# Grublegruppe 19. sept. 2011: Algebra I

Ivar Staurseth
ivarsta@math.uio.no

## Innledning, definisjoner

Vi har så langt jobbet med mengder, $X$, hvor vi har hatt et avstandsbegrep og hvor vi har vært i stand til å drive matematisk analyse, dvs. studere konvergens av følger, kontinuitet av funksjoner osv. Vi begynte med $\mathbb{R}$, $\mathbb{R}^n$ og generaliserte teorien til generelle metriske rom.

Nå skal vi bevege oss inn i en annen del av matematikken, nemlig den *algebraiske*. Vi skal se på mengder hvor vi har en algebraisk struktur, dvs. hvor vi har en veldefinert idé om hvordan vi *legger sammen* elementer:

**Definisjon 1.** *La $G$ være en mengde. En binær operasjon på $G$ er en funksjon $\star : G \times G \to G$, som tar to elementer, $a, b \in G$ og returnerer et tredje element $\star(a, b) \in G$. Vi skriver gjerne $\star(a, b) = a \star b$.*

Eksempler på kjente binære operasjoner er addisjon og multiplikasjon av reelle tall. Eller av heltall. Eller av komplekse tall.

**Definisjon 2.** *En **gruppe** er et par $(G, \star)$, hvor $G$ er en mengde og $\star$ en binær operasjon på $G$, som oppfyller følgende:*

- *For alle $a, b, c \in G$ har vi: $a \star (b \star c) = (a \star b) \star c$ Det vil si at den binære operasjonen må være **assosiativ**.*
- *Det finnes et unikt element $e \in G$ slik at $e \star x = x \star e = x$ for alle $x \in G$ Vi kaller $e$ for **identitetselementet** i $G$.*
- *For alle $a \in G$ finnes et element $a'$ slik at $a \star a' = a' \star a = e$. $a'$ er det **inverse elementet** til $a$.*

Legg merke til at det ikke er noe krav om at den binære operasjonen skal være *kommutativ*, dvs. at $a \star b = b \star a$. Det er en ektra egenskap som av og til er tilfelle, og denne typen grupper har et eget navn:

**Definisjon 3.** *Vi sier at en gruppe $(G, \star)$ er en **abelsk gruppe** dersom den binære operasjonen er kommutativ, dvs. hvis $a \star b = b \star a$ for alle $a, b \in G$.*

.

**Eksempel 1.** $(R, +)$ *(De reelle tallene, under addisjon) er en gruppe. Her er identitetselementet* $0$ *(*$a + 0 = 0 + a = a$*) og den inverse til et tall* $x$ *er* $-x$ *(*$x + (-x) = 0$*)*

**Eksempel 2.** $(\mathbb{C}^*, \star)$ *(De komplekse tallene som er forskjellig fra 0, under multiplikasjon) er også en gruppe. Her er identiteten* $1$ *(*$1z = z1 = z$*) og den inverse til et tall* $z$ *er* $1/z$ *(*$z(1/z) = (1/z)z = 1$*)*

Litt notasjon: I mange tilfeller vil vi snakke om en gruppe $G$, uten å presisere hvilket symbol vi bruker for den binære operasjonen, dersom den er opplagt. Ofte vil vi skrive $a \star b$ som $ab$. Dere vil også se notasjonen $+$ brukt, også om andre binære operasjoner enn vanlig addisjon, men det er brudd på god matteskikk å bruke $+$ om binære operasjoner som ikke er kommutative. $1 + 4 \neq 4 + 1$ kan se unødvendig blasfemisk ut!

Dersom vi bruker *multiplikativ* notasjon, dvs. skriver $a \star b$ som $ab$ er det vanlig å bruke tallet 1 som symbol for identitetselementet og $a^{-1}$ for det inverse elementet til $a$ - selv om gruppen består av andre ting enn tall. Tilsvarende for additiv notasjon: 0 for identitetselementet og $-a$ for inverselement.

