Øving 13 - TMA4150 - Ailo Aasen

SEKSJON 23

13 Et polynom av grad 3 over en kropp er reduserbelt hvis og bare hvis det har et nullpunkt i kroppen. Ved å evaluere $2x^3+x^2+2x+2$ i alle elementer i $\mathbb{Z}_5[x]$ finner vi at det ikke har noen nullpunkter, så polynomet er irreduserbelt. de

14 $a \in \mathbb{Q}$ er et nullpunkt for $f(x)$ bare hvis $a|2$. $f(-2)=-14$, $f(-1)=-11$, $f(1)=7$, $f(2)=18$. Siden ingen av divisorene av 2 er et nullpunkt, er $f(x)$ irreduserbelt over $\mathbb{Q}$. Siden vi kan skrive $f(x)=x^2+2\cdot 4x+4^2-4^2-2=(x+4)^2-18$, ser vi at $x=\pm\sqrt{18}-4$ er to nullpunkter, så $f(x)$ er reduserbelt over $\mathbb{R}[x]$ Siden $\mathbb{R} \leq \mathbb{C}$, er $f(x)$ også reduserbelt over $\mathbb{C}$. de

34 Fermats teorem gir at $x^p=x \ \forall x \in \mathbb{Z}_p$. spesielt er $(-a)^p=-a$, så $(x+a)|(x^p+a)$. Siden $p>1$, betyr dette at x^p+a er reduserbelt over $\mathbb{Z}_p$.

de

SESSION 26

12 Siden $\mathbb{Z}$ er et integritetsområde og $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$, får vi et eksempel for hvert primtall p.

13 $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$, og i $\mathbb{Z}_4$ er $2^2 = 0$.

14 $\mathbb{Z}_6$ er en ring med 0-divisorer, siden $2 \cdot 3 = 0$. $I = \{0,2,4\}$ er et ideal i $\mathbb{Z}_6$, og $\mathbb{Z}_6/I \simeq \mathbb{Z}_3$, og $\mathbb{Z}_3$ er et integritetsområde.

18 La $\phi : F \to R$ være en homomorfi fra en kropp F til en ring R. Hvis $\ker\phi = \{0_F\}$ er ϕ 1-1. Anta $0_F \neq a \in F$ er i $\ker(\phi)$. Da vil $\phi(a) = 0_R \Rightarrow \phi(a)\phi(b) = 0_R\,\phi(b) = 0 \Rightarrow \phi(ab) = 0_R \;\forall b \in F$. Men da er $\phi(c) = 0_R \;\forall c \in F$; bare la $b = a^{-1}c$.

Ekvt
$\ker\phi \subset F$ ideal
siden F er en kropp
er idealen lik
0 eller F
$\Leftrightarrow \ker\phi = 0 \vee \ker\phi = F$

22 a) At $(\phi[N], +) \leq (\phi[R], +)$ følger av gruppeteori siden $(N,+) \leq (R,+)$.

La h være i R, og la n være i N. Da er $\phi(h)\phi(n) = \phi(hn)$, $\phi(n)\phi(h) = \phi(nh)$. Siden N er et ideal i R, følger det at $\phi(h)\phi(n), \phi(n)\phi(h) \in \phi[N]$ ■

b) Betrakt $\phi: \mathbb{Z} \to \mathbb{R}$ gitt ved $\phi(n) = n$. Vi har at $\mathbb{Z}$ er et ideal av $\mathbb{Z}$, men $\phi[\mathbb{Z}] = \mathbb{Z}$ er ikke et ideal av $\mathbb{R}$, siden $\sqrt{2} \cdot 1 = \sqrt{2} \notin \mathbb{Z}$.

c) Gruppeteori gir at inverse bilder av undergrupper er undergrupper, så $\phi^{-1}[N]$ er i alle tilfeller en additiv undergruppe av R

