1. Gruppearbeid A i 23F

Oppgave 1.
(a) Vis at $(p(x)) \subseteq \mathbb{Z}_2[x]$ er et maksimalt ideal, der $p(x) = x^3 + x^2 + \overline{1}$.
(b) Vis at $(p(x)) \subseteq \mathbb{Z}_2[x]$ er et maksimalt ideal, der $p(x) = x^5 + x^2 + \overline{1}$.

Fasit. Vi bruker at et ideal $(p(x))$ i $\mathbb{Z}_2[x]$ genererert av et polynom $p(x)$ er maksimalt hvis og bare $p(x)$ er irredusibelt over $\mathbb{Z}_2$.

(a) Siden $p(\overline{0}) = \overline{1}$ og $p(\overline{1}) = \overline{1} + \overline{1} + \overline{1} = \overline{1}$, hvor begge er forskjellige fra null og $\deg p(x) \leq 3$, så har vi at $p(x)$ er irredusibelt over $\mathbb{Z}_2$. Dette viser at $(p(x))$ er et maksimalt ideal in $\mathbb{Z}_2[x]$.

(b) Siden $p(\overline{0}) = \overline{1}$ og $p(\overline{1}) = \overline{1} + \overline{1} + \overline{1} = \overline{1}$, hvor begge er forskjellige fra null, så har $p(x)$ ingen lineære faktorer. Av dette følger det at hvis $p(x)$ er redusibelt, så må $p(x)$ være et produkt av to irredusible polynomer av grad 2 og 3. I oppgavene for 21B fant vi alle irredusible polynomer av grad 2 og 3 over $\mathbb{Z}_2$:

$$p_1(x) = x^2 + x + \overline{1},$$
$$q_1(x) = x^3 + x^2 + \overline{1},$$
$$q_2(x) = x^3 + x + \overline{1}.$$

Vi har at

$$p_1(x)q_1(x) = x^5 + x + \overline{1},$$
$$p_1(x)q_2(x) = x^5 + x^4 + \overline{1},$$

Ingen av disse er lik $p(x)$, slik at dette viser at $p(x)$ er et irredusibelt polynom over $\mathbb{Z}_2$ og at $(p(x))$ er et maksimalt ideal i $\mathbb{Z}_2[x]$.

Vektorrom over en kropp

Definisjon. La F være en kropp. Et *vektorrom* V over F er en abelsk gruppe $(V, +)$ med en virkning av F på V, dvs. det fins en funksjon

$$F \times V \xrightarrow{\varphi} V,$$

der vi skriver $\varphi(a, v) = av$ (skalarmultiplikasjon) slik at følgende aksiomer er oppfylt

(1) $(a + b)v = av + bv$,
(2) $a(v + w) = av + bw$,
(3) $a(bv) = (ab)v$,
(4) $1_F \cdot v = v$,

for alle $a, b \in F$ og $v, w \in V$.

Merk: 1) De samme aksiomene som for vektorrom over $\mathbb{R}$ eller $\mathbb{C}$.

2) Mange resultater i linear algebra bruker elementære radoperasjoner og at de har inverse operasjoner. Har vi det tilsvarende for vektorrom over en kropp?

Elementær radoperasjon	Invers av radoperasjonen over F
Multiplisere en rad med $c \in F \setminus \{0\}$	Multiplisere samme rad med c^{-1}.
To rader bytter plass $i \leftrightarrow j$	Radene bytter plass igjen, $i \leftrightarrow j$.
Legger et ikke-null multiplum c av rad i til rad j, der $i \neq j$	Legger $-c \cdot$ rad i til rad j.

Sjekk bevisene for vektorrom over $\mathbb{R}$ og $\mathbb{C}$ for å se at de ikke bruker annet enn at $\mathbb{R}$ og $\mathbb{C}$ er kropper. Dette gjør at vi har de samme resultatene og definisjonene, spesielt de følgende, der F er en kropp og V er vektorrom over F:

Definisjon. (a) En mengde $\{v_i\}_{i \in I} \subseteq V$

(i) *utspenner* V hvis for alle $v \in V$ eksisterer $a_i \in F$ slik at

$$v = \sum_{i \in I} a_i v_i,$$

der kun endelig mange av a_i'ene er $\neq 0$.

