TMA4150 – Algebra

Jarl Sondre Sæther

Contents

Chapter 1

Gruppeteori

Dette kapittelet kommer til å dekke gruppeteorien i pensumet.

1.1 Grupper

Definition 1.1.1: Binæroperasjon

La S være en mengde. En **binæroperasjon** på S er da definert som en funksjon $* : S \times S \to S$.

Eksempler:

1. La $S = \mathbb{Z}$ og $* =$ addisjon. Da er $*$ en binæroperasjon på S.
2. La $S = \mathbb{Z}$ og $* =$ multiplikasjon. Da er $*$ en binæroperasjon.
3. Et moteksempel: La $S = \mathbb{N}$ og $* =$ divisjon. Da er $*$ ikke en gyldig binæroperasjon siden det finnes $a, b \in \mathbb{N}$ slik at $a * b = \frac{a}{b} \notin \mathbb{N}$.
4. La $S = \{\text{Alle } m \times n \text{ matriser over } \mathbb{R}\}$ og la $*$ være matriseaddisjon.
5. La $S = \{\text{Alle } m \times n \text{ matriser over } \mathbb{R}\}$ og la $*$ være matrisemultiplikasjon.
6. La $S = \mathbb{R}$ og definer $a * b = \pi \ \forall a, b \in \mathbb{R}$. Da er $*$ en gyldig binæroperasjon.
7. La

$$S = C([0,1]) = \{f : [0,1] \to \mathbb{R} \mid f \text{ er en kontinuerlig funksjon}\} \tag{1.1}$$

og la $*$ være definert som addisjon av funksjoner, altså at

$$(f+g)(x) = f(x) + g(x) \ \forall x. \tag{1.2}$$

Da er $*$ en gyldig binæroperasjon.

Definition 1.1.2: Gruppe

En **gruppe**, $(G, *)$ er en ikke-tom mengde G sammen med en binæroperasjon $*$ på G slik at følgende krav er tilfredsstilte:

$\mathscr{G}1$) $(g * h) * k = g * (h * k) \ \forall g, h, k \in G$. (Assosiativitet)

$\mathscr{G}2$) Det finnes en $e \in G$ med $e * g = g * e = e \ \forall g \in G$. (Identitet)

$\mathscr{G}3$) For alle $g \in G$ så finnes det en $g' \in G$ med $g * g' = g' * g = e$. (Invers)

Definition 1.1.3: Abelsk Gruppe

Dersom en gruppe $(G, *)$ har egenskapen at $g * h = h * g \ \forall g, h \in G$, så kaller vi gruppen **abelsk**. Denne egenskapen kalles også kommutativitet.

Eksempler:

1. $(\mathbb{Z}, +)$ er en abelsk gruppe.
2. $(\mathbb{Z}, *)$ er "nesten" en gruppe, ettersom at $\mathscr{G}1$ og $\mathscr{G}2$ holder, men ikke $\mathscr{G}3$.
3. $G = \{1, -1\}$, $*$ = multiplikasjon er en abelsk gruppe.

   $\mathscr{G}1$) Denne holder fordi det er kjent at multiplikasjon er assosiativt.

   $\mathscr{G}2$) Denne holder med $e = 1$.

   $\mathscr{G}3$) Denne ser vi holder ved $1 * 1 = 1$ og $(-1) * (-1) = 1$.

   Videre er det kjent at multiplikasjon er kommutativt. Dermed er dette en abelsk gruppe.
4. Vi har at $(\mathbb{Q}, +), (\mathbb{R}, +)$ og $(\mathbb{C}, +)$ er abelske grupper.
5. $(\mathbb{N}, +)$ er ikke en gruppe ettersom det ikke finnes inverser for alle tall.
6. $(C([0, 1]), +)$ er en abelsk gruppe med $e = 0$.
7. La $G = \mathcal{M}_2(\mathbb{R})$ og $*$ være matriseaddisjon. Da er $(G, *)$ en abelsk gruppe.
8. La
$$G = \mathrm{GL}(2, \mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) \mid \det A \neq 0\} \tag{1.3}$$
og definer $*$ som matrisemultiplikasjon. Da er $(G, *)$ en gruppe, men den er ikke abelsk.
9. La
$$G = \mathrm{SL}(2, \mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) \mid \det A = 1\} \tag{1.4}$$
og definer $*$ som matrisemultiplikasjon. Da er $(G, *)$ en gruppe, men den er ikke abelsk.
10. $\mathbb{Q} \setminus \{0\}$ med $*$ definert som multiplikasjon er en abelsk gruppe.
11. La $U = \{z \in \mathbb{C} \mid |z| = 1\}$ og $*$ være multiplikasjon. Da er $(U, *)$ en abelsk gruppe.
12. La $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$, altså alle komplekse n-te røtter av tallet 1. Disse kan skrives på formen $e^{\frac{2\pi k}{n}}$ for $k = 1, \ldots, n$. Dette, med multiplikasjon, er en endelig abelsk gruppe.
13. La V være et vektorrom. Da er $(V, +)$ en abelsk gruppe.
14. La $\mathbb{R}^+ = \{a \in \mathbb{R} \mid a > 0\}$. Da er $(\mathbb{R}^+, \cdot)$, hvor $\cdot$ er vanlig multiplikasjon, en abelsk gruppe. Vi kan også lage en ny abelsk gruppe $(\mathbb{R}^+, *)$ ved å definere $a * b = \frac{ab}{\pi}$.

Theorem: 4.15

La $(G, *)$ være en gruppe. Da gjelder følgende:

1. $a * b = a * c \implies b = c$
2. $b * a = c * a \implies b = c$

Bevis: La oss anta at det første punktet gjelder. Da har vi fra $\mathscr{G}3$ at det må eksistere $a' \in G$ slik at $a * a' = e$. Dermed får vi at

$$b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) \tag{1.5}$$
$$= (a' * a) * c = e * c = c, \tag{1.6}$$

altså at $b = c$, som var det vi ville vise. Tilsvarende holder for punkt 2. □

Theorem: 4.17

La $(G, *)$ være en gruppe. Da gjelder følgende:

1. Identiteten e i $\mathscr{G}2$ er unik.
2. Inversen a' i $\mathscr{G}3$ er unik.

Bevis:

1. La oss anta at $e_1, e_2 \in G$ med $e_i * g = g * e_i = g$ for alle $g \in G$. Da følger det at $e_1 = e_1 * e_2 = e_2$. □
2. La $a \in G$ og la oss anta at $a_1, a_2 \in G$ slik at $a * a_i = a_i * a = e$. Da har vi at

$$a_1 = a_1 * e = a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2, \tag{1.7}$$

som var det vi ville vise. □

1.1.1 Multiplikasjonstabell

La oss anta at $(G, *)$ er en endelig gruppe med $|G| = n$. Da kan man liste opp elementene i G i en tabell:

$*$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_n$

La oss se på noen eksempler på forskjellige tabeller:

1. $|G| = 1 \implies G = \{1\}$ og $e * e = e$.
2. $|G| = 2 \implies G = \{e, a\}$. Da får vi følgende tabell

$*$	e	a
e	e	a
a	a	e

   Merk at $a * a = e$ her fordi alle elementer i en gruppe må ha en invers.
3. $|G| = 3 \implies G = \{e, a, b\}$. Da får vi følgende tabell:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

   Her kan man bruke Teorem 4.15 for å vise at $a * a = b$ og $b * b = a$.

Definition 1.1.4: Isomorfe Grupper

La $(G, *_G)$ og $(H, *_H)$ være grupper. Da sier vi at de er **isomorfe** dersom det eksisterer en bijeksjon

$$f : G \to H \tag{1.8}$$

slik at $f(a *_G b) = f(a) *_H f(b)$ for alle $a, b \in G$.

Nå kommer en liste med konvensjoner innenfor algebra:

1. Binæroperasjonen $*$ betegnes som oftest med $\cdot$ eller $+$. Dersom man bruker multiplikativ notasjon så skriver man ofte ab for $a \cdot b$.
2. $+$ er normalt forbeholdt abelske grupper.
3. Identiteten fra $\mathscr{G}2$ betegnes ofte som "1" eller "e" med multiplikativ notasjon og som "0" med additiv notasjon.
4. Inversen fra $\mathscr{G}3$ betegnes ofte som a^{-1} med multiplikativ notasjon og $-a$ med additiv notasjon.
5. La $a \in G$. Dersom vi har multiplikativ notasjon så betegner vi normalt $a^0 = 1$ og $a^n = a \cdots a$ som a ganget med seg selv n ganger. Videre betegner vi $a^{-n} = a^{-1} \cdots a^{-1}$ som a^{-1} ganget med seg selv n ganger.

   Dersom vi har additiv notasjon så betegner vi $n \cdot a = a + \cdots + a$ som a addert med seg selv n ganger og $-n \cdot a = (-a) + (-a) + \cdots + (-1)$ som $-a$ addert med seg selv n ganger.

1.2 Undergrupper

Definition 1.2.1: Ordenen til en gruppe

La G være en gruppe. Da kaller vi $|G|$ for **ordenen** til G og vi sier at G er en **endelig gruppe** dersom $|G| < \infty$.

Definition 1.2.2: Undergruppe

La G være en gruppe. Da sier vi at en delmengde $H \subseteq G$ er en **undergruppe** dersom den tilfredsstiller de følgende kravene:

1. H er lukket under binæroperasjonen på G.
2. H er selv en gruppe med binæroperasjonen på G

Vi skriver i så fall $H \leq G$, med $H < G$ dersom $H \neq G$. Dersom $H < G$, så sier vi at H er en **ekte undergruppe** og vi kaller $\{e\}$ den **trivielle undergruppen**.

Eksempler:

1. La $G = (\mathbb{Z}, +)$ og la $m \in \mathbb{N}$. Definer $H = m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$. Da er $H < G$ for $m \neq 1$ og $H = G$ for $m = 1$.
2. La $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Vi har tidligere sett at $(U, \cdot)$ er en abelsk gruppe. For $m \in \mathbb{N}$, la $U_m = \{z \in \mathbb{C} \mid z^m = 1\}$. Da er $U_m < U$.
3. Selv om $G := (\mathbb{Q}, +)$ er en gruppe og $H := (\mathbb{Q} \setminus \{0\}, \cdot)$ er en gruppe, så er ikke $H < G$ selv om det er en delmengde. Dette er fordi de ikke har samme binæroperasjon.

Theorem: 5.14 (superversjon)

La G være en gruppe og $H \subset G$ en ikke-tom delmengde. Da er H en undergruppe hvis og bare hvis $a, b \in H \implies ab^{-1} \in H$.

Eksempler:

1. Vi har sett at $\mathrm{GL}(2,\mathbb{R})$ er en gruppe med matrisemultiplikasjon. La

$$\mathrm{O}(2,\mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) \mid A \text{ er orthogonal}\} \tag{1.9}$$
$$= \left\{A \in \mathcal{M}_2(\mathbb{R}) \mid A^{-1} = A^\intercal\right\} \tag{1.10}$$

   Da vil $\mathrm{O}(2,\mathbb{R}) \neq \emptyset$ og $\mathrm{O}(2,\mathbb{R}) \subset \mathrm{GL}(2,\mathbb{R})$.

   La $M, N \in \mathrm{O}(2,\mathbb{R})$. Da har vi at $MN^{-1} = MN^\intercal$, $(MN^\intercal)^\intercal = NM^\intercal$ og at $MN^\intercal NM^\intercal = \mathcal{I}$, så $(MN^{-1})^{-1} = (MN^{-1})^\intercal$. Altså er $MN^{-1} \in \mathrm{O}(2,\mathbb{R})$, så $\mathrm{O}(2,\mathbb{R})$ er en undergruppe av $\mathrm{GL}(2,\mathbb{R})$.

2. For $n \in \mathbb{N}$ så definerer vi $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Da er $(\mathbb{Z}_n, +_n)$ en abelsk gruppe, hvor $+_n$ er addisjon modulo n.

   Eksempelvis er $\mathbb{Z}_9 = 0, 1, \ldots, 8$ og $7 +_9 8 = 6$, fordi $7 + 8 = 15 \equiv 6 \pmod 9$.

   Merk $|\mathbb{Z}_n| = n$, så for alle $n \in \mathbb{N}$ så finnes det en abelsk gruppe G med $|G| = n$.

1.3 Sykliske Grupper

Notasjon: Dersom G er en gruppe, $a \in G$ og vi bruker multiplikativ notasjon, så skriver vi $\langle a \rangle = \{a^t \mid t \in \mathbb{Z}\}$.

Theorem: 5.17

La G være en gruppe og $a \in G$. Da er $\langle a \rangle$ en undergruppe av G.

Bevis: Vi har at $\langle a \rangle \neq \emptyset$ og for $a^m, a^n \in \langle a \rangle$ så er $a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle$. Dermed har vi fra Teorem 5.14 at $\langle a \rangle \leq G$. □

Definition 1.3.1: Syklisk Undergruppe

Vi kaller $\langle a \rangle$ den **sykliske undergruppen** av G generert av a, og vi sier at G er **syklisk** dersom det finnes en $a \in G$ slik at $G = \langle a \rangle$.

Merk:

1. En syklisk gruppe kan ha flere generatorer
2. $|\langle a \rangle|$ kan være endelig, f.eks. at $a^s = a^t$ med $s \neq t$.

Eksempler:

1. 1 og -1 er generatorer i $\mathbb{Z}$, så $\mathbb{Z}$ er syklisk.
2. For $\mathbb{Z}_9$ så har vi at
   - $\langle 3 \rangle = \{0, 3, 6\} = \langle 6 \rangle$
   - $\langle 0 \rangle = \{0\}$
   - $\langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle$

   Vi ser at $\langle a \rangle = \mathbb{Z}_9 \iff \gcd(a, 9) = 1$
3. På øving: $a \in \mathbb{Z}_n$ er en generator $\iff \gcd(n, 1) = 1$
4. La $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Da er $\langle i \rangle = \{i, 1, -1, -i\} = U_4$.

Definition 1.3.2: Ordenen til et gruppeelement

La G være en gruppe og $a \in G$. Da sier vi at **ordenen** til a er $|\langle a \rangle|$.

Eksempel: Vi har sett på $\mathbb{Z}_9$. Der så vi at $\langle 3\rangle = \langle 6\rangle = \{0, 3, 6\}$. Dermed har vi at 3 og 6 har orden 3.

Theorem: 6.1

La G være en gruppe. Hvis G er syklisk, så er G abelsk.

Bevis: Hvis $G = \langle a\rangle$, altså syklisk, så kan vi skrive alle elementer i G som en potens av a. La $x, y \in G$. Da kan vi skrive $x = a^n$ og $y = a^m$. Dermed har vi at $xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$. Altså må G være abelsk. □

Theorem

La G være en gruppe og $H \leq G$ en undergruppe. Da er H syklisk.

Bevis: Dersom $H = \{e\}$, så er H trivielt syklisk, så la oss derfor anta at H ikke er triviell. La $a \in G$ med $G = \langle a\rangle$, altså at a er en generator av G. Siden $H \neq \{e\}$, så vil det finnes $a^n \in H$ med $n \neq 0$. Siden H er en undergruppe og derfor også en gruppe, så må også $a^{-n} = (a^n)^{-1} \in H$. Med andre ord så vil ikke mengden $I = \{n \in \mathbb{N} \mid a^n \in H\}$ være tom, altså $I \neq \emptyset$. Videre må det derfor finnes et minste element i I, n_0. Vi skal se at a^{n_0} kommer til å generere H.

