ALGEBRAISKA STRUKTURER

Juliusz Brzezinski

MATEMATISKA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA OCH
GÖTEBORGS UNIVERSITET
GÖTEBORG 2005

FÖRORD

Detta kompendium täcker innehållet i kursen ”Algebraiska strukturer”, men berör mer än man brukar ta upp i kursen. Delar av kompendiet har använts som en del av kompendiet i ”Tillämpade diskreta strukturer”. Några tillämpningar av grupper, ringar och kroppar på kryptering eller kodning finns i den senare texten som också är tillgänglig från min hemsida.

I sin nuvarande form har kompendiet aldrig använts (möjligen av några studenter som läste kursen på egen hand). Av denna anledning finns det säkert olika brister och tryckfel är ganska naturliga. Alla kommentarer om innehållet (synpunkter och rättelser) mottas gärna av författaren: Juliusz Brzezinski (**jub at math. chalmers.se**).

Februari, 2005

Innehåll

Kapitel 1

DELBARHET OCH PRIMTAL

Vi börjar med en kort repetition av några viktiga egenskaper hos **heltalen**:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

(1.1) Definition. Om a och b är två heltal så säger man att b **delar** a om $a = bq$, där q är ett heltal. Man säger också att a är **delbart** med b eller att a är en **multipel** av b. Man skriver då $a|b$. □

Exempel. $3|6$, $641|2^{32}+1$ (det är inte så lätt att bevisa - se dock övning 5.3 i Kapitel 5.) □

Rent allmänt gäller följande viktiga och välkända egenskap:

(1.2) Divisionsalgoritmen. *Om a och b är heltal och $b \neq 0$ så är*

$$a = bq + r, \quad \text{där} \;\; 0 \leq r < |b|.$$

Både q och r är definierade entydigt av a och b.

Bevis. Betrakta alla heltal $a - bx$, där x är ett godtyckligt heltal. Bland dessa tall finns det positiva ty olikheten $a - bx > 0$ har med all säkerhet heltaliga lösningar ($x > a/b$ då $b > 0$ och $x < a/b$ då $b < 0$). Låt r vara det minsta icke-negativa heltalet bland talen $a - bx$ då x är ett heltal och låt $r = a - bq$. Vi påstår att $0 \leq r < |b|$. Annars är, $r \geq |b|$ så att $0 \leq r - |b| < r$ och $r - |b| = a - bq - |b| = a - b(q \pm 1)$ dvs $r - |b|$ är ett icke-negativt tal på formen $a - bx$ som är mindre än r. Detta strider mot definitionen av r. Alltså har vi

$$a = bq + r \quad \text{och} \quad 0 \leq r < |b|.$$

Bevis att q och r definieras entydigt av a och b lämnar vi som övning 1.1. □

(1.3) Definition. Om $a = bq + r$, där $0 \leq r < |b|$ (som i Divisionsalgoritmen ovan) så kallas q **kvoten**, och r **resten** vid division av a med b. □

Ofta utnyttjar man följande egenskaper hos delbarhetsrelationen:

(1.4) Proposition. *Låt a, b, c, d beteckna heltal. Då gäller:*

(a) *om $d|a$ och $d|b$ så $d|a \pm b$,*

(b) *om $a|b$ och $b|c$ så $a|c$,*

(c) *om i likheten $a + b = c$ är två av talen a, b, c delbara med d så är också det tredje talet delbart med d,*

(d) *om $a|b$ och $b|a$ så är $b = \pm a$.*

Alla dessa egenskaper är mycket enkla och vi lämnar ett bevis som övning (se övning 1.2).

Med **största gemensamma delaren** till a och b menar man ett positivt heltal d som delar a och b och är delbart med varje gemensam delare till a och b. Den största gemensamma delaren till a och b är definierad entydigt därför att om både d och d' är sådana delare så gäller $d|d'$ och $d'|d$, vilket innebär att $d' = \pm d$. Men både d och d' är positiva så att $d' = d$. Största gemensamma delaren till a och b betecknas med $SGD(a, b)$. Man brukar definiera $SGD(0, 0) = 0$.

Med **minsta gemensamma multipeln** till a och b menar man ett positivt heltal m som är delbart med a och b och som delar varje gemensam multipel av a och b. Även minsta gemensamma multipeln av a och b definieras entydigt av dessa tal (motivera detta påstående med liknande argument som för $SGD(a, b)$ ovan!). Minsta gemensamma multipeln av a och b betecknas med $MGM(a, b)$. Som för SGD definierar man $MGM(0, 0) = 0$.

Följande egenskap av största gemensamma delaren till två heltal kommer att användas flera gånger under kursens gång.

(1.5) Proposition. *Om a och b är heltal och $d = SGD(a, b)$ så existerar två heltal x_0 och y_0 sådana att*

$$d = ax_0 + by_0.$$

Bevis. Om $a = b = 0$ så är påståendet klart (som x och y kan man välja helt godtyckliga heltal). Anta att a eller b inte är 0. Det är klart att det finns positiva heltal som kan skrivas på formen $ax + by$ t ex om $a \neq 0$ så är $\pm a = a \cdot (\pm 1) + b \cdot 0$ och antingen a eller $-a$ är ett positivt heltal. Även $b = a \cdot 0 + b \cdot 1$ kan skrivas på formen $ax + by$. Låt d_0 vara det minsta positiva heltal som kan skrivas på den önskade formen dvs

$$(*) \qquad d_0 = ax_0 + by_0.$$

Vi påstår att $d_0 = d$. Först observerar vi att varje heltal $ax + by$ är delbart med d_0, ty

$$ax + by = qd_0 + r,$$

där resten r är mindre än delaren d_0. Men

$$r = a(x - qx_0) + b(y - qy_0)$$

så att r måste vara 0 ty annars får man ett tal som är mindre än d_0 och som kan skrivas på den önskade formen. Alltså dividerar d_0 både a och b ty bägge kan skrivas på formen $ax + by$. Ekvationen $(*)$ säger att om d' är en delare till a och b så är d' en delare till d_0. Alltså är d_0 den största gemensamma delaren till a och b. □

Den sista propositionen säger inte hur man kan hitta x och y. För det mesta spelar det inte någon större roll – existensen är helt tillräcklig. Men ibland vill man beräkna x_0 och y_0. Det gör man ofta (och ganska snabbt) med hjälp av **Euklides algoritm**. Euklides algoritm säger hur man kan beräkna $SGD(a, b)$. Man bildar en divisionskedja:

$$\begin{array}{rcll}
a & = & bq_1 + r_1, & 0 \le r_1 < |b|, \\
b & = & r_1q_2 + r_2, & 0 \le r_2 < r_1, \\
r_1 & = & r_2q_3 + r_3, & 0 \le r_3 < r_2, \\
\vdots & & \vdots & \vdots \\
r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1}, & 0 \le r_{n-1} < r_{n-2}, \\
r_{n-2} & = & r_{n-1}q_n + r_n, & 0 \le r_n < r_{n-1}, \\
r_{n-1} & = & r_nq_{n+1}. &
\end{array}$$

Varje kedja av den här typen måste vara ändlig därför att en avtagande kedja av resterna $r_1 > r_2 > r_3 > \ldots \ge 0$ måste vara ändlig. Vi påstår att den sista icke-försvinnande resten i denna kedja, dvs r_n, är den största gemensamma delaren till a och b. Att det verkligen är sant kontrollerar man mycket enkelt med hjälp av definitionen av $SGD(a, b)$. Den sista likheten i kedjan säger att r_n är delaren till r_{n-1}. Alltså visar den näst sista likheten att r_n är delaren till r_{n-2}. Nu vet vi att r_n delar r_{n-1} och r_{n-2}. Alltså visar likheten för r_{n-3} att även denna rest är delbar med r_n. Vi fortsätter vår vandring uppåt och steg efter steg visar vi att alla tal r_{n-1}, r_{n-2}, r_{n-3}, …, r_1, b, a är delbara med r_n. Alltså är r_n en gemensam delare till a och b.

Om nu d är en godtycklig gemensam delare till a och b så visar den första likheten att d delar r_1. Alltså ger den andra likheten att d delar r_2. Då vi vet att d delar r_1 och r_2 så får vi ur den tredje likheten att d också delar r_3. På det sättet får vi att d är en delare till alla tal i sekvensen $a, b, r_1, r_2, r_3, \ldots, r_{n-2}, r_{n-1}, r_n$. Detta visar att r_n är den största gemensamma delaren till a och b. Det är klart att man kan formalisera vårt resonemang genom att använda matematiskt induktion.

Med hjälp av Euklides algoritm kan man inte bara beräkna $SGD(a, b)$ utan också två heltal x, y sådana att $SGD(a, b) = ax + by$. Vi illustrerar detta med ett exempel:

(1.6) Exempel. Låt $a = 2406$ och $b = 654$. Euklides algoritm ger

$$\begin{aligned} 2406 &= 654 \cdot 3 + 444 \\ 654 &= 444 \cdot 1 + 210 \\ 444 &= 210 \cdot 2 + 24 \\ 210 &= 24 \cdot 8 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 \end{aligned}$$

så att $SGD(2406, 654) = 6$ (den sista nollskilda resten). Nu har vi

$$\begin{aligned} 6 &= \underline{24} - \underline{18} \cdot 1 = \underline{24} - (\underline{210} - \underline{24} \cdot 8) \cdot 1 = \\ &= \underline{24} \cdot 9 - \underline{210} = (\underline{444} - \underline{210} \cdot 2) \cdot 9 - \underline{210} = \\ &= \underline{444} \cdot 9 - \underline{210} \cdot 19 = \underline{444} \cdot 9 - (\underline{654} - 444 \cdot 1) \cdot 19 = \\ &= \underline{444} \cdot 28 - \underline{654} \cdot 19 = (\underline{2406} - \underline{654} \cdot 3) \cdot 28 - \underline{654} \cdot 19 = \\ &= \underline{2406} \cdot 28 + \underline{654} \cdot (-103) \end{aligned}$$

□

Det finns en annan möjlighet att beräkna $SGD(a, b)$ då a och b är två heltal. Även om denna möjlighet inte är särskilt praktisk används den flitigt i skolan. Den bygger på faktoruppdelningar av heltal i produkt av primtal.

Man säger att ett positivt heltal p är ett **primtal** om p har exakt två olika delare: 1 och sig självt. Primtalen mindre än 100 är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Följden av primtalen är oändlig. Detta påstående visades för mer än 2000 år sedan av Euklides. Innan vi visar Euklides sats tittar vi närmare på primtalens viktiga roll som byggstenar för alla heltal – varje heltal större än 1 är en produkt av primtal. Vi skall visa detta påstående om en liten stund. Först behöver vi en mycket viktig egenskap hos primtalen:

(1.7) Sats. *En primdelare till en produkt av två heltal är en delare till (minst) en av faktorerna dvs om $p|ab$ så $p|a$ eller $p|b$, då p är ett primtal och a, b är heltal.*

Bevis. Antag att $p \nmid a$. Då är $SGD(p, a) = 1$ därför att p är ett primtal. Enligt (1.5) existerar två heltal x, y sådana att $px + ay = 1$. Om man multiplicerar den likheten med b får man $b = pbx + aby$. Men enligt förutsättningen är $ab = pq$ för ett heltal q. Alltså är $b = p(bx + qy)$ dvs $p|b$. □

Nu kan vi visa satsen om faktoruppdelningar av heltal i produkter av primtal:

(1.8) Aritmetikens fundamentalsats. *Varje heltal större än* 1 *är en entydig produkt av primtal dvs om*

$$n = p_1 p_2 \cdots p_m = p_1' p_2' \cdots p_n',$$

där p_i *och* p_j' *är primtal så är* $m = n$ *och vid en lämplig numrering av faktorerna är* $p_i = p_i'$.

Bevis. Först visar vi med induktion att varje heltal $N > 1$ är en produkt av primtal. Vi börjar med $N = 2$ då vårt påstående gäller. Låt $N > 2$ och antag att varje positivt heltal större än 1 och mindre än N är en produkt av primtal. Låt p beteckna den minsta delaren till N. Det är klart att p är ett primtal, ty motsatsen innebär att p har en delare $d \neq 1, p$ så att $1 < d < p$ och d är en delare till N (se (1.2) (b)) som är mindre än p. Vi har $N = pq$, där $1 \leq q < N$. Men om $q > 1$ så är q en produkt av primtal enligt induktionsantagandet, vilket visar att N också är en sådan produkt.

Entydigheten visar vi med induktion med avseende på summan $s = m + n$. Om $s = 2$ så har vi $m = n = 1$ och $p_1 = p_1'$. Antag att vårt påstående gäller då antalet faktorer är mindre än s och låt

$$p_1 p_2 \cdots p_m = p_1' p_2' \cdots p_n',$$

där $m + n = s$. Primtalet p_m är en delare till produkten till höger så att enligt (1.7) är p_m en delare till en av faktorerna. Genom att eventuellt nummrera om dessa faktorer kan vi anta att $p_m | p_n'$. Men båda dessa tal är primtal så att $p_m = p_n'$. Alltså gäller

$$p_1 p_2 \cdots p_{m-1} = p_1' p_2' \cdots p_{n-1}',$$

och i denna likhet är antalet primfaktorer lika med $s - 2 < s$. Enligt induktionsantagandet är antalet faktorer till vänster lika med antalet faktorer till höger dvs $m - 1 = n - 1$. Alltså är $m = n$. Dessutom kan man numrera faktorerna så att $p_i = p_i'$ då $i = 1, \ldots, n - 1$. □

(1.9) Anmärkning. Ofta kallar man sats (1.7) för aritmetikens fundamentalsats. Även om formuleringen ovan handlar om positiva heltal så kan vi säga rent allmänt att varje heltal $N \neq \pm 1$ är en produkt

$$N = \varepsilon p_1 p_2 \cdots p_n,$$

där p_i är primtal och $\varepsilon = \pm 1$. Eligt aritmetikens fundamentalsats är sådan framställning entydig så när som på faktorernas ordningsföljd. Faktoruppdelningar av liknande typ är kända t ex för polynom. Vi diskuterar både faktoruppdelningar för heltalen och för polynom i ett senare kapitel. □

Nu kan vi bevisa att det finns oändligt många primtal.

(1.10) Euklides sats. *Det finns oändligt många primtal.*

Bevis. Antag att $p_1, p_2, \ldots, p_n$ är alla primtal. Bilda talet

$$N = p_1 p_2 \cdots p_n + 1.$$

Talet N är större än 1 så att det måste vara en produkt av primtal dvs något av primtalen $p_1, p_2, \ldots, p_n$ är en delare till N. Låt oss beteckna en sådan delare med p dvs $N = pq$, där p är ett av primtalen $p_1, p_2, \ldots, p_n$. Alltså är

$$1 = N - p_1 p_2 \cdots p_n = p(q - \frac{p_1 p_2 \cdots p_n}{p}).$$

Detta betyder att p dividerar 1, vilket är helt orimligt därför att p som ett primtal är större än 1. Vårt antagande att det endast finns ändligt många primtal har lett oss till en motsägelse. Alltså måste antagandet vara falskt dvs det finns oändligt många primtal. □

ÖVNINGAR

1.1. Visa att kvoten och resten vid division av två heltal är entydigt definierade dvs om $a = bq + r = bq' + r'$, där $a, b \neq 0, q, r, q', r'$ är heltal och $0 \leq r < |b|, 0 \leq r' < |b|$, så är $q = q'$ och $r = r'$.

1.2. Visa Proposition (1.4).

1.3. Faktoruppdela följande tal i produkt av primtal:

(a) 2704, (b) 392688, (c) 749088.

1.4. Beräkna $SGD(a, b)$ samt två heltal x och y sådana att $SGD(a, b) = ax + by$ då

(a) $a = 577, b = 257$,

(b) $a = 1111, b = 1133$.

1.5. Låt a och b vara två heltal. Visa att $SGD(a, b)MGM(a, b) = ab$.

Kapitel 2

RELATIONER

Begreppet ”relation” i matematiska sammanhang anknyter till betydelsen av samma ord i vardagliga situationer då en relation är ofta ett samband mellan två individer (dvs ett par).

(2.1) Definition. Med en **relation** R på en mängd X menas en godtycklig mängd bestående av par (x, y), där $x, y \in X$. Med andra ord är en relation på X en godtycklig delmängd R till den kartesiska produkten

$$X \times X = \{(x, y) : x, y \in X\}.$$

□

Om $x, y \in X$ och $(x, y) \in R$, där R är en relation på X så skriver man ofta $x \sim y$. Men ”$\sim$” ersätts oftast med andra tecken som traditionellt betecknar kända relationer t ex med ”$\leq$” eller ”$|$”.

(2.2) Exempel. (a) Låt $X = \{1, 2, 3, 4\}$ och låt $R = \{(1, 3), (2, 4), (2, 2), (4, 4)\}$. Man kan skriva $1 \sim 3$ eller $2 \sim 2$. Man har sammanlagt 16 par (x, y), men endast 4 par ingår i relationen R.

(b) Låt $X = \mathbb{R}$ vara mängden av de reella talen. Definiera $R = \{(x, x^2) : x \in \mathbb{R}\} \subset X \times X$. Relationen R är helt enkelt grafen av funktionen $f(x) = x^2$ dvs den består av alla punkter på parabeln $y = x^2$. Här har vi $x \sim y$ precis då $y = x^2$. □

Ett så allmänt relationsbegrepp är inte särskilt användbart. Men i matematiska situationer har man överallt olika relationer som satisfierar olika ytterligare villkor. Vi diskuterar först ekvivalensrelationer och därefter, mycket kort, ordningsrelationer och funktionsgrafer.

(2.3) Definition. En relation ”$\sim$” på en mängd X kallas för en **ekvivalensrelation** om

(a) $x \sim x$ (reflexivitet),

(b) $x \sim y$ implicerar $y \sim x$ (symmetri),

(c) $x \sim y$ och $y \sim z$ implicerar $x \sim z$ (transitivitet),

då $x, y, z \in X$. □

(2.4) Exempel. (a) Låt $X = \mathbb{Z}$ och låt $x \sim y$ då och endast då $5 \mid x - y$ för $x, y \in \mathbb{Z}$. Då gäller $x \sim x$, ty $5|x - x = 0$, $x \sim y$ implicerar $y \sim x$, ty $5|x - y$ implicerar $5|y - x = -(x - y)$ samt $x \sim y$ och $y \sim z$ ger $x \sim z$, ty $5|x - y$ och $5|y - z$ ger $5|x - z = (x - y) + (y - z)$.

(b) Låt $X = \mathbb{N} = \{1, 2, \ldots\}$ och låt $x \sim y$ då och endast då x och y har exakt samma primtalsdelare. Man kontrollerar mycket lätt att " $\sim$ " är en ekvivalensrelation (gör det!).

(c) Låt X vara en mängd och låt X_i vara icke-tomma delmängder till X för i tillhörande en indexmängd I. Låt oss anta att dessa mängder utgör en **partition** av X, vilket betyder att $X = \cup X_i$ är unionen av alla X_i och X_i är parvis disjunkta dvs $X_i \cap X_j = \emptyset$ om $i \neq j$. Definiera nu $x \sim y$ om och endast om det finns i så at $x, y \in X_i$. Man får en ekvivalensrelation på X. Man kan tänka på X som mängden av alla elever i en skola medan X_i betecknar alla elever i samma klass (vi förutsätter att skolan är av "gammal modelså att varje elev tillhör exakt en klass). Två elever x och y är relaterade (dvs $x \sim y$) precis då x och y går i samma klass. Vi visar strax att varje ekvivalensrelation på en godtycklig mängd X får man på detta sätt. □

(2.5) Definition. Låt $\sim$ vara en ekvivalensrelation på en mängd X. Med ekvivalensklassen av $x \in X$ menas mängden

$$[x] = \{y \in X : y \sim x\}.$$

□

(2.6) Proposition. (*a*) $x \in [x]$.

(*b*) $[x] = [y] \Leftrightarrow x \sim y$.

(*c*) *Två olika ekvivalensklasser är disjunkta.*

(*d*) X *är unionen av alla ekvivalensklasser.*

Bevis. (a) Klart från (2.3) (a).

(b) $[x] = [y] \Rightarrow x \in [x] = [y] \Rightarrow x \sim y$. Antag nu att $x \sim y$. Om $z \in [x]$ så ger $z \sim x$ och $x \sim y$ att $z \sim y$ så att $z \in [y]$. Alltså är $[x] \subseteq [y]$. Av symmetriskäl har man också $[y] \subseteq [x]$.

(c) Om $z \in [x] \cap [y]$ så är $z \sim x$ och $z \sim y$ så att $x \sim y$ ur symmetrin och transitiviteten ($z \sim x$ ger $x \sim z$ som med $z \sim y$ ger $x \sim y$). Enligt (b) är $[x] = [y]$. Detta betyder att om $[x] \neq [y]$ så saknar dessa klasser något gemensamt element z.

(d) Följer direkt ur (a). □

(2.7) Följdsats. *Ekvivalensklasserna av varje ekvivalensrelation på* X *bildar en partition av* X.

Bevis. Följer omedelbart från (c) och (d) i (2.6). □.

(2.8) Exempel. (a) För ekvivalensrelationen i (2.4) (a) har man

$$[x] = [r],$$

där r är resten vid division av x med 5 ty $5|x - r$ dvs $x \sim r$. Eftersom det finns 5 olika rester r så finns det exakt 5 olika ekvivalensklasser [0], [1], [2], [3], [4].

(b) I exempel (2.4) (c) är alla ekvivalensklasser av följande form: $[x] = [p_1 p_2 \cdots p_r]$, där $p_1, p_2, \ldots, p_r$ är alla olika primdelare till x om $x \neq 1$ och [1] (bestående av enbart 1). Kontrollera detta påstående!

(c) I exempel (2.4) (c) är just partitionsmängderna X_i ekvivalensklasserna, ty om x tillhör X_i så är $[x] = X_i$. □

Mängden av alla ekvivalensklasser för en ekvivalensrelation " $\sim$ " på X betecknas med $X/\sim$. Denna mängd kallar man ofta för X **modulo** $\sim$.

En annan mycket vanlig typ av relationer är ordningsrelationer.

(2.9) Definition. En relation " $\leq$ " på en mängd X kallas en **partiell ordningsrelation** (eller en **partiell ordning**) om

(a) $x \leq x$ (reflexivitet),

(b) $x \leq y$ och $y \leq z$ implicerar att $x \leq z$ (transitivitet),

(c) $x \leq y$ och $y \leq x$ implicerar att $x = y$ (antisymmetri).

Man skriver $x < y$ om $x \leq y$ och $x \neq y$. Om dessutom en relation " $\leq$ " satisfierar

(d) för godtyckliga $x, y \in X$ gäller det att $x < y$ eller $y < x$ eller $x = y$

så säger man att relationen är en **ordningsrelation** (eller en **ordning** på X). □

(2.10) Exempel. (a) Låt $X = \mathbb{R}$ och låt $X \leq y$ betecknar den vanliga ordningsrelationen på de reella talen. Vi vet mycket väl att den relationen är en ordningsrelation i enlighet med definitionen ovan.

(b) Låt $X = \mathbb{N} = \{1, 2, 3, \ldots\}$ vara mängden av de naturliga talen. Relationen $x|y$ är en partiell ordningsrelation på $\mathbb{N}$ ty $x|x$, om $x|y$ och $y|z$ så $x|z$ samt $x|y$ och $y|x$ ger $x = y$. Men "|" är inte en ordningsrelation, ty (d) i definitionen ovan gäller inte då man t ex väljer $x = 2$ och $y = 3$. □

(2.11) Vi avslutar med en observation att varje funktion $f : X \to X$ definierar en relation – nämligen mängden av alla par $(x, f(x)) \in X \times X$. Låt oss påminna att med en funktion från en mängd X till en mängd Y menar man vanligen en regel som mot varje $x \in X$ ordnar exakt ett element $y \in Y$. Då skriver man $y = f(x)$ och $f : X \to Y$. I vårt fall har vi $X = Y$

och vi får en relation på X då $x \sim y$ om och endast om $y = f(x)$. Parmängden som svarar mot f består alltså av alla par $(x, f(x))$.

$$\Gamma_f = \{(x, f(x)) : x \in X\}$$

kallas ofta **grafen** av funktionen f.

ÖVNINGAR

2.1. Vilka av de följande relationerna på den givna mängden X är ekvivalensrelationer:

(a) $X = \mathbb{Z}$, $x \sim y$ då och endast då $n|x - y$, där n är ett fixt positivt heltal.

(b) $X = \mathbb{N}$, $x \sim y$ då och endast då xy är en kvadrat av ett naturligt tal.

(c) $X = \mathbb{R}^2$, $(a, b) \sim (c, d)$ då och endast då $b = d$.

(d) $X = \mathbb{R}^2$, $(a, b) \sim (c, d)$ då och endast då $a = c$ eller $b = d$.

(e) $X = \mathbb{R}$, $a \sim b$ då och endast då $a - b$ är ett heltal.

(f) $X = \mathbb{R}$, $a \sim b$ då och endast då $ab > 0$.

2.2. Är det sant att reflexivitet i definitionen av en ekvivalensrelation följer ur symmetrin och transitivitet enligt följande resonemang: Låt $x \in X$. $x \sim y$ ger $y \sim x$ eftersom " $\sim$ " är symmetrisk. Alltså ger transitiviteten $x \sim x$.

2.3. Bestäm ekvivalensklasserna i alla fall då relationerna i den första övningen är ekvivalensrelationer. Försök tolka ekvivalensklasserna geometriskt då sådana tolkningar är möjliga.

2.4. Vilka av följande relationer på de givna mängderna X är partiella ordningsrelationer? Vilka av dem är ordningsrelationer?

(a) $X = \mathbb{R}$, $a \sim b$ då och endast då $a^2 \leq b^2$.

(b) $X = \mathbb{N}$, $a \sim b$ då och endast då $a^2|b^2$.

(c) $X =$ alla reella funktioner $f : \mathbb{R} \to \mathbb{R}$ och $f \sim g$ då och endast då $f(x) \leq g(x)$ för varje $x \in \mathbb{R}$.

Kapitel 3

MÄNGDER MED OPERATIONER

De fyra räknesätten: addition, subtraktion, multiplikation och division är, vad man ofta kallar, (aritmetiska) operationer i mängden av alla tal. Addition och multiplikation av vanliga funktioner kända från analyskurser är också operationer. Även matrisaddition eller matrismultiplikation är operationer i mängden av matriser av lämplig storlek.

I algebran är man ofta intresserad av olika egenskaper hos operationer. Två mängder som tillåter operationer med samma egenskaper kan ofta studeras samtidigt – man behöver inte bevisa samma satser flera gånger om man vet att dessa satser gäller för varje mängd med operationer som satisfierar vissa villkor. I detta avsnitt definierar vi begreppet operation och några mycket allmänna egenskaper hos operationer t ex associativiteten och kommutativiteten.

Begreppet operation är ett specialfall av begreppet funktion. Därför repeterar vi först att med en funktion f från en mängd X till en mängd Y menar man vanligen en regel som till varje $x \in X$ ordnar exakt ett element $y \in Y$. Då skriver man $y = f(x)$ och $f : X \to Y$. Låt oss också repetera att $X \times Y$ betecknar (den kartesiska) produkten av mängderna X och Y dvs

$$X \times Y = \{(x, y) : x \in X \text{ och } y \in Y\}.$$

Nu är vi beredda att definiera begreppet operation:

(3.1) Definition. Med en **(binär) operation** på mängden M menar man en avbildning från $M \times M$ till M. Bilden av paret (a, b) betecknas ofta med $a * b$, och mängden M med operationen "$*$" med $(M, *)$. □

Definitionen säger att en operation på M ordnar mot två godtyckliga element $a, b \in M$ ett element $a * b \in M$. Här följer några exempel på operationer:

(3.2) Exempel. (a) Låt M vara en av mängderna $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ och låt $a * b = a + b$ vara den vanliga summan av a och b.

(b) Med samma M som i (a), låt $a * b = ab$ vara den vanliga produkten av a och b.

(c) Låt $M = M_2(\mathbb{R})$ vara mängden av (2×2)-matriser med reella element och $A * B = AB$ den vanliga matrisprodukten för $A, B \in M_2(\mathbb{R})$.

(d) Låt M vara mängden av alla reella funktioner och $f * g = f + g$ den vanliga summan av två funktioner $f, g \in M$ dvs $(f + g)(x) = f(x) + g(x)$ då $x \in \mathbb{R}$. □

Enbart det faktum att man har en operation på en mängd är oftast inte tillräckligt för att studera mängden. Därför vill man veta lite mera om olika egenskaper hos operationer.

(3.3) Definition. Man säger att operationen $*$ på M är **associativ** om $(a*b)*c = a*(b*c)$ då $a, b, c \in M$. Operationen är **kommutativ** om $a * b = b * a$ då $a, b \in M$. □

Exempel. (a) Alla operationer i Exempel (3.2) är associativa och enbart (3.2)(c) är inte kommutativ.

(b) Subtraktionen är varken kommutativ eller associativ på $\mathbb{Z}$ dvs om $a*b = a-b$ så gäller inte att $a*b = b*a$ eller $(a*b)*c = a*(b*c)$ ty vanligen $a-b \neq b-a$ och $(a-b)-c \neq a-(b-c)$. Bästa sättet att visa dessa påståenden är att ge exempel: t ex $2-3 \neq 3-2$ och $(3-2)-1 \neq 3-(2-1)$. □

(3.4) Definition. Man säger att $e \in M$ är ett **neutrallt element** för operationen $*$ om $e*a = a*e = a$ då $a \in M$. Man säger att $a' \in M$ är en **invers** till $a \in M$ om $a*a' = a'*a = e$. □

Exempel. (a) 0 är ett neutralt element för additionen på $M = \mathbb{Z}$ (eller $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) ty $0 + a = a + 0 = a$ då $a \in M$. Inversen till $a \in M$ är $-a$ ty $a + (-a) = (-a) + a = 0$. Inversen kallas här motsatta talet.

(b) Talet 1 är ett neutralt element för multiplikationen på M ur (a) ty $1 \cdot a = a \cdot 1 = a$ då $a \in M$. Inversen till $a \in M$ finns enbart då $a' = 1/a \in M$. Om $M = \mathbb{R}$ så har alla tal invers utom 0. Om $M = \mathbb{Z}$ så har enbart $a = \pm 1$ inversen (motivera varför!).

(c) Nollmatrisen

$$\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

är ett neutralt element för matrisadditionen på $M = M_2(\mathbb{R})$. Inversen till $A \in M$ är då $-A$ ty $A + (-A) = (-A) + A = \mathbf{0}$. I stället för invers säger man då den motsatta matrisen. Enhetsmatrisen

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

är ett neutralt element för matrismultiplikationen ty $EA = AE = A$ då $A \in M$. Inversen till $A \in M$ är $A' = A^{-1}$ om $\det A \neq 0$. Om $\det A = 0$ så saknar A invers (om $AA' = E$ så ger $\det(AA') = \det A \det A' = \det E = 1$ en motsägelse $0 = 1$ om $\det A = 0$). □

(3.5) Proposition. *Ett neutralt element $e \in M$ är entydigt bestämt. Om operationen på M är associativ och $a \in M$ har invers så är den entydig.*

Bevis. Om e' också är ett neutralt element så har vi

$$e' = e * e' = e.$$

Låt a_1' vara också en invers till a. Då gäller

$$a_1' = a_1' * e = a_1' * (a * a') = (a_1' * a) * a' = e * a' = a'.$$

□

(3.6) Anmärkning. Om $M = \{a_1, a_2, \ldots, a_n\}$ är en ändlig mängd så definierar man ofta operationer på M med hjälp av **"multiplikationstabeller"**:

$*$	a_1	$\ldots$	a_j	$\ldots$	a_n
a_1					
$\vdots$					
a_i			$a_i * a_j$		
$\vdots$					
a_n					

Varje sådan tabell ger en operation på M. Med hjälp av tabellen kan man lätt avgöra om operationen på M är kommutativ (hur?) eller om det finns ett neutralt element (hur?). Men det är mycket besvärligare att avgöra om operationen är associativ (se övningar). □

ÖVNINGAR

3.1. Vilka av följande operationer på $\mathbb{Z}$ är associativa, kommutativa, vilka har ett neutralt element? Varje gång då det finns ett neutralt element bestäm alla element som har invers.

(a) $m * n = mn + 1$
(b) $m * n = mn + m + n$
(c) $m * n = m^2 + n^2$
(d) $m * n = 2$
(e) $m * n = 2^{mn}$
(f) $m * n = SGD(m, n)$
(g) $m * n = \max(m, n)$
(h) $m * n = MGM(m, n)$

3.2. Hur många operationer finns det på en mängd med n element? Hur många av dessa är kommutativa?

3.3. Ge exempel på en mängd med en operation som är

(a) associativ, men ej kommutativ;

(b) kommutativ, men ej associativ.

3.4. Låt M vara en mängd med en operation $*$ och med ett neutralt element e. Visa att om

$$a * (b * c) = (a * c) * b \quad \text{för} \quad a, b, c \in M$$

så är operationen $*$ kommutativ och associativ.

3.5. (svårt?) Låt M vara en mängd med en operation $*$ sådan att

$$a * a = a \quad \text{och} \quad (a * b) * c = (a * c) * a$$

för $a, b, c \in M$. Visa att operationen är kommutativ och associativ.

Kapitel 4

GRUPPER: DEFINITIONER OCH EXEMPEL

En grupp är en mängd med en operation som uppfyller några mycket enkla villkor. Dessa enkla villkor leder till en mycket rik och intressant teori som har tillämpningar i hela matematiken och andra naturvetenskapliga ämnen (fysik, kemi). Grupper trädde in i matematiken redan under 1700-talet även om en formell definition av gruppbegreppet formulerades betydligt senare. Olika konkreta grupper studerades redan av L. Euler (restgrupper) och J. Lagrange som först introducerade begreppet permutationsgrupp. E. Galois visade hur man kan använda permutationsgrupper för att lösa viktiga och, under hans tid, mycket svåra problem i teorin för algebraiska ekvationer. Men den moderna definitionen av begreppet grupp gavs 1870 av L. Kronecker.

(4.1) Definition. Låt G vara en mängd och låt $*$ vara en operation på G dvs

(0) $a * b \in G$ då $a, b \in G$ (slutenhet).

Man säger att $(G, *)$ är en **grupp** om

(1) $(a * b) * c = a * (b * c)$ då $a, b, c \in G$ (associativitet),

(2) det finns $e \in G$ så att $e * a = a * e = a$ då $a \in G$ (neutralt element),

(3) till varje $a \in G$ finns $a' \in G$ så att $a * a' = a' * a = e$ (invers). □

Observera att i varje grupp finns det endast ett neutralt element. Om både e och e' är neutrala, så är $e = e * e' = e'$ enligt (2). Man visar också mycket enkelt att varje element $a \in G$ endast har en invers – om både a' och a'' är inversa element till $a \in G$ så har man:

$$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e * a' = a'.$$

(4.2) Exempel. (a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ är grupper. Om man utelämnar 0 ur $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ får man grupper med avseende på multiplikation. Det hjälper inte att utelämna 0 ur $\mathbb{Z}$ för att

få en grupp med avseende på multiplikation därför att t ex heltalet 2 saknar heltalig invers (inversen i $\mathbb{Z}$ enbart existerar för ± 1).

(b) Alla $(n \times n)$-matriser med reella element och med determinant $\neq 0$ bildar en grupp med avseende på matrismultiplikation. Denna grupp har en standard beteckning $GL_n(\mathbb{R})$. Vi har

$$A, B \in GL_n(\mathbb{R}) \Rightarrow \det A \neq 0 \neq \det B \Rightarrow \det(AB) = \det A \cdot \det B \neq 0 \Rightarrow AB \in GL_n(\mathbb{R}),$$

vilket visar slutenheten. Associativiteten $(AB)C = A(BC)$ då $A, B, C \in GL_n(\mathbb{R})$ är en välkänd egenskap hos matrismultiplikation. Om E betecknar $(n \times n)$-enhetsmatrisen så är $EA = AE = A$ då $A \in GL_n(\mathbb{R})$ dvs E är det neutrala elementet. Slutligen $AA^{-1} = A^{-1}A = E$ om $A \in GL_n(\mathbb{R})$ dvs A^{-1} är inversen till A (observera att $\det A \neq 0$ så att inversen A^{-1} existerar).

(c) Låt $G = \{1, -1\}$ med vanlig multiplikation. G är en grupp med följande multiplikationstabell:

$\cdot$	1	-1
1	1	-1
-1	-1	1

□

(4.3) Anmärkning. En multiplikationstabell för en ändlig grupp (som ovan) kallar man ofta för **grupptabell** eller **Cayleys tabell**. Det är inte lätt att avgöra om en operation på en ändlig mängd G definierar en grupp genom att studera grupptabellen:

$*$	$a_1 \ \ldots$	$a_j \ \ldots$	a_n
a_1	$a_1 \ \ldots$	$a_j \ \ldots$	a_n
$\vdots$			
a_i	$a_i \ \ldots$	$a_i * a_j \ \ldots$	
$\vdots$			
a_n	a_n		

Genom en inspektion av multiplikationstabellen inser man lätt om mängden är sluten med avssende på operationen – slutenheten innebär att varje element i tabellen tillhör mängden G. Det är också lätt att upptäcka om det finns ett neutralt element: om $a_1 = e$ är det neutrala elementet så är de första två raderna och kolonnerna identiska. Man kan se enkelt om varje element har invers – varje rad och varje kolonn måste innnehålla e. I själva verket är det så att varje rad och varje kolonn är en omkastning av den första raden (eller kolonnen). Detta följer ur en mycket enkel observation i nästa proposition. Men att kontrollera att operationen är associativ är inte lika lätt. □

(4.4) Proposition. *Låt G vara en grupp och $a, b, c \in G$. Då gäller strykningslagarna:*

(a) $a * c = b * c \Rightarrow a = b$,

(b) $c * a = c * b \Rightarrow a = b$.

Bevis. Vi visar (a). Multiplicera från vänster med inversen a' till a. Tack vare associativiteten får vi att $a' * a * b = a' * a * c$ ger $e * b = e * c$ dvs $b = c$. □

(4.5) Anmärkning. En rad i tabellen ovan består av produkterna $a_i * a_1, \ldots a_i * a_j, \ldots, a_i * a_n$. Alla dessa produkter ger olika element i G därför att likheten $a_i * a_j = a_i * a_k$ ger att $a_j = a_k$ enligt strykningsegenskapen ovan. □

(4.6) Definition. Man säger at gruppen $(G, *)$ är **abelsk** (= kommutativ) om $a * b = b * a$ då $a, b \in G$. □

Exempel. Alla grupper i (4.2) (a) är abelska. Gruppen i (4.2) (b) är icke-abelsk då $n \geq 2$ ty vanligen $AB \neq BA$ för två $(n \times n)$-matriser. □

(4.7) Definition. Antalet element i en ändlig grupp kallas **gruppens ordning** och betecknas $o(G)$ (eller $|G|$). Om G inte är ändlig säger man att G har oändlig ordning och skriver $o(G) = \infty$. □

(4.8) Anmärkning. (a) När man definierar en grupp så beskriver man mängden G av dess element och gruppoperationen $*$. Formelt borde man säga att $(G, *)$ är en grupp. Icke desto mindre säger man oftast at G är en grupp.

(b) Vi vet redan att symbolen "$*$" som betecknar en operation kan tolkas på olika sätt. När det gäller beteckningar finns det två vanliga typer som dels beror på traditionen dels på bekvämligheten. Det är säkert bekvämare att skriva ab i stället för $a * b$. Då säger man om **multiplikativ notation**. Inversen betecknas då med a^{-1}. Ibland är denna notation inte helt naturlig, speciellt när gruppoperationen är addition. Då använder man **additiv notation** dvs man tolkar "$*$" som "$+$". Villkoren (0) - (3) i (4.1) har då följande form:

(0) $a, b \in G \Rightarrow a + b \in G$

(1) $(a + b) + c = a + (b + c)$ då $a, b, c \in G$.

(2) Det finns $e \in G$ så att $e + a = a + e = a$ (man skriver ofta $e = 0$).

(3) Till varje $a \in G$ finns $a' \in G$ så att $a + a' = a' + a = e$ (man skriver ofta $a' = -a$). □

I exempel (4.2) har vi ett antal grupper med avseende på addition:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Man säger då att $\mathbb{Z}$ är en delgrupp till $\mathbb{Q}$ (eller $\mathbb{R}$ eller $\mathbb{C}$), $\mathbb{Q}$ är en delgrupp till $\mathbb{R}$ (eller $\mathbb{C}$) osv. Formellt har vi:

(4.9) Definition. Låt $H \subseteq G$. Man säger att H är en **delgrupp** till G om elementen i H bildar en grupp med avseende på operationen i G. □

(4.10) Proposition. *Låt $H \subseteq G$. H är en delgrupp till G då och endast då*

(a) $a, b \in H \Rightarrow a * b \in H$,

(b) $e \in H$,

(c) $a \in H \Rightarrow a^{-1} \in H$.

Bevis. Se övn. 4.7. □

(4.11) Cykliska grupper Låt G vara en grupp och $g \in G$. Elementet g definierar en delgrupp till G – den minsta delgrupp till G som innehåller g. Den måste innehålla ala potenser av G dvs $g, gg, ggg, \ldots$, deras inverser $g^{-1}, g^{-1}g^{-1}, g^{-1}g^{-1}g^{-1}, \ldots$ och e. Vi betecknar med g^n produkten $gg \ldots g$ av n stycken faktorer g, med g^{-n} potensen $(g^{-1})^n$, och med g^0 elementet e. Man visar lätt likheten $g^m g^n = g^{m+n}$ för godtyckliga hela m och n. Potenserna g^n, $n \in \mathbb{Z}$, bildar en delgrupp till G som innehåller g. Den betecknas med $< g >$ och kallas **den cykliska gruppen genererad av** g. Antalet element i $< g >$ kallas **ordningen av** g och beteckas $o(g)$. Ibland händer det att $G =< g >$. Då säger man att G är en **cyklisk grup** och g är dess generator. Då är $G = \{g^n : n \in \mathbb{Z}\}$. Observera att med den additiva notationen måste man ersätta g^n med $ng\,(= g + \ldots + g$ då $n > 0)$. Ordet "potens" ersätter man då med "multipel".

Exempel. (a) Låt $G = \mathbb{C}^*$ vara gruppen av de komplexa talen med avseende på multiplikation. Om $g = i$ så får vi

$$i = 1,\ i^1 = i,\ i^2 = -1,\ i^3 = -1,\ i^4 = 1,\ i^5 = i,\ i^6 = -1, \ldots$$

osv så att vi endast får 4 olika tal. Å andra sidan är $i^{-1} = i^3$ så att varje negativ potens är lika med en positiv $(i^{-1})^n = i^{3n}$. Alltså får man $< i >= \{1, i, -1, -i\}$. Termen cyklisk förklaras delvis av detta exempel – likheten $i^4 = 1$ medför att vi får en cyklisk upprepning av potenserna $i^5 = i, i^6 = i^2, i^7 = i^3, i^8 = 1$ osv.

(b) Låt $G = \mathbb{Z}$ med addition och $g = 1$. Då är $< 1 >$ mängden av alla multipler $n \cdot 1$ (t ex $2 \cdot 1 = 1 + 1, 3 \cdot 1 = 1 + 1 + 1$, $-2 \cdot 1 = -(1 + 1)$ osv). Alltså är $< 1 >= \mathbb{Z}$ så att $\mathbb{Z}$ är en oändlig cyklisk grupp □.

Anmärkning. Termen "cyklisk"kan te sig lite egendomlig om man konstaterar att $\mathbb{Z}$ är en cyklisk grupp. Terminologin är historisk motiverad – från början studerade man enbart ändliga grupper för vilka begreppet "cyklisk"är helt klart (se också nästa proposition). □

Man kan ge en helt allmän beskrivning av cykliska grupper:

(4.12) Proposition. *Låt G vara en grupp och $g \in G$.*

(a) *Om $o(g) = n$ så är $< g >= \{e, g, g^2, \ldots, g^{n-1}\}$ och $g^n = e$ (dvs n är den minsta positiva exponent sådan att $g^n = e$).*

(b) *Om $o(g) = \infty$ så är alla potenser g^n, $n \in \mathbb{Z}$, olika.*

Bevis. Antag att $g^m = e, m > 0$. Då finns det högst m olika potenser av g, nämligen $g^0 = e, g, g^2, \ldots, g^{m-1}$, ty om $N = mq + r$ med $0 \leq r < m$, så är $g^N = g^{mq+r} = (g^m)^q g^r = g^r$. Detta betyder att varje potens av g är lika med en av potenserna $e, g, g^2, \ldots, g^{m-1}$.

(a) $o(g) = n$ betyder att det finns n olika potenser av g. Vi påstår att just $g^0 = e, g, g^2, \ldots, g^{n-1}$ är olika ty $g^i = g^j, 0 \leq i < j < n$ ger att $g^{j-i} = e$, där $j - i = m < n$. Men likheten $g^m = e$ med $0 < m < n$ är omöjlig (om $g^m = e$ så finns det endast m olika potenser av g). Alltså är $< g >= \{e, g, g^2, \ldots, g^{n-1}\}$. g^n är lika med någon av dessa potenser. Men $g^n = g^i$ där $0 < i < n$ ger $g^{n-i} = e$, dvs $g^m = e$ med $m = n - i < n$. En sådan likhet är utesluten så att $g^n = g^0 = e$.

(b) Om $o(g) = \infty$ så måste alla potenser $g^n, n \in \mathbb{Z}$, vara olika ty $g^i = g^j$ för $i < j$ ger $g^m = e$ där $m = j - i > 0$, vilket är omöjligt (enligt första stycket i beviset). □

Vi avslutar detta kapitel med en mycket allmän konstruktion som möjliggör att definiera nya grupper med hjälp av sådana som man redan känner.

