UPPSALA UNIVERSITET
Matematiska institutionen
Isac Hedén

Prov i matematik
KandMat1, Frist
Algebra II, 5 hp
2011–06–01

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. Låt R vara en ring. Ordna följande påståenden så att det första medför det andra, det andra medför det tredje osv.

- R är faktoriell.
- Varje nollskilt element i R är inverterbart.
- Produkten av två element i R blir noll endast om en av elementen är noll.
- R är euklidisk.

Lösning: Det andra villkoret innebär att R är en kropp, och det tredje att R är ett integritetsområde. Om vi numrerar påståendena (1), (2), (3), (4), så har vi:

$$(2) \Rightarrow (4) \Rightarrow (1) \Rightarrow (3).$$

2. **a)** Vad är inversen till 8, om den existerar, i ringen $\mathbb{Z}_{17}$?

b) Givet en ring R och två inverterbara element $a, b \in R$, följer det att ab^{-1} är inverterbart?

c) Givet ett integritetsområde R, gäller det att $ax = ay$ medför $x = y$ om $a \neq 0$?

d) Ge exempel på en ring R och element $x, y \in R$ sådana att $ax = ay$ för något nollskilt $a \in R$, men $x \neq y$.

e) Låt $R = C^0(\mathbb{R})$ vara ringen av kontinuerliga funktioner från $\mathbb{R}$ till $\mathbb{R}$. Visa att

$$I := \{f \in C^0(\mathbb{R}) \mid f(3) = 0\}$$

är ett ideal i R.

Lösning:

a) Inversen till 8 existerar modulo 17 eftersom $\text{sgd}(8, 17) = 1$. Om vi räknar modulo 17, har vi $8 \cdot 2 \equiv 16 \equiv -1$. Inversen till 8 är alltså (-2) (denna restklass kan förstås även representeras av t.ex. 15).

b) Ja, ab^{-1} är inverterbart, med invers ba^{-1}.

c) Ja, det gäller:

$$ax = ay \implies ax - ay = 0 \implies a(x - y) = 0 \implies x - y = 0 \implies x = y.$$

I implikationen $a(x - y) = 0 \Rightarrow x - y = 0$ använde vi att $a \neq 0$ och att R är ett integritetsområde.

d) Låt $R = \mathbb{Z}_4$, $a = 2$, $x = 0$, och $y = 2$. Då gäller $ax = ay$ trots att $x \neq y$.

e) Låt $f(x) \in C^0(\mathbb{R})$ och $g(x), h(x) \in I$ (dvs. $g(x)$ och $h(x)$ uppfyller $g(3) = h(3) = 0$). Då gäller $(g + h)(3) = g(3) + h(3) = 0 + 0 = 0$ och $(fg)(3) = f(3)g(3) = f(3) \cdot 0 = 0$. Alltså har vi $g(x) + h(x) \in I$ och $f(x)g(x) \in I$. Eftersom I dessutom är icke-tomt ($0 \in I$), är I ett ideal.

3. Låt ϕ beteckna Eulers ϕ-funktion.

a) Formulera Eulers sats (bevis krävs ej).

b) Beräkna $\phi(136)$.

c) Förenkla $19^{65} \pmod{136}$, dvs. bestäm den minsta positiva resten då 19^{65} divideras med 136.

d) Visa att $17^{64} \not\equiv 1 \pmod{136}$. Bryter detta mot Eulers sats?

e) Hitta alla nollställen i $\mathbb{Z}_{13}$ till polynomet $x^{13} + 12x \in \mathbb{Z}_{13}[x]$.

Lösning:

a) Låt a och m vara heltal, med $m > 1$. Eulers sats säger att om $\text{sgd}(a, m) = 1$, så gäller

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

b) Vi primfaktoriserar 136: $136 = 2^3 \cdot 17$. Eftersom $\text{sgd}(2^3, 17) = 1$ har vi $\phi(136) = \phi(2^3 \cdot 17) = \phi(2^3) \cdot \phi(17) = (2^3 - 2^2)(17 - 17^0) = 64$.

c) Eftersom $\text{sgd}(19, 136) = 1$, följer det från Eulers sats att $19^{64} \equiv 1 \pmod{136}$. Multiplikation med 19 ger $19^{65} \equiv 19 \pmod{136}$.

d) Eftersom $17^{64} - 1$ inte är delbart med 17 ($17^{64} - 1 \equiv -1 \pmod{17}$), kan det inte heller vara delbart med $8 \cdot 17 = 136$. Alltså gäller $17^{64} \not\equiv 1 \pmod{136}$. Detta bryter inte mot Eulers sats, eftersom $\text{sgd}(17, 136) \neq 1$.

e) Lägg märke till att $x^{13} + 12x = x^{13} - x$ i $\mathbb{Z}_{13}[x]$. Enligt Fermats lilla sats gäller att $a^{13} \equiv a \pmod{13}$ för alla heltal a, så alla element i $\mathbb{Z}_{13}$ är nollställen till polynomet $x^{13} + 12x \in \mathbb{Z}_{13}[x]$.

