TMA4150 ALGEBRA - DEFINISJONER OG RESULTATER

Contents

1. Grupper

Definisjon. (i) En *binær operasjon* $*$ på en menge S er en funksjon fra $S \times S$ til S. For $(a, b) \in S \times S$, så skriver vi

$$*((a, b)) = a * b.$$

(ii) For en binær operasjon $*$ på en mengde S med en delmengde $H \subseteq S$, så kalles H *lukket under* $*$ hvis for alle $a, b \in H$ impliserer at $a * b \in H$.

Definisjon. La $*$ være en binær operasjojn på en mengde S.

(i) $*$ kalles *kommutativ* hvis

$$a * b = b * a$$

for alle $a, b \in S$.

(ii) $*$ kalles *assosiativ* hvis

$$a * (b * c) = (a * b) * c$$

for alle $a, b, c \in S$.

(iii) $e \in S$ kalles et *identitetselement* for $*$ på S hvis

$$e * a = a = a * e$$

for alle $a \in S$.

Setning 1. *En binær operasjone $*$ på en mengde S har høyst et identitetselement.*

Definisjon. La $*$ være en binær operasjon på en mengde S. Hvis $*$ har et identitetselement e i S og gitt et element $a \in S$, så er b en *invers av a* hvis

$$a * b = e = b * a.$$

Definisjon. En *gruppe* $(G, *)$ er en ikke-tom mengde G med en binær operasjon $*$ slik at følgende holder:

(i) $\mathcal{G}_1$: $*$ er assosiativ.

(ii) $\mathcal{G}_1$: $*$ har et identitetselement e i G.

(iii) $\mathcal{G}_1$: Alle elementer a i G har en invers, dvs. det eksisterer en $a' \in G$ slik at

$$a * a' = e = a' * a.$$

Elementet a' kalles en invers av a.

Definisjon. En gruppe $(G, *)$ er *abelsk*, hvis $*$ er en kommutativ binær operasjon.

Setning 2. *I enhver gruppe $(G, *)$ holder både den høyre og den venstre kanselleringsloven, dvs.*

$$a * b = a * c \Rightarrow b = c$$

og

$$b * a = c * a \Rightarrow b = c.$$

Setning 3. *La $(G, *)$ være en gruppe, og la $a, b \in G$ være vilkårlig. Likningene*

$$a * x = b \qquad y * a = b$$

har entydige løsninger x og y i G.

Setning 4. *La $(G, *)$ være en gruppe. For enhver $a \in G$, så eksisterer bare ett element $a' \in G$ slik at*

$$a' * a = e = a * a',$$

hvor e betegner identitetselementet i G.

Korollar 5. *La $G = (G, *)$ være en gruppe. For alle $a, b \in G$, så er*

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

Setning 6. *La $(G, *)$ være en gruppe med identitetselement e. En ikke-tom delmengde $H \subseteq G$ er en* undergruppe *av G hvis og bare hvis*

(i) *H er lukket under $*$,*
(ii) *$e \in H$,*
(iii) *$a \in H \quad \Rightarrow \quad a^{-1} \in H$.*

Setning 7. *La G være en gruppe, og la $a \in G$. Da er*

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

en undergruppe av G, og den er den minste som inneholder a.

1.1. **Sykliske grupper.**

Definisjon. (a) H kalles den *sykliske undergruppen av G generert av a*
indexundergruppe!syklisk, og vi skriver $H = \langle a \rangle$.
(b) Hvis $G = \langle a \rangle$ for en $a \in G$, så kalles G en *syklisk* gruppe med *generator a*.

Definisjon. La G være en gruppe.
(a) *Ordenen til G*,

$$|G| = \text{ antall elementer i } G\}.$$

(b) *Ordenen til et element a* i G er gitt ved $|\langle a \rangle|$.

Setning 8. *La $m \in \mathbb{Z}$ med $m > 0$, og la $n \in \mathbb{Z}$. Da eksisterer entydig $q, r \in \mathbb{Z}$ slik at*

$$n = qm + r$$

med $0 \leq r < m$.

Setning 9. *All undergrupper av $(\mathbb{Z}, +)$ er på formen*

$$\langle m \rangle = \{qm \mid q \in \mathbb{Z}\}$$

for en $m \in \mathbb{Z}$.

Setning 10. *Enhver syklisk gruppe er abelsk.*

Setning 11. *En undergruppe av en syklisk gruppe er syklisk.*

Definisjon. For $r, s \in \mathbb{Z}$ er $\mathrm{GCD}(r, s)$ den positive generatoren av undergruppen H av $\mathbb{Z}$ generert av r og s, dvs.

$$H = \{nr + ms \mid m, n \in \mathbb{Z}\}.$$

Vi har at $\mathrm{GCD}(r, s) = \gcd(r, s)$.

Lemma 12. *Anta at* $\gcd(r, s) = 1$. *Hvis* $r \mid sm$, *da vil* $r \mid m$.

Lemma 13. *La* $G = \langle a \rangle$ *være en syklisk gruppe med generator* $a \neq e$. *Anta at* $a^m = e$ *med* $m > 0$ *og minst mulig. Da er*

$$G = \{e, a, a^2, \ldots, a^{m-1}\}$$

og

$$|G| = m.$$

Setning 14. *La* $G = \langle a \rangle$ *være en syklisk gruppe med generator* $a \neq e$.
(a) *Hvis ordenen til* G *er* ∞, *da er*

$$G \simeq (\mathbb{Z}, +).$$

(b) *Hvis ordenen til* G *er endelig, da er*

$$G \simeq (\mathbb{Z}_n, +),$$

der $n = |G|$.

