1. Gruppearbeid B i 20F

Oppgave 4. La R være en ring med 1.

(i) Definer et *polynom* $f(x)$ med koeffisienter i R til å være en uendelig formell sum

$$\sum_{i\geq 0} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots ,$$

der $a_i \in R$ og $a_i \neq 0$ for bare et endelig antall i'er. Elementene $\{a_i\}_{i\geq 0}$ er *koeffisientene til polynomet* $f(x)$. Skriver

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

hvis $a_i = 0$ for alle $i > n$.

(ii) *Graden til* $f(x)$ er gitt ved

$$\deg f(x) = \begin{cases} n, & \text{hvis } a_n \neq 0 \text{ og } a_i = 0 \text{ for } i > n. \\ -\infty, & \text{hvis } a_i = 0 \text{ for alle } i \geq 0. \end{cases}$$

(iii) La $f(x) = \sum_{i\geq 0} a_i x^i$ og $g(x) = \sum_{i\geq 0} b_i x^i$ være polynomer med koeffisienter i R. Da er $f(x) = g(x)$ hvis $a_i = b_i$ for alle $i \geq 0$.

La $R[x]$ betegne mengden av alle polynomer med koeffisienter i R. Definer to binære operasjoner på $R[x]$, $+$ og $\cdot$: La

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

og

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n,$$

der $n = \max\{\deg f(x), \deg g(x)\}$. Definer

(i) $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_n+b_n)x^n$.

(ii) $f(x)g(x) = d_0+d_1x+d_2x^2+\cdots+d_nx^n$, der $d_t = \sum_{i=0}^{t} a_i b_{t-i} \in R$.

Vis at $R[x]$ er en ring med 1. Spesielt, finn 1 og 0 i $R[x]$.

Fasit. Gir her bare en skisse av beviset.

Addisjon og multiplikasjon av polynomer i $R[x]$ gir nye polynomer i $R[x]$, slik at de er to binære operasjoner på $R[x]$.

$(R[x], +)$ **er en abelsk gruppe:** (i) Assosiativ lov: Bruker assosiativ lov i $(R, +)$.

(ii) Nullelement: $0_{R[x]} = 0 + 0x + 0x^2 + 0x^3 \cdots$.

(iii) Invers: $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, da er $-f(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$.

(iv) Abelsk: Bruker at $(R, +)$ er abelsk.

Multiplikasjon i $R[x]$ assosiativ: Bruker assosiativitet for multiplikasjonen i R.

Distributive lover: Bruker distributive lover i R.

Identitetselement: $1_{R[x]} = 1 + 0x + 0x^2 + 0x^3 + \cdots$.

Oppgave 5. La $R = \mathbb{R}[x]$ være ringen av alle polynomer med koeffisienter i $\mathbb{R}$. La $f(x) = 2x^2 + 3x + 1$ og $g(x) = 3x^3 + 2$.
(a) Beregn $f(x)g(x)$.
(b) Hva kan vi si om graden til $f(x)g(x)$ for $f(x), g(x) \in R$?

Fasit. (a) Vi har

$$\begin{aligned} f(x)g(x) &= (2x^2 + 3x + 1)(3x^3 + 2), \\ &= 6x^5 + 4x^2 + 9x^4 + 6x + 4x^2 + 2, \\ &= 6x^5 + 9x^4 + 8x^2 + 6x + 2. \end{aligned}$$

(b) La

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

og

$$g(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1} + b_mx^m,$$

der $a_n \neq 0$ og $b_m \neq 0$. Da er

$$f(x)g(x) = \text{polynom av grad høyst } m + n - 1 + a_nb_mx^{m+n}.$$

Siden $a_nb_m \neq 0$, har vi at $\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x)$.

Oppgave 6. La $R = \mathbb{Z}_6[x]$. være ringen av alle polynomer med koeffisienter i $\mathbb{Z}_6$. La $f(x) = \overline{2}x^2 + \overline{3}x + \overline{1}$ og $g(x) = \overline{3}x^3 + \overline{2}$.
(a) Beregn $f(x)g(x)$.
(b) Hva kan vi si om graden til $f(x)g(x)$ for $f(x), g(x) \in R$?
(c) Hvorfor får vi ulik konklusjon i Oppgave 5 og Oppgave 6?

