LINJÄR OCH MULTILINJÄR ALGEBRA

J. Brzezinski

MATEMATISKA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
GÖTEBORG 2004

FÖRORD

Linjär algebra, vars huvuduppgift är att studera linjära rum och deras avbildningar, ger mycket viktiga tekniska medel för att hantera många matematiska objekt och är grunden för flera tillämpningar av matematiska metoder. Inte minst är linjär algebra utgångspunkten till olika generaliseringar som skapar möjligheter att studera andra matematiska strukturer t ex moduler över ringar, både algebraiska och analytiska mångfalder, gruppprepresentationer, Liealgebror och flera andra.

Kursens syfte är att ge en fördjupad förståelse av linjär algebra och bygga en grund för vidare studier inom alla områden som kräver bredare kunskaper i ämnet. Kursen börjar med en relativt kort repetition och utvidgning av valda delar av GU-kursen "Algebraiska strukturer"[†].

Den egentliga kursen börjar med en inledning till moduler över ringar som ger en möjlighet till att se linjära rum och linjära avbildningar från ett lämpligt perspektiv. Här repeteras flera grundläggande satser om linjära rum kända från inledande kurser i ämnet. Vidare fortsätter kursen med multilinjär algebra – tensorer (symmetriska, antisymmetriska), tensoralgebror, yttrealgebror, bilinjära och sesquilinjära avbildningar (kvadratiska och hermitska former) och Cliffordalgebror. I samband med olika typer av tensorer betraktas klassiska matrisgrupper (GL, SL, O, SO, U, SU osv.). Därefter studeras kanoniska former av linjära avbildningar (matriser) som t ex Jordans normalform. Några avsnitt ger en inledning till gruppprepresentationer, Liealgebror och homologisk algebra – tre områden som kan uppfattas som en långtgående utveckling och tillämpning av linjär algebrans idéer.

Kursens innehåll är grunden för flera matematiska och fysikaliska teorier och därför är kursen oumbärlig om man tänker läsa fortsättningskurser i t ex algebra, matematisk analys, teoretisk fysik och alla områden där kunskaper om linjära rum och linjära avbildningar (matriser) har betydelse.

Kursen är en fördjupnigskurs i grundutbildningen och ingår också som första delen i en grundkurs i algebra för doktorander. Fortsättningen ges som en efterföljande kurs i kommutativ algebra med början under andra läsperioden.

Huvuddelen av dessa föreläsningsanteckningar består av 11 kapitel ur en tidigare algebrakurs

[†]Kursen är tillgänglig för alla som besitter förkunskaper motsvarande denna kurs.

för doktorander som har varit ett återkommande inslag i doktorandutbildningen vartannat år mellan 1979 och 2001. Dessa kapitel har omarbetats och kompletterats för anpassa innehållet till kursens nya roll. Kapitel 9 är en omarbetad version av ett avsnitt om gruppprepresentationer i den gamla fördjupningskursen i linjär algebra. Första upplagan kom ut 2001. I denna upplaga har endast några tryckfel och formuleringar korrigerats.

J.B.

Göteborg

Augusti, 2004

KOMPENDIETS STRUKTUR

Kapitel **1, 2** och **3** är grunden för alla efterföljande kapitel.

Kapitel **4, 5, 6** och **7** borde läsas i denna ordning.

Kapitel **11** är beroende av alla tidigare kapitel utom **5**.

Kapitel **8** bygger enbart på kapitel **2** och **3**.

Kapitel **9** och **10** utnyttjar endast kapitel **1, 2** och **3**. De bör läsas i given ordning.

Kapitel **12** är väsentligen beroende av kapitel **2, 3** och **11**.

INNEHÅLL

Kapitel 1

GRUPPER

Grupper trädde in i matematiken redan under 1700-talet även om en formell definition av gruppbegreppet formulerades betydligt senare. Leonhard Euler (1707 – 1783) studerade grupper av rester vid division med heltal. Joseph Louis Lagrange (1736 – 1833) introducerade gruppbegreppet år 1770 i samband med sina studier av polynomekvationer. Dessa idéer utvecklades av Évariste Galois (1811 – 1832) som berikade gruppteorin och visade hur den kunde användas för att lösa intressanta matematiska problem. Ett av Galois berömda resultat säger att det för ekvationer av grader ≥ 5 inte finns allmänna formler som uttrycker lösningar till en godtycklig ekvation med hjälp av ekvationens koefficienter, de fyra räknesätten och rotutdragnigar. Liknande resultat visade nästan samtidigt Nils Henrik Abel (1802 – 1829). Det tog flera decennier innan den moderna definitionen av begreppet grupp gavs 1870 av Leopold Kronecker (1823 – 1891). Viktiga bidrag gjordes tidigare i arbeten av Arthur Cayley (1821 – 1895) och James Joseph Sylvester (1814 – 1897). Galois sätt att utveckla och utnyttja en abstrakt algebraisk teori för att lösa konkreta matematiska problem hade stor betydelse för utvecklingen av den moderna matematiken. Mycket tack vare Camille Jordan (1838 – 1922) blev Galois idéer tillgängliga för andra matematiker. Jordan var också först med att studera oändliga grupper. Det är mycket intressant att både Felix Klein (1849 – 1925) och den store norske matematikern Sophus Marius Lie (1842 - 1899) vistades samtidigt hos Jordan i Paris. Feliks Klein definierade i sitt berömda "Erlangenprogram" från 1872 begreppet geometri i olika 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. Dessa idéer kunde förklara likheter och olikheter mellan Euklidiska och icke-Euklidiska geometrier och ledde till helt nya teorier – t ex till relativitetsteorin som beskriver olika egenskaper i $\mathbb{R}^4$ som bevaras under verkan av Lorenzgrupper (se Kap. 6). 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 (se Kap. 10), har mycket stor betydelse både inom matematiken och fysiken. Kapitel 1 ägnas åt en kort introduktion till gruppteorin.

(1.1) Definition. Med en **grupp** menas en mängd G med en operation $\circ$ som

(0) mot två godtyckliga element $g_1, g_2 \in G$ ordnar ett element $g_1 \circ g_2 \in G$ [†] varvid

(1) $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ för $g_1, g_2, g_3 \in G$,

(2) det finns $e \in G$ så att för varje $g \in G$, $e \circ g = g \circ e = g$,

(3) till varje $g \in G$ existerar $g' \in G$ så att $g \circ g' = g' \circ g = e$.

□

Elementet e i (2) är entydigt bestämt, ty om $e' \in G$ också satisfierar (2) så är $e' \circ e = e$ och $e' \circ e = e'$ enligt (2), dvs $e = e'$. e kallas det **neutrala elementet** i G eller **enhetselementet** i G. Varje $g \in G$ bestämmer entydigt $g' \in G$ som uppfyller (3). I själva verket, om $g'' \in G$ också uppfyller (3) så är

$$g'' = e \circ g'' = (g' \circ g) \circ g'' = g' \circ (g \circ g'') = g' \circ e = g'.$$

g' kallas **inversen** till g.

(1.2) Exempel. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ och $\mathbb{C}$ är grupper då man tolkar "$\circ$" som vanlig addition av tal. I dessa grupper är $e = 0$ och $g' = -g$. De betecknas $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$.

□

(1.3) Exempel. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ är grupper då man tolkar "$\circ$" som vanlig multiplikation av tal. I dessa grupper är $e = 1$ och $g' = \frac{1}{g}$.

□

(1.4) Anmärkning. Om i en grupp $(G, \circ)$ operationen "$\circ$" betecknas med "+" (och kallas addition) så säger man att notationen är **additiv**. Då betecknar man vanligen e med 0 och g' med $-g$. Om operationen "$\circ$" skrivs som "$\cdot$" (och kallas multiplikation), så säger man att notationen är **multiplikativ**. Då betecknar man vanligen e med 1 och g' med g^{-1}. I detta fall brukar man skriva $g_1 g_2$ i stället för $g_1 \cdot g_2$.

□

(1.5) Exempel. Låt $G = GL_n(\mathbb{R})$ vara mängden av alla reella $(n \times n)$–matriser med determinant $\neq 0$. $GL_n(\mathbb{R})$ är en grupp med avseende på matrismultiplikation. Här är $e = E_n$ ($(n \times n)$ – enhetsmatrisen), och för $g = A$ är $g' = A^{-1}$ inversen till A.

[†] en (binär) operation på G är en funktion $G \times G \to G$.

□

Gruppen i sista exemplet är inte kommutativ om $n > 1$.

(1.6) Definition. En grupp $(G, \circ)$ är **abelsk** (efter Nils Henrik Abel) eller **kommutativ** om $g_1 \circ g_2 = g_2 \circ g_1$ för godtyckliga $g_1, g_2 \in G$.

□

(1.7) Exempel. Låt X vara en mängd och låt G bestå av en-entydiga funktioner som avbildar X på hela X[†]. Antag att sammansättningen $f \circ g \in G$ för godtyckliga funktioner $f, g \in G$, $f^{-1} \in G$ då $f \in G$, och $I \in G$, där $I(x) = x$ för $x \in X$ (den identiska funktionen). Då är $(G, \circ)$ en grupp. Associativiteten gäller för sammansättningen av helt godtyckliga funktioner: $X \xrightarrow{f} X \xrightarrow{g} X \xrightarrow{h} X$ ger att

$$\begin{aligned} [(f \circ g) \circ h](x) &= (f \circ g)(h(x)) = f(g(h(x))), \\ [f \circ (g \circ h)](x) &= f(g \circ h)(x)) = f(g(h(x))), \end{aligned}$$

för varje $x \in X$ dvs $(f \circ g) \circ h = f \circ (g \circ h)$.

□

Gruppen G i sista exemplet kallas för en **transformationsgrupp** av X (eller en **permutationsgrupp** av X då X är ändlig). Om $X = \{1, 2, \ldots, n\}$ och G består av alla bijektiva funktioner på X så betecknas G med S_n och kallas den **symmetriska gruppen** av grad n. Om X är en figur i planet eller rymden och G består av alla funktioner (= avbildningar) som bevarar avståndet så kallas G **symmetrigruppen** av X (se vidare Övn. 6).

(1.8) Definition. Antalet element i en ändlig grupp G kallas för gruppens **ordning** och betecknas med $|G|$ eller $o(G)$. Om G har oändligt många element så säger man att G är oändlig eller har **oändlig ordning**. Man skriver då $|G| = \infty$.

□

(1.9) Definition. Om $(G, \circ)$ är en grupp och H är en delmängd till G vars element bildar en grupp m a p operationen "$\circ$" så säger man att $(H, \circ)$ är en **delgrupp** (eller **undergrupp**) till $(G, \circ)$ (kortare: H är en delgrupp till G).

□

[†] $f : X \to X$ är **en-entydig** om $x_1 \neq x_2$ ger $f(x_1) \neq f(x_2)$. Man säger också att f är **injektiv**. $f : X \to X$ är **på hela** X om $\forall_{x' \in X} \exists_{x \in X} f(x) = x'$. Man säger också att f är **surjektiv**. En funktion $f : X \to X$ som är surjektiv och injektiv kallas **bijektiv**.

(1.10) Proposition. *Om $H \subseteq G$, så är H en delgrupp till G då och endast då*

(a) $h_1, h_2 \in H \Rightarrow h_1 \circ h_2 \in H$,

(b) $e \in H$,

(c) $h \in H \Rightarrow h^{-1} \in H$,

eller kortare:

(abc) $H \neq \emptyset$ *och* $h_1, h_2 \in H \Rightarrow h_1^{-1} \circ h_2 \in H$.

Ett mycket enkelt bevis av (1.10) lämnar vi som övning.

(1.11) Exempel. $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$; $\mathbb{Z}^+ \subset \mathbb{Q}^+ \subset \mathbb{R}^+ \subset \mathbb{C}^+$.

□

(1.12) Cykliska grupper. Om $g \in G$ och n är ett naturligt tal ≥ 1, så definieras

$$g^n = \underbrace{gg\ldots g}_{n \text{ stycken}}, \quad g^{-n} = (g^{-1})^n \quad \text{och} \quad g^0 = e.$$

Med dessa definitioner är $g^m g^n = g^{m+n}$ (kontrollera!). Alla potenser g^n, $n \in \mathbb{Z}$ bildar en delgrupp till G. Denna betecknas med $< g >$ och kallas den **cykliska gruppen** genererad av g. Om $H =< g >$ så säger man att g är en **generator** för H. Ibland betecknas en cyklisk grupp av ordningen n med C_n.

(1.13) Exempel. (a) Låt $G = \mathbb{C}^*$ och $g = i$. Då är $< i >= \{1, -1, i, -i\}$ ty $i^4 = 1$, vilket implicerar $i^{n+4} = i^n$ för $n \in \mathbb{Z}$. Detta förklarar termen "cyklisk".

(b) Om $G = \mathbb{Z}$ (m a p taladdition), så är $\mathbb{Z} =< 1 >$.

(c) Låt $G = U_n = \{z \in \mathbb{C} : z^n = 1\}$ vara gruppen av alla n-te enhetsrötter (m a p talmultiplikation). Då är $U_n =< \varepsilon >$, där $\varepsilon = e^{\frac{2\pi i}{n}}$.

□

(1.14) Exempel. Låt $n > 0$ vara ett heltal och låt $[a]_n$ (eller kortare $[a]$) beteckna resten av a vid division med n. Observera att $[x]_n = [y]_n$ är ekvivalent med att $n|x - y$ (ofta skriver man $x \equiv y \pmod{n}$ och säger att "x **är kongruent med** y **modulo** n"). Som bekant finns det heltal q och r sådana att

$$a = qn + r \quad \text{där} \quad 0 \leq r < n.$$

Vi skriver $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ för mängden av alla rester vid division med n. Nu definierar vi

$$[a]_n \oplus [b]_n = [a+b]_n.$$

För att kontrollera att den definitionen är korrekt måste man veta att $[a]_n = [a']_n$ och $[b]_n = [b']_n$ ger $[a+b]_n = [a'+b']_n$. Men detta är klart ty $n|a-a'$ och $n|b-b'$ ger att $n|(a+b)-(a'+b')$. $(\mathbb{Z}_n, \oplus)$ är en abelsk grupp: $e = 0$ är neutrala elementet och $n - r$ är motsatta elementet till r då $r \neq 0$. Associativiteten visas direkt:

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

så att $[a]_n \oplus ([b]_n \oplus [c]_n) = ([a]_n \oplus [b]_n) \oplus [c]_n$. Det är klart att $[a]_n \oplus [b]_n = [b]_n \oplus [a]_n$ så att $(\mathbb{Z}_n, \oplus)$ är abelsk. Man kan också definiera operationen $\odot$ på $\mathbb{Z}_n$ genom

$$[a]_n \odot [b]_n = [ab]_n.$$

Med denna operation är $\mathbb{Z}_n$ inte en grupp (om $n \neq 1$). Se dock Övn. 8.

□

I fortsättningen betecknar H och G grupper. Notationen är som regel multiplikativ.

(1.15) Definition. Låt $H \subseteq G$ och $g \in G$. Mängden

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

kallas en **högersidoklass** till H i G.

□

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

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

(1.17) Exempel. (a) Låt $G = \mathbb{C}^*$ och $H = U = \{z \in \mathbb{C} : |z| = 1\}$. Vi har

$$z' \in Uz \Leftrightarrow z'z^{-1} \in U \Leftrightarrow |z'z^{-1}| = 1 \Leftrightarrow |z'| = |z|.$$

Alltså består (höger)sidoklassen Uz av alla komplexa tal med beloppet lika med $|z|$.

(b) Låt $G = GL_n(\mathbb{R})$ (se (1.5)) och $H = SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$. Nu har vi

$$B \in HA \Leftrightarrow \det(BA^{-1}) = 1 \Leftrightarrow \det B = \det A.$$

Alltså består högersidoklassen HA av alla matriser ur G med determinanten lika med det A.

(c) Låt $G = \mathbb{Z}$ (med addition), $H =< 5 >= \{5k : k \in \mathbb{Z}\}$. Vi har:

$$b \in H + a \Leftrightarrow b - a \in H \Leftrightarrow 5|b - a \Leftrightarrow [b]_5 = [a]_5.$$

Alltså är (höger)sidoklassen $< 5 > +a$ identisk med mängden av alla heltal b som är lika med a modulo 5. Sidoklasserna är:

$$< 5 >, \quad < 5 > +1, \quad < 5 > +2, \quad < 5 > +3, \quad < 5 > +4,$$

ty det finns exakt 5 olika rester $[a]_5$.

□

Exemplen visar att sidoklasserna bildar en partition av G dvs en uppdelning av G i parvis disjunkta mängder. Vi skall bevisa den observationen:

(1.18) Proposition. *(a)* $g \in Hg$.

(b) $Hg' = Hg \Leftrightarrow g' \in Hg$.

(c) $g \in Hg_1 \cap Hg_2 \Rightarrow Hg_1 = Hg_2$.

Anmärkning. (a) säger att varje element $g \in G$ tillhör minst en sidoklass; (c) säger att g tillhör högst en sidoklass. Detta betyder att sidoklasserna Hg bildar en partition av G – se vidare Appendix A. (b) säger att varje element i Hg definierar (eller representerar) just denna sidoklass. □

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

(b) Om $Hg' = Hg$ så har man enligt (a) $g' \in Hg' = Hg$. Om $g' \in Hg$ så är $g' = hg$ för ett $h \in H$. Alltså är $h'g' = h'hg \in Hg$ för varje $h' \in H$ dvs $Hg' \subseteq Hg$. Men även $g = h^{-1}g' \in Hg'$ så att av symemtriskäl är $Hg \subseteq Hg'$ dvs $Hg' = Hg$.

(c) $g \in Hg_1 \cap Hg_2 \Rightarrow Hg = Hg_1$ och $Hg = Hg_2$ (enligt (b)) så att $Hg_1 = Hg_2$. □

(1.19) Proposition. *Låt H vara en ändlig delgrupp till G. Då är $|Hg| = |H|$ för varje $g \in G$.*

Bevis. $h \mapsto hg$ är en en-entydig avbildning av H på hela Hg ty $h_1g = h_2g$ implicerar att $h_1 = h_2$ (dvs $h_1 \neq h_2 \Rightarrow h_1g \neq h_2g$). Alltså ger $H = \{h_1, h_2, \ldots, h_m\}$ att $Hg = \{h_1g, h_2g, \ldots, h_mg\}$ med alla h_ig olika. □

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

Bevis. Låt $H \subseteq G, |G| = n$ och $|H| = m$. Låt i vara antalet högersidoklasser till H i G. Sidoklasserna bildar en partition av G enligt (1.18). Varje sidoklass har m element enligt (1.19). Alltså är $n = i \cdot m$. □

(1.21) Vänstersidoklasserna $gH = \{gh : h \in H\}$ till H i G har exakt samma egenskaper som högersidoklasserna. Man kan också bevisa Lagranges sats med deras hjälp. Observera dock att en vänstersidoklassen gH behöver inte vara lika med högersidoklassen Hg (se vidare exempel 1.27 (c)).

(1.22) Följdsats. *Antalet vänstersidoklasser till H i G är lika med antalet högersidoklasser till H i G.*

Bevis. Enligt bevis för (1.20) (i dess vänster-version) är bägge talen lika med $|G|/|H|$. □

(1.23) Definition. Antalet vänster– eller högersidoklasser till H i G kallas **index** för H i G och betecknas med $(G : H)$.

□

(1.24) Definition. Med **ordningen av** $g \in G$ menas ordningen av den cykliska grupp $< g >$ som g genererar. Ordningen av g betecknas med $o(g)$.

□

I samband med den definitionen se också Övn. 2. Definitionen implicerar omedelbart:

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

(1.26) Definition. Man säger att H är en **normal undergrupp** till G om det för varje $g \in G$ gäller att $gH = Hg$. Då skriver man $H \lhd G$.

□

(1.27) Exempel. (a) Varje undergrupp till en abelsk grupp är normal.

(b) Låt $G = GL_n(\mathbb{R})$ och $H = SL_n(\mathbb{R})$ (se (1.17)(b)). Vi vet ((1.17)(b)) att varje högersidklass HA består av alla $B \in G$ sådana att $\det B = \det A$. På samma sätt kan vi beskriva AH:

$$\begin{aligned} B \in AH &\Leftrightarrow A^{-1}B \in H \quad \text{(vänstervarianten av (1.16)(c))} \\ &\Leftrightarrow \det(BA^{-1}) = 1 \Leftrightarrow \det B = \det A. \end{aligned}$$

Alltså är $AH = HA$.

