

Session 5a/5b.

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

Fredag den 27/5 er overskriften „UFD og PID“, med materiale fra RNG5; øvelser fra RNG3: 1; POL2: 1, **3**, 4, **5**, 6; POL3: 6, 11.

Nøgleord: Rod i polynomium, multipel rod, enhedsrødder, Wilson's sætning, \mathbb{F}_p^* er cyklisk, normere et polynomium.

Og nøgleord til fredagen: Brøk (som ækvivalensklasse af par), brøklegeme for integritetsområde. Enhed=invertibelt element, divisor, multiplum, gå op i, associerede elementer, trivielle divisorer, irreducibelt element, primelement, hovedidealområde (PID), irreducibel opløsning, primopløsning, faktoriel ring (UFD),

Jeg når ikke at omtale det hele, så noget må du læse selv: Euklid's algoritme POL(2.5) for polynomiumsringen $L[X]$ (L et legeme) er helt analog med den „klassiske“ algoritme TAL(3.6). Hovedidealsætningen POL(2.6) for $L[X]$ vender jeg tilbage til i denne uge.

Kommentar. Kapitlet om brøklegemer er kursorisk, men du skal naturligvis vide, at brøkerne $2/14$ og $3/21$ er *det samme* (rationale) tal. Hvis man „kender“ legemet \mathbb{R} , der omfatter ringen \mathbb{Z} af hele tal, så kan man *definere rationale tal*, altså *brøker*, som tal af formen $a/s := as^{-1}$, hvor $a, s \in \mathbb{Z}$ og $s \neq 0$. Med denne definition er det et *resultat*, at $2/14 = 3/21$. Hvis man ikke „kender“ et legeme, som omfatter ringen \mathbb{Z} , kan man *konstruere* brøklegemet: Brøker er ækvivalensklasser af par af hele tal (a, s) med $s \neq 0$, og betegnelsen a/s er en snedig betegnelse for den ækvivalensklasse, der indeholder (a, s) .

Et springende punkt er naturligvis, hvornår to par er ækvivalente: Af hensyn til generaliseringen til vilkårlige integritetsområder er det bedst at vedtage, at to par (a, s) og (a', s') er ækvivalente, når de kan forlænges til det samme par. (For ringen \mathbb{Z} er det ensbetydende med, at parrene kan forkortes til det samme par, men det er ikke tilfældet for generelle ringe.) Det er således en konsekvens af *definitionen*, at $2/14 = 3/21$: de to par $(2, 14)$ og $(3, 21)$ kan forlænges til $(6, 42)$.

Faktoriseringsteorien i RNG5 er vores meget udførlige analyse af Aritmetikkens Fundamentalsætning: *Ethvert $a \neq 0$ har en entydigt bestemt primopløsning.* Vi præciserer! Vi stiller matematikerens evindelige spørgsmål: hvorfor? – Og vi besvarer det!

I den generelle ramme erstattes ringen \mathbb{Z} af hele tal med et kommutativt integritetsområde R . Svarende til fortegn, der kommer ind hvis man vil primopløse negative tal, har man *enhederne*, dvs de invertible elementer i R . I faktoriseringssteori prøver man at „reducere“ elementerne i R ved at skrive dem som produkter af simple elementer. De simpleste elementer (byggestenene), er dem, som ikke kan reduceres: det er de *irreducible* elementer. I beviset for at Aritmetikkens Fundamentalsætning gælder i \mathbb{Z} spiller Det fundamentale Primtalslemma en (nåh ja!) fundamental rolle. For den generelle situation kaldes elementer, der har en tilsvarende egenskab, for *primelementerne* i R .

Et integritetsområde R , hvori Aritmetikkens Fundamentalsætning gælder, kaldes et UFD. I almindelighed er det en overordentlig kompliceret opgave at afgøre, om et givet integritetsområde R er et UFD. I princippet må man først undersøge de irreducible elementer: er der så mange af dem, at ethvert element har en irreducibel opløsning, dvs kan skrives som produkt af irreducible elementer? Denne undersøgelse er ofte ikke-konstruktiv: som vi skal se, kan man for visse ringe fastlå, at hvert element er et produkt af irreducible elementer uden at man eksplicit har angivet bare ét eneste irreducibelt element.

