninger.

### Definitioner

**Definition 11.** Lad  $G$  være en gruppe og lad  $g \in G$ . Da betegner  $g^0 := 1$ . For  $n \in \mathbb{N}$  betegner  $g^n := g^{n-1} \cdot g$  og  $g^{-n} := g^{-n+1} \cdot g^{-1}$ .

**Definition 12.** Lad  $G$  være en gruppe og lad  $g \in G$ . Da er ordenen af  $g$  det mindste tal  $n \in \mathbb{N}$  så  $g^n = 1$ . Dette skrives  $|g| = n$  hvis sådan tal ikke eksistere skrives  $|g| = \infty$ .

**Definition 13.** Lad  $G$  være en gruppe og  $g_1, g_2, \dots, g_n \in G$ . Da betegner  $\langle g_1, g_2, \dots, g_n \rangle$  den mindste undergruppe af  $G$  der indeholder  $g_1, g_2, \dots, g_n$ .

**Definition 14.** Lad  $G$  være en gruppe og  $H, K \leq G$ . Da betegner

$$HK := \{hk | \forall h \in H \forall k \in K\} = \bigcup_{h \in H} hK$$

### Vis selv

**Sætning 26.** Lad  $G$  være en gruppe og  $g \in G$ . Da er  $|g| = |\langle g \rangle|$ .

**Sætning 27.** Lad  $G$  være en gruppe,  $g \in G$  og  $n \in \mathbb{N}$ . Da er

$$|x^n| = \frac{|x|}{\gcd(|x|, n)}$$

### Sætninger

**Sætning 28.** Lad  $G$  være en gruppe og  $H, K \leq G$ . Da er

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

*Proof.* Da

$$HK = \{hk | \forall h \in H \forall k \in K\} = \bigcup_{h \in H} hK$$

Hvilket betyder at der skal tælles forskellige  $K$  side klasser i  $H$ . Det ses dog for  $h_1, h_2 \in H$  at

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K)$$

Altså er antallet af  $hK$  sideklasser for  $h \in H$  antallet af  $H \cap K$  sideklasser i  $H$ . Det ses fra lagrange at dette antal er  $\frac{|H|}{|H \cap K|}$  og da hver  $K$  sideklasse indeholder  $|K|$  elementer fåes det ønskede:

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

□

**Sætning 29.** Lad  $G$  være en abelsk gruppe hvor  $p \mid |G|$  hvor  $p$  er et primtal. Da eksistere et element med orden  $p$ .

*Proof.* Sætningen gælder trivielt hvis  $|G| = p$ . Antag for induction at sætningen gælder for alle grupper  $|H| < |G|$ . Betragt et element  $x$  hvor  $p \mid |x| = p \cdot n$ . Da må  $|x^n| = p$ . Hvis  $p \nmid |x|$ . Da  $F$  er abelsk er  $\langle x \rangle \trianglelefteq G$  og dermed er  $|G/\langle x \rangle| < |G|$ . Fra Lagrange og  $p \nmid |x|$  ses det at

$$p \mid |G/\langle x \rangle| = \frac{|G|}{|\langle x \rangle|}$$

Da eksistere en et element  $\bar{y} \in G/\langle x \rangle$  med  $|\bar{y}| = p$ . Da eksistere  $y \in G$  så  $\bar{y} = yN$ . Da ses det at  $y \notin \langle x \rangle$  og  $y^p \in \langle x \rangle$ . Da er  $\langle y^p \rangle \leq \langle x \rangle$  ergo er  $\langle y \rangle \neq \langle y^p \rangle$  og dermed  $p \mid |y|$ . Da er  $|y| = p \cdot n$  og  $|y^n| = p$ . □

# Konjugens klasser

Der er stadig en bid vej til Sylows sætning så vi begynder nu at se på konjugens klasser for at vise klasse sætningen.

## Definitioner

**Definition 15.** Lad  $G$  være en gruppe og  $a, b \in G$ . Da kaldes  $a$  og  $b$  konjugerede af hinanden hvis der eksisterer  $g \in G$  så  $gag^{-1} = b$ .