(4.13) Exempel. Låt $G_1, G_2, \ldots, G_n$ vara godtyckliga gruper. Vi definierar en ny grupp $G_1 \times G_2 \times \ldots \times G_n$ vars element är $(g_1, g_2, \ldots, g_n)$, där $g_i \in G_i$ för $i = 1, 2, \ldots, n$. Operationen är definierad på följande sätt:

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$$

Det är klart at den operationen är associativ (man multiplicerar ju i varje grupp G_i separat). Det neutrala elementet är $e = (e_2, e_2, \ldots, e_n)$ där e_i är det neutrala elementet i G_i. Inversen till $(g_1, g_2, \ldots, g_n)$ är $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. Gruppen $G_1 \times G_2 \times \ldots \times G_n$ kallas **direkta produkten** av G_i. Om $G_1 = G_2 = \ldots = G_n = G$ skriver man G^n.

Om tex $G = \mathbb{R}$ är gruppen av de reella talen med addition så är $\mathbb{R}^2 = \{(r_1, r_2) : r_1, r_2 \in \mathbb{R}\}$ med koordinatvis addition. $\mathbb{R}^2$ kan tolkas som gruppen av alla vektorer i planet. På samma sätt är $\mathbb{R}^3$ gruppen av alla vektorer i rymden. Om t ex $G = \{1, -1\}$ med multiplikation så består $G \times G$ av $(1, 1), (1, -1), (-1, 1), (-1, 1)$ med koordinatvis multiplikation. □

ÖVNINGAR

4.1. Vilka av följande talmängder är grupper med avseende på multiplikaton av tal ?

(a) $\mathbb{Q}^*$ = alla rationella tal $\neq 0$, (b) $\mathbb{Z} \setminus \{0\}$ = alla heltal $\neq 0$,

(c) $\mathbb{C}^*$ = alla komplexa tal $\neq 0$, (d) $U = \{z \in \mathbb{C} : |z| = 1\}$,

(e) $\mathbb{R}_{>0}$ = positiva reella tal, (f) $G = \{2^m 3^n, m, n \in \mathbb{Z}\}$.

4.2. Visa att följande talmängder är grupper med avseende på multiplikation av tal:

(a) $C_n = \{z \in \mathbb{C} : z^n = 1, n \text{ ett fixt positivt heltal}\}$ (alla n:te enhetsrötter),

(b) $C_\infty = \{z \in \mathbb{C} : z^n = 1 \text{ för något } n \geq 1\}$.

4.3. Bestäm ordningarna av matriserna:

(a) $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, (b) $B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, (c) $C = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$

i gruppen av alla (2×2)-matriser med determinant $\neq 0$ med avseende på multiplikation (dvs i $GL_2(\mathbb{R})$).

4.4. Låt G vara en grupp och $a, b \in G$. Visa att

(a) $(a^{-1})^{-1} = a$, (b) $(ab)^{-1} = b^{-1}a^{-1}$.

4.5. Visa att G är en abelsk grupp då och endast då $(ab)^{-1} = a^{-1}b^{-1}$ för $a, b \in G$.

4.6. Visa att G är en abelsk grupp då och endast då $(ab)^2 = a^2b^2$ för $a, b \in G$.

4.7. Visa Proposition (4.10).

4.8. Låt H vara en icke-tom ändlig delmängd till en grupp G sådan at $h, h' \in H$ implicerar $hh' \in H$. Visa att H är en delgrupp till G.

4.9. Visa att om ordningen av en grupp G är jämn så finns det ett element $g \in G$ av ordningen 2.

4.10. Låt $G =< a >= \{e, a, \ldots, a^{n-1}\}$, där $a^n = e$.

(a) Visa att $G =< a^k >$ då och endast då $SGD(k, n) = 1$.

(b) Visa at om $H \subseteq G$ och $o(H) = m$ så är $H =< a^d >$ där $d = \frac{n}{m}$.

Ledning. Visa att d är det minsta positiva heltalet sådant att $a^d \in H$ om $H \neq< e >$.

4.11. Visa att varje delgrupp till en cyklisk grupp är cyklisk.

Ledning. Utnyttja övn. 4.10.

4.12. Låt G vara en grupp och A en icke-tom delmängd till G. Visa at den minsta delgrupp till G som innehåller A är

$$< A >= \{a_1 a_2 \ldots a_n : a_i \in A \quad \text{eller} \quad a_i^{-1} \in A \quad \text{och} \quad n \geq 1\}$$

Anmärkning. Om $G =< A >$ så säger man att A är ett generatorsystem för G. Om $A = \{a\}$ så är $< A >=< a >$ den cykliska gruppen genererad av a.

Kapitel 5

RESTGRUPPER

Grupper av rester vid division med naturliga tal är troligen de första exemplen på grupper som har använts i matematiska sammanhang. De har mycket intressanta tillämpningar både i talteorin och t ex i samband med konstruktioner av både koder och krypteringssystem som kommer att diskuteras i fortsättningen av kursen.

Låt n vara ett positivt heltal. Vi skall beteckna med $[a]_n$ resten av ett heltal a vid division med n. T ex är $[11]_5 = 1, [8]_3 = 2$ osv. Vi har:

$$[a]_n = [b]_n \quad \text{då och endast då} \quad n|a-b$$

(se övning 5.4). Likheten $[a]_n = [b]_n$ skriver man ofta som

$$a \equiv b \pmod{n}.$$

Man säger då att a **och** b **är kongruenta modulo** n. Den beteckningen är mycket vanlig och introducerades av C. F. Gauss. Uttrycket $a \equiv b \pmod{n}$ kallas **kongruens**.

Mängden av alla rester vid division med n kommer att betecknas med $\mathbb{Z}_n$. T ex är $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ och allmänt $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Resterna vid division med n kan adderas och multipliceras på följande sätt:

$$r_1 \underset{n}{\oplus} r_2 = [r_1 + r_2]_n, \quad r_1 \underset{n}{\odot} r_2 = [r_1 r_2]_n \tag{5.1}$$

Dessa operationer kallas **addition och multiplikation modulo** n. T ex är $2 \underset{5}{\oplus} 1 = [2+1]_5 = 3$, $3 \underset{5}{\oplus} 3 = [3+3]_5 = 1$, $3 \underset{5}{\odot} 3 = [9]_5 = 4$ osv. Ofta utelämnar man "n" i symbolerna "$\underset{n}{\oplus}$" och "$\underset{n}{\odot}$" som förenklas till "$\oplus$" och "$\odot$" eller till "$+$" och "$\cdot$". För addition och multiplikation modulo 2 och 3 har vi

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

$\underset{n}{\oplus}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\underset{n}{\odot}$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Det är klart att $\underset{n}{\oplus}$ och $\underset{n}{\odot}$ är kommutativa operationer. Det är också klart att bägge har neutrala element — för addition 0, för multiplikation 1. Men det är inte lika självklart att dessa operationer är associativa. För addition och multiplikation modulo 10 vet vi det sedan länge. När man adderar tre tal t ex

$$\begin{array}{r} 123 \\ 25 \\ 38 \\ \hline ...6 \end{array}$$

så räknar man ut den sista siffran genom att addera 3+5+8 vilket ger sista siffran 6. Med vår nya addition betyder det att $3 \underset{10}{\oplus} 5 \underset{10}{\oplus} 8 = 6$. Det är just addition modulo 10 och det faktum att vi inte bryr oss om hur parenteserna placeras beror på att vi litar på associativiteten. För att bevisa den helt allmänt behöver vi en viktig egenskap hos $\oplus$ och $\odot$:

(5.2) Lemma. *Låt a, b vara godtyckliga heltal. Då gäller:*

$$\begin{aligned} [a+b]_n &= [a]_n \oplus [b]_n, \\ [ab]_n &= [a]_n \odot [b]_n. \end{aligned}$$

Bevis. Låt

$$a = nq_a + r_a, \;\; 0 \le r_a < n, \quad b = nq_b + r_b, \;\; 0 \le r_b < n$$

och

$$a + b = nq_{a+b} + r_{a+b}, \;\; 0 \le r_{a+b} < n, \quad ab = nq_{ab} + r_{ab}, \;\; 0 \le r_{ab} < n.$$

Vi har:

$$[a]_n \oplus [b]_n = r_a \oplus r_b \quad = \quad [r_a + r_b]_n = r_{a+b} = [a+b]_n,$$

ty $r_a + r_b = (a - nq_a) + (b - nq_b) = n(q_{a+b} - q_a - q_b) + r_{a+b}$, dvs r_{a+b} är resten vid division av $r_a + r_b$ med n, och

$$[a]_n \odot [b]_n = r_a \odot r_b \quad = \quad [r_a r_b]_n = r_{ab} = [ab]_n,$$

ty $r_a r_b = (a - nq_a)(b - nq_b) = n(q_{ab} - q_a b - q_b a + nq_a q_b) + r_{ab}$, dvs r_{ab} är resten vid division av $r_a r_b$ med n. □

(5.3) Följdsats. *$\oplus$ och $\odot$ är associativa operationer på $\mathbb{Z}_n$.*

Bevis.

$$\begin{aligned} (r_1 \oplus r_2) \oplus r_3 &= [r_1 + r_2]_n \oplus [r_3]_n = [(r_1 + r_2) + r_3]_n \\ r_1 \oplus (r_2 \oplus r_3) &= [r_1]_n \oplus [r_2 + r_3]_n = [r_1 + (r_2 + r_3)]_n \end{aligned}$$

så att $(r_1 \oplus r_2) \oplus r_3 = r_1 \oplus (r_2 \oplus r_3)$ ty $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$.

Exakt samma argument för $\odot$ som för $\oplus$ ger associativiteten av multiplikation modulo n. □

Nu kan vi konstatera:

(5.4) Proposition. *$(\mathbb{Z}_n, \oplus)$ är en grupp. Den är cyklisk.*

Bevis. Slutenheten följer direkt ur definitionen av $\oplus$ i (5.1). Associativiteten har vi just bevisat. 0 är det neutrala elementet. Inversen till r kallas den motsatta resten och är $n - r$ då $r \neq 0$, ty $r \oplus (n - r) = [n]_n = 0$. Vi har $r = 1 + \cdots + 1$ (r ettor) så att $\mathbb{Z}_n =< 1 >$. □

$(\mathbb{Z}_n, \odot)$ är aldrig en grupp ty resten 0 saknar invers ($r \odot 0 = 0$). Man kan försöka rädda situationen genom att eliminera 0. Men $\mathbb{Z}_n \setminus \{0\}$ behöver inte heller vara en grup. T ex är $2 \odot 3 = [6]_6 = 0$ i $\mathbb{Z}_6$ så att $\mathbb{Z}_6 \setminus \{0\}$ inte är sluten med avseende på $\odot$. Skälet till att man får 0 är att 2 och 3 har gemensamma delare med 6. För att få en grupp räcker det att eliminera den situationen. Låt $\mathbb{Z}_n^*$ beteckna alla rester som saknar gemensamma delare $\neq 1$ med n dvs $r \in \mathbb{Z}_n^*$ då och endast då $SGD(r, n) = 1$. T ex

$$\mathbb{Z}_2^* = \{1\}, \;\; \mathbb{Z}_3^* = \{1, 2\}, \;\; \mathbb{Z}_4^* = \{1, 3\}, \;\; \mathbb{Z}_5^* = \{1, 2, 3, 4\}, \;\; \mathbb{Z}_6^* = \{1, 5\}.$$

Nu har vi

(5.5) Proposition. *$(\mathbb{Z}_n^*, \odot)$ är en grupp.*

Bevis. För at bevisa slutenheten betrakta två rester sådana att $SGD(r_1, n) = 1$ och $SGD(r_2, n) = 1$. Då är även $SGD(r_1 r_2, n) = 1$. Motsatsen betyder att det finns ett primtal p sådant att $p|n$

och $p|r_1r_2$. Då är $p|r_1$ eller $p|r_2$, vilket strider mot vårt antagande att r_1 och r_2 saknar gemensamma delare $\neq 1$ med n. Associativiteten av $\odot$ visade vi i (5.3). Det neutrala elementet är 1. Låt $r \in \mathbb{Z}_n^*$. Som vi vet kan man med t ex Euklides algoritm bestämma två heltal x och y sådana att

$$rx + ny = 1$$

(ty $SDG(r, n) = 1$). Detta betyder att $1 = [rx + ny]_n = [rx]_n = [r]_n \odot [x]_n = r \odot [x]_n$ så att $[x]_n$ är inversen till $r \in \mathbb{Z}_n^*$. □

(5.6) Anmärkning. Det framgår från propositionen att för varje $a \in \mathbb{Z}_n^*$ har ekvationen $ax = 1$ exakt en lösning $x \in \mathbb{Z}_n$. I termer av kongruenser kan man säga att kongruensen $ax \equiv 1 \pmod{n}$ har en lösning då $\mathrm{SGD}(a, n) = 1$. Observera att beviset av (5.5) visar att kongruensen kan lösas med hjälp av Euklides algoritm. □

Exempel. Låt $n = 12$. Då är $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ och multiplikationstabellen är

$\odot$	1	5	7	11
1	1	5	7	1
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

□

Ett särskilt viktigt fall får man då $n = p$ är ett primtal. Då är $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$. Här räcker det alltså att utelämna 0 ur $\mathbb{Z}_p$ för at få en grupp med avseende på multiplikation.

(5.7) Definition. Ordningen av $\mathbb{Z}_n^*$ betecknas med $\varphi(n)$. Funktionen $\varphi(n)$ kallas Eulers funktion. Alltså är:

$$\varphi(n) = \text{antalet heltal } k \text{ sådana att } 0 \leq k < n \quad \text{och } SGD(k, n) = 1.$$

□

Exempel. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(6) = 2$ osv. Om p är ett primtal så är $\varphi(p) = p - 1$ (varför?). □

Här följer några viktiga egenskaper hos Eulers funktion:

(5.8) Proposition. *Eulers funktion har följande egenskaper:*

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ *då* p *är ett primtal och* $\alpha \geq 1$,

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ *då* $SGD(a, b) = 1$,

(c) $\varphi(n) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$, *där* p_i *är alla olika primdelare till* n.

Bevis. (a) är en enkel övning (se övning 5.8). Ett bevis av (b) ger vi senare. (c) följer direkt ur (a) och (b): Låt $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Då är

$$\begin{aligned}\varphi(n) = \varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k}) \quad \text{(enligt (b))} \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \quad \text{(enligt (a))} \\ &= p_1^{\alpha_1} \dots p_k^{\alpha_k}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).\end{aligned}$$

□

Med hjälp av (5.8) kan man räkna ut $\varphi(n)$. T ex $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3)\varphi(5^3) = 4 \cdot 100 = 400$.

Vi avslutar detta kapitel med en intressant och mycket gammal sats om restaritmetiker som brukar kallas "Kinesiska restsatsen". I det enklaste fallet säger satsen att man alltid kann finna ett heltal som ger givna rester modulo två givna relativt prima heltal.

(5.9) Kinesiska restsatsen. *Låt $n_1, n_2, \dots, n_k$ vara relativt prima positiva heltal och låt $r_1 \in \mathbb{Z}_{n_1}$, $r_2 \in \mathbb{Z}_{n_2}$, …, $r_k \in \mathbb{Z}_{n_k}$. Då existerar ett heltal x entydigt bestämt modulo $n_1 n_2 \dots n_k$ sådant att*

$$[x]_{n_1} = r_1,\ [x]_{n_2} = r_2,\ \dots,\ [x]_{n_k} = r_k.$$

Bevis. Vi skall visa hur man kan beräkna ett tal x som har den önskade egenskapen och därefter visa att det är entydigt modulo $N = n_1 n_2 \cdots n_k$. Beräkna först x_i så att

$$\frac{N}{n_i} x_i \equiv 1 \pmod{n_i}, \qquad \text{dvs} \qquad \frac{N}{n_i} x_i = 1 \quad \text{i} \quad \mathbb{Z}_{n_i}.$$

Eftersom SGD $(\frac{N}{n_i}, n_i) = 1$ enligt förutsättningen kan man beräkna x_i med hjälp av Euklides algoritm (se (5.6)). Välj nu

$$x = r_1 \frac{N}{n_1} x_1 + r_2 \frac{N}{n_2} x_2 + \dots + r_k \frac{N}{n_k} x_k.$$

Då gäller:

$$[x]_{n_i} = [\sum_{j=1}^{k} r_j \frac{N}{n_j} x_j]_{n_i} = \bigoplus_{j=1}^{k} [r_j]_{n_i} \odot [\frac{N}{n_j} x_j]_{n_i} = [r_i]_{n_i} \odot [\frac{N}{n_i} x_i]_{n_i} = [r_i]_{n_i}$$

ty

$$[\frac{N}{n_j} x_j]_{n_i} = \begin{cases} 1 & \text{om} \quad j = i \\ 0 & \text{om} \quad j \neq i \end{cases}$$

Alltså är $x \equiv r_i \pmod{n_i}$ för $i = 1, 2, \ldots, k$.

Antag nu att x och x' ät två heltal sådana att $[x]_{n_i} = [x']_{n_i} = r_i$ för alla i. Då gäller det att $n_i | x - x'$ för alla i och detta innebär att $n_1 n_2 \cdots n_k | x - x'$ därför att alla n_i är relativt prima. Alltså lämnar x och x' samma rest modulo $N = n_1 n_2 \cdots n_k$. □

(5.10) Anmärkning. Kinesiska restsatsen formuleras ofta med hjälp av kongruenser. Då säger den att för relativt prima positiva heltal $n_1, n_2, \ldots, n_k$ och godtyckliga heltal $r_1, r_2, \ldots, r_k$ existerar ett heltal x så att

$$x \equiv r_1 \pmod{n_1}, \;\; x \equiv r_2 \pmod{n_2}, \;\; \ldots \;\; , x \equiv r_k \pmod{n_k}.$$

Man behöver inte förutsätta att r_i är resten vid division med n_i därför att för varje heltal a gäller ju att $a \equiv [a]_{n_i} \pmod{n_i}$. □

Exempel. Låt oss bestämma ett heltal x som vid division med 3 ger resten 2, med 4 resten 3 och med 5 resten 4 dvs

$$x \equiv 2 \pmod{3}, \;\; x \equiv 3 \pmod{4}, \;\; x \equiv 4 \pmod{5}.$$

Låt $n = 3 \cdot 4 \cdot 5 = 60$. Först måste vi bestämma x_1, x_2, x_3 sådana att

$$\frac{60}{3} x_1 = 20 x_1 \equiv 1 \pmod{3}, \;\; \frac{60}{4} x_2 = 15 x_2 \equiv 1 \pmod{4}, \;\; \frac{60}{5} x_3 = 12 x_3 \equiv 1 \pmod{5}.$$

Detta betyder att vi måste lösa ekvationerna:

$$2x_1 = 1 \quad \text{i} \quad \mathbb{Z}_3, \quad 3x_2 = 1 \quad \text{i} \quad \mathbb{Z}_4, \;\; 2x_3 = 1 \quad \text{i} \quad \mathbb{Z}_5.$$

Vi hittar lätt (utan Euklides algoritm) att $x_1 = 2, x_2 = 3, x_3 = 3$. Enligt beviset av (5.9) är

$$x = 2 \cdot \frac{60}{3} \cdot 2 + 3 \cdot \frac{60}{4} \cdot 3 + 4 \cdot \frac{60}{5} \cdot 3 = 359$$

en lösning. Den minsta icke-negativa lösningen är $[359]_{60} = 59$ (lösningen är entydigt bestämd modulo 60 enligt (5.9)). Lägg märke till att $x = 60q + 59$ med ett godtyckligt $q \in \mathbb{Z}$ är en lösning (ty $[x]_{60} = 59$) och att sådana x ger alla lösningar (se övning 5.5). Observera också att en uppmärksam student kunde skriva en lösning direkt utan att använda Kinesiska restsatsen (hur?). □

Vi skall avsluta detta kapitel med en annan formulering och ett annat bevis av Kinesiska restsatsen därför att det finns flera tillämpningar som baseras just på den formen av satsen.

(5.11) Sats. *Låt $n_1, n_2, \ldots, n_k$ vara parvis relativt prima positiva heltal (dvs $SGD(n_i, n_j) = 1$ då $i \neq j$). Då är*

$$\mathbb{Z}_{n_1 n_2 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

och

$$\mathbb{Z}^*_{n_1 n_2 \cdots n_k} \cong \mathbb{Z}^*_{n_1} \times \mathbb{Z}^*_{n_2} \times \ldots \times \mathbb{Z}^*_{n_k}.$$

Bevis. Låt $N = n_1 n_2 \cdots n_k$. Betrakta funktionen:

$$\theta : \mathbb{Z}_N \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

sådan att $\theta([a]_N) = ([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k})$. Definitionen av denna funktion beror inte på heltalet a som definierar resten: Om $[a]_N = [b]_N$ så är $[a]_{n_1} = [b]_{n_1}$, $[a]_{n_2} = [b]_{n_2}$, …, $[a]_{n_k} = [b]_{n_k}$ ty $N|a-b$ implicerar att $n_1|a-b$, $n_2|a-b$, …, $n_k|a-b$. Vi har

$$\theta([a+b]_N) = ([a+b]_{n_1}, [a+b]_{n_2}, \ldots, [a+b]_{n_k}) =$$

$$([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k}) + ([b]_{n_1}, [b]_{n_2}, \ldots, [b]_{n_k}) = \theta([a]_N) + \theta([b]_N)$$

så att θ är en grupphomomorfism. Vi vill visa att θ är en isomorfism. Man kontrollerar lätt att olika rester $[a]_N$ och $[b]_N$ har olika bilder: $[a]_{n_1} = [b]_{n_1}$, $[a]_{n_2} = [b]_{n_2}$, …, $[a]_{n_k} = [b]_{n_k}$ betyder att $n_1|a-b$, $n_2|a-b$, …, $n_k|a-b$, vilket ger $N = n_1 n_2 \cdots n_k | a-b$, därför att $n_1, n_2, \ldots, n_k$ är parvis relativt prima. Detta innebär att $[a]_N = [b]_N$. Funktionen θ är alltså en-entydig. Men antalet element i $\mathbb{Z}_N$ är N och antalet element i $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ är lika stort, vilket innebär att varje element i produkten är bilden av ett element i $\mathbb{Z}_N$. Detta visar att θ är en isomorfism.

Det återstår att visa den andra isomorfismen. Först observerar vi att om a är relativt primt med N så är också a relativt primt med varje faktor n_i av N. Dettta visar att θ avbildar $\mathbb{Z}^*_N$ i produkten $\mathbb{Z}^*_{n_1} \times \mathbb{Z}^*_{n_2} \times \ldots \times \mathbb{Z}^*_{n_k}$. Å andra sidan om $([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k}) \in \mathbb{Z}^*_{n_1} \times \mathbb{Z}^*_{n_2} \times \ldots \times \mathbb{Z}^*_{n_k}$, så är a relativt primt med alla n_i och således med $N = n_1 n_2 \cdots n_k$. Detta visar att funktionen θ avbildar en-entydigt $\mathbb{Z}^*_N$ på hela $\mathbb{Z}^*_{n_1} \times \mathbb{Z}^*_{n_2} \times \ldots \times \mathbb{Z}^*_{n_k}$. För att kunna påstå att funktionen θ definierar en isomorfism mellan dessa grupper kontrollerar vi att

$$\theta([ab]_N) = ([ab]_{n_1}, [ab]_{n_2}, \ldots, [ab]_{n_k}) =$$

$$([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k})([b]_{n_1}, [b]_{n_2}, \ldots, [b]_{n_k}) = \theta([a]_N)\theta([b]_N).$$

□

(5.12) Anmärkning. Det är mycket lätt att härleda Kinesiska restsatsen från gruppisomorfismen $\mathbb{Z}_{n_1 n_2 \ldots n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$. Om $(r_1, r_2, \ldots, r_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ så säger satsen att det finns exakt en rest $x \in \mathbb{Z}_{n_1 n_2 \ldots n_k}$ sådan att

$$[x]_{n_1} = r_1, \;\; [x]_{n_2} = r_2, \ldots, \;\; [x]_{n_k} = r_k.$$

□

(5.13) Exempel. Gruppen $\mathbb{Z}_{100}$ kan enligt sats (5.11) skrivas som produkt av mindre grupper: $100 = 2^2 5^2$ så att $\mathbb{Z}_{100} \cong \mathbb{Z}_4 \times \mathbb{Z}_{25}$.

□

Nu kan vi bevisa multiplikativiteten av Eulers funktion (se (5.8)(b)):

(5.14) Följdsats. *För Eulers funktion φ gäller det att $\varphi(ab) = \varphi(a)\varphi(b)$ då a och b är relativt prima naturliga tal.*

Bevis. Enligt (5.11) är $\mathbb{Z}_{ab}^* \cong \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. Antalet element till vänster är $\varphi(ab)$, medan till höger $\varphi(a)\varphi(b)$. □

ÖVNINGAR

5.1. Bestäm sista siffran av talet:

a) 2^{1986}, b) $13^{20} + 22^{30}$, c) 7^{7^7}.

5.2. Bestäm resten vid division av

a) 3^{100} med 7, b) 2^{1000} med 3,5,11,13.

5.3. Talen $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$, kallas Fermattalen. $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ är alla primtal. Pierre Fermat (1601-1665) påstod att alla tal F_n är primtal, men 100 år senare visade Leonard Euler (1707-1783) att $641 | F_5$. Visa det genom att utnyttja likheterna $5 \cdot 2^7 + 1 = 646$ och $5^4 + 2^4 = 641$. Räkna i $\mathbb{Z}_{641}$.

5.4. Låt $a, b, n \in \mathbb{Z}$ och $n > 0$. Visa att $[a]_n = [b]_n$ då och endast då $n | a - b$.

5.5. Låt a och n vara relativt prima heltal. Låt x_0 vara en lösning till kongruensen $ax \equiv b \pmod{n}$ för ett heltal b. Visa att alla andra lösningar till denna kongruens kan skrivas på formen $x_0 + kn$, där $k = 0, \pm 1, \pm 2, \ldots$.

5.6. Visa att grupperna $\mathbb{Z}_5^*$, $\mathbb{Z}_7^*$ och $\mathbb{Z}_9^*$ är cykliska men $\mathbb{Z}_8^*$ inte är cyklisk.

5.7. Skriv ut grupptabelerna för

a) $\mathbb{Z}_2 \times \mathbb{Z}_3$, b) $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Är dessa gruper cykliska?

5.8. Visa att $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ då p är ett primtal och $\alpha \geq 1$.
Ledning. Skriv ut alla heltal k sådana at $0 \leq k < p^\alpha$ och $p | k$.

5.9. Skriv följande grupper som produkt av mindre restgrupper

(a) $\mathbb{Z}_{36}$, (b) $\mathbb{Z}_{75}$, (c) $\mathbb{Z}_{15} \times \mathbb{Z}_{28}$, (d) $\mathbb{Z}_{75600}$.

5.10. Lös följande ekvationer:

(a) $17x = 1$ i $\mathbb{Z}_{23}$, (b) $6x = 17$ i $\mathbb{Z}_{41}$, (c) $x^2 = 5$ i $\mathbb{Z}_{29}$.

5.11. Låt $\theta : \mathbb{Z}_{360} \to \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ vara definierad som i beviset av (5.11). Bestäm $\theta^{-1}(1, 0, 0)$, $\theta^{-1}(0, 1, 0)$, $\theta^{-1}(0, 0, 1)$. Beräkna därefter $\theta^{-1}(1, 2, 3)$.

Kapitel 6

TRANSFORMATIONSGRUPPER

Även detta kapital handlar om exempel på grupper. Vi bekantar oss med grupper relaterade till olika geometriska rum och geometriska figurer i dessa rum. En stor del av gruppteorin utvecklades med utgångspunkt från dessa exempel och den slutliga definitionen av gruppbegreppet formulerades först när man upptäckte att grupper är lika vanliga i geometrin som i algebran (se vidare anmärkning (6.8)). Eftersom funktioner mellan olika rum kallas ofta transformationer (eller avbildningar) kallar man grupper bestående av sådana funktioner för transformationsgrupper.

Först måste vi repetera och komplettera något våra kunskaper om funktioner:

(6.1) Definition. Låt $f : X \to Y$ vara en funktion. Man säger att f är **injektiv** (eller en-entydig) om f avbildar olika element i X på olika element i Y dvs om $x_1 \neq x_2$ ger $f(x_1) \neq f(x_2)$. f kallas **surjektiv** (eller på hela Y) om till varje $y \in Y$ finns $x \in X$ så att $f(x) = y$. En funktion som samtidigt är injektiv och surjektiv kallas **bijektiv**.

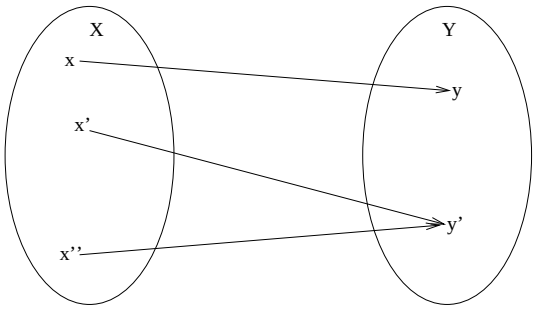
Man säger att två funktioner $f_1 : X \to Y$ och $f_2 : X \to Y$ är lika om $f_1(x) = f_2(x)$ för varje $x \in X$.

Med **sammansättningen** av två funktioner $f : X \to Y$ och $g : Y \to Z$ menar man funktionen $g \circ f : X \to Z$ ("g ring f") sådan att:

$$(g \circ f)(x) = g(f(x)).$$

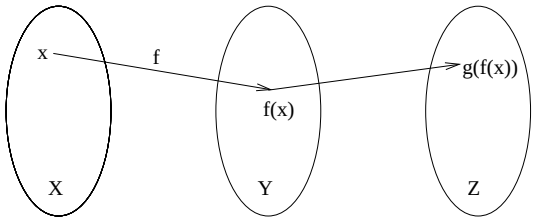
Man säger att en funktion $g : Y \to X$ är en **invers** till $f : X \to Y$ om $g \circ f = i_X$ och $f \circ g = i_Y$, där i_X är den **identiska funktionen** på X och i_Y den identiska funktionen på Y dvs $i_X(x) = x$ då $x \in X$ och $i_Y(y) = y$ då $y \in Y$. □

Om man tänker på en funktion f från X till Y som pilar från alla element i X till vissa element i Y (se fig. 1) så kan man lätt åskodliggöra alla dessa begrepp. f är injektiv om pilar som startar från olika punkter i X kommer fram till olika punkter i Y, f är surjektiv om till varje punkt i Y kommer en pil, och f är bijektiv om de bägge egenskaperna gäller. Om f är



bijektiv så kan man vända på alla pilar från X till Y och då får man inversen g till f (vi visar detta påstående helt formellt i nästa proposition).

Sammansättningen av $g(f(x))$ innebär geometriskt att man först följer pilen från punkten $x \in X$ till punkten $f(x) \in Y$ och därefter pilen från punkten $f(x) \in Y$ till punkten $g(f(x)) \in Z$.



(6.2) Proposition. *$f : X \to Y$ har en invers $g : Y \to X$ då och endast då f är bijektiv. Inversen g är entydigt bestämd (den betecknas f^{-1}).*

Bevis. "$\Rightarrow$" Låt g vara en invers till f dvs $g(f(x)) = x$ då $x \in X$ och $f(g(y)) = y$ då $y \in Y$. Om $x_1 \neq x_2$ så har vi $f(x_1) \neq f(x_2)$ ty likheten $f(x_1) = f(x_2)$ ger $g(f(x_1)) = g(f(x_2))$ dvs $x_1 = x_2$. Alltså är f injektiv. Låt $y \in Y$. Då är $y = f(g(y))$ dvs f avbildar $g(y)$ på y. Detta visar att f är surjektiv. Följaktligen är f bijektiv.

"$\Leftarrow$" Låt f vara bijektiv. Då är varje element $y \in Y$ bilden av exakt ett element $x \in X$. Definiera:

$$g(y) = x \Leftrightarrow f(x) = y.$$

Då har vi: $(g \circ f)(x) = g(f(x)) = g(y) = x$ för $x \in X$ och $(f \circ g)(y) = f(g(y)) = f(x) = y$ för $y \in Y$. Detta visar att g är en invers till f. Slutligen om även g' är en invers till f så har vi

$$f(g(y)) = f(g'(y)) = y$$

då $y \in Y$. Men f är injektiv så att $g(y) = g'(y)$ för varje $y \in Y$ vilket visar att $g = g'$. □

Vi antecknar också följande egenskaper hos funktioner vars bevis lämnar vi som övning.

(6.3) Proposition. *Låt $f : X \to Y$ och $g : Y \to Z$ vara funktioner.*

(a) *Om f och g är injektiva så är $g \circ f$ injektiv.*

(b) *Om f och g är surjektiva så är $g \circ f$ surjektiv.*

(c) *Om f och g är bijektiva så är $g \circ f$ bijektiv.*

Låt nu X vara en mängd och låt $G(X)$ vara mängden av alla bijektiva funktioner (med andra ord: bijektiva transformationer) $f : X \to X$.

(6.4) Proposition. *$(G(X), \circ)$ är en grupp med avseende på sammansättningen av funktioner.*

Bevis. Om $f : X \to X$ och $g : X \to X$ är bijektiva funktioner så är även $g \circ f : X \to X$ en bijektiv funktion enligt (6.3) (c). Alltså är $G(X)$ sluten med avseende på operationen. För att visa associativiteten låt $h : X \to X$ vara en bijektiv funktion. Då är:

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x)))$$

och

$$[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x)))$$

för $x \in X$. Alltså är $(f \circ g) \circ h = f \circ (g \circ h)$. Det neutrala elementet är den identiska funktionen $i_X(x) = x$ för $x \in X$. Inversen till f är den inversa funktionen f^{-1} som existerar (och är bijektiv) enligt (6.2). □

(6.5) Permutationsgrupper. Låt $X = \{1, 2, \ldots, n\}$. $G(X)$ består av alla bijektiva funktioner $f : X \to X$ dvs $f(1) = p_1, f(2) = p_2, \ldots, f(n) = p_n$, där $p_1, p_2, \ldots, p_n$ är en ordningsföljd av talen $1, 2, \ldots, n$. Sådana funktioner kallas som bekant **permutationer**. Vi kommer att skriva:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}.$$

Gruppen $G(X)$ betecknas ofta med S_n och kallas **symmetriska gruppen** av graden n. Låt oss påminna om at $o(S_n) = n!$ (antalet olika permutationer av n element). T ex då $n = 3$ får man gruppen S_3 bestående av $3! = 6$ permutationer

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Gruppen S_2 har 2 element:

$$I = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Permutationerna kan representeras mera kompakt. Låt $p_1, p_2, \ldots, p_k \in \{1, 2, \ldots, n\}$ och låt $(p_1, p_2, \ldots, p_k)$ beteckna funktionen:

$$f(p_1) = p_2, f(p_2) = p_3, \ldots, f(p_k) = p_1.$$

och $f(i) = i$ då $i \neq p_1, p_2, \ldots, p_k$.

Exempel. $(1, 2, 3) \in S_3$ är beteckningen av $\binom{123}{231}$, $(2, 4) \in S_4$ betyder $\binom{1234}{1432}$, $(3, 2, 4) \in S_4$ är $\binom{1234}{1423}$, $(1) \in S_3$ är $\binom{123}{123}$. □

Man säger att permutationen $(p_1, p_2, \ldots, p_k)$ är en **cykel** av längden k. Låt

$$f = (p_1, p_2, \ldots, p_k) \quad \text{och} \quad g = (p'_1, p'_2, \ldots, p'_l),$$

där alla tal $p_1, p_2, \ldots, p_k, p'_1, p'_2, \ldots, p'_l$ är olika. Då säger man att f och g är disjunkta cykler. För sådana cykler har vi $f \circ g = g \circ f$ (kontrollera att $(f \circ g)(x) = (g \circ f)(x)$ för varje $x \in \{1, 2, \ldots, n\}$). Varje permutation är en sammansättning av disjunkta cykler. T ex

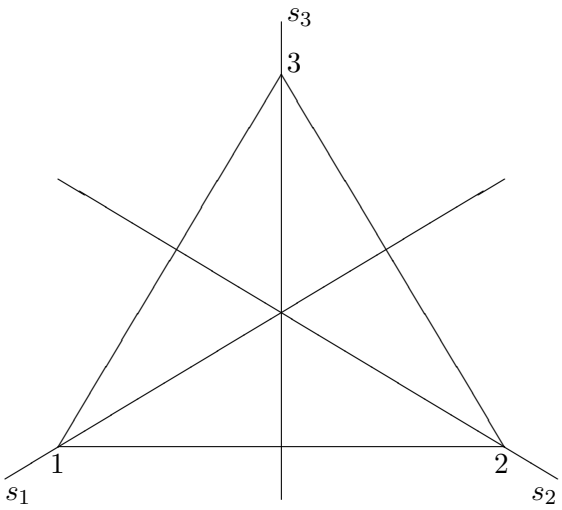
$$\begin{pmatrix} 123456789 \\ 217439568 \end{pmatrix} = (1, 2) \circ (3, 7, 5) \circ (6, 9, 8).$$

Hur får man en sådan framställning? Nedan följer ett enkelt recept:

(6.6) Hur skriver man en permutation som produkt av cykler? Man väljer ett tal p_1 som inte avbildas på sig självt. Därefter tar man bilden p_2 av p_1, bilden p_3 av p_2 osv, tills man får p_1 igen. Då har man en cykel. Nu tar vi ett tal som inte ingår i första cykeln och vi upprepar proceduren. Det gör vi så länge det finns tal som inte ingår i en tidigare bildad cykel och som inte avbildas på sig självt.

Ofta är man intresserad av olika delgruper till $G(X)$. Man betraktar då bijektiva funktioner $f : X \to X$ med en viss egenskap och visar att funktioner med den egenskapen bildar en delgrupp till $G(X)$. Låt oss betrakta några exempel:

(6.7) Exempel. (a) Låt X vara en liksidig triangel i planet och låt G bestå av alla transformationer av planet som bevarar avståndet och avbildar triangeln på sig själv. G är en grupp med avseende på sammansättningen av avbildningarna (en delgrupp till $G(X)$) och kallas ofta **triangelgruppen** eller, mera exakt, **symmetrigruppen av en liksidig triangel**. Det är inte svårt att beskriva alla element i G. Man kan vrida triangeln $0°, 120°$ och $240°$ kring dess mittpunkt och spegla den i de tre symmetriaxlarna S_1, S_2, S_3. Man får alltså 6 transformationer som ges i form av permutationer av triangelns 3 hörn:



$$I = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1);\ v_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (1,2);\ v_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (1,3,2)$$

$$s_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (2,3);\ s_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (1,3);\ s_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (1,2).$$

På det sättet får vi alla möjliga avbildningar ty varje avbildning är en permutation av hörnen 1, 2, 3. Men det finns exakt 6 permutationer av talen 1, 2, 3 (de bildar den symmetriska gruppen av graden 3). Lägg märke till att gruppen inte är kommutativ. T ex $v_1 = s_1 \circ s_2 \neq s_2 \circ s_1 = v_2$. Gruppen G har följande grupptabell:

	I	v_1	v_2	s_1	s_2	s_3
I	I	v_1	v_2	s_1	s_2	s_3
v_1	v_1	v_2	I	s_3	s_1	s_2
v_2	v_2	I	v_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	I	v_1	v_2
s_2	s_2	s_3	s_1	v_2	I	v_1
s_3	s_3	s_1	s_2	v_1	v_2	I

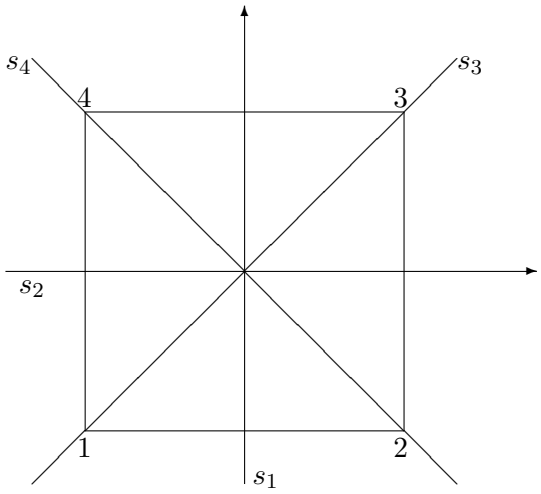
(b) Låt X vara en kvadrat i planet och låt G bestå av alla transformationer av planet som bevarar avståndet och kvadraten. Denna grupp kallas ofta **kvadratgruppen**. G består i detta fall av följande 8 transformationer: 4 vridningar $0°, 90°, 180°, 270°$ kring kvadratens mittpunkt och 4 speglingar i linjerna s_1, s_2, s_3 och s_4. Man kan beskriva dessa avbildningar med hjälp av följande permutationer av kvadratens hörn 1,2,3,4:

$$I = (1),\ v_1 = (1,2,3,4),\ v_2 = (1,3)(2,4),\ v_3 = (1,4,3,2)$$

(de fyra vridningarna) och

$$s_1 = (1,2)(3,4),\ s_2 = (1,4)(2,3),\ s_3 = (2,4),\ s_4 = (1,3)$$

(de fyra speglingarna).



Dessa 8 permutationer bildar en grupp därför att sammansättningen av två transformationer i G ger en transformation i G. Allt detta är relativt enkelt att se direkt men det följer också ur grupptabellen:

	I	v_1	v_2	v_3	s_1	s_2	s_3	s_4
I	I	v_1	v_2	v_3	s_1	s_2	s_3	s_4
v_1	v_1	v_2	v_3	I	s_4	s_3	s_1	s_2
v_2	v_2	v_3	I	v_1	s_2	s_1	s_4	s_3
v_3	v_3	I	v_1	v_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	I	v_2	v_1	v_3
s_2	s_2	s_4	s_1	s_3	v_2	I	v_3	v_1
s_3	s_3	s_2	s_1	s_3	v_2	v_4	I	v_2
s_4	s_4	s_1	s_3	s_2	v_4	v_3	v_2	I

(c) Helt allmänt kan man betrakta en godtycklig figur X i planet eller i rymden. Mängden G av alla transformationer som bevarar avståndet och figuren X är en grupp med avseende på sammansättningen av transformationerna. Denna grupp kallas ofta **symmetrigruppen av** X. Grupper av den typen har en stor betydelse i olika praktiska sammanhang. Bland annat utnyttjas sådana grupper i kristalografin där man klassificerar kristalografiska strukturer beroende på deras transformationsgrupper (dvs alla transformationer i rymden som bevarar avstånden och strukturen – man förutsätter då att kristalen fyller ut hela rymden). □

(6.8) Anmärkning. Från kursen i linjär algebra känner vi ortogonala avbildningar i Euklidiska rum. Om $\mathbb{R}^n$ betraktas med det vanliga avståndsbegreppet dvs

$$d(\mathbf{x},\mathbf{y}) = \sqrt{(x_1-y_1)^2+\cdots+(x_n-y_n)^2}$$

för två vektorer $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$) så säger man att en linjär avbildning $f : \mathbb{R}^n \to \mathbb{R}^n$ är ortogonal (eller isometrisk) om f bevarar avståndet dvs $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$. Då är $f(\mathbf{x}) = A\mathbf{x}$, där A är en ortogonal matris dvs $A^{-1} = A^t$, där A^t är den transponerade matrisen till A. Man kontrollerar mycket lätt (se övn. 6.6) att alla ortogonala transformationer bildar en grupp. Den Euklidiska geometrin i $\mathbb{R}^n$ är en studie av alla egenskaper hos $\mathbb{R}^n$ som bevaras vid ortogonala transformationer (exempel på sådana egenskaper är avstånden, vinklarna, volymerna osv). Man kan betrakta andra grupper av linjära avbildningar t ex alla icke-singulära avbildningar dvs alla f som ovan där A är en godtycklig matris med nollskild determinant dvs $A \in GL_n(\mathbb{R})$. En studie av alla egenskaper som bavaras vid dessa transformationer är uppgiften för den **affina geometrin** i $\mathbb{R}^n$. År 1872 formulerade den store tyske matematikern Felix Klein en allmän strategi för studier av olika rum. Hans "Erlangenprogrammet" definierar begreppet geometri i ett rum (t ex i $\mathbb{R}^n$) som alla de egenskaper i rummet som bevaras under verkan av en grupp. Kleins idéer hade stor betydelse för utvecklingen inom både matematiken och fysiken. Så småningom ledde dessa ideer till relativitetsteorin som beskriver olika egenskaper hos vektorer i $\mathbb{R}^4$ som bevars under verkan av Lorenzgruppen och dess delgrupper (se övning 6.6(b)). Det är mycket intressant att Felix Klein fick många av sina idéer under en vistelse i Paris hos C. Jordan då denne studerade Galois arbeten. Tack vare Jordan blev Galois idéer kända för den bredda matematiska allmänheten. Även den store norske matematikern Sophus Lie vistades hos Jordan samtidigt med Klein. S. Lie tillämpade gruppteorin på problem i matematisk analys bl a associerade han grupper med differentialekvationer. Teorin för Liegrupper, som samtidigt är grupper och analytiska mångfalder, har mycket stor betydelse både inom matematiken och inom fysiken. T ex har grupperna $O(n), SO(n), U(n), SU(n)$ den karaktären (se vidare ovningar 6.6 och 6.7). □

ÖVNINGAR

6.1. Låt $f : X \to Y$ och $g : Y \to X$. Visa att om $g \circ f = i_X$ så är f injektiv och g surjektiv.

6.2. Låt $f : X \to X$ där X är en ändlig mängd. Visa att om f är injektiv eller surjektiv så är den bijektiv.

6.3. Låt G vara mängden av funktionerna

$$f_1(x) = x,\ f_2(x) = -x,\ f_3(x) = \frac{1}{x},\ f_4(x) = -\frac{1}{x},\ x \in \mathbb{R}^*.$$

Visa att G är en grupp m.a.p. sammanstättning. Skriv ut grupptabellen.

6.4. Skriv ut gruptabeller för följande gruper:

(a) symmetrigruppen av en rektangel som inte är en kvadrat,

(b) symmetrigruppen av bokstaven **H**.

Anmärkning: Gruppen i (a) kallas ofta **Kleinsfyra(gruppen)** och betecknas med V_4.