(ii) er *lineært uavhengig* hvis

$$\sum_{i \in I} a_i v_i = 0,$$

der kun endelig mange av a_i'ene er $\neq 0$, impliserer at $a_i = 0$ for alle $i \in I$.

(iii) er *en basis for* V hvis den utspenner V og er lineært uavhengig.

(b) V er et *endelig dimensjonalt vektorrom* hvis en endelig delmengde av V utspenner V.

Oppgave 2'. La V være et endelig dimensjonalt vektorrom over en kropp F. Vis en av følgende påstander:

(a) Vis at enhver lineær uavhengig mengde kan utvides til en basis for V.

(b) Enhver mengde som utspenner V inneholder en basis for V.

(c) V har en basis, og alle basiser for V består av det samme antall elementer, betegnes $\dim_F V$, og kalles *dimensjonen til* V *over* F.

(d) La $\{v_i\}_{i=1}^n$ være en delmengde av V som utspenner V. Vis at $\{v_i\}_{i=1}^n$ er en basis for V hvis og bare hvis for alle $v \in V$ så kan v skrives entydig på formen

$$v = \sum_{i=1}^{n} a_i v_i$$

med $a_i \in F$.

Fasit. (a) Siden V er et endelig dimensjonalt vektorrom, så vil en endelig delmengde $\mathcal{G} = \{w_i\}_{i=1}^s$ av V utspenne V.

La $\mathcal{S}_t = \{v_i\}_{i=1}^t$ være en lineært uavhengig delmengde av V. La V_t være underrommet av V utspent av $\mathcal{S}_t$.

Hvis $V_t = V$, så er det ingenting å vise. Anta at $V_t \subsetneq V$. Velg $v_{t+1} \in V \setminus V_t$ slik at $v_{t+1} \in \mathcal{G}$. Dette er mulig da $\mathcal{G}$ utspenner V. La V_{t+1} være underrommet av V utspent av $\mathcal{S}_{t+1} = \{v_i\}_{i=1}^{t+1}$. Vi påstår av S_{t+1} er en lineært uavhengig mengde. Anta at

$$\sum_{i=1}^{t+1} a_i v_i = 0.$$

Hvis $a_{t+1} = 0$, så må $a_i = 0$ for alle $i \in \{1, 2, \ldots, t\}$, siden $\mathcal{S}_t$ er lineært uavhengig. Hvis $a_{t+1} \neq 0$, så har vi at

$$v_{t+1} = -\frac{1}{a_{t+1}} \sum_{i=1}^{t} a_i v_i \in V_t.$$

Dette er en selvmotsigelse per valg av elementet v_{t+1}. Dette viser at $\mathcal{S}_{t+1}$ er lineært uavhengig.

Hvis $V_{t+1} \subsetneq V$, kan vi gjøre sammen konstruksjonen som over. Dette gir at vi kan konstruere en oppadstigende kjede

$$V_t \subseteq V_{t+1} \subseteq V_{t+2} \subseteq \cdots \subseteq V_{t+m} \subseteq V.$$

Siden $\mathcal{G}$ er en endelig mengde, så er denne kjeden endelig og vi har $V_{t+m} = V$ for en $m \geq 1$. Delmengden $\mathcal{S}_{t+m}$ er lineært uavhengig og den utspenner V, slik at $\mathcal{S}_{t+m}$ er en basis for V som inneholder $\mathcal{S}_t$.

(b) Siden V er et endelig dimensjonalt vektorrom, så vil en endelig delmengde $\mathcal{G} = \{w_i\}_{i=1}^s$ av V utspenne V. Hvis $V = (0)$, så er per definisjon $\emptyset$ en basis for V og dette er en delmengde av $\mathcal{G}$. Anta at $V \neq (0)$. Etter eventuell renummerering av elementene i $\mathcal{G}$ anta at $w_1 \neq 0$. Da er $\mathcal{S}_1 = \{w_1\}$ en lineært uavhengig mengde. Dette viser at det finnes lineært uavhengige delmengder av $\mathcal{G}$. Velg den største delmengden $\mathcal{S}_t$ av $\mathcal{G}$ som er lineært uavhengig, og anta at $\mathcal{S}_t = \{w_i\}_{i=1}^t$. La V_t være underrommet av V utspent av $\mathcal{S}_t$. Vi ønsker å vise at $V_t = V$.