## Undergrupper

**Definisjon 4.** *La* $G$ *være en mengde,* $\star$ *en binær operasjon på* $G$ *og* $H \subset G$ *en delmengde av* $G$*. Vi sier at* $H$ *er lukket under den binære operasjonen* $\star$ *dersom vi for alle par av elementer* $x, y \in H$ *har at også* $x \star y \in H$

**Definisjon 5.** *La* $(G, \star)$ *være en gruppe. Dersom en delmengde* $H \subseteq G$ *er lukket under den binære operasjonen* $\star$*, og dersom* $H$*, sammen med denne binære operasjonen selv er en gruppe, sier vi at* $(H, \star)$ *er en* ***undergruppe*** *av* $(G, \star)$*. Vi skriver* $(H, \star) \leq (G, \star)$ *(Evt.* $(H, \star) < (G, \star)$ *dersom* $H \neq G$*)*

Faktisk er det tilfelle at:

**Teorem 1.** *En delmengde* $H$ *av en gruppe* $G$ *er en undergruppe av* $G$ *hvis og bare hvis:*

- $H$ *er lukket under den binære operasjonen til* $G$
- *identitetselementet* $e$ *til* $G$ *er med i* $H$
- *for alle* $a \in H$ *har vi at det inverse elementet* $a^{-1} \in H$

For eksempel: dersom vi studerer $\mathbb{Z}$, sammen med vanlig addisjon, vil delmengden som består av alle partallene være lukket under addisjon, mens odetallene ikke vil være lukket under addisjon

Enhver gruppe $G$ vil alltid ha minst to undergrupper, nemlig den **trivielle** undergruppen $\{e\} < G$ som bare består av identitetselementet, og den **uekte undergruppen** $G \leq G$ som består av $G$ selv.

Her er et par eksempler på grupper og undergrupper:

**Eksempel 3.** *La $\mathbb{C}^\star$ være gruppen av alle komplekse tall forskjellig fra null, under (vanlig) multplikasjon. Da er $U_n = \{z \in \mathbb{C} | z^n = 1$ (alle komplekse n-te-røtter av 1) en undergruppe av $\mathbb{C}^\star$.*

**Eksempel 4.** *$(\mathbb{Z}, +)$ er en undergruppe av $(\mathbb{R}, +)$*

**Definisjon 6.** *Dersom $(G, *)$ er en gruppe sier vi at den er av **orden** $n$ ($|G| = n$) dersom $G$ har $n$ elementer. Dersom $G$ har uendelig mange elementer, sier vi at den er av uendelig orden.*

## Funksjoner mellom grupper, homomorfier, isomorfier

Nå skal vi se litt på funksjoner mellom grupper. Først et par-tre-fire definisjoner:

**Definisjon 7.** *En funksjon $f : X \to Y$ er **injektiv**, eller en-til-en, dersom: for alle $x, y \in X$, med $x \neq y$, har vi at $f(x) \neq f(y)$. Eller ekvivalent: $f(x) = f(y) \implies x = y$. Det vil si at forskjellige elementer i $X$ sendes på forskjellige elementer i $Y$.*

Et eksempel på en injektiv funksjon fra $\mathbb{R}$ til $\mathbb{R}$ er $f(x) = x^3+1$ (hvorfor?), mens $f(x) = x^2$ ikke er injektiv. (Moteksempel: $-a \neq a$, men $f(-a) = f(a) = a^2$ )

**Definisjon 8.** *En funksjon $f : X \to Y$ er **surjektiv** dersom: for alle $y \in Y$ finnes (minst) en $x \in X$ slik at $f(x) = y$.*

Dersom funksjonen er både injektiv og surjektiv sier vi at den er **bijektiv** eller at den er en **bijeksjon**.

