Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA2201/TMA4150 Vår 2018

Løsningsforslag — Øving 10

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

Seksjon 26

3 Et ideal i en ring må være en additiv undergruppe av ringen. Dermed ser vi på alle additive undergrupper N av $\mathbb{Z}_{12}$. Vi sjekker først om N er lukket under multiplikasjon med alle elementer fra $\mathbb{Z}_{12}$, og regner så ut $\mathbb{Z}_{12}/N$

N	Ideal?	$\mathbb{Z}_{12}/N$
$\langle 0\rangle$	Ja	$\mathbb{Z}_{12}$
$\langle 1\rangle$	Ja	$\{0\}$
$\langle 2\rangle$	Ja	$\mathbb{Z}_2$
$\langle 3\rangle$	Ja	$\mathbb{Z}_3$
$\langle 4\rangle$	Ja	$\mathbb{Z}_4$
$\langle 6\rangle$	Ja	$\mathbb{Z}_2 \times \mathbb{Z}_3$

17 $R = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$, åpenbart. Vi kan vise at denne mengden er lukket under addisjon og multiplikasjon; dermed er det en underring.

Tilsvarende ser vi at $R' = \left\{ \left[\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right] | a, b \in \mathbb{Z} \right\} \subseteq M_2(\mathbb{Z})$. Igjen kan vi vise at mengden er lukket under addisjon og multiplikasjon, og dermed er en underring.

Å vise at $\phi : R \to R'$ respekterer addisjon er relativt enkelt, så vi holder oss her til å vise at den respekterer multiplikasjon:

$$\begin{aligned}\phi((a + b\sqrt{2})(c + d\sqrt{2})) &= \phi((ac + 2bd) + (ad + bc)\sqrt{2} \\ &= \begin{pmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bc \end{pmatrix} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix} \\ &= \phi(a + b\sqrt{2})\phi(c + d\sqrt{2})\end{aligned}$$

ϕ er altså en ringhomomorfi, og den er åpenbart 1-1 også.

22 **a)** $\phi(N)$ er en underring; jamfør teorem 26.3. La nå $r \in R$ og $n \in N$:

$$\begin{aligned}\phi(r)\phi(n) &= \phi(rn) \in \phi[N] \\ \phi(n)\phi(r) &= \phi(nr) \in \phi[N]\end{aligned}$$

(vi har her brukt at N er et ideal). Det følger at $\phi[N]$ er et ideal i $\phi[R]$.

b) Se på injeksjonen $\phi : \mathbb{Z} \to \mathbb{Q}$, gitt ved $\phi(n) = n$. $2\mathbb{Z}$ er et ideal i Z, men ikke i $\mathbb{Q}$.

c) Fra teorem 26.3 vet vi at $\phi^{-1}[N']$ er en underring. La nå $r \in R$.

$$\phi(\phi^{-1}[N']r) = N'\phi(r) = N' \Rightarrow \phi^{-1}[N']r = \phi^{-1}[N']$$
$$\phi(r\phi^{-1}[N']) = \phi(r)N' = N' \Rightarrow r\phi^{-1}[N'] = \phi^{-1}[N']$$

Følgelig er $\phi^{-1}[N']$ et ideal.

30 Vi skal altså sjekke om mengden av nilpotente elementer er et ideal. Vi sjekker derfor definisjonen steg for steg:

Additiv undergruppe Her sjekker vi gruppeaksiomene:

Lukket under addisjon La a og b være to nilpotente elementer, si at $a^n = 0$ og $b^m = 0$. Da er $(a + b)^{m+n} = 0$, se øving 9, oppgave 18.46. Dermed er mengden lukket under addisjon.

Identitetselement 0 er nilpotent

Inverser Anta at a er nilpotent med $a^n = 0$. Vi ser at $(-a)^n = ((-1)(a))^n = (-1)^n a^n = 0$; her har vi brukt at ringen er kommutativ.

