UPPSALA UNIVERSITET
Matematiska institutionen
Elin Persson Westin
076-80 46 726

Prov i matematik
MaKand, fristående
Algebra II
2021–03–22

Skrivtid: 8.00-13.20.
Tillåtna hjälpmedel: Skrivdon, kompendiet av Hedén och Björklund samt föreläsningsanteckningar. Lösningarna skall åtföljas av förklarande text. För betygen 3, 4 och 5 krävs 18, 25 resp. 32 poäng inklusive eventuella bonuspoäng.

1. Avgör om följande påståenden är sanna eller falska. Ge ett *kort* bevis eller ett motexempel.

a) Polynomet $3x^4 - 6x^3 + 12x + 18$ är irreducibelt i $\mathbb{Q}[x]$.

b) $\mathbb{Z}_{45} \cong \mathbb{Z}_3 \times \mathbb{Z}_{15}$.

c) Ett reellt polynom är irreducibelt om och endast om det saknar reella rötter.

d) Låt R vara en nollskild kommutativ ring. Om $\{0\}$ och R är de enda idealen i R så är R en kropp.

e) Om R är ett integritetsområde så är R/I ett integritetsområde för alla ideal $I \subseteq R$.

(10 poäng)

2. Låt φ beteckna Eulers φ-funktion.

a) Beräkna $\varphi(75)$.

b) Hitta det minsta positiva heltal x så att $14^{40} \equiv x \pmod{75}$.

c) Visa att $5^{40} \equiv 25 \pmod{75}$. Motsäger detta Eulers sats?

(5 poäng)

3. Låt K vara mängden av alla reella 2×2-matriser på formen $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}$, där $a, b \in \mathbb{R}$.

a) Visa att $K = \left\{ \begin{bmatrix} a & b \\ -2b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq M_{2\times 2}(\mathbb{R})$ är en delring.

b) Visa att K är kommutativ.

c) Visa att K är en kropp.

(5 poäng)

4. Visa att om $\varphi : R \to S$ är en isomorfism så är $a \in R$ ett primelement om och endast om $\varphi(a)$ är ett primelement.

(5 poäng)

5. **a)** Låt $\varphi : \mathbb{Z}_{21} \to \mathbb{Z}_3$ definieras via $\varphi\left(a + 21\mathbb{Z}\right) = a + 3\mathbb{Z}$. Visa att φ är en epimorfism. *Glöm inte att visa att φ är väldefinierad.*

b) Visa att $\mathrm{Ker}(\varphi) = \overline{3}\mathbb{Z}_{21} = \{\overline{x} \in \mathbb{Z}_{21} \mid \overline{x} = \overline{3} \cdot \overline{y}, \text{ för något } \overline{y} \in \mathbb{Z}_{21}\}$.

c) Visa att $\mathbb{Z}_{21}/\overline{3}\mathbb{Z}_{21}$ är isomorf med $\mathbb{Z}_3$.

(5 poäng)

Fortsätter på nästa sida!

6. Hitta alla maximala ideal i $\mathbb{C}[x]$.

Tips: börja med att motivera varför $\mathbb{C}[x]$ är en huvudidealring.

(5 poäng)

7. Låt $I = \langle -3 + 9i, -5 + 25i \rangle \subseteq \mathbb{Z}[i]$.

a) Förklara varför det måste finnas ett Gaussiskt heltal $a + bi$ så att $I = \langle a + bi \rangle$.

b) Hitta ett sådant $a + bi$.

(5 poäng)

Lycka till!

Lösningar till tentamen i Algebra II 2021–03–22

Lösning till problem 1. **a)** Sant! Eftersom 2 är ett primelement i $\mathbb{Z}$ och $2|18$, $2|12$, $2|(-6)$, $2 \nmid 3$ och $2^2 \nmid 18$ så är $3x^4 - 6x^3 + 12x + 18$ irreducibelt i $\mathbb{Q}[x]$ enligt Eisensteins kriterium.

Obs: det går även bra att bryta ut det inverterbara elementet 3 och titta på det associerade polynomet $x^4 - 2x^3 + 4x + 6$, men det är inte nödvändigt!

b) Falskt! Vi noterar först att $\text{sgd}(3, 15) = 3 > 1$. Vi vet att $\mathbb{Z}_{45} \cong \mathbb{Z}_{3^2} \times \mathbb{Z}_5$ och $\mathbb{Z}_3 \times \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ enligt Sats 10.2 från föreläsningsanteckningarna. Men enligt Sats 10.5 från föreläsningsanteckningarna är $\mathbb{Z}_{3^2} \ncong \mathbb{Z}_3 \times \mathbb{Z}_3$. Alltså gäller $\mathbb{Z}_{3^2} \times \mathbb{Z}_5 \ncong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ och därmed även $\mathbb{Z}_{45} \ncong \mathbb{Z}_3 \times \mathbb{Z}_{15}$.

