1. Gruppearbeid B i 18F

Oppgave 6. La

$$R = \{\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$$

med vanlig matriseaddisjon og matrisemultiplikasjon. Vi har sett at R er en kropp.

(a) Vis at R er isomorf med $\mathbb{C}$.
(b) Hvilken operasjon O svarer det å transponere en matrise til i $\mathbb{C}$?

Fasit. (a) Definer $\varphi\colon R \to \mathbb{C}$ ved at $\varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)) = a + bi$. Vi har at

$$\begin{aligned} \varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & -b' \\ b' & a' \end{smallmatrix}\right)) &= \varphi(\left(\begin{smallmatrix} aa'-bb' & -ab'-ba' \\ ba'+ab' & -bb'+aa' \end{smallmatrix}\right)) \\ &= aa' - bb' + (ab' + ba')i \\ \varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right))\varphi(\left(\begin{smallmatrix} a' & -b' \\ b' & a' \end{smallmatrix}\right)) &= (a + bi)(a' + b'i) \\ &= aa' - bb' + (ab' + ba')i, \end{aligned}$$

$$\begin{aligned} \varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & -b' \\ b' & a' \end{smallmatrix}\right)) &= \varphi(\left(\begin{smallmatrix} a+a' & -b-b' \\ b+b' & a+a' \end{smallmatrix}\right)) \\ &= a + a' + (b + b')i \\ &= (a + bi) + (a' + b'i) \\ &= \varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)) + \varphi(\left(\begin{smallmatrix} a' & -b' \\ b' & a' \end{smallmatrix}\right)) \end{aligned}$$

og

$$\varphi(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = 1.$$

Dette viser at φ er en homomorfi av ringer. Gitt $a + bi \in \mathbb{C}$, så er $\varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)) = a + bi$ og φ er på. Anta at $\varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)) = 0$. Det betyr at $a + bi = 0$ som skjer hvis og bare hvis $a = b = 0$. Dette gir at $\operatorname{Ker}\varphi = \{\left(\begin{smallmatrix} 0 & -0 \\ 0 & 0 \end{smallmatrix}\right)\}$ og at φ er en-til-en. Dette viser at φ er en isomorfi av ringer.

(b) For det første, den transponerte av et element i R er igjen et element i R. Vi har at

$$\varphi(\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)^T) = \varphi(\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)) = a - bi = \overline{a + bi},$$

slik at transponering av en matrise i R svarer til å ta den kompleks konjugerte i $\mathbb{C}$.

Oppgave 7. La R være en kropp. Vis at R er et integritetsområde.

Fasit. Anta at R er en kropp. La $a, b \in R$ og anta at $ab = 0$. Vi ønsker å vise at $a = 0$ eller $b = 0$. Hvis $a = 0$, så er det ingenting å vise. Anta at $a \neq 0$. Siden R er en kropp, så har a en invers a^{-1}. Dette gir at

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (ab) = (a^{-1}a) \cdot b = 1 \cdot b = b.$$

Dette viser at R er et integritetsområde.

Oppgave 8. Vis at $\mathbb{Z}_n$ er et integritetsområde hvis og bare hvis $\mathbb{Z}_n$ er en kropp.

Fasit. Vi har at nulldivisorene i $\mathbb{Z}_n$ er gitt ved

$$\{\overline{r} \in \mathbb{Z}_n \mid \gcd(r, n) > 1\}.$$

Anta at $\mathbb{Z}_n$ er et integritetsområde. Det betyr at det ikke finnes noen nulldivisorer. Av beskrivelse over vil det si at for alle r med $0 < r < n$ så er $\gcd(r, n) = 1$. Dette viser at n er et primtall, og da er $\mathbb{Z}_n$ en kropp.

Vi viste i Oppgave 7 at enhver kropp er et integritetsområde.

Oppgave 9. La $R = R_1 \times R_2$ være det direkte produktet av to ringer R_1 og R_2. Vis at

$$U(R) = U(R_1) \times U(R_2).$$

Fasit. Et element $r = (r_1, r_2)$ i R er en enhet i R hvis og bare hvis det eksisterer $r' = (r_1', r_2') \in R$ slik at

$$rr' = (r_1 r_1', r_2 r_2') = 1_R = (1_{R_1}, 1_{R_2}) = r'r = (r_1' r_1, r_2' r_2).$$

Dette er ekvivalent med at

$$r_1 r_1' = 1_{R_1} = r_1' r_1$$

og

$$r_2 r_2' = 1_{R_2} = r_2' r_2$$

for to element $r_1' \in R_1$ og $r_2' \in R_2$. Dette viser at

$$U(R) = U(R_1) \times U(R_2).$$

Oppgave 10. Definer

$$\psi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

ved at $\psi(\overline{a}_{mn}) = (\overline{a}_m, \overline{a}_n)$, der $\overline{a}_t$ betyr heltallet a modulo heltallet t.

(a) Vis at $\psi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ er en isomorfi av ringer når $\gcd(m, n) = 1$.

(b) Bruk Oppgave 9 til å vise at

$$\varphi(mn) = \varphi(m)\varphi(n)$$

når $\gcd(m, n) = 1$ og φ er Eulers phi-funksjon.