Hvis N' er et ideal av $\phi[R]$ eller R', må $\phi(h)\phi(n'), \phi(n')\phi(h) \in N'$ $\forall h \in R, n' \in \phi^{-1}[N']$, siden ϕ er en homomorfisme, følger det at hn' og $n'h$ er i $\phi^{-1}[N']$, og vi er ferdige ■

26 Anta $b, c \in I_a$ Da er $a(b+c) = ab + ac = 0 + 0 = 0$, så I_a er lukket under addisjon Vi har selvfølgelig $a0 = 0$ så $0 \in I_a$ Siden $a(-b) = -ab = -0 = 0$, har vi også inverser, så $(I_a, +) \leq (R, +)$

La $n \in I_a$, $h \in R$ Da er $a(hn) = h(an) = h0 = 0$ $a(nh) = 0h = 0$ (siden R er kommutativ), så nh og hn er i R, og vi kan fastslå at I_a er et ideal. ■

27 La I_1, I_2 være idealer i R, da er $(I_1, +)$ og $(I_2, +)$ undergrupper av $(R, +)$, og gruppeteori gir at $(I_1 \cap I_2, +) \leq R$.

La $n \in I_1 \cap I_2$, $h \in R$. Da er $n \in I_1$, og siden I_1 er et ideal, er $nh, hn \in I_1 \cap I_2$. ■

SEKSJON 27.

2 $\langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$ og $\langle 6 \rangle$ er alle ekte, ikke-trivielle idealer i $\mathbb{Z}_{12}$. Vi har $\langle 4 \rangle \leq \langle 2 \rangle$ og $\langle 6 \rangle \leq \langle 2 \rangle$, $\langle 6 \rangle < \langle 3 \rangle$ så kun $\langle 2 \rangle$ og $\langle 3 \rangle$ er maksimale idealer.

7 $\mathbb{Z}_3[x]/\langle x^3 + cx^2 + 1 \rangle$ er en kropp hvis og kun hvis $f(x) = x^3 + cx^2 + 1$ er irreduserbelt over $\mathbb{Z}_3$. Vi har $f(0) = 1$, $f(1) = 2 + c$, $f(2) = 2c$, så vi må ha $c \neq 1$ og $c \neq 0$, og vi står igjen med $c = 2$, som er OK.

18 Siden $x^2 - 5x + 6 = (x-2)(x-3)$, er $x^2 - 5x + 6$ reduserbelt over $\mathbb{Q}$. Det følger at $\mathbb{Q}[x]/\langle x^2 - 5x + 6 \rangle$ ikke er en kropp.

1 a) $40 = 2^3 \cdot 5$. Fundamentalteoremet for end gen. abelsk grupper gir følgende grupper: $\mathbb{Z}_5 \times \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$, altså 3 stykker. du

b) Det er klart at $(a,b) \in \mathbb{Z}_5 \times \mathbb{Z}_{11}$ er enhet hvis og bare hvis a og b er enheter i sine respektive grupper. Enhetene i $\mathbb{Z}_n$ er nøyaktig de elementene som er koprime med n. Siden $\phi(5) = 4$, $\phi(11) = 10$ (ϕ er Eulers phi-funksjon), har gruppen $4 \cdot 10 = 40$ enheter

Vi har $G \simeq A \times B$, der $A = \{1,2,3,4\}$ under multiplikasjon mod 5, $B = \{1,2,3,4,5,6,7,8,9,10\}$ under multiplikasjon mod 11. Vi finner at $\langle 2_A \rangle = A$ og $\langle 2_B \rangle = B$, så A og B er sykliske. Derfor er $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$. bl

2 i) $\gcd(9,12) = 3$, og siden $3 \nmid 7$, har $9x \equiv 7 \pmod{12}$ ingen løsninger

ii) $6x \equiv 9 \pmod{15} \iff 2x \equiv 3 \pmod 5 \iff x \equiv 4 \pmod 5$.