Siden $a^{n_0} \in H$, så vil $\langle a^{n_0}\rangle \leq H$. Se nå på et tilfeldig element $a^m \in H$. Fra divisjonsalgoritmen har vi at $m = qn_0 + r$ for $0 \leq r \leq n_0 - 1$. Dette betyr også at $r = m - qn_0$. Merk at $a^{qn_0} = (a^{n_0})^q \in H$ siden $a^{n_0} \in H$, så $a^{-qn_0} \in H$ også. I tillegg har vi at $a^r = a^{m-qn_0} = a^m a^{-qn_0} \in H$.

Dersom $r > 0$ så kan ikke $a^r \in H$, fordi $r < n_0$ og vi har antatt at n_0 er den minste. Så vi har at $r = 0$, men dette betyr at $m = qn_0$, som igjen betyr at a^{n_0} genererer H, som var det vi ville vise. □

Theorem: (Korollar) 6.7

Alle undergrupper av $\mathbb{Z}$ er på formen $m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$.

Vis følgende utsagn:

1. Dersom $p \in \mathbb{N}$ er et primtall så vil $\mathbb{Z}_p$ kun ha to undergrupper, $\{0\}$ og $\mathbb{Z}_p$.
2. La $m, n \in \mathbb{Z}$ og definer $H = \{am + bn \mid a, b \in \mathbb{Z}\}$. Da vil $H \leq Z$ og det vil finnes $d \in \mathbb{Z}$ med $H = \langle d\rangle$. Vis at $d = \gcd(m, n)$ er en gyldig kandidat.
3. Vi har at $a \in \mathbb{Z}_n$ er en generator hvis og bare hvis $\gcd(a, n) = 1$. Derfor kan vi si at $\phi(n) =$ antall generatorer i $\mathbb{Z}_n$. (Hint: $\gcd(a, b) = 1 \iff \exists r, s \in \mathbb{Z} : ra + sb = 1$)

Theorem: 6.10

La G være en gruppe. Dersom G er syklisk så har vi følgende:
- $|G| = \infty \implies G$ er isomorf med $\mathbb{Z}$.
- $|G| = n \implies G$ er isomorf med $\mathbb{Z}_n$.

Eksempel: Se på gruppen $U_4 = \left\{z \in \mathbb{C} \mid z^4 = 1\right\} = \{\pm 1, \pm i\}$ med multiplikasjon som binæroperator. Siden denne er syklisk (med $\pm i$ som generator) og $|U_4| = 4$, så må $(U_4, \cdot) \cong (\mathbb{Z}_4, +_4)$. En slik isomorfi er gitt ved

$$f : U_4 \to \mathbb{Z}_4 \tag{1.11}$$
$$i^n \mapsto n \tag{1.12}$$

Vis at f er en isomorfi ved å vise at den er bijektiv og homomorf.

Theorem: 6.14

La G være en gruppe generert av a med $|G| = n$ og la $a^t \in G$ være et vilkårlig element. Da er ordenen til a^t gitt ved

$$\left|\langle a^t \rangle\right| = \frac{n}{\gcd t, n} \tag{1.13}$$

Videre så gjelder $\langle a^t \rangle = \langle a^s \rangle \iff \gcd(n,t) = \gcd(n,s)$.

Theorem: (Korollar) 6.16

La G være en gruppe. Dersom G er syklisk av orden n og $a^t \in G$ så har vi at

$$\left\langle a^t \right\rangle = G \iff \gcd(n,t) = 1 \tag{1.14}$$

1.4 Permutasjoner

Definition 1.4.1: Permutasjon

En **permutasjon** av en mengde A er en bijeksjon $A \to A$

Eksempler:

1. Bijeksjonen $\sigma : \mathbb{Z} \to \mathbb{Z}$ gitt ved $\sigma(n) = -n$
2. Bijeksjonen $\sigma : \mathbb{Z} \to \mathbb{Z}$ gitt ved $\sigma(n) = n + a$ hvor $a \in \mathbb{Z}$ er fiksert

Notasjon: Dersom $A = \{1, \ldots, n\}$ og $\sigma : A \to A$ er en permutasjon så skriver vi følgende:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \tag{1.15}$$

Eksempel: Dersom vi har $A = \{1,2,3,4\}$ og $\sigma : A \to A$ er en permutasjon med

$$\sigma(1) = 3 \tag{1.16}$$
$$\sigma(2) = 2 \tag{1.17}$$
$$\sigma(3) = 4 \tag{1.18}$$
$$\sigma(4) = 1 \tag{1.19}$$

Så skriver vi

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \tag{1.20}$$

Merk: Komposisjon av to permutasjoner, $\tau, \sigma : A \to A$ gir oss en ny permutasjon $\tau\sigma(a) : A \to A$, definert som

$$\tau\sigma(a) = \tau(\sigma(a)) \ \forall a \in A \tag{1.21}$$

Eksempel: For følgende permutasjoner,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \tag{1.22}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \tag{1.23}$$

hvor $A = \{1, 2, 3, 4\}$ så har vi at

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \tag{1.24}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \tag{1.25}$$

Theorem

La $A \neq \emptyset$ være en vilkærlig mengde og

$$S_A = \{\sigma : A \to A \mid \sigma \text{ er en permutasjon}\} \tag{1.26}$$

Da er S_A en gruppe med komposisjon som binæroperasjon.

Bevis: Siden A er en ikke-tom mengde så er ogsa S_A en ikke-tom mengde. Det følger fra definisjonen av komposisjon at S_A må være lukket under komposisjon.

$\mathscr{G}1$) Det er kjent at komposisjon av funksjoner alltid er assosiativt

$\mathscr{G}2$) Dersom vi definerer $I : A \to A, I(a) = a$ så vil $I\sigma = \sigma = \sigma I \ \forall \sigma \in A$. Altså er I et gyldig identitetselement

$\mathscr{G}3$) La $\sigma \in S_A$ og ta $a \in A$. Siden σ er surjektiv så må det finnes en $b \in A$ slik at $\sigma(b) = a$. Siden σ er injektiv, så må b være unik.

Definer $\sigma^{-1} : A \to A$ med $\sigma^{-1}(a) = b$. Gjør dette med alle $a \in A$ for den valgte permutasjonen σ, så vil $\sigma\sigma^{-1} = \sigma^{-1}\sigma = I$, som betyr at σ^{-1} er inversen til σ. □

Definition 1.4.2

Når $A = \{1, \cdots, n\}$ så skriver vi S_n, som kalles den **n'te symmetriske gruppen**

Merk:

1. $|S_n| = n!$
2. For $n \geq 3$ så er ikke S_n abelsk (vis).

Theorem: Cayley

Enhver gruppe er isomorf med en undergruppe av S_A for en mengde A.

1.4.1 Gruppen S_3

Vi kan tolke S_3 som symmetrigruppen til et likesidet triangel. En illustrasjon av dette kan ses i Figure 1.1.

Her definerer vi følgende elementer:

- ρ_0: Rotasjon med 0° mot klokken, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
- ρ_1: Rotasjon med 120° mot klokken, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- ρ_2: Rotasjon med 240° mot klokken, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

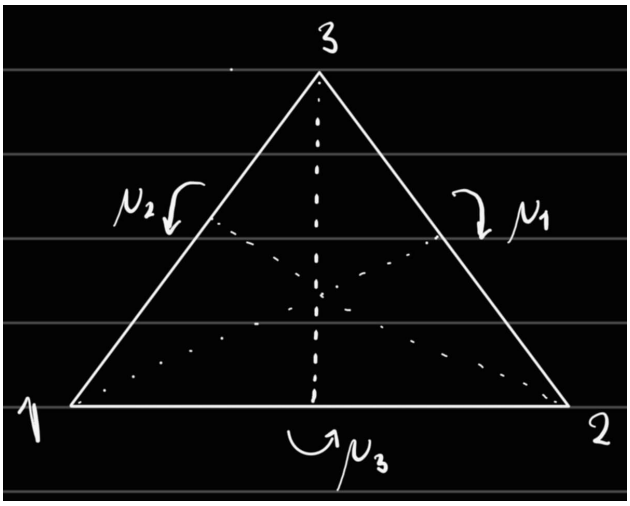

Figure 1.1: Illustrasjon av S_3

- μ_1: Speiling om linje 1, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
- μ_2: Speiling om linje 2, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
- μ_3: Speiling om linje 3, som tilsvarer $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Binæroperasjonen i S_3 er komposisjon av permutasjoner, men dette svarer til komposisjon av symmetrier.

Eksempel: Vi har at

$$\mu_3\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{1.27}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.28}$$

$$= \mu_2 \tag{1.29}$$

Multiplikasjonstabell til S_3

Følgende er multiplikasjonstabellen til den tredje symmetrigruppen:

$*$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Undergrupper:

- $\{\rho_0\}$
- $\{\rho_0, \rho_1, \rho_2\} = \langle\rho_1\rangle = \langle\rho_2\rangle$

- $\{\rho_0, \mu_i\}_{i=1,2,3}$
- S_3 selv, som ikke er syklisk

1.5 Baner, Sykler og A_n

Definition 1.5.1: Banen til et element

La A være en mengde, $\sigma \in S_A$ og $a \in A$. Da sier vi at **banen** til a er

$$\{\sigma^n(a) \mid n \in \mathbb{Z}\} \subset A \tag{1.30}$$

Eksempel: La

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 2 & 3 \end{pmatrix} \in S_6 \tag{1.31}$$

Da ser vi at

$$\sigma(1) = 5 \tag{1.32}$$
$$\sigma^2(1) = 2 \tag{1.33}$$
$$\sigma^3(1) = 1 \tag{1.34}$$
$$\sigma^4(1) = 5 \tag{1.35}$$

noe som betyr at $\{1, 2, 5\}$ er banen til 1, 2 og 5. Videre ser vi at

$$\sigma(3) = 6 \tag{1.36}$$
$$\sigma^2(3) = 3 \tag{1.37}$$

som betyr at $\{3, 6\}$ er banen til 3 og til 6. Til slutt så ser vi at

$$\sigma(4) = 4 \tag{1.38}$$

som betyr at $\{4\}$ er banen til 4.

Definition 1.5.2: Sykel

$\sigma \in S_n$ er en **sykel** hvis det maksimalt er en bane med mer enn et element.

Eksempel: Se på $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 56 & \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix} \in S_6$. Denne permutasjonen har banene

$$\{1\}, \{2\}, \{4\}, \{5\}, \{3, 6\} \tag{1.39}$$

Dermed er τ en sykel, mens σ fra over ikke er det.

Merk:

1. Vi bruker notasjonen $\tau = (3, 6)$ for τ definert som over
2. La $\mu = (1, 5, 2)$ og $\tau = (3, 6)$ i S_6. Altså at

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 4 & 2 & 6 \end{pmatrix} \tag{1.40}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix} \tag{1.41}$$

   Da er $\mu\tau = \sigma = \tau\mu$ (vis)

Theorem: 9.8

Ethvert element i S_n er et produkt av sykler.

Definition 1.5.3: Transposisjon

En sykel av lengde 2 er en **transposisjon**.

Merk: La $(a_1, a_2, \ldots, a_t)$ være en sykel i S_n. Da er

$$(a_1, a_2, \ldots, a_t) = (a_1, a_t)(a_1, a_{t-1}) \cdots (a_1, a_2) \tag{1.42}$$

Eksempel: I S_6 så er $(1, 5, 2) = (1, 2)(1, 5)$ og i S_{39} så er $(2, 8, 13, 38) = (2, 38)(2, 13)(2, 8)$

Theorem: (Korollar) 9.12

Ethvert element i S_n er et produkt av transposisjoner.

Eksempler:

1. σ fra eksempelet tidligere kan skrives som: $\sigma = (1, 5, 2)(3, 6) = (1, 2)(1, 5)(3, 6)$
2. $(a, b)(a, b)$ blir til identiteten i S_n. F.eks. så har vi at $(1, 2)(1, 2) = \text{id}$.
3. For σ i punkt 1 så kan vi skrive

$$\sigma = (1, 2)(1, 5)(3, 6) = (1, 2)(2, 4)(2, 4)(1, 5)(3, 6) \tag{1.43}$$

siden $(2, 4)(2, 4)$ blir identiteten.

Theorem: 9.15

Et element i S_n kan ikke både skrives som et produkt av et odde antall transposisjoner og som et produkt av et partall antall transposisjoner.

Definition 1.5.4: Like og Odde

Vi sier at $\sigma \in S_n$ er **like** dersom σ er et produkt av et partall antall transposisjoner og **odde** dersom σ er et produkt av et odde antall transposisjoner.

Eksempler:

1. σ fra tidligere er odde siden $\sigma = (1, 6)(1, 5)(3, 6)$.
2. Identitetselementet i S_n er like fordi det kan skrives som $(1, 2)(1, 2)$.

Theorem: 9.20

For $n \geq 2$ la $A_n = \{\sigma \in S_n \mid \sigma \text{ er like}\}$. Da er $A_n \leq S_n$ med $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Bevis: Først så har vi at $A_n \neq \emptyset$ siden $n \geq 2$.

La

$$\sigma = (a_1, b_1) \cdots (a_{2s}, b_{2s}) \in A_n \tag{1.44}$$
$$\tau = (c_1, d_1) \cdots (c_{2t}, d_{2t}) \in A_n \tag{1.45}$$
$$\tag{1.46}$$

Da har vi at

$$\sigma\tau^{-1} = [(a_1, b_1)\cdots(a_{2s}, b_{2s})]\,(c_{2t}, d_{2t})\cdots(c_1, d_1) \tag{1.47}$$

som betyr at $\sigma\tau^{-1}$ kan skrives som et produkt av et partalls antall transposisjoner, som igjen betyr at $\sigma\tau^{-1}$ må være like. Dermed er $\sigma\tau^{-1} \in A_n$, som betyr at A_n er en gyldig undergruppe av S_n. □

La $B_n = \{\sigma \in S_n \mid \sigma \text{ er odde}\}$.

Theorem: (Korollar) 9.12

$S_n = A_n \cup B_n$

Theorem: 9.15

$A_n \cap B_n = \emptyset$ og $|S_n| = |A_n| + |B_n|$.

1.6 Restklasser og Lagranges Teorem

I dette kapittelet kommer vi til å anta at $H \leq G$.

Mål:

1. Vise at dersom $|G| < \infty$ så vil $|H| \mid |G|$.
2. Etter hvert: Lage en ny gruppe G/H for visse undergrupper H.

Definition 1.6.1: Restklasse

La $a \in G$. Da er $Ha = \{ha \mid h \in H\}$ den **høyre restklassen** til H mhp. a, og $aH = \{ah \mid h \in H\}$ den **venstre restklassen** til H mhp. a.
Dersom G er abelsk så er $Ha = aH\ \forall a \in G$.

