Eksamen i Algebra og Talteori 11. august, 2007.

1 a) Det finnes 3 abelske grupper av orden 8, opp til isomorfi:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \,,\quad \mathbb{Z}_4 \times \mathbb{Z}_2 \,,\quad \mathbb{Z}_8$$

b) $|\mathbb{Z}_4 \times \mathbb{Z}_8| = 32$.

$\langle (1,2) \rangle = \{(1,2), (2,4), (3,6), (0,0)\} \leq \mathbb{Z}_4 \times \mathbb{Z}_8$

$\Rightarrow \left| \mathbb{Z}_4 \times \mathbb{Z}_8 / \langle (1,2) \rangle \right| = 8 \Rightarrow$ Denne faktorgruppa er isomorf med en av gruppene i a).

Ser at $(0,1) \notin \langle (1,2) \rangle$

$(0,1) + (0,1) = (0,2) \notin \langle (1,2) \rangle$

$(0,1) + (0,1) + (0,1) + (0,1) = (0,4) \notin \langle (1,2) \rangle$

Siden ordenen til et element deler ordenen til gruppa, må derfor $(0,1) + \langle (1,2) \rangle$ ha orden 8 i $\mathbb{Z}_4 \times \mathbb{Z}_8 / \langle (1,2) \rangle$.

Følgelig er $\mathbb{Z}_4 \times \mathbb{Z}_8 / \langle (1,2) \rangle \cong \underline{\underline{\mathbb{Z}_8}}$.

2 $\sigma = (3,4)(1,4)(2,5) \in S_5$

$\sigma = (1,3,4)(2,5)$

$\Rightarrow |\langle \sigma \rangle| = \operatorname{lcm}(3,2) = 6 \Rightarrow \underline{\underline{(S_5 : \langle \sigma \rangle)}} = \dfrac{|S_5|}{|\langle \sigma \rangle|} = \dfrac{120}{6} = \underline{\underline{20}}$

$\langle \sigma \rangle = \{ \overset{\sigma}{(1,3,4)(2,5)}, \overset{\sigma^2}{(1,4,3)}, \overset{\sigma^3}{(2,5)}, \overset{\sigma^4}{(1,3,4)}, \overset{\sigma^5}{(1,4,3)(2,5)}, id \}$

Ser at $(1,2)\underbrace{(2,5)}_{\in \langle \sigma \rangle}(1,2)^{-1} = (1,2)(2,5)(1,2) = (1,5) \notin \langle \sigma \rangle$

så $\langle \sigma \rangle$ er ikke normal i S_5.

3 i) Viser: (ab) har orden $n \Rightarrow (ba)$ har orden n

- $(ab)^n = \underbrace{abab\cdots ab}_{n \times ab} = e$

  $\Rightarrow b(ab)^n = b\underbrace{abab\cdots ab} = be = b$

  $\Rightarrow b(ab)^n b^{-1} = b\underbrace{abab\cdots ab}\underbrace{b^{-1}} = (ba)^n = b \cdot b^{-1} = e$

  $\Rightarrow$ ordenen til ba er ikke større enn n.

- Anta $(ba)^k = e$ for en $1 \leq k < n$.
  Tilsvarende argument som over gir at da må $(ab)^k = e$, noe som er umulig, da (ab) har orden n.

Så (ba) har orden n.

ii) La $X = \{g \in G \mid g \text{ har orden } 2\}$

$Y = \{g \in G \mid g \text{ har orden } > 2\}$

Da er $G = X \cup Y \cup \{e\}$ (disjunkt union)

Y må ha et partall antall element, for vi kan parre dem slik: $Y = \{y_1, y_1^{-1}, y_2, y_2^{-1}, \ldots, y_k, y_k^{-1}\}$

Hvis $|G| = 2m$ har vi da

$$|G| = |X| + |Y| + |\{e\}|$$

$$2m = |X| + 2k + 1$$

$$|X| = 2(m-k) - 1 \quad \text{, et oddetall.}$$

4 For et hvert positivt heltall n er

$\varphi(n) = |\{x \in \mathbb{Z} \mid 1 \leq x \leq n \ \& \ \gcd(x,n) = 1\}$

Eulers teorem sier at hvis $\gcd(a,n) = 1$, så er $a^{\varphi(n)} \equiv 1 \pmod{n}$.
Siste siffer i et tall er resten vi får modulo 10.
$\varphi(10) = 4$, så

$$7^{1000000} = 7^{4 \cdot (250000)} = (7^{\varphi(10)})^{250000} \equiv 1^{250000} \equiv 1 \pmod{10}$$

Så det siste sifferet i $7^{1000000}$ er 1.

