1. Gruppearbeid B i 21F

Oppgave 8.

(a) Finn alle irredusible polynomer av grad 2 over $\mathbb{Z}_2$.
(b) Finn alle irredusible polynomer av grad 3 over $\mathbb{Z}_2$.
(c) **Utfordring:** Finn alle irredusible polynomer av grad 4 over $\mathbb{Z}_2$.

Fasit. (a) Et polynom av grad 2 over $\mathbb{Z}_2$ svarer til et trippel av elementer fra $\mathbb{Z}_2$ av formen $(\overline{a}_0, \overline{a}_1, \overline{1})$, der elementene er koeffisientene i polynomet. Dette gir oss fire valg

$(\overline{0}, \overline{0}, \overline{1})$	$f_1(x) = \overline{0} + \overline{0}x + x^2$	$f_1(\overline{0}) = \overline{0}, \quad f_1(\overline{1}) = \overline{1}$
$(\overline{1}, \overline{0}, \overline{1})$	$f_2(x) = \overline{1} + \overline{0}x + x^2$	$f_2(\overline{0}) = \overline{1}, \quad f_2(\overline{1}) = \overline{0}$
$(\overline{0}, \overline{1}, \overline{1})$	$f_3(x) = \overline{0} + \overline{1}x + x^2$	$f_3(\overline{0}) = \overline{0}, \quad f_3(\overline{1}) = \overline{0}$
$(\overline{1}, \overline{1}, \overline{1})$	$f_4(x) = \overline{1} + \overline{1}x + x^2$	$f_4(\overline{0}) = \overline{1}, \quad f_4(\overline{1}) = \overline{1}$

Dette viser at det eneste polynomet som ikke har røtter i $\mathbb{Z}_2$ er $f_4(x) = \overline{1} + x + x^2$, dvs. det eneste irredusible polynomet av grad 2 over $\mathbb{Z}_2$.

(b) Et polynom av grad 3 over $\mathbb{Z}_2$ svarer til et kvadruple av elementer fra $\mathbb{Z}_2$ av formen $(\overline{a}_0, \overline{a}_1, \overline{a}_2, \overline{1})$, der elementene er koeffisientene i polynomet. Dette gir oss åtte valg. Hvis $\overline{a}_0 = \overline{0}$, så er x en faktor i det tilhørende polynomet $f(x)$ og $f(\overline{0}) = \overline{0}$. Slik at for å oppnå et irredusibelt polynom så er det kun fire valg igjen:

$(\overline{1}, \overline{0}, \overline{0}, \overline{1})$	$f_1(x) = \overline{1} + \overline{0}x + \overline{0}x^2 + x^3$	$f_1(\overline{0}) = \overline{1}, \quad f_1(\overline{1}) = \overline{0}$
$(\overline{1}, \overline{1}, \overline{0}, \overline{1})$	$f_2(x) = \overline{1} + \overline{1}x + \overline{0}x^2 + x^3$	$f_2(\overline{0}) = \overline{1}, \quad f_2(\overline{1}) = \overline{1}$
$(\overline{1}, \overline{0}, \overline{1}, \overline{1})$	$f_3(x) = \overline{1} + \overline{0}x + \overline{1}x^2 + x^3$	$f_3(\overline{0}) = \overline{1}, \quad f_3(\overline{1}) = \overline{1}$
$(\overline{1}, \overline{1}, \overline{1}, \overline{1})$	$f_4(x) = \overline{1} + \overline{1}x + \overline{1}x^2 + x^3$	$f_4(\overline{0}) = \overline{1}, \quad f_4(\overline{1}) = \overline{0}$

Dette viser at de eneste polynomene som ikke har røtter i $\mathbb{Z}_2$ er $f_2(x)$ og $f_3(x)$ og dermed de eneste irredusible polynomene av grad 3 over $\mathbb{Z}_2$.

(c) Tilsvarende som over må $\overline{a}_0 = \overline{1}$, slik at vi har 8 valg.

