**UPPSALA UNIVERSITET**
**Matematiska institutionen**
Johan Björklund

Prov i matematik
Ma kandidat, lärare, fristående
LÖSNINGAR för Algebra II, 5 p
2008–05–23

*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 ett integritetsområde.
- $R$ är en kropp.
- $R$ är euklidisk.
- $R$ är faktoriell.

**Lösning, uppgift 1**

Kropp⇒Euklidisk⇒Faktoriell⇒Integritetsområde.

**2.** **a)** Existerar det en ring $R$ och en nolldelare $a \in R$ så att $a$ är inverterbar? Exempel eller motbevis.

**b)** Visa att en ring $K$ är en kropp om och endast om ringen $K$ enbart innehåller två ideal.

**c)** Givet en godtycklig ring $R$ och två inverterbara element $a, b \in R$, följer det att $a \cdot b$ är inverterbart? Bevis eller motexempel.

**d)** Givet en godtycklig ring $R$ och två inverterbara element $a, b \in R$, följer det att $a + b$ är inverterbart? Bevis eller motexempel.

**Lösning, uppgift 2**

**a)** Nej. Bevis: antag att det finns en nolldelare $a$ som är inverterbar. Då existerar $b, c$ så att $b \neq 0, ab = 0$ samt $ca = 1$. Då är $b = 1 \cdot b = (ca)b = c(ab) = c \cdot 0 = 0$ vilket ger motsägelse.

**b)** Antag att $K$ är en ring som innehåller endast två ideal. Då måste dessa vara hela ringen $K$ samt $\{0\}$ då dessa alltid är ideal. Antag att vi har ett godtyckligt element $a \neq 0$. Då måste $\langle a \rangle$ vara ett ideal som inte enbart innehåller noll, men då kan det endast vara idealet $K$. Alltså så ligger 1 i $\langle a \rangle$ vilket ger att det existerar $b$ sådant att $1 = ba$ vilket ger att $a$ är inverterbart. Då har vi viast ena hållet. Antag nu att $K$ är en kropp. Tag ett ideal $I \subset K$. Om $I \neq \{0\}$ så existerar det $a \neq 0$ i $I$. Då $K$ är en kropp så existerar det ett tal $b \in K$ så att $ba = 1$. Då följer det att $ba = 1 \in I$ och om ett ligger i ett ideal så är det idealet hela ringen. Alltså så kan ett ideal antingen vara $\{0\}$ eller hela ringen, dvs vi har endast två ideal.

**c)** Det följer. Bevis: Låt $a, b$ vara inverterbara, då existerar $c, d$ så att $ac = 1, bd = 1$. Då gäller att $(ab)(dc) = a(bd)c = a \cdot 1 \cdot c = ac = 1$ alltså så har vi en invers (nämligen $dc$).

**d)** Det följer inte. Motexempel: Låt ringen vara $\mathbb{Z}$. 1 samt $-1$ är inverterbara men deras summa 0 är ej inverterbar.

**3.** Faktorisera $(6+2i)(3-4i)$ 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 $w = (6+2i)(3-4i)$. Vi ser omedelbart att vi kan faktorisera ut en tvåa från den första faktorn. Då får vi $w = 2(3+i)(3-4i)$. 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.

Vi studerar faktorn $3+i$ härnäst. Det är inget primtal, och dess norm är $3^2+1^1 = 10$ inte heller ett primtal. Dock så gäller det tydligen att $(3+i)(3-i) = 10 = 2\cdot 5 = (1+i)(1-i)\cdot 5$. Faktorerna $1+i$ och $1-i$ är alltså möjliga delare. Ifall man kollar detta så ser man snabbt att $3+i = (1+i)(2-i)$. Faktorn $(2-i)$ är nu också irreducibel då $2^2+1^2 = 5$ som är ett primtal.
Den enda faktorn kvar att undersöka är $3-4i$, 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 $(3-4i)(3+4i) = 5\cdot 5$. $5 = 2^2+1^2 = (2+i)(2-i)$ 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 $(3-4i) = (2-i)^2$. Så när vi plockar samman alla våra faktorer så får vi att

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

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

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

Alla faktorerna är irreducibla och vi är klara.

**4.** **a)** Bevisa Fermats lilla sats: givet ett primtal $p$ och ett godtyckligt heltal $x$ så är $x^p - x$ delbart med $p$.

