Forelesning 11. mars 2024

Defn 22.1.

R ring

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$ for en $n \in \mathbb{Z}_+$ og $a_i \in R$

kalles et polynom med koeffisienter i R.

Følgende gir mening:

$f(x) + g(x)$

$f(x) \cdot g(x)$

$f(x) = 0$ null-polynom (konstant)

$f(x) = 1$

$-f(x)$ Additiv invers

+ Assosiativitet og distributivitet

$\Rightarrow$ $R[x]$ Polynomringen (kommutativ ring)

Eksempler: $\mathbb{R}[x]$ reelle koeffisienter

$\mathbb{Z}_2[x]$: $(x+1) + (x+1) = 0$

$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$

Thm. 22.4.

$F \subset E \ni a$ under kropp.

$\varphi_a(f(x)) = f(a) = a_0 + a_1 a + \cdots + a_n a^n$

homomorfi $\varphi_a : F[x] \to E$

$\varphi_a|_F = id_F$

Evalueringshomomorfien i $x = a$

Ex.

1) $\varphi_\pi : \mathbb{Q}[x] \to \mathbb{R}$ $f(x) \mapsto f(\pi)$ Har ingen kjerne $\Rightarrow \mathbb{Q}[\pi] \cong \mathbb{Q}[x]$

2) $\varphi_i : \mathbb{Q}[x] \to \mathbb{C}$

$x^2 + 1 \mapsto i^2 + 1 = -1 + 1 = 0$

Kjernen til φ_i inneholda (er generert av) $x^2 + 1$.

Defn 22.10

$F \subset E \ni \alpha \quad \varphi_\alpha : F[x] \longrightarrow E$

underkropp

La $f(x) \in F[x]$. Dersom $f(\alpha) = 0$ sier vi at α er en rot i f.

Thm 22.11 $\left(\mathbb{Q} \subset \mathbb{R} \ni \sqrt{2} \quad \varphi_{\sqrt{2}} : \mathbb{Q}[x] \longrightarrow \mathbb{R}, \; x^2 - 2 \mapsto \sqrt{2}^2 - 2 = 0 \right)$

$\sqrt{2} \notin \mathbb{Q}$.

Bevis

Anta $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ $\quad \gcd(a,b) = 1$ (forkortet mest mulig)

$\Rightarrow 2 = \frac{a^2}{b^2}$ eller $a^2 = 2b^2$

$\Rightarrow 2 \mid a \; ; \; a = 2c$

$\Rightarrow 4c^2 = 2b^2$ eller $2c^2 = b^2$

$\Rightarrow 2 \mid b$ Motsigelse $\square$

Faktorisering av et Polynom

$f(x) = g(x) h(x)$

Thm 23.1 Divisjons algoritme — betyr $\exists!$ entydig

$f(x), g(x) \in F[x] \Rightarrow \exists! \; q(x), r(x)$ slik at

$\deg f = n, \deg g = m > 0$ $\quad f(x) = q(x) g(x) + r(x)$

hvor $r(x) = 0$ eller $\deg r < m$

Bevis

La $S = \{ f(x) - g(x) s(x) \mid s(x) \in F[x] \}$

Hvis $0 \in S$ så må $f(x) = g(x) s(x)$

og $q(x) = s(x), \; r(x) = 0$

Hvis $0 \notin S$ kan vi finne et element i S med minimal grad (ikke entydig), kall denne $r(x)$

$$\Rightarrow \quad f(x) = q(x)g(x) + r(x)$$

Anta $\deg r > m$; $r(x) = c_t x^t +$ lavere grads ledd $\quad t > m$

La $r'(x) = r(x) - c_t \frac{g(x)}{b_m} x^{t-m}$ hvor $g(x) = b_m x^m + \ldots$

$$\Rightarrow \quad f(x) = q(x)g(x) + r'(x) + \frac{c_t}{b_m} x^{t-m} g(x)$$

$$= \left(q(x) + \frac{c_t}{b_m} x^{t-m}\right) g(x) + r'(x)$$

Men $\quad r'(x) = c_t x^t + \text{lavere} - c_t \frac{b_m x^m + \text{lavere}}{b_m} x^{t-m}$

$$= c_t x^t - c_t x^m \cdot x^{t-m} + \text{lavere}$$

$$= \text{lavere ledd, dvs } \deg r' < \deg r$$

Men $\deg r$ var antatt å være minst.