Eksempler:

1. La $G = \mathbb{Z}$ og $H = 5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$. Da finnes det fem restklasser:

$$0 + 5\mathbb{Z} = 5\mathbb{Z} \tag{1.48}$$
$$1 + 5\mathbb{Z} = \{\ldots, -9, -4, 1, 6, \ldots\} \tag{1.49}$$
$$2 + 5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, \ldots\} \tag{1.50}$$
$$3 + 5\mathbb{Z} = \{\ldots, -7, -2, 3, 8, \ldots\} \tag{1.51}$$
$$4 + 5\mathbb{Z} = \{\ldots, -6, -1, 4, 9, \ldots\} \tag{1.52}$$
$$5 + 5\mathbb{Z} = 5\mathbb{Z} \tag{1.53}$$
$$6 + 5\mathbb{Z} = 1 + 5\mathbb{Z} \tag{1.54}$$

2. La $U_4 = \{1, -1, i, -i\}$ med multiplikasjon og $H = -1, 1$. Da har vi følgende restklasser:

$$H \cdot 1 = H \cdot (-1) = H \tag{1.55}$$
$$H \cdot i = H \cdot (-i) = \{-i, i\} \tag{1.56}$$

   Så det finnes totalt to restklasser

3. La $G = S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ og $H = \{\rho_0, \mu_1\}$. Da ser vi at:

$$H\rho_1 = \{\rho_1, \mu_2\} \tag{1.57}$$
$$\rho_1 H = \{\rho_1, \mu_3\} \tag{1.58}$$

Så vi ser at $H\rho_1 \neq \rho_1 H$.

Merk (for både høyre og venstre restklasser):

1. $a \in Ha$ fordi $ea = a$
2. $Ha = H \iff a \in H$.

   Dersom $Ha = H$ så er $a \in H$ fra punkt 1. Dersom $a \in H$ så er $Ha \subseteq H$ siden H er lukket. La nå $h \in H$. Da kan vi skrive $h = (ha^{-1})a$, men $ha^{-1} \in H$, så $h \in Ha$. □
3. $Ha \cap Hb \neq \emptyset \iff Ha = Hb$. Her er $\Longleftarrow$-retningen triviell.

   Hvis $Ha \cap Hb \neq \emptyset$ så finnes $h_1, h_2 \in H$ slik at $h_1 a = h_2 b$. Dette gir oss at $a = h_1^{-1} h_2 b$. Dermed har vi at for $h \in H$ så er $ha = (hh_1^{-1}h_2)b \in Hb$. Siden vi valgte h vilkårlig så må da $Ha \subseteq Hb$. Vi kan bruke et tilsvarende argument for å see at $Hb \subseteq Ha$, noe som betyr at $Hb = Ha$. □
4. $Ha = Hb \iff ab^{-1} \in H \iff ba^{-1} \in H$.

   Vi ser at $Ha = Hb \iff Hab^{-1} = Hbb^{-1} \iff Hab^{-1} = H \iff ab^{-1} \in H$, hvor vi i det siste steget brukte resultatet fra punkt 2.
5. $Ha = Hb \iff b \in Ha$ fra punkt 1 og 4.
6. Definer $f : H \to Ha$ ved $f(h) = ha$. Dette er en bijeksjon, så $|H| = |Ha|$.

Theorem: Lagrange

Hvis $|G| < \infty$ og $H \leq G$ så vil $|H|$ være en divisor i $|G|$.

Bevis: Fra resultatene over og siden G er endelig så må det eksistere elementer $a_1, a_2, \ldots, a_t \in G$ slik at

1. $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_t$
2. $Ha_i \cap Ha_j = \emptyset$ for alle $i \neq j$ (siden alle restklassene er disjunkte eller fullstendig overlappende)

Så siden $|Ha_i| = |H|$ så må $|G| = t\,|H|$. □

Theorem: (Korollar) 10.11

Anta $|G| = p$ hvor p er et primtall. Da har G kun to undergrupper, $\{e\}$ og G selv.
Dersom $a \neq e$ så vil $\langle a \rangle = G$. Spesielt er G syklisk og G er isomorf med $\mathbb{Z}_p$.

Eksempel (Vår 2012, oppgave 1): La G være en gruppe som inneholder minst ett element av orden 3 og minst ett av orden 4. Hva er den minste ordenen en slik gruppe kan ha og gi et eksempel.

Siden 3 må dele ordenen og 4 må dele ordenen til gruppen så ma $3 \cdot 4$ også dele ordenen, så ordenen må minst være 12. Et eksempel på en slik gruppe er $\mathbb{Z}_{12}$.

Definition 1.6.2: Indeks

Vi sier at **indeksen** til H i G er $(G : H)$ = antall ulike høyre restklasser til H (som er det samme som antall venstre restklasser).

Eksempel: $(\mathbb{Z} : 5\mathbb{Z}) = 5$.

Merk: Når $|G| < \infty$ så er $(G : H) = \frac{|G|}{|H|}$.

1.7 Produkt av grupper

Vi er kjente med at dersom $S_1, S_2, \ldots, S_t$ er mengder, så er det kartesiske produktet mellom de definert som

$$S_1 \times S_2 \times \cdots \times S_t = \{(s_1, s_2, \ldots, s_t) \mid s_i \in S_i\} \tag{1.59}$$

Eksempel:

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{C} = \{(x, y, z) \mid x, y \in \mathbb{Z}, z \in \mathbb{C}\} \tag{1.60}$$

Merk: Vi har at

$$|S_1 \times S_2 \times \cdots \times S_t| = \prod_{i=1}^{t} |S_i| \tag{1.61}$$

Theorem: 11.2

La $G_1, \ldots, G_t$ være grupper. Da har vi at $G_1 \times \cdots \times G_t$ er en gruppe med binæroperasjon

$$(a_1, \ldots, a_t)(b_1, \ldots, b_t) = (a_1 b_1, \ldots, a_t b_t) \tag{1.62}$$

hvor multiplikasjonen skjer elementvis og hører til hver enkelt gruppe. Dette er det **direkte produktet** av $G_1, \ldots, G_t$.

Bevis: Oppgave

Merk:

1. Vi bruker $\prod_{i=1}^{t} G_i$ notasjon.
2. Identitetselementet er $(e_1, e_2, \ldots, e_t)$ hvor $e_i \in G_i$ er identiteten.
3. Vi har at $(a_1, a_2, \ldots, a_t)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_t^{-1})$
4. Vi har at $\prod G_i$ er abelsk $\iff$ G_i er abelsk $\forall i$

Eksempler:

1. La oss se på $(\mathbb{Z}, +)$ og $(U, \cdot)$, hvor $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Da har vi at binæroperasjonen til $\mathbb{Z} \times U$ er gitt ved $(a, z)(b, w) = (a + b, zw)$.
2. $\mathbb{Z}_2 \times \mathbb{Z}_2$ har fire elementer, $\{(0,0), (0,1), (1,0), (1,1)\}$

   Vi ser at $(1,0) + (1,0) = (1+1, 0+0) = (0,0)$.

   Elementene $(1,0)$, $(0,1)$ og $(1,1)$ har orden 2 i $\mathbb{Z}_2 \times \mathbb{Z}_2$, så ingen elementer har orden 4, altså finnes det ingen elementer som genererer hele grupper. Dermed er den ikke syklisk.

   Altså har vi at $\mathbb{Z}_4$ og $\mathbb{Z}_2 \times \mathbb{Z}_2$ er ikke-isomorfe abelske grupper med 4 elementer.

Theorem: 11.5

$\mathbb{Z}_m \times \mathbb{Z}_n$ er syklisk (og dermed isomorf med $\mathbb{Z}_{mn}$) $\iff$ $\gcd(m, n) = 1$.

Bevis: Anta at $\gcd m, n = 1$. Vis da at $(1,1)$ genererer hele $\mathbb{Z}_m \times \mathbb{Z}_n$

Motsatt, dersom $\gcd(m, n) = d \geq 2$, kan man vise at ingen elementer i gruppen genererer hele gruppen.

Ordenen til $(a, b) \leq \frac{m \cdot n}{d} < m \cdot n$.

Theorem: (Korollar) 11.6

$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$ er syklisk (og isomorf med $\mathbb{Z}_{\prod_{i=1}^{t} n_i}$) $\iff$ $\gcd(n_i, n_j) = 1 \ \forall i \neq j$

Theorem: 11.9

La $G_1, \ldots, G_t$ være grupper og $a_i \in G_i$ være elementer av orden n_i. Da har vi at $(a_1, \ldots, a_t)$ har orden $\text{lcm}(n_1, n_2, \ldots, n_t)$.

Eksempel: Se på $\mathbb{Z}_5 \times \mathbb{Z}_8$ og elementet $(2, 3)$. Siden 2 har orden 5 i $\mathbb{Z}_5$ og 3 har orden 8 i $\mathbb{Z}_8$, så har $(2, 3)$ orden $\text{lcm}(5, 8) = 40$. Altså må $(2, 3)$ være en generator.

Se på $(2, 4)$. Siden 4 har orden 2 i $\mathbb{Z}_8$ så har $(2, 4)$ orden $\text{lcm}(5, 2) = 10$.

Theorem: 11.12 (Fundamentalteoremet for endeliggenererte abelske grupper)

Enhver endeliggenerert abelsk gruppe er isomorf med et direkte produkt på formen

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_t^{n_t}} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \tag{1.63}$$

hvor p_i er primtall (men ikke nødvendigvis disinkte) og det er unikhet. Spesielt så har vi at dersom G er en endelig abelsk gruppe så er G isomorf med et direkte produkt på formen

$$\mathbb{Z}_{p_i^{n_1}} \times \cdots \times \mathbb{Z}_{p_t^{n_t}} \tag{1.64}$$

Bevis: MA3201, Ringer og Moduler

Eksempel (Eksamen vår 2021, oppgave 1): La G være en abelsk gruppe med $|G| = 72$. Hvilke grupper kan G være isomorf med?

Vi har at $72 = 3^2 \cdot 2^3$. Da har vi fra fundamentalteoremet for endeliggenererte abelske grupper at G må være isomorf med en av følgende:

- $\mathbb{Z}_9 \times \mathbb{Z}_8 \cong \mathbb{Z}_{72}$
- $\mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8$
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

1.8 Homomorfier

La G og H være grupper.

Definition 1.8.1: Homomorfi

En funksjon $\phi : G \to H$ er en (gruppe-)**homomorfi** dersom

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \ \forall g_1, g_2 \in G \tag{1.65}$$

Eksempler

1. La e_H være identiteten i H og sett $\phi(g) = e_H$ for alle $g \in G$. Da har vi at
$$\phi(g_1 g_2) = e_H = e_H e_H = \phi(g_1)\phi(g_2) \tag{1.66}$$
2. Fikser $a \in \mathbb{Z}$ og definer $\phi_a : \mathbb{Z} \to \mathbb{Z}$ ved $n \mapsto an$. Da har vi at
$$\phi_a(m+n) = a(m+n) = am + an = \phi_a(m) + \phi_a(n) \tag{1.67}$$
Vis at enhver homomorfi $\phi : \mathbb{Z} \to \mathbb{Z}$ er på formen ϕ_a for $a \in \mathbb{Z}$. Når er ϕ_a en isomorfi?
3. Definer $\phi : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ ved $\phi(M) = \det M$. Da har vi at
$$\phi(MN) = \det(MN) = \det(M)\det(N) = \phi(M)\phi(N) \tag{1.68}$$
som betyr at ϕ er en homomorfi.
4. Definer $\phi : S_n \to S_{n+1}$ ved
$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma_1 & \dots & \sigma_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & n & n+1 \\ \sigma_1 & \dots & \sigma_1 & n+1 \end{pmatrix} \tag{1.69}$$
Vis at $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$
5. Se på $(\mathbb{R}, +)$ og $(U, \cdot)$ hvor $U = \{z \in \mathbb{C} \mid |z| = 1\}$.
$$\phi : \mathbb{R} \to U \tag{1.70}$$
$$r \mapsto e^{ir} \tag{1.71}$$
Da har vi at $\phi(r+s) = e^{i(r+s)} = e^{ir}e^{is} = \phi(r)\phi(s)$.

Theorem: 13.12

La $\phi : G \to H$ være en homomorfi. Da har vi at følgende holder:

1. Dersom $e \in G$ er identitetselementer så er $\phi(e)$ identitetselementet i H
2. $\phi(g^{-1}) = \phi(g)^{-1}\ \forall g \in G$
3. $K \leq G \implies \phi[K] = \{\phi(k) \mid k \in K\} \leq H$
4. $L \leq H \implies \phi^{-1}[L] = \{g \in G \mid \phi(g) \in L\} \leq G$

Med andre ord impliserer homomorfier en slags strukturbevaring.

Bevis:

1. Vi har at $\phi(e) = \phi(ee) = \phi(e)\phi(e)$. Gang nå med $\phi(e)^{-1}$ på begge sider. Da får du $\phi(e)^{-1}\phi(e) = \phi(e)^{-1}\phi(e)\phi(e) \implies e_H = \phi(e)$. □
2. Vi ser at
$$e_H = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \implies \phi(g^{-1}) = \phi(g)^{-1} \quad \square \tag{1.72}$$

Definition 1.8.2: Kjernen

La e_H være identitetselementet i H. Da er kjernen til ϕ definert som:
$$\ker \phi = \{g \in G \mid \phi(g) = e_H\} \tag{1.73}$$

Merk: $\ker \phi \leq G$. Dette kommer fra punkt 4 i teoremet over siden det inverse bildet til e_H vil være kjernen til ϕ.

Eksempler: (Her bruker vi de samme eksemplene som over)

1. $\ker \phi = G$
2. $\ker \phi_a = \begin{cases} \{0\} & a \neq 0 \\ \mathbb{Z} & a = 0 \end{cases}$
3. $\ker \phi = \mathrm{SL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$
4. $\ker \phi = \{\sigma \in S_n \mid \phi(\sigma) = \mathrm{id}_{n+1}\} = \{e\}$
5. Vi har at:

$$\ker \phi = \{a \in \mathbb{R} \mid \phi(a) = 1\} \tag{1.74}$$
$$= \left\{a \in \mathbb{R} \mid e^{ir} = 1\right\} \tag{1.75}$$
$$= \{n \cdot 2\pi \mid n \in \mathbb{Z}\} \tag{1.76}$$

Theorem: (Korollar) 13.18

For en homomorfi $\phi : G \to H$ så har vi at ϕ er injektiv hvis og bare hvis $\ker \phi = \{e\}$.

Bevis: La oss først anta at ϕ er injektiv og at $g \in G$ med $\phi(g) = e_H$. Siden $\phi(e) = e_H$ og ϕ er injektiv, så må da $g = e_H$.

Anta nå at ϕ ikke er injektiv. Da må det finnes $g_1, g_2 \in G$ slik at $g_1 \neq g_2$ men $\phi(g_1) = \phi(g_2)$. Da har vi at

$$e_H = \phi(g_1)\phi(g_1)^{-1} \tag{1.77}$$
$$= \phi(g_2)\phi(g_1)^{-1} \tag{1.78}$$
$$= \phi(g_2)\phi(g_1^{-1}) \tag{1.79}$$
$$= \phi(g_2 g_1^{-1}). \tag{1.80}$$

Legg merke til at $g_2 g_1^{-1} \neq e$ siden inverser er unike. Dermed har vi vist at $\ker \phi \neq \{e\}$, som var det vi ville vise. □

1.9 Faktorgrupper

Mål: For en gruppe G og visse undergrupper $H \leq G$ så vil vi lage en ny gruppe G/H hvor elementene i G/H er restklassene til H i G.

