Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

**Løsningsforslag — Øving 9**

## Seksjon 18

**18** Et element i $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ er et trippel $(a, q, b)$, der $a, b \in \mathbb{Z}$, $q \in \mathbb{Q}$. Anta nå at dette trippelet har en invers $c, p, d$. Da er altså $ac = bd = 1$ og $pq$=1. Følgelig er $a$ og $b$ enheter i $Z$ og må dermed være lik $\pm 1$. $q$ er en enhet i $\mathbb{Q}$, og siden $\mathbb{Q}$ er en kropp betyr det bare at $q \neq 0$.

Vi får altså enhetene i $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ er

$$(1, q, 1) \qquad (1, q, -1) \qquad (-1, q, 1) \qquad (-1, q, -1)$$

der $q \in \mathbb{Q}$, $q \neq 0$.

**37** Vi viser først at $U$ er lukket under multiplikasjon; hvis $U$ er det har vi en veldefinert binæroperasjon på $U$ og kan dermed sjekke gruppeaksiomene. La derfor $u, v \in u$, og la $u', v'$ være deres multiplikative inverser. Da er $(uv)(v'u') = u(vv')u' = uu' = 1$. Dermed har $uv$ en multiplikativ invers, så $uv \in U$.

Vi sjekker så gruppeaksiomene:

- Multiplikasjon på $U$ er assosiativt fordi multiplikasjon i $R$ er det.
- $R$ inneholder multiplikativ identitet (unity), og denne er åpenbart en enhet og dermed inneholdt i $U$, og virker som identitetelement i $(U, \cdot)$.
- $u \in U$ har per definisjon en multiplikativ invers $u' \in R$. Denne $u'$ er igjen en enhet (med invers $u$), og dermed inneholdt i $U$.

**46** Anta at $a, b \in R$ er nilpotente elementer, slik at $a^n = 0 = b^m$ for $n, m > 0$. Da finner vi ved hjelp av binomialsetningen at:

$$\begin{aligned}
(a+b)^{m+n} &= \sum_{i=0}^{n+m} \binom{m+n}{i} a^{m+n-i} b^i \\
&= \sum_{i=0}^{m-1} \binom{m+n}{i} a^{m+n-i} b^i + \sum_{i=m}^{n+m} \binom{m+n}{i} a^{m+n-i} b^i \\
&= \underbrace{a^n}_{=0} \sum_{i=0}^{m-1} \binom{m+n}{i} a^{m-i} b^i + \underbrace{b^m}_{=0} \sum_{i=m}^{n+m} \binom{m+n}{i} a^{m+n-i} b^{i-m} = 0
\end{aligned}$$

## Seksjon 19

$\boxed{1}$ For å forstå oppgaven ed det lurt å først lese eksempel 19.1. Den greieste metoden for å finne alle røtter er nok å sjekke elementene i $\mathbb{Z}_{12}$.

Røttene er -4, -3, -1, 0, 3 og 5

$\boxed{2}$ Siden både 7 og 23 er primtall er $\mathbb{Z}_7$ og $\mathbb{Z}_{23}$ begge kropper. Derfor kan vi bruke kanselleringslovene; det vil si at vi kan skrive $x = 3^{-1}2$.

Vi ser først på $\mathbb{Z}_7$. Der er $3^{-1} = 5$. Dermed har vi at $x = 5 \cdot 2 = 3$.
Vi ser så på $\mathbb{Z}_{23}$. Der er $3^{-1} = 8$. Dermed har vi at $x = 8 \cdot 2 = 16$.

$\boxed{23}$ La $R$ være en divisjonsring, og la $a \in R$ være idempotent, det vil si at $a^2 = a$. Da har vi at $a(a-1) = a^2 - a = 0$. $R$ kan ikke inneholde nulldivisorer, altså må enten $a = 0$ eller så må $a - 1 = 0$, og dermed $a = 1$. Altså inneholder $R$ kun to idempotente elementer, nemlig 0 og 1.

## Ekstraoppgaver

$\boxed{1}$ Det er åpenbart at $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$. Videre kan vi se at $\mathbb{Z}[\sqrt{n}]$ er lukket under addisjon og multiplikasjon ved å regne ut henholdsvis summen og produktet av $a + b\sqrt{n}$ og $c + d\sqrt{n}$.

Vi ser så på ringaksiomene fra definisjon 18.1:

**R**1 Følger av at $(\mathbb{C}, +)$ er en abelsk gruppe og $(\mathbb{Z}[\sqrt{n}], +)$ er en undergruppe.

**R**2 Følger av at multiplikasjon er assosiativt i $\mathbb{C}$.

**R**3 Følger av at distributive lover holder i $\mathbb{C}$.

$\boxed{2}$ I denne oppgaven er det nyttig å huske tilbake til lineær algebra 1 eller matte 3. Husk først at om vi har to matriser $A, B \in M_n(\mathbb{C})$, og skriver $b_i$ for $i$'te kolonnevektor i $B$ (så $B = [b_1 \ldots b_n]$), så er $AB = [Ab_1 \ldots Ab_n]$.