Lukket under multiplikasjon med vilkårlig ringelement: Anta at a er nilpotent med $a^n = 0$, la b være et vilkårlig element i R. $(ab)^n = a^n b^n = 0$. Merk at det første likhetstegnet kun stemmer for en kommutativ ring!

31 Vi oppsummerer resultatene:

Ring	$\mathbb{Z}_{12}$	$\mathbb{Z}$	$\mathbb{Z}_{32}$
Nilideal	$\{0, 6\}$	$\{0\}$	$\{0, 2, 4, \ldots, 30\}$

Seksjon 27

6 $\mathbb{Z}_3[x]/\langle x^3 + x^2 + c\rangle$ er en kropp hvis og bare hvis $\langle x^3 + x^2 + c\rangle$ er et maksimalt ideal (Teorem 27.9). $\langle x^3 + x^2 + c\rangle$ er et maksimalt ideal hvis og bare hvis $x^3 + x^2 + c$ er et irredusibelt polynom (Teorem 27.25). $x^3 + x^2 + c$ er et irredusibelt polynom hvis og bare hvis det ikke har noen røtter i $\mathbb{Z}_3$ (Teorem 23.10). Vi må altså finne ut hvilke elementer $c \in \mathbb{Z}_3$ som gjør at polynomet ikke har noen røtter i $\mathbb{Z}_3$.

La $p(x) = x^3 + x^2 + c$. Da har vi at $p(0) = c$, $p(1) = 2 + c$ og $p(2) = c$. Altså er polynomet irredusibelt (og $\mathbb{Z}_3[x]/\langle x^3 + x^2 + c\rangle$ er en kropp) for $c = 2$.

31 $f(x)|g(x)$ hvis og bare hvis det finnes et polynom $p(x) \in F[x]$ slik at $g(x) = f(x)p(x)$. Men dette holder hvis og bare hvis $g(x) \in \langle f(x)\rangle$.

34 **a)** Vi trenger å vise at $A + B$ er en additiv undergruppe, og at $A + B$ er lukket under multiplikasjon med elementer fra R:

Lukket under addisjon: La $a, a' \in A$, $b, b' \in B$. Da er $(a + b) + (a' + b') = (a + a') + (b + b') \in A + B$, for A og B er lukket under addisjon

Inneholder nullelement: $0 \in A, B$, dermed er $0 + 0 \in A + B$

Inneholder additive inverser: For $a+b \in A+B$, er $-(a+b) = (-a)+(-b) \in A + B$.

Lukket under multiplikasjon med elementer fra R: Følger av at A og B er lukket under multiplikasjon med elementer fra R.

b) For alle $a \in A$ er $a+0 \in A+B$; dermed er $A \subseteq A+B$. Tilsvarende er $B \subseteq A+B$.

Seksjon 29

32 **a.** Hvis $p \neq 2$, så er $1 \neq p - 1$ i $\mathbb{Z}_p$, men $1^2 = (p - 1)^2$, og følgelig er ikke kvadrering en injektiv funksjon $\mathbb{Z}_p$ *to*$\mathbb{Z}_p$. Nærmere bestemt, så kan bildet av funksjonen høyst inneholde $p-1$ elementer. Med andre ord er det et element i $\mathbb{Z}_p$ som ikke er et kvadrat såfremt $p \neq 2$.

b. Man kan se i Eksempel 29.19 at det eksisterer en kropp med fire lementer. La p være et odde primtall. Ved del **a.**, eksisterer det en $a \in \mathbb{Z}_p$ slik at $x^2 - a$ ikke har noen røtter i $\mathbb{Z}_p$. Siden dette polynomet er av grad to og ikke har noen røtter, er det irredusibelt i $\mathbb{Z}_p[x]$. Hvis α er en rot av $x^2 - a$ i en kroppsutvidelse av $\mathbb{Z}_p$, blir $\mathbb{Z}_p(\alpha)$ et vektorrom over $\mathbb{Z}_p$ av dimensjon 2 (med e.g. basis $\{1, \alpha\}$. Siden det er p valg for hver koeffisient av en basisvektor, så må kroppen ha p^2 elementer.

