Intro til Kryptografi

Jon-Magnus Rosenblad

23. november 2023

Innhold

1 Grunnleggende notasjon og mengdelære

Definisjon 1.1. En *mengde* er en samling objekter S hvor vi kan for ethvert objekt e vite om e tilhører S, skrevet $e \in S$, eller ikke, skrevet $e \notin S$.

Objektene som tilhører en mengde kalles *elementene* i mengden.

Vi noterer ofte en mengde med elementene den inneholder, til eksempel skriver vi de naturlige tallene som

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

Eksempel 1.2. De naturlige tallene $\mathbb{N}$, heltallene $\mathbb{Z}$, de rasjonale tallene $\mathbb{Q}$, de reelle tallene $\mathbb{R}$ og de komplekse tallene $\mathbb{C}$ danner alle mengder.

Det finnes en tom mengde $\emptyset = \{\}$, og vi kan lage mengder av mengder, slik som mengden av den tomme mengden $\{\emptyset\} \neq \emptyset$.

Det finnes også samlinger av objekter som ikke danner mengder.

Eksempel 1.3. Samlingen av alle mengder som ikke inneholder seg selv er ikke en mengde. Om vi snakker om samlinger som ikke er mengder fremhever vi ofte at de ikke er mengder ved å bruke for eksempel klammeparenteser, så denne samlingen kan skrives som

$$[S \mid S \notin S]$$

Bemerkning 1.4. Et element er enten med i en mengde eller ikke – det finnes ingen idè om flere av det samme elementet i en mengde. Altså om vi har $S = \{a, b\}$, men $a = b = 1$, så vil $S = \{1\}$.

Om vi vil ha flere elementer, og samtidig bryr oss om rekkefølgen av elementer så bruker vi en *tuppel* (a, b), så om $a = b = 1$ har vi $(a, b) = (1, 1) \neq (1)$, men for $a \neq b$ har vi $(a, b) \neq (b, a)$.

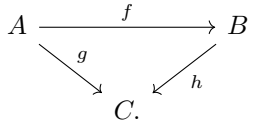
Definisjon 1.5. En *avbildning* $f\colon A \to B$ mellom to mengder er en regel som for ethvert element $a \in A$ assosierer et element $b = f(a) \in A$.

Vi kaller A *definisjonsmengden* til f og B *verdimengden*. Vi definerer også en delmengde av B

$$\operatorname{im} f = \{b \in B \mid \text{det finnes } a \in A \text{ slik at } f(a) = b\} \subset B$$

som vi kaller *bildet* av f.

Vi tegner ofte opp avbildninger som piler, så om vi har flere mengder A, B, C, men flere avbildninger $f\colon A \to B, g\colon A \to C, h\colon B \to C$ imellom seg kan vi tegne det opp som



For ethvert element $a \in A$ finnes det bare èn verdi for $f(a) \in B$. Derimot kan flere verdier a, a' avbilde på samme verdi $f(a) = f(a')$.

Eksempel 1.6. For enhver mengde A finnes det en naturlig avbildning $\mathrm{id}_A \colon A \to A$ som sender hvert element $a \in A$ på seg selv $a \mapsto a$

Bemerkning 1.7. Merk at for enhver mengde A så finnes det nøyaktig en avbildning $\emptyset \to A$, men det finnes ingen avbildning $A \to \emptyset$ med mindre $A = \emptyset$.

Eksempel 1.8. Om vi har to avbildninger $A \xrightarrow{f} B \xrightarrow{g} C$ kan vi lage en ny avbildning $g \circ f \colon A \to C$ ved å sende $g \circ f(a) = g(f(a))$ for alle $a \in A$.

Definisjon 1.9. En avbildning $f \colon A \to B$ er *injektiv* om for alle $a, b \in A$ med $a \neq b$ så er $f(a) \neq f(b)$. Om f er injektiv skriver vi ofte pilen som $f \colon A \hookrightarrow B$ og sier at f er en *inklusjon*.

Avbildningen er *surjektiv* om for alle $b \in B$ så finnes en $a \in A$ slik at $f(a) = b$. Om f er surjektiv skriver vi noen ganger pilen som $f \colon A \twoheadrightarrow B$ og sier at f er en *surjeksjon*.

Om f er både injektiv og surjektiv sier vi den er *bijektiv* og sier f er en *bijeksjon*.

Lemma 1.10. *Om $f \colon A \to B$ er en bijeksjon så finnes en unik avbildning $g \colon B \to A$ slik at $f \circ g = \mathrm{id}_B$ og $g \circ f = \mathrm{id}_A$, dvs. $f(g(b)) = b$ for alle $b \in B$ og $g(f(a)) = a$ for alle $a \in A$. Vi kaller g inversavbildningen til f og skriver $f^{-1} = g$.*

Bevis. Definer en regel $g \colon B \to A$ som for hver $b \in B$ finner en $a \in A$ slik at $f(a) = b$. En slik a finnes alltid for enhver b siden f er surjektiv.

La g' være en annen funksjon konstruert på samme måte, det vil si g' tilfredsstiller $f(g'(b)) = b$ for alle $b \in B$. Men $f(g(b)) = b = f(g'(b))$ og f er injektiv, så $g(b) = g'(b)$ for alle $b \in B$, så $g = g'$. □

Eksempel 1.11. For en mengde A er id_A en bijeksjon, og inversavbildningen er avbildningen selv $\mathrm{id}_A = \mathrm{id}_A^{-1}$.

Eksempel 1.12. Vi kan ta *snitt* og *union* av mengder for å skape nye mengder. Snittet av to mengder A, B er mengden av elementer som ligger i både A og B

$$A \cap B = \{e \mid e \in A \text{ og } e \in B\},$$

mens unionen er mengden av elementer i enten A eller B

$$A \cup B = \{e \mid e \in A \text{ eller } e \in B\}.$$

Når vi tar snitt og union følger det med naturlige inklusjoner

$$\begin{array}{ccc} A \cap B & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A & \hookrightarrow & A \cup B \end{array}$$

. Disse er så naturlige at vi benevner dem som $A \cap B \subset A, B \subset A \cup B$ utenfor diagrammer, altså er snittet $A \cap B$ en *delmengde* av A (og B), og A (og B) er en delmengde av $A \cup B$.

Eksempel 1.13. Vi har

$$\{1, \ldots, 10\} \cap \{5, \ldots, 15\} = \{5, 6, 7, 8, 9, 10\},$$

og

$$\{1, \ldots, 10, \} \cup \{5, \ldots, 15\} = \{1, \ldots, 15\}.$$

Definisjon 1.14. Vi kan ta *komplementet* av to mengder A, B

$$A \setminus B = \{a \in A \mid a \notin B\} \subset A.$$

Eksempel 1.15. Vi kan ta produktet av to mengder A, B. Dette er mengden

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

Her følger også med noen avbildninger

$$A \xleftarrow{p} A \times B \xrightarrow{q} B$$

hvor $p\colon (a, b) \mapsto a$ og $q\colon (a, b) \mapsto b$ er projeksjonene til første og andre element henholdsvis.

Eksempel 1.16. Produktmengden til $\{0, \ldots, 9\}$ med seg selv består av hunder elementer, og vi har en bijeksjon $\{0, \ldots, 9\} \times \{0, \ldots, 9\} \to \{0, \ldots, 99\}$ gitt ved $(n, m) \mapsto 10n + m$.

Definisjon 1.17. Vi kan snakke om størrelsen på en mengde A – altså *kardinaliteten* til mengden, som vi benevner $|A|$ eller $\#A$. Om A inneholder et endelig antall elementer, så er $\#A$ antall elementer i A. Om A ikke er endelig kan vi fortsatt snakke om kardinaliteten til A, og vi kan sammenligne kardinaliteter, for om det finnes en inklusjon $A \hookrightarrow B$ kan vi si $\#A \leq \#B$, og om det finnes en bijeksjon så har vi $\#A = \#B$.

Eksempel 1.18. Vi har

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

så åpenbart har vi

$$\#\mathbb{N} \leq \#\mathbb{Z} \leq \#\mathbb{Q} \leq \#\mathbb{R} \leq \#\mathbb{C},$$

men det viser seg at

$$\#\mathbb{N} = \#\mathbb{Z} = \#\mathbb{Q} < \#\mathbb{R} = \#\mathbb{C}.$$

Merk at $\mathbb{Z}$ og $\mathbb{R}$ har forskjellig kardinalitet, men begge er uendelige. Vi benevner den første uendeligheten med $\aleph_0 = \#\mathbb{Z}$, og den sistnevnte som $\aleph_1 = \#\mathbb{R}$.

Eksempel 1.19. La A, B være to mengder. Vi kan lage mengden av alle avbildninger fra A til B

$$\mathrm{Map}(A, B) = \{f\colon A \to B\}.$$

Vi sier to avbildninger $f, g\colon A \to B$ er like om $f(a) = g(a)$ for alle $a \in A$.

Oppgaver

1. Vis at om $f\colon A \hookrightarrow B$ er en injeksjon så finnes en $g\colon B \twoheadrightarrow A$ slik at $g \circ f = \mathrm{id}_A$. Er den unik?

2. La $A \xrightarrow{f} B \xrightarrow{g} C$ være to avbildninger.

   (a) Anta $g \circ f$ er surjektiv. Vis at da må f være surjektiv.

   (b) Anta $g \circ f$ er injektiv. Vis at da må f være injektiv.

   (c) Om $g \circ f$ er en bijeksjon, må f eller g være en bijeksjon?

3. La U være en mengde, og $A, B \subset U$ to delmengder. Vis identiteten

$$U \setminus (A \cap B) = (U \setminus A) \cup (U \setminus B).$$

4. La A, B være to endelige mengder, og la $n = \#A$ og $m = \#B$, vis at da er $\#\mathrm{Map}(A, B) = m^n$. Dette motiverer hvorfor flere forfattere velger å skrive $\mathrm{Map}(A, B) = B^A$.

5. La $\mathrm{Bij}(A)$ benevne mengden av bijeksjoner $s\colon A \to A$, og la $f\colon A \to B$ være en bijeksjon. Vis at avbildningen $\tilde{f}\colon \mathrm{Bij}(A) \to \mathrm{Bij}(B)$ gitt ved $s \mapsto f \circ s \circ f^{-1}$ er en bijeksjon.

Mengdeteoretisk definerer vi ofte en avbildning $A \to B$ som en samling data (A, B, Γ) med $\Gamma \subset A \times B$ slik at for alle $a \in A$ så finnes en unik $b \in B$ slik at $(a, b) \in \Gamma$. Denne delmengden Γ kalles *grafen* til funksjonen, for om vi skal gi den tilhørende "regelen" f får vi $f(a) = b$ for alle $(a, b) \in \Gamma$.

Bemerkning 1.20. Merk at for en $A \to B$ er både A og B del av dataen, så for to avbildninger f, g med definisjonsmengde A og samme graf $\Gamma_f = \Gamma_g$ så kan de være forskjellige om de har forskjellige verdimengder B_f, B_g, til eksempel om $B_g \subsetneq B_f$.

