Fasit til TMA 4150
Algebra & tallteori.
12. aug. 2004

Opg. 1

a)
$\mathbb{Z}_{16}$
$\mathbb{Z}_2 \times \mathbb{Z}_8$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$
$\mathbb{Z}_4 \times \mathbb{Z}_4$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Vi har at $\langle u \rangle = \mathbb{Z}_{16}$ for $u \in \mathbb{Z}_{16}$ hvis & bare hvis gcd. $(u, 16) = 1$, så
$\{1, 3, 5, 7, 9, 11, 13, 15\}$ er alle elementer som genererer $\mathbb{Z}_{16}$.

b) Et element $(u, v, w) \in \mathbb{Z}_6 \times \mathbb{Z}_4 \times \mathbb{Z}_{10}$ er en enhet hvis & bare hvis u er en enhet i $\mathbb{Z}_6$, v enhet i $\mathbb{Z}_4$ & w enhet i $\mathbb{Z}_{10}$

Enhetene i $\mathbb{Z}_6$: $\{1, 5\}$
$\mathbb{Z}_4$: $\{1, 3\}$
$\mathbb{Z}_{10}$: $\{1, 3, 7, 9\}$

Vi får da at G har $2 \cdot 2 \cdot 4 = 16$ elementer.

Ser at $\{1, 5\}$ gir den abelske gruppa $\mathbb{Z}_2$ som undergruppe av gruppa $(\mathbb{Z}_6, \cdot)$.
Vi får også at $\{1, 3\}$ er $\mathbb{Z}_2$ som undergruppe av $(\mathbb{Z}_4, \cdot)$.

Siden $3^2 = 9$, og $3 \cdot 9 = 7$ i $\mathbb{Z}_{10}$, så må $\{1,3,7,9\}$ være isomorf med $\mathbb{Z}_4$ som undergruppe av $\mathbb{Z}_{10}$.

Dette gir at $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{10}$

Opg 2

a) La A_n være undermengden av S_n bestående av like permutasjoner, og B_n være den bestående av odd.

Definer en funksjon $\varphi : A_n \longrightarrow B_n$ ved å la $\varphi(\tau) = \sigma\tau$, hvor $\sigma = (1,2)$.

φ er 1-1: Anta $\varphi(\tau) = \varphi(\tau')$

$$\sigma\tau = \sigma\tau' \Rightarrow \tau = \tau'$$

φ er på: La $\tau \in B_n$, da er $\sigma\tau \in A_n$, og

$$\varphi(\sigma\tau) = \sigma\sigma\tau = \tau$$

Siden φ er 1-1 & på, så er $|A_n| = |B_n|$.

b) $A_4 = \{(1), (1,2,3), (1,2,4), (1,3,4), (1,4,2), (1,4,3), (1,3,2)$
$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (2,3,4), (2,4,3)\}$

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

Venstre restklasser:

$(1)H = H$

$(1,2,3)H = H$

$(1,3,2)H = H$

$(1,2,4)H = \{(1,2,4), (1,4)(2,3), (1,3,4)\} = (1,4)(2,3)H = (1,3,4)H$

$(1,4,2)H = \{(1,4,2), (2,3,4), (1,3)(2,4)\} = (2,3,4)H = (1,3)(2,4)H$

$(1,4,3)H = \{(1,4,3), (1,2)(3,4), (2,4,3)\} = (1,2)(3,4)H = (2,4,3)H$

Høyre restklasser:

$H(1) = H = H(1,2,3) = H(1,3,2)$

$H(1,2,4) = \{(1,2,4), (1,3)(2,4), (2,4,3)\} = H(1,3)(2,4) = H(2,4,3)$

$H(1,3,4) = \{(1,3,4), (2,3,4), (1,2)(3,4)\} = H(2,3,4) = H(1,2)(3,4)$

$H(1,4,2) = \{(1,4,2), (1,4,3), (1,4)(2,3)\} = H(1,4,3) = H(1,4)(2,3)$

Vi ser at venstre & høyre restklasser ikke er like, f. eks. er $(1,2,4)H \neq H(1,2,4)$, derfor er H ikke normal i A_4.