Husk det er lop av denne linjen du skrev hvis

Så løsningsmengden er $4 + 15\mathbb{Z}, 9 + 15\mathbb{Z}, 14 + 15\mathbb{Z}$

3 Vi viser først at $T \leq U$

* T lukket: La $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \in T$. Da er $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & (a+b)\\ 0 & 1\end{pmatrix}$, som klart er i T.
* Identitet: Det er klart at $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = I_2 \in T$
* Inverser: Gitt $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \in T \; \exists \begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix} \in T$, og $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix} = I_2$ ✓

~~La nå $\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}$ være et vilkårlig element i U.~~
~~Da er $\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}^{-1} = \frac{1}{ac}\begin{pmatrix}c & -b\\ 0 & a\end{pmatrix}$. For en vilkårlig $\begin{pmatrix}1 & d\\ 0 & 1\end{pmatrix} \in T$,~~
~~er $\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}1 & d\\ 0 & 1\end{pmatrix}\frac{1}{ac}\begin{pmatrix}c & -b\\ 0 & a\end{pmatrix} = \frac{1}{ac}\begin{pmatrix}a & (ad+b)\\ 0 & c\end{pmatrix}\begin{pmatrix}c & -b\\ 0 & a\end{pmatrix} = \frac{1}{ac}\begin{pmatrix}ac & a^2d\\ 0 & ac\end{pmatrix}$~~
~~$= \begin{pmatrix}1 & \frac{d}{c}\\ 0 & 1\end{pmatrix} \in T$, så T er en normal undergruppe~~ ✗

Definer $\phi: U \to D$ med $\phi\left(\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\right) = \begin{pmatrix}a & 0\\ 0 & c\end{pmatrix}$.

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

$\phi\left(\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\right)\phi\left(\begin{pmatrix}a' & b'\\ 0 & c'\end{pmatrix}\right) = \begin{pmatrix}a & 0\\ 0 & c\end{pmatrix}\begin{pmatrix}a' & 0\\ 0 & c'\end{pmatrix} = \begin{pmatrix}aa' & 0\\ 0 & cc'\end{pmatrix}$. Derfor er ϕ en homomorfi. Siden $\phi\left(\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\right) = I_2 \Rightarrow a = c = 1$, og $\phi\left(\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\right) = I_2$ for alle $b \in \mathbb{R}$, er $\ker\phi = T$. Det følger at T er en normal undergruppe av U. Det er klart at ϕ er surjektiv, så $\operatorname{Im}\phi = D$. Siden $U/\ker\phi \simeq \operatorname{Im}\phi$, er $U/T \simeq D$ ■ ✓

4 Hvis $a \in I$, må $ba \in I \; \forall b \in R$. Velg $b = a^{-1}$, som er mulig siden a er en enhet. Da får vi $1 \in R$

Dette gir at $1_U \in I \; \forall U \in R$, d.v.s. $R \subseteq I$. Siden $I \subseteq R$, må $I = R$.

5 La $A = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$, $B = \begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} \in R$. Anta $AB = I$, da må

$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix}\begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} = \begin{pmatrix} xx' & 0 \\ yx'+zy' & zz' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow xx' = zz' = 1 \wedge yx' + zy' = 0$

$\Leftrightarrow x = x' = z = z' = 1 \wedge y + y' = 1$. Så enhetene er $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ og $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Ingen av disse er også 0-divisorer, for hvis A er enhet vil $AB = 0 \Rightarrow A^{-1}AB = A^{-1}0 \Rightarrow IB = 0 \Rightarrow B = 0$.

Vi finner at $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, så alle elementer forskjellig fra 0_R som ikke er enheter er 0-divisorer. R er ikke en divisjonsring, siden ringen har elementer ulik 0_R som ikke har inverser.

6 Z lukket: La $z_1, z_2 \in Z$, $g \in G$. Da er $(z_1 z_2)g = z_1(z_2 g) = z_1(g z_2) = (z_1 g) z_2 = g z_1 z_2$, så $z_1 z_2 \in Z$.

Enhet: Siden $eg = g = ge \; \forall g \in G$, er $e \in Z$.

