KTH Teknikvetenskap

SF2703 ALGEBRA GRUNDKURS
ANTECKNINGAR
2009-03-05

Vi löser några uppgifter från kapitel 7 och 8 i Abstract Algebra [1].

Övning 0.1 (7.1.4)**.** *Visa att snittet av en uppsättning delringar är en delring.*

Lösning. Om a, b ligger i snittet av en uppsättning av delringar så ligger de i alla delringar. Alltså ligger $a - b$ och ab i alla delringar, och därmed i snittet. Alltså är snittet en delring. □

Övning 0.2 (7.1.7)**.** *Centret i en ring R är alla element som kommuterar med alla andra element i R under multiplikation. Visa att centret i en divisionsring (skevkropp) är en kropp.*

Lösning. Centret är en delring i och med att $(a-b)c = ac - bc = ca - cb = c(a-b)$ och $abc = acb = cab$ om a och b ligger i centret och c är ett element i R. Det är en kommutativ ring eftersom elementen speciellt kommuterar med andra element i centret, och ettan ligger i centret. Inversen till ett element i centret ligger också i centret, eftersom

$$a^{-1}c = ca^{-1} \iff aa^{-1}ca = aca^{-1}a \iff ca = ac.$$

Alltså är centret en kommutativ ring med etta där alla element är inverterbara, dvs en kropp. □

Övning 0.3 (7.1.14)**.** *Låt x vara ett nilpotent element i en kommutativ ring R med etta.*

a) *Visa att x antingen är noll eller en nolldelare.*
b) *Visa att rx är en nilpotent för alla $r \in R$.*
c) *Visa att $1 + x$ är en enhet i R.*
d) *Dra slutsatsen att summan av nilpotenta element med en enhet är en enhet.*

Lösning.
a) Om $x \neq 0$ och n är det minsta positiva tal så att $x^n = 0$ har vi att $x \cdot x^{n-1} = 0$ utan att någon av faktorerna är noll. Allstå är x en nolldelare.
b) Om $x^n = 0$ får vi att $(rx)^n = r^n x^n = r^n \cdot 0 = 0$, eftersom R är kommutativ. Alltså är även rx nilpotent.
c) Vi har att $(1+x)(1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1}) = 1 + (-1)^n x^n = 1$ om $x^n = 0$. Alltstå är $(1+x)$ en enhet.
d) Om x är nilptent och y är en enhet får vi att $x + y = y(1 + xy^{-1})$, där $1 + xy^{-1}$ är en enhet enligt c) eftersom xy^{-1} är nilpotent enligt b).

□

Övning 0.4 (7.3.5)**.** *Beskriv alla ringhomomorfier från $\mathbb{Z} \times \mathbb{Z}$ till $\mathbb{Z}$. Bestäm i varje fall kärnan och bilden.*

Lösning. En ringhomomorfi $\Phi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ bestäms helt av värdena på $(1,0)$ och $(0,1)$ eftersom värdet på (m,n) kan fås genom upprepad addition:

$$\Phi(m,n) = m\Phi(1,0) + n\Phi(0,1) = \sum_{i=1}^{m} \Phi(1,0) + \sum_{i=1}^{n} \Phi(1,0).$$

Vi får alltså en möjligt homomorfi $\Phi_{a,b}$ för varje par $a, b \in \mathbb{Z}$ genom

$$\Phi(m,n) = ma + nb, \qquad m,n \in \mathbb{Z}.$$

Kärnan fås som

$$\ker \Phi_{a,b} = \{(m,n) | am + bn = 0\} = \left\{ k \left(\frac{b}{\mathrm{sgd}(a,b)}, -\frac{a}{\mathrm{sgd}(a,b)} \right) \mid k \in \mathbb{Z} \right\}$$

Bilden blir

$$\mathrm{im}\Phi_{a,b} = \{ma + nb | m,n \in \mathbb{Z}\} = (\mathrm{sgd}(a,b)) \subseteq \mathbb{Z}$$

□

Övning 0.5 (7.3.13)**.** *Visa att ringen $M_2(\mathbb{R})$ innehåller en delring som är isomorf med $\mathbb{C}$.*

