Eksamen MA2201/TMA4150 28. mai 2010, løsningsforslag

Oppgave 1

(a) $(1,2)(2,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$
$(2,3)(1,2)(2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$ $\Rightarrow$ Permutasjonene er de samme.

(b) Fra (a) har vi at $(1,2)(2,3)(1,2) = (1,3)$, som må være i H da H skal være lukket under sammensetning av permutasjoner som ligger i H. Dette gir at alle 2-sykler eller transposisjoner ligger i H. Siden alle permutasjoner kan skrives som et produkt av 2-sykler, så må $H = S_3$.

(c) La $\sigma \in S_3$. Da er $\varphi(\sigma) = \tilde{\sigma}$, der $\tilde{\sigma}(i) = \begin{cases} \sigma(i), & i \in \{1,2,3\} \\ 4, & i = 4. \end{cases}$

Vil vise at $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$, eller ekvivalent at $\widetilde{\sigma_1\sigma_2} = \tilde{\sigma}_1\tilde{\sigma}_2$. Har at

$$\widetilde{\sigma_1\sigma_2}(i) = \begin{cases} (\sigma_1\sigma_2)(i), & i = 1,2,3. \\ 4, & i = 4. \end{cases}$$

og
$$\tilde{\sigma}_1 \cdot \tilde{\sigma}_2(i) = \tilde{\sigma}_1(\tilde{\sigma}_2(i)) = \begin{cases} \tilde{\sigma}_1(\sigma_2(i)), & i \in \{1,2,3\} \\ \tilde{\sigma}_1(4), & i = 4 \end{cases}$$
$$= \begin{cases} \sigma_1(\sigma_2(i)), & i \in \{1,2,3\} \\ 4, & i = 4 \end{cases}$$

Siden $(\sigma_1\sigma_2)(i) = \sigma_1(\sigma_2(i))$ for $i \in \{1,2,3\}$, følger det at $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$ og φ er en gruppehomomorfi.

Vi har at $\varphi((1,2)) = (1,2) \in H$, mens $(1,4)(1,2)(1,4)^{-1} = (1,4)(1,2)(1,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4) \notin H$. Dette viser at $\operatorname{Im}\varphi$ ikke er normal i S_4.

Oppgave 2

La H være en ekte undergruppe av G. Av Lagrange Teorem har vi at $|H| \mid |G| = pq$, dvs. $|H| \in \{1, p, q\}$ siden $H \neq G$. Enhver triviell gruppe (gruppe av orden 1) og enhver gruppe av primtalls orden er syklisk, slik at det følger av dette at H er syklisk.

Oppgave 3

(a) En undergruppe av orden 2 i D_{10} svarer til et element av orden 2. Elementene $\{\rho_1, \rho_2, \rho_3, \rho_4\}$ har alle orden 5, og ρ_0 har orden 1. Siden μ_i for $i = 1,2,3,4,5$ er speilinger, så har de orden 2. Dette gir at alle undergruppene av D_{10} av orden 10 er:

$\{\rho_0, \mu_1\}, \{\rho_0, \mu_2\}, \{\rho_0, \mu_3\}, \{\rho_0, \mu_4\}, \{\rho_0, \mu_5\}$.

(b) i) La $|G| = 2^t m$, der $2 \nmid m$. Da er en undergruppe $H \leq G$ en Sylow 2-undergruppe hvis H er en maksimal 2-undergruppe av G, dvs hvert element i H har orden 2^i for en $i \geq 0$ (H er en 2-undergruppe) og H er ikke inneholdt i noen større 2-undergruppe, dvs. H har orden 2^t.

ii) To undergrupper H og H' av G er konjugerte hvis det eksisterer $g \in G$ slik at $H' = gHg^{-1}$.

iii) Ordenen til D_{10} er $10 = 2 \cdot 5$, slik at en Sylow 2-undergruppe av D_{10} har orden 2. Dette gir at alle undergruppene av orden 2 av D_{10} er Sylow 2-undergruper, og av 2. Sylow teorem så er alle disse konjugerte.