Definition 1.9.1: Normal Undergruppe

Vi kaller en undergruppe $H \leq G$ **normal** dersom $gH = Hg \ \forall g \in G$.

Eksempler:

1. $H = \{e\} \implies gH = \{g\} = Hg$ for alle $g \in G$, så her er H normal.
2. Dersom G er abelsk så er $H \leq G$ automatisk normal.
3. La $G = S_3$ tolket som symmetrier på et triangel, $\{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$. Vi har tidligere sett at $H = \{\rho_0, \rho_1, \rho_2\}$ er en undergruppe. Vi har at $\rho_i H = H = H\rho_i$ siden $\rho_i \in H$.

   Vis at $\mu_i H = H\mu_i$.

   Altså har vi at $H \leq G$ er en normal undergruppe.
4. La oss fortsatt se på S_3, men sett nå $H = \{\rho_0, \mu_1\}$. Da har vi at $\rho_1 H = \{\rho_1, \mu_3\}$, men at $H\rho_1 = \{\rho_1, \mu_2\}$. Altså er ikke H normal i dette tilfellet.

Theorem: 14.12

Følgende er ekvivalent for $H \leq G$:

1. H er normal
2. gHg^{-1} $\forall g \in G$, hvor $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$
3. $ghg^{-1} \in H$ $\forall h \in H, g \in G$

Fra tidligere så har vi:

1. $g \in G$
2. $gH = H \iff g \in H$
3. $g_1H \cap g_2H \neq \emptyset \iff g_1H = g_2H \iff g_1^{-1}g_2 \in H \iff g_2^{-1}g_1 \in H \iff g_2 \in g_1H$

Eksempel: La $G = S_3$. Da ser vi at

1. $H = \{\rho_0, \rho_1, \rho_2\} \implies \rho_1 H = H$ og $\mu_i H = \{\mu_1, \mu_2, \mu_3\}$
2. La $H = \{\rho_1, \mu_1\}$. Da ser vi at $\rho_1 H = \{\rho_1, \mu_3\}$, altså at $\mu_3 \in \rho_1 H$, som må bety at $\rho_1 H = \mu_1 H$ (siden de enten er helt disjunkte eller helt like).

Theorem: 14.14 og korollar 14.5

Anta at $H \leq G$ er normal og la G/H være mengden av restklasser til H i G. For g_1H og g_2H i G/H, definer

$$(g_1H)(g_2H) = (g_1g_2)H \in G/H \tag{1.81}$$

Dette er en binæroperasjon på G/H, som blir en gruppe sammen med denne.

Bevis: Må vise at binæroperasjonen er veldefinert i følgende forstand: La $g_1' \in g_1H$. Da vet vi at $g_1H = g_1'H$. Tilsvarende har vi at for $g_2' \in g_2H$ er $g_2H = g_2'H$. Må vise

$$(g_1g_2)H = (g_1'g_2')H \tag{1.82}$$

Med andre ord så må vi vise at dersom to elementer i domenet er like så må de også ende opp på samme sted i ko-domenet.

Siden $(g_1H)(g_2H) = (g_1'H)(g_2'H)$, så kan vi ta et element $g_1'g_2'h \in (g_1'g_2')H$. Siden $g_1' \in g_1H$ og $g_2' \in g_2H$, så finnes $h_1, h_2 \in H$ slik at $g_1' = g_1h_1$ og $g_2' = g_2h_2$. Da har vi at

$$\begin{aligned} g_1'g_2'h &= (g_1h_1)(g_2h_2)h && (1.83)\\ &= g_1(e)h_1g_2h_2h && (1.84)\\ &= g_1(g_2g_2^{-1})h_1g_2h_2h && (1.85)\\ &= g_1g_2(g_2^{-1}h_1g_2)h_2h && (1.86) \end{aligned}$$

Husk at siden H er normal og $h_1 \in H$, så må $g_2^{-1}h_1g_2 \in H$. Dermed kan vi skrive $\widetilde{h} := g_2^{-1}h_1g_2$. Videre har vi at $\widetilde{h}h_2h \in H$ siden H er lukket. Dermed får vi altså

$$g_1'g_2'h = g_1g_2\widetilde{h}h_2h \in (g_1g_2)H \tag{1.87}$$

Derfor har vi at $(g_1'g_2')H \subseteq (g_1g_2)H$. Vi kan gjøre tilsvarende argument andre vei og få $(g_1g_2)H \subseteq (g_1'g_2')H$, som tilsammen må bety at $(g_1g_2)H = (g_1'g_2')H$, som var det vi ville vise. Dermed har vi vist at operatoren over er veldefinert.

La oss nå vise at dette blir en gruppe.

$\mathscr{G}1$) Assosiativitet:

$$\begin{aligned} g_1H\left[(g_2H)(g_3H)\right] &= g_1H((g_2g_3)H) && (1.88)\\ &= g_1(g_2g_3)H && (1.89)\\ &= (g_1g_2)g_3H && (1.90)\\ &= \dots && (1.91)\\ &= \left[(g_1H)(g_2H)\right]g_3H && (1.92) \end{aligned}$$

$\mathscr{G}2$) Identitet: Vi har at $eH = H$ er identitetselementet:

$$(eH)(gH) = (eg)H = gH = (ge)H = (gH)(eH)\ \forall g \in G \tag{1.93}$$

$\mathscr{G}3$) Invers: Vi har at $(gH)^{-1} = g^{-1}H$:

$$(gH)(g^{-1}H) = (gg^{-1})H = eH = (g^{-1}g)H = (g^{-1}H)(gH) \tag{1.94}$$

Definition 1.9.2: Faktorgruppe/Kvotientgruppe

Dersom G er en gruppe og H er en normal undergruppe så kaller vi G/H en **faktorgruppe** eller **kvotientgruppe**.

Merk:

1. Vi brukte at $H \leq G$ er normal for å få at binæroperasjonen er veldefinert.
2. binæreoperatoren for faktorgrupper er rett og slett a gange sammen restklasser:

$$\begin{aligned} (g_1H)(g_2H) &= \{g_1h_1g_2h_2 \mid h_1, h_2 \in H\} && (1.95)\\ &= \left\{g_1g_2g_2^{-1}h_1g_2h_2 \mid h_1, h_2 \in H\right\} && (1.96)\\ &= \{g_1g_2h \mid h \in H\} && (1.97)\\ &= (g_1g_2)H && (1.98) \end{aligned}$$

Eksempler:

1. La $G = \mathbb{Z}$ og see på $H = 4\mathbb{Z}$. Vi har at H her er normal siden $\mathbb{Z}$ er en abelsk gruppe. Den har fire restklasser:

$$\begin{aligned} 0 + 4\mathbb{Z} = 4\mathbb{Z} && (1.99)\\ 1 + 4\mathbb{Z} && (1.100)\\ 2 + 4\mathbb{Z} && (1.101)\\ 3 + 4\mathbb{Z} && (1.102) \end{aligned}$$

som også er de fire elementene i $\mathbb{Z}/4\mathbb{Z}$. La oss se på addisjon i $\mathbb{Z}/4\mathbb{Z}$:

$$\begin{aligned} (1 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = (1 + 2) + 4\mathbb{Z} = 3 + 4\mathbb{Z} && (1.103)\\ (0 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = (0 + 2) + 4\mathbb{Z} = 2 + 4\mathbb{Z} && (1.104)\\ (2 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = (2 + 2) + 4\mathbb{Z} = 0 + 4\mathbb{Z} = 4\mathbb{Z} && (1.105)\\ (3 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = (3 + 2) + 4\mathbb{Z} = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z} && (1.106)\\ && (1.107) \end{aligned}$$

Merk her at $-(2+4\mathbb{Z}) = 2+4\mathbb{Z}$, altså at dette er inversen siden $4\mathbb{Z}$ er identiteten. Vi ser at $|\mathbb{Z}/4\mathbb{Z}| = 4$ og at dette ligner på $(\mathbb{Z}_4, +_4)$!

2. La nå $G = S_3$ hvor vi ser på $H = \{\rho_0, \rho_1, \rho_2\}$. Vi har allerede sett at denne er normal. Det finnes to elementer i S_3/H:
   - $H = \rho_0 H = \{\rho_0, \rho_1, \rho_2\} = \rho_1 H = \rho_2 H$
   - $\mu_1 H = \{\mu_1, \mu_2, \mu_3\} = \mu_2 H = \mu_3 H$

   Altså har vi at $|S_3/H| = 2$ med $\rho_0 H$ som identitetselement og $(\mu_1 H)(\mu_2 H) = \mu_1^2 H = \rho_0 H$. Dette ligner på $(\mathbb{Z}_2, +_2)$!

Merk:

1. Dersom $\phi : G \to G'$ er en homomorfi så er $\ker \phi$ normal i G.
2. $\phi[G] := \{\phi(g) \mid g \in G\} \leq G'$. Vi har også trivielt at $\phi : G \to \phi[G]$ er en surjektiv homomorfi.

Fra dette får vi at dersom $H \leq G$ er normal så kan vi lage følgende homomorfi:

$$\Pi : G \to G/H \tag{1.108}$$
$$g \mapsto gH \tag{1.109}$$

Da ser vi at $\Pi(g_1 g_2) = g_1 g_2 H = (g_1 H)(g_2 H) = \Pi(g_1)\Pi(g_2)$. Videre har vi at

$$\ker \Pi = \{g \in G \mid \Pi(g) = eH\} = \{g \in G \mid g \in H\} = H \tag{1.110}$$

Theorem: 14.11 - Fundamentalteoremet for (gruppe-)homomorfier

La $\phi : G \to G'$ være en homomorfi og $H = \ker \phi$. Da er funksjonen

$$\bar{\phi} : G/H \to \phi[G] \tag{1.111}$$
$$gH \mapsto \phi(g) \tag{1.112}$$

en veldefinert homomorfi og en isomorfi. Videre har vi at $\phi = \bar{\phi} \circ \Pi$.

Bevis:

- Veldefinert:

$$g_1 H = g_2 H \implies g_2 \in g_1 H \tag{1.113}$$
$$\implies g_2 = g_1 h \tag{1.114}$$
$$\implies \bar{\phi}(g_2 H) = \phi(g_2) = \phi(g_1 h) = \phi(g_1)\phi(h) = \phi(g_1) = \bar{\phi}(g_1) \tag{1.115}$$

- Homomorfi:

$$\bar{\phi}((g_1 H)(g_2 H)) = \bar{\phi}((g_1 g_2)H) \tag{1.116}$$
$$= \phi(g_1 g_2) \tag{1.117}$$
$$= \phi(g_1)\phi(g_2) \tag{1.118}$$
$$= \bar{\phi}(g_1 H)\bar{\phi}(g_2 H) \tag{1.119}$$

- Bijektiv: Vis
- Kommutativt diagram:

$$(\bar{\phi} \circ \Pi)(g) = \bar{\phi}(\Pi(g)) \tag{1.120}$$
$$= \bar{\phi}(gH) \tag{1.121}$$
$$= \phi(g) \tag{1.122}$$

som var det vi ville vise. □

Eksempler:

1. Se på $\phi : \mathbb{Z} \to \mathbb{Z}_4$ med $n \mapsto n \pmod 4$. Dette er en homomorfi. ϕ er surjektiv og $\ker\phi = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 4\} = 4\mathbb{Z}$. Da følger det fra teoremet over at $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}_4$ er en isomorfi ved $\bar{\phi}$.
2. Se på $\phi : \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$ ved $\phi(M) = \det M$. Dette er en homomorfi som er surjektiv med $\ker\phi = \mathrm{SL}(n,\mathbb{R})$. Så $\bar{\phi} : \mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \to \mathbb{R}^*$ er en isomorfi.
3. Se på

$$\phi : S_n \to \mathbb{Z}_2 \tag{1.123}$$

$$\sigma \mapsto \begin{cases} 0 & \sigma \text{ like} \\ 1 & \sigma \text{ odde} \end{cases} \tag{1.124}$$

   Da er ϕ en surjektiv homomorfi og $\ker\phi = A_n$. Så $S_n/A_n \to \mathbb{Z}_2$ er en isomorfi.
4. Vi ser at $G/\{e\} \cong G$ med $\phi(g) = g$ og $G/G \cong \{e\}$ med $\phi(g) = e$.

Strategi for å vise at G/H er isomorf med en gruppe G':

1. Finn en surjektiv homomorfi $\phi : G \to G'$ med $\ker\phi = H$
2. Da gir funtamentalteoremet oss at $G/H \to G'$ er en isomorfi siden $\phi[G] = G'$.

Eksempel - Eksamen Sommer 2023, oppgave 4: La G være en endelig gruppe og $H_1, H_2 \leq G$ normale undergrupper.

a) La $\phi : G \to G/H_1 \times G/H_2$ med $\phi(g) = (gH_1, gH_2)$. Vis at ϕ er en homomorfi.

   Løsning:

$$\phi(g_1g_2) = (g_1g_2H_1, g_1g_2H_2) \tag{1.125}$$
$$= ((g_1H_1)(g_2H_1), (g_1H_2)(g_2H_2)) \tag{1.126}$$
$$= (g_1H_1, g_1H_2)(g_2H_1, g_2H_2) \tag{1.127}$$
$$= \phi(g_1)\phi(g_2) \tag{1.128}$$

   Så ϕ er en homomorfi.

b) Finn en injektiv homomorfi

$$G/(H_1 \cap H_2) \to G/H_1 \times G/H_2 \tag{1.129}$$

   og vis at denne er en isomorfi hvis og bare hvis

$$\frac{|H_1|\,|H_2|}{|H_1 \cap H_2|} = |G| \tag{1.130}$$

   Løsning:

$$\ker\phi = \{g \in G \mid \phi(g) = e\} \tag{1.131}$$
$$= \{g \in G \mid \phi(g) = (H_1, H_2)\} \tag{1.132}$$
$$= \{g \in G \mid g \in H_1 \wedge g \in H_2\} \tag{1.133}$$
$$= \{g \in G \mid g \in H_1 \cap H_2\} \tag{1.134}$$
$$= H_1 \cap H_2 \tag{1.135}$$

   Fra fundamentalteoremet har vi da at $\bar{\phi} : G/H_1 \cap H_2 \to \phi[G]$ er en isomorfi. Men merk at $\phi[G] \subseteq G/H_1 \times G/H_2$, så vi kan ikke garantere at $\bar{\phi} : G/H_1 \cap H_2 \to G/H_1 \times G/H_2$ er surjektiv. Den må

likevel være injektiv, siden isomorfien er det. Vi har at

$$\phi \text{ surjektiv} \iff |G/H_1 \cap H_2| = |G/H_1 \times G/H_2| \tag{1.136}$$

$$\iff \frac{|G|}{|H_1 \cap H_2|} = \frac{|G|}{|H_1|} \cdot \frac{|G|}{|H_2|} \tag{1.137}$$

$$\iff \frac{|H_1||H_2|}{|H_1 \cap H_2|} = \frac{|G|^2}{|G|} = |G| \quad \square \tag{1.138}$$

Definition 1.9.3: Simpel

Vi sier at en gruppe G er **simpel** dersom det ikke finnes en normal undergruppe H slik at

$$\{e\} < H < G \tag{1.139}$$

Eksempel: Dersom $|G| = p$ hvor p er et primtall så vet vi fra lagrange at G må være simpel, siden det ikke kan finnes noen undergrupper H med $\{e\} < H < G$.

