Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Løsningsforslag — Øving 12

Med forbehold om feil. Gi gjerne beskjed til mads.sandoy alfakrøll ntnu.no hvis en finner noen.

Seksjon 37

$\boxed{4}$ Ved Teorem 36.11, altså det første Sylow-teoremet, har vi at en gruppe G av orden $5 \cdot 7 \cdot 47$ inneholder en unik undergruppe H av orden 47 som må være normal. Likeledes og av samme grunn, må den inneholde unike normale undergrupper av ordener 5 og 7.

Vi kan bruke Lemma 37.8 til å se at LK har orden 35 siden $L \cap K = \{e\}$, noe som følger av at elementene av L og K har forskjellige ordener. Ved beviset av Lemma 37.8, kan vi se at $(LK)H$ har orden $35 \cdot 47$ slik at $(LK)H = G$. Vi kan også observere at LK er den unike undergruppen av orden 35 og at $LK = L \times K$ ved Lemma 37.5, siden hvis det fantes en annen gruppe H' av orden 35 ville den ved Cauchys teorem ha undergrupper av orden 5 og 7 forskjellige fra L og K, en absurditet siden vi allerede har sett at disse var unike av den ordenen.

Siden LK er unik av orden 35 er den normal. Det følger at vi kan bruke Lemma 37.5 til å dedusere at G er isomorf med $LK \times H = L \times K \times H$, hvorav sistnevnt er åpenbart abelsk og syklisk da den er produktet av sykliske grupper av relativt primisk orden.

$\boxed{5}$ En gruppe av orden G har enten 1 eller 3 undergrupper av orden 32. Hvis det er kun en slik undergruppe så må den være normal og vi er ferdige. Anta følgelig at det ikke er kun en, og la H og K være distinkte undergrupper av orden 32. Ved Lemma 37.6, må $H \cap K$ ha orden 16, og er normal i både H og K siden den er av indeks 2 i begge. (Husk at hvis en undergruppe er av indeks 2, så er venstre restklasser og høyre restklasser nødvendigvis like, og undergruppen må være normal: når indeksen er 2, er det kun én ikke triviell restklasse i begge tilfeller og disse må isåfall være like siden venstre restklasser og høyre restklasser begge partisjonerer gruppen.)

Det følger at $N[H \cap K]$ inneholder H og K slik at de er undergrupper av $N[H \cap K]$ slik at de deler ordenen til $N[H \cap K]$ ved Lagranges teorem. Med andre ord må den ha orden et multiplum > 1 av 32. (Multiplumet kan ikke være 1 siden H og K ikke er like.) Siden $N[H \cap K]$ er en undergruppe av G må den også dele 96 ved Lagranges teorem, slik at den er av orden lik 96, altså er lik G. Siden normalisatoren til $H \cap K$ er lik hele G, følger det at $H \cap K$ er normal i G, slik at G ikke er simpel.

$\boxed{6}$ En gruppe G av orden 160 har enten 1 eller 5 undergrupper av orden 32 og enten 1 eller 16 undergrupper av orden 5. Vi kan ignorere tilfellene hvor det finnes kun én av hver av disse undergruppene, siden en slik gruppe må være normal, i hvilket tilfelle vi ville være ferdige.

La derfor H og K være distinkte undergrupper av orden 32. Ved Lemma 37.8, må $H \cap K$ være av orden 16 eller 8. Hvis ordenen til $H \cap K$ er 16, er den av indeks 2 i både H og K, altså normal i de, slik at $N[H \cap K]$ har orden et multiplum > 1 av 32 og en divisor av 160 slik at $N[H \cap K] = G$ og $H \cap K$ er normal i G og vi er ferdige. Dette følger av argumenter lik de i siste avsnitt i LF til forrige oppgave.

Hvis ordenen til $H \cap K$ er 8, følger det at HK er av orden $(32)(32)/8 = 128$ ved Lemma 37.8, slik at G har minst 127 elementer av orden delelig med 2. Samtidig ville 16 undergrupper av orden 5 gi 64 elementer av orden 5, og $127 + 64 > 64$, hvilket er absurd. Med andre ord er ikke G simpel.

$\boxed{7}$ Ved Eksempel 37.12, har en gruppe G av orden 30 en normal undergruppe av orden 5 eller av orden 3. Anta derfor at G har en normal undergruppe H av orden 5. Da er G/H en gruppe av orden 6, som ved Sylows første teorem eller Cauchys teorem har en undergruppe K av orden 3. Ved Sylows tredje teorem må denne være normal. Hvis $\pi\colon G \to G/H$ er den kanoniske gruppehomomorfien, så er $\pi^{-1}(K)$ en normal undergruppe av G av orden $3 \cdot 5 = 16$. Hvis G ikke har en normal undergruppe av orden 5, så må den ha en normal undergruppe av orden 3. Vi kan da gjennomføre det samme argumentet med de åpenbare endringene og igjen konkludere at det finnes en undergruppe av orden 15.

