Løsningsforslag, eksamen i Algebra og Tallteori 2006

① a) $\mathbb{Z}_4 \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

b) Siden enheter i $\mathbb{Z}_7$ har orden 1, 2, 3 eller 6 i $\mathbb{Z}_7^*$, er det ingen elementer i gruppen av enheter i $\mathbb{Z}_2 \times \mathbb{Z}_7$ som har orden 4 eller 9.

$\Rightarrow$ (gp. av enheter i $\mathbb{Z}_2 \times \mathbb{Z}_7$) $\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

② a) • $a, b \in U$

$\Rightarrow (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$ (med assosiativitet i $R$)

$\Rightarrow U$ lukket under den binære operasjonen.

• assosiativitet i $U$ følger fra assosiativitet i $R$

• $1 \cdot a = a \cdot 1 = a$ $\forall\, a \in U$, siden dette gjelder $\forall\, a \in R$.

• $a \in U \Leftrightarrow \exists\, a^{-1} \in R$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1 \Leftrightarrow a^{-1} \in U$

$\Rightarrow U$ er en gruppe.

b) Enhetene i $R = \mathbb{Z}/n\mathbb{Z}$ er de restklassene som representeres av heltall $a$ med $\gcd(a, n) = 1$. Antall slike er $\varphi(n)$ (per def. av $\varphi$). Altså er $|U| = \varphi(n)$. Ordenen til et element deler ordenen til gruppa, så dermed er $a^{\varphi(n)} = (a^{\mathrm{ord}(a)})^k = 1^k = 1 \in U$ $\forall\, a \in U$.

Def. av $\varphi$: $a^{\varphi(n)} \equiv 1 \pmod{n}$, for $\gcd(a, n) = 1$.

③ a) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ må være med i $H_{r,s}$, så enten $r = 1$ eller $s = 1$. Anta $r = 1$. Da er $s > 1$. La $S$ være en matrise med $\det S = s$, så $S \in H_{r,s}$. Men $\det(S \cdot S) = \det(S)^2 = s^2 > s$, så $S^2 \notin H_{r,s}$, og $H_{r,s}$ er ikke lukket under (matrise-)multiplikasjon. Dermed må $s = 1$, og $r < 1$. La $R$ være en matrise med $\det(R) = r$, så $R \in H_{r,s}$. $\det(R^2) = \det(R)^2 = r^2 \neq r$ (siden $r \neq 1$ og $r \neq 0$).

Vi må derfor ha $r^2=1$, altså $r=-1$, for at $H_{r,s}$ skal være lukket under multiplikasjon.

$H_{-1,1}$ er en gruppe:

- $A,B \in H_{-1,1} \Rightarrow \det(AB) = \det A \cdot \det B = (\pm 1)\cdot(\pm 1) = \pm 1 \Rightarrow AB \in H_{-1,1}$
- $\det(A) = \pm 1 \Rightarrow \det(A^{-1}) = \frac{1}{\det(A)} = \pm 1 \Rightarrow A^{-1} \in H_{-1,1}$
- $\det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1 \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H_{-1,1}$

$\Rightarrow H_{-1,1} \leq G$.

b) $H_{-1,1} \trianglelefteq G$ fra a).

La $X \in G$, $A \in H$. Da er $\det(XAX^{-1}) = \det(X)\cdot\det(A)\cdot\det(X^{-1})$

$= \det(X)\cdot\det(A)\cdot\frac{1}{\det(X)} = \det(A) = \pm 1$

$\Rightarrow XAX^{-1} \in H_{-1,1}$

Siden $X$ og $A$ var vilkårlige, er $H_{-1,1}$ normal i $G$.

La

$$\varphi : G \longrightarrow (\mathbb{Q}^+, \cdot)$$

være gitt ved $\varphi(X) = |\det(X)|$ for $X \in G$.

- $\varphi$ er en homomorfi:

$$\varphi(X_1X_2) = |\det(X_1X_2)| = |\det(X_1)\det(X_2)|$$
$$= |\det(X_1)||\det(X_2)| = \varphi(X_1)\cdot\varphi(X_2)$$

- $\varphi$ er på: la $q \in \mathbb{Q}^+$. Da

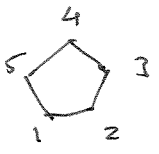
$$\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}\right) = \det\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} = q$$

- $\ker\varphi = \{X \in G \mid |\det(X)| = 1\} = H_{-1,1}$

Vi får dermed at

$$G/H = G/\ker\varphi \cong \varphi[G] = \mathbb{Q}^+$$

(4) a)




$G$ = gp. av symmetrier av 5-kanten
(= dihedral gp. med 10 elementer)

$$G = \{id, \rho = (1\ 2\ 3\ 4\ 5), \rho^2, \rho^3, \rho^4,$$

$$\mu_1 = (25)(34), \mu_2 = (13)(45), \mu_3 = (15)(24), \mu_4 = (12)(35), \mu_5 = (14)(23)\}$$

$$\leq S_5$$

b) La $X$ være mengden av fargeleggingen av (den merkede) femkanten. Da er $X$ en $G$-mengde, og vi vil finne antall baner.