Fasit. (a) Vi har

$$\begin{aligned} f(x)g(x) &= (\overline{2}x^2 + \overline{3}x + \overline{1})(\overline{3}x^3 + \overline{2}), \\ &= \overline{6}x^5 + \overline{4}x^2 + \overline{9}x^4 + \overline{6}x + \overline{4}x^2 + \overline{2}, \\ &= \overline{3}x^4 + \overline{2}x^2 + \overline{2}. \end{aligned}$$

(b) Tilsvarende som i forrige oppgave så kan vi si

$$f(x)g(x) = \text{polynom av grad høyst } m + n - 1 + \overline{a_n}\overline{b_m}x^{m+n},$$

hvor $f(x)$ og $g(x)$ er gitt tilsvarende som i forrige oppgave. Siden $\overline{a_n}\overline{b_m}$ kan være lik $\overline{0}$, så kan vi generelt si at

$$\deg f(x)g(x) \leq \deg f(x) + \deg g(x).$$

(c) Fordi R er eller ikke er et integritetsområde.

Oppgave 7. Bevis eller gi et moteksempel til følgende utsagn:

(i) $R[x]$ er kommutativ hvis og bare hvis R er kommutativ?
(ii) $R[x]$ er et integritetsområde hvis og bare hvis R er et integritetsområde?
(iii) $R[x]$ er en kropp hvis og bare hvis R er en kropp?

Fasit. (i) La

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

og

$$g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n.$$

Da er

$$f(x)g(x) = d_0 + d_1x + \cdots + d_{2n-1}x^{2n-1} + sd_{2n}x^{2n},$$

der $d_t = \sum_{i=0}^{t} a_ib_{t-i}$.

Anta at R er en kommutativ ring med 1. Da har vi at

$$\begin{aligned} d_t &= \sum_{i=0}^{t} a_ib_{t-i}, \\ &= \sum_{i=0}^{t} b_{t-i}a_i, \ R \text{ is kommutativ}, \\ &= \sum_{j=0}^{t} b_ja_{t-j}, \ \text{la } j = t-i, \qquad\qquad = e_t, \end{aligned}$$

hvor e_t er koeffisientene av polynomet $g(x)f(x)$. Dette viser at $R[x]$ er kommutativ.

Anta at $R[x]$ er kommutativ. Betrakt polynomene $f(x) = a$ og $g(x) = b$ for $a, b \in R$. Siden $R[x]$ er kommutativ, så er

$$ab = f(x)g(x) = g(x)f(x) = ba.$$

Dette viser at R er kommutativ.

(ii) Anta at R er et integritetsområde. La

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

og

$$g(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1} + b_mx^m,$$

der $a_n \neq 0$ og $b_m \neq 0$,k dvs. $f(x) \neq 0$ og $g(x) \neq 0$ i $R[x]$. Ønsker å vise at $f(x)g(x) \neq 0$. I såfall er $R[x]$ et integritetsområde.

Vi har at

$$f(x)g(x) = \text{polynom av grad høyst } mn - 1 + a_nb_mx^{m+n}.$$

Siden R er et integritetsområde, så er $a_n b_m \neq 0$ og følgelig er $f(x)g(x) \neq 0$ og $R[x]$ er et integritetsområde.

Anta at $R[x]$ er et integritetsområde. Betrakt polynomene $f(x) = a$ og $g(x) = b$ for $a, b \in R \setminus \{0\}$. Siden $R[x]$ er et integritetsområde, så er

$$0 \neq f(x)g(x) = ab.$$

Dette viser at R er et integritetsområde.

(iii) La R være en kropp. La $f(x) = 1 + x$ i $R[x]$. For alle polynom $g(x) = a_0 + a_1 x + \cdot + a_n x^n$ i $R[x]$ with $a_n \neq 0$, så er

$$\begin{aligned} f(x)g(x) &= \text{polynom av grad høyst } n + a_n x^{n+1}, \\ &\neq 1, \text{for alle polynom } g(x) \text{ i } R[x]. \end{aligned}$$

Dette viser at $f(x)$ ikke har en invers i $R[x]$, slik at $R[x]$ er ikke en kropp.