Eksempel 1.21. La $f\colon \mathbb{Z} \to \mathbb{Z}$ og $g\colon \mathbb{Z} \to 2\mathbb{Z}$ hvor

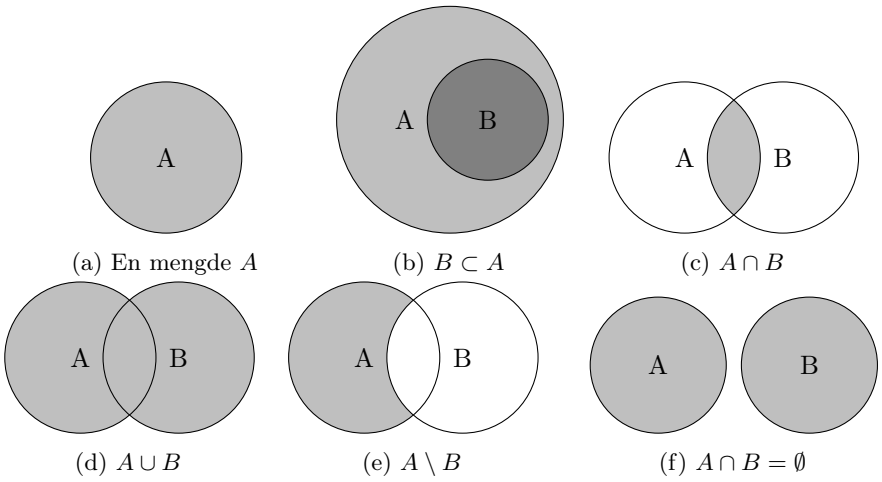
$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Både f og g er gitt ved $f(n) = g(n) = 4n$ for alle $n \in \mathbb{Z}$, så de har samme bilde i $\mathrm{im}\, f = \mathrm{im}\, g \subset \mathbb{Z}$, men de har forskjellig verdimengde, så $f \neq g$.

6. (a) Hva betyr det for Γ at f er injektiv?

   (b) Hva betyr det for Γ at f er surjektiv?

   (c) Kan du bevise Lemma 1.10 på en annen måte ved å bruke denne nye definisjonen av en avbildning?



(a) En mengde A (b) $B \subset A$ (c) $A \cap B$

(d) $A \cup B$ (e) $A \setminus B$ (f) $A \cap B = \emptyset$

Figur 1: Konsepter om mengder.

1.1 Mengdelære i kryptografi

Mengdelære er et veldig fundamentalt område innen matematikken, men enda kan vi bruke noen av disse primitive redskapene til å si noe om kryptografiske metoder.

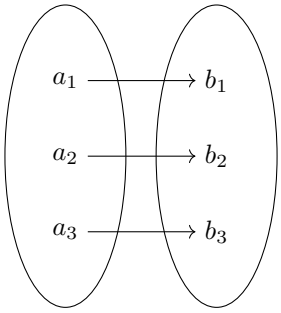
Vi har sett fire kategorier av kryptografiske metoder, nemlig

- hashing,
- symmetrisk kryptering,
- asymmetrisk kryptering, og
- nøkkelutveksling.

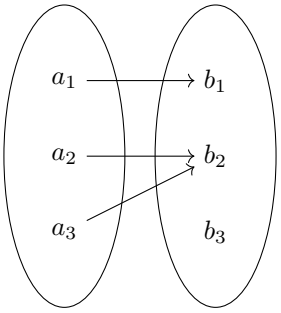
Disse kan alle beskrives som avbildninger, og vi kan allerede si at disse avbildningene må tilfredsstille visse egenskaper, men først må vi definere mengdene disse avbildningene avbilder imellom.

Ofte er det tre mengder vi har i tankene,

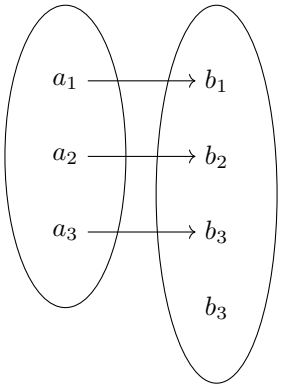
- $\mathscr{M}$ – mengden av meldinger som Alice og Bob kan tenke seg å sende. Dette kan være mengden av alle tekster som kan tenkes og skrives, eller det kan være en forhåndsbestemt mengde av bare et fåtall uttrykk, slik som $\{\text{Ja}, \text{Nei}\}$.
- $\mathscr{K}$ – mengden av nøkler som kan velges av Alice og Bob.
- $\mathscr{C}$ – mengden av mulige chiffertekster.



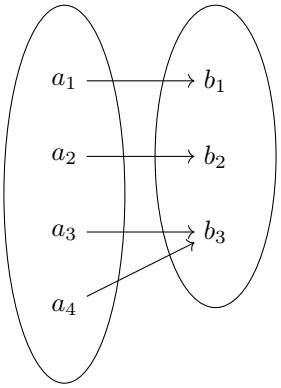
(a) En bijeksjon.



(b) Hverken en injeksjon eller surjeksjon.



(c) En injeksjon.



(d) En surjeksjon.

Figur 2: Konsepter om avbildninger.

1.1.1 Hash-funksjoner

En hashfunksjon i generell forstand er bare en avbildning $h\colon \mathscr{M} \to \mathscr{C}$. Ofte ønsker vi noe som heter en *perfekt* hash som vil si at om vi har to forskjellige meldinger $m \neq m' \in \mathscr{M}$ så hashes meldingene til forskjellige chiffertekster $h(m) \neq h(m') \in \mathscr{C}$. I kryptografi er det ofte tilstrekkelig at det ikke er "for mange" meldinger som har samme chiffertekst, men vi stiller ofte andre strenge krav til hvordan chifferteksten skal skille seg mellom ulike meldinger.

1.1.2 Symmetrisk kryptering

En symmetrisk krypteringsalgoritme er to avbildninger $f\colon \mathscr{M} \times \mathscr{K} \to \mathscr{C}$ og $g\colon \mathscr{C} \times \mathscr{K}t \to \mathscr{M}$ slik at for alle $m \in \mathscr{M}$ og $k \in \mathscr{K}$ har vi $g(f(m,k),k) = m$. Om vi velger en fast nøkkel $k \in \mathscr{K}$ kan vi definere to nye funksjoner

$$f_k\colon \begin{cases} \mathscr{M} \to \mathscr{C} \\ m \mapsto f(m,k) \end{cases}$$

og

$$g_k\colon \begin{cases} \mathscr{C} \to \mathscr{M} \\ c \mapsto g(c,k), \end{cases}$$

så $g_k \circ f_k = \mathrm{id}_{\mathscr{M}}$. Spesielt betyr dette at f_k må være injektiv, og g_k blir dermed surjektiv.

1.1.3 Asymmetrisk kryptering

En asymmetrisk algoritme er nesten det samme, men nå kan vi tenke oss at f og g bruker bare delvis informasjon om nøkkelen. Nå kan vi tenke oss en nøkkel $k \in \mathscr{K}$ som et par $k = (k_a, k_b)$ hvor $k_a \in \mathscr{K}_a$ velges blant en mengde private nøkler, og $k_b \in \mathscr{K}_b$ velges blant en mengde offentlige nøkler, så $\mathscr{K} \subset \mathscr{K}_a \times \mathscr{K}_b$.

Nå blir de to funksjonene gitt ved

$$f\colon \mathscr{M} \times \mathscr{K}_a \to \mathscr{C}$$
$$g\colon \mathscr{C} \times \mathscr{K}_b \to \mathscr{M}$$

slik at $g_{k_b} \circ f_{k_a} = \mathrm{id}_{\mathscr{M}}$. Det som er viktig her er at (k_a, k_b) alltid opptrer i par slik at for hver $k_a \in \mathscr{K}_a$ finnes en unik $k_b \in \mathscr{K}_b$ slik at $g_{k_b} \circ f_{k_a} = \mathrm{id}_{\mathscr{M}}$ og visa versa. Det følger at vi har en bijeksjon $\mathscr{K}_a \to \mathscr{K}_b$ som for hver private nøkkel gir den tilhørende offentlige nøkkelen, men denne bijeksjonen må være umulig å beregne for at algoritmen skal være sikker. Merk at $\mathcal{K} \subset \mathcal{K}_a \times \mathcal{K}_b$ er grafen til denne bijeksjonen. For at algoritmen skal være brukbar må det derimot være mulig å trekke tilfeldige nøkkelpar (k_a, k_b) fra $\mathcal{K}$.

1.1.4 Nøkkelutveksling

I klassisk Diffie-Hellman er algoritmen for Alice og Bob identisk, så vi har to funksjoner

$$f \colon \mathscr{K} \times \mathscr{K} \to \mathscr{K}$$
$$g \colon \mathscr{K} \to \mathscr{K}$$

slik at om Alice velger en nøkkel k_a og Bob en nøkkel k_b har vi $f(k_a, g(k_b)) = f(k_b, g(k_a))$. Her er $g(k_a$ Alice sin offentlige nøkkel som hun deler med Bob, og $g(k_b)$ er Bob sin offentlige nøkkel som han deler med Alice. For algoritmens sikkerhet er det viktig at man ikke kan regne ut k fra $g(k)$, og at gitt $g(k_a)$ og $g(k_b)$ kan vi ikke regne ut $f(k_a, g(k_b))$.

2 Grunnleggende gruppeteori

Definisjon 2.1. En *gruppe* $(G, *)$ er en mengde G sammen med en avbildning $*\colon G \times G \to G$. For to elementer $g, h \in G$ skriver vi $*(g, h)$ som $g * h$. Paret $(G, *)$ må tilfredsstille at

- det finnes et element $e \in G$ hvor for alle $g \in G$ har vi $e * g = g * e = g$. Dette elementet er unikt med denne egenskapen (vis dette!) og kalles *identitetselementet* $e_G = e \in G$.
- for $g, h, i \in G$ har vi $g * (h * i) = (g * h) * i$, altså $*$ er *assosiativ*, og
- for hver g finnes et element $h \in G$ slik at $g * h = e$. Dette elementet h er unikt med denne egenskapen (vis dette!) og vi benevner det $h = g^{-1}$, *inverselementet*.

Vi sier at $*$ er *gruppeoperatoren* til gruppen $(G, *)$.

For å gjøre notasjonen enklere skriver vi ofte bare G for gruppen $(G, *)$ når gruppeoperatoren er åpenbar. Vi forkorter ofte også $g * h$ som gh.

Definisjon 2.2. En avbildning $f\colon G \to H$ mellom to grupper er en *morfi* om

- $f(e_G) = e_H$, og
- for alle $g, g' \in G$ har vi $f(gg') = f(g)f(g')$.

Definisjon 2.3. En delmengde $H \subset G$ av en gruppe $(G, *)$ er en *undergruppe* om

- $e \in H$,
- for alle $h, h' \in H$ er $h * h' \in H$, og
- for alle $h \in H$ er $h^{-1} \in H$.

Bemerkning 2.4. Inklusjonen av en undergruppe $H \subset G$

$$H \hookrightarrow G$$

er en morfi.

Eksempel 2.5. Vi kjenner allerede til mange eksempler på grupper, slik som kjeden av delmengder

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

hvor vi lar $\mathbb{C} = (\mathbb{C}, +)$ være en gruppe under addisjon danner en kjede av undergrupper. Merk at $\mathbb{N}$ ikke er en gruppe under addisjon siden det ikke finnes invers elementer.

Om vi fjerner 0 fra alle mengdene

$$\mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$$

og utruster $\mathbb{C}$ med multiplikasjon isteden, så danner dette en kjede med undergrupper.

Eksempel 2.6. Mengden bestående av ett element $G = \{0\}$ er en gruppe under den eneste mulige avbildningen $G \times G \to G$. Denne kalles den *trivielle gruppen* og benevnes ofte bare som $0 = G$. Akkurat som vi alltid har en inklusjon av den tomme mengden i en mengde $\emptyset \subset S$, har alltid en inklusjon av den trivielle gruppen $0 \hookrightarrow H$ til en annen H ved å sende $0 \mapsto e_H$.

Merk at den tomme mengden $\emptyset$ ikke er en gruppe siden den ikke har et identitetelement.

Eksempel 2.7. Om $(G, *_G), (H, *_H)$ er to grupper så danner $(G \times H, *)$ en gruppe hvor $*$ er operatoren

$$(g, h) * (g', h') = (g *_G g', h *_H h').$$

Til eksempel er det reelle planet $\mathbb{R}^2$ en gruppe under vektor-addisjon.

Eksempel 2.8. La $\mathrm{Bij}(A)$ være mengden av bijeksjoner $A \to A$. Da er $(\mathrm{Bij}(A), \circ)$ en gruppe.

Eksempel 2.9. Mengden $\mathrm{Mat}_{2\times 2}$ av (2×2)-matriser under addisjon danner en gruppe.

