UPPSALA UNIVERSITET
Matematiska institutionen
Jakob Zimmermann

Prov i matematik
Ma kandidat, lärare, fristående
Algebra II, 5 p
2016–xx–xx

Tillåtna hjälpmedel: Skrivdon, passare och linjal. Lösningarna skall åtföljas av förklarande text. Uppgift 4 ger maximalt 10 poäng alla andra uppgifter maximalt 5. Om inget annat anges så antags alla ringar vara kommutativa ringar med egenskapen att $1 \neq 0$. Notera att uppgifterna är utplacerade i slumpmässig ordning, dvs ordning korresponderar inte nödvändigtvis mot svårighetsgrad.
Skrivtid: *xx.xx–xx.xx.*

1. Faktorisera $(6+2i)\cdot(3-4i)$ i irreducibla faktorer i $\mathbb{Z}[i]$. *Svar:* Observera att $a+bi \in \mathbb{Z}[i]$ är irreducibel om antingen $a+bi$ är ett primtal kongruent 3 (mod 4) eller om a^2+b^2 är ett primtal, eller om $a+bi$ är associerat till ett element på den formen. Vi kan faktorisera $6+2i$ och $3-4i$ var för sig och sedan sätta ihop resultatet.
Notera att $6+2i = 2(3+i)$, då $2 = (1+i)(1-i)$ och både $1+i$ och $1-i$ är irreducibla ty $1^2+1^2 = 2$ är ett primtal. Om vi sedan beräknar normen av $3+i$ så får vi $N(3+i) = 3^2+1^2 = 10 = 2\cdot 5$. Som vi redan har sett har 2 faktorerna $1 \pm i$. Vi får

$$\frac{3+i}{1+i} = \frac{(3+i)(1-i)}{2} = \frac{4-2i}{2} = 2-i,$$

dvs $3+i = (1+i)(2-i)$. $2-i$ är irreducibelt eftersom att $2^2+1^2 = 5$ är ett primtal.
Faktorisera nu $3-4i$: Först ser vi att $3^2+4^2 = 25 = 5^2$. Därför har vi att antingen $2+i$ eller $2-i$ är en faktor i $3-4i$. Vi testar:

$$\begin{aligned}\frac{3-4i}{2+i} &= \frac{(3-4i)(2-i)}{5} = \frac{2-11i}{5} \notin \mathbb{Z}[i],\\ \frac{3-4i}{2-i} &= \frac{(3-4i)(2+i)}{5} = \frac{10-5i}{5} = 2-i,\end{aligned}$$

dvs $3-4i = (2-i)^2$.
Tilsammans får vi

$$(6+2i)\cdot(3-4i) = (1+i)^2(1-i)(2-i)^3 = -(1-i)^3(2-i)^3,$$

där vi för den sista likheten använde att $1+i = i(1-i)$.

2. Låt R vara en kommutativ ring. Ett element $x \in R$ är *nilpotent* om det finns ett heltal $n > 0$ så att $x^n = \prod_{i=1}^{n} x = 0$.

- **a)** Visa att om x är nilpotent så är $x = 0$ eller en nolldelare.
- **b)** Låt $x, y \in R$ nilpotenta element, $r \in R$. Visa att $x+y$ och rx är nilpotent.
- **c)** Låt $x \in R$ vara nilpotent och $u \in R$ inverterbart. Visa att $1-x$ är inverterbart och dra slutsatsen att $u-x$ är inverterbart.

Svar:

- **a)** Antag att $x \in R$ är nilpotent och $x \neq 0$. Då ska vi visa att x är en nolldelare. Välj $n > 0$ så att $x^n = 0$ och $x^{n-1} \neq 0$, ett sådant finns eftersom x är nollskilt och nilpotent. Då är $0 = x^n = x \cdot x^{n-1}$ och eftersom x och x^{n-1} är nollskilda, är x en nolldelare.
- **b)** Låt $x, y \in R$ vara nilpotenta och $r \in R$. Då finns det $n, m > 0$ så att $x^n = 0 = y^m$. Nu använder vi att R är en kommutativ ring och vi därmed har att $(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i}$. Vi ser direkt

att $\binom{k}{i} a^i b^{k-i} = 0$ om $i > n$ eller $k-i > m$ vilket är uppfyllt om $k = i+(k-i) > n+m$. Därför är $(x+y)^{n+m+1} = 0$ och $x+y$ nilpotent. Vidare är $(rx)^k = r^k x^k$ eftersom R är kommutativ vilket innebär att $(rx)^n = 0$ ty $x^n = 0$ och rx är nilpotent.

