Oblig 1 - MAT2400

Fredrik Meyer

1 Oppgave 1

Påstand 1 (a)**.** *$\mathbb{Z}_5$ har fire generatorer og Aut$(\mathbb{Z}_5) \simeq \mathbb{Z}_4$*

Bevis. Hvert ikke-null-element i $\mathbb{Z}_5$ genererer en undergruppe. Siden 5 er et primtall, må denne undergruppen ha orden 5 eller 1. Undergruppen av orden er 1 er den trivielle gruppen $\{0\}$. Alle de andre undergruppene må ha orden 5, og derfor generere hele gruppen. $\mathbb{Z}_5$ har derfor 4 generatorer.

Siden enhver automorfisme må sende generatorer på generatorer (for ellers ville $\sigma(\langle 1 \rangle)$ ikke vært lik $\mathbb{Z}_5$), er $\mathrm{Aut}(\mathbb{Z}_5)$ av orden 4. Det finnes to grupper av orden 4, og vi må finne ut hvilken det er ($\mathbb{Z}_4$ eller $\mathbb{Z}_2 \times \mathbb{Z}_2$).

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \tag{1}$$

Vi ser raskt at $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$, og dette er ikke identitetsautomorfismen, så vi må ha at $\mathrm{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_4$, siden det dobbelte av alle elementer i $\mathbb{Z}_2 \times \mathbb{Z}_2$ er identitetselementet.

$\square$

Påstand 2. *Finne alle endelige abelske grupper av orden 96.*

Bevis. Først ser vi at $96 = 3 \cdot 2^5$. Fra fundamentalteoremet om endeliggenererte abelske grupper vet vi at enhver slik gruppe kan skrives på formen $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}}$ der p_i er primtall. Dermed er mulighetene våre følgende: $\mathbb{Z}_{96}, \mathbb{Z}_3 \times \mathbb{Z}_{32}, \mathbb{Z}_3 \times \mathbb{Z}_{16} \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_8, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. $\square$

Påstand 3. *Finn to undergrupper av S_4 som er isomorfe med S_3.*

Bevis. S_4 består av alle permutasjoner av $(1, 2, 3, 4)$. La H være undergruppen av S_4 som lar 4 være fiksert. At H er en undergruppe ses lett: $\iota \in H$ fordi $\iota(4) = 4$ og om $\sigma \in H$ er $4 = \iota(4) = \sigma^{-1}\sigma(4) = \sigma^{-1}(4)$, så $\sigma^{-1} \in H$. Og om $\sigma, \delta \in H$, er $\sigma\delta(4) = \sigma(4) = 4$, så H er lukket under komposisjon. Dermed er H en undergruppe. La nå $\psi : S_3 \to H$ være definert med $\psi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 \end{pmatrix}$. Vi må vise at ψ er en homomorfi: $\psi(\sigma\zeta) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1)\zeta(1) & \sigma(2)\zeta(2) & \sigma(3)\zeta(3) & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta(1) & \zeta(2) & \zeta(3) & 4 \end{pmatrix} = \psi(\sigma)\psi(\zeta)$, så ψ er en homomorfi. At ψ er en-en og på er selvsagt fra definisjonen. Så $H \simeq S_3$. På samme måte kan vi definere K som undergruppen som lar 3 være fiksert, og vi får akkurat samme bevis. $\square$

2 Oppgave 2

La G og G' være abelske grupper. La $\mathrm{Hom}(G, G')$ betegne mengden av alle homomorfismer fra G til G'. Vi definerer en operasjon på $\mathrm{Hom}(G, G')$:

$$f + g : G \to G', (f + g)(x) = f(x) + g(x) \, \forall x \in G$$

Påstand 4. $f + g \in Hom(G, G')$

Bevis. Vi må vise at $(f + g)(x + y) = (f + g)(x) + (f + g)(y)$. Dette er rett fram utregning:

$$\begin{aligned} (f+g)(x+y) &= f(x+y) + g(x+y) && (2) \\ &= f(x) + f(y) + g(x) + g(y) && (3) \\ &= f(x) + g(x) + f(y) + g(y) && (4) \\ &= (f+g)(x) + (f+g)(y) && (5) \end{aligned}$$

I overgangen fra ligning 3 til 4 bruker vi at f og g er homomorfier, og i overgangen fra 4 til 5 bruker vi at G' er abelsk. $\square$

Påstand 5. *$(Hom(G, G'), +)$ er en abelsk gruppe.*

Bevis. Vi må vise at det eksisterer inverselementer og identitetselement. La $0 : G \to G'$ være definert som $0(x) = 0 \forall x \in G$. Da er $(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x)$, så 0 er et identitetselement. Definer nå $(-f)$ som $(-f)(x) = -f(x)$. Da er $(-f)$ et inversen til f: $(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0$ for alle x. Så vi har både inverser og identitetselement. At mengden er lukket under operasjonen ble vist i påstand

4. Så vi har en gruppe. At gruppen er abelsk følger fra $(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$ siden G' er abelsk. Så $(\mathrm{Hom}(G, G'), +)$ er en abelsk gruppe. □