Eksempel 2.10. Mengden $\mathrm{GL}_2(\mathbb{R})$ av inverterbare (2×2)-matriser med koeffisienter i $\mathbb{R}$ danner en gruppe under matrise multiplikasjon.

Eksempel 2.11. La $f \colon G \to H$ være en morfi. Husk at for en avbildning definerte vi bildet av avbildningen $\operatorname{im} f \subset H$ som en delmengde. Denne delmengden er også en undergruppe.

La $f \colon G \to H$ være en morfi. I tillegg til bildet $\operatorname{im} f \subset H$ kan vi lage en annen undergruppe.

Definisjon 2.12. Vi definerer *kjernen* til $f \colon G \to H$ som

$$\ker f = \{g \in G \mid f(g) = e_H\} \subset G.$$

Lemma 2.13. *Kjernen* $\ker(f \colon G \to H) \subset G$ *av en morfi er en undergruppe av* G*.*

Bevis. Vi trenger å vise at $e_G \in \ker f$, at $\ker f$ er lukket under gruppe-operatoren, og at det finnes inverser. Den førstnevnte følger fra at $f(e_G) = e_H$ siden f er en morfi.

La $g, g' \in \ker f$, da har vi $f(g) = f(g') = e_H$, men $f(gg') = f(g)f(g') = e_H$, så $gg' \in \ker f$).

La $g \in \ker f$, så $f(g) = e_H$, men $f(g^{-1}) = f(g)^{-1} = e_H$, så $g^{-1} \in \ker f$. □

Korollar 2.14. *La* $f \colon G \to H$ *være en morfi slik at* $\ker f = \{e_G\}$ *(skriver ofte* $\ker f = 0$*). Da er* f *injektiv.*

Bevis. Anta det finnes g, g' slik at $f(g) = f(g')$. Da har vi at

$$f(g^{-1}g') = f(g)^{-1}f(g') = e_H,$$

så $g^{-1}g' \in \ker f$, men $\ker f = \{e_G\}$, så $g = g'$. □

Vi så med mengder at om $f\colon A \to B$ er en bijeksjon så finnes det en avbildning $g\colon B \to A$ slik at $g \circ f = \mathrm{id}_A$ og $f \circ g = \mathrm{id}_B$. Det tilsvarende konseptet for grupper er "isomorfier", og vi tar denne egenskapen som definisjonen.

Definisjon 2.15. En morfi $f\colon G \to H$ er en *isomorfi* dersom det finnes en morfi $g\colon H \to G$ slik at $g \circ f = \mathrm{id}_G$ og $f \circ g = \mathrm{id}_H$.

Definisjon 2.16. La $(G, *_G), (H, *_H)$ være to grupper. Vi kan definere en operator $*_{G\times H}$ på $G \times H$ ved

$$(g, h) *_{G\times H} (g', h') = (g *_G g', h *_H h').$$

Dette gjør $G \times H$ til en gruppe med identitetselement (e_G, e_H).

Som med mengder har vi fortsatt de to projeksjonene

$$G \xleftarrow{\ p\ } G \times H \xrightarrow{\ q\ } H,$$

men vi har også inklusjoner den andre veien

$$G \xrightarrow{\mathrm{id}_G \times e_H} G \times H \xleftarrow{e_G \times \mathrm{id}_H} H,$$

gitt ved $(\mathrm{id}_G \times e_H)\colon g \mapsto (g, e_H)$ og $(e_G \times \mathrm{id}_H)\colon h \mapsto (e_G, h)$. Disse tilfredsstiller $p \circ (\mathrm{id}_G \times e_H) = \mathrm{id}_G$ og $q \circ (e_G \times \mathrm{id}_H) = \mathrm{id}_H$. Merk også at $\mathrm{im}(\mathrm{id}_G \times e_H) = \ker q$.

Oppgaver

1. Finn enhetselementet og inverselementene til alle eksemplene på grupper nevnt ovenfor.

2. Vis at det bare finnes ett element $e \in G$ slik at $e * g = g * e = g$ for alle $g \in G$, altså at identitetselementet er unikt.

3. Vis at for enhver $g \in G$ så finnes det bare ett element $h \in G$ slik at $gh = e$.

4. Vis at for en morfi $f\colon G \to H$ så har vi for alle $g \in G$ at $f(g^{-1}) = f(g)^{-1}$.

5. Vis at for en morfi $f\colon G \to H$ så er $\mathrm{im}\, f \subset H$ en undergruppe.

6. (a) La $f\colon G \to H$ være en bijektiv morfi. Vis at den bijektive inversen $f^{-1}\colon H \to G$ er en morfi, altså er f er isomorfi.

   En morfi $f\colon G \to H$ kalles en *monomorfi* om det finnes en morfi $g\colon H \to G$ slik at $g \circ f = \mathrm{id}_G$. En morfi kalles en *epimorfi* om det finnes en morfi $h\colon H \to G$ slik at $f \circ h = id_H$.

   (b) Vis at $f\colon G \to H$ er en monomorfi hvis og bare hvis f er en injektiv morfi.

   (c) Vis at $f\colon G \to H$ er en epimorfi hvis og bare hvis f er en surjektiv morfi.

7. La $\phi\colon G \to G'$ og $\psi\colon H \to H'$ være to isomorfier. Vis at morfien

$$\phi \times \psi\colon \begin{cases} G \times H \to G' \times H' \\ (g,h) \mapsto (\phi(g), \psi(h)) \end{cases}$$

er en isomorfi.

Så langt har vi sett mange eksempler på uendelige grupper, slik som $\mathbb{C}$ og dens undergrupper. Vi ønsker å se på flere eksempler av *endelige* grupper, det vil si grupper hvor den underliggende mengden er endelig.

8. La $S^1 \subset \mathbb{C}$ være enhetsirkelen

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

   (a) Vis at S^1 er en gruppe under (kompleks) multiplikasjon.

   (b) La n være et heltall og la $\mu_n \subset S^1$ være mengden av n-te enhetrøtter

$$\mu_n = \{e^{\frac{k}{n}2\pi i} \mid k \in \mathbb{Z}\}.$$

   Vis at $\#\mu_n = n$ og at μ_n er en delgruppe av S^1.

   (c) Ta for deg μ_3, μ_4 og μ_{12}. Vis at $f\colon \mu_{12} \to \mu_3 \times \mu_4$ gitt ved

$$e^{\frac{k}{12}2\pi i} \mapsto (e^{\frac{k}{3}2\pi i}, e^{\frac{k}{4}2\pi i})$$

   er en isomorfi.

   Det finnes en slik isomorfi $\mu_{nm} \to \mu_n \times \mu_m$ så lenge $\gcd(n,m) = 1$.

   (d) Vis at det ikke finnes noen isomorfi $\mu_4 \to \mu_2 \times \mu_2$.

   (e) La n, m være to heltall slik at $m|n$. Vis at $\mu_m \subset \mu_n$ er en undergruppe.

9. Ta for deg gruppen $\mathrm{Bij}(S)$ av bijeksjoner $S \to S$ hvor S er en endelig mengde. Vi så at om vi har en bijeksjon $f\colon S \to S'$ så er avbildningen $\tilde{f}\colon \mathrm{Bij}(S) \to \mathrm{Bij}(S')$ gitt ved $\sigma \mapsto f \circ \sigma \circ f^{-1}$ for hver $(\sigma\colon S \to S) \in \mathrm{Bij}(S)$ en bijeksjon.

   (a) Vis at $\tilde{f}$ er en morfi. Det følger dermed at at $\tilde{f}$ er en isomorfi.

   (b) Vis (ved induksjon) at om S, S' er to endelige mengder slik at $\#S = \#S'$. Da finnes det en bijeksjon $S \to S'$.

   Vi har nå sett at om to endelige mengder S, S' har samme antall elementer så er gruppene av bijeksjoner $\mathrm{Bij}(S), \mathrm{Bij}(S')$ isomorfe. La $n = \#S$. Vi gir denne gruppen det generelle navnet *gruppen av permutasjoner av n elementer* $S_n = \mathrm{Bij}(\{1, \ldots, n\})$.

   (c) Vis at $\#S_n = n!$.

10. La G være en endelig gruppe. En nært beslektet mengde til S_n er mengden $\mathrm{Aut}(G) = \mathrm{Iso}(G, G)$ av isomorfier $G \to G$, såkalte *automorfier* av G.

(a) Vis at $(\mathrm{Aut}(G), \circ)$ er en gruppe.

(b) Vis at om en bijeksjon $f\colon G \to H$ er en isomorfi, så er $\tilde{f}\colon \mathrm{Aut}(G) \to \mathrm{Aut}(H)$ en isomorfi.

(c) Vis at $\mathrm{Aut}(\mu_4)$ ikke er isomorf med $\mathrm{Aut}(\mu_2 \times \mu_2)$. [Merk at $\#\mathrm{Aut}(\mu_4) = 2$.]

3 Restklasser

Definisjon 3.1. La $H \subset G$ være en undergruppe. En *restklasse* av H i G er en mengde på formen

$$gH = \{gh \mid h \in H\}$$

for en $g \in H$. Merk at $g \in gH$ siden $e \in H$.

Eksempel 3.2. La $G = \mathbb{Z}$ være gruppen av heltall under addisjon. Ta for deg undergruppen $H = 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ av partall. Partallene har to restklasser i $\mathbb{Z}$, nemlig mengden vi får når vi legger til et partall $2m$

$$2m + (2H) = \{2m + 2n = 2(m + n) \mid n \in \mathbb{Z}\} = 2\mathbb{Z}$$

som blir partallene selv, og mengden vi får når vi legger til et oddetall

$$(2m + 1) + (2H) = \{2m + 1 + 2n = 2(m + n) + 1 \mid n \in \mathbb{Z}\} = 1 + 2\mathbb{Z}$$

som blir alle oddetallene.

Lemma 3.3. *La g, g' være to elementer i G, og la $H \subset G$ være en undergruppe av G. Vi har*

$$gH = g'H$$

hvis og bare hvis $g^{-1}g' \in H$.

Bevis. Anta at $gH = g'H$, så for alle $h \in H$ finnes en $h' \in H$ slik at $gh = g'h'$, men da kan vi regne

$$\begin{aligned} gh &= g'h' \\ g^{-1}gh = h &= g^{-1}g'h' \\ h(h')^{-1} &= g^{-1}g'h'(h')^{-1} = g^{-1}g' \end{aligned}$$

så $g^{-1}g' = h(h')^{-1} \in H$ siden H er en undergruppe.

For den andre veien anta at $g^{-1}g' \in H$. Anta for motsigelse at $gH \neq g'H$, så ved symmetri kan vi anta ("uten tap av generalitet") at det finnes et element $gh \in gH$ slik at $gh \notin g'H$. Men $g^{-1}g' \in H$, så $h' = (g^{-1}g')^{-1}h \in H$, så $gh = g(g^{-1}g')h' = g'h' \in g'H$, men vi antok at $gh \notin g'H$, så vi har en motsigelse. □

Korollar 3.4. *Om $gH \cap g'H \neq \emptyset$ så har vi $gH = g'H$.*

Korollar 3.5. *Restklassene til $H \subset G$ danner en partisjon av G, det vil si vi kan finne en **delmengde** (ikke en gruppe) elementer $S \subset G$ slik at $gH \cap g'H = \emptyset$ for alle $g, g' \in S$ med $g \neq g'$, og*

$$\bigcup_{g \in S} gH = G.$$

Bevis. La $\mathscr{S}$ være mengden delmengder $S \subset G$ slik at for alle $g, g' \in G$ så har vi $gH \cap g' = \emptyset$ for $g \neq g'$. Anta $\tilde{S} \in \mathscr{S}$ er maksimal, det vil si det finnes ingen $S \in \mathscr{S}$ slik at $\tilde{S} \subsetneq S$. Vi påstår at $\bigcup_{g \in \tilde{S}} gH = G$. Anta for motsigelse at det finnes en $g' \in G$ slik at $g' \notin \bigcup_{g \in \tilde{S}} gH$. Da har vi at $g'H \cap gH = \emptyset$ for alle $g \in \tilde{S}$, for ellers har vi $g' \in gH$ ved Korollar 3.4, men da har vi at $\tilde{S} \cup \{g'\} \in \mathscr{S}$ som motsier at $\tilde{S}$ er maksimal, så det finnes ingen slik g' og $\bigcup_{s \in \tilde{S}} gH = G$. □

Bemerkning 3.6. Hvordan vet vi egentlig at det i det hele tatt finnes en maksimal mengde $\tilde{S}$ i $\mathscr{S}$? Om gruppen er uendelig kan man tenke seg at vi alltid har plass til å legge til flere og flere elementer til $\tilde{S}$. Det som redder oss er at vi vet at $\tilde{S}$ er ihvertfall mindre enn G, så vi kan på en litt innviklet måte bruke et ganske abstrakt aksiom kalt *Zorns lemma* til å vite at det finnes et maksimalt element, men vi vet ikke nødvendigvis hvordan vi skal finne et slikt element!