To andre begreper som er nyttige i forbindelse med funksjoner mellom grupper er **kjernen** og **bildet** til funksjonen:

**Definisjon 9.** *La $f : X \to Y$ være en funksjon mellom to grupper. Kjernen til avbildningen er mengden av alle elementer i $X$ som sendes på identitetselementet i $Y$, dvs: $ker(f) = \{x \in X | f(x) = e_Y\}$*

**Definisjon 10.** *La $f : X \to Y$ være en funksjon mellom to grupper. Bildet til avbildningen er definert ved: $im(f) = \{f(x)|x \in X\}$. Det vil si alle elementer i $Y$ som er på formen $f(x)$ for et element i $X$*

Funksjoner dukker opp i alle greiner av matematikk. Vi har funksjoner mellom metriske rom, funksjoner mellom topologiske rom og ikke overraskende: funksjoner mellom grupper. Alt dette er i bunn og grunn mengder, men vi har lagt litt forskjellig *struktur* på mengdene. I alle disse *kategoriene* (grupper, topologiske rom, vektorrom, metriske rom, ...) finnes det noen funksjoner som er penere enn andre - dvs. funksjoner som bevarer den strukturen vi har lagt på mengdene. Blant alle tenkelige avbildninger mellom metriske rom er de kontinuerlige funksjonene spesielt fine. Ett eksempel på det: hvis $f : X \to Y$ er kontinuerlig, $\{x_n\}$ en konvergent følge i $X$ med grense $x$, så vet vi at også følgen $\{f(x_n)\}$ konvergent i $Y$ - med grense $f(x)$. Kan det bli bedre?

Når vi jobber med grupper blir vi veldig glad hver gang vi støter på det vi kaller en *gruppehomomofri*, eller bare *homomorfi* på kortform:

**Definisjon 11.** *La $\phi : (G, \star) \to (H, \bullet)$ være en funksjon mellom gruppene $(G, \star)$ og $(H, \bullet)$. (Dvs. mellom mengdene $G$ og $H$). Vi sier at $\phi$ er en* ***gruppehomomorfi*** *dersom $\phi(a \star b) = \phi(a) \bullet \phi(b)$ for alle $a, b \in G$.*

Vi sier gjerne at gruppehomomorfiene *respekterer* den algebraiske strukturen. Om vi først multipliserer to elementer i $G$ (med $G$ sin binære operasjon), og deretter avbilder resultatet til $H$ med $\phi$, så får vi samme element som hvis vi først avbildet begge elementene til $H$ og deretter multipliserte dem i $H$ (med $H$ sin binære operasjon.) En gruppehomomorfi vil også sende identitetselement på identitetselement ( $\phi(e_G) = e_H$) og inverse elementer på inverse elementer ($\phi(a)^{-1} = \phi(a^{-1})$). (Dette får du anledning til å bevise i en av oppgavene)

**Eksempel 5.** *La $(\mathbb{R}, +)$ være gruppen av de reelle tallene med addisjon (identitetselement 0) og $(\mathbb{R}^\star, *)$ gruppen av ikke-null reelle tall med multiplikasjon (identitetselement 1). La $\phi : (\mathbb{R}, +) \to (\mathbb{R}^\star, *)$ være definert ved $\phi(x) = e^x$. Da er $\phi$ en gruppehomomorfi.*

**Bevis:** Vi må vise at $\phi(a + b) = \phi(a) * \phi(b)$ for alle $a, b \in (\mathbb{R}, +)$. Vi ser lett at $\phi(a + b) = e^{(a+b)} = e^a * e^b = \phi(a) * \phi(b)$.

Vi legger merke til at identitetselementet i $(\mathbb{R}, +)$, som er 0, sendes på identitetselementet i $(\mathbb{R}^\star, *)$, som er 1. ($\phi(0) = e^0 = 1$). Vi ser også at inverselementet til $\phi(a) = e^a$ er $\phi(-a) = e^{-a}$)

Nå skal vi se på en spesiell form for homomorfier, nemlig *isomorfier*:

**Definisjon 12.** *La $(S, *)$ og $(S', *')$ være to grupper, og $\phi : (S, *) \to (S', *')$ en funksjon mellom $S$ og $S'$. $\phi$ er en **isomorfi** dersom:*

- *$\phi$ er en bijeksjon mellom mengdene $S$ og $S'$ (Se definisjon 6 og 7)*
- *$\phi$ er en homomorfi: $\phi(x * y) = \phi(x) *' \phi(y)$ for alle $x, y \in S$*

