EN KONCIS INTRODUKTION TILL GRUPPTEORI

DANIEL LARSSON

Sammanfattning. En kort introduktion till gruppteori.

Innehåll

1. Binär operation, slutenhet, grupper

Låt $\mathcal{G}$ vara en godtycklig mängd. Vi börjar med att definiera vad som menas med en binär operation och slutenhet under denna operation.

Definition 1 (Binär operation, slutenhet)**.** En **binär operation** på en mängd $\mathcal{G}$ är en operation $\cdot \diamond \cdot$ som till varje ordnat par av element $(a, b) \in \mathcal{G}$ associerar ett element $a \diamond b$. Operationen kallas **sluten** om $a \diamond b \in \mathcal{G}$. Man säger också att $\mathcal{G}$ är **sluten under** $\cdot \diamond \cdot$. En mängd med en binär operation kallar vi en **binär mängd**.

Notera att det är viktigt att det är ett **ordnat** par: $a \diamond b$ behöver inte vara samma som $b \diamond a$.

Exempel 1.1. Låt $\mathcal{G}$ vara $\mathbb{Z}$. Då definierar följande binära operationer på $\mathbb{Z}$:

- $(a, b) \mapsto a \diamond b := a + b$ (vanlig addition);
- $(a, b) \mapsto a \diamond b := a \times b$ (vanlig multiplikation);
- $(a, b) \mapsto a \diamond b := a/b$ (vanlig division);
- $(a, b) \mapsto a \diamond b := \max(a, b)$ (välj det största av a och b);
- $(a, b) \mapsto a \diamond b := a^b$ (exponent).

Notera att operation tre inte är sluten och att den sista utnyttjar att det är ett ordnat par (a, b).

Nu kommer vi till definitionen av en grupp. I korthet kan sägas att det är en binär mängd som uppfyller en samling axiom.

Definition 2 (Grupp)**.** Låt $(\mathcal{G}, \diamond)$ vara en sluten binär mängd. Då är $(\mathcal{G}, \diamond)$ en **grupp** om följande tre axiom håller:

Gr1: Det finns ett element $\mathbf{e} \in \mathcal{G}$ sådant att

$$\mathbf{e} \diamond g = g \diamond \mathbf{e} = g, \qquad \text{för alla } g \in \mathcal{G}.$$

Detta element kallas för gruppens **enhet**;

Gr2: För alla $a, b, c \in \mathcal{G}$ har vi att

$$a \diamond (b \diamond c) = (a \diamond b) \diamond c.$$

Med andra ord ska $\cdot \diamond \cdot$ vara **associativ**.

Gr3: För alla $a \in \mathcal{G}$ finns ett element $a^{-1} \in \mathcal{G}$ så att

$$a \diamond a^{-1} = a^{-1} \diamond a = \mathbf{e}.$$

Elementet a^{-1} kallas för **inversen till** a.

Notera att det bara är den första strukturen i Exempel 1.1 som definierar en grupp struktur på $\mathbb{Z}$.

Definition 3. Antag att $\mathcal{G}$ är en grupp. Antalet element i $\mathcal{G}$ kallas gruppens **ordning**, $\operatorname{ord}(\mathcal{G})$. Om $\operatorname{ord}(\mathcal{G}) < \infty$ säges $\mathcal{G}$ vara en **ändlig grupp**.

2. Exempel, abelska grupper

Här följer nu en lång lista med kända och mindre kända exempel. Ni gör er själva en stor tjänst genom att faktiskt kontrollera att exemplen är grupper.

Notera! Vissa grupper som följer betecknas med klassiska beteckningar som jag kommer att följa. Godtyckliga grupper kommer jag alltid att beteckna med kaligrafiskt typsnitt som t ex $\mathcal{G}$, $\mathcal{H}$, $\mathcal{E}$, e t c.

Exempel 2.1. Uppenbarligen är $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ alla grupper under addition. Varför är inte $\mathbb{N}$ en grupp?

Exempel 2.2. Lite mindre självklart är att $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, är en grupp under multiplikation. Också $\mathbb{R}^*$ och $\mathbb{C}^*$ är grupper under multiplikation. Vad hände nu med $\mathbb{Z}^*$?

Exempel 2.3. Vi har faktiskt bevisat under en lektion att $\mathbb{Z}_n$, kongruensklasserna modulo n, är en grupp. Detta är ett av de allra viktigaste exemplen som ni kommer att få se!

Exempel 2.4. Bilda mängden $\mathbb{U}_n := \{\mathrm{e}^{i\frac{2\pi\ell}{n}} \mid 0 \leq \ell < n\}$. Detta är en grupp under multiplikation, kallad gruppen av n:te enhetsrötter. Namnet kommer sig av att alla $u \in \mathbb{U}_n$ löser ekvationen $x^n = 1$ och alla lösningar till denna ekvation är ett element i $\mathbb{U}_n$.

Exempel 2.5. Låt $\mathbf{R}$ vara någon av $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ eller $\mathbb{Z}_n$. Då är mängden $\operatorname{Mat}_{n,m}(\mathbf{R})$ av $n \times m$-matriser med element i $\mathbf{R}$ en grupp under matrisaddition.

Alla exempel här har haft egenskapen att

$$a \diamond b = b \diamond a, \qquad \text{för alla } a, b \in \mathcal{G}. \tag{2.1}$$

Detta kallas för den **kommutativa lagen** och strukterar som uppfyller denna lag kallas för **kommutativa**. **Utom** när det gäller grupper! Kommutativa grupper brukar kallas för **abelska**, till den norske matematikern Niels Henrik Abels (1802–1829) ära. Jag tror inte man kan överskatta hans bidrag till matematiken, vilket tydligt ses från de viktiga grupper som nu bär hans namn!

3. Exempel, icke-abelska grupper

Här följer nu en lista med grupper som alltså **inte** uppfyller den kommutativa lagen (2.1). Återigen, var noga med att kontrollera mina påståenden att detta är grupper!

Exempel 3.1. Ett av de absolut viktigaste exemplen på grupper överhuvudtaget, och ett som vi redan stött på, är den **symmetriska gruppen**, $\mathbf{S}_n$, av permutationer av n-element (kom ihåg att antalet element i $\mathbf{S}_n$ är lika med $n!$). Detta är en grupp under komposition av permutationer och denna är abelsk bara om $n < 3$. Faktum är att alla grupper med mindre än sex element är abelska! Eftersom antalet element i $\mathbf{S}_3 = 3! = 6$ så är $\mathbf{S}_3$ den minsta icke-abelska gruppen som existerar.

Exempel 3.2. Mängden av alla bijektiva funktioner $f : \mathbb{R} \to \mathbb{R}$ är en icke-abelsk grupp under komposition. Notera att detta är en generalisering av förra exemplet.

Exempel 3.3. Låt $\mathrm{GL}_n(\mathbf{R})$, $\mathbf{R} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, vara mängden av alla linjära avbildningar $A : \mathbf{R}^n \to \mathbf{R}^n$ ($n \times n$-matriser) med icke-noll determinant,

$$\mathrm{GL}_n(\mathbf{R}) := \left\{ \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \;\middle|\; \begin{vmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{vmatrix} \neq 0,\ r_{ij} \in \mathbf{R},\ 1 \leq i, j \leq n \right\}$$

är en icke-abelsk grupp under matrismultiplikation. Denna grupp kallas den **allmänna linjära gruppen** (eng. 'general linear group'). Eftersom alla element i $\mathrm{GL}_n(\mathbf{R})$ har icke-noll determinant så representerar dessa de inverterbara avbildningarna $\mathbf{R}^n \to \mathbf{R}^n$.

Exempel 3.4. Intimt sammankopplade med förra exemplet är följande tre mycket viktiga grupper från linjär algebra.

- Gruppen av ortogonala avbildningar, den **ortogonala gruppen**:
$$\mathrm{O}_n(\mathbf{R}) := \{A \in \mathrm{GL}_n(\mathbf{R}) \mid A^T A = A A^T = \mathbf{1}\},$$
som är en grupp under matrismultiplikation.
- Gruppen av speciella ortogonala avbildningar, den **speciella ortogonala gruppen**:
$$\mathrm{SO}_n(\mathbf{R}) := \{A \in \mathrm{O}_n(\mathbf{R}) \mid \det(A) = 1\},$$
också denna en grupp under matrismultiplikation. Geometriskt är $\mathrm{O}_n(\mathbf{R})$ och $\mathrm{SO}_n(\mathbf{R})$ **rotationsgrupper** som roterar vektorer i $\mathbf{R}^n$ runt någon axel. Skillnaden mellan $\mathrm{O}_n(\mathbf{R})$ och $\mathrm{SO}_n(\mathbf{R})$ är att $\mathrm{O}_n(\mathbf{R})$ är **isometrisk**, d v s, den bevarar längden på vektorerna.