6.5. Försök beskriva geometriskt alla 24 element i symmetrigruppen av en regelbunden tetraeder.

6.6. Visa att följande $(n \times n)$-reella matriser (= linjära avbildningar av $\mathbb{R}^n$) bildar en grupp med avseende på matrismultiplikation (= sammansättning):

(a) alla ortogonala matriser (dvs alla $(n \times n)$-matriser A sådana att $A^tA = E$),

(b) alla (4×4)-matriser A sådana att $A^tMA = M$, där

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Anmärkning: Villkoret $A^tMA = M$, där M är en godtycklig symmetrisk matris betyder att A bevarar den kvadratiska form som har matrisen M (visas enkelt i kursen Linjär algebra). I (a) handlar det om formen $X_1^2 + X_2^2 + X_3^2$ och villkoret $A^tA = E$ betyder att om man tar en vektor $\mathbf{x}^t = (x_1, x_2, x_3)$ så är $(A\mathbf{x})^tA\mathbf{x} = \mathbf{x}^t\mathbf{x}$ dvs vektorns längd bevaras då den transformeras med hjälp av A (den kvadratiska formen har samma värde för både $\mathbf{x}$ och $A\mathbf{x}$). I (b) är M matrisen för $X_1^2 + X_2^2 + X_3^2 - T^2$ och villkoret $A^tMA = M$ säger att denna kvadratiska form har samma värde för både $\mathbf{x}$ och $A\mathbf{x}$ dvs $(A\mathbf{x})^tMA\mathbf{x} = \mathbf{x}^tM\mathbf{x}$. Gruppen i (b) kallas **Lorentzgruppen** och spelar en mycket viktig roll i relativitetsteorin). Gruppen i (a) kallas **den ortogonala gruppen** och betecknas ofta med $O(n)$. Den delgrupp till $O(n)$ som består av alla matriser med determinanten lika med 1 kallas **den speciella ortogonalla gruppen** och betecknas med $SO(n)$. Lorenzgruppen betecknas ofta $O(3,1)$.

6.7. (a) Visa att alla **unimodulära** $(n \times n)$-matriser A dvs alla $(n \times n)$-matriser med komplexa element och sådana att $A^{-1} = \overline{A}^t$ ($\overline{A}$ betecknar matrisen som man får genom att konjugera alla element i A) bildar en grupp $U(n)$.

(b) Visa att alla **speciella unimodulära** $(n \times n)$-matriser dvs alla matriser A i (a) sådana att $\det A = 1$ bildar en delgrupp till $U(n)$. Denna delgrupp betecknas med $SU(n)$.

(c) Visa att varje matris i $SU(2)$ kan skrivas på formen

$$\begin{bmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{bmatrix}$$

där z_1 och z_2 är komplexa tal sådana att $|z_1|^2 + |z_2|^2 = 1$.

6.8. Skriv ut de givna permuationerna som produkt av disjunkta cykler:

(a) $\binom{123456789}{214359678}$, (b) $\binom{1234567}{3542176}$.

6.9. (a) Låt $a = (p_1, p_2, \ldots p_k)$ vara en cykel i S_n. Visa att ordningen av a i denna grupp är lika med dess längd dvs $o(a) = k$.

(b) Visa at om en permutation är en produkt av disjunkta cykler så är dess ordning lika med MGM av längderna av dessa cykler.

(Exempel: Låt $f = (1,2,3)(4,5,7,6)(8,9) \in S_9$. Då är $o(f) = 3 \cdot 4 = 12$)

(c) Ge exempel på en abelsk grupp G och $a, b \in G$ sådana att $o(ab) \neq MGM(o(a), o(b))$.

6.10. Bevisa Proposition (6.3).

Kapitel 7

SIDOKLASSER OCH LAGRANGES SATS

Lagranges sats, som visades i gruppteorins begynnelse, säger att ordningen av en delgrupp till en ändlig grupp är en delare till gruppens ordning. I grunden för ett mycket enkelt bevis av satsen ligger en uppdelning av gruppens element i parvis disjunkta delmängder – sidoklasser till delgruppen. Sidoklasserna spelar en mycket viktig roll i hela gruppteorin.

(7.1) Definition. Mängden Hg av alla produkter hg, där g är ett fixt element av G och h är ett godtyckligt element av H kallar man för en **högersidoklass** till H i G. Alltså är

$$Hg = \{hg : h \in H\} \quad (\text{additivt} : H + g = \{h + g : h \in H\}).$$

Man säger att g är en **representant** för Hg. □

(7.2) Exempel. Låt $G = \mathbb{Z}$ (heltalen med addition) och låt $H =< 5 >$ dvs $H = \{0, \pm 5, \pm 10, \ldots\} = \{5k, k = 0, \pm 1, \pm 2, \ldots\}$. Här är

$$H + 1 = \{5k + 1,\ k = 0, \pm 1, \pm 2, \ldots\}$$

mängden av alla heltal som lämnar resten 1 vid division med 5. På liknande sätt är $H + 2 = \{5k + 2;\ k = 0, \pm 1, \pm 2, \ldots\}$ mängden av alla heltal som lämnar resten 2 vid division med 5. Sidoklasserna $H + 0 = H$, $H + 1$, $H + 2$, $H + 3$ och $H + 4$ är olika och består av alla heltal som är delbara med 5 ($H + 0 = H$), lämnar vid division med 5 resten 1 ($H + 1$), 2 ($H + 2$), 3 ($H + 3$) och 4 ($H + 4$). Dessa 5 mängder täcker hela mängden $\mathbb{Z}$ eftersom varje heltal lämnar (exakt) en av dessa 5 rester vid division med 5. Finns det några andra sidoklasser? $H + 5 = \{5k + 5, k = 0, \pm 1, \pm 2, \ldots\} = \{5(k + 1), k = 0, \pm 1, \pm 2, \ldots\} = H$. Vidare är $H + 6 = \{5k + 6, k = 0, \pm 1, \pm 2, \ldots\} = \{5(k + 1) + 1, k = 0, \pm 1, \pm 2, \ldots\} = H + 1$ osv. Det finns faktiskt inte några andra sidoklasser. Detta är inte en tillfällighet utan en konsekvens av några enkla egenskaper hos sidoklasserna. Nu skall vi diskutera dessa egenskaper och därefter återkomma till exempel. □

(7.3) Proposition. (a) $g \in Hg$

dvs. varje element $g \in G$ tillhör en vänstersidoklass till H.

(b) $g \in Hg_1 \cap Hg_2 \Rightarrow Hg_1 = Hg_2$

dvs två högersidoklasser som har ett gemensamt element är identiska, eller med andra ord, två olika högersidoklasser saknar gemensamma element.

(c) $g' \in Hg \Leftrightarrow Hg' = Hg$

dvs varje element i en högersidoklass kan väljas som dess representant.

(d) $g' \in Hg \Leftrightarrow g'g^{-1} \in H$ (*additivt:* $g' \in H + g \Leftrightarrow g' - g \in H$).

Bevis. (a) $g = eg \in Hg$ ty $e \in H$.

(b) Enligt förutsättningen är $g = h_1g_1 = h_2g_2$ där $h_1, h_2 \in H$. Vi har $x \in Hg_1 \Rightarrow x = hg_1, h \in H \Rightarrow x = h(h_1^{-1}h_2g_2) = (hh_1^{-1}h_2)g_2 \Rightarrow x \in Hg_2$ ty $hh_1^{-1}h_2 \in H$. Detta visar att $Hg_1 \subseteq Hg_2$. På samma sätt får vi $Hg_2 \subseteq Hg_1$. Alltså är $Hg_1 = Hg_2$.

(c) $g' \in Hg \Rightarrow g' \in Hg' \cap Hg$ (ty $g' \in Hg'$) $\Rightarrow Hg' = Hg$ enligt (b).

(d) $g' \in Hg \Leftrightarrow g' = g' = hg$ för något $h \in H \Leftrightarrow g'g^{-1} = h \in H$. □

(7.4) Anmärkning. Egenskaperna (a) och (b) säger att högersidoklasserna Hg ger en partition av G dvs en uppdelning av alla element i G i parvis disjunkta delmängder (se (2.4) (c)). Detta betyder att högersidoklasserna definierar en ekvivalensrelation på G (se definitionen av ekvivalensrelationer (2.3)). Två gruppelement $x, y \in G$ är relaterade till varandra om de tillhör samma högersidoklass, vilket betyder att $x \sim y$ då och endast då det finns $z \in G$ så att $x, y \in Hz$. Enligt (b) ovan betyder det att $Hx = Hy$ dvs $xy^{-1} \in H$ enligt (d) ($Hx = Hy$ ger $x \in Hy$ så att $xy^{-1} \in H$ enligt (d)). Vi skall titta på några ytterligare exempel på partitioner av grupper med hjälp av högersidoklasser. I praktiska sammanhang när man vill beskriva alla element hörande till en högersidoklass Hg utnyttjar man egenskapen (d). □

(7.5) Exempel. (a) Vi fortsätter exempel (7.2). Vi har $n' \in < 5 > +n$ då och endast då $n' - n \in < 5 >$ enligt (7.3) (d), dvs $5|n' - n$. Man kan uttrycka det också som

$$n' \in < 5 > +n \Leftrightarrow [n']_5 = [n]_5.$$

Detta betyder att sidoklassen $< 5 > +n$ består av alla tal som lämnar resten $[n]_5$ vid division med 5. Men $[n]_5 = 0, 1, 2, 3, 4$ så at sidoklassrna är $< 5 > +0 = < 5 >, < 5 > +1, < 5 > +2, < 5 > +3, < 5 > +4$.

(b) Låt $G = \mathbb{R}^*$ vara gruppen av de reella talen $\neq 0$ och låt $H = \mathbb{R}^*_{>0}$ bestå av positiva reella tal. Då $r \in Hr \Leftrightarrow r'r^{-1} \in H = \mathbb{R}^*_{>0}$ enligt (7.3) (d) dvs $\frac{r'}{r} > 0$. Alltså tillhör r' sidoklassen Hr då och endast då r' har samma tecken som r. Men r kan ha två tecken – plus eller minus. Alltså får vi två sidoklasser – den ena är $H = \mathbb{R}^*_{>0}$ med $+1$ som en representat, den andra $H \cdot (-1) = -\mathbb{R}^*_{>0}$ med -1 som en representant.

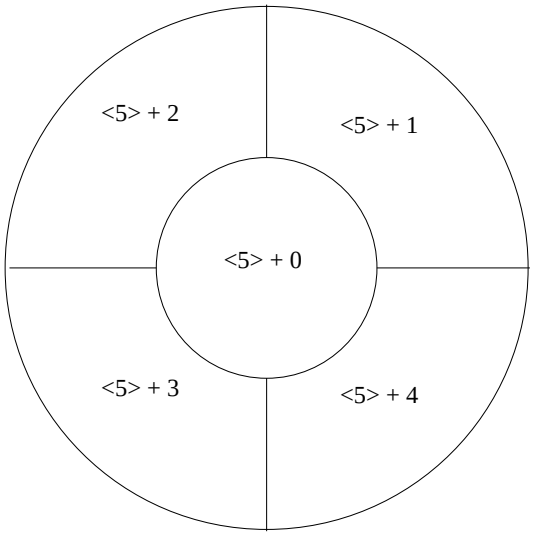


fig. 1

(c) Låt $G = \mathbb{R}^2$ vara gruppen av alla vektorer i planet med avseende på addition av vektorer. Låt H vara den undergrupp till G som består av alla vektorer på x-axeln (fig. 2). Om $\mathbf{v}$ är en vektor så består sidoklassen $H + \mathbf{v}$ av alla vektorer som man får genom att addera $\mathbf{v}$ till alla vektorer på x-axeln. Då får man alla vektorer som slutar på den linje som är parallell med x-axeln och som går genom ändpunkten av $\mathbf{v}$. Olika sådana linjer svarar mot olika sidoklasser. Allmänt är $\mathbf{v}' \in H + \mathbf{v} \Leftrightarrow \mathbf{v}' - \mathbf{v} \in H$ dvs $\mathbf{v}' - \mathbf{v}$ är parallell med x-axeln, eller med andra ord, ändpunkten av $\mathbf{v}'$ ligger på den linje som går genom ändpunkten av $\mathbf{v}$ och är parallell med x-axeln. □

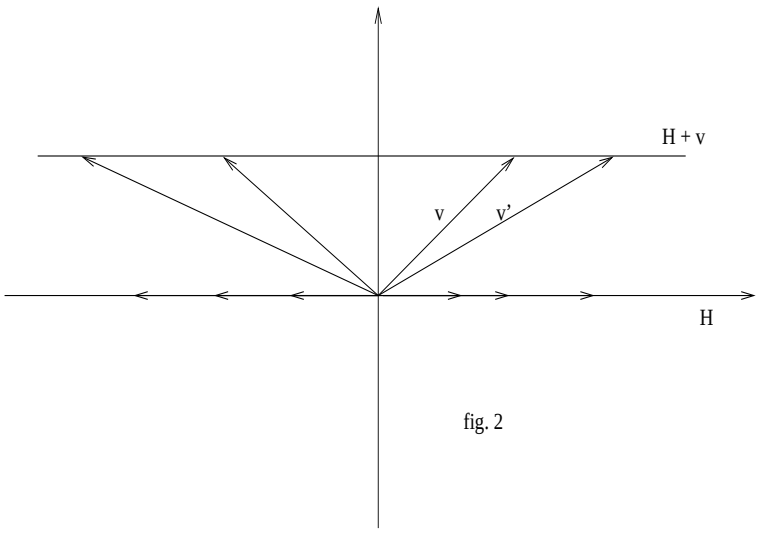


fig. 2

(7.6) Anmärkning. Man kan naturligtvis definiera **vänstersidoklasser**

$$gH = \{gh : h \in H\}.$$

Om gruppen är abelsk har vi $gH = Hg$. Då använder vi oftast termen "sidoklass" i stället för "vänstersidoklass" eller "högersidoklass". Alla egenskaper hos högersidoklasser i (7.3) visas analogt för vänstersidoklasser. När gruppen inte är abelsk kan det finnas en distinktion mellan vänster– och högersidoklasser.

Betrakta nu ett exempel. □

(7.7) Exempel. Låt G vara symmetrigruppen av en liksidig triangel (se exempel (6.7) (a)). Låt $H = \{I, s_1\}$, där $s_1 = (2, 3)$. Här har vi följande vänster- och höger- sidoklasser:

$$\begin{aligned} IH &= s_1H = \{I, s_1\}, \qquad HI = Hs_1 = \{I, s_1\}, \\ v_1H &= s_3H = \{v_1, s_3\}, \qquad Hv_1 = Hs_2 = \{v_1, s_2\}, \\ v_2H &= s_2H = \{v_2, s_2\}, \qquad Hv_2 = Hs_3 = \{v_2, s_3\}. \end{aligned}$$

Vi ser att t ex $s_2H \neq Hs_2$. □

Antalet sidoklasser till H i G är nära relaterat till ordningarna av H och G. Vi har redan sett att antalet element i varje sidoklass är lika med antalet element i H. Detta är ingen tillfällighet:

(7.8) Proposition. *Låt H vara en ändlig grupp. Då är $|Hg| = |H|$ för $g \in G$.*

Bevis. Låt $H = \{h_1, h_2, \ldots, h_m\}$. Då är $Hg = \{h_1g, h_2g, \ldots, h_mg\}$. Alla produkter h_ig är olika ty $h_ig = h_jg$ ger $h_i = h_j$ (multiplicera med g^{-1} från höger!). □

(7.9) Lagranges sats*. *Ordningen av en undergrupp till en ändlig grupp är en delare till gruppens ordning.*

Bevis. Låt G vara en ändlig grupp och H en delgrupp till G. Vi vill visa att $o(H)|o(G)$. Vi delar G i högersidoklasserna till H. Sidoklasserna täcker hela gruppen enligt (7.3) (a). Olika sidoklasser saknar gemensamma element enligt (7.3) (b). Antalet element i varje sidoklass är lika emd antalet element i H enligt (7.8). Låt i vara antalet högersidoklasser. Då är $o(G) = o(H) \cdot i$ dvs $o(H)$ är en delare till $o(G)$ och kvoten $o(G)/o(H)$ är lika med antalet högersidoklasser. □

(7.10) Följdsats. *Låt G vara en ändlig grupp och H dess delgrupp. Då är antalet högersidoklasser till H i G lika med antalet vänstersidoklasser till H i G. Bägge är lika med $o(G) : o(H)$.*

*Joseph Louis Lagrange 1736 - 1813.

Bevis. Beviset av Lagranges sats visar att antalet högersidoklasser är lika med $o(G) : o(H)$. När man bevisar Lagranges sats med hjälp av vänstersidoklasser i stället för högersidoklasser (som ovan) får man att $o(G) : o(H)$ är lika med antalet vänstersidoklasser. □

(7.11) Definition. Antalet högersidoklasser (eller vänstersidoklasser) till H i G kallar man för **index** av H i G. Indexet betecknas ofta med $[G : H]$. □

(7.12) Följdsats. *Ordningen av ett element i en ändlig grupp är en delare till gruppens ordning.*

Bevis. Om $g \in G$ så är ordningen $o(g)$ av g lika med ordningen av den undergrupp som g genererar (dvs den undergrupp som består av alla potenser av g). Enligt Lagranges sats är alltså $o(g)$ en delare till $o(G)$. □

(7.13) Följdsats. *Om $o(G) = N$ och $g \in G$ så är $g^N = e$.*

Bevis. Om $o(g) = n$ så är $n|N$ enligt (7.12). Låt $N = n \cdot i$. Då är $g^N = (g^n)^i = e$ ty $g^n = e$ se ((4.12)). □

(7.14) Exempel. Med hjälp av Lagranges sats skall vi beskriva alla undergrupper till kvadratgruppen. $G = \{I, v_1, v_2, v_3, s_1, s_2, s_3, s_4\}$ och grupptabellen finns på sid. 36. Vi har $o(v_1) = o(v_3) = 4, o(v_2) = 2, o(s_1) = o(s_2) = o(s_3) = o(s_4) = 2$. Om H är en undergrupp till G, så är $o(H) = 1, 2, 4$ eller 8. Det är klart att $o(H) = 1$ ger $H = \{I\}$, och $o(H) = 8$ ger $H = G$ – de två triviala undergrupperna. Om $o(H) = 2$, så måste $H = \{I, g\}$, där g har ordningen 2. Vi vet att det finns 5 sådana $g : g = v_2$ eller s_1 eller s_2 eller s_3 eller s_4. Alltså har vi fem undergrupper av ordningen 2: $\{I, v_2\}, \{I, s_1\}, \{I, s_2\}, \{I, s_3\}, \{I, s_4\}$.

Nu antar vi att $o(H) = 4$ Det finns säkert en undergrupp – $H_1 = \{I, v_1, v_2, v_3\}$. Den består av alla vridningar av kvadraten. Låt H vara en undergrupp som innehåller minst en symmetri. H kan inte innehålla v_1 eller v_3 eftersom deras potenser ger alla vridningar (4 stycken). Detta innebär att H måste innehålla två symmetrier. Om H innehåller s_1, så måste den andra vara s_2, ty $s_1S_2 = v_2$, däremot är $s_1s_3 = v_1$ och $s_1s_4 = v_3$ inte tillåtna. Om H innehåller s_3, så måste den andra vara s_4, ty $s_3s_4 = v_2$, däremot $s_3s_1 = v_3$ och $s_3s_2 = v_1$. Vi får två möjliga undergrupper av ordningen 4: $H_2 = \{I, v_2, s_1, s_2\}$ och $H_3 = \{I, v_2, s_3, s_4\}$. Det finns alltså högst 3 undergrupper av ordningen 4. Vi vet att H_1 är en undergrupp och vi kontrollerar enkelt att H_2 och H_3 också är undergrupper. Det är intressant att tolka dessa grupper geometriskt. H_1 består av alla vridningar av kvadraten. H_2 är symmetrigruppen av en rektangel som inte är en kvadrat (fig. 3 (a)), däremot H_3 är symmetrigruppen av en romb som inte är en kvadrat (fig. 3 (b)). □

ÖVNINGAR

7.1. Beskriv alla (höger-)sidoklasser till H i G då

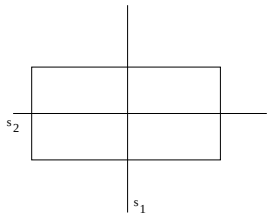


fig. 3 (a)

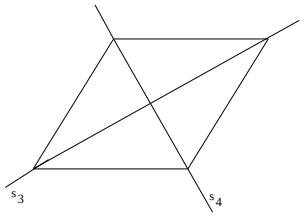


fig. 3 (b)

(a) $G = \mathbb{Z}$ (med addition) och $H =< 3 >$,

(b) $G = \mathbb{C}^*$ (de komplexa talen med multiplikation) och $H = \{z \in \mathbb{C}^* : |z| = 1\}$,

(c) $G = \mathbb{C}^*, H = \mathbb{R}^*$ (de reella talen $\neq 0$ med multiplikation),

(d) $G = \mathbb{C}^*, H = \mathbb{R}^*_+$ (de reella positiva talen),

(e) $G = GL_2(\mathbb{R})$ ((2×2)-reella matriser med determinant $\neq 0$), $H = SL_n(\mathbb{R}) = \{A \in G : \det A = 1\}$,

(f) $G = \mathbb{Z}_{18}$, $H =< 3 >$.

7.2. Låt $g \in G$ och $o(g) = n$. Visa att om $g^N = e$ så är $n|N$.

7.3. Låt $G = \mathbb{Z}_2^3$. Skriv ut alla sidoklasser till $H = \{000, 111\}$ i G.

7.4. Beskriv alla delgrupper till följande grupper:

(a) symmetrigruppen av en rektangel som inte är en kvadrat,

(b) symmetrigruppen av en liksidig triangel,

(c) $\mathbb{Z}_6$, (d) $\mathbb{Z}_{100}$, (e) $\mathbb{Z}_2 \times \mathbb{Z}_2$, (f) $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Ledning: I (c) och (d) utnyttja övning 4.11 som säger att varje delgrupp till en cyklisk grupp är cyklisk.

7.5. Ge exempel på en delgrupp H till $\mathbb{Q}^*$ (de rationella talen $\neq 0$ med multiplikation) sådan att $H \neq \mathbb{Q}^*$ och index av H i $\mathbb{Q}^*$ är ändligt.

7.6. Visa att en oändlig grupp har oändligt många delgrupper.

7.7. Visa att en grupp G har exakt två delgrupper ($< e >$ och G) om och endast om $o(G)$ är ett primtal.

7.8. Med **exponenten** av en grupp G menas det minsta positiva heltalet m sådant att $g^m = e$ för varje element $g \in G$. Om m inte existerar säger man att gruppens exponent är oändlig.

(a) Visa att varje ändlig grupp har en ändlig exponent.

(b) Ge exempel på en oändlig grupp med en ändlig exponent.

(c) Beräkna exponenten för: $\mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_m \times \mathbb{Z}_n$.

(d) Visa att exponenten av en ändlig abelsk grupp är lika med maximalordningen av gruppens element

Ledning: I (d) utnyttja formeln $o(ab) = o(a)o(b)$ då a, b är två element i gruppen vars ordningar är relativt prima (se övning 6.9).

7.9. Skriv ut alla element i gruppen A_4 av alla jämna permutationer av 1,2,3,4. Visa att denna grupp saknar en delgrupp av ordning 6 ($o(A_4) = 12$).

7.10. Visa att en grupp G vars ordning är ett primtal är cyklisk.

Kapitel 8

RINGAR OCH KROPPAR

Grupper är mängder med en operation. Men så viktiga mängder som $\mathbb{Z}$ eller $\mathbb{Z}_n$ har två naturliga operationer – addition och multiplikation. Den situationen är så pass vanlig att man har en allmän teori av liknande matematiska objekt. De kallas ringar.

(8.1) Definition. Låt R vara en mängd med två binära operationer – addition "+" och multiplikation "$\cdot$". $(R, +, \cdot)$ kallas **ring** om

(a) $(R, +)$ är en abelsk grupp,

(b) $a(bc) = (ab)c$ då $a, b, c \in R$ dvs multiplikation är associativ,

(c) $a(b + c) = ab + ac$ och $(b + c)a = ba + ca$ då $a, b, c \in R$ dvs multiplikation är distributiv m.a.p. addition. □

(8.2) Anmärkning. Observera att vi oftast skriver ab i stället för $a \cdot b$. Det neutrala elementet i gruppen $(R, +)$ brukar betecknas med 0. Vanligen säger man att R är en ring utan att använda beteckningen $(R, +, \cdot)$. □

(8.3) Exempel. (a) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ är ringar.

(b) $(\mathbb{Z}_n, \oplus, \odot)$ är en ring. Den enda egenskap som vi inte visade i Kapitel 5 är distributiviteten av $\odot$ m.a.p. $\oplus$. Den visas lätt med hjälp av (5.1) och (5.2):

$$\begin{aligned} a \odot (b \oplus c) &= a \odot [b + c]_n = [a(b + c)]_n = [ab + ac]_n = \\ &= [ab]_n \oplus [ac]_n = [a]_n \odot [b]_n \oplus [a]_n \odot [c]_n \\ &= a \odot b \oplus a \odot c \end{aligned}$$

för $a, b, c \in \mathbb{Z}_n$.

(c) Låt $R = M_n(\mathbb{R})$ mängden av alla $(n \times n)$-reella matriser med matrisaddition och matrismultiplikation. $M_n(\mathbb{R})$ är en ring vilket sammanfattar de viktigaste räknelagarna för matrisaritmetik. Dessa räknelagar visas i alla kurser i linjär algebra (oftast utan att använda termen ring).

(d) Låt $R = C(0,1)$ vara mängden av alla kontinuerliga funktioner på intervallet $(0,1)$ med addition $f+g$ och multiplikation fg av funktioner dvs

$$(f+g)(x) = f(x)+g(x) \quad \text{och} \quad (fg)(x) = f(x)g(x)$$

då $x \in (0,1)$. R är en ring. Man kan naturligtvis ersätta intervallet $(0,1)$ med ett godtyckligt intervall. □

I en ring $(R,+,\cdot)$ har man en blandning av två operationer. Men medan man kräver relativt mycket från den ena – $(R,+)$ skall vara en abelsk grupp, ställer man inte så stora krav på den andra – $(R,\cdot)$ behöver enbart vara en halvgrupp (dvs en mängd med en associativ multiplikation). Ofta betraktar man ringar i vilka $(R,\cdot)$ uppfyller hårdare restriktioner. Här följer några sådana villkor:

(8.4) Definition. Låt $(R,+,\cdot)$ vara en ring.

(a) R är **kommutativ** om $ab = ba$ då $a,b \in R$.

(b) R har en **etta** om det finns ett neutralt element $1 \in R$ m.a.p. multiplikation dvs $1a = a1 = a$ då $a \in R$.

(c) R saknar **nolldelare** om $ab = 0$ ger $a = 0$ eller $b = 0$ då $a,b \in R$ (om $ab = 0$ där $a \neq 0$ och $b \neq 0$ så kallas a och b **nolldelare**).

(d) R är en **kropp** om $(R \setminus \{0\},\cdot)$ är en abelsk grup. □

(8.5) Exempel. (a) Alla ringar i exempel (8.3) är kommutativa med undantag av $M_n(\mathbb{R})$ då $n \geq 2$.

(b) Alla rignar i exempel (8.3) har en etta. Ett exempel på en ring utan etta är ringen av de jämna heltalen med vanlig addition och multiplikation.

(c) Alla rignar i exempel (8.3) (a) saknar nolldelare. Men det finns nolldelare i t.ex. $\mathbb{Z}_6$ ty $2 \odot 3 = 0$ (se vidare övning 8.9). Ringen $M_2(\mathbb{R})$ ur (8.3) (c) har nolldelare ty t.ex.

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

(d) $(\mathbb{Q},+,\cdot), (\mathbb{R},+,\cdot), (\mathbb{C},+,\cdot)$ är exempel på kroppar. $(\mathbb{Z},+,\cdot)$ är inte en kropp ty $(\mathbb{Z} \setminus \{0\},\cdot)$ är inte en grup. □

Ringarna ur (8.3) (b) är särskilt viktiga:

(8.6) Sats. *$(\mathbb{Z}_n, \oplus, \odot)$ är en kropp då och endast då n är ett primtal.*

Bevis. Om $n = p$ är ett primtal så är $\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*$ en grupp m.a.p. $\odot$ enligt (5.4) dvs $\mathbb{Z}_p$ är en kropp. Om n inte är ett primtal dvs $n = kl$ med $1 < k,l < n$ så är $k \odot l = 0$ i $\mathbb{Z}_n$ dvs

$\mathbb{Z}_n \setminus \{0\}$ är inte sluten m.a.p. multiplikation. Detta betyder att $\mathbb{Z}_n \setminus \{0\}$ inte är en grupp och följaktligen $(\mathbb{Z}_n, \oplus, \odot)$ inte är en kropp. □

(8.7) Definition. Man säger att en ring R är ett **integritetsområde** om R är kommutativ, saknar nolldelare och har en etta $1 \neq 0$. □

(8.8) Exempel. (a) Varje kropp K är ett integritetsområde ty $ab = 0$ och $a \neq 0$ ger att $a^{-1}(ab) = b = 0$, där $a, b \in K$ så att K saknar nolldelare.

(b) $\mathbb{Z}_n$ är ett integritetsområde då och endast då n är ett primtal. Detta följer ur (8.6). Om n är ett primtal så är $\mathbb{Z}_n$ en kropp och vi kan hänvisa till (a). Om $n = kl$, $1 < k, l < n$ så har $\mathbb{Z}_n$ nolldelare ty $k \odot l = 0$ trots att $k \neq 0 \neq l$. □

Nu skall vi utvidga vår lista med exempel på ringar med två viktiga ringkonstruktioner:

(8.9) Polynomringar. Låt R vara en komutativ ring med etta. Med ett polynom med koefficienter i R menar man ett uttryck

$$a_0 + a_1X + \ldots + a_nX^n,$$

där $a_i \in R$. Mängden av alla polynom med koefficienter i R är en ring med avseende på addition:

$$(a_0 + a_1X + a_2X^2 + \ldots) + (b_0 + b_1X + b_2X^2 + \ldots) =$$

$$= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 \ldots$$

och multiplikation:

$$(a_0 + a_1X + a_2X^2 + \ldots)(b_0 + b_1X + b_2X^2 + \ldots) =$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \ldots$$

Polynomringen av alla polynom med koefficienter i R betecknas med $R[X]$. Det faktum att $R[X]$ är en ring med avseende på addition och multiplikation av polynom kräver naturligtvis en kontroll av alla villkor i definitionen (8.1) men vår erfarenhet av vanliga polynom med t.ex. reella koefficienter (dvs ringen $\mathbb{R}[X]$) borde vara tillräcklig för att kunna acceptera att alla formella villkor i ringdefinitionen verkligen gäller.

Det finns dock en aspekt av definitionen av $R[X]$ som en läsare krävande en större matematisk stringens kan ifrågasätta. Ett polynom definieras som "ett uttryck". Och en sådan formulering

kan vara otillfrädställande (t.ex. för den som inte ser uttrycket). Vill man undvika den, kan man definiera ett polynom som en oändlig följd:

$$(a_0, a_1, a_2, \ldots, a_n, \ldots)$$

där $a_i \in R$ och $a_i \neq 0$ endast för ett ändligt antal i. Man definierar addition och multiplikation av följderna så att:

$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$

och

$$(a_0, a_1, \ldots, a_n, \ldots)(b_0, b_1, \ldots, b_n, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, \ldots, a_0b_n + a_1b_{n-1} + \ldots + a_nb_0, \ldots)$$

Nu kan vi definiera $X = (0, 1, 0, \ldots)$. Då är

$$\begin{aligned} X^2 &= (0, 0, 1, 0, 0, \ldots), \\ X^3 &= (0, 0, 0, 1, 0, 0, \ldots) \\ X^4 &= (0, 0, 0, 0, 1, \ldots) \\ &\ldots \end{aligned}$$

och vi har:

$$(a_0, a_1, a_2, \ldots, a_n, \ldots) =$$
$$(a_0, 0, \ldots) + (a_1, 0, \ldots)X + (a_2, 0, \ldots)X^2 + \ldots + (a_n, 0, \ldots)X^n + \ldots$$

Om vi nu kommer överens om att i stället för $(a, 0, \ldots)$ skriva a (dvs vi identifierar a med "konstantpolynom" $(a, 0, \ldots)$) så har vi vårt tidigare uttryck:

$$(a_0, a_1, a_2, \ldots, a_n, \ldots) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n + \ldots$$

fast med oändligt många koefficienter a_i (men enbart ett ändligt antal av dessa är $\neq 0$). Det utan tvivel viktigaste exemplet för olika typer av tilämpningar är ringen $\mathbb{Z}_2[X]$ av alla polynom med koefficienter i $\mathbb{Z}_2$. Vi diskuterar polynomringarna närmare i (9).

(8.10) Produkt av rignar. Låt $R_1, R_2, \ldots, R_k$ vara ringar. Mängden

$$R_1 \times R_2 \times \ldots \times R_k$$

är en ring med avseende på koordinatvis addition och multiplikation dvs

$$\begin{aligned} (r_1, r_2, \ldots, r_k) + (r_1', r_2', \ldots, r_k') &= (r_1 + r_1', r_2 + r_2', \ldots, r_k + r_k'), \\ (r_1, r_2, \ldots, r_k)(r_1', r_2', \ldots, r_k') &= (r_1r_1', r_2r_2', \ldots, r_kr_k'). \end{aligned}$$

Ringen $R_1 \times R_2 \times \ldots \times R_k$ kallas **produkten** av ringarna $R_1, R_2, \ldots, R_k$. Om $R_1 = R_2 = .. = R_k = R$ skriver man oftast R^k.

Exempel. $\mathbb{R}^2$ är ringen av alla reella talpar med koordinatvis addition och multiplikation. $\mathbb{Z}^2$ är ringen av alla heltaliga talpar med samma operationer. □

(8.11) Definition. Man säger att S är en **delring** till R om $S \subseteq R$ och elementen i S bildar en ring med avseende på operationerna i R. □

Exempel. $(\mathbb{Z}, +, \cdot) \subset (\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot) \subset (\mathbb{C}, +, \cdot)$. □

(8.12) Definition. Ett element $r \in R$ kallar man för en **enhet** om r har en multiplikativ invers dvs det finns $r' \in R$ så att $rr' = r'r = 1$. Mängden av alla enheter i R betecknas med R^*. □

(8.13) Sats. *Alla enheter i en kommutativ ring med etta R bildar en (abelsk) grupp med avseende på multiplikation.*

Bevis. Om $r_1, r_2 \in R^*$ så $r_1 r_2 \in R^*$ ty $r_1 r_1' = 1$ och $r_2 r_2' = 1$ ger att $(r_1 r_2)(r_1' r_2') = 1$. Multiplikation är associativ, det neutrala elementet är 1 och definitionsmässigt finns en invers till varje $r \in R$. □

(8.14) Exempel. (a) $\mathbb{Z}$ har enbart två enheter ± 1.

(b) Om K är en kropp så är alla element $a \in K$, $a \neq 0$ enheter ty $(K \setminus \{0\}, \cdot)$ är en grupp. □

(8.15) Sats. *Gruppen av alla enheter i $\mathbb{Z}_n$ är $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n : SGD(k, n) = 1\}$.*

Bevis. Vi vet redan från (5.4) att varje $k \in \mathbb{Z}_n$ sådant att $SGD(k, n) = 1$ har invers. Antag att $k \in \mathbb{Z}_n$ har invers $k' \in \mathbb{Z}_n$ dvs $k \odot k' = 1$. Alltså är $kk' - 1 = nq$ för ett heltal q. Den sista likheten visar att k och n saknar gemensamma delare $\neq 1$ dvs $SGD(k, n) = 1$. □

ÖVNINGAR

8.1. Vilka av följande talmängder är ringar med avseende på addition och multiplikation av tal? Vilka är kroppar?

(a) $3\mathbb{Z}$,
(b) $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$,
(c) $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a, b, d \in \mathbb{Z}\}$,
(d) alla tal $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$,
(e) alla tal $a + b\sqrt[3]{2}$, $a, b \in \mathbb{Q}$,
(f) alla tal $\frac{a}{b}$, $a, b \in \mathbb{Z}, b$ udda.

8.2. Vilka av följande mängder av matriser är ringar med avseende på matrisaddition och matrismultiplikation? Vilka är kroppar?

(a) $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, a, b \in \mathbb{R}$,
(b) $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, a, b, c \in \mathbb{Z}$,
(c) $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in \mathbb{Z}_2$,
(d) $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a, b \in \mathbb{R}$,
(e) $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a, b \in \mathbb{Z}_2$,
(f) $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a, b \in \mathbb{Z}_3$.

8.3. Låt R vara en ring och X en mängd. Visa att alla funktioner $f : X \to R$ bildar en ring $\mathcal{F}(X, R)$ under operationerna:

$$(f+g)(x) = f(x) + g(x) \quad \text{och} \quad (fg)(x) = f(x)g(x) \quad \text{för} \quad x \in X.$$

Har $\mathcal{F}(X, R)$ en etta? Har $\mathcal{F}(X, R)$ nolldelare?

8.4. Låt $\mathcal{F}(\mathbb{R}, \mathbb{R})$ vara ringen ur 8.3 ($X = \mathbb{R}, R = \mathbb{R}$). Vilka av följande delmängder till $\mathcal{F}(\mathbb{R}, \mathbb{R})$ är delringar?

(a) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(x) = f(-x)\}$ (jämna funktioner)

(b) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(-x) = -f(x)\}$ (udda funktioner)

(c) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f$ kontinuerlig$\}$

(d) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f$ deriverbar$\}$

(e) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(x_0) = 0, x_0$ et fixt reellt tal$\}$.

8.5. Låt $R \subseteq S$ vara ringar med en gemensam etta och låt $a \in S$. Visa att varje delring till S som innehåller R och a innehåller alla polynomuttryck $a_0 + a_1 a + \ldots + a_n a^n$ där $a_i \in R$, $n \geq 1$. Den ringen betecknas med $R[a]$. Visa att

(a) $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$, (b) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$,
(c) $\mathbb{Q}[i] = \{a + bi, a, b \in \mathbb{Q}\}$, (d) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, a, b \in \mathbb{Z}\}$,
(e) $\mathbb{Z}[5] = \mathbb{Z}$, (f) $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^m}, a, m \in \mathbb{Z}, m \geq 0\}$.

8.6. Låt $K \subseteq L$ vara kroppar och låt $\alpha \in L \setminus K, \alpha^2 \in K$. Visa att $K[\alpha] = \{a + b\alpha, a, b \in K\}$ är en kropp.

8.7. Visa att alla matriser

$$\begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix}$$

där $z_1, z_2 \in \mathbb{C}$ bildar en ring med avseende på matrisaddition och matrismultiplikation (en delring till ringen $M_2(\mathbb{C})$ av alla 2×2 komplexa matriser). Visa att ringen är icke-kommutativ och att varje element $\neq 0$ har invers.

Anmärkning: En ring med den egenskapen kallas **skevkropp** eller **divisionsring**. Ringen i övningen kallas **kvaternioner** eller mera exakt **Hamiltons kvaternioner**. Hamilton kom på idéen om kvaternioner år 1843 under en promenad längs Royal Canal i Dublin. Till minne av den händelsen finns idag en tavla vid Hamiltons promenadväg på Brougham Bridge där man återfinner huvudregler för kvaternionaritmetiken: $i^2 = j^2 = k^2 = ijk = -1$. Med vår definition är

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad j = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}, \quad k = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \quad .$$

8.8. Visa att i en godtycklig ring R:

(a) $0a = a0 = 0$

(b) $a(-b) = (-a)b = -ab$

(c) $(-a)(-b) = ab$

(d) $-(-a) = a$

8.9. Visa att $\mathbb{Z}_n$ har nolldelare då och endast då n är sammansatt.

8.10. Visa att ett ändligt integritetsområde är en kropp.

Ledning. Låt $R = \{0, a_1, a_2, \ldots, a_n\}$, där $a_1 = 1$ och låt $a \in R$, $a \neq 0$. Betrakta produkterna $aa_1, aa_2, \ldots, aa_n$ och visa att 1 är bland dem.

8.11. Bestäm alla enheter i följande ringar:

(a) $\mathbb{R}[X]$,

(b) $\mathbb{Z}[i]$

(c) $\mathbb{Z}[\sqrt{-d}], d \in \mathbb{Z}, d > 0$.

8.12. (a) Låt R_1 och R_2 vara två kommutativa ringar med etta. Visa att $(R_1 \times R_2)^* = R_1^* \times R_2^*$.

(b) Låt a och b vara två relativt prima positiva heltal. Utnyttja (a) och isomorfismen $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ (se (5.9)) för att bevisa att Eulers funktion är multiplikativ dvs $\phi(ab) = \phi(a)\phi(b)$ då $SGD(a, b) = 1$.

8.13. En funktion $E : \mathbb{Z}_n \to \mathbb{Z}_n$ kallas **modulär krypteringsfunktion** om $E(x) = r \odot x \oplus k$ (vi skriver vidare $rx + k$), där $SGD(r, n) = 1$. Om $r = 1$ kallar man E för **Caesarkryptot** (med t.ex. $n = 26$). Visa att E är en bijektion och bestäm inversen D till E.

Anmärkning: Med hjälp av en modulär krypteringsfunktion krypteras klartexten $r_1 r_2 \ldots r_n$ till $E(r_1)E(r_2)\ldots E(r_n)$. Låt $E_i : \mathbb{Z}_n \to \mathbb{Z}_n$ vara modulära krypteringsfunktioner för $i = 1, 2, \ldots, p$. Med ett **periodiskt substitutionskrypto** menar man karypterignsfunktionen $E : \mathbb{Z}_n^N \to \mathbb{Z}_n^N$ sådan att en klartext av längden N:

$$r_1 r_2 \ldots r_p r_{p+1} r_{p+2} \ldots r_{2p} \ldots$$

krypteras till

$$E_1(r_1)E_2(r_2)\ldots E_p(r_p)E_1(r_{p+1})E_2(r_{p+2})\ldots E_p(r_{2p})\ldots$$

Ett specialfall av detta krypto är **Vigenérekryptot**. Då är $E_i(x) = x + k_i$ varvid $k_1 k_2 \ldots k_p \in \mathbb{Z}_n^p$ svarar mot ett "ord" (t.ex. $n = 26, (k_1, k_2, k_3, k_4, k_5, k_6)$=(0, 11,6,4,1,17,0) = "ALGEBRA"). **Vernamskryptot** är uppbyggt på liknande sätt mend $i = 1, 2, \ldots, N$ dvs $(k_1, k_2, \ldots, k_n)$ har smama längd som klartexten dvs $r_1 r_2 \ldots r_n$ krypteras till $E_1(r_1)E_2(r_2)\ldots E_N(r_n)$. Sekvensen $(k_1, k_2, \ldots, k_N)$ är lagrad både hos sändaren och mottagaren och är helt slumpmässigt vald.

Kapitel 9

POLYNOMRINGAR

Låt R vara en kommutativ ring med etta. Som vi redan vet från (8.9) är ett polynom med koefficienter i R ett uttryck

$$a_0 + a_1X + \ldots + a_nX^n,$$

där $a_i \in R$. Mängden av alla polynom med koefficienter i R är en ring med avseende på addition:

$$(a_0 + a_1X + a_2X^2 + \ldots) + (b_0 + b_1X + b_2X^2 + \ldots) =$$

$$= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \ldots$$

och multiplikation:

$$(a_0 + a_1X + a_2X^2 + \ldots)(b_0 + b_1X + b_2X^2 + \ldots) =$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \ldots$$

Polynomringen av alla polynom med koefficienter i R betecknas med $R[X]$. Det faktum att $R[X]$ är en ring med avseende på addition och multiplikation av polynom kräver naturligtvis en kontroll av alla villkor, men vår erfarenhet av vanliga polynom med t.ex. reella koefficienter (dvs ringen $\mathbb{R}[X]$) borde vara tillräcklig för att kunna acceptera att alla formella villkor i ringdefinitionen verkligen gäller.

(9.1) Definition. Låt $f(X) = a_0 + a_1X + \ldots + a_nX^n \in R[X]$ där R är en kommutativ ring med etta. Om $a_n \neq 0$ så säger man att **graden** av $f(X)$ är n. Vi antar att graden av nollpolynomet (dvs $a_0 = a_1 = \ldots = a_n = 0$) är -1. a_n kallas **högsta koefficienten** av $f(X)$. Polynom av graden 0 kallas **konstanta polynom**. □

(9.2) Divisionsalgoritmen. *Låt $f(X), g(X) \in R[X]$, där $g(X)$ är ett polynom vars högsta koefficient är en enhet i R. Då finns det två entydigt bestämda polynom $q(X), r(X) \in R[X]$ sådana att*

$$f(X) = g(X)q(X) + r(X)$$

där $\operatorname{grad} r(X) < \operatorname{grad} g(X)$.

Bevis. Vi bevisar satsen med hjälp av induktion efter graden av $f(X)$. Om graden av $f(X)$ är -1 (dvs $f(X)$ är nollpolynomet) så är $f(X) = g(X) \cdot 0$ dvs $q(X) = 0$ och $r(X) = 0$. Nu antar vi att satsen gäller för alla polynom $f(X)$ vars grad är $< n$, där $n \geq 0$. Låt $f(X) = a_nX^n + \ldots + a_0$, $g(X) = b_mX^m + \ldots + b_0$ där $a_n \neq 0$, och b_m är en enhet. Om $n < m$ så har vi $f(X) = g(X) \cdot 0 + f(X)$ dvs $q(X) = 0$ och $r(X) = f(X)$. Antag att $n \geq m$. Låt

$$f_1(X) = f(X) - \frac{a_n}{b_m} g(X) X^{n-m}$$

Då är grad $f_1(X) <$ grad $f(X)$ så att

$$f_1(X) = g(X)q_1(X) + r(X), \text{ grad } r(X) < \text{grad } g(X)$$

enligt induktionsantagandet. Men då är

$$f(X) = f_1(X) + \frac{a_n}{b_m} g(X) X^{n-m} = g(X)(q_1(X) + \frac{a_n}{b_m} X^{n-m}) + r(X)$$

dvs

$$f(X) = g(X)q(X) + r(X), \quad \operatorname{grad} r(X) < \operatorname{grad} g(X)$$

där $q(X) = q_1(X) + \frac{a_n}{b_m} X^{n-m}$.

