UPPSALA UNIVERSITET
Matematiska institutionen
Johan Björklund

Prov i matematik
Ma kandidat, lärare, fristående
Algebra II, 5 p
2009–06–04

Tillåtna hjälpmedel: Skrivdon, passare och linjal. Lösningarna skall åtföljas av förklarande text. Varje uppgift ger maximalt 5 poäng. Om inget annat anges så antags alla ringar vara kommutativa ringar med egenskapen att $1 \neq 0$.
Skrivtid: *08.00–13.00.*

1. Ordna följande fyra påståenden i en följd så att det första påståendet implicerar det andra, det andra implicerar det tredje osv. R antags vara en ring. Inga bevis krävs.

- R är en huvudidealring.
- R är en kropp.
- R är euklidisk.
- R är faktoriell.

Lösning, uppgift 1

R är en kropp $\Rightarrow$ R är euklidisk $\Rightarrow$ R är en huvudidealring $\Rightarrow$ R är faktoriell.

2. **a)** Ge ett exempel på en ickekommutativ ring.

b) Visa att $\mathbb{Z}_n$ är en kropp om och endast om $n > 1$ är ett primtal.

c) Givet en godtycklig ring R och två irreducibla element $a, b \in R$, följer det att $a + b$ är irreducibelt? Bevis eller motexempel.

d) Formulera Noethers (första) isomorfisats.

Lösning, uppgift 2

a) Ringen av reella 2×2 matriser bildar en ickekommutativ ring. Exempel på två element som inte kommuterar är projektion på x axeln och rotation med $\pi/2$ radianer.

b) Om n ej är ett primtal så existerar $a, b > 1$ så att ab. Då är $ab = 0$ i $\mathbb{Z}_n$ även fast $a, b \neq 0$. Eftersom ingen kropp innehåller nolldelare, drar vi slutsatsen att $\mathbb{Z}_n$ inte är en kropp.

Antag å andra sidan att n är ett primtal, och låt m vara en representant för ett godtyckligt element i $\mathbb{Z}_n \setminus \{0\}$. Då, eftersom m och n är relativt prima, kan vi hitta två heltal r och s med hjälp av Euklides algoritm sådana att $rm + sn = 1$. Det följer att det elementet som m representerar i $\mathbb{Z}_n$ har invers lika med r. Alltså har alla nollskilda element i $\mathbb{Z}_n$ en multiplikativ invers, så vi drar slutsatsen att $\mathbb{Z}_n$ är en kropp.

c) Det följer ej, tag exempelvis x och $1 - x$ i $\mathbb{R}[x]$. Dessa två är irreducibla eftersom de är av grad ett, men summan av dem är inverterbar. Inverterbara element är inte irreducibla per definition.

d) Givet en ringhomomorfism $f : R \to R'$ så är $\mathrm{Im} f \cong R/\mathrm{Ker}(f)$. Om f är surjektiv, kan man förstås ersätta $\mathrm{Im} f$ med R', och då få $R/\mathrm{Ker}(f) \cong R'$.

