RINGER

Vise **ring**: en ring $(R, +, \cdot)$:

i) $(R,+)$ er en abelsk gruppe

ii) Multiplikasjonen er assosiativ
$(a \cdot b)\, c = a \cdot (b \cdot c)$

iii) Distributive lover holder:
- $a \cdot (b+c) = a \cdot b + a \cdot c$
- $(a+b) \cdot c = a \cdot c + b \cdot c$

Spesielle ringer:

i) R er **kommutativ** hvis
$ab = ba \quad \forall a, b \in R$

ii) R er en **divisjonsring**, hvis hver $a \neq 0$ i R har en invers m.h.p. multiplikasjonen, dvs. $\exists$ $a' \in R$ s.a. $a \cdot a' = 1 = a' \cdot a$

iii) R er en **kropp** hvis R er en kommutativ divisjonsring

Vise **underring**: S ikke-tom delmengde av en ring med 1:

i) $0, 1 \in S$

ii) $(a-b) \in S, \forall\ a, b \in S$

iii) $ab \in S, \forall\ a, b \in S$

Vise **ringhomomorfi** $\varphi : R \to R'$

i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$

iii) $\varphi(1_R) = 1_{R'}$

En ringhom. er en **isomorfi** hvis φ er en-til-en og på.

La R_1. Hvis $a, b \in R \setminus \{0\}$ med $ab = 0$ så kalles a og b **nulldivisorer** i R.
Null divisorene i $\mathbb{Z}_n$ er lik:
$\{\bar{r} \in \mathbb{Z}_n \mid gcd(r, n) > 1\}$

Polynomringer

For polynom $P(x)$ av grad n i $\mathbb{Z}_n$, da er $p(x)$ **irredusibelt** $\iff p(\alpha) \neq 0$ $\forall \alpha \in \mathbb{Z}_n$. Hvis ikke er $(x - \alpha)$ en faktor.

Sammensetningen av to **ring-homomorfi**, slik at $\varphi(\varphi(x))$ er også ringhomomorfier.

KROPPER

- $\mathbb{Z}_p$ - p primtall, da er $\mathbb{Z}_p$ en kropp
- En kropp har ingen nulldivisorer
-
Gruppen $\mathbb{Z}_n \times \mathbb{Z}_m$ er syklisk og isomorf med $\mathbb{Z}_{nm} \iff gcd(n, m) = 1$

- en gruppe er **abelsk**, hvis b.o. * er **kommutativ**
- **Abelske** grupper er **normale**

GRUPPER

Vise $(G, *)$ er en **gruppe**, med bin.op. $*$:

i) $*$ assosiativ $\to a * b = b * a$

ii) G lukket under $*$, $a * b \in G$

iii) $*$ har et id.elem. $e \in G$

iv) alle elem. $a \in G$ har en invers, $\exists\, a' \in G$ s.a. $a * a' = e = a' * a$

Vise at H **undergruppe** av G:

i) H lukket under $*$, $\forall a, b \in H$ så er $a * b \in H$. $H = \{a^n \mid n \in \mathbb{Z}\}$

ii) $e \in H$

iii) $a \in H \Rightarrow a^{-1} \in H$

Generelt: $H \neq \varphi$, $H \subseteq G$. $\forall h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.
Feks matriser, der id matrisen er en ikke-tom mengde.

Syklisk gruppe → abelsk
Kommutativ gruppe → abelsk

Vise **normal gruppe**:
$aH = Ha$ eller $gHg^{-1} = H$

Vise G **homomorfi**: $\varphi : G \to G'$
Hvis $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$ kalles φ en **gruppehomomorfi**

Vise G **isomorfi**:
- Homomorfi
- Den er på
- Ker

↑ $\varphi(a^{-1}) = \varphi(a)^{-1}$
$\varphi(e) = e'$

Setn. 4.1 G gruppe.

a) $H \subseteq G$ normal undergruppe. Def. $\delta : G \to G/H$ ved at $\delta(a) = aH$. δ en gruppehomom. og $\ker \delta = H$.

b) $\varphi : G \to G'$ grp. homomorfi:
$\psi : G/\ker\varphi \to \operatorname{Im}\varphi$
gitt ved at:
$\psi(a \ker \varphi) = \varphi(a)$

$\varphi : G \to G'$ grp.hom. **kjernen** til φ:
$\varphi^{-1}(\{e'\}) = \{g \in G \mid \varphi(g) = e'\}$
$\to \ker\varphi = \varphi^{-1}(\{e^{-1}\})$

"$\iff$". G gruppe med H und.gp.:

i) $aHa^{-1} \in H$ $\forall a \in G, h \in H$

ii) $bHb^{-1} = H$ $\forall b \in G$

iii) $H \subseteq G \to$ **normal undergruppe**.

