MAT1100 - Grublegruppen
Notat 9

Jørgen O. Lye

Gruppeteori

Oppvarmingseksempel

La oss som vanlig ta en historisk vinkling. En klassisk måte grupper (som jeg straks skal definere) oppstod er gjennom å lete etter symmetrier. Tenk deg en trekant med alle vinklene 60°. La hjørnene hete v_1, v_2 og v_3, numerert fra venstre hjørne og mot klokken. Hva kan du gjøre med trekanten uten at den endrer seg etterpå? Du kan tenke deg at du roterer alle hjørnene 60°, f.eks. mot klokken. Da vil hjørnene ha byttet plass, men trekanten ser lik ut. La oss kalle denne operasjonen for ρ, for rotasjon. Hvis man skriver hjørnene som en tuppel (v_1, v_2, v_3) kan man si at ρ gjør følgende med denne tuppelen:

$$(v_1, v_2, v_3) \xrightarrow{\rho} (v_3, v_1, v_2)$$

Du kan like godt rotere mer, og totalt ha rotert 120°. Dette er jo klart det samme som å rotere 60° 2 ganger, dvs anvende ρ to ganger. Vi kaller da denne operasjonen $\rho^2 = \rho\rho$. Vi skriver

$$(v_1, v_2, v_3) \xrightarrow{\rho^2} (v_2, v_3, v_1)$$

Hvis man roterer enda en gang er man tilbake der man startet. Dvs $\rho^3 = e$, hvor med e mener jeg operasjonen hvor man ikke gjør noe.[1] Hva annet kan vi gjøre med trekanten? Vel, hvis man tenker seg en linjen som går fra hjørnet på toppen og står normalt på grunnflaten, så kan man speile om denne. La oss kalle denne for μ_3, hvor μ står for "mirror". På samme måte har man en linje fra det venstre hjørnet som står normalt på motstående side. La oss

[1] Man kunne vært filosof og stilt spørsmålet om "operasjonen som ikke gjør noe" er en operasjon, men vi dropper det. På samme måte som det viser seg å være lurt å tillate å legge til 0 viser det seg å være lurt å tillate e.

kalle denne μ_1. Den siste linjen man kan trekke er fra det høyre hjørnet til den motstående siden, og denne kaller vi μ_2. Nøyaktig nummerering på μ kan egentlig velges fritt. Det er kanske klart at om man speiler 2 ganger om den samme linjen så har man netto gjort ingenting. Med symboler: $\mu_i^2 = e$ for $i = 1, 2, 3$. Hva skjer om man blander? Dvs først bruker μ_1, så μ_2? Altså hva er $\mu_2\mu_1$? Merk rekkefølgen jeg har skrevet dem opp i! Det som skjer først er lengst til høyre. La oss se hva som skjer med hjørnene. Jeg påstår at følgende skjer:

$$(v_1, v_2, v_3) \xrightarrow{\mu_1} ((v_1, v_3, v_2) \xrightarrow{\mu_2} (v_2, v_3, v_1)$$

Kombinert har vi da at $(v_1, v_2, v_3) \to (v_2, v_3, v_1)$. Med andre ord det samme som ρ^2 gjør! Vi har altså at $\mu_2\mu_1 = \rho^2$. 2 rotasjoner gav en rotasjon, men 2 speilinger gir det samme som en rotasjon med 120°.

Hva om vi speiler motsatt vei? Dvs først μ_2, så μ_1? Det kan være en grubleoppgave å vise at $\mu_1\mu_2 = \rho \neq \rho^2 = \mu_2\mu_1$. Vi har altså vist at

$$\mu_1\mu_2 \neq \mu_2\mu_1$$

Man kan leke seg med de andre muligheten, dvs blande inn μ_3, rotasjoner og speilinger, osv. Hvis man vil kan man lage seg en tabell over alle mulighetene. De vi sakte med sikkert har gjort her er å liksom glemme trekanten litt og heller konsentrere oss om hvordan symmetriene dens virker seg imellom. Det er kanskje på tide med den abstrakte definisjonen av en gruppe.