$$\Rightarrow \quad \deg r < m$$

Må vise entydighet. Anta

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

$$\Rightarrow \quad \left(q_1(x) + q_2(x)\right) g(x) = r_2(x) - r_1(x)$$

Siden $\deg r_2(x) - r_1(x) < \deg g$ må vi ha $r_1(x) = r_2(x)$

$$\Rightarrow \quad \left(q_1(x) - q_2(x)\right) g(x) = 0$$

Siden F er et integritetsområde vil alltid $\deg(fg) = \deg(f) + \deg(g)$

$$\Rightarrow \quad q_1(x) - q_2(x) = 0. \qquad \square$$

Hvorfor $f(x) = a_n x^n +$ lave , $g(x) = b_m x^m +$ lavere

$$\Rightarrow f(x)g(x) = a_n b_m x^{n+m} + \text{lavere}$$

og $a_n, b_m \neq 0 \Rightarrow a_n b_m \neq 0$

Kor. 23.3

$a \in F$ rot i $f(x) \in F[x]$ $\iff$ $(x-a) \mid f(x)$ dvs $f(x) = (x-a)\,g(x)$

Bevis $f(x) = q(x)(x-a) + r(x)$

Hvis $f(a) = 0$, dvs $q(a)(a-a) + r(a) = r(a) = 0$

Men $\deg(r) < \deg(x-a) = 1$, dvs $r(x)$ konstant

$\Rightarrow r(x) = 0$ □

Kor 25.5

$f(x) \in F[x]$, $\deg f = n$. $\Rightarrow$ f kan ha max n røtter i F

Bevis $f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$

Kor 25.6

$G \subset F^* = F \setminus \{0\}$ $\Rightarrow$ G syklisk

G: endelig gruppe; F: kropp

Spesielt hvis $|F| < \infty \Rightarrow F^*$ er syklisk

Bevis

Ved strukturteoremet: $G \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_m^{r_m}}$

La m være $m = \max(p_1^{r_1}, \ldots, p_m^{r_m}) \leq |G|$

Velg $a \in \mathbb{Z}_{p_i^{r_i}}$, dvs $a^{d_i} = 1$ $d_i = p_i^{r_i}$

og a er rot i $x^{d_i} - 1$; og derfor også rot i $x^m - 1$

Nå har $x^m - 1$ max m røtter, dvs $|G| \leq m$.

$\Rightarrow |G| = m \Rightarrow m = \max(p_1^{r_1}, \ldots, p_m^{r_m}) = p_1^{r_1} \cdots p_m^{r_m}$

$\Rightarrow$ alle $p_i \neq p_j$ og

$G \simeq \mathbb{Z}_m$. $m = p_1^{r_1} \cdots p_m^{r_m}$.

□

Ex. $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1.$

Defn 23.7

Motsatt: REDUSIBEL

$f(x) \in F[x]$ IRREDUSIBEL $\quad f(x) = g(x)h(x) \Rightarrow \deg g = 0$ eller $\deg h = 0$

Ex – $x^2 - 2 \in \mathbb{Q}[x]$ irredusibel

– $x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ irredusibel

$f(x)$ forts. $f(0) = 2,\ f(1) = 1\ f(2) = 6$

$f(3) = 3\ f(4) = 3$

dvs. ingen lineær faktor

Thm. 23.10

$f(x) \in F[x] \Rightarrow f(x)$ er redusibel

$\deg f = 2, 3$ dersom $\exists \alpha \in F$ s.a $f(\alpha) = 0$

Bevis $f(x) = g(x)h(x) \Rightarrow$ Minst én av ggh har grad 1., dvs $g(x) = x - \alpha$.

Ex. $f(x) = x^4 + x^3 - x^2 - 2x - 2$ er redusibel, men har ingen rotte over $\mathbb{Q}$

$\Rightarrow x^4 + x^3 - x^2 - 2x - 2 = (x^2 - 2)(x^2 + x + 1)$

$x = \pm\sqrt{2}$ $\quad x = \frac{-1 \pm \sqrt{-3}}{2}$

P primtall $\quad \Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$

irredusibel over $\mathbb{Q}$

Thm 23.18

$p(x) \in F[x]$ irreducibel Hvis $p(x) \mid r(x)s(x)$, så må vel $p(x) \mid r(x)$ eller $p(x) \mid s(x)$

$\Rightarrow$ (induksjon) $p(x) \mid r_1(x) \cdots r_t(x) \Rightarrow p(x) \mid r_c(x)$ for en c.

$\Rightarrow$ $f(x) = p_1(x) \cdots p_r(x)$ $p_c(x)$ irreducibel

Faktorisering en entydig opp til permutasjoner.

Ex. $x^3 + 3x^2 + 1 \in \mathbb{Z}_5[x]$

har faktorisering

$$x^3 + 3x^2 + 1 = (x-1)(x-3)(x+2)$$
$$= (3x+2)(2x-1)(x-3)$$