Lösning. Vi har att $\mathbb{C}$ är ett tvådimensionellt vektorrum över $\mathbb{R}$ med en bas som ges av 1 och i. Därmed kan vi representera multiplikaion med ett komplext tal som en 2×2-matris. Det räcker att se hur matriserna för 1 och i ser ut:

$$1 \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{och} \qquad i \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Därmed motsvarar $a + ib$ matrisen

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

□

Övning 0.6 (7.3.29)**.** *Låt R vara en kommutativ ring. Visa att mängden av nilpotenta element i R bildar ett ideal $\mathfrak{N}(R)$.*

Lösning. Tag två nilpotenta element x och y. Vi har att $x^m = 0$ och $y^n = 0$ för heltal m och n. Vi kan nu se att

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} (-1)^i x^i y^{m+n-i} = 0$$

eftersom $x^i = 0$ för $i = m, m+1, \ldots, m+n$ och $y^{m+n-i} = 0$ för $i = 0, 1, \ldots, m$. Vi har redan visat i en tidigare uppgift att xr är nilpotent om x är nilpotent och $r \in R$. Alltså är $\mathfrak{N}(R)$ ett ideal i R. □

Övning 0.7 (7.4.9)**.** *Låt R vara ringen av kontinuerliga funktioner på intervallet $[0,1]$ och låt $I = \{f \in R | f(1/3) = f(1/2) = 0\}$. Visa att I är ett ideal men inte är ett primideal i R.*

Lösning. Vi har i allmänhet att $I_a = \{f \in R | f(a) = 0\}$ är ett ideal i R för $a \in [0,1]$ eftersom $f(a) = g(a) = 0$ innebär att $f(a) - g(a) = 0$ och $f(a)h(a) = 0$ för alla h i R.

Nu är den givna mängden $I = I_{1/2} \cap I_{1/3}$ som är ett ideal eftersom det är en skärning av ideal.

I är inte ett primideal eftersom vi kan hitta en produkt av funktioner som är noll i båda punkterna utan att båda faktorerna är noll i båda punkterna, tex har vi att $f(x) = (2x-1)(3x-1)$ ligger i I, trots att $2x-1$ inte ligger $I_{1/3}$ och $3x-1$ inte ligger i $I_{1/2}$. □

Övning 0.8 (7.4.15)**.** *Låt $x^2 + x + 1$ vara ett element i polynomringen $\mathbb{Z}_2[x]$ och låt $E = \mathbb{Z}_2[x]/(x^2 + x + 1)$.*

a) *Visa att E innehåller fyra element; $\overline{0}$, $\overline{1}$, $\overline{x}$ och $\overline{x+1}$.*
b) *Skriv upp addtionstabellen för E och se att den additiva gruppen är isomorf med Kleins fyrgrupp*
c) *Skriv upp multiplikationstabellen för E och se att den multiplikatica gruppen är cyklisk av ordning tre. Dra slutsatsen att E är en kropp.*

Lösning. a) Kvoten blir ett vektorrumm över $\mathbb{Z}_2$ som genereras av $\overline{1}$ och $\overline{x}$ eftersom alla högre potenser av x kan reduceras till polynom av lägre grad med hjälp av relationen $x^2 + x + 1 = 0$. Eftersom $\overline{1}$ och $\overline{x}$ är linjärt oberoende är E ett vektorrum av dimension två, isomorft med $\mathbb{Z}_2^2$. Alltså finns bara de fyra elementen $\overline{0}$, $\overline{1}$, $\overline{x}$ och $\overline{1+x}$.

b) Vi skriver upp additionstabellen

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1+x}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1+x}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1+x}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{1+x}$	$\overline{0}$	$\overline{1}$
$\overline{1+x}$	$\overline{1+x}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

som är grupptabellen för Kleins fyrgrupp.

c) Vi skriver upp multiplikationstabellen

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1+x}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{1+x}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{1+x}$	$\overline{1}$
$\overline{1+x}$	$\overline{0}$	$\overline{1+x}$	$\overline{1}$	$\overline{x}$

Alla element utom $\overline{0}$ är inverterbara och multiplikationen är kommutativ, så E är en kropp. Den multiplikativa gruppen är cyklisk av ordning tre. □

Övning 0.9 (7.5.3)**.** *Låt k vara en kropp. Visa att k innehåller en kropp k_0 som antingen är isomorf med $\mathbb{Q}$, eller med $\mathbb{Z}_p$ för något primtal p*

Lösning. Tag det minsta positiva heltal n sådant att $n \cdot 1 = 0$ i k. Om det finns ett sådant heltal måste det vara ett primtal, eftersom vi annars skulle ha att

$$0 = n \cdot 1 = (m \cdot 1)(q \cdot 1)$$

vilket skulle motsäga minimaliteten hos n om $m < n$ och $q < n$. Vi säger att k har karakteristik p om $p \cdot 1 = 0$ i k för något primtal p.