3.1 Kvotientgruppen

Lemma 3.7. *La G være en gruppe, $H \subset G$ en undergruppe og $g \in G$ et element. Da er $\#gH = \#H$.*

Bevis. Vi har en naturlig avbildning $f\colon H \to gH$ gitt ved $h \mapsto gh$. Denne er surjektiv per definisjon av gH, så det gjenstår å vise at den er injektiv.

Anta at $f(h) = f(h')$ for to $h, h' \in H$, altså at $gh = gh'$, men da har vi at

$$h = g^{-1}f(h) = g^{-1}f(h') = h'.$$

□

Definisjon 3.8. La G være en gruppe og $H \subset G$ en undergruppe. Vi definerer mengden av restklasser

$$G/H = \{gH \mid g \in G\}.$$

Bemerkning 3.9. Merk at avbildningen $G \to G/H$ gitt ved $g \mapsto gH$ ikke er injektiv, for det er flere ulike $g \neq g'$ slik at $gH = g'H$, og dette er akkurat de parene (g, g') slik at $g^{-1}g' \in H$.

Eksempel 3.10. La $H \subset G$ være endelige grupper. Vi har allerede sett at restklassene danner en partisjon av G, og nå har vi sett at alle restklassene er like store. Det følger umiddelbart at vi må ha

$$\#G = \#(G/H)\#H,$$

altså

$$\#G/\#H = \#(G/H)$$

som motiverer notasjonen. Dette er et kjent resultat.

Korollar 3.11 (Lagranges teorem)**.** *La $H \subset G$ være en undergruppe av en endelig gruppe. Da er H endelig og $\#H | \#G$.*

Vi kan tenke oss en naturlig gruppeoperator på mengden G/H, nemlig at for to restklasser gH og $g'H$ definerer vi produktet deres som

$$(gH)(g'H) = (gg')H,$$

men husk at vi har flere elementer $\hat{g} \in G$ som gir samme restklasse $\bar{g}H = gH$ enda $\bar{g} \neq g$. Så for at denne operatoren skal være "veldefinert" på G/H trenger vi at $(\bar{g}g')H = (gg')H$, det vil si at $(gg')^{-1}(\bar{g}g') = (g')^{-1}hg' \in H$ hvor $h = g^{-1}g \in H$, men dette er ikke automatisk!

Eksempel 3.12. Ta for deg gruppen av permutasjoner $G = S_3$ av mengden på tre elementer $\{1, 2, 3\}$, og la H være undergruppen bestående av identiteten og permutasjonen

$$(12)\colon \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3. \end{cases}$$

La $g = (13)$ og $g'(23)$. Vi ser at $gH = \{(13)e, (13)(12)\} = \{(13), (123)\}$, så $\bar{g}H = gH$ hvor $\bar{g} = (123)$, men $gg' = (13)(23) = (321)$, mens $\bar{g}g' = (123)(23) = (12)$, så

$$(gg')H = (321)H \neq H = (12)H = (\bar{g}g')H.$$

Definisjon 3.13. En undergruppe $H \subset G$ er *normal* dersom

$$gH = Hg = \{hg \mid h \in H\}$$

for alle $g \in G$.

Lemma 3.14. *Om $H \subset G$ er en normal undergruppe så er "multiplikasjon" veldefinert på mengden av restklasser G/H, så G/H danner en gruppe – kvotientgruppen av G over H.*

Bevis. Om vi har $gH = Hg$ for alle $g \in H$ så følger det at $H = g^{-1}Hg$, så $g^{-1}hg \in H$ for alle $h \in H$. □

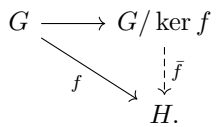
Lemma 3.15. *La $f\colon G \to H$ være en morfi. Da er $\ker f \subset G$ en normal undergruppe.*

Bevis. La $vg \in (\ker f)g$. Vi ønsker å vise at $vg \in g \ker f$, men det er det samme som at $g^{-1}vg \in \ker f$. Vi ser at

$$\begin{aligned} f(g^{-1}vg) &= f(g^{-1})f(v) \\ &= (f(g))^{-1}e_H f(g) \\ &= e_H, \end{aligned}$$

så $g^{-1}vg \in \ker f$. □

Teorem 3.16 (Isomorfiteoremet)**.** *La $f\colon G \to H$ være en surjektiv morfi. Da har vi en isomorfi $\hat{f}\colon G/\ker f \to H$, det vil si vi kan fylle inn følgende avbildning*



Bevis. Vi benevner restklassen $g + \ker f$ i $G/\ker f$ ved $\bar{g}$. Vi konstruerer en avbildning $\bar{f}\colon G/\ker f \to H$ ved at for en $\bar{g} \in G/\ker f$ setter vi $\bar{f}(\bar{g}) = f(g)$ for en representant g.

Om vi velger en annen representant g' med $\bar{g}' = \bar{g}$ har vi at $g^{-1}g' \in \ker f$, så $f(g) = f(g)f(g^{-1}g') = f(gg^{-1})f(g') = f(g')$, så definisjonen av $\bar{f}$ er uavhengig av hvordan vi velger representanter.

For alle $h \in H$ så finnes en $g \in G$ slik at $f(g) = h$, så $\bar{f}(\bar{g}) = h$, og $\bar{f}$ er surjektiv.

La g, g' slik at $f(g) = f(g')$. Da er $f(g^{-1}g') = f(g)^{-1}f(g') = e$, så $g^{-1}g' \in \ker f$, så $\bar{g} = \bar{g}'$.

Det gjenstår å vise at $\bar{f}$ er en morfi, det vil si at for alle $\bar{g}, \bar{g}' \in G/\ker f$ så er $\bar{f}(\bar{g}\bar{g}') = \bar{f}(\bar{g})\bar{f}(\bar{g}')$. Vi har at $\bar{g}\bar{g}' = \overline{(gg')}$, og vi vet allerede at dette er veldefinert siden $\ker f$ er normal, så det gjenstår bare å sjekke at $f(g)f(g') = f(gg')$ for et vilkårlig valg av representanter g, g', men dette følger av at f er en morfi. □

Oppgaver

1. (a) Hvilke restklasser har $3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$ i $\mathbb{Z}$? Hva med $5\mathbb{Z} \subset \mathbb{Z}$?
   (b) For et generelt heltall $n \in \mathbb{Z}$, vis at $n\mathbb{Z} \subset \mathbb{Z}$ har n restklasser, det vil si $\#(\mathbb{Z}/n\mathbb{Z}) = n$.
2. Bevis Korollar 3.4
3. Vi skal undersøke mengden av restklasser til $\mathbb{Z} \subset \mathbb{R}$.
   (a) Vi har sett at to restklasser $a+\mathbb{Z} = b+\mathbb{Z}$ hvis og bare hvis $(a-b) \in \mathbb{Z}$. Bruk dette til å konstruere en bijeksjon $[0,1) \to \mathbb{R}/\mathbb{Z}$.
   (b) Vi har at $a + \mathbb{Z} = \mathbb{Z} + a$, så $\mathbb{Z} \subset \mathbb{R}$ er en normal undergruppe og $\mathbb{R}/\mathbb{Z}$ danner en gruppe. Vis at avbildningen
   $$\exp\colon \begin{cases} (\mathbb{R}, +) \mapsto (S^1, \times) \\ x \mapsto e^{2\pi i x} \end{cases}$$
   er en gruppe-morfi (merk at vi går fra addisjon til multiplikasjon) og at den danner en bijeksjon $[0,1) \to S^1$. Her er S^1 enhetsirkelen
   $$S^1 = \{z \mid |z| = 1\} \subset \mathbb{C}.$$
   Dette viser at vi har en isomorfi $\mathbb{R}/\mathbb{Z} \to S^1$.
   (c) Kan du forestille deg hva som skjer om vi tar $\mathbb{R}/\mathbb{Q}$?

4 Sykliske grupper

Definisjon 4.1. En gruppe $(G, *)$ er *abelsk* om for alle $g, h \in G$ har vi $g*h = h*g$. En operator som tilfredsstiller dette kalles *kommutativ*.

Eksempel 4.2. Alle eksemplene er med addisjon som gruppeoperator ovenfor er abelske. Generelt, om vi benevner en operator med symbolet "+" så er operatoren kommutativ.

Eksempel 4.3. Gruppen av invertible (2×2)-matriser under multiplikasjon $\mathrm{GL}_2(\mathbb{R})$ er ikke abelsk, siden til eksempel

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$$

mens

$$\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}.$$

Definisjon 4.4. La $g_1, \ldots, g_n \subset G$ være et endelig antall elementer i G. Vi definerer *gruppen generert av* $g_1, \ldots, g_n$

$$H = \langle g_1, \ldots, g_n\rangle \subset G$$

som den minste undergruppen av G som inneholder alle elementene $g_1, \ldots, g_n$.

Om det finnes en $g \in G$ slik at $G = \langle g\rangle$ sier vi at G er en *syklisk* gruppe.

Eksempel 4.5. Heltallene $\mathbb{Z}$ er en syklisk gruppe generert av 1. Alle undergruppene $n\mathbb{Z} \subset \mathbb{Z}$ er også sykliske generert av n.

Lemma 4.6. *La G være en gruppe. Da er G syklisk hvis og bare hvis det finnes en surjektiv morfi $\mathbb{Z} \to G$.*

Bevis. Anta det finnes en surjektiv avbildning $f\colon \mathbb{Z} \to G$. Da har vi at for alle $g \in G$ så finnes en $n \in \mathbb{Z}$ slik at $f(n) = f(1)^n = g$, så $G = \langle f(1)\rangle$.

Anta at $G = \langle g\rangle$ for en $g \in G$. Vi konstruerer en avbildning $f\colon \mathbb{Z} \to G$ gitt ved $n \mapsto g^n$. Åpenbart har vi at $\operatorname{im} f \subset G$, men $\operatorname{im} f$ er en undergruppe av G og $g \in \operatorname{im} f$, så $\langle g\rangle \subset \operatorname{im} f$ siden $\langle g\rangle$ er den minste undergruppen som inneholder g. Men $\langle g\rangle = G$, så dermed har vi at $\langle g\rangle = \operatorname{im} f = G$, så f er surjektiv. □

Korollar 4.7. *Undergruppene $k\mathbb{Z} = \langle k\rangle \subset \mathbb{Z}$ er de eneste undergruppene $\mathbb{Z}$ har.*

Bevis. La $k_1, \ldots, k_n$ være en endelig samling elementer i $\mathbb{Z}$. Da finnes det heltall $c_1, \ldots, c_n$ slik at $c_1k_1 + \cdots + c_nk_n = k$ hvor $k = \gcd(k_1, \ldots, k_n)$ er største felles nevner for $k_1, \ldots, k_n$. Dette følger fra Euclids algoritme. Da vil $\langle k_1, \ldots, k_n\rangle = \langle k\rangle$.