Det återstår att visa entydigheten av q och r. Antag att

$$f(X) = g(X)q(X) + r(X) = g(X)q_1(X) + r_1(X)$$

där även $\operatorname{grad} r_1(X) < \operatorname{grad} g(X)$. Då är

$$(*) \qquad g(X)(q(X) - q_1(X)) = r_1(X) - r(X)$$

Men $\operatorname{grad}(r_1(X) - r(X)) < \operatorname{grad} g(X)$, medan likheten $(*)$ säger att om $q(X) - q_1(X) \neq 0$ så är

$$\operatorname{grad}(r_1(X) - r(X)) = \operatorname{grad} g(X)(q(X) - q_1(X)) \geq \text{grad } g(X)$$

(observera att här utnyttjar vi förutsättningen om högsta koefficienten av $g(X)$). Alltså är $q(X) - q_1(X) = 0$ dvs $q(X) = q_1(X)$ och likheten $(*)$ ger att $r_1(X) = r(X)$. □

Exempel. Låt $f(X) = 2X^3 + 3X^2 + X + 1$, $g(X) = X^2 + 2$ i $\mathbb{Z}_4[X]$. Vi har

$$\begin{array}{rrcl} & 2X + 3 & = & q(X) \\ \underline{X^2 + 2}| & 2X^3 + 3X^2 + X + 1 & & \\ & -2X^3 & & \\ \hline & 3X^2 + X + 1 & & \\ & -X^3 \quad -2 & & \\ \hline & X + 3 & = & r(X) \end{array}$$

(tänk på det att $2 \cdot 2 = 0$ i $\mathbb{Z}_4$). □

(9.3) Definition. Man säger att $g \in R[X]$ är en **delare** till $f \in R[X]$ om $f = gq$, där $q \in R[X]$. Man skriver då $g|f$. □

Från och med nu förutsätter vi att $R = K$ är en kropp.

(9.4) Definition. Om $f, g \in K[X]$ säger man att $d \in K[X]$ är en **största gemensamma delare** till f och g ($SGD(f, g)$) om

(a) $d|f$ och $d|g$,

(b) $d'|f$ och $d'|g$, där $d' \in K[X]$ implicerar att $d'|d$.

Om $f = g = 0$ definierar man $SGD(0, 0) = 0$. □

Genom att utnyttja divisionsalgoritmen kan man beräkna $SGD(f, g)$ för godtyckliga polynom $f, g \in K[X]$ med hjälp av Euklides algoritm (precis som för heltalen). Vidare kan man bevisa att precis som för heltalen gäller följande sats:

(9.5) Sats. *Om $d = SGD(f, g)$, där $f, g \in K[X]$ så existerar $s, t \in K[X]$ så att*

$$d = fs + gt$$

Man kan visa satsen på liknande sätt som motsvarande sats för heltalen.

(9.6) Anmärkning. $SDG(f, g)$ är inte entydig. Om $f \neq 0$ eller $g \neq 0$ och d_1, d_2 är två polynom som uppfyller villkoren i (9.4) så är $d_1|d_2$ och $d_2|d_1$. Alltså är $d_2 = d_1 q$, där q har grad 0 ty d_1 och d_2 har samma grad ($\operatorname{grad} d_1 \geq \operatorname{grad} d_2$ och $\operatorname{grad} d_2 \geq \operatorname{grad} d_1$). Detta betyder att d_1 och d_2 är lika så när som på en konstant. Genom ett lämpligt val av den konstanten kan vi välja en största gemensamma delare med högsta koefficienten 1. Man kallar en sådan **den största gemensamma delaren**. Två polynom vars största **gemensamma delare är 1 kallas relativt prima**. □

Med hjälp av (9.5) visar man som för heltalen följande egenskap:

(9.7) Sats. *Om $f|h, g|h$ och $SGD(f,g) = 1$, där $f, g, h \in K[X]$ så $fg|h$.*

Bevis. Låt $h = fq_f$, $h = gq_g$ och $1 = fs + gt$. Då är $h = hfs + hgt = fgq_gs + fgq_ft = fg(q_gs + q_ft)$ dvs $fg|h$. □

(9.8) Definition. Man säger att $a \in K$ är ett **nollställe** till $f \in K[X]$ om $f(a) = 0$. □

(9.9) Faktorsatsen. (a) *Resten vid division av $f \in K[X]$ med $X - a$, $a \in K$, är lika med $f(a)$;*

(b) *$a \in K$ är ett nollställe till $f \in K[X]$ då och endast då $X - a|f(X)$.*

Bevis. (a) Enligt divisionsalgoritmen är

$$f(X) = (X - a)q(X) + r,$$

där $\operatorname{grad} r < 1$ dvs r är en konstant. Alltså är $f(a) = r$.

(b) $f(a) = 0 \Leftrightarrow r = f(a) = 0$. □

(9.10) Definition. Man säger att $a \in K$ har multipliciteten m som ett nollställe till $f \in K[X]$ om $(X - a)^m|f(X)$ och $(x - a)^{m+1} \nmid f(X)$. □

(9.11) Sats. *Summan av multipliciteterna av alla nollställen till $f \in K[X]$ är högst lika med $\operatorname{grad} f$.*

Bevis. Låt $a_1, \ldots, a_r$ vara nollställen till f och låt $m_1, \ldots, m_r$ vara deras respektive multipliciteter. Detta betyder att

$$(X - a_1)^{m_1}|f(X), \ldots, (X - a_r)^{m_r}|f(X).$$

Men polynomen $(X - a_i)^{m_i}$ är parvis relativt prima så att

$$(X - a_1)^{m_1} \ldots (X - a_r)^{m_r}|f(X)$$

dvs $\operatorname{grad} f \geq m_1 + \ldots + m_r$. □

(9.12) Derivatan av ett polynom. Låt $f(X) = a_0 + a_1X + \ldots + a_nX^n \in K[X]$. Derivatan av $f(X)$ definieras helt formellt som

$$f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

De vanliga deriveringsreglerna

$$(f + g)' = f' + g',\ (fg)' = f'g + fg'$$

visas genom en direkt kontroll (se övning 9.7).

(9.13) Sats. *$a \in K$ är ett multipelt nollställe till $f \in K[X]$ (dvs a har multipliciteten > 1) då och endast då $f(a) = f'(a) = 0$.*

Bevis. "$\Rightarrow$" Låt $f(X) = (X-a)^2 q(X)$ (multipliciteten av a är minst 2). Då är $f'(X) = 2(X-a)q(X) + (X-a)^2 q'(X)$ så att $f(a) = f'(a) = 0$.

"$\Leftarrow$" Antag att $f(a) = f'(a) = 0$ och att multipliciteten av a är 1 dvs $f(X) = (X-a)q(X)$ och $q(a) \neq 0$. Då är $f'(X) = q(X) + (X-a)q'(X)$ så att $f'(a) = q(a) \neq 0$ – en motsägelse. □

Mot primtalen i $\mathbb{Z}$ svarar irreducibla polynom i $K[X]$.

(9.14) Definition. Man säger att ett polynom $f \in K[X]$ är **reducibelt** om $f = gh$, där $g, h \in K[X]$ och $\operatorname{grad} g < \operatorname{grad} f$ samt $\operatorname{grad} h < \operatorname{grad} f$. Ett icke-konstant polynom som inte är reducibelt kallas **irreducibelt**. □

(9.15) Exempel. (a) Varje polynom av grad 1 är irreduciblet.

(b) Ett polynom $f \in K[X]$ av grad 2 eller 3 är reduciblet i $K[X]$ då och endast då f har ett nollställe i K dvs det finns $x_0 \in K$ så att $f(x_0) = 0$. I själva verket, om $f(x_0) = 0$ så är $f(X) = (X - x_0)f_1(X)$ där $f_1(X) \in K[X]$ och $\operatorname{grad} f_1(X) \geq 1$ dvs $f(X)$ är reducibelt. Omvänt om $f(X) = g(X)h(X)$ är en faktoruppdelning av $f(X)$ i två icke-konstanta faktorer så måste någon av dessa ha grad 1. Låt $g(X) = b_0 + b_1 X \in K[X]$. Då är $x_0 = -b_0/b_1$ ett nollställe till $f(X)$. Till exempel är $f(X) = X^2 + 1 \in \mathbb{Q}[X]$ irreducibelt i $\mathbb{Q}[X]$ ty det saknar nollställen i $\mathbb{Q}[X]$ ($\pm i \notin \mathbb{Q}$). Det är irreducibelt även i $\mathbb{R}[X]$, men i $\mathbb{C}[X]$ är $X^2 + 1 = (X+i)(X-i)$ så att $X^2 + 1$ är reduciblet i den sista polynomringen.

(c) $f(X) = X^2 + X + 1$ är irreducibelt i $\mathbb{Z}_2[X]$ ty $f(0) = 0^2 + 0 + 1 + 1$ och $f(1) = 1^2 + 1 + 1 = 1$ så att polynomet saknar nollställen i $\mathbb{Z}_2$. Vi har $X^2 + 1 = (X+1)^2$ i $\mathbb{Z}_2[X]$ så att $X^2 + 1$ är reducibelt i $\mathbb{Z}_2[X]$.

(d) Polynomet $f(X) = X^4 + 4$ saknar rationella (även reella) nollställen. Men man får inte påstå att f är irreduciblet i $\mathbb{Q}[X]$. Detta är ett polynom av grad 4 så att (b) inte är användbar här! I själva verket har vi

$$X^4 + 4 = X^4 + 4X^2 + 4 - 4X^2 = (X^2+2)^2 - (2X)^2 = (X^2 + 2X + 2)(X^2 - 2X + 2)$$

så att $X^4 + 4$ är reducibelt i $\mathbb{Q}[X]$. □

(9.16) Sats. *Om $p \in K[X]$ är irreducibelt och $p | fg$, där $f, g \in K[X]$ så $p | f$ eller $p | g$.*

Bevis. Satsen visas på samma sätt som för heltal. □

(9.17) Sats. *Varje polynom av grad ≥ 1 i $K[X]$ är en produkt av irreducibla polynom. Om*

$$f = p_1 \dots p_k = p_1' \dots p_l',$$

där p_i och p_i' är irreducibla polynom så är $k = l$ och vid en lämplig numrering $p_i' = c_i p_i$, där $c_i \in K$.

Bevis. Satsen bevisas på exakt samma sätt som motsvarande sats om primfaktoruppdelning av heltalen. □

Vi avslutar med några fakta om irreducibla polynom i olika polynomringar:

(9.18) Exempel. (a) **Ringen $\mathbb{C}[X]$.** Irreducibla polynom är endast alla polynom av grad 1. Detta är innehållet i "(polynom)algebrans fundamentalsats". Om $f(X) \in \mathbb{C}[X]$ så är $f(X) = c(X - z_1) \dots (X - z_n)$ där n är polynomets grad och $z_i \in \mathbb{C}$. Satsen visas enklast med hjälp av analytiska funktioner. Den visades för första gången av C. F. Gauss 1799.

(b) **Ringen $\mathbb{R}[X]$.** Irreducibla är alla polynom av grad 1 och alla polynom $c(X^2+pX+q)$ med $\Delta = p^2 - 4q < 0$ och $c \neq 0$. Detta följer lätt ur (a) och visades i tidigare kurser (nyckeln till beviset är det faktum att om $f(X)$ har reella koefficienter och $f(z) = 0$ så är även $p(\bar{z}) = 0$, där $\bar{z}$ är det konjugerade talet till z.).

(c) Ringen $\mathbb{Q}[X]$. Här finns irreducibla polynom av godtyckliga grader. T.ex. är $X^n - 2$ irreduciblet för varje $n \geq 1$. (se övning 9.5).

(d) **Ringen $\mathbb{Z}_2[X]$.** Här finns det också irreducibla polynom av godtyckliga grader (vi bevisar inte detta påstående). Antalet polynom av en fixerad grad är ändligt (2^{n+1} polynom av grad n – räkna!). Man kan tabullera irreducibla polynom (det finns mycket omfattande tabeller med tanke på tillämpningarna). Här följer en kort lista över irreducibla polynom av grad ≤ 5.

grad1 $X, X + 1$

grad2 $X^2 + X + 1$

grad3 $X^3 + X + 1, X^3 + X^2 + 1$

grad4 $X^4 + X + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1$

grad5 $X^5 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^3 + X^2 + X + 1,$
$X^5 + X^4 + X^2 + X + 1, X^5 + X^4 + X^3 + X + 1, X^5 + X^4 + X^3 + X^2 + 1$

Som exempel visar vi att $p(X) = X^4 + X + 1$ är irreducibelt. $p(X)$ saknar förstagradsfaktorer ty $p(0) = 1$ och $p(1) = 1$ dvs $p(X)$ saknar nollställen i $\mathbb{Z}_2$. Antag i så fall att $p(X)$ har en faktoruppdelning $p(X) = p_1(X)p_2(X)$ i en produkt av två irreducibla andragradsfaktorer. Då är $p_1(X) = p_2(X) = X^2 + X + 1$ ty det finns enbart ett irreducibelt polynom av grad 2. Men $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X + 1$ så att $p(X)$ måste vara irreducibelt ($p(X)$ kunde ha varit en produkt av p_1 och p_2 med graderna 1, 3 eller 2, 2). □

ÖVNINGAR

9.1. Bestäm kvoten och resten vid division av $f(X)$ med $g(X)$:

(a) $f(X) = X^3 + X^2 + 1, g(X) = X^2 + X + 1$ i $\mathbb{Z}_2[X]$;

(b) $f(X) = 3X^4 + 2X^2 + 4, g(X) = 2X^2 + 4X$ i $\mathbb{Z}_5[X]$.

9.2. Bestäm $SGD(f(X), g(X))$ då

(a) $f(X) = X^4 + 1, g(X) = X^2 + 1$ i $\mathbb{Z}_2[X]$;

(b) $f(X) = X^9 + 1, g(X) = X^6 + 1$ i $\mathbb{Z}_2[X]$;

(c) $f(X) = X^4 + 2X^3 + X^2 + 4X + 2, g(X) = X^2 + 3X + 1$ i $\mathbb{Z}_5[X]$.

Bestäm s, t sådana att $SGD(f, g) = fs + gt$.

9.3. Faktorisera följande polynom i produkt av irreducibla:

(a) $X^4 + 4$ i $\mathbb{Q}[X]$,
(b) $X^4 + 1$ i $\mathbb{R}[X]$,
(c) $X^7 - 1$ i $\mathbb{Z}_2[X]$,
(d) $X^4 + 2$ i $\mathbb{Z}_5[X]$,
(e) $X^3 - 2$ i $\mathbb{Q}[X]$,
(f) $X^3 + X + 1$ i $\mathbb{R}[X]$,
(g) $X^2 + 1$ i $\mathbb{Z}_3[X]$,
(h) $X^4 + X + 2$ i $\mathbb{Z}_3[X]$.

9.4. Visa att om $p \in K[X]$ är irreducibelt och $p|fg$ så $p|f$ eller $p|g$.

Ledning: Bevis som för heltal.

9.5. Låt $f(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$ och låt p vara ett primtal sådant att $p|a_0, p|a_1, \ldots, p|a_{n-1}, p \nmid a_n$ och $p^2 \nmid a_0$. Visa att $f(X)$ är irreduciblet i $\mathbb{Z}[X]$.

Ledning: Påståendet kallas **Eisensteins kriterium**. Antag att $f(X) = g(X)h(X)$ i $\mathbb{Z}[X]$ där $\operatorname{grad} g(X) = k < n$ och $\operatorname{grad} h(X) = l < n, g(X), h(X) \in \mathbb{Z}[X]$ och se vad som händer med $f(X), g(X), h(X)$ vid homomorfismen $\theta : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$. I själva verket är $f(X)$ också irreducibelt i $\mathbb{Q}[X]$. Om ett polynom med heltaliga koefficienter inte kan faktoriseras i produkt av två polynom av lägre grader i $\mathbb{Z}[X]$ så kan det inte heller faktoriseras på detta sätt i $\mathbb{Q}[X]$. Detta påstående kallas Gauss lemma och dess bevis är inte svårt.

9.6. Definiera $-\infty + n = -\infty$ och $\max(-\infty, n) = n$. Visa att

$$\operatorname{grad}(f(X) + g(X)) = \max(\operatorname{grad} f(X), \operatorname{grad}\ g(X))$$

och

$$\operatorname{grad}(f(X)g(X)) \leq \operatorname{grad}\ f(X) + \operatorname{grad}\ g(X)$$

varvid likheten gäller om $a_nb_m \neq 0$ där $f(X) = a_0 + \ldots + a_nX^n$ och $g(X) = b_0 + \ldots + b_mX^m$ är polynom ur $R[X]$.

9.7. Visa att $(fg)' = f'g + fg'$ då $f, g \in K[X]$.

Ledning: Utnyttja den självklara formeln för $(f + g)'$ och börja beviset med $f = aX^m, g = bX^n$.

Kapitel 10

NORMALA DELGRUPPER OCH KVOTGRUPPER

Vi vet redan att sidoklasserna till $< 5 >$ i $\mathbb{Z}$ svarar mot olika rester vid division med 5. Dessa rester bildar en grupp med avseende på addition modulo 5. Sidoklasserna till de reella positiva talen i gruppen $\mathbb{R}^*$ (alla reella tal $\neq 0$) svarar mot $+1$ och -1 (se exempel (7.5) (b)). Dessa två tal bildar en grupp med avseende på multiplikation. Är det en tillfällighet eller är det så att sidoklasserna till en delgrupp av en grupp också bildar en grup? För att kunna definiera en grupp måste man kunna utföra en operation på sidoklasserna. Det finns en naturlig operation för delmängder till G:

$$AB = \{ab : a \in A \quad \text{och} \quad b \in B\} \tag{10.1}$$

där $A, B \subseteq G$. Delmängder av den typen är t ex sidoklasser: $A = H$ och $B = \{g\}$ ger $AB = Hg$. Det är klart att

$$(AB)C = A(BC)$$

då $A, B, C \subseteq G$ därför att operationen i gruppen är associativ. Det är ganska klart att

$$HH = H$$

om H är en delgrupp till G. Inklusionen $HH \subseteq H$ är självklar ty H är en delgrup. $H \subseteq HH$ gäller ty $h = he \in HH$ då $h \in H$. Bägge inklusionerna $HH \subseteq H$ och $H \subseteq HH$ ger likheten $HH = H$.

Nu kan vi försöka multiplicera två sidoklasser $A = Hg_1$ och $B = Hg_2$ dvs bilda produkten $AB = Hg_1Hg_2$. Frågan är om vi får en högersidoklass. Det är klart att om $g_1H = Hg_1$ så är $Hg_1Hg_2 = HHg_1g_2 = Hg_1g_2$ ty $HH = H$. För detta krävs dock att höger- och vänstersidoklassen av g_1 sammanfaller.

(10.2) Definition. Man säger att H är en **normal delgrupp** till G om $gH = Hg$ för varje $g \in G$. Man skriver då $H \lhd G$. □

(10.3) Exempel. (a) Varje delgrupp till en abelsk grupp är normal.

(b) Låt G vara kvadratgruppen (se exempel (6.7) (b)) och låt H bestå av alla vridningar. Här är $o(G) = 8$ och $o(H) = 4$ så att antalet sidoklasser är $o(G) : o(H) = 2$. Den ena sidoklassen är H, den andra måste vara $G \setminus H = \{s_1, s_2, s_3, s_4\}$. Detta betyder att höger- och vänstersidoklasserna är lika dvs H 'r en normal delgrupp till G:

(c) Låt G vara symmetrigruppen av en liksidig triangel och låt $H = \{(1), (2, 3)\}$ (se exempel (7.7)). Då är H inte en normal delgrupp ty $s_2H \neq Hs_2$, där $s_2 = (1, 3)$. □

Vi noterar en enkel och viktig situation då man får en normal delgrupp:

(10.4) Proposition. *Låt G vara en grupp och H en delgrupp till G sådan att $[G : H] = 2$ dvs det finns exakt två sidoklasser till H i G. Då är H en normaldelgrupp till G.*

Bevis. Man argumenterar på precis samma sätt som i exempel (10.3) (b) ovan. □

Nu kan vi besvara frågan om gruppstrukturen på mängden av alla sidoklasser (se också övning 10.10).

(10.5) Sats. *Låt H vara en normal delgrupp till G. Då bildar alla sidoklasser till H i G en grupp med avseende på multiplikation av delmängder till G. Det neutrala elementet är H och inversen till Hg är Hg^{-1}.*

Bevis. Vi har

$$Hg_1Hg_2 = HHg_1g_2 = Hg_1g_2$$

tack vare (8.2) och (8.3) dvs produkten av två sidoklasser är en sidoklass (slutenheten). Associativiteten gäller för multiplikation av godtyckliga delmängder till G. Det är klart att $HgH = HHg = Hg$ sluteligen är $HgHg^{-1} = HHgg^{-1} = H = Hg^{-1}Hg$ dvs Hg^{-1} är inversen till Hg. □

(10.6) Definition. Om H är en normal delgrupp till G så kallar man gruppen av alla sidoklasser till H i G för **kvotgruppen** av G modulo H. Den betecknas med G/H.

□

(10.7) Exempel. (a) Låt $G = \mathbb{Z}$ med addition och låt $H =< 5 >$. Då har vi 5 sidoklasser $< 5 > +r$, där $r = 0, 1, 2, 3, 4$. Vi skall skriva $< 5 > +r = \bar{r}$. Grupptabellen för gruppen $\mathbb{Z}/ < 5 >$ är alltså

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

(b) Låt $G = \mathbb{R}^*$ och $H = \mathbb{R}^*_{>0}$ som i exempel (**??**) (b). Sidoklasserna är $\overline{1} = \mathbb{R}^* \cdot 1 = \mathbb{R}^*_{>0}$ och $\overline{-1} = \mathbb{R}^*(-1) = -\mathbb{R}^*_{>0}$ är alltså följande:

	$\overline{1}$	$\overline{-1}$
$\overline{1}$	$\overline{1}$	$\overline{-1}$
$\overline{-1}$	$\overline{-1}$	$\overline{1}$

(c) Låt $G = \mathbb{Z}_{12}$ med addition $\oplus$ modulo 12 och $H =< 3 >= \{0, 3, 6, 9\}$. Vi har 3 sidoklasser ty $o(G) : o(H) = 3$. Den ena är som vanligt H. Den andra är $H + 1 = \{1, 4, 7, 10\}$, och den tredje $H + 2 = \{2, 5, 8, 11\}$ vi skall beteckna dessa sidoklasser med $\bar{0}, \bar{1}, \bar{2}$. Då får vi grupptabellen för $\mathbb{Z}_{12}/ < 3 >$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

□

Om man utelämnar strecket i tabellerna ur exemplet (10.7) får man grupptabellerna för grupper som vi redan känner mycket väl: $\mathbb{Z}_5$ i (a), gruppen $\{1, -1\}$ med multiplikation i (b), och $\mathbb{Z}_3$ i (c). Detta är ingen tillfällighet. Vi skall förklara det närmare i nästa avsnitt. Detta avsnitt avslutar vi med en mera användbar karakterisering av normala delgrupper än den som ges i definitionen (10.2):

(10.8) Proposition. *H är en normal delgrupp till G då och endast då $gHg^{-1} \subseteq H$ för varje $g \in G$ dvs $ghg^{-1} \in H$ då $g \in G$ och $h \in H$.*

Bevis. "⇒" Om $gH = Hg$ för varje $g \in G$ så är $gHg^{-1} = H$ (multiplicera med g^{-1} från höger).

"⇐" $gHg^{-1} \subseteq H$ implicerar $gH \subseteq Hg$ (multiplicera med g från höger – se övning 10.14). Inklusionen gäller för varje $g \in G$. Alltså gäller den då man ersätter g med g^{-1} dvs $g^{-1}H \subseteq Hg^{-1}$. Multiplicera den inklusionen med g både från vänster och höger. Då är $Hg \subseteq gH$ som tillsammans med $gH \subseteq Hg$ ger $gH = Hg$. □

(10.9) Exempel. Låt $G = GL_n(\mathbb{R})$ (alla $n \times n$-matriser med reella element och determinant $\neq 0$ under matrismultiplikation). Låt H bestå av alla $A \in G$ med $\det A = 1$. Först konstaterar

vi att H är en delgrupp till G ty $A, B \in H$ ger $\det(AB) = \det A \det B = 1$ så att $AB \in H$ (H är sluten m.a.p. operationen). Vidare gäller $E \in H$ (E identitetsmatrisen) och $A^{-1} \in H$ då $A \in H$ ty $\det A^{-1} = 1/\det A = 1$. H är en normal delgrupp till G. För att visa det utnyttjar vi (10.8). Låt $A \in H$ och $B \in G$. Då är $\det(BAB^{-1}) = \det B \det A (\det B)^{-1} = \det A = 1$ så att $BAB^{-1} \in H$. □

ÖVNINGAR

10.1. Vilka av följande delgrupper H till $G = GL_2(\mathbb{R})$ (2×2 reella matriser med $\det \neq 0$) är normala?

(a) $H = \{A \in G : \det A = 1\}$,

(b) $H =$ alla diagonala matriser $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $ab \neq 0$,

(c) $H =$ alla triangulära matriser $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $ac \neq 0$.

10.2. Är H normal i G om:

(a) $G = S_n$, $H = A_n$ (jämna permutationer av talen $1, 2, \ldots, n$)?

(b) $G = S_n$, $H = \{f \in S_n : f(1) = 1\}$?

10.3. (a) Låt G vara symmetrigruppen av en kvadrat. Ge exempel på en normal delgrupp till G som är $\neq < e >, G$ och på en icke-normal delgrupp till G.

10.4. Med centrum $C(G)$ av en grupp G menar man:

$$C(G) = \{g \in G : gx = xg \quad \forall_{x \in G}\}$$

Visa att $C(G)$ är en normal delgrupp till G.

10.5. Låt H vara en normal delgrupp till G och $o(H) = 2$. Visa att $H \subseteq C(G)$ (se 10.4).

10.6. Bestäm alla normala delgrupper till

(a) symmetrigruppen av en liksidig triangel,

(a) symmetrigruppen av en kvadrat.

10.7. Låt $H_1 \subset H_2 \subset G$ där H_1 är normal i H_2 och H_2 är normal i G. Är det sant att H_1 är normal i G?

10.8. Visa att om N_1, N_2 är normala delgrupper till G så är även N_1N_2 och $N_1 \cap N_2$ normala i G.

10.9. Låt H vara en delgrupp till G. och N en normal delgrupp till G. Visa att:

(a) HN är en delgrupp till G,

(b) $H \cap N$ är en normal delgrupp till H.

10.10. (a) Ge exempel på en gruppp G och en delgrupp $H \subseteq G$ och två sidoklasser Hg_1 och Hg_2 sådana att Hg_1Hg_2 inte är en högersidoklass.

(b) Visa att om H inte är normal i G så kan man alltid hitta två högersidoklasser till H i G vars produkt inte är en högersidoklass.

10.11. Skriv upp grupptabeller för följande kvotgrupper G/H:

(a) $G = \mathbb{Z}_6$, $H =< 2 >$,

(b) $G = \mathbb{Z}_{18}$, $H =< 6 >$,

(c) $G = \mathbb{Z} \times \mathbb{Z}$, $H = \{a, b) : 2|a \quad \text{och} \quad 2|b\}$,

(d) $G = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H =< (1, 2) >$.

10.12. Välj en representant för varje sidoklass ur G/H då

(a) $G = \mathbb{R}^*$, $H = \mathbb{R}^*_+$,

(b) $G = \mathbb{C}^*$, $H = \{z \in \mathbb{C}^* : |z| = 1\}$,

(c) $G = \mathbb{R}$, $H = \mathbb{Z}$.

Försök välja representaterna så att de bildar en delgrupp till G (om det går). Om ett sådant val inte är möjligt försök beskriva gruppoperationen i G/H med hjälp av representanterna.

10.13. (a) Visa att varje element i gruppen $\mathbb{Q}/\mathbb{Z}$ har ändlig ordning.

(b) Visa att varje element av ändlig ordning i $\mathbb{R}/\mathbb{Z}$ tillhör $\mathbb{Q}/\mathbb{Z}$.

10.14. Låt A, B, C vara delmängder till en grupp G och $g \in G$. Visa att:

(a) $A \subseteq B \Rightarrow AC \subseteq BC$,

(b) $Ag \subseteq Bg \Leftrightarrow A \subseteq B$.

Kapitel 11

HOMOMORFISMER OCH ISOMORFISMER AV GRUPPER

Vi har redan märkt att två gruper som definieras på olika sätt kan ha grupptabeller som skiljer sig enbart oväsentligt. T ex har $\mathbb{Z}_4 =< 1 >= \{0, 1, 2, 3\}$ och $U_4 =< i >= \{1, i, -1, -i\}$ liknande grupptabeller:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	i^0	i^1	i^2	i^3
$1 = i^0$	i^0	i^1	i^2	i^3
$i = i^1$	i^1	i^2	i^3	i^0
$-1 = i^i$	i^2	i^3	i^0	i^1
$-i = i^3$	i^3	i^0	i^1	i^2

(stryk i överallt i den andra!). Nu kan vi förklara sambandet närmare.

(11.1) Definition. Låt G, G' vara grupper. En funktion $\theta : G \to G'$ kallas **homomorfism** om

$$\theta(ab) = \theta(a)\theta(b)$$

för godtyckliga $a, b \in G$. En bijektiv homomorfism kallas **isomorfism**. En isomorfism θ kallas **automorfism** då $G' = G$. □

(11.2) Anmärkning. Observera att produkten ab är i gruppen G, medan $\theta(a)\theta(b)$ i gruppen G'. □

(11.3) Exempel. (a) Låt $G = \mathbb{Z}$ med addition och $G' = \mathbb{Z}_n$ med addition modulo n. Funktionen $\theta : \mathbb{Z} \to \mathbb{Z}_n$ sådan att $\theta(a) = [a]_n$ är en homomorfism ty

$$\theta(a + b) = [a + b]_n = [a]_n \oplus [b]_n = \theta(a) \oplus \theta(b)$$

(se (5.2)).

(b) Låt $G = \mathbb{R}$ med addition och låt $G' = \mathbb{R}^*_{>0}$ vara gruppen av de positiva reella talen med multiplikation. Funktionen $\theta : \mathbb{R} \to \mathbb{R}^*_{>0}$ där $\theta(r) = e^r$ är en homomorfism ty

$$\theta(r_1 + r_2) = e^{r_1+r_2} = e^{r_1}e^{r_2} = \theta(r_1)\theta(r_2)$$

som bekant är θ en bijektion så att θ är en isomorfism. Inversen till θ är funktionen $\theta^{-1} : \mathbb{R}^*_{>0} \to \mathbb{R}$ där $\theta^{-1}(y) = \ln y$. θ^{-1} är också en homomorfism ty

$$\theta^{-1}(y_2y_2) = \ln y_1y_2 = \ln y_1 + \ln y_2 = \theta^{-1}(y_1) + \theta^{-1}(y_2).$$

□

Här följer några enkla egenskaper hos homomorfismer:

(11.4) Proposition. *Låt $\theta : G \to G'$ vara en grupphomomorfism: Då är*

(a) $\theta(e) = e'$ *(e, e' de neutrala elementen i G respektive G').*

(b) $\theta(a^{-1}) = \theta(a)^{-1}$.

Bevis. (a) $\theta(e) = \theta(ee) = \theta(e)\theta(e)$. Alltså är $\theta(e) = e'$.

(b) Vi har $e' = \theta(e) = \theta(aa^{-1}) = \theta(a)\theta(a^{-1})$. Alltså är $\theta(a^{-1}) = \theta(a)^{-1}$. □

(11.5) Sats. (a) *Om $\theta : G \to G'$ och $\theta' : G' \to G$ är homomorfismer (isomorfismer) så är även $\theta' \circ \theta : G \to G'$ en homomorfism (isomorfism).*

(b) *Om $\theta : G \to G'$ är en isomorfism så är även $\theta^{-1} : G' \to G$ en isomorfism.*

Bevis. (a) $(\theta' \circ \theta)(ab) = \theta'(\theta(ab)) = \theta'(\theta(a)\theta(b)) = \theta'(\theta(a))\theta'(\theta(b)) = (\theta' \circ \theta)(a)(\theta' \circ \theta)(b)$.

(b) Låt $a' = \theta(a)$ och $b' = \theta(b)$. Då är $a'b' = \theta(a)\theta(b) = \theta(ab)$. Alltså är $\theta^{-1}(a'b') = ab = \theta^{-1}(a')\theta^{-1}(b')$ så att θ^{-1} är en homomorfism. Men θ^{-1} är bijektiv (se (6.2)) så att det är en isomorfism. □

(11.6) Anmärkning. Den sista satsen säger att om det finns en isomorfism från G till G' så finns det också en isomorfim från G' till G. Därför säger man att G och G' är **isomorfa grupper** om det finns en isomorfism från den ena till den andra. Man skriver då $G \cong G'$ (eller $G' \cong G$). Om två isomorfa grupper säger man att de tillhör samma **isomorfiklass** av grupper. □

Alla cykliska grupper av samma ordning tillhör samma isomorfiklass:

(11.7) Sats. (a) *Om G är cyklisk och $o(G) = n$ så är $G \cong \mathbb{Z}_n$*

(b) *Om G är cyklisk och $o(G) = \infty$ så är $G \cong \mathbb{Z}$.*

Bevis. (a) Vi vet att $G =< g >= \{e, g, \ldots, g^{n-1}\}$ och $g^n = e$ (se (4.8)). Observera först att om N är ett heltal och $N = ng + r$ så är $g^N = g^r$ ty $g^n = e$. Definiera

$$\theta : \mathbb{Z}_n \to G$$

så att $\theta(r) = g^r$.

Då är θ en bijektion och

$$\theta(r_1 \oplus r_2) = g^{r_1 \oplus r_2} = g^{[r_1+r_2]_n} = g^{r_1+r_2} = g^{r_1}g^{r_2} = \theta(r_1)\theta(r_2)$$

så att θ är en isomorfism.

(b) Här vet vi att $G =< g >= \{\ldots g^{-2}, g^{-1}, g^0 = e, g, g^2, \ldots\}$ och alla potenser g^m är olika (se (4.12) (b)). Definiera $\theta(m) = g^m$. Då gäller

$$\theta(m_1 + m_2) = g^{m_1+m_2} = g^{m_1}g^{m_2} = \theta(m_1)\theta(m_2)$$

så att θ är en isomorfism. □

Exempel. Gruppen $U_4 =< i >= \{1, i, i^2, i^3\}$ är cyklisk och $\theta : \mathbb{Z}_4 \to U_4$ där $\theta(r) = i^r$ är en isomorfism. Det är vår förklaring av likheten mellan grupptabellerna i början av detta avsnitt. □

(11.8) Exempel. Låt $\theta : G \to G'$ vara en isomorfism mellan ändliga grupper. Om $G] = \{g_1, g_2, \ldots, g_n\}$ så är $G' = \{\theta(g_1), \theta(g_2), \ldots, \theta(g_n)\}$. Grupptabellerna för G och G' är identiska så när som på beteckningarna:

	g_1	g_2	$\ldots$	g_j	$\ldots$	g_n
g_1						
g_2						
$\vdots$				$\vdots$		
g_i			$\ldots$	g_ig_j		
$\vdots$						
g_n						

	$\theta(g_1)$	$\theta(g_2)$	$\ldots$	$\theta(g_j)$	$\ldots$	$\theta(g_n)$
$\theta(g_1)$						
$\theta(g_2)$						
$\vdots$				$\vdots$		
$\theta(g_i)$			$\ldots$	$\theta(g_ig_j)$		
$\vdots$						
$\theta(g_n)$						

Mot g_ig_j som står i i:te raden och j:te kolonnen i grupptabellen för G svarar $\theta(g_i)\theta(g_j) = \theta(g_ig_j)$ i i:te raden och j:te kolonnen i grupptabellen för G'. Som exempel jämför grupptabellerna för $\mathbb{Z}_4$ och U_4 i början av detta avsnitt! Två isomorfa grupper har alltså väsentligen identiska grupptabeller. Från algebraisk synpunkt är de helt identiska trots att i praktiska sammanhang kan de beskrivas på olika sätt. □

Låt oss betrakta några ytterligare exempel.

(11.9) Exempel. (a) Vi vet att varje grupp av ordningen 1 eller p där p är ett primtal är cyklisk (se övning 7.10). Alltså finns det enbart en isomorfiklass av grupper för dessa ordningar (t ex $1, 2, 3, 5, 7, \ldots$)

(b) Låt G vara en grupp av ordningen 4. Här har vi två fall. Om $g \in G$ så är $o(g) = 1, 2$ eller 4 (enligt Lagranges sats (7.9)). Om det finns $g \in G$ sådant att $o(g) = 4$ så är $G = \{e, g, g^2, g^3\}$ och $g^4 = e$. Grupptabellen är

	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$g^4 = e$

G är isomorf med $\mathbb{Z}_4$. Antag att det inte finns något g med $o(g) = 4$. Då är $o(g) = 2$ för varje $g \neq e$. Låt g och h vara två olika element av ordningen 2. Då är $gh \neq e, g, h$ (ty $gh = e \Rightarrow h = g^{-1} = g$, $gh = g \Rightarrow h = e$, $gh = h \Rightarrow g = e$). Alltså är $G = \{e, g, h, gh\}$. Vad kan man säga om hg? Det är klart att $hg \neq e, g, h$ (på samma sätt som ovan). Alltså är $hg = gh$. Vi får följande grupptabell:

	e	g	h	gh
e	e	g	h	gh
g	g	e	gh	h
h	h	gh	e	g
gh	gh	h	g	e

$g^2 = h^2 = e$
$gh = hg$

En grupp med en sådan tabell är t.ex. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{00, 01, 10, 11\}$. Om vi tar $g = 01$ och $h = 10$ så får vi just den tabelen (med additiv notation). Gruppen $\mathbb{Z}_4$ med den första tabellen och gruppen $\mathbb{Z}_2 \times \mathbb{Z}_2$ med den andra är inte isomorfa. Vi utnyttjar här en ganska självklar sanning att en cyklisk och en icke-cyklisk grupp inte är isomorfa. Detta kräver dock ett (okomplicerat) bevis (se övning 11.9).

(c) Även för grupper av ordningen 6 finns det två typer av grupptabeller (dvs två isomorfismklasser). Den ena representeras av den cykliska gruppen $\mathbb{Z}_6$, den andra av gruppen S_3 av alla permutationer av talen 1, 2, 3 (se (6.7) (a)). Dessa två grupper är inte isomorfa ty $\mathbb{Z}_6$ är abelsk och S_3 är inte abelsk (se vidare övning 11.9). □

(11.10) Anmärkning. Antalet icke-isomorfa grupper av en fix ordning n varierar mycket kraftigt med n. Och det finns inte någon chans att kunna beskriva den funktionen mera exakt. Här följer en kort tabell med antalet icke-isomorfa grupper av ordningarna 1 – 18

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5

□

Det är dock möjligt att säga lite mera i vissa specialfall. T.ex. vet vi redan att för varje primtal p finns det bara en isomorfiklass av gruper – varje grupp av primtalsordning är cyklisk (se övning 7.10) så att den är isomorf med $\mathbb{Z}_p$. Situationen är också klar för ändliga abelska grupper. Här gäller följande sats vars bevis måste vi tyvärr utelämna:

(11.11) Huvudsatsen om ändliga abelska grupper. *Om G är en ändlig abelsk grupp så är*

$$G \cong G_1 \times \ldots \times G_k$$

där G_i är cykliska grupper vaars ordningar är primtalspotenser. Om även

$$G = G_1' \times \ldots \times G_l'$$

där G_i' är cykliska grupper vars ordningar är primtalspotenser så är $k = l$ och $G_i' \cong G_i$ för $i = 1, \ldots, k$ vid en lämplig numrering av grupperna G_i'.

Exempel. Det finns 3 icke-isomorfa abelska grupper av ordningen 8:

$$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4 \quad \text{och} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

därför att 8 kan representeras som produkt av primtalspotenser på 3 olika sätt. Dessutom finns det två icke-abelska icke-isomorfa grupper av den ordningen – kvadratgruppen (se (**??**) (b)) och kvaterniongruppen (se övning 11.8). □

När det gäller icke-abelska ändliga gruper är situationen mycket mera invecklad. Byggstenarna är s.k. enkla grupper.

(11.12) Definition. Man säger att G är en **enkel grupp** om G saknar normala delgrupper $\neq < e >, G$. □

Exempel. En abelsk grupp $\neq < e >$ är enkel då och endast då den har primtalsordning (se övning 7.7). Det är inte så lätt att ge exempel på icke-abelska enkla grupper. Den minsta är gruppen A_5 av alla jämna permutationer av talen 1,2,3,4,5. Den består av 60 element. Alla grupper $A_n, n \geq 5$, av jämna permutationer av talen $1, 2, \ldots, n$ är enkla. □

Det finns ett antal liknande oändliga serier av enkla grupper. Alla dessa serier var kända sedan en ganska lång tid tillbaka. Men man visste om existensen av s.k. **sporadiska enkla gruper** som låg vid sidan av alla serier. Problemet att hitta alla enkla grupper sysselsatte många framstående matematiker under många decenier. Klassifikationsproblemet av enkla grupper löstes slutligen år 1981 som resultat av en gemensam ansträngning av många matematiker från flera olika länder. Lösningen av problemet betraktas allmänt som en av de största vetenskapliga bedrifterna. Den sista sporadiska gruppen upptäcktes just 1981 av en tysk matematiker R.

Griess som publicerade sitt arbete "The friendly gigant" i 1982. Gruppen kallas ": **Fischer-Griess monstergruppen** och betecknas (F_1). Den 25:e gruppen är "baby monster" med beteckningen F_2 – se tabellen:

Sporadiska enkla grupper

Grupp	**Antalet element**
M_{11}	$2^r \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	$2^7 \cdot 3^3 \cdot 5 \cdot 7$
J_3	$2^7 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19$
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
MC	$2^7 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
Sz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
C_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
C_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
F_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
F_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
F_{24}	$2^{21} c\dot{1}3^{16} \cdot 5^2 \cdot 6^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19 \cdot 31\dot{3}7 \cdot 67$
O	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
R	$2^{14} \cdot 3^3 \cdot 5^6 \cdot 7 \cdot 13 \cdot 29$
F_5	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
F_3	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
F_2	$2^{14} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17\dot{1}9 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

ÖVNINGAR

11.1. Vilka av följande par av grupper är isomorfa:

(a) $\mathbb{Z}_6$ och S_3,

(b) $\mathbb{Z}_4$ och $\mathbb{Z}_2 \times \mathbb{Z}_2$,

(c) $(\mathbb{Q}, +)$ och $(\mathbb{Q}^*, \cdot)$,

(d) $(\mathbb{Q}, +)$ och $(\mathbb{R}, +)$,

(e) $(\mathbb{Z}, +)$ och $(\mathbb{Q}, +)$.

11.2. Vilka av följande funktioner $f : G \to G'$ är homomorfismer, vilka är isomorfismer?

(a) $G = (\mathbb{R}, +), G' = (\mathbb{R}^*, \cdot), f(x) = 2^x$,

(b) $G = G' = (\mathbb{Z}, +), f(x) = x + 1$,

(c) $G = \mathbb{C}^*, G' = \mathbb{R}^*, f(z) = |z|$,

(d) $G = \mathbb{R}^*, G' = U_2 = (\{1, -1\}, \cdot)$, $f(r) = \operatorname{sgn}(r)$,

(e) $G = \mathbb{Z}, G'$ godtycklig, $f(n) = g^n$, $g \in G'$ ett fixt element,

(f) $G = GL_n(\mathbb{R}), G' = \mathbb{R}^*, f(A) = \det A$.

11.3. Låt N vara en normaldelgrupp till G. Visa att $\theta : G \to G/N$ där $\theta(g) = Ng$ är en surjektiv grupphomomorfism.

11.4. Låt $\theta : G \to G'$ vara en grupphomomorfism. Låt H vara en delgrupp till G och H' en delgrupp till G'. Visa att

(a) $\theta(H)$ är en delgrupp till G'.

(b) $\theta^{-1}(H') = \{g \in G : \theta(g) \in H'\}$ är en delgrupp till G.

(c) Om H' är en normal delgrupp till G' så är $\theta^{-1}(H')$ en normal delgrupp till G.

(d) Om H är en normal delgrupp till G så behöver $\theta(H)$ inte vara normal i G' men den är normal om θ är surjektiv.

11.5. Visa att $\theta : G \to G$ där $\theta(g) = g^{-1}$ är en automorfism då och endast då G är abelsk.

11.6. Låt $\theta : G \to G'$ vara en grupphomomorfism. Visa att

$$o(\theta(g)) | o(g).$$

Om θ är en isomorfism är $o(\theta(g)) = o(g)$.

11.7. (a) Visa att $\mathbb{Z}$ har exakt två automorfismer.

(b) Visa att $\theta : \mathbb{Z}_n \to \mathbb{Z}_n$ är en automorfism då och endast då $\theta(r) = kr$ där $SGD(k, n) = 1$.

11.8. Visa att följande 8 matriser bildar en grupp:

$$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \pm \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}, \quad \pm \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \quad i^2 = -1.$$

Denna grupp kallas **kvaterniongruppen**. Visa att den inte är isomorf med kvadratgruppen.

Ledning. Beteckna matriserna ovan med respektive $1, A, B, C$ ("+" framför). Visa att $A^2 = B^2 = C^2 = -1$, $AB = -BA$, $AC = -CA$, $BC = -CB$. Jämför ordningarna av elementen i kvaterniongruppen och i kvadratgruppen.

11.9. (a) Visa att en cyklisk grupp inte är isomorf med en icke-cyklisk.