4. Hitta alla heltalslösningar till ekvationssystemet

$$\begin{cases} x \equiv 0 \pmod{4}, \\ x \equiv 1 \pmod{9}, \\ 8x \equiv 1 \pmod{17}. \end{cases}$$

Lösning: Enligt problem **2 a)** är kongruensen $8x \equiv 1 \pmod{17}$ ekvivalent med $x \equiv 15 \pmod{17}$, så vi betraktar ekvationssystemet

$$\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 1 \pmod{9} \\ x \equiv 15 \pmod{17}, \end{cases}$$

och ansätter en lösning $x = a \cdot 9 \cdot 17 + 4 \cdot b \cdot 17 + 4 \cdot 9 \cdot c$. Vi sätter in ansatsen i första ekvationen och erhåller $a \cdot 9 \cdot 17 \equiv 0 \Leftrightarrow a \cdot 1 \cdot 1 \equiv 0 \Leftrightarrow a = 0 \pmod{4}$.
Den andra ekvationen ger $4 \cdot b \cdot 17 \equiv 1 \Leftrightarrow -4b \equiv 1 \Leftrightarrow 4b \equiv -1 \Leftrightarrow 4b \equiv 8 \Leftrightarrow b \equiv 2 \pmod{9}$.
Till sist ger den tredje ekvationen $4 \cdot 9 \cdot c \equiv 15 \Leftrightarrow 2c \equiv 15 \Leftrightarrow 2c \equiv -2 \Leftrightarrow c \equiv -1 \pmod{17}$. Vi sätter in $(a, b, c) = (0, 2, -1)$ i vår ansats, och får $x = 100$. **Svar:** Eftersom 4, 9 och 17 är parvis relativt prima, säger kinesiska restsatsen att systemets samtliga lösningar ges av $x = 100 + 612n$, $n \in \mathbb{Z}$.

5. Faktorisera $140 + 245i$ i irreducibla faktorer i $\mathbb{Z}[i]$.

Lösning: Vi börjar med att bryta ut heltalsfaktorn $\text{sgd}(140, 245) = 5 \cdot 7$: $140 + 245i = 5 \cdot 7(4 + 7i)$. Eftersom 7 är ett (naturligt) primtal och $7 \equiv 3 \pmod{4}$, är 7 ett primelement även i $\mathbb{Z}[i]$, men 5 är det inte då $5 \equiv 1 \pmod{4}$. Det faktoriseras som $5 = (1 + 2i)(1 - 2i)$. Nu återstår att faktorisera talet $4 + 7i$. Vi har $N(4 + 7i) = 4^2 + 7^2 = 65 = 5 \cdot 13$, och eftersom $5 = 1^2 + 2^2$, måste endera $1 + 2i$ eller $1 - 2i$ vara en primfaktor i $4 + 7i$. Prövning visar att $4 + 7i$ är delbart med $1 - 2i$, och vi erhåller $4 + 7i = (1 - 2i)(-2 + 3i)$.
Svar: $140 + 245i = 7(1 + 2i)(1 - 2i)^2(-2 + 3i)$, där var och en av faktorerna i högerledet är primelement i $\mathbb{Z}[i]$: 7 är ett naturligt primtal med $7 \equiv 3 \pmod{4}$ och normen av var och en av de övriga faktorerna är ett (naturligt) primtal.

6. Låt $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ vara ett icke-inverterbart element, så att $\langle \alpha \rangle \subset \mathbb{Z}[i]$ är ett nollskilt äkta huvudideal.

a) Visa att $\mathbb{Z}[i]/\langle \alpha \rangle$ är en ring med ändligt många element.

b) Eftersom irreducibla element i huvudidealringar genererar maximala ideal, är $\mathbb{Z}[i]/\langle \alpha \rangle$ en kropp när α är irreducibelt. Låt $\alpha := 1 + 2i \in \mathbb{Z}[i]$; då är α irreducibelt, och $\mathbb{Z}[i]/\langle 1 + 2i \rangle$ en kropp. Hur många element har denna kropp, och vilken är dess karaktäristik?

c) Låt $\beta := i + \langle 1 + 2i \rangle \in \mathbb{Z}[i]/\langle 1 + 2i \rangle$ beteckna den restklass som innehåller elementet i. Visa att $1 + \beta \neq 0$ i $\mathbb{Z}[i]/\langle 1 + 2i \rangle$, och beräkna $(1 + \beta)^{-1}$.