(c) Låt $G = S_3$ vara gruppen av alla permutationer av $\{1, 2, 3\}$. G kan beskrivas som gruppen av alla avbildningar av planet som bevarar avståndet och en given liksidig triangel – se fig.1. Låt $H = \{I, s_1\}$ där

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{och} \quad s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

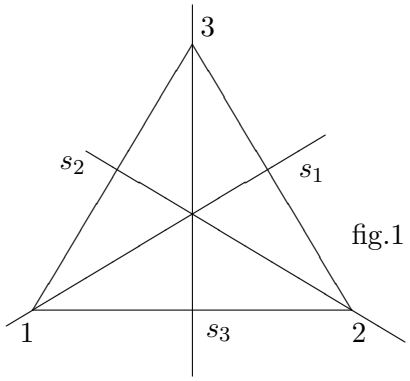


fig.1

H är en icke-normal delgrupp till G, ty t ex $s_2H \neq Hs_2$, där $s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. I själva verket,

$$s_2H = \{s_2, s_2 \circ s_1\} \neq \{s_2, s_1 \circ s_2\} = Hs_2$$

ty $s_2 \circ s_1 \neq s_1 \circ s_2$. (Vi har $s_1 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $\quad s_2 \circ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$).

□

(1.28) Proposition. *Villkoren:*

(*a*) $gH = Hg$ *för varje* $g \in G$,

(*b*) $gHg^{-1} \subseteq H$ *för varje* $g \in G$

är ekvivalenta.

Bevis. Implikationen (a) ⇒ (b) är klar. Omvänt har man $gHg^{-1} \subseteq H \Leftrightarrow gH \subseteq Hg$. Den inklusionen gäller för varje $g \in G$. Alltså gäller den också för g^{-1} dvs $g^{-1}H \subseteq Hg^{-1}$, vilket ger $Hg \subseteq gH$. Tillsammans med $gH \subseteq Hg$ får man $gH = Hg$. □

(1.29) Definition. Låt G vara en grupp och A, B två delmängder till G. Produkten av A och B definieras som mängden

$$AB = \{ab : a \in A \quad \text{och} \quad b \in B\} \, (\text{additivt} : A + B = \{a + b : a \in A \quad \text{och} \quad b \in B\}).$$

□

Det är klart att $(AB)C = A(BC)$ då A, B, C är tre delmängder till G. Notera att i fall $A = \{g\}$ och $B = H$ (en delgrupp till G) är $AB = gH$. Notera också att $HH = H$.

(1.30) Proposition. *Om H är en normal undergrupp så bildar alla sidoklasser till H i G en grupp med avseende på multiplikation av delmängder till G. Neutrala elementet är H, inversen till gH är $g^{-1}H$.*

Bevis. Om $A = gH$ och $B = g'H$ så är $AB = (gH)(g'H) = g(Hg')H = g(g'H)H = gg'HH = gg'H$ dvs det är en sidoklass igen. Multiplikationen är associativ. Vidare är $e = H$ enhetselementet. Inversen till gH är $g^{-1}H$, ty $gHg^{-1}H = gg^{-1}HH = H$. □

(1.31) Definition. Gruppen definierad i (1.30) betecknas med G/H och kallas **kvotgruppen** av G modulo (eller genom) H.

□

(1.32) Exempel. Låt $G = \mathbb{Z}$ (som vanligt med taladdition) och $H =< 5 >$. Vi vet (se (1.17)(c)) att sidoklasserna är $H, 1 + H, 2 + H, 3 + H, 4 + H$. Vi skall beteckna dem med $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$. $G/H = \mathbb{Z}/ < 5 >$ består av 5 element och har grupptabellen:

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

(t ex är $2 + H + 3 + H = 2 + 3 + H + H = 5 + H = H$ ty $5 \in H$).

□

(1.33) Definition. En funktion $f : G \to G'$ kallas en **homomorfism** om

$$f(g_1g_2) = f(g_1)f(g_2).$$

för alla $g_1, g_2 \in G$.

□

Lägg märke till att till vänster multipliceras i G och till höger i G'.

(1.34) Exempel. (a) Låt $G = \mathbb{R}^*_{>0}$ (de positiva reella talen med multiplikation), $G' = \mathbb{R}^+$ och $f(x) = \ln x$. Då är $f(x_1x_2) = \ln x_1x_2 = \ln x_1 + \ln x_2 = f(x_1) + f(x_2)$ dvs $f : G \to G'$ är en homomorfism.

(b) Låt $G = \mathbb{C}^*, G' = \mathbb{R}^*$ och $f(z) = |z|$. Då är $f(z_1z_2) = |z_1z_2| = |z_1||z_2| = f(z_1)f(z_2)$ dvs $f : \mathbb{C}^* \to \mathbb{R}^*$ är en homomorfism.

(c) Låt $G = \mathbb{R}^+$, $G' = U = \{z \in \mathbb{C}^* : |z| = 1\}$ och $f(x) = e^{ix}$. Då är $f(x_1 + x_2) = e^{i(x_1+x_2)} = e^{ix_1}e^{ix_2} = f(x_1)f(x_2)$ dvs $f : \mathbb{R}^+ \to U$ är en homomorfism.

(d) Låt G/N vara en kvotgrupp av G (N är en normal undergrupp till G) och låt $f : G \to G/N$ vara den funktion som avbildar g på gN. Då är f en homomorfism ty $f(g_1g_2) = g_1g_2N = g_1Ng_2N = f(g_1)f(g_2)$. f kallas den **naturliga surjektionen**.

□

(1.35) Proposition. *Om $f : G \to G'$ är en homomorfism så är $f(e) = e'$ och $f(g^{-1}) = f(g)^{-1}$ (e och e' är de neutrala elementen i G resp. G').*

Bevis. $f(e) = f(ee) = f(e)f(e)$ dvs $f(e) = e'$; $e' = f(e) = f(gg^{-1}) = f(g)f(g^{-1})$ dvs $f(g^{-1}) = f(g)^{-1}$. □

(1.36) Definition. Man säger att en homomorfism $f : G \to G'$ är en **isomorfism** om f avbildar en-entydigt G på hela G'. Om G och G' är isomorfa (dvs en isomorfism f existerar) så skriver man $G \cong G'$. Om $G = G'$ kallas f en **automorfism**. Om f är surjektiv (dvs på hela G') så kallas den **epimorfism**, och om den är injektiv (dvs en-entydig) så kallas den **monomorfism**.

□

Bland exemplen i (1.34) är (a) en isomorfism (inversen $f^{-1}(y) = e^y$).

(1.37) Definition. Med **kärnan** till en homomorfism $f : G \to G'$ menar man mängden av alla element i G vars bild är enhetselementet i G'. Kärnan betecknas med $\mathrm{Ker}f$. Alltså

$$\mathrm{Ker}f = \{g \in G : f(g) = e'\}.$$

Bilden $f(G)$ betecknas ofta $\mathrm{Im}f$[†].

□

(1.38) Proposition. *Låt $f : G \to G'$ vara en homomorfism.*

(*a*) $\mathrm{Ker}f$ *är en normal undergrupp till G.*

(*b*) $G/\mathrm{Ker}f \cong \mathrm{Im}f$*, där en isomorfism är given då $g(\mathrm{Ker}f)$ avbildas på $f(g)$.*

Bevis. (a) Om $g_1, g_2 \in \mathrm{Ker}f$, så $f(g_1) = f(g_2) = e'$. Alltså är $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = e'$ dvs $g_1 g_2^{-1} \in \mathrm{Ker}f$. Men $e \in \mathrm{Ker}f$, så att enligt (1.10) är $\mathrm{Ker}f$ en delgrupp till G. Den är normal ty om $g \in G$ och $n \in \mathrm{Ker}f$, så är $gng^{-1} \in \mathrm{Ker}f$. I själva verket, $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = e'$.

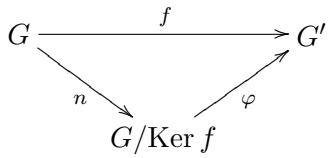
(b) Vi har $g' \in g(\mathrm{Ker}f) \Leftrightarrow g^{-1}g' \in \mathrm{Ker}f \Leftrightarrow f(g^{-1}g') = e' \Leftrightarrow f(g') = f(g)$ dvs sidoklassen $g(\mathrm{Ker}f)$ består av alla element i G vars bild i G' är $f(g)$. Nu definierar vi $\varphi : G/\mathrm{Ker}f \to \mathrm{Im}f$ genom att ordna mot sidoklassen $g(\mathrm{Ker}f)$ bilden av ett godtyckligt element i denna, säg $f(g)$ (alla element har samma bild!) dvs $\varphi(g\mathrm{Ker}f) = f(g)$. På det sättet avbildas olika sidoklasser på olika element i $\mathrm{Im}f$ och varje element i $\mathrm{Im}f$ är bilden av en sidoklass.

Vidare är

$$\varphi(g_1\mathrm{Ker}f\, g_2\mathrm{Ker}f) = \varphi(g_1 g_2 \mathrm{Ker}f) = f(g_1 g_2) = f(g_1)f(g_2) = \varphi(g_1\mathrm{Ker}f)\varphi(g_2\mathrm{Ker}f),$$

dvs φ är en-entydig homomorfism av $G/\mathrm{Ker}f$ på hela $\mathrm{Im}f$ dvs en isomorfism. □

Del (b) av Prop. (1.38) kallas ofta **Huvudsatsen om grupphomomorfismer**. Den kan formuleras på följande sätt: Det finns ett kommutativt diagram



(dvs $f = \varphi n$) sådant att n är den naturliga surjektionen (se (1.34)(d)) och φ är en monomorfism. Man kan också uttrycka det så att varje homomorfism $f : G \to G'$ kan faktoriseras i produkt (= skrivas som sammansättning) av den naturliga surjektionen $n : G \to G/\mathrm{Ker}f$ och en monomorfism $\varphi : G/\mathrm{Ker}\, f \to G'$.

[†] "Ker"="Kernel", "Im"="Image".

(1.39) Exempel. (a) Låt $f : \mathbb{Z} \to \mathbb{Z}_n$ där $f(a) = [a]_n$. Då är f en grupphomomorfism ty

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

Vi har Ker$f = \{a \in \mathbb{Z} : f(a) = [a]_n = [0]_n\} =< n >$ och Im$f = \mathbb{Z}_n$.
Alltså är $\mathbb{Z}/ < n > \cong \mathbb{Z}_n$ och en isomorfism är given då $< n > +a$ avbildas på $[a]_n$

(b) Låt $f : \mathbb{R}^+ \to \mathbb{C}^*$, $f(x) = e^{2\pi ix}$. Då är

$$f(x_1 + x_2) = e^{2\pi i(x_1+x_2)} = e^{2\pi ix_1}e^{2\pi ix_2} = f(x_1)f(x_2)$$

dvs f är en grupphomomorfism. Här är Ker$f = \{x \in \mathbb{R} : f(x) = e^{2\pi ix} = 1\} = \mathbb{Z}$ och Im$f = \{e^{2\pi ix}, x \in \mathbb{R}\} = U$, där $U = \{z \in \mathbb{C} : |z| = 1\}$. Enligt homomorfismsatsen (1.38) är $\mathbb{R}/\mathbb{Z} \cong U$ och en isomorfism är given då $\mathbb{Z} + x$ avbildas på $e^{2\pi ix}$.

□

Vi avslutar detta kapitel med några resultat och kommentarer om olika typer av grupprepresentationer och deras betydelse i samband med datorberäkningar i grupper. Ett mycket gammalt resultat som kommer från Artur Cayley säger att varje ändlig grupp kan beskrivas som en permutationsgrupp. Mera exakt:

(1.40) Cayleys sats. *Varje ändlig grupp G med n element är isomorf med en delgrupp till den symmetriska gruppen S_n.*

Innan vi visar satsen betraktar vi ett exempel:

(1.41) Exempel. Låt $G =< g >$, $g^4 = e$, vara en cyklisk grupp med 4 element. Vi numrerar gruppens element e, g, g^2, g^3 med respektive $1, 2, 3, 4$. Varje rad i grupptabellen

	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

svarar mot en permutation av $1, 2, 3, 4$ (som numrerar gruppelementen):

$$e \mapsto \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix},\ g \mapsto \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix},\ g^2 \mapsto \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix},\ g^3 \mapsto \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,2\,3 \end{pmatrix}.$$

□

Bevis av Cayleys sats Beviset följer konstruktionsmetoden i exemplet ovan. Låt $G = \{g_1, g_2, \ldots, g_n\}$. Låt $\varphi_g(x) = gx$ då $x \in G$. Funktionen φ_g har som sin värdemängd alla element $gg_1, gg_2, \ldots, gg_n$ (i den rad av grupptabellen för G som svarar mot g). Mot g ordnar vi permutationen

$$g \mapsto \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ gg_1 & gg_2 & \ldots & gg_n \end{pmatrix}$$

Vi kan identifiera elementet g_i med talet i och ersätta $gg_i = g_{p_i}$ med p_i för ett lämpligt index p_i. Då representerar vi g med en permutation av talen $1, 2, \ldots, n$:

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

Det är klart att varje g definierar en permutation (den svarar mot en rad i grupptabellen). Vi kontrollerar också att funktionen $\Phi(g) = \varphi_g$ är en injektiv grupphomomorfism av G i den symmetriska gruppen S_n. Olika g ger olika permutationer (olika rader i grupptabellen) och

$$\Phi(gg')(x) = gg'x = \phi_g(g'x) = \phi_g(\phi_{g'}(x)) = \phi_g\phi_{g'}(x) = \Phi(g)\Phi(g')(x),$$

dvs $\Phi(gg') = \Phi(g)\Phi(g')$. □

I historiskt perspektiv hade Cayleys sats en mycket stor betydelse – den visar att alla ändliga grupper kan representeras som permutationsgrupper och studeras som delgrupper till de symmetriska grupperna S_n. Rent praktiskt ger den beskrivningen inte så stora fördelar, men permutationsbeskrivning av en grupp är mycket lämplig som inmatning i datorprogram. Flera kända programpaket tillåter en sådan beskrivning av grupper. T ex i MAPLE ger kommandot

$$> G := \text{permgroup}(3, \{a = [1, 2], b = [1, 2, 3]\});$$

den symmetriska gruppen S_3 dvs symmetrigruppen av en liksidig triangel. Kommandot säger att G är en delgrupp till S_3 och genereras av permutationerna a (en symmetri) och b (vridningen 120°) dvs består av alla produkter av faktorer som är lika med a eller b.

En mycket viktig generalisering av permutationsrepresentationer är representationer av gruppelementen med hjälp av matriser. Observera att varje permutation kan tolkas som en matris vars element är 0 eller 1 varvid en etta förekommer exakt en gång i varje rad och i varje kolonn. Matrisrepresentationer som utgör ett oerhört viktigt redskap i undersökningar av grupper diskuterar vi i ett senare kapitel.

Från både teoretisk och praktisk synpunkt är det viktigt att kunna beskriva grupper på ett kompakt sätt. Ett exempel är cykliska grupper: $G =< a >$, där a satisfierar relationen $a^n = e$. Den metoden kan generaliserars då man tillåter flera generatorer (som a) och flera relationer (som $a^n = e$). Vi antar följande definition:

(1.42) Definition. Låt G vara en grupp. Man säger att $a_1, \ldots, a_t$ **genererar** G om varje element i G kan skrivas som produkt av potenser av dessa element. Man säger då att G är **ändligt genererad** och man skriver $G =< a_1, \ldots, a_t >$. Med en **relation** mellan generatorerna menar man varje likhet $f(a_1, \ldots, a_t) = g(a_1, \ldots, a_t)$, där f och g är monom i icke–kommuterande variabler $X_1, \ldots, X_t$.

□

En cyklisk grupp av ordningen n har en generator och en relation: $G =< a >$ och $a^n = e$. Som ett annat exempel betrakta gruppen $G = U_2 \times U_2$, där $U_2 = \{\pm 1\}$ med multiplikation. Elementen $a = (1, -1)$ och $b = (-1, 1)$ genererar denna grupp dvs $G =< a, b >$ (observera att gruppen inte är cyklisk). Som relationer har vi t ex $a^2 = e, b^2 = e$ och $ab = ba$ $(e = (1, 1))$.

Ofta är man intresserad av minimala uppsättningar av relationer $f_1 = g_1, \ldots, f_r = g_r$ sådana att varje annan relation för generatorerna $a_1, \ldots, a_t$ av G är en konsekvens av dessa (och gruppaxiomen). Rent allmänt är det inte alltid lätt att bestämma en minimal generatoruppsättning (inga "onödiga" generatorer) eller avgöra om en generatoruppsättning består av det minsta möjliga antalet av gruppelement. Samma problem gäller relationer mellan generatorerna. Det finns flera programpaket som hjälper lösa dessa problem för grupper av måttlig storlek. T ex i MAPLE ger kommandot

$$> G := \text{grelgroup}(\{a, b\}, \{[a, a, a], [b, b], [b, a, 1/b, 1/a, 1/a]\});$$

en beskrivning av en grupp $G =< a, b >$ med två generatorer a och b samt med tre relationer $a^3 = e$, $b^2 = e$ och $bab^{-1}a^{-2} = e$ (dvs $ba = a^2b$). Symmetrigruppen av en liksidig triangel kan i själva verket beskrivas på detta sätt (a är en vridning, b är en spegling). Observera att när man skriver ut relationer av typen $a^k = e$ så menar man alltid att a har ordningen k (ej en äkta delare till k).

ÖVNINGAR

1.1. Låt K vara en delkropp till de komplexa talen (t ex $K = \mathbb{R}$ eller $\mathbb{C}$) och låt $M_n(K)$ vara mängden av alla $(n \times n)$-matriser $A = [a_{ij}]$ med $a_{ij} \in K$. Låt $A^t = [a_{ji}]$ beteckna den transponerade matrisen till A och $\bar{A} = [\bar{a}_{ij}]$ den konjugerade matrisen till A. Visa att följande matriser bildar en grupp m a p matrismultiplikation:

(a) $GL_n(K) = \{A \in M_n(K) : \det A \neq 0\}$ (fulla linjära gruppen),

(b) $SL_n(K) = \{A \in GL_n(K) : \det A = 1\}$ (speciella linjära gruppen),

(c) $O_n(K) = \{A \in M_n(K) : AA^t = E\}$ (ortogonala gruppen),

(d) $SO_n(K) = \{A \in O_n(K) : \det A = 1\}$ (speciella ortogonala gruppen),

(e) $U_n(K) = \{A \in M_n(K) : A\bar{A}^t = E\}$ (unitära gruppen),

(f) $SU_n(K) = \{A \in U_n(K) : \det A = 1\}$ (speciella unitära gruppen),

(g) $T_n(K) = \{A \in GL_n(K) : a_{ij} = 0 \quad \text{då} \quad i > j\}$ (övre triangulära gruppen),

(h) $N_n(K) = \{A \in T_n(K) : a_{ii} = 1\}$ (övre unitriangulära gruppen; matriser av denna typ kallas unipotenta),

(i) $D_n(K) = \{A \in GL_n(K) : a_{ij} = 0 \quad \text{då} \quad i \neq j\}$ (diagonala gruppen).

1.2. Låt G vara en grupp och $g \in G$. Låt $n > 0$ vara ett heltal sådant att $g^n = e$ och $g^m \neq e$ då $0 < m < n$. Visa att $< g >= \{e, g, \ldots, g^{n-1}\}$.

Anmärkning. Uppgiften visar att ordningen av g kan definieras som det minsta naturliga talet n sådant att $g^n = e$ och ∞ om n inte existerar.

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

1.4. Visa att en delgrupp till en cyklisk grupp är cyklisk.

1.5. Visa att

(a) en cyklisk grupp med n element är isomorf med $\mathbb{Z}_n$,

(b) en oändlig cyklisk grupp är isomorf med $\mathbb{Z}$.

1.6. Skriv ut grupptabeller för symmetrigrupper (se (1.7)) av:

(a) en liksidig triangel,

(b) en kvadrat,

(c) en rektangel som inte är en kvadrat.

Ge en beskrivning av alla dessa grupper med hjälp av generatorer och relationer.

Anmärkning. Om X är en regelbunden n-hörning så betecknas dess symmetrigrupp med D_n och kalls **dihedrala gruppen**. Gruppen i (c) kallas **Kleins fyragrupp** och betecknas med V_4.

1.7. (a) Visa att om $f : G \to G'$ är en homomorfism och $g \in G$ så är $o(f(g)) \mid o(g)$. Om f är en isomorfism så är $o(g) = o(f(g))$.

(b) Avgör om följande par av grupper är isomorfa:

(b)$_1$ $\mathbb{Z}_4$ och V_4, (b)$_2$ $\mathbb{Q}^*$ och $\mathbb{Q}^+$, (b)$_3$ $\mathbb{R}^*_{>0}$ och $\mathbb{R}^+$,

1.8. Visa att alla rester vid division med n som är relativt prima med n bildar en grupp under multiplikation modulo n. Den betecknas med $\mathbb{Z}_n^*$ och dess ordning med $\varphi(n)$. Funktionen $\varphi(n)$ kallas **Eulers funktion**.

1.9. Antalet icke-isomorfa grupper av nedan givna ordningar ges av tabellen:

$o(G)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
antalet G	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5

Visa detta då $o(G) \leq 7$.