Om det inte finns något sådant primtal p säger vi att karakteristiken är noll och vi har då en injektiv homomorfi från $\mathbb{Z}$ in i k genom att skicka n på $n \cdot 1$. Eftersom alla element i k utom noll är inverterbara, får vi enligt den universella egenskapen hos fraktionsringar en injektiv homomorfi från $\mathbb{Q}$ till k.

Om k har karakteristik p så har homomorfin $\mathbb{Z} \longrightarrow k$ en kärna (p) och därmed är bilden av den homomorfin isomorf med $\mathbb{Z}_p$. Allstså innehåller k en delkropp isomorf med $\mathbb{Z}_p$. □

Övning 0.10 (7.5.4)**.** *Visa att alla delkroppar av* $\mathbb{R}$ *måste innehålla* $\mathbb{Q}$.

Bevis. Lösning Om k är en delkropp av $\mathbb{R}$ måste $1 \in k$. Därmed får vi att $\mathbb{Z} \in k$, men eftersom alla element i k är inverterbara kommer även alla rationella tal ligga i k. Därmed innehåller k de rationella talen $\mathbb{Q}$ som en delkropp. □

Övning 0.11 (7.6.1)**.** *Ett element* $e \in R$ *är en idempotent om* $e^2 = e$*. Antag att* e *är en idempotent i centret till* R*. Visa att* Re *och* $R(1-e)$ *är tvåsidiga ideal i* R *och att* $R \cong Re \times R(1-e)$*. Visa att* e *och* $1-e$ *är identitetselement i delringarna* Re *och* $R(1-e)$.

Lösning. Om e är en idempotent så är $(1-e)^2 = 1 - 2e + e^2 = 1 - e$, vilket visar att $1 - e$ är en idempotent. Eftersom e ligger i centret om och endast om $1 - e$ ligger i centret räcker det till att börja med att visa att Re är ett ideal för en idempotent e.

Det är en additiv delgrupp eftersom det är ett vänsterideal. Det räcker att visa att det också är ett högerideal, men det är klart i och med att e ligger i centret och

$$Rea = Rae \subseteq Re$$

för ett godtyckligt element $a \in R$.

Summan av de två idealen Re och $R(1-e)$ är hela R eftersom $1 = e + (1-e)$. Därmed kan vi använda kinesiska restsatsen och se att

$$R \longrightarrow R/Re \times R/R(1-e)$$

är en isomorfi eftersom $Re \cap R(1-e) = \{0\}$. Det återstår att se att $R/Re \cong R(1-e)$. Vi ser det genom att definiera en homomorfi $R \longrightarrow R(1-e)$ genom multiplikation med $(1-e)$ till höger. Det är en homomorfi eftersom $a(1-e)b(1-e) = ab(1-e)^2 = ab(1-e)$ då $1-e$ är en idempotent i centret.

Homomorfin är per definition surjektiv och kärnan ges av

$$\{a \in R | a(1-e) = 0\} = \{a \in R | a = ae\} = Re.$$

Alltså är $R/Re \cong R(1-e)$ och på motsvarande sätt $R/R(1-e) \cong Re$. Vi har visat att $R \cong Re \times R(1-e)$.

Vi kan också göra det direkt genom att definiera en homomorfi $R \longrightarrow Re \times R(1-e)$ genom $a \mapsto (ae, a(1-e))$ och sedan visa att denna är injektiv och surjektiv.