**b)** Använd detta för att beräkna $17^{18^{19}} \pmod{19}$.

**Lösning, uppgift 4**

**a)** Vi visar detta med induktion. Tag ett primtal $p$. Om $x = 0$ så är $x^p - x$ delbart med $p$ så basen i induktionen är klar (det kanske bör noteras att det fungerar att starta med noll och gå uppåt ty alla negativa tal ligger ju i samma restklass som något positivt tal vilket gör att vi får med dem också). Antag att det det är sant för $x = n$ att $n^p - n$ är delbart med $p$ och undersök $x = n+1$. Vi använder binomialsatsen på $(n+1)^p - n - 1 = n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^k 1^{p-k}$. Vi noterar snabbt att termerna i summan alla har en faktor $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ där $1 \le k \le p-1$ då detta är ett heltal samt nämnaren ej innehåller en faktor $p$ så måste $\binom{p}{k}$ vara delbart med $p$. Då varje term i summan är delbar med $p$ så är summan delbar med $p$, den andra termen $n^p - n$ är delbar med $p$ pga det tidigare induktionsfallet.

**b)** Vi vet att $(17, 19) = 1$ samt att 19 är ett primtal. Då säger Eulers sats att $17^{18} \equiv 1 \pmod{19}$ (detta kan också härledas ur Fermats genom att multiplicera med inversen till 17 räknat modulo 19). Då gäller

$$17^{18^{19}} = 17^{18\cdot 18^{18}} \equiv (17^{18})^{18^{18}} \equiv 1^{18^{18}} \equiv 1 \pmod{19}.$$

**5.** Hitta alla heltalslösningar till ekvationssystemet

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

**Lösning, uppgift 5** Vi noterar att $3, 7, 8$ är relativt prima så kinesiska restsatsen säger att det finns en unik lösning modulo $3 \cdot 7 \cdot 8$, vi finner denna genom att ansätta $x = x_1 \cdot 7 \cdot 8 + x_2 \cdot 3 \cdot 8 + x_3 \cdot 3 \cdot 7$. Detta ger oss efter insättning och ett par trivial moduloräkningar.

$$\begin{cases} 2x_1 & \equiv & 2 & \pmod 3 \\ 3x_2 & \equiv & 3 & \pmod 7 \\ 5x_3 & \equiv & 1 & \pmod 8 \end{cases}$$

Genom att prova oss fram så får vi snabbt att $x_1 = x_2 = 1, x_3 = 5$ vilket ger oss

$$x \equiv 7 \cdot 8 + 3 \cdot 8 + 5 \cdot 3 \cdot 7 \pmod{3 \cdot 7 \cdot 8}$$

vilket nu är ett svar tack vare våra beräkningar, och ett unikt svar (räknat modulo $3 \cdot 7 \cdot 8$ tack vare kinesiska restsatsen.

**6.** Ge definitionen av en ring. Är de udda heltalen en ring med standardaddition/multiplikation?

**Lösning, uppgift 6** Använd definitionen i kompendiet. Det är kanske enklare att minnas om man tänker på att det ska vara fyra axiom för addition (nollan, kommutativitet, associativitet samt additiv invers), två för multiplikation (ettan samt associativitet) samt en för hur man blandar dem (distributivitet). Man bör också minnas att det faktiskt ingår i definitionen att en ring är en mängd med två operationer så att man inte bara skriver axiomen. De udda heltalen är inte en ring, exempelvis så är summan av två udda tal inte ett udda tal vilket strider mot att additionen ska gå från par ur ringen till ringen.

**7.** **a)** Studera $f : \mathbb{Z}[i] \to \mathbb{Z}_5$ definierad av $f(a + bi) = \overline{a + 2b}$, dvs $(a + 2b)$:s restklass $\pmod 5$. Visa att $f$ är en surjektiv homomorfism.

**b)** Visa att $\ker(f) \subset \langle 2 - i \rangle$. Som vi vet så är $\ker(f) = \{x \in \mathbb{Z}[i] : f(x) = 0\}$.