- Den **speciella linjära gruppen**

$$\mathrm{SL}_n(\mathbf{R}) := \{A \in \mathrm{GL}_n(\mathbf{R}) \mid \det(A) = 1\},$$

är liksom de andra matrisgrupperna, en grupp under matrismultiplikation. Geometriskt bevarar $\mathrm{SL}_n(\mathbf{R})$ volymer och orientering (vänster- eller högerhänta baser).

4. Multiplikationstabeller

Ett bra sätt att notarieföra grupper av låg ordning samt få en känsla för olika gruppstrukturer är att göra en så kallad multiplikationstabell (ja, tillbaka till lågstadiet!) eller grupptabell med ett annat namn.

Detta är helt enkelt en tabell som, precis som vanliga multiplikationstabeller, talar om hur olika gruppelement multipliceras. Enklast förklaras detta med illustrationens hjälp i form av exempel.

Exempel 4.1. Låt oss börja med $\mathbb{Z}_3$. Gruppelementen kallar vi $0, 1, 2$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Utan att överanalysera detta tar vi $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Exempel 4.2. Som ett sista exempel här (det kommer fler senare) tar jag $\mathcal{G} = \mathrm{S}_3$. Vi vet att S_3 har 6 element $a_0 = \mathbf{e}, a_1, a_2, a_3, a_4, a_5$. Vi har följande tabell:

$\circ$	$\mathbf{e}$	a_1	a_2	a_3	a_4	a_5
$\mathbf{e}$	$\mathbf{e}$	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	$\mathbf{e}$	a_4	a_5	a_3
a_2	a_2	$\mathbf{e}$	a_1	a_5	a_3	a_4
a_3	a_3	a_5	a_4	$\mathbf{e}$	a_2	a_1
a_4	a_4	a_3	a_5	a_1	$\mathbf{e}$	a_2
a_5	a_5	a_4	a_3	a_2	a_1	$\mathbf{e}$

Kontrollera detta genom att skriva upp alla element i S_3 som permutationer och beräkna kompositionerna! Detta exempel är som synes inte lika enkelt och genomskådligt som de förra. Det är naturligtvis inte så konstigt med tanke på att S_3 är den minsta icke-abelska gruppen.

Övning 4.3. Notera att i varje rad och kolumn i tabellerna ovan förekommer varje element bara en gång. Är detta ett generellt mönster månne? Motivera ert svar! Hur ser man i multiplikationstabellerna vilka element som är varandras inverser? Motivera!

5. Interlude

Nu har vi sett ett antal exempel på grupper vilka jag hoppas har övertygat er om det naturliga med att studera gruppstrukturer. Än så länge har vi dock inte sagt

något om generella egenskaper till grupper. Uppenbarligen är det så att om vi kan bevisa resultat i generella termer där vi bara använder egenskaperna av en mängd som följer med gruppstrukturen så gäller dessa resultat för alla grupper! Därför, om vi t ex har bevisat att en egenskap P gäller för alla grupper (vi har alltså bara använt axiomen **Gr**1–**Gr**3 som definierar grupper), så gäller denna egenskap automatiskt för **alla** exempel på grupper som vi kan komma på! Vi behöver därför inte kontrollera P i alla exempel var för sig.

Detta kallas för att **abstraktifiera** en struktur. Ett annat fint ord är **axiomatisera**. Man uttrycker alltså egenskaper så generellt som möjligt i axiom och allt man kan bevisa med **endast** dessa axiom gäller för alla strukturer som uppfyller dessa axiom.

6. Grundläggande satser

Satserna som nu följer är exempel på abstrakta utsagor om **alla** grupper. För att bevisa dem använder vi **bara** axiomen **Gr**1–**Gr**3 för grupper.

Notera! Från och med nu så kommer jag att följa en algebraisk tradition att beteckna den binära operationen för abelska grupper med ett '+' och för icke-abelska grupper med en '$\cdot$', eller, som är vanligt i elementär algebra, helt utan tecken, t ex '$a \cdot b$' blir ab. Dra er också till minnes att kaligrafiska bokstäver som $\mathcal{G}$ betecknar godtyckliga grupper.

Sats 6.1. Antag att $ab = ac$ för $a, b, c \in \mathcal{G}$. Då är $b = c$.

Bevis. För varje element $a \in \mathcal{G}$ existerar ett element $a^{-1} \in \mathcal{G}$ så att $aa^{-1} = a^{-1}a = \mathbf{e}$ (Axiom **Gr**1). Multiplicera $ab = ac$ från vänster med a^{-1}:

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) \quad \Longleftrightarrow \\ (a^{-1}a)b &= (a^{-1}a)c \quad (\text{Axiom } \mathbf{Gr}2) \quad \Longleftrightarrow \\ \mathbf{e}b &= \mathbf{e}c \quad (\text{Axiom } \mathbf{Gr}3) \quad \Longleftrightarrow \\ b &= c \quad (\text{Axiom } \mathbf{Gr}1). \end{aligned}$$

Beviset är klart. □

Nästa bevis kommer inte att vara förklarat i lika stor detalj som ovanstående.

Sats 6.2. Låt $a, b \in \mathcal{G}$. Då har varje ekvation $ax = b$ och $xa = b$ en unik lösning i $\mathcal{G}$.

Bevis. Det är klart att $x := a^{-1}b$ respektive $x := ba^{-1}$ löser ekvationerna (visa detta!). Vi måste visa att det i vardera fallet bara finns **en** lösning. Antag att både $a^{-1}b$ och y löser den första ekvationen. Då har vi att dels $b = aa^{-1}b$ och $b = ay$. Sätt dessa lika varandra. Då får vi $aa^{-1}b = ay$. Sats 6.1 säger nu att vi kan stryka a från vänster och vi får då kvar: $a^{-1}b = y$. Alltså finns bara en lösning. Analogt visas det för den andra ekvationen (gör det!). □

Beviset för satsen som följer här är så vackert och listigt att man kan gråta!

Sats 6.3. Enhetselementet $\mathbf{e} \in \mathcal{G}$ är unikt.

Bevis. Antag att det finns två olika enhetselement $\mathbf{e}$ och $\mathbf{e}'$. Vi utnyttjar nu att båda uppfyller **Gr**1:

$$\mathbf{e} = \mathbf{e}\mathbf{e}' = \mathbf{e}'.$$

Så var det beviset till ända. □

Sats 6.4. Inversen a^{-1} till ett element a är unik.

Bevis. Antag att det finns ett annat element y så att $ya = \mathbf{e}$. Multiplicera denna ekvation från höger med a^{-1}: $(ya)a^{-1} = \mathbf{e}a^{-1}$. Detta är ekvivalent med $y = a^{-1}$. Det är klart att samma sak gäller för $ay = \mathbf{e}$. □

Låt mig återigen poängtera (blir det tjatigt?) att jag bara har använt axiomen för en grupp. Ingenting annat. Därför gäller ovanstående satser för **alla** strukturer som uppfyller **Gr**1–**Gr**3 (d v s, grupper) oavsett i vilken färg, form eller skepnad dessa strukturer kommer.

7. Undergrupper, cykliska grupper, generatorer och snitt

Givet någon algebraisk struktur är man ofta intresserad av vilka delstrukturer som finns. I fallet med grupper är det de så kallade undergrupperna man är intresserad i.

Definition 4. Låt $\mathcal{H}$ vara en icke-tom delmängd i $\mathcal{G}$. Då är $\mathcal{H}$ en **undergrupp** i $\mathcal{G}$ om för alla $a, b \in \mathcal{H}$ så är $ab^{-1} \in \mathcal{H}$. Vi betecknar att $\mathcal{H}$ är en undergrupp i $\mathcal{G}$ genom att, som brukligt är, skriva $\mathcal{H} \trianglelefteq \mathcal{G}$. En undergrupp $\mathcal{H}$ kallas **triviell** om $\mathcal{H} = \mathbf{e}$ och **proper** om $\mathcal{H} \neq \mathcal{G}$. En proper undergrupp betecknas $\mathcal{H} \triangleleft \mathcal{G}$.