5

1	2	3
4	5	6
7	8	9

X = mengden av alle fargeleggingen av brettet (uten rotasjon)

$|X| = 3^9$

$\mathbb{Z}_4$ virker på X med rotasjon av brettet.

$|X_{id}| = |X| = 3^9$

$|X_\rho| = 3^3$ $\quad$ ρ: rotasjon $90°$ med klokka

$\{1,3,7,9\}$ må ha samme farge

$\{2,4,6,8\}$ — " —

$|X_{\rho^2}| = 3^5$ $\quad$ $\{1,9\}$ må ha samme farge

$\{2,8\}$ — " —

$\{3,7\}$ — " —

$\{4,6\}$ — " —

$|X_{\rho^3}| = 3^3$ $\quad$ (som for ρ)

Burnsides formel gir antall baner:

$$\#\text{baner} = \frac{1}{|\mathbb{Z}_4|} \sum_{g \in \mathbb{Z}_4} |X_g| = \frac{1}{4}(3^9 + 3^3 + 3^5 + 3^3)$$

$$= 4995$$

Og dette er også antall essensielt forskjellige fargelegginger.

- La $h(x) = h_0 + h_1 x + \dots + h_r x^r \in \mathbb{Z}_5[x]$ og $g(x) = g_0 + g_1 x + \dots + g_s x^s \in \mathbb{Z}_5[x]$, hvor $h_r \neq 0$ og $h_s \neq 0$.

  Da er $(h \cdot g)(x) = (\dots) + h_r g_s x^{r+s}$.

  Siden $\mathbb{Z}_5$ er et integritetsområde, er $h_r g_s \neq 0$, så graden til $(h \cdot g)(x)$ er $r+s$.

- <u>Enheter</u>: for å få $(h \cdot g)(x) = 1$ må $r = s = 0$.

  Vi får at enhetene i $\mathbb{Z}[x]$ er alle polynom av grad 0 som ikke er nullpolynomet.

- <u>Nulldivisorer</u>: hvis $h(x) \neq 0$ og $g(x) \neq 0$ har vi $(h \cdot g)(x) \neq 0$ (fra det øverste punktet)

  Dermed er det <u>ingen</u> nulldivisorer, og <u>$\mathbb{Z}_5[x]$ er et integritetsområde</u>.

- Siden f.eks. $f(x) = x+1$ ikke er en enhet (se over), er $\mathbb{Z}_5[x]$ <u>ikke</u> en kropp.

7 a) $x^5 + x^4 + 1$ har ingen nullpkt i $\mathbb{Z}_2$, og dermed ingen lineære faktorer i $\mathbb{Z}_2[x]$. Vi kan faktorisere $p(x)$ som $x^5 + x^4 + 1 = (x^2+x+1)(x^3+x+1)$. Disse faktorene er irreducible, og generer derfor maksimale ideal. $p(x)$ ligger i begge disse idealene:

$$p(x) \in \langle (x^2+x+1) \rangle \quad \text{og} \quad p(x) = \langle (x^3+x+1) \rangle.$$

b) Som nevnt i a) er $\langle (x^3+x+1) \rangle$ maksimalt, siden x^3+x+1 er irreducibelt, og dermed er F en kropp.

F har 8 element, så $F \setminus \{0\}$ har orden 7.

La $\alpha = x + \langle (x^3+x+1) \rangle$. Da er $\mathrm{ord}(\alpha) = 7$, siden $\alpha \neq 1 + \langle (x^3+x+1) \rangle$ og $\mathrm{ord}(\alpha) \mid 7$ $\Rightarrow \alpha$ generator.