Oppgave 4

(a) Polynomet $p(x)$ har grad 3, slik at $p(x)$ er irredusiblet hvis og bare hvis $p(\alpha) \neq 0$ for alle $\alpha \in \mathbb{Z}_3$. Vi har at $p(0) = 1$, $p(1) = 1$, $p(2) = 2$, slik at $p(x)$ er irredusibelt over $\mathbb{Z}_3$.

Siden $\mathbb{Z}_3[x]$ er en kommutativ ring, så er $\mathbb{Z}_3[x]/(p(x))$ en kropp hvis og bare hvis $(p(x))$ er et maksimalt ideal. Vi vet at et element $p(x) \neq 0$ i $\mathbb{Z}_3[x]$ genererer et maksimalt ideal hvis og bare hvis $p(x)$ er irredusibelt over $\mathbb{Z}_3$. Av første del av dette punkt får vi at $\mathbb{Z}_3[x]/(p(x))$ er en kropp.

(b) Vi har at

$$
\begin{aligned}
p(\alpha) &= (x + (p(x)))^3 + 2(x + (p(x)))^2 + 1 \\
&= (x^3 + (p(x))) + (2x^2 + (p(x))) + 1 \\
&= (x^3 + 2x^2 + 1) + (p(x)) \\
&= p(x) + (p(x)) = 0 \quad i \quad E = \mathbb{Z}_3[x]/(p(x)).
\end{aligned}
$$

Siden $p(\alpha) = 0$ for $\alpha \in E$, så vil $x - \alpha \mid p(x)$ over E, dvs. det eksisterer $g(x) \in E[x]$ slik at $p(x) = (x-\alpha)g(x)$. Finner $g(x)$ ved divisjon:

$$
\begin{aligned}
&x^3 + 2x^2 + 1 : x - \alpha = x^2 + (2+\alpha)x + (\alpha^2 + 2\alpha) \\
&\underline{x^3 - \alpha x^2} \\
&\quad (2+\alpha)x^2 + 1 \\
&\quad \underline{(2+\alpha)x^2 - \alpha(2+\alpha)x} \\
&\qquad\qquad (\alpha^2 + 2\alpha)x + 1 \\
&\qquad\qquad \underline{(\alpha^2 + 2\alpha)x - \alpha(\alpha^2 + 2\alpha)} \\
&\qquad\qquad\qquad \alpha^3 + 2\alpha^2 + 1 = 0
\end{aligned}
$$

Dette gir at $p(x) = (x-\alpha)[x^2 + (2+\alpha)x + \alpha^2 + 2\alpha]$.

Oppgave 5

(a) X er en H-mengde hvis $\underbrace{\text{(i) } e * x = x \text{ for alle } x \in X \text{ og}}_{* : H \times X \longrightarrow X \text{ og}}$ (ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$, for alle $x \in X$ og alle $g_1, g_2 \in H$, der e er identiteten i H. ($e = \sigma^0$). Vi har at

$$\sigma^0 * (g_1, \dots, g_\ell) = (g_1, g_2, \dots, g_\ell),$$

slik at $e * x = x$ for alle $x \in X$. La σ også betegne permutasjonen $\begin{pmatrix} 1 & 2 & 3 & \cdots & \ell-1 & \ell \\ \ell & 1 & 2 & \cdots & \ell-2 & \ell-1 \end{pmatrix}$. Da vil

$$\sigma^i * (g_1, g_2, \dots, g_\ell) = (g_{\sigma^{-i}(1)}, g_{\sigma^{-i}(2)}, \dots, g_{\sigma^{-i}(\ell)}).$$