(b) Visa att en abelsk grupp inte är isomorf med en icke-abelsk.

Kapitel 12

HUVUDSATSEN OM GRUPPHOMOMORFISMER

I detta avsnitt kommer vi att förklara samband mellan grupphomomorfismer och kvotgruper. Det blir bland annat klart varför kvotgrupen $\mathbb{Z}/ < 5 >$ och restgruppen $\mathbb{Z}_5$ är isomorfa.

(12.1) Definition. Låt $\theta : G \to G'$ vara en grupphomomorfism. Med **kärnan** till θ menar man

$$\text{Ker}\theta = \{g \in G : \theta(g) = e'\}$$

□

Exempel. (a) Låt $\theta : \mathbb{Z} \to \mathbb{Z}_2$ där $\theta(a) = [a]_2$. Då är $\text{Ker}\theta = \{a \in \mathbb{Z} : \theta(a) = [a]_2 = 0\} =< 2 >$.

(b) Låt $\theta : GL_n(\mathbb{R}) \to \mathbb{R}^*$ där $\theta(A) = \det A$ ($GL_n(\mathbb{R})$ betecknar alla $n \times n$-matriser A med $\det A \neq 0$). Vi har

$$\theta(AB) = \det AB = \det A \cdot \det B = \theta(A)\theta(B)$$

så att θ är en homomorfism.

$$\text{Ker}\theta = \{A \in GL_n(\mathbb{R}) : \theta(A) = \det A = 1\}$$

dvs kärnan består av alla matriser A med $\det A = 1$.

(c) Låt $\theta : \mathbb{R} \to \mathbb{R}^*$ där $\theta(r) = e^r$ (se exempel (11.3) (b)). Nu är

$$\text{Ker}\,\theta = \{r \in \mathbb{R} : \theta(r) = e^r = 1\} =< 0 > .$$

□

(12.2) Sats. *Låt $\theta : G \to G'$ vara en grupphomomorfism. Då är*

(a) *$\mathrm{Ker}\,\theta$ en normal delgrupp till G.*

(b) *$\theta(G)$ en delgrupp till G'.*

Bevis. (a) Först visar vi att $\mathrm{Ker}\,\theta$ är en delgrupp till G. Om $a, b \in \mathrm{Ker}\,\theta$ dvs $\theta(a) = \theta(b) = e'$ så är $\theta(ab) = \theta(a)\theta(b) = e'$ dvs $ab \in \mathrm{Ker}\,\theta$ (slutenhet). $e \in \mathrm{Ker}\,\theta$ ty $\theta(e) = e'$ enligt (11.4) (a). Om $a \in \mathrm{Ker}\,\theta$ dvs $\theta(a) = e'$ så är $\theta(a^{-1}) = \theta(a)^{-1} = e'$ dvs $a^{-1} \in \mathrm{Ker}\,\theta$. För att visa att $\mathrm{Ker}\,\theta$ är normal utnyttjar vi proposition (10.8). Låt $a \in \mathrm{Ker}\,\theta$ och $b \in G$. Då är $\theta(bab^{-1}) = \theta(b)\theta(a)\theta(b)^{-1} = \theta(b)\theta(b)^{-1} = e'$ ty $\theta(a) = e'$. Alltså $bab^{-1} \in \mathrm{Ker}\,\theta$.

(b) se övning 11.4. □

Det visar sig att normala delgrupper är exakt kärnor till homomorfismer:

(12.3) Sats. *Låt N vara en normal delgrupp till G. Då är funktionen $\eta : G \to G/N$ där $\eta(a) = Na$ en surjektiv homomorfism och $\mathrm{Ker}\,\eta = N$.*

Bevis. Vi har

$$\eta(ab) = Nab = NaNb = \eta(a)\eta(b)$$

så att η är en homomorfism. η är en surjektion ty sidoklassen Na (a godtyckligt) är bilden av a. Slutligen är $\mathrm{Ker}\,\eta = \{a \in G : \eta(a) = Na = N\} = N$ ty $Na = N$ då endast då $a \in N$ (se (7.3) (c). □

Nu kan vi förklara sambandet mellan kvotgrupper och homomorfsimer.

(12.4) Huvudsatsen om grupphomomorfismer. *Låt $\theta : G \to G'$ vara en grupphomomorfism och $N = \mathrm{Ker}\,\theta$. Då är*

$$G/N \cong \theta(G)$$

och en isomorfism $\bar{\theta}$ får man då $\bar{\theta}(Na) = \theta(a)$.

Bevis. Vi har

$$b \in Na \Leftrightarrow ba^{-1} \in N \Leftrightarrow \theta(ba^{-1}) = e' \Leftrightarrow \theta(b) = \theta(a)$$

Alltså består sidoklassen Na av alla element $b \in G$ som har samma bild som a vid homomorfismen θ. Låt oss definiera funktionen $\bar{\theta} : G/N \to G'$ så att bilden av en sidoklass är lika med bilden av ett godtyckligt element tillhörande den (alla element i sidoklassen har ju samma bild) dvs $\bar{\theta}(Na) = \theta(a)$. Då

$$\bar{\theta}(NaNb) = \bar{\theta}(Nab) = \theta(ab) = \theta(a)\theta(b) = \bar{\theta}(Na)\bar{\theta}(Nb)$$

Alltså är $\bar{\theta}$ en homomorfism. $\bar{\theta}$ är injektiv ty för två olika sidoklasser Na och Nb är bilderna $\theta(a)$ och $\theta(b)$ också olika. Slutligen är $\bar{\theta}$ en surjektion på bilden $\theta(G)$ ty varje element $\theta(a) \in \theta(G)$ är bilden av sidoklassen Na. Alltså är $\bar{\theta}$ en bijektiv (dvs injektiv och surjektiv) homomorfism. □

(12.5) Exempel. (a) Låt $\theta : \mathbb{Z} \to \mathbb{Z}_5$ där $\theta(a) = [a]_5$ (se (11.3) (a)). Då är $\operatorname{Ker}\theta = \{a \in \mathbb{Z} : \theta(a) = [a]_t = 0\} =< 5 >$ och $\theta(\mathbb{Z}) = \mathbb{Z}_5$. Enligt (12.4)

$$\bar{\theta} : \mathbb{Z}/ < 5 > \cong \mathbb{Z}_5,$$

där $\bar{\theta}$ är en isomorfism sådan att sidoklassen $< 5 > +r$ avbildas på $[r]_5 = r$ dvs $\theta(< 5 > +r) = r$ för $r = 0, 1, 2, 3, 4$.

(b) Helt allmänt är $\theta : \mathbb{Z} \to \mathbb{Z}_n$, där $\theta(a) = [a]_n$ en grupphomomorfism med $\operatorname{Ker}\theta = \{a \in \mathbb{Z} : \theta(a) = [a]_n = 0\} =< n >$. Enligt huvudsatsen om grupphomomorfismer är

$$\bar{\theta} : \mathbb{Z}/ < n > \cong \mathbb{Z}_n$$

en isomorfism sådan att $\bar{\theta}(< n > +r) = r$ för $r = 0, 1, \ldots, n-1$.

(c) Låt $\theta : \mathbb{R}^* \to U_2$ där $U_2 = \{1, -1\}$ med multiplikation och $\theta(r) = sgn\,(r)$ där $sgn\,(r) = 1$ då $r > 0$ och $sgn\,(r) = -1$ då $r < 0$*. □

Vi har

$$\operatorname{Ker}\theta = \{r \in \mathbb{R}^* : sgn\,(r) = 1\} = \mathbb{R}^*_{>0}$$

och enligt huvudsatsen om grupphomomorfismer är

$$\mathbb{R}^*/\mathbb{R}^*_{>0} \cong U_2.$$

Detta bekräftar vår tidigare observation att grupptabellen för $\mathbb{R}^*/\mathbb{R}^*_{>0}$ är väsentligen identisk med grupptabellen för U_2

Vi avslutar detta kapitel med ett intressant exempel på en grupphomomorfism nära relaterad till en mycket gammal sats som kallas "Kinesiska restsatsen".

(12.6) Sats. *Låt $n_1, n_2, \ldots, n_k$ vara parvis relativt prima positiva heltal (dvs $SGD(n_i, n_j) = 1$ då $i \neq j$). Då är*

$$\mathbb{Z}_{n_1 n_2 \ldots n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}.$$

Bevis. Betrakta funktionen:

$$\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

* "sgn" betyder "signum"= "tecken"

sådan att $\theta(a) = ([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k})$. Vi har $\theta(a+b) = ([a+b]_{n_1}, [a+b]_{n_2}, \ldots, [a+b]_{n_k}) = ([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k}) + ([b]_{n_1}, [b]_{n_2}, \ldots, [b]_{n_k}) = \theta(a) + \theta(b)$ så att θ är en grupphomomorfism.

$$\text{Ker}\theta = \{a \in \mathbb{Z} : [a]_{n_1} = 0, [a]_{n_2} = 0, \ldots, [a]_{n_k} = 0\} =< n_1 n_2 \ldots n_k >$$

ty $n_1|a, n_2|a, \ldots, n_k|a$ då och endast då $n_1 n_2 \ldots n_k|a$ tack vare förutsättningen att $n_1, n_2, \ldots, n_k$ är parvis relativt prima. Enligt huvudsatsen om homomorfismer är

$$\mathbb{Z}/ < n_1 n_2 \ldots n_k > \cong \theta(\mathbb{Z}) \subseteq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

Men $\mathbb{Z}/ < n_1 n_2 \ldots n_k > \cong \mathbb{Z}_{n_1 n_2 \ldots n_k}$ enligt exempel (11.5) b) så att $\theta(\mathbb{Z})$ har $n_1 n_2 \ldots n_k$ element. Lika många element finns det i produkten $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$. Alltså är $\theta(\mathbb{Z}) = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ dvs

$$\mathbb{Z}_{n_1 n_2 \ldots n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

varvid mot $a \in \mathbb{Z}_{n_1 n_2 \ldots n_k}$ svarar $([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k})$. □

(12.7) Kinesiska restsatsen. *Låt $n_1, n_2, \ldots, n_k$ vara relativt prima positiva heltal och låt $r_1 \in \mathbb{Z}_{n_1}, r_2 \in \mathbb{Z}_{n_2}, \ldots, r_k \in \mathbb{Z}_{n_k}$. Då existerar ett heltal x entydigt bestämt modulo $n_1 n_2 \ldots n_k$ sådant att*

$$[x]_{n_1} = r_1, [x]_{n_2} = r_2, \ldots, [x]_{n_k} = r_k.$$

Bevis. $(r_1, r_2, \ldots, r_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$. Enligt förra satsen finns det exakt en rest $x \in \mathbb{Z}_{n_1 n_2 \ldots n_k}$ sådan att

$$[x]_{n_1} = r_1,\ [x]_{n_2} = r_2, \ldots, [x]_{n_k} = r_k.$$

□

(12.8) Anmärkning. Kinesiska restsatsen formuleras ofta med hjälp av kongruenser. Då säger den att för relativt prima positiva heltal $n_1, n_2, \ldots, n_k$ och godtyckliga heltal $r_1, r_2, \ldots, r_k$ existerar ett heltal x så att

$$x \equiv r_1 \pmod{n_1},\ x \equiv r_2 \pmod{n_2}, \ldots, x \equiv r_k \pmod{n_i}.$$

Man behöver inte förutsätta att r_i är resten vid division med n_i därför att för varje heltal a gäller ju att $a \equiv [a]_{n_i} \pmod{n_i}$. □

Den bevismetod vi har valt säger inte hur man hittar x_0 då $n_1, n_2, \ldots, n_k$ och $r_1;, r_2, \ldots, r_k$ är givna. Vi skalla beskriva en algoritm som möjliggör att beräkna x_0. På det sättet får vi även ett annat bevis av (1.2) (men vårt första bevis har andra fördelar).

(12.9) Algoritm för kinesiska restsatsen. Givna positiva heltal $n_1, n_2, \ldots, n_k$ sådana att $SGD(n_i, n_j) = 1$ då $i \neq j$ och godtyckliga heltal $r_1, r_2, \ldots, r_k$. Bestäm x så att $x \equiv r_i \pmod{n_i}$ för $i = 1, 2, \ldots, k$.

(a) Låt $n = n_1 n_2 \dots n_k$. Beräkna x_i så att

$$(\frac{n}{n_i})x_i \equiv 1 \pmod{n_i}, \quad \text{dvs} \quad \frac{n}{n_i}x_i = 1 \quad \text{i } \mathbb{Z}_{n_i}.$$

Kommentar: $SGD(\frac{n}{n_i}, n_i) = 1$ enligt förutsättningen. Man måste hitta x_i så att $n_i|(\frac{n}{n_i})x_i - 1$ dvs $(\frac{n}{n_i})x_i - 1 = n_i y_i$ för ett heltal y_i dvs $(\frac{n}{n_i})x_i + n_i(-y_i) = 1$. Vi vet att x_i (och y_i) kan beräknas med hjälp av Euklides algoritm.

(b) Låt

$$x = r_1\frac{n}{n_1}x_1 + r_2\frac{n}{n_2}x_2 + \ldots + r_k\frac{n}{n_k}x_k.$$

Kommentar. Vi har:

$$[x]_{n_i} = [\sum_{j=1}^{k} r_j\frac{n}{n_j}x_j]_{n_i} = [r_i\frac{n}{n_i}x_i]_{n_i} = [r_i]_{n_i} \odot [\frac{n}{n_i}x_i]_{n_i} = [r_i]_{n_i}$$

ty

$$[\frac{n}{n_j}x_j]_{n_i} = \begin{cases} 1 & \text{om} \quad j = i \\ 0 & \text{om} \quad j \neq i \end{cases}$$

Alltså är $x \equiv r_i \pmod{n_i}$ för $i = 1, 2, \dots, k$.

Exempel. Låt oss bestämma ett heltal x som vid division med 3 ger resten 2, med 4 resten 3 och med 5 resten 4 dvs

$$x \equiv 2 \pmod 3,\ x \equiv 3 \pmod 4,\ x \equiv 4 \pmod 5.$$

Låt $n = 3 \cdot 4 \cdot 5 = 60$. Först måste vi bestämma x_1, x_2, x_3 sådana att

$$\frac{60}{3}x_1 = 20x_1 \equiv 1 \pmod 3,\ \frac{60}{4}x_2 = 15x_2 \equiv 1 \pmod 4,\ \frac{60}{5}x_3 = 12x_3 \equiv 1 \pmod 5.$$

Detta betyder att vi måste lösa ekvationerna:

$$2x_1 = 1 \quad \text{i } \mathbb{Z}_3,\ 3x_2 = 1 \quad \text{i } \mathbb{Z}_4,\ 2x_3 = 1 \quad \text{i } \mathbb{Z}_5$$

Vi hittar lätt (utan Euklides algoritm) att $x_1 = 2, x_2 = 3, x_3 = 3$ Enligt (11.4) (b) är

$$x = 2 \cdot \frac{60}{3} \cdot 2 + 3 \cdot \frac{60}{4} \cdot 3 + r \cdot \frac{60}{5} \cdot 3 = 359$$

en lösning. Den minsta icke-negativa lösningen är $[359]_{60} = 59$ (lösningen är entydigt bestämd modulo 60 enligt (11.2)). Lägg märke till att $x = 60q + 59$ med ett godtyckligt $q \in \mathbb{Z}$ är en lösning (ty $[x]_{60} = 59$) och att sådana x ger alla lösningar (se övning 12.6) □

ÖVNINGAR

12.1. Låt

$\mathbb{C}^*$ de komplexa talen med multiplikation,

$\mathbb{R}^*$ de reella talen med multiplikation,
$\mathbb{R}_+^*$ de reella positiva talen med multiplikation,
$U = \{z \in \mathbb{C}^* : |z| = 1\}$ med multiplikation,
$U_n = \{z \in \mathbb{C}^* : z^n = 1\}$ med multiplikation,
$U_\infty = \cup_{n=1}^{\infty} U_n$,
$\mathbb{R}$ de reella talen med addition,
$\mathbb{Z}$ heltalen med addition,
$\mathbb{Q}$ de rationella talen med addition.

Visa att

(a) $\mathbb{C}^*/U \cong \mathbb{R}_+^*$,

(b) $\mathbb{C}^*/\mathbb{R}_+^* \cong U$,

(c) $\mathbb{C}^*/U_n \cong \mathbb{C}^*$,

(d) $\mathbb{R}/\mathbb{Z} \cong U$,

(e) $U/U_n \cong U$,

(f) $\mathbb{Q}/\mathbb{Z} \cong U_\infty$,

(g) $\mathbb{R}^*/\mathbb{R}_+^* \cong U_2$.

12.2. Låt $G = GL_n(\mathbb{R})$ vara gruppen av alla $n \times n$ reella matriser med determinant $\neq 0$ med matirsmultiplikation. Visa att

(a) $G/H \cong \mathbb{R}^*$ om $H = \{A \in G : \det A = 1\}$

(b) $G/H \cong \mathbb{R}_+^*$ om $H = \{a \in G : |\det A| = 1\}$

(c) $G/H \cong U_2$ om $H = \{A \in G : \det A > 0\}$

(se 12.1 för beteckningarna).

12.3. Låt S_n vara den symmetriska grupen av grad n (alla permutationer av $1, 2, \ldots, n$) Låt $\theta : S_n \to U_2$ där

$$\theta(f) = \prod_{1 \leq i < j \leq n} sgn \frac{f(i) - f(j)}{i - j}$$

Visa att θ är en homomorfism vars kärna består av alla jämna permutationer dvs $\operatorname{Ker} \theta = A_n$ den alternerande grupen. ($f \in A_n \Leftrightarrow$ antalet par (i, j) sådana att $i < j$ och $f(i) > f(j)$ är jämnt). Visa att $S_n/A_n \cong U_2$.

12.4. Låt G vara en godtycklig grupp och $g \in G$. Visa att $\theta_g(x) = gxg^{-1}$ är automorfism av G (den kallas **den inre automorfismen** generad av g). Visa att alla inre automorfismer av G bildar en grupp.

12.5. Låt G vara en abelsk grupp och låt ett primtal p vara en delare till $o(G)$. Visa at G innehåller ett element av ordningen p.

Ledning. Induktion m.a.p. $o(G)$. Börja med $o(G) = p$. Antag därefter att det finns $g \in G$ så att $p|o(g)$ och visa satsen då. Om det inte finns g med den egenskapen betrakta $G/ < g >$. Utnyttja därefter den naturliga surjektionen $G \xrightarrow{\eta} G/ < g >= G'$ och induktionsantagandet om G'. Man kan utnyttja det att $o(\eta(g(o))|o(g)$.

Anmärkning: Påståendet gäller utan förutsättningen att G är abelsk. Det är Cauchys sats. Satsen har ett mycket enkelt bevis som enbart baseras på definitionen av begreppet grupp (men det är mycket svårt att komma på detta bevis.)

12.6. Låt H vara en delgrupp till G och N en normaldelgrupp till G. Då är $HN/N \cong H/N \cap H$.

Kapitel 13

RINGHOMOMORFISMER OCH IDEAL

(13.1) Definition. Låt R och R' vara ringar. Man säger att en funktion $\theta : R \to R'$ är en **(ring)homomorfism** om

$$\theta(a+b) = \theta(a) + \theta(b) \quad \text{och} \quad \theta(ab) = \theta(a)\theta(b)$$

då $a, b \in R$. Om θ är bijektiv kallas den **isomorfism**. En isomorfism θ kallas **automorfism** om $R' = R$. □

(13.2) Exempel. (a) låt $\theta : \mathbb{Z} \to \mathbb{Z}_n$ där $\theta(a) = [a]_n$. Då är

$$\begin{aligned} \theta(a+b) &= [a+b]_n = [a]_n \oplus [b]_n = \theta(a) \oplus \theta(b), \\ \theta(ab) &= [ab]_n = [a]_n \odot [b]_n = \theta(a) \odot \theta(b), \end{aligned}$$

så att θ är en ringhomomorfism.

(b) Låt $\theta : \mathbb{R}[X] \to \mathbb{R}$ där $\theta(p) = p(1)$ där $p \in \mathbb{R}[X]$. Då är

$$\begin{aligned} \theta(p_1 + p_2) &= (p_1 + p_2)(1) = p_1(1) + p_2(1) = \theta(p_1) + \theta(p_2), \\ \theta(p_1 p_2) &= p_1 p_2(1) = p_1(1)p_2(1) = \theta(p_1)\theta(p_2) \end{aligned}$$

dvs θ är en ringhomomorfism.

(c) Om $n = n_1 n_2 \dots n_k$ där n_i är parvis relativt prima positiva heltal så har vi en gruppisomorfism

$$\theta : \mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

sådan att $\theta(a) = ([a]_{n_1}, \dots, [a]_{n_k})$ (se Kinesiska restsatsen (5.9)). Nu kan vi konstatera att θ också är en ringisomorfism ty

$$\theta(ab) = ([ab]_{n_1}, \dots, [ab]_{n_k}) = ([a]_{n_1}, \dots, [a]_{n_k})([b]_{n_1}, \dots, [b]_{n_k}) = \theta(a)\theta(b).$$

□

Precis som för grupphomomorfismer har man följande enkla egenskaper som direkt följer ur definitionen:

(13.3) Sats. *Låt $\theta : R \to R'$ vara en ringhomomorfism. Då är:*

(a) $\theta(0) = 0$,

(b) $\theta(-a) = -\theta(a)$,

(c) *Om θ är en isomorfism så är även θ^{-1} en isomorfism.*

Bevis. (a) och (b) följer ur det faktum att $\theta : (R, +) \to (R', +)$ är en grupphomomorfism (ref se (10.3)). (c) bevisas på samma sätt som liknande påstående för grupphomomorfismer (se ref (10.4)b)). □

Det är klart att en ringhomomorfism $\theta : R \to R'$ är en gruphomomorfism $\theta : (R, +) \to (R', +)$. Alltså är

$$\operatorname{Ker}\theta = \{a \in R : \theta(a) = 0\}$$

en (normal) delgrupp till $(R, +)$. Men $\operatorname{Ker}\theta$ är inte bara en delgrupp till R. $\operatorname{Ker}\theta$ är en delring med en mycket speciell och mycket viktig egenskap.

(13.4) Definition. En icke-tom delmängd I till R kallas **ideal** om

(a) $a, b \in I \Rightarrow a - b \in I$,

(b) $r \in R$ och $a \in I \Rightarrow ra, ar \in I$. □

Observera att I är en delring till R ty (a) säger att $(I, +)$ är en delgrupp till $(R, +)$ (se rref (4.7)) och ur (b) följer att $a, b \in I$ ger $ab \in I$ dvs I är sluten med avseende på multiplikation.

(13.5) Exempel. (a) Låt $R = \mathbb{Z}$ och $I =< n >= \{0, \pm n, \pm 2n \ldots\}$, där n är ett fixt heltal. Man kontrollerar mycket lätt att I är ett ideal i R. I själva verket har varje ideal i $\mathbb{Z}$ just den här formen (se övning ref 14.8)

(b) Mera allmänt än i (a) låt R vara en godtycklig kommutativ ring och $a \in R$. Låt

$$I = (a) = \{ra, r \in R\}.$$

(a) är ett ideal i R ty $r_1a, r_2a \in I$ ger $r_1a - r_2a = (r_1 - r_2)a \in I$ och $r' \in R$, $ra \in I$ ger $r'ra \in I$ (R är kommutativ). Man säger att (a) är ett **huvudideal** (eller **principalideal**) och a dess **generator**. Observera notationen (a) i stället för $< a >$ som vi använde för grupper (i exempel (a) ovan är $< n >$ och (n) samma mängd). Ett integritetsområde (rref se (13.9)) i vilket varje ideal är principalt kallas **huvudidealområde**. $\mathbb{Z}$ och polynomringarna $K[X]$, K en kropp, är just exempel på huvudidealområden – vi visar detta påstående i övningar (se övning rref).

(c) Man kan gå lite längre och generalisera (b). Låt R vara en godtycklig kommutativ ring och $a_1, a_2, \ldots, a_k \in R$. Låt

$$I = (a_1, a_2, \ldots, a_k) = \{r_1a_1 + r_2a_2 + \ldots + r_ka_k, r_1, r_2, \ldots, r_k \in R\}.$$

I är ett ideal, vilket följer lika enkelt som fallet $k = 1$ i (b): om $x = r_1a_1+r_2a_2+\ldots+r_ka_k, x' = r'_1a_1 + r'_2a_2 + \ldots + r'_ka_k \in I$ så är

$$x - x' = (r_1 - r'_1)a_1 + (r_2 - r'_2)a_2 + \ldots + (r_k - r'_k)a_k \in I$$

och

$$rx = rr_1a_1 + rr_2a_2 + \ldots + rr_ka_k \in I.$$

Man säger att detta ideal **genereras** av $a_1, a_2, \ldots, a_k$. □

(13.6) Sats. *Låt $\theta : R \to R'$ vara en ringhomomorfism. Då är $\mathrm{Ker}\,\theta$ ett ideal i R.*

Bevis. Om $a, b \in \mathrm{Ker}\,\theta$ så är $\theta(a - b) = \theta(a) - \theta(b) = 0$ dvs $a - b \in \mathrm{Ker}\,\theta$. Om $r \in R$ och $a \in \mathrm{Ker}\,\theta$ så är $\theta(ra) = \theta(r)\theta(a) = 0$ och $\theta(ar) = \theta(a)\theta(r) = 0$ dvs $ra, ar \in \mathrm{Ker}\,\theta$. Villkoren (a) och (b) i (13.4) är alltså uppfyllda. □

Med utgångspunkt från den abelska gruppen $(R, +)$ och dess delgrupp $(I, +)$ kan man bilda kvotgruppen $(R/I, +)$ i enlighet med vår tidigare konstruktion (se ref (9.6)). Men R är en ring så att man gärna vill ha en ringstruktur även på R/I. Låt oss påminna om att $(R/I, +)$ består av alla sidoklasser $I + a$ med addition $(I + a) + (I + b) = I + (a + b)$. Låt oss också påminna om att $I + a = I + b$ då och endast då $a - b \in I$.

(13.7) Sats. *Låt R vara en ring och I ett ideal i R. Då bildar sidoklasserna $I + a, a \in R$, en ring med addition:*

$$(I + a) + (I + b) = I + (a + b)$$

och multiplikation som definieras så att

$$(I + a)(I + b) = I + ab.$$

Bevis. Vi vet redan at $(R/I, +)$ är en abelsk grupp. Vår definition av produkten av sidoklasserna är lite känslig. Den beror nämligen på representanterna a och b av sidoklasserna $I+a$ och $I + b$. Det kan hända att $I + a = I + a'$ och $I + b = I + b'$. Är då $I + ab = I + a'b'$? Med andra ord är det så att $a - a' \in I$ och $b - b' \in I$ ger $ab - a'b' \in I$? Svaret följer enkelt:

$$ab - a'b' = (a - a')b + a'(b - b') \in I \quad \text{ty} \quad (a - a')b, a'(b - b') \in I.$$

Nu vet vi att vår definition av multiplikation av sidoklasserna är helt korrekt (beror inte på sidoklassernas representanter). Det är lätt att kontrollera resten av ringdefinitionen dvs associativiteten:

$$[(I + a)(I + b)](I + c) = (I + ab)(I + c) = I + (ab)c = I + a(bc) = (I + a)[(I + b)(I + c)]$$

och distributiviteten (den ena, den andra på samma sätt):

$$\begin{aligned}(I+a)(I+b+I+c) &= (I+a)(I+b+c) = I+a(b+c) = \\ &= I+ab+ac = I+ab+I+ac = \\ &= (I+a)(I+b)+(I+a)(I+c)\end{aligned}$$

□

(13.8) Definition. Ringen R/I dvs ringen av alla sidoklasser $I+a$ med addition $(I+a)+(I+b) = I+a+b$ och multiplikation $(I+a)(I+b) = I+ab$ kallas **kvotringen** av R modulo idealet I. □

(13.9) Exempel. $R = \mathbb{Z}$ och $I = (5)$. Då består $\mathbb{Z}/(5)$ av sidoklasserna $\bar{0} = (5)+0, \bar{1} = (5)+1, \bar{2} = (5)+2, \bar{3} = (5)+3, \bar{4} = (5)+4$ och additions- och multiplikationstabellerna för $\mathbb{Z}/(5)$ är följande:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

□

Precis som varje normal delgrupp är kärnan till en grupphomomorfism är varje ideal kärnan till en ringhomomorfism.

(13.10) Sats. *Låt I vara ett ideal i R. Då är funktionen $\eta : R \to R/I$ där $\eta(a) = I+a$ en surjektiv ringhomomorfism och $Ker\,\eta = I$.*

Bevis. Vi har

$$\begin{aligned}\eta(a+b) &= I+(a+b) = I+a+I+b = \eta(a)+\eta(b), \\ \eta(ab) &= I+ab = (I+a)(I+b) = \eta(a)\eta(b),\end{aligned}$$

så att η är en ringhomomorfism. η är surjektiv ty sidoklassen $I+r$ (r godtyckligt) är bilden av $r \in R$. Slutligen är $\mathrm{Ker}\,\eta = \{a \in R : \eta(a) = I+a = I\} = I$ ty $I+a = I$ då och endast då $a \in I$ (se rref (7.3)c)). □

Mot huvudsatsen om grupphomomorismer svarar följande sats:

(13.11) Huvudsatsen om ringhomomorismer. *Låt $\theta : R \to R'$ vara en ringhomomorism och $I = Ker\theta$. Då är*

$$R/I \cong \theta(R)$$

och en isomorfism $\bar{\theta}$ får man då $\bar{\theta}(I+a) = \theta(a)$.

Bevis. Vi vet redan att $\bar{\theta}$ definierar en isomorfism mellan grupperna $(R/I, +)$ och $(\theta(R), +)$. Det enda som återstår är att kontrollera den multiplikativa egenskapen hos $\bar{\theta}$:

$$\bar{\theta}((I+a)(I+b)) = \bar{\theta}(I+ab) = \theta(ab) = \theta(a)\theta(b) = \bar{\theta}(I+a)\bar{\theta}(I+b).$$

□

(13.12) Exempel. (a) Låt $\theta : \mathbb{Z} \to \mathbb{Z}_5$ där $\theta(a) = [a]_5$ (se ref (14.2) a)). Här är $\operatorname{Ker}\theta = \{a \in \mathbb{Z} : \theta(a) = [a]_5 = 0\} = (5)$. Enligt ref (14.11) är

$$\bar{\theta} : \mathbb{Z}/(5) \cong \mathbb{Z}_5$$

där $\bar{\theta}((5)+r) = r$ för $r = 0, 1, 2, 3, 4$. Helt allmänt är $\mathbb{Z}/(n) \cong \mathbb{Z}_n$, där $\bar{\theta}((n)+r) = r$ för $r = 0, 1, \ldots, n-1$ ger en ringisomorfism mellan dessa grupper.

(b) Låt R vara ringen av alla reella funktioner $f : \mathbb{R} \to \mathbb{R}$ med addition $(f+g)(x) = f(x) + g(x)$, $x \in \mathbb{R}$, och multiplikation $(fg)(x) = f(x)g(x)$, $x \in \mathbb{R}$. Låt $\theta : R \to \mathbb{R}$ där $\theta(f) = f(0)$. θ är en ringhomomorfism ty

$$\begin{aligned} \theta(f+g) &= (f+g)(0) = f(0) + g(0) = \theta(f) + \theta(g), \\ \theta(fg) &= (fg)(0) = f(0)g(0) = \theta(f)\theta(g). \end{aligned}$$

Vi har $\operatorname{Ker}\theta = \{f \in R : \theta(f) = f(0) = 0\} =: I_0$ (idealet bestående av alla funktioner som antar värdet 0 i punkten $x = 0$). Vi har $\theta(R) = \mathbb{R}$ ty varje $r \in \mathbb{R}$ är bilden av en funktion (t ex den konstanta funktionen $f(x) = r$, $x \in \mathbb{R}$). Enligt sats rref (14.11) är

$$R/I_0 \cong \mathbb{R}$$

där en isomorfism är given då $\bar{\theta}(f) = f(0)$ dvs mot sidoklassen $I_0 + f$ svarar $f(0)$ (sidoklassen består av alla funktioner som i punkten 0 antar samma värde).

(c) Låt R vara en ring med etta 1 och låt

$$\theta : \mathbb{Z} \to R,$$

där $\theta(a) = a1$. Då är θ en ringhomomorfism ty

$$\begin{aligned} \theta(a+b) &= (a+b)\cdot 1 = a\cdot 1 + b\cdot 1 = \theta(a) + \theta(b), \\ \theta(ab) &= (ab)\cdot 1 = (a\cdot 1)\cdot(b\cdot 1) = \theta(a)\theta(b). \end{aligned}$$

Vi har $\operatorname{Ker}\theta = \{a \in \mathbb{Z} : \theta(a) = a1 = 0\} = (n)$ för något heltal $n \geq 0$ (se rref (14.5) a)). Enligt huvudsatsen om ringhomomorfismer är

$$\mathbb{Z}/(n) \cong \theta(\mathbb{Z}) \subseteq R.$$

Men $\mathbb{Z}/(n) \cong \mathbb{Z}$ då $n = 0$ eller $\mathbb{Z}_n$ då $n > 0$. Alltså innehåller R en delring isomorf med $\mathbb{Z}$ eller $\mathbb{Z}_n$ som består av alla heltaliga multipler av ettan i R. □

Sista exemplet är grunden för följande definition:

(13.13) Definition. Man säger att **karakteristiken** av en kommutativ ring R med etta är n om alla multipler $k \cdot 1$, där $k \in \mathbb{Z}$, bildar en ring isomorf med $\mathbb{Z}_n$ och att den är 0 om dessa multipler bildar en ring isomorf med $\mathbb{Z}$. □

Vi noterar en särskilt viktig egenskap hos karakteristiken av en ring:

(13.14) Sats. *Karakteristiken av ett integritetsområde är 0 eller ett primtal.*

Bevis. Om karakteristiken inte är 0 så genererar alla multipler av 1 en delring isomorf med $\mathbb{Z}_n$. Men $\mathbb{Z}_n$ saknar nolldelare då och endast då n är ett primtal (se rref (13.10) a) b)). □

ÖVNINGAR

13.1. Vilka av följande funktioner är ringhomomorfismer? Bestäm kärnan och bilden för varje ringhomomorfism.

(a) $\theta : \mathbb{R}[X] \to \mathbb{C}$, $\theta(p) = p(a)$, $a \in \mathbb{R}$, a fixt.

(b) $\theta : \mathbb{R}[X] \to \mathbb{C}$, $\theta(p) = p(i)$.

(c) $\theta : \mathbb{Z}[X] \to \mathbb{C}$, $\theta(p) = p(\sqrt{2})$.

(d) $\theta : \mathbb{R}[X] \to \mathbb{C}$, $\theta(p) = p(\sqrt{2})$.

(e) $\theta : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\theta((a, b)) = a$.

(f) $\theta : \mathbb{R}[X] \to \mathbb{R}[X]$, $\theta(p) = p'$ (derivatan).

13.2. Visa att följande funktioner är ringautomorfismer:

(a) $\theta : \mathbb{R}[X] \to \mathbb{R}[X]$, $\theta(p(X)) = p(-X)$.

(b) $\theta : \mathbb{C} \to \mathbb{C}$, $\theta(z) = \bar{z}$.

(c) $\theta : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $\theta((a, b)) = (b, a)$.

(d) $\theta : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$ (se övn. rref 13.5 b)).

13.3. Ge exempel på en ringhomomorfism $\theta : R \to R'$ så att

(a) R saknar en etta, R' har en etta.

(b) R har nolldelare, R' saknar nolldelare.

(c) R saknar nolldelare, R' har nolldelare.

(d) R har en etta, R' saknar en etta.

13.4. Låt $\theta : R \to R'$ vara en ringhomomorfism. Visa att även $\theta^* : R[X] \to R'[X]$ där $\theta^*(a_0 + a_1X + \ldots + a_nX^n) = \theta(a_0) + \theta(a_1)X + \ldots + \theta(a_n)X^n$ är en ringhomomorfism.

13.5. Låt $\theta : R \to R'$ vara en ringhomomorfism. Visa att

(a) $\theta^{-1}(I')$ är ett ideal i R som innehåller $\operatorname{Ker}\theta$ då I' är ett ideal i R'.

(b) $\theta(I)$ behöver inte vara ett ideal i R' då I är ett ideal i R men $\theta(I)$ är ett ideal i R' om θ är en surjektion.

13.6. Låt $\theta : R \to R'$ vara en surjektiv ringhomomorfism. Man ordnar mot ett ideal I' i R' dess urbild $\theta^{-1}(I')$ i R. Visa att olika ideal i R' ger olika ideal i R som innehåller $\operatorname{Ker}\theta$ och att man får alla sådana ideal i R.

13.7. Visa att en ringhomomorfism $\theta : R \to R'$ är injektiv då och endast då $\operatorname{Ker}\theta = (0)$.

13.8. Bestäm alla ideal i följande ringar:

(a) $\mathbb{Z}$, (b) $\mathbb{Z}_4$, (c) $\mathbb{Z}_5$, (d) $\mathbb{Z}_n$.

13.9. Visa att om I_1, I_2 är ideal i en kommutativ ring R så är

(a) $I_1 + I_2 = \{a + b, a \in I_1, b \in I_2\}$,

(b) $I_1 I_2 = \{\sum a_k b_k, a_k \in I_1, b_k \in I_2\}$,

(c) $I_1 \cap I_2$

ideal i R.

13.10. Visa att om $I_1 = (a), I_2 = (b)$ är ideal i $\mathbb{Z}$ så är $I_1 + I_2 = (SGD(a, b))$ och $I_1 \cap I_2 = (MGM(a, b))$ (se rref 14.9).

13.11. Visa att följande ideal inte är huvudideal:

(a) $(2, X)$ i ringen $\mathbb{Z}[X]$,

(b) (X, Y) i ringen $\mathbb{R}[X, Y]$.

13.12. Visa att

(a) $\mathbb{R}[X]/(X) \cong \mathbb{R}$, (b) $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$,
(c) $\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{R} \times \mathbb{R}$, (d) $\mathbb{Z}[Z]/(X^2 + 1) \cong \mathbb{Z}[i]$,
(e) $\mathbb{Z}[X]/(X^2 - X) \cong \mathbb{Z} \times \mathbb{Z}$, (f) $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}_2$.

13.13. Bestäm karakteristiken av följande ringar:

(a) $\mathbb{Z}_n$, (b) $\mathbb{Z}$, (c) $\mathbb{Q}$,
(e) $\mathbb{R}$, (f) $\mathbb{Z}_2[X]$, (g) $\mathbb{Z}_n[X]$.

13.14. Låt R vara en kommutativ ring av karakteristiken p, där p är ett primtal. Visa att om $a, b \in R$ så är

$$(a + b)^p = a^p + b^p$$

och, mera allmänt,

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Kapitel 14

FAKTORUPPDELNINGAR I RINGAR

Aritmetikens fundamentalsats säger att varje positivt heltal större än 1 är en produkt av primtal och primtalsfaktorerna är entydiga så när som på ordningsföljden. T ex $10 = 2{\cdot}5 = 5{\cdot}2$. Liknande påstående gäller för alla heltal, men det finns något större variationsmöjligheter t ex $10 = 2 \cdot 5 = (-2) \cdot (-5) = (-5) \cdot (-2) = 5 \cdot 2$. Den här gången är varje heltal skilt från 0 och ± 1 en produkt av primtal multiplicerade med ± 1. Framställningen är också entydig så när som på faktorernas ordning. I detta kapitel vill vi besvara frågan om möjligheten att definiera liknande faktoruppdelningar i andra ringar. Vi kommer att se att denna fråga är mycket naturlig och leder till mycket intressanta tillämpningar. Samtidigt får vi en mycket bättre förståelse av primtalen och irreducibla polynom.

Först måste vi definiera i godtyckliga ringar element som svarar mot enheterna ± 1 i heltalen och som kan "störa" faktoruppdelningar.

(14.1) Definition. Ett element $\varepsilon \in R$ kallar man för en **enhet** om ε har en multiplikativ invers dvs det finns $\varepsilon' \in R$ så att $\varepsilon\varepsilon' = 1$. Mängden av alla enheter i R betecknas med R^*. □

(14.2) Sats. *Alla enheter i en kommutativ ring med etta R bildar en (abelsk) grupp med avseende på multiplikation.*

Bevis. Om $\varepsilon_1, \varepsilon_2 \in R^*$ så $\varepsilon_1\varepsilon_2 \in R^*$ ty $\varepsilon_1\varepsilon_1' = 1$ och $\varepsilon_2\varepsilon_2' = 1$ ger att $(\varepsilon_1\varepsilon_2)(\varepsilon_1'\varepsilon_2') = 1$. Multiplikation är associativ, det neutrala elementet är 1 och definitionsmässigt finns en invers till varje $\varepsilon \in R$. □

(14.3) Exempel. (a) $\mathbb{Z}$ har enbart två enheter ± 1.

(b) Om K är en kropp så är alla element $a \in K$, $a \neq 0$ enheter ty $(K \setminus \{0\}, \cdot)$ är en grupp.

(c) Om K är en kropp så är alla enheter i polynomringen $K[X]$ konstanta nollskilda polynom dvs $K[X]^* = K^*$

(d) Enheterna i ringen av de Gaussiska heltalen $\mathbb{Z}[i]$ är $\pm 1, \pm i$. Om $a + bi$ är en enhet, så är $(a + bi)(c + di) = 1$, där $c + di \in \mathbb{Z}[i]$. Om man tar beloppen och kvadrerar bägge leden i den sista likheten så får man $(a^2 + b^2)(c^2 + d^2) = 1$. Alltså är $a^2 + b^2 = 1$. Detta ger $a = \pm 1$ och $b = 0$ eller $a = 0$ och $b = \pm 1$, vilket leder till de fyra enheterna ovan.

□

Enheterna kan inplanteras i faktorupdelningar av godtyckliga element i ringen: $a \in R$ kan skrivas som produkt $a = \varepsilon\varepsilon' a$ dvs enheten ε är en faktor i ett godtyckligt element i ringen. Detta betyder att varje faktoruppdelning kan störas" med enheter. Det märkte vi redan i heltalsringen $\mathbb{Z}$ där $\mathbb{Z}^* = \{+1, -1\}$, vilket ger att t ex $10 = 2 \cdot 5 = (-2) \cdot (-5)$. Hur kan vi definiera motsvarigheten till primtal i godtyckliga ringar? Vi har följande begrepp:

(14.4) Definition. Ett nollskilt element $p \in R$ kallas **irreducibelt** om p inte är en enhet och varje faktoruppdelning av p i två faktorer måste innehålla en enhet dvs om $p = ab$ så är a eller b en enhet. □

(14.5) Exempel. (a) Irreducibla element i $\mathbb{Z}$ är alla tal $\pm p$, där p är ett primtal. Detta påstående är självklart, men tänk en stund på motiveringen att alla sammansatta tal inte är irreducibla.

(b) Irreducibla element i polynomringen $\mathbb{C}[X]$ är alla irreducibla polynom (observera att definitionen (**??**) är ett specialfall av definitionen (14.4)). På samma sätt sammanfaller alla irreducibla element i en godtycklig polynomring $K[X]$ över en kropp K med alla irreducibla polynom i denna ring. Termen "irreducibelt" element sammanfaller här med termen "irreducibelt polynom".

(c) Vi skall visa att talet $2 + i$ är irreducibelt i ringen av de Gaussiska heltalen $\mathbb{Z}[i]$. Först låt oss repetera att enheterna i denna ring är ± 1 och $\pm i$ (se (14.3)(d)). Antag nu att

$$2 + i = (a + bi)(c + di),$$

där $a + bi$ och $c + di$ är Gaussiska heltal dvs $a, b, c, d \in \mathbb{Z}$. I den sista likheten tar vi beloppet och kvadrerar både vänster och högerled. Då får vi att $5 = (a^2 + b^2)(c^2 + d^2)$, vilket implicerar att $a^2 + b^2 = 1$ eller $c^2 + d^2 = 1$. I det första fallet är $a + bi$ en enhet, och i det andra, är $c + di$ en enhet. Observera att t ex $a^2 + b^2 = 1$ ger $a = \pm 1, b = 0$ eller $a = 0, b = \pm 1$. Det är inte så lätt att beskriva alla irreducibla element bland de Gaussiska heltalen. Se vidare övning 14.6.
□

Om p är ett irreducibelt element och ε är en enhet så är också εp ett irreducibelt element. Vi säger att dessa två irreducibla element är associerade. Rent formellt noterar vi det i följande form:

(14.6) Definition. Man säger att två irreducibla element p och p' är **associerade** om $p' = \varepsilon p$, där ε är en enhet. □

T ex är $+5$ och -5 två associerade irreducibla element i $\mathbb{Z}$.

Nu kan vi definiera vad vi menar med entydig faktoruppdelning i ett godtyckligt integritetsområde.

(14.7) Definition. Låt R vara ett integritetsområde. Man säger att R har **entydig faktoruppdelning** eller är UFD *

om varje nollskilt element $a \in R$ som inte är en enhet kan skrivas som produkt av irreducibla element i R:

$$a = p_1 p_2 \cdots p_k$$

och om

$$a = p_1 p_2 \cdots p_k = p_1' p_2' \cdots p_l'$$

där alla p_i' är irreducibla, så är $k = l$ (dvs antalet irreducibla faktorer i varje faktoruppdelningen av a är samma) och vid en lämplig numrering av faktorerna är p_i associerat med p_i' för $i = 1, 2, \ldots, k$. □

(14.8) Exempel. (a) Heltalsringen $\mathbb{Z}$ har entydig faktoruppdelning. Detta påstående är just aritmetikens fundamentalsats.

(b) Vi vet redan (se (**??**)) att varje polynomring $K[X]$ över en kropp K har entydig faktoruppdelning.

□

Det sista exemplet är ett specialfall av ett mera allmänt påstående om en hel klass av ringar som tillåter divisionsalgoritmen precis som heltalsringen $\mathbb{Z}$ och polynomringarna $K[X]$. Innan vi definierar denna klass av ringar som kallas Euklidiska (från Euklides algoritm), ger vi ett intressant exempel på en ett integritetsområde som saknar entydig faktoruppdelning.