Fasit. ψ veldefinert: Anta at $\overline{r}_{mn} = \overline{s}_{mn}$ i $\mathbb{Z}_{mn}$, der $\overline{x}_N$ betyr x modulo et heltall N. Dette betyr at $r - s = mnt$ for et heltall t. Dette gir at både $\overline{r}_m = \overline{s}_m$ og $\overline{r}_n = \overline{s}_n$, som viser at avbildningen ψ er veldefinert.

Vi har at $\overline{x}_N \overline{y}_N = \overline{xy}_N$ for alle heltall x, y, N. Dette gir at

$$\begin{aligned}
\psi(\overline{r}_{mn}\overline{s}_{mn})) &= \psi(\overline{rs}_{mn}) \\
&= (\overline{rs}_m, \overline{rs}_n) \\
&= (\overline{r}_m\overline{s}_m, \overline{r}_n\overline{s}_n) \\
&= (\overline{r}_m, \overline{r}_n)(\overline{s}_m, \overline{s}_n) \\
&= \psi(\overline{r}_{mn})\psi(\overline{s}_{mn})
\end{aligned}$$

Vi har at $\overline{x}_N + \overline{y}_N = \overline{x+y}_N$ for all heltall x, y, N. Dette gir at

$$\begin{aligned}
\psi(\overline{r}_{mn} + \overline{s}_{mn})) &= \psi(\overline{r+s}_{mn}) \\
&= (\overline{r+s}_m, \overline{r+s}_n) \\
&= (\overline{r}_m + \overline{s}_m, \overline{r}_n + \overline{s}_n) \\
&= (\overline{r}_m, \overline{r}_n) + (\overline{s}_m, \overline{s}_n) \\
&= \psi(\overline{r}_{mn}) + \psi(\overline{s}_{mn})
\end{aligned}$$

Videre er $\psi(\overline{1}_{mn}) = (\overline{1}_m, \overline{1}_n) = 1_{\mathbb{Z}_m \times \mathbb{Z}_n}$. Alt dette tilsammen viser at ψ er en homomorfi av ringer.

Anta at $\gcd(m, n) = 1$. Anta at $\psi(\overline{r}_{mn}) = (\overline{r}_m, \overline{r}_n) = (\overline{0}_m, \overline{0}_n)$. Dette gir at r er et multiplum av både m og n, dvs.

$$r \in \langle m \rangle \cap \langle n \rangle = \langle \operatorname{lcm}(m, n) \rangle.$$

Vi har at $\operatorname{lcm}(m, n) \gcd(m, n) = mn$. Siden $\gcd(m, n) = 1$, så er $\operatorname{lcm}(m, n) = mn$ og r er et multiplum av mn. Dette medfører at $\overline{r}_{mn} = \overline{0}_{mn}$ og $\operatorname{Ker} \psi = \{\overline{0}_{mn}\}$. Dette viser at ψ er en-til-en. Antall elementer i $\mathbb{Z}_{mn}$ og $\mathbb{Z}_m \times \mathbb{Z}_n$ er begge mn, slik at siden ψ er en-til-en, så må ψ også være på. Vi har nå vist at ψ er en isomorfi av ringer.

(b) Anta at $\psi \colon R \to S$ er en isomorfi av ringer. Vi påstår at r er en enhet i R hvis og bare hvis $\psi(r)$ er en enhet i S. Anta at r er en enhet i R. Da eksisterer det $r' \in R$ slik at $rr' = 1_R = r'r$. Anvend ψ på denne likheten og vi får:

$$\psi(rr') = \psi(r)\psi(r') = \psi(1_R) = 1_S = \psi(r'r) = \psi(r')\psi(r).$$

Dette viser at $\psi(r)$ er en enhet i S.

Anta at s er en enhet i S, dvs. det finnes en $s' \in S$ slik at $ss' = 1_S = s's$. Siden ψ er på, så finnes det en $r, s \in R$ slik at $\psi(r) = s$ og $\psi(r') = s'$. Da er

$$1_S = ss' = \psi(r)\psi(r') = \psi(rr')$$

og

$$1_S = s's = \psi(r')\psi(r) = \psi(r'r).$$

Siden ψ er en-til-en og $\psi(1_R) = 1_S$, så må $rr' = 1_R = r'r$. Dette viser at ψ gir isomorfi mellom de to multiplikative gruppene $U(R)$ og $U(S)$.

Observasjonen over anvendt på isomorfien $\psi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ gir en isomorfi mellom $U(\mathbb{Z}_{mn}$ og $U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Antall elementer i $U(\mathbb{Z}_t)$ for et positivt heltall t er $\phi(t)$. Ved å sammenligne antall elementer i $U(\mathbb{Z}_{mn}$ og $U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ får vi at

$$\phi(mn) = \phi(m)\phi(n)$$

når $\gcd(m, n) = 1$.

Utfordring. Vi har allerede fylt ut et liknende diagram. Nå er det en klasse ringer til. Fyll inn eksempler som tar hensyn til den nye klassen av ringer.