Setning 15. *La* $G = \mathbb{Z}_n$.
(a) *La* $\langle \overline{s} \rangle \subseteq \mathbb{Z}_n$, *og la* $\gcd(s, n) = d$. *Da er*

$$\langle \overline{s} \rangle = \{\overline{0}, \overline{d}, 2\overline{d}, \ldots, (\frac{n}{d} - 1)\overline{d}\} = \langle \overline{d} \rangle$$

. *Spesielt er* $|\langle \overline{s} \rangle = \frac{n}{d}$.
(b) $\langle \overline{s} \rangle = \langle \overline{t} \rangle$ *hvis og bare hvis* $\gcd(s, n) = \gcd(r, n)$.

Korollar 16. *Et element* $\overline{s} \in \mathbb{Z}_n$ *er en generator for* $\mathbb{Z}_n$ *hvis og bare hvis* $\gcd(s, n) = 1$.

2. Permutasjoner

Definisjon. La A være en ikke-tom mengde. En funksjon $\sigma \colon A \to A$ som er en-til-en og på dvs. bijektiv, kalles en *permutasjon av* A.

Setning 17. *La* $A \neq \emptyset$. *La*

$$S_A = \{\textit{alle permutsjoner av } A\}.$$

Da er S_A *en gruppe under sammensetning av permutasjoner.*

Setning 18. *Enhver permutasjon i* S_n *kan skrives som et produkt av disjunkte sykler.*

Definisjon. En sykel i S_n av lengde 2 er en *transposisjon*.

Korollar 19. *Enhver permutasjon i S_n med $n \geq 2$ er et produkt av transposisjoner.*

Setning 20. *Ingen permutasjon i S_n kan uttrykkes både som et produkt av et liketall transposisjoner og som et produkt av et oddetall transposisjoner.*

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

Setning 21. *La*

$$A_n = \{\theta \in S_n \mid \theta \text{ like permutasjon}\}.$$

Da er A_n en undergruppe av S_n.

Gruppen A_n kalles den *n-te alternerende gruppen*.

Definisjon. La G og G' være to grupper, og la $\varphi\colon G \to G'$ være en funksjon. Hvis φ tilfredsstiller

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

for alle $a, b \in G$, så kalles φ en *gruppehomomorfi*.

Lemma 22. *La G og G' være to grupper, og la $\varphi\colon G \to G'$ være en homomorfi av grupper.*

(a) *La* $\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$. *Vis at* $\operatorname{Im}\varphi \subseteq G'$ *er en undergruppe.*
(b) *Hvis φ er en-til-en, vis at φ induserer en isomorfi $\varphi\colon G \to \operatorname{Im}\varphi$.*

3. Restklasser

Vi minner om følgende definisjon.

Definisjon.

Setning 23 (Cayleys teorem)**.** *Enhver gruppe er isomorf med en undergruppe av permutasjoner.*

Definisjon. La $A \neq$ være en mengde.

(a) En *partisjon* av A er en samling av ikke-tomme delmengder $\{A_i\}_{i\in I}$ slik at hvert element i A tilhører **nøyaktig** en delmengde A_i (celle).
(b) En *relasjon* $\mathcal{R}$ på A er en delmengde $\mathcal{R}$ av $A \times A = \{(a, b) \mid a, b \in A\}$. Skriver
$$a\mathcal{R}b \text{ når } (a, b) \in \mathcal{R}.$$
(c) En relasjon $\mathcal{R}$ er en *ekvivalensrelasjon* hvis
  (i) $a\mathcal{R}a$, for alle $a \in A$ (refleksiv),
  (ii) $a\mathcal{R}b \Rightarrow b\mathcal{R}a$ (symmetrisk),

(iii) $a\mathcal{R}b$ og $b\mathcal{R}a \Rightarrow a\mathcal{R}c$ (transitiv).

La G være en gruppe med en undergruppe $H \subseteq G$. Definer en relasjon $\sim_L$ på G ved at

$$a \sim_L b \iff a^{-1}b \in H.$$

Setning 24. *$\sim_L$ er en ekvivalensrelasjon på G.*

Definisjon. La G være en gruppe med en undergruppe $H \subseteq G$. Delmengden

$$aH = \{ah \mid h \in H\}$$

av G kalles den *venstre restklassen av H* som inneholder a.

Merk: H er en venstre restklasse, da $H = eH$.

Lemma 25. *La G være en endelig gruppe med en undergruppe $H \subseteq G$ og $a \in G$. Da er*

$$|H| = |aH|.$$

Setning 26 (Lagrange teorem)**.** *La G være en gruppe, og $H \subseteq G$ en undergruppe. Da deler ordenen til H ordenen til G, dvs.*

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

Definisjon. La H være en undergruppe av en gruppe G. Da kaller vi antall venstre restklasser av H i G for indeksen til H i G, og vi skriver

$$(G : H).$$

Setning 27. *La G være en endelig gruppe.*

(a) *Ordenen til et element $a \in G$ deler ordenen til G.*
(b) *Hvis ordenen til G er et primtall, så er G en syklisk gruppe.*

4. Direkte produkt og endelige abelske grupper

Setning 28. *La G_1 og G_2 være to grupper. Da er det* direkte produktet *av G_1 og G_2 gitt som mengden*

$$\{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}.$$

Vi minner om den tallteoretiske definisjonen av minste felles multiplum av to heltall.