(14.9) Exempel. Låt $R = \mathbb{Z}[\sqrt{-5}]$. Vi påminner om att denna ring är den minsta delring till de komplexa talen som innehåller både $\mathbb{Z}$ och $\sqrt{-5}$ så att $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\}$. Enheterma i denna ring är ± 1 (se 14.7). Vi har

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

och vi tänker visa att talen $3, 2 \pm \sqrt{-5}$ är irreducibla. Detta betyder att talet 9 har två helt olika faktoruppdelningar i produkt av irreducibla tal därför att faktorerna 3 och $2 \pm \sqrt{-5}$ inte är associerade (det är klart att $3 \neq 2 \pm \sqrt{-5}$). Antag att $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Genom

*"UFD" betyder "unique factorization domain".

att kvadrera absolutbeloppen av bägge leden får man likheten $9 = (a^2 + 5b^2)(c^2 + 5d^2)$. Den första faktorn till höger måste vara lika med 1, 3 eller 9. Om $a^2 + 5b^2 = 1$ så är $a + b\sqrt{-5}$ en enhet (ty $a = \pm 1$ och $b = 0$). Likheten $a^2+5b^2 = 3$ är inte möjlig. Slutligen ger $a^2+5b^2 = 9$ att $c^2 + 5d^2 = 1$, så att i detta fall $c + d\sqrt{-5}$ är en enhet. Detta visar att minst en av faktorerna i faktoruppdelningen av 3 måste vara en enhet dvs talet 3 är irreducibelt. På liknande sätt visas att $2 \pm \sqrt{-5}$ är irreducibla: $2 \pm \sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$ ger också $9 = (a^2+5b^2)(c^2+5d^2)$ och man resonerar precis som ovan. □

Nu skall vi diskutera en liten, men ganska intressant klass av ringar som har entydig faktoruppdelning.

(14.10) Definition. Man säger att ett integritetsområde R är **Euklidiskt** om det finns en funktion $d : R \setminus \{0\} \to \mathbb{N}$ (här är $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$) sådan att

(a) $d(ab) \geq d(a)$,

(b) för godtyckliga $a, b \in R$, $b \neq 0$, existerar $q, r \in r$ så att $a = bq + r$ och $d(r) < d(b)$ eller $r = 0$. □

Villkoret (b) säger att i ringen R gäller en egenskap som påminner om Euklides divisionsalgoritm för heltalen eller polynom. Detta motiverar termen "Euklidisk ring".

(14.11) Exempel. (a) Vi vet mycket väl att både $\mathbb{Z}$ och polynomringarna $K[X]$, K en kropp, har divisionsalgoritmen och således är Euklidiska ringar. I $\mathbb{Z}$ har vi funktionen $d(a) = |a|$, medan i polynomringarna fungerar divisionsalgoritmen med funktionen $d(f) = grad(f)$ för nollskilda polynom $f \in K[X]$.

(b) Vi skall visa att de Gaussiska heltalen $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ är en Euklidisk ring med funktionen $d(z) = |z|^2 = a^2 + b^2$ då $z = a + bi$. Den första egenskapen $d(z_1 z_2) \geq d(z_1)$ är självklar ty $|z_1 z_2|^2 \geq |z_1|^2$. För att visa det andra villkoret låt $z_1 = a + bi$ och $z_2 = c + di \neq 0$. Vi vill visa att det finns $q, r \in \mathbb{Z}[i]$ så att $z_1 = z_2 q + r$ och $d(r) \leq d(z_2)$ eller $r = 0$ (vilket betyder här att $d(r) = 0$). Låt

$$\frac{z_1}{z_2} = \alpha + \beta i,$$

där $\alpha\beta \in \mathbb{Q}$. Låt oss välja två heltal q_1 och q_2 så att $|\alpha - q_1 \leq 1/2$ samt $|\beta - q_2| \leq 1/2$ (tänk på α och β som punkter på den rella axeln och q_1 och q_2 som de heltal som ligger närmast dem – ibland kan q_1 eller q_2 väljas på två olika sätt). Definiera nu $q = q_1 + q_2 i$. Då är

$$\frac{z_1}{z_2} = q + (\alpha - q_1) + (\beta - q_2)i$$

och $z_1 = z_2 q + r$, där $r = [(\alpha - q_1) + (\beta - q_2)i]z_2$. Det är klart att $q \in \mathbb{Z}[i]$ så att $r = z_1 - z_2 q \in \mathbb{Z}[i]$ ty $z_1, z_2 \in \mathbb{Z}[i]$. Dessutom

$$d(r) = |[(\alpha - q_1) + (\beta - q_2)i]z_2|^2 = [(\alpha - q_1)^2 + (\beta - q_2)^2]|z_2|^2 < (\frac{1}{4} + \frac{1}{4})|z_2|^2 < \frac{1}{2}|z_2|^2 < |z_2|^2 = d(z_2)$$

□

För Euklidiska ringar gäller följande egenskap:

(14.12) Sats. *Varje Euklidisk ring har entydig faktoruppdelning.*

Man kan bevisa detta påstående genom att följa argumenteringen i beviset för aritmetikens huvudsats (se (**??**)) med induktion med avseende på värdet av funktionen $d(a)$ för a tillhörande ringen (se 14.11). Men satsen följer från en annan, mera allmän, sats som säger att varje huvudidealområde (dvs ett integritetsområde i vilket varje ideal är principalt – se (**??**)) har entydig faktoruppdelning. Vi skall först visa att Euklidiska ringar verkligen är huvudidealringar. Satsen om entydiga faktoruppdelningar i huvudidealringar lämnar vi som något svårare övning 14.10.

(14.13) Sats. *Varje Euklidisk ring är en huvudidealring.*

Bevis. Låt I vara ett ideal i en Euklidisk ring R med avseende på en funktion d. Om $I = (0)$ så är I ett huvudideal. Låt $I \neq (0)$. Välj $a \in I$, $a \neq 0$, så att funktionen $d(x)$ med $x \in I$ antar sitt minsta värde. Detta är möjligt ty funktionsvärdena $d(x)$ är naturliga tal. Vi påstår att $I = (a)$. Det är klart att varje multipel av a tillhör I ty $a \in I$. Alltså $(a) \subseteq I$. För att visa den motsatta inklusionen tag $x \in I$. Enligt (14.10) (b) är $x = aq + r$, där $q, r \in R$ och $d(r) < d(a)$ eller $r = 0$. Men $r = x - aq \in I$ så att $d(r)$ kan inte vara mindre än $d(a)$ enligt definitionen av a. Alltså måste $r = 0$ så att $x = aq \in (a)$. Slutligen får vi att $I = (a)$. □

Nu noterar vi

(14.14) Sats. *Varje huvudidealområde har entydig faktoruppdelning.*

Bevis. Se övning 14.10 □.

(14.15) Anmärkning. Om $D < 0$ så har ringen $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{-D}, a, b \in \mathbb{Z}\}$ entydig faktoruppdelning endast då $D = -1$ och -2. Ringarna med $D > 0$ är ganska ofta huvuidealringar och således har de då entydig faktoruppdelning, men det är inte känt om det finns oändligt många sådana huvuidealringar. Man har bevisat att ringarna $\mathbb{Z}[\sqrt{D}]$ är Euklidiska med avseende på normfunktionen" $d(a + b\sqrt{D}) = |a^2 - Db^2|$ då $D = 2, 3, 6, 7, 11, 19, 55$, men man förmodar att om en sådan ring är en huvudidealring så är den Euklidisk med avseende på en lämplig funktion d. Tyvärr känner man inte ett enda exempel på en ring $\mathbb{Z}[\sqrt{D}]$ som är Euklidisk, men inte med avseende på funktionen d ovan. Ringen $\mathbb{Z}[\sqrt{14}]$ är en huvuidealring (inte så enkelt att visa) och troligen är den också Euklidisk fast med all säkerhet inte med avseende på normfunktionen ovan utan på en helt annan funktion. □

Vi skall avsluta detta kapitel med en tillämpning av satsen (14.13). För flera tusen år sedan intresserade man sig för naturliga tal som kan skrivas som summor av två heltaliga kvadrater dvs tal n sådana att $n = x^2 + y^2$, där x och y är heltal. Den som gav en lösning var den franske matematikern Pierre Fermat. Låt oss börja med en enkel observation:

(14.16) Proposition. *Om n är ett naturligt tal som lämnar resten 3 vid division med 4 så kan man inte skriva n som summa av två heltaliga kvadrater.*

Bevis. Om $n = x^2 + y^2$ så kan vi ta rester av bägge leden vid division med 4. Vi får då likheten

$$[n]_4 = 3 = [x]_4^2 + [y]_4^2.$$

Men för varaje heltal x är $[x]_4^2 = 0$ eller 1 beroende på om x är jämnt eller udda. Detta betyder att i den sista likheten är höger led lika med 0, 1 eller 2, men aldrig 3. Detta visar vårt påstående. □

Om $n = p$ är ett primtal så är villkoret i den sista propositionen det enda hindret för att kunna skriva talet p som summa av två heltaliga kvadrater. Alltså är varje primtal som inte lämnar resten 3 vid division med 4 en summa av två heltaliga kvadrater. Hur är det mera allmänt framgår av övningar (se övning 14.8).

(14.17) Sats. *Om p är ett primtal som inte lämnar resten 3 vid division med 4 så är p en summa av två heltaliga kvadrater.*

Bevis. Om $p = 2$ så är påståendet klart ty $2 = 1^2 + 1^2$. Antag att p är udda. Enligt förutsättningen lämnar p resten 1 vid division med 4 ty ett udda heltal lämnar antingen resten 1 eller 3 vid division med 4. Som vi vet satisfierar varje rest r modulo p ekvationen

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) = 0.$$

Hälften av $p-1$ rötter till denna ekvation är nollställen till den första faktorn och den andra hälften till den andra faktorn. Alltså finns det en rest r_0 sådan att $r_0^{\frac{p-1}{2}} = -1$. Men $p = 4k+1$ så att $(r_0^k)^2 = -1$ dvs $r = r_0^k$ satisfierar ekvationen $r^2 = -1$. Med andra ord är $p|r^2 + 1$.

Betrakta nu idealet $(p, r + i)$ genererat av p och $r + i$ i ringen $\mathbb{Z}[i]$. Detta är ett huvudideal precis som alla ideal i den ringen. Låt $(p, r + i) = (a + bi)$. Detta betyder att $a + bi$ dividerar både p och $r + i$. Men $(a + bi)|p$ och $(a + bi)|(r + i)$ ger att $a^2 + b^2|p^2$ och $a^2 + b^2|(r^2 + 1)$ (tag beloppen – se också övning 14.4). Men $r^2 + 1 < (p - 1)^2 + 1 < p^2$, så att $a^2 + b^2 = 1$ eller p. Vi vill utesluta den första möjligheten. $a^2 + b^2 = 1$ innebär att $a + bi$ är en enhet och då är $(p, r + i) = \mathbb{Z}[i]$. Vi får då $1 = px + (r + i)y$, där x, y är Gaussiska heltal. Multiplicera bägge leden med $r - i$. Då är $r - i = px(r - i) + (r^2 + 1)y$, vilket visar att $p|r - i$ ty p dividerar de två termerna till höger. Detta är dock inte sant så att likheten $a^2 + b^2 = 1$ måste uteslutas.

Det återstår den andra möjligheten att $a^2 + b^2 = p$, vilket visar att p är en summa av två kvadrater.

□

ÖVNINGAR

14.1. Bestäm alla enheter i följande ringar:

(a) $\mathbb{R}[X]$,

(b) $\mathbb{Z}[i]$

(c) $\mathbb{Z}[\sqrt{-d}], d \in \mathbb{Z}, d > 0$.

14.2. (a) Låt R_1 och R_2 vara två kommutativa ringar med etta. Visa att $(R_1 \times R_2)^* = R_1^* \times R_2^*$.

(b) Låt a och b vara två relativt prima positiva heltal. Utnyttja (a) och isomorfismen $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ (se (5.9)) för att bevisa att Eulers funktion är multiplikativ dvs $\phi(ab) = \phi(a)\phi(b)$ då $SGD(a, b) = 1$.

14.3. Visa att följande ringar är Euklidiska

(a) $\mathbb{Z}[\sqrt{-2}]$ med funktionen $d(z) = a^2 + 2b^2$, då $z = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$,

(b) $\mathbb{Z}[\sqrt{2}]$ med funktionen $d(z) = |a^2 - 2b^2|$, då $z = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

14.4. Låt $d(z) = |z|^2$ for ett Gaussiskt heltal z. Visa att om $z_1|z_2$ så $d(z_1)|d(z_2)$ for två Gaussiska heltal z_2 och z_2.

14.5. Faktoruppdela följande element i produkt av irreducibla i ringen av de Gaussiska heltalen:

(a) $1 + 3i$,

(b) $21 - 12i$.

14.6. Visa att ett gaussiskt heltal $a + bi$ är irreducibelt då och endast då $d(a + bi) = a^2 + b^2$ är ett primtal eller $b = 0$ och a är ett primtal som lämnar resten 3 vid division med 4.

14.7. Visa att enhetsgruppen i ringen $\mathbb{Z}[\sqrt{-D}]$, där D är ett heltal större än 1, består av ± 1.

14.8. (a) Visa att kongruensen $x^2 \equiv -1 (\text{mod } p)$ saknar lösningar då p lämnar resten 3 vid division med 4.

Ledning. Se beviset av sats (14.17) där man visar att kongruensen ovan har en lösning då p lämnar resten 1 vid division med 4.

(b) Låt p vara ett primtal som lämnar resten 3 vid division med 4 och låt $p|a^2 + b^2$, där a och b är heltal. Visa att $p|a$ och $p|b$.

(c) Låt $z_1 = a^2 + b^2$ och $z_2 = c^2 + d^2$ vara summor av två heltaliga kvadrater. Visa att även $z_1 z_2$ är en summa av två heltaliga kvadrater.

Ledning. Representera z_1 och z_2 som beloppen av komplexa tal.

(d) Visa att ett naturligt tal n är en summa av två kvadrater då och endast då varje primfaktorer av n som lämnar resten 3 vid division med 4 förekommer ett jämnt antal gånger.

14.9. Låt R vara ett integritesområde och låt $a, b \in R$. Man säger att $d \in R$ är en största gemensamma delare till a och b om d dividerar a och b samt varje $d' \in R$ som dividerar både a och b är en delare till d.

(a) Låt R vara ett huvudidealområde. Visa att $(a, b) = (d)$, där $(a, b) = \{ra+sb, r, s \in R\}$ är idealet genererat av a och b.

(b) Låt p vara ett irreducibelt element i ett huvudidealområde R. Visa att om $p|ab$ så $p|a$ eller $p|b$.

Ledning. Antag att p inte är delare till a. Motivera att $(p, a) = R$ så att $1 = px + ay$. Multiplicera den likheten med b.

Anmärkning. Ett nollskilt element p i en godtycklig ring kallas **primt** om p inte är en enhet och $p|ab$ implicerar att $p|a$ eller $p|b$ då $a, b \in R$. (b) säger att irreducibla element i huvudidealområden är prima. Observera att p är primt då och endast då idealet (p) är ett primideal (se **??**).

14.10. Låt R vara ett huvudidealområde.

(a) Låt $r_1, r_2, r_3 \ldots$ vara en följd av element i R sådana att $r_2|r_1$, $r_3|r_2$, …, $r_{n+1}|r_n$,…. Visa att det finns ett index N så att alla element r_i med $i \geq N$ är associerade.

Ledning. Låt I vara mängden av alla multipler av r_i för $i = 1, 2, \ldots$ dvs $I = \bigcup_{i=1}^{\infty}(r_i)$, där (r_i) är idealet genererat av r_i. Motivera att I är ett ideal och således $I = (r)$. Observera att $r \in (r_N)$ för något N.

(b) Med hjälp av (a) visa att varje nollskilt element $r \in R$ som inre är en enhet har en irreducibel faktor.

(c) Med hjälp av (a) visa att varje nollskilt element $r \in R$ som inre är en enhet är en produkt av irreducibla faktorer.

(d) Med hjälp av (c) och övning 12.1 visa att R har entydig faktoruppdelning.

14.11. Låt R vara en Euklidisk ring med avseende på en funktion $d : R \setminus \{0\} \to \mathbb{N}$.

(a) Visa att a är en enhet då och endast då $d(a)$ antar sitt minsta värde.

(b) Visa att varje $a \in R \setminus \{0\}$ som inte är en enhet har en irreducibel faktor.

Ledning. Välj en faktor till a med minsta möjliga värdet av d större än $d(1)$.

(c) Visa att varje $a \in R \setminus \{0\}$ som inte är en enhet är en produkt av irreducibla faktorer.

Ledning. Använd induktion med avseende på $d(a)$.

Anmärkning. (c) ger en något enklare bevis för 14.10 (c). Genom att använda samma argument som i övning 14.10 (d) kan man visa att Euklidiska ringar har entydig faktoruppdelning.

Kapitel 15

KROPPSUTVIDGNINGAR

Låt K vara en kropp och $p_0(X) \in K[X]$. Polynomet $p_0(X)$ behöver inte ha något nollställe i K, men det visar sig att det alltid finns en kropp $L \supseteq K$ sådan att $p_0(X)$ har ett nollställe i L. Det är till och med möjligt att konstruera en kropp $L \supseteq K$ så att $p_0(X)$ är en produkt av förstagradsfaktorer med koefficienter i L. Vi visar i detta kapitel hur en sådan kropp L (en kroppsutvidgning av K) kan konstrueras då K och $p_0(X) \in K[X]$ är givna. Först definierar vi kvotringen $K[X]/(p_0(X))$ som kommer att ha en stor betydelse i detta och i efterföljande kapitel.

(15.1) Kvotringen $K[X]/(p_0(X))$. Låt $p_0(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ vara ett godtyckligt icke-konstant polynom med koefficienter i K. Låt $p(X) \in K[X]$. Vi skall beteckna med $[p(X)]_{p_0}$ resten vid division av $p(X)$ med $p_0(X)$. Observera att

$$[p(X)]_{p_0} = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$$

där $r_i \in K$, därför att polynomet p_0 har graden n. Vi vill definiera addition och multiplikation av resterna precis som vi gjorde det för addition och multiplikation av rester vid division med ett fixt heltal:

$$[p_1(X)]_{p_0} + [p_2(X)]_{p_0} = [p_1(X) + p_2(X)]_{p_0}$$

och

$$[p_1(X)]_{p_0}[p_2(X)]_{p_0} = [p_1(X)p_2(X)]_{p_0}.$$

Man kontrollerar utan svårigheter att resterna vid division med p_0 bildar en ring med avseende på dessa operationer. Man gör det på samma sätt som för addition och multiplikation av rester vid division med heltal i avsnittet om restgrupper.

Observera att addition av resterna sammanfaller med vanlig addition därför att summan av två rester är också en rest (har graden $< n$), medan produkten av två rester kan ha graden

$> n$. Då måste man räkna ut resten av denna produkt vid division med p_0. Vi ger exempel snart, men först låt oss notera att konstanta polynom adderas och multipliceras precis som elementen i K:

$$[a] + [b] = [a + b] \qquad \text{och} \qquad [a][b] = [ab].$$

då $a, b \in K$. För att undvika missförstånd, då vi arbetar med rester och ej polynom, låt oss beteckna $[X] = \alpha$. Vi kommer att utelämna p_0 i $[p(X)]_{p_0}$ då detta är klart från texten. I enlighet med våra additions och multiplikationsregler har vi då:

$$[r_0 + r_1X + \cdots + r_{n-1}X^{n-1}] = [r_0] + [r_1][X] + \cdots + [r_{n-1}][X] = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}.$$

Dessutom har man:

$$0 = [p_0(X)]_{p_0} = [a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0] = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0.$$

Låt oss sammanfatta våra observationer:

(15.2) Sats. *Låt $p_0(X) = a_0 + a_1X + \ldots + a_nX^n, a_n \neq 0$. Varje element i kvotringen $K[X]/(p_0(X))$ kan entydigt skrivas på formen $r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}$, där $r(X) = r_0 + r_1X + \ldots + r_{n-1}X^{n-1} \in K[X]$ och $\alpha = [X]$ uppfyller ekvationen $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Ringen $K[X]/(p_0(X))$ innehåller kroppen K och kommer att betecknas med $K[\alpha]$.*

(15.3) Anmärkning. Satsen kan också formuleras så att $K[\alpha]$ som ett vektorrum över K har en bas $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. □

(15.4) Exempel. (a) Låt $p_0(X) = 1 + X + X^2 \in \mathbb{Z}_2[X]$. $\mathbb{Z}_2[X]/(p_0)$ består av resterna $[a + bX]$, $a, b \in \mathbb{Z}_2$ dvs $[0], [1], [X], [1 + X]$. Låt $[X] = \alpha$. Då kan vi anteckna resterna som: $0, 1, \alpha, 1 + \alpha$. Vi har $[p_0(X)]_{p_0} = [1 + X + X^2]_{p_0} = 0$ så att $1 + \alpha + \alpha^2 = 0$ dvs $\alpha^2 = \alpha + 1$. Additions- och multiplikationstabellerna ser ut så här:

	0	1	α	$1+\alpha$
0	0	1	$1+\alpha$	α
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

(b) Låt $p_0(X) = X^2 + 1 \in \mathbb{R}[X]$. $\mathbb{R}[X]/(X^2 + 1)$ består av alla rester $r = a + bX$, $a, b \in \mathbb{R}$. Låt $[X]_{p_0} = \alpha$. Då är $[r] = [a + bX] = a + b\alpha$. Men $[X^2 + 1]_{p_0} = 0$ så att $\alpha^2 + 1 = 0$ dvs $\alpha^2 = -1$. Vi har alltså:

$$\begin{aligned} (a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha \\ (a + b\alpha)(c + d\alpha) &= (ac - bd) + (bc + ad)\alpha \end{aligned}$$

dvs resterna adderas och multipliceras som komplexa tal. Med andra ord är $\mathbb{R}[X]/(X^2+1)$ isomorf med $\mathbb{C}$. □

Nu vill vi veta när $K[X]/(p_0)$ är en kropp.

(15.5) Sats. *$K[X]/(p_0)$ är en kropp då och endast då p_0 är irreducibelt i $K[X]$.*

Bevis. "⇒" Låt p_0 vara irreducibelt och låt $r \in K[X]/(p_0)$, $r \neq 0$, $\operatorname{grad} r < \operatorname{grad} p_0$ och p_0 är irreducibelt. Alltså finns det två polynom $s, t \in K[X]$ så att

$$rs + p_0 t = 1$$

Nu är $[rs + p_0 t]_{p_0} = [r][s] + [p_0][t] = 1$ dvs $[r][s] = 1$ ty $[p_0] = 0$. Alltså är $[s]$ inversen till $[r]$. Detta visar att $K[X]/(p_0)$ är en kropp ty varje $[r] \neq 0$ har invers.

"⇐" Antag att p_0 är reducibelt. Då är $p_0 = r_1 r_2$, där $r_1, r_2 \in K[X] \operatorname{grad}\ r_1 < \operatorname{grad}\ p_0$ och $\operatorname{grad} r_2 < \operatorname{grad} p_0$. Alltså är $0 = [p_0]_{p_0} = [r_1][r_2]$, vilket betyder att ringen $K[X]/(p_0)$ har nolldelare ty $[r_1] \neq 0$ och $[r_2] \neq 0$. I så fall är $K[X]/(p_0)$ inte en kropp ty kroppar saknar nolldelare[†]. □

(15.6) Exempel. Både $\mathbb{Z}_2[X]/(X^2+X+1)$ (se (15.4)(a)) och $\mathbb{R}[X]/(X^2+1)$ (se (15.4)(b)) är kroppar. □

Nu kan vi visa att varje polynom med koefficienter i en kropp kan uppdelas i förstagradsfaktorer i en lämplig utvidgning av denna kropp. Vi gör det i två steg.

(15.7) Lemma. *Låt $p_0 \in K[X]$ vara ett irreducibelt polynom. Då existerar en kropp $L \supseteq K$ sådan att p_0 har ett nollställe i L.*

Bevis. Låt $L = K[X]/(p_0)$. Vi vet all L är en kropp som innehåller K. Låt $p_0(X) = a_0 + a_1 X + \ldots + a_n X^n$ och låt $[X]_{p_0} = \alpha$. Då är

$$0 = [p_0]_{p_0} = [a_0 + a_1 X + \ldots + a_n X^n] = a_0 + a_1[X] + \cdots + a_n[X]^n = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

så att $p_0(\alpha) = 0$. □

(15.8) Sats. *Låt $p \in K[X]$ och $\operatorname{grad} p \geq 1$. Då existerar en kropp $L \supseteq K$ sådan att p är en produkt av förstagradsfaktorer i $L[X]$ dvs $p(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ där $\alpha_i \in L$ och $n = \operatorname{grad} p$.*

[†]Om L är en kropp och $ab = 0$ för $a, b \in L$ med $a \neq 0$ så är $a^{-1}ab = b = 0$

Bevis. Vi visar satsen med hjälp av induktion. Om K är en godtycklig kropp och $\operatorname{grad} p = 1$ så är beviset klart. Antag att satsen gäller för alla kroppar och alla polynom av grad $< n$. Låt $\operatorname{grad} p = n$ och låt p_0 vara en irreducibel faktor av p. Enligt (15.7) finns en kropp $L_0 \supseteq K$ sådan att p_0, och följaktligen p, har ett nollställe $\alpha \in L_0$ dvs $p(X) = (X - \alpha)q(X)$, där $q(X) \in L_0[X]$. Då är $\operatorname{grad} q < \operatorname{grad} p$ så att det finns en kropp $L \supseteq L_0 \supseteq K$ sådan att $q(X)$ är en produkt av förstagradsfaktorer med koefficienter i L. Men då är även $p(X)$ en sådan produkt ty $p(X) = (X - \alpha)q(X)$. □

(15.9) Anmärkning. Satsen visades för första gången av L. Kronecker. Den räcker gott och väl för våra syften, men den är inte helt tillfrädsställande om man t ex tänker på de komplexa talen: **Varje** icke-konstant polynom med koefficienter i en delkropp K till $\mathbb{C}$ kan skrivas som produkt av förstagradspolynom med komplexa koefficienter. För varje kropp K finns en liknande utvidgning $\bar{K}$ sådan att varje polynom med koefficienter i K sönderfaller i produkt av förstagradsfaktorer med koefficienter i $\bar{K}$. Dessutom kan man hitta $\bar{K}$ så att ingen av dess äkta delkroppar som innehåller K har samma egenskap som $\bar{K}$. $\bar{K}$ kallas **algebraiska höljet** till K. $\bar{K}$ är till och med entydigt bestämd så att om $\bar{K}'$ är en annan kropp med samma egenskaper som $\bar{K}$ så är $\bar{K}'$ isomorf med $\bar{K}$ (man kan välja en isomorfism mellan dessa kroppar så att elementen i K avbildas på sig självt). □

Vi skall avsluta detta avsnitt med en enkel följdsats till satserna (15.2) och (15.5).

(15.10) Följdsats. *Om K är en ändlig kropp med q element och $p_0(X) \in K[X]$ är ett irreducibelt polynom av grad n så är kvotringen $L = K[X]/(p_0(X))$ en kropp med q^n element.*

Bevis. Enligt (15.2) kan varje element i L skrivas entydigt på formen $r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}$, där $r_i \in K$ (och $\alpha = [X]_{p_0}$). Eftersom varje r_i antar q olika värden är antalet element i L lika med q^n. Det följer ur (15.5) att L är en kropp. □

Exempel. För att konstruera en kropp med 4 element måste man välja ett irreducibelt polynom av grad 2 över $\mathbb{Z}_2$. Som vi vet är $X^2 + X + 1$ ett sådant polynom och således är $L = \mathbb{Z}_2[X]/(X^2 + X + 1)$ en kropp med 4 element (se (15.4) (a)). □

ÖVNINGAR

15.1. Skriv ut additions- och multiplikationstabellerna för följande ringar:

(a) $\mathbb{Z}_2[X]/(X^2)$, (b) $\mathbb{Z}_2[X]/(X^2 + X)$, (c) $\mathbb{Z}_3[X]/(X^2 + 1)$,

(d) $\mathbb{Z}_2[X]/(X^3 + X + 1)$, (e) $\mathbb{Z}_2[X]/(X^4 + X + 1)$.

15.2. Vilka av följande ringar är kroppar:

(a) $\mathbb{Z}_3[X]/(X^2 + 2)$, (b) $\mathbb{Z}_5[X]/(X^2 + 2)$.

15.3. Konstruera en kropp med

(a) 8, (b) 1024, (c) 25, (d) 3125

element.

15.4. Motivera att kvotringen $\mathbb{Z}_2[X]/(X^3+X+1)$ är en kropp och för varje nollskilt element i denna kropp bestäm dess invers.

15.5. Motivera att kvotringen $\mathbb{Z}_2[X]/(X^5+X^2+1) = \mathbb{Z}_2[\alpha]$, där $\alpha = [X]$ är en kropp och bestäm i denna kropp ett element vars potenser genererar den multiplikativa gruppen.

15.6. Bestäm alla lösningar till ekvationen $p_0(X) = 0$ i K då

(a) $p_0(X) = X^2+X+1, \quad K = \mathbb{Z}_2[X]/(X^2+X+1) = \mathbb{Z}_2[\alpha]$, där $\alpha = [X]$,

(b) $p_0(X) = X^3+X+1, \quad K = \mathbb{Z}_2[X]/(X^3+X^2+1) = \mathbb{Z}_2[\alpha]$, där $\alpha = [X]$.

15.7. Låt $p_0(X) \in K[X]$ vara ett polynom av grad n. Motivera att om kroppen K har q element så har $K[X]/(p_0(X))$ q^n element.

Kapitel 16

ÄNDLIGA KROPPAR

Ändliga kroppar är grunden för många mycket viktiga tillämpningar. Vi har redan sett exempel på sådana kroppar: $\mathbb{Z}_p$ där p är ett primtal och $\mathbb{Z}_p[X]/(p_0)$ där p_0 är ett irreducibelt polynom. Här visar vi att dessa exempel omfattar alla ändliga kropar. Följande sats sammanfattar de viktigaste egenskaperna hos de ändliga kropparna:

(16.1) Sats. (a) *Antalet element i en ändlig kropp är en primtalspotens.*

(b) *Om $q = p^n$, p ett primtal, så existerar en kropp med q element.*

(c) *Två ändliga kroppar med lika många element är isomorfa.*

(16.2) Anmärkning. Ändliga kroppar definierades av E. Galois (1811-1832). Till hans ära betecknas ofta en ändlig kropp med $q = p^n$ element med $GF(q)$ och kallas Galoiskropp. Vi skall använda en lite mera kompakt beteckning $\mathbb{F}_q$ (observera att från och med nu skriver vi ofta $\mathbb{F}_p$ i stället för $\mathbb{Z}_p$). □

Innan vi bevisar (16.1) visar vi ett mycket allmänt och intressant resultat.

(16.3) Sats. *K vara en kropp och G en ändlig delgrupp till K^* (den multiplikativa gruppen av K). Då är G cyklisk.*

Bevis. Låt $o(G) = n$. Vi vet att exponenten m av G (dvs det minsta positiva heltalet sådant att $g^m = e$ för varje $g \in G$) är lika med maximalordningen av gruppens element (se övn. 7.8). Alla element i G uppfyller ekvationen $X^m - 1 = 0$ som har högst m lösningar i kroppen K. Alltså är $n \leq m$. Men $m \leq n$ ty $g^n = 1$ för varje $g \in G$ (se (7.12). Alltså är $m = n$ dvs det finns $g \in G$ vars ordning är n. Detta visar att $G =< g >$ är cyklisk. □

(16.4) Bevis av (16.1) (a) Låt K vara en ändlig kropp. Alla heltaliga multipler av 1 bildar en delring till K isomorf med $\mathbb{Z}_p$ för ett primtal p ty karakteristiken av K är ett primtal (se rref (14.13)). Vi identifierar den delringen med $\mathbb{Z}_p$ och skriver $\mathbb{Z}_p \subseteq K$. Låt α vara en

generator av den cykliska gruppen K^* är en potens av α (se (16.3)). Men varje element i $\mathbb{Z}_p[\alpha]$ kan skrivas entydigt på formen $r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}$, där $r_i \in \mathbb{Z}_p$ och n är graden av minimalpolynomet för α över $\mathbb{Z}_p$ (se rref (19.5) (a)). Antalet element av den typen är just p^n.

(b) Betrakta en kroppsutvidgning $L \supseteq \mathbb{Z}_p$ sådan att polynomet $p_0(X) = X^q - X$ är en produkt av förstagradsfaktorer i L dvs

$$p_0(X) = (X - \alpha_1)\ldots(X - \alpha_g),$$

där $q = p^n$ och $\alpha_i \in L$. Alla α_i är olika ty $p_0(X)$ och dess derivata $p_0'(X) = qX^{q-1} = -1$ (observera att $q = 0$ i $\mathbb{Z}_p$!) saknar gemensamma nollställen i L (se (15.13)). Låt $K = \{\alpha_1, \ldots, \alpha_q\}$. Vi påstår att K är en kropp (med $q = p^n$ element). Vi har

$$(\alpha_i + \alpha_j)^q = \alpha_i^q + \alpha_j^q = \alpha_i + \alpha_j$$

(se övn. 14.13) och

$$(\alpha_i\alpha_j)^q = \alpha_i^q\alpha_j^q = \alpha_i\alpha_j$$

dvs $\alpha_i, \alpha_j \in K$ ger att $\alpha_i + \alpha_j, \alpha_i\alpha_j \in K$. Om $\alpha \in K$ och $\alpha \neq 0$ så ger $\alpha^q = \alpha$ att

$$(\frac{1}{\alpha})^q = \frac{1}{\alpha^q} = \frac{1}{\alpha}$$

dvs $1/\alpha \in K$. Detta visar att K är en delkropp till L.

(c) Låt K vara en kropp med $q = p^n$ element. Då är $o(K^*) = q - 1$ så att $X^{q-1} = 1$ för varje $x \in K^*$. Alltså gäller likheten $X^q = X$ för alla $x \in K$ (även $x = 0$). Detta visar att elementen i K är exakt alla lösningar till ekvationen $X^q - X = 0$. Låt K och K' vara två kroppar med q element. Låt α vara en generator av den cykliska gruppen K^* (se (16.3)). Låt m_α vara minimalpolynomet för α över $\mathbb{Z}_p$ (se punkt a) i beviset). Då är $m_\alpha | p_0(X) = X^q - X$ ty $p_0(\alpha) = 0$ (se (19.3) a)). Låt $\alpha' \in K'$ vara ett nollställe till m_α i K' (elementen i K' är precis alla lösningar till ekvationen $X^9 - X = 0$). Men $K = \mathbb{Z}_p[\alpha]$ (se a) ovan) och $\mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[\alpha']$ ty bägge ringarna är isomorfa med $\mathbb{Z}_p[X]/(m_\alpha)$, där m_α är minimalpolynomet för α (se (19.7)). Alltså innehåller $\mathbb{Z}_p[\alpha']$ lika många element som $\mathbb{Z}_p[\alpha] = K$ dvs q så att $\mathbb{Z}_p[\alpha'] = K'$ (ty K' har också q element). Detta visar att K och K' är isomorfa.

Vi skall avsluta detta Kapitel med en karakterisering av en mycket viktig klass av irreducibla polynom över ändliga kroppar.

(16.5) Definition. Låt $p(X) \in \mathbb{F}_q[X]$ vara ett irreducibelt polynom av grad n. Med **exponenten** av $p(X)$ menar man minsta heltalet $e > 0$ sådant att $p(X) | X^e - 1$. Om $e = q^n - 1$ kallas $p(X)$ **primitivt**. □

(16.6) Sats. *Låt $p(X) \in \mathbb{F}_q[X]$ vara ett irreducibelt polynom av grad n och låt $K = \mathbb{F}_q[\alpha]$ är $p(\alpha) = 0$.*

(a) *Exponenten e av $p(X)$ är en delare till $q^n - 1 = o(K^*)$.*

(b) *e är lika med ordningen av α i gruppen K^* (så att $p(X)$ är primitivt precis då α genererar K^*).*

Bevis. Låt oss påminna om att K har q^n element (se (19.5) (a)). Låt m vara ordningen av α i K^*. Vi har $\alpha^m = 1$ dvs $\alpha^m - 1 = 0$ så att $p(X)|X^m - 1$ ty $p(X)$ är minimalpolynomet för α över $\mathbb{F}_q$ (se (19.3) a) b)). Alltså har $p(X)$ en exponent e och $e \leq m$. Men om $p(X)|X^e - 1$ så är $\alpha^e - 1 = 0$ dvs $\alpha^e = 1$ så att $m \leq e$ och till och med $m|e$ (ty e är ordningen av α i K^*). Detta betyder att $e = m$ och att $e|o(K^*) = q^n - 1$ (ordningen av ett element $e\alpha \in K^*$ är en delare till gruppens K^* ordning). □

(16.7) Exempel. (a) Vi skall visa att $p(X) = X^4 + X + 1$ är ett primitivt polynom över $\mathbb{F}_2$. Låt $K = \mathbb{F}_2[\alpha]$ där $\alpha^4 + \alpha + 1 = 0$. Då är $\alpha^4 = \alpha + 1$. K har 16 element så att $|K^*| = 15$. Detta betyder att $o(\alpha) = 3, 5$ eller 15. Det är klart att $o(\alpha) \neq 3$. Vi har $\alpha^5 = \alpha^2 + \alpha \neq 1$ så att $o(\alpha) \neq 5$. Alltså är $o(\alpha) = 15$ dvs $e = 15$ för $p(X)$. Detta visar att $p(X)$ är primitivt.

(b) Alla irreducibla polynom av grad 5 över $\mathbb{F}_2$ är primitiva. Om $p(X)$ är ett sådant polynom så är $K = \mathbb{F}_2[X]/(p(X))$ en kropp med $2^5 = 32$ element. Alltså är $o(K^*) = 31$ så att $e|31$. Detta ger $e = 31$ dvs $p(X)$ är primitivt. □

(16.8) Anmärkning. De viktigaste tillämpningarna av ändliga kroppar är ofta relaterade till primitiva polynom. Därför finns det omfattande tabeller av irreducibla polynom över $\mathbb{F}_2$ och deras exponenter. □

ÖVNINGAR

16.1. Bestäm exponenten för följande polynom över $\mathbb{F}_2$:

(a) $X^2 + X + 1$, (c) $X^4 + X^3 + X^2 + X + 1$,
(b) $X^3 + X + 1$, (d) $X^5 + X^2 + 1$.

(visa att polynomen är irreducibla).

16.2. Visa att en kropp med p^n element innehåller en kropp med p^m element då och endast då $m|n$.

16.3. Låt $p(X) \in \mathbb{F}_p(X]$ vara ett irreducibel polynom. Visa att $p(X)|X^{p^n} - X$ då och endast då $\operatorname{grad} p(X)|n$.

16.4. Visa att antalet primitiva polynom av grad n över $\mathbb{F}_p$ är lika med $\frac{1}{n}\varphi(p^n - 1)$ där φ är Eulers funktion.

16.5. Låt $p(X) \in \mathbb{F}_p[X]$ vara ett irreducibelt polynom av grad n och låt $p(\alpha) = 0$ där $\alpha \in K \supset \mathbb{F}_p$. Visa att $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$ är alla nollställen till $p(X)$ i kroppen K.

16.6. Visa att för varje n finns det ett irreducibelt polynom av grad n över $\mathbb{F}_p$ (Sats (16.1) får användas i beviset).

Kapitel 17

MODULER OCH LINJÄRA RUM

Vanliga vektorer i planet eller i rymden är sekvenser av (två eller tre) reella tal. Datasignaler kan ofta uppfattas som sekvenser av de binära symbolerna 0 och 1. Polynom kan beskrivas som sekvenser av deras koefficienter. Ofta är man intresserad av sekvenser som uppfyller vissa ekvationer (t.ex. en linje i planet består av alla talpar som uppfyller en lämplig ekvation). Det matematiska objekt som lämpar sig bäst för hanteringen av olika sekvenser bestående av element i en ring är moduler över den ringen. Om ringen är en kropp kallar man dessa objekt för vektorrum eller linjära rum.

Vi skall enbart betrakta kommutativa ringar med etta.

(17.1) Definition. Låt R vara en ring. Med en **modul över** R (eller en R**-modul**) menar man en abelsk grupp $(M, +)$ sådan att till varje $r \in R$ och $m \in M$ finns et element $rm \in M$ varvid följande villkor är uppfyllda:

(a) $r(m_1 + m_2) = rm_1 + rm_2$,

(b) $(r_1 + r_2)m = r_1m + r_2m$,

(c) $(r_1r_2)m = r_1(r_2m)$,

(d) $1m = m$,

där $r, r_1, r_2 \in R$ och $m, m_1, m_2 \in M$.

Om R är en kropp kallas M ett **vektorrum** eller ett **linjärt rum** över R. □

(17.2) Exempel. (a) Låt $M = V$ vara mängden av alla vektorer (a, b) i planet (dvs $a, b \in \mathbb{R}$) med vanlig addition av vektorer. Om man definierar $r(a, b) = (ra, rb)$ får man en modul (dvs ett vektorrum) över de reella talen. På liknande sätt bildar alla vektorer (a, b, c) i rymden ett vektorrum över de reella talen $\mathbb{R}$.

(b) Låt $R' \supseteq R$ vara två ringar. Då är $M = R'$ en R-modul med addition i R' och multiplikation $rr' \in R'$ för $r \in R$ och $r' \in R'$.

(c) Låt R vara en ring och låt $M = R^n = \{(a_1, a_2, \ldots, a_n),\ a_i \in R\}$ med koordinatvis addition. $M = R^n$ är en R-modul om man definierar:

$$r(a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n).$$

(Kontrollera villkoren (a) – (d) i definitionen rref). T.ex. bildar alla binära sekvenser $(a_1, a_2, \ldots, a_n)$ där $a_i = 0$ eller 1 ett vektorrum över $\mathbb{F}_2$.

(d) Låt $M = I$ vara ett ideal i en ring R. Då är I en R-modul då ri för $r \in R$ och $i \in I$ är produkten i ringen R (vi vet att $ri \in I$ enligt definitionen av I). □

(17.3) Definition. Låt M och N vara R-moduler. Man säger att en funktion $\theta : M \to N$ är en R-**homomorfism** om

$$\begin{aligned} \theta(m_1 + m_2) &= \theta(m_1) + \theta(m_2), \\ \theta(rm) &= r\theta(m), \end{aligned}$$

där $r \in R$, $m, m_1, m_2 \in M$. Om R är en kropp kallas θ en **linjär avbildning**. θ kallas **isomorfism** om den är bijektiv. □

(17.4) Exempel. Låt $A = [a_{ij}]$ vara en $(m \times n)$-matris och låt

$$\theta : \mathbb{R}^n \to \mathbb{R}^m, \quad \text{där} \quad \theta(\bar{x}) = A\bar{x} \quad \text{för} \quad \bar{x} \in \mathbb{R}^n$$

dvs

$$\theta\Big(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\Big) = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

θ är en linjär avbildning av $\mathbb{R}^n$ i $\mathbb{R}^m$. På liknande sätt får man exempel på R-homomorfismer $\theta : R^n \to R^m$ då man ersätter $\mathbb{R}$ med en godtycklig ring R. Vi skall betrakta detta exempel i två specialfall. □

(17.5) Exempel. Hillkryptot.[†] Låt $R = \mathbb{Z}_n$ och låt H vara en $(N \times N)$-matris vars element tillhör $\mathbb{Z}_n$ och sådan att determinanten[†] $\det H \in \mathbb{Z}_n^*$. En sådan matris har invers H^{-1} (den kan man beräkna på precis samma sätt som inversen till en reell matris). Låt

$$E : \mathbb{Z}_n^N \to \mathbb{Z}_n^N,$$

där $E(\bar{x}) = H\bar{x}$ för $\bar{x} = (x_1, \ldots, x_N)^t \in \mathbb{Z}_n^N$. E är en isomorfism (dvs en automorfism av $\mathbb{Z}_n^N$) därför att E har inversen

$$D : \mathbb{Z}_n^N \to \mathbb{Z}_n^N$$

[†]L.S. Hill publicerade sina arbeten om detta krypto 1929-1931.