Notera att definitionen säger att den binära operationen på $\mathcal{H}$ ska vara den samma som den på $\mathcal{G}$ och att operationen ska vara sluten på $\mathcal{H}$.

Exempel 7.1. Mängden $n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$ är en proper undergrupp till $\mathbb{Z}$.

Sats 7.1. Vi har att $\mathcal{H}$ är en undergrupp till $\mathcal{G}$ om och endast om:

(i) $\mathbf{e} \in \mathcal{H}$;
(ii) $a \in \mathcal{H} \Longrightarrow a^{-1} \in \mathcal{H}$;
(iii) $ab \in \mathcal{H}$ närhelst $a, b \in \mathcal{H}$.

Bevis. Antag först att $\mathcal{H}$ är en undergrupp. Definitionen säger att om $a, b \in \mathcal{H}$ så är $ab^{-1} \in \mathcal{H}$. Ta $b = a$. Då följer att $\mathbf{e} \in \mathcal{H}$. Sätt nu $a = \mathbf{e}$ så följer att $b \in \mathcal{H}$ medför att $b^{-1} \in \mathcal{H}$. Eftersom $y^{-1} \in \mathcal{H}$ när $y \in \mathcal{H}$ så ser vi om vi sätter $b = y^{-1} \in \mathcal{H}$ att $\mathcal{H} \ni ab^{-1} = a(y^{-1})^{-1} = ay$.

Antag nu att ovanstående (i)–(iii) håller. Krav (i) ger oss att $\mathcal{H}$ är icke-tom. Från (ii) ser vi att $a, b^{-1} \in \mathcal{H}$ om $a, b \in \mathcal{H}$ och från (iii) ser vi att $ab^{-1} \in \mathcal{H}$. □

Ett lätt sätt att konstruera undergrupper till en grupp är att göra följande. Ta ett element $a \in \mathcal{G}$. Bilda mängden av alla potenser

$$\langle a \rangle := \{b \mid b = a^n := aa \cdots a \quad (n \text{ ggr})\}.$$

Naturligtvis gör man som vanligt konventionerna att $a^0 = \mathbf{e}$ och $a^1 = a$. Kontrollera nu själva att $\langle a \rangle \trianglelefteq \mathcal{G}$.

Definition 5. Undergrupper på formen $\langle a \rangle \trianglelefteq \mathcal{G}$ kallas **cykliska undergrupper**. Elementet $a \in \mathcal{G}$ kallas för **generator** till $\langle a \rangle$. Om hela gruppen $\mathcal{G}$ kan genereras av ett element $a \in \mathcal{G}$, alltså, om $\mathcal{G} = \langle a \rangle$, kallas $\mathcal{G}$ för **cyklisk**.

Observera att alla element a i en grupp $\mathcal{G}$ genererar en undergrupp (som inte behöver vara icke-triviell eller proper) i $\mathcal{G}$, nämligen $\langle a \rangle$. Jag ber också om att få göra er uppmärksamma på att i normalt gruppteoretiskt beteckningslingo så betecknar $\mathcal{H} \trianglelefteq \mathcal{G}$ att $\mathcal{H}$ är en så kallad "normal" undergrupp till $\mathcal{G}$ (mer om detta senare); för alla er som funderar på en karriär inom gruppteori!

7.1. **Cykliska grupper och undergrupper.** Vi kommer nu att fokusera lite på cykliska grupper och undergrupper. Följande sats är enkel.

Sats 7.2. Varje cyklisk grupp $\mathcal{C} = \langle a \rangle$ är abelsk.

Bevis. Givet två element $x := a^n$ och $y := a^m$ ser vi att

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$$

Beviset är klart. □

Sats 7.3. Varje undergrupp till en cyklisk grupp är cyklisk.

Bevis. Låt $\mathcal{C} = \langle a \rangle$ vara en cyklisk grupp och $\mathcal{H}$ en undergrupp $\mathcal{H} \trianglelefteq \mathcal{C}$. Låt $m \in \mathbb{Z}$ vara det minsta tal så att $a^m \in \mathcal{H}$. Jag påstår att $\mathcal{H} = \langle a^m \rangle$. Givet ett annat $b \in \mathcal{H}$ så har vi att $b = a^n$ för något $n \in \mathbb{Z}$. Vi har att $m \leq n$ så divisionsalgoritmen ger oss att $n = qm + r$, $0 \leq r < m$. Sålunda har vi $a^n = a^{qm+r} = (a^m)^q a^r$. Detta kan skrivas om som $a^r = a^n (a^m)^{-q}$ och då $a^n \in \mathcal{H}$ så ligger $a^{-n} \in \mathcal{H}$ och $(a^m)^q \in \mathcal{H}$. Alltså ligger $a^r \in \mathcal{H}$, men eftersom m var det minsta talet så att $a^m \in \mathcal{H}$ och $0 \leq r < m$ så måste $r = 0$ och detta betyder att $a^n = (a^m)^q$. □

För att bevisa nästa sats behöver vi följande talteoretiska lemma.

Lemma 7.4. Det minsta tal m så att $n | mk$ är $n/\gcd(n,k)$.

Bevis. Vi vet att $\gcd(n,k) = xn + yk$ för $x, y \in \mathbb{Z}$. Alltså är $n/\gcd(n,k)$ och $k/\gcd(n,k)$ relativt prima (varför?). Det betyder att

$$\frac{mk}{n} = \frac{m\big(k/\gcd(n,k)\big)}{n/\gcd(n,k)}$$

vilket ger att $(n/\gcd(n,k)) | m$ (varför?). Alltså är det minsta m sådant att $n | mk$, $m = n/\gcd(n,k)$. □

Sats 7.5. Låt $\mathcal{H} \trianglelefteq \mathcal{C} = \langle a \rangle$ vara genererad av a^k, d v s, $\mathcal{H} = \langle a^k \rangle$. Då är

$$\operatorname{ord}(\mathcal{H}) = \frac{\operatorname{ord}(\mathcal{C})}{\gcd(\operatorname{ord}(\mathcal{C}), k)}.$$

Bevis. Det är klart att om $m = \operatorname{ord}(\mathcal{H})$ så är $(a^k)^m = \mathbf{e}$ och m är det minsta sådant (varför?). Eftersom ordningen n till $\mathcal{C}$ är det minsta tal så att $a^n = \mathbf{e}$ följer att $n \mid mk$ och det minsta sådant m är $n/\gcd(n,k)$ enligt föregående lemma. □

Exempel 7.2. Följande är exempel på undergrupper:

- I $\mathbb{Z}_4$ så är $\langle 2 \rangle = \{0, 2\}$ en proper icke-triviell undergrupp (faktiskt den enda).
- I $\mathbb{Z}_{12}$ finns $\langle 6 \rangle = \{0, 6\}$, $\langle 3 \rangle = \{0, 3, 6, 9\}$ som propra undergrupper, medan t ex $\langle 7 \rangle = \mathbb{Z}_{12}$.

Övning 7.3. Använd ovanstående sats 7.5 för att bestämma alla andra undergrupper i $\mathbb{Z}_{12}$.

Meta-sats 7.6. Det finns essentiellt bara två typer av cykliska grupper:

(i) $\mathbb{Z}$, om $\mathcal{C}$ har oändlig ordning;
(ii) $\mathbb{Z}_n$, om $\mathcal{C}$ har ändlig ordning n.

7.2. **Snitt och generatorer.** Nu återgår vi till generella grupper.

Sats 7.7. Låt $\mathcal{H}_i$, $i \in I \subseteq \mathbb{N}$ vara en (ändlig eller oändlig, beroende på indexmängden I) familj av undergrupper av en grupp $\mathcal{G}$. Då är

$$\bigcap_{i\in I} \mathcal{H}_i := \mathcal{H}_1 \cap \mathcal{H}_2 \cap \cdots \cap \mathcal{H}_n \cap \cdots$$

en undergrupp till $\mathcal{G}$.