**c)** Visa att $\langle 2 - i \rangle \subset \ker(f)$.

**d)** Använd Noethers första isomorfisats för att visa $\mathbb{Z}[i]/\langle 2 - i \rangle \simeq \mathbb{Z}_5$.

**Lösning, uppgift 7**

**a)** Vi visar först att vi har en homomorfism. $f(1) = 1$ så det första kravet är klart. Låt $a+bi$ samt $c + di$ ligga i $\mathbb{Z}[i]$. Vi kontrollerar så att funktionen respekterar addition samt multiplikation.

$$f(a+bi)+f(c+di) = a+2b+c+2d = (a+c)+2(b+d) = f((a+c)+(b+d)i) = f(a+bi+c+di)$$

$$f(a + bi) \cdot f(c + di) = (a + 2b)(c + 2d) = ac + 4bd + 2(bc + ad) =$$
$$= ac - bd + 2(bc + ad) = f((ac - bd) + (bc + ad)i) = f((a + bi)(c + di)).$$

Alltså så är $f$ en homomorfism. Den är uppenbart surjektiv eftersom $f(n) = \overline{n}$ där $n$ är ett heltal.

**b)** Låt $z = a + bi \in ker(f)$. Då gäller att $a + 2b = 0 \pmod 5$. Dvs $a = -2b + 5c$ där $c$ är ett heltal. $z = -2b + 5c + bi = (2 - i)b + 5c$, vi vet också att $5 = (2 + i)(2 - i)$. Då får vi $z = (-b + 2c - ic)(2 - i)$, dvs $z \in \langle 2 - i \rangle$. Då $z$ var ett godtycklig element i kärnan så följer att kärnan ligger i det idealet.

**c)** Låt $z \in \langle 2 - i \rangle$ då är $z = w(2 + i)$ enligt definition. $f(z) = f(w(2 - i)) = f(w)f(2 - i) = f(w) \cdot 0 = 0$ så alltså så ligger varje element i idealet också i kärnan.

**d)** Enligt tidigare så har vi $ker(f) = \langle 2 - i \rangle$. Vi har en surjektiv homomorfism $f : \mathbb{Z}[i] \to \mathbb{Z}_5$. Enligt Noethers första så har vi då att $\mathbb{Z}[i]/\langle 2 - i \rangle \simeq \mathbb{Z}_5$. Då vi visste att $ker(f) = \langle 2 - i \rangle$ så har vi $\mathbb{Z}[i]/\langle 2 - i \rangle \simeq \mathbb{Z}_5$.

**8.** Givet ett ideal $I \subset R$ definierar vi $\sqrt{I}$ som mängden av alla element $x \in R$ så att det existerar något $n \in \mathbb{N}$ sådant att $x^n \in I$. Visa att $\sqrt{I}$ är ett ideal.

**Lösning, uppgift 8** För att visa att någon mängd $I \subset R$ är ett ideal så ska det uppfylla tre krav, det skall vara en icketom mängd, om $a, b \in I$ så skall $a + b \in I$ samt om $a \in I, r \in R$ så skall $ra \in I$. Vi observerar snabbt att det första kravet uppfylls lätt, sätt $n = 1$ så ser vi att $I \subset \sqrt{I}$, och då $I$ var ett ideal så måste det ju speciellt vara icketomt. Det tredje kravet är också lätt, ty om $a \in \sqrt{I}$ och $r \in R$ så måste ju $a^n \in I$ enlight definitionen av vårt nya förslag på ideal, men då måste även $r^n a^n = (ra)^n \in I$ (då $r^n$ måste ligga i ringen om $r$ ligger i ringen) och alltså så är $ra \in \sqrt{I}$. Endast ett krav är kvar. Låt $a, b \in \sqrt{I}$. Då existerar positiva heltal $m, n$ sådana att $a^n, b^m \in I$. Studera $(a + b)^{m+n}$. Om vi kan visa att det ligger i $I$ så är vi klara. Vi använder binomialsatsen. En godtycklig term kommer att vara på utseendet $\binom{n+m}{k} a^k b^{m+n-k}$. Om vi kan vissa att alla dessa termer ligger i $I$ så är vi klara ty då måste ju även deras summa ligga i $I$ då $I$ är ett ideal. Om $k \geq n$ så ligger $a^k$ i $I$ och vi är klara då även dess produkt med resten av sakerna (binomialfaktorn, $b$ faktorn) måste stanna i idealet. Om $k < n$ så är $m+n-k > m$ och vi kan upprepa samma argument för $b$-faktorn.