[†]Begreppet determinant definieras för en matris $[a_{ij}]$ med a_{ij} tillhörande en godtycklig (kommutativ) ring på precis samma sätt som för $a_{ij} \in \mathbb{R}$.

där $D(\bar{x}) = H^{-1}\bar{x}$ (dvs $(E \circ D)(\bar{x}) = E(D(\bar{x})) = E(h^{-1}\bar{x}) = HH^{-1}\bar{x} = \bar{x}$ och $(D \circ E)(\bar{x}) = D(E(\bar{x})) = D(H\bar{x}) = H^{-1}H\bar{x} = \bar{x}$ så att $E \circ D = I$ och $D \circ E = I$). Mera konkret låt $n = 26$ och

$$E : \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2,$$

där

$$E(\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]) = \begin{bmatrix} 2 & 1 \\ 23 & 24 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = H\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right].$$

Genom att översätta $A \mapsto 0$, $b \mapsto 1, \ldots, Z \mapsto 25$ kan man kryptera par av bokstäver

$$E(\text{“}PI'') = E(\left[\begin{smallmatrix} 15 \\ 8 \end{smallmatrix}\right]) = \begin{bmatrix} 2 & 1 \\ 23 & 24 \end{bmatrix} \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 12 \\ 17 \end{bmatrix} = \text{“}MR''.$$

Dekrypteringen sKer med hjälp av $H^{-1} = H$ (kontrollera genom att räkna $HH = E$). T.ex.:

$$D(\text{“}MR'') = D(\left[\begin{smallmatrix} 12 \\ 17 \end{smallmatrix}\right]) = \begin{bmatrix} 2 & 1 \\ 23 & 24 \end{bmatrix} \begin{bmatrix} 12 \\ 17 \end{bmatrix} = \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \text{“}PI''.$$

Ofta väljer man H så att $H^{-1} = H$ dvs $HH = E$. Då kan H användas som både krypterings- och dekrypteringsnyckel. En matris H sådan att $H^2 = E$ kallas **involutiv** (eller involutionsmatris). När $n = 26$ och $N = 2$ finns 736 sådana matriser, men för $N = 3$ är antalet matriser av den typen 1 360 832. Det finns många olika varianter av Hillkryptot precis som för Caesarkryptot (se övning rref)

□

(17.6) Exempel. Herkle-Hellmans kappsäckskrypto[†]**.** Låt $a_1, a_2, \ldots, a_n \in \mathbb{Z}_m$ och $w \in \mathbb{Z}_m^*$. Definiera

$$E : \mathbb{Z}_m^n \to \mathbb{Z}_m$$

så att

$$E_w(\bar{x}) = x_1wa_1 + x_2wa_2 + \ldots + x_nwa_n = w(\bar{x} \cdot \bar{a})$$

där för $\bar{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$ och $\bar{a} = (a_1, a_2, \ldots, a_n)$ är $\bar{x} \cdot \bar{a}$ den skalära produkten av $\bar{x}$ och $\bar{a}$. Då är E_w en $\mathbb{Z}_m$-homomorfism ty

$$\begin{aligned} E_w(\bar{x} + \bar{y}) &= w((\bar{x} + \bar{y}) \cdot \bar{a}) = w(\bar{x} \cdot \bar{a}) + w(\bar{y} \cdot \bar{a}) = E_w(\bar{x}) + E_w(\bar{y}), \\ E_w(r\bar{x}) &= w(r\bar{x} \cdot \bar{a}) = rw(\bar{x} \cdot \bar{a}) = rE_w(\bar{x}) \end{aligned}$$

där $\bar{x}, \bar{y} \in \mathbb{Z}_m^n$ och $r \in \mathbb{Z}_m$. Funktionen E_w är nästan aldrig injektiv men om man lämpligt väljer $\bar{a} = (a_1, a_2, \ldots, a_n)$ som s.k. ordnad kappsäck så är den injektiv för vektoer $\bar{x} = (x_1, x_2, \ldots, x_n)$ sådana att $x_i = 0$ eller 1. Ett sådanat val är t.e.x $a_i = 2^{i-1}$, $i = 1, \ldots, n$ och $m > 2^n$. Med ett hemligt val av $w \in \mathbb{Z}_m^*$ får man då ett Merkle-Hellmans kappsäckskrypto ($\bar{a} = (a_1, a_2, \ldots, a_n)$ är en ordnad kappsäck och $w\bar{a} = (wa_1, wa_2, \ldots, wa_n)$ är oordnad). Se övning rref . □

(17.7) Definition. Låt M vara en R-modul. Om $(M', +)$ är en delgrupp till $(M, +)$ och $rm' \in M'$ då $r \in R$ och $m' \in M'$ så säger man at M' är en **delmodul** till M. Om R är en kropp så kallas M' ett **delrum** till M. □

[†]R.C. Merkle, M.E. Hellman publicerade sina arbeten om detta krypto 1979-1982.

(17.8) Exempel. (a) Låt $M = \mathbb{R}^3 = \{(x_1, x_2, x_3) : x_i \in \mathbb{R}\}$ och låt $W = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$. Då är W ett delrum till $\mathbb{R}^3$. Motiveringen av detta påstående är ett specialfall av vårt nästa exempel.

(b) Låt $M = \mathbb{R}^n$ och låt $W = \{\bar{x} \in \mathbb{R}^n : A\bar{x} = 0\}$ där A är en $(m \times n)$-reell matris. Detta betyder att $\bar{x}^t = (x_1, x_2, \ldots, x_n) \in W$ då och endast då

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ - - - - - - - - - - - \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases}$$

där $A = [a_{ij}]$. W är ett delrum till $\mathbb{R}^n$ ty $\bar{x}_1, \bar{x}_2 \in W$ ger $\bar{x}_1 - \bar{x}_2 \in W(A)\bar{x}_1 - A\bar{x}_2 = \bar{0}$ om $A\bar{x}_1 = A\bar{x}_2 = \bar{0}$) och $r \in \mathbb{R}, \bar{x} \in W$ ger $r\bar{x} \in W(A(r\bar{x}) = rA\bar{x} = \bar{0}$ om $A\bar{x} = \bar{0})$. □

(17.9) Definition. Man säger att $e_1, e_2, \ldots, e_n \in M$ **genererar** R-modulen M om varje $m \in M$ kan skrivas på formen:

$$m = r_1e_1 + r_2e_2 + \ldots + r_ne_n,$$

där $r_i \in R$. $e_1, e_2, \ldots, e_n$ är en **bas för** M över R om en sådan framställning är entydig. Man säger att m är en **linjär kombination** av $e_1, e_2, \ldots, e_n$. □

(17.10) Exempel. (a) Låt $M = R^n = \{(r_1, r_2, \ldots, r_n) : r_i \in R\}$. Då bildar vektorerna:

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0) \\ e_2 &= (0, 1, \ldots, 0) \\ &- - - - - - - \\ e_n &= (0, 0, \ldots, 1) \end{aligned}$$

en bas för R^n över R ty

$$m = (r_1, r_2, \ldots, r_n) = r_1(1, 0, \ldots, 0) + r_2(0, 1, \ldots, 0) + \ldots + r_n(0, 0, \ldots, 1) = r_1e_1 + r_2e_2 + \ldots + r_ne_n$$

och en sådan representation är entydig (om $r_1'e_1 + r_2'e_2 + \ldots + r_n'e_n = r_1e_1 + r_2e_2 + \ldots + r_ne_n$ så är $(r_1', r_2', \ldots, r_n') = (r_1, r_2, \ldots, r_n)$ dvs $r_1 = r_1', r_2 = r_2', \ldots, r_n = r_n'$).

(b) Talen $e_1 = 1, e_2 = i$ bildar en bas för de komplexa talen $\mathbb{C}$ över $\mathbb{R}$ ty varje komplext tal kan entydigt skrivas på formen $z = ae_1 + be_2 = a + bi$. □

(17.11) Anmärkning. Om $e_1, e_2, \ldots, e_n$ generar V så bildar dessa vektorer en bas för V över K om $0 \in V$ har entydig framställning som linjär kombination av $e_1, e_2, \ldots, e_n$ ty $r_1e_1 + r_2e_2 + \ldots + r_ne_n = r_1'e_1 + r_2'e_2 + \ldots + r_n'e_n$ ger $(r_1 - r_1')e_1 + (r_2 - r_2')e_2 + \ldots + (r_n - r_n')e_n = 0$ så att $r_1 - r_1' = 0, r_2 - r_2' = 0, \ldots, r_n - r_n' = 0$ i fall 0 har entydig framställning. □

Nu antar vi att $R = K$ är en kropp. I den situationen gäller följande sats:

(17.12) Sats. *Låt V vara ett vektorrum över K som kan genereras av ett ändligt antal vektorer. Då har V en bas över K och alla baser för V över K har lika många element.*

Bevis av den satsen är exakt samma som i Linjär Algebra (dvs då $K = \mathbb{R}$).

(17.13) Definition. Om v har en bas över K så kallas antalet element i den **dimensionen** av V över K. Den betecknas med $\dim_K V$. □

(17.14) Exempel. Låt $V = K^n = \{a_1, a_2, \ldots, a_n) : a_i \in K\}$. Då är $e_1, e_2, \ldots, e_n$ en bas för K^n enligt rref (18.10) (a). Alltså är $\dim_K V = n$. □

(17.15) Exempel. Man säger att $e_1, e_2, \ldots, e_m \in V$ är **linjärt oberoende** om $r_1e_1 + r_2e_2 + \ldots + r_me_m = 0$ är uppfyllt endast då $r_1 = r_2 = \ldots = r_m = 0$. Om man kan uppfylla likheten med minst en koefficient $r_i \neq 0$ så kallas $e_1, e_2, \ldots, e_m$ **linjärt beroende**. □

(17.16) Sats. *Om* $\dim_K V = n$ *så är varje uppsättning av* $n+1$ *vektorer i* V *linärt beroende.*

Satsen visas på samma sätt som i kurser i Linjär algebra för $K = \mathbb{R}$.

(17.17) Sambandet mellan linjära avbildningar och matriser. Låt

$$\theta : V \to W$$

vara en linär avbildning där V, W är två vektorrum över K. Låt $e_1, e_2, \ldots, e_n$ vara en bas för V och $f_1, f_2, \ldots, f_m$ en bas för W.

Låt

$$\begin{array}{l} \theta(e_1) = a_{11}f_1 + a_{21}f_2 + \ldots + a_{m1}f_m \\ \theta(e_2) = a_{12}f_1 + a_{22}f_2 + \ldots + a_{m2}f_m \\ - - - - - - - - - - - - - - - - - - \\ \theta(e_n) = a_{1n}f_1 + a_{2n}f_2 + \ldots + a_{mn}f_m \end{array}$$

Matrisen

$$M_\theta = \begin{array}{c} \left[\begin{array}{cccc} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{array}\right] \\ \begin{array}{cccc} \uparrow & \uparrow & & \uparrow \\ \theta(e_1) & \theta(e_2) & & \theta(e_n) \end{array} \end{array}$$

kallas matrisen för θ med avseende på baserna $e_1, e_2, \ldots, e_n$ för V och $f_1, f_2, \ldots, f_m$ för W. M_θ innehåller en fullständig information om θ därför att bilden av en godtycklig vektor $x = x_1e_1 + x_2e_2 + \ldots + x_ne_n \in V$ kan beräknas på följande sätt:

$$\begin{aligned} \theta(x) &= \theta(x_1e_1 + x_2e_2 + \ldots + x_ne_n) = x_1\theta(e_1) + x_2\theta(e_2) + \ldots + x_n\theta(e_n) = \\ &= x_1(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)f_1 + (a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n)f_2 \\ &\quad + \ldots + (a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n)f_m = \\ &= y_1f_1 + y_2f_2 + \ldots + y_mf_m. \end{aligned}$$

I matrisform är

$$\bar{y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = A\bar{x}$$

där $A = M_\theta$. Omvänt, om vi har en $(m \times n)$-matris A med element $a_{ij} \in K$ så kan vi definiera en linjär avbildning $\theta : V \to W$ med hjälp av $A : \theta(e_i) = a_{1i}f_1 + a_{2i}f_2 + \ldots + a_{mi}f_m$ och $\theta(x)$ definieras som i rref . Detta visar att om vi har valt en bas i V och en bas i W får vi på detta sätt en bijektiv motsvarighet mellan linjära avbildningar $\theta : V \to W$ och $(m \times n)$-matriser med element ur $K(\theta \mapsto A \mapsto \theta$ och $A \mapsto \theta \mapsto A)$.

ÖVNINGAR

17.1. Bestäm en bas för vektorrummet V då

(a) $V = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\}$,

(b) $V = \{(x, y, z) \in \mathbb{R}^3 : x + 2y - z = 0 \quad \text{och} \quad x - y = 0\}$,

(c) $V = \{(x, y, z, t) \in \mathbb{R}^4 : x + y + z + t = x - y - z = 0\}$.

17.2. Låt N vara en delmodul till en R-modul M. Låt M/N vara kvotgruppen av M modulo N. Visa att M/N är en R-modul om man definierar $r(N + m) = N + rm$.

17.3. Låt $\theta : M \to N$ vara en R-homomorfism av R-moduler M, N.

(a) Visa att $\operatorname{Ker}\theta = \{m \in M : \theta(m) = 0\}$ är en delmodul till M.

(b) Visa att $\bar{\theta} : M/\operatorname{Ker}\theta \to \theta(M)$ där $\bar{\theta}(\operatorname{Ker}\theta + m) = \theta(m)$ är en isomorfism.

17.4. Låt M, N vara R-moduler. Visa att $M \oplus N = \{(m, n) : m \in M,\ n \in N\}$ är en R-modul då man definierar $r(m, n) = (rm, rn)$.

17.5. Visa att avbildningen $\theta : V \to V$ är linjär och skriv upp dess matris i den givna basen:

(a) $V =$ alla polynom av grad ≤ 3 över $\mathbb{R}$, $\theta(p) = p'$, basen: $1, X, X^2, X^3$.

(b) $V = \mathbb{C}$, $\theta(z) = iz$, basen: 1,i.

(c) $V = M_2(\mathbb{R})$, $\theta(A) = A\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$, basen: $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

17.6. Låt R vara en ring (kommutativ med etta) och låt $M = M_2(R)$ vara gruppen av alla 2×2-matriser över R med matrisaddition. Visa att M är en R-modul om $r\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} ra & rb \\ rc & rd \end{smallmatrix}\right]$ då $r \in R$ och $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in M_2(R)$.

17.7. Låt $H = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 5 \end{smallmatrix}\right]$ och låt $E : M_2(\mathbb{Z}_{28}) \to M_2(\mathbb{Z}_{28})$ (se 18.6 ovan) där $E(X) = HX$.

(a) Visa att E är en $\mathbb{Z}_{28}$-homomorfism.

(b) Man definierar ett Hillkrypto (en version av (18.5)) så att $X = \left[\begin{smallmatrix} a & b \\ c & c \end{smallmatrix}\right]$ svarar mot 4 bokstäver “abcd” i en klartext ($A = 0, B = 1, \ldots Z = 25, 26$ betyder mellanrum och

27 punkt.) Kryptera "TEXT" och konstruera dekrypteringsfunktionen $D : M_2(\mathbb{Z}_{28}) \to M_2(\mathbb{Z}_{28})$ (dvs inversen till E).

(c) Hillkryptot (som i (18.5) används med variabel vektor $\bar{a}$ så att $E : \mathbb{Z}_n^N \to \mathbb{Z}_n^N$, $E(\bar{x}) = H\bar{x} + \bar{a}$ varvid $\bar{a}$ kan väljas olika för olika klartexter av längden E. En sådan funktion E är inte linjär (dvs E är inte en homomorfism) om $\bar{a} \neq \bar{0}$. Bestäm inversen till E då H uppfyller det vanliga villkoret att H^{-1} existerar ($E^{-1} = D$ är dekrypteringsfunktionen). $\bar{a}$ väljs ofta så att $\bar{a}_1$ är givet och $\bar{a}_{m+1} = B\bar{a}_m$ där B är en given $(N \times N)$-matris ur $M_N(\mathbb{Z}_g)$. Klartexten är då uppdelat i ett antal vektorer av längden $N : \bar{x}_1\bar{x}_2 \ldots, \bar{x}_i \in \mathbb{Z}_n^N$.

17.8. Låt $\bar{a} = (4, 10, 64, 101, 200, 400, 800, 1980, 4000, 9000)$ vara en ordnad kappsäck och låt $E_{200} : \mathbb{Z}_{19999}^{10} \to \mathbb{Z}_{19999}$ ges av $E_{200}(\bar{x}) = 200(\bar{x} \cdot \bar{a})$. Låt vidare

A	B	C	D	E	F	G	H	i	
00001	00010	00011	00100	00101	00110	00111	01000	01001	
J	K	L	M	N	O	P	Q	R	
01010	01011	01100	01101	01110	01111	10000	10001	10010	
S	T	U	V	W	X	Y	Z	·	m-rwn
10011	10100	10101	10110	10111	11000	11001	11010	11011	00000

Krypteringen sker så att t.ex.

$$E(''BQ'') = E(0, 0, 0, 1, 0, 1, 0, 0, 0, 1) = 200(\bar{a} \cdot \bar{x}) = 295.$$

$$\bar{z} \cdot \bar{x} = 101 + 400 + 9000 = 0501 \quad \text{och } 200 \cdot 9501 = 295 \text{ i } \mathbb{Z}_{19999}$$

Dekrypteringen baseras på det faktum att E_{200} är injektiv på mängden av alla vektorer $\bar{x} = (x_1, \ldots, x_{10})$ där $x_i = 0$ eller 1.

(a) Kontrollera att $\bar{a}$ är en ordnad kappsäck.

(b) Beräkna $200\bar{a}$ (det blir en oordnad kappsäck).

(c) Dekryptera 17070 (svar: SN) genom att beräkna $w^{-1} = 200^{-1}$ i $\mathbb{Z}_{19999}(200\bar{a} \cdot \bar{x} = 17070 \Rightarrow \bar{a} \cdot \bar{x} = 200^{-1} \cdot 17070$. Därefter fungerar metoden från sidan 9:9 ty $\bar{a}$ är en ordnad kappsäck).

Anmärkning. I 1982 visade A. Shamir att säKer heten av Merkle-Hellman kryptot är mycket dålig (det fanns en misstanke om detta redan 1976 då krypteringssystemet introducerades).

17.9. Låt V_1 och V_2 vara två delrum till ett linjärt rum V. Visa att $\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2)$ där $V_1 + V_2 = \{v_1 + v_2 : v_i \in V_i\}$. Motivera att $V_1 + V_2$ är ett delrum till V.

17.10. Låt $\theta : V \to W$ vara en linjär avbildning och låt $\operatorname{Ker}\theta$ vara dess kärna (se övn. 18.3). Visa att

$$\dim V = \dim \operatorname{Ker}\theta + \dim \theta(V)$$

Ledning. Låt $e_1, \ldots, e_k$ vara en bas för $\operatorname{Ker}\theta$ och låt $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$ vara en bas för V. Visa att $\theta(e_{k+1}), \ldots, \theta(e_n)$ är en bas för $\theta(V)$.

Kapitel 18

ALGEBRAISKA OCH TRANSCENDENTA ELEMENT

Det finns en mycket viktig uppdelning av komplexa tal i algebraiska och transcendenta. Algebraiska tal är nollställen till nollskilda polynom med rationella koefficienter. Transcendeta är de tal som inte har den egenskapen. Bland de transcendenta talen finns bl a π och e. Vi skall diskutera en liknande uppdelning för godtyckliga kroppar.

(18.1) Definition. Låt $\alpha \in L \supseteq K$. Man säger att α är ett **algebraiskt element** över K om α är ett nollställe till ett polynom $p \in K[X]$ som inte är nollpolynomet. Med ett **minimalpolynom** för α över K menar man ett sådant polynom av minsta möjliga grad. Dess grad kallas **graden** av α över K. Ett element α som inte är algebraiskt kallas **transcendet**. □

(18.2) Exempel. (a) Låt $\alpha = i \in \mathbb{C} \supset \mathbb{R}$. Talet i är algebraiskt över $\mathbb{R}$ ty $p(i) = 0$ där $p(X) = X^2 + 1$. Detta är ett minimalpolynom för i över $\mathbb{R}$ ty i kan inte vara ett nollställe till ett reellt polynom av grad 1 ($i \notin \mathbb{R}$). Graden av i över $\mathbb{R}$ är 2.

(b) Låt $\alpha = \sqrt{2} \in \mathbb{R} \supset \mathbb{Q}$. $\sqrt{2}$ är ett nollställe ill $p(X) = X^2 - 2 \in \mathbb{Q}[X]$ så att $\sqrt{2}$ är algebraisk över $\mathbb{Q}$. graden av $\sqrt{2}$ över $\mathbb{Q}$ är 2 ty $\sqrt{2} \notin \mathbb{Q}$ (dvs $\sqrt{2}$ är inte ett nollställe till ett polynom ur $\mathbb{Q}[X]$ av grad 1).

(c) Låt $\alpha = \sqrt[3]{2} \in \mathbb{R} \supset \mathbb{Q}$. $\sqrt[3]{2}$ upfyller ekvationen $p(X) = X^3 - 2 = 0$ så att det är ett algebraiskt element. Det är lite svårare att bestämma graden av $\sqrt[3]{2}$ över $\mathbb{Q}$. Den är 3. Detta följer lätt tack vare en karakterisering av minimalpolynom i vår nästa sats.

(d) $\alpha = \sqrt{2} + i$ är algebraiskt över $\mathbf{Q}$ ty $\alpha^2 = 1 + 2i\sqrt{2}$ ger $(\alpha^2 - 1)^2 = -8$, dvs α satisfierar ekvationen $p(X) = 0$, där $p(X) = X^4 - 2X^2 + 9$. Graden av α över $\mathbb{Q}$ är lika med 4 (se övning rref). □

(18.3) Anmärkning. Med ett **algebraiskt tal** menar man ett algebraiskt element i $\mathbb{C}$ över $\mathbb{Q}$. **Transcendenta tal** är icke-algebraiska komplexa tal. Exempel på transcendenta tal är

$\pi, e, 2^{\sqrt{2}}$ men det är relativt svårt att bevisa den egenskapen. Det faktum att π är transcendent visades av C.L.F. Lindemann 1882 (en konsekvens av detta är att cirkelns kvadratur† är omöjlig). Samma egenskap hos e visade C. Hermite 1873. Transcendensen av talen a^b där a är ett algebraiskt tal $\neq 0, 1$ och b är ett algebraiskt icke-rationellt (t ex $2^{\sqrt{2}}$) tal visades 1934 av A.O. Gelfond och (helt oberoende) Th. Schneider. De första exemplen på transcendenta tal gavs av J. Liouville 1844. □

(18.4) Sats. *Låt $\alpha \in L \supseteq K$ vara ett algebraiskt element över K.*

(a) *Varje minimalpolynom för α över K är irreducibelt och det är en delare till varje polynom ur $K[X]$ som har α som sitt nollställe.*

(b) *Varje irreducibelt polynom $p \in K[X]$ sådant att $p(\alpha) = 0$ är ett minimalpolynom för α över K.*

(c) *Två minimalpolynom för α över K är lika så när som på en nollskild konstant ur K.*

Bevis. (a) Låt p_0 vara minimalpolynomet för α över K. Det är klart att p_0 är irreducibelt ty $p_0 = p_1 p_2$, där $\operatorname{grad} p_i < \operatorname{grad} p_0$ ger $p_1(\alpha)p_2(\alpha) = p_0(\alpha) = 0$ dvs $p_1(\alpha) = 0$ eller $p_2(\alpha) = 0$. Detta strider dock mot definitionen av p_0. Låt $p(\alpha) = 0$, $p \in K[X]$. Då är

$$p = p_0 q + r, \quad \operatorname{grad} r < \operatorname{grad} p_0.$$

Alltså är $r(\alpha) = p(\alpha) - p_0(\alpha)g(\alpha) = 0$. I så fall är $r = 0$ därför att dess grad är lägre än $\operatorname{grad} p_0$, vilket ger $p_0 | p$.

(b) Om p_0 är ett minimalpolynom för α över K så är $p_0 | p$ enligt (a). Men p är irreducibelt så att $p = ap_0$, $a \in K$. Detta visar att $\operatorname{grad} p = \operatorname{grad} p_0$ så att p också är ett minimalpolynom.

(c) Om p och p_0 är minimalpolynom så är $\operatorname{grad} p = \operatorname{grad} p_0$ och $p_0 | p$ (enligt (a)). Alltså är $p = ap_0$, $a \in K$ och $a \neq 0$ (ty $p \neq 0$). □

(18.5) Anmärkning. Med tanke på rref (19,3) (c) kan man välja bland alla minimalpolynom för α över K ett som har högsta koefficienten lika med 1. Det kallas **minimalpolynomet** för α över K. Det kommer att betecknas med m_α. □

Exempel. (a) Minimalpolynomet för $\alpha = i$ över $\mathbf{Q}$ (eller $\mathbf{R}$) är $p(X) = X^2 + 1$, ty detta polynom är irreducibelt över $\mathbf{Q}$ (eller $\mathbf{R}$) och $p(i) = 0$. (b) Minimalpolynomet för $\alpha = \sqrt[5]{2}$ över $\mathbf{Q}$ är $p(X) = X^5 - 2$, ty detta polynom är irreducibelt över $\mathbf{Q}$ (se t ex Eisenstein's kriterium - övning rref) och $p(\sqrt[5]{2}) = 0$. □

Låt $\alpha \in L \supseteq K$. Vi påminner om att $K[\alpha]$ betecknar den minsta delring till L som innehåller både K och α (se övn. rref). Den består av alla uttryck $a_0 + a_1\alpha + \ldots + a_m\alpha^m$, där $a_i \in K$ (varje delring till L som innehåller K och α måste innehålla sådana uttryck. Samtidigt bildar elementen på den formen en ring.)

†Med cirkelns kvadratur menar man att med passare och linjal konstruera en kvadrat vars area är lika med arean av en given cirkelskiva.

(18.6) Sats. *Låt $\alpha \in L \supseteq K$.*

(a) *Om α är ett algebraiskt element av grad n över K så är $K[\alpha]$ en kropp. Varje element i den kroppen kan skrivas entydigt på formen*

$$r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}, \quad r_i \in K.$$

(b) *Om α är transcendent över K över K så är $K[\alpha]$ isomorf med polynomringen $K[X]$.*

Bevis. (a) Betrakta ringhomomorfismen:

$$\theta : K[X] \to L$$

där $\theta(p) = p(\alpha)$ (se exempel rref (14.2) och övn. 14.1). Vi har $\theta(K[X]) = K[\alpha]$ och

$$\operatorname{Ker}\theta = \{p \in K[X] : \theta(p) = p(\alpha) = 0\} = (m_\alpha)$$

enligt (19.3) rref (a). Enligt huvudsatsen om ringhomomorfismer är

$$\bar{\theta} : K[X]/(m_\alpha) \cong K[\alpha]$$

där $\bar{\theta}(\bar{r}) = r(\alpha)$. Sidoklasserna $\bar{r}$ kan skrivas entydigt med $r(X) = r_0 + r_1X + \ldots + r_{n-1}X^{n-1}$ (se (17.2) rref). Detta betyder att $K[\alpha]$ består av alla element

$$\bar{\theta}(\bar{r}) = \theta(r) = r(\alpha) = r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}$$

och framställningen är entydig. Slutligen är $K[\alpha]$ en kropp ty m_α är ett irreducibelt polynom (se rref (a) så att $K[X]/(m_\alpha)$ är en kropp (se ref).

(b) Från (a) har vi den surjektiva homomorfismen $\theta : K[X] \to K[\alpha]$ där $\theta(p) = p(\alpha)$. Men

$$\operatorname{Ker}\theta = \{p \in K[X] : \theta(p) = p(\alpha) = 0\} = (0)$$

ty α är ett transcendent element. Alltså är θ en isomorfism ty den är både surjektiv och injektiv (se övn. rref) □

(18.7) Följdsats. *Låt $\alpha, \alpha' \in L \supseteq K$ vara två algebraiska element med samma minimalpolynom $m(X)$ över K. Då är $K[\alpha] \cong K[\alpha']$.*

Bevis. Ur beviset av rref (19.5) (a) följer (se rref (19.6)) att bägge ringarna är isomorfa med $K[X]/(m)$. □

(18.8) Anmärkning. Om $\alpha \in L \supseteq K$ så betecknar man med $K(\alpha)$ den **minsta delkropp till L som innehåller K och α**. Första delen av satsen rref (19.5) säger att $K(\alpha) = K[\alpha]$ (därför att $K[\alpha]$ är en kropp och varje delkropp till L som innehåller K och α måste innehålla $K[\alpha]$). Om α är transcendent över K så är $K(\alpha) \supset K[\alpha]$ (de är inte längre lika) därför att en kropp som innehåller K och α måste förutom $K[\alpha]$ innehålla inverser till alla skilda från

0 element i polynomringen $K[\alpha]$. Men t.ex. $1/\alpha \notin K[\alpha]$ (övn. rref 19.9). $K(\alpha)$ består av alla uttryck

$$\frac{a_0 + a_1\alpha + \ldots + a_k\alpha^k}{b_0 + b_1\alpha + \ldots + b_l\alpha^l}$$

(nämnaren $\neq 0$) ty sådana uttryck bildar en kropp och de ligger i varje kropp som innehåller K och α. Elementen i $K(\alpha)$ kallas **rationella funktioner** av α med koefficienter i K. □

Exempel. (a) Låt $\alpha = i \in \mathbb{C} \supset \mathbb{Q}$. minimalpolynomet för i över $\mathbb{Q}$ är $m(X) = X^2 + 1$. ($m(i) = 0$ och $m(X)$ är irreducibelt i $\mathbb{Q}[X]$ – se rref (1.58) (b)). Alltså är graden av i över $\mathbb{Q}$ lika med 2. Enligt rref (19.5) (a) består $\mathbb{Q}(i)$ av talen $r_0 + r_1 i$, där $r_0, r_1 \in \mathbb{Q}$.

(b) Låt $\alpha = \sqrt[3]{2} \in \mathbb{R} \supset \mathbb{Q}$. minimalpolynomet för α över $\mathbb{Q}$ är $m(X) = X^3 - 2$ (irreducibiliteten följer ur rref (15.8) (b)). graden av α över $\mathbb{Q}$ är 3 och $\mathbb{Q}(\sqrt[3]{2})$ består av talen $r_0 + r_1\sqrt[3]{2} + r_2\sqrt[3]{4}$, där $r_0, r_1, r_2 \in \mathbb{Q}$. □

(18.9) Definition. Man säger att $K \subseteq L$ är en **ändlig kroppsutvidgning** om L har ändlig dimension som ett vektorrum över K. Dimensionen $\dim_K L$ kallas **graden av L över K** och betecknas med $[L : K]$. Man skriver $[L : K] = \infty$ om L inte är en ändlig utvidgning av K. □

(18.10) Exempel. (a) Vi har $[\mathbb{C} : \mathbb{R}] = 2$ ty $1, i$ är en bas för $\mathbb{C}$ över $\mathbb{R}$ (se Exempel rref (18.10) b)).

(b) Sats rref (19.5) säger att $[K(\alpha) : K] = n$ då α är ett algebraiskt element av grad n över K. En bas består av $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. □

(18.11) Sats. *Om $K \subseteq L \subseteq M$ och alla utvidgningar är ändliga så är $[M : K] = [M : L][L : K]$.*

Bevis. Låt $e_1, e_2, \ldots, e_r$ vara en bas för L över K och låt $f_1, f_2, \ldots, f_s$ vara en bas för M över L. Vi visar att alla produkter $e_i f_j$ bildar en bas för M över K. Varje $m \in M$ kan skrivas entydigt som lnjärkombination $m = \sum_{j=1}^{s} l_j f_j$, där $l_j \in L$. Varje l_j kan skrivas entydigt som linjärkombination $l_j = \sum_{i=1}^{r} k_{ij} e_i$. Alltså har man entydig framsällning:

$$m = \sum_{j=1}^{s} l_j f_j = \sum_{j=1}^{s} (\sum_{i=1}^{r} k_{ij} e_i) f_j = \sum_{j=1}^{s} \sum_{i=1}^{r} k_{ij} e_i f_j.$$

Detta visar att alla produkter $e_i f_j$ bildar en bas för M över K, vilket betyder att $[M : K] = [M : L][L : K]$. □

Exempel. Vi skall bestämma en bas och beräkna graden för $\mathbb{Q}(\sqrt{2}, i)$ över $\mathbb{Q}$. Vi har:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, i).$$

Nu är $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ty enligt sats rref (19.5) (a) består $\mathbb{Q}(\sqrt{2})$ av talen $a + b\sqrt{2}, a, b \in \mathbb{Q}$. Talet i är algebraiskt av grad 2 över kroppen $\mathbb{Q}(\sqrt{2})$ ty polynomet $X^2 + 1$ är irreducibelt i $\mathbb{Q}(\sqrt{2})[X]$. Alltså är $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ enligt samma sats rref (19.5) (a). Kroppen

$\mathbb{Q}(\sqrt{2}, i)$ består enligt denna sats av $r_0 + r_1 i, r_0, r_1 \in \mathbb{Q}(\sqrt{2})$ dvs $r_0 = a + b\sqrt{2}, r_1 = c + d\sqrt{2}, a, b, c, d \in \mathbb{Q}$. Det ger att $\mathbb{Q}(\sqrt{2}, i)$ består av talen

$$a + b\sqrt{2} + ci + di\sqrt{2}, , a, b, c, d \in \mathbb{Q}.$$

Vi har $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(i) : \mathbb{Q}] = 4$. □

(18.12) Definition. Man säger att $L \supseteq K$ är en **algebraisk utvidgning** om varje element i L är algebraisk över K. Om $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$ så betecknar $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ kropen $K(\alpha_1)(\alpha_2)\ldots(\alpha_m)$. Man säger att L är **ändligt genererad** över K om $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$. □

(18.13) Sats. *Om $L \supseteq K$ är en ändlig utvidgning så är den algebraisk.*

Bevis. Låt $[L : K] = n$ och låt $\alpha \in L$. Antalet element $1, \alpha, \alpha^2, \ldots, \alpha^n$ är $n + 1$ så att dessa potenser av α är linjärt beroende över K dvs det finns $a_i \in K$ som inte alla är $= 0$ sådana att

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$$

Detta visar att α uppfyller ekvationen $p(X) = 0$ där $p(X) = a_0 + a_1X + \ldots + a_nX^n$. □

(18.14) Sats. *Låt $K \subseteq L$ vara en kroppsutvidgning. Alla element i L som är algebraiska över K bildar en kropp.*

Bevis. Låt $\alpha, \beta \in L$ vara algebraiska över K. Vi måste bevisa att även $\alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$ är algebraiska över K. Utvidgningarna $K(\alpha) \supseteq K$ och $K(\alpha, \beta) \supseteq K(\alpha)$ är ändliga ty α är algebraiskt över K och β är algebraiskt över $K(\alpha)$ (β är t.o.m. algebraiskt över K). Detta gäller enligt sats rref (19.5) (a). Alltså är $K(\alpha, \beta) \supseteq K$ en ändlig utvidgning enligt sats rref (19.11). I så fall är den algebraisk enligt rref (19.13). Men $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$ så att dessa element är algebraiska över K. □

Exempel. Talet $\sqrt{2} + \sqrt{3}$ är algebraiskt över $\mathbb{Q}$ ty $\sqrt{2}$ och $\sqrt{3}$ är algebraiska. Det är lättare att konstatera detta än att hitta den polynomekvation som $\alpha = \sqrt{2} + \sqrt{3}$ uppfyller. Men

$$\alpha^2 = 5 + 2\sqrt{6}$$

så att

$$(\alpha^2 - 5)^2 = 24$$

dvs $\alpha^4 - 10\alpha^2 + 1 = 0$. Detta visar att α uppfyller $X^4 - 10X^2 + 1 = 0$. □

ÖVNINGAR

18.1. Vilka av följande tal är algebraiska?

(a) $1 + \sqrt{2} + \sqrt{3}$, (c) $\sqrt{\pi} + 1$,
(b) $\sqrt{2} + \sqrt[5]{2}$, (d) $\sqrt{\pi} + \sqrt{2}$.

18.2. Bestäm minimalpolynomet och graden för α över K då:

(a) $K = \mathbb{Q}$, $\alpha = \sqrt[3]{\sqrt{3}+3}$, (c) $K = \mathbb{Q}(i)$, $\alpha = \sqrt{2}$,
(b) $K = \mathbb{Q}$, $\alpha = \sqrt{2}+i$, (d) $K = \mathbb{Q}$, $\alpha^5 = 1$ och $\alpha \neq 1$.

18.3. Bestäm graden och en bas för följande utvidgningar $L \supseteq K$

(a) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, (c) $K = \mathbb{F}_2$, $L = \mathbb{F}_2(\alpha), \alpha^4 + \alpha^3 + 1 = 0$,
(b) $K = \mathbb{Q}$, $L = \mathbb{Q}(i, \sqrt[4]{2})$, (d) $K = \mathbb{F}_2$, $L = \mathbb{F}_2(\alpha), \alpha^3 + \alpha + 1 = 0$.

18.4. Visa att $\cos(x\pi)$ och $\sin(x\pi)$ är algebraiska tal då x är rationellt.

18.5. Låt $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Bestäm $a, b, c, d \in \mathbb{Q}$ så att $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ om

(a) $x = \frac{1}{\sqrt{2}+\sqrt{3}}$, (b) $x = \frac{\sqrt{2}+\sqrt{3}}{1+\sqrt{2}+\sqrt{3}}$.

18.6. Låt $L = \mathbb{F}_2(\alpha)$ där $\alpha^4 + \alpha + 1 = 0$. Bestäm $a, b, c, d \in \mathbb{F}_2$ så att $x = a + b\alpha + c\alpha^2 + d\alpha^3$ om

(a) $x = \frac{1}{2}$, (b) $x = \alpha^5$, (c) $x = \frac{1}{\alpha^2+\alpha+1}$.

18.7. Låt $L = \mathbb{F}_2(\alpha)$ där $\alpha^4 + \alpha^3 + 1 = 0$. Bestäm $\beta \in L$ så att $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 2$.

18.8. Låt $L = \mathbb{F}_2(\alpha)$, där $\alpha^3 + \alpha + 1 = 0$. Bestäm minimalpolynomet för $\beta = \alpha^2 + \alpha$ över $\mathbb{F}_2$.

18.9. Låt $\alpha \in L \supset K$ vara ett transcendent element över K. Visa att $1/\alpha \notin K[\alpha]$.

18.10. Låt $K \subseteq L$ vara en kroppsutvidgning. Visa att om utvidgningen är ändligt genererad och algebraisk så är den ändlig.

Kapitel 19

GEOMETRISKA KONSTRUKTIONER

Låt X vara en godtycklig punktmängd i planet.

- En linje är definierad av X om den går genom två olika punkter tillhörande X.
- En cirkel är definierad av X om dess centrum tillhör X och dess radie är lika med avståndet mellan två punter tillhörande X.

Man säger att en punkt $P = (a, b)$ **kan direkt konstrueras ur** X med passare och linjal om P är skärningspunkten av två linjer eller två cirklar eller en linje med en cirkel som är definierade av X. Låt X_1 vara mängden av alla punkter i planet som kan direkt konstrueras ur $X = X_0$, X_2 mängden av alla punkter som kan direkt konstrueras ur X_1, X_3 mängden av alla punkter som kan direkt konstrueras ur X_2 osv. Man säger att en punkt $P = (a, b)$ **kan konstrueras ur** X med passare och linjal om $P \in X^\star = \bigcup_{i=0}^{\infty} X_i$ (dvs $P \in X_i$ för något $i \geq 0$).

Man definierar också **reella tal konstruerbara** ur X som sådana $r \in \mathbf{R}$ att $|r|$ = avståndet mellan två punkter konstruerbara ur X. Det är klart att en punkt $P = (a, b)$ kan konstrueras ur X då och endast då dess koordinater kan konstrueras ur X (en mycket enkel övning !).

Ofta börjar man med två punkter i planet – säg (0,0) och (1,0) – och försöker beskriva alla punkter i planet som med hjälp av passare och linjal kan konstrueras från dessa två. Med andra ord väljer man $X = \{(0, 0), (1, 0)\}$. De tal som är konstruerbara ur $X = \{(0, 0), (1, 0)\}$ kommer vi att beteckna med $\mathbf{K}$. Den minsta talkropp som innehåller koordinaterna av $(0, 0)$ och $(1, 0)$ är självklart $\mathbf{Q}$. Rent allmänt (med godtycklig punktmängd X) har man följande hjälpresultat:

(19.1) Lemma. *Låt K vara den minsta talkropp som innehåller koordinaterna av alla punkter tillhörande X. Varje punkt som kan direkt konstrueras ur X har koordinater in en talkropp L sådan att $[L : K] \leq 2$.*

Bevis. En linje som går genom två punkter med koordinater i en kropp K har en ekvation $ax + by + c = 0$ med koefficienter a, b, c i K. Koordinaterna för snittpunkten av två linjer ges av lösningen till ett linjärt ekvationssystem bestående av två sådana ekvationer. Alltså tillhör dessa koordinater samma kropp K.

En cirkel vars centrum (p, q) har koordinater i K och vars radie är lika med avståndet d mellan två punkter med koordinater i K har ekvationen $(x-p)^2 + (y-q)^2 = d^2$. Det är klart att $d^2 \in K$. Snittpunkterna av en sådan cirkel med en linje som ovan får man som lösningar till ekvationssystemet:

$$\begin{aligned} ax + by + c &= 0, \\ (x-p)^2 + (y-q)^2 &= d^2. \end{aligned}$$

För att lösa ekvationssystemet uttrycker man y med hjälp av x (eller tvärtom) ur den första ekvationen och sätter in i den andra. Man får då en kvadratisk ekvation med avseende på x (eller y) av typen $x^2 + Ax + B = 0$. Koefficienterna A, B tillhör K medan lösningarna $x = -A/2 \pm \sqrt{A^2/4 - B}$ ligger i kroppen $L = K(\sqrt{A^2/4 - B})$ vars grad över K är högst 2.

Om man har två cirklar som ovan och söker deras snittpunkter så måste man lösa ekvationssystemet

$$\begin{aligned} (x-p)^2 + (y-q)^2 &= d^2, \\ (x-p')^2 + (y-q')^2 &= d'^2. \end{aligned}$$

Man kan lösa systemet genom att subtrahera dessa två ekvationer. Då får man ett ekvationssystem bestående av en linjeekvation och en cirkelekvation dvs samma situation som i förra fallet. □

Nu kan vi rent allmänt karakterisera de punkter som kan konstrueras ur X med passare och linjal:

(19.2) Sats. *Låt K vara den minsta talkropp som innehåller koordinaterna av alla punkter tillhörande X. Om en punkt $P = (a, b)$ kan konstrueras ur X med passare och linjal så finns det en kedja av kroppar*

$$K = K_0 \subset K_1 \subset \ldots K_n = L$$

sådan att $a, b \in L$ och $[K_{i+1} : K_i] = 2$ för $i = 0, 1, \ldots, n$.

Bevis. Punkten P kan konstrueras ur X i ett ändligt antal steg. Enligt Lemma leder varje ny punkt till en utvidgning av grad ≤ 2 av den kropp som innehåller koordinaterna för alla föregående punkter. Detta visar att koordinaterna a, b av punkten P måste tillhöra en kropp

L som man får ur K genom konsekutiva utvidgningar av grader ≤ 2 (vi tar med endast de utvidgningar vars grader är 2). □

Med hjälp av Satsen kan man bevisa att en rad geometriska konstruktioner inte kan genomföras med passare och linjal. Om vi väljer $X = \{(0,0),(1,0)\}$ så är kroppen $K = \mathbf{Q}$. En punkt $P = (a,b)$ kan konstrueras med passare och linjal endast om dess koordinater tillhör en kroop L vars grad över K är en 2-potens, ty $[K_n : K] = 2^n$.

Exempel. (a) **Kubens fördubbling.** En kub med kanten 1 är given. Är det möjligt att med passare och linjal konstruera en kub med volymen 2 ? Kanten av den sökta kuben är $x = \sqrt[3]{2}$. Om vi väljer $X = \{(0,0),(1,0)\}$ så vill vi veta om det är möjligt att konstruera en sträcka av längden $x = \sqrt[3]{2}$, eller punkten $(\sqrt[3]{2}, 0)$. Om det är möjligt så existerar en kropp L sådan att $\sqrt[3]{2} \in L$ och graden av L över $\mathbf{Q}$ är en 2-potens dvs vi har en kroppskedja:

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}) \subset L.$$

Men $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ så att $3|[L : \mathbf{Q}] =$ en 2-potens, vilket är orimligt. Alltså är kubens fördubbling med passare och linjal inte möjlig.

(b) **Vinkelns tredelning.** Vinkeln 60^0 är given. Är det möjligt att tredela den (dvs dela i tre lika delar) med passare och linjal ? Om vi välljer vinkelns spets i punkten (0,0) och punkten (1,0) på vinkelns ena arm så kan vi konstruera en cirkel med centrum i origo och med radien 1. Att kunna tredela vinkeln betyder att vi kan konstruera en halvlinje som går från origo och bildar vinkeln 20^0 med x-axeln. Denna halvlinje skär enhetscirkeln i punkten $(\cos 20^0, \sin 20^0)$ så att denna punkt kan konstrueras med passare och linjal från (0,0) och (1,0). Detta betyder att det finns en kropp L som innehåller $\cos 20^0$ och vars grad över $\mathbf{Q}$ är en 2-potens. Formeln $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ ger med $\alpha = 20^0$ ekvationen $8x^3 - 6x - 1 = 0$, där $x = \cos 20^0$. Vi har följande kedja:

$$\mathbf{Q} \subset \mathbf{Q}(\cos 20^0) \subset L.$$

Men polynomet $8x^3 - 6x - 1$ är irreducibelt så att $[\mathbf{Q}(\cos 20^0) : \mathbf{Q}] = 3$. På samma sätt som ovan får vi en motsägelse, ty $[L : \mathbf{Q}] =$ 2-potens. Alltså kan man inte tredela vinkeln 60^0 med passare och linjal.

(c) **Cirkelns kvadratur.** En cirkelskiva med radie 1 är given. Är det möjligt att konstruera med passare och linjal en kvadrat vars area är lika med cirkelskivans area ? Vi kan placera cirkelskivans centrum i origo. Punkten (1,0) ligger då på cirkeln. Vi vill konstruera kvadratens sida som måste vara lika $\sqrt{\pi}$, ty cirkelskivans area är just π. Om konstruktionen är möjlig så får vi en kedja

$$\mathbf{Q} \subset \mathbf{Q}(\pi) \subset L.$$

Men graden $[\mathbf{Q}(\pi) : \mathbf{Q}]$ är oändlig, ty talet π är transcendent. Alltså kan inte $\mathbf{Q}(\pi)$ inneslutas in en kropp L av ändlig grad över $\mathbf{Q}$. Detta visar att cirkelns kvadratur är omöjlig. Den

som kom först med detta påstående var C.L.F. Lindemann då han 1892 visade att talet π är transcendent.