Lösning:

a) Låt $\overline{\gamma} \in \mathbb{Z}[i]/\langle \alpha \rangle$ vara ett element som representeras av $\gamma \in \mathbb{Z}[i]$. Eftersom $\mathbb{Z}[i]$ är en euklidisk ring, kan vi dividera γ med α med kvot och rest: $\gamma = q\alpha + r$ med $N(r) < N(\alpha)$ eller $r = 0$. Men då gäller $\overline{\gamma} = \overline{r}$, så ett godtyckligt element i $\mathbb{Z}[i]/\langle \alpha \rangle$ har en representant $r \in \mathbb{Z}[i]$ på avstånd högst $|\alpha|$ från origo. Sådana element finns det bara ändligt många av, så $|\mathbb{Z}[i]/\langle \alpha \rangle| < \infty$.

b) Låt $\overline{z}$ beteckna den restklass i $\mathbb{Z}[i]/\langle \alpha \rangle$ som representeras av ett element $z \in \mathbb{Z}[i]$.[1] Lägg märke till relationen $\overline{1 + 2i} = \overline{0}$. Det följer att $\overline{-2i} = \overline{1}$, och multiplikation med $\overline{i}$ ger relationen $\overline{2} = \overline{i}$. Vi beräknar $n \cdot \overline{1}$ för $n = 0, 1, 2, \ldots$ (på varje rad läggs $\overline{1}$ till den föregående).
$1 \cdot \overline{1} = \overline{1}$.
$2 \cdot \overline{1} = \overline{1} + \overline{1} = \overline{2} = \overline{i}$.
$3 \cdot \overline{1} = \overline{i} + \overline{1} = \overline{1 + i}$.
$4 \cdot \overline{1} = \overline{1 + i} + \overline{1} = \overline{2 + i} = \overline{i + i} = \overline{2i}$
$5 \cdot \overline{1} = \overline{2i} + \overline{1} = \overline{2i + 1} = \overline{0}$. Karaktäristiken är alltså 5, och vi misstänker att $\mathbb{Z}[i]/\langle 1 + 2i \rangle \simeq \mathbb{Z}_5$ (i så fall har kroppen har 5 element). För att bevisa detta, söker vi en surjektiv homomorfism $\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5$ med $\ker(\phi) = \langle 1 + 2i \rangle$ – då följer isomorfin med $\mathbb{Z}_5$ direkt från Noethers första isomorfisats. För ϕ måste gälla att $\phi(1) = 1$ och att $\phi(i)\phi(i) = \phi(i^2) = \phi(-1) = -1$. Det enda elementet i $\mathbb{Z}_5$ vars kvadrat är lika med -1 är 2, så $\phi(i) = 2$. Det finns alltså bara en möjlighet för $\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5$, nämligen $\phi(a + ib) = \phi(a) + \phi(i)\phi(b) = a + 2b$. Det är enkelt att kontrollera att ϕ respekterar addition och multiplikation, så ϕ är en ringhomomorfism. Den är uppenbarligen surjektiv, eftersom $\phi(a) = a$ för alla heltal a.
Nu undersöker vi dess kärna. Vi har $\langle 1 + 2i \rangle \subset \ker(\phi)$ eftersom $\phi(\beta(1 + 2i)) = \phi(\beta)\phi(1 + 2i) = \phi(\beta) \cdot 0 = 0$ för alla $\beta \in \mathbb{Z}[i]$. Men $\langle 1 + 2i \rangle$ är ett maximalideal då $1 + 2i \in \mathbb{Z}[i]$ är irreducibelt, och $\ker(\phi)$ är ett äkta ideal, så inklusionen $\langle 1 + 2i \rangle \subset \ker(\phi)$ kan ej vara strikt. Därmed har vi $\ker(\phi) = \langle 1 + 2i \rangle$. **Svar:** Kroppen har 5 element, och dess karaktäristik är 5.