Definisjon. La r, s være to positive heltall. Da er $t > 0$ *minste felles multiplum*, skrevet $t = \text{lcm}(r, s)$, hvis

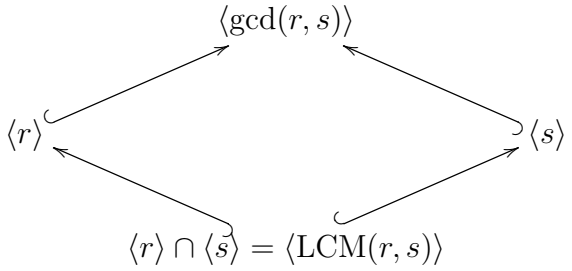
(1) $r \mid t$ og $s \mid t$,
(2) hvis $r \mid u$ og $s \mid u$, så er $t \leq u$.

Oppgave 3. La G være en gruppe. La H_1 og H_2 være to undergrupper av G. Vis at $H_1 \cap H_2$ er en undergruppe av G.

Nå definerer vi en størrelse gruppeteoretisk, som vi skal vise er det samme som minste felles multiplum.

Definisjon. (Se 11.8) La r, s være to positive heltall. Da er $\mathrm{LCM}(r, s)$ den positive generatoren for undergruppen $\langle r \rangle \cap \langle s \rangle$ av $\mathbb{Z}$.

Merk at vi har følgende sammenhenger:



Setning 29. *La G_1, G_2 være to grupper. La $(a, b) \in G_1 \times G_2$, og anta at a har endelig orden r i G_1, og b har endelig orden s i G_2. Da har (a, b) orden $\mathrm{lcm}(r, s)$ i $G_1 \times G_2$.*

Setning 30. *Gruppen $\mathbb{Z}_n \times \mathbb{Z}_m$ er syklisk og isomorf med $\mathbb{Z}_{nm}$ hvis og bare hvis $\gcd(n, m) = 1$.*

Setning 31. *La $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$ for noen grupper $\{G_i\}_{i=1}^n$. Hvis a_i har endelig orden r_i i G_i for $1 \leq i \leq n$, så er ordenen til $(a_1, a_2, \ldots, a_n)$ i $G_1 \times G_2 \times \cdots \times G_n$ lik minste felles multiplum av $r_1, r_2, \ldots, r_n$.*

Setning 32. *Gruppen*

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$$

er syklisk og isomorf med $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ hvis og bare hvis $m_1, m_2, \ldots, m_n$ er parvist relativt primiske, dvs. $\gcd(m_i, m_j) = 1$ for $i \neq j$.

Setning 33 (Strukturteorem for endelige abelske grupper)**.** *La G være en endelig abelsk gruppe. Da er G isomorf med en gruppe*

$$\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_m^{r_n}}$$

der $p_1, p_2, \ldots, p_n$ er (ikke-nødvendigvis forskjellige) primtall og $r_i \geq 1$ for $1 \leq i \leq n$. Videre er denne fremstillingen entydig opp til rekkefølge på de sykliske gruppene $\mathbb{Z}_{p_i^{r_i}}$.

Definisjon. Enn gruppe G er *dekomponerbar* hvis den er isomorf med et direkte produkt av to ekte ikke-trivielle undergrupper (mer enn et element). Ellerls kalles G *ikke-dekomponerbar*.

Setning 34. *De endelige ikke-dekomponerbare abelske gruppene med mer enn ett element er isomorf med $\mathbb{Z}_{p^r}$ for et primtall p og $1 \leq r \in \mathbb{Z}$.*

Definisjon. La H være en undergruppe av en gruppe G. Da kaller vi antall venstre restklasser av H i G for *indeksen til H i G*, og vi skriver $(G : H)$.

Setning 35. *La G være en endelig gruppe.*

(a) *Ordenen til et element $a \in G$ deler ordenen til G.*
(b) *Hvis ordenen til G er et primtall, så er G en syklisk gruppe.*

Setning 36. *Hvis m er et kvadratfritt positivt heltall, dvs. m er ikke delelig med p^2 for et primtall p, da er enhver abelsk gruppe av orden m syklisk.*

Setning 37. *La $\varphi\colon G \to G'$ være en gruppehomomorfi, og la e, e' være identiteten i henholdsvis G og G'. Da gjelder:*

(a) $\varphi(e) = e'$,
(b) *For $a \in G$, så er $\varphi(a^{-1}) = \varphi(a)^{-1}$.*
(c) *Hvis $H \subseteq G$ er en undergruppe, da er*

$$\varphi(H) = \{\varphi(h) \mid h \in H\} \subseteq G'$$

en under gruppe av G'.
(d) *Hvis $H' \subseteq G$ er en undergruppe, da er*

$$\varphi^{-1}(H') = \{g \in G \mid \varphi(g) \in H'\} \subseteq G$$

en undergruppe av G.

Definisjon. La $\varphi\colon G \to G'$ være en gruppehomomorfi. Da er

$$\varphi^{-1}(\{e'\}) = \{g \in G \mid \varphi(g) = e'\}$$

kjernen til φ. Skriver $\operatorname{Ker}\varphi = \varphi^{-1}(\{e'\})$.