Dersom det finnes en isomorfi mellom to grupper, $S$ og $S'$ sier vi at $S$ og $S'$ er *isomorfe*. Det skriver vi som $S \cong S'$. Isomorfi er et eksempel på en ekvivalensrelasjon. I gruppeteorien er det viktig å vite når to grupper er isomorfe. To isomorfe grupper er så like at en gruppeteoretiker ikke ser noen grunn til å skille mellom dem. For å illustrere dette kan vi tenke oss et helt banalt eksempel: Vi kan se på gruppen $\mathbb{Z}_{kjell}$ som består av elementene: $\{... - 2_{kjell}, -1_{kjell}, 0_{kjell}, 1_{kjell}, 2_{kjell}, ...\}$ sammen med addisjonen $a_{_{kjell}} +' b_{kjell} = (a + b)_{kjell}$

Det er opplagt at gruppen $(\mathbb{Z}_{kjell}, +')$ er isomorf med $(\mathbb{Z}, +)$. Det finnes en bijeksjon $n_{kjell} \leftrightarrow n$ begge veier, som bevarer den algebraiske strukturen i begge gruppene. Å gi alle heltallene etternavnet (?) Kjell tilfører ikke gruppen noe nytt, vi har i realiteten å gjøre med samme gruppe. Det er også tilfelle hvis isomorfien ikke er like opplagt:

**Eksempel 6.** *La $U_n = \{e^{i0}, e^{i\frac{\pi}{2}}, e^{i\pi}, e^{i\frac{3\pi}{2}}\}$ være gruppen av alle de komplekse 4.-røttene til 1, sammen med vanlig multiplikasjon av komplekse tall. La $\mathbb{Z}_4$ være den additive gruppen av heltall, modulo 4. (Dvs. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ og $a + b = r$ hvor $r$ er resten du får i divisjonen $(a + b)/4$.)*

*Da er $(U_n, *) \cong (\mathbb{Z}_4, +)$ ved isomorfien $f : (\mathbb{Z}_4, +) \to (U_n, *)$, hvor $f(n) = e^{i\frac{n\pi}{2}}$.*

I gruppe-verden er dette to forskjellige måter å skrive én og samme gruppe på - nemlig den sykliske gruppen av orden 4. Slektskapet er like nært som mellom $\mathbb{Z}$ og $\mathbb{Z}_{kjell}$, selv om både elementene og den binære operasjonen er temmelig forskjellig i dette siste eksempelet.

## Oppgaver

**Oppgave 1.** *Avgjør om den binære operasjonen $*$ gir en gruppestruktur på de oppgitte mengdene:*

1. $\mathbb{Z}$ *med* $a * b = ab$ *(vanlig multiplikasjon)*
2. $7\mathbb{Z} = \{7n | n \in \mathbb{Z}\} = \{..., -21, -14, -7, 0, 7, 14, 21, ...\}$ *med* $a * b = a + b$ *(vanlig addisjon)*
3. $\mathbb{R}^+$ *(positive reelle tal) med* $a * b = \sqrt{ab}$
4. $\mathbb{Q}$ *med* $a * b = ab$
5. $\mathbb{R}^*$ *(reelle tall, forskjellig fra 0) med* $a * b = a/b$
6. $\mathbb{C}$ *med* $a * b = |ab|$

**Oppgave 2.** *Vis at definisjonen av en undergruppe (Definisjon 5 s. 2) medfører at Teorem 1 (samme side) er riktig.*

**Oppgave 3.** *Forklar hvorfor mengden av alle oddetall, $\{2n - 1 | n \in \mathbb{Z}\}$, ikke er en undergruppe av $(\mathbb{Z}, +)$.*

**Oppgave 4.** *La $(\mathbb{C}, +)$ være gruppen av komplekse tall, under addisjon. Avgjør hvilke av følgende delmengder av $\mathbb{C}$ som er en undergruppe av $(\mathbb{C}, +)$.*

1. $\mathbb{R}$
2. $\mathbb{Q}^+$ *(positive rasjonale tall)*
3. $i\mathbb{R} = \{ix | x \in \mathbb{R}\}$ *(rent imaginære tall, inklusiv 0)*
4. $5\mathbb{Z} = \{5n | n \in \mathbb{Z}\} = \{..., -15, -10, -5, 0, 5, 10, 15, ...\}$
5. $\pi\mathbb{Q} = \{q\pi | q \in \mathbb{Q}\}$ *(rasjonale multipler av $\pi$)*
6. $\{\pi^n | n \in \mathbb{Z}\}$