I delringen eR verkar e som ett identitetselement eftersom $ae \cdot e = ae$ och $e \cdot ae = ae^2 = ae$, eftersom e ligger i centret. På samma sätt verkar $(1-e)$ som ett identitetselement i $R(1-e)$. □

Övning 0.12 (7.6.2)**.** *Visa att en ändlig boolesk ring R med identitet $1 \neq 0$ uppfyller*

$$R \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2.$$

Lösning. Vi vet redan sedan tidigare att ringen är kommutativ om den är Boolesk. Tag nu ett nollskilt element $e \in R$. Vi kan använda föregående uppgift för att skriva $R \cong Re \times R(1-e)$. Om R har fler än två element kan vi välja e så att $e \neq 1$ och $e \neq 0$. Det innebär att både Re och $R(1-e)$ innehåller minst två elemennt och därmed måste de också vara strikt mindre än R. Därför kan vi använda induktion på antalet element i R för att visa att Re och $R(1-e)$ är isomorfa med en produkter av kopior av $\mathbb{Z}_2$ eftersom en delring av en Boolesk ring också är Boolesk. Därmed är $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. □

Övning 0.13 (8.1.7)**.** *Bestäm en generator för idealet $(85, 1+13i)$ i $\mathbb{Z}[i]$ genom att använda Euklides algoritm.*

Lösning. Vi vet att idealet ska genereras av ett enda element och det måste vara den största gemensamma delaren mellan 85 och $1+13i$. Vi använder Euklides algoritm och skriver

$$85 = (-7i) \cdot (1+13i) + -6 + 7i$$

och

$$1 + 13i = (1-i) \cdot (-6+7i)$$

vilket säger att $-6+7i$ är den största gemensamma delaren mellan 85 och $1+13i$. Vi skulle också ha tittat på möjliga faktorer $85 = 5 \cdot 17 = (1+2i)(1-2i)(4+i)(4-i)$ som också delar $1+13i$. □

Övning 0.14 (8.3.6)**.** a) *Visa att kvotringen $\mathbb{Z}[i]/(1+i)$ är en kropp med två element.*

b) *Låt $q \in \mathbb{Z}$ vara et primtal med $q \equiv 2 \pmod 4$. Visa att $\mathbb{Z}[i]/(q)$ är en kropp med q^2 element.*

c) *Låt p vara ett primtal med $p \equiv 1 \pmod 4$ och skriv $p = (a+ib)(a-ib)$. Visa att $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(a+ib) \times Z[i]/(a-ib)$ som ringar och att båda ringarna $\mathbb{Z}[i]/(a+ib)$ och $\mathbb{Z}[i]/(a-ib)$ är kroppar med p element.*

Lösning. a) Enligt divisionsalgoritmen har vi att varje element i $\mathbb{Z}[i]$ har en rest med norm strikt mindre än 2 modulo $1+i$. Det finns fem sådana element, 0, ± 1 och $\pm i$. Eftersom $(1+i)(1-i) = 2$ så är $1 \equiv -1 \pmod{1+i}$ och $i \equiv -1 \pmod{1+i}$, men vi har också att $1-(-i) = 1+i \equiv 0 \pmod{1+i}$, vilket ger att det bara finns två olika element i kvoten, restklasserna $[0]$ och $[1]$. Eftersom $1+i$ är irreducibelt får vi att kvoten är ett integritetsområde och därmed i det här fallet en kropp med två element.

b) Om q är ett primtal med $q \equiv 3 \pmod 4$ har vi att $\mathbb{Z}[i]/(q) \cong \mathbb{Z}_q[x]/(x^2+1)$, där x^2+1 är irreducibelt i $\mathbb{Z}_q[x]$. Alltså är $\mathbb{Z}[i]/(q)$ en kropp med q^2 element.

c) Om p är ett primtal med $p \equiv 1 \pmod 4$ kan vi faktorisera $p = (a+ib)(a-ib)$ i $\mathbb{Z}[i]$. Vi har också att x^2+1 faktoriserar i ringen $\mathbb{Z}_p[x]$. Därmed har vi att

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[x]/(x^2+1) \cong \mathbb{Z}_p[x]/(x-\alpha) \times \mathbb{Z}_p[x]/(x+\alpha)$$

där bägge faktorerna är kroppar av ordning p. Dessa kroppar är isomorfa med $\mathbb{Z}[i]/(a+ib)$, respektive $\mathbb{Z}[i]/(a-ib)$.

□

REFERENSER

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.