

Session 11.

Program. Den syvende uge har overskriften „Polynomier; rødder“, med emner fra POL1–2, men jeg mangler også de sidste emner fra RNG1. Der er kun undervisning tirsdag T2/6. Øvelserne er GRP7: 8; GRP8: skrf6, 9, 11, 13, 15*, 16; RNG1: 1, 2, 5.

Husk, at der også er undervisning den ottende uge.

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.

Kommentar. Den „algebraiske struktur“, der behandles i resten af kurset hedder en ring. Det er en mængde R forsynet med to kompositioner, *addition og multiplikation*, som opfylder krav svarende til de sædvanlig regneregler. Den kommutative lov kan undværes, men bortset fra et par eksempler kigger vi kun på kommutative ringe. Bemærk, at vi kræver, at en ring har et *et-element* 1, som er neutralt element for multiplikation. Man kan naturligvis også studere „ringe uden et-element“, og gør man det jævnlige, er det nok dem man vil kalde ringe; „vores“ ringe hedder så *ringe med et-element*.

Med hensyn til additionen er ringen en kommutativ gruppe $(R, +)$. Når man taler om *invertible* elementer i en ring R , er det derfor altid „invertibel med hensyn til multiplikation“. De invertible elementer udgør en gruppe, der betegnes R^* .

Det er vigtigt at vide, at den kommutative gruppe \mathbb{Z}/n af restklasser modulo n , med den naturlige multiplikation af restklasser, er et godt eksempel på en endelig ring. Den kaldes også restklasseringen modulo n . Gruppen af invertible elementer $(\mathbb{Z}/n)^*$ er netop gruppen af primiske restklasser modulo n .

Eksempler på ringe falder naturligt i 3 klasser: *Talringe* (og restklasseringene \mathbb{Z}/n) optræder i talteori, *funktionsringe* indgår i analyse og geometri, og *matrixringe* og andre ikke-kommutative ringe indgår i lineær algebra og repræsentationsteori (herunder i den videregående gruppeteori). Som nævnt betragter vi kun kommutative ringe.

Nul-reglen, som hører til vores sædvanlige regler for regning med tal, gælder *ikke* i almindelighed, fx næsten aldrig for funktionsringe: Antag, at intervallet I er en foreningsmængde, $I = A \cup B$. Hvis $f(t) = 0$ for $t \in A$ og $g(t) = 0$ for $t \in B$, så er produktfunktionen fg lig med nul-funktionen. Eksempler kan konstrueres med C^∞ -funktioner. Ved $f(t) := e^{-1/t}$ for $t > 0$ og $f(t) := 0$ for $t \leq 0$ defineres en funktion f i $C^\infty(\mathbb{R})$. Med $g(t) := f(-t)$ gælder $fg = 0$.

De „pæneste“ ringe hedder *legemer*. De næstpæneste hedder integritetsområder. Det er vigtigt at vide, at for et primtal p er restklasseringen \mathbb{Z}/p et legeme; det betegnes \mathbb{F}_p . Generelt betegner \mathbb{F}_q et legeme med q elementer; sådan et endeligt legeme findes, præcis når q er en potens af et primtal.

Vektorrummet \mathbb{R}^n kan organiseres med en multiplikation til et legeme for $n = 1$ (det er blot \mathbb{R} selv) og for $n = 2$ (det er \mathbb{C}). Hamilton prøvede længe for $n = 3$, men opdagede så, at det kunne gøres for $n = 4$, hvis man droppede den kommutative lov. Det er Hamilton's skævlegeme \mathbb{H} af kvaternioner. Sidst i bogen vises Frobenius' sætning, at det *kun* kan gøres for disse værdier af n , altså for $n = 1, 2, 4$. Hvis man tillader en svækket associativ lov, kan det også gøres for $n = 8$. Wedderburn viste, at et endeligt skævlegeme nødvendigvis er kommutativt.

29. maj 2009

Små (endelige) ringe spiller ikke nogen særlig rolle. Her er en liste med nogle af de mindste, af ordener $n = 1, \dots, 8$:

$$1 \left| \begin{array}{c} 2 \\ \mathbb{F}_2 \end{array} \right| 3 \left| \begin{array}{c} 4 \\ \mathbb{Z}/4, \mathbb{F}_2 \times \mathbb{F}_2, \mathbb{F}_4, \dots \end{array} \right| 5 \left| \begin{array}{c} 6 \\ \mathbb{F}_5 \end{array} \right| 7 \left| \begin{array}{c} 8 \\ \mathbb{Z}/6 \end{array} \right| \mathbb{F}_7 \left| \begin{array}{c} 8 \\ \mathbb{Z}/8, \mathbb{Z}/4 \times \mathbb{Z}/2, \mathbb{F}_8, T_2(\mathbb{F}_2), \dots \end{array} \right.$$

hvor $T_2(\mathbb{F}_2) \subseteq \text{Mat}_2(\mathbb{F}_2)$ betegner delringen af øvre trekantsmatricer. Det er en ikke-kommutativ ring. Der er én til af orden 4, og mange flere af orden 8.

Det beskedne hovedresultat i POL1 er, at et polynomium $r_0 + r_1X + \dots + r_nX^n$ blot er listen (r_0, r_1, r_2, \dots) af sine koefficienter, og at koefficienterne kan tages fra en vilkårlig (kommutativ) ring. 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 $(0, 1, 0, 0, \dots)$.

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 , 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 “.

Kuglerne.

• *Gruppen er produktet af sine Sylowundergrupper*, $G = S_1 \times \dots \times S_r$, hvis der for hver primdivisor p_i i G 's orden kun findes én Sylow- p_i -undergruppe S_i .

• *Smågrupper*. Sylow's sætninger er vigtige redskaber i klassifikationen af endelige grupper. Du kan fx udvide din helt egen liste over smågrupper ved at bruge følgende (p og q er primtal):

(1) Hvis $|G| = qp$ med $q < p$ og $p \not\equiv 1 \pmod{q}$, så er $G = C_{qp}$.

(2) Hvis $|G| = 2p$, så er enten $G = C_{2p}$ eller $G = D_p$.

(3) Hvis $|G| = p^2$, så er enten $G = C_{p^2}$ eller $G = C_p \times C_p$.

(Det sidste har naturligvis intet med Sylow's sætninger at gøre!)

• *En lille morsom ring* består alene af nulelementet. Ringen har altså kun det ene element 0, og kompositionerne er $0 + 0 = 0$ og $0 \cdot 0 = 0$. Den kaldes *nul-ringen*, og det eneste interessante ved den er, at vi må medregne den til ringene.

• *Invertible elementer* (også kaldet enheder) er de λ i ringen Λ , for hvilke der findes et $\mu \in \Lambda$ med $\lambda\mu = \mu\lambda = 1$.

• *Karakteristikken er positiv*, hvis der for et passende $n > 0$ gælder, at $\overbrace{1 + 1 + \dots + 1}^n = 0$. Det ser jo aldeles usædvanligt ud, og 0 og 1 i udtrykket da også nul- og et-element i en abstrakt ring. „Sædvanlige“ ringe har karakteristik 0 (men restklasseringen \mathbb{Z}/n har karakteristik n).

Anders Thorup