Eksamensoppgaver

$\boxed{\text{V2011 - 3}}$ Vi vet (via argumentet fra oppgave 27.6.) at $\mathbb{Z}_5/\langle f(x)\rangle$ er en kropp. Videre vet vi[1] at $|\mathbb{Z}_5/\langle f(x)\rangle| = 5^{\deg f(x)}$; dermed leter vi etter et polynom av grad 2. Ved å prøve oss frem (med kvalifiserte gjetninger) finner vi at $f(x) = x^2 + 2$ er irredusibelt. Altså er $\mathbb{Z}_5/\langle x^2 + 2\rangle$ en kropp med 25 elementer.

$\boxed{\text{H2010 - 3}}$ **a)** De irredusible polynomene av grad 3 i $\mathbb{Z}_2[x]$ er alle på formen $p(x) = x^3 + ax^2 + bx + c$. Vi kan igjen bruke teorem 23.10 for å se at $p(x)$ er irredusibelt hvis og bare hvis det ikke har noen røtter. Vi regner ut at $p(0) = c$ og $p(1) = 1 + a + b + c$. For at 0 ikke skal være en rot må vi altså ha $c = 1$. For at 1 ikke skal være en rot må vi ha $1 + a + b + c = a + b = 1$. Dermed ser vi at de irredusible polynomene av grad 3 i $\mathbb{Z}_2[x]$ er $x^3 + x^2 + 1$ og $x^3 + x + 1$.

b) Vi kan finne at $c_A = \det(A - xI_3) = x^3 + x + 1$ (på eksamen bør du ha med mellomregningen...). Siden $c_A(A) = 0$, har vi at $c_a(x) \in \ker\psi$, så $\langle c_a(x)\rangle \subseteq \ker\psi \subseteq \mathbb{Z}_2[x]$. Siden $c_A(x)$ er irredusibelt, er $\langle c_A(x)\rangle$ et maksimalt ideal. Dermed har vi at $\ker\psi = \langle c_A(x)\rangle$ eller $\ker\psi = \mathbb{Z}_2[x]$. Det siste stemmer ikke, for $x \notin \ker\psi$. Dermed er $\ker\psi = \langle c_A\rangle$.

[1] se notat om konstruksjon av endelige kropper

c) $\operatorname{im}\psi = \mathbb{Z}_2[x]/\ker\psi = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ er en kropp med åtte elementer.

d) $A = \psi(x) \in \operatorname{im}\psi$. Vi vet at $\operatorname{im}\psi$ er en kropp med åtte elementer; da er $\operatorname{im}\psi\setminus\{0\}$ en gruppe under multiplikasjon, som inneholder sju elementer. Dermed har vi at $A^7 = 1$, identitetselementet under multiplikasjon.

V2009 - 4

a) Om vi går systematisk frem ser vi at de irredusible, moniske andregradspolynomene i $\mathbb{Z}_3[x]$ er:

$$x^2+1 \qquad x^2+x+2 \qquad x^2+2x+2$$

De moniske irredusible andregradspolynomene i $\mathbb{Z}_5[x]$ er:

$$\begin{array}{lll} x^2+2 & x^2+3 & x^2+x+1 \\ x^2+x+2 & x^2+2x+3 & x^2+2x+4 \\ x^2+3x+3 & x^2+3x+4 & x^2+4x+1 \\ x^2+4x+2 & & \end{array}$$

b) Vi finner (for eksempel via bruk av karakteristisk polynom) at $x^2+1 \in \ker\phi$, så $\langle x^2+1\rangle \subseteq \ker\phi$. Etter et tilsvarende argument som i H2010-3 b, ser vi at $\ker\phi = \langle x^2+1\rangle$.

c) Her kan vi ikke bruke samme argument som over, for x^2+1 er ikke irredusibelt i $\mathbb{Z}_5[x]$. Tvert imot finner vi at $x^2+1 = (x-2)(x-3)$. Siden $\phi(x^2+1) = 0$ fortsatt, vet vi at $x^2+1 \in \ker\phi$, så da må enten $\ker\phi = \langle x^2+1\rangle$, $\ker\phi = \langle (x-3)\rangle$, $\ker\phi = \langle x-2\rangle$ eller $\ker\phi = \mathbb{Z}_5[x]$. De tre siste mulighetene kan det ikke være, for $x-3$ og $x-2$ blir ikke sendt på null av ϕ. Dermed har vi at $\ker\phi = \langle x^2+1\rangle$.

V2008 - 5

a) Polynomet er ikke irredusibelt for $a = 0, 3, 4$.
Polynomet er irredusibelt for $a = 1, 2, 5, 6$.

b) Merk at

$$\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}^2 = \begin{pmatrix} 4 & 4 \\ 4 & 1 \end{pmatrix} = 4\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}$$

Dermed er $p(x) = x^2+5x+3 \in \ker\phi$.

Siden dette polynomet er irredusibelt, og ϕ ikke er en nullhomomorfi, har vi at $\ker\phi = \langle x^2+5x+3\rangle$.

c)

$$\operatorname{im}\phi \cong \mathbb{Z}_7[x]/\ker\phi \cong \mathbb{Z}_7[x]/\langle x^2+5x+3\rangle$$

Dette er en kropp med 49 elementer.