Løsningsforslag, TMA4150 Eksamen 17. august 2006

1 a) $24 = 3 \cdot 2^3 = 3 \cdot 2^2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 2$

Det er 3 ikke-isomorfe abelske grupper av orden 24:

$\mathbb{Z}_3 \times \mathbb{Z}_8$

$\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

b) $\langle (2,2,0) \rangle = \{(2,2,0), (0,0,0)\}$ har indeks

$\dfrac{|\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3|}{|\langle (2,2,0)\rangle|} = \dfrac{4 \cdot 4 \cdot 3}{2} = 24$, så faktorgruppen er

isomorf med én av gruppene i a).

- Det er ingen elementer av orden ~~24~~ 8 i $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3$, og dermed er det heller ikke det i faktorgruppen. Dermed er $\mathbb{Z}_3 \times \mathbb{Z}_8$ utelukket.
- På den andre siden har elementet $(1,0,0)\langle (2,2,0)\rangle$ orden 4, siden vi må legge $(1,0,0)$ til seg selv fire ganger for å komme inn i $\langle (2,2,0)\rangle$. Siden $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ikke har noen elementer av orden 4, er denne utelukket.
- Vi sitter igjen med at

$$\underline{\underline{\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 / \langle (2,2,0)\rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2}}$$

2 a) $\tau = (243)(164) = (16324) = (14)(12)(13)(16)$

τ er et produkt av et like antall transposisjoner, så τ er en like permutasjon.

$\sigma\tau = (213)(2146)(56)(16324) = (15)(26)(3)(4)$

Vi ser at $\sigma\tau$ har orden 2, og dermed er indeksen $(S_6 : \langle \sigma\tau \rangle) = \frac{|S_6|}{|\langle\sigma\tau\rangle|} = \frac{6!}{2} = 360$

b) $A_6 = \{ \alpha \in S_6 \mid \alpha$ er en like permutasjon $\}$

- A_6 er lukket under multiplikasjon:

  $\alpha_1, \alpha_2 \in A_6$: $\alpha_1\alpha_2 = (a_{11}\, a_{12}) \cdots (a_{k1}\, a_{k2})(b_{11}\, b_{12}) \cdots (b_{l1}\, b_{l2})$

  der k og l er like tall. Dermed er også $\alpha_1\alpha_2$ et produkt av et like antall permutasjoner $(k+l)$ og $\alpha_1\alpha_2 \in A_6$

- $id_{S_6} = (12)(12) \in A_6$

- A_6 inneholder inversene:

  $\alpha \in A_6 \Rightarrow \alpha = (\alpha_{11}\, \alpha_{12}) \cdots (\alpha_{n1}\, \alpha_{n2})$ der n er et partall.

  $\alpha^{-1} = (\alpha_{n1}\, \alpha_{n2}) \cdots (\alpha_{11}\, \alpha_{12})$, et produkt av n transposisjoner

  $\Rightarrow \alpha^{-1} \in A_6$.

Så A_6 er en undergruppe av S_6.
Skal vise at A_6 er en normal undergruppe.
La $\alpha \in S_6$. Må vise at $\alpha A_6 = A_6 \alpha$.
For $\alpha \in A_6$ er $\alpha A_6 = A_6 = A_6 \alpha$, så anta $\alpha \notin A_6$.

Da αA_6 og A_6 er disjunkte, og har like mange elementer, må αA_6 bestå av nøyaktig de elementene i S_6 som ikke er i A_6. Dette fordi A_6 består av nøyaktig halvparten av elementene i S_6 (opplyst i oppgaven).
Det samme gjelder for $A_6 \alpha$, og dermed får vi $\alpha A_6 = S_6 \setminus A_6 = A_6 \alpha$.

Dermed er A_6 en normal undergruppe.

3 En sykel av orden 3 genererer en syklisk undergruppe av orden 3. Vi finner fire slike:

$\langle (1\ 2\ 3) \rangle = \{id, (1\ 2\ 3), (1\ 3\ 2)\} = G_4$

$\langle (1\ 2\ 4) \rangle = \{id, (1\ 2\ 4), (1\ 4\ 2)\} = G_3$

$\langle (1\ 3\ 4) \rangle = \{id, (1\ 3\ 4), (1\ 4\ 3)\} = G_2$

$\langle (2\ 3\ 4) \rangle = \{id, (2\ 3\ 4), (2\ 4\ 3)\} = G_1$

Hver av disse undergruppene består av 3-sykler der ett bestemt tall ikke forekommer (og dessuten id).
For å komme fra G_i til G_j bruker vi transposisjonen $(i\ j)$ og konjugerer: $(i\ j) G_i (i\ j) = G_j$.
Eksempelvis: $(1\ 4)(1\ 2\ 3)(1\ 4) = (2\ 3\ 4)$ og $(1\ 4)(1\ 3\ 2)(1\ 4) = (2\ 4\ 3)$.

4 $H \leq G$. Skal vise at G er en H-gruppe under $h * g = hgh^{-1} \in G$.