$(\overline{1}, \overline{0}, \overline{0}, \overline{0}, \overline{1})$	$\overline{1}$	$\overline{0}$
$(\overline{1}, \overline{1}, \overline{0}, \overline{0}, \overline{1})$	$\overline{1}$	$\overline{1}$
$(\overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{1})$	$\overline{1}$	$\overline{1}$
$(\overline{1}, \overline{0}, \overline{0}, \overline{1}, \overline{1})$	$\overline{1}$	$\overline{1}$
$(\overline{1}, \overline{1}, \overline{1}, \overline{0}, \overline{1})$	$\overline{1}$	$\overline{0}$
$(\overline{1}, \overline{1}, \overline{0}, \overline{1}, \overline{1})$	$\overline{1}$	$\overline{0}$
$(\overline{1}, \overline{0}, \overline{1}, \overline{1}, \overline{1})$	$\overline{1}$	$\overline{0}$
$(\overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1})$	$\overline{1}$	$\overline{1}$

De to siste kolonne viser verdiene av $f(\overline{0})$ og $f(\overline{1})$. Dette viser at de eneste polynomene uten røtter i $\mathbb{Z}_2$ er

$$f_2(x) = \overline{1} + \overline{1}x + \overline{0}x^2 + \overline{0}x^3 + x^4$$
$$f_3(x) = \overline{1} + \overline{0}x + \overline{1}x^2 + \overline{0}x^3 + x^4$$
$$f_4(x) = \overline{1} + \overline{0}x + \overline{0}x^2 + \overline{1}x^3 + x^4$$
$$f_8(x) = \overline{1} + \overline{1}x + \overline{1}x^2 + \overline{1}x^3 + x^4$$

Dette viser at disse polynomene ikke er et produkt av et polynom av grad 1 og et polynom av grad 3. Men de kan være et produkt av to grad 2 polynomer. Fra (a) har vi at $p(x) = \overline{1} + x + x^2$ er det eneste polynomet av grad 2 over $\mathbb{Z}_2$. Vi har at

$$p(x)^2 = \overline{1} + x^2 + x^4.$$

Dette gir at $f_3(x)$ ikke er irredusibelt. Derfor er de eneste irredusible polynomene av grad 4 over $\mathbb{Z}_2$ gitt ved $f_2(x), f_4(x), f_8(x)$.

Oppgave 9. Vis første del av følgende result:

Setning 79. *La F være en kropp. Ethvert polynom $f(x) \in F[x] \backslash F$ kan faktoriseres i $F[x]$ i et endelig produkt av irredusible polynomer, og de irredusible polynomene er entydig opp til rekkefølge og opp til enheter.*

Fasit. Beviset går ved induksjon på graden til polynomet $f(x)$. Anta at $\deg f(x) = 1$. Da er $f(x) = a_0 + a_1 x$ hvor $a_1 \neq 0$. Hvis $f(x) = g(x)h(x)$, så er $1 = \deg g(x) + \deg h(x)$, slik at enten er $\deg g(x) = 0$ eller $\deg h(x) = 0$ og $g(x)$ eller $h(x)$ er i F. Dette viser at $f(x)$ er irredusibelt selv, og dette viser påstanden for grad 1 polynomer.

Anta at påstanden er vist for alle polynomer av grad n. La $f(x)$ være et polynom av grad $n+1$. Hvis $f(x)$ er et irredusibelt polynom selv, så er det ingenting å vise. Anta at $f(x)$ er redusibelt, dvs. $f(x) = g(x)h(x)$ der $g(x), h(x) \notin F$. Dette gir at $\deg g(x) < \deg f(x)$ og $\deg h(x) < \deg f(x)$, og spesielt at $\deg g(x) \leq n$ og $\deg h(x) \leq n$. Per induksjon er da $g(x)$ og $h(x)$ et endelig produkt av irredusible polynomer, og dermed blir også $f(x)$ et endelig produkt av irredusible polynomer.

Oppgave 10': Utfordring. La

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

være et polynom over en kropp F. Anta at $f(x)$ har n røtter $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ i en kropp E som inneholder F.

(a) Hva er a_0 som funksjon $s_0(\alpha_1, \alpha_2, \ldots, \alpha_n)$ av røttene $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$?
(b) Hva er a_{n-1} som funksjon $s_{n-1}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ av røttene $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$?

(c) Hva er forholdet mellom $s_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$ og $s_i(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)})$ for hver av $i \in \{0, n-1\}$, hvor π er en permutasjon av $\{1, 2, \ldots, n\}$?

(d) Hva med de andre koeffisientene s_i foran x^i for $i = 2, 3, \ldots, n-2$? Har de noen tilsvarende egenskaper som s_0 og s_{n-1}?

Fasit. (a) $a_0 = (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n = s_0(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

(b) $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n) = s_{n-1}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

(c) Vi har at $s_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = s_i(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)})$ for hver av $i \in \{0, n-1\}$ for alle permutasjoner π av $\{1, 2, \ldots, n\}$.

(d) Vi har at

$$s_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^{n-i} \sum_{1 \le r_1 < r_2 < \cdots < r_i \le n} \alpha_{r_1} \alpha_{r_2} \cdots \alpha_{r_i}.$$

Funksjonen s_i har samme egenskap som s_0 og s_{n-1} med hensyn til permutasjoner.