

Grublegruppe 19. sept. 2011: Algebra II: kvotientgrupper

Ivar Staurseth
ivarsta@math.uio.no

Kosett av normale undergrupper

I forrige uke så vi på grupper og undergrupper. I dag skal vi konstruere det vi kaller *kvotientgruppa* G/H , for en gruppe G og en normal undergruppe H av G .

Definisjon 1. En undergruppe H av en gruppe G er en normal undergruppe dersom den er invariant under konjugasjon med elementer i G . Eller sagt matematisk: for alle $h \in H$ har vi at også $g * h * g^{-1} \in H$ for alle $g \in G$

Vi ser med en gang at alle undergrupper av abelske grupper må være normale, siden vi i abelske grupper kan bytte om på rekkefølgen av faktorene slik at $ghg^{-1} = (gg^{-1})h = 1h = h$, som opplagt er med i H for alle $g \in G, h \in H$.

Definisjon 2. La $(H, *)$ være en normal undergruppe av en gruppe $(G, *)$. For en gitt $g \in (G, *)$ definerer vi kosettet $g * H = \{g * h | h \in H\}$

Eksempel 1. I dette eksempelet skal vi se på heltallene med vanlig addisjon: $(\mathbb{Z}, +)$ og på undergruppa:

$$5\mathbb{Z} = \{5z | z \in \mathbb{Z}\} = \{\dots, -15, -10, -5, 0, 5, 10, 15\}$$

Et eksempel på et kosett av $5\mathbb{Z}$ er $(1 + 5\mathbb{Z}) = \{\dots, -14, -9, -4, 1, 6, 11, 16\}$. Faktisk er dette nøyaktig det samme kosettet som $(6+5\mathbb{Z}), (11+5\mathbb{Z})$ og ethvert kosett på formen $((1+5k) + 5\mathbb{Z})$, hvor $k \in \mathbb{Z}$. Det viser seg at undergruppa $5\mathbb{Z}$ har et endelig antall kosett, som vi gir en bestemt notasjon:

$$\begin{aligned}[0] &= (0 + 5\mathbb{Z}) = \{\dots, -15, -10, -5, 0, 5, 10, 15\} \\ [1] &= (1 + 5\mathbb{Z}) = \{\dots, -14, -9, -4, 1, 6, 11, 16\} \\ [2] &= (2 + 5\mathbb{Z}) = \{\dots, -13, -8, -3, 2, 7, 12, 17\} \\ [3] &= (3 + 5\mathbb{Z}) = \{\dots, -12, -7, -2, 3, 8, 13, 18\} \\ [4] &= (4 + 5\mathbb{Z}) = \{\dots, -11, -6, -1, 4, 9, 14, 19\} \end{aligned}$$

Prøver vi å lage flere, vil vi se at $[5] = [0], [6] = [1], [7] = [2], \dots$ osv.

Vi ser at $[a]$ er **kongruensklassen til a , mod 5**, dvs. mengden av alle tall som er på formen $a + 5k$, hvor k er et vilkårlig heltall.

Vi ser at kosettene er disjunkte mengder og at unionen av dem er hele den gruppa vi startet med, i vårt tilfelle: \mathbb{Z}

Det vi ser konturene av her gjelder generelt:

Teorem 1. Vi har tidligere definert ordenen til en gruppe G (notasjon: $|G|$) som antall elementer i G . Dersom G er en gruppe av (endelig) orden n og H en undergruppe av G av orden m , gjelder følgende:

- $\frac{n}{m}$ er et heltall (dvs. m er en faktor i n)
- H har $\frac{n}{m}$ disjunkte komengder (inkl H selv), hver av dem har m elementer og unionen av dem er hele G .

Bevis: Jeg vil bevise at alle kosettene til H har m elementer, at de er disjunkte og at unionen av dem er hele G . Det vil følge av det at hvis det er k kosett, så må $km = n$, og beviset er i boks.