Theorem: 15.15

A_n er simpel når $n \geq 5$.

Theorem: Klassifisering av endelige simple grupper

La G være en endelig, simpel gruppe. Da er den isomorf med en av følgende:

1. $\mathbb{Z}_p$ hvor p er et primtall
2. A_n når $n \geq 5$
3. En simpel gruppe av Lie-type
4. En av de 26 sporadiske gruppene

1.10 Gruppevirkninger

Definition 1.10.1: Gruppevirkning

La G være en gruppe og X være en mengde. En **gruppevirkning** på X fra G er en funksjon $G \times X \to X$ som tilfredsstiller to krav:

- $(e, x) = x$ for alle $x \in X$.
- $(g_1 g_2, x) = (g_1, (g_2, x))$ for alle $g_1, g_2 \in G, x \in X$.

Dersom disse kravene tilfredsstilles så kaller vi X en **G-mengde**.

Notasjon: Dersom $g \in G$ og $x \in X$ så skriver vi normalt sett $(g, x) = gx$.

Eksempler:

1. La $G = S_n$ og $X = \{1, \ldots, n\}$. For en permutasjon $\sigma \in G$ og $x \in X$ så er $\sigma x = \sigma(x)$ en gruppevirkning.
2. La G være en gruppe og $X = \{H \leq G\}$ være mengden av alle undergrupper av G. La oss videre definere en funksjon

$$G \times X \to X \tag{1.140}$$

$$gH = (g, H) \mapsto gHg^{-1} = \left\{ghg^{-1} \mid h \in H\right\} \tag{1.141}$$

Sjekk at dette er en undergruppe av G. Vi har at $eH = eHe^{-1} = H$ og at $(g_1g_2)H = g_1g_2Hg_2^{-1}g_1^{-1} = g_1(g_2Hg_2^{-1})g_1^{-1} = g_1(g_2H)$. Denne gruppevirkningen kalles **Konjugasjon**.

3. La

$$G = \{A \in \mathcal{M}_3(\mathbb{R}) \mid A \text{ er ortogonal}\} \tag{1.142}$$
$$= \left\{A \in \mathcal{M}_3(\mathbb{R}) \mid A^{-1} = A^\intercal\right\} \tag{1.143}$$
$$= \mathrm{O}_3(\mathbb{R}) \tag{1.144}$$

være en gruppe med matrisemultiplikasjon som binæroperator. Merk at $||Av|| = ||v|| \forall v \in \mathbb{R}^3, A \in G$, altså at A bevarer normen til vektorer. Fiksér en $a > 0$ og la $X = \left\{r \in \mathbb{R}^3 \mid ||r|| = a\right\}$. For $A \in G$ og $v \in X$ så er $||Av|| = ||v||$, så $Av \in X$.

Videre har vi at:

(a) $Iv = v \forall v \in X$

(b) $(AB)v = A(Bv)\ \forall A, B \in G, v \in X$

Dermed følger det at X er en G-mengde og at vi har en gruppevirkning.

4. La $G = \mathbb{Z}_2$ og $X = \mathbb{R}$. Definer så

$$G \times X \to X \tag{1.145}$$
$$mx \mapsto \begin{cases} x & m = 0 \\ -x & m = 1 \end{cases} \tag{1.146}$$

Da er $0x = x$ og (sjekk) $(m+n)x = m(nx)$.

Definition 1.10.2: Transitiv Virkning

La G være en gruppe og X en mengde. Vi sier at G virker **transitivt** på X dersom $\forall x_1, x_2 \in X\ \exists g \in G$ hvor $gx_1 = x_2$.

Eksempel: Vi har at (1) og (3) fra det forrige eksempelet er transitive virkninger. Spesielt så ser vi at $forall v_1, v_2 \in \mathbb{R}^3$ med $||v_1|| = ||v_2||$ så vil det finnes en $A \in \mathrm{O}_3(\mathbb{R})$ slik at $Av_1 = v_2$ (ikke helt trivielt).

Videre har vi at (2) ikke er transitiv. Vi ser at $|H| = \left|gHg^{-1}\right|$, så derfor kan man ikke gå fra en størrelse til en annen.

Definition 1.10.3

La G være en gruppe og X en mengde, og la $g \in G$ og $x \in X$. Da definerer vi følgende mengder:

$$G_x = \{h \in G \mid hx = x\} \subseteq G \tag{1.147}$$
$$X_g = \{y \in X \mid gy = y\} \subseteq X \tag{1.148}$$

Theorem

La G være en gruppe, X være en mengde og $x \in X$. Da vil $G_x \leq G$.

Bevis: La oss først merke at $G_x \neq \emptyset$ siden $e \in G_x$. La nå $h_1, h_2 \in G_x$. Da er $h_ix = x$, noe som betyr at $x = h_i^{-1}x$. Da vil

$$(h_1h_2^{-1})x = h_1(h_2^{-1}x) \tag{1.149}$$
$$= h_1(x) \tag{1.150}$$
$$= x \tag{1.151}$$

noe som betyr at $h_1 h_2^{-1} \in G_x$. Altså må $G_x \leq G$. □

Definition 1.10.4: Isotropi-undergruppen

G_x kalles **isotropi-undergruppen** til x i G.

Definition 1.10.5: Bane til element in mengde

La G være en gruppe, X være en mengde og $x \in X$. Da sier vi at **banen** til x er $Gx = \{gx \mid g \in G\}$.

Eksempler:

1. La G være en gruppe og definer $X = \{H \leq G\}$. Da vet vi at $g \cdot H = gHg^{-1}$ for $H \in X$. Da er $G_H = \left\{g \in G \mid gHg^{-1} = H\right\}$.
2. La $G = \mathrm{O}_3(\mathbb{R})$ og $X = \left\{v \in \mathbb{R}^3 \mid ||v|| = a\right\}$. Da har vi at
$$G_v = \{A \in \mathrm{O}_3(\mathbb{R}) \mid Av = v\} \tag{1.152}$$
$$= \{A \in \mathrm{O}_3(\mathbb{R}) \mid v \text{ egenvektor av } A \text{ med } \lambda = 1\} \tag{1.153}$$
3. Vi har at 'transitiv virkning $\iff$ $Gx = X\ \forall x \in X$'

Theorem: 16.16

La G være en gruppe, X være en mengde og $x \in X$ et element. Da har vi at $|Gx| = (G : G_x)$, hvor $(G : G_x)$ betegner indeksen til G_x i G, altså antall venstre restklasser.

Bevis: For $g_1, g_2 \in G$ så har vi at $g_1 x = g_2 x \iff g_2^{-1} g_1 x = x \iff g_2^{-1} g_1 \in G_x \iff g_1 G_x = g_2 G_x$. Dermed har vi altså en veldefinert funksjon:

$$Gx \to \{\text{venstre restklasser til } G_x \text{ i } G\} \tag{1.154}$$
$$gx \mapsto gG_x \tag{1.155}$$

Ettersom denne funksjonen er bijektiv så må mengdene være like store, som var det vi ville vise. □

Vis følgende:

1. $\forall x_1, x_2 \in X, x_1 \in Gx_2 \iff Gx_1 = Gx_2 \iff x_2 \in Gx_1$
2. Definer relasjonen på X ved $x_1 \in Gx_2$. Dette er en ekvivalensrelasjon.
3. De følgende utsagnene er ekvivalente:
   (a) G virker transitivt på X
   (b) $Gx = X\ \forall x \in X$
   (c) Det finnes $x \in X$ med $Gx = X$
   (d) X har kun én ekvivalensklasse for relasjonen i 2)

1.10.1 Burnsides Formel

Theorem: Burnsides Formel

La G være en endelig gruppe og X en endelig G-mengde med r baner i X. Da følger det at:

$$r \cdot |G| = \sum_{g \in G} |X_g| \tag{1.156}$$

Bevis: Se på undermengden M av $G \times X$:

$$M = \{(g, x) \mid gx = x\} \tag{1.157}$$

Da har vi at

$$\sum_{g \in G} |X_g| = \sum_{g \in G} |\{x \in X \mid gx = x\}| = |M| \tag{1.158}$$

$$= \sum_{x \in X} |\{g \in G \mid gx = x\}| \tag{1.159}$$

$$= \sum_{x_i n X} |G_x| \tag{1.160}$$

Videre har vi at for alle $x \in X$ så er $|Gx| = (G : G_x) = \frac{|G|}{|G_x|}$. Da må vi ha at

$$|M| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \cdot \sum_{x \in X} \frac{1}{|Gx|} \tag{1.161}$$

La nå B være en av banene i X, altså at $B = Gx$ for en $x \in X$. Da har vi at alle elementene i B har B selv som bane, altså at $B = Gx' \ \forall x' \in B$ og at

$$\sum_{x \in B} \frac{1}{|Gx|} = \sum_{x \in B} \frac{1}{B} = 1 \tag{1.162}$$

Dette betyr altså at hver bane, B, gir et bidrag på 1 i $\sum_{x \in X} \frac{1}{|Gx|}$. Siden banene må være helt disjunkte og vi har r baner så betyr dette at

$$|M| = |G| \sum_{x \in X} \frac{1}{|Gx|} = |G| \cdot r \tag{1.163}$$

og siden $|M| = \sum_{g \in G} |X_g|$ så må altså

$$\sum_{g \in G} |X_g| = |G| \cdot r \tag{1.164}$$

som var det vi ville vise. □

Eksempel (Eksamen Vår 2013, oppg. 4):

Anta et perlekjede skal være bestående av 11 like store perler, hvorav 5 skal være sorte og 6 skal være hvite. Hvor mange ulike slike perlekjeder kan du lage?

Først, sett G til å være symmetrigruppen til perlekjedet. Da vil elementene i G bestå av 11 rotasjoner, $\{\rho_0, \ldots, \rho_1 0\}$ og 11 speilinger, $\{\mu_1, \ldots, \mu_1 1\}$. Her tenker vi at μ_i holder perle i i ro. Da vil $|G| = 22$.

La nå X være mengden av alle fargelagte perlekjeder uten å ta hensyn til symmetrier. Da vil G virke på X og antall baner vil være antall ulike perlekjeder som vi skal frem til. Fra Burnsides formel har vi

$$22 \cdot r = \sum_{g \in G} |X_g| = \sum_{i=0}^{10} |X_{\rho_i}| + \sum_{j=1}^{11} \left|X_{\mu_j}\right| \tag{1.165}$$

Merk at $|X| = \binom{11}{5}$ og at

$$|X_{\rho_i}| = \begin{cases} |X| = \binom{11}{5} & i = 0 \\ 0 & i \neq 0 \end{cases} \tag{1.166}$$

siden ingen elementer holdes i ro da det finnes 5 sorte og 6 hvite.

Hva med X_{μ_i}? Dersom $x \in X$ skal ligge i X_{μ_i} så må perle i være sort slik at vi kan ha et partall antall sorte på hver side, også må det faktisk være et partall på hver side, altså to perler i dette tilfellet. Det vil finnes $\binom{5}{2}$ slike perlekjeder, fordi man vil ha fem perler på hver side og man har kun frihet til å velge den ene siden, siden den andre må være lik. Når man velger den ene siden, som består av fem perler, så kan man velge hvor de to sorte skal være. Altså har vi at

$$|X_{\mu_i}| = \binom{5}{2} \tag{1.167}$$

Dersom vi nå setter alt inn i Burnsides formel får vi:

$$22r = \binom{11}{5} + \sum_{i=1}^{11} \binom{5}{2} \tag{1.168}$$

$$= 572 \tag{1.169}$$

som betyr at $r = 26$. Altså finnes det 26 slike perlekjeder.

1.11 Sylowteori

Da vi lærte om Lagrange, så vi at dersom G er en endelig gruppe, og $H \leq G$ en undergruppe, så ville $|H| \mid |G|$. Man kan også stille seg det motsatte spørsmålet: Dersom $d \mid |G|$, finnes det en undergruppe $H \leq G$ slik at $|H| = d$?

- Dersom G er abelsk, ja
- Dersom G ikke er abelsk, ikke nødvendigvis

Som et eksempel, ta $A_4 = \{\sigma \in S_4 \mid \sigma \text{ er like}\} \leq S_4$. Da ser vi at $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 12$. Men, det finnes ingen undergruppe $H \leq A_4$ slik at $|H| = 6$.

Mål: Vise at når $|G| = p_1^{n_1} \cdots p_t^{n_t}$, hvor p_i er primtall og $n_i \in \mathbb{N} \cup \{0\}$, så finnes det $H \leq G$ med $|H| = p_i^m \ \forall i, 0 \leq m \leq n_i$.

Definition 1.11.1: p-gruppe

La p være et primtall. Da er en gruppe G en p-gruppe hvis hvert element i G har som orden en potens av p.

Delmål: G er en p-gruppe $\iff |G| = p^t$.

Theorem: 36.1

La G være en gruppe med $|G| = p^t$ for et primtall p og en potens $t \in \mathbb{N}$, la X være en endelig G-mengde og sett

$$X_G = \bigcap_{g \in G} X_g = \{x \in X \mid gx = x \forall g \in G\}. \tag{1.170}$$

Da er

$$|X| \equiv |X_G| \pmod{p}, \tag{1.171}$$

dvs. $p \mid (|X| - |X_G|)$.

Bevis: Vi vet fra før at for $x, y \in X$ så er enten $Gx = Gy$ eller $Gx \cap Gy = \emptyset$. Merk nå at dersom $|Gx| = 1 \iff x \in X_G$. Siden X er endelig så må det finnes $x_1, \ldots, x_n \in X$ slik at $X = Gx_1 \cup \cdots \cup Gx_n$

og $Gx_i \cap Gx_j = \emptyset$ for $i \neq j$. La nå $y_1, \ldots, y_s \in \{x_1, \ldots, x_n\}$ være de elementene som har at $|Gy_i| = 1$ og $z_1, \ldots, z_t \in \{x_1, \ldots, x_n\}$ med $|Gz_i| \geq 2$. Da har vi at $X_G = \{y_1, \ldots, y_2\}$ og

$$X = G_{y_1} \cup \cdots \cup G_{y_s} \cup G_{z_1} \cup \cdots \cup G_{z_t} \tag{1.172}$$
$$= X_G \cup G_{z_1} \cup \cdots \cup G_{z_1}. \tag{1.173}$$

Dette betyr at $|X| = |X_G| + \sum_{i=1}^{t} |G_{z_i}|$. Fra Teorem 16.16 så er $|G_{z_i}| = (G : G_{z_i}) = \frac{|G|}{|G_{z_i}|}$. Siden $|G| = p^t$ og $|G_{z_i}| \geq 2$ så må $p \mid |G_{z_i}|$, som også betyr at p må dele $\sum_{i=1}^{t} |G_{z_i}| = |X| - |X_G|$, som var det vi ville vise. □

Theorem: 36.3 (Cauchy)

Anta at p er et primtall, G en gruppe og at $p \mid |G|$. Da har G minst ett element – og dermed også en undergruppe – av orden p.

