Eksamen, algebra (og tallteori) 30. mai 2007.

① a) Det er 3 ikke-isomorfe abelske grupper av orden 40:

- $\mathbb{Z}_8 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$

b) G = gp. av enheter i $\mathbb{Z}_5 \times \mathbb{Z}_{11}$ under multiplikasjon.

- Det er $\varphi(5) = 4$ enheter i $\mathbb{Z}_5$, og $\varphi(11) = 10$ enheter i $\mathbb{Z}_{11}$. $(u,v) \in \mathbb{Z}_5 \times \mathbb{Z}_{11}$ er en enhet hvis og bare hvis u er en enhet i $\mathbb{Z}_5$ og v er en enhet i $\mathbb{Z}_{11}$. Dermed har G $4 \cdot 10 = 40$ elementer.
- ordenen til (u,v) i $\mathbb{Z}_5 \times \mathbb{Z}_{11}$ (multiplikativt) er minste felles multiplum av den multiplikative ordenen til hhv. u i $\mathbb{Z}_5$ og v i $\mathbb{Z}_{11}$.
u har orden 1, 2 eller 4 og v har orden 1, 2, 5 eller 10.
Dermed kan $(u,v) \in G$ ikke ha orden 40, så $G \neq \mathbb{Z}_8 \times \mathbb{Z}_5$.
Videre har $(2,1) \in G$ orden 4, så $G \neq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.
Vi konkluderer med at

$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5.$$

(2) (i) $9x \equiv 7 \pmod{12}$ (*)

$\gcd(9,12) = 3 \nmid 7 \Rightarrow$ (*) har ingen løsninger.

(ii) $6x \equiv 9 \pmod{15}$ (**)

$\gcd(6,15) = 3 \mid 9 \Rightarrow$ (**) har løsninger.

Deler gjennom med $\gcd(6,15)$:

$2x \equiv 3 \pmod 5$

$\Rightarrow x \equiv 4 \pmod 5$

Løsningene er gitt ved $x \in 4 + 5\mathbb{Z} = \{\ldots, -1, 4, 9, 14, \ldots\}$

(3)

$\varphi : U \longrightarrow D$

$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$

- φ er en homomorfi:

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) = \varphi\begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ 0 & cc' \end{pmatrix}$$

$$\varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\varphi\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\cdot\begin{pmatrix} a' & 0 \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ 0 & cc' \end{pmatrix}$$

- φ er på:

La $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in D$. Da er $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in U$ og $\varphi\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.

- $\ker\varphi = T$:

$$\ker\varphi = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in U \mid \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in U \mid \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in U\right\} = T.$$

Dermed har vi en isomorfi av grupper: $U/T = U/\ker\varphi \cong \operatorname{im}\varphi = D$

(4) $a \in I$, a enhet.

Siden $a \in I$ og $a^{-1} \in R$ er $1 = a \cdot a^{-1} \in I$.

Dermed er, $\forall r \in R$, $r = r \cdot 1 \in I$, så $R \subseteq I$.

Siden $I \subseteq R$, er $R = I$.

(5) Enhetene kan ikke være nullelinisorer ($ab = 0$ & a enhet $\Rightarrow b = a^{-1}ab = 0$)

I R er disse $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ og $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ er per. def. ikke en nullelinisor.

Alle andre elementer er nullelinisorer:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Nullelinisorer i R: $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

(6)

- Z er en undergruppe:
  - $eg = g = ge \ \forall g$ per def. av id. elementet $\Rightarrow e \in Z$.
  - $a, b \in Z \Rightarrow (ab)g = agb = g(ab) \ \forall g \in G \Rightarrow ab \in Z$.
  - $a \in Z \Rightarrow ag = ga \ \forall g \in G = a^{-1}agg^{-1} = a^{-1}gaa^{-1} \ \forall g \in G$
    $\Rightarrow ga^{-1} = a^{-1}g \ \forall g \in G \Rightarrow a^{-1} \in Z$.

  $\Rightarrow Z \leq G$.
- Z er normal: For alle $z \in Z$ og $g \in G$ er $gzg^{-1} = zgg^{-1} = z \in Z$

  Så Z er en normal undergruppe.

- G ikke abelsk $\Rightarrow G/Z$ ikke syklisk:

Anta G/Z er syklisk, generert av (aZ).

Da kan alle restklassen skrives som $a^t Z$ for en eller annen $t \in \mathbb{Z}$.