Vi kan även visa att påståendet är falskt då $\text{char}(\mathbb{Z}_{45}) = 45$ och $\text{char}(\mathbb{Z}_3 \times \mathbb{Z}_{15}) = \text{mgm}(3, 15) = 15 \neq 45$. Men karakteristik är något som bevaras under isomorfism, enligt Sats 9.13.

c) Falskt! Ett reellt polynom kan sakna reella rötter men ändå inte vara irreducibelt. T.ex. $(x^2 + 1)^2$ saknar reella rötter men är inte irreducibelt eftersom $x^2 + 1$ inte är inverterbart.

Ett reellt polynom kan även ha ett reellt nollställe men ändå vara irreducibelt, t.ex. $x - 1$.

d) Sant! En kropp är en nollskild kommutativ ring där alla nollskilda element är inverterbara. Om $a \in R \setminus \{0\}$ så är $\langle a \rangle = R$, eftersom det inte är lika med $\{0\}$. Då gäller $1 \in \langle a \rangle$ och alltså finns det ett $b \in R$ så att $1 = ab = ba$ (kom ihåg att R är kommutativ). Alltså är a inverterbart och R är därmed en kropp.

e) Falskt! Till exempel så är $\mathbb{Z}$ ett integritetsområde, men $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$ är inte ett integritetsområde.

Lösning till problem 2. **a)** Eftersom $75 = 3 \cdot 5^2$, där 3 och 5 är relativt prima, så gäller

$$\varphi(75) = \varphi(3)\varphi(5^2) = (3 - 1) \cdot 5(5 - 1) = 40$$

enligt Proposition 3.9 från föreläsningsanteckningarna.

b) Eftersom att 14 och 75 är relativt prima, och $\varphi(75) = 40$, så säger Eulers sats att

$$14^{40} = 14^{\varphi(75)} \equiv 1 \pmod{75}.$$

Alltså är $x = 1$.

c) Vi använder algoritmen från Föreläsning 2:

k	40	20	10	5	4	2	1
$5^k \pmod{75}$	$25^2 \equiv \mathbf{25}$	$25^2 \equiv \mathbf{25}$	$(-25)^2 \equiv \mathbf{25}$	$25 \cdot 5 = 125 \equiv \mathbf{-25}$	$25^2 = 625 \equiv \mathbf{25}$	$5^2 = \mathbf{25}$	$\mathbf{5}$

Detta visar att vi har $5^{40} \equiv 25 \pmod{75}$. Här använder vi att $625 = 600 + 25 = 75 \cdot 8 + 25$ och $125 = 150 - 25 = 75 \cdot 2 - 25$.

Eftersom 5 och 75 *inte är relativt prima* så motsäger detta INTE Eulers sats!

Lösning till problem 3. **a)** Vi använder Sats 5.6 för att visa att detta är en delring. Om $a = b = 0$ så får vi nollmatrisen, vilket är det additivt neutrala elementet i $M_{2\times 2}(\mathbb{R})$. Om $a = 1, b = 0$ så får vi enhetsmatrisen, vilket är det multiplikativt neutrala elementet i $M_{2\times 2}(\mathbb{R})$.

Nu kontrollerar vi om K är sluten under addition, multiplikation och additiv invers. Notera att de reella talen såklart är sluten under addition, multiplikation och additiv invers!

Låt $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix} \in K$, då gäller även $\begin{bmatrix} -a & -b \\ 2b & -a \end{bmatrix} \in K$, vilket är den additiva inversen.