Oppgave 8. La p være et primtall. Betrakt polynomet $f(x) = x^p - x$ i $\mathbb{Z}_p[x]$.

(a) Vis at $f(\overline{a}) = \overline{0}$ for alle $\overline{a}$ i $\mathbb{Z}_p$.
(b) La $p = 3$. Vis at $x(x-\overline{1})(x-\overline{2}) = x^3 - x$ og at $(x-\overline{1})(x-\overline{2}) = x^2 - \overline{1}$.
(c) Anta at vi har vist at $\prod_{i=0}^{p-1}(x - \overline{i}) = x^p - x$. Vis at

$$\prod_{i=0}^{p-1}(x + \overline{p-i}) = x^p - x.$$

(d) Under samme antakelse som i (c), vis at

$$\prod_{i=1}^{p-1}(x + \overline{p-i}) = x^{p-1} - \overline{1}.$$

(e) **Utfordring:** Vis en implikasjon av Wilsons teorem, nemlig at

$$(p-1)(p-2)\cdots 2 \cdot 1 = (p-1)! \equiv -1 \mod p.$$

Fasit. (a) Et korollar av Fermats lille teorem sier at $a^p \equiv a \mod p$ for alle heltall a. Evaluerer vi $f(x)$ i $\overline{a}$ betraktet som et element i $\mathbb{Z}_p$, får vi at

$$\overline{a}^p - \overline{a} = \overline{0}$$

av korollaret av Fermats lille teorem. Dette betyr at $f(x) = 0$ for alle $\overline{a}$ i $\mathbb{Z}_p$.

(b) Vi har at

$$\begin{aligned} x(x-\overline{1})(x-\overline{2}) &= (x^2-x)(x-\overline{2}), \\ &= x^3 - x^2 - \overline{2}x^2 + \overline{2}x, \\ &= x^3 - x^2 + x^2 - x, \\ &= x^3 - x. \end{aligned}$$

og

$$\begin{aligned} (x-\overline{1})(x-\overline{2}) &= x^2 - \overline{2}x - x + \overline{2}, \\ &= x^2 + x - x - \overline{1}, \\ &= x^2 - \overline{1}. \end{aligned}$$

(c) Siden $-\bar{i} = \overline{p-i}$, så følger påstanden direkte.

(d) Anta at $\prod_{i=0}^{p-1}(x-\bar{i}) = x^p - x$. La

$$\prod_{i=1}^{p-1}(x-\bar{i}) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{p-1}}x^{p-1},$$

siden vi vet at $\prod_{i=1}^{p-1}(x-\bar{i})$ har høyst grad $p-1$. Da er

$$\begin{aligned} x\prod_{i=1}^{p-1}(x-\bar{i}) &= x(\overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{p-2}}x^{p-2} + \overline{a_{p-1}}x^{p-1}), \\ &= \overline{a_0}x + \overline{a_1}x^2 + \cdots + \overline{a_{p-2}}x^{p-1} + \overline{a_{p-1}}x^p, \\ &= -x + x^p. \end{aligned}$$

Dette gir at

$$\begin{aligned} \overline{a_0} &= -\overline{1}, \\ \overline{a_i} &= \overline{0}, \text{ for } i \in \{1, 2, \ldots, p-2\}, \\ \overline{a_{p-1}} &= \overline{1}. \end{aligned}$$

Vi får fra dette at

$$\prod_{i=1}^{p-1}(x-\bar{i}) = x^{p-1} - \overline{1}.$$

(e) Polynomet $f(x) = \prod_{i=1}^{p-1}(x-\bar{i}) = x^{p-1} - \overline{1}$ evaluert i $x = \overline{0}$, gir ved å observere som over at $-\bar{i} = \overline{p-i}$, at

$$\prod_{i=1}^{p-1}(\overline{0}-\bar{i}) = \prod_{i=1}^{p-1}(\overline{p-i}) = \overline{(p-1)(p-2)\cdots 2\cdot 1} = \overline{0}^{p-1} - \overline{1} = -\overline{1}.$$

Betraktet modulo p, så får vi

$$(p-1)(p-2)\cdots 2\cdot 1 = (p-1)! \equiv -1 \mod p.$$

Dette er en implikasjon i Wilsons teorem.