Et tilsvarende argument holder for uendelige samlinger $\{k_i\}$ ved å velge en endelig delmengde. □

Korollar 4.8. *La G være en syklisk gruppe. Da finnes en isomorfi $\mathbb{Z}/n\mathbb{Z} \to G$ hvor $n = \#G$.*

Bevis. Siden G er syklisk finnes en surjektiv morfi $f\colon \mathbb{Z} \to G$ ved Lemma 4.6. Vi har at $\ker f \subset \mathbb{Z}$ er en undergruppe, så det finnes en $n \in \mathbb{Z}$ slik at $\ker f = n\mathbb{Z}$ ved Korollar 4.7, så $\bar{f}\colon \mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} \to G$ er en isomorfi. Merk at en isomorfi er en bijeksjon, så $\#G = \#\mathbb{Z}/n\mathbb{Z} = n$. □

Bemerkning 4.9. De endelige gruppen $\mathbb{Z}/n\mathbb{Z}$ er en slags "modell" for alle sykliske grupper av n elementer, så vi kommer til å bruke den mye og skriver ofte bare

$$\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}.$$

Eksempel 4.10. Enhetrøttene μ_n er en syklisk gruppe, så vi har en isomorfi $\mathbb{Z}/n \to \mu_n$.

Teorem 4.11 (Kinesisk restteorem)**.** *La $n \in \mathbb{Z}$ og la $k_1, \dots, k_r \in \mathbb{Z}$ være en rekke heltall. Vi har naturlige morfier $f_i\colon \mathbb{Z} \to \mathbb{Z}/k_i$ for alle $i = 1, \dots, r$. La n_i være restklassen til n i $\mathbb{Z}/k_i$. Da har vi at $f_i(n') = n_i$ for alle $i = 1, \dots, r$ hvis og bare hvis $n - n' \in k\mathbb{Z}$ hvor*

$$k = \operatorname{lcm}(k_1, \dots, k_r) = \frac{k_1 \dots k_n}{\gcd(k_1, \dots, k_n)}.$$

Bevis. Siden $\operatorname{lcm}(k_1, \dots, k_r) = \operatorname{lcm}(k_1, \operatorname{lcm}(k_2, \dots, k_r))$ viser vi resultatet ved induksjon på r.

Om $r = 1$ er $\operatorname{lcm}(k_1) = k_1 = k$, så resultatet er umiddelbart.

Før vi går videre observerer vi at vi kan omformulere teoremet ved hjelp av diagrammet

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/\operatorname{lcm}(k_1, \dots, k_r) \\ & \searrow^{f_1 \times \dots \times f_r} & \downarrow{\scriptstyle \bar{f}_1 \times \dots \times \bar{f}_r} \\ & & (\mathbb{Z}/k_1) \times \dots \times (\mathbb{Z}/k_r). \end{array}$$

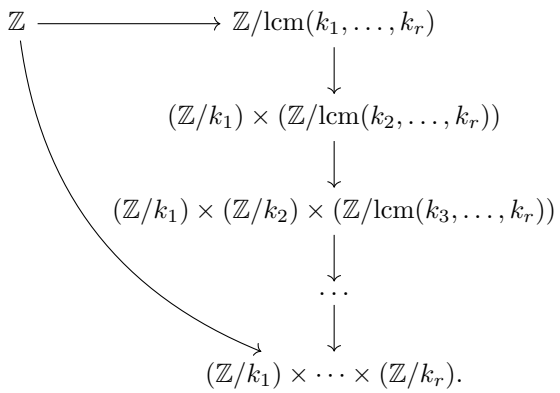
Teoremet sier at om vi har et element $(n_1, \dots, n_r) \in (\mathbb{Z}/k_1) \times \dots \times (\mathbb{Z}/k_r)$ i bildet av $f_1 \times \dots \times f_r$) så finnes en unik restklasse $n + (k\mathbb{Z})$ slik at

$$(\bar{f}_1 \times \dots \times \bar{f}_r)(n + (k\mathbb{Z})) = (n_1, \dots, n_r),$$

altså har vi en isomorfi

$$\mathbb{Z}/k \xrightarrow{\sim} \operatorname{im}(f_1 \times \dots \times f_2).$$

Tanken er at vi filtrerer dette bildet



Anta at $f_i(n') = n_i$ for alle $i = 2, \ldots, r$ hvis og bare hvis $n' - n \in k'\mathbb{Z}$ hvor $k' = \mathrm{lcm}(k_2, \ldots, k_r)$. Anta også at $f_1(n') = n_1$. Da har vi at

$$n = n_1 + k_1 m_1 = n' + k' m_2$$

og $n' = n_1 + k_1 m_1'$, så

$$n - n' = k_1(m_1 - m_1') = k' m_2.$$

Merk at $k_1 | n - n'$, og $k' | n - n'$, så $\mathrm{lcm}(k_1, k') = k | n - n'$, så $n - n' \in k\mathbb{Z}$. □

Oppgaver

1. La A være en abelsk gruppe og $H \subset A$ en undergruppe.

   (a) Vis at H er abelsk.

   (b) Vis at H er en normal undergruppe.

2. La n, m være heltall. Vi har sett at om $m \mid n$ så finnes en injeksjon $\mathbb{Z}/m \hookrightarrow \mathbb{Z}/n$ som identifiserer $\mathbb{Z}/m$ som en undergruppe av $\mathbb{Z}/n$.

   (a) Vis at dersom $\gcd(n, m) = 1$ så er den eneste morfien $\mathbb{Z}/m \to \mathbb{Z}/n$ den som sender hele $\mathbb{Z}/m$ på 0.

   (b) Vis at dersom $\gcd(n, m) = d$ så kan alle morfier $f\colon \mathbb{Z}/m \to \mathbb{Z}/n$ faktoriseres som
   $$\mathbb{Z}/m \xrightarrow{g} \mathbb{Z}/d \xhookrightarrow{i} \mathbb{Z}/n,$$
   det vil si f kan skrives som $f = i \circ g$.

   La G være en gruppe. En *ekte* undergruppe $H \subset G$ er en undergruppe slik at $H \neq \{e_H\}$ og $H \neq G$.

   (c) Vis at $\mathbb{Z}/p$ ikke har noen ekte undergrupper. En gruppe uten ekte undergrupper kalles en *simpel* gruppe.

Ta for deg en endelig syklisk gruppe $\mathbb{Z}/n\mathbb{Z}$. Multiplikasjon gir oss en avbildning $\mu\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ gitt ved $(a,b)\mapsto ab$. Om vi tar a',b' slik at $a'-a, b'-b\in n\mathbb{Z}$, det vil si at det finnes $k,l\in\mathbb{Z}$ slik at $a'=a+kn$ og $b'=b+lb$, så har vi at

$$\begin{aligned}\mu(a',b') &= \mu(a+kn, b+ln)\\ &= (a+kn)(b+ln)\\ &= ab+(al+bk+kln)n\\ &= \mu(a,b)+(al+bk+kln)n,\end{aligned}$$

så $\mu(a',b')-\mu(a,b)\in\mathbb{Z}$. Det følger at vi kan lage en morfi $\hat{\mu}$ som passer i diagrammet

$$\begin{array}{ccc}\mathbb{Z}\times\mathbb{Z} & \xrightarrow{\quad\mu\quad} & \mathbb{Z}\\ \downarrow & & \downarrow\\ (\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}) & \xrightarrow{\hat{\mu}} & \mathbb{Z},\end{array}$$

altså kan vi definere multiplikasjon på $\mathbb{Z}/n\mathbb{Z}$ også.

3. Vis at om $\gcd(a,n)=d$ så finnes det en b slik at $\bar{\mu}(a,b)=d\in\mathbb{Z}/n\mathbb{Z}$. Spesielt om $n=p$ er et primtall så finnes det for alle

   $$a\in(\mathbb{Z}/p\mathbb{Z})\setminus\{0\}=(\mathbb{Z}/n\mathbb{Z})^\times$$

   et element $b\neq 0$ slik at $\overline{\mu}(a,b)=1$, det vil si at multiplikasjon $\bar{\mu}$ på $(\mathbb{Z}/p\mathbb{Z})^\times$ har inverselementer, så $((\mathbb{Z}/p\mathbb{Z})^\times,\bar{\mu})$ danner en gruppe.

4. Vi benevner $\bar{\mu}$ ovenfor som $\times$ og skriver $\bar{\mu}(a,b)$ bare som ab. Vis at $((\mathbb{Z}/p\mathbb{Z})^\times,\times)$ er syklisk, så

   $$((\mathbb{Z}/p\mathbb{Z})^\times,\times)\cong(\mathbb{Z}/(p-1)\mathbb{Z},+).$$

Bemerkning 4.12. Denne isomorfien er viktig for flere kryptografiske algoritmer, slik som Diffie-Hellman, for selv om det ser ut som vi jobber over gruppen $\mathbb{Z}/p\mathbb{Z}$, så jobber vi over den multiplikativt. Det handler i prinsipp om at vi jobber over $(\mathbb{Z}/p\mathbb{Z})^\times$ slik at vi har en komplisert måte å jobbe med $\mathbb{Z}/(p-1)\mathbb{Z}$.

Selv om n ikke er et primtall kan vi definere en gruppe under multiplikasjon som en del av $\mathbb{Z}/n\mathbb{Z}$. La

$$(\mathbb{Z}/n\mathbb{Z})^\times=\{a\mid\gcd(a,n)=1\}.$$

Merk at denne definisjonen sammenfaller med vår tidligere definisjon når n er et primtall.

5. La $n=p_1\dots p_r$ være en faktorisering av n slik at p_i er primtall for alle $i=1,\dots,r$. Vis at $\#(\mathbb{Z}/n\mathbb{Z})^\times=(p_1-1)\dots(p_r-1)$.

5 Endelige abelske grupper

5.1 Fermats lille teorem

Lemma 5.1. *La $x, y \in \mathbb{Z}$ og $n \geq 1$ være heltall. Da har vi formelen*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Av og til tar vi dette som definisjonen av *binomialkoeffisientene* $\binom{n}{m}$, men om vi heller bruker definisjonen fra Pascals trekant $\binom{n}{0} = \binom{n}{n} = 1$ for alle $n \in \mathbb{N}$ og $\binom{n}{m-1} + \binom{n}{m} = \binom{n+1}{m}$ for alle n, m kan vi vise Lemma 5.1 ved induksjon som følger.

Bevis. Tilfellet $n = 1$ er enkelt siden $(x+y)^1 = x + y$ og $\binom{1}{0} = \binom{1}{1} = 1$.

Anta $(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}$. Vi har

$$\begin{aligned}
(x+y)^{k+1} &= (x+y)(x+y)^k \\
&= (x+y) \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i} \\
&= \sum_{i=0}^{k} \binom{k}{i} x^{i+1} y^{k-i} + \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i+1} \\
&= \sum_{i=1}^{k+1} \binom{k}{i-1} x^i y^{(k+1)-i} + \sum_{i=0}^{k} \binom{k}{i} x^i y^{(k+1)-i} \\
&= \sum_{i=0}^{k+1} \binom{k+1}{i} x^i y^{(k+1)-i}
\end{aligned}$$

□

Korollar 5.2 (Fermats lille teorem)**.** *La p være et primtall. Da har vi at*

$$a^p \cong a \mod p$$

for alle $a \in \mathbb{Z}$.