Om $\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}$ och $\begin{bmatrix} c & d \\ -2d & c \end{bmatrix}$ ligger i K så ligger även

$$\begin{bmatrix} a & b \\ -2b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -2d & c \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ -2(b + d) & a + c \end{bmatrix}$$

och

$$\begin{bmatrix} a & b \\ -2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -2d & c \end{bmatrix} = \begin{bmatrix} ac-2bd & ac+bd \\ -2(ac+bd) & ac-2bd \end{bmatrix}$$

i K. Alltså är $K \subseteq M_{2\times 2}(\mathbb{R})$ en delring.

b) Om vi testar att multiplicera två godtyckliga element i K ser vi direkt att multiplikationen är kommutativ eftersom $\mathbb{R}$ är en kommutativ ring:

$$\begin{bmatrix} a & b \\ -2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -2d & c \end{bmatrix} = \begin{bmatrix} ac-2bd & ac+bd \\ -2(ac+bd) & ac-2bd \end{bmatrix} = \begin{bmatrix} ca-2db & ca+db \\ -2(ca+db) & ca-2db \end{bmatrix} = \begin{bmatrix} c & d \\ -2d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ -2b & a \end{bmatrix}.$$

Alltså är K en kommutativ ring.

c) En kropp är en nollskild kommutativ ring där varje nollskilt element har en invers. Vi vet redan att K är en nollskild kommutativ ring, så vi behöver bara visa att alla nollskilda element har inte invers.

Från Linjär algebra vet vi att en reell matris är inverterbar om och endast om dess determinant är nollskild. Men om inte både a och b är lika med 0 (d.v.s. om vår matris inte är nollmatrisen) så gäller

$$\det\left(\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}\right) = a^2 + 2b^2 \neq 0.$$

Vi kan även skriva upp inversen till en matris i K

$$\begin{bmatrix} a & b \\ -2b & a \end{bmatrix}^{-1} = \frac{1}{a^2+2b^2} \begin{bmatrix} a & -b \\ -2(-b) & a \end{bmatrix}.$$

Vi ser att inversen är ett element i K. Alltså har vi visat att K är en kropp!

Lösning till problem 4. Antag att $a \in R$ är ett primelement och att $\varphi(a)|xy$ där $x, y \in S$. Vi vill visa att $\varphi(a)|x$ eller $\varphi(a)|y$.

Eftersom $\varphi(a)|xy$ så finns det $z \in S$ så att $\varphi(a)z = xy$. Då φ är surjektiv finns det $b, c, d \in R$ så att $\varphi(b) = x$, $\varphi(c) = y$ och $\varphi(d) = z$. Vi har då $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$ vilket är ekvivalent med att $\varphi(ad) = \varphi(bc)$ eftersom φ är en ringhomomorfism. Då φ är injektiv implicerar $\varphi(ad) = \varphi(bc)$ att $ad = bc$, d.v.s. $a|bc$.

Eftersom a är ett primelement så gäller $a|b$ eller $a|c$. Detta är enligt definition ekvivalent med att det finns $e \in R$ så att $ae = b$ eller att det finns $f \in R$ så att $af = c$. Genom att applicera φ på båda sidor av dessa två likheter får vi att $\varphi(a)\varphi(e) = \varphi(b) = x$ eller $\varphi(a)\varphi(f) = \varphi(c) = y$. Notera att vi här har använt att φ är en ringhomomorfism. Men detta betyder att $\varphi(a)|x$ eller $\varphi(a)|y$. Detta visar att $\varphi(a)$ är ett primelement.

Antag nu att $\varphi(a)$ är ett primelement. Eftersom att φ^{-1} också är en isomorfism och $a = \varphi^{-1}(\varphi(a))$ så följer det från det vi precis visat att a är ett primelement.

Lösning till problem 5. **a)** Vi visar först att φ är väldefinierad. Antag att $a + 21\mathbb{Z} = b + 21\mathbb{Z}$. Då gäller $21|(a-b) \Rightarrow 3|(a-b)$ eftersom $3|21$. Men detta betyder att $\varphi(a+21\mathbb{Z}) = a+3\mathbb{Z} = b+3\mathbb{Z} = \varphi(b+21\mathbb{Z})$, och alltså är φ väldefinierad.

Vi visar nu att φ är en ringhomomorfism:

$$\varphi((a+21\mathbb{Z})+(b+21\mathbb{Z})) = \varphi((a+b)+21\mathbb{Z})) = (a+b)+3\mathbb{Z} = (a+3\mathbb{Z})+(b+3\mathbb{Z}) = \varphi(a+21\mathbb{Z})+\varphi(b+21\mathbb{Z}),$$

$$\varphi((a+21\mathbb{Z})\cdot(b+21\mathbb{Z})) = \varphi((a\cdot b)+21\mathbb{Z})) = (a\cdot b)+3\mathbb{Z} = (a+3\mathbb{Z})\cdot(b+3\mathbb{Z}) = \varphi(a+21\mathbb{Z})\cdot\varphi(b+21\mathbb{Z}),$$

$$\varphi(1_{\mathbb{Z}_{21}}) = \varphi(1+21\mathbb{Z}) = 1+3\mathbb{Z} = 1_{\mathbb{Z}_3}.$$

Alltså uppfyller φ de tre axiomen för en ringhomomorfism.