Opg 3

a) La $A, B \in H$. Da er $\det(AB) = \det(A) \cdot \det(B) = (\pm 1)(\pm 1)$
$= \pm 1 \Rightarrow AB \in H$

$\det I = 1 \Rightarrow I \in H$

La $A \in H$, da er $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{\pm 1} = \pm 1$
$\Rightarrow A^{-1} \in H$
$\Rightarrow$ H er en undergruppe av G.

La $A \in H$ og $B \in G$, da er
$\det(BAB^{-1}) = \det(B) \det(A) \frac{1}{\det(B)} = \det(A) = \pm 1$
$\Rightarrow BAB^{-1} \in H \Rightarrow$ H er normal undergruppe av G.

b) La $\varphi : G \longrightarrow \mathbb{R}^+$ være gitt ved
$$\varphi(A) = |\det(A)|$$
Ser at $\varphi(AB) = |\det(AB)| = |\det(A) \det(B)|$
$= |\det(A)| |\det(B)| = \varphi(A) \varphi(B)$,
så φ er en gruppe homomorfi.

For $r \in \mathbb{R}^+$ ser vi at
$$\varphi\left(\begin{bmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = r$$, så φ er på

$\ker \varphi = \{B \in G \mid \varphi(B) = 1\} = \{B \in G \mid |\det(B)| = 1\}$
$= H$
$$\Rightarrow G/H \simeq \mathbb{R}^+$$

c)

La $A, B \in K$

Da er $\det(AB) = \det(A) \cdot \det(B) = (\pm 2)(\pm 2) = \pm 4$

$\Rightarrow AB \notin K$, så K er ingen undergruppe av G.

Opg 4

Først må vi vise at $*: G \times X \longrightarrow X$, hvor $g * (aH) = (ga)H$, er en veldefinert avbildning.

La $aH = bH$. Da er $b = ah$ for en $h \in H$.

La $g \in G$. Da er
$$g * (bH) = (gb)H = (gah)H = (ga)H = g * (aH)$$
så avbildningen er veldefinert.

Undersøker så om X er en G-mengde:

1) $e * (aH) = (ea)H = aH$

2) $(g_1 g_2) * (aH) = (g_1 g_2 a)H = g_1 * ((g_2 a)H)$
$= g_1 * (g_2 * (aH))$

$\Rightarrow X$ er en G-mengde.

Opg 5

a) Anta at $\langle p(x) \rangle \subseteq N \subseteq F[x]$. Siden alle idealer i $F[x]$ er generert av ett element, har vi at $N = \langle g(x) \rangle$ for et polynom $g(x) \in F[x]$.

Siden $\langle p(x) \rangle \subseteq \langle g(x) \rangle$ har vi at $p(x) \in \langle g(x) \rangle$, og dermed $\exists\, q(x) \in F[x]$ slik at $p(x) = g(x)\, q(x)$. Siden $p(x)$ er irredusibelt må enten $g(x) \in F$ eller $q(x) \in F$.
Hvis $g(x) \in F$, så er $N = F[x]$, og hvis $q(x) \in F$ så er $\langle p(x) \rangle = N \Rightarrow$
$\langle p(x) \rangle$ er et maksimalt ideal i $F[x]$.

b) $p(0) = 1$ & $p(1) = 1$, så $p(x)$ har ingen lineare faktorer i $\mathbb{Z}_2[x]$

$x^2 + x + 1$ er det eneste irreducible 2-grads polynomet i $\mathbb{Z}_2[x]$.

$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1 \neq p(x)$

$\Rightarrow x^4 + x + 1$ er irredusibelt.

c) Siden $p(x) = x^4 + x^2 + 1$ er irredusibelt over $\mathbb{Z}_2[x]$, så vil $\langle p(x) \rangle$ være et maksimalt ideal, og dermed blir $\mathbb{Z}_2[x] / \langle p(x) \rangle$ en kropp.

La $\alpha = x + \langle p(x) \rangle$, da vil elementene i $\mathbb{Z}_2[x] / \langle p(x) \rangle$ være på formen $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ hvor $a_i \in \mathbb{Z}_2$ og $\alpha^4 = \alpha + 1$. Ser dermed at $\left| \mathbb{Z}_2[x] / \langle p(x) \rangle \right| = 2^4 = 16$.