Bevis. Detta bevis är enkelt och lämnas till läsaren. □

Definition 6. Låt $\mathsf{a} := \{a_i \in \mathcal{G} \mid i \in I\}$ vara en mängd element och låt $\mathcal{H}_j$, $j \in J \subseteq \mathbb{N}$ vara alla undergrupper så att $\mathcal{H}_j \supseteq \mathsf{a}$ för alla $j \in J$. Då säges

$$\mathcal{H} := \bigcap_{j\in J} \mathcal{H}_j \supseteq \mathbf{a},$$

vara undergruppen av $\mathcal{G}$ **genererad** av a och a är **generatorerna** till $\mathcal{H}$. Om dessutom $\operatorname{ord}(\mathsf{a}) < \infty$ säges $\mathcal{H}$ vara **ändligt genererad**; om $\mathcal{H} = \mathcal{G}$, kallas $\mathcal{G}$ för **genererad**, respektive, **ändligt genererad** och a är då generatorerna för $\mathcal{G}$. Vi betecknar att a genererar $\mathcal{H}$ som $\mathcal{H} = \langle \mathsf{a} \rangle$.

Notera två saker:

- ovanstående definition generaliserar cykliska grupper och undergrupper (men är inte i allmänhet abelska!);
- $\mathcal{H}$ är den minsta undergrupp till $\mathcal{G}$ som innehåller a.

Sats 7.8. Undergruppen $\langle \mathsf{a} \rangle$ innehåller precis alla ordnade produkter av element från a.

Bevis. Lämnas åt läsaren. □

Exempel 7.4. Betrakta gruppen $\mathrm{SL}_2(\mathbb{Z})$ av alla heltaliga 2×2-matriser med determinant 1:

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ac - bd = 1 \right\}.$$

Av historiska skäl brukar man i $\mathrm{SL}_2(\mathbb{Z})$ identifiera två matriser upp till tecken, d v s, $M = -M$ i $\mathrm{SL}_2(\mathbb{Z})$ (ska man vara riktigt petig får man då gruppen $\mathrm{PSL}_2(\mathbb{Z})$, den **projektiva specialla linjära gruppen**). Låt oss anamma denna konvention här också. Matriserna

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \text{och} \qquad B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

genererar en undergrupp Γ till $\mathrm{SL}_2(\mathbb{Z})$. Detta betyder att varje element i Γ kan skrivas som en ändlig produkt av A och B. Man kan t o m visa att A och B genererar **hela** $\mathrm{SL}_2(\mathbb{Z})$ så vi har $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Gruppen Γ kallas den **modulära gruppen** och är oerhört viktig i talteori och komplex analys.

7.3. **Fria grupper, generatorer, relationer.** Låt $\mathsf{a} := \{a_1, a_2, \ldots, a_n\}$ (i princip kan $n = \infty$) vara en mängd symboler. I dessa sammanhang brukar a kallas för ett **alfabet** och element i a för **bokstäver**. Ett **ord** i alfabetet a är då en ändlig kombination med element från a, t ex, $a_4a_4a_5a_2^{-3}a_4a_1$. Naturligtvis brukar man skriva $aaa^{-1}aaa^{-1}a$ som a^5 så föregående ord skrivs $a_4^2a_5a_2^{-3}a_4a_1$. Notera att man inte kan byta plats på bokstäverna och få, t ex, $a_4^3a_5a_1$. Med andra ord, $a_4^2a_5a_2^{-3}a_4a_1 \neq a_4^3a_2^{-3}a_5a_1$.

Den **fria gruppen på alfabetet** a, betecknat $\mathbf{F}(\mathsf{a})$, är mängden av alla ord i a med sammansättning som multiplikation. Man gör konventionerna att $a_i^0 = \mathbf{e}$ och $a_i^1 = a_1$ för alla i som vanligt. Så är t ex, $a_1a_4^3 \cdot a_1a_3a_2 = a_1a_4^3a_1a_3a_2$.

Notera att $\mathbf{F}(\mathsf{a})$ **aldrig** är abelsk, såvida inte $\mathsf{a} = \{a\}$.

Definition 7. En **relation** på $\mathbf{F}(\mathsf{a})$ är ett ord i a satt lika med $\mathbf{e}$.

Exempel 7.5. Om $\mathsf{a} = \{a, b\}$ så är

- $ab^2a^{-1} = \mathbf{e}$
- $aba^{-1}b^{-1} = \mathbf{e}$
- $a^{17}b^{-32}aba^2 = \mathbf{e}$

olika relationer. Notera att relationerna kan skrivas om till exempel kan de två första skrivas som $ab^2 = a$, respektive, $ab = ba$ (känner ni igen den kommutativa lagen?).

En grupp med generatorer och relationer är nu löst uttryckt mängden av alla ord i ett alfabet med gruppstruktur sammansättning precis som i $\mathbf{F}(\mathsf{a})$, men där det finns relationer mellan generatorerna (bokstäverna). Observera dock att resultatet inte är en fri grupp eftersom en sådan inte har några relationer alls. En stringent definition får vänta till ett senare tillfälle. Men några exempel ska nog få er att genomskåda idéen. Först några bekväma notationer och termer.

Man brukar beteckna att $\mathcal{G}$ är givet av generatorerna a och relationerna R genom att skriva $\mathcal{G} = \langle \mathsf{a} \mid R \rangle$. Detta kallas för en **presentation** av $\mathcal{G}$. Om a och R är ändliga mängder så säges $\mathcal{G}$ vara av **ändlig presentation**.

Exempel 7.6. Här följer då några väl valda exempel.

- $\mathbb{Z} = \langle a \mid \emptyset \rangle$.
- $\mathbb{Z}_n = \langle a \mid \{a^n = \mathbf{e}\} \rangle$.
- $\mathbf{A}(\mathsf{a}) := \langle \mathsf{a} \mid \{aba^{-1}b^{-1} = \mathbf{e} \mid \forall a, b \in \mathsf{a}\} \rangle$, den **fria abelska gruppen på** a.
- Man kan visa att $\mathrm{S}_3 = \langle \{a, b\} \mid \{a^3 = \mathbf{e}, b^2 = \mathbf{e}\} \rangle$.
- Den n**-te dihedrala gruppen**, D_n är given av

  $$\mathrm{D}_n := \langle \{a, b\} \mid \{a^n = \mathbf{e}, b^2 = \mathbf{e}, abab = \mathbf{e}\} \rangle.$$

  Vi har att $\mathrm{ord}(\mathrm{D}_n) = 2n$. Denna grupp är **gruppen av rotationssymmetrier av plana** n**-polygoner**. Notera att $\mathrm{D}_3 = \mathrm{S}_3$.
- Dessutom kan man visa att

  $$\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \langle \{A, B\} \mid \{A^2 = \mathbf{e}, (AB)^3 = \mathbf{e}\} \rangle.$$

  Notera här att $(AB)^3 \neq A^3B^3$ utan $(AB)^3 = ABABAB$.

Jag skrev ovan att två grupper är lika. Men det är inte helt självklart vad man ska mena med det. Jag återkommer till detta i näst-sista sektionen.

7.4. **Direkta produkter, ändligt genererade abelska grupper.** Dra er till minnes att om A och B är två mängder så är deras direkta produkt $A \times B$ mängden av alla par (a, b), med andra ord,

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

Om vi istället lägger på ytterligare struktur och betraktar två grupper $\mathcal{G}$ och H, är då direkta produkten $\mathcal{G} \times \mathcal{H}$ en grupp och hur definieras i så fall multiplikationen där?

Definition-Sats 7.9. Låt $\mathcal{G}$ och $\mathcal{H}$ vara två grupper. Definiera en multiplikation på den direkta produkten $\mathcal{G} \times \mathcal{H}$ såsom

$$(a, b)(c, d) := (ac, bd).$$

Under denna multiplikation är $\mathcal{G} \times \mathcal{H}$ en grupp.

Bevis. Enkelt och lämnas till läsaren. □

Uppenbarligen kan detta generaliseras till godtyckliga (ändliga eller oändliga) direkta produkter $\mathcal{G}_1 \times \mathcal{G}_2 \times \cdots \times \mathcal{G}_n \times \cdots$ (även om fallet med oändliga direkta produkter är lite mer "tongue-in-cheek" att definiera rigoröst).

Låt mig bryta in med lite fler exempel samt i samma andetag passa på att ge fler multiplikationstabeller.

Exempel 7.7. Följande grupp $\mathbb{Z}_2 \times \mathbb{Z}_2$ är det minsta exemplet på en icke-cyklisk grupp:

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Denna grupp brukar kallas **Kleins Viergruppe**. Generellt sätt är $\mathbb{Z}_n \times \mathbb{Z}_n$ aldrig cyklisk.