Bevis. Vi definerer en avbildning $\pi_p \colon \mathbb{Z}/p \to \mathbb{Z}/p$ ved $a \mapsto a^p$. La $a, b \in \mathbb{Z}$. Vi ser at

$$\begin{aligned}
\pi_p(a+b) &= (a+b)^p \\
&= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \\
&= a^p + b^p \\
&= \pi_p(a) + \pi_p(b)
\end{aligned}$$

siden $p | \binom{p}{i}$ for $i \neq 0, p$, så π_p er en morfi. Vi ser også at $\pi_p(1) = 1^p = 1$, og det er bare èn morfi $\mathbb{Z}/p \to \mathbb{Z}/p$ som tilfredsstiller dette, nemlig identiteten $\mathrm{id}_{\mathbb{Z}/p}$, så $\pi_p = \mathrm{id}_{\mathbb{Z}/p}$. □

5.2 Klassifisering av endelige abelske grupper

Vi har allerede sett at alle endelige sykliske grupper kan skrives på formen $\mathbb{Z}/n$ for et heltall n. Vi ønsker å generalisere dette til alle endelige abelske grupper. Vi har sett at det finnes endelige abelske grupper som ikke er sykliske slik som $\mathbb{Z}/2 \times \mathbb{Z}/2$ og genereres av minst to elementer. Andre grupper som vi genererer av to elementer kan vise seg å være sykliske derimot, slik som $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6$. Som en konsekvens av Teorem 4.11 kan vi vise

Korollar 5.3. *La $p_1, \dots, p_n$ være primtall slik at $p_i \neq p_j$ for alle $i \neq j$, og la $r_1, \dots, r_n$ være heltall. Da har vi en isomorfi*

$$\mathbb{Z}/(p_1^{r_1} \dots p_n^{r_n}) \cong \mathbb{Z}/p_1^{r_1} \times \dots \times \mathbb{Z}/p_n^{r_n}.$$

Vi ønsker noe i denne stilen som tar hånd om alle endelige abelske grupper.

Lemma 5.4. *La A være en endelig abelsk gruppe og la $\langle a \rangle$ være en syklisk undergruppe av maksimal orden. La $\langle a' \rangle$ være en annen syklisk undergruppe. Da $\#\langle a' \rangle | \#\langle a \rangle$.*

Bevis. La l være det minste positive heltallet slik at $\langle a \rangle \cap \langle a' \rangle = \langle la' \rangle$. La $m = \#\langle a \rangle$, $n = \#\langle a' \rangle$, og $d = \gcd(m, l)$. Merk at $\frac{n}{l} = \#\langle la' \rangle$. Da har vi $\gcd(m, l/d) = 1$, men $\#\langle \frac{nd}{l} a' \rangle = l/d$, så

$$a \in \langle \frac{l}{d} a \rangle \subset \langle a + \frac{nd}{l} a' \rangle,$$

men $\langle a \rangle$ er maksimal, så $l = d$ og $\frac{nd}{l} a' = na' = 0$. Det følger også at $l | m$, så $n = l\frac{n}{l} | m$. □

Korollar 5.5. *Let $a, a' \subset A$ slik at $\langle a \rangle$ er en maksimal syklisk undergruppe. Da finnes a'' slik at*

$$\langle a, a' \rangle = \langle a, a'' \rangle,$$

men $\langle a \rangle \cap \langle a'' \rangle = 0$.

Bevis. La l være det minste positive heltallet slik at $\langle a \rangle \cap \langle a' \rangle = \langle la' \rangle$. La k være det minste helltallet slik at $ka = la'$. La $n = \#\langle a \rangle$ og $m = \#\langle a' \rangle$, så $m | n$ siden $\langle a \rangle$ er maksimal. Vi har også at $\frac{n}{l} la' = \frac{n}{l} ka = 0$, så $m | \frac{n}{l} k$. Siden $n | m$ følger det at $\frac{m}{n} | \frac{k}{l}$, så $l | k$. La $a'' = a' - \frac{m}{l} a$. Vi har $a' \in \langle a, a'' \rangle$.

La s være det minste positive heltallet slik at $sa'' \in \langle a \rangle$, så $sa' - s\frac{m}{l} a \in \langle a \rangle$, men da må $sa' \in \langle a \rangle$, så $s = l$ og $sa'' = 0$. Det følger at $\langle a \rangle \cap \langle a'' \rangle = 0$. □

Lemma 5.6. *La $A = \langle a_1, \dots, a_k \rangle$ være en abelsk gruppe. Da har vi en surjektiv morfi*

$$\phi \colon \mathbb{Z}^k \to A$$

gitt ved $e_i \mapsto a_i$ for alle $i = 1, \dots, k$.

Bevis. Merk at ϕ er en morfi og $a_i \in \operatorname{im} \phi$, så $\langle a_1, \dots, a_k \rangle \subset \operatorname{im} \phi \subset A$, så ϕ er surjektiv. □

Korollar 5.7. *La A være en endelig abelsk gruppe og $a \in A$ et element slik at $\langle a \rangle$ er en maksimal syklisk undergruppe. Da har inklusjonen $\iota\colon \langle a \rangle \to A$ en venstre invers $\rho\colon A \to \langle a \rangle$, det vil si $\rho \circ \iota = \mathrm{id}$. Det følger at vi har en isomorfi*

$$A \to \langle a \rangle \times (A/\langle a \rangle).$$

Bevis. La $\langle a_1, \ldots, a_k$ være et valg av generatorer for A. For hver $i = 1, \ldots, k$ velg en a_i' slik at $\langle a \rangle \cap \langle a_i' \rangle = 0$ og $a_i \in \langle a, a_i' \rangle$. Da har vi at $\langle a, a_1', \ldots, a_k' \rangle = A$, men $\langle a \rangle \cap \langle a_1', \ldots, a_k' \rangle = 0$. Vi påstår sammensetningen

$$\langle a \rangle \overset{\iota}{\hookrightarrow} A \overset{\phi}{\to} A/\langle a_1', \ldots, a_k' \rangle$$

er en isomorfi.

For injektivitet ser vi at om $\phi(na) = \phi(ma)$, så må $\phi((n-m)a) = 0$, så $na = ma$ siden $\ker \phi = \langle a_1', \ldots, a_k' \rangle$.

For surjektivitet la $b \in A/\langle a_1, \ldots, a_k \rangle$. Da finnes en $a' \in A$ slik at $b = \phi(a')$. Ved Lemma 5.6 har vi at $a' = c_0 a + c_1 a_1 + \cdots + c_k a_k$, så

$$b = \phi(a') = c_0 \phi(a) \in \mathrm{im}(\phi \circ \iota).$$

La $\rho = (\phi \circ \iota)^{-1} \circ \phi$, så $\rho \circ \iota = \mathrm{id}$. □

Teorem 5.8 (Basis-teoremet for endelige abelske grupper)**.** *Anta at A er en endelig abelsk gruppe. Da finnes en sekvens tall $d_1, d_2, \ldots, d_m$ slik at $d_{i+1} | d_i$ for alle $i = 1, \ldots, m-1$, og en isomorfi*

$$A \to \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_m.$$

Bevis. Beviset følger ved en algoritme. La $A_1 = A$ og $\psi_1 = \mathrm{id}_A$. For alle $i \leq 1$ la a_i være et element slik at $\langle a_i \rangle$ er en maksimal syklisk undergruppe av A_i. La $d_i = \#\langle a_i \rangle$, så vi har en isomorfi $\mathbb{Z}/d_i \to \langle a_i \rangle$ gitt ved $1 \mapsto a_i$. La $A_{i+1} = A_i/\langle a_i \rangle$ og la $\phi_i\colon A_i \to \mathbb{Z}/d_i \times A_{i+1}$ være isomorfien som følger av Korollar 5.7, og la ψ_{i+1} være komposisjonen

$$A \xrightarrow{\psi_i} \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_{i-1} \times A_i \xrightarrow{\mathrm{id} \times \phi_i} \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_i \times A_{i+1}.$$

Vi ser at $\#A_{i+1} < \#A_i$, så for en endelig N har vi $A_N = 0$ så ψ_N er isomorfien vi er ute etter. Merk at ved hvert steg kan vi identifisere $\phi_i^{-1}(A_{i+1})$ med en undergruppe av A_i, så

$$d_{i+1} = \#\langle a_{i+1} \rangle = \#\langle \phi_i^{-1}(a_{i+1}) \rangle | \#\langle a_i \rangle = d_i$$

ved Lemma 5.4. □

Korollar 5.9 (Klassiske basis-teoremet for endelige abelske grupper)**.** *La A være en endelig abelsk gruppe. Da finnes det primtall $p_1, \ldots, p_m$, eksponenter $r_1, \ldots, r_m$, og en isomorfi*

$$\mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_m^{r_m} \to A.$$

Bevis. Dette følger direkte fra Teorem 5.8 og Korollar 5.3. □

Oppgaver

1. La A være en abelsk gruppe. La
$$A_{\text{tors}} = \{a \in A \mid \text{det finnes } n \in \mathbb{Z} \text{ slik at } na = 0.\}$$
   (a) Vis at A_{tors} er en undergruppe av A.
   (b) Vis at det finnes en venstre invers til inklusjonen $A_{\text{tors}} \hookrightarrow A$, så vi har en isomorfi
   $$\phi\colon A \to A_{\text{tors}} \times (A/A_{\text{tors}}).$$
   (c) La $A_{\text{free}} = \phi^{-1}(0 \times (A/A_{\text{tors}})$. Anta det finnes et endelig antall elementer $a_1, \ldots, a_k$ slik at $\langle a_1, \ldots, a_k\rangle = A$. Vis at $A_{\text{free}} \cong \mathbb{Z}^n$ for et heltall n, og vis at A_{tors} er endelig.

Vi har flere ganger brukt at om vi har en undergruppe $H \hookrightarrow G$ og inklusjonen har en venstre invers $G \to H$ så har vi en isomorfi $H \times (G/H) \cong G$. Dette resultatet passer bedre i en annen kontekst.

Definisjon 5.10. La G, G', G'' være tre grupper si vi har morfier
$$G' \xrightarrow{f} G \xrightarrow{g} G''.$$
Vi sier denne sekvensen av morfier er *eksakt* i G om $\operatorname{im} f = \ker g$.

For en lengre (mulig uendelig) sekvens av morfier sier vi den er *eksakt* om den er eksakt i hvert ledd.

2. La $f\colon G \to H$ være en morfi.
   (a) Vis at f er injektiv hvis og bare hvis
   $$0 \to G \xrightarrow{f} H$$
   er eksakt.
   (b) Vis at f er surjektiv hvis og bare hvis
   $$G \xrightarrow{f} H \to 0$$
   er eksakt.

3. En *kort eksakt sekvens* er en eksakt sekvens på formen
$$0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0.$$
   En kort eksakt sekvens er *splitt* om det finnes en morfi $h\colon G \to G'$ slik at $h \circ f = \mathrm{id}_{G'}$ og morfien
   $$h \times g\colon G \to G' \times G''$$
   er en isomorfi. Vis at følgende er ekvivalente
   - Det finnes en morfi $h\colon G \to G'$ slik at $h \circ f = \mathrm{id}_{G'}$.
   - Det finnes en morfi $i\colon G'' \to G$ slik at $g \circ i = \mathrm{id}_{G''}$.
   - Den korte eksakte sekvensen er splitt.

A Diffie-Hellman

Diffie-Hellman er en metode for nøkkelutveksling, det vil si at to parter Alice og Bob klarer å komme frem til en felles hemmelig nøkkel uten at en tredje part kan enkelt beregne hva nøkkelen er.

Algoritmen, etter [DH76], er som følger:

1. Alice og Bob er enige om et primtall p og et tall $2 \leq g \leq p-2$.
2. Alice velger et tilfeldig tall $2 \leq a \leq p-2$ og beregner $k_a = g^a \mod p$. Hun sender denne nøkkelen k_a til Bob.
3. Bob velger et tilfeldig tall $2 \leq b \leq p-2$, beregner $k_b = g^b \mod p$ og sender nøkkelen k_b til Alice.
4. Alice beregner $k_{ab} = k_b^a$ og Bob beregner $k'_{ab} = k_a^b$. Siden $k_b^a = g^{ab} = k_a^b$ har vi at $k_{ab} = k'_{ab}$. Dette er Alice og Bob sin felles hemmelige nøkkel.