1.10. Beskriv alla undergrupper till

(a) S_3, (b) V_4, (c) $\mathbb{Z}_6$.

1.11. (a) Visa att en oändlig grupp har oändligt många delgrupper.

(b) G har endast två delgrupper (vilka?) då och endast då $|G| = p, p$ ett primtal.

1.12. En grupp kallas **enkel** om den saknar icke-triviala normala delgrupper. Visa att en abelsk grupp är enkel då och endast då dess ordning är 1 eller ett primtal.

Anmärkning. Icke-abelska enkla grupper spelar en mycket viktig roll i gruppteorin. T ex är grupper A_n av alla jämna permutationer av talen $1, 2, \ldots, n$ enkla om $n \geq 5$, vilket bl a implicerar att lösningar till polynomekvationer av grader ≥ 5 inte kan uttryckas på liknande sätt som lösningar till ekvationer av lägre grader (se inledningen till detta kapitel och definitionen av en lösbar grupp i Övn. 15). I början av 1980-talet avslutades ett mycket omfattande och svårt forskningsprojekt som tog mer än 150 år att genomföra och engagerade hundratals matematiker – klassifikationen av alla enkla grupper. Man visste att enkla grupper bildar ett antal oändliga serier (som t ex A_n, $n \geq 5$) och att dessutom finns ett ändligt antal s k **sporadiska enkla grupper** som inte ingår i någon av dessa serier. Problemet med att klassificera alla sporadiska grupper visade sig vara oerhört svårt. År 1981 avslutades klassifikationen med en konstruktion av den största enkla gruppen – "Monstergruppen" vars ordning är $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 10^{54}$. Fortfarande publiceras delar av lösningen i arbeten som tillsammans omfattar flera tusen sidor (cirka 10 000 enligt insatta personer).

1.13. Om G_1, G_2 är grupper så bildar alla par (g_1, g_2), där $g_i \in G_i$ en grupp m a p koordinatvis multiplikation. Den betecknas $G_1 \times G_2$ och kallas **produkten** av G_1 och G_2. På samma sätt definieras $G_1 \times \ldots \times G_n$ då $n \geq 2$. Visa att

(a) $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$,

(b) $\mathbb{C}^* \cong \mathbb{R}^*_{>0} \times U$, där $U = \{z \in \mathbb{C}^* : |z| = 1\}$

Anmärkning. Varje ändlig abelsk grupp är isomorf med en produkt av cykliska grupper vars ordningar är primtalspotenser. En mera allmän sats som kallas "Huvudsatsen om ändligt genererade abelska grupper" säger att varje sådan grupp är isomorf med en

produkt av cykliska grupper – ändliga vars ordningar är primtalspotenser och oändliga (om gruppen är oändlig). Denna sats som också ger en mycket mera exakt information om den direkta produktens faktorer bevisas i ett senare kapitel om moduler över huvudidealringar.

1.14. Låt G vara en transformationsgrupp av en mängd X. Om $g \in G$ och $x \in X$ så skriver vi gx i stället för $g(x)$. Mängden $Gx = \{gx : g \in G\}$ kallas **banan** av x och $St(x) = \{g \in G : gx = x\}$ kallas **stabilisatorn** av x. Låt G vara en ändlig grupp. Visa att

(a) $St(x)$ är en delgrupp till G,

(b) $|Gx| = (G : St(x))$,

(c) om $gx = x'$ så är $St(x') = gSt(x)g^{-1}$,

(d) olika banor är disjunkta och $|X| = \sum_x (G : St(x))$, där man summerar över representanter ur olika banor för G.

1.15. Låt G vara en grupp och $X = G$. Låt $G \times X \to X$ vara given genom $(g, x) \mapsto gxg^{-1}$. Om x_1, x_2 tillhör samma bana för G (se Övn. 14) så kallas de **konjugerade**. Med **centrum** av G menas $Z(G) = \{x \in G : \forall_{g \in G} gx = xg\} = \{x \in G : St(x) = G\}$, där $St(x)$ betecknar stabilisatorn av x för konjugering.

(a) Visa att $x \mapsto gxg^{-1}$ är en automorfism av G. Den kallas en **inre automorfism**.

(b) Utnyttja 14 (d) för att visa att om $|G| = p^n, p$ ett primtal, så är $Z(G) \neq < e >$.

Anmärkning. En grupp G med $|G| = p^m$ där, p är ett primtal, kallas en **p-grupp**.

(c) Utnyttja (b) för att visa med induktion att om G är en p-grupp så existerar en kedja $G = G_0 \supset G_1 \supset \ldots \supset G_n =< e >$ sådan att G_{i+1} är en normaldelgrupp till G_i då $i = 0, \ldots, n-1$ och G_i/G_{i+1} är cyklisk.

Anmärkning. En ändlig grupp med denna egenskap kallas **lösbar** beroende på att sådana grupper svarar mot polynomekvationer som är lösbara i Galoisteorins mening.

1.16. Låt G vara en ändlig grupp.

(a) Visa att om $2 \mid |G|$ så existerar $g \in G$ med $o(g) = 2$.

(b) Visa att om G är abelsk och $p \mid |G|$ för ett primtal p så existerar $g \in G$ med $o(g) = p$.

Ledning. Ge ett induktivt bevis. Börja med $|G| = p$. Observera att påståendet är banalt för cykliska grupper.

Anmärkning. (b) är ett specialfall av Cauchys sats som gäller för godtyckliga ändliga grupper. En allmänare sats bevisades av Sylow. Den säger att om $p^m \mid |G|$ så existerar en delgrupp H till G med $|H| = p^m$ ((b) följer för alla ändliga grupper då $m = 1$). Om $p^m \mid |G|$ och $p^{m+1} \nmid |G|$ så är alla delgrupper till G av ordningen p^m konjugerade (dvs om H, H' är två sådana delgrupper så existerar $g \in G$ så att $H' = gHg^{-1}$). Alla delgrupper av ordningen p^m kallas **Sylows delgrupper** till G.

(c)* (Sylows sats) Visa att om $p^m \mid |G|$ så existerar en delgrupp H till G sådan att $|H| = p^m$.

Ledning. Visa satsen med induktion m a p ordningen av G. Om det finns en äkta delgrupp H till G sådan att $p^m \mid |H|$ gäller påståendet. Om en sådan delgrupp inte

finns gäller $p \mid [G : H]$ för varje äkta delgrupp H. Utnyttja då Övn. 14 (d) och visa att det finns $g \in Z(G), o(g) = p$. Betrakta då $G \to G/ < g >$.

Anmärkning. Sylows namn associeras med tre satser vars innehåll varierar något i olika läroböcker. I princip är påståendet i (c) Sylows första sats. Den andra konstaterar att varje p–delgrupp till G ligger i en Sylows p–delgrupp och att alla Sylows p–delgrupper till G är konjugerade, och den tredje säger att antalet s av Sylows p–delgruper till G är en delare till $|G|/p^m$ samt att s lämnar resten 1 vid division med p.

1.17. Låt G vara en grupp. Med **kommutatorgruppen** av G menas den minsta delgrupp till G som innehåller alla element av typen $xyx^{-1}y^{-1}$, $x, y \in G$. Den betecknas G' (eller $[G, G]$). Visa att

(a) G' är en normal undergrupp till G,

(b) G/G' är abelsk,

(c) om $G' \subseteq H \subseteq G$ så är $H \lhd G$,

(d) om $H \lhd G$ och G/H är abelsk, så är $H \supseteq G'$.

Anmärkning. $xyx^{-1}y^{-1}$ kallas **kommutatorn** av x och y. Den betecknas ofta $[x, y]$. Vi har $xy = [x, y]yx$ dvs $[x, y]$ "mäter" avvikelsen av xy från yx.

1.18. Visa följande isomorfismer

(a) $\mathbb{R}^+/\mathbb{Z} \cong U$; (b) $\mathbb{C}^*/\mathbb{R}^*_{>0} \cong U$; (c) $\mathbb{C}^*/U \cong \mathbb{R}^*_{>0}$; (d) $U/U_n \cong U$;

(e) $\mathbb{C}^*/U_n \cong \mathbb{C}^*$; (f) $\mathbb{R}^*/\mathbb{R}^*_{>0} \cong U_2$; (g) $\mathbb{R}^+/2\pi\mathbb{Z} \cong U$,

där $U = \{z \in \mathbb{C} : |z| = 1\}$, $U_n = \{z \in \mathbb{C} : z^n = 1\}$.

1.19. Låt G vara en topologisk grupp (dvs G är ett topologiskt rum sådant att funktionen $(x, y) \mapsto xy^{-1}$ från $G \times G$ till G är kontinuerlig). Med en karaktär av G menas en kontinuerlig homomorfism $f : G \to U$, där $U = \{z \in \mathbb{C} : |z| = 1\}$ (U har den topologi som induceras från den naturliga topologin i $\mathbb{C}$). Visa att:

(a) varje karaktär av $\mathbb{R}^+$ (med den vanliga toplogin) är $x \mapsto e^{ixx_0}$ där x_0 är ett fixerat reellt tal och $x \in \mathbb{R}^+$;

(b) varje karaktär av $\mathbb{R}^+/\mathbb{Z}$ (med topologin som induceras från $\mathbb{R}^+$) är $x \mapsto e^{2\pi in\bar{x}}$, där n är ett heltal och $\bar{x} \in \mathbb{R}^+/\mathbb{Z}$;

(c) varje karaktär av $\mathbb{Z}$ (med diskret topologi) är $x \mapsto e^{2\pi inx}$, där n är ett heltal och $0 \leq x < 1$.

1.20. (a) Låt G vara en ändlig abelsk grupp (med diskret topologi – se Övn. 19) och $|G| = n$. Visa att G har n olika karaktärer.

(b) Med en Dirichlet–karaktär menar man en funktion $\chi : \mathbb{Z} \to U$ sådan att

$$\chi(k) = \begin{cases} 0 & \text{om} \quad (k, m) \neq 1, \\ \psi([k]) & \text{om} \quad (k, m) = 1, \end{cases}$$

där ψ är en karaktär av $\mathbb{Z}^*_m$ (se Övn. 8) och $[k]$ är resten vid division av k med m. Visa att $\chi(xy) = \chi(x)\chi(y)$ och $\chi(x + m) = \chi(x)$ då $x, y \in \mathbb{Z}$.

Ledning till (a): Antag först att G är cyklisk. Utnyttja sedan anmärkningen efter Övn. 13.

1.21. Låt N vara en normal undergrupp till G och H en undergrupp till G. Visa att HN är en delgrupp till G och $HN/N \cong H/(N \cap H)$.

1.22. Låt G_1, G_2 vara grupper och $N_1 \lhd G_1$, $N_2 \lhd G_2$. Låt $f : G_1 \to G_2$ vara en homomorfism sådan att $f(N_1) \subseteq N_2$. Visa att det finns exakt en homomorfism $f^* : G_1/N_1 \to G_2/N_2$ sådan att diagrammet

$$\begin{array}{ccc} G_1 & \xrightarrow[f]{} & G_2 \\ {\scriptstyle n_1}\downarrow & & \downarrow{\scriptstyle n_2} \\ G_1/N_1 & \xrightarrow[f^*]{} & G_2/N_2 \end{array}$$

kommuterar (n_1, n_2 de naturliga surjektionerna). Visa att

$$\mathrm{Ker} f^* = \frac{N_1 f^{-1}(N_2)}{N_1} \quad \text{och} \quad \mathrm{Im} f^* = \frac{(\mathrm{Im} f)N_2}{N_2}.$$

Ledning: Visa att $f^*(g_1N_1) = f(g_1)N_2$ är en väldefinierad homomorfism.

1.23. Låt $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ vara Riemannsfären och $D \subset \bar{\mathbb{C}}$ en öppen sammanhängande delmängd till $\bar{\mathbb{C}}$. Låt $\mathcal{A}(D)$ vara gruppen av alla en-entydiga konforma avbildningar $f : D \to D$ m a p sammansättning. $\mathcal{A}(D)$ kallas automorfismgruppen av D. Alla påståenden som gäller beskrivningen av grupperna $\mathcal{A}(D)$ nedan finns t ex i H. Cartan, Théorie élémentaire des fonctions analitiques, Chap. VI, §2.

(a) $\mathcal{A}(\bar{\mathbb{C}}) = \{z \mapsto \frac{az+b}{cz+d}, ad - bc \neq 0\}$. Visa att $\mathcal{A}(\bar{\mathbb{C}}) \cong SL_2(\mathbb{C})/ < \pm E_2 >$.

(b) Med hjälp av (a) visa att $\mathcal{A}(\mathbb{C}) = \{z \mapsto az + b, a \neq 0\}$.

(c) Med hjälp av (a) visa att $\mathcal{A}(\mathcal{H}) = \{z \mapsto \frac{az+b}{cz+d}, a, b, c, d \in \mathbb{R}, ad-bc \neq 0\} \cong SL_2(\mathbb{R})/ < \pm E_2 >$, där $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im} z > 0\}$.

1.24. Visa att om H är en ändlig delmängd till en grupp G sådan att $H \neq \emptyset$ och $x, y \in H$ implicerar att $xy \in H$ så är H en delgrupp till G.

1.25. Låt $f : G \to G'$ vara en grupphomomorfism.

(a) Visa att bilden av en delgrupp till G är en delgrupp till G', och inversa bilden av en delgrupp till G' är en delgrupp till G.

(b) Är (a) sant om man ersätter orden "delgrupp" med orden "normal delgrupp"?

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

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

(b) Visa att exponenten av en ändlig grupp är en delare till gruppens ordning.

(c) Låt $M = MGM(o(g))$ för alla $g \in G$. Visa att $\exp(G) = M$.

(d) Visa att exponenten av en ändlig abelsk grupp är lika med maximalordningen av gruppens element. Är detta påstående sant för icke-abelska grupper?

(e) Visa att i en abelsk grupp har $\exp(G)$ och $o(G)$ samma primdelare.

APPENDIX A: EKVIVALENSRELATIONER

(A.1) Definition. En relation $\sim$ på en mängd X kallas för **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 $x, y, z \in X$. □

(A.2) Exempel. (a) Låt $X = \mathbb{Z}$ och låt $x \sim y$ då och endast då $5 \mid x - y$ för $x, y \in \mathbb{Z}$.

(b) Låt $X = G$ och låt H vara en delgrupp till G. Definiera $x \sim y$ då och endast då $Hx = Hy$ ($\Leftrightarrow xy^{-1} \in H$) för $x, y \in G$.

(c) Låt $X = \mathbb{N} = \{1, 2, \ldots\}$ och låt $x \sim y$ då och endast då x och y har exakt samma primtalsdelare.

(d) 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 dvs $X = \cup X_i$ är unionen av alla X_i och X_i är parvis disjunkta. Definiera nu $x \sim y$ om och endast om det finns i så at $x, y \in X_i$. Vi visar strax att varje ekvivalensrelation på X får man på detta sätt. □

(A.3) Definition. Låt $\sim$ vara en ekvivalensrelation på en mängd X. Med ekvivalensklassen av $x \in X$ menas mängden

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

□

(A.4) 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 (A.1) (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 transitiviteten. Enligt (b) är $[x] = [y]$.

(d) Följer direkt ur (a) och (c). □

(c) och (d) säger at ekvivalensklasserna av en ekvivalensrelation $\sim$ på X bildar en partition av X.

(A.5) Exempel. (a) För ekvivalensrelationen i (A.2) (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 (A.2)(b) har vi

$$y \in [x] \Leftrightarrow y \sim x \Leftrightarrow Hy = Hx \Leftrightarrow y \in Hx$$

(se (1.18)). Alltså är $[x] = Hx$.

(c) I exempel (A.2)(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).

(d) I exempel (A.2) (d) 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 $\sim$.

(A.6) Anmärkning. Om $X = G$ är en grupp och $\sim$ är relationen från (A.2)(b) så är $G/\sim$ mängden av alla högersidoklasser till H i G. Ofta använder man beteckningen $H \setminus G$. Om $\sim$ är relationen $x \sim y$ då och endast då $xH = yH$, så är ekvivalensklasserna identiska med vänstersidoklasserna till H i G. Man betecknar då $G/\sim$ med G/H. Om H är en normaldelgrupp, så är $H \setminus G = G/H$. Som vi vet i detta fall har G/H strukturen av en grupp (kvotgruppen av G modulo H) då sidoklasserna multipliceras enligt formeln $HxHy = Hxy$.

Rent allmänt betraktar man ofta mängder X med en binär operation $\circ$ och med en ekvivalensrelation $\sim$. I sådana fall vill man vanligen veta om operationen $\circ$ kan definieras på ekvivalensklasserna så att

$$[x][y] = [x \circ y]. \tag{A.7}$$

Det är klart att en sådan operation på ekvivalensklasserna är väl-definierad endast om den inte beror på valet av ekvivalensklassernas presentation dvs om

$$[x] = [x'] \quad \text{och} \quad [y] = [y'] \quad \text{implicerar att} \quad [x \circ y] = [x' \circ y'],$$

eller med andra beteckningar om

$$x \sim x' \quad \text{och} \quad y \sim y' \quad \text{implicerar att} \quad x \circ y \sim x' \circ y'.$$

Kapitel 2

RINGAR

Begreppet ring härstammar från Gauss studier av binära kvadratiska former med heltalskoefficienter. Försök att klassificera sådana former ledde till ringar bestående av talen $a + b\omega$, där $a, b \in \mathbb{Z}$ och ω löser en kvadratisk ekvation med heltaliga koefficienter och högsta koefficienten lika med 1. De Gaussiska heltalen $a + bi$, där $i^2 = -1$, är ett exempel. Gauss kallade dessa talmängder för ordningar troligen därför att de påtvingar en naturlig ordning bland ekvivalensklasser av motsvarande binära kvadratiska former. Senare under 1800-talet i samband med försök att bevisa Fermats stora sats började man intressera sig för liknande talmängder $a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1}$, där $a_i \in \mathbb{Z}$ och ω löser en ekvation av grad n med heltaliga koefficienter och högsta koefficienten lika med 1: Om n är ett udda naturligt tal så kan $x^n + y^n = z^n$ faktoruppdelas i produkt

$$(x + y)(x + \omega y) \cdots (x + \omega^{n-1} y) = z^n,$$

där $\omega^n = -1$. Faktoruppdelningar av den här typen och talteorin i dessa talmängder ledde till bevis av satsen i olika specialfall: För $n = 3$ av Leonhard Euler, för $n = 5$ av Peter Gustav Lejeune Dirichlet (1805 – 1859) och Adrien-Marie Legendre (1752 – 1833) samt Carl Friedrich Gauss (1777 – 1855), för $n = 7$ av Gabriel Lamé (1795 – 1870) och Henri Lebesgue (1875 – 1941). Ernst Edward Kummer (1810 – 1893) visade satsen för alla $n \leq 100$ och introducerade flera viktiga metoder som lade grunden för den moderna ringteorin. Fermats stora sats visades slutligen av Andrew Wiles år 1994 med avancerade metoder från olika matematiska teorier bland vilka ringteorin spelar en mycket viktig roll. Den första abstrakta definitionen av begreppet ring gavs ungefär år 1870 av Richard Dedekind (1831 – 1916), som fortfarande använde termen ordning. Eftersom ordningsbegreppet förekommer också i andra, mera naturliga sammanhang, föreslog David Hilbert (1862 – 1943) termen ring. Men termen ordning lever kvar och används ofta i algebraisk talteori. Ringbegreppet är mycket allmänt och är relaterad till oerhört många viktiga matematiska objekt. I denna kurs är vi mest intresserade av huvudidealringar och olika typer av algebror som vi diskuterar i efterföljande kapitel. En mera noggrann studie av ringteorin följer i kursen Kommutativ algebra. Kapitel 2 ägnas åt en kort introduktion till ringteorin och innehåller endast mycket allmänna resultat

som gäller i stort sett för alla ringar.

(2.1) Definition. En **ring** är en mängd R med två operationer "+" (addition) och "·" (multiplikation) sådana att:

(a) $(R, +)$ är en abelsk grupp (med neutrala elementet 0),

(b) $a(b+c) = ab + ac$ och $(b+c)a = ba + ca$ för godtyckliga $a, b, c \in R$.

R kallas **associativ** om

(c) $(ab)c = a(bc)$

för alla $a, b, c \in R$ och **kommutativ** om

(d) $ab = ba$ för godtyckliga $a, b \in R$.

Man säger att R är en **divisionsring** (eller en **skevkropp**) om

(e) $(R \setminus \{0\}, \cdot)$ är en grupp.

Om denna grupp är abelsk säger man att R är en **kropp**.

En ring R kallas **Liering** (efter den store norske matematikern Sophus Lie) om

(f) $(ab)c + (bc)a + (ca)b = 0$ och $a^2 = 0$ för alla $a, b, c \in R$.

□

(2.2) Exempel. (a) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ är ringar (associativa och kommutativa). De sista tre är kroppar.

(b) Mängden $M_n(\mathbb{R})$ av alla reella $(n \times n)$-matriser med matrisaddition och matrismultiplikation är en ring (associativ men inte kommutativ då $n > 1$).