Exempel 7.8. Gruppen $\mathbb{Z} \times \mathbb{Z}$ är inte heller cyklisk.

Exempel 7.9. Precis som man börjar ana att direkta produkter av grupper aldrig är cykliska kommer följande exempel: $\mathbb{Z}_2 \times \mathbb{Z}_3$,

+	(0,0)	(1,0)	(0,1)	(1,1)	(0,2)	(1,2)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)	(0,2)	(1,2)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)	(1,2)	(0,2)
(0,1)	(0,1)	(1,1)	(0,2)	(1,2)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,2)	(0,2)	(1,0)	(0,0)
(0,2)	(0,2)	(1,2)	(0,0)	(1,0)	(0,1)	(1,1)
(1,2)	(1,2)	(0,2)	(1,0)	(0,0)	(1,1)	(0,1)

Denna grupp är cyklisk. Generellt har vi följande sats.

Sats 7.10. Låt $\mathcal{G} = \mathbb{Z}_n$ och $\mathcal{H} = \mathbb{Z}_m$. Då är $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ (grupperna till vänster och höger är "lika") om och endast om $\gcd(n, m) = 1$. Följaktligen är då $\mathbb{Z}_n \times \mathbb{Z}_m$ cykliska.

Återigen är det inte helt självklart vad man ska mena med att två grupper är "lika". Nu skrev jag '$\cong$' och inte '$=$' för att betona detta. Trots det kan ni temporärt

tänka er det som om det stod att grupperna är lika. Detta kommer att klarna i sinom tid (hoppas jag).

Övning 7.10. Beräkna multiplikationstabellerna till följande grupper:

- $\mathbb{Z}_2 \times \mathbb{Z}_4$;
- $\mathbb{Z}_2 \times \mathrm{S}_3$;
- $\mathrm{GL}_2(\mathbb{Z}_2) \times \mathbb{Z}_2$ (Denna är ganska klurig.)

Sats 7.11. Ordningen till ett element $(a, b) \in \mathcal{G} \times \mathcal{H}$ är $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$, där lcm är **minsta gemensamma multipel** (eng. "least common multiple").

Det borde vara intuitivt klart vad minsta gemensamma multipel betyder: man plockar ut alla gemensamma primfaktorer och multiplicerar ihop dessa. Till exempel, $\mathrm{lcm}(20, 24) = 4$.

Båda dessa satser kan generaliseras till direkta produkter av ändligt många grupper på ett uppenbart sätt.

Följande sats kan sägas vara huvudsatsen för ändligt genererade abelska grupper. Beviset är tämligen komplicerat och väl utanför vad som ingår i denna kurs. Likväl tycker jag att satsen är så pass viktig och vacker att den förtjänas att nämnas och komma ihåg.

Sats 7.12 ("Primtalsfaktorisering av grupper")**.** Låt $\mathcal{G}$ vara en **ändligt genererad abelsk** grupp. Då är

$$\mathcal{G} \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

där p_i är primtal, $k_i \in \mathbb{N}_0$ och dessa är unika (d v s, bara beroende på $\mathcal{G}$). Antalet $\mathbb{Z}$ är också unikt för $\mathcal{G}$ och kallas $\mathcal{G}$'s **Betti-tal**.

Denna sats säger alltså att alla ändligt genererade abelska grupper är på formen

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

En ganska överraskande sats!

Lägg märke till att, till exempel,

$$\mathbb{Z}_{p_3^{k_3}} \times \mathbb{Z} \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}} \times \mathbb{Z} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}$$

är samma grupp som

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

så ordningen mellan faktorerna spelar ingen roll.

8. Sidoklasser, Lagranges sats, normala undergrupper

Givet en undergrupp $\mathcal{H} \trianglelefteq \mathcal{G}$ kan man införa en ekvivalensrelation på $\mathcal{G}$ som följer.

Definition-Sats 8.1. Låt $\mathcal{H} \trianglelefteq \mathcal{G}$ och inför relationen $\sim$ på $\mathcal{G}$, $a \sim b$, om och endast om $a^{-1}b \in \mathcal{H}$. Detta är en ekvivalensrelation.

Bevis. Att $a \sim a$ (reflexivitet) är klart (kom ihåg att $\mathbf{e} \in \mathcal{H}$). Symmetri-egenskapen $a \sim b \Rightarrow b \sim a$ följer av att inversen till ett element i $\mathcal{H}$ också ligger i $\mathcal{H}$. I detalj: $a \sim b \Leftrightarrow a^{-1}b \in \mathcal{H}$ vilket medför att $\mathcal{H} \ni (a^{-1}b)^{-1} = b^{-1}a \Leftrightarrow b \sim a$. Slutligen, transitiviteten: givet $a^{-1}b \in \mathcal{H}$, $b^{-1}c \in \mathcal{H}$ ser vi , eftersom $\mathcal{H}$ är en grupp, att $\mathcal{H} \ni a^{-1}bb^{-1}c = a^{-1}c$, vilket avslutar beviset. □

Denna sats medför att varje undergrupp $\mathcal{H}$ i en grupp $\mathcal{G}$ delar upp $\mathcal{G}$ ("partitionerar") i disjunkta ekvivalensklasser. Dessa ekvivalensklasser kallas för **vänster-sidoklasser till** $\mathcal{H}$ **i** $\mathcal{G}$. Analogt definierar man **höger-sidoklasser**. Notera att om $\mathcal{H} = \langle \mathbf{e} \rangle$ så är ekvivalensklasserna precis elementen i $\mathcal{G}$.

Att $a \sim b$ är ekvivalent med att $\exists h \in \mathcal{H}$ så att $b = ah$. Med andra ord är

$$[a] := \{b \in \mathcal{G} \mid a \sim b\} = \{b \in \mathcal{G} \mid b = ah, h \in \mathcal{H}\}.$$

Detta leder till att man brukar skriva vänster-sidoklasserna $[a]$ som $a\mathcal{H}$. Notera att $a\mathcal{H} = b\mathcal{H}$ om och endast om $a \sim b$. Varje vänster-sidoklass har $\text{ord}(\mathcal{H})$ element eftersom $a\mathcal{H} = \{ah \mid h \in \mathcal{H}\}$. Från denna enkla iakttagelse följer följande mycket användbara sats:

Sats 8.2 (Lagranges sats)**.** Ordningen till varje undergrupp i en ändlig grupp är en divisor till ordningen på gruppen. Med andra ord, om $\text{ord}(\mathcal{H}) = m$ och $\text{ord}(\mathcal{G}) = n$, $\mathcal{H} \trianglelefteq \mathcal{G}$, så är $n = km$ för något $k \in \mathbb{N}$.

Bevis. Eftersom $\mathcal{G}$ är en disjunkt union av vänster-sidoklasser och varje (vänster-) sidoklass innehåller lika många element som $\mathcal{H}$, så följer satsen. □

Följdsats 8.3. Om $\text{ord}(\mathcal{G}) = p$, ett primtal, så finns inga icke-triviala, propra undergrupper.

Definition 8. Antalet vänster-sidoklasser till $\mathcal{H} \trianglelefteq \mathcal{G}$ kallas $\mathcal{H}$'s **index** i $\mathcal{G}$ och betecknas $[\mathcal{G} : \mathcal{H}]$. Från föregående sats ser vi att om $\text{ord}(\mathcal{G}) < \infty$ så är

$$[\mathcal{G} : \mathcal{H}] = \frac{\text{ord}(\mathcal{G})}{\text{ord}(\mathcal{H})}.$$

Definition 9. En undergrupp $\mathcal{H} \trianglelefteq \mathcal{G}$ är **normal** om $a\mathcal{H} = \mathcal{H}a$ för alla $a \in \mathcal{G}$. Eller omformulerat, höger- och vänster-sidoklasserna är lika.

Alla undergrupper till en abelsk grupp är normala.

9. Homomorfi, kärna, bild och isomorfi

Jag har hittills undlåtit att prata om avbildningar mellan grupper, men det ska nu åtgärdas.

En avbildning mellan två grupper $\phi : \mathcal{G} \to \mathcal{H}$ är naturligtvis först och främst en mängdteoretisk avbildning, d v s, $\phi(\mathcal{G}) \subseteq \mathcal{H}$, **men** man vill också att varje avbildning ska respektera gruppstrukturerna hos de inblandade grupperna. Vad menar jag med detta?