Abstrakt definisjon

Med en gruppe skal vi mene en menge G med et product $*$ som tilfredsstiller følgende:

- $g_1, g_2 \in G \implies g_1 * g_2 \in G$
- $\exists\, e \in G$ slik at $e * g = g * e = g \;\forall\, g \in G$
- $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
- $g \in G \implies g^{-1} \in G$ hvor $g * g^{-1} = g^{-1} * g = e$

Punkt 1 kunne man også ha skrevet $* : G \times G \to G$ om man ville. Merk også at vi ikke krever $g_1 * g_2 = g_2 * g_1$. Grupper som tilfredsstiller dette kalles abelske grupper (abelian groups).

Noen eksempler på grupper

Det trivielle tilfellet

Gruppen $G = \{e\}$ er en gruppe med bare 1 element. Den tilfredsstiller aksiomene, men er også veldig kjedelig.

$\mathbb{Z}, +$

Mengden er heltallene $\mathbb{Z}$, og operasjonen $*$ er $+$. Da kan man sjekke at dette er en gruppe, hvor $g^{-1} = -g$ og $e = 0$. Denne gruppen er abelsk.

$\mathbb{R}$ eller $\mathbb{C}, +$

De reelle eller de komplekse tallene med operasjonen $+$ er også en gruppe på helt samme måte som $\mathbb{Z}$. Disse er også abelske grupper.

$\mathbb{R}^*$ eller $\mathbb{C}^*, \cdot$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, dvs alle reelle tall bortsett fra 0. På samme måte med $\mathbb{C}^*$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Operasjonen her er nå multiplikasjon, og $g^{-1} = \frac{1}{g}$. $e = 1$. Merk at denne mengden ikke er en gruppe når man bruker $+$ istedenfor multiplikasjon.

$\mathbb{S}^1, \cdot$

Enhetssirkelen, tenkt på som å ligge inni $\mathbb{C}$ kan skrives som

$$\mathbb{S} = \{z \in \mathbb{C} \big| |z| = 1\}$$

dvs $z = e^{i\theta}$. Identitetselementet er ennå 1 og man multipliserer sammen elementer som man vanligvis gjør for komplekse tall: $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$.

$\mathbb{Z}_2, +$

La $\mathbb{Z}_2 = \{0, 1\}$ og adder modulo 2. Dvs $0 + 0 = 0$, $1 + 0 = 1$, $1 + 1 = 0$. Da er dette en abelsk gruppe.

$\mathbb{Z}_n, +$

Generaliseringen av tilfellet over. Nå er $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ og addisjonen foregår modulo n. I praksis betyr dette at du legger sammen tall som vanlig. Hvis du er over n totalt, trekk fra n til du er mellom 0 og n igjen.

Matrisegrupper

Den store gruppen er

$$GL(n, \mathbb{K}) = \{n \times n \text{ inverterbare matriser med koeffisienter i } \mathbb{K}\}$$

Vi skal se på disse i neste notat. Denne gruppen har en rekke undergrupper (definisjon under) som vi er interessert i. $\mathbb{K}$ er som før enten $\mathbb{R}$ eller $\mathbb{C}$. Det er disse som er typiske eksempler på Lie-grupper. Lie-grupper defineres nok helt til slutt.

Litt mer formelle ting

Hvis man har 2 grupper G og H, så kaller man en avbildning mellom dem $\phi : G \to H$ en homomorfi dersom

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$

Denne ligningen sier at hvis man vil regne ut operasjonen mellom 2 elementer kan man enten regne dem ut i G, så så sende bort til H, eller man kan sende hvert element bort, så regner man ut operasjonen i denne nye gruppen.