$|X| = 3^5 = 243$

$|X_{id}| = 243$

$|X_\rho| = |X_{\rho^2}| = |X_{\rho^3}| = |X_{\rho^4}| = 3$ (må ha samme farge på alle hjørnene)

$|X_{\mu_1}| = |X_{\mu_2}| = \cdots = |X_{\mu_5}| = 3^3 = 27$ (Eks: $X_{\mu_1}$: må ha samme farge på 2 og 5, og på 3 og 4)

Burnsides formel for antall baner:

$$\#\text{baner} = \frac{1}{6} \cdot \sum_{g \in G} |X_g| = \frac{1}{10}(243 + 4 \cdot 3 + 5 \cdot 27) = \underline{\underline{39}}$$

(5) a) La $a(x) = a_n x^n + \cdots + a_1 x + a_0$, $b(x) = b_m x^m + \cdots + b_1 x + b_0$ være i $R[x]$ med $a_n \neq 0$, $b_m \neq 0$. Da er

$$a(x) \cdot b(x) = a_n b_m x^{n+m} + (\text{ledd av lavere grad})$$

Siden $R$ er et integritetsområde, er $a_n \cdot b_m \neq 0$, og $a(x) \cdot b(x) \neq 0$ i $R[x]$.

$\Rightarrow R[x]$ har ingen nullotdisorer

$\Rightarrow R[x]$ er et integritetsområde.

b) $p(x) = (x+1)^2(x+2)(x^2+x+2) \in \mathbb{Z}_3[x]$

$x^2+x+2$ har ingen nullpkt i $\mathbb{Z}_3$ og er av grad $\leq 3$

$\Rightarrow x^2+x+2$ er irred. i $\mathbb{Z}_3[x]$

⑥ (MA2201)

$|G| = 105 = 3 \cdot 5 \cdot 7$

$r$ = # Sylow 7-undergp = 1 eller 15
$s$ = # Sylow 5-undergp = 1 eller 21

} Siden # Sylow p-u.gp. er kongruent 1 modulo p og deler $|G|$

Anta $r=15$ og $s=21$. En Sylow 7-undergruppe har 7 elementer. Snittet av to ulike slike er en undergruppe av begge, og må derfor være $\{e\}$ ved Lagranges teorem (siden 7 er et primtall). Følgelig vil hver Sylow 7-undergruppe ha 6 elementer som ikke er i noen av de andre Sylow 7-undergruppene. Dermed er det $15 \cdot 6 = 90$ distinkte elementer av orden 7 i $G$.
På samme måte: Det må være $21 \cdot 4 = 84$ elementer av orden 5.
Tatt sammen blir dette $90+84 = 174$ distinkte elementer, og dette er en selvmotsigelse da $|G| = 105$.
Altså må $r=1$ eller $s=1$.

---

La $P$ være en Sylow p-undergruppe. Da er $g^{-1}Pg$ en undergruppe av $G$, med $|g^{-1}Pg| = |P|$ for alle $g \in G$.
Så $g^{-1}Pg$ er også en Sylow p-undergruppe. Dersom det bare er én Sylow p-undergruppe, må derfor $g^{-1}Pg = P$ for alle $g \in G$. $P$ er derfor normal
$\Rightarrow$ Siden enten $r=1$ eller $s=1$, har $G$ en normal undergruppe.

(6) (TMA4150)

$f(x) = x^4 + x + 1$ har ingen nullpkt i $\mathbb{Z}_2$

$\Rightarrow$ $f(x)$ har ingen lineære faktorer i $\mathbb{Z}_2[x]$

$\Rightarrow$ Hvis $f(x)$ er reduserbelt, er $f(x)$ et produkt av to irreduserible andregradspolynom.

$x^2+x+1$ eneste irreduserible andregradspolynom i $\mathbb{Z}_2[x]$:

$x^2 = x \cdot x$ - reduserbelt

$x^2+1 = (x+1)(x+1)$ - reduserbelt

$x^2+x = x\cdot(x+1)$ - reduserbelt

$x^2+x+1$ : ingen nullpkt i $\mathbb{Z}_2$ & grad $\leq 3$

$\Rightarrow$ irreduserbelt

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

$\Rightarrow (x^2+x+1) \nmid f(x)$

$\Rightarrow f(x)$ irreduserbelt

$\Rightarrow \langle f(x)\rangle$ er et maks. ideal i $\mathbb{Z}_2[x]$

$\Rightarrow \mathbb{Z}_2[x]/\langle f(x)\rangle$ er en kropp.

---

$|F\setminus\{0\}| = 15 \Rightarrow$ ordenen til et element er 1, 3, 5 el. 15

La $\alpha = x + \langle f(x)\rangle$. Da er

$\alpha^2 = x^2 + \langle f(x)\rangle \neq 1 + \langle f(x)\rangle$

$\alpha^3 = x^3 + \langle f(x)\rangle \neq 1 + \langle f(x)\rangle$

$\alpha^4 = x^4 + \langle f(x)\rangle = (x^4+x+1) + (x+1) + \langle f(x)\rangle = x+1 + \langle f(x)\rangle \neq 1 + \langle f(x)\rangle$

$\alpha^5 = x^2+x + \langle f(x)\rangle \neq 1 + \langle f(x)\rangle$

$\Rightarrow \text{ord}(\alpha) > 5$

$\Rightarrow \text{ord}(\alpha) = 15$

$\Rightarrow \alpha$ generer $F\setminus\{0\}$.