

Ugeseddel 12.

Program. Emnerne i den 12. uge, 28/4-2/5, er: Brøklegame, PID og UFD fra RNG4-5. Afsnittet om brøklegame er kursorisk. Ugens øvelser er RNG2: 3, 5, 7*; RNG3: 3, 6; POL2: 3, 4; POL3: 2, 3. UO: 16, 17.

I den 11. uge afsluttede jeg RNG3 og POL3.

Nøgleord: Ringhomomorfi, billedring, kerne, homomorfisætning, isomorfisætning, Noether's anden Isomorfisætning (for ringe); rod i polynomium, multipel rod, enhedsrødder, Wilson's sætning, \mathbb{F}_p^* er cyklisk, normere et polynomium.

Kommentar. Bemærk, at Noether's anden Isomorfisætning giver et alternativt bevis for karakteriseringen af maksimalidealer i RNG(2.12): Lad \mathfrak{m} være et ideal i R . Der er da en bijektiv forbindelse mellem idealer $\mathfrak{a} \supseteq \mathfrak{m}$ og samtlige idealer i R/\mathfrak{m} . Idealet \mathfrak{m} er et maksimalideal, hvis og kun hvis der er præcis to idealer \mathfrak{a} i R , som opfylder $\mathfrak{a} \supseteq \mathfrak{m}$ (nemlig $\mathfrak{a} = \mathfrak{m}$ og $\mathfrak{a} = R$). Følgelig er \mathfrak{m} et maksimalideal, hvis og kun hvis der er præcis to idealer i R/\mathfrak{m} ; den sidste egenskab karakteriserer legemerne ifølge Observation (2.10).

Sætningen om division med rest giver resultater om rødder i polynomier med koefficienter i R . 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.

• *Isomorfisætning.* For en ringhomomorfi $\varphi: R \rightarrow R'$ er kernen $\varphi^{-1}(0) \subseteq R$ et ideal, billedet $\varphi(R) \subseteq R'$ er en delring, og

$$R/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(R).$$

Videre gælder Noether's anden Isomorfisætning: Der er en bijektiv forbindelse mellem idealer $\mathfrak{a} \subseteq R$ med $\varphi^{-1}(0) \subseteq \mathfrak{a}$ og samtlige idealer $\bar{\mathfrak{a}}$ i $\varphi(R)$, bestemt som $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ og $\bar{\mathfrak{a}} \mapsto \varphi^{-1}(\bar{\mathfrak{a}})$. Når $\mathfrak{a} \supseteq \varphi^{-1}(0)$ findes en isomorfi,

$$R/\mathfrak{a} \xrightarrow{\sim} \varphi(R)/\varphi(\mathfrak{a}).$$

• *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. Hvis R er et integritetsområde, at faktoriseringen af denne form entydig, og a_i 'erne er netop rødderne i f .

29. april 2003

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:

$$X^{p-1} - [1] = (X - [1])(X - [2]) \cdots (X - [p-1]).$$

Efter sammenligning af konstantled fås Wilson's sætning:

$$(p-1)! \equiv -1 \pmod{p}.$$

• *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? John Wilson, 1741–1793.

På sigt: I den 13. uge, 5/5-9/5, er overskriften „PID og UFD; kvadratisk talring“ fra RNG5-6. Ugens øvelser er:

RNG3: 1; POL1: 7; POL2: 1, 5, 6; POL3: 4, 6, 11.

Ak og ve, de var alligevel ikke fejlfri! I RNG6, på side 218, skal man rette:

RNG(6.18)⁹: for $k \geq 0 \mapsto$ for $k \geq 0$, $c \geq 2$.

Endvidere er min påstand i TAL(2.11)₃₋₂, om at „ingen læsere af dette kapitel nogensinde vil være i stand til at angive et sådant primtal p “ ubarmhjertigt blev afsløret som falsk¹.

Anders Thorup

¹På initiativ af Jes Hansen blev n (ganske let) faktoriseret i april 2003 af en gruppe under NFSNET.