På denne måten kalles homomorfier strukturbevarende; man tenker på en gruppe som en mengde med ekstra struktur, nemlig at gruppeaksiomene er oppfylt. Det er 2 konsekvenser av definisjonen av en homomorfi som det kan være greit å merke seg, og som man klarer å vise med bare de betingelsene jeg har skrevet ned for grupper:

$$\phi(e_G) = e_H$$
$$\phi(g^{-1}) = \phi(g)^{-1}$$

Eksempler på homomorfier

De trivielle

Trivielt er alltid $id : G \to G$, dvs avbildningen som ikke gjør noe en homomorfi. Omtrent like trivielt er $\phi : G \to H$ gitt ved $\phi(g) = e_H$ for alle g. Dvs en avbildning som sender alt til ett element.

Inklusjon

Hvis $H \subset G$ som mengder og de har "lik" gruppestruktur så kan man sende den lille inn i den store. Eksempler er:

$$\mathbb{R}^+ \to \mathbb{R}^*$$
$$\mathbb{S}^1 \to \mathbb{C}^*$$

Ting som ikke er homomorfier

Man kan ikke generelt bruke inklusjon dersom gruppene har forskjellig produkt:

$$\mathbb{R}^* \to \mathbb{R}$$

og

$$\mathbb{C}^* \to \mathbb{C}$$

er ikke homomorfier når venstresiden har multiplikasjon som sitt produkt og høyresiden har addisjon. Dette utsagnet er nøyaktig like dypt som å si at $a + b \neq a \cdot b$. generelt.

Videre er ikke $\phi_a(x) = x + a$ en homomorfi fra $\mathbb{R}$ til $\mathbb{R}$ med mindre $a = 0$. Bare se hva som skjer med 0: $\phi_a(0) = 0 + a = a \neq 0$.

På samme måte er ikke $\phi_a(x) = ax$ en homomorfi fra $\mathbb{R}^*$ til $\mathbb{R}^*$ med multiplikasjon. Den er derimot en homomorfi fra $\mathbb{R}$ til $\mathbb{R}$ med addisjon.

Isomorfier

Man har et begrep om når 2 grupper er like, og det er som følger. G er "lik" H dersom det finnes en homomorfi $\phi : G \to H$ slik at ϕ^{-1} finnes, og som er slik at $\phi^{-1} : H \to G$ er en homomorfi. Man skriver da at $G \cong H$. Av og til skriver folk $G = H$, men det er litt misvisende.

Sagt med ord så er ϕ en 1-1 avbildning mellom gruppene som mengder som også bevarer gruppestrukturen.

Det trivielle eksempelet er $id : G \to G$.

Merk at ϕ er en injektiv homomorfi hvis og bare hvis det eneste den sender til identitet er e. Dvs $\phi(g) = e_H$ betyr at $g = e_G$. Dette kan man vise med de regnereglene vi har for homomorfier, og overlates derfor til timen eller som grubleoppgave.

Småtrivielt eksempel

Gruppen bestående av 2 elementer $\mathbb{Z}_2$ kunne det tenkes at man ikke hadde tenkt på som 0 og 1, men som $\mathbb{Z}_2 = \{a, b\}$ og med regnereglene $a * a = a$, $a * b = b$, $b * b = a$. Da ville denne gruppen vært isomorf med $\mathbb{Z}_2 = \{0, 1\}$ ved å bare skifte navn på ting.

Mindre trivielt eksempel

La $\mu_2 = \{-1, +1\}$ med operasjon multiplikasjon. Da påstår jeg at $\mu_2 \cong \mathbb{Z}_2$. For å se dette, la $\phi : \mathbb{Z}_2 \to \mu_2$ være gitt ved at $\phi(0) = 1$, $\phi(1) = -1$. Da kan

man sjekke at dette er en homomorfi med invers som også er en homomorfi.

Ikke-trivielt eksempel

Påstanden er at $\mathbb{R}$ med addisjon er isomorf med $\mathbb{R}^+$ med multiplikasjon. Avbildningen er nemlig ekpsonensialavbildningen!

$$\exp : \mathbb{R} \to \mathbb{R}^+$$

Denne er gitt som vanlig: $\exp(a) = e^a$. Dette er en homomorfi fordi

$$\exp(a+b) = \exp(a)\exp(b)$$

Dvs man tar $\mathbb{R}$ sin additive struktur og gjør om til multiplikativ struktur!