c) Med samma notation som i **b)**-uppgiften, har vi $1 + \beta = \overline{1 + i}$. Detta element är nollskilt eftersom $(1 + 2i) \nmid (1 + i)$ i $\mathbb{Z}[i]$, och alltså inverterbart då $\mathbb{Z}[i]/\langle 1 + 2i \rangle$ är en kropp. Vi skulle kunna testa oss fram för att hitta inversen eftersom $\mathbb{Z}[i]/\langle 1 + 2i \rangle$ har få element, men ett mer systematiskt sätt är att använda isomorfismen $\overline{\phi} : \mathbb{Z}[i]/\langle 1 + 2i \rangle \longrightarrow \mathbb{Z}_5$ från **b)** (vi kallar den för φ): om $z \in \mathbb{Z}[i]/\langle 1 + 2i \rangle$ är inversen till $\overline{1 + i}$, så gäller $\varphi(z)\varphi(\overline{1 + i}) = \varphi(z(\overline{1 + i})) = \varphi(\overline{1}) = 1$. Men $\varphi(\overline{1 + i}) = 3$, så $3 \cdot \varphi(z) = 1 \in \mathbb{Z}_5 \Rightarrow \varphi(z) = 2$. Då får vi $z = \varphi^{-1}(\varphi(z)) = \varphi^{-1}(2) = \overline{i}$.
Mycket riktigt har vi också $\overline{i} \cdot \overline{1 + i} = \overline{i - 1} = \overline{2 - 1} = \overline{1}$. **Svar:** $(1 + \beta)^{-1} = \beta$.

7. Betrakta ringarna $\mathbb{Z}[i]/\langle 3 \rangle$, $\mathbb{Z}_9$ och $\mathbb{Z}_3[x]/\langle x^2 - 1 \rangle$. Finns det något par av dem som är isomorfa? Bevis eller motexempel.

Lösning: Den första ringen, $\mathbb{Z}[i]/\langle 3 \rangle$, är en kropp eftersom elementet $3 \in \mathbb{Z}[i]$ är irreducibelt och således genererar ett maximalideal. Dock är ingen av de andra två ringarna en kropp eftersom de innehåller nolldelare: $3 \cdot 3 = 0$ i $\mathbb{Z}_9$ och i den tredje ringen har vi $(\beta + 1)(\beta - 1) = 0$, där $\beta \in \mathbb{Z}_3[x]/\langle x^2 - 1 \rangle$ är det element som representeras av $x \in \mathbb{Z}_3[x]$ ($\beta \pm 1 \neq 0$ eftersom $(x^2 - 1) \nmid (x \pm 1)$ i $\mathbb{Z}_3[x]$). Men egenskapen att vara en kropp bevaras under isomorfi, så $\mathbb{Z}[i]/\langle 3 \rangle$ är inte isomorf med någon av de övriga två ringarna. Inte heller är de sista två ringarna isomorfa med varandra: $1 + 1 + 1 \neq 0 \in \mathbb{Z}_9$, men $1 + 1 + 1 = 0 \in \mathbb{Z}_3[x]/\langle x^2 - 1 \rangle$.[2] **Svar:** Det finns inget par av ringar bland dessa tre som är isomorfa.

[1] inte z-konjugat alltså.

[2] Antag att $f : \mathbb{Z}_3[x]/\langle x^2 - 1 \rangle \longrightarrow \mathbb{Z}_9$ är en isomorfism. Då gäller $0 = f(0) = f(1+1+1) = f(1)+f(1)+f(1) = 1+1+1 \neq 0$ i $\mathbb{Z}_9$, vilket är en motsägelse.

8. Låt R vara en ring där varje element $x \in R$ uppfyller $x^n = x$ för något heltal $n > 1$ (n kan bero på x). Visa att varje primideal i R är ett maximalideal.

Lösning: Låt $I \subset R$ vara ett ideal. Då är I ett primideal omm R/I är ett integritetsområde och I är ett maximalideal omm R/I är en kropp. Uppgiften kan alltså formuleras: Visa att om R/I är ett integritetsområde så är R/I en kropp. Antag att R/I är ett integritetsområde, och att $y := \overline{x}$ är ett nollskilt element i R/I som representeras av $x \in R$; vi behöver visa att y är inverterbar.[3] Välj ett $n > 1$ sådant att $x^n = x$; då gäller $y^n = y$ i R/I, så $y(y^{n-1} - 1) = 0$. Eftersom R/I är ett integritetsområde måste $y^{n-1} - 1 = 0$ då $y \neq 0$. Men då är y inverterbar med invers y^{n-2}.

[3] En ring är en kropp om alla nollskilda element är inverterbara.