- enhver **faktorgruppe** av en **syklisk gruppe** er **syklisk**.

SYKLER / PERMUTASJONER

Et element i S_n er et produkt av høyst n disjunkte sykler.

Orden: $\sigma = \gamma_1 \gamma_2 \cdots \gamma_t$ der γ_i er disjunkte sykler i S_n. La d_i være ordenen til γ_i. Da er ordenen til σ: $\text{lcm}(d_1, d_2, \ldots, d_t)$

En permutasjon $\theta \in S_n$ er **like** eller **odde** hvis θ er et produkt av liketall eller et oddetall transposisjoner.

$A_n = \{\theta \in S_n \mid \theta \text{ like perm.}\}$ Da kalles A_n den **alternerende gruppen**.

SYLOWTEORI

Cauchy p primtall, G endelig gruppe med $p \mid G$. Da har G et element av orden p.

Normalisatoren til H i G ($H \subseteq G$ endelig)
$N(H) = \{g \in G \mid gHg^{-1} = H\}$

Sylows 1. G end.gruppe, p primtall og $|G| = p^n m$, $n \geq 1$ og $p \nmid m$:
a) G har en u.g. med orden p^i for hver i med $1 \leq i \leq n$.
b) Hver u.g. $H \subseteq G$ av orden p^i er en normal undergruppe av en u.g. av orden p^{i+1} for $0 \leq i < n$.

Sylow p-und.grp P av en gruppe G er en maksimal p-und.grp. av G.

Sylows 2. P_1 og P_2 to Sylow p-und.grp. av en endelig gruppe G hvor p er et primtall med $p \mid |G|$. Da er P_1 og P_2 konjugerte und.grp. av G.

Sylows 3. endelig G, p primtall, og s er antall Sylow p-undergrupper:
Hvis $p \mid |G|$ da er:
i) $s \equiv 1 \bmod p$
ii) $s \mid |G|$

$28 = 2^2 \cdot 7$
i) $n_7 = 1 \bmod 7$
ii) $n_7 \mid 28$, $n_7 \in \{\ldots\}$

Simpel
En gruppe er **simpel** hvis den er ikke-triviell og har ingen ikke-trivielle normale undergrupper.

IDEAL

$I \neq \emptyset$: $I \subseteq R$ er et **ideal** hvis:
i) $(I, +) \subseteq (R, +)$ er en und.grp.
ii) $\forall r \in R, \forall a \in I \rightarrow ra (= ar)$ et element i I.

$f: R \rightarrow S$ ringhomomorfi av ring med 1. Da er $\ker f = \{r \in R \mid f(r) = 0\}$ et **ideal** i R

- La R_1. Et ideal $I \subseteq R$ er et **maksimalt ideal** hvis $I \neq R$, og I og R er de eneste idealene i R som inneholder I.

- R komm. ring med 1, $I \subseteq R$ ideal. Da er I et **maksimalt ideal** $\iff$ R/I er en kropp.

- F kropp, $0 \neq p(x) \in F[x]$. Da vet vi at idealet $(p(x)) \subseteq F[x]$ er et maksimalt ideal $\iff$ $p(x)$ irreduserbelt polynom.

Orden

- $a^p \equiv 1 \pmod n \rightarrow$ "p" orden
- antall elementer i en gruppe
- ordenen til en sykel er dens lengde
- Hvis orden er en **primtalls-orden** (a^n) så er gruppen **syklisk**

- ordenen til en **symmetri-gruppe** er dens fakultet $|S_7| = 7!$

Binomialformel $\binom{p}{i} \equiv 0 \bmod p$