UPPSALA UNIVERSITET
Matematiska institutionen
Johan Björklund

Prov i matematik
Ma kandidat, lärare, fristående
ÖVNINGSTENTA, Algebra II, 5 p
2008–XX–YY

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 medför det andra, det andra implicerar det tredje osv. Inga bevis krävs. R antags vara en ring.

- R är en kommutativ ring.
- R är en kropp.
- R är en huvudidealring.
- R är faktoriell.

2. **a)** Om en ring R är ett integritetsområde och $I \subset R$ ett äkta ideal, måste då R/I vara ett integritetsområde? Bevis eller motexempel.

b) Om R/I är ett integritetsområde (R är en ring och $I \subset R$ ett äkta ideal), måste då I vara ett primideal? Bevis eller motexempel.

c) I denna kurs så har vi mestadels studerat kommutativa ringar. Ge ett exempel på en icke-kommutativ ring.

d) I denna kurs så har vi mestadels studerat ringar med egenskapen att $0 \neq 1$. Ge ett exempel på en ring där $0 = 1$.

3. Hitta alla heltalslösningar till ekvationssystemet

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{12} \\ x \equiv 1 \pmod{7} \end{cases}$$

4. **a)** Beräkna $\phi(18)$.

b) Beräkna $2^{2^{17}} \pmod{19}$ med hjälp av Eulers sats.

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

5. Antag att vi har två stora primtal q och p. Beskriv hur RSA-algoritmen kan användas för att koda ett meddelande med hjälp av dessa primtal och en publik nyckel $e = 3$ så att $3 \nmid (p-1)(q-1)$.

6. Faktorisera $x^{16} - 1$ i $\mathbb{Z}_{17}[x]$ i irreducibla faktorer.

Fortsättning följer på andra sidan!

7. **a)** Ge definitionen för att ett element a i en ring R ska vara irreducibelt.

b) Ge definitionen för att ett element a i en ring R ska vara ett primelement.

c) Ge definitionen för att en ring R ska vara ett integritetsområde.

d) Visa att om a är ett primelement i ett integritetsområde R så är a irreducibelt.

8. Låt R vara en ring så att $|R| < \infty$ (dvs en ändlig ring). Låt $I \subset R$ vara ett ideal. Visa att $|R/I| = \dfrac{|R|}{|I|}$.

Tips: Varje element i R/I är en ekvivalensklass. Visa först att alla ekvivalensklasser innehåller lika många element.