(c) Mängden $C(a, b)$ av alla kontinuerliga funktioner på intervallet (a, b) med addition $(f + g)(x) = f(x) + g(x)$ och multiplikation $(fg)(x) = f(x)g(x)$ då $x \in (a, b)$ är en ring (kommutativ och associativ).

(d) Mängden $\mathcal{A}(U)$ av alla analytiska funktioner i en öppen delmängd U till $\mathbb{C}$ med addition och multiplikation som i (c) är en ring.

(e) Mängden av alla vektorer i $\mathbb{R}^3$ med vanlig vektoraddition och vektorprodukt som multip-

likation dvs:

$$\begin{aligned}(a,b,c)+(a_1,b_1,c_1) &= (a+a_1,b+b_1,c+c_1),\\ (a,b,c)\times(a_1,b_1,c_1) &= (bc_1-cb_1,ca_1-ac_1,ab_1-ba_1)\end{aligned}$$

är en ring. $(\mathbb{R}^3,+,\times)$ är varken associativ eller kommutativ. Det är ett exempel på en Liering (ringar av den typen kommer vi att diskutera i Kap. 10).

(f) Om X är en mängd och R är en ring så bildar alla funktioner $f: X \to R$ en ring då man definierar $(f+g)(x) = f(x)+g(x)$ och $(fg)(x) = f(x)g(x)$ (till höger i dessa likheter adderas och multipliceras i R).

(g) $(\mathbb{Z}_n, \oplus, \odot)$ är en associativ och kommutativ ring (se (1.14)). Den är en kropp då och endast då n är ett primtal (se (2.30)).

(h) Låt G vara en grupp och R en associativ ring. Med $R[G]$ betecknar man ringen av alla funktioner $\varphi: G \to R$ sådana att $\varphi(g) \neq 0$ för ett ändligt antal $g \in G$ med addition

$$(\varphi+\psi)(g) = \varphi(g)+\psi(g) \quad \text{då} \quad g \in G,$$

och multiplikation

$$(\varphi\psi)(g) = \sum_{g'g''=g} \varphi(g')\psi(g'').$$

Ofta skriver man formellt $\varphi = \sum_{g\in G} \varphi(g)g$. $R[G]$ kallas **gruppringen** av G med koefficienter i R.

T ex om $R = \mathbb{Z}$ så består $\mathbb{Z}[G]$ av alla summor $\sum_{g\in G} n_g g$, där $n_g \in \mathbb{Z}$, $n_g \neq 0$ för ett ändligt antal $g \in G$ och

$$\sum n_g g + \sum m_g g = \sum (n_g+m_g)g,$$

$$\sum n_g g \sum m_g g = \sum r_g g, \quad \text{där} \quad r_g = \sum_{g'g''=g} n_{g'} m_{g''}.$$

□

(2.3) Definition. En ring R har en **etta** om det finns ett element $1 \in R$, $1 \neq 0$, sådant att $1r = r1 = r$ för varje $r \in R$.

□

Det är klart att om R har en etta så är den entydigt bestämd ($1, 1' \in R \Rightarrow 1\cdot 1' = 1$ och $1\cdot 1' = 1'$ så att $1 = 1'$).

(2.4) Exempel. Alla ringar i Exempel (2.2) (a) – (d) har etta. Ringen i (e) saknar etta (helt allmänt saknas etta i varje Liering ty $1 \cdot 1 = 0$ så att $a = a \cdot 1 \cdot 1 = 0$ för varje a i ringen). De jämna heltalen med vanlig addition och multiplikation är ett exempel på en associativ och kommutativ ring utan etta.

□

I fortsättningen kommer vi att använda termen "ring" i betydelsen av "associativ ring". Bland icke-associativa ringar kommer vi att senare diskutera Lieringar. De definitioner och satser vars bevis gäller utan ändringar för Lieringar (och mera allmänt för alla ringar) betecknas i detta kapitel med "l".

(2.5)^l Definition. R' är en **delring** till R om $R' \subseteq R$ och elementen i R' bildar en ring m a p addition och multiplikation definierade i R.

□

Om $R' \subseteq R$ och $R' \neq \emptyset$ så är R' en delring till R om och endast om $r_1, r_2 \in R'$ implicerar $r_1 - r_2 \in R'$ och $r_1 r_2 \in R'$.

Här följer några ytterligare exempel på ringar.

(2.6) Exempel. (a) Om R är en kommutativ ring så betecknar $R[X]$ ringen av alla polynom med koefficienter i R. $R[X]$ består av alla uttryck:

$$p = a_0 + a_1 X + \ldots + a_n X^n,$$

där $a_i \in R$, $n \geq 0$ ($X^0 = 1$). sådana uttryck adderas och multipliceras som vanliga polynom med hänsyn till addition och multiplikation av a_i i R. Formellt kan man definiera polynom som följder $(a_0, a_1, \ldots, a_n, \ldots)$, där $a_i \in R$ och $a_i = 0$ för nästan alla[†] i med addition och multiplikation:

$$\begin{aligned} (a_0, a_1, \ldots) + (b_0, b_1, \ldots) &= (a_0 + b_0, a_1 + b_1, \ldots), \\ (a_0, a_1, \ldots)(b_0, b_1, \ldots) &= (c_0, c_1, \ldots), \end{aligned}$$

där $c_n = \sum_{i+j=n} a_i b_j$. Om $a_i = 0$ för $i > n$ och $a_n \neq 0$ så säger man att polynomet $(a_0, a_1, \ldots, a_n, \ldots)$ har **graden** n. Graden av **nollpolynomet** dvs polynomet vars alla koefficienter är lika med 0 definierar vi här som -1.

(b) **Formella potensserier** med koefficienter i R (R en kommutativ ring) bildar en ring som betecknas $R[[X]]$. Elementen i $R[[X]]$ är

$$p = a_0 + a_1 X + \ldots + a_n X^n + \ldots,$$

[†] "för nästan alla i" betyder att $a_i \neq 0$ endast för ett ändligt antal i.

där $a_i \in R$. Addition och multiplikation definieras som för polynom (se (a)). En formell definition kan ges exakt som för polynom i (a) i form av följder $(a_0, a_1, \ldots, a_n, \ldots)$. Om $R = \mathbb{C}[[X]]$ kan man betrakta potensserier med konvergensradie > 0. sådana serier bildar en delring till $\mathbb{C}[[X]]$ (samma sak gäller för t ex $\mathbb{R}[[X]]$).

□

(2.7)^l Definition. En funktion $\varphi : R \to R'$ är en **homomorfism** från ringen R till ringen R' om

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \quad \text{och} \quad \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2).$$

Man säger att φ är en **isomorfism** om φ är bijektiv. Man skriver då $R \cong R'$.

□

Det följer lätt ur definitionen av φ att $\varphi(0) = 0$ och $\varphi(-r) = -\varphi(r)$, ty $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ ger $\varphi(0) = 0$, och $\varphi(r) + \varphi(-r) = \varphi(0)$ ger $\varphi(-r) = -\varphi(r)$.

(2.8)^l Definition. Om $\varphi : R \to R'$ är en homomorfism så kallas $\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0\}$ **kärnan** till φ.

□

(2.9) Exempel. (a) $R = \mathbb{R}[X], R' = \mathbb{C}$, $\varphi : R \to R'$ definieras av $\varphi(p) = p(i)$. Här är $\operatorname{Ker}\varphi = \{p \in \mathbb{R}[X] : p(i) = 0\} = (X^2 + 1)$ (alla polynommultipler av $X^2 + 1$).

(b) $R = C(0, 1)$, $R' = \mathbb{R}$, $\varphi : R \to R'$ ges av $\varphi(f) = f(x_0)$, där $x_0 \in (0, 1)$. Vi har $\operatorname{Ker}\varphi = \{f \in C(0, 1) : f(x_0) = 0\} =: I_{x_0}$.

(c) $R = \mathbb{Z}$, $R' = \mathbb{Z}_n$, $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ definieras som $\varphi(x) = [x]_n$, där $[x]_n$ är resten vid division av x med n. $\operatorname{Ker}\varphi = \{x \in \mathbb{Z} : [x]_n = 0\} = (n)$ (alla multipler av n).

□

Kärnan till en homomorfism $\varphi : R \to R'$ är en mycket viktig delring till R:

(2.10)^l Definition. I kallas ett (tvåsidigt) **ideal** i R om $I \subseteq R$, $I \neq \emptyset$ och

(a) $i_1, i_2 \in I \Rightarrow i_1 - i_2 \in I$,

(b) $i \in I$, $r \in R \Rightarrow ri$, $ir \in I$.

Om, i stället för (b), $i \in I$ och $r \in R$ endast implicerar att $ri \in I$, kallas I ett **vänsterideal**. På liknande sätt definieras ett **högerideal**.

□

Ur definitionen följer lätt att varje vänster eller högerideal är en delring till R.

Anmärkning. Termen ideal introducerades av Richard Dedekind (1870). Den härstammar från E. Kummers studier av faktoruppdelningar av algebraiska heltal. Kummer betraktade "idealtal". Han definierade begreppet för att återställa entydig faktoruppdelning i de ringar som används för att bevisa Fermats stora sats. Termen tvåsidigt ideal (i icke-kommutativa ringar) introducerades år 1898 av Elie Cartan (1869 – 1951). Begreppen högerideal och vänsterideal definierades år 1920 av Emmy Noether (1882 – 1935). □

(2.11) Exempel. (a) Om R är en godtycklig ring och $a_1, a_2, \ldots, a_m \in R$ så bildar alla element

$$r_1a_1 + r_2a_2 + \ldots + r_ma_m, \quad \text{där} \quad r_1, r_2, \ldots, r_m \in R,$$

ett vänsterideal i R (en mycket enkel övning). Om R är en kommutativ ring så betecknar man ett sådant ideal med $(a_1, a_2, \ldots, a_m)$ och man säger att det **genereras** av $a_1, a_2, \ldots, a_m$. Ett ideal $I = (a)$, $a \in R$ (R fortfarande kommutativ) kallas **principalt** (eller **huvudideal**). En kommutativ ring R i vilken varje ideal är principalt kallas **huvudidealring**.

(b) Om I är ett ideal i ringen $\mathbb{Z}$ så består I av alla heltaliga multipler av ett naturligt tal n. Liknande påstående gäller för polynomringen $K[X]$ (K en kropp): Varje ideal I i $K[X]$ kan skrivas på formen $I = (p)$ dvs mängden av alla polynommultipler av ett polynom p. Med andra ord är både $\mathbb{Z}$ och $K[X]$ huvudidealringar. Se vidare övn. 6.

(c) Hilberts bassats säger att varje ideal i polynomringen $R = K[X_1, X_2, \ldots, X_n]$ (K en kropp, $X_1, X_2, \ldots, X_n$ variabler) kan genereras av ett ändligt antal element dvs varje ideal I kan skrivas på formen $I = (p_1, p_2, \ldots, p_m)$, där $p_i \in R$ (vi visar Hilberts sats senare). Allmänt säger man att en kommutativ ring R är **noethersk** (efter Emmy Noether) om varje ideal i R kan genereras av ett ändligt antal element.

□

(2.12)^l Proposition. *Kärnan I till en homomorfism $\varphi : R \to R'$ är ett ideal.*

Bevis. $i_1, i_2 \in I \Rightarrow \varphi(i_1) = \varphi(i_2) = 0 \Rightarrow \varphi(i_1 - i_2) = \varphi(i_1) - \varphi(i_2) = 0 \Rightarrow i_1 - i_2 \in I$.
$i \in I, r \in R \Rightarrow \varphi(ir) = \varphi(i)\varphi(r) = 0$ och $\varphi(ri) = \varphi(r)\varphi(i) = 0 \Rightarrow ir, ri \in I$. □

En normal undergrupp N till en grupp G ger upphov till kvotgruppen G/N. På samma sätt ger ett ideal I i R en möjlighet till att konstruera kvotringen R/I.

(2.13)^l Konstruktionen av kvotringar. Om I är ett ideal i R så kan vi först betrakta (den abelska) kvotgruppen R/I, där R och I är grupper m a p addition. Det faktum att I är ett ideal gör det möjligt att definiera multiplikation av sidoklasserna:

$$(a+I)(b+I) := ab+I.$$

Frågan är om den definitionen är korrekt dvs om uttrycket till höger är oberoende av valet av a' och b' i sidoklasserna $a+I$ och $b+I$ dvs om $a+I=a'+I$ och $b+I=b'+I$ implicerar $ab+I=a'b'+I$ (jfr Appendix A). Men detta följer ur definitionen av I:

$$a'b'-ab=(a'-a)b'+a(b'-b)\in I \quad \text{ty} \quad a'-a\in I \quad \text{och} \quad b'-b\in I.^\dagger$$

Alltså är $a'b'+I=ab+I$. □

Lägg märke till att ideal i R är exakt de delringar för vilka konstruktionen av R/I kan genomföras (se Övn. 8).

(2.14)^l Proposition. *Låt I vara ett ideal i R. Funktionen $\eta : R \to R/I$ sådan att $\eta(r) = r+I$ är en surjektiv homomorfism med kärnan I (η kallas* **den naturliga surjektionen**).

Bevis. Vi har $\eta(r_1+r_2)=r_1+r_2+I=(r_1+I)+(r_2+I)=\eta(r_1)+\eta(r_2)$ och $\eta(r_1r_2)=r_1r_2+I=(r_1+I)(r_2+I)=\eta(r_1)\eta(r_2)$. Dessutom är $\operatorname{Ker}\eta=\{r : r+I=I\}=I$. □

(2.15) Exempel. (a) Varje ideal I i $\mathbb{Z}$ är av formen $I=(n)$, där n är ett heltal (se Övn. 6). $\mathbb{Z}/(n)$ består av n element $0+(n), 1+(n), \dots, n-1+(n)$ (se (1.16)(c)). Ringen $\mathbb{Z}/(n)$ är isomorf med $\mathbb{Z}_n$ (se vidare (2.16)).

(b) Om I är ett ideal i polynomringen $K[X]$, där K är en kropp, så är $I=(p_0)$, där p_0 är ett polynom ur $K[X]$ (se Övn. 6). Vi påstår att varje element i $K[X]/(p_0)$, där $p_0\neq 0$, kan skrivas entydigt på formen $r+(p_0)$, där $\operatorname{grad}(r)<\operatorname{grad}(p_0)$. Om $p+(p_0)$ är en sidoklass och $p=qp_0+r$, där $\operatorname{grad}(r)<\operatorname{grad}(p_0)$, så är $p+(p_0)=r+(p_0)$ ty $p-r=qp_0\in(p_0)$. Å andra sidan ger $r_1+(p_0)=r_2+(p_0)$, där $\operatorname{grad}(r_1), \operatorname{grad}(r_2)<\operatorname{grad}(p_0)$ att $r_1-r_2\in(p_0)$ dvs $p_0|r_1-r_2$, vilket medför att $r_1=r_2$.

Som ett konkret exempel låt oss betrakta $\mathbb{R}[X]/(X^2+1)$. Då kan varje sidoklass skrivas som $a+bx+(X^2+1)$, där $a,b\in\mathbb{R}$. Om $\overline{a+bx}=a+bx+(X^2+1)$ så gäller:

$$\overline{a+bx}+\overline{c+dx}=\overline{(a+c)+(b+d)x} \quad \text{och} \quad \overline{(a+bx)(c+dx)}=\overline{(ac-bd)+(ad+bc)x},$$

ty $x^2=(x^2+1)\cdot 1+(-1)$ dvs $\overline{x^2}=\overline{-1}$. Man ser lätt att sidoklasserna $\overline{a+bx}$ bildar en ring isomorf med $\mathbb{C}$, där $\overline{a+bx}\mapsto a+bi\in\mathbb{C}$ definierar en isomorfism (se (2.17)(a)).

†Observera att $r+I=r'+I \Leftrightarrow r-r'\in I$ (se (1.16), (1.18) och Appendix A).

□

Observationen ovan att $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ och $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ är specialfall av en allmän sats om ringhomomorfismer, som ibland kallas **huvudsatsen om ringhomomorfismer**:

(2.16)^l Sats. *Om $\varphi : R \to R'$ är en ringhomomorfism och $I = \operatorname{Ker}\varphi$ dess kärna så är $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$ och en isomorfism är given av $a + I \mapsto \varphi(a)$.*

Bevis. Enligt homomorfismsatsen för grupper (se (1.38)) vet vi att $\varphi^*(a+I) = \varphi(a)$ definierar en isomorfism av gruppen $(R/I, +)$ med $(\varphi(R), +)$. Men $\varphi^*((a+I)(b+I)) = \varphi^*(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi^*(a+I)\varphi^*(b+I)$ så att φ^* också är en ringhomomorfism. □

(2.17) Exempel. (a) Isomorfismen $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ ur (2.15)(b) följer på följande sätt. Låt $\varphi : \mathbb{R}[X] \to \mathbb{C}$ vara homomorfismen $\varphi(p) = p(i)$. Vi har

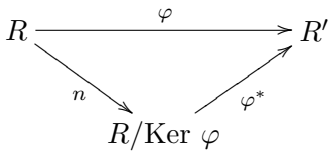
$$\operatorname{Ker}\varphi = \{p \in R[X] : p(i) = 0\} = (X^2+1).$$

φ avbildar $\mathbb{R}[X]$ på $\mathbb{C}$, ty $a + bX \mapsto a + bi$. Alltså är $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ och φ inducerar isomorfismen $\overline{a+bX} \mapsto a + bi$.

(b) Låt $\varphi : C(0,1) \to \mathbb{R}$ där $\varphi(f) = f(1/2)$. Då är $\operatorname{Ker}\varphi = \{f \in C(0,1) : f(1/2) = 0\} = I_{1/2}$. φ är en surjektiv ringhomomorfism (ty $f(x) \equiv r \mapsto r \in \mathbb{R}$). Alltså är $C(0,1)/I_{1/2} \cong \mathbb{R}$ och φ inducerar isomorfismen $f + I_{1/2} \mapsto f(1/2)$.

□

(2.18)^l Anmärkning. Sats 2.16 kan formuleras på följande sätt: För varje ringhomomorfism $\varphi : R \to R'$ existerar (exakt) en injektiv ringhomomorfism $\varphi^* : R/\operatorname{Ker}\varphi \to R'$ sådan att diagrammet



är kommutativt (n den naturliga surjektionen) dvs $\varphi^* n = \varphi$. Kommutativiteten betyder just att bilden av $r + \operatorname{Ker}\varphi$ är $\varphi(r)$.

□

(2.19)^l Proposition. *Låt $\varphi : R \to R'$ vara en surjektiv ringhomomorfism. Funktionen $I' \mapsto \varphi^{-1}(I')$ avbildar en-entydigt alla ideal i R' på alla ideal i R som innehåller* $\operatorname{Ker}\varphi$.

Bevis. Lämnas som en mycket enkel, men något tråkig övning. □

I fortsättningen av detta kapitel är alla ringar kommutativa och associativa. Vi skall betrakta två viktiga klasser av ideal – primideal och maximalideal.

(2.20) Definition. Ett ideal I i en ring R kallas **primt** om $I \neq R$ och $ab \in I$ implicerar att $a \in I$ eller $b \in I$.

□

(2.21) Exempel. Ett ideal $I = (n) \neq (0)$ i $\mathbb{Z}$ är ett primideal då och endast då n är ett primtal (ty $ab \in (n) \Leftrightarrow n|ab$ och $n|ab \Leftrightarrow n|a$ eller $n|b$ då endast då n är ett primtal). På samma sätt är ett ideal $I = (p) \neq (0)$ i $K[X]$ ett primideal då och endast då p är ett primpolynom i $K[X]$ (dvs p är ett icke-konstant polynom som inte är en produkt av två icke-konstanta polynom). Motiveringen är exakt samma som för $\mathbb{Z}$ (med orden "primtal" och "primpolynom" utbytta). I bägge fallen är (0) ett primideal.

□

(2.22) Definition. Man säger att $a \in R$ är en **nolldelare** om $a \neq 0$ och det finns $b \in R$, $b \neq 0$ så att $ab = 0$. R kallas **integritetsområde** om R saknar nolldelare (dvs $ab = 0$ med $a, b \in R$ implicerar att $a = 0$ eller $b = 0$) och har etta. Man säger att R är ett **huvudidealområde** [†]**)** om R är en huvudidealring utan nolldelare.

□

(2.23) Exempel. (a) $\mathbb{Z}$ och $K[X]$ är integritetsområden.

(b) $C(0,1)$ har nolldelare dvs det finns $f, g \in C(0,1)$ så att $f \neq 0$, $g \neq 0$, men $fg = 0$ (ge ett exempel!).

(c) $\mathcal{A}(U)$ (alla analytiska funktioner i en öppen sammanhängande mängd $U \subseteq \mathbb{C}$) är ett integritetsområde (visa detta påstående!).

