

Session 11-12.

Program. Den sidste uge har overskriften „Polynomier, rødder“, på basis af POL1-3. Øvelserne: Tirsdag 3/6 er det POL1: 4, 6; POL2: 1, 3, 4, 5, 6; POL3: 2, 3, 4, 6, 11 .

Og fredag 6/6 er det Eksamensopgaver .

Bemærk. Bemærk, at der er kommet en indskrænkning af pensum: POL(2.6) hører ikke med til pensum. Ordet *ringhomomorfi* nævnes et par gange i pensum, og ordet *ideal* nævnes en enkelt gang, selv om selve definitionen står afsnit, der ikke opgives. De forsøges forklaret i teksten, hvor de forekommer, men du kan roligt springe over ordene. De bliver ikke brugt i eksamensopgaverne.

Nøgleord: Ring, distributiv lov, nul-element, modsat element, et-element, kommutativ ring, invertibelt element (enhed), stabil delmængde (mht + og \cdot), delring, nul-ringen, talringe, restklasseringe, funktionsringe, matrixringe, karakteristik, primring, nul-reglen, integritetsområde, skævlegeme, legeme. Polynomium, koefficient, normeret polynomium, ledende koefficient, 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, normere et polynomium.

Kommentar. Det beskedne hovedresultat i POL1 er, at et polynomium $r_0 + r_1X + \dots + r_nX^n$ simpelthen *defineres som* listen (r_0, r_1, r_2, \dots) af sine koefficienter. Det nye er, at koefficienterne kan tages fra en vilkårlig (kommutativ) ring R . Men hvad er X ? Der er to (lige rigtige) svar. Enten: X^i er en „pladsholder“, der fortæller, at det element i R , der står foran, er den i 'te koefficient. Eller: X er selv et polynomium, nemlig det specielle polynomium med koefficienter $(0, 1, 0, 0, \dots)$.

Polynomierne med koefficienter i R udgør en ring, betegnet $R[X]$, idet man regner med polynomier som vi er vant til: Det er noget der sker med koefficienterne foran potenserne X^i . Specielt kan man betragte polynomier i $\mathbb{Z}[X]$ (heltalskoefficienter) og polynomier i $\mathbb{F}_p[X]$ (koefficienter, der er restklasser modulo et primtal p).

Sætningen om division med rest for polynomier er i princippet kendt fra gymnasiet. For polynomier med koefficienter i en vilkårlig ring R antages, at „divisorpolynomiet“ d er normeret, $d = X^n + \dots$. For polynomier med koefficienter i \mathbb{Q} eller \mathbb{R} (som i gymnasiet) eller mere generelt, med koefficienter i et legeme L , fx \mathbb{C} eller \mathbb{F}_p) kan man blot antage, at d ikke er nulpolynomiet. Det induktive bevis for sætningen er blot en nedskrivning af hvad man faktisk gør, når man dividerer et polynomium op i et andet.

Polynomiumsringen $L[X]$ med koefficienter i et legeme L har en række egenskaber fælles med ringen \mathbb{Z} af hele tal. Det bygger på, at man i begge ringe har en sætningen om division med rest. Fx kan man i begge ringe udføre Euklid's algoritme, og man kan bruge algoritmen til at bestemme den største fælles divisor d for to elementer f, f_1 . I polynomiumsringen skal „største“ tages i betydningen: „enhver anden fælles divisor er divisor i d “. Tilsvarende gælder i begge ringe, at hvert ideal er et hovedideal, dvs af formen (f) .

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 multiplisitet). Bemærk i øvrigt hvordan slutresultatet i POL(3.10) tillader at formulere Algebraens

30. maj 2008

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 $r \in R$.

• *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.

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

Anders Thorup