Setning 38. *La $\varphi\colon G \to G'$ være en gruppehomomorfi, og la $H = \operatorname{Ker}\varphi$. For $a \in G$, så er*

$$\varphi^{-1}(\{\varphi(a)\}) = \{x \in G \mid \varphi(x) = \varphi(a)\} = aH = Ha.$$

Korollar 39. *En gruppehomomorfi $\varphi\colon G \to G'$ er en-til-en hvis og bare hvis $\operatorname{Ker}\varphi = \{e\}$.*

Definisjon. La G være en gruppe, og la H være en undergruppe. For $a \in G$, så kalles $Ha = \{ha \mid h \in H\}$ *den høyre restklassen til a.*

Definisjon. En undergruppe $H \subseteq G$ er en *normal* undergruppe, hvis

$$aH = Ha$$

for all $a \in G$.

Setning 40. *La G være en gruppe, og la $H \subseteq G$ være en normal undergruppe. La*

$$G/H = \text{mengden av venstre restklasser} = \{aH\}_{a \in G}.$$

Da er G/H en under den binære operasjonen

$$(aH)(bH) = (ab)H$$

for alle $a, b \in G$.

Setning 41. *La G være en gruppe.*

(a) *La $H \subseteq G$ være en normal undergruppe. Definer*

$$\gamma \colon G \to G/H$$

ved at $\gamma(a) = aH$. Da er γ en gruppehomomorfi og $\operatorname{Ker} \gamma = H$.

(b) *La $\varphi \colon G \to G'$ være en gruppehomomorfi. Da er*

$$\psi \colon G/\operatorname{Ker} \varphi \to \operatorname{Im} \varphi$$

gitt ved at

$$\psi(a \operatorname{Ker} \varphi) = \varphi(a)$$

en isomorfi av grupper.

Definisjon. En isomorfi $\varphi \colon G \to G$ for en gruppe G kalles en *automorfi*.

Setning 42. *La G væer en gruppe med en undergruppe H. Følgene er ekvivalent:*

(a) *$aha^{-1} \in H$ for alle $a \in G$ og $h \in H$.*
(b) *$bHb^{-1} = H$ for alle $b \in G$.*
(c) *$H \subseteq G$ er en normal undergruppe.*

Setning 43. *Enhver faktorgruppe av en syklisk gruppe er syklisk.*

Setning 44. *La G være en gruppe med en normal undergruppe H. Hvis G er abelsk, vis at faktorgruppen G/H er abelsk.*

Setning 45. *La G være en gruppe og $H \subseteq G$ en normal undergruppe.*

(a) *Hvis $a \in G$ har orden $n < \infty$, så vil ordenen til aH i G/H dele n.*
(b) *Mer generelt: La $\varphi \colon G \to G'$ være en gruppehomomorfi. Hvis $a \in G$ har orden $n < \infty$, så vil ordenen til $\varphi(a)$ dele n. Spesielt, hvis φ er en-til-en, så er ordenen til $\varphi(a)$ lik a.*

Korollar 46. *La G og G' være to grupper. Hvis G har et element av orden n og G' ikke har et element av orden n, så er $G \not\cong G'$.*

5. Gruppevirkninger og G-mengder

Definisjon. La X være en mengde, og la G være en gruppe. *En virkning av G på X* er en avbildning

$$- * - : G \times X \to X$$

slik at

(i) $e * x = x$, for alle $x \in X$,
(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$, for alle $x \in X$ og $g_1, g_2 \in G$.

Da kalles X en *G-mengde*.

Definisjon. La X være en G-mengde.

(a) Delmengden
$$G * x = \{g * x \mid g \in G\} \subseteq X$$
kalles *banen til x ved G*.
(b) $X_g = \{x \in X \mid g * x = x\}$, g gitt i G,
(c) $G_x = \{g \in G \mid g * x = x\}$, x gitt i X.

Setning 47. *La X være en G-mengde. Da er G_x en undergruppe av G for hver $x \in X$.*

Definisjon. G_x er *isotropi-undergruppe* av x i G.

Setning 48. *La X være en G-mengde, og la $x \in X$. Da er*

$$|G * x| = (G : G_x) = \textit{antall venstre restklasser av } G_x \textit{ i } G.$$

Hvis $|G|$ er endelig, så er

$$|G| = |G_x||G * x|.$$

Definisjon. La X være en G-mengde. La

$$N = \{g \in G \mid g * x = x \text{ for alle } x \in X\}.$$

Vi har vist at N er en normal undergruppe av G.

(i) Hvis $N = \{e\}$, så kalles virkningen av G på X *trofast*.
(ii) Gruppen G virker *transitivt* på X, hvis for ethvert par av elementer x_1 og x_2 i X, så finnes det en $g \in G$ slik at $g * x_1 = x_2$.

Setning 49 (Burnside's teorem)**.** *La X være en endelig G-mengde for en endelig gruppe G. La*

$$r = \textit{antall baner i } X.$$

Da er

$$r|G| = \sum_{g \in G} |X_g|.$$

6. Sylowteori

Setning 50. *La G være en gruppe av orden p^n for $n \geq 1$, og X en endelig G-mengde. Da er*

$$|X| \equiv |X_G| \mod p,$$

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

Setning 51 (Cauchy's teorem)**.** *La p være et primtall og G en endelig gruppe med $p \mid G$. Da har G et element av orden p, dvs. G har en undergruppe av orden p.*

Definisjon. La G være en gruppe og p et primtall.

(a) Da er G en *p-gruppe* hvis hvert element i G har orden p^i for en $i \geq 0$.
(b) En *p-undergruppe* er en undergruppe som er en p-gruppe.

Definisjon. La G være en endelig gruppe med en undergruppe H. La

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

som kalles *normalisatoren til H i G*.