Dersom $\det A = 0$, eksisterer det en vektor $x \neq 0$ slik at $Ax = 0$. Dermed er $A[x \ldots x] = 0$, så $A$ er en nulldivisor.

Dersom $A$ er en nulldivisor, finnes det altså en ikkenull-matrise $B$ slik at $Ab_i = 0$ for alle $b_i$; siden minst en kolonnevektor i $B$ er ikke-null, eksisterer det altså en vektor $x \neq 0$ slik at at $Ax = 0$. Følgelig er $\det A = 0$

Altså: $A$ er en nulldivisor hvis og bare hvis $\det A = 0$.

**3** **a)**

$$
\begin{gathered}
(a,b) \text{ enhet i } R \times S \\
\Leftrightarrow \\
\exists (c,d) \in R \times S : (a,b)(c,d) = (1_R, 1_S) \\
\Leftrightarrow \\
\exists c \in R, d \in S : ac = 1_R, bd = 1_S \\
\Leftrightarrow \\
a \text{ enhet i } R, b \text{ enhet i } S
\end{gathered}
$$

**b)** La $R$ og $S$ være ringer og la $f : R \to S$ være en ringisomorfi.

$$
\begin{gathered}
a \text{ enhet i } R \\
\Leftrightarrow \\
\exists c \in R : ac = 1_R \\
\Leftrightarrow \\
\exists c \in R : f(a)f(c) = f(1_R) = 1_S \\
\Leftrightarrow \\
f(a) \text{ enhet i } S
\end{gathered}
$$

**c)** At $f(a+b) = f(a) + f(b)$ og at $f(ab) = f(a)f(b)$ kontrolleres ved innsetting. $f$ er dermed en ringhomomorfi

$f(a,b) = (0,0)$ hvis og bare hvis $a \equiv 0 \mod m$ og $a = \equiv 0 \mod n$. Siden $\gcd(m,n) = 0$ må da $a \equiv 0 \mod mn$. $f$ er altså 1-1.

At $f$ er på følger av det kinesiske restleddsteoremet, eller eventuelt at $f$ er en 1-1 funksjon mellom to endelige mengder. Dermed er $f$ en ringisomorfi.

**d)** Vi starter med følgende observasjon:

$$\gcd(a, mn) = 1 \Leftrightarrow \exists b, x \in \mathbb{Z} : ba + xmn = 1 \Leftrightarrow a \text{ er en enhet i } \mathbb{Z}_{mn}.$$

Dette har vi i punkt b vist at inntreffer hvis og bare hvis $f(a)$ er en enhet i $\mathbb{Z}_m \times \mathbb{Z}_n$, noe som igjen bare skjer hvis $a \mod m$ og $a \mod n$ er enheter i henholdsvis $\mathbb{Z}_m$ og $\mathbb{Z}_n$. Altså har vi at:

$$
\begin{aligned}
\phi(mn) &= |\{\text{enheter i } \mathbb{Z}_{mn}\}| \\
&= |\{\text{enheter i } \mathbb{Z}_m \times \mathbb{Z}_n\}| \\
&= |\{\text{enheter i } \mathbb{Z}_m\} \times \{\text{enheter i } \mathbb{Z}_n\}| \\
&= \phi(m) \cdot \phi(n)
\end{aligned}
$$

**4** **a)** La $a \in \mathbb{C}$ være et vilkårlig element. Vi regner ut:

$$f(0) = f(a - a) = f(a) - f(a) = 0$$

Anta nå at $a \in \mathbb{C}$ er slik at $f(a) \neq 0$ (dersom $f$ er ikketriviell, må minst ett slikt element finnes). Da har vi at

$$f(a) = f(1 \cdot a) = f(1) \cdot f(a)$$

Siden $\mathbb{R}$ er en kropp kan vi nå bruke kanselleringslovene til å se at $f(1) = 1$. Til slutt ser vi at

$$f(-1) + 1 = f(-1) + f(1) = f(1 - 1) = f(0) = 0$$

Dermed er $f(-1) = -1$.

**b)** Vi har at

$$f(i)^2 = f(i^2) = f(-1) = -1$$

Altså må $f(i)$ være et tall som opphøyd i andre blir $-1$, men noe slikt tall eksisterer ikke i $\mathbb{R}$. Følgelig finnes det ingen ikke-trivielle ringisomorfier fra $\mathbb{C}$ til $\mathbb{R}$.