Vi vet at $|H| = m$, så $H = \{e, h_1, h_2, \dots, h_{m-1}\}$ Studerer vi kosettet $g * H$ for en eller annen $g \in G$ får vi noe på formen $\{g, g * h_1, \dots, g * h_{m-1}\}$

Vi ser med en gang at $g * H$ ikke kan ha flere enn m elementer, men kan mengden ha færre? Det kan skje dersom $g * h_i = g * h_j$ for $i \neq j$. Men det vil medføre at $g^{-1} * g * h_i = g^{-1} * g * h_j \implies h_i = h_j$, som ikke kan stemme siden H har nøyaktig m elementer. Ergo må $g * H$ ha m elementer.

Så må vi vise at kosettene er parvis disjunkte, dvs. at to kosett, $g_1 * H$ og $g_2 * H$ enten består av nøyaktig de samme elementene eller er disjunkte. Vi antar (og håper på en selvmotsigelse) det motsatte av dette, dvs. at det finnes to kosett $g_1 * H, g_2 * H$ som snitter hverandre delvis, det vil si at det finnes minst ett element x som er med i begge, og samtidig minst ett element y som er med i det ene kosettet, men ikke det andre. Sagt matematisk $x \in g_1 * H, x \in g_2 * H, y \in g_1 * H, y \notin g_2 * H$

Dette vil si at det finnes elementer $h_1, h_2, h_3 \in H$ slik at $x = g_1 * h_1, x = g_2 * h_2, y = g_1 * h_3$. Vi ser at $g_1 * h_1 = g_2 * h_2 = x$. Ved å multiplisere med inverser får vi $g_1 = g_2 * h_2 * h_1^{-1}$. Vi har derfor at $y = g_1 * h_3 = g_2 * h_2 * h_1^{-1} * h_3$. Siden H er en gruppe må $h_2 * h_1^{-1} * h_3 \in H$. Kaller vi dette elementet h ender vi opp med at $y = g_2 * h$ for et element $h \in H$, som vil si at $y \in g_2 * H$, som strider mot vår antakelse om at $y \notin g_2 * H$.

Vi har altså vist at kosettene er disjunkte mengder, hver av dem med m elementer. Det gjenstår å vise at unionen av dem er hele G , det vil si at hvert element $g \in G$ er med i ett av disse kosettene. Det er enkelt - vi kan se på kosettet $g * H$, hvor g må være med siden $g = g * e$, og identitetselementet $\in H$ siden H er en gruppe.

Kvotientgrupper

I forrige seksjon har vi sett hvordan vi kan konstruere kosettene til en normal undergruppe H av en gruppe G . Nå skal vi gi mengden av alle kosettene en gruppestruktur.

Definisjon 3. La G være en gruppe og H en normal undergruppe av G . Kvotientgruppa G/H er (som mengde) definert som mengden av kosettene til H i G . Gruppstrukturen er gitt ved den binære operasjonen

$$(g_1 * H) * (g_2 * H) = ((g_1 * g_2) * H)$$

Vi sier gjerne at den binære operasjonen er gitt ved å **plukke representanter**. Som vi har sett tilhører hvert element i G ett entydig kosett.

Når vi skal finne summen, produktet (eller hva man velger å kalle den binære operasjonen) av to kosett kan man velge et hvilket som helst element, x , fra det ene kosettet, et hvilket som helst element, y , fra det andre kosettet, legge dem sammen/gange dem sammen/(kjært barn har...) i G (og få $x * y$) og se hvilket kosett elementet $x * y$ ligger i. Denne binære operasjonen er veldefinert - det vil si at for et gitt par av kosett vil man alltid havne i ett og samme tredje kosett når man følger denne prosedyren, uansett hvilke representanter man velger fra de to kosettene.

Eksempel 2. $\mathbb{Z}/5\mathbb{Z}$ er en gruppe av orden 5, og den er isomorf med den sykliske gruppen av orden 5 som vi så på i forrige uke.