Teorien som gjør at dette fungerer er bare at vi jobber i $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$. En angriper er interessert i å vite k_{ab} gitt den offentlige informasjonen k_a, k_b, g og p. Tallene p og g er ofte forhåndsbestemt som en del av algoritmen, så vi kan tenke oss at en angriper er godt forberedt med dette i tankene. Spesielt vil en angriper kunne vite primtallsfaktoriseringen av $p-1$.

A.1 Diskrete logaritmer

Den tenkte måten å angripe algoritmen er å først finne enten a eller b for å beregne k_{ab}. Generelt er problemet å finne et tall n slik at $g^n \equiv m \mod p$ gitt g, m og p kjent som diskret logaritme problemet, ettersom vi tenker oss at dette definerer en logaritme avbildning $\log_g \colon (\mathbb{Z}/p)^\times \to \mathbb{Z}/(p-1)$ slik at $\log_g(m) = n$. Merk at denne sjeldent gir de samme verdiene som den vanlige reelle logaritmen $\log \colon \mathbb{R}^\times \to \mathbb{R}$. Merk også at g må være en generator for $(\mathbb{Z}/p)^\times$ for at $\log_g(m)$ skal være definert for alle $m \in (\mathbb{Z}/p)^\times$.

Anta g er en generator for $(\mathbb{Z}/p)^\times$. Da har vi en isomorfi $\phi \colon \mathbb{Z}/(p-1) \to (\mathbb{Z}/p)^\times$ gitt ved $n \mapsto g^n$. Denne har da en invers $\phi^{-1} \colon (\mathbb{Z}/p)^\times \to \mathbb{Z}/(p-1)$, som for g^n gir tilbake n. Om vi kan beregne ϕ^{-1} har vi altså løst diskret logaritme problemet, men merk at morfien ϕ^{-1} er akkurat avbildningen $\log_g$, så det å kunne beskrive den multiplikative gruppen $(\mathbb{Z}/p)^\times$ som en additiv gruppe $\mathbb{Z}/(p-1)$ er ekvivalent til å løse diskret logaritme problemet for en gitt base.

A.2 Kinesisk rest

Selv om vi ikke kan beregne isomorfien $\log_g \colon (\mathbb{Z}/p)^\times \to \mathbb{Z}/(p-1)$, så kan vi utnytte at det finnes en slik isomorfi. La $q | p-1$ være et primtall, og la $d = (p-1)/q$. Da kan vi beregne $k_a^d = g^{ad}$. Merk at $(k_a^d)^q = g^{a(p-1)} = 1$, så k_a^d kan bare ha én av q mulige verdier avhengig av verdien til $a' = a \mod q$. Altså kan vi finne verdien av a' ved å løse diskret logaritme problemet $a' = \log_{g^d}(k_a^d)$ i $\langle g^d \rangle \subset (\mathbb{Z}/p)^\times$.

Det samme holder for høyere potenser av et primtall, så om vi har en primtallsfaktorisering $q_1^{r_1} \dots q_k^{r_k} = p - 1$ kan vi ved Teorem 4.11 finne a om vi klarer å løse diskret logaritme problemet for alle delgruppene tilsvarende primtallsfaktorene i $p - 1$.

Det er derfor viktig for sikkerheten av Diffie-Hellman at $p - 1$ også har store primtallsfaktorer.

A.3 Pollard rho

En standard metode [Pol78] for å løse diskret logaritme problemet baserer seg på at vi kan dele opp søket etter verdien for a. Vi vet grovt sett at $0 \leq a \leq p-1$, så la $q = \lceil \sqrt{p-1} \rceil$, det vil si q er det minste heltallet større enn $\sqrt{p-1}$. Da finnes heltall $0 \leq m < q$ og $0 \leq n \leq \lfloor (p-1)/q \rfloor \leq q$ slik at $a = nq + m$, så $g^{nq+m} = k_a$. Om vi nå lager en tabell over verdiene for $k_a g^{-m}$ for alle $0 \leq m < q$ kan vi gå igjennom verdiene g^{nq} for alle $0 \leq n \leq q$ og se om verdien dukker opp i tabellen. Når vi får et treff har vi verdier n og m slik at, $g^{nq} = k_a g^{-m}$, altså har vi at $g^{nq+m} = k_a$, så $a = nq + m$.

Fordelen med denne metoden er at vi trenger bare å teste med $q + (q+1) \approx 2\sqrt{p-1}$ tall for n og m sammenlagt, isteden for å teste alle $p - 1$ mulige verdier for a. Ulempen er at vi trenger å holde styr på en tabell med rundt q verdier, så når p blir dette ofte for mye data å ha kontroll på.

Pollards rho-metode [Pol78] deler inn søket på en annen måte. Her er tanken at vi går ser på verdien av $g^n k_a^m$ for mange verdier av n og m helt til vi finner to par (n, m) og (n', m') slik at

$$g^n k_a^m = g^{n'} k_a^{m'}.$$

Dette kan vi skrive om som

$$g^{n-n'} = k_a^{m'-m}.$$

Isåfall kan vi bruke Euklids algoritme til å finne heltall l, k slik at $l(p-1) + k(m'-m) = d$ hvor $d = \gcd(p-1, m'-m)$. Da har vi at

$$\begin{aligned} g^{(n-n')k} &= k_a^{(m'-m)k} \\ &= k_a^d k_a^{-l(p-1)} \\ &= k_a^d \end{aligned}$$

Siden vi antar det finnes en løsning $g^a = k_a^d$ må vi ha at $d | (n-n')k$, så vi kan beregne $a' = (n-n')k/d$. Det er ikke gitt at $a' = a$, siden det finnes flere mulige d-te røtter av g. La $\theta = g^{(p-1)/d}$ benevne den primitive d-te roten til g i $(\mathbb{Z}/p)^\times$. Da finnes én $0 \leq i < d$ slik at $g^{a'} \theta^i = k_a$, så $a' + i\frac{p-1}{d} = a$.

Denne metoden har to steg som potensielt dominerer kompleksiteten. Det første er å finne verdier (n, m) og (n', m') slik at $g^n k_a^m = g^{n'} k_a^{m'}$. Det andre er når vi tester alle mulige verdier for i for å finne riktig rot av g.

For sistnevnte er vi reddet av at sjansen for at d skal ha en stor primtallsfaktor er omvendt proporsjonal med størrelsen på faktoren, så d har mest sannsynlig små faktorer, som vi kan løse ved å bruke Teorem 4.11.

For det førstnevnte steget presenterer Pollard en avbildning (ikke en morfi) $\rho\colon (\mathbb{Z}/p)^\times (\mathbb{Z}/p)^\times$ som er laget på en slik måte at gitt at gitt eksponentene n, m for $g^n k_a^m$ så kan vi beregne eksponenter n', m' slik at $g^{n'} k_a^{m'} = \rho(g^n k_a^m)$.

Tanken her er at ρ oppfører seg som en tilfeldig avbildning, og for en ekte tilfeldig avbildning $\eta\colon (\mathbb{Z}/p)^\times \to (\mathbb{Z}/p)^\times$ forventer vi at vi får $\eta^n(1) = \eta^{2n}(1)$ for en n i størrelsesorden $\sqrt{p}$. Verdien n kalles *epoken* til η.

Å finne epoken til ρ kan vi gjøre uten å lagre annen informasjon enn verdien til $\rho^k(1)$ og $\rho^{2k}(1)$ for en gitt k ved å iterere gjennom alle $k = 1, \ldots, n$. Dette kalles Floyds algoritme.

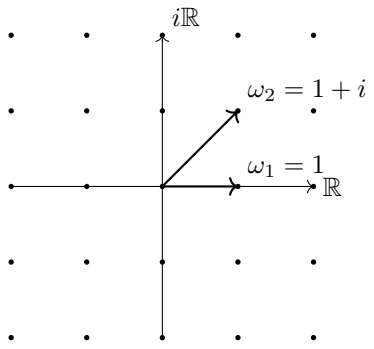
B Elliptiske kurver

Elliptiske kurver er en familie kurver som også har egenskapen at de danner grupper under en gitt gruppe-operator. [Sil09]

B.1 Komplekse elliptiske kurver

Definisjon B.1. En undergruppe $\Lambda \subset \mathbb{C}$ er et *gitter* dersom det kan skrives som bildet av en morfi $\phi\colon \mathbb{Z}^2 \to \mathbb{C}$. Det er av *full rang* om ϕ er injektiv og $\phi(e_1)/\phi(e_2) \notin \mathbb{R}$.

Et gitter er unikt definert av to punkter $\omega_1, \omega_2 \in \mathbb{C}$, ved å la ϕ være morfien $e_1 \mapsto \omega_1$, $e_2 \mapsto \omega_2$, så gitteret $\Lambda = \langle \omega_1, \omega_2 \rangle$. Men flere ulike valg av ω_1, ω_2 gir samme elliptiske kurve. Til eksempel er $\langle 1, i \rangle = \langle 1, 1+i \rangle$.



Figur 3: Gitteret $\Lambda = \langle 1, 1+i \rangle$.

På samme måte som vi kan konstruere enhetsirkelen som restgruppen

$$0 \to \langle 1 \rangle \to \mathbb{R}\mathbb{S}^1 \to 1$$

så kan vi se på restgruppen $\mathbb{C}/\Lambda$ som en torus

$$0 \to \Lambda \to \mathbb{C} \to S^1 \times S^1 \to 1.$$

En torus er et eksempel på en genus 1 flate, fordi den har ett "hull", men når vi konstruerer det som et kvotient av $\mathbb{C}$ får den noe struktur i likhet med strukturen på $\mathbb{C}$ som skiller den fra $\mathbb{R}^2$. Spesielt bør vi tenke på $\mathbb{C}/\Lambda$ som noe av samme "komplekse" dimensjon som $\mathbb{C}$, altså 1. Dermed ser vi på $\mathbb{C}/\Lambda$ som en kurve av genus 1, heller enn som en flate.

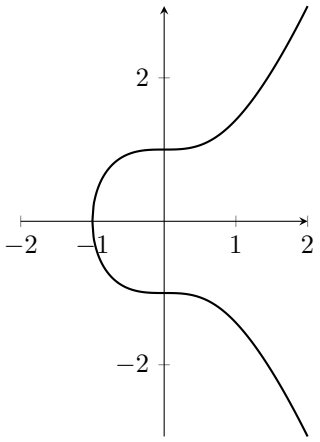
B.2 Reelle elliptiske kurver

En kompleks elliptisk kurve kan også avbildes inn i det komplekse planet, på en slik måte at vi kan gjenkjenne gruppestrukturen til kurven. Spesielt kan alle kurvene skrives som løsningsmengden til en likning på formen

$$y^2 = x^3 + Ax + B \tag{B.1}$$

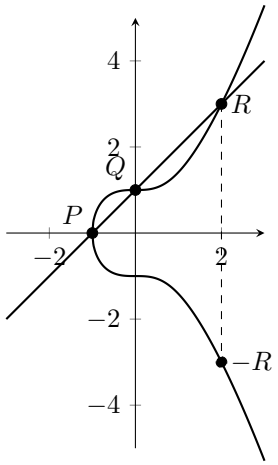
for tall $A, B \in \mathbb{C}$. Denne likningen kalles *Weierstrass likningen* [Sil09, p. 45].

Det komplekse planet er av reell dimensjon 4, så for å forstå hvordan gruppestrukturen til kurven er bevart kan vi restriktere til de løsningene av Likning (B.1) hvor $x, y \in \mathbb{R}$ og $A, B \in \mathbb{R}$. Dette gir oss reelle elliptiske kurver.



Figur 4: Løsningsmengden $\{y^2 = x^3 + 1\} \subset \mathbb{R}^2$.

La $C \subset \mathbb{R}^2$ være en elliptisk kurve, og la $P, Q \in C$ være to punkter på kurven. For å regne ut summen trekker vi en linje l mellom P og Q, eller om $P = Q$ tar vi tangenten til C i P. Ved Bezouts teorem finnes det et tredje punkt $R \in C \cap l$, med $R \neq P, Q$. Vi definerer speilingen av R om x-aksen $-R = P + Q$.