Påstand 6. *$Hom(\mathbb{Z}, G') \simeq G'$*

Bevis. Definer $\psi : \mathrm{Hom}(\mathbb{Z}, G') \to G'$ ved $\psi(f) = f(1)$. Da er ψ en homomorfi fordi $\psi(f+g) = (f+g)(1) = f(1) + g(1) = \psi(f) + \psi(g)$. Må vise at ψ er en-en og på. Anta $\psi(f) = \psi(g)$. Altså at $f(1) = g(1)$. Da er $f(k) = f(1+1+\ldots+1) = f(1)+\ldots+f(1) = g(1)+\ldots+g(1) = g(k)$ for alle $k > 0$. Men $f(-k) = f(0-k) = f(0) - f(k) = 0 - f(k) = 0 - g(k) = g(0) - g(k) = g(0-k) = g(-k)$. Så $f(x) = g(x)$ for alle x, og derfor må $f = g$. ψ er altså en-en. Anta $a \in G'$. Definer nå en homomorfi $f : \mathbb{Z} \to G'$ ved $f(1) = a$. Ved samme metode som ovenfor definerer dette unikt en homomorfi, så ψ er på. Vi har dermed en isomorfi fra $\mathrm{Hom}(\mathbb{Z}, G') \to G'$ og vi må derfor ha $\mathrm{Hom}(\mathbb{Z}, G') \simeq G'$. □

Påstand 7. *Beskrive elementene i $Hom(\mathbb{Z}, \mathbb{Z})$.*

Bevis. Fra forrige oppgave er $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}$, så funksjonene i $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$ oppfører seg akkurat som heltallene. □

3 Oppgave 3

La $G = \mathbb{Z} \times \mathbb{Z}$.

Påstand 8. *La $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z})$, og anta $\det(A) = \pm 1$. Da er $\phi_A : G \to G$ gitt ved $\phi_A(x, y) = (ax + by, cx + dy)$ en automorfisme av G.*

Bevis. At ϕ_A er en homomorfisme er selvsagt siden lineærtransformasjoner er lineære. Siden $\det A \neq 0$, vet vi fra lineær algebra at ϕ_A er en-en. Siden A er invertibel, er invers-transformasjonen gitt ved $\phi_A^{-1}(x, y) = (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} (x, y)$, og siden $\det A = \pm 1$, er $(\det A)^{-1} \in \mathbb{Z}$, så ϕ_A er også på. □

Påstand 9. *Anta $\phi : G \to G$ er en homomorfisme. Da $\exists A \in M(2, \mathbb{Z})$ slik at $\phi = \phi_A$.*

Bevis. Anta $\phi(1, 0) = (a, c)$ og $\phi(0, 1) = (b, d)$. Da er $\phi(x, 0) = (ax, cx)$ og $\phi(0, y) = (by, dy)$. Siden ϕ er en homomorfisme er $\phi(x, y) = \phi(x, 0) + \phi(0, y)$, så vi har at $\phi(x,y) = \phi(x,0) + \phi(0,y) = (ax,cx) + (by,dy) = (ax+by, cx+dy) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (x,y) = A(x,y) = \phi_A(x,y)$. □

Påstand 10. *Anta ϕ er en automorfisme av G, og at $\phi = \phi_A$. Da er* $\det(A) = \pm 1$.

Bevis. Fra forrige påstand vet vi at $\phi = \phi_A$ der $A \in M(2,\mathbb{Z})$. Anta nå $A(x_1,x_2) = (y_1,y_2)$. Da er ved Cramers regel

$$x_1 = \begin{vmatrix} y_1 & b \\ y_2 & d \end{vmatrix} / \det(A)$$

og på samme måte med x_2. Men vi vil at $x_1 \in \mathbb{Z}$. For at dette skal gå for alle y_1, y_2, må $\det A = \pm 1$. □

4 Oppgave 4

La G være en gruppe og la $H \leq G$.

Påstand 11. *La X være samlingen av venstresideklassene av H. La G virke på X ved venstretranslasjon $g(xH) = gxH$ for $g \in G$ og $xH \in X$. La $\phi : G \to S_X$ være homomorfismen gitt ved $\phi(g) = \sigma_g$ for $g \in G$ hvor $\sigma_g(xH) = gxH$ for alle $xH \in X$. Da er $\ker\phi \subset H$.*

Bevis. La $I = \{x \in G | x \neq y \Rightarrow xH \neq yH$ for $y \in G\}$ være representativer for venstreklassene til H. Vi har at:

$$\begin{aligned} \ker\phi &= \{g \in G|\phi(g) = \iota\} && (6)\\ &= \{g \in G|\sigma_g(xH) = xH \forall xH \in X\} && (7)\\ &= \{g \in G|gxH = xH \forall x \in G\} && (8)\\ &= \left\{g \in G|x^{-1}gx \in H \forall x \in G\right\} && (9) \end{aligned}$$

Anta $g \in \ker\phi$. Da er fra ligningene over $x^{-1}gx \in H$. Om $x \notin H$, må $g \in H$, for ellers kunne umulig produktet vært med i H. Om $x \in H$, har vi at $x^{-1}gx \in H \Leftrightarrow x^{-1}gxH = H \Leftrightarrow gxH = xH = H \Leftrightarrow g(xH) = gH = H \Leftrightarrow g \in H$. Så $\ker\phi \subset H$. □

Påstand 12. *Anta $|G| = pn$ hvor p er et primtall slik at $p > n$ og anta H har orden p. Da er H normal i G.*

Bevis. Siden $p > n$ kan ikke p dele n. Så vi har at H er en Sylow p-undergruppe. Fra andre Sylow-teorem vet vi at om K er en annen Sylow p-undergruppe, så er $K = gHg^{-1}$ for en eller annen $g \in G$. Fra tredje Sylow-teorem er antall Sylow p-undergrupper kongruent med 1 modulo p og deler pn. Tallene som er kongruente med 1 modulo p er $\{1, p+1, 2p+1, \ldots\}$. Men siden $p > n$ er 1 eneste mulighet, og dermed er H den eneste Sylow p-undergruppen. Fra andre Sylow-teorem har vi dermed at $H = gHg^{-1}$ for alle $g \in G$, så H er normal. $\square$