Korollar 52. *La G være en endelig gruppe, og la p være et primtall. Da er G en p-gruppe hvis og bare hvis $|G| = p^n$ for en $n \geq 0$.*

Lemma 53. *La H være en p-undergruppe av en endelig gruppe G. Da er*

$$(N(H) : H) \equiv (G : H) \mod p.$$

Setning 54 (1. Sylowteorem)**.** *La G være en endelig gruppe, p et primtall og $|G| = p^n m$ med $n \geq 1$ og $p \not| m$. Da har vi*

(a) *G har en undergruppe med orden p^i for hver i med $1 \leq i \leq n$.*
(b) *Hver undergruppe $H \subseteq G$ av orden p^i er en normal undergruppe av en undergruppe av orden p^{i+1} for $0 \leq i < n$.*

Definisjon. En *Sylow p-undergruppe P* av en gruppe G er en maksimal p-undergruppe av G, dvs. en p-undergruppe som ikke er inneholdt i noen større p-undergruppe.

Setning 55 (2. Sylowteorem)**.** *La P_1 og P_2 være to Sylow p-undergrupper av en endelig gruppe G hvor p er et primtall med $p \mid |G|$. Da er P_1 og P_2 konjugerte undergrupper av G.*

Setning 56 (3. Sylowteorem)**.** *La G være en endelig gruppe hvor p er et primtall og s er antall Sylow p-undergrupper. Hvis $p \mid |G|$, da er*

(i) $s \equiv 1 \mod p$,
(ii) $s \mid |G|$.

7. Ringer

Definisjon. En *ring* $(R, +, \cdot)$ er en mengde R med to binære operasjoner $+$ og $\cdot$ (addisjon og multiplikasjon) slik at

(i) $(R, +)$ er en abelsk gruppe,
(ii) multiplikasjonen er assosiativ: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(iii) distributive lover holder:
- $a \cdot (b + c) = a \cdot b + a \cdot c$,
- $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definisjon. En ring R er en ring med 1 (identitetselement) hvis det eksisterer nøytralt element $1 \in R$ med hensyn på multiplikasjonen, dvs. det eksisterer $1 \in R$ slik at

$$1 \cdot a = a = a \cdot 1$$

for alle $a \in R$.

Definisjon. Her definerer vi noen spesielle ringer.

(i) R er *kommutativ* hvis $ab = ba$ for alle $a, b \in R$.
(ii) R er en *divisjonsring*, hvis hver $a \neq 0$ i R har en invers med hensyn på multiplikasjonen, dvs. det eksisterer en $a' \in R$ slik at $aa' = 1 = a'a$.
(iii) R er en *kropp* hvis R er en kommutativ divisjonsring.

Setning 57. *La R være en ring med 1 og 0 identitetselement med hensyn på $+$. Vis følgende for alle elementer $a, b \in R$:*

(a) $0 \cdot a = 0 = a \cdot 0$.
(b) $a(-b) = (-a)b = -(ab)$.
(c) $(-a)(-b) = ab$.

Lemma 58. *La R være en ring med 1. Da har R mer enn ett element hvis og bare hvis $1 \neq 0$.*

Lemma 59. *La R være en ring med 1 hvor $1 \neq 0$. Da er R en divisjonring hvis og bare hvis $(R \setminus \{0\}, \cdot)$ er en gruppe.*

Setning 60. *La $n \geq 1$. Da er $\mathbb{Z}_n$ en kropp hvis og bare hvis n er et primtall.*

8. Homomorfier

Definisjon. La R og R' være ringer med 1. En funksjon $\varphi \colon R \to R'$ er en *ringhomomorfi* hvis

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$,
(iii) $\varphi(1_R) = 1_{R'}$.

Lemma 61. *La $\varphi\colon R \to R'$ være en ringhomomorfi. Da er φ en-til-en hvis og bare hvis*

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\} = \{0\}.$$

Definisjon. En ringhomomorfi $\varphi\colon R \to R'$ er en *isomorfi* hvis φ er en-til-en og på.

Definisjon. La R være en ring med $1(\neq 0)$. Et element $u \in R$ er en *enhet* hvis u har en invers i R med hensyn på multiplikasjonen, dvs. det eksisterer en $u' \in R$ slik at

$$uu' = 1 = u'u.$$

Definisjon. La R være en ring med 1. Hvis $a, b \in R \setminus \{0\}$ med $ab = 0$, så kalles a og b *nulldivisorer* i R.

Setning 62. *Nulldivisorene i $\mathbb{Z}_n$ er lik*

$$\{\overline{r} \in \mathbb{Z}_n \mid \gcd(r, n) > 1\}.$$

Definisjon. La R være en kommutativ ring med 1. Ringen R kalles et *integritetsområde* hvis R ikke har noen nulldivisorer, dvs. $ab = 0$ medfører at $a = 0$ eller $b = 0$.

8.1. **Direkte produkt av ringer.** Gitt to ringer R_1 og R_2 med 1. Det *direkte produktet av ringene R_1 og R_2* er gitt ved den underliggende mengden

$$R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\},$$

der addisjonen er gitt ved

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$$

og multiplikasjonen er gitt ved

$$(r_1, r_2) \cdot (r_1', r_2') = (r_1 \cdot r_1', r_2 \cdot r_2')$$

og identitetselement

$$1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2}).$$

Setning 63. *Hvis R er et endelig integritetsområde, da er R en kropp.*

Setning 64. *La $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ være gitt ved at*

$$\varphi(a + n\mathbb{Z}) = \overline{r_a},$$

der $a = nq_a + r_a$ for q_a, r_a i $\mathbb{Z}$ med $0 \leq r_a < n$. Vis at φ er en isomorfi av ringer med 1.

