

Session 12-13.

Program. Den ottende og sidste uge har overskriften „Polynomier, rødder“, på basis af POL1-3. Tirsdag T9/6 erstatter i princippet to fredage, men afholdes efter sædvanligt tirsdagsskema. Øvelser: RNG1: 4, 3, 6, 12, 13, 16, 18; POL1: 1, 2, 3, 7.

Og fredag F12/6 er det øvelserne POL1: 4, 6; POL2: 1, 3, 4, 5, 6; POL3: 2, 3, 4, 6, 11.

Kommentar. Et par steder i pensum bruges begreber, der er defineret uden for pensum. Fx omtales en *ringhomomorfi*, se kuglen nedenfor. Det er en simpel sag at bruge bogens register til at finde den korrekte definition. Begreber, der ikke er defineret i pensum, forudsættes naturligvis ikke kendt ved den skriftlige eksamen.

Nøgleord: primring, nul-reglen, integritetsområde, skævlegeme, legeme. Polynomium, koefficient, normeret polynomium, ledende koefficient, normere et polynomium, konstant polynomium, grad, nul-polynomium, grad af sum og produkt. Division med rest (for polynomier).

Euklid's algoritme, rod i polynomium, multipel rod, enhedsrødder, Wilson's sætning, \mathbb{F}_p^* er cyklisk.

Kommentar. Vi bruger sætningen om division med rest til at sige noget om rødderne i et polynomium. 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.

• *Jeg nævner det lige*, selv om det ikke hører med til pensum: En afbildning $\varphi: R \rightarrow R'$ mellem ringe kaldes en *ringhomomorfi*, hvis $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$, og $\varphi(1_R) = 1_{R'}$.

Og et *ideal* i en ring R er en delmængde $\mathfrak{a} \subseteq R$, som indeholder 0, er stabil under addition og stabil under multiplikation med et vilkårligt element $r \in R$.

• *Nul-reglen* gælder, hvis der af $\lambda\mu = 0$ følger, at $\lambda = 0$ eller $\mu = 0$.

• *Et skævlegeme* er en ring, hvori ethvert element $\lambda \neq 0$ er invertibelt og et *integritetsområde* er en ring, hvori nul-reglen gælder; begge definitioner med den yderligere præcision, at ringen ikke må være nul-ringen.

• *Der er kun én ring* med p elementer (hvor p er et primtal), nemlig \mathbb{Z}/p , og den er et legeme, betegnet \mathbb{F}_p .

8. juni 2009

• *Division med rest i $R[X]$* . For et givet normeret „divisorpolynomium“ d kan hvert polynomium f entydigt skrives $f = qd + r$, hvor $\text{grad}(r) < \text{grad}(d)$. Når R er et legeme, gælder konklusionen, når blot $d \neq 0$.

• *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, William Rowan Hamilton 1805–1865, Ferdinand Georg Frobenius 1849–1917, Joseph Henry Maclagen Wedderburn 1882–1948.

På sigt: I skal læse til eksamen, og jeg skal rette besvarelser.

Anders Thorup