För att illustrera detta, låt mig beteckna multiplikationen i $\mathcal{G}$ med '$*$' och i $\mathcal{H}$ med '$\smile$'. Låt ϕ vara en mängdteoretisk avbildning mellan de underliggande mängderna till $\mathcal{G}$ och $\mathcal{H}$. För varje $g \in \mathcal{G}$ så är $\phi(g) \in \mathcal{H}$. Man vill nu att om $g = g_1 * g_2$ så ska ϕ avbilda detta på ett specifikt element i $\mathcal{H}$, nämligen $\phi(g_1) \smile \phi(g_2)$. Med andra ord vill man att

$$\phi(g_1 * g_2) = \phi(g_1) \smile \phi(g_2).$$

Man vill alltså att varje avbildning ϕ kopplar samman gruppstrukturen på $\mathcal{G}$ med gruppstrukturen på $\mathcal{H}$, så att man kan få information angående $\mathcal{H}$ från $\mathcal{G}$ och vice versa.

Definition 10. En mängdteoretisk avbildning $\phi : \mathcal{G} \to \mathcal{H}$, där $\mathcal{G}$ och $\mathcal{H}$ är grupper, så att $\phi(g_1 * g_2) = \phi(g_1) \smile \phi(g_2)$, kallas för en **grupphomomorfi**, eller bara **homomorfi**.

Alla avbildningar mellan grupper kommer från och med nu att vara homomorfier. Dessutom kommer vi till en början att beteckna enheten i $\mathcal{G}$ med $\mathbf{e}$ och i $\mathcal{H}$ med $\mathbf{e}'$ samt att gruppmultiplikationerna kommer att betecknas på samma sätt. I de fall där det finns risk för missförstånd eller allmänn förvirring kommer jag att påpeka explicit vilken struktur eller enhet som gäller.

Exempel 9.1. Här kommer nu en samling exempel.

- Till varje direkt produkt $\mathcal{G}\times\mathcal{H}$ av två grupper $\mathcal{G}$ och $\mathcal{H}$ finns två kanoniska homomorfier, nämligen projektionerna:
$$\begin{array}{ccc} \mathcal{G}\times\mathcal{H} & \xrightarrow{\mathrm{pr}_2} & \mathcal{H} \\ {\scriptstyle \mathrm{pr}_1}\downarrow & & \\ \mathcal{G} & & \end{array}$$
där $\mathrm{pr}_1(a,b) := a$ och $\mathrm{pr}_2(a,b) := b$.
- Det är lätt att visa att $\mathbb{R}^{>0} := \{r \in \mathbb{R} \mid r > 0\}$ är en grupp under multiplikation (gör detta!). Vi vet sedan tidigare att $\mathbb{R}$ är en grupp under addition. Avbildningen $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ given av $\exp(a) := \mathrm{e}^a$ (exponentialavbildningen) är en grupphomomorfi. Detta följer av att $\exp(a+b) = \mathrm{e}^{a+b} = \mathrm{e}^a\mathrm{e}^b = \exp(a)\exp(b)$. Notera att gruppstrukturerna är till synes helt 0 olika. Strax ska vi dock visa att från ett gruppteoretiskt perspektiv är de faktiskt lika!
- Fixera ett tal $n \geq 2$. För varje element $a \in \mathbb{Z}$ kan man betrakta **reduktionen modulo** n $\mathrm{red}_n(a)$: skriv $a = qn + r$ enligt divisionsalgoritmen. Då är $\mathrm{red}_n : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto r$. Jag lämnar till er att visa att det är en homomorfi (tips: använd kongruenser).
- Låt $\mathbb{S}^1$ vara alla komplexa tal $z \in \mathbb{C}$ med $|z| = 1$. Detta är ekvivalent med att om $z = x + iy$ så är $|z| = x^2 + y^2 = 1$. Med andra ord så är $\mathbb{S}^1$ enhetscirkeln i $\mathbb{C}$. Detta är en (abelsk) grupp under multiplikation (visa detta! Tips: använd representationen $z = \mathrm{e}^{i\theta}$). Definiera en avbildning $\mathbb{S}^1 \to \mathrm{SL}_2(\mathbb{C})$ genom
$$z = \mathrm{e}^{i\theta} \mapsto \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$
Detta är en grupphomomorfi (kontrollera! Glöm inte att visa att matrisen verkligen ligger i $\mathrm{SL}_2(\mathbb{C})$).
- Gruppen $\mathbb{T}^1 := \mathbb{S}^1 \times \mathbb{S}^1$ är också en abelsk grupp. Geometriskt är det en **torus** (tänk på det som om det är två cirklar som är sammanklistrade på något sätt).

Definition 11. Låt $\mathcal{G} \xrightarrow{\phi} \mathcal{H}$ och för $h \in \mathcal{H}$ låt $\phi^{-1}(h) := \{g \in \mathcal{G} \mid \phi(g) = h\}$. Detta kallas den **inversa bilden av** h eller **fibern över** h. Sätt
$$\ker(\phi) := \phi^{-1}(\mathbf{e}') = \{g \in \mathcal{G} \mid \phi(g) = \mathbf{e}'\}.$$
Denna mängd kallas **kärnan** till ϕ. Låt dessutom
$$\mathrm{im}(\phi) := \{h \in \mathcal{H} \mid \exists g \in \mathcal{G},\ \phi(g) = h\},$$
vilket är **bilden** till ϕ.

På engelska kallas dessa **kernel** och **image**, varifrån förkortningarna härstammar.

Sats 9.1. För varje homomorfi $\phi : \mathcal{G} \to \mathcal{H}$ gäller att

(i) $\phi(\mathbf{e}) = \mathbf{e}'$,
(ii) $\phi(a^{-1}) = \phi(a)^{-1}$,
(iii) $\ker(\phi)$ en normal undergrupp till $\mathcal{G}$, och
(iv) $\mathrm{im}(\phi)$ en undergrupp (i allmänhet inte normal) till $\mathcal{H}$.

Bevis. Vi delar upp beviset i flera steg.

Steg 1. Vi har att $\phi(\mathbf{e}) = \phi(\mathbf{ee}) = \phi(\mathbf{e})\phi(\mathbf{e})$. Multiplicera denna ekvation från höger (till exempel) med $\phi(\mathbf{e})^{-1}$. Då får vi $\mathbf{e}' = \phi(\mathbf{e})$. Alltså är (i) klar.

Steg 2. För (ii) notera att $\mathbf{e}' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. Eftersom inversen i en grupp är unik så följer att $\phi(a^{-1}) = \phi(a)^{-1}$.

Steg 3. För att visa att $\ker(\phi)$ är en undergrupp till $\mathcal{G}$ måste vi dessutom visa att $a^{-1} \in \ker(\phi)$ om $a \in \ker(\phi)$ och $ab \in \ker(\phi)$ om $a, b \in \ker(\phi)$. Vi har $\phi(a^{-1}) = \phi(a)^{-1} = (\mathbf{e}')^{-1} = \mathbf{e}'$, så $a^{-1} \in \ker(\phi)$; att $ab \in \ker(\phi)$ om $a, b \in \ker(\phi)$ följer av homomorfi-egenskapen, ty, $\phi(ab) = \phi(a)\phi(b) = \mathbf{e}'\mathbf{e}' = \mathbf{e}'$.

Steg 4. Vi ska nu visa att $\ker(\phi)$ är normal. Det betyder att vi ska visa att $a\ker(\phi)$ och $\ker(\phi)a$ är lika. Standardsättet att visa att två mängder U och V är lika är att visa att, dels $U \subseteq V$, och dels $U \supseteq V$.

- $a\ker(f) \subseteq \ker(\phi)a$: Ta $x \in a\ker(\phi)$. Vi vill visa att $x \in \ker(\phi)a$. Att $x \in a\ker(\phi) \Leftrightarrow \exists h_1 \mid x = ah_1$. Skriv om detta som $x = ah_1a^{-1}a = h_2a$. Så om $h_2 := ah_1a^{-1} \in \ker(\phi)$ är vi klara. Men det är uppenbart så: $\phi(ah_1a^{-1}) = \phi(a)\phi(h_1)\phi(a^{-1}) = \phi(a)\mathbf{e}'\phi(a^{-1}) = \phi(a)\phi(a)^{-1} = \mathbf{e}'$.
- $a\ker(\phi) \supseteq \ker(\phi)a$: Detta visas på samma sätt men man skriver $\ker(\phi) \ni x = h_1a = aa^{-1}h_1a$.

