KONSTRUKSJON AV ENDELIGE KROPPER (NOTAT FOR TMA4510)

Nummerene i parantes refererer til det samme resultatet i Fraleigh *A first course in abstract algebra.*

Setning 1 (27.9). *R kommutativ ring med $1 \neq 0$, $I \neq R$ ideal i R. Da har vi at I er et maksimalt ideal hvis og bare hvis R/I er en kropp.*

Setning 2 (27.25). *F kropp, $p(x) \in F[x]$, grad $p(x) \geq 1$. Da er $p(x)$ irredusibelt hvis og bare hvis $\langle p(x) \rangle$ er et maksimalt ideal.*

Setning 3 (27.10). *$n > 0$ i $\mathbb{Z}$. Da er $\langle n \rangle$ er et maksimalt ideal hvis og bare hvis n er et primtall.*

Setning 4. *En endelig kropp F inneholder en kropp $K \simeq \mathbb{Z}_p$, p primtall.*

Bevis. La F være en endelig kropp, og konstruer en ringhomomorfi $\mathbb{Z} \to F$ ved å sende den multiplikative enheten i $\mathbb{Z}$ på den multiplikative enheten i F, altså $f(1) = 1_F$. Vi veit at $\operatorname{Ker} f$ er et ideal i $\mathbb{Z}$, og $\mathbb{Z}/\operatorname{Ker} f \simeq \operatorname{Im} f$, hvor $\operatorname{Im} f$ er en underring av F. Vi ser at $\operatorname{Im} f$ må være et integritetsområde, siden den er en underring av F som er en kropp, og dermed et integritetsområde. Da $\operatorname{Ker} f$ er et ideal i $\mathbb{Z}$ må $\operatorname{Ker} f = \langle p \rangle$ hvor $p \in \mathbb{N}$. Siden $\mathbb{Z}/\operatorname{Ker} f \simeq \operatorname{Im} f$ hvor $\operatorname{Im} f$ er et integritetsområde, må p være et primtall. Ved å la $K = \operatorname{Im} f \simeq \mathbb{Z}/\operatorname{Ker} f = \mathbb{Z}/\langle p \rangle \simeq \mathbb{Z}_p$, ser vi at påstanden er bevist. □

Setning 5 (33.2). *En endelig kropp F har p^r elementer, der p primtall, $r > 0$.*

Setning 6. *La $p(x) \in \mathbb{Z}_p[x]$, grad $p(x) = r$. Da er $\{1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \ldots, x^{r-1} + \langle p(x) \rangle\}$ en basis for $\mathbb{Z}_p[x]/\langle p(x) \rangle$ over $\mathbb{Z}_p$.*

Bevis. Vi viser først at $\{1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \ldots, x^{r-1} + \langle p(x) \rangle\}$ er lineært uavhengige i $\mathbb{Z}_p[x]/\langle p(x) \rangle$. Vi antar derfor at $a_0(1 + \langle p(x) \rangle) + a_1(x + \langle p(x) \rangle) + \cdots + a_{r-1}(x^{r-1} + \langle p(x) \rangle) = a_0 + a_1 x + \cdots + a_{r-1}x^{r-1} + \langle p(x) \rangle = \langle p(x) \rangle$, hvor $a_i \in \mathbb{Z}_p$ for $i \in [0, r-1]$. Dette gir at $a_0 + a_1 x + \cdots + a_{r-1}x^{r-1} \in \langle p(x) \rangle$. Siden alle elementer ulik 0 i $\langle p(x) \rangle$ har grad større enn r, betyr dette at $a_0 + a_1 x + \cdots + a_{r-1}x^{r-1} = 0$. Dermed må $a_i = 0$ for $i \in [0, r-1]$ så vi ser at elementene er lineært uavhengige.

Det står da igjen å vise at $\{1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \ldots, x^{r-1} + \langle p(x) \rangle\}$ genererer $\mathbb{Z}_p[x]/\langle p(x) \rangle$. La derfor $f(x) + \langle p(x) \rangle \in \mathbb{Z}_p[x]/\langle p(x) \rangle$. Vi veit fra divisjonsalgoritmen at $f(x) = r(x) + g(x)p(x)$ hvor graden av $r(x)$ er mindre enn graden av $p(x)$, altså mindre enn r. Siden graden av $r(x)$ er mindre enn r, så er $r(x)$ generert av $\{1, x, \ldots, x^{r-1}\}$, og derfor er $r(x) + \langle p(x) \rangle$ generert av $\{1 + \langle p(x) \rangle, x + \langle p(x) \rangle, \ldots, x^{r-1} + \langle p(x) \rangle\}$.

Nå er $f(x) + \langle p(x)\rangle = r(x) + \langle p(x)\rangle$, så også $f(x) + \langle p(x)\rangle$ er generert av $\{1 + \langle p(x)\rangle, x + \langle p(x)\rangle, \ldots, x^{r-1} + \langle p(x)\rangle\}$. □

Korollar 7. *$p(x)$ irredusibel i $\mathbb{Z}_p[x]$, p primtall, grad $p(x) = r \geq 1$. Da er $\mathbb{Z}_p[x]/\langle p(x)\rangle$ en kropp med p^r elementer.*

Eksempel:

(1) $x^2 + x + 1$ er irredusibel i $\mathbb{Z}_2[x]$, så $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ har $2^2 = 4$ elementer. Beskrivelse av $F = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$: La $\alpha = x + \langle x^2 + x + 1\rangle$. Nå er $\{1, \alpha\}$ er basis for F over $\mathbb{Z}_2$, så elementene i F er $0, 1, \alpha, 1 + \alpha$. For å multiplisere brukes likningen $\alpha^2 + \alpha + 1 = 0$. Eksempel: $\alpha(\alpha + 1) = \alpha^2 + \alpha = -\alpha - 1 + \alpha = -1 = 1$.

(2) $x^3 + x + 1$ er irredusibel i $\mathbb{Z}_2[x]$, så $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ har $2^3 = 8$ elementer.

(3) $x^2 + 1$ er irredusibel i $\mathbb{Z}_3[x]$, så $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ har $3^2 = 9$ elementer.

(4) $p(x) = x^4 + x^3 + x^2 + x + 1$ er irredusibel i $\mathbb{Z}_2[x]$, så $F = \mathbb{Z}_2[x]/\langle p(x)\rangle$ er en kropp med $2^4 = 16$ elementer. $F \setminus \{0\}$ er da en syklisk gruppe med 15 elementer. La $\alpha = x + \langle p(x)\rangle$, vi har da $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$. Det kan vises at $1 + \alpha$ en generator for $F \setminus \{0\}$, mens α har orden 5.