Bevis: Sett $X = \{(g_1, \ldots, g_p) \in G \times \cdots \times G \mid g_1 g_2 \ldots g_p = e\}$. Da kan vi velge $g_1, \ldots, g_{p-1}$ fritt i G, for så å sette $g_p = (g_1 \ldots g_{p-1})^{-1}$. Altså vil $|X| = |G|^{p-1}$ og dermed $p \mid |X|$.

Se nå på $\sigma = (1, 2, 3, \ldots, p) \in S_p$. Vi har at ordenen til σ er p, så $H = \langle \sigma \rangle = \left\{e, \sigma, \ldots, \sigma^{p-1}\right\} \leq S_p$ har p elementer. Gruppen H vil virke på X. La $x = (g_1, \ldots, g_p) \in X$ og definer σ slik at $\sigma x = (g_2, \ldots, g_{p-1}, g_1)$. Da er $\sigma x \in X$, fordi $g_1 = (g_2 \ldots g_{p-1})^{-1}$, altså at $g_2 \ldots g_{p-1} g_1 = e$. Ved utvidelse så virker H på X. Siden $|H| = p$ så sier Teorem 36.1 at $|X| \equiv |X_H| \pmod{p}$ og siden $p \mid |X|$ så må $p \mid |X_H|$.

$$X_H = \{x \in X \mid hx = x \ \forall h \in H\} \tag{1.174}$$
$$= \{(g_1, \ldots, g_p) \in X \mid \sigma x = x\} \tag{1.175}$$
$$= \{(g_1, \ldots, g_p) \in X \mid g_1 = g2 = \cdots = g_p\} \tag{1.176}$$
$$= \{(g_1, \ldots, g_p) \in X \mid g^p = e\} \tag{1.177}$$
$$\tag{1.178}$$

Siden $(e, \ldots, e) \in X_H$ så er $|X_H| \geq 1$ og videre siden $p \mid |X_H|$ og $p \geq 2$ så må $|X_H| \geq 2$. Altså har vi at det finnes en $g \in G$ slik at $g^p = e$ hvor $g \neq e$. Siden p er et primtall så må dermed $|\langle g \rangle| = p$. □

Theorem: (Korollar) 36.4

Anta at p er et primtall og at G er en endelig gruppe. Da har vi at

$$G \text{ er en } p\text{-gruppe} \iff |G| = p^t \tag{1.179}$$

Bevis: Øving 8. Høyre til venstre kommer fra Lagrange og venstre til høyre kommer fra å se på negasjonen av begge sider.

Definition 1.11.2: Sylow-p-undergruppe

La G være en endelig gruppe og p et primtall med $p \mid |G|$. Skriv nå $|G| = pm$ hvor $p \nmid m$. Da sier vi at en **Sylow-p-undergruppe** av G er en undergruppe av orden p^t.

Theorem: Sylowteoremene

La G være en endelig gruppe og p et primtall med $p \mid |G|$. Da holder følgende:

- **Første Sylowteorem**: Skriv $|G| = p^t m$ hvor $p \nmid m$. Da har vi at
  a) $\forall 1 \leq i \leq t \; \exists H \leq G$ med $|H| = p^t$
  b) Hvis $H \leq G$ og $|H| = p^i$ for $1 \leq i \leq t-1$ så $\exists K \leq G$ med $|K| = p^{i+1}$ og slik at H er normal i K
- **Andre Sylowteorem**: Hvis P, P' er Sylow-p-undergrupper så finnes det en $g \in G$ slik at $P' = gPg^{-1}$.
- **Tredje Sylowteorem**: La n_p være antall Sylow-p-undergrupper. Da har vi at
  a) $n_p \mid |G|$
  b) $n_p \equiv 1 \pmod{p}$

Merk: For andre Sylowteorem så har vi sett at for en gruppe G og $H \leq G$ så er $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \leq G$. Videre så har vi også at $P = gP'g^{-1} \iff P = g^{-1}P'g$.

Bevis (for andre Sylowteorem): La X være mengden av alle restklasser til P i G, altså at $X = \{gP \mid g \in G\}$. Da virker P' på X med $h(gP) = (hg)P \; \forall h \in P'$. Siden $|P'| = p^t$ så gir Teorem 36.1 oss at $|X| \equiv |X_{P'}| \pmod{p}$ hvor $X_{P'} = \{x \in X \mid hx = x \; \forall h \in P'\}$. Vi har at $|X| = (G : P) = \frac{|G|}{|P|}$, så $p \nmid |X|$ og siden $|X| \equiv |X_{P'}| \pmod{p}$ så vil da $p \nmid |X_{P'}|$. Det betyr at $|X_{P'}| \neq 0$, dvs $X_{P'} \neq \emptyset$. Da må det finnes en $x \in X$ slik at $hx = x \; \forall h \in P'$, dvs. det finnes en restklasse gP med $h(gP) = gP \; \forall h \in P'$, dvs. $(hg)P = gP$, dvs. $(g^{-1}hg)P = P \; \forall h \in P'$, dvs. $g^{-1}hg \in P \; \forall h \in P$, dvs. $g^{-1}P'g \leq P$. Men, $|g^{-1}P'g| = |P'|$, så $g^{-1}P'g = P$. □

Eksempel (Eksamen Vår 2023, Oppg. 5):

La G være en gruppe slik at $|G| = p^t m$ for et primtall p, $t \geq 1$ og $1 < m < p$. Bruk et Sylowteorem til å vise at G ikke er simpel.

Må altså vise at det finnes en normal undergruppe $\{e\} < H < G$. La n_p være antall Sylow-p-undergrupper. Fra tredje Sylowteorem så må $n_p \mid p^t m$ og $n_p \equiv 1 \pmod{p}$. Siden $p \nmid 1$ så må $p \nmid n_p$ også. Videre så må også $n_p \mid p^t m$ (fra tredje Sylowteorem), så vi må ha at $n_p \mid m$.

Siden $m < p$ så må $n_p < p$, men da må $n_p = 1$, fordi $n_p \equiv 1 \pmod{p}$, som igjen betyr at G har en unik Sylow-p-undergruppe P, og denne må ha orden p^t. Siden $m > 1$ og $t \geq 1$ så må altså P være slik at $\{e\} < P < G$. Videre så må P være normal fra andre Sylowteorem. Dermed er ikke G simpel, som var det vi ville vise. □

Eksempel (Eksamen Vår 2013, Oppg. 5b):

Vis at dersom $|G| = 105$ så er ikke G simpel.

Vi har at $105 = 3 \cdot 7 \cdot 5$. La nå n_5 være antall Sylow-5-undergrupper og n_7 være antall Sylow-7-undergrupper. Fra tredje Sylowteorem har vi da at

- $n_5 \mid |G|$ og $n_5 \equiv 1 \pmod{5}$
- $n_7 \mid |G|$ og $n_7 \equiv 1 \pmod{7}$

La oss nå se på alle divisorne til 105: $\{1, 3, 5, 7, 15, 21, 35, 105\}$. Fra dette og utsagnene over så ser vi at $n_5 \in \{1, 21\}$ og $n_7 \in \{1, 15\}$. Vi vil nå vise at enten n_7 eller n_5 må være 1.

La $H, H' \leq G$ med $|H| = |H'| = 5$ være forskjellige Sylow-5-undergrupper. Da vil $H \cap H' = \{e\}$ fra Lagrange. Dermed har vi at 21 forskjellige undergrupper med 5 elementer vil gi oss $(5-1) \cdot 21 = 84$ ulike elementer. Et tilsvarende element holder for de 15 Sylow-7-undergruppene, som gir oss $(7-1) \cdot 15 = 90$ ulike elementer. Siden disse gruppene ikke kan overlappe så må G da ha minst 90+84 elementer, men siden vi

vet at $|G| = 105$ så er ikke dette mulig. Dermed må altså enten n_5 eller n_7 være lik 1, og vi så fra forrige oppgave at $n_p = 1$ vil gi en normal undergruppe som ikke er triviell. □

Chapter 2

Ringer og Kropper

2.1 Ringer og Kropper

Definition 2.1.1: Ring

En **ring** er en ikke-tom mengde R med to operasjoner, $+$ og $\cdot$, slik at følgende holder:

$\mathscr{R}1$) $(R, +)$ er en abelsk gruppe

$\mathscr{R}2$) Den andre operatoren, $\cdot$, skal være assossiativ, altså at $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for alle $a, b, c \in R$

$\mathscr{R}3$) De følgende distributive lovene skal holde:

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(a + b) \cdot c = a \cdot c + b \cdot c$

Dersom vi også har at $a \cdot b = b \cdot a$ for alle $a, b \in R$, så sier vi at R er en **kommutativ ring**.

Eksempler:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ med vanlig addisjon og multiplikasjon er alle kommutative ringer.
2. $M_n(\mathbb{R})$, altså alle $n \times n$ matriser over $\mathbb{R}$, er en ring, men den er ikke kommutativ.

Merk:

1. Vanligvis så kaller vi $+$ "addisjon" og $\cdot$ "multiplikasjon". Vi skriver også ab for $a \cdot b$.
2. Siden $(R, +)$ skal være en abelsk gruppe, så må det finnes en identitet for denne operatoren. Denne kaller vi vanligvis for 0.
3. Ringene vi ser på i dette faget vil også ha identiteter for den multiplikative operatoren som vi kaller 1, slik at $1 \cdot a = a \cdot 1 = a$ for alle $a \in R$.

Eksempler:

1. Den multiplikative identiteten i $M_2(\mathbb{R})$ er $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. La $n \geq 2$ og $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Vi har tidligere sett at $(\mathbb{Z}_n, +_n)$ er en abelsk gruppe. La $\cdot_n$ være multiplikasjon modulo n. Da har vi at $(\mathbb{Z}_n, +_n, \cdot_n)$ er en kommutativ ring.

Definition 2.1.2: Enhet

La R være en ring. Et element $a \in R$ kalles en **enhet** dersom det finnes $b \in R$ slik at $ab = ba = 1$.

Definition 2.1.3: Divisjonsring

La R være en ring. Da sier vi at R er en **divisjonsring** dersom alle elementene i $R \setminus \{0\}$ er enheter.

Definition 2.1.4: Kropp

La R være en ring. Da sier vi at R er en **kropp** dersom den er en kommutativ divisjonsring.

Eksempler

1. $\mathbb{Z}$ er ikke en kropp siden det kun er 1 og -1 som er enheter.
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ er kropper.
3. $M_n(\mathbb{R})$ er ikke en divisjonsring og dermed heller ikke en kropp.

Vis

1. R er en kropp $\iff$ $(R, +)$ og $(R \setminus \{0\}, \cdot)$ er abelske grupper og $a(b + c) = ab + ac$.
2. La $U(R) = \{a \in R \mid a \text{ er en enhet}\}$. Da er $(U(R), \cdot)$ en gruppe, men ikke nødvendigvis abelsk.
3. Dersom $a \in U(R)$ så finnes det kun én $b \in R$ med $ab = 1 = ba$.

Theorem: 18.8

La R være en gruppe og $a, b \in R$. Da holder følgende:

1. $0 \cdot a = a \cdot 0 = 0$
2. $a \cdot (-b) = (-a) \cdot b = -a \cdot b$
3. $(-a) \cdot (-b) = ab$

Definition 2.1.5: Ringhomomorfi

La R og S være ringer. Da sier vi at en funksjon $\phi : R \to S$ er en **ringhomomorfi** dersom:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

for alle $a, b \in R$. Dersom ϕ også er bijektiv så sier vi at det er en isomorfi. Kjernen av ϕ er alle elementene som sendes til 0.

Eksempler:

1. Har sett at $\phi : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto a \pmod n$ er en gruppehomomorfi. Vis at $\phi(ab) = \phi(a) \cdot_n \phi(b)$ $\forall a, b \in \mathbb{Z}$. Kjernen til ϕ er $n\mathbb{Z}$.
2. La $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$. Da er dette en ring. Definer nå $\phi : R \to \mathbb{R}$ ved $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$. Da ser vi (ved litt regning) at $\phi(A + B) = \phi(A) + \phi(B)$ og at $\phi(AB) = \phi(A)\phi(B)$. Altså er ϕ en ringhomomorfi.
3. La $\phi : \mathbb{C} \to \mathbb{C}$ ved $z \mapsto \overline{z}$, altså konjugasjon. Da er dette en bijektiv ringhomomorfi, altså en isomorfi.

2.2 Integritetsområder

Definition 2.2.1: Nulldivisor

La R være en ring og $a \in R$ et element. Da sier vi at a er en **nulldivisor** dersom $a \neq 0$ og det eksisterer $b \in R$ med $b \neq 0$ og $ab = 0$ eller $ba = 0$.

Eksempler:

1. Det finnes ingen nulldivisorer i $\mathbb{Z}$, fordi $ab = 0 \implies a = 0 \vee b = 0$ for alle $a, b \in \mathbb{Z}$.
2. Se på $\mathbb{Z}_6$: Der har vi at $2 \cdot_6 3 = 0$ og at $3 \cdot_6 4 = 0$, så 2, 3 og 4 er nulldivisorer.
3. Vis at dersom a er en enhet, så er ikke a en nulldivisor.

   Anta $a \in R$ er en enhet. Da må det finnes $b \in R$ slik at $ab = ba = 1$. Anta videre, *reductio ad absurdum*, at a også er en nulldivisor, altså at det finnes en $c \in R$, $c \neq 0$, slik at $ac = 0$. Da har vi at $ab - ac = a(b - c) = 1 - 0 = 1$. Så vi har at $a(b - c) = ab$ hvor $a \neq 0$. Da må $b - c = b$, som betyr at $c = 0$, men dette er en kontradiksjon, siden $c \neq 0$. □
4. La $R = M_n(\mathbb{R})$ for $n \geq 2$. Da har vi at for en $A \in R$ med $\det A = 0$ så vil det finnes en $v \in \mathbb{R}^n$ med $Av = 0$ hvor $v \neq 0$. Da kan vi bare sette sammen n slike: $v_n = \begin{pmatrix} v & v & \cdots & v \end{pmatrix}$. Da vil $Av_n = 0$ og $v_n \in R$.

Theorem: 19.3

Nulldivisorne i $\mathbb{Z}_n$ er $\{a \in \mathbb{Z}_n \mid a \neq 0, \gcd(a, n) > 1\}$.

Bevis: Anta $a \neq 0$ i $\mathbb{Z}_n$. Dersom $\gcd(1, n) = 1$, så har vi fra tallteorien at $ax \equiv 1 \pmod{n}$ er løsbar. Da finnes det $b \in \mathbb{Z}_n$ med $ab \equiv 1 \pmod{n}$, altså at $a \cdot_n b = 1$, så da er a en enhet og fra eksempel 3 så kan dermed ikke a være en nulldivisor.

