# Läsanvisning till Discrete matematics av Norman Biggs - 5B1118 Diskret matematik

Mats Boij

18 november 2001

## 15 Ringar, kroppar och polynom

Det fjortonde kapitlet behandlar *ringar*. En ring har till skillnad från en grupp två operationer, $+$ och $\cdot$.

**Rekommenderade uppgifter**

| | lättare | svårare |
|---|---|---|
| 15.1 | | |
| 15.2 | 1 | 3 |
| 15.3 | 2 | |
| 15.4 | 1,3 | 4 |
| 15.5 | 1 | |
| 15.6 | 1,2 | 3 |
| 15.7 | 6 | 3 |
| 15.8 | 1,2 | |
| 15.9 | 1,2,5 | 17 |

### 15.1 Ringar

Ringaxiomen bygger i stor grad vidare på gruppaxiomen och liknar i mångt och mycket axiomen för heltalen. Utöver att en ring är en abelsk grupp under addition är den associativ under multiplikation. Biggs säger här att den skall ha ett identitetselement för multiplikation, en etta, men det är inte alla ringar som har det, även om alla ringar som dyker upp i denna bok har det. Exempelvis har ringen av jämna heltal ingen etta, men uppfyller övriga ringaxiom.

Det tredje kravet på en ring är att den skall uppfylla de distributiva lagarna. Eftersom multiplikationen inte i allmänhet är kommutativ måste vi ha en distributiv lag från vänster och en från höger.

Exempel på ringar är förstås $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$ och $\mathbf{Z}_n$, men vi skall snart stöta på andra ringar - polynomringar.

**Översättningar**

**ring** *ring*
**distributive laws** *distributiva lagar*
**closure** *slutenhet*
**associativity** *associativitet*
**identity** *identitet*

## 15.2 Inverterbara element i en ring

Om det finns en etta i en ring kan vi prata om inverterbara element, de element som multiplicerade med något annat element blir ett. Eftersom elementen i en ring inte i allmänhet är inverterbara kan vi inte hoppas på att en ring skall vara en grupp under multiplikation. Nollan är exempelvis aldrig inverterbar. Däremot bildar mängden av inverterbara element i en ring $R$ en grupp $U(R)$, eller $R^*$. Att den kallas just $U(R)$ beror på att inverterbara element också kallas *enheter* (*eng. units*).

**Översättningar**

**invertible** *inverterbar*
**inverse** *invers*

## 15.3 Kroppar

Om alla element utom nollan är inverterbara och dessutom multiplikationen är kommutativ kallas ringen för en *kropp*. Här har det svenska och det engelska namnet inte mycket med varandra att göra. Det är bara att hålla reda på att det svenska *kropp* svarar mot engelskans *field*.

I en kropp pratar vi om den additiva och den multiplikativa gruppen. I det senare fallet måste vi ta bort nollan, eftersom den inte är inverterbar.

Det viktigaste exemplet på en kropp i den här kursen är $\mathbf{Z}_p$ när $p$ är ett primtal. Vi har sedan tidigare sett att alla element utom nollan är inverterbara i detta fall, och multiplikationen är kommutativ.

Exemplet som ges i avsnittet använder matriser, men vi skulle lika gärna kunna byta ut matriserna mot uttryck $a + ib$, där $a$ och $b$ ligger i en kropp $F$, exempelvis $\mathbf{Z}_3$ eller $\mathbf{Z}_5$, och $i$ uppfyller $i^2 = -1$, precis som när vi definierar de komplexa talen från de reella. Vi får att $S_2(F)$ bildar en kropp i de fall det inte finns någon kvadratrot ur $-1$ i kroppen $F$ som vi börjar med. Därmed får vi kroppen $\mathbf{C}$ om vi börjar med de reella talen, men vi får inte någon ny kropp om vi börjar med de komplexa talen. Eftersom dfet inte finns någon kvadratrot ut $-1$ i $\mathbf{Z}_3$ får vi på detta sätt en kropp med nio element. Det är det första exemplet vi ser på en ändlig kropp som inte är $\mathbf{Z}_p$ för något primtal.