Ekvivalent sier vi at om tre punkter P, Q, R ligger på samme linje så er $P + Q + R = 0$. Merk at for at Bezout skal holde må vi i teorien regne med punkter som ligger i "uendeligheten". Dette oppstår nøyaktig når vi velger punkter P, Q som er speilingen av hverandre om x-aksen, altså når $P = -Q$. For vår

kurve finnes det bare ett punkt i uendeligheten, og dette kaller vi ∞. Merk at ∞ er identitetselementet i gruppen.

B.3 Elliptiske kurver over $\mathbb{Z}/n$

Husk at for en gruppe $\mathbb{Z}/n$ kan vi i tillegg definere multiplikasjon $\mu\colon (\mathbb{Z}/n) \times (\mathbb{Z}/n) \to \mathbb{Z}/n$. Multiplikasjon oppfører seg ganske likt som multiplikasjon på til eksempel $\mathbb{R}$. Spesielt har vi at $(a+b)c = ac + bc$.

Siden vi kan snakke om både multiplikasjon og addisjon på $\mathbb{Z}/n$, gir det også mening å definere polynomer for $\mathbb{Z}/n$, så vi kan til eksempel finne løsninger til likningen

$$y^2 = x^3 + Ax + B$$

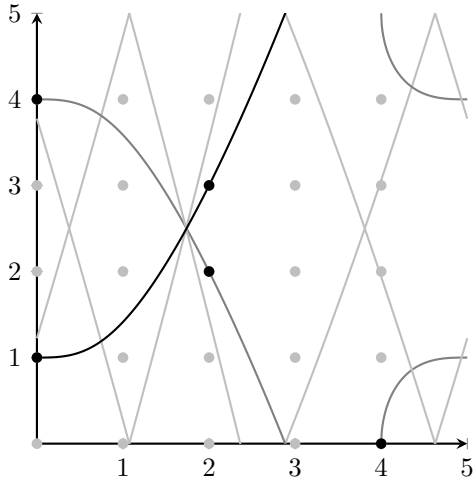
i $(\mathbb{Z}/n)^2$ om vi lar $A, B \in \mathbb{Z}/n$.

Tilsvarende kan vi definere en linje i $(\mathbb{Z}/n)^2$ som løsningsnmengden av en likning på formen

$$ax + by = c,$$

og om vi velger $n = p$ et primtall kan vi igjen forvente å finne tre punkter i skjæringen

$$\{y^2 = x^3 + Ax + B\} \cap \{ax + by = c\}.$$



Figur 5: Kurven $C = \{y^2 = x^3 + 1\} \subset \mathbb{Z}/5 \times \mathbb{Z}/5$. Merk at $\#C = 6$ om vi teller med punktet ∞.

B.4 Elliptiske kurver i kryptografi

La nå $n = p$ være et primtall (eller en potens av et primtall) og $C \subset (\mathbb{Z}/_{\mathrm{I}})^2$ være en elliptisk kurve på Weierstrass form. Siden $\#(Z/p)^2 = p^2$ er endelig må også $\#C$ være endelig, altså en endelig (abelsk) gruppe.

Et resultat kjent som Hasses teorem [Sil09, Thm. V.1.1] gir oss et grovt estimat på $\#C$. Det forteller oss at

$$|\#C - p - 1| \leq 2\sqrt{p},$$

altså forventer vi omtrent p punkter på C, så om vi kan konstruere kurver slik at $\#C$ har store primtallsfaktorer har vi en erstatning for $(\mathbb{Z}/p)^\times$ som er minst like god for beregning av til eksempel Diffie-Hellman.

C RSA

RSA (Rivest-Shamir-Adleman) [RSA78] er en metode for asymmetrisk kryptering basert på modulær aritmetikk. Algoritmen for kryptering på Alice sin side er som følger:

1. Velg to primtall p, q og la $n = pq$.
2. Velg en $e \in 3, \ldots, (p-1)(q-1) - 3$ slik at $\gcd(e, (p-1)(q-1)) = 1$.
3. Beregn d slik at $ed \equiv 1 \mod (p-1)(q-1)$.
4. La m være meldingen til Alice gitt ved et tall $m \in \mathbb{Z}/n$. Beregn chifferteksten som $M = m^e \mod n$.
5. Alice publiserer chifferteksten M sammen med tallet n. Tallet d sendes hemmelig og kan brukes til å dekryptere M.

Gitt n, M og d kan vi enkelt dekryptere meldingen ved å beregne $m' = M^d \mod n$. Siden $M^d = (m^e)^d = m^{ed} = m$ ved Korollar 5.2 og Teorem 4.11.

C.1 Eulers totient-funksjon

Men hvorfor regner vi modulo $(p-1)(q-1)$? Tallet kommer av at *Eulers totient-funksjon* ϕ. For et heltall n har vi

$$\phi(n) = \#\{m \mid 0 \leq m < n, \gcd(n, m) = 1\}.$$

Merk at dette er det samme som å si at restklassen til m i $\mathbb{Z}/n$ har en multiplikativ invers ved Euclids algoritme, så $\phi(n) = (\mathbb{Z}/n)^\times$.

For et primtall p har vi åpenbart at $\phi(p) = p - 1$ siden alle tallene mindre en tallet selv er relativt primisk til p. For et produkt av primtall $n = pq$ så er et tall m ikke relativt primisk hvis og bare hvis $p|m$ eller $q|m$, det vil si

$$m \in \{p, 2p, \ldots, (q-1)p\} \cup \{q, 2q, \ldots, (p-1)q\},$$

så da gjenstår $(pq-1)-(p-1)-(q-1) = (p-1)(q-1)$ tall, så $\phi(pq) = (p-1)(q-1)$.

Merk at dette henger sammen med at $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$ og $(\mathbb{Z}/pq)^\times \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/(q-1)$. Det følger at vi kan jobbe med en enda mindre gruppe, for for et valg av melding m jobber vi bare i den syklsiske undergruppen $\langle m \rangle \subset (\mathbb{Z}/n)^\times$. I beste fall er dette den største syklsike undergruppen. For $n = pq$ har denne orden $\lambda(n) = \operatorname{lcm}(p-1, q-1)$ ved Teorem 4.11, og størrelsen på alle andre sykler deller $\lambda(n)$, så det rekker å regne modulo $\lambda(n) \leq \phi(n)$. Funksjonen λ som gir oss størrelsen på den største syklen i $(\mathbb{Z}/n)^\times$ for en vilkårlig n kalles *Carmichaels totient-funksjon*.

C.2 Sikkerhet ved signering

Det er flere tenkelige måter å angripe RSA på. Om Alice bruker RSA som en metode for å "signere" så kan vi som angriper anta at vi vet n, m, M og d. Målet vårt da er å finne e slik at vi kan signere meldinger med Alice sin hemmelige nøkkel.

Om vi vet p og q så kan vi enkelt regne regne ut e ved hjelp av d og Euclids algoritme slik Alice gjorde for å finne d fra e i RSA. Dette er ikke noe problem siden vi kjenner bare til produktet $n = pq$. Alternativt kan vi forsøke å beregne $\phi(n)$ direkte fra n, men $\phi(n)$ er nødvendigvis også vanskelig å beregne, for om vi vet $\phi(n)$ kan vi enkelt beregne p og q.

Merk at om vi lar $n = p$, altså velger n som et primtall isteden for et produkt av primtall er det trivielt å finne $\phi(n) = n - 1$, så får sikkerheten av algoritmen er det viktig at n er et sammensatt tall. Om vi derimot lar n være et produkt av flere primtall må vi sørge for at primtallene er store nok slik at vi ikke kan enkelt finne faktorer.

Eksempel C.1. La n være et vilkårlig sammensatt tall, og anta vi kjenner til en faktor $p|n$. Da har vi at $\phi(p) = p-1|\phi(n)$. Faktisk vet vi at $p-1|\lambda(n)$. La e, d og M være slik som beregnet i RSA, og anta vi kjenner til d og M. Vi har at $de \equiv 1 \mod (p-1)$. La $e' \in (\mathbb{Z}/p)^\times$ slik at $de' \equiv 1 \mod (p-1)$, så ved Teorem 4.11 har vi at

$$e = e'(1 + k(p-1))$$

for en $k \in \{0, \ldots, \lambda(n)/(p-1)\}$ siden

$$\begin{aligned} m^{e'(1+k(p-1))d} &= \left(m^{e'd}\right)^{1+k(p-1)} \\ &\equiv m^{1+k(p-1)} && \mod (p-1) \\ &= m(m^{p-1})^k \\ &\equiv m && \mod (p-1). \end{aligned}$$

Antall k som må testes synker enda mer om $\#\langle m \rangle < \lambda(n)$.

Vi kan også finne e ved å løse "discret logaritmeproblemet" $e = \log_m(M)$ i $\mathbb{Z}/n$, se Tillegg A.1.

C.3 Sikkerhet ved kryptering

Alice kan også bruke RSA som en offentlig krypteringsalgoritme, dvs. at Alice oppgir e og holder d hemmelig slik at alle andre kan beregne en chiffertekst $M = m^e$ men bare Alice kan finne tilbake meldingen $m = M^d$. Isåfall kan vi anta at vi kjenner til e og n fra Alice, og en hemmelig melding M fra Bob. Isåfall er det interessant å bare finne $m = M^d$ for å lytte på samtalen til Alice og Bob. Om vi klarer å finne d så er resten enkelt, men dette er enda vanskeligere enn å låse signeringsproblemet, siden vi ikke vet renteksten m. Vi søker derfor etter en metode som bare finner renteksten m i håp om at dette er enklere.

Altså trenger vi å finne e-te roten av M. Om m tilfredsstiller noen mildere betingelser finnes en metode som kan beregne denne roten, kjent som Coppersmiths

metode [Cop96]. Det metoden gjør spesifikt er at om vi har et polynom $p(x)$ slik at $p(x_0) = 0 \mod n$ for en x_0 tilstrekkelig liten så kan vi finne et annet polynom $q(x)$ med så små koeffisienter at $q(x_0) = 0$ uten å redusere modulo n. Når vi har et slikt polynom kan vi finne x_0 med klassiske numeriske metoder, som til eksempel Newtons metode.

Referanser

[Cop96] Don Coppersmith. «Finding a Small Root of a Univariate Modular Equation». I: *Advances in Cryptology — EUROCRYPT '96*. Red. av Ueli Maurer. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1996, s. 155–165. ISBN: 978-3-540-68339-1. DOI: 10.1007/3-540-68339-9_14.

[DH76] W. Diffie og M. Hellman. «New directions in cryptography». I: *IEEE Transactions on Information Theory* 22.6 (nov. 1976). Conference Name: IEEE Transactions on Information Theory, s. 644–654. ISSN: 1557-9654. DOI: 10.1109/TIT.1976.1055638. URL: https://ieeexplore.ieee.org/document/1055638 (sjekket 07.11.2023).

[Pol78] J. M. Pollard. «Monte Carlo Methods for Index Computation (mod p)». I: *Mathematics of Computation* 32.143 (jul. 1978), s. 918. ISSN: 00255718. DOI: 10.2307/2006496. URL: https://www.jstor.org/stable/2006496?origin=crossref (sjekket 09.10.2023).

[RSA78] R. L. Rivest, A. Shamir og L. Adleman. «A method for obtaining digital signatures and public-key cryptosystems». I: *Communications of the ACM* 21.2 (1. feb. 1978), s. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://dl.acm.org/doi/10.1145/359340.359342 (sjekket 06.11.2023).

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Bd. 106. Graduate Texts in Mathematics. New York, NY: Springer, 2009. ISBN: 978-0-387-09493-9 978-0-387-09494-6. DOI: 10.1007/978-0-387-09494-6. URL: http://link.springer.com/10.1007/978-0-387-09494-6 (sjekket 08.11.2023).