Steg 5. Vi har kvar att visa att $\mathrm{im}(\phi)$ är en undergrupp till $\mathcal{H}$. Klart är att $\mathbf{e}' \in \mathrm{im}(\phi)$ eftersom $\phi(\mathbf{e}) = \mathbf{e}'$. Lika klart är att $\phi(a)^{-1} \in \mathrm{im}(\phi)$ då $\phi(a)^{-1} = \phi(a^{-1}) \in \mathrm{im}(\phi)$. Dessutom: $\phi(a)\phi(b) = \phi(ab) \in \mathrm{im}(\phi)$. Beviset är klart. □

Analogt med mängdteoretiska avbildningar så har vi följande definition med en adderad detalj.

Definition 12. Låt $\mathcal{G} \xrightarrow{\phi} \mathcal{H}$ vara en homomorfi av grupper. Då säger man att

- ϕ är en **surjektion**, eller **surjektiv**, om $\mathrm{im}(\phi) = \mathcal{H}$;
- ϕ är en **injektion**, eller **injektiv**, om $\ker(\phi) = \mathbf{e}$, och
- ϕ är en **isomorfi** om den är bijektiv (d v s, både injektiv och surjektiv). Man säger då att $\mathcal{G}$ och $\mathcal{H}$ är **isomorfa** och man skriver det som $\mathcal{G} \cong \mathcal{H}$.

Det lönar sig att analysera denna definition lite mer.

Det är tämligen klart vad det innebär att ϕ är surjektiv: För varje element $h \in \mathcal{H}$ finns (minst) ett element $g \in \mathcal{G}$ så att $\phi(g) = h$. Intuitivt kan man se det som om $\mathcal{G}$ är "större" än $\mathcal{H}$, även om alla intuitiva idéer har allvarliga begränsningar.

Att $\ker(\phi) = \mathbf{e}$ är ekvivalent med den vanliga (mängdteoretiska) definitionen på injektivitet: ϕ är injektiv om (och endast om) $\phi(a) = \phi(b)$ medför att $a = b$. Hur ser man detta? Antag först att, $\ker(\phi) = \mathbf{e}$ och anta att $\phi(a) = \phi(b)$. Detta är ekvivalent med $f(ab^{-1}) = \mathbf{e}$, så enligt förutsättningen är då $ab^{-1} = \mathbf{e} \Leftrightarrow a = b$. Om nu $\phi(a) = \phi(b)$ medför att $a = b$ så är $a \in \ker(\phi) \Leftrightarrow \phi(a) = \mathbf{e} = \phi(\mathbf{e})$ så $a = \mathbf{e}$ enligt förutsättningen.

En injektiv avbildning (även mängdteoretisk) kallas ofta för “ett-till-ett” (eng. ’one-to-one’). Surjektioner har ett motsvarande uttryck på engelska, “onto”, men jag känner inte till någon svensk version av detta.

Vad betyder det nu att ϕ är en isomorfi? Varje element i $\mathcal{H}$ ha en partner i $\mathcal{G}$ (surjektivitet) och det finns **precis** en partner. Det betyder att, om vi tänker elementvis, det finns lika många element i $\mathcal{G}$ som i $\mathcal{H}$ (även om det är oändligt många). Dessutom säger homomorfi-egenskapen $\phi(ab) = \phi(a)\phi(b)$ att gruppstrukturerna på $\mathcal{G}$ och $\mathcal{H}$ är kompatibla, man kan t o m betrakta de som lika. Så, som grupper, är isomorfa grupper att betrakta som om de vore väsentligen samma grupp!

Dra er nu till minnes Meta-sats 7.6. Där påstod jag att alla cykliska grupper var väsentligen av två typer. Detta kan nu göras fullständigt korrekt till en sats genom att formulera det som:

Sats 9.2 (Korrektion)**.** Varje cyklisk grupp $\mathcal{C}$ är isomorf med en av följande grupper:

(i) $\mathbb{Z}$, om $\mathcal{C}$ har oändlig ordning;
(ii) $\mathbb{Z}_n$, om $\mathcal{C}$ har ändlig ordning n.

Bevis. Nu är denna sats enkel att bevisa:

(i) Låt $\mathcal{C} = \langle a \rangle$ vara en cyklisk grupp av oändlig ordning genererad av $a \in \mathcal{C}$. Definiera en avbildning $\mathcal{C} \xrightarrow{\mathbb{Z}}$: $\phi(g) = \phi(a^m) := m \in \mathbb{Z}$. Detta är en homomorfi: $\phi(a^n a^m) = \phi(a^{n+m}) = n + m = \phi(a^n) + \phi(a^m)$. Det är också en bijektion, ty: för varje $n \in \mathbb{Z}$ finns ett element $a^n \in \mathcal{C}$ så att $\phi(a^n) = n$, och om $\phi(a^n) = 0$ (tänk på att 0 är enhetselementet i $\mathbb{Z}$) så måste $n = 0$. Alltså är ϕ en homomorfi och bijektion, med andra ord, en isomorfi.
(ii) Denna del bevisas på samma sätt, men nu är $\phi(a^m) := [m]$, resten med division med n. Jag lämnar till er att fylla i detaljerna. □

På samma sätt kan Sats 7.10 korrigeras till en korrekt version:

Sats 9.3 (Korrektion)**.** Låt $\mathcal{G} = \mathbb{Z}_n$ och $\mathcal{H} = \mathbb{Z}_m$. Då är $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ om och endast om $\gcd(n, m) = 1$.

Så denna sats säger att $\mathbb{Z}_n \times \mathbb{Z}_m$ och $\mathbb{Z}_{nm}$ har samma gruppstruktur även om de ser annorlunda vid en första anblick; som grupper är de lika.

Exempel 9.2. Grupperna $\mathbb{Z}_n$ och $\mathbb{Z}_m$ är isomorfa om och endast om $n = m$ (annars har de olika antal element).

Exempel 9.3. Vi har $\mathbb{U}_n \cong \mathbb{Z}_n$. Nämligen, definiera en avbildning $\phi : \mathbb{U}_n \to \mathbb{Z}_n$ genom $\mathrm{e}^{i\frac{2\pi\ell}{n}} \mapsto (\ell \mod n)$.

Övning 9.4. Visa att ϕ är en isomorfi.

Exempel 9.5. Tidigare såg vi att $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ är en homomorfi. Men det är t o m en isomorfi: varje element $r \in \mathbb{R}^{>0}$ kan fås som bilden av ett element i $\mathbb{R}$, nämligen $\ln(r)$, så exp är surjektiv. Att den är injektiv följer av att om $\exp(a) = \exp(b) \Leftrightarrow \mathrm{e}^a = \mathrm{e}^b \Leftrightarrow \mathrm{e}^{a-b} = 1 \Leftrightarrow a - b = 0$, där den sista ekvivalensen följer av att $\mathrm{e}^a = 1$ om och endast om $a = 0$.

Notera att detta exemplet är ganska överraskande: här har vi två grupper som till synes har olika gruppstrukturer, som trots allt är “lika”!

Exempel 9.6. Tvärtemot föregående exempel har vi $(\mathbb{Q},+) \ncong (\mathbb{Q}^{>0},\cdot)$. Det finns inte ens någon homomorfi mellan dessa grupper. Antag att det funnes en sådan ϕ. Då skulle vi ha att

$$\phi(a) = \phi(a/2 + a/2) = \phi(a/2)\phi(a/2) = \phi(a/2)^2$$

och om välj a så att $\phi(a) = 2$ får man $2 = \phi(1)^2$ och det enda tal $\phi(1)$ som uppfyller detta är $\sqrt{2}$ vilket inte är ett rationellt tal. Alltså får vi en motsägelse.

10. Kvotgrupper, första isomorfisatsen

Som sista del i denna gruppteoretiska odyssée ska vi införa en gruppstruktur på mängden av alla sidoklasser till en normal undergrupp. I samband med detta kommer jag att visa en oerhört användbar sats som sammankopplar sidoklasser och homomorfier.

