Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA2201/TMA4150 Vår 2015

Løsningsforslag — Øving 11

Seksjon 23

7 Fra Korollar 6.16 vet vi at hvis vi har funnet én generator, kan vi også regne ut resten av generatorene. Merk at $|\mathbb{Z}_{17}^*| = 16$, slik at alle elementer vil ha en orden som er en potens av 2.

Vi starter med å finne en generator. $2^8 \equiv 1 \mod 17$, så 2 er ikke en generator av gruppa. Derimot har vi at $3^8 \equiv 16 \mod 17$, slik at 3 er en generator av gruppa.

Gitt en generator a, er alle andre generatorer gitt som a^r, der r er relativt prim til ordenen til gruppa. I dette tilfellet vil det si at r er et oddetall. Dermed er generatorene (jeg sløyfer fra nå av modulo-notasjon) $3^1 = 3$, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$ og $3^{15} = 6$.

9 Fra korrolar 23.3 vet vi at $(x - a)$ er en lineær faktor av $x^4 + 4$ hvis og bare hvis a er en rot av polynomet, det vil si $a^4 + 4 = 0$. Vi merker oss at 1, 2, 3 og 4 alle er røtter av polynomet. Dermed er $x^4 + 4 = (x - 1)(x - 2)(x - 3)(x - 4)$.

35 Vi har $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$. Siden a er en rot av $f(x)$ har vi at

$$f(a) = a_0 + a_1a + \ldots + a_{n-1}a^{n-1} + a_na^n = 0$$

Siden F er en kropp og $a \neq 0$ har a en invers $\frac{1}{a}$. Vi ganger likningen over med $\left(\frac{1}{a}\right)^n$ og får at

$$a_0\left(\frac{1}{a}\right)^n + a_1a\left(\frac{1}{a}\right)^n + \ldots + a_{n-1}a^{n-1}\left(\frac{1}{a}\right)^n + a_na^n\left(\frac{1}{a}\right)^n = 0.$$

Vi forkorter og får

$$a_0\left(\frac{1}{a}\right)^n + a_1\left(\frac{1}{a}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{1}{a}\right) + a_n = 0.$$

Dermed har vi at $\left(\frac{1}{a}\right)^n$ er en rot av $a_n + a_{n-1}x + \ldots + a_1x^{n-1} + a_0x^n$.

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 $r \in R$.

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

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	$\{0, 6\}$	$\{0\}$	$\{0, 2, 4, \ldots, 30\}$

Eksamensoppgaver

V2013 - 3 **a)** Her er det nok å sjekke definisjonen: R er lukket under addisjon og multiplikasjon, og multiplikasjon er kommutativt.

b)
- For å vise ϕ er en ringhomomorfi, må vi vise at ϕ respekterer addisjon og multiplikasjon. Dette er ganske rett frem ved innsetting.
- $\ker \phi = \left\{ \begin{bmatrix} 0 & y & z \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} | x, y, \in \mathbb{Z}_3 \right\}$
- $R/\ker \phi \cong \phi[R] = \mathbb{Z}_3$, i følge fundamentalteoremet for homomorfier (26.17). $\mathbb{Z}_3$ er som kjent en kropp med tre elementer.

K2007 - 6 Vi vet at et produkt av to polynomer, henholdsvis av grad m og n, over en kropp[1] er et polynom av grad $m + n$. Ut ifra det ser vi at enhetene i $\mathbb{Z}_5[x]$ er alle konstante polynomer unntatt 0.

Videre ser vi at $\mathbb{Z}_5[x]$ er et integritetsområde (ingen nulldivisorer), men ikke en kropp (alle polynomer av grad større en null mangler inverser).

V2007 - 4 **a)** La $I \subseteq R$ være et ideal i en kommuttativ ring, og anta at $a \in I$ er en enhet. Da har vi at $1 = a^{-1}a \in a^{-1}I = I$, og dermed har vi at for enhver $r \in R$, så er $r = r1 \in rI = I$, så $R = I$.

b) Kjernen til ϕ er et ideal i K.

Dersom $\ker \phi = \{0\}$ er ϕ 1-1, og vi er i mål.

Dersom $\ker \phi \neq \{0\}$, så finnes det et ikke-null element $a \in \ker \phi$. Da K er en kropp må a være en enhet. Dermed har vi fra (a) at $\ker \phi = K$, så *phi* er nullavbildningen.

[1] Strengt tatt er det nok med et integritetsområde

V2007 - 5

$$R = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} | x, y, z \in Z_2 \right\}$$
$$= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Nulldivisorene er

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Enhetene er

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Dette er ikke en divisjonsring, da det finnes ikke-null elementer som ikke enheter.

H2006 - 7 Vi har p et primtall og $0 \leq a < p$ et heltall. Videre lar vi $q(x) \in \mathbb{Z}_p(x)$ være gitt ved $q(x) = x^p - a$. Fermats lille teorem forteller oss at $a^p \equiv a \mod p$. Dermed er a en rot av q, og siden Z_p er en kropp må da $(x - a)$ være en (lineær) faktor av $q(x)$.