1) $e \in H$. $e * g = ege^{-1} = ege = ge = g \in G \quad \forall g \in G$.

2) $h_1, h_2 \in H$.

- $(h_1 h_2) * g = (h_1 h_2) g (h_1 h_2)^{-1} = h_1 h_2 g h_2^{-1} h_1^{-1} \in G$
- $h_1 * (h_2 * g) = h_1 * (h_2 g h_2^{-1}) = h_1 (h_2 g h_2^{-1}) h_1^{-1} = h_1 h_2 g h_2^{-1} h_1^{-1} \in G$

Vi ser at kravene for en gruppevirkning er tilfredsstilt, og G er en H-gruppe.

5 G gruppe, $H \leq G$ med $(G:H) = n$.

- Anta H er en normal undergruppe i G. Da har faktorgruppen G/H orden $|G/H| = n$. Dermed har vi at i faktorgruppen er $(aH)^n = a^n H = H$. Det igjen vil si at $a^n \in H, \ \forall a \in G$.
- La $G = S_4$ og $H = G_4 = \langle (1\,2\,3) \rangle$ fra oppg. 3. Da er indeksen $(S_4 : G_4) = \frac{2 \cdot 3 \cdot 4}{3} = 8$.

  La $a = (1\,2\,4) \in S_4$. Da er $a^8 = (1\,2\,4)^8 = ((1\,2\,4)^3)^2 \cdot (1\,2\,4)^2 = (1\,4\,2)$

  Så $a^8 \notin G_4 = \{id, (1\,2\,3), (1\,3\,2)\}$.

6 Eulers φ-funksjon er definert på de positive heltallene som

$$\varphi(n) = \text{antall positive heltall} < n \text{ som er relativt primiske til } n \ (\gcd(x,n)=1).$$

for alle $n \in \mathbb{N}$.

Vi skal finne $0 \le x \le 20$ slik at $2^{3456} \equiv x \pmod{21}$

Vi har at $\varphi(21) = 12$, og Eulers teorem sier da at

$$a^{12} \equiv 1 \pmod{21}$$

for alle a med $\gcd(a,21)=1$, spesielt for $a=2$.

Vi har at $3456 = 12 \cdot 288$, og dermed er

$$\underline{\underline{2^{3456}}} = (2^{12})^{288} \equiv 1^{288} \underline{\underline{\equiv 1 \pmod{21}}}.$$

7 a) Vi har at
$$0^3 + 2\cdot 0 + 1 = 1 \in \mathbb{Z}_3$$
$$1^3 + 2\cdot 1 + 1 = 1 \in \mathbb{Z}_3$$
$$2^3 + 2\cdot 2 + 1 = 1 \in \mathbb{Z}_3$$

Så $p(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$ har ingen nullpunkter.

Da $p(x)$ er av grad 3, er det dermed irreduktibelt i $\mathbb{Z}_3[x]$, siden det ikke har noen lineære faktorer.

Siden $p(x)$ er irreduktibelt, er $\langle p(x) \rangle$ et maksimalt ideal. Dermed vil igjen $F = \mathbb{Z}_3[x]/\langle p(x) \rangle$ være en kropp.

b) F har $3^3 = 27$ elementer, så $F \setminus \{0\}$ har 26 elementer. Ordenen til et element deler ordenen til gruppa, så elementene i $F \setminus \{0\}$ har orden 1, 2, 13 eller 26. Vi må finne et element α ulikt $1 + \langle p(x) \rangle$ som har egenskapen at $\alpha^2 \neq 1 + \langle p(x) \rangle$ og $\alpha^{13} \neq 1 + \langle p(x) \rangle$.

La $\alpha = x + \langle p(x) \rangle \in F \setminus \{0\}$

Da har vi
$$\begin{aligned}
\alpha^2 &= x^2 + \langle p(x) \rangle \neq 1 + \langle p(x) \rangle \\
\alpha^3 &= x^3 + \langle p(x) \rangle = x + 2 + \langle p(x) \rangle \\
\alpha^4 &= x^2 + 2x + \langle p(x) \rangle \\
\alpha^5 &= 2x^2 + x + 2 + \langle p(x) \rangle \\
\alpha^6 &= x^2 + x + 1 + \langle p(x) \rangle \\
\alpha^7 &= x^2 + 2x + 2 + \langle p(x) \rangle \\
\alpha^8 &= 2x^2 + 2 + \langle p(x) \rangle \\
\alpha^9 &= x + 1 + \langle p(x) \rangle \\
\alpha^{10} &= x^2 + x + \langle p(x) \rangle \\
\alpha^{11} &= x^2 + x + 2 + \langle p(x) \rangle \\
\alpha^{12} &= x^2 + 2 + \langle p(x) \rangle \\
\alpha^{13} &= 2 + \langle p(x) \rangle \neq 1 + \langle p(x) \rangle
\end{aligned}$$

Vi ser at α har orden > 13, og dermed orden 26.

Dermed er $\underline{\alpha = x + \langle p(x) \rangle}$ en generator for $F \setminus \{0\}$.