Inverser: La $z \in Z$, $g \in G$. Da er $g^{-1} \in G$, og $g^{-1}z = zg^{-1}$

$\Rightarrow (g^{-1}z)^{-1} = (zg^{-1})^{-1} \Rightarrow z^{-1}(g^{-1})^{-1} = (g^{-1})^{-1} z^{-1} \Rightarrow z^{-1} g - g z^{-1} \Rightarrow z \in Z$

Z normal: gitt $g \in G$, $z \in Z$, er $gzg^{-1} = gg^{-1}z = z \in Z$.

Anta at G/Z er syklisk, og la aZ være en generator. Da kan vi skrive alle $bZ \in G/Z$ som $a^n Z$ for en $n \in \mathbb{Z}$, som betyr at $bz_1 = a^n z_2$ for noen $z_1, z_2 \in Z$. Vi kan altså skrive alle $b \in G$ på formen $b = a^n z_3$ ($z_3 = z_2 z_1^{-1} \in Z$). La nå $b = a^n z$, $c = a^m z' \in G$. Da har vi at

$$bc = b^n z a^m z' = a^n a^m z z' = a^m a^n z' z = (a^m z')(a^n z) = cb,$$

så $bc = cb$, og derfor er G abelsk. Så siden $(G/Z \text{ syklisk}) \Rightarrow (G \text{ abelsk})$, har vi kontrapositivt at $(G \text{ ikke abelsk}) \Rightarrow (G/Z \text{ ikke syklisk})$.

7 i) $(1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), i = (1,2)(1,2)$

ii) La A_4 virke på mengden av de $2^4 = 16$ fargede tetraederne som "gjør forskjell" på sideflatene, og kall denne X. Vi vil finne antall baner i X under G, som ifølge Burnsides formel er $\frac{1}{|A_4|} \sum_{g \in A_4} |X_g|$.

Vi finner $|X_{(12,)}| = 2 \cdot 2 = 4$, siden den nederste sideflaten (på figuren) kan ha 2 vegge fargene, og de tre andre må alle ha samme, men hvilke som helst av de to fargene. Av symmetri finner vi også $|X_a| = 4$ for alle elementer a i A_4 som er sykler, untatt i.

Vi får også $|X_{(1,2)(3,4)}| = 2 \cdot 2 = 4$, siden flaten omsluttet av 2, 3, 4 og den omsluttet av 1, 3, 4 må ha samme farge, og de to siste sidene også må ha det. Vi får også $|X_b| = 4$ for alle $b \in A_4$ som ikke er sykler.

Til slutt er det klart at $|X_i| = 16$, så antall distinkte farginger er

$$\frac{1}{|A_4|} \sum_{g \in A_4} |X_g| = \frac{1}{12} \cdot (8 \cdot 1 + 3 \cdot 4 + 16) - \frac{1}{12} \cdot 60 = \underline{\underline{5}} \text{ de}$$

8 ii) Vi påstår at G_1 Vare har én Sylow 7-undergruppe. 1. Sylowteorem gir at minst én finnes, og 3. Sylow gir at antallet deler 35 og er 1 mod 7. Divisorene av 35 er 1, 5, 7, 35,

og av disse er kun 1 kongruent med 1 mod 7, så det finnes kun 1 Sylow 7-undergruppe. Nå gir 2. Sylowteorem at alle Sylow 7-undergrupper (kun 1) er konjugerte, så undergruppen mappes til seg selv av alle indre automorfier i G_1, så den er normal ✓

ii) Vi vare generaliserer det forrige argumentet:

Anta $q > p$. 3. Sylowteorem gir at antallet Sylow q-undergrupper av G_2 deler pq og er 1 mod q. Siden $1, p, q, pq$ er alle divisorene, og siden $q \nmid q$, $q \mid qp$ og $1 < p < q$, er det kun 1 som er 1 mod q. Så det finnes vare én Sylow q-undergruppe, kall den S. 2. Sylowteorem gir nå at alle Sylow q-undergrupper er konjugerte, så vi må ha at $gSg^{-1} = S \; \forall g \in G_2$, og det følger at S er en normal undergruppe av G_2.

✓