Låt $a + 3\mathbb{Z}$ vara ett godtyckligt element i $\mathbb{Z}_3$. Då kommer $a + 3\mathbb{Z}$ ligga i bilden av φ eftersom $\varphi(a + 21\mathbb{Z}) = a + 3\mathbb{Z}$. Alltså är φ surjektiv och därmed en epimorfism.

b) Antag att $a + 21\mathbb{Z} \in \text{Ker}(\varphi)$, d.v.s. $\varphi(a + 21\mathbb{Z}) = a + 3\mathbb{Z} = 0 + 3\mathbb{Z}$. Då gäller $3|(a - 0)$, d.v.s. $a = 3k$ för något $k \in \mathbb{Z}$. Men då är $a + 21\mathbb{Z} = 3k + 21\mathbb{Z} = (3 + 21\mathbb{Z})(k + 21\mathbb{Z}) \in \overline{3}\mathbb{Z}_{21}$. Alltså gäller $\text{Ker}(\varphi) \subseteq \overline{3}\mathbb{Z}_{21}$.

Antag att $a + 21\mathbb{Z} \in \overline{3}\mathbb{Z}_{21}$. Då finns det $k + 21\mathbb{Z}$ så att $a + 21\mathbb{Z} = (3 + 21\mathbb{Z})(k + 21\mathbb{Z}) = 3k + 21\mathbb{Z}$. Det betyder att $\varphi(a + 21\mathbb{Z}) = \varphi(3k + 21\mathbb{Z}) = 3k + 3\mathbb{Z} = 0 + 3\mathbb{Z}$. Alltså gäller $\overline{3}\mathbb{Z}_{21} \subseteq \text{Ker}(\varphi)$. De två inklusionerna ger oss att $\text{Ker}(\varphi) = \overline{3}\mathbb{Z}_{21}$.

c) Eftersom att $\varphi : \mathbb{Z}_{21} \to \mathbb{Z}_3$ är en homomorfism där $\text{Im}(\varphi) = \mathbb{Z}_3$ och $\text{Ker}(\varphi) = \overline{3}\mathbb{Z}_{21}$ så säger Noethers första isomorfi sats att $\mathbb{Z}_{21}/\overline{3}\mathbb{Z}_{21} \cong \mathbb{Z}_3$.

Lösning till problem 6. Eftersom att $\mathbb{C}$ är en kropp så är $\mathbb{C}[x]$ en Euklidisk ring (enligt Sats 13.6 från föreläsningsanteckningarna) och varje Euklidisk ring är en huvudidealring (enligt Sats 13.10). Vi vet alltså att alla polynom är på formen $I = \langle p(x) \rangle$ för något $p(x) \in \mathbb{C}[x]$. Enligt Sats 11.17 så är $\langle p(x) \rangle$ ett maximalt ideal om och endast om $p(x)$ är irreducibelt.

Först kommer vi ihåg att ett komplext polynom är inverterbart om och endast om det är ett nollskilt konstant polynom. Enligt Algebrans fundamentalsats har varje icke-konstant komplext polynom ett nollställe $x = z$, och enligt Faktorsatsen kan $p(x)$ då skrivas som $(x - z)q(x)$ för något $q(x) \in \mathbb{C}[x]$. Om $\deg(p) > 1$ så är $\deg(q) > 0$ och $p(x)$ är då en produkt av två icke-inverterbara element, d.v.s. $p(x)$ är *inte* irreducibelt.

Om $\deg(p) = 1$ och $p(x) = q(x)r(x)$ så får vi följande likhet (eftersom $\mathbb{C}[x]$ är ett integritetsområde):

$$1 = \deg(p) = \deg(q) + \deg(r).$$

Alltså måste någon av q, r ha grad 0 och är därmed inverterbara. Alltså är de irreducibla elementen precis förstagradspolynomen. Notera att varje komplext förstagradspolynom är associerat med ett moniskt förstagradspolynom. Två associerade element genererar samma ideal!

Alltså är de maximala idealen i $\mathbb{C}[x]$ precis idealen $\langle x - z \rangle$ för varje $z \in \mathbb{C}$.

