

Ugeseddel 16.

Programmet er forbi, i hvert fald undervisningsdelen. I den sidste uge gennemgik jeg resten af POL5. I øvrigt holder jeg spørgetime inden mundtlig,

fredag den 18. juni kl 10 i auditorium II.

Ved eksamen bedømmes der i to spor, nemlig af Gunnar Forst og af undertegnede. Der eksamineres skriftligt den 2. juni, og mundtligt i fire dage: 22.–25. juni. Ved den skriftlige eksamen får man lejlighed til at udtrykke ønske om ikke at komme op en bestemt dag. Et eventuelt ønske skal vedlægges besvarelsen. Kort efter den skriftlige eksamen offentliggøres (på hjemmesiden og på opslagstavlen) listen over eksaminationsrækkefølgen ved den mundtlige.

Nøgleord: Konstruktion af endelige legemer.

Kommentar. Ringen $\mathbb{Z}[X]$ 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 $K := L[X]/(d)$, hvor d 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 ét 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 d i den større ring K har en rod, nemlig $d(\xi) = 0$.

Hvis d er irreducibelt, så er hovedidealet (d) 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.

• *Diophantiske ligninger* er ligninger, hvortil man søger heltalsløsninger (eller rationale løsninger). Eksempler er ligningerne $x^n + y^n = z^n$, som ikke kan løses med naturlige tal, når $n > 2$, og ligningen $x^2 + bxy + cy^2 = k$ (for givne $a, b, k \in \mathbb{Z}$). Den sidste ligning svarer til at bestemme tal $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ med $N(\alpha) = k$. Specielt, for $k = \pm 1$, fremkommer Pell's ligning $x^2 + bxy + cy^2 = \pm 1$, der svarer til at bestemme enheder ($N(\alpha) = \pm 1$) i talringen $\mathbb{Z}[\xi]$.

Hvornår var det nu det var? Diophantus 200–284, John Pell 1611–1685.

God læseferie!

Anders Thorup