Setning 65 (Fermat's lille teorem)**.** *La p være et primtall. Hvis $a \in \mathbb{Z}$ og $p \not| a$, da er*

$$a^{p-1} \equiv 1 \mod p.$$

Korollar 66. *La p være et primtall. Hvis $a \in \mathbb{Z}$, da er*

$$a^p \equiv a \mod p.$$

Setning 67 (Euler's teorem)**.** *La $n > 1$, $a \in \mathbb{Z}$ med $\gcd(a, n) = 1$. Da er*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Setning 68. *La $a, b \in \mathbb{Z}$ med $1 \leq a, b < n$, og anta at $\gcd(a, n) = 1$. Da har likningen*

$$\overline{a}x = \overline{b}$$

en entydig løsning i $\mathbb{Z}_n$.

Korollar 69. *Hvis $\gcd(a, n) = 1$, da har $ax \equiv b \mod n$ som løsninger alle tallene i nøyaktig en restklasse modulo n, dvs.*

$$s + n\mathbb{Z} = \{s + qn \mid q \in \mathbb{Z}\}$$

for en $s \in \mathbb{Z}$.

Setning 70. *La $a, b \in \mathbb{Z}$ med $1 \leq a, b < n$, og la $d = \gcd(a, n)$. Da har likningen*

$$\overline{a}x = \overline{b}$$

en løsning i $\mathbb{Z}_n$ hvis og bare hvis $d \mid b$. Hvis $d \mid b$, så har likningen nøyaktig d løsninger i $\mathbb{Z}_n$.

Setning 71. *La $n > 1$ i $\mathbb{Z}$ hvor $n = p_1 p_2 \cdots p_t$, der p_i er primtall med $p_i \neq p_j$ for $i \neq j$ (dvs. n er kvadratfritt). For $a \in \mathbb{Z}$, så har vi*

$$a^{\varphi(n)+1} \equiv a \mod n,$$

der φ betegner Eulers phi-funksjon.

Korollar 72. *La $n > 1$ være et kvadratfritt heltall, og la $a \in \mathbb{Z}$. For hver $k \geq 1$, så er*

$$a^{k\varphi(n)+1} \equiv a \mod n,$$

der φ betegner Eulers phi-funksjon.

9. Polynomringer

La R være en ring med 1.

(i) Definer et *polynom* $f(x)$ med koeffisienter i R til å være en uendelig formell sum

$$\sum_{i \geq 0} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots,$$

der $a_i \in R$ og $a_i \neq 0$ for bare et endelig antall i'er. Elementene $\{a_i\}_{i\geq 0}$ er *koeffisientene til polynomet* $f(x)$. Skriver

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

hvis $a_i = 0$ for alle $i > n$.

(ii) *Graden til* $f(x)$ er gitt ved

$$\deg f(x) = \begin{cases} n, & \text{hvis } a_n \neq 0 \text{ og } a_i = 0 \text{ for } i > n. \\ -\infty, & \text{hvis } a_i = 0 \text{ for alle } i \geq 0. \end{cases}$$

(iii) La $f(x) = \sum_{i\geq 0} a_ix^i$ og $g(x) = \sum_{i\geq 0} b_ix^i$ være polynomer med koeffisienter i R. Da er $f(x) = g(x)$ hvis $a_i = b_i$ for alle $i \geq 0$.

La $R[x]$ betegne mengden av alle polynomer med koeffisienter i R. Definer to binære operasjoner på $R[x]$, $+$ og $\cdot$: La

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

og

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n,$$

der $n = \max\{\deg f(x), \deg g(x)\}$. Definer

(i) $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n$.

(ii) $f(x)g(x) = d_0+d_1x+d_2x^2+\cdots+d_nx^n$, der $d_t = \sum_{i=0}^{t} a_ib_{t-i} \in R$.

Setning 73. *La R være en ring med 1. Da er*

(a) *$R[x]$ er en ring med 1, der $+$ og $\cdot$ er som over.*

(b) *R er en kommutativ ring hvis og bare hvis $R[x]$ er en kommutativ ring.*

(c) *R er et integritetsområde hvis og bare hvis $R[x]$ er et integritetsområde.*

Definisjon. La R være en ring med 1. En ikke-tom delmengde $S \subseteq R$ er en *underring* av R hvis

$$(S, +|_{S\times S}, \cdot|_{S\times S})$$

er en ring med $1_S = 1_R$.

Oppgave. Vis følgende resultat:

En ikke-tom delmengde S av en ring R med 1 er en underring hvis og bare hvis

(i) $0, 1 \in S$,

(ii) $(a - b) \in S$ for alle $a, b \in S$,

(iii) $ab \in S$ for alle $a, b \in S$.

Definisjon. La E være en kropp. En underring $F \subseteq E$ kalles en *underkropp*, hvis F er en kropp.

Setning 74. *La E være en kropp med en underkropp $F \subseteq E$. La $\alpha \in E$. Definer*

$$\varphi_\alpha \colon F[x] \to E$$

ved a

$$\varphi_\alpha(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n,$$

dvs. $\varphi_\alpha(f(x)) = f(\alpha)$. Da er φ_α en homomorfi av ringer.

