

Session 4b.

Program. Fredag den 20/5 er overskriften „Polynomier; Ringhomomorfi, isomorfi“, fra POL3 og RNG3; øvelserne er RNG1: 4, 18; RNG2: 1, 8, 9; POL1: 1, 2, 7.

Nøgleord: Polynomium, koefficient, normeret polynomium, ledende koefficient, konstant polynomium, grad, nul-polynomium, grad af sum og produkt, division med rest (for polynomier), Euklid's algoritme, Hovedidealsætningen for $L[X]$.

Kommentar. Sætningen om division med rest giver resultater om rødder i polynomier med koefficienter i R . Hvis R er et integritetsområde, er antallet af rødder højst lig med graden af polynomiet. I almindelighed afhænger resultaterne af egenskaber ved ringen R . For $R = \mathbb{C}$ kan Algebraens Fundamentalsætning anvendes: Et polynomium i $\mathbb{C}[X]$ af grad n har n rødder (talt med multiplicitet). Bemærk i øvrigt hvordan slutresultatet i POL(3.10) tillader at formulere Algebraens Fundamentalsætning uden brug af komplekse tal: Ethvert polynomium $f \in \mathbb{R}[X]$ af grad $n \geq 1$ er deleligt enten med et polynomium af formen $X - a$ (nemlig hvis f har en reel rod a) eller med et polynomium af formen $(X - a)^2 + b^2$.

Bemærk også hvordan resultaterne, i POL(3.13)–(3.14), bruges til at vise, for et primtal p , at gruppen $(\mathbb{Z}/p)^*$ af primiske restklasser modulo p er en cyklisk gruppe. Beviset er ikke konstruktivt, og det fortæller *ikke* hvordan man bestemmer et tal $a < p$ således, at restklassen $[a]$ er en frembringer for $(\mathbb{Z}/p)^*$.

Kuglerne.

• *Isomorfiætning.* For en ringhomomorfi $\varphi: R \rightarrow R'$ er kernen $\varphi^{-1}(0) \subseteq R$ er ideal, billedet $\varphi(R) \subseteq R'$ er en delring, og

$$R/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(R).$$

Videre gælder Noether's anden Isomorfiætning: Der er en bijektiv forbindelse mellem idealer $\mathfrak{a} \subseteq R$ med $\varphi^{-1}(0) \subseteq \mathfrak{a}$ og samtlige idealer $\bar{\mathfrak{a}}$ i $\varphi(R)$, bestemt som $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ og $\bar{\mathfrak{a}} \mapsto \varphi^{-1}(\bar{\mathfrak{a}})$. Når $\mathfrak{a} \supseteq \varphi^{-1}(0)$ findes en isomorfi,

$$R/\mathfrak{a} \xrightarrow{\sim} \varphi(R)/\varphi(\mathfrak{a}).$$

• *Rødder.* Elementet $a \in R$ er rod i $f \in R[X]$ (dvs $f(a) = 0$), hvis og kun hvis man kan faktorisere: $f = q \cdot (X - a)$.

• *Rødderne.* Man kan faktorisere $f \neq 0$ i $R[X]$ på formen $f = q \cdot (X - a_1) \cdots (X - a_r)$, hvor $q \in R[X]$ er et polynomium uden rødder i R . Hvis R er et integritetsområde, er faktoriseringen af denne form entydig, og a_i 'erne er netop rødderne i f .

Konsekvens (når R er et integritetsområde): Antal rødder i f , talt med multiplicitet, er r , og altså højst lig med graden af f .

• *Anvendelse.* Lad p være et primtal. Af Fermat's lille Sætning følger modulo p , for $k = 1, \dots, p - 1$, at $[k]^{p-1} = [1]$, altså at $[k]$ er rod i polynomiet $X^{p-1} - 1 \in \mathbb{F}_p[X]$. Faktoriseringen af $X^{p-1} - 1$ må altså være følgende:

$$X^{p-1} - [1] = (X - [1])(X - [2]) \cdots (X - [p - 1]). \quad (*)$$

Koefficienten til X^i er den samme på begge sider. Specielt, for $i = 0$, fås *Wilson's sætning*:

$$(p - 1)! \equiv -1 \pmod{p}.$$

[Hovsa! Hvad blev der af faktoren $(-1)^{p-1}$, der naturligt indgår når faktorerne i (*) ganges sammen?]

• *Sætning*. Enhver endelig undergruppe af L^* , hvor L er et legeme, er cyklisk. Specielt: For et primtal p er den multiplikative gruppe $(\mathbb{Z}/p)^* = \mathbb{F}_p^*$ en cyklisk gruppe af orden $p - 1$.

Hvornår var det nu det var? Euklid (ca) 365–300, John Wilson, 1741–1793, Emmy Noether 1882–1935.

På sigt: Tirsdag den 24/5 er overskriften „Brøklegame; UFD og PID“, med materiale fra RNG4-5; øvelser fra **OBL**; POL1: 3, 4, 6; RNG2: 3, 5, 7*; RNG3: 3, 6; UO: 16, 17.

Anders Thorup