1. Gruppearbeid B i 22F

Oppgave 5. Vis følgende resultat:

Setning 86. *La $f\colon R \to S$ være en ringhomomorfi av (kommutative) ringer med 1. Da har vi følgende:*

(a) $\operatorname{Im} f = \{f(r) \mid r \in R\} \subseteq S$ *er en underring.*

(b) $\overline{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$, *der*

$$\overline{f}(a + \operatorname{Ker} f) = f(a)$$

er en ringisomorfi.

Fasit. (a) Vet at $(\operatorname{Im} f, +) \subseteq (S, +)$ er en undergruppe, siden f er en gruppehomomorfi.

(i) Dette gir at

$$0_S = f(0_R) \text{ og } f(a) - f(b) = f(a - b)$$

er i $\operatorname{Im} f$.

(ii) Per definisjon så er $1_S = f(1_R) \in \operatorname{Im} f$.

(iii) Vi har at

$$f(a)f(b) = f(ab)$$

er i $\operatorname{Im} f$, dvs. $\operatorname{Im} f$ er lukket under multiplikasjon.

Punktene (i)–(iii) gir at $\operatorname{Im} f \subseteq S$ er en underring.

(b) Har at $\operatorname{Ker} f$ er et ideal i R, slik at $R/\operatorname{Ker} f$ er en ring. Vet at $\overline{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$ er en isomorfi av grupper. Vi trenger at

$$\overline{f}((a + \operatorname{Ker} f)(b + \operatorname{Ker} f)) = \overline{f}(a + \operatorname{Ker} f)\overline{f}(b + \operatorname{Ker} f).$$

Vi har at

$$\begin{aligned}\overline{f}((a + \operatorname{Ker} f)(b + \operatorname{Ker} f)) &= \overline{f}(ab + \operatorname{Ker}) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \overline{f}(a + \operatorname{Ker} f)\overline{f}(b + \operatorname{Ker} f)\end{aligned}$$

I tillegg har vi at $\overline{f}(1_{R/\operatorname{Ker} f}) = \overline{f}(1_R + \operatorname{Ker} f) = f(1_R) = 1_S$. Dette viser at $\overline{f}$ er en isomorfi av ringer.

Oppgave 6. La $F = \mathbb{Z}_2[x]/(x^2 + x + \overline{1})$.

(a) Hvor mange elementer har F?

(b) Vis at F er en kropp.

(c) Vis at $\mathbb{Z}_2$ er en underkropp av F.

(d) Har $p(x) = x^2 + x + \overline{1}$ en rot i $\mathbb{Z}_2$? Har $p(x) = x^2 + x + \overline{1}$ en rot i F?

(e) Finn en multiplikativ generator for gruppen $(F \setminus \{0\}, \cdot)$.

Fasit. (a) La $f(x) \in \mathbb{Z}_2[x]$. Da eksisterer det polynomer $q(x), r(x) \in \mathbb{Z}_2[x]$ slik at

$$f(x) = q(x)(x^2 + x + \overline{1}) + r(x),$$

der $r(x) = 0$ eller $0 \leq \deg r(x) < \deg(x^2 + x + \overline{1}) = 2$. Da har vi at

$$f(x) - r(x) = q(x)(x^2 + x + \overline{1}),$$

slik at $f(x) + ((x^2 + x + \overline{1})) = r(x) + ((x^2 + x + \overline{1}))$. Dette gir at ethvert element i F kan representeres av et polynom av fra høyst grad 1, og at vi har opptil fire elementer

$$\begin{array}{l} \overline{0} + ((x^2 + x + \overline{1})), \\ \overline{1} + ((x^2 + x + \overline{1})), \\ x + ((x^2 + x + \overline{1})), \\ \overline{1} + x + ((x^2 + x + \overline{1})) \end{array}$$

i F. Differansen av representantene av to forskjellige elementer i denne mengden er et første grads polynom, slik at de kan ikke være like (Husk: $r(x) + (g(x)) = s(x) + ((g(x)) \Leftrightarrow r(x) - s(x) \in ((g(x)))$. Så alle disse elementene er forskjellige, slik at F har fire elementer.

(b) Betegn elementene

$$\begin{array}{l} \overline{0} + ((x^2 + x + \overline{1})), \\ \overline{1} + ((x^2 + x + \overline{1})), \\ x + ((x^2 + x + \overline{1})), \\ \overline{1} + x + ((x^2 + x + \overline{1})) \end{array}$$

i F med henholdsvis $\{0, 1, \alpha, 1 + \alpha\}$. Da har vi at

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

Dette gir følgende multiplikasjonstabell for $F \setminus \{0\}$:

	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

Vi ser at alle elementer forskjellig fra 0 har en multiplikativ invers, slik at F er en kropp.

(c) Definer $\varphi\colon \mathbb{Z}_2 \to F$ ved at $\varphi(a) = a + ((x^2 + x + \overline{1}))$. Vis at φ er en homomorfi av ringer med 1 som er en-til-en. Dette gjør av vi kan identifisere $\mathbb{Z}_2$ med $\operatorname{Im}\varphi \subseteq F$, dvs. vi kan betrakte $\mathbb{Z}_2$ som en underkropp av F.