Seksjon 33

5 $GF(19)^*$ er en syklisk gruppe under multiplikasjon (siden det er gruppen av enheter av en endelig kropp) av orden 18, og har $\phi(18) = 6$ generatorer, slik at det er 6 primitive 18nde røtter av enheten.

10 La $p(x)$ være irredusibelt av grad m i $\mathbb{Z}_p[x]$. La så K være den endelig utvidelse av $\mathbb{Z}_p$ man får ved å legge til alle røttene til $p(x)$ i $\bar{\mathbb{Z}}_p$.

Bemerkning/advarsel: Merk at man får K ved å bruke konstruksjonen i Kroneckers teorem, og man må underveis undersøke ved hvert steg om man behøver/kan legge til flere røtter. I mange tilfeller får man flere eller til og med alle røttene av et gitt polynom når man legger til en rot, e.g. skjer dette hvis man legger til en rot av x^2+1 til $\mathbb{R}$.

Man får da at K er en endelig kropp av orden p^n for et eller annet positivt heltall n, og består presist av alle røttene til $x^{p^n} - x$ i $\bar{\mathbb{Z}}_p$. Nå er det slik at $p(x)$ faktoriserer inn i lineære faktorer i $K[x]$, og de lineære faktorene må være blant de lineære faktorene av $x^{p^n} - x$ i $K[x]$. Med andre ord er $p(x)$ en divisor av $x^{p^n} - x$.

11 Siden $\alpha \in F$, har vi $\mathbb{Z}_p(\alpha) \subseteq F$. Men siden α er en generator av den multiplikative gruppen $F*$, ser vi at $(Z)_p(\alpha) = F$. Videre, siden ordenen til F er p^n, så må graden til α over $(Z)_p$ være n.

Eksamensoppgaver

H2011-2 **a)** I denne oppgaven skal vi vise at enhetene (elementene med multiplikativ invers) i en ring R med enhet (multiplikativ identitet) danner en abelsk gruppe under multiplikasjon. Vi sjekker derfor gruppeaksiomene:

Mengde med binæroperasjon: Før vi kan bruke aksiomene må vi sjekke det nulte aksiomet": At enhetene i R er en mengde, og at multiplikasjonen fra R er en binæroperasjon. Det første følger av at elementene i R utgjør er en mengde. Det andre er oppfylt dersom mengden av enheter i R er lukket under multiplikasjon; la derfor a og b være enheter, med a' og b' som deres respektive inverser. Vi har da at $(ab)(b'a') = 1$, så ab er igjen en enhet i R.

$\mathcal{G}_1$ Multiplikasjonen er assosiativ i R (fordi R er en ring), så da er den det her også.

$\mathcal{G}_2$ Det multiplikative identitetetselementet er en enhet, og fungerer som identitetselement også i gruppa.

$\mathcal{G}_3$ Inversen av en enhet er igjen en enhet.

b) $\mathbb{Z}_n$ er en kommuttativ ring. Enhetene i $\mathbb{Z}_n$ er elementene som er relativt primiske til n, og som vi har sett i (a) danner disse en abelsk gruppe U. Per definisjon er $|U| = \phi(n)$. Dermed har vi at for $u \in U$, så er $u^{\phi(n)} = u^{|U|} = 1$, identiteten i U - dette følger for eksempel fra Lagranges teorem. Altså har vi at for a relativt primisk til n så er $a^{\phi(n)} \equiv 1 \mod n$.

H2006-1 **a)** Det finnes to abelske grupper av orden 12 opp til isomorfi: $\mathbb{Z}_4 \times \mathbb{Z}_3$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

b) Det finnes 12 enheter i $\mathbb{Z}_{21}$, nemlig $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Ingen av disse har orden 4. Dermed må gruppen være isomorf til $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.