Dette gir

$$(\sigma^i \sigma^j) * (g_1, g_2, \dots, g_\ell) = \sigma^{i+j} * (g_1, g_2, \dots, g_\ell)$$
$$= (g_{\sigma^{-(i+j)}(1)}, g_{\sigma^{-(i+j)}(2)}, \dots, g_{\sigma^{-(i+j)}(\ell)})$$

og

$$\sigma^i * (\sigma^j * (g_1, g_2, \dots, g_\ell)) = \sigma^i * (g_{\sigma^{-j}(1)}, g_{\sigma^{-j}(2)}, \dots, g_{\sigma^{-j}(\ell)})$$
$$= (g_{\sigma^{-i}(\sigma^{-j}(1))}, g_{\sigma^{-i}(\sigma^{-j}(2))}, \dots, g_{\sigma^{-i}(\sigma^{-j}(\ell))})$$
$$= (g_{\sigma^{-(i+j)}(1)}, g_{\sigma^{-(i+j)}(2)}, \dots, g_{\sigma^{-(i+j)}(\ell)})$$
$$= (\sigma^i \sigma^j) * (g_1, g_2, \dots, g_\ell),$$

slik at (ii) er oppfylt.

La $g = g_1 g_2 \cdots g_{\ell-i}$, når $(g_1, g_2, \dots, g_\ell) \in X$. Siden

$$e = g_1 g_2 \cdots g_\ell = g\, g_{\ell-i+1} g_{\ell-i+2} \cdots g_\ell, \text{ så er } g_{\ell-i+1} g_{\ell-i+2} \cdots g_\ell = g^{-1}.$$

Dette gir at $e = g_{\ell-i+1} g_{\ell-i+2} \cdots g_\ell\, g = g_{\ell-i+1} g_{\ell-i+2} \cdots g_\ell\, g_1 g_2 \cdots g_{\ell-i}$, dvs. $\sigma^i * (g_1, g_2, \dots, g_\ell) \in X$ for alle $i \in \{0, 1, 2, \dots, \ell-1\}$. Dette viser at X er en H-mengde.

(b) Siden $\sigma \in H$, så har vi pr. definisjon at $X_H \subseteq X_\sigma$. La $x \in X_\sigma$. Siden X er en H-mengde, så er

$$\sigma^i * x = \overbrace{\sigma * (\sigma * (\cdots (\sigma * x)))}^{i \text{ ganger}}$$
$$= \underbrace{\sigma * (\sigma * (\cdots (\sigma * x)}_{i-1 \text{ ganger}}, \text{ siden } \sigma * x = x \text{ da } x \in X_\sigma$$

Gjentatt bruk av at $x \in X_\sigma$, gir at $\sigma^i * x = x$ for alle i, slik at $x \in H_H$. Dette gir at $X_\sigma = X_H$.

La $(g_1, g_2, \dots, g_\ell) \in X$. Da er $\sigma * (g_1, g_2, \dots, g_\ell) = (g_\ell, g_1, g_2, \dots, g_{\ell-1})$ $= (g_1, g_2, \dots, g_\ell)$. Dette gir at $g_\ell = g_1, g_1 = g_2, g_2 = g_3, \dots$ $g_{\ell-1} = g_\ell$, som impliserer at $g_1 = g_2 = \cdots = g_{\ell-1} = g_\ell = g$ og vi kan identifisere X_σ med alle elementene g i G som er slik at $g^\ell = e$. Dvs. X_σ kan identifiseres med alle elementene g i G som har orden t, der $t \mid \ell$.

(c) La $\ell = p^w$ for en w slik at $1 \leq w \leq t$. Fra (a) og (b) har vi at H er gruppe av orden p^w og X er en H-mengde. Da vet vi at

$$|X| \equiv |X_H| \mod p.$$

Fra beviset av Cauchys teorem har vi at $|X| = |G|^{p^w - 1}$. Siden $|G| = p^t m$ med $t \geq 1$, så er $|X| \equiv 0 \mod p$ og

$$|X_H| \equiv 0 \mod p.$$

Vi har at $X_H = X_\sigma = \{g \in G \mid g \text{ har orden } p^i \text{ der } 1 \leq i \leq w\} \cup \{e\}$ og at $|X_H| = N_w + 1$. Dette gir at

$$N_w \equiv -1 \mod p.$$

(d) Antall elementer i G med orden p^i for en i med $2 \leq i \leq t$, er det samme som $N_i - N_{i-1}$. Da er

$$N_i - N_{i-1} \equiv -1 - (-1) \equiv 0 \mod p,$$

dvs. antall elementer i G med orden p^i, $2 \leq i \leq t$, er delelig med p.