La $x, y \in G$. x og y vil ligge i restklasser:

$x \in a^{t_1} Z$, så $x = a^{t_1} z_1$ for en $z_1 \in Z$

$y \in a^{t_2} Z$, så $y = a^{t_2} z_2$ for en $z_2 \in Z$.

$$\Rightarrow xy = a^{t_1} z_1 \cdot a^{t_2} z_2 = a^{t_1+t_2} z_1 z_2 = a^{t_2+t_1} z_2 z_1$$
$$= a^{t_2} z_2 \cdot a^{t_1} z_1 = y \cdot x$$

Her har vi altså brukt at $z_1, z_2 \in Z$.

Siden x og y var vilkårlige, er G abelsk.

(Som vi sjøl gir $Z = G$ og G/Z trivielt.)

(7) (i) $A_4 = \{ id = (), (123), (132), (124), (142),$
$(134), (143), (234), (243),$
$(12)(34), (13)(24), (14)(23) \}$

(ii) X_g = mengden av fargelegginger som blir holdt fast av $g \in A_4$.

$|X_{id}| = 2^4$ (fritt valg på alle hjørnene)

$|X_g| = 2^2$ for g en 3-sykel ($g = (abc)$ m a, b, c må ha samme farge, og dermed er resten gitt av det siste hjørnet.)

$|X_\mu| = 2^2$ for $\mu = (ab)(cd)$ (disjunkt) (må ha samme farge på a og b, og på c og d.

Burnside-formelen gir da

$$\#\text{fargelegginger} = \frac{1}{|A_4|}\sum_{g\in A_4}|X_g|$$

$$= \frac{1}{12}(16+11\cdot 4) = \underline{\underline{5}}$$

⑧ (TMA4150)

- f er irreduserbar:
  - $f(0)=1$, $f(1)=1$ $\Rightarrow$ f har ingen nullpkt over $\mathbb{Z}_2$, så f har ingen lineære faktorer i $\mathbb{Z}_2[x]$.
  - x^2+x+1 er eneste irreduserbare 2. gradspolynom i $\mathbb{Z}_2[x]$:
    - $0^2+0+1=1$, $1^2+1+1=1$ $\Rightarrow$ x^2+x+1 har ingen lineære faktorer, og må derfor være irreduserbart.
    - $x^2+x = x(x+1)$
    - $x^2 = x\cdot x$
    - $x^2+1 = (x+1)(x+1)$
  - $f(x) \neq (x^2+x+1)^2$:

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

$\Rightarrow f(x)$ er irreduserbart i $\mathbb{Z}_2[x]$.

- Dermed er $\langle f(x)\rangle$ et maksimalt ideal i den kommutative ringen $\mathbb{Z}_2[x]$. Følgelig er $\mathbb{Z}_2[x]/\langle f(x)\rangle$ en kropp.
- $F\setminus\{0\}$ har 15 elementer. Alle elementer har orden 1, 3, 5 eller 15. La $\alpha = x+\langle f(x)\rangle$

$$x+\langle f(x)\rangle \neq 1+\langle f(x)\rangle$$
$$x^2+\langle f(x)\rangle$$
$$x^3+\langle f(x)\rangle \neq 1+\langle f(x)\rangle$$
$$x^4+\langle f(x)\rangle = x^3+x+\langle f(x)\rangle$$
$$x^5+\langle f(x)\rangle = x^4+x+\langle f(x)\rangle = x^3+x+1+\langle f(x)\rangle \neq 1+\langle f(x)\rangle$$

$\Rightarrow \text{ord}(\alpha) > 5$, $\Rightarrow \text{ord}(\alpha) = 15$, $\Rightarrow \alpha$ er en generator for $F\setminus\{0\}$

(8) (MA2201)

(i) $|G_1| = 21 = 3 \cdot 7$.

Sylow 7-undergrupper er en divisor i 21 og kongruent 1 mod 7.

Eneste mulighet er at det kun er én slik undergruppe, S_7.

Siden gS_7g^{-1} er en undergruppe av G med like mange elementer som S_7. Siden S_7 er den eneste Sylow 7-gruppen, er da $gS_7g^{-1} = S_7$. Siden g var vilkårlig, er S_7 derfor en normal undergruppe (med 7 elementer).

(ii) Siden p og q er forskjellige, kan vi anta (uten tap av generalitet) at $p > q$.

Sylow p-undergrupper i G_2 er da en divisor i $|G_2| = pq$ og kongruent 1 modulo p. Siden $q < p$ er eneste mulighet at det kun er én Sylow p-undergruppe. Denne er normal med samme argument som i (i).