Lösning till problem 7. **a)** Eftersom ringen av Gaussiska heltal är en Euklidisk ring så det även en huvudidealring enligt Sats 13.10. Alltså är alla ideal på formen $\langle a + bi \rangle$ för något $a + bi \in \mathbb{Z}[i]$.

b) Enligt Sats 13.14 så är generatorn till $\langle -3+9i, -5+25i \rangle$ lika med den största gemensamma faktorn till $-1 + 3i$ och $-5 + 24i$. Vi behöver alltså faktorisera de två Gaussiska heltalen!

Vi börjar med att faktorisera $-3 + 9i$.

i) Vi bryter ut $\text{sgd}(-3, 9) = 3$: $-3 + 9i = 3(-1 + 3i)$

ii) Vi noterar att 3 är ett primtal.

iii) Eftersom $3 \equiv 3 \pmod 4$ så är 3 ett irreducibelt Gaussiskt heltal.

iv) Vi börjar faktoriseringen av $-1 + 3i$ genom att beräkna $N(-1 + 3i) = (-1)^2 + 3^2 = 10$.

v) Vi faktoriserar normen i primtal: $10 = 2 \cdot 5$.

vi) Vi faktoriserar primtalsfaktorer i irreducibla Gaussiska heltal:

$$2 = (1 + i)(1 - i), 5 = (1 + 2i)(1 - 2i).$$

vii) Vi kontrollerar vilket Gaussiskt heltal i de konjugerade paren som delar $-1 + 3i$:

$$\begin{aligned} \frac{-1 + 3i}{1 - 2i} &= \frac{(-1 + 3i)(1 + 2i)}{5} \\ &= \frac{-7 + i}{5} \notin \mathbb{Z}[i]. \end{aligned}$$

$$\begin{aligned} \frac{-1 + 3i}{1 + 2i} &= \frac{(-1 + 3i)(1 - 2i)}{5} \\ &= \frac{5 + 5i}{5} \\ &= 1 + i \end{aligned}$$

viii) Eftersom $N(1 + i) = 2$ så är $1 + i$ irreducibel och vi är klara!

Vi har nu kommit fram till att följande är en faktorisering av $-3+9i$ i irreducibla Gaussiska heltal:

$$-3+9i = 3(1+i)(1+2i).$$

Nu vill vi faktorisera $-5+25i$.

i) Vi bryter ut $\text{sgd}(-5, 25) = 5$: $-5+25i = 5(-1+5i)$

ii) Vi noterar att 5 är ett primtal.

iii) Eftersom $5 \not\equiv 3 \pmod 4$ så kan 5 skrivas som en summa av två kvadrater: $5 = 1^2 + 2^2 = (1+2i)(1-2i)$, där $1+2i$ och $1-2i$ är irreducibla Gaussiska heltal.

iv) Vi börjar faktoriseringen av $-1+5i$ genom att beräkna $N(-1+5i) = (-1)^2 + 5^2 = 26$.

v) Vi faktoriserar normen i primtal: $26 = 2 \cdot 13$.

vi) Vi faktoriserar primtalsfaktorer i irreducibla Gaussiska heltal:

$$2 = (1+i)(1-i), 13 = (2+3i)(2-3i).$$

vii) Vi kontrollerar vilket Gaussiskt heltal i de konjugerade paren som delar $-1+5i$:

$$\begin{aligned}\frac{-1+5i}{2-3i} &= \frac{(-1+5i)(2+3i)}{13} \\ &= \frac{-17+7i}{13} \notin \mathbb{Z}[i]\end{aligned}$$

$$\begin{aligned}\frac{-1+5i}{2+3i} &= \frac{(-1+5i)(2-3i)}{13} \\ &= \frac{13+13i}{13} \\ &= 1+i\end{aligned}$$

viii) Eftersom $N(1+i) = 2$ så är $1+i$ irreducibel och vi är klara!

Vi har nu kommit fram till att följande är en faktorisering av $-5+25i$ i irreducibla Gaussiska heltal:

$$-5+25i = (1+2i)(1-2i)(1+i)(2+3i).$$

Den största gemensamma faktorn till de två Gaussiska heltalen är alltså:

$$\text{sgd}(-3+9i, -5+25i) = \text{sgd}(3(1+i)(1+2i), (1+2i)(1-2i)(1+i)(2+3i)) = (1+i)(1+2i) = -1+3i.$$

Detta betyder att $I = \langle -3+9i, -5+25i \rangle = \langle -1+3i \rangle$.