(d) Vi har tidligere sett at $x^2 + x + \overline{1}$ ikke har en rot i $\mathbb{Z}_2$.

Definer $\varphi_\alpha\colon \mathbb{Z}_2[x] \to F$ ved at $\varphi_\alpha(f(x)) = f(\alpha)$ (evalueringshomomorfien gitt ved elementet α i F). Da er

$$\begin{aligned}\varphi_\alpha(x^2 + x + \overline{1}) &= \alpha^2 + \alpha + \overline{1} + ((x^2 + x + \overline{1})) \\ &= (x + ((x^2 + x + \overline{1})))^2 + (x + ((x^2 + x + \overline{1}))) \\ &\qquad + \overline{1} + ((x^2 + x + \overline{1})) \\ &= (x^2 + x + \overline{1}) + ((x^2 + x + \overline{1})) \\ &= 0 + ((x^2 + x + \overline{1}))\end{aligned}$$

Dette viser at α er en rot i $x^2 + x + 1$.

(e) Vi ser fra multiplikasjonstabellen for $F \setminus \{0\}$ at $\alpha^2 = \alpha + 1$ og at $\alpha(\alpha + 1) = 1$, dvs. at $\alpha^3 = 1$ og at α er en multiplikativ generator for $F \setminus \{0\}$.

Oppgave 7'. La

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(a) Har $p(x) = x^2 - 2$ en rot i $\mathbb{Q}$? Har $p(x) = x^2 - 2$ en rot i $\mathbb{Q}(\sqrt{2})$?
(b) Vis at $\mathbb{Q}(\sqrt{2})$ er en kropp.
(c) Vis at $\mathbb{Q}$ er en underkropp av $\mathbb{Q}(\sqrt{2})$.
(d) Vis at $\mathbb{Q}(\sqrt{2})$ er isomorf med $\mathbb{Q}[x]/(x^2 - 2)$.

Fasit. (a) La $\frac{t}{n} \in \mathbb{Q}$, der $n, t \in \mathbb{Z}$ og $\gcd(t, n) = 1$. Anta at $(\frac{t}{n})^2 - 2 = 0$. Dette impliserer at $t^2 = 2n^2$, og dermed at $2 \mid t^2$. Siden 2 er et primtall, så må $2 \mid t$ og $t = 2t'$ for en $t' \in \mathbb{Z}$. Dette gir at $t^2 = 2^2(t')^2 = 2n^2$, som betyr at $2(t')^2 = n^2$. Tilsvarende som for t, så får vi at $n = 2n'$. Men da er $\gcd(t, n) \geq 2$, som er en selvmotsigelse. Altså, har ikke $x^2 - 2$ en rot i $\mathbb{Q}$.

Siden $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, så har $x^2 - 2$ en rot i $\mathbb{Q}(\sqrt{2})$.

(b) Vi må vise at $\mathbb{Q}(\sqrt{2})$ er en ring. Anta at dette er gjort. La $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \setminus \{0\}$, dvs. at $a, b \neq 0$. Da er

$$(a+b\sqrt{2})\left(\frac{1}{a^2-2b^2}(a-b\sqrt{2})\right) = \frac{1}{a^2-2b^2}(a^2-2b^2) = 1,$$

siden $\frac{a^2}{b^2} - 2 \neq 0$ for vilkårlige rasjonale tall a og b. Dette viser at alle elementer forskjellige fra 0 i $\mathbb{Q}(\sqrt{2})$ har en invers, og at $\mathbb{Q}(\sqrt{2})$ er en kropp.

(c) Vi har at kroppen $\mathbb{Q}$ er en delmengde av $\mathbb{Q}(\sqrt{2})$, og addisjonen og multiplikasjonen i $\mathbb{Q}$ er restriksjonen av addisjonen og multiplikasjonen i $\mathbb{Q}(\sqrt{2})$. Både $\mathbb{Q}$ og $\mathbb{Q}(\sqrt{2})$ har 1 som multiplikativ identitet. Dette viser at $\mathbb{Q}$ er en underkropp av $\mathbb{Q}(\sqrt{2})$.

(d) Definer $\varphi_{\sqrt{2}} \colon \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ ved at $\varphi_{\sqrt{2}}(f(x)) = f(\sqrt{2})$, evalueringshomomorfien gitt ved elementet $\sqrt{2}$ i $\mathbb{Q}(\sqrt{2})$. Sjekk at $\varphi_{\sqrt{2}}$ har bilde i $\mathbb{Q}(\sqrt{2})$. Siden $\varphi_{\sqrt{2}}(a+bx) = a+b\sqrt{2}$, så er $\varphi_{\sqrt{2}}$ på. Vi har at $\sqrt{2}$ er en rot i x^2-2, og dette er et polynom av minst grad i $\mathbb{Q}[x]$ slik at $\sqrt{2}$ er en rot. Kjernen til $\varphi_{\sqrt{2}}$ er alle polynomer i $\mathbb{Q}[x]$ med $\sqrt{2}$ som rot. Siden x^2-2 er polynomet av minst grad i $\mathbb{Q}[x]$ med $\sqrt{2}$ som rot, så har vi at $\operatorname{Ker}\varphi_{\sqrt{2}} = ((x^2-2))$. Da følger det fra Setning 86 at

$$\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}(\sqrt{2}).$$