Hva med inversen? $\ln : \mathbb{R}^+ \to \mathbb{R}$ er også klart en homomorfi, siden

$$\ln(a \cdot b) = \ln(a) + \ln(b)$$

Den generelle påstanden min over om at $\phi(g^{-1}) = \phi(g)^{-1}$ stemmer også her:

$$\ln\left(\frac{1}{a}\right) = -\ln(a)$$

Dette er et godt eksempel på hvorfor man ikke burde skrive $G = H$ om isomorfe grupper. $\mathbb{R} \cong \mathbb{R}^+$, men de reelle tallene er ikke lik de positive reelle tallene.

Fungerer ikke for $\mathbb{C}$

Man kunne tro at eksempelet over også holder for $\mathbb{C}$, men dessverre ikke. Det er klart at

$$\exp : \mathbb{C} \to \mathbb{C}^*$$

er en homomorfi, men den har ikke en invers, siden den ikke er injektiv:

$$\exp(z + 2i\pi) = \exp(z)$$

men $z \neq z + 2\pi i$.

Produkter av grupper

Hvis G og H er 2 grupper (de trenger ikke være relaterte på noen måte), så definerer vi produktet av dem $G \times H$ som det vanlige kartesiske produktet

av mengdene med produkt som bare er de gamle produktene i hver faktor. Her er hva jeg mener:

$$G \times H = \{(g,h) \big| g \in G, h \in H\}$$

med produktet

$$(g_1, h_1) *_{G\times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

Merk at identitetselementet i $G \times H$ er bare $e_{G\times H} = (e_G, e_H)$. Man kan godt sjekke at $G \times H$ blir en gruppe på denne måten. Hvis man har flere grupper $G_1, \cdots G_n$ så gjentar man bare denne konstruksjonen:

$$G_1 \times \cdots G_n = \{(g_1, \cdots g_n) \big| g_i \in G_i\}$$

hvor produktet ennå er komponentvis de gamle produktene.

Gruppene G og H kan man naturlig tenke på som undergrupper i $G \times H$ ved å si at $G \cong G \times \{e\}$ og $H \cong \{e\} \times H$.

Eksempler på produkter

Det letteste eksempelet er $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Da er addisjon definert komponentvis nøyaktig slik den er for vektorer. På samme måte med $\mathbb{R}^n$.

Et litt mindre kjent eksempel er $\mathbb{R}^* \times \mathbb{R}^*$. Da er

$$(x_1, y_1) * (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2)$$

Man kan også ta produkter når produktene "ikke matcher": $\mathbb{R}^* \times \mathbb{R}$ er helt fint, med "produkt"

$$(x_1, y_1) * (x_2, y_2) = (x_1 \cdot x_2, y_1 + y_2)$$

Det man leser av dette er produkter av grupper behandler hver faktor som uavhengig.

Det er generelt sett sant at $G \times H \cong H \times G$, selv om $G \times H \neq H \times G$ som mengder.

En liten oppgave

La oss se litt på 2 grupper som har 4 elementer hver. $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ og $H = \mathbb{Z}_4$. Er disse isomorfe? Hvis man skriver opp en tabell som sier hva alle elementene gjør med hverandre, dvs finner ut av hva som skjer med alle par $a * b$ i hver gruppe, så kan man svare på dette spørsmålet mer eller mindre gjennom "brute force". Det finnes andre måter å avgjøre dette, som er nødvendige når gruppene har flere elementer.