I boken visas också att mängden $\mathbf{K}$ av alla konstruerbara tal är en kropp (se Sats 54.1 och dess bevis). □

Kapitel 20

TALBEGREPPET

Våra kunskaper om olika talområden bygger på vår förmåga att hantera talen. I praktiken betyder det att vi följer en rad olika regler när vi utför olika räkneoperationer. Vad är det för regler? Du kan säkert nämna eller skriva ut sådana regler som t ex associativiteten för addition: $a + (b + c) = (a + b) + c$, eller kommutativiteten för multiplikation: $ab = ba$. Hur många sådana regler finns det? Är alla lika viktiga? När kan man vara säker på att man har alla nödvändiga regler? Sådana frågor har sysselsatt många människor och svaren på dem bygger på matematisk forskning under en ganska lång tidsperiod. Här följer en förteckning över de viktigaste räknelagarna i en talmängd R i vilken de kan vara uppfyllda eller ej – allt beror på hur man väljer R :

Addition:

(a) slutenhet:	$\forall_{a,b\in R}$	$a, b \in R \Rightarrow a + b \in R$,	
(b) associativitet:	$\forall_{a,b,c\in R}$	$(a + b) + c = a + (b + c)$,	
(c) kommutativitet:	$\forall_{a,b\in R}$	$a + b = b + a$,	
(d) neutralt element:	$\exists_{0\in R}\forall_{a\in R}$	$0 + a = a$,	
(e) motsatt element:	$\forall_{a\in R}\exists_{a'\in R}$	$a + a' = 0$	(a' betecknas med $-a$).

Multiplikation:

(f) slutenhet:	$\forall_{a,b\in R}$	$a, b \in R \Rightarrow ab \in R$,	
(g) associativitet:	$\forall_{a,b,c\in R}$	$(ab)c = a(bc)$,	
(h) kommutativitet:	$\forall_{a,b\in R}$	$ab = ba$,	
(i) neutralt element:	$\exists_{1\in R}\forall_{a\in R}$	$1a = a$,	
(j) inverst element:	$\forall_{a\in R\setminus\{0\}}\exists_{a'\in R}$	$aa' = 1$	(a' betecknas med a^{-1}).

Addition och multiplikation:

(k) distributivitet: $\forall_{a,b,c\in R}$ $a(b + c) = ab + ac$.

Alla dessa regler gäller då R är en talkropp t ex $\mathbb{Q}$, $\mathbb{R}$ eller $\mathbb{C}$. Om $R = \mathbb{Z}$ så gäller alla räknelagar med undantag av (j) – t ex $2 \in \mathbb{Z}$, men $1/2 \notin \mathbb{Z}$. Egenskapen (j) ger just skillnaden mellan en talkropp och en talring. I en talkropp gäller alla räknelagarna (a) – (k), medan i en talring gäller alla utom (j).

Räknelagarna (a) – (k) är grunden för all manipulation med talen och man måste vara medveten om deras giltighet i det talområde man vill arbeta med. Andra räknelagar som t ex

(a) $a0 = 0$ då $a \in R$,

(b) $(-1)(-1) = 1$,

(c) $-(-a) = a$ då $a \in R$,

(d) $(-a)b = -ab$ då $a, b \in R$,

(e) $(-a)(-b) = ab$ då $a, b \in R$,

kan man bevisa om man vet att R är en ring. I själva verket gäller de i en helt godtycklig ring med etta, vilket kunde vi konstatera tidigare.

I samband med definitionerna av begreppen ring och kropp har du säkert observerat att man inte nämner subtraktion och division. Förklaringen är att subtraktion och division kan definieras i efterhand med hjälp av addition och multiplikation:

(20.1) Definition. (a) Om R är en ring och $a, b \in R$ så säger man att

$$a - b = a + (-b)$$

är **skillnaden** mellan a och b.

(b) Om R är en kropp och $a, b \in R$, $b \neq 0$, så säger man att

$$a : b = ab^{-1}$$

är **kvoten** av a genom b. Kvoten betecknas också med $\frac{a}{b}$. □

Vårt syfte i detta kapitel är att förklara hur man definierar talbegreppet. Som vi redan vet finns det oändligt många olika talringar och talkroppar. På vilket sätt intar $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ och $\mathbb{C}$ en särställning bland dem? Ett kort svar som kräver många förklaringar är följande: $\mathbb{Z}$ är den minsta talringen, $\mathbb{Q}$ är den minsta talkroppen, $\mathbb{R}$ är den största talkroppen som tillåter ordningsrelationen $\leq$ och $\mathbb{C}$ är den största talkroppen överhuvudtaget. Man inser säkert att alla dessa svar förutsätter att man vet vad ett tal är. Svaret på den frågan är inte enkelt och det tog en mycket lång tid i mänsklighetens utveckling innan man kunde komma till ett tillfredsställande svar. Trots det har man sedan en lång tid tillbaka kunnat räkna med alla typer av tal och utveckla vetenskapliga teorier som bygger på beräkningar och som framgångsrikt beskriver världen runt omkring oss. De naturliga talen är med all säkerhet lika gamla som den mänskliga civilisationen, rationella tal (åtminstone positiva) är nästan lika gamla, negativa tal (hela, rationella och reella) användes för ungefär 1000 år sedan, och komplexa tal introducerades under 1500-talet. Därför finns det inte någon större anledning till oro om våra svar

inte visar sig bli fullständiga. Vi skall försöka förklara olika aspekter av talbegreppet utan att förutsätta några större förkunskaper. Mera tillfredsställande förklaringar väntar den som läser fortsättningskurser i matematik.

Det finns två möjligheter att introducera talbegreppet. Den ena är att börja med de naturliga talen och försöka steg för steg konstruera andra typer av tal. Den metoden ter sig naturlig och tilltalande men den är mycket arbetsam och, tyvärr, ganska lång om man vill kontrollera alla detaljer. Vi skall berätta om den senare i detta kapitel.

Den andra möjligheten utgår från att man kan hantera talen om man vet vilka regler som styr deras användning. Det räcker om man kommer överens om dessa regler och följer dem för att kunna använda talen, men man behöver inte bry sig om hur de är konstruerade. En sådan inställning till talen är mycket praktisk, men en matematiker vill gärna veta hur talen konstrueras (och alla andra som använder talen måste tro på möjligheten av dessa konstruktioner). Man kan jämföra den inställningen med inställningen till tekniken – om man har läst en instruktionsbok till en TV-apparat så vet man hur man använder den utan att behöva veta hur den är konstruerad (eller att den finns). En beskrivning av en programvara är troligen ännu bättre som jämförelse – man får en förteckning över kommandon och deras effekt utan att behöva veta hur programvaran är konstruerad eller om den finns tillgänglig.

Vi skall försöka beskriva de egenskaper som karakteriserar de reella talen. Valet av dessa egenskaper är ett resultat av matematisk forskning huvudsakligen under 1800-talet. De reella talen spelar en mycket central roll. Å ena sidan har alla människor en intuitiv uppfattning om dessa tal som kommer från erfarenheten av att räkna och mäta i vardagslivet. Å andra sidan bygger alla vetenskaper, och bland dem matematiken själv, på de reella talens egenskaper.

Som vi redan vet bildar de reella talen en kropp. Men det finns många kroppar så att man måste välja egenskaper som utmärker just den. En viktig egenskap är att man kan jämföra de reella talen med hjälp av $\leq$ – de reella talen bildar en ordnad kropp. Låt oss definiera helt allmänt vad detta betyder:

(20.2) Definition. Man säger att en kropp K är **ordnad** om den innehåller en delmängd P sådan att:

(a) om $x \in K$ så gäller exakt ett av de tre alternativen: $x \in P$ eller $x = 0$ eller $-x \in P$,

(b) om $x, y \in P$ så gäller att $x + y \in P$ och $xy \in P$.

Man säger att P är mängden av de positiva elementen i K. □

Det är klart att i $K = \mathbb{R}$ kan vi välja $P =$ alla positiva reella tal. Detta betyder att $\mathbb{R}$ är en ordnad kropp. $\mathbb{Q}$ är också ordnad därför att vi kan välja $P =$ alla positiva rationella tal. Vi skall visa senare att $\mathbb{C}$ inte är en ordnad kropp (det är enkelt att visa om man vet att $i^2 = -1$).

Vi skall uppehålla oss en stund vid definitionen (20.2). Man kan definiera:

$$x > y \quad (\text{eller} \quad y < x) \quad \text{om} \quad x - y \in P. \tag{20.3}$$

Man brukar också skriva $x \geq y$ (eller $y \leq x$) om $x > y$ eller $x = y$. $x > 0$ betyder att $x - 0 \in P$ dvs $x \in P$; $x < 0$ betyder att $0 - x \in P$ dvs $-x \in P$.

Om K är en ordnad kropp så kan man definiera de naturliga och de rationella talen i K. Först observerar vi att $1 > 0$ ($1 \in K$ är neutralt för multiplikation). Vi vet att $1 \neq 0$ så att $1 \in P$ eller $-1 \in P$. Antag att $-1 \in P$. Då är $1 = (-1)(-1) \in P$ enligt (b) i (20.2). Detta ger att både 1 och -1 tillhör P vilket strider mot (a) i (20.2). Därför måste $1 \in P$. De naturliga talen i K får vi som

$$1, 1+1, 1+1+1, 1+1+1+1, \ldots$$

vilka definitionsmässigt betecknas med 1,2,3,4,.... Observera att $1 < 2 < 3 < 4...$ därför att $2-1 = 1 > 0$, $3-2 = 1 > 0$, $4-3 = 1 > 0$ osv. Heltalen i K definieras som: alla naturliga tal x, deras motsatta $-x$ samt 0 dvs 0, ± 1, ± 2, ± 3, ± 4, ... De rationella talen definieras som alla kvoter ab^{-1} , där a, b är hela och $b \neq 0$ (se (20.1)). Både $\mathbb{Q}$ och $\mathbb{R}$ är ordnade kroppar så att en

definition av de reella talen måste bygga på en annan egenskap (utöver det att $\mathbb{R}$ är ordnad). Innan vi formulerar en lämplig egenskap, låt oss återkomma för en stund till definitionen av en ordnad kropp. I en sådan kropp kan man definiera absolutbelopp:

$$|x| = \begin{cases} x & \text{om } x \geq 0, \\ -x & \text{om } x < 0. \end{cases} \tag{20.4}$$

Man kan också säga vad det betyder att en följd x_1, x_2, x_3, ... går mot 0. Man säger så om det för varje naturligt tal n finns ett N sådant att $|x_i| < \frac{1}{n}$ då $i > N$. Nu kan vi formulera en grundläggande egenskap som skiljer $\mathbb{Q}$ från $\mathbb{R}$. Låt x_1, x_2, ..., x_i, ... vara en växande och begränsad följd av rationella tal dvs $x_1 \leq x_2 \leq ... \leq x_i \leq ...$ och det finns ett tal B så att $x_i \leq B$ då $i = 1, 2, ...$ Vad kan man säga om gränsvärdet $\lim_{i\to\infty} x_i$? Från analyskursen vet vi att gränsvärdet existerar. Är gränsvärdet ett rationellt tal? Låt oss betrakta ett exempel. Definiera

$$x_n = 1, a_1 a_2 ... a_n, \quad n \geq 1,$$

där a_i är i :te siffran i decimalutvecklingen av $\sqrt{2}$ dvs

$x_1 = 1, 4,$
$x_2 = 1, 41,$
$x_3 = 1, 414,$
$x_4 = 1, 4142,$
. . .

Det är klart att alla x_n är rationella och att följden är växande och begränsad. Ändå är det också klart att $\lim_{n\to\infty} x_n = \sqrt{2}$ dvs följden konvergerar mot ett icke-rationellt tal $\sqrt{2}$ (vi visar om en stund att $\sqrt{2}$ inte är rationellt). Men gränsvärdet är ett reellt tal och det är sant helt allmänt att en växande och begränsad följd av reella tal konvergerar mot ett reellt tal.

Man säger att de reella talen bildar en fullständig kropp[†]. Allmänt har man följande begrepp:

(20.5) Definition. En ordnad kropp kallas **fullständig** om varje växande och begränsad följd av kroppens element konvergerar mot ett element i kroppen. □

Mera exakt, om K är en ordnad kropp så är den fullständig om för varje följd $x_1 \leq x_2 \leq ... \leq x_n \leq ...$ sådan att $x_n \in K$ och det finns $B \in K$ så att $x_n \leq B$ då $n = 1, 2, ...$ man kan hitta $x \in K$ så att $\lim_{n\to\infty} x_n = x$.

Nu kan vi definiera de reella talen:

(20.6) Definition. Med **reella tal** menar man elementen i en ordnad och fullständig kropp K. □

Dessa få ord döljer ett ganska sammansatt matematiskt innehåll: K är en kropp dvs uppfyller villkoren (a) – (k) på sidan 131, K är ordnad dvs upfyller (a) och (b) i (20.2), och slutligen är K fullständig dvs uppfyller (20.5). Nu kan man ställa två frågor:

> Finns det en ordnad och fullständig kropp?
> Hur många ordnade och fullständiga kroppar finns det?

Man behöver inte veta svaret på dessa två frågor för att kunna räkna med de reella talen därför att (20.6) är en exakt förteckning över alla grundläggande egenskaper hos dessa tal och det räcker att följa dem och deras logiska konsekvenser. Men svaren på dessa två frågor är mycket viktiga inte bara för en matematiker (en matematiker vill dessutom se själv hur man kommer fram till svaren). De är följande: Det finns ordnade och fullständiga kroppar. Om K_1 och K_2 är två sådana så finns det en bijektiv funktion $f : K_1 \to K_2$ (dvs enentydig och på hela K_2) som uppfyller $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ och om $a > 0$ så är $f(a) > 0$ [†]. Intuitivt säger existensen av f att K_1 och K_2 skiljer sig bara när det gäller beteckningar dvs om $a \in K_1$ så kan $f(a)$ uppfattas som ett annat namn på a. Addition och multiplikation i K_1 översätter man med hjälp av f till addition och multiplikation i K_2. Likaså positiva element ur K_1 övergår med hjälp av f i positiva element i K_2. I den meningen är kroppen av de reella talen entydig.

Vi vet redan att om vi har de reella talen så kan vi definiera de naturliga, hela och rationella. På så sätt har vi en möjlighet att tillfredsställa vårt behov av någorlunda ordentlig presentation av talbegreppet. Men även om den för många ändamål är helt tillfredsställande, går vi ett steg längre och försöker beskriva konstruktioner av olika talmängder. Behovet av sådana konstruktioner insåg man under 1800-talet då utvecklingen av matematiken gick så långt att intuitiva föreställningar om talen inte längre kunde accepteras. Man försökte konstruera olika

[†]Detta bevisas i analyskurser med hjälp av sk supremumaxiomet som är ekvivalent med den egenskapen.
[†]En sådan funktion f kallas isomorfism och man säger att K_1 och K_2 är isomorfa ordnade kroppar.

talområden genom att utgå från de naturliga talen och succesivt gå till de hela, rationella, reella och komplexa. Den vägen är ganska lång, arbetsam (man måste kontrollera många detaljer), och det värsta, rätt så tråkig om man bortser från mera allmänna principer som styr dessa konstruktionr och har betydelse i andra sammanhang. Därför behövs möjligen ett varningens ord att inte fördjupa sig i alla detaljer och inte ta vår genomgång på fullt allvar.

(20.7) De naturliga talen. De äldsta talen är de naturliga (och de är mest naturliga därför att de är de äldsta). Varifrån kommer de? En stor tysk matematiker L.Kronecker sade någon gång att "Gud skapade de naturliga talen, allt annat är människans skapelse". Det vore för enkelt med detta svar men det är mycket djupsinnigt. Den enda möjligheten att definiera de naturliga talen är den metod som vi använde tidigare för att definiera de reella: Man kan beskriva deras grundläggande egenskaper. Varifrån kommer de egenskaper som betraktas som grundläggande? Svaret är att de kommer från mänsklighetens erfarenhet av experimentel hantering av talen och det faktum att de regler som man har följt under en mycket lång tid ger en bild av verkligheten som överensstämmer med våra observationer. En analys av sådana regler kunde göras enbart av matematiker. Det var R. Dedekind † och G. Peano † som föreslog ett urval av sådana grundläggande regler under senare delen av 1800-talet. Den mest kända definitionen kommer från G. Peano och låter så här:

(20.8) Definition. Med **naturliga tal** menar man elementen i en mängd $\mathbb{N}$ som satisfierar följande villkor:

(a) det finns ett utvalt element $1 \in \mathbb{N}$;

(b) det finns en injektiv funktion som mot varje element $n \in \mathbb{N}$ ordnar ett element $n^* \in \mathbb{N}$ så att $n^* \neq 1$;

(c) om $X \subseteq \mathbb{N}$ och

(d_1) $1 \in X$,

(d_2) $\forall_n n \in X \Rightarrow n^* \in X$,

så är $X = \mathbb{N}$. □

Intuitivt betyder n^* talet $n + 1$ (n^* kallas efterföljaren till n). Sista villkoret (d) kallas ofta "induktionsaxiomet"(det behandlas närmare i samband med matematisk induktion). Lägg märke till att man inte nämner addition och multiplikation i definitionen. De definieras i efterhand. Peanos definition överenstämmer väl med vår intuition, den är lätt att förstå, den är kort och elegant. Den uppfyller många av de kriterier som man vill uppfylla när man definierar ett matematiskt objekt. Vidare kan man härleda ur den definitionen alla kända egenskaper hos de naturliga talen.

Men hur är det egentligen med existensen och entydigheten av den mängden? När det gäller entydigheten är svaret enkelt: Man kan visa att om N_1 och N_2 är två mängder som uppfyller

†Richard Dedekind (1831-1916) en tysk matematiker.
†Giuseppe Peano (1858-1932) en italiensk matematiker.

villkoren i definitionen (20.8) så är de isomorfa vilket betyder att det finns en bijektiv funktion $f : N_1 \to N_2$ sådan att $f(1) = 1$ samt $f(n^*) = f(n)^*$ (jämför ett liknande påstående om de reella talen på sidan 135). Existensen av de naturliga talen vilar på vår övertygelse om att åtminstone en mängd av de naturliga talen existerar – nämligen den som under mänsklighetens historia så troget och framgångsrikt har tjänat till att räkna, resonera och dra korrekta slutsatser om världen runt omkring oss. Med andra ord är existensen av de naturliga talen ett axiom. Här har vi närmat oss matematikens grunder som har mycket gemensamt med vetenskapernas filosofi.

Alla andra talområden kan nu succesivt konstrueras: De hela talen från de naturliga, de rationella från de hela, de reella från de rationella och de komplexa från de reella [†].

Nu skall vi börja vår vandring från de naturliga talen genom rationella och reella till de komplexa. Vi utelämnar många detaljer och begränsar oss till allmänna idéer.

Det finns två huvudorsaker till att talbegreppet utvidgades. Det första var behov i samband med mätningar. Man upptäckte mycket tidigt att det behövdes bråktal för att uttrycka dimensioner (längder och areor) av jordlotter. Men icke-rationella tal dök upp även i samband med mätningar (vi får se det i samband med konstruktionen av de reella talen). Den andra orsaken har en mera abstrakt karaktär. Nya typer av tal behövdes för att kunna lösa ekvationer. Ett typiskt exempel är de komplexa talen. På 1500-talet kände man formeln:

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

för lösningar till andragradsekvationen $x^2 + px + q = 0$. Löser man ekvationen $x^2 - 3x + 2 = 0$ så får man enligt den formeln $x_1 = 1$ och $x_2 = 2$. Tar man i stället $x^2 - 2x + 2 = 0$ så blir $x_1 = 1 + \sqrt{-1}$ och $x_2 = 1 - \sqrt{-1}$. En del människor skulle kanske säga att ekvationen $x^2 - 2x + 2 = 0$ i så fall saknar lösningar därför att $\sqrt{-1}$ är helt utan mening. Andra skulle acceptera symbolen $\sqrt{-1}$, tillskriva den egenskapen att $(\sqrt{-1})^2 = -1$ och sätta in $1 + \sqrt{-1}$ i ekvationen $x^2 - 2x + 2 = 0$. Då är

$$(1 + \sqrt{-1})^2 - 2(1 + \sqrt{-1}) + 2 = 1 + 2\sqrt{-1} + (-1) - 2 - 2\sqrt{-1} + 2 = 0$$

dvs $1 + \sqrt{-1}$ är en lösning till ekvationen. Så gjorde några italienska matematiker under 1500-talet. Om man anser att $1 + \sqrt{-1}$ bör uppfattas som en lösning till ekvationen $x^2 - 2x + 2 = 0$ så bör man också ha en bra förklaring till varför. Det gäller att motivera användningen av $\sqrt{-1}$. Det tog 300 år innan man kunde ge en tillfredsställande förklaring och konstruera rent formellt de komplexa talen. Men exakt samma situation som med de komplexa talen har man med de hela, rationella och reella. Om man frågar ett barn om x sådant att $2 + x = 3$ så får man svaret $x = 1$. Tar man istället $3 + x = 2$ riskerar man att bli utskrattad. Ekvationen $2 + x = 3$ kan lösas i mängden av de naturliga talen, men $3 + x = 2$ kräver ett nytt talområde – de hela talen (i synnerhet de negativa). På liknande sätt går det att dela 4 i två lika delar

[†]En anmärkning är på sin plats. När vi sade tidigare att det går att bevisa existensen av de reella talen så menade vi just att det var möjligt att konstruera dessa tal från de naturliga.

(dvs lösa $2x = 4$) i heltalen, men det går inte att dela 3 i två lika delar i den mängden (dvs lösa $2x = 3$) – det behövs rationella tal för att göra det. Slutligen kan man hitta ett rationellt tal som multiplicerat med sig självt ger 4 (dvs lösa $x^2 = 4$), men det går inte att hitta ett rationellt tal som multiplicerat med sig självt ger 2 (dvs lösa $x^2 = 2$) – för att göra det behövs ett nytt talområde. Det naturliga önskemålet att polynomekvationer alltid skall gå att lösa, tvingar oss således att succesivt utvidga talområden. Om det finns en slutstation för denna utvidgningsprocess får vi veta lite senare. Så låt oss börja!

(20.9) Från de naturliga talen till de hela. Ekvationen $3 + x = 5$ definierar $x = 2$ som sin lösning. Samma lösning ger $4 + x = 6$, $5 + x = 7$ osv. Man kan uppfatta 2 som paret (5,3) eller (6,4) eller (7,5) osv. Paret (a, b) ger lösningen till $b + x = a$ med $a > b$. Paren (a, b) och (c, d) ger samma x om $a - b = c - d$ dvs $a + d = b + c$. Men det finns par (a, b) med $a = b$ och $a < b$. Har de en liknande tolkning ? T ex kan (3,5) uppfattas som lösningen till $5 + x = 3$. En sådan lösning finns inte bland de naturliga talen men själva tolkningen ger en idé hur man kan definiera heltalen.

Låt oss betrakta alla par (a, b) där $a, b \in \mathbb{N}$. Vi säger att (a, b) och (c, d) tillhör samma klass (eller definierar samma heltal) då och endast då $a + d = b + c$

Alla par som tillhör samma klass som (a, b) betecknas med $[(a, b)]$. En sådan klass kallar vi för ett heltal och kommer överens om följande beteckningar:

$$[(a,b)] = \begin{cases} \text{a - b} & \text{om } a > b, \\ 0 & \text{om } a = b, \\ \text{-(b - a)} & \text{om } a < b. \end{cases}$$

T ex är $[(1, 3)] = -2$ och paren (1,3), (2,4), (3,5) osv tillhör samma klass. Vidare definierar man addition och multiplikation av heltal:

$$[(a, b)] + [(c, d)] = [(a + c,\ b + d)],$$

$$[(a, b)][(c, d)] = [(ac + bd,\ ad + bc)].\ ^{\dagger}$$

Nu kan man kontrollera att heltalen bildar en ring men att gå igenom alla detaljer är ganska omständligt (se övning 20.11).

(20.10) Från de hela talen till de rationella. Konstruktionen är nästan identisk med den förra. Ekvationen $2x = 1$ definierar $1/2$. Samma lösning ger $4x = 2$, $6x = 3$ osv. Vi kan uppfatta $1/2$ som paren (1,2), (2,4), (3,6) osv. $-1/2$ får man som t ex $(-1, 2)$, $(-2, 4)$ osv. Allmänt kan lösningen till $bx = a$ uppfattas som paret (a, b). Observera att $b \neq 0$. Två par

†Tänk på $[(a, b)]$ och $[(c, d)]$ som $a - b$ och $c - d$. Då är

$$(a - b)(c - d) = (ac + bd) - (ad + bc) = [(ac + bd, ad + bc)].$$

(a, b) och (c, d) ger samma rationella tal om $\frac{a}{b} = \frac{c}{d}$. Men vi vill undvika bråk (de skall ju definieras!). Därför skriver vi villkoret på formen $ad = bc$. Nu kan vi starta vår konstruktion.

Betrakta alla par (a, b) sådana att $a, b \in \mathbb{Z}$ och $b \neq 0$. Man säger att (a, b) och (c, d) , $d \neq 0$, tillhör samma klass om $ad = bc$. Alla par som tillhör klassen av (a, b) betecknas med $[(a, b)]$. En sådan klass kallar vi för ett rationellt tal och inför beteckningen

$$[(a, b)] = \frac{a}{b} \text{ (eller } \quad a : b).$$

t ex är $[(1, 3)] = \frac{1}{3}$ och paren (1,3), (2,6), (3,9) tillhör samma klass (definierar samma rationella tal). Nu kan vi definiera addition och multiplikation av rationella tal:

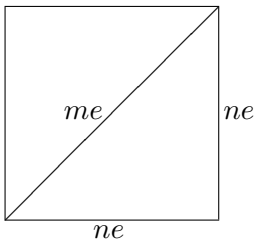
$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b}\frac{c}{d} &= \frac{ac}{bd}, \end{aligned}$$

och kontrollera att man verkligen får en kropp (se övning 20.12). Observera att:

$$\begin{aligned} \frac{a}{1} + \frac{c}{1} &= \frac{a + c}{1}, \\ \frac{a}{1}\frac{c}{1} &= \frac{ac}{1}, \end{aligned}$$

dvs talen $\frac{a}{1}$ adderas och multipliceras precis som heltalen a. Man kommer överens om att skriva $\frac{a}{1} = a$ så att de vanliga heltalen kan betraktas som en delmängd till de rationella talen.

(20.11) Från de rationella talen till de reella. Den biten av vägen är lite annorlunda och utgör ett mycket större steg än de två föregående. Först och främst hittar man lätt ekvationer med rationella koefficienter som saknar rationella lösningar, t ex $x^2 = 2$ (se nedan). Sådana ekvationer kräver en utvidgning av de rationella talen. Men det finns en annan mycket viktig anledning till att man inser behovet av nya tal. Man upptäckte mycket tidigt att rationella tal inte är tillräckliga för att kunna mäta längder av sträckor. Följande klassiska exempel spelade en mycket viktig roll i matematikens utveckling. Betrakta en kvadrat och anta att man har fixerat en enhet e sådan att kvadratens sida rymmer exakt n enheter och dess diagonal m enheter (m och n är naturliga tal).



Nu vet vi att $(ne)^2 + (ne)^2 = (me)^2$ så att $2n^2 = m^2$ dvs $\sqrt{2} = \frac{m}{n}$. Detta visar att om e finns så är $\sqrt{2}$ ett rationellt tal. Pythagoras † och hans elever visste mycket väl att det inte var fallet (vi skall visa om en stund att $\sqrt{2}$ inte är rationellt). Sin upptäckt om förhållandet mellan kvadratens sida och dess diagonal betraktade de som något som stred mot naturens ordning och försökte hemlighålla under en tid. Men konsekvensen blev att Euklides † kort därefter kunde utveckla geometrin och läran om reella tal som mått på sträckor.

Hur visar man att $\sqrt{2}$ inte är rationellt? Vi skall visa det genom att utnyttja entydigheten av primfaktoruppdelningar av de naturliga talen. Antag att $\sqrt{2}$ är rationellt dvs att

$$\sqrt{2} = \frac{m}{n} \ ,$$

där m, n är naturliga tal. Då är $2n^2 = m^2$. Eftersom m^2 och n^2 är kvadrater av heltal innehåller de ett jämnt antal primfaktorer 2 (möjligen 0 sådana faktorer). Alltså förekommer 2 som primfaktor i $2n^2$ ett udda antal gånger, medan i m^2 ett jämnt antal gånger så att $2n^2 \neq m^2$. Detta motsäger likheten $2n^2 = m^2$ och visar att $\sqrt{2}$ inte kan vara rationellt.

Låt oss nu konstruera de reella talen. Vi kan inte längre använda oss av tekniken med par av rationella tal. Men vi kan utnyttja följder av rationella tal. Reella tal (enligt gymnasiekunskaper) är decimaltal av typen $A = a, a_1a_2...a_n...$, där a är heltasdelen och $0, a_1a_2...a_n...$ är decimaldelen av A. Varje sådant tal kan approximeras med rationella tal – följden:

$x_1 = a, a_1$,
$x_2 = a, a_1a_2$,
$x_3 = a, a_1a_2a_3$,
. . .
$x_n = a, a_1a_2a_3...a_n$,
. . .

består av rationella tal och konvergerar mot A dvs $\lim_{n\to\infty} x_n = A$. T ex är för $A = \pi$:

$x_1 = 3, 1$,
$x_2 = 3, 14$,
$x_3 = 3, 141$,
. . .

†Pythagoras (572-500 f Kr)
†Euklides (ca 350 f Kr)

$x_8 = 3,14159265$,
. . .

Låt nu A vara ett positivt tal. Följden $\{x_1, x_2, ..., x_n, ...\} = \{x_n\}_1^\infty$ består då av rationella tal , den är växande och begränsad (ty $x_n \leq A$ för alla n). Vi vet att en sådan följd alltid har ett gränsvärde. Två följder $\{x_n\}$ och $\{x'_n\}$ har samma gränsvärde då och endast då deras skillnad går mot 0 dvs $\lim_{n\to\infty}(x_n - x'_n) = 0$. Positiva reella tal är alltså gränsvärden av växande och begränsade följder av rationella tal och två följder definierar samma reella tal som sitt gränsvärde om deras skillnad går mot 0. Men vi kan inte definiera reella tal som gränsvärden av sådana följder så länge de reella talen inte är konstruerade därför att en sådan definition skulle förutsätta att de reella talen (dvs gränsvärdena) är kända. Ändå identifierar vi varje reellt tal med ett gränsvärde på följande sätt. (Här börjar den formella definitionen.)

Betrakta alla växande och begränsade följder $\{x_1, x_2, ..., x_n, ...\} = \{x_n\}_1^\infty$, där x_n är positiva rationella tal. Man säger att två följder $\{x_n\}_1^\infty$ och $\{x'_n\}_1^\infty$ tillhör samma klass (definierar samma reella tal) om deras skillnad $\{x_n - x'_n\}_1^\infty$ konvergerar mot 0 dvs $\lim_{n\to\infty}(x_n - x'_n) = 0$. Alla följder som tillhör klassen av $\{x_n\}_1^\infty$ betecknas med $[\{x_n\}_1^\infty]$. En sådan klass kallar man för ett positivt reellt tal. Nu kan man definiera addition och multiplikation av de positiva reella talen:

$$[\{x_n\}_1^\infty] + [\{x'_n\}_1^\infty] = [\{x_n + x'_n\}_1^\infty],$$

$$[\{x_n\}_1^\infty][\{x'_n\}_1^\infty] = [\{x_n x'_n\}_1^\infty].$$

För att nu konstruera de negativa reella talen och talet 0 måste man upprepa sama konstruktion som ledde oss från de naturliga talen till de hela: Man betraktar alla par (a, b), där a och b är positiva reella tal, och man identifierar (a, b) med (c, d) om $a + d = b + c$. Kontrollen att man får en kropp, att den är ordnad och fullständig är ganska lång men inte särskilt svår (detaljerna behandlas närmare i fortsättnigskurser i matematik †).

(20.12) Från de reella talen till de komplexa. Vi vet redan att behovet av de komplexa talen upptäcktes i samband med andragradsekvationer med reella koefficienter. En så enkel ekvation som $x^2 = -1$ saknar reella lösningar. Antag att vi har en kropp K som innehåller de reella talen $\mathbb{R}$ och sådan att det finns $\alpha \in K$ som satisfierar ekvationen $x^2 = -1$ dvs $\alpha^2 = -1$. Man kontrollerar utan större svårigheter (se (**??**)) att talen

$$a + b\alpha, \text{ där } \quad a, b \in \mathbb{R} ,$$

bildar en kropp. Det finns en mycket lång tradition att α betecknas med i (ibland j) †. I den

†Vanligen brukar man i stället för växande och begränsade följder betrakta godtyckliga följder av rationella tal $x_1, x_2, ..., x_n, ...$ sådana att avståndet mellan talen x_i och x_j går mot 0 då i och j växer dvs $|x_i - x_j| \to 0$ då $i, j \to \infty$. Följder av den typen kallas Cauchyföljder.

†"i" kommer från ordet "imaginär". Det finns ett mycket intressant val av terminologi när det gäller nya typer av tal. De naturliga talen bland de hela kallas positiva, de övriga negativa. Bråktalen bland de reella kallas rationella, de övriga irrationella. Komplexa talen $a + bi$ har realdel a och en imaginärdel b. Alltså var allt nytt negativt, irrationellt och imaginärt (samt en lång tid impopulärt)

kroppen har vi:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\ ,\\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i.\end{aligned} \tag{20.13}$$

Än så länge har vi inte någon formell konstruktion av de komplexa talen (vi sade ju "Antag att en kropp K..."). Men vi har i alla fall en klar bild av hur en kropp som innehåller lösningen till $x^2 = -1$ måste se ut. Konstruktionen är mycket enkel. Idén är (som flera gånger tidigare) att uppfatta nya tal som par av redan kända: $a + bi$ kan uppfattas som (a, b), där $a, b \in \mathbb{R}$.

(20.14) Definition. Med **komplexa tal** menar man alla par (a, b), där $a, b \in \mathbb{R}$, som adderas och multipliceras på följande sätt:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Mängden av de komplexa talen betecknas med $\mathbb{C}$. □

Beteckningen (a, b) är lite omständlig. Därför observerar man att:

$$(a, 0) + (b, 0) = (a + b, 0),$$

$$(a, 0)(b, 0) = (ab, 0),$$

dvs paren (a,0) adderas och multipliceras precis som vanliga reella tal a. Man kommer överens om att skriva $(a, 0) = a$ så att $\mathbb{R} \subset \mathbb{C}$. Därefter noterar man att $(0, 1)(0, 1) = (-1, 0) = -1$. Man betecknar $(0, 1) = i$. Nu har vi $(0, b) = (b, 0)(0, 1) = bi$ så att

$$(a, b) = (a, 0) + (0, b) = a + bi$$

och vi får våra gamla beteckningar (20.13). Det som återstår är kroppstrukturen:

(20.15) Sats. *De komplexa talen $a + bi$, där $a, b \in \mathbb{R}$ och $i^2 = -1$, bildar en kropp.*

Satsen visas lätt, men beviset tar lite tid därför att man måste kontrollera alla villkor (a) – (k) på sidan 131.

Innan vi tittar på möjligheten att gå vidare med liknande konstruktioner låt oss summera våra kunskaper. Nu kan vi säga att med ett tal menar man alltid ett komplext tal. I synnerhet kan det vara fråga om ett naturligt, helt, rationellt eller reellt tal. Med en talring (eller talkropp) menas alltid en ring (eller kropp) bestående av tal.

$\mathbb{Z}$ är den minsta talringen därför att om R är en talring så gäller att $1 \in R$ vilket ger att $1+1$, $1+1+1, ... \in R$ dvs R innehåller de naturliga talen. Vidare måste $0 \in R$ och $-x \in R$ om $x \in R$ så att R innehåller $\mathbb{Z}$. $\mathbb{Q}$ är den minsta talkroppen därför att varje kropp K innehåller $\mathbb{Z}$ och därmed också alla tal $\frac{a}{b}$, där $a, b \in \mathbb{Z}$ och $b \neq 0$, dvs $K \supseteq \mathbb{Q}$.

De reella talen bildar den största ordnade talkroppen. Låt oss först konstatuera att $\mathbb{C}$ inte är ordnad. Antag nämligen att man kan välja en mängd P av positiva element i $\mathbb{C}$. Då är $i \in P$ eller $-i \in P$. I varje fall är $(\pm i)^2 = -1 \in P$ vilket är omöjligt ty redan $1 \in P$ (se (20.2)). Man visar (men det är inte helt banalt) att om en talkropp kan ordnas så kan den inte innehålla något komplext tal $a + bi$ med $b \neq 0$ dvs den ligger i $\mathbb{R}$. I den meningen är $\mathbb{R}$ den största ordnade talkroppen.

De komplexa talen bildar den största talkroppen. I vilken mening? Man kan fråga sig som tidigare om det finns polynomekvationer, den gången med komplexa koefficienter, som inte kan lösas i komplexa talområdet. Svaret på den frågan kommer från C.F. Gauss som år 1799 visade följande sats:

(20.16) Polynomalgebrans fundamentalsats. *Varje polynomekvation av positiv grad med komplexa koefficienter har en komplex lösning.*

Satsen säger att om $p(X) = a_n X^n + ... + a_1 X + a_0$, där $a_i \in \mathbb{C}$, $n > 0$ och $a_n \neq 0$ så är $p(z) = 0$ för ett komplext tal $z \in \mathbb{C}$. Man säger också att kroppen av de komplexa talen är algebraiskt sluten. Det finns flera olika bevis för den satsen men alla kräver lite större förkunskaper [†].

Den sista satsen säger att det inte finns något vidare behov att utvidga komplexa talkroppen p g a olösbara polynomekvationer. I den meningen bildar de komplexa talen den största talkroppen. Men en lång tid innan man var medveten om detta, upptäckte man matematiska objekt som kunde användas till att beskriva och utforska naturen och som i många avseenden liknade talen. Du har säkert hört om sådana begrepp som vektor, matris, kvaternion eller tensor. Vektorer och matriser är uppsättningar av tal som också kan adderas och multipliceras på ett lämpligt sätt. De ger en möjlig generalisering av talbegreppet. Kvaternioner, som enklast kan beskrivas med hjälp av matriser, är ett annat exempel på en algebraisk struktur som ligger mycket nära de komplexa talen. Vi skall avsluta detta kapitel genom att säga några ord om just kvaternioner.

W.R. Hamilton [†] som gav en formell definition av komplexa tal i form av reella talpar försökte gå vidare med sin idé och betrakta par av komplexa tal. Han ville definiera addition och multiplikation av sådana par och möjligen få en ny kropp. Faktum är att det finns många kroppar som innehåller de komplexa talen, men de måste alltid innehålla element som inte

[†] Beviset ges i kursen "Analytiska funktioner". Ett nästan rent algebraiskt bevis i "Galoisteori".

[†] W.R. Hamilton (1805-1865).

uppfyller någon icke-trivial polynomekvation med komplexa koefficienter (t ex kroppen $\mathbb{C}(X)$ av alla rationella funktioner med komplexa koefficienter dvs alla bråk $\frac{p(X)}{q(X)}$, där $p(X)$ och $q(X)$ är polynom med komplexa koefficienter – variabeln X är inte ett nollställe till något nollskilt polynom med komplexa koefficienter). Därför är det inte längre möjligt att konstruera en kropp större än $\mathbb{C}$ vars element uppfyller polynomekvationer med komplexa koefficienter. Hamilton lyckades dock att konstruera en struktur som har den egenskapen och som uppfyller alla räknelagar för en kropp med bara ett undantag. På Brougham Bridge i Dublin där Hamilton bodde finns idag en tavla med följande text: "Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ and cut it in on a stone of this bridge". Han publicerade sina resultat år 1853. Konstruktionen av kvaternioner, som spelar en mycket viktig roll i många matematiska och fysikaliska teorier, är följande. Betrakta alla par (z_1, z_2), där z_1, z_2 är komplexa tal. Definiera

$$(z_1, z_2) + (z_1', z_2') = (z_1 + z_1', z_2 + z_2'),$$

och

$$(z_1, z_2)(z_1', z_2') = (z_1 z_1' - z_2 \bar{z}_2', z_1 z_2' + \bar{z}_1' z_2),$$

där $\bar{z} = a - bi$(z konjugat) om $z = a + bi$. Man observerar att

$$(z_1, 0) + (z_1', 0) = (z_1 + z_1', 0),$$

och

$$(z_1, 0)(z_1', 0) = (z_1 z_1', 0).$$

Detta visar att de komplexa talen kan identifieras med paren $(z, 0)$. Därför skriver vi $(z, 0) = z$. Beteckna också $(0, 1) = j$ och $(0, i) = k$. Vi har $j^2 = (0, 1)(0, 1) = (-1, 0) = -1$ och $k^2 = (0, i)(0, i) = (-1, 0) = -1$. Dessutom har vi $(0, c + di) = (0, c) + (0, di) = (c, 0)(0, 1) + (d, 0)(0, i) = cj + dk$. Därför kan vi skriva:

$$q = (a + bi, c + di) = (a + bi, 0) + (0, c + di) = a + bi + cj + dk.$$

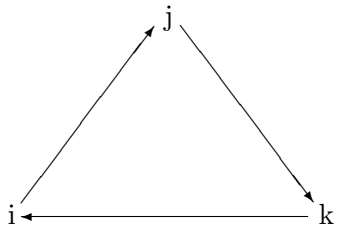
Detta är en typisk kvaternion. Man kan kontrollera direkt att $ijk = -1$ (se övning 20.13).

Men för att snabbt kunna räkna med kvaternioner är det bäst att kontrollera följande multiplikationsregler:

ij = -ji = k,

jk = -kj = i,

ki = -ik = j.



Vi ser att multiplikation av kvaternioner inte är kommutativ. Låt oss sammanfatta**:**

(20.17) Sats. *Alla kvaternioner $a+bi+ci+dk$, där $i^2 = j^2 = k^2 = -1$ och $ij = -ji = k$ bildar en algebraisk struktur* $\mathbf{H}$ *som uppfyller alla villkor i definitionen av en kropp med undantag av multiplikationens kommutativitet. Dessutom uppfyller varje kvaternion en andragradsekvation med reella koefficienter.*

För det sista påståendet i satsen se övning 20.14. Ibland säger man att H är en icke-kommutativ kropp, men termerna **skevkropp** eller **divisionsring** är mera vanliga. Satsen är inte svår att bevisa.

ÖVNINGAR

20.1. (a) Bestäm decimalutvecklingen av talen $\frac{3}{11}$ och $\frac{1}{7}$.

(b) Motivera att decimalutvecklingen av ett rationellt tal är periodiskt.

Ledning: Analysera divisionsalgoritmen i samband med decimalutvecklingen av bråktalen.
Anmärkning. Man visar ganska enkelt att om ett reellt tal har periodisk decimalutveckling så är det rationellt.

20.2. Låt a och b vara irrationella tal. Vad kan man säga om talen a^{-1} och ab ? Är de också irrationella?

20.3. Förklara varför $0{,}999... = 1$.

I uppgifterna 20.4 – 20.7 nedan är K en ordnad kropp och $a, b, c \in K$.

20.4. Visa att K har följande egenskaper:

(a) $a < b \Rightarrow a + c < b + c$,

(b) $a < b$ och $c > 0 \Rightarrow ac < bc$,

(c) hur förändras (b) då man ersätter $a < b$ med $a \leq b$?

20.5. Visa att relationen $a \leq b$ är en partiell ordning i K dvs

(a) $a \leq a$ (reflexivitet),

(b) $a \leq b$ och $b \leq a \Rightarrow a = b$ (antisymmetri),

(c) $a \leq b$ och $b \leq c \Rightarrow a \leq c$ (transitivitet).

20.6. Visa att

(a) $|ab| = |a||b|$,

(b) $|a + b| \leq |a| + |b|$ (triangelolikheten).

20.7. Är följande implikationer sanna eller falska?

(a) $a < b \Rightarrow a^2 < b^2$,

(b) $a < b \Rightarrow a^3 < b^3$?

20.8. (a) De naturliga talen bildar en växande följd $1 < 2 < 3$ ... . Visa att den inte är begränsad.

Ledning: Utnyttja fullständigheten av de reella talen så som den formuleras på sid. 574 i analysboken.

(b) Visa "Arkimedes princip": Om a, b är två positiva reella tal så finns det ett naturligt tal n så att $na > b$.

(c) Låt a, b vara två reella tal och låt $a < b$. Visa att det finns ett rationellt tal $\frac{m}{n}$ sådant att $a < \frac{m}{n} < b$.

Ledning: Välj n så att $n(a-b) > 1$. Välj därefter minsta m så att $m > nb$.

20.9. (a) Visa att $\sqrt{3}$ är icke-rationellt genom att jämföra antalet primfaktorer 3 i likheten $3n^2 = m^2$ till vänster och till höger.

(b) Visa på liknande sätt att $\sqrt{p}$ är icke-rationellt då p är ett godtyckligt primtal.

(c) Har Du några förslag till hur man kan generalisera (b)?

20.10. (a) Visa att talet ${}^2\log 5$ är icke-rationellt.

(b) Kan Du föreslå några andra tal i stället för 5 i (a) för att samma påstående skall gälla?

20.11. Betrakta alla par (a, b), där $a, b \in \mathbb{N}$ och visa att relationen

$$(a, b)R(c, d) \iff a + d = b + c$$

är en ekvivalensrelation. Motivera därefter att det finns en bijektion mellan ekvivalensklasserna och heltalen.

20.12. (a) När har ett rationellt tal $\frac{a}{b}$ en invers? Skriv inversen på formen $[(c, d)]$.

(b) Kontrollera att om

$$[(a, b)] = [(a', b')] \quad \text{och} \quad [(c, d)] = [(c', d')]$$

är två rationella tal ($ab' = a'b$ och $cd' = c'd$) så gäller

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \quad \text{och} \quad \frac{a}{b}\frac{c}{d} = \frac{a'}{b'}\frac{c'}{d'}$$

(dvs summan och produkten av två rationella tal beror inte på hur dessa tal representeras i form av bråk).

20.13. Skriv följande kvaternioner på formen $a + bi + cj + dk$:

(a) $(1 + i)(1 + j)$,

(b) $(i + j + k)^2$,

(c) $(1 + 2i + 3j + 4k)(1 - 2i - 3j - 4k)$,

(d) ijk.

20.14. (a) Visa att $q = 1 + i + j + k$ och $\bar{q} = 1 - i - j - k$ satisfierar ekvationen $x^2 - 2x + 4 = 0$.

(b) Visa att $q = a + bi + cj + dk$ satisfierar en kvadratisk ekvation med reella koefficienter.