**Oppgave 5.** *Hvilke av delmengdene 1-6 i forrige oppgave er undergrupper av $(\mathbb{C}^*, \star)$ (komplekse tall, forskjellig fra 0, under multiplikasjon)?*

**Oppgave 6.** *Legg læreboka foran deg på pulten og se på mengden av rotasjoner av læreboka (plasser et tredimensjonalt koordinatsystem med origo midt i boka (midt på midterste side) og se på rotasjoner på 90, 180, 270 og 360 grader rundt hver av aksene, samt speiling om diagonalene. Definer en binær operasjon på mengden ved å la komposisjonen av to rotasjoner, $\rho_i\rho_j$ være rotasjonen hvor du først utfører $\rho_i$ og deretter $\rho_j$. La $\rho_0$ være identiteten, dvs. rotasjonen som ikke gjør noen verdens ting. Greier du å lage en gruppe av rotasjoner? I så fall: er den abelsk??*

**Oppgave 7.** *Se på definisjon 10 (s. 4) av en gruppehomomorfi. La $\phi : (G, +) \to (H, \star)$ være en homomorfi mellom grupper. La $e_G$ være identitetselementet i $G$ og $e_H$ identitetselementet i $H$. Vis at $\phi(e_G) = e_H$. La $-a$ betegne inverselementet til $a \in G$ og la $h^{-1}$ betegne inverselementet til $h \in H$. Vis at hvis $\phi(g) = h$ så må $\phi(-a) = h^{-1}$.*

**Oppgave 8.** *Dersom $(G, *)$ er en gruppe, $a \in G$ et element i $G$ lar vi $a^n$ være definert ved: $a^n = a * a * ... * a$ ($n$ ganger), $a^0 = e$ og $a^{-m} = a^{-1} * a^{-1} * ... * a^{-1}$ ($m$ ganger) (NB! Vi bruker denne notasjonen, også om den binære operasjonen er vanlig addisjon. Dvs. at i gruppen $(\mathbb{Z}, +)$ er $5^3 = 5 + 5 + 5 = 15$).*

1. *La $a$ være et element i en gruppe $(G, *)$ og la $\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$. Vis at $\langle a\rangle$ er en undergruppe av $(G, *)$. Vis at $\langle a\rangle$ er den **minste** undergruppen av $G$ som inneholder $a$.*

2. *Vis at dersom $\langle a\rangle$ er av uendelig orden, må $\langle a\rangle \cong (\mathbb{Z}, +)$.*

3. *Vis at dersom $\langle a\rangle$ er av orden $n$ må $\langle a\rangle$ være på formen $\{e, a, a^2, ..., a^{n-1}\}$, hvor $a^n = e$. Vis deretter at $\langle a\rangle$ i så fall er isomorf med $(\mathbb{Z}_n, +_n)$, hvor $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ og $+_n$ er addisjon, modulo $n$. Dvs. at $a +_n b = r$, hvor $r$ er resten du får (det du ikke får delt) når du forsøker deg på divisjonen $(a + b)/n$.*

*(Under-)grupper som er generert av ett element på denne måten kalles sykliske. De sykliske gruppene er enten endelige (og isomorfe med $(\mathbb{Z}_n, +_n)$) eller uendelige (og isomorfe med $(\mathbb{Z}, +)$)*

**Oppgave 9.** *La $\phi : G \to G'$ være en* ***isomorfi*** *mellom gruppene $(G, *)$ $(G', *')$.*

1. *Hvis at dersom $H$ er en undergruppe av $G$ så må $H' = \phi[H] = \{\phi(g) \in G' | g \in G\}$ være en undergruppe av $G'$*

2. *Hvis at dersom $G$ er en syklisk gruppe, generert av ett element, dvs. $G = \{g^n | n \in Z\}$ (se oppgave 8), så må også $G'$ være syklisk.*