(d) Varje kropp K saknar nolldelare ty $ab = 0$ och $a \neq 0$ i K implicerar $a^{-1}(ab) = b = 0$.

□

(2.24) Proposition. *I är ett primideal i R då och endast då R/I saknar nolldelare.*

[†]Den engelska termen är "principal ideal domain", vilket ofta förkortas till PID.

Bevis. $\bar{a}\bar{b} = \bar{0} \Leftrightarrow (a+I)(b+I) = ab + I = I \Leftrightarrow ab \in I$. Nu har vi:

"$\Rightarrow$" $\bar{a}\bar{b} = \bar{0} \Rightarrow ab \in I \Rightarrow a \in I$ eller $b \in I \Rightarrow \bar{a} = \bar{0}$ eller $\bar{b} = \bar{0}$,

"$\Leftarrow$" $ab \in I \Rightarrow \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ eller $\bar{b} = \bar{0} \Rightarrow a \in I$ eller $b \in I$. □

(2.25) Definition. Ett ideal I i R kallas **maximalt** om $I \neq R$ och om J är ett ideal i R som innehåller I så är $J = I$ eller $J = R$ (dvs $I \subseteq J \subseteq R$, där J är ett ideal i R, medför att $J = I$ eller $J = R$.

□

(2.26) Exempel. (a) I $\mathbb{Z}$ är (n) ett maximalideal då och endast då n är ett primtal. I själva verket, $(n) \subseteq (m) \subseteq \mathbb{Z}$ betyder att $m|n$. Om $n = p$ är ett primtal, så är $m|p$ ekvivalent med $m = \pm 1$ eller $m = \pm p$ dvs $(m) = \mathbb{Z}$ eller $(m) = (p)$. Omvänt, om $n = mq$, $m \neq 1 \neq q$, så är $(n) \subset (m) \subset \mathbb{Z}$. Samma argument visar att ett ideal (p) i $K[X]$ är maximalt då och endast då p är ett primpolynom (= irreducibelt polynom). Detta betyder att i $\mathbb{Z}$ och $K[X]$ sammanfaller primidealen $\neq (0)$ med maximalidealen.

(b) I $\mathbb{R}[X,Y]$ är t ex (X) ett primideal (se Övn. 17) som inte är maximalt ty $(X) \subset (X,Y) \subset \mathbb{R}[X,Y]$.

(c) Hilberts Nullstellensatz säger att varje maximalideal I i $\mathbb{C}[X_1, \ldots, X_n]$ kan skrivas på formen $I = (X_1 - a_1, \ldots, X_n - a_n)$, där $a_i \in \mathbb{C}$ (satsen visas senare).

□

(2.27) Proposition. *Låt R vara en ring med etta. R saknar icke-triviala ideal (dvs $\neq (0), R$) då och endast då R är en kropp.*

Bevis. Om R är en kropp och $I \neq (0)$ är ett ideal i R så finns det $a \in I$, $a \neq 0$. Då är $a \cdot a^{-1} = 1 \in I$ vilket betyder att för varje $r \in R$ är $r \cdot 1 = r \in I$ dvs $I = R$.

Omvänt, om R saknar icke-triviala ideal och $a \in R$, $a \neq 0$, så är aR ett ideal i R skilt från (0). Alltså är $aR = R$ vilket betyder att det finns $x \in R$ så att $ax = 1$. Detta visar att $R \setminus (0)$ är en (abelsk) grupp m a p multiplikation dvs R är en kropp. □

(2.28) Proposition. *Låt R vara en ring med etta. I är ett maximalideal i R då och endast då R/I är en kropp.*

Bevis. Den naturliga surjektionen $n : R \to R/I$ (se (2.14)) i kombination med (2.19) visar att I är maximalt då och endast då R/I saknar icke-triviala ideal. Påståendet följer nu ur (2.27). □

(2.29) Följdsats. *I en ring med etta är varje maximalideal primt.*

Bevis. Om I är maximalt i R så är R/I en kropp enligt (2.28). Alltså finns det inga nolldelare i R/I (se (2.23) (d)) vilket betyder att I är primt enligt (2.24). □

(2.30) Exempel. $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ är en kropp då och endast då (n) är ett maximalideal dvs n är ett primtal (se (2.26)(a)). På samma sätt är $K[X]/(p)$ en kropp då och endast då (p) är ett maximalideal dvs p är ett irreducibelt polynom.

□

(2.31) Anmärkning. I en godtycklig ring R kan man betrakta maximala vänster- och högerideal. Ett vänsterideal I är maximalt i R om $I \neq R$ och $I \subseteq J \subseteq R$ för ett vänsterideal J implicerar $J = I$ eller $J = R$. På liknande sätt definieras maximala högerideal. En ring R med etta är en divisionsring då och endast då den saknar icke-triviala vänsterideal (eller högerideal). Bevis är exakt samma som för (2.27).

□

Vi avslutar detta kapitel med några ord om ringar med entydig faktoruppdelning. Huvudidealringar tillhör denna klass och de kommer att spela en viktig roll senare då vi studerar kanoniska former av matriser (linjära avbildningar).

(2.32) Definition. Låt R vara ett integritetsområde. Ett element $p \in R$, $p \neq 0$ kallas **irreducibelt** om likheten $p = rr', r, r' \in R$, implicerar att exakt en av faktorerna r, r' är inverterbart i R. Man säger att R har **entydig faktoruppdelning**[†] om varje icke-inverterbart element $r \in R$, $r \neq 0$, är en produkt av irreducibla och om

$$r = p_1 \dots p_k = q_1 \dots q_l,$$

där p_i, q_j är irreducibla i R, så är $k = l$ och, vid lämplig numrering av faktorerna, är $Rp_i = Rq_i$ (dvs $p_i = \varepsilon_i q_i$, där $\varepsilon_i \in R^*$). Man säger då att p_i och q_i är **associerade**.

□

(2.33) Exempel. (a) Varje huvudidealområde är UFD (se vidare Övn. 26). Varje polynomring $K[X_1, \dots, X_n]$, K en kropp, är UFD. Mera allmänt kan man bevisa (se Övn. 28) att om R är UFD så är också $R[X]$ UFD. T ex har $\mathbb{Z}[X_1, \dots, X_n]$ entydig faktoruppdelning.

(b) Låt $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5},\ a, b \in \mathbb{Z}\}$. I den ringen har vi

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

[†]Den engelska termen är "unique factorization domain", vilket ofta förkortas till UFD.

Talen 3, $2 \pm \sqrt{-5}$ är irreducibla. För att visa det betrakta normen $N(z) = |z|^2 = a^2 + 5b^2$ för $z = a + b\sqrt{-5}$. Låt oss observera att om $N(z) = 1$ dvs $z\bar{z} = 1$ så är z inverterbart i $\mathbb{Z}[\sqrt{-5}]$, och omvänt om $zz' = 1$ så är $N(z) = N(z') = 1$. Om nu $3 = z_1 z_2$, där z_1, $z_2 \in \mathbb{Z}[\sqrt{-5}]$, så är $9 = |z_1|^2|z_2|^2$ dvs $|z_i|^2 \in \{1, 3, 9\}$. Men $|z_i|^2 \neq 3$, så att antingen z_1 eller z_2 måste vara inverterbart dvs 3 är irreducibelt. På samma sätt visas att $2 \pm \sqrt{-5}$ är irreducibla. Vidare konstaterar vi att 3 inte är associerat med $2 \pm \sqrt{-5}$ (om $3 = \varepsilon(2 \pm \sqrt{-5})$ så är $N(\varepsilon) = 1$ dvs $\varepsilon = \pm 1$, vilket ger en motsägelse). Allt detta visar att $\mathbb{Z}[\sqrt{-5}]$ inte är UFD.

□

En liten, men ändå relativt viktig klass av ringar med entydig faktoruppdelning utgör **euklidiska ringar** (se Övn. 22). Eftersom varje euklidisk ring är ett huvudidealområde så följer entydigheten av faktoruppdelningar i euklidiska ringar från att denna egenskap gäller i denna större klass (se Övn. 26).

ÖVNINGAR

2.1. Visa att följande funktioner $f : \mathbb{Z}[X] \to \mathbb{C}$ är homomorfismer. Bestäm Ker$f$.

(a) $f(p(X)) = p(i)$; (b) $f(p(X)) = p(0)$; (c) $f(p(X)) = p(\sqrt{2})$.

2.2. Visa att följande avbildningar $f : R \to R$ är automorfismer av R:

(a) $R = \mathbb{C}, f(z) = \bar{z}$; (b) $R = \mathbb{R}[X], f(p(X)) = p(-X)$;

(c) $R = \mathbb{Z} \times \mathbb{Z}, f((m, n)) = (n, m)$.

2.3. Visa att om $f : R \to R'$ är en homomorfism av ringar så är $F : R[X] \to R'[X]$, där $F(a_0 + a_1X + \ldots + a_nX^n) = f(a_0) + f(a_1)X + \ldots + f(a_n)X^n$, en homomorfism av polynomringarna.

2.4. Visa följande isomorfismer:

(a) $\mathbb{R}[X]/(X) \cong \mathbb{R}$; (b) $\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{R} \times \mathbb{R}$; (c) $\mathbb{Z}[X]/(X^2 - X) \cong \mathbb{Z} \times \mathbb{Z}$;

(d) $\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i]$; (e) $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}_2$.

2.5. Visa att om I_1, I_2 är ideal i en kommutativ ring R så är också (a) $I_1 + I_2 = \{a + b : a \in I_1 \quad \text{och} \quad b \in I_2\}$ (summan),

(b) $I_1 \cap I_2$, (snittet),

(c) $I_1I_2 = \{\sum a_ib_i : a_i \in I_1 \quad \text{och} \quad b_i \in I_2\}$ (produkten)

ideal i R.

2.6. Visa att $\mathbb{Z}$ och $K[X]$ (K en kropp) är huvudidealringar.

Ledning. Utnyttja divisionsalgoritmen i dessa ringar. I varje ideal $I \neq (0)$ välj ett element $a \neq 0$ med minsta beloppet i $\mathbb{Z}$ och av minsta grad i $K[X]$ och visa att $I = (a)$.

2.7. Bestäm alla ideal i följande ringar:

(a) $\mathbb{Z}_4$; (b) $\mathbb{Z}_6$; (c) $K[X]/(X^2)$ (K en kropp); (d) $K \times K$ (K en kropp); (e) $\mathbb{R}[X]/(X^2 - 1)$.

2.8. Låt R' vara en delring till R sådan att formeln $(a + R')(b + R') = ab + R'$ ger en korrekt definition av produkt i mängden av alla sidoklasser till $(R', +)$ i $(R, +)$. Visa att R' då är ett ideal.

2.9. Låt R och R' vara kommutativa ringar och $\varphi : R \to R'$ en ringhomomorfism. Visa att om I' är ett primideal i R' så är $\varphi^{-1}(I')$ ett primideal i R. Vad kan man säga om $\varphi^{-1}(I')$ då I' är ett maximalideal i R'?

2.10. Visa att det finns en homomorfism $\mathbb{Z}_m \to \mathbb{Z}_n$ sådan att $1 \mapsto 1$ då och endast då $n|m$.

2.11. Låt R vara ett huvudidealområde med etta (dvs ett integritetsområde i vilket alla ideal är huvudideal). Visa att varje primideal $\neq (0)$ är maximalt.

2.12. Låt $\varphi : R \to K$ vara en homomorfism av en kommutativ ring med etta på en kropp K. Motivera att Ker φ är ett maximalideal.

2.13. Låt R vara en kommutativ ring med etta. Med **karakteristiken** av R menar man det minsta naturliga talet n sådant att $n \cdot 1 = 0$ eller 0 om ett sådant n inte existerar (dvs karakteristiken av R är lika med ordningen av den cykliska delgruppen $< 1 >$ till $(R, +)$ om den delgruppen är ändlig och 0 om den är oändlig). Karakteristiken av R kommer att betecknas med $\text{char}(R)$.

(a) Låt $\text{char}(R) = n$. Visa att $n \cdot a = 0$ för varje $a \in R$.

(b) Visa att karakteristiken av ett integritetsområde är ett primtal eller 0.

(c) Visa att varje kropp innehåller exakt en delkropp som är isomorf med antingen $\mathbb{Z}_p, p$ ett primtal, då karakteristiken av kroppen är p, eller $\mathbb{Q}$ då karakteristiken av kroppen är 0.

2.14. Låt $\varphi : R_1 \to R_2$ vara en ringhomomorfism sådan att $\varphi(I_1) \subseteq I_2$, där I_1 är ett ideal i R_1 och I_2 ett ideal i R_2. Visa att det finns exakt en homomorfism $\varphi^* : R_1/I_1 \to R_2/I_2$ sådan att diagrammet

$$\begin{array}{ccc} R_1 & \xrightarrow[\varphi]{} & R_2 \\ {\scriptstyle \eta_1}\downarrow & & \downarrow{\scriptstyle \eta_2} \\ R_1/I_1 & \xrightarrow[\varphi^*]{} & R_2/I_2 \end{array}$$

kommuterar, där η_1 och η_2 är de naturliga surjektionerna.

2.15. Låt $I \subseteq J$ vara ideal i en ring R. Visa att det finns en naturlig ringisomorfism

$$\frac{\frac{R}{I}}{\frac{J}{I}} \cong \frac{R}{J}.$$

2.16. Visa att varje maximalideal i ringen $C[0,1]$ av de kontinuerliga funktionerna på $[0,1]$ är av formen $J_{x_0} = \{f \in C[0,1] : f(x_0) = 0\}$, där $x_0 \in [0,1]$. Formulera en lämplig generalisering.

2.17. Låt $G = \mathbb{R}^+$ och låt $L^1(G)$ vara $\mathbb{C}$–algebran av alla kontinuerliga funktioner $f : \mathbb{R} \to \mathbb{C}$ sådana att $\int_{-\infty}^{\infty} |f(x)|dx$ existerar, med vanlig addition av funktioner och multiplikation given av

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x-y)g(y)dy.$$

(a) Visa att $L^1(G)$ verkligen är en associativ ring.

(b) Man kan visa (se t ex L. H. Loomis, An introduction to abstract harmonic analysis, §23D) att varje surjektiv ringhomomorfism $F : L^1(G) \to \mathbb{C}$ är definierad på följande sätt:

$$F(f) = \int_{-\infty}^{\infty} f(x)\overline{\alpha(x)}dx,$$

där $\alpha : \mathbb{R}^+ \to U$ är en karaktär av $\mathbb{R}^+$ (se Övn. 1.18) dvs $\alpha(x) = e^{iyx}$, där $y \in \mathbb{R}$ är fixerat (detta innebär att om F_y svarar mot $\alpha_y(x) = e^{iyx}$ så är

$$\hat{f}(y) = F_y(f) = \int_{-\infty}^{\infty} f(x)e^{iyx}dx$$

Fouriertransformen av f). Motivera att F verkligen är en surjektiv ringhomomorfism av $L^1(G)$ på $\mathbb{C}$.

Anmärkning. Kärnan till F är ett maximalideal i $L^1(G)$ (se Övn. 12). Man kan visa att om man ordnar mot F dess kärna så får man 1 – 1 motsvarighet mellan alla karaktärer av $\mathbb{R}^+$ och alla reguljära maximalideal i $L^1(G)$ (ett ideal I i en ring R kallas reguljärt om R/I har en etta). Resultat av den övningen är ett specialfall av en allmän sats om lokalt kompakta abelska grupper (här $\mathbb{R}^+$) – se t ex boken av Loomis, §34B).

2.18. Låt R vara en ring med etta. Ett element $r \in R$ kallas **inverterbart** eller en **enhet** om det finns $r' \in R$ så att $rr' = r'r = 1$. Visa att alla enheter i R bildar en grupp m a p multiplikation. Den gruppen betecknas ofta med R^*. Vad kan man säga om alla element $r \in R$ sådana att $rr' = 1$ för något $r' \in R$? Samma fråga för $r \in R$ med $r'r = 1$ för något $r' \in R$.

2.19. Låt $p(X, Y)$ vara ett irreducibelt polynom i $\mathbb{C}[X, Y]$. Motivera att (p) är ett primideal och visa att det inte är maximalt.

2.20. Avgör om följande ideal i $\mathbb{Z}[X]$ är maximala:

a) $(3, X)$; b) $(3, X^2 + 1)$; c) $(3, X^2 + 2)$.

2.21. Med ett nilpotent element i en ring R menas ett element $r \in R$ sådant att $r^n = 0$ för något naturligt $n \geq 1$. Låt R vara kommutativ.

(a) Visa att alla nilpotenta element i R bildar ett ideal $\mathcal{N}$ (det kallas den **nilpotenta radikalen** av R).

(b)* Visa att $\mathcal{N}$ är snittet av alla primideal i R (använd Zorns lemma).

2.22. Ett integritetsområde R kallas **euklidiskt** om det finns en funktion $N : R \to \mathbb{N}$ sådan att:

(i) $N(a) = 0 \Leftrightarrow a = 0$,

(ii) $N(ab) = N(a)N(b)$,

(iii) om $a, b \in R$, $b \neq 0$ så existerar $q, r \in R$ sådana att $b = qa + r$ och $r = 0$ eller $N(r) < N(b)$.

Visa att följande ringar är euklidiska:

(a) $\mathbb{Z}$, (b) $K[X], K$ en kropp, (c) $\mathbb{Z}[i]$, (d) $\mathbb{Z}[\sqrt{2}]$, (e) $\mathbb{Z}[\sqrt{-2}]$.

Anmärkning. Bland ringarna Det är inte svårt att visa att bland ringarna $\mathbb{Z}[\sqrt{d}]$ med $d < 0$ finns det enbart 2 som är euklidiska. De ges av $d = -1, -2$ och är euklidiska med avseende på den vanliga normen $N(a+b\sqrt{d}) = a^2 - db^2$. Om $d > 0$ så är $\mathbb{Z}[\sqrt{d}]$ euklidisk med avseende på normen $N(a + b\sqrt{d}) = |(a^2 - db^2|$ endast då d = 2,3,6,7,11,19. Det är inte känt om $\mathbb{Z}[\sqrt{d}]$ kan vara euklidisk för andra $d > 0$ (med avseende på en lämplig funktion N). Man förmodar att det är så för t.ex. $\mathbb{Z}[\sqrt{14}]$ och för oändligt många andra d.

2.23. Visa att varje euklidisk ring är ett huvudidealområde.

2.24. Visa att om R är euklidisk med avseende på en funktion N så är $a \in R$ inverterbart då och endast då $N(a) = 1$.

2.25. Låt R vara ett integritetsområde. Ett icke-inverterbart element $p \in R$ kallas **primt** om villkoret $p|ab$ implicerar $p|a$ eller $p|b$ ($a, b \in R$). Med andra ord: p är primt då och endast då idealet (p) är ett primideal.

(a) Visa att ett primelement är irreducibelt och ge ett exempel på ett irreducibelt element som inte är primt (t.ex. i $\mathbb{Z}[\sqrt{-5}]$).

(b) Visa att om R är UFD så är varje irreducibelt element primt.

(c) Låt varje element i R vara en produkt av irreducibla element. Visa att R är UFD då och endast då varje irreducibelt element är primt.

2.26. (a) Visa att varje nollskilt element i ett huvudidealområde är en produkt av irreducibla element.

(b) Utnyttja Övn. 25 för att visa att om R är ett huvudidealområde så har R entydig faktoruppdelning.

2.27. Låt R vara ett huvudidealområde. Om $a, b \in R$ så definierar man största gemensamma delaren $\mathrm{SGD}(a, b)$ till a, b som ett element $d \in R$ sådant att

(i) $d|a$ och $d|b$,

och

(ii) om $d'|a$ och $d'|b$ så $d'|d$.

Visa att om $a \neq 0$ eller $b \neq 0$ så är d entydigt bestämd så när som på associering och att det finns $x, y \in R$ sådana att $d = ax + by$. (Man definierar ofta $\mathrm{SGD}(0, 0) = 0$.)