Som mengde består $\mathbb{Z}/5\mathbb{Z}$ av de fem kongruensklassene vi definerte på side 1, dvs. $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$. Den binære operasjonen er gitt ved $[a] + [b] = [a + b]$. Siden $[a] = [a + 5 * k]$ for alle $k \in \mathbb{Z}$ får vi følgende addisjonstabell:

	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]



De sykliske gruppene $\mathbb{Z}/n\mathbb{Z}$ (\mathbb{Z} modulo n) skrives ofte på kortformen \mathbb{Z}_n .

Definisjon 4. La G være en gruppe og H en normal undergruppe av G . Da finnes det en naturlig, surjektiv gruppehomomorf $\pi : G \rightarrow G/H$, definert ved $\pi(g) = g * H$. Den kalles ofte **projeksjonen** av G ned på kvotientgruppa G/N .

Under følger tre teoremer - de såkalte isomorfiteoremmene:

Teorem 2. La G og H være grupper og $\phi : G \rightarrow H$ en gruppehomomorf (se forrige uke), og la e_G, e_H være identitetselementene i hhv. G og H . Da er følgende tilfelle:

- $\ker(\phi) = \{x \in G | \phi(x) = e_H\}$ er en normal undergruppe av G
- $\text{im}(\phi) = \phi[G] = \{\phi(x) \in H | x \in G\}$ er en undergruppe av H
- $\text{im}(\phi) \cong G/\ker(\phi)$

Teorem 3. La G være en gruppe, S en undergruppe av G og N en normal undergruppe av G . Da er følgende tilfelle:

- $SN = \{s * n | s \in S, n \in N\}$ er en undergruppe av G
- Snittet $S \cap T$ er en normal undergruppe av G
- N er en normal undergruppe av SN , og $(SN)/N \cong S/(S \cap N)$

Teorem 4. La N og K være normale undergrupper av en gruppe G , med $K \subseteq N \subseteq G$. Da er følgende tilfelle:

- N/K er en normal undergruppe av G/K
- $(G/K)/(N/K) \cong G/N$

Produkt av grupper

Definisjon 5. Hvis vi har to grupper $(G, *)$ og $(G', *')$ kan vi konstruere produktet av gruppene, $G \times G'$. Som mengde består det av elementene:

$G \times G' = \{(x, y) | x \in G, y \in G'\}$. Den binære operasjonen er gitt ved $(x_1, y_1) * (x_2, y_2) = (x_1 * x_2, y_1 *' y_2)$. Dersom e_G og $e_{G'}$ er identitetselementene i hhv. G og G' , er $(e_G, e_{G'})$ identitetselementet i $G \times G'$. Inverselementet til (a, b) er (a^{-1}, b^{-1}) .

På tilsvarende måte kan man definere produkt av flere grupper: $G_1 \times G_2 \times \dots \times G_n$. For et slikt produkt av grupper har vi naturlige gruppehomomorfier:

$\pi_i : G_1 \times G_2 \times \dots \times G_n \rightarrow G_i$ gitt ved $\pi_i(g_1, g_2, \dots, g_i, \dots, g_n) = g_i$. Disse homomorfiene er surjektive, og kalles gjerne **projeksjonen** på den i -te faktoren.

Oppgaver (1-4 er pensumrelevante oppgaver, mens 5-7 er relevant for stoffet i dette notatet)

Oppgave 1. Vis at dersom likningen $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x = 0$ har en positiv løsning $x = x_0$, så har likningen $na_0x^{n-a} + (n-1)a_1x^{n-2} + \dots + a_{n-1} = 0$ en positiv løsning $x = x_1$, med $x_1 < x_0$

Oppgave 2. (fritt etter Oblig 1 i MAT1300 vår 2009) I denne oppgaven skal vi se på når $x^y = y^x$. Det skjer selvsagt når $x = y$, men også f.eks. når $x = 2, y = 4$. La $f : (0, \infty) \rightarrow \mathbb{R}$ være gitt ved: $f(x) = \frac{\ln(x)}{x}$.