Definition-Sats 10.1. Låt $\mathcal{H}$ vara en **normal** undergrupp till $\mathcal{G}$. Bilda mängden

$$\mathcal{G}/\mathcal{H} := \{a\mathcal{H} \mid a \in \mathcal{G}\},$$

d v s mängden av all sidoklasser. Detta är en grupp under multiplikation inducerad från $\mathcal{G}$:

$$(a\mathcal{H})(b\mathcal{H}) := ab\mathcal{H}.$$

Denna multiplikation är väl-definierad eftersom $\mathcal{H}$ är normal. Dessutom är $\mathbf{e}\mathcal{H} = \mathcal{H}$ enhetselementet i denna grupp och inversen till $a\mathcal{H}$ är $a^{-1}\mathcal{H}$. Gruppen $\mathcal{G}/\mathcal{H}$ som bildas här kallas för **kvotgruppen** (eller **faktorgruppen**) **av** $\mathcal{G}$ **modulo** $\mathcal{H}$.

Bevis. Det enda som egentligen behöver kontrolleras här är att multiplikationen är väl-definierad. Men detta följer av att

$$(a\mathcal{H})(b\mathcal{H}) = a(\mathcal{H}b)\mathcal{H} = ab\mathcal{H}\mathcal{H} = ab\mathcal{H}$$

eftersom $\mathcal{H}$ var en normal undergrupp. Resten av beviset är uppenbart och lämnas till er. □

Man kan fråga sig vad meningen är med att bilda kvotgrupper. För att ge ett kort svar på den frågan låt mig säga så här: Observera att satsen säger att i $\mathcal{G}/\mathcal{H}$ är $\mathcal{H}$ enhetselementet. Med andra ord tar vi från $\mathcal{G}$ en mängd element och sätter till "noll" (enhetselementen är ju "nollor" i grupper). Detta innebär att man får en förenklad version av $\mathcal{G}$ men som behåller mycket av $\mathcal{G}$'s struktur som grupp eftersom multiplikationen på $\mathcal{G}/\mathcal{H}$ är i princip lika den på $\mathcal{G}$.

Sats 10.2 (Första isomorfisatsen)**.** Låt $\phi : \mathcal{G} \to \mathcal{G}'$ vara en homomorfi mellan två grupper. Då faktorerar ϕ unikt genom $\mathcal{G}/\ker(\phi)$ och ϕ inducerar en isomorfi $\mathcal{G}/\ker(\phi) \cong \mathrm{im}(\phi)$.

Uppenbarligen måste jag föklara mig här! Vad betyder nu detta? Jag gör detta i punktform.

- Det första man bör göra är att komma ihåg att $\ker(\phi)$ är en normal undergrupp till $\mathcal{G}$ så att forma kvotgruppen $\mathcal{G}/\ker(\phi)$ är tillåtet.
- Det finns en kanonisk homomorfi $\mathcal{G} \to \mathcal{G}/\mathcal{H}$ för alla $\mathcal{G}$ och (normala) $\mathcal{H}$ givet av $\mathcal{G} \ni a \mapsto a\mathcal{H} \in \mathcal{G}/\mathcal{H}$. Det är lätt att kontrollera att detta är en homomorfi (gör det!). Detta brukar kallas för den **kanoniska projektionen** av $\mathcal{G}$ på $\mathcal{G}/\mathcal{H}$ och vi betecknar den med $\pi : \mathcal{G} \to \mathcal{G}/\mathcal{H}$.
- Låt nu $\mathcal{H} = \ker(\phi)$. Då har vi en homomorfi $\pi : \mathcal{G} \to \mathcal{G}/\ker(\phi)$.

- Definiera en avbildning $\phi_* : \mathcal{G}/\ker(\phi) \to \mathcal{G}'$ genom $\phi_*(a\ker(\phi)) := \phi(a) \in \mathcal{G}'$. Detta är en homomorfi (visa!).
- Men det är dessutom en isomorfi mellan grupperna $\mathcal{G}/\ker(\phi)$ och $\mathrm{im}(\phi)$, ty för varje $b \in \mathrm{im}(\phi)$ finns ett $a \in \mathcal{G}$ så att $\phi(a) = b$ och då finns $a\ker(\phi) \in \mathcal{G}/\ker(\phi)$ så att $\phi_*(a\ker(\phi)) = \phi(a) = b$ så ϕ_* är surjektiv. Att den är injektiv följer av att om $\phi_*(a\ker(\phi)) = \phi_*(b\ker(\phi))$ så är $\phi_*(ab^{-1}\ker(\phi)) = \mathbf{e}' \in \mathrm{im}(\phi) \subseteq \mathcal{G}'$ vilket betyder att $\phi(ab^{-1}) = \mathbf{e}'$ vilket i sin tur betyder att $ab^{-1} \in \ker(\phi)$, så a och b ligger i samma sidoklass och alltså är $a\ker(\phi) = b\ker(\phi)$.
- Att ϕ_* är unik är klart med tanke på hur den är definierad (den definierades ju genom ϕ).
- Vi har att $\phi = \phi_* \circ \pi$, och det är detta som "ϕ faktoriserar (unikt) genom $\mathcal{G}/\ker(\phi)$" betyder.

Nu har jag både förklarat och bevisat satsen!

Exempel 10.1. Låt $\phi : \mathcal{G} \to \mathcal{G}$ vara given som $\phi(g) := g$ (d v s, identitetshomomorfin). Då är $\ker(\phi) = \{\mathbf{e}\}$ och satsen säger då att $\mathcal{G}/\ker(\phi) = \mathcal{G}/\{\mathbf{e}\} \cong \mathcal{G}$. I det andra extremfallet, låt $\psi : \mathcal{G} \to \mathcal{G}$ vara given av $\psi(g) := \mathbf{e}$. Då är $\ker(\psi) = \mathcal{G}$ och $\mathcal{G}/\ker(\psi) = \mathcal{G}/\mathcal{G} \cong \{\mathbf{e}\}$.

Exempel 10.2. Studera homomorfin "reduktion modulo n" från förut: $\mathrm{red}_n : \mathbb{Z} \to \mathbb{Z}_n$. Det är lätt att inse att $\ker(\mathrm{red}_n) = \{a \in \mathbb{Z} \mid a = kn, k \in \mathbb{Z}\}$, d v s, alla tal som delas av n. Alltså säger satsen att $\mathbb{Z}/\ker(\mathrm{red}_n) \cong \mathrm{im}(\mathrm{red}_n) = \mathbb{Z}_n$. Här sätter man alltså alla multiplar av n till noll.

Exempel 10.3. Ta $\mathrm{pr}_1 : \mathcal{G} \times \mathcal{H} \to \mathcal{G}$. Då är $\ker(\mathrm{pr}_1) = \{\mathbf{e}\} \times \mathcal{H}$ och

$$\mathcal{G} \cong \mathcal{G} \times \mathcal{H}/(\{\mathbf{e}\} \times \mathcal{H})$$

enligt satsen. Vi "kvotar bort $\mathcal{H}$ från $\mathcal{G} \times \mathcal{H}$ och får kvar $\mathcal{G}$". Det är antagligen detta och liknande exempel som har givit namn åt kvotgrupper.

Exempel 10.4. Låt $\mathbf{R}$ vara $\mathbb{Q}$, $\mathbb{R}$ eller $\mathbb{C}$. Definiera en surjektiv homomorfi mellan $\mathrm{GL}_n(\mathbf{R})$ och $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$, genom att ta determinanten. Alltså,

$$\det : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^*, \quad A \mapsto \det(A) \in \mathbf{R}.$$

(Varför är detta en surjektiv homomorfi?) Kärnan till denna homomorfi är $\mathrm{SL}_n(\mathbf{R})$ så $\mathrm{SL}_n(\mathbf{R})$ är en normal undergrupp till $\mathrm{GL}_n(\mathbf{R})$. Första isomorfisatsen säger nu att

$$\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^*.$$

Notera att trots att både $\mathrm{GL}_n(\mathbf{R})$ och $\mathrm{SL}_n(\mathbf{R})$ är högst icke-abelska så är kvotgruppen abelsk. Så man skulle kunna säga att $\mathrm{SL}_n(\mathbf{R})$ skiljer sig från $\mathrm{GL}_n(\mathbf{R})$ bara med $\mathbf{R}^*$, för när man sätter $\mathrm{SL}_n(\mathbf{R})$ lika med "noll" så får man bara $\mathbf{R}^*$ kvar.

Övning 10.5. Om $\mathcal{G}$ är en ändlig grupp, hur många element har då $\mathcal{G}/\mathcal{H}$? Analysera fallet då $\mathcal{G}/\mathcal{H}$ cyklisk. Vad kan sägas om $\mathcal{G}$ och $\mathcal{H}$ då?