Definisjon. La E være en kropp med en underkropp $F \subseteq E$. Et element $\alpha \in E$ er en *rot* i $f(x) \in F[x]$, hvis

$$f(\alpha) = 0,$$

dvs. $\varphi_\alpha(f(x)) = 0$, ekvivalent at $f(x) \in \operatorname{Ker} \varphi_\alpha$.

Setning 75 (Divisjonsalgoritme for polynomer)**.** *La F være en kropp. La*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

og

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1} + x^m$$

i $F[x]$ med $a_n \neq 0$ og $m > 0$. Da fins entydige polynomer $q(x)$ og $r(x)$ i $F[x]$, slik at

$$f(x) = q(x)g(x) + r(x),$$

der $r(x) = 0$ eller $0 \leq \deg r(x) < m$.

Setning 76. *La F være en kropp, $f(x)$ et polynom i $F[x]$ og $a \in F$. Da er a en rot i $f(x)$ hvis og bare hvis $f(x) = q(x)(x - a)$ for et polynom $q(x)$ i $F[x]$.*

Korollar 77. *Et ikke-null polynom $f(x) \in F[x]$ for en kropp F har høyst $\deg f(x)$ antall røtter i F.*

Definisjon. La F være en kropp. Et ikke-konstant polynom $f(x) \in F[x]$ er *irredusibelt over F* hvis

$$f(x) = g(x)h(x)$$

med $g(x), h(x) \in F[x]$ medfører at $g(x) \in F$ eller $h(x) \in F$.

Setning 78. *La F være en kropp, og la $f(x) \in F[x]$ med $\deg f(x) = 2$ eller 3. Da er $f(x)$ irredusibelt over F hvis og bare hvis $f(x)$ har ingen røtter i F.*

Setning 79. *La F være en kropp. Ethvert polynom $f(x) \in F[x] \setminus F$ kan faktoriseres i $F[x]$ i et endelig produkt av irredusible polynomer, og de irredusible polynomene er entydig opp til rekkefølge og opp til enheter.*

Setning 80. *La F være en endelig kropp. Da er $(F \setminus \{0\}, \cdot)$ en syklisk gruppe.*

9.1. **Idealer. MERK:** Vi antar fra nå av at alle ringene vi betrakter er kommutative.

Definisjon. En ikke-tom delmengde $I \subseteq R$ er et *ideal* hvis

(i) $(I, +) \subseteq (R, +)$ er en undergruppe,
(ii) for alle $r \in R$ og for alle $a \in I$, så er $ra (= ar)$ et element i I.

Setning 81. *La F være en kropp. Alle idealene i $F[x]$ er av formen $(g(x))$ for et polynom $g(x)$ i $F[x]$.*

Setning 82. *La $f\colon R \to S$ være en ringhomomorfi av (kommutative) ring mer 1. Da er*

$$\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$$

et ideal i R.

9.2. **Faktorring.** La R være en ring med et ideal $I \subseteq R$. Vet at $(I, +) \subseteq (R, +)$ er en normal undergruppe, siden $(R, +)$ er en abelsk gruppe. Da kan vi danne oss faktorgruppen

$$(R/I, +).$$

Ønsker å vise at vi kan betrakte R/I som en ring.

Elementer: $r + I$, for alle $r \in R$,
Addisjon: $(r + I) + (r' + I) \stackrel{\text{def}}{=} (r + r') + I$,
Multiplikasjon: $(r + I) \cdot (r' + I) \stackrel{\text{def}}{=} rr' + I$.
Husk: $r + I = r' + I \iff r - r' \in I$.

Setning 83. *La R være en (kommutativ) ring med 1, og la $I \subseteq R$ være et ideal. Da er R/I en ring med 1, der*

$$(r + I) + (r' + I) \stackrel{def}{=} (r + r') + I,$$

$$(r + I) \cdot (r' + I) \stackrel{def}{=} rr' + I,$$

og

$$1_{R/I} = 1_R + I.$$

Spesielt, R kommutativ medfører at R/I er kommutativ.

Setning 84. *La $f\colon R \to S$ være en ringhomomorfi av (kommutative) ringer med 1. Da har vi følgende:*

(a) $\operatorname{Im} f = \{f(r) \mid r \in R\} \subseteq S$ *er en underring.*
(b) $\overline{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$, *der*

$$\overline{f}(a + \operatorname{Ker} f) = f(a)$$

er en ringisomorfi.

9.3. **Maksimale idealer.**

Definisjon. La R være en ring med 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.

Setning 85. *La R være en kommutativ ring med 1, og la $I \subseteq R$ være et ideal. Da er I et maksimalt ideal hvis og bare hvis R/I er en kropp.*

Setning 86. *La F være en kropp. La $0 \neq p(x) \in F[x]$. Da har vi at idealet $(p(x)) \subseteq F[x]$ er maksimalt hvis og bare hvis $p(x)$ er et irredusibelt polynom over F.*

9.4. **Vektorrom over en kropp.**

Definisjon. La F være en kropp. Et *vektorrom* V over F er en abelsk gruppe $(V, +)$ med en virkning av F på V, dvs. det fins en funksjon

$$F \times V \xrightarrow{\varphi} V,$$

der vi skriver $\varphi(a, v) = av$ (skalarmultiplikasjon) slik at følgende aksiomer er oppfylt

(1) $(a + b)v = av + bv$,
(2) $a(v + w) = av + bw$,
(3) $a(bv) = (ab)v$,
(4) $1_F \cdot v = v$,

for alle $a, b \in F$ og $v, w \in V$.

