

Ugeseddel 16.

Programmet er forbi, i hvert fald undervisningsdelen. I den sidste uge gennemgik jeg POL4 (kursorisk) og POL5.

Jeg holder spørgetime inden mundtlig,

fredag den 13. juni kl 13 i auditorium 4.

På nogle af øvelsesholdene afholdes en spørgetime inden skriftlig eksamen (der er fri adgang):

Ruth (hold 1): fredag den 30. maj kl 11.15 auditorium 9.

Henrik (hold 3): fredag den 30. maj kl 10 i lokale A107.

Jonas (hold 5): fredag den 30. maj kl 11 i A104.

Troels (hold 4): fredag den 30. maj kl 10.15 i lokale A106.

Ved eksamen bedømmes der i to spor, nemlig af Gunnar Forst og af undertegnede. Der eksamineres skriftligt den 2. juni, og mundtligt i de tre dage: 17., 18. og 19. juni. Ved den skriftlige eksamen får man lejlighed til at udtrykke ønske om ikke at komme op en bestemt dag. Kort efter den skriftlige eksamen offentliggøres (på hjemmesiden og på opslagstavlen) listen over eksaminationsrækkefølgen ved den mundtlige.

Nøgleord: Primitivt polynomium, Gauss' lemma, Gauss' sætning ($\mathbb{Z}[X]$ er et UFD), Eisenstein's irreducibilitetskriterium; struktur af polynomiumskvotient.

Kommentar. En diofantisk ligning er typisk en ligning, hvortil man søger heltalsløsninger. Et eksempel er ligningen for pytagoræiske talsæt: $x^2 + y^2 = z^2$. Et andet eksempel er Pell's ligning, $x^2 - Dy^2 = \pm 1$. Begge ligninger omtales i RNG6.

Ringene $\mathbb{Z}[X]$ af polynomier med heltalskoefficienter er *ikke* et hovedidealområde. Fx er det let at se, at polynomierne med lige konstantled er et ideal, og at dette ideal ikke er et hovedideal. Gauss' sætning udsiger, at ringen $\mathbb{Z}[X]$ er faktoriel. Denne ring er altså et eksempel på et UFD, der ikke er et PID. Der er naturligvis en sammenhæng mellem polynomier i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$, som er nøjere beskrevet i POL4 (kursorisk). Eisenstein's kriterium tillader at slutte, at en række polynomier i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$ er irreducible. Fx følger det, at der i $\mathbb{Q}[X]$ er irreducible polynomier af enhver positiv grad. Det samme gælder i øvrigt i ringen $\mathbb{F}_p[X]$.

Bogens sidste kapitel, POL5, fortæller specielt om strukturen af en kvotientring $K := L[X]/(f)$, hvor f er et normeret polynomium af grad $n \geq 1$ (og L er et legeme). Elementerne i K er ækvivalensklasser. Af sætningen om division med rest følger, at der i hver ækvivalensklasse ligger præcis et polynomium af grad mindre end n , altså præcis et polynomium af formen $r_0 + r_1X + \dots + r_{n-1}X^{n-1}$. Ækvivalensklasser svarer herved bijektivt til n -sæt (r_0, \dots, r_{n-1}) . Alternativt betyder resultatet, at de n potenser $1, \xi, \dots, \xi^{n-1}$, hvor $\xi := [X]$ er ækvivalensklassen der indeholder X , er en basis for K som vektorrum over L .

Den vigtige egenskab ved konstruktionen er, at det givne polynomium f i den større ring K har en rod, nemlig $f(\xi) = 0$.

Hvis f er irreducibelt, så er hovedidealet (f) i $L[X]$ et maksimalideal (fordi $L[X]$ er et PID). Derfor er kvotientringen K et legeme. Hvis $L = \mathbb{F}_p$ er legemet med p elementer, bliver K altså et legeme med p^n elementer. Man kan i øvrigt vise, at alle endelige (skæv-)legemer fremkommer på denne måde.

Kuglerne.

• *Primitivt polynomium.* Et polynomium f i $\mathbb{Z}[X]$ er primitivt, hvis 1 er den største fælles divisor for koefficienterne i f .

• *Gauss' Lemma.* Af en ligning $f = \psi h$, hvor $f, g \in \mathbb{Z}[X]$ og $\psi \in \mathbb{Q}[X]$, og hvor h antages at være primitivt, følger, at $\psi \in \mathbb{Z}[X]$.

• *Primelementer i $\mathbb{Z}[X]$.* Polynomiumsringen $\mathbb{Z}[X]$ er et UFD; specielt er primelement og irreducibelt element det samme.

Et sædvanligt primtal p er et primelement i $\mathbb{Z}[X]$. Med andre ord: hvis et produkt fg har alle koefficienter delelige med p , så har en af faktorerne den samme egenskab.

Et polynomium f af grad ≥ 1 er et primelement=irreducibelt element i $\mathbb{Z}[X]$, hvis og kun hvis f er primitivt, og irreducibelt i $\mathbb{Q}[X]$.

• *Eisenstein's kriterium* fortæller specielt, at hvis der for et normeret polynomium i $\mathbb{Z}[X]$,

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

og et primtal p gælder, at $p \mid a_i$ for alle i og $p^2 \nmid a_0$, så er f irreducibelt.

Hvornår var det nu det var? Diophantus 200–284, John Pell 1611–1685, Karl Friedrich Gauss 1777–1855, Ferdinand Gotthold Max Eisenstein 1823–1852.

God læseferie!

Anders Thorup