3. Faktorisera $(2 + 4i)(4 + 3i)$ i irreducibla faktorer i $\mathbb{Z}[i]$.

Lösning, uppgift 3 Vi börjar med att minnas vilka tal som är irreducibla i $\mathbb{Z}[i]$. Det är tal $z = a + bi$ så att antingen: $|z|^2 = a^2 + b^2 = p$ där p är ett primtal eller $z = p$ där p är ett primtal på formen $4k + 3$. Låt $w = (2 + 4i)(4 + 3i)$. Vi ser omedelbart att vi kan faktorisera ut en tvåa från den första faktorn. Då får vi $w = 2(1 + 2i)(4 + 3i)$. Vi undersöker faktorerna separat.
2 är visserligen ett primtal, men inte på formen $4k + 3$ så det måste kunna skrivas som summan av två kvadrater $2 = a^2 + b^2$. Det inses lätt att den enda (positiva) möjligheten är $a = b = 1$ dvs $2 = (1+i)(1-i)$. Då $|1 + i|^2 = |1 - i|^2 = 2$ och två onekligen är ett primtal så är de faktorerna irreducibla.
Nästa faktor, $1 + 2i$ har normen 5. Då 5 är ett primtal så är alltså $1 + 2i$ irreducibelt.
Den enda faktorn kvar att undersöka är $4 + 3i$, igen så har vi inte ett primtal. Vi undersöker $3^2 + 4^2 = 25 = 5 \cdot 5$. 25 är tyvärr inte heller ett primtal, men vi kan ju faktorisera 25 som $5 \cdot 5$. Vi har nu att $(4 + 3i)(4 - 3i) = 5 \cdot 5$. $5 = 2^2 + 1^2 = (2 + i)(2 - i)$ där $2 \pm i$ onekligen är irreducibla (ty $5 = 2^2 + 1^2$, och 5 är ett primtal). Då är $(3 - 4i)(3 + 4i) = 5^2 = (2 + i)^2(2 - i)^2$ och när man provar att dividera med dessa irreducibla så syns direkt att $(4 + 3i) = i(2 - i)^2$. Så när vi plockar samman alla våra faktorer så får vi att

$$w = i(1 + i)(1 - i)(1 + 2i)(2 - i)^2 = -(1 + i)(1 - i)(2 - i)^3.$$

Vi kan notera att $i(1 + i) = -(1 - i)$ (dvs att $1 + i$ och $1 - i$ är associerade för att få det marginellt snyggare svaret

$$(2 + 4i)(4 + 3i) = i(1 + i)^2(2 - i)^3$$

Alla faktorerna är irreducibla och vi är klara.

4. Formulera Fermats lilla sats och använd den för att visa att $(pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \mod pqr$ där p, q, r är parvis olika primtal.

Lösning, uppgift 4 Fermats lilla säger att givet ett primtal p och ett godtyckligt heltal x så är $x^p - x$ delbart med p. Då p, q, r är relativt prima så säger kinesiska restsatsen att $(pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \mod pqr$ är ekvivalent med systemet

$$\begin{cases} (pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \pmod p \\ (pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \pmod q \\ (pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \pmod r. \end{cases}$$

I den första av dessa ekvationer har två av termerna en faktor p, och är alltså lika med noll eftersom vi räknar modulo p. Därför kan hela första ekvationen reduceras till

$$(qr)^{p-1} \equiv 1 \pmod p.$$

På grund av Fermats lilla sats vet vi att $(qr)^p \equiv qr \pmod p$. Vidare, eftersom qr är relativt prima med p, kan vi multiplicera denna likhet med inversen till qr modulo p (se uppg. 2b), och då får vi $(qr)^{p-1} \equiv 1 \mod p$. Man visar på helt analogt sätt att även de två sista kongruensekvationerna stämmer, så $(pq)^{r-1} + (qr)^{p-1} + (rp)^{q-1} \equiv 1 \mod pqr$.

5. Hitta alla heltalslösningar till ekvationssystemet

$$\begin{cases} x \equiv 7 \pmod 3, \\ x \equiv 2 \pmod{11}, \\ x \equiv 5^{49} \pmod 8. \end{cases}$$

Lösning, uppgift 5 Vi börjar med att reducera 5^{49} modulo 8. Eftersom 5 och 8 är relativt prima, säger Eulers sats att $5^{\phi(8)} \equiv 1 \pmod 8$. Eftersom $\phi(8) = 4$, får vi $5^{49} \equiv (5^4)^{12} \cdot 5^1 \equiv 1^{12} \cdot 5 \equiv 5 \pmod 8$. Vi lägger också märke till att den första kongruensen kan reduceras till $x \equiv 1 \pmod 3$.