c) Låt $x^n = 0$. Då gäller

$$1 = 1 - x^n = (1-x)(1 + x + x^2 + \cdot + x^{n-1},$$

dvs $1-x$ är inverterbart. Alternativt kan man observera att $(1-x)(1+) = 1-x^2$, $(1-x^2)(1+x^2) = (1-x)(1+x)(1+x^2) = 1-x^4$, $(1-x^4)(1+x^4) = (1-x)(1+x)(1+x^2)(1+x^4) = 1-x^8$. Man kan då ha idÃ©n att $(1-x)\prod_{i=0}^{k} 1 + x^{2i} = 1 - x^{2k+1}$ vilket kan visas med induktion. Nu använder man att x är nilpotent och får återigen att $(1-x)\prod_{i=0}^{k} 1 + x^{2i} = 1 - x^{2k+1} = 1$ för något $k > 0$ vilket medför att $1-x$ är inverterbart. För den sista delen observerar man att $u - x = u(1 - u^{-1}x)$ och enligt b) är $u^{-1}x$ nilpotent och därmed $1 - u^{-1}x$ inverterbart. Då är $u - x$ som en produkt av två inverterbara element, inverterbart.

3. I denna uppgift ska du hitta olika typer av ideal. Självklart ingår det att du måste visa att ditt exempel är ett exempel på den typen av ideal som söks.

a) Hitta ett maximalt ideal i $\mathbb{Z} \times \mathbb{Z}$.

b) Hitta ett primideal i $\mathbb{Z} \times \mathbb{Z}$ som inte är maximalt.

c) Hitta ett icke-trivialt äkta ideal i $\mathbb{Z} \times \mathbb{Z}$ som inte är ett primideal.

Svar:

a) $2\mathbb{Z} \times \mathbb{Z}$, beviset för maximalitet går nästan samma som att $2\mathbb{Z}$ är ett maximalt ideal i $\mathbb{Z}$.

b) $0\mathbb{Z} \times \mathbb{Z} = \{0\} \times \mathbb{Z}$ är ett primideal ty $\mathbb{Z}$ saknar nolldelare och inte maximalt ty $\{0\} \times \mathbb{Z} \subsetneq 2\mathbb{Z} \times \mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z}$.

c) $4\mathbb{Z} \times \mathbb{Z}$, ty $(2,1)(2,1) = (4,1) \in 4\mathbb{Z} \times \mathbb{Z}$ men $(2,1) \notin 4\mathbb{Z} \times \mathbb{Z}$.

4. Visa eller motbevisa (t.ex. med hjälp av ett motexempel) följande påståenden

a) Varje integritetsområde är en faktoriell ring.

b) Låt R, S vara ringar och $f : R \to S$ en homomorfism. Då är $\ker(f) = \{x \in R \mid f(x) = 0\}$ ett ideal i R.

c) Mängden av alla udda heltal är ett ideal i $\mathbb{Z}$.

d) Låt R vara en ring och $a \in R$ en nolldelare. Då är a inte inverterbart.

e) Låt R, S vara integritetsområden. Då är $R \times S$ ett integritetsområde.

Svar:

a) Falskt, ty t ex i $\mathbb{Z}[i\sqrt{5}]$ är $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ och varken 2 eller 3 är associerat till $1 \pm i\sqrt{5}$ och heller inget av dem är inverterbart.

b) Sant, ty $0 \in \ker(f)$, dvs $\ker(f) \neq \emptyset$. Vidare gäller för $a, b \in \ker(f)$ och $r \in R$ att $f(a+b) = f(a) + f(b) = 0 + 0$ och $f(ra) = rf(a) = 0 = f(a)r = f(ar)$, vilket innebär att $a + b, ra, ar \in \ker(f)$.

c) Falskt, ty $1, 3$ är udda tal men $1 + 3 = 4$ är inte det, dvs mängden är inte sluten under addition.

d) Sant, ty antag att a är en nolldelare som är inverterbar. Då är $a \neq 0$ och det finns ett $b \neq 0$ så att $ab = 0$. Då är $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$ en motsägelse.

e) Falskt, ty $(1_R, 0_S)(0_R, 1_S) = (0_R, 0_S) = 0_{R\times S}$ i varje produktring och $(1_R, 0_S) \neq (0_R, 0_S) = 0_{R\times S}$, $(0_R, 1_S) \neq (0_R, 0_S) = 0_{R\times S}$ om R, S är integritetsområden.

5. **a)** Visa att $(a+b)^p \equiv a^p + b^p \pmod p$ med hjälp av Fermats lilla sats.

b) Visa att $(a+b)^p \equiv a^p + b^p \pmod p$ utan Fermats lilla sats.

c) Visa Fermats lilla sats med hjälp av b).