(a) For $x, y > 0$ vis at:

1. $x^y < y^x \iff f(x) < f(y)$
2. $x^y = y^x \iff f(x) = f(y)$
3. $x^y > y^x \iff f(x) > f(y)$

(Hint: bruk at $\ln(x)$ er strengt voksende)

(b) Beregn $f'(x)$, vis at $f'(x) > 0$ for $x \in (0, e)$, $f'(e) = 0$ og $f'(x) < 0$ for $x \in (e, \infty)$.

(c) Avgjør hvilket av tallene $\pi^{\sqrt{10}}$ og $\sqrt{10}^\pi$ som er størst, uten å regne dem ut. (Hint: du har lov til å sjekke at $\pi < e < \sqrt{10}$)

(d) Beregn $f(e)$ og $\lim_{x \rightarrow \infty} f(x)$. Bruk skjæringssetningen til å vise at f avbilder intervallet (e, ∞) på intervallet $(0, 1/e)$ dvs. at $f((e, \infty)) = \{f(x) | x \in (e, \infty)\} = (0, 1/e)$

(e) Beregn $f(1)$ og vis at for en gitt, kjent $x \in (0, 1]$ har likningen $x^y = y^x$ (med $y \in (0, \infty)$ som ukjent) kun en løsning, nemlig $x = y$. Vis også at når $x = e$ har likningen kun en løsning: $y = e$

(f) Vis at for en gitt $x \in (1, e)$ har likningen $x^y = y^x$ (med $y \in (0, \infty)$ som ukjent) nøyaktig to løsninger: en der $y = x$ og en der $y \in (e, \infty)$.

Oppgave 3. (oppgave fra avsluttende eksamen i MAT1100 høst 2007) Vi vet at de åpne delmengdene, A , av \mathbb{R} er slik at det for hver $a \in A$ finnes en $\delta > 0$ slik at $(a - \delta, a + \delta) \subset A$. Vis at dersom $f : \mathbb{R} \rightarrow \mathbb{R}$ er en kontinuerlig funksjon, så er mengden $A = \{x \in \mathbb{R} | f(x) \neq 0\}$ en åpen delmengde.

Oppgave 4. La $P(z)$ og $Q(z)$ være to polynomer med komplekse koeffisienter. Vis at dersom $P(x) = Q(x)$ for alle reelle tall x , så må $P(z) = Q(z)$ for alle komplekse tall z .

Oppgave 5. La $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ være den sykliske gruppen av orden 6. Vis at $H = \{0, 3\}$ er en undergruppe av \mathbb{Z}_6 . Skriv opp kosettene til H i \mathbb{Z}_6 , dvs. elementene i \mathbb{Z}_6/H .

Oppgave 6. for ethvert element $a \in G$ kan vi konstruere en undergruppe generert av a , dvs. $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$, hvor $a^n = a * a * \dots * a$ (n faktorer), $a^{-n} = a^{-1} * a^{-1} * \dots * a^{-1}$ (n faktorer) og $a^0 = e$. Dersom et element $a \in G$ er slik at $\langle a \rangle = G$ sier vi at a er en generator for G , eller at G er generert av a .

- Vis at $\langle a \rangle$ oppfyller kravene til en undergruppe.
- Hvilke elementer i gruppa \mathbb{Z}_5 (under addisjon) er generatorer for gruppa? Hva med \mathbb{Z}_6 ? Hva med \mathbb{Z}_p , hvor p er primtall?
- Hvilkens orden (i.e. hvor mange elementer) har undergruppa $\langle (2, 3) \rangle$ i $\mathbb{Z}_6 \times \mathbb{Z}_{15}$?

Oppgave 7. (Prøv å) bevis (så mye som mulig av) teorem 2-4 på side 4