Kinesiska restsatsen säger (eftersom 3,8 och 11 är parvis relativt prima) att alla lösningar till detta system av kongruenser ges av $x = x_0 + 3 \cdot 11 \cdot 8n$, $n \in \mathbb{Z}$, där x_0 är en lösning. För att hitta en lösning, ansätter vi $x = a \cdot 11 \cdot 8 + 3 \cdot b \cdot 8 + 3 \cdot 11 \cdot c$. Om vi sätter in detta i systemet av kongruenser, får vi följande ekvationer för a, b och c:

$$\begin{cases} 88a \equiv 1 \pmod 3 \\ 24b \equiv 2 \pmod{11} \\ 33c \equiv 5 \pmod 8 \end{cases} \Rightarrow \begin{cases} a \equiv 1 \pmod 3 \\ 2b \equiv 2 \pmod{11} \\ c \equiv 5 \pmod 8. \end{cases}$$

En lösning till detta system är $(a, b, c) = (1, 1, 5)$, och genom insättning i ansatsen för x får vi $x = 277$. En annan representant för samma element modulo 264 är 13. Samtliga lösningar ges alltså av:

$$x = 13 + 264n,\ n \in \mathbb{Z}.$$

6. Betrakta ringarna $R_1 = \mathbb{Z}_9$, $R_2 = \mathbb{Z}_3 \times \mathbb{Z}_3$ och $R_3 = \mathbb{Z}_3[x]/\langle x^2 \rangle$. Finns det något par av dem som är isomorfa? Exempel eller motbevis.

Lösning, uppgift 6 Vi noterar snabbt att alla tre ringarna har 9 element, så det går inte att dra någon slutsats angående vilka av dem som är isomorfa med varandra bara genom att räkna element.

Vi kan se att $R_1 \not\cong R_2$ genom att anta att vi har en isomorfism f från R_1 till R_2. $f(1) = (1, 1)$ enligt reglerna för isomorfismer. $f(3) = f(1+1+1) = f(1)+f(1)+f(1) = (3, 3) = 0 = f(0)$ ger motsägelse mot injektivitetskravet. $R_2 \not\cong R_3$ kan visas på följande sätt. Antag att f är en isomorfism från R_3 till R_2. Då är $f(\bar{x}) = (a, b)$ för något par a, b. Här betecknar $\bar{x}$ elementet i R_3 som representeras av x. Då $\bar{x}^2 = 0$ i R_3 så gäller $(0, 0) = f(0) = f(\bar{x}^2) = f(\bar{x})^2 = (a^2, b^2)$. De enda talen som är noll efter att man kvadrerat dem i $\mathbb{Z}_3$ är noll själv. Alltså så är $a = b = 0$ och $f(\bar{x}) = (0, 0)$ vilket motsäger injektivitet. Att $R_1 \not\cong R_3$ visas på ett liknande sätt som i början av lösningen. Antag att en isomorfism f existerar från R_1 till R_3. Då följer att $f(3) = f(1)+f(1)+f(1) = 1+1+1 = 0 = f(0)$ vilket igen motsäger injektivitet.

7. Givet en polynomring $K[x]$ där K är en kropp så definierar vi en funktion $D : K[x] \to K[x]$ kallad formell derivering som definieras som följer: $D(kx^n)kx^{n-1}$ då $n > 0$, $D(k) = 0$ för $k \in K$ samt $D(p(x) + h(x)) = D(p(x)) + D(h(x))$. Exempel: $D(3x^2 + 4) = 6x$.

- **a)** Gäller det att om $D(p(x)) = 0$ så följer det att $p(x) = c$ för något $c \in K$? Bevis eller motexempel.
- **b)** Ge ett nödvändigt och tillräckligt krav på K för att påståendet ovan ska gälla.