Per valg av $\mathcal{S}_t$, vil for ethvert valg av element w fra $\mathcal{G}$ som ikke er i $\mathcal{S}_t$, så vil $\mathcal{S}_t \cup \{w\}$ være en lineært avhengig mengde. Dette vil si at det finnes $a_i \in F$ for $i = 1, 2, \ldots, t+1$ slik at

$$\sum_{i=1}^{t} a_i w_i + a_{t+1} w = 0,$$

hvor ikke alle elementene a_i er lik null. Siden $\mathcal{S}_t$ er en lineært uavhengig mengde, så må $a_{t+1} \neq 0$, ellers må alle a_i være lik null. Tilsvarende som over får vi at

$$w = -\frac{1}{a_{t+1}} \sum_{i=1}^{t} a_i w_i,$$

og at $w \in V_t$. Dette viser at alle elementer w i $\mathcal{G}$ som ikke er med i $\mathcal{S}_t$, så vil $w \in V_t$. Det følger fra dette at vektorrommet utspent av $\mathcal{G}$, dvs. V, er inneholdt i V_t, og vi har $V_t = V$. Dette viser at en delmengde som utspenner V inneholder en basis for V.

(c) At V har en basis følger fra (b). Anta at $\mathcal{B}_1 = \{v_i\}_{i=1}^n$ og $\mathcal{B}_2 = \{w_i\}_{i=1}^m$ er to forskjellige basiser for V. Elementet v_1 kan uttrykkes som

$$v_1 = \sum_{i=1}^{m} a_i w_i,$$

siden $\mathcal{B}_2$ er en basis. Ikke alle a_i'ene kan være lik null. Anta uten tap av generalitet at $a_1 \neq 0$. Dvs. w_1 kan uttrykkes av mengden $\mathcal{G}_1 = \{v_1, w_2, w_3, \ldots, w_m\}$, og det følger at $\mathcal{G}_1$ utspenner V. Vi kan gjenta den samme prosedyren med v_2, og få at $\mathcal{G}_2 = \{v_1, v_2, w_3, \ldots, w_m\}$ også utspenner V (etter passende renummerering av elementene). Ved å fortsette denne prosessen, så får vi til slutt at $\mathcal{G}_m = \{v_1, v_2, \ldots, v_m\}$ utspenner V. Hvis $m < n$, så følger det at $\mathcal{B}_1$ er en lineært avhengig mengde. Dette er en selvmotsigelse, slik at $m \geq n$. Hvis vi bytter rollene til $\mathcal{B}_1$ og $\mathcal{B}_2$, så viser vi at $n \geq m$. Dette gir at $n = m$, som er det vi skal vise.

(d) Anta at $\mathcal{B} = \{v_i\}_{i=1}^n$ er en basis for V. Anta at et element $v \in V$ kan skrives som

$$v = \sum_{i=1}^{n} a_i v_i$$

og

$$v = \sum_{i=1}^{n} b_i v_i$$

for $a_i, b_i \in F$. Da vil

$$0 = v - v = \sum_{i=1}^{n} (a_i - b_i) v_i.$$

Siden $\mathcal{B}$ er en basis for V, så må $a_i - b_i = 0$, eller ekvivalent av $a_i = b_i$ for alle i. Dette viser av fremstillingen av v er entydig.

Anta at alle $v \in V$ så kan v skrives entydig på formen

$$v = \sum_{i=1}^{n} a_i v_i$$

med $a_i \in F$. Anta at

$$0 = \sum_{i=1}^{n} a_i v_i$$

med $a_i \in F$. Vi har også at

$$0 = \sum_{i=1}^{n} 0 v_i.$$

Siden fremstillingen er entydig, så må $a_i = 0$ for alle i. Det følger at $\mathcal{B}$ er en lineært uavhengig delmengde av V som utspenner V, og $\mathcal{B}$ er en basis for V.