2.28. Visa att $R[X]$ är UFD om R är UFD.

APPENDIX B: ZORNS LEMMA

(B.1) Definition. En relation $\leq$ på en mängd X kallas för **partiell ordning** om

(a) $x \leq x$,

(b) $x \leq y$ och $y \leq z \Rightarrow x \leq z$,

(c) $x \leq y$ och $y \leq x \Rightarrow x = y$,

där $x, y, z \in X$. Om $x \leq y$ kommer vi också att skriva $y \geq x$. □

(B.2) Exempel. (a) $(\mathbb{R}, \leq)$; (b) $X=$ alla delmängder till en mängd M med avseende på $\subseteq$; (c) $(\mathbb{N}, |)$, där $|$ betecknar delbarhet. □

(B.3) Definition. Ett element $x^* \in X$ kallas **maximalt** (m a p $\leq$) om $x^* \leq x$, där $x \in X$ medför att $x = x^*$. Ett element $y_0 \in X$ kallas **majorant** för en delmängd $Y \subseteq X$ om $y \leq y_0$ för varje $y \in Y$. En delmängd $Y \subseteq X$ kallas en **kedja** om $\forall_{y_1, y_2 \in Y}\, y_1 \leq y_2$ eller $y_2 \leq y_1$. □

(B.4) Zorns Lemma. *Låt $(X, \leq)$ vara en partiellt ordnad mängd, $X \neq \emptyset$. Om varje kedja i X har en majorant så innehåller X ett maximalt element. Mera exakt existerar för varje $x \in X$ ett maximalt element x^* sådant att $x \leq x^*$.*

Zorns Lemma är ekvivalent med urvalsaxiomet. Som exempel visar vi:

(B.5) Sats. *Varje äkta ideal i en kommutativ ring med etta ligger i ett maximalideal.*

Bevis. Låt I_0 vara ett äkta ideal i R. Låt $X = \{\text{alla ideal} \neq R \text{ som innehåller } I_0\}$. Då är $X \neq \emptyset$ ty $I_0 \in X$. Betrakta X med $\subseteq$. Låt $Y \subseteq X$ vara en kedja och $J = \cup_{I \in Y} I$. Vi påstår att J är ett äkta ideal. Låt $r_1, r_2 \in J$ dvs $r_1 \in I_1 \in Y$ och $r_2 \in I_2 \in Y$, där $I_1 \subseteq I_2$ eller $I_2 \subseteq I_1$. Alltså är $r_1 - r_2 \in I_1$ eller $r_1 - r_2 \in I_2$, vilket ger $r_1 - r_2 \in J$. Om $r \in R$ och $r' \in J$ dvs $r' \in I$ för något $I \in Y$, så är $rr' \in I \subseteq J$. Alltså är J ett ideal som innehåller I_0 (ty $I_0 \subseteq I \in Y$). Det är äkta ty $1 \notin J$. J är dessutom en majorant för Y. Enligt Zorns Lemma existerar ett maximalt element $I^* \in X$, vilket betyder just att I^* är ett maximalideal som innehåller I_0. □

Kapitel 3

MODULER ÖVER RINGAR

Begreppet modul över en ring generaliserar begreppet vektorrum över en kropp – rent formellt ersätter man skalärer från en kropp med skalärer från en ring. Beroende på att ringar utgör en betydligt bredare och rikare klass än kroppar leder modulbegreppet till mycket djupare resultat än linjär algebra har att erbjuda. Flera viktiga resultat i gruppteorin eller i linjär algebra visas för övrigt med hjälp av moduler över ringar som inte är kroppar (t ex fundamentalsatsen om ändligt genererade abelska grupper och satsen om Jordans normalform för linjära avbildningar visas i Kap. 8 med hjälp av samma sats om moduler över huvudidealringar). Modulbegreppet, liksom ringbegreppet, är mycket allmänt så att mera intressanta resultat endast kan förväntas om man betraktar lämpliga klasser av ringar eller moduler. I detta kapitel introduceras de mest grundläggande egenskaperna hos moduler över ringar. Som ett specialfall betraktar vi moduler över kroppar dvs vektorrum. På det sättet kan detta kapitel betraktas som en repetition av flera viktiga egenskaper hos vanliga vektorrum. Vi skall dock försöka introducera olika begrepp för helt godtyckliga ringar. R kommer att beteckna en associativ ring med etta och vi förutsätter att varje ringhomomorfism avbildar ettan i den ena ringen på ettan i den andra. Om ringen R är en kropp kommer vi som regel skriva K i stället för R.

(3.1) Definition. En vänster R–**modul** är en abelsk grupp M sådan att mot varje $r \in R$ och $m \in M$ svarar $rm \in M$ så att

(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 $m, m_1, m_2 \in M$. En höger R-modul definieras analogt. Om $R = K$ är en kropp så kallas K-moduler för **vektorrum** eller **linjära rum** över kroppen K. Deras element kallas då **vektorer**.

□

I fortsättningen menar vi alltid med en R–modul (utan adjektiv) en vänster R–modul.

(3.2) Exempel. (a) Låt $R = \mathbb{Z}$ och $M = G$, där G är en godtycklig abelsk grupp. Om man definierar $\mathbb{Z} \times G \to G$ som den vanliga multipeln: $(n, g) \mapsto ng$ så förvandlas G till en $\mathbb{Z}$-modul.

(b) Låt R vara en ring och I ett vänsterideal i R. Då är I en R-modul om man definierar $R \times I \to I$ genom $(r, i) \mapsto ri$. I synnerhet är R en R-modul (med $I = R$).

(c) Låt $\varphi : R \to R'$ vara en ringhomomorfism och N en R'-modul. Då kan N betraktas som R-modul om man definierar $rn := \varphi(r)n$ (dvs $R \times N \to N$ ges av $(r, n) \mapsto \varphi(r)n$). I synnerhet kan R' betraktas som R-modul. Till exempel är R' en R-modul då $R \subseteq R'$ (φ är inbäddningen). Ett annat viktigt specialfall får vi då $\varphi : R \to R/I$, där I är ett ideal i R och φ den naturliga surjektionen – R/I är en R-modul (via φ).

(d) Låt M_i för $i \in J$ vara R-moduler. Mängden av alla vektorer $(m_i)_{i\in J}$ sådana att $m_i \in M_i$ är en R-modul då man definierar $(m_i) + (m_i') = (m_i + m_i')$ och $r(m_i) = (rm_i)$. Den modulen betecknas med $\prod_{i\in J} M_i$ och kallas **(direkta) produkten** av M_i, $i \in J$. Man skriver också $M_1 \times \cdots \times M_n$ då $J = \{1, \ldots, n\}$. Med **direkta summan** av M_i, $i \in J$ menas mängden av alla (m_i) sådana att $m_i = 0$ för nästan alla $i \in J$, med avseende på addition och multiplikation som ovan. Direkta summan av M_i betecknas med $\coprod_{i\in J} M_i$. I stället för "direkt summa" säger man ofta "**koprodukt**". Det är klart att den direkta produkten och den direkta summan sammanfaller då J är ändlig. Se vidare Övn. 3.7.

□

(3.3) Anmärkning. Definition (3.1) kan formuleras på följande sätt. Låt $\mathrm{End}(M)$ vara mängden av alla endomorfismer av M dvs funktioner $f : M \to M$ sådana att $f(m_1 + m_2) = f(m_1) + f(m_2)$. $\mathrm{End}(M)$ är en ring då $(f + g)(m) = f(m) + g(m)$ och $(fg)(m) = f(g(m))$ för $m \in M$. Nu har vi att M är en R-modul då och endast då det finns en homomorfism av ringar $\Phi : R \to \mathrm{End}(M)$ sådan att $1 \mapsto Id$ (den identiska avbildningen av M). I själva verket, om M är en R-modul så definierar vi $\Phi : R \to \mathrm{End}(M)$ genom $\Phi(r)(m) = rm$. Då har vi enligt (3.1) (a):

$$\Phi(r)(m_1 + m_2) = r(m_1 + m_2) = rm_1 + rm_2 = \Phi(r)(m_1) + \Phi(r)(m_2),$$

dvs $\Phi(r) \in \mathrm{End}(M)$. Vidare är enligt (3.1) (b) och (c):

$$\Phi(r_1 + r_2)(m) = (r_1 + r_2)m = r_1m + r_2m = \Phi(r_1)(m) + \Phi(r_2)(m) = [\Phi(r_1) + \Phi(r_2)](m),$$

$$\Phi(r_1r_2)(m) = (r_1r_2)m = r_1(r_2m) = \Phi(r_1)(\Phi(r_2)(m)) = (\Phi(r_1)\Phi(r_2))(m),$$

dvs $\Phi(r_1+r_2) = \Phi(r_1)+\Phi(r_2)$ och $\Phi(r_1r_2) = \Phi(r_1)\Phi(r_2)$ så att Φ är en ringhomomorfism. Till sist är $\Phi(1)(m) = 1m = m$ enligt (3.1)(d) så att $\Phi(1) = Id$. Omvänt, om $\Phi : R \to \mathrm{End}(M)$ är en homomorfism sådan att $\Phi(1) = Id$, så visar samma resonemang att M är en R-modul (med $rm = \Phi(r)(m)$). Funktionen Φ kallas ofta för en **representation** av R (i endomorfismringen av M) (se vidare Övn. 3 och Kapitel 9 i samband med grupprepresentationer).

□

(3.4) Definition. Man säger att en funktion $f : M \to N$, där M, N är R-moduler, är en **R-homomorfism** om

$$f(m_1 + m_2) = f(m_1) + f(m_2) \quad \text{och} \quad f(rm) = rf(m).$$

Mängden av alla R-homomorfismer $f : M \to N$ betecknas med $\mathrm{Hom}_R(M, N)$. Om $R = K$ är en kropp så säger man oftast att f är en **linjär avbildning** eller en **linjär transformation**.

□

$\mathrm{Hom}_R(M, N)$ är en abelsk grupp då $(f+g)(m) = f(m)+g(m)$. Om R är en kommutativ ring så är $\mathrm{Hom}_R(M, N)$ en R-modul då $(rf)(m) = rf(m)$ (kontrollera!). Termerna epimorfism (dvs surjektiv homomorfism), monomorfism (dvs injektiv homomorfism), isomorfism, automorfism och endomorfism används för modulhomomorfismer i exakt samma betydelse som för grupper.

(3.5) Exempel. Låt R vara en kommutativ ring och M en R–modul. Låt $r_0 \in R$. Då är $f : M \to M$, där $f(m) = r_0m$ en R-homomorfism ty

$$f(m_1 + m_2) = r_0(m_1 + m_2) = r_0m_1 + r_0m_2 = f(m_1) + f(m_2)$$

och

$$f(rm) = r_0(rm) = (r_0r)m = (rr_0)m = r(r_0m) = rf(m).$$

□

Nu skall vi diskutera delmoduler och kvotmoduler.

(3.6) Definition. Låt M vara en R–modul. En (R–)**delmodul** N till M är en delgrupp $N \subseteq M$ sådan att $rn \in N$ för varje $r \in R$ och $n \in N$. Om R är en kropp så ersätter man oftast termen delmodul med termen **delrum** eller **underrum**.

□

(3.7) Exempel. (a) Om M är en R-modul och $m \in M$ så är $Rm = \{rm : r \in R\}$ en delmodul till M. Mera allmänt, om $m_i \in M$, där $i \in J$ (en indexmängd), så är mängden $\sum_{i\in J} Rm_i$ av alla ändliga linjärkombinationer $\sum_{i\in J} r_i m_i$ en delmodul N till M. Man säger att mängden av alla m_i, $i \in J$, genererar N. Elementen m_i kallas då **generatorer** för N. Om M är genererad av ett ändligt antal av sina element dvs $M = Rm_1 + \cdots + Rm_k$, där $m_i \in M$, så säger man att M är en **ändligt genererad** modul. Om $M = Rm$ så kallas den **cyklisk**.

(b) Om N_i, $i \in J$ är delmoduler till M så är också deras snitt $\cap_{i\in J} N_i$ och deras summa $\sum N_i$ delmoduler till M. Med $\sum N_i$ menas mängden av alla summor $\sum n_i$, där $n_i \in N_i$ och $n_i = 0$ för nästan alla $i \in J$.

(c) Låt I vara ett vänsterindeal i R och M en R-modul. Då är $IM = \{\sum i_k m_k$ (ändlig summa), $i_k \in I$, $m_k \in M\}$ en delmodul till M.

□

(3.8) Proposition. *Låt N vara en delmodul till M och M/N kvotgruppen av de abelska grupperna M och N. Då är M/N en R-modul om man definierar $r(m+N) := rm+N$. Den naturliga surjektionen $M \to M/N$ är då en R-epimorfism.*

Bevis. Vi har

$$m_1 + N = m_2 + N \Leftrightarrow m_1 - m_2 \in N \Rightarrow r(m_1 - m_2) \in N \Rightarrow rm_1 + N = rm_2 + N$$

dvs multiplikationen $(r, m + N) \mapsto rm + N$ är korrekt definierad. Det är mycket lätt att kontrollera villkoren (a)–(d) i definitionen (3.1). För den naturliga surjektionen $f : M \to M/N$ har vi $f(rm) = rm + N = r(m + N) = rf(m)$. □

(3.9) Definition. Låt $f : M \to N$ vara en homomorfism av R-moduler. Med **kärnan** till f menas $\mathrm{Ker}f = \{m \in M : f(m) = 0\}$. **Bilden** $f(M)$ av M betecknas ofta med $\mathrm{Im}f$. Med **kokärnan** av f menar man $\mathrm{Coker}f = N/\mathrm{Im}f$, och **kobilden** $\mathrm{Coim}f = M/\mathrm{Ker}f$. Om $R = K$ är en kropp och således är $f : M \to N$ en linjär avbildning så kallas kärnan till f för **nollrummet** (till f), och bilden av f kallas för **värderummet** (till f).

□

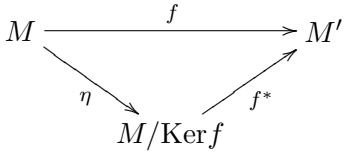
(3.10) Proposition. *Om $f : M \to N$ är en R-homomorfism så är* $\mathrm{Ker}f$ *en delmodul till M och* $\mathrm{Im}f$ *är en delmodul till N. (Om $R = K$ är en kropp så är nollrummet till f ett delrum till M och värderummet till f är ett delrum till N.)*

Bevis. Det är klart att $\mathrm{Ker}f$ är en delgrupp till M och $\mathrm{Im}f$ är en delgrupp till N. Om $m \in M$ och $r \in R$ så är $f(rm) = rf(m) = 0$ dvs $rm \in \mathrm{Ker}f$. Om $f(m) \in \mathrm{Im}f$ och $r \in R$ så är $rf(m) = f(rm) \in \mathrm{Im}f$. □

(3.11) Proposition. *Om $f : M \to M'$ är R-homomorfism så definierar $f^*(m + \mathrm{Ker}f) = f(m)$ en R-isomorfism $M/\mathrm{Ker}f \cong \mathrm{Im}f$.*

Bevis. Vi vet att f^* är en isomorfism av (de abelska) grupperna $M/\mathrm{Ker}f$ och $\mathrm{Im}f$ (se (1.38)). Men $f^*(r(m + \mathrm{Ker}f)) = f^*(rm + \mathrm{Ker}f) = f(rm) = rf(m) = rf^*(m + \mathrm{Ker}f)$ så att f^* är R-linjär. □

(3.12) Anmärkning. Precis som (1.38) för grupper och (2.16) för ringar kan (3.11) formuleras på följande sätt: Om $f : M \to M'$ är en R-homomorfism så existerar exakt en monomorfism $f^* : M/\mathrm{Ker}f \to M'$ sådan att diagrammet:



kommuterar (η är den naturliga surjektionen) dvs $f^*\eta = f$.

□

(3.13) Proposition. *En R-homomorfism $f : M \to M'$ är injektiv (= en monomorfism) då och endast då* $\mathrm{Ker}f = (0)$.

Bevis. "⇒" $x \in \mathrm{Ker}f \Rightarrow f(x) = 0 \Rightarrow f(x) = f(0) \Rightarrow x = 0$.

"⇐" Låt $\mathrm{Ker}f = (0)$. Om $f(x_1) = f(x_2)$ så är $f(x_1 - x_2) = 0$ dvs $x_1 - x_2 = 0$. Alltså är $x_1 = x_2$. □

(3.14) Proposition. *Låt I vara ett ideal i en ring R och M en R-modul. Då är M/IM en R/I-modul då man definierar $(r + I)(m + IM) = rm + IM$.*

Bevis. Produkten $(r + I, m + IM) \mapsto rm + IM$ är korrekt definierad ty $r + I = r' + I$ och $m+IM = m'+IM$ ger att $r-r' \in I$ och $m-m' \in IM$ dvs $rm-r'm' = (r-r')m+r'(m-m') \in IM$ så att $rm + IM = r'm' + IM$. Villkoren (a)–(d) i (3.1) följer nu direkt. □

De moduler över ringar som ligger närmast vektorrum över kroppar kallas fria.

(3.15) Definition. En R-modul F kallas **fri** om den har en R–**bas** dvs om det finns element $e_i \in F$, $i \in J$ sådana att varje element $x \in F$ kan skrivas entydigt som en linjärkombination

med koefficienter i R av ett ändligt antal e_i. Detta betyder att om $x \in F$ så är $x = \sum_{i \in J} r_i e_i$, där $r_i \in R$ och nästan alla $r_i = 0$ samt en sådan framställning är entydig. Nollmodulen $F = (0)$ är definitionsmässigt fri.

□

(3.16) Anmärkning. Villkoret i (3.15) som säger att varje $x \in F$ har framställning $x = \sum r_i e_i$ med ändligt många e_i och entydigt bestämda koefficienter r_i kan ersättas med villkoret att $x = \sum r_i e_i$ (a'priori ej nödvändigt entydigt) och e_i, $i \in J$, är **linjärt oberoende** dvs om $\sum r_i e_i = 0$ med nästan alla $r_i = 0$ så är alla $r_i = 0$. Ekvivalensen av dessa två villkor kontrolleras mycket enkelt och lämnas som Övn. 18. Rent allmänt säger man att en delmängd B till F är linjärt oberoende om $\sum r_i e_i = 0$ med $e_i \in B$, $r_i \in R$ och nästan alla $r_i = 0$ implicerar att alla $r_i = 0$. Man uttrycker detta villkor så att varje ändligt delmängd till B är linjärt oberoende.

□

(3.17) Exempel. (a) Om K är en kropp och V är ett godtyckligt linjärt rum över K så är V en K-fri modul. Detta påstående är ett standardexempel på en tillämpning av Zorns Lemma och lämnas som en viktig övning – se Övn. 19 och eventuellt dess lösning. I denna övning visar vi att varje delmängd till V bestående av linjärt oberoende vektorer i ett vektorrum kan kompletteras till en bas för hela rummet. Om ett rum har en ändlig bas så är alla baser ändliga och har lika många element (se Övn. 20). Ett mera allmänt resultat som säger att alla baser för ett och samma vektorrum har samma kardinalitet är lite svårare att bevisa och kräver något djupare kunskaper om aritmetiken av kardinaltal.

(b) Om R är en godtycklig ring och J en godtycklig indexmängd så finns det en fri R-modul med bas e_i, $i \in J$. Man kan konstruera en sådan modul på följande sätt. Låt F vara mängden av alla funktioner $f : J \to R$ sådana att $f(i) = 0$ för nästan alla $i \in J$. F är en R-modul med addition av funktioner dvs $(f + g)(i) = f(i) + g(i)$ och multiplikation $(rf)(i) = rf(i)$. Låt $e_i : J \to R$ vara funktionen som definieras genom $e_i(j) = \delta_{ij}$ (dvs $\delta_{ij} = 0$ om $i \neq j$ och $\delta_{ii} = 1$). Då bildar e_i, $i \in J$, en bas för F ty för $f : J \to R$ har vi $f = \sum f(i)e_i$ och en sådan framställning är entydig. F kan helt enkelt definieras som $\coprod_{i \in J} M_i$, där $M_i = R$ för varje $i \in J$. Ibland betecknar man den modulen med $R^{|J|}$.

□

Vårt nästa resultat säger att en R–homomorfism av en fri modul i en helt godtycklig modul över R definieras och bestäms entydigt av bilderna av baselementen.

(3.18) Proposition. *Låt R vara en ring och F en fri R-modul med bas e_i, $i \in J$. Om M är en godtycklig R-modul och m_i, $i \in J$, godtyckligt valda element i M så existerar en och endast en R-homomorfism $f : F \to M$ sådan att $f(e_i) = m_i$. Om m_i, $i \in J$ bildar en bas för M (dvs M är fri med bas m_i, $i \in J$) så är f en isomorfism.*

Bevis. Om $x = \sum r_i e_i$ (med entydigt bestämda r_i!) så definierar vi $f(x) = \sum r_i m_i$. Då får vi en R-homomorfism sådan att $f(e_i) = m_i$. Om $g : F \to M$ är en R-homomorfism sådan att $g(e_i) = m_i$ så är $g(x) = g(\sum r_i e_i) = \sum r_i g(e_i) = \sum r_i m_i = f(x)$ dvs $g = f$. Om nu m_i bildar en bas för M så ger $f(x) = \sum r_i m_i = 0$ att $r_i = 0$ dvs f är en monomorfism (se (3.13)). Men f är också en epimorfism (trivialt) så att f är en isomorfism. □

(3.19) Följdsats. *Om F, F' är två fria R-moduler med baser vars kardinaliteter är lika så är F och F' R-isomorfa.*

Bevis. Om e_i, $i \in J$, är en bas för F och e'_i, $i \in J$, för F' så ordnar vi e'_i mot e_i. Då får vi en R-isomorfism $\sum r_i e_i \mapsto \sum r_i e'_i$ enligt (3.18). □

Det är klart att en R–modul F' som är isomorf med en fri R–modul F är också fri och har bas av samma kardinalitet som F – om $f : F \to F'$ är en sådan isomorfism och e_i, $i \in J$, bildar en bas för F så bildar $f(e_i)$ en bas för F'.