Undergrupper og Kvotientgrupper

Undergrupper

Hvis G og H er grupper, så kalles H en undergruppe dersom det finnes en injektiv $\phi : H \to G$ som er en homomorfi. Det man skal tenke på dette som er at H ligger inni G (noe den typisk gjør), og H har samme gruppestruktur som G. Eksempler er at $\mathbb{Z}$ med addisjon er en undergruppe av $\mathbb{Q}$ med addisjon, som er en undergruppe av $\mathbb{R}$ med addisjon, som til slutt er en undergruppe av $\mathbb{C}$ med addisjon. Andre eksempler er at $\mathbb{S}^1$ er en undergruppe av $\mathbb{C}^*$, og at $\mathbb{R}^+$ er en undergruppe av $\mathbb{R}^*$.

Normale undergrupper

En undergruppe N kalles normal dersom for alle $g \in G$ og alle $n \in N$, så er $g * n * g^{-1} \in N$. Dette kan se litt rart ut, og man kan i første omgang tenke på det som en teknisk ting for å få neste punkt til å gå opp. Merk at det ikke kreves $g * n * g^{-1} = n$. Dette vil være tilfellet om G er abelsk, men ikke generelt. Så for abelske grupper så er alle undergrupper normale, men ikke generelt sett ellers.

Hvis N er en faktor i gruppen G, f.eks hvis G kan skrives som $N \times H$ for en eller annen gruppe H så er H normal. Dette skyldes rett og slett at i det tilfellet så er

$$g^{-1} * n * g = (n_g^{-1}, h_g^{-1}) * (n, e) * (n_g, h_g) = (n_g^{-1} * n * n_g, e)$$

som klart må være med i N, siden N er en gruppe. Tenk litt på dette utsagnet om det ikke er klart.

Kvotientgrupper

Nå skrus abstraksjonsnivået opp et hakk. Anta $H \subset G$ er en normal undergruppe. Velg en $g \in G$. Dens venstre coset (sideklasse kanskje? Vanligvis sier man bare coset) er mengden $gN = \{g * n \big| n \in N\}$. Da er vi klare for kvotientgrupper. Uformelt sett skal vi med G/H mene "G men hvor vi ignorerer ting fra H". Formelt sett er elementene i G/H ekvivalensklasser av cosetene. Dvs man tenker på hele mengden gN som ett punkt. Gruppeoperasjonen er den fra G, "modulo H". Vi kommer ikke til å bruke disse så mye fremover, så hvis dette faller tungt kan man la være å bekymre seg mer over det. La oss se på noen eksempler på kvotienter til slutt.

Eksempler på G/H

Den greieste måten å få intuisjon med slike grupper er å la $\mathbb{Z}$ være G, og $n\mathbb{Z} = \{nx \big| x \in \mathbb{Z}\}$ være H. Da vil nemlig $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Det er jo en ikke så verst regel!

Andre eksempler er at $G/G = \{e\}$, $G/\{e\} = G$. Et annet eksempel er at $\mathbb{R}^*/\mu_2 = \mathbb{R}^+$.

Hvis, som over $G = N \times H$, så vil $G/N = H$. Det er jo heller ikke så verst å huske.

exp og $\mathbb{C}$

Dette er et vanskelig eksempel. Vi så over at

$$\exp : \mathbb{C} \to \mathbb{C}^*$$

ikke var injektiv. Den sendte nemlig hele $2\pi i\mathbb{Z} = \{2\pi in \big| n \in \mathbb{Z}\}$ til 1. Men dersom man identifiserer hele $2\pi i\mathbb{Z}$ med ett punkt, så sender exp bare ett punkt til 1, og den blir injektiv. Påstanden er altså at

$$\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^*$$

Man kan prøve å gruble litt på dette, men det krever sannsynligvis litt trening i abstrakt algebra for å bli komfortabel med resonnementet over.

Topologisk sett kan man prøve å overbevise seg (ved visuell resonnering) om at $\mathbb{C}/2\pi i\mathbb{Z}$ (eller bare $\mathbb{C}/\mathbb{Z}$) er det samme som en uendelig lang syllinder, som man så kan "dytte inn" i den ene enden og "strekke ut" i den andre for å dekke hele $\mathbb{C}^*$. Det jeg påstår over er at denne strekkingen og dyttingen også bevarer gruppestrukturen.