**Definition 16.** Lad  $G$  være en gruppe og  $H \leq G$  da kaldes  $H$  en konjugens klasse hvis der eksisterer et element  $h \in G$  så

$$H = \{ghg^{-1} | \forall g \in G\}$$

## Sætninger

**Sætning 30.** Lad  $G$  være en gruppe og lad  $H$  være en konjugens klasse med

$$H = \{ghg^{-1} | \forall g \in G\}$$

For et element  $h$ . Da er

$$|H| = |G : C_G(h)|$$

*Proof.* Betragt en afbildningen  $f$  fra sideklasserne til  $C_G(h)$  til  $H$  med

$$f(aC_G(h)) = aha^{-1}$$

Først skal det lige vises at  $f$  er veldefineret. Fra sætning 18 fås det at

$$aC_G(h) = bC_G(h) \Leftrightarrow b^{-1}a \in C_G(h) \Leftrightarrow h = (b^{-1}a)h(b^{-1}a)^{-1} = b^{-1}aha^{-1}b \Leftrightarrow aha^{-1} = bhb^{-1} \Leftrightarrow f(a) = f(b)$$

Dette viser også at  $f$  også er injektiv. Så mangler det blot at  $f$  er surjektiv. Betragt  $a \in H$  da eksisterer  $g$  så

$$a = ghg^{-1} = f(gC_G(H))$$

Hvilket viser at  $f$  er bijektiv hvilket medfører at

$$|H| = |G : C_G(h)|$$

□

**Sætning 31** (Klasse sætningen). Lad  $G$  være en endelig gruppe og lad  $g_1, g_2, \dots, g_r$  være repræsentanter for alle konjugensklasser med mere end et element. Da er

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$$

*Proof.* Fra sætning 32 ses det at konjugens klasser er en partition af  $G$  så alle elementer ikke betragtet i de førnævnte konjugens klasser er de elementer hvor

$$\{ghg^{-1} | \forall g \in G\} = \{a\}$$

Hvilket netop er alle elementer i  $Z(G)$ . Dette giver

$$|G| = |Z(G)| + \sum_{i=1}^r |\{ag_i a^{-1} | \forall a \in G\}| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$$

□

## Vis selv

**Sætning 32.** Lad  $G$  være en gruppe og  $a, b \in G$  være konjugere af hinanden. Da er

$$\{gag^{-1} | \forall g \in G\} = \{gbg^{-1} | \forall g \in G\}$$

og

$$a \in \{gag^{-1} | \forall g \in G\}$$

# Eksistens af Sylow gruppe

Vi er nu klar til at definere og vise eksistensen af Sylow grupper

## Definitioner

**Definition 17.** Lad  $G$  være en endelig gruppe,  $p$  være et primtal hvor  $\exists \alpha, k \in \mathbb{N}_0$  så  $|G| = p^\alpha k$  med  $p \nmid k$ . Da er en Sylow  $p$ -undergruppe en gruppe med orden  $p^\alpha$ .

## Vis selv

**Sætning 33.** Lad  $G$  være en gruppe,  $H \trianglelefteq G$  og  $\bar{P} \leq G/H$ . Da er

$$P = \bigcup_{S \in \bar{P}} S$$

en undergruppe af  $G$  med  $|P| = |\bar{P}| \cdot |H|$ .

**Sætning 34.** Lad  $G$  være en gruppe og  $H \leq Z(G)$ . Da er  $H \trianglelefteq G$ .

## Sætninger

**Sætning 35** (Sylows sætning del 1). Lad  $G$  være en endelig gruppe og  $p$  være et primtal. Da eksisterer en Sylow  $p$ -undergruppe i  $G$ .

*Proof.* Vi vil vise sætningen ved induktion. Sætningen gælder trivielt for  $|G| = 1$ . Da  $G \leq G$  er en undergruppe med  $|G| = p^0$ . Så antag at alle grupper med orden mindre end  $|G|$  har Sylow  $p$ -undergrupper. Antag at  $p \nmid |Z(G)|$ . Fra sætning 29 eksisterer et element  $g \in Z(G)$  med orden  $p$  da  $Z(G)$  er abelsk. Da er  $N = \langle g \rangle$  en undergruppe med orden  $p$ . Da  $N \leq Z(G)$  er  $G/N$  veldefineret. Da  $N \neq \{1\}$  er  $|G/N| < |G|$ . Specielt er  $|G| = \frac{|G|}{p} = p^{\alpha-1}k$ . Fra induktions antagelsen eksisterer en Sylow  $p$ -undergruppe  $\bar{P}$  af  $G/N$  med orden  $p^{\alpha-1}$ . Fra sætning 33 fås en undergruppe  $P$  med  $|P| = |\bar{P}| \cdot |N| = p^\alpha$ . Hvilket fuldfører caset  $p \nmid |Z(G)|$ . Hvi dette ikke gælder kan klasse sætningen betragtes

