Gruppearbeid

Generelt ved gruppearbeid:

(1) Presentasjon av deltakerne, navn, studieprogram, kull.
(2) Velg en deltaker til å dele "whiteboard".
(3) Husk å spørre om alle er enige/er med, og husk å si i fra om du ikke skjønner noe eller har en annen måte å tenke på. I forelesningene skal vi lære og ikke prestere.

1. Gruppearbeid A i 18F

Oppgave 1. La

$$R = M_2(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{R}\}.$$

Finn enhetene i R.

Fasit. En enhet i R er det samme som en inverterbar matrise. Fra lineær algebra har vi at $r = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ i R er en enhet hvis og bare hvis $\det(r) = ad - bc \neq 0$.

Oppgave 2. La R være en ring med 1. La

$$U(R) = \{u \in R \mid \ u \text{ en enhet i } R\}.$$

Vis at $U(R) = (U(R), \cdot)$ er en gruppe under multiplikasjonen i R.

Fasit. Vi har at $1 \in U(R)$, slik at $U(R) \neq \emptyset$. Derfor har vi at identitetselementet med hensyn til multiplikasjonen, som er 1, er i $U(R)$. Hvis u_1, u_2 er i $U(R)$, så er $(u_1u_2)^{-1} = u_2^{-1}u_1^{-1}$ og spesielt at u_1u_2 er en enhet i R. Dette gir at $U(R)$ er lukket under multiplikasjon. Siden multiplikasjonen i R er assosiativ (R er en ring), så er den binære operasjonen i $U(R)$ assosiativ. Hvis $u \in U(R)$, så vil u^{-1} eksistere og i tillegg per definisjon være en enhet, slik at $u^{-1} \in U(R)$. Dette medfører at $U(R)$ er en gruppe under multiplikasjon.

Oppgave 3. For en ring R med 1 betrakt de følgende egenskapene for R:

(i) For alle $a, b \in R$ med $ab = 0 \Rightarrow a = 0$ eller $b = 0$.
(ii) For alle $a, b \in R$ med $ab = ac$ og $a \neq 0 \Rightarrow b = c$.
(iii) For alle $a, b \in R$ med $ab = cb$ og $b \neq 0 \Rightarrow a = c$.

Vis at alle egenskapene (i)–(iii) er ekvivalente for en ring R.

Fasit. Anta at (i) holder i R. Vi ønsker å vise at (ii) holder i R. Anta at $a, b \in R$ med $ab = ac$ og $a \neq 0$. Vi har at

$$ab = ac \Leftrightarrow a(b - c) = 0.$$

Siden (i) holder, har vi at $a = 0$ eller $b - c = 0$. Siden $a \neq 0$, så må vi ha at $b - c = 0$ eller ekvivalent at $b = c$. Dette viser at (ii) holder i R.

Anta at (ii) holder i R. Vi ønsker å vise at (i) holder i R. Anta at $a, b \in R$ med $ab = 0$. Da er $ab = a \cdot 0$. Hvis $a = 0$, så er det ingenting å vise. Hvis $a \neq 0$, da har vi fra (ii) at $b = 0$. Tilsammen viser dette at (i) holder i R.

Tilsvarende som over kan vi vise at (i) og (iii) er ekvivalente.

Oppgave 4.

(a) Finn nulldivisorene in $\mathbb{Z}_{10}$.
(b) Finn enhetene i $\mathbb{Z}_{10}$.

Fasit. Vi har at

$$\overline{3} \cdot \overline{7} = \overline{1}$$
$$\overline{9} \cdot \overline{9} = \overline{1}$$

og

$$\overline{2} \cdot \overline{5} = \overline{0}$$
$$\overline{4} \cdot \overline{5} = \overline{0}$$
$$\overline{6} \cdot \overline{5} = \overline{0}$$
$$\overline{8} \cdot \overline{5} = \overline{0}$$

Dette gir at $\{\overline{3}, \overline{7}, \overline{9}\}$ er enhetene i $\mathbb{Z}_{10}$. Videre viser det at $\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\}$ er nulldivisorer.

Oppgave 5. Vis at $\overline{r}$ er en enhet i $\mathbb{Z}_n$ hvis og bare hvis $\gcd(r, n) = 1$.

Hint: Kan bruke de samme argumentene som i beviset for Setning 60.

Fasit. Anta at $\overline{r}$ er en enhet i $\mathbb{Z}_n$. Da eksisterer $\overline{s}$ i $\mathbb{Z}_n$ der $0 < s < n$ slik at $\overline{s} \cdot \overline{r} = \overline{1}$ i $\mathbb{Z}_n$. Vi har at

$$\overline{1} = \overline{s} \cdot \overline{r} = \overline{sr} = \overline{\underbrace{r + r + \cdots + r}_{s}} = \underbrace{\overline{r} + \overline{r} + \cdots + \overline{r}}_{s} = s \cdot \overline{r}$$

Dette gir at $\overline{1} \in \langle \overline{r} \rangle \subseteq (\mathbb{Z}_n, +)$, som gir at $\langle \overline{r} \rangle = \mathbb{Z}_n = \langle \overline{1} \rangle$. Setning 15 (b) gir da at $\gcd(r, n) = 1$.

Anta at $\gcd(r, n) = 1$. Da vet vi det eksisterer $s, t \in \mathbb{Z}$ slik at $rs + nt = 1$. Beregner dette modulo n, så får vi at $\overline{r} \cdot \overline{s} = \overline{1}$ i $\mathbb{Z}_n$. Dette betyr at $\overline{r}$ har en invers i $\mathbb{Z}_n$ og $\overline{r}$ er en enhet i $\mathbb{Z}_n$.