Dersom $\gcd(a, n) = d > 1$ så må $a = m_1 d$ og $n = m_2 d$ for to tall $1 \leq m_1 m_2 \leq n - 1$. Vi kan nå velge $b := m_2$. Da har vi at $b \neq 0$ og $ab = m_1 m_2 d = m_1 n$, som betyr at $ab \equiv 0 \pmod{n}$, som betyr at a er en nulldivisor. □

Theorem: (Korollar) 19.4

$\mathbb{Z}_n$ har ingen nulldivisorer $\iff$ n er et primtall

Definition 2.2.2: Integritetsområde

La R være en ring. Vi sier at R er et **integritetsområde** dersom følgende er oppfylt:

1. R er en kommutativ ring
2. R har ingen nulldivisorer

Eksempler

1. Vi har at $\mathbb{Z}$ er et integritetsområde
2. Vi har at $\mathbb{Z}_n$ er et integritetsområde når n er et primtall

Theorem: 19.9

La F være en ring. Da har vi at F er en kropp hvis og bare hvis F er et integritetsområde.

Bevis: Se eksempel 3

Theorem: 19.11

La R være en ring. Dersom R er et integritetsområde og R er endelig så er R en kropp.

Bevis: La $a_1, \ldots, a_n$ være elementene i $R \setminus \{0\}$. Da må ett av elementene være 1. Velg nå en vilkårlig $a \in \{a_1, \ldots, a_n\}$ og se på $\{aa_1, aa_2, \ldots, aa_n\}$. Ingen av disse kan være 0, siden R er et integritetsområde og dermed ikke har noen nulldivisorer. Videre så kan ikke denne mengden ha noen duplikater, fordi hvis den hadde det, så kunne man tatt $aa_i - aa_j = a(a_i - a_j) = 0$, men da må $a_i = a_j$. Dermed må vi ha at $\{aa_1, aa_2, \ldots, aa_n\} = \{a_1, \ldots, a_n\}$, som betyr at den må inneholde elementet 1. Dermed finnes det $a_i \in R$ slik at $aa_i = 1$, og da må a være en enhet siden R er kommutativ. □

Theorem: 19.12

Følgende utsagn er ekvivalente for $n \geq 2$:

- n er et primtall
- $\mathbb{Z}_n$ er et integritetsområde
- $\mathbb{Z}_n$ er en kropp

2.3 Fermats Teorem og Eulers Teorem

Husk:

1. Dersom G er en gruppe med $|G| = n$ og $H \leq G$ er en undergruppe, så må $|H| \mid n$. Spesielt, dersom $g \in G$, så må $|\langle g \rangle| \mid n$. Dermed er $|\langle g \rangle| := t$ det minste tallet med $g^t = 1$. Videre så må da også $g^n = 1$.
2. La R være en ring og $U(R) = \{a \in R \mid a \text{ er en enhet}\}$. Da vil $(U(R), \cdot)$ være en gruppe. Spesielt så har vi at dersom F er en kropp, så er $U(F) = F \setminus \{0\} = F^*$ en gruppe under multiplikasjon.

Theorem: 20.1 (Fermats lille teorem)

La $a \in \mathbb{Z}$ og p et primtall med $p \nmid a$. Da har vi at

$$a^{p-1} \equiv 1 \pmod{p}, \tag{2.1}$$

altså at $p \mid (a^{p-1} - 1)$.

Bevis: Fra Korollar 19.12 så må $\mathbb{Z}_p$ være en kropp. Velg nå $b \in \mathbb{Z}_p$ med $a \equiv b \pmod{p}$. Det må finnes nøyaktig én slik b. Vi har at b ikke kan være 0, fordi da vil $a \equiv 0 \pmod{p}$, som vil bryte med antagelsen vår. Derfor har vi at $b \neq 0$. Ved å slå sammen punkt 1 og 2 fra listen over så får vi at $b^{p-1} = 1$ i $\mathbb{Z}_p$. Men da må $b^{p-1} \equiv 1 \pmod{p}$, og siden $a \equiv b \pmod{p}$ så må også $a^{p-1} \equiv 1 \pmod{p}$, som var det vi ville vise. □

Theorem: (Korollar) 20.2

La $a \in \mathbb{Z}$ og p være et primtall. Da må $a^p \equiv a \pmod{p}$.

Bevis: Dersom $p \mid a$ så er $a \equiv 0 \pmod{p}$ og $a^p \equiv 0 \pmod{p}$, så da må $a^p \equiv a \pmod{p}$. Dersom $p \nmid a$ så kan vi bruke Teorem 20.1. □

Fra før så har vi: Se på $\mathbb{Z}_n$ for $n \geq 2$. Fra beviset for teorem 19.3 så har vi

$$U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid a \neq 0, \gcd(a, n) = 1\}. \tag{2.2}$$

For eksempel så har vi da at for $\mathbb{Z}_9 = \{0, 1, 2, \ldots, 8\}$, så er $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$.

Definition 2.3.1: Eulers phi-funksjon

For $n \in \mathbb{N}$ så definerer vi $\phi(n) = |\{1 \leq a \leq n \mid \gcd(a, n) = 1\}|$, hvor ϕ er Eulers phi-funksjon.

Eksempler:

- $\phi(1) = 1, \{1\}$
- $\phi(2) = 1, \{1\}$
- $\phi(3) = 2, \{1, 2\}$
- $\phi(2) = 2, \{1, 3\}$
- $\phi(10) = 4, \{1, 3, 7, 9\}$
- $\phi(p) = p - 1$ dersom p er et primtall

Merk: For $n \geq 2$ så er $\phi(n) = |U(\mathbb{Z}_n)|$.

Theorem: 20.8 (Eulers Teorem)

La $a \in \mathbb{Z}$ og $n \in \mathbb{N}$ slik at $\gcd(a, n) = 1$. Da har vi at $a^{\phi(n)} \equiv 1 \pmod{n}$.

2.4 Polynomringer

Definition 2.4.1

La R være en ring. Da definerer vi følgende:

1. Et **polynom** med koeffisienter i R er definert som

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{2.3}$$

hvor $a_i \in R$. Vi sier at $f(x)$ har **grad** n dersom n er den største indeksen slik at $a_n \neq 0$ og skriver $\deg f(x) = n$.

2. Vi definerer **polynomringen** over R som

$$R[x] = \{p(x) \mid p \text{ er et polynom med koeffisienter i } R\} \tag{2.4}$$

En slik polynomring har følgende ringstruktur:

Dersom $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ og $q(x) = b_0 + b_1 x + \cdots + b_n x^n$ så vil

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \tag{2.5}$$

$$p(x)q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots, \tag{2.6}$$

altså slik som vi er vandte med fra før.

Merk

1. $R[x]$ kommutativ $\iff$ R kommutativ.
2. $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$ og $\deg(p(x)q(x)) \leq \deg p(x) + \deg q(x)$.

   For eksempel: Dersom vi er i $\mathbb{Z}_8[x]$, så har vi $(4x^2 03)(2x + 1) = 8x^3 + 4x^2 + 6x + 3 = 4x^2 + 6x + 3$ siden $8x^3$ forsvinner i $\mathbb{Z}_8$.
3. $R[x]$ integritetsområde $\iff$ R integritetsområde

I så fall er $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$.

Spesielt så har vi at dersom F er en kropp så er $F[x]$ et integritetsområde (men ikke en kropp).

4. Den multiplikative identiteten i $R[x]$ er $p(x) = 1$.

Theorem: 22.4

La $F \subseteq E$ være kropper og $\alpha \in E$. Da er $\phi_\alpha : F[x] \to E, p(x) \mapsto p(\alpha)$ en ringhomomorfi. Denne kaller vi **evaluering** i α.

Eksempel: Se på $\mathbb{Q} \subseteq \mathbb{R}$ og $\alpha = \sqrt{2} \in \mathbb{R}$. Definer $\phi_{\sqrt{2}} :\to \mathbb{R}, p(x) \mapsto p(\sqrt{2})$. Da ser vi at for $p(x) = x^2 - 2$ så er $\phi_{\sqrt{2}}(p) = 0$ og for $q(x) = x^3 + 1$ så er $\phi_{\sqrt{2}}(q) = 2\sqrt{2} + 1$.

Definition 2.4.2: Rot

La $F \subseteq E$ være kropper, $p(x) \in F[x]$ og $\alpha \in E$. Da sier vi at α er en **rot** i $p(x)$ dersom $p(\alpha) = 0$.

Eksempler:

1. Polynomet $p(x) = x^2 + 1$ i $\mathbb{R}$ har ingen røtter.
2. Polynomet $p(x) = x^2 + x + 1 \in \mathbb{Z}_7[x]$ har to røtter i $\mathbb{Z}_7$: $\{2, 4\}$.

2.5 Polynomfaktorisering

Merk: Dersom $f(x) = g_1(x)g_2(x) \in E$, hvor E er et integritetsområde, så er α en rot av $f(x)$ hvis og bare hvis α er en rot av $g_1(x)$ eller $g_2(x)$. Dette er fordi $f(\alpha) = g_1(\alpha)g_2(\alpha) = 0$ og siden E er et integritetsområde så må da enten $g_1(\alpha) = 0$ eller $g_2(\alpha) = 0$.

Husk: Dersom $a, b \in \mathbb{Z}$ med $b > 0$, så finnes det $q, r \in \mathbb{Z}$ slik at

1. $a = qb + r$
2. $0 \leq r \leq b$

Theorem

La $f(x), g(x) \in F[x]$ med $g(x) \neq 0$. Da finnes unike polynomer $q(x), r(x) \in F[x]$ slik at

1. $f(x) = q(x)g(x) + r(x)$
2. $r(x) = 0$ eller $\deg r(x) < \deg g(x)$

Bevis:

Eksistens: Anta først at $g(x) \mid f(x)$, altså at $f(x) = q(x)g(x)$ for et polynom $q(x) \in F[x]$. La nå $r(x) = 0$. Da er $f(x) = q(x)g(x) + r(x)$, som betyr at punkt 1 og 2 må stemme.

Anta at $g(x) \nmid f(x)$ og definer $M = \{f(x) - h(x)g(x) \mid h(x) \in F[x]\}$. Merk at $0 \notin M$. La $r(x) \in M$ med lavest mulig grad. Da er $r(x) = f(x) - q(x)g(x)$ for $q(x) \in F[x]$. Dette må bety at $f(x) = q(x)g(x) - r(x)$, som betyr at punkt 1 stemmer.

Vi må nå vise at punkt 2 stemmer. Vi vet at $r(x) = 0$, så må vise at $\deg r(x) < \deg g(x)$. La oss derfor anta at $\deg r(x) \geq \deg g(x)$. Vi kan skrive $g(x) = b_n x^n + \ldots b_1 x + b_0$ og $r(x) = r_t x^t + \cdots + r_1 x + r_0$, hvor

$b_n, r_t \neq 0$ og $t > r$. Se nå på $\bar{q}(x) = q(x) + \frac{r_t}{b_n}x^{t-n} \in F[x]$ og

$$s(x) = f(x) - g(x)\bar{q}(x) \in M \tag{2.7}$$

$$= f(x) - g(x)\left(q(x) + \frac{r_t}{b_n}x^{t-n}\right) \tag{2.8}$$

$$= r(x) - r_t x^t - (\text{ledd med lavere grad}) \tag{2.9}$$

Dermed får vi at $\deg s(x) < \deg r(x)$, men siden vi har antatt at $r(x)$ har minimal grad så må dette være en kontradiksjon, som igjen betyr at $\deg r(x) < \deg p(x)$. Altså har vi vist eksistens, som var det vi ville vise.

Unikhet: Anta at det finnes $q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$ slik at $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ med $r_i = 0$ eller $\deg r_i(x) < \deg g(x)$. Vi må vise at $q_1(x) = q_2(x)$ og at $r_1(x) = r_2(x)$.

Begynn med å anta at $q_1(x) \neq q_2(x)$. Da har vi at siden $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ så må $(q_1(x) - q_2(x))\, g(x) = r_2(x) - r_1(x)$. Her har vi at venstresiden ikke kan være null siden $q_1(x) \neq q_2(x)$. Videre har vi at

$$\deg\left(q_1(x) - q_2(x)\right) g(x) \geq \deg g(x) \tag{2.10}$$

$$> \max\left(\deg(r_1(x)), \deg(r_2(x))\right) \tag{2.11}$$

$$\geq \deg\left(r_2(x) - r_1(x)\right), \tag{2.12}$$

men dette er en selvmotsigelse, så $q_1(x) = q_2(x)$. Dette impliserer også at $r_1(x) = r_2(x)$. □

Eksempler:

1. La $f(x) = x^3 + 3x + 2, g(x) = x^2 + 1$ i $\mathbb{R}[x]$. Vil finne $q(x), r(x)$ slik som i teoremet over. Da gjør vi polynomdivisjon med $f(x) : g(x)$ (for hånd) og får at $q(x) = x$ og at $r(x) = 2x + 2$, slik at vi kan skrive $f(x) = x(x^2 + 1) + (2x + 1)$.
2. La $f(x) = 4x^3 + x^2 - 3x + 2$ og $g(x) = x^2 + 1$ i $\mathbb{Z}_7[x]$. Ved polynomdivisjon finner vi da at $f(x) = (4x + 1)g(x) + 1$, altså at $q(x) = 4x + 1$ og at $r(x) = 1$.

Theorem: (Korollar) 23.3

La $f(x) \in F(x)$ og $\alpha \in F$. Da har vi at α er en rot av $f(x)$ hvis og bare hvis $x - \alpha$ er en faktor i $f(x)$.

Bevis:

($\Longleftarrow$): Anta $f(x) = q(x)(x - \alpha)$ for $q(x) \in F[x]$. Da vil $f(\alpha) = q(\alpha)(\alpha - \alpha) = 0$, så α er en rot av f.

($\Longrightarrow$): Anta at α er en rot, altså at $f(\alpha) = 0$. Fra teorem 23.1 finnes det da polynomer $q(x), r(x) \in F[x]$ slik at $f(x) = q(x)(x - \alpha) + r(x)$ med $r(x) = 0 \vee \deg r(x) < \deg(x - \alpha) = 1$. Altså må $r(x)$ være en konstant, altså at $r(x) = b \in F$. Så $f(x) = q(x)(x - \alpha) + b$, men hvis vi setter inn α så får vi $0 = q(\alpha) \cdot 0 + b \implies b = 0$. Dermed kan vi skrive $f(x) = q(x)(x - \alpha)$. □

Theorem: (Korollar) 23.5

La $f(x) \in F[x]$ og $f(x) \neq 0$. Da er antall røtter av $f(x)$ mindre enn eller lik graden til $f(x)$.

Bevis: Oppgave (hint: korollar 23.2)

Theorem: (Korollar) 23.6

La F være en kropp og $F^* = F \setminus \{0\}$ være en gruppe med enheter i F under multiplikasjon. Dersom $G \leq F^*$ er en endelig undergruppe så er G syklisk.

Bevis: Oppgave (eventuelt se i boka)

Eksempel: Se på $F = \mathbb{Z}_p$ hvor p er et primtall. Da sier korollar 23.6 at $\mathbb{Z}_p^*$ er en syklisk gruppe.

Husk: Vi sier at $p \in \mathbb{Z}$ er et primtall dersom $p > 1$ og hvis $p = ab$ så må enten $a = 1$ eller $b = 1$ for alle $a, b \in \mathbb{Z}$.

