Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA2201/TMA4150
Vår 2015

Løsningsforslag — Øving 12

Seksjon 27

$\boxed{6}$ $\mathbb{Z}_3[x]/\langle x^3+x^2+c\rangle$ 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 $c = 2$.

$\boxed{31}$ $f(x)|g(x)$ 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 $g(x) \in \langle f(x)\rangle$.

$\boxed{34}$ **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 $B \subseteq A+B$.

Andre oppgaver

$\boxed{1}$ $I = \{0\}$ er ok, for da er $I = \langle 0\rangle$.
Anta nå at $I \neq \{0\}$; da eksisterer det et ikke-null element $a \in I$. Da er også $-a \in I$, så vi kan uten tap av generalitet anta at a er positivt. La nå $n \in I$ være det *minste strengt positive elementet* i I. Siden I er et ideal, vet vi at $n\mathbb{Z} \subseteq I$ Vi vil nå vise at $I = n\mathbb{Z}$.

Anta at $m \in I$ er slik at $m \notin n\mathbb{Z}$. Da har vi fra divisjonsalgoritmen at $m = nq+r$, der $q \in \mathbb{Z}$ og $0 < r < n$. Dermed er også $r \in I$, men n skal være det minste positive elementet i I. Det følger at $m \in n\mathbb{Z}$ og dermed at $I = n\mathbb{Z}$.

$\boxed{2}$ $\Rightarrow$ Anta at $n\mathbb{Z}$ er et maksimalt ideal, og anta at $p \in \mathbb{Z}^+$ deler n. Da er $n \in p\mathbb{Z}$, så $n\mathbb{Z} \subseteq p\mathbb{Z}$, som impliserer at $p\mathbb{Z} = \mathbb{Z}$ eller $p\mathbb{Z} = n\mathbb{Z}$, siden $n\mathbb{Z}$ er et maksimalt ideal. Dermed må $p = n$ eller $p = 1$, så n er et primtall.

$\Leftarrow$ Anta at n er et primtall, og la $n\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$. Siden I er et ideal, vet vi fra forrige oppgave at det kan skrives som $I = m\mathbb{Z}$. Siden $n \in m\mathbb{Z}$ må $n = mx$ for en $x \in \mathbb{Z}$. Siden n er et primtall, må vi ha $m = 1$ eller $m = n$, så dermed er $I = \mathbb{Z}$ eller $I = n\mathbb{Z}$. Dermed er $n\mathbb{Z}$ et maksimalt ideal.

$\boxed{3}$ $I = \{0\}$ er ok, for da er $I = \langle 0 \rangle$.
Anta nå at $I \neq \{0\}$; la $f(x) \in I$ være et ikke-null polynom av lavest mulig grad i I. Vi vet da at $\langle f(x) \rangle \subseteq I$; vi vil nå vise at denne inklusjonen i virkeligheten er en likhet.

La $g(x) \in I$; $\deg g(x) \geq \deg f(x)$, så vi kan bruke divisjonsalgoritmen for polynomer til å få $g(x) = f(x)p(x) + r(x)$, der $\deg r(x) < \deg f(x)$. Siden $f(x)$ ble valgt til å være et ikke-null polynom av lavest mulig grad i I, og $r(x) \in I$, må vi ha at $r(x) = 0$. Følgelig er $g(x) \in \langle f(x) \rangle$, og $I = \langle f(x) \rangle$.

$\boxed{4}$ $\Rightarrow$ Anta at $\langle f(x) \rangle$ er et maksimalt ideal, og anta at $g(x)$ deler $f(x)$, med $\deg g(x) < \deg f(x)$. Da er $f(x) \in \langle g(x) \rangle$, så $\langle f(x) \rangle \subseteq \langle g(x) \rangle$, som impliserer at $\langle g(x) \rangle = F[X]$ eller $\langle g(x) \rangle = \langle f(x) \rangle$, siden $\langle f(x) \rangle$ er et maksimalt ideal. $\langle g(x) \rangle = F[x]$ impliserer at g er et konstant polynom. $\langle g(x) \rangle = \langle f(x) \rangle$ gir at $\deg g(x) = \deg f(x)$, som går imot antagelsene over. Følgelig er f irredusibelt.

$\Leftarrow$ Anta at $f(x)$ er et irredusibelt polynom, og la $\langle f(x) \rangle \subseteq I \subseteq F[x]$. Siden I er et ideal, vet vi fra forrige oppgave at det kan skrives som $I = \langle g(x) \rangle$. Siden $f(x) \in \langle g(x) \rangle$ må $f(x) = g(x)p(x)$ for en $p(x) \in F[x]$. Siden $f(x)$ er irredusibelt, må vi ha at $\deg g(x) = 1$, som gir $\langle g(x) \rangle = F[x]$, eller $\deg g(x) = \deg f(x)$, som gir $\langle g(x) \rangle = \langle f(x) \rangle$. Dermed er $\langle f(x) \rangle$ et maksimalt ideal.

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 $x^3 + x + 1$.

[1] se notat om konstruksjon av endelige kropper

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 $\ker\psi = \langle c_A\rangle$.

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.