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$$

Da  $p$  ikke deler  $|Z(G)|$ . Må der eksisterer et  $g_i$  så  $p \nmid |G : C_G(g_i)|$  Men da  $|G : C_G(g_i)| = \frac{|G|}{|C_G(g_i)|}$  må  $p^\alpha$  dele  $|C_G(g_i)|$ . Da  $g_i$  per definition ikke ligger i  $Z(G)$  er  $C_G(g_i) < G$  og dermed er  $|C_G(g_i)| < |G|$ . Fra induktions antagelsen eksisterer en Sylow  $p$ -undergruppe  $P$  af  $C_G(g_i)$  med orden  $p^\alpha$  men da er  $P \leq C_G(g_i) \leq G$ .  $\square$

# Orbits under konjugation

## Definitioner

**Definition 18.** Lad  $G$  være en gruppe og  $H, K \leq G$ . Betragt mængden

$$S = \{gHg^{-1} | \forall g \in G\}$$

For et element  $A \in S$  kaldes følgende mængde for  $A$ 's orbit under operation fra  $K$ .

$$O_A = \{kAk^{-1} | \forall k \in K\}$$

## Vis selv

**Sætning 36.** Lad  $G$  være en gruppe og  $H, K \leq G$ . Da er  $H \cup K \leq H$  og  $H \cup N \leq N$ .

**Sætning 37.** Lad  $G$  være en endelig gruppe,  $g \in G$  og  $H \leq G$ . Da er  $gHg^{-1} \leq G$ .

**Sætning 38.** Lad  $G$  være en gruppe,  $H \leq G$  og  $a, b \in G$  da gælder det at

$$H = (a^{-1}b)H(b^{-1}a) \Leftrightarrow aHa^{-1} = bHb^{-1}$$

**Sætning 39.** Lad  $G$  være en gruppe,  $H, K \leq G$ ,  $S = \{gHg^{-1} | \forall g \in G\}$  og  $O$  være mængden af alle orbits af elementer i  $S$  under operation fra  $K$ . Skrevet som mængde:

$$O = \{\{kAk^{-1} | \forall k \in K\} | \forall A \in S\}$$

Da er  $O$  en partition af  $S$ .

## Sætninger

**Sætning 40.** Lad  $G$  være en gruppe,  $H, K \leq G$ ,  $S = \{kHk^{-1} | \forall k \in K\}$ . Da er

$$|S| = |K : N_K(H)|$$

*Proof.* Lad  $M$  være mængden af  $N_K(A)$  sideklasser i  $K$ . Betragt  $f : M \rightarrow S$  defineret ved  $f(aN_K(A)) = aAa^{-1}$ . Først ses det at  $f$  er veldefineret og injektiv. Betragt  $a, b \in K$ . Da er

$$\begin{aligned} aN_K(A) = bN_K(A) &\Leftrightarrow a^{-1}b \in N_K(A) \\ &\Leftrightarrow A = (a^{-1}b)A(a^{-1}b)^{-1} = (a^{-1}b)A(b^{-1}a) \\ &\Leftrightarrow f(aN_K(A)) = aAa^{-1} = bAb^{-1} = f(bN_K(A)) \end{aligned}$$

Det ses let at  $f$  er surjektiv da for alle  $kAk^{-1}$  er  $f(kN_K(A)) = kAk^{-1}$ . Ergo er  $f$  en bijektion hvilket viser det ønskede.  $\square$

**Korollar 41.** Lad  $G$  være en gruppe,  $H \leq G$  og  $S = \{gHg^{-1} | \forall g \in G\}$ ,  $A \in S$ . Da er

$$|S| = |G : N_G(H)|$$

*Proof.* Dette følger fra sætning 40 med  $K = G$ .  $\square$

**Korollar 42.** Lad  $G$  være en gruppe,  $H, K \leq G$ ,  $S = \{gHg^{-1} | \forall g \in G\}$ ,  $A \in S$  og  $O_A$  være  $A$ 's orbit under operation fra  $K$ . Da er

$$|O_A| = |K : N_K(A)|$$

*Proof.* Dette følger fra sætning 40 da  $A \leq G$  fra sætning 37.  $\square$