Definition 2.5.1

La $f(x) \in F[x]$ med $f(x) \neq 0$. Da sier vi at $f(x)$ er **irredusibelt** i $F[x]$ dersom

1. $\deg f(x) \geq 1$
2. $f(x) = g_1(x)g_2(x), g_1(x), g_2(x) \in F[x] \implies$ enten $g_1(x)$ eller $g_2(x)$ er et konstant polynom.

Eksempel: $f(x) = x^2 + 1 \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$ er ikke irredusibelt i $\mathbb{C}[x]$ men er irredusibelt i $\mathbb{R}[x]$.

Theorem: 23.10

Hvis $f(x) \in F[x]$ og $\deg f(x) \in \{2, 3\}$, så er $f(x)$ irredusibelt i $F[x]$ hvis og bare hvis $f(x)$ ikke har noen røtter i F.

Bevis: Det er nok å vise at $f(x)$ ikke er irredusibelt i $F[x]$ hvis og bare hvis $f(x)$ har en rot i F.

Anta $f(x)$ har en rot $\alpha \in F$. Da er $f(x) = q(x)(x - \alpha)$ for $q(x) \in F[x]$ i følge korollar 23.2. Da er $\deg f(x) \geq 2$, så $\deg q(x) \geq 1$, så da er $f(x)$ ikke irredusibelt.

Anta at $f(x)$ ikke er irredusibelt i $F[x]$. Da er $f(x) = g_1(x)g_2(x)$ med $g_1(x)g_2(x) \in F[x]$ og $\deg g_1(x), \deg g_2(x) \geq 1$, $\deg f(x) \in \{2, 3\}$, så minst ett av $g_1(x), g_2(x)$ må ha grad 1. La oss si at $\deg g_1(x) = 1$. Da har $g_1(x)$ en rot, så da må $f(x)$ ha en rot også. □

2.6 Homomorfier og Faktorgrupper

Definition 2.6.1

La R være en kommutativ ring. Et **ideal** i R er en delmengde $I \neq \emptyset$ med

1. $a, b \in I \implies a - b \in I$
2. $a \in I, r \in R \implies ra \in I$

Merk: Siden R er en ring så betyr dette at $(R, +)$ er en abelsk gruppe. Dermed følger det fra punkt 1 over at I må være en undergruppe av $(R, +)$.

Eksempler:

1. La $n \in \mathbb{Z}$ og se på $I = n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$. Da er I et ideal i $\mathbb{Z}$.
2. Se på $R = (\mathbb{Z}_8, +_8, \cdot_8) = \{0, 1, \ldots, 7\}$ og $I = \{0, 2, 4, 6\}$. Da har vi at
   (a) For $a, b \in I$ så vil $a -_8 b \in I$
   (b) For $a \in I, b \in R$ så vil $ra \in I$

   Dermed må I være et ideal i R.
3. La F være en kropp og se på polynomringen $F[x]$. Fikser så $f(x)$ og se på $I = (f) = \{fg \mid g \in F[x]\}$. Dette er et ideal i $F[x]$.

   Merk: Notasjonen (f) betyr elementene som kan lages ved å multiplisere med elementet f.

Definition 2.6.2: Faktorring

La R være en kommutativ ring, $I \subseteq R$ et ideal. Da har vi at faktorringen R/I er gitt ved:

1. Elementene i R/I er restklassene $a + I$ for $a \in R$
2. Vi har at

$$(a + I) + (b + I) = (a + b) + I \tag{2.13}$$
$$(a + I)(b + I) = ab + I \tag{2.14}$$

for alle $a, b \in R$.

Theorem

Operasjonene definert i definisjonen over er veldefinerte.

Merk: Dersom vi har at $\phi : R \to S$ er en ringhomomorfi med kjerne $\ker \phi = \{\alpha \in R \mid \phi(\alpha) = 0\}$, så har vi at:

1. $\ker \phi$ er et ideal i R:
   (a) $a, b \in \ker \phi \implies a - b \in \ker \phi$
   (b) $a \in \ker \phi, r \in R \implies ra \in \ker \phi$
2. Vi kan lage faktorringen $R/\ker \phi$ fra første merknad.
3. Vi har at $\phi[R] = \{\phi(\alpha) \mid \alpha \in R\}$ er en underring av S

Theorem: 26.17 (Fundamentalteoremet for ringhomomorfier)

La $\phi : R \to S$ være en ringhomomorfi og R en kommutativ ring med $I = \ker \phi$. Da er funksjonen

$$\mu : R/I \to \phi[R] \tag{2.15}$$
$$a + I \mapsto \phi(n) \tag{2.16}$$

en ringisomorfi, altså en ringhomomorfi som er injektiv og surjektiv.

Strategi: Dersom vi har et ideal $I \subset R$, så kan vi "finne" faktorringen R/I, altså å finne en enklere ring som er isomorf, ved å bruke følgende strategi:

1. Finn en ring S og en surjektiv ringhomomorfi $\phi : R \to S$ med $\ker \phi = I$
2. Fra fundamentalteoremet for ringhomomorfier har vi da at $R/I \cong S$

Eksempler:

1. La $R = \mathbb{Z}$ og $I = (n) = n\mathbb{Z}$. Finn $\mathbb{Z}/I$.

   Dersom vi følger stegene fra strategien over, så ser vi at vi må finne en surjektiv ringhomomorfi $\phi : \mathbb{Z} \to S$ med $\ker \phi = I$. La oss prøve med $S = (\mathbb{Z}_n, +_n, \cdot_n)$, hvor vi definerer funksjonen

$$\phi : \mathbb{Z} \to \mathbb{Z}_n \tag{2.17}$$
$$a \mapsto a \pmod n \tag{2.18}$$

Dette er en gyldig ringhomomorfi, fordi

$$\phi(a+b) = \phi(n) +_n \phi(b) \tag{2.19}$$
$$\phi(ab) = \phi(a) \cdot_n \phi(b) \tag{2.20}$$

Videre så er ϕ surjektiv med $\ker \phi = I$. Dermed er altså $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

2. Se på $\phi : \mathbb{R}[x] \to \mathbb{C}$ gitt ved $\phi(f) = f(i)$, altså funksjonen som sender $a_n x^n + \cdots + a_1 x + a_0 \mapsto a_n(i)^n + \cdots + a_1 i + a_0$. Da er ϕ en ringhomomorfi, fordi $\phi(f+g) = (f+g)(i) = f(i) + g(i)$ og $\phi(fg) = (fg)(i) = f(i) \cdot g(i)$.

   Merk at dersom $z = a + bi$ sa vil $\phi(bx + a) = z$, noe som betyr at ϕ er surjektiv. Videre har vi at $\ker \phi = \{f \in \mathbb{R}[x] \mid \phi(f) = 0\} = \{f \in \mathbb{R}[x] \mid f(i) = 0\}$. Vi har i alle fall at $x^2 + 1$ er et element i denne mengden.

   Vis at $\ker \phi = (x^2+1)g(x) \forall g(x) \in \mathbb{R}[x]$. (Kan bruke divisjonsalgoritmen)

2.7 Maksimale Idealer og Endelige Kropper

Theorem: 27.5

La R være en ring og $I \subseteq R$ et ideal. Da har vi følgende:

$$I = R \iff I \text{ inneholder en enhet} \tag{2.21}$$

Theorem: (Korollar) 27.6 & 27.11

La R være en kommutativ ring. Da har vi følgende ekvivalens:

$$R \text{ er en kropp} \iff (0) \text{ og } R \text{ er de eneste idealene til } R \tag{2.22}$$

Bevis: La R være en kropp og I et ideal slik at $I \neq (0)$. Da må det finnes en $a \in R$ med $a \neq 0$. Siden R er en kropp så må a være en enhet, og da følger det at $I = R$ fra teorem 27.5.

Anta nå at (0) og R er de eneste idealene og velg en $a \in R$ slik at $a \neq 0$. Se nå på idealet generert av a:

$$(a) = \{ar \mid r \in R\} \tag{2.23}$$

Siden $a \neq 0$ så kan ikke $(a) = (0)$, men siden (a) må være et ideal så må da $(a) = R$ per antagelsen vår. Dette betyr blant annet at $1 \in (a)$, som igjen betyr at det finnes en $r \in R$ med $ar = 1$. Men merk at da må a være en enhet og dermed er R en kropp. □

Definition 2.7.1: Maksimalt Ideal

La R være en ring og $M \subseteq R$ et ideal. Vi sier at M er et **maksimalt ideal** dersom følgende krav tilfredsstilles:

1. $M \neq R$
2. Det finnes ingen idealer I hvor $M \subset I \subset R$

Eksempler:

1. For $p \in \mathbb{Z}$, er det slik at (p) er et maksimalt ideal i $\mathbb{Z}$?

   Anta at $(p) \subset I$ for et ideal $I \subseteq \mathbb{Z}$. Da må det finnes et element $a \in I \setminus (p)$, og siden $a \notin (p)$ sa må da $p \nmid a$, altså er $\gcd(p, a) = 1$. Da vet vi at det må finnes $m_1, m_2 \in \mathbb{Z}$ slik at $1 = m_1 a + m_2 p$. Siden $a, p \in I$ så må også $m_1 a + m_2 p \in I$, altså er $1 \in I$. Da har vi at $I = R$ fra teorem 27.5. Så (p) er et maksimalt ideal i $\mathbb{Z}$.

2. Anta at $n \in \mathbb{Z}$ ikke er et primtall og at $n \geq 0$. Da er ikke (n) et maksimalt ideal i $\mathbb{Z}$.

   - Dersom $n = 0$ så er $(n) = \{0\}$, altså ikke et maksimalt ideal
   - Dersom $n = 1$ så er $(n) = \mathbb{Z}$, altså ikke et maksimalt ideal
   - Dersom $n > 1$ så kan vi skrive $n = ab$ hvor $1 < a, b < n$. Da må nødvendigvis (a) og (b) begge inneholde (n), altså er blant annet $(n) \subset (a) \subset \mathbb{Z}$, så da er ikke (n) et maksimalt ideal

3. La F være en kropp og $p(x) \in F[x]$ et irredusibelt polynom. Da er $(p(x)) = \{p(x)q(x) \mid q(x) \in F[x]\}$ et maksimalt ideal i $F[x]$.

   Anta at $(p(x)) \in I$ for et ideal $I \subset F[x]$. Et resultat fra øving 12 sier da at det finnes et polynom $f(x) \in F[x]$ med $I = (f(x))$. Da er $p(x) \in (f(x))$, som betyr at det finnes $g(x) \in F[x]$ slik at $p(x) = f(x)g(x)$. Siden vi har antatt at $p(x)$ er irredusibelt så må da enten $f(x)$ eller $g(x)$ være konstant og $f(x), g(x) \neq 0$. Dersom $f(x)$ er konstant så er $(f(x)) = F[x]$ og hvis $g(x)$ er konstant så må $(f(x)) = (p(x))$. Uansett så vil $(p(x))$ være et maksimalt ideal.

4. Dersom $f(x) \in F[x]$ er redusibelt så er ikke $(f(x))$ et maksimalt ideal.

Theorem: 27.9

Anta at R er en kommutativ ring og at $M \subseteq R$ er et ideal. Da holder følgende ekvivalens:

$$M \text{ er et maksimalt ideal} \iff R/M \text{ er en kropp} \tag{2.24}$$

Konsekvensen av dette og resultatene fra øving 12 er at i $\mathbb{Z}$ og $F[x]$ så er ethvert ideal generert av et element:

- $I \subset \mathbb{Z}$ er et ideal $\implies \exists n \in \mathbb{Z}$ med $I = (n)$.
- $I \subset F[x]$ er et ideal $\implies \exists f(x) \in F[x]$ med $I = (f(x))$.

Sammen med teorem 27.9 og de tidligere eksemplene har vi:

1. Følgende utsagn er ekvivalente for et ideal $I \subset \mathbb{Z}$:
   - I er et maksimalt ideal
   - I er generert av et primtall
   - $\mathbb{Z}/I$ er en kropp
2. Følgende utsagn er ekvivalente for et ideal $I \subset F[x]$:
   - I er et maksimalt ideal
   - I er generert av et irredusibelt polynom
   - $F[x]/I$ er en krop

Eksempel: Se på $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Er $p(x)$ irredusibelt? Husk at fra teorem 23.10 så har vi at dersom et polynom har grad 2 eller 3 så er det irredusibelt hvis og bare hvis det ikke har noen røtter. La oss sjekke $p(x)$:

- $p(0) = 1 \neq 0$
- $p(1) = 2 \neq 0$
- $p(2) = 2 \neq 0$

Så vi har at $p(x)$ er irredusibelt. Da vet vi at $\mathbb{Z}_3[x]/(x^2 + 1)$ er en kropp og har 3^2 elementer.

La nå F være en endelig kropp. Da må vi etter hvert få elementet 0, altså den additive inversen, som et

element i denne lista

$$\{1, 1+1, 1+1+1, \ldots\} := \{1, 2, 3, \ldots\} \tag{2.25}$$

Vi sier at **karakteristikken** til F er $\min\{n \geq 0 \mid n = 0\}$. Dette må være et primtall, fordi hvis ikke måtte en av faktorene vært 0 selv. Dersom vi definerer p til å være karakteristikken til F, så får vi en injektiv ringhomomorfi:

$$\mathbb{Z}_p \to F \tag{2.26}$$

$$a \mapsto \underbrace{1+1+\cdots+1}_{a \text{ ganger}} \tag{2.27}$$

Altså har vi at F inneholder en underkropp som er isomorf med $\mathbb{Z}_p$. La oss identifisere denne med $\mathbb{Z}_p$. Derfor sier vi at: F er en endelig kropp hvis og bare hvis F inneholder $\mathbb{Z}_p$ som underkropp for et primtall p, hvor p er karakteristikken til F.

Siden F er endelig så er $\dim F = d < \infty$. Da har vi en basis $b_1, \ldots, b_d$ i F, så $|F| = p^d$.

Theorem

La p være et primtall. Da har vi at:

1. For alle $d \geq 1$ så finnes det et irredusibelt polynom $p(x) \in \mathbb{Z}_p[x]$ med $\deg p(x) = d$.
2. Vi vet da at $F = \mathbb{Z}_p[x]/(p(x))$ er en kropp.

   Den har $\mathbb{Z}_p$ som underkropp og en basis som vektorrom over $\mathbb{Z}_p$ er $\big(1 + (p(x)), x + (p(x)), \ldots, x^{d-1} + (p(x))\big)$, hvor elementene i basisen er restklasser.
3. Spesielt er $\dim_{\mathbb{Z}_p} F = d$ og $|F| = p^d$
4. Hvis F og F' er to endelige kropper med $|F| = |F'|$ så er de isomorfe.

Algoritme (for å konstruere en kropp med p^d elementer hvis $d \geq 2$):

1. Finn et irredusibelt polynom $p(x) \in \mathbb{Z}_p[x]$ med $\deg p(x) = d$
2. Da vil $\mathbb{Z}_p[x]/(p(x))$ være en kropp med p^d elementer

Merk: $\mathbb{Z}_{p^d}$ er en ring, men ikke en gyldig kropp.