(3.20) Proposition. *Låt R vara en kommutativ ring med etta och F en fri R-modul. Då har två godtyckliga baser för F samma kardinalitet.*

Bevis. Låt e_i, $i \in J$, vara en bas för F över R och låt I vara ett maximalideal i R (se Appendix B, (B.5)). Låt oss betrakta R/I-modulen F/IF (se (3.14)). Det är en fri R/I-modul med bas $\bar{e}_i$, $i \in J$, där $\bar{e}_i = e_i + IF$. Vi har nämligen $\bar{x} = \sum \bar{r}_i \bar{e}_i$ då $x = \sum r_i e_i$ så att F/IF genereras av $\bar{e}_i$ ($\bar{x} = x + IF$). Vidare ger $\sum \bar{r}_i \bar{e}_i = \bar{0}$ att $\sum r_i e_i \in IF$, vilket implicerar att alla $r_i \in I$ (ty e_i, $i \in J$, är en bas för F). Alltså är $\bar{r}_i = \bar{0}$ dvs $\bar{e}_i$ är linjärt oberoende. Men R/I är en kropp (se (2.28)) så att F/IF är ett vektorrum över R/I. Vi vet att två baser för ett linjärt rum har samma kardinalitet (se också Övn. 20). Detta implicerar att varje bas för F har samma kardinalitet som basen e_i, $i \in J$. □

(3.21) Definition. Om alla baser för en fri R-modul F har samma kardinalitet (t ex om F är fri över en kommutativ ring R – se (3.20)) så kallas denna kardinalitet för **rangen** av F över R och betecknas med $\mathrm{rg}_R F$. Om $R = K$ är en kropp talar man i stället om **dimensionen** av F över K som betecknas med $\dim_K F$.

□

I samband med övningar kommer vi i kontakt med vektorrum som har oändliga baser (se Övn. 24), men fria moduler (vektorrum) som vi möter i fortsättningen kommer oftast att ha ändlig rang (dimension).

En mycket viktig konstruktion ordnar mot varje fri R-modul dess duala modul.

(3.22) Definition. Låt M vara en R-modul över en ring R. Med **duala modulen** till M menar man $M^* = \mathrm{Hom}_R(M, R)$ (se (3.4)).

□

(3.23) Proposition. *Om F är en fri R-modul,* $\dim_R F = n$ *och e_i, $i = 1, \ldots, n$ är en bas för F över R så bildar R–homomorfismerna $f_i : F \to R$ sådana att $f_i(e_j) = \delta_{ij}$ för $i = 1, 2, \ldots, n$ en bas för F^* (den* **duala** *basen till e_i, $i = 1, \ldots, n$). I synnerhet är F^* fri och* $\mathrm{rang}_R F^* = \mathrm{rang}_R F$.

Bevis. Notera först att f_i är väl–definierade som R–homomorfismer enligt (3.18). Om $f \in F^*$ så är $f = \sum_{i=1}^n f(e_i)f_i$ ty för varje vektor e_j har vi

$$(\sum_{i=1}^{n} f(e_i)f_i)(e_j) = \sum_{i=1}^{n} f(e_i)f_i(e_j) = f(e_j)$$

dvs $\sum_{i=1}^n f(e_i)f_i$ och f är lika på alla basvektorer. Alltså är $f = \sum f(e_i)f_i$. Vidare ger $f = \sum a_i f_i$ att $f(e_j) = (\sum a_i f_i)(e_j) = a_j$ så att representationen av f är entydig. □

(3.24) Proposition. *Låt V vara ett vektorrum över en kropp K. Då existerar en naturlig monomorfism $\Phi : V \longrightarrow V^{**}$ som mot $v \in V$ ordnar $\Phi(v)$, där $\Phi(v)(f) = f(v)$ då $f \in V^*$. Om* $\dim_K V < \infty$ *så är Φ en isomorfism.*

Bevis. Vi har

$$\Phi(v_1 + v_2)(f) = f(v_1 + v_2) = f(v_1) + f(v_2) = \Phi(v_1)(f) + \Phi(v_2)(f) = (\Phi(v_1) + \Phi(v_2))(f),$$

dvs $\Phi(v_1 + v_2) = \Phi(v_1) + \Phi(v_2)$. Vidare är

$$\Phi(av)(f) = f(av) = af(v) = (a\Phi(v))(f),$$

dvs $\Phi(av) = a\Phi(v)$. Detta visar att Φ är en homomorfism av K-vektorrum. Vi har $\mathrm{Ker}\Phi = \{v \in V : \Phi(v)(f) = f(v) = 0 \quad \forall_{f \in V^*}\} = (0)$ ty om $v \in V$ och $v \neq 0$ så existerar $f : V \to K$ sådan att $f(v) \neq 0$ (komplettera $v \neq 0$ till en bas för V och definiera f så att $f(v) \neq 0$ enligt (3.18)). Alltså är Φ en monomorfism (se (3.13)) så att $\dim_K V = \dim_K \Phi(V)$. Om $\dim_K V < \infty$ så är $\dim_K V = \dim_K V^* = \dim_K V^{**}$ enligt (3.23). I detta fall är alltså $\dim_K \Phi(V) = \dim_K V^{**}$ dvs $\Phi(V) = V^{**}$ så att Φ är en isomorfism (se vidare Övn. 26). □

Vi avslutar detta kapitel med en viktig definition som vi utnyttjar i senare kapitel och i samband med övningar.

(3.25) Definition. Man säger att en sekvens

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

av R-moduler och R-homomorfismer är **exakt** om $\mathrm{Im}f = \mathrm{Ker}g$.

□

(3.26) Exempel. (a) $0 \to M' \xrightarrow{f} M$ är exakt då och endast då $\mathrm{Ker}f = 0$ dvs f är en monomorfism. $M \xrightarrow{g} M'' \to 0$ är exakt då och endast då $\mathrm{Im}g = M''$ dvs g är en epimorfism.

(b) Låt $f : M \to N$ vara en homomorfism. Då är sekvensen

$$0 \longrightarrow \mathrm{Ker}f \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{p} \mathrm{Coker}f \longrightarrow 0$$

exakt, där i är inbäddaningen och $p : N \to N/\mathrm{Im}f = \mathrm{Coker}f$ den naturliga surjektionen.

(c) Låt $M = M_1 \times M_2$ (se (3.2) (e)). Då är

$$0 \longrightarrow M_1 \xrightarrow{i} M_1 \times M_2 \xrightarrow{p_2} M_2 \longrightarrow 0$$

exakt då $i(m_1) = (m_1, 0)$ och $p_2(m_1, m_2) = m_2$.

(d) I $M' \xrightarrow{f} M \xrightarrow{g} M''$ har vi $\mathrm{Im}f \subseteq \mathrm{Ker}g$ då och endast då $gf = 0$.

□

ÖVNINGAR

3.1. Låt R vara en ring och M en R-modul. Låt $\mathrm{End}_R(M)$ (se (3.3)) vara endomorfismringen av M. Visa att M är en $\mathrm{End}_R(M)$-modul då man definierar $\mathrm{End}_R(M) \times M \to M$ genom $(f, m) \mapsto f(m)$.

3.2. Låt V vara ett vektorrum över en kropp K och $F : V \to V$ en linjär avbildning. Visa att V är en $K[X]$-modul då man definierar $p(X)v = a_0v + a_1F(v) + \ldots + a_nF^n(v)$, där $p(X) = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ och $v \in V$.

3.3. Låt G vara en grupp, K en kropp och $K[G]$ gruppringen för G över K (se (2.2) (h)). Med en representation av G över K menas en grupphomomorfism $G \to GL_K(V)$, där $GL_K(V)$ betecknar gruppen av alla inverterbara linjära avbildningar av V över K. Visa att det finns en en-entydig motsvarighet mellan alla representationer av G över K och alla $K[G]$-moduler V.

3.4. Låt R vara en ring och M en R-modul.

(a) Visa att $\mathrm{Ann}(M) = \{r \in R : rM = 0\}$ är ett ideal i R ($rM = \{rm, m \in M\}$).

(b) Visa att M är en $R/\mathrm{Ann}(M)$ modul då $\bar{r}m := rm$ för $r \in R$, $m \in M$. Idealet $\mathrm{Ann}(M)$ kallas **annulatorn** av M.

3.5. Låt R vara en ring och $f : R \to R$ en endomorfism av R som en vänster R-modul. Visa att det finns $r_0 \in R$ så att $f(r) = rr_0$ för $r \in R$.

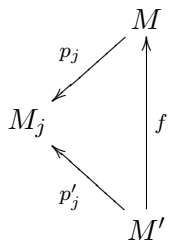
3.6. Låt I_1, I_2 vara två ideal i en ring med etta R sådana att det finns en R-isomorfism av R-moduler R/I_1 och R/I_2. Visa att $I_1 = I_2$. (Observera att R/I betraktas som R-modul i enlighet med (3.2)(d)).

3.7. (a) Låt M_1, M_2 vara delmoduler till en R-modul M. Man säger att M är en (intern) **direkt summa** av M_1 och M_2 om varje element $m \in M$ har en entydig framställning $m = m_1 + m_2$, där $m_1 \in M_1$, $m_2 \in M_2$. Visa att $M \cong M_1 \times M_2$ ($= M_1 \coprod M_2$). Ofta skriver man $M = M_1 \oplus M_2$.

(b) Generalisera (a) till ett påstående om en godtycklig familj $(M_i)_{i \in J}$ av delmoduler till M.

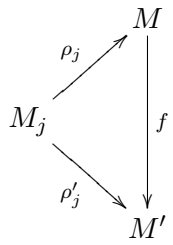
3.8. Låt $M' \xrightarrow{f} M \xrightarrow{g} M'$ vara en sekvens av R-moduler och R-homomorfismer sådana att $gf = id_{M'}$. Visa att $M = \mathrm{Im}f \oplus \mathrm{Ker}g$.

3.9. (a) Låt $M = \prod_{i \in J} M_i$, där M_i är R-moduler och låt $p_j : M \to M_j$ definieras av $p_j((m_i)) = m_j$. Visa att för varje R-modul M' och R-homomorfismer $p'_j : M' \to M_j$ existerar exakt en R-homomorfism $f : M' \to M$ sådan att alla diagram



kommuterar.

(b) Låt $M = \coprod_{i\in J} M_i$ och låt $\rho_j : M_j \to M$ ges av $\rho_j(m_j) = (m_i)_{i\in J}$, där $m_i = 0$ då $i \neq j$. Visa att för varje R-modul M' och R-homomorfismer $\rho'_j : M_j \to M'$ existerar exakt en R-homomorfism $f : M \to M'$ sådan att alla diagram



kommuterar.

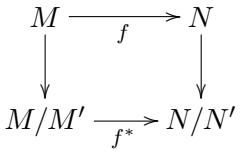
3.10. Låt N_1, N_2 vara delmoduler till en R-modul M. Visa att

(a) $\frac{N_1+N_2}{N_1} \cong \frac{N_2}{N_1\cap N_2}$,

(b) om $N_1 \subseteq N_2$ så är $\frac{M}{N_2} \cong \frac{M/N_1}{N_2/N_1}$.

3.11. Låt $f : M \to N$ vara en R-homomorfism av R-moduler. Visa att funktionen $N' \mapsto f^{-1}(N')$ avbildar en–entydigt alla delmoduler till N på alla delmoduler till M som innehåller $\operatorname{Ker} f$.

3.12. Låt $f : M \to N$ vara en R-homomorfism av R-moduler sådan att $f(M') \subseteq N'$, där $M' \subseteq M$ och $N' \subseteq N$ är delmoduler. Visa att det finns exakt en R-homomorfism $f^* : M/M' \to N/N'$ sådan att diagrammet



kommuterar. Visa också att $\operatorname{Ker} f^* = \frac{f^{-1}(N')}{M'}$ och $\operatorname{Im} f^* = \frac{f(M)+N'}{N'}$.

3.13. Låt M vara en R-modul. Visa att M är ändligt genererad då och endast då det finns en epimorfism $R^n \to M$ ($R^n = R \times R \times \ldots \times R$, n faktorer R).

3.14. Visa att följande ringar R' är fria som R-moduler då

(a) $R = \mathbb{Z}, R' = \mathbb{Z}[X]$; (b) $R = \mathbb{Z}[X^3], R' = \mathbb{Z}[X]$;
(c) $R = \mathbb{Z}, R' = \mathbb{Z}[\sqrt[3]{5}]$; (d) $R = \mathbb{Z}[\sqrt[4]{2}], R' = \mathbb{Z}[\sqrt{2}]$.

3.15. Visa att följande ringar R' inte är fria som R-moduler:

(a) $R = \mathbb{Z}$, $R' = \mathbb{Q}$; (b) $R = \mathbb{Z}$, $R' = \mathbb{Z}[\frac{1}{2}]$;
(c) $R = \mathbb{Z}[\frac{1}{2}]$, $R' = \mathbb{Q}$; (d) $R = \mathbb{Q}[X^2, X^3]$, $R' = \mathbb{Q}[X]$.

3.16. Låt $R^* = C_{\mathbb{R}}[0,1]$ vara ringen av alla kontinuerliga funktioner på $[0,1]$. Låt $R = \{f \in R^* : f(0) = f(1)\}$ och $M = \{f \in R^* : f(0) = -f(1)\}$. Visa att

(a) R är en delring till R^* och M en R-delmodul till R^*.

(b)* $M \oplus M \cong R \oplus R$ som R-moduler men $M \ncong R$ (visa att M inte är fri).

(c) Om R^* = ringen av alla funktioner på $[0,1]$ så är $M \cong R$.

3.17. Låt V vara ett linjärt rum över en kropp K och låt B vara en delmängd till V. Visa att följande egenskaper är ekvivalenta (bägge definierar begreppet bas i ett linjärt rum):

(a) Varje element i V kan skrivas entydigt som en linjärkombination av ett ändligt antal element i B dvs för varje $v \in V$ är $v = \sum_i a_i e_i$ med (ändligt många) $e_i \in B$, $a_i \in K$ och framställningen är entydig (dvs om $v = \sum_i a_i e_i = \sum_i a_i' e_i$ så är $a_i = a_i'$).

(b) Varje element i V kan skrivas som en linjärkombination av ändligt många element i B (dvs B genererar V) och B är linjärt oberoende dvs om $\sum a_i e_i = 0$, med $a_i \in K$ och $e_i \in B$ så är alla $a_i = 0$.

3.18. Låt V vara ett linjärt rum över en kropp K och låt B vara en icke–tom delmängd till V. Visa att följande tre egenskaper är ekvivalenta:

(a) B är en bas för V,

(b) B är en maximal linjärt oberoende delmängd till V dvs B är linjärt oberoende i V (se (3.16)) och $B \cup \{v\}$ är linjärt beroende för varje vektor $v \in V$,

(c) B är en minimal mängd av generatorer för V dvs B genererar V (se (3.7)) och varje äkta delmängd till B saknar denna egenskap.

3.19. Låt V vara ett vektorrum över K och W ett delrum till V.

(a) Visa att om $V \neq (0)$ så existerar en bas för V över K.

(b) Visa att varje linjärt oberoende uppsättning av vektorer i V kan kompletteras till en bas.

(c) Visa att varje bas för W kan kompletteras till en bas för V.

Lösning till (a) och (b). Låt oss kalla en delmängd E till V linjärt oberoende om varje likhet $\sum a_i e_i = 0$ med ändligt många $e_i \in E$ och $a_i \in K$ implicerar att alla $a_i = 0$. Låt E_0 vara en linjärt oberoende delmängd till V och X mängden av alla linjärt oberoende delmängder till V som innehåller E_0 med partiell ordning given av $\subset$. Låt oss notera att (a) följer ur (b) ty som E_0 kan väljas t.ex. $E_0 = \{v\}$, $v \in V$, $v \neq 0$. Låt Y vara en kedja i X och $E_Y = \cup_{E \in Y} E$. Då är E_Y linjärt oberoende ty om $\sum a_i e_i = 0$, där $e_i \in E_Y$ så existerar $E_i \in Y$ så att $e_i \in E_i$. Men alla E_i bildar en kedja så att det finns i_0 med $e_i \in E_{i_0}$ för alla i. E_{i_0} är linjärt oberoende vilket ger att alla $a_i = 0$. Detta visar att $E_Y \in X$. Enligt Zorns lemma existerar ett maximalt element i X. Beteckna det med E^*. Nu är E^* en bas för V. Vi vet att E^* är linjärt oberoende. Å andra sidan, om $v \in V$ och $v \notin E^*$ så är $E^* \cup \{v\}$ linjärt beroende som en mängd större än E^*. Alltså finns det en relation $\sum a_i e_i + av = 0$ med a_i, $a \in K$ och inte alla a_i, $a = 0$. Men då $a \neq 0$, ty annars är $e_i \in E^*$ linjärt beroende, vilket är omöjligt. Alltså är $v = -\sum(a_i/a)e_i$ dvs E^* är en bas.

3.20. (a) Låt V vara ett linjärt rum över K och låt $[e_1, \ldots, e_m]$ beteckna linjära delrummet genererat av vektorerna $e_1, \ldots, e_m \in V$ dvs mängden av alla linjärkombinationer $a_1e_1 + \ldots + a_me_m$, där $a_1, \ldots, a_m \in K$. Låt $v = a_1e_1 + \ldots + a_me_m$ och $a_1 \neq 0$. Visa att $[e_1, \ldots, e_m] = [v, e_2, \ldots, e_m]$.

(b) Visa att om ett linjärt rum V har ändlig dimension över K så består två godtyckliga baser för V (över K) av lika många vektorer.

Ledning. Utnyttja (a) för att bevisa (b). Man kan ge ett annat bevis av (b) genom att utnyttja Övn. 23 (b).

3.21. (a) Låt $f : V \to V'$ vara en linjär avbildning av vektorrum över en kropp K. Visa att om e_i, $i \in I$, bildar en bas för $\mathrm{Ker}f$ och e_j, $j \in J$, där $J \supseteq I$, är en utvidgning av denna bas till en bas för V, så bildar $f(e_j)$, där $j \in J \setminus I$ en bas för bilden $\mathrm{Im}f = f(V)$.

(b) Låt V vara ett vektorrum av ändlig dimension över K och W ett delrum till V. Visa att både W och V/W har ändlig dimension och $\dim(V/W) = \dim V - \dim W$.

Anmärkning. Påståendet i (b) brukar kallas **dimensionssatsen.**

3.22. Låt K vara en kropp.

(a) Om $0 \to V' \to V \to V'' \to 0$ är en exakt sekvens av K-vektorrum så är $\dim V = \dim V' + \dim V''$.

(b) Generalisera (a): Om $0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$ är en exakt sekvens av K vektorrum så är $\sum(-1)^i \dim V_i = 0$.

(c) Visa att om $V' \xrightarrow{f} V \xrightarrow{g} V'$ är exakt så är $\dim V = \dim \mathrm{Im}f + \dim \mathrm{Im}g$.

3.23. Låt $V = \mathbb{R}^n$ och $W = \mathbb{R}^m$ vars vektorer betecknas som kolonner. Låt A vara en $m \times n$–matris och låt $f(x) = Ax$ då $x \in \mathbb{R}^n$.

(a) Motivera att f är en linjär avbildning och karakterisera kärnan $\mathrm{Ker}f$ och bilden $\mathrm{Im}f$ i termer av matrisens A rader och kolonner.

(b) Visa med hjälp av dimensionssatsen (se Övn. 21) att om $n > m$ så $\mathrm{Ker}f \neq (0)$. Vad säger detta påstående i termer av linjära ekvationssystem?

(c) Motivera att rangen av matrisen A (som den definieras i inlednde kurser i linjär algebra) är dimensionen av bildrummet $\mathrm{Im}f$. Motivera att ekvationen $Ax = B$, där $B \in \mathbb{R}^m$ har en lösning då och endast då rangen av A är lika med rangen av matrisen A utvidgad med kolonnen B ("rangen av den utvidgade matrisen").

Anmärkning. Kroppen $\mathbb{R}$ i denna övning kan ersättas med en godtycklig kropp K.

3.24. Konstruera baser för följande linjära rum över K:

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

(b) $K = \mathbb{C}$, $V = \mathbb{C}(X)$,

(c) $K = \mathbb{R}$, $V =$ alla periodiska följder $(a_1, a_2, \ldots)$, där $a_i \in \mathbb{R}$ med perioden n.

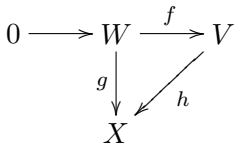
(d) $K = \mathbb{R}$, $V =$ alla periodiska följder $(a_1, a_2, \ldots), a_i \in \mathbb{R}$, av alla ändliga perioder.

3.25. Låt W vara ett delrum till ett linjärt rum V över K. Visa att det finns ett delrum U till V sådant att $V = W \oplus U$.