Merk: 1) De samme aksiomene som for vektorrom over $\mathbb{R}$ eller $\mathbb{C}$.

2) Mange resultater i linear algebra bruker elementære radoperasjoner og at de har inverse operasjoner. Har vi det tilsvarende for vektorrom over en kropp?

Elementær radoperasjon	Invers av radoperasjonen over F
Multiplisere en rad med $c \in F \setminus \{0\}$	Multiplisere samme rad med c^{-1}.
To rader bytter plass $i \leftrightarrow j$	Radene bytter plass igjen, $i \leftrightarrow j$.
Legger et ikke-null multiplum c av rad i til rad j, der $i \neq j$	Legger $-c \cdot$ rad i til rad j.

Sjekk bevisene for vektorrom over $\mathbb{R}$ og $\mathbb{C}$ for å se at de ikke bruker annet enn at $\mathbb{R}$ og $\mathbb{C}$ er kropper. Dette gjør at vi har de samme resultatene og definisjonene, spesielt de følgende, der F er en kropp og V er vektorrom over F:

Definisjon. (a) En mengde $\{v_i\}_{i \in I} \subseteq V$

(i) *utspenner* V hvis for alle $v \in V$ eksisterer $a_i \in F$ slik at

$$v = \sum_{i \in I} a_i v_i,$$

der kun endelig mange av a_i'ene er $\neq 0$.

(ii) er *lineært uavhengig* hvis

$$\sum_{i \in I} a_i v_i = 0,$$

der kun endelig mange av a_i'ene er $\neq 0$, impliserer at $a_i = 0$ for alle $i \in I$.

(iii) er *en basis for* V hvis den utspenner V og er lineært uavhengig.

(b) V er et *endelig dimensjonalt vektorrom* hvis en endelig delmengde av V utspenner V.

Oppgave 2'. La V være et endelig dimensjonalt vektorrom over en kropp F. Vis en av følgende påstander:

(a) Vis at enhver lineær uavhengig mengde kan utvides til en basis for V.

(b) Enhver mengde som utspenner V inneholder en basis for V.

(c) V har en basis, og alle basiser for V består av det samme antall elementer, betegnes $\dim_F V$, og kalles *dimensjonen til* V *over* F.

(d) La $\{v_i\}_{i=1}^n$ være en delmengde av V som utspenner V. Vis at $\{v_i\}_{i=1}^n$ er en basis for V hvis og bare hvis for alle $v \in V$ så kan v skrives entydig på formen

$$v = \sum_{i=1}^{n} a_i v_i$$

med $a_i \in F$.

9.5. **Endelig kropper.** La R være et integritetsområde. Definer $\varphi \colon \mathbb{Z} \to R$ ved at

$$\varphi(z) = \begin{cases} \underbrace{1_R + 1_R + \cdots + 1_R}_{z \text{ ganger}}, & z > 0, \\ 0, & z = 0, \\ \underbrace{(-1_R) + (-1_R) + \cdots + (-1_R)}_{-z \text{ ganger}}, & z < 0, \end{cases}$$

(a) Vis at φ er en homomorfi av ringer.

(b) Vis at enten er $\operatorname{Ker} \varphi = (0)$ eller $\operatorname{Ker} \varphi = p\mathbb{Z}$ for et primtall p.

Hvis R er en kropp, så kalles den ikke-negative generatoren av $\operatorname{Ker} \varphi$ for *karakteristikken* til kroppen R.

Setning 87. *La E være en endelig kropp.*

(a) *Det eksisterer en underkropp $F \subseteq E$ med $F \simeq \mathbb{Z}_p$ for et primtall p (p er karakteristikken til E (og F)).*

(b) *E er et vektorrom over $F \simeq \mathbb{Z}_p$.*

(c) *E har p^n elementer der $n = \dim_F E$.*
(d) *$E \simeq \mathbb{Z}_p[x]/(p(x))$ for et irredusibelt polynom $p(x)$ over $\mathbb{Z}_p$ av grad n.*

Setning 88. *La F være en kropp, og la $f(x) \in F[x]$ med $\deg f(x) \geq 1$.*
(a) *Da eksisterer en kropp E med F som underkropp slik at $f(a) = 0$ for en $a \in E$, dvs. $f(x)$ har en rot i E.*
(b) *Det eksisterer en kroppp $\widetilde{F}$ slik at $f(x)$ er et produkt av lineære faktorerer over $\widetilde{F}$ (og alle røttene i $f(x)$ er i $\widetilde{F}$).*

Setning 89. *La F være en kropp med karakteristikk p og la $n \geq 1$. La $\widetilde{F}$ være en kropp som inneholder alle røttene i $x^{p^n} - x$, og $F \subseteq \widetilde{F}$ er en underkropp. Polynomet $x^{p^n} - x$ har p^n forskjellige røtter i $\widetilde{F}$.*

Lemma 90. *La F være en kropp med karakteristikk $p > 0$. For $\alpha, \beta \in F$ så er*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

for alle $n \geq 1$.

Setning 91. *For hvert primtall p og heltall $n \geq 1$, så eksisterer det en kropp E med p^n elementer og $\mathbb{Z}_p \subseteq E$ er en underkropp.*

Setning 92. *La p være et primtall og n et heltall med $n \geq 1$. Hvis E og E' er to kropper med p^n elementer, da er $E \simeq E'$.*

Mangler et eller annet sted???????

Setning 93. *La G være en endelig abelsk gruppe. Hvis $m \mid |G|$, så finnes det en undergruppe H av G med orden m.*

Index