**Översättningar**

**field** *kropp*
**additive group** *additiv grupp*
**multiplicative group** *multiplikativ grupp*

## 15.4 Polynom

*Polynom* har vi sett tidigare i exempelvis Matematik I. Det fanns då polynom med *reella koefficienter* och polynom med *komplexa koefficienter*. Vi kan använda poynom med koefficienter i en valfri ring $R$, men det är bara när $R$ är en kroppp som vi får de resultat vi är vana vid när det gäller *rötter* och *faktorer*. Därför skall vi koncentrera oss på det fallet när koefficienterna ligger i en kropp.

Den *ledande koefficienten* i ett polynom $p(x)$ är koefficienten för den term i polynomet som har högst *grad*, dvs högst potens av $x$.

Om den ledande koefficienten är $1$ kallas polynomet *moniskt*, eller *monärt*. Sådana polynom är trevliga att handskas med när vi skall dividera med dem.

**Översättningar**

**polynomial** *polynom*
**leading coefficient** *ledande koefficient*
**monic** *monärt, moniskt*

## 15.5 Divisionsalgoritmen för polynom

Divisionalgoritmen som vi lärt oss för polynom med reella eller komplexa koefficienter använder sig inte av något som hindrar oss från att göra likadant med polynom med koefficienter i en kropp. I själva verket kan vi använda koefficienter i en valfri ring så länge den ledande koefficienten i det polynom vi delar med är inverterbar, eller allra helst $1$.

För att kunna formulera satsen om kvot och rest vid division med polynom behöver vi veta vad *graden* för ett polynom $p(x)$ är. Det är den högsta potens av $x$ som förekommer.

Vi får nu nästan precis samma sats som för division av heltal. Skillnaden blir att vi får att resten antingen är noll, och då har den ingen grad, eller så är graden för resten mindre än graden av det vi delar med. $p(x) = q(x)s(x) + r(x)$ där $r(x) = 0$ eller grad$r(x) <$ grad$s(x)$.

**Översättningar**

**degree** *grad*
**quotient** *kvot*
**remainder** *rest*

## 15.6 Euklides algoritm för polynom

När vi väl har divisionsalgoritmen precis som för heltal är steget inte långt till Euklides algoritm. Vi får en största gemensam delare mellan två polynom genom att använda Euklides algoritm och vi kan precis som för heltalen uttrycka den största gemensamma delaren mellan $p(x)$ och $q(x)$ som

$$s(x)p(x) + t(x)q(x)$$

för några polynom $s(x)$ och $t(x)$.

### Översättningar

**divisor** *delare*
**factor** *faktor*
**grestest common divisor (gcd)** *största gemensamma delare (sgd)*
**Euclidean algorithm** *Euklides algoritm*

## 15.7 Faktorisering av polynom i teorin

Analogin till primtal för polynom kallas *irreducibla polynom*. Det är polynom som inte är konstanta, och inte har någon icke-trivial faktorisering, dvs ingen faktorisering där inte ett av polynomen är konstant.

Precis som för heltalen kan man visa att det finns en unik faktorisering av polynom med koefficienter över en kropp i irreducibla faktorer. Här kan vi inte bara kasta om ordningen mellan faktorerna, utan också multiplicera dem med konstanter.

### Översättningar

**irreducible** *irreducibelt*

## 15.8 Factorisering av polynom i praktiken

Även om polynom i den här meningen inte är funktioner kan vi för varje polynom bilda en funktion genom att byta ut $x$ mot element i kroppen där koefficienterna ligger. Vi får då ett sätt att tala om *nollställen* till polynom och vi har faktorsatsen precis som för vanliga polynom, dvs $a$ är ett nollställe till $p(x)$ precis om $x - a$ är en faktor i $p(x)$. Det betyder att vi vid faktorisering av polynom kan finns linjära faktorer genom att sätta in olika värden istället för $x$.

Sats 15.8.2 säger att ett polynom av grad $n$ kan ha högst $n$ nollställen.

En skillnad mot vanliga polynom är att ett polynom nu kan ha nollställen överallt utan att vara nollpolynomet. Exempelvis är polynomet $x(x + 1)$ noll för alla element i $\mathbf{Z}_2$.

Exemplet visar hur vi kan finna en faktorisering av ett fjärdegradspolynom i två irreducibla andragradspolynom.

**Översättningar**

**linear factor** *linjär faktor*
**evaluating** *evaluera, utvärdera*
**polynomial function** *polynomfunktion*
**factor theorem** *faktorsatsen*
**root** *rot*
**quadratic** *kvadratisk, andragrads-*
**cubic** *kubisk, tredjegrads-*