Lösning, uppgift 7

- **a)** Det gäller inte, tag exempelvis x^2 i $\mathbb{Z}_2[x]$. Då är $D(x^2) = 2x = 0$ även om x^2 ej är ett konstant polynom.
- **b)** Om karaktäristiken för kroppen är noll så gäller det. Nödvändighet följer av att om karaktäristiken av K är $p > 0$ så är $D(x^p) = px^{p-1} = 0$. Tillräcklighet får vi då vi ser att om vi har karaktäristik noll så är $D(ax^k) = kax^{k-1}$ lika med noll om och endast om a eller $k = 0$. sålänge vi verkligen har en term ax^k (dvs om $a \neq 0$) så kommer alltså dess grad bara att sjunka med 1. Då kommer samma sak att gälla på polynomnivå då D verkar på de enskila monomen varför sig. Men om $D(p(x)) = 0$ så kan den alltså inte ha grad 1 eller högre, kvar återstår endast de konstanta polynomen.

8. Givet en ring R definierar vi $\sqrt{\{0\}}$ som mängden av alla element $x \in R$ för vilka det existerar något positivt heltal n sådant att $x^n = 0$, dvs $\sqrt{\{0\}} = \{x \in R | \exists n \in \mathbb{Z}_+; x^n = 0\}$. Visa att $\sqrt{\{0\}}$ är ett ideal. Visa att $\sqrt{\{0\}} \subset P$ där vi definierar P som skärningen av alla primideal i R.

Lösning, uppgift 8 För att visa att mängden $\sqrt{\{0\}}$ är ett ideal, behöver vi visa att

$$\begin{aligned}
&I \neq \emptyset, \\
&a, b \in \sqrt{\{0\}} \Rightarrow a + b \in \sqrt{\{0\}}, \text{ samt} \\
&a \in \sqrt{\{0\}}, r \in R \Rightarrow ra \in \sqrt{\{0\}}.
\end{aligned}$$

Att $I \neq \emptyset$ följer omedelbart av att $0^1 = 0$, alltså så ligger 0 i I. Antag att $a, b \in \sqrt{\{0\}}$, så att $a^n = 0$ och $b^m = 0$ för några $m, n \in \mathbb{Z}_+$. Då får vi att

$$(a + b)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} = 0.$$

Den sista likheten följer av att alla termerna i summan är noll. Om nämligen $k \leq n-1$, så blir exponenten för b större än m, så den faktorn blir noll, och om $k \geq n$, så blir $a^k = 0$. Det visar att om a och b är nilpotenta (dvs. ligger i $\sqrt{\{0\}}$), så är även deras summa nilpotent. Observera att binomialsatsen gäller i alla kommutativa ringar.

Om $r \in R$, och $a^n = 0$ för något $n \in \mathbb{Z}+$, så får vi $(ra)^n = r^n a^n = r^n \cdot 0 = 0$.

Då återstår det bara att visa att detta ideal ligger i snittet av alla primideal. Det gör vi genom att låta $\mathfrak{p}$ vara ett godtyckligt primideal, och så visar vi att $\sqrt{\{0\}} \subset \mathfrak{p}$. Låt $x \in \sqrt{\{0\}}$, så att $x^n = 0$ för något $n \in \mathbb{Z}_+$. Då gäller $x^n \in \mathfrak{p}$ eftersom alla ideal innehåller 0. Men om $x \notin \mathfrak{p}$, kan inte heller x^2 ligga i $\mathfrak{p}$, eftersom ett primideal per definition har egenskapen att om man tar två element som inte ligger däri, så gör inte heller deras produkt det. Alltså kan inte heller $x^3 = x^2 \cdot x$ ligga i $\mathfrak{p}$, och då kan inte heller $x^4 = x^3 \cdot x$... Vi inser att om $x \notin \mathfrak{p}$, så följer det att $x^n \notin \mathfrak{p}$ - en motsägelse. Alltså har vi $x \in \mathfrak{p}$, så $\sqrt{\{0\}}$ ligger i $\mathfrak{p}$, men då följer det att $\sqrt{\{0\}}$ ligger i snittet av alla primideal, eftersom $\mathfrak{p}$ var godtyckligt.