Svar:

a) Enligt Fermats lilla sats gäller $a^p \equiv a \pmod p$ för alla $a \in \mathbb{Z}$. Därför är $(a+b)^p \equiv (a+b) \equiv a^p + b^p \pmod p$.

b) Enligt binomialsatsen har vi att $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$. Observera att $\binom{p}{k}$ är ett heltal större än 1 om $1 \le k \le p-1$ och $p \nmid k$. Därför måste $p | \binom{p}{k}$. Med andra ord har vi att $\sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \equiv 0 \pmod p$ vilket visar påståendet.

c) Vi ska visa att $a^p \equiv a \pmod p$ för alla $a \in \mathbb{Z}$. Observera att $p | a^p - a \Leftrightarrow p | (-a)^p + a = -(a^p - a)$ om $p > 2$, är $p = 2$ så gäller också att $p | (-a)^2 + a$ och därmed kan vi visa påståendet med induktion. Basfallet är $a = 0$ och då gäller att $0^p = 0 \equiv 0 \pmod p$. Antag nu att $a^p \equiv a \pmod p$. Då har vi att $(a+1)^p \equiv a^p + 1^p$ enligt förra uppgift. Vidare är $a^p + 1^p \equiv a + 1 \pmod p$ enligt induktionsantagandet och vi är klara.

6. **a)** Studera $f : \mathbb{R}[X] \to \mathbb{C}$ definierad av $f(p(X)) = p(i)$, dvs $p(X)$ utvärderat i i. Visa att f är en surjektiv homomorfism.

b) Visa att $\langle X^2 + 1 \rangle \subset \ker(f)$.

c) Visa att $\ker(f) \subset \langle X^2 + 1 \rangle$.

d) Visa att $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathbb{C}$.

Svar:

a) Låt $p(X), q(X) \in R[X]$. Då är $f(p(X) + q(X)) = f((p+q)(X)) = (p+q)(i) = p(i) + q(i) = f(p(X)) + f(q(X))$ och likadant för multiplikationen. Dessutom är $f(1) = 1(i) = 1$ och f därmed en homomorfism. Surjektivitet följer direkt ty $f(a + bX) = a + bi$ för varje $a + bi \in \mathbb{C}$.

b) Låt $p(X) \in \langle X^2 + 1 \rangle$ dvs $p(X) = (X^2 + 1)q(X)$. Då är $f(p(X)) = f((X^2 + 1)q(X)) = (i^2 + 1)q(i) = 0$, dvs $p(X) \in \ker(f)$.

c) Låt $p(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$. Vi observerar först att $p(i) = 0 \Leftrightarrow p(-i) = 0$. Detta följer eftersom vi kan sortera summanderna i $\sum_{k=0}^{n} a_k i^k$ beroende på deras paritet (dvs en summa med alla jämna k och en med alla udda k). Den första summan är reell och den andra är rent imaginär, dvs vi kan bryta ut i. Vi får då att $p(i)$ är på formen $a+bi$ och ser att $p(-i)$ har samma uppdelning upp till tecken. Därmed är $f(p(i)) = 0 \Leftrightarrow f(p(-i))$. Om vi betraktar $p(X)$ som ett komplext polynom får vi enligt faktorsatsen att $p(X) = (X - i)(X + i)q(X) = (X^2 + 1)q(X)$ för något $q(X) \in \mathbb{C}[X]$. Men eftersom $p(X)$ är ett reellt polynom och $X^2 + 1$ har bara reella koefficienter måste även $q(X)$ vara ett reellt polynom. Därför är $p(X) \in \langle X^2 + 1 \rangle$ och därmed $\ker(f) \subset \langle X^2 + 1 \rangle$.

d) Enligt Noethers 1:a isomorfisats gäller $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathrm{im}(f) = \mathbb{C}$, ty f är surjektiv och $\langle X^2 + 1 \rangle = \ker(f)$.

7. Hitta alla heltalslösningar till ekvationssystemet

$$\begin{cases} x \equiv 5 & \pmod 3 \\ x \equiv 3 & \pmod 7 \\ x \equiv 1 & \pmod 8 \end{cases}$$

Svar: Vi ser direkt att $(3, 7) = (3, 8) = (7, 8) = 1$ så att vi kan använda kinesika restsatsen. Sätt $x = 56b_1 + 24b_2 + 21b_3$ och lös kongruensen för $b_1, b_2, b_3 \in \mathbb{Z}$. Vi får då det ekvivalenta systemet

$$\begin{cases} 56b_1 \equiv 2 & \pmod 3 \\ 24b_2 \equiv 3 & \pmod 7 \\ 21b_3 \equiv 1 & \pmod 8 \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 & \pmod 3 \\ x \equiv 3 & \pmod 7 \\ x \equiv 1 & \pmod 8 \end{cases}$$

Vi får då att $b_1 = 1 + 3k_1$, $b_2 = 1 + 7k_2$, $b_3 = 5 + k_3$, $k_1, k_2, k_3 \in \mathbb{Z}$ vilket medför att lösningarna är på formen $x = 56 \cdot (1 + k_1) + 24 \cdot (1 + k_2) + 21 \cdot (5 + k_3)$ dvs $x = 17 + 168k$ för $k \in \mathbb{Z}$.