Dernæst skal man undersøge entydigheden af irreducible fremstillinger. Det er typisk konstruktivt, når man fastlår, at entydighed mangler: man angiver et element med to forskellige irreducible opløsninger. Derimod vil det sædvanligvis være indirekte at fastslå, at en forelagt ring er et UFD; det er her det virkelig komplicerede ligger.

Kuglerne.

• *Brøkleget* for et integritetsområde R består af brøker $a/s = \frac{a}{s}$, hvor $a, s \in R$ og $s \neq 0$. To brøker er ens i brøkleget, når de kan forlænges til den samme brøk. Fx består brøkleget for polynomiumsringen $L[X]$ af alle *rationale funktioner*,

$$\frac{a_n X^n + \dots + a_1 X + a_0}{s_m X^m + \dots + s_1 X + s_0},$$

med $s_i \neq 0$ for mindst et i .

- *Enheder etc.* (i) $u \in R$ er en *enhed*, hvis der findes $v \in R$ med $uv = 1$.
- (ii) $a, a' \in R$ er *associerede*, hvis der findes en enhed u med $a' = ua$.
- (iii) d er *divisor* i a , hvis $a = rd$ med passende r , og d er *triviel divisor*, hvis d er en enhed eller d er associeret med a .
- (iv) $q \in R$ er *irreducibelt*, hvis $q \notin \{0\} \cup R^*$ og q kun har trivielle divisorer.
- (v) p er et *primelement*, hvis $p \notin \{0\} \cup R^*$ og der for alle a, b gælder, at $p \mid ab \implies p \mid a \vee p \mid b$. **Øv dig!** „Oversæt“ definitionerne til noget med hovedidealer. Fx er u en enhed, hvis og kun hvis $(u) = (1)$.

• *Primopløsninger* er entydige. Med andre ord: af en ligning $p_1 \cdots p_r = q_1 \cdots q_s$, hvor faktorerne er primelementer, følger, at $r = s$ og at (efter eventuel permutation af q 'erne) p_i er associeret med q_i for alle i .

• *Irreducible opløsninger findes*, for mange ringe. Med andre ord: for „mange“ ringe kan man vise, at hvert $a \notin \{0\} \cup R^*$ kan skrives som produkt af irreducible elementer. En sådan fremstilling er ikke nødvendigvis entydig.

• *PID og UFD*. PID=Hovedidealområde, UFD=faktoriel ring. **Hovedsætning.** *Et PID er et UFD.*

• *Numeriske betingelser*. Antag for R , at der er givet en funktion $v: R \rightarrow \mathbb{Z}$, som er nedad begrænset.

(1) Hvis der for hvert a og hver ikke-triviel divisor d i a gælder $v(d) < v(a)$, så findes irreducible opløsninger i R . (Eksempel: kan bruges på \mathbb{Z} med $v(a) = |a|$, på $L[X]$ med $v(a) = \deg(a)$, og på *alle* kvadratiske talringe $\mathbb{Z}[\xi]$ (som vi møder i næste uge!) med $v(a) = |N(a)|$.)

(2) Hvis der for hvert a og $d \neq 0$ findes $q \in R$ med $v(a - qd) < v(d)$, så er R et PID. (Eksempel: kan bruges på \mathbb{Z} med $v(a) = |a|$, på $L[X]$ med $v(a) = \deg(a)$, og på *visse* kvadratiske talringe $\mathbb{Z}[\xi]$ med $v(a) = |N(a)|$.)

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

På sigt: Tirsdag den 31/5 er overskriften „Kvadratiske talringe“, med materiale fra RNG6; øvelser fra POL3: 2, 3, 4; UO: 10*, 11, 12*, 13; Eks.opg.