3.26. Visa att monomorfismen $V \to V^{**}$, V ett vektorrum över K, inte behöver vara en isomorfism (se (3.24)).

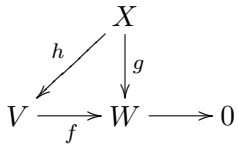
3.27. Låt K vara en kropp, V, W, X linjära rum över K.

(a) Låt $f : W \to V$ vara en monomorfism och $g : W \to X$ en K-homomorfism. Visa att det finns en K-homomorfism $h : V \to X$ så att diagrammet



kommuterar.

(b) Låt $f : V \to W$ vara en epimorfism och $g : X \to W$ en homomorfism. Visa att det finns en homomorfism $h : X \to V$ så att diagrammet



kommuterar.

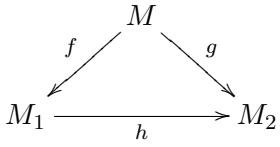
Anmärkning. (a) säger att varje K-vektorrum X är **injektivt**, däremot (b) att det är **projektivt**. Definitionerna av projektiva och injektiva moduler givna i (a) och (b) (då K är en ring) diskuterar vi senare.

(c) Visa att en fri R-modul F är projektiv.

3.28. Låt $W \subseteq V$ vara två vektorrum över K. Låt $W^\perp = \{f \in V^* : \forall_{w \in W} f(w) = 0\}$. Visa att $W^* \cong V^*/W^\perp$ och $\dim W^\perp = \dim V - \dim W$ (då $\dim V < \infty$).

3.29. Låt W_1, W_2 vara delrum till V och $f_1 : W_1 \to U$, $f_2 : W_2 \to U$ K-homomorfismer sådana att $f_1|_{W_1 \cap W_2} = f_2|_{W_1 \cap W_2}$. Visa att det finns en homomorfism $f : V \to U$ sådan att $f|_{W_i} = f_i$ för $i = 1, 2$.

3.30. Låt M vara en R-modul, $f : M \to M_1$ och $g : M \to M_2$ R-homomorfismer. Visa att om f är en epimorfism och $\mathrm{Ker} f \subseteq \mathrm{Ker} g$ så existerar exakt en homomorfism $h : M_1 \to M_2$ så att diagrammet



kommuterar.

3.31. (a) Låt

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d'} \\ N & \xrightarrow[g]{} & N' \end{array}$$

vara ett kommutativt diagram av R-moduler och R-homomorfismer dvs $d'f = gd$. Visa att $f(\operatorname{Ker} d) \subseteq \operatorname{Ker} d'$ och $g(\operatorname{Im} d) \subseteq \operatorname{Im} d'$.

(b) Låt

$$\begin{array}{ccccc} M_1' & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & M_1'' \\ \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} \\ M_2' & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & M_2'' \end{array}$$

vara ett kommutativt diagram av R-moduler och R-homomorfismer med exakta rader. Visa att följderna

$$\operatorname{Ker} d' \longrightarrow \operatorname{Ker} d \longrightarrow \operatorname{Ker} d''$$

och

$$\operatorname{Im} d' \longrightarrow \operatorname{Im} d \longrightarrow \operatorname{Im} d''$$

som induceras i enlighet med (a) också är exakta.

Kapitel 4

TENSORPRODUKTER

Tensorprodukter ger en möjlighet till att ersätta bilinjära funktioner på t ex vektorrum med linjära, vilket har en stor praktisk betydelse. Detta kapitel ägnas åt konstruktioner av tensorprodukter och deras grundläggande egenskaper. Vi förutsätter här att R är en associativ och kommutativ ring med etta. Låt oss repetera en tidigare definition:

(4.1) Definition. Om M, N är R-moduler så betecknar $\mathrm{Hom}_R(M, N)$ R-modulen av alla R-homomorfismer $f : M \to N$ med addition: $(f + g)(m) = f(m) + g(m)$ och multiplikation med elementen ur R: $(rf)(m) = rf(m)$, då $m \in M$ och $r \in R$.

□

R-homomorfismer är R-linjära funktioner. Mycket ofta har man att göra med bilinjära (och multilinjära) funktioner:

(4.2) Definition. Låt M, N, P vara R-moduler. Man säger att en funktion $\varphi : M \times N \to P$ är (R-)bilinjär om:

$$\begin{aligned} \varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n), \quad \varphi(rm, n) = r\varphi(m, n), \\ \varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m_1, n_2), \quad \varphi(m, rn) = r\varphi(m, n), \end{aligned}$$

där $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ och $r \in R$.

Alla bilinjära funktioner bildar en R-modul $\mathrm{Bil}_R(M \times N, P)$ om man definierar:

$$(\varphi + \psi)(m, n) = \varphi(m, n) + \psi(m, n) \quad \text{och} \quad (r\varphi)(m, n) = r\varphi(m, n)$$

då $\varphi, \psi \in \mathrm{Bil}_R(M \times N, P)$, $m \in M$, $n \in N$ och $r \in R$.

□

(4.3) Exempel. (a) Låt V vara ett vektorrum över en kropp K och $\varphi : V \times V \to K$ en bilinjär funktion. Om V har en bas e_i, $i = 1, 2, \ldots, n$, så är

$$\varphi(\mathbf{x}, \mathbf{y}) = \varphi(\sum x_i e_i, \sum y_j e_j) = \sum a_{ij} x_i y_j,$$

där $a_{ij} = \varphi(e_i, e_j)$. Funktionen φ kallas ofta **bilinjär form**.

(b) Låt $\varphi : V \times V^* \to K$, där $V^* = \mathrm{Hom}_K(V, K)$ (se (3.22)) och $\varphi(v, f) = f(v)$, där $v \in V$ och $f \in V^*$. Då är φ bilinjär.

(c) Låt $\varphi : M \times N \to P$ vara R-bilinjär och $f : P \to P'$ R-linjär. Då är

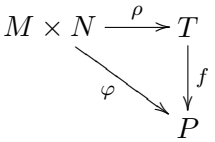
$$\varphi' = f\varphi : M \times N \to P'$$

en R-bilinjär funktion.

□

Tensorprodukten av två R-moduler M och N är en R-modul T som gör det möjligt att ersätta bilinjära avbildningar $M \times N \to P$ med linjära $T \to P$ (tensorprodukten "linjäriserar" bilinjära avbildningar). Detta har en stor betydelse eftersom linjära funktioner är lättare att hantera än bilinjära.

(4.4) Definition. Med **tensorprodukten** över R av två R-moduler M och N menas en R-modul T och en bilinjär avbildning $\rho : M \times N \to T$ sådana att för varje R-modul P och varje bilinjär avbildning $\varphi : M \times N \to P$ existerar en och endast en R-homomorfism $f : T \to P$ sådan att diagrammet



kommuterar dvs $f\rho = \varphi$.

□

(4.5) Anmärkning. Definitionen säger inte om (T, ρ) existerar. Vi skall visa existensen av (T, ρ) genom en direkt konstruktion. Men själva konstruktionen är av underordnad betydelse i förhållande till egenskapen av (T, ρ) som ges av (4.4).

□

Vi skall motivera först att (T, ρ) verkligen "linjäriserar" bilinjära avbildningar.

(4.6) Proposition. *Låt (T, ρ) vara en tensorprodukt av M och N över R. Då är*

$$\mathrm{Hom}_R(T, P) \cong \mathrm{Bil}_R(M \times N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$

för varje R-modul P.

Bevis. Den första isomorfismen följer direkt ur definitionen (4.4): Mot φ (se diagrammet i (4.4)) ordnar man f sådan att $f\rho = \varphi$. Det är en R-homomorfism tack vare entydigheten av f (t. ex. om $\varphi \mapsto f$, $\psi \mapsto g$ så är $\varphi + \psi \mapsto f + g$, ty $(f+g)\rho = f\rho + g\rho = \varphi + \psi$). På samma sätt kontrollerar man att den avbildningen är en monomorfism (om $\varphi \neq \psi$ så är $f \neq g$). Den är en epimorfism tack vare (4.3)(c).

Den andra isomorfismen (som kommer att spela en väsentlig roll senare) bevisas så här: Om $\varphi : M \times N \to P$ är bilinjär och man fixerar $m \in M$, så får man en R-homomorfism $\varphi_m : N \to P$ sådan att $\varphi_m(n) = \varphi(m, n)$, dvs varje φ definierar

$$\psi : M \to \mathrm{Hom}_R(N, P),$$

där $\psi(m) = \varphi_m$. Omvänt, om $\psi : M \to \mathrm{Hom}_R(N, P)$ är given så definiera $\varphi : M \times N \to P$ genom $\varphi(m, n) = \psi(m)(n)$. Nu måste man kontrollera att dessa två avbildningar ($\varphi \mapsto \psi$ och $\psi \mapsto \varphi$) är R-homomorfismer och varandras inverser. Vi lämnar det som en enkel övning. □

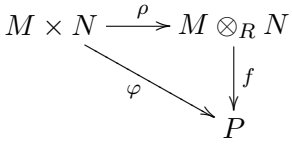
(4.7) Konstruktionen av (T, ρ). Låt M, N vara två R-moduler och låt F vara den fria R-modul som har alla par $(m, n), m \in M, n \in N$ som sin bas (se (3.16 (b))). Låt F_0 vara den delmodul till F som genereras av följande element i F:

$$(4.8) \qquad \begin{cases} (m_1 + m_2, n) - (m_1, n) - (m_2, n), & (m, n_1 + n_2) - (m, n_1) - (m, n_2), \\ (rm, n) - r(m, n), & (m, rn) - r(m, n). \end{cases}$$

Kvotmodulen F/F_0 betecknas med $M \otimes_R N$, och bilden av paret (m, n) i denna kvot betecknas med $m \otimes n$. Definiera $\rho : M \times N \to M \otimes_R N$ genom $\rho((m, n)) = m \otimes n$. $(M \otimes_R N, \rho)$ är en tensorprodukt av M och N över R. För att bevisa det låt oss först konstatera att definitionen av F_0 innebär att alla uttryck (4.8) övergår på 0 i F/F_0 dvs

$$\begin{aligned} &(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \;\; m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \\ &rm \otimes n = r(m \otimes n), \quad m \otimes rn = r(m \otimes n). \end{aligned}$$

Alltså är det klart att $\rho : M \times N \to M \otimes_R N$ är bilinjär. Låt nu $\varphi : M \times N \to P$ vara en bilinjär avbildning. Vi måste visa att det finns exakt en R-homomorfism $f : M \otimes_R N \to P$ sådan att diagrammet



kommuterar. För f måste i så fall gälla $f(m \otimes n) = \varphi(m, n)$, och eftersom elementen $m \otimes n$ genererar $M \otimes_R N$ är f entydigt bestämd (om den existerar). För att visa existensen av f definierar man först en modulhomomorfism $f_0 : F \to P$ sådan att $f_0((m, n)) = \varphi(m, n)$ (se (3.18)). Men $f_0(F_0) = (0)$ ty

$$\begin{aligned} f_0((m_1 + m_2, n) - (m_1, n) - (m_2, n)) &= \varphi(m_1 + m_2, n) - \varphi(m_1, n) - \varphi(m_2, n) = 0, \\ f_0((rm, n) - r(m, n)) &= \varphi(rm, n) - r\varphi(m, n) = 0. \end{aligned}$$

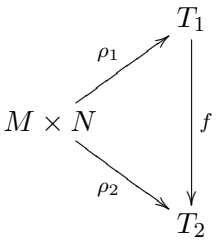
På samma sätt visar vi att bilderna av de övriga elementen som genererar F_0 är 0. Alltså inducerar f_0 en homomorfism $f : F/F_0 \to P$ sådan att $f(m \otimes n) = \varphi(m, n)$ (se Övn. 3.11) dvs vi har $f : M \otimes_R N \to P$ med de önskade egenskaperna. □

(4.9) Anmärkning. Observera att varje element i $M \otimes_R N$ är en **summa** av element $m \otimes n$, $m \in M$, $n \in N$ och behöver inte kunna reduceras till **ett** sådant element.

□

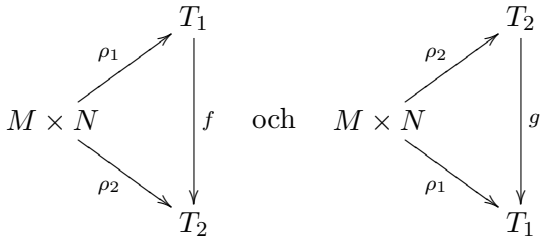
Vi har konstruerat en tensorprodukt $(M \otimes_R N, \rho)$. Finns det andra tensorprodukter? Svaret är att alla tensorprodukter är isomorfa i följande mening:

(4.10) Proposition. *Om (T_1, ρ_1) och (T_2, ρ_2) är två tensorprodukter av M och N över R så existerar en R-isomorfism $f : T_1 \to T_2$ så att diagrammet*

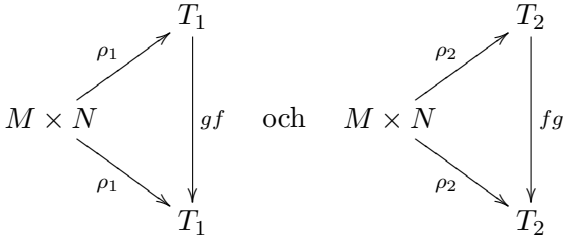


kommuterar.

Bevis. I enlighet med definitionen (4.4) existerar exakt en homomorfism f och exakt en homomorfism g sådana att



kommuterar dvs $f\rho_1 = \rho_2$ och $g\rho_2 = \rho_1$. Betrakta nu

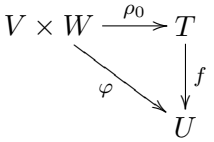


Dessa diagram kommuterar ty $gf\rho_1 = g\rho_2 = \rho_1$ och $fg\rho_2 = f\rho_1 = \rho_2$. Men de kommuterar också då man ersätter gf med identiteten id_1 på T_1 och fg med identiteten id_2 på T_2. Enligt definitionen (4.4) måste då $gf = id_1$ och $fg = id_2$ dvs f och g är inversa R-isomorfismer. □

(4.11) Anmärkning. Resonemanget i (4.10) kallas för **"abstract nonsense"**. Det är ett typiskt resonemang då ett objekt (här tensorprodukt) är definierat med hjälp av en s.k. universell egenskap – en egenskap som definitionsmässigt garanterar entydigheten av ett objekt så när som på isomorfism (om ett sådant objekt existerar). I fortsättningen kommer vi att betrakta sådana påståenden som självklara och hänvisa till "abstract nonsense" (vilket borde ha en positiv klang).

□

(4.12) Exempel. (a) Låt K vara en kropp och V, W vektorrum över K (eller mera allmänt: K är en ring och V, W är fria K-moduler). Låt (e_i) vara en bas för V och (f_j) för W. Vi påstår att tensorprodukten av V och W över K kan konstrueras på följande sätt: T är den fria modul som genereras över K av alla par $[e_i, f_j]$ med $\rho_0 : V \times W \to T$ som ges av $(\sum a_i e_i, \sum b_j f_j) \mapsto \sum a_i b_j [e_i, f_j]$. I själva verket, om $\varphi : V \times W \to U$ är bilinjär så definierar vi en linjär avbildning f sådan att $f([e_i, f_j]) = \varphi(e_i, f_j)$ (se (3.18)). f är då entydigt bestämd av villkoret att diagrammet



kommuterar (ty f är entydigt bestämd av sin verkan på basen $[e_i, f_j]$ för T). Om vi jämför den konstruktionen med den tidigare (4.7) så kan vi konstatera att $e_i \otimes f_j$ bildar en bas för $V \otimes_K W$ över K. Vi har nämligen en isomorfism f som gör att diagrammet

$$\begin{array}{ccc} V \times W & \xrightarrow{\rho_0} & T \\ & \searrow^{\rho} & \downarrow f \\ & & V \otimes_K W \end{array}$$

kommuterar (se (4.10)). Alltså är $f([e_i, f_j]) = e_i \otimes f_j$ så att $e_i \otimes f_j$ bildar en bas för $V \otimes_K W$ dvs varje element i $V \otimes_K W$ kan skrivas entydigt på formen $\sum a_{ij}(e_i \otimes f_j)$, $a_{ij} \in K$. I synnerhet har vi $\dim_K(V \otimes_K W) = \dim_K V \cdot \dim_K W$.

(b) Låt M vara en R-modul och I ett ideal i R. Då är $R/I \otimes_R M \cong M/IM$ (se (3.7)(c)). Betrakta diagrammet

$$\begin{array}{ccc} R/I \times M & \xrightarrow{\rho} & R/I \otimes_R M \\ & \searrow^{\varphi} & \downarrow f \\ & & M/IM \end{array}$$

där $\varphi((\bar{r}, m)) = \overline{rm}$. Man kontrollerar enkelt att φ är bilinjär, så att det finns en R-homomorfism f som uppfyller $f(\bar{r} \otimes m) = \overline{rm}$. Det är klart att f är en epimorfism, ty $\bar{m} = f(\bar{1} \otimes m)$. Å andra sidan, om $x \in R/I \otimes_R M$ så är $x = \sum \bar{r}_k \otimes m_k = \sum \bar{1} \otimes r_k m_k = \bar{1} \otimes m$, $m \in M$. Om nu $f(x) = \bar{m} = \bar{0}$ så är $m \in IM$ dvs $m = \sum i_r m_r$, där $i_r \in I$. Detta ger att $\bar{x} = \bar{1} \otimes m = \bar{1} \otimes \sum i_r m_r = \sum \bar{i}_r \otimes m_r = 0$ ty $\bar{i}_r = \bar{0}$. Alltså är $\mathrm{Ker} f = (0)$. Allt detta visar att f är en isomorfism. Observera fallet $I = (0)$ då $R \otimes_R M \cong M$ $(r \otimes m \mapsto rm)$.

(c) Låt M, N vara R-moduler. Då är $M \otimes_R N \cong N \otimes_R M$. Betrakta diagrammet

$$\begin{array}{ccc} M \times N & \xrightarrow{\rho_1} & M \otimes_R N \\ {\scriptstyle \delta_1}\uparrow\downarrow{\scriptstyle \delta_2} & & {\scriptstyle f}\downarrow\uparrow{\scriptstyle g} \\ N \times M & \xrightarrow[\rho_2]{} & N \otimes_R M \end{array}$$

där $\delta_1(n, m) = (m, n)$, $\delta_2(m, n) = (n, m)$ och ρ_1, ρ_2 är de bilinjära avbildningarna ur definitionen av tensorprodukten. $\rho_2\delta_2$ är bilinjär så att det finns f med $\rho_2\delta_2 = f$ dvs $f(m \otimes n) = n \otimes m$. Av liknande anledning finns också g med $g(n \otimes m) = m \otimes n$. Nu är $fg = id_{N \otimes M}$ och $gf = id_{M \otimes N}$ så att f och g är isomorfismer som är varandras inverser.

□

I vår nästa proposition samlar vi några enkla och viktiga egenskaper hos tensorprodukter:

(4.13) Proposition. *Låt M, N, P var R-moduler. Då gäller:*

(*a*) $M \otimes_R N \cong N \otimes_R M$ *då* $m \otimes n \mapsto n \otimes m$,

(*b*) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$ *då* $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$,

(*c*) $R \otimes_R M \cong M$ *då* $r \otimes m \mapsto rm$.

Bevis. För (a) se (4.12) (c), för (c) se (4.12) (b) och för (b) se Övn. 2. □

(4.14) Anmärkning. (a) Tensorprodukter av moduler över icke-kommutativa ringar definieras på liknande sätt, men man konstruerar sådana produkter för par bestående av en höger R-modul M och en vänster R-modul N. Då kräver man att F_0 genereras av $(mr, n) - (m, rn), m \in M$, $n \in N$, $r \in R$, i stället för elementen i andra raden i (4.8). $M \otimes_R N$ är en abelsk grupp som linjäriserar alla biadditiva avbildningar $\varphi : M \times N \to P$ sådana att $\varphi(mr, n) = \varphi(m, rn)$.

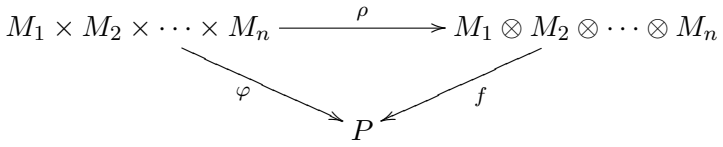
(b) Alla begrepp som vi hittills har introducerat i detta kapitel kan lätt generaliseras till en allmännare situation. Om $M_1, M_2, \ldots, M_n, P$ är R-moduler (R kommutativ igen) så definieras en **multilinjär funktion** $\varphi : M_1 \times M_2 \times \ldots \times M_n \to P$ som sådan att:

$$\varphi(m_1, \ldots, m_i' + m_i'', \ldots, m_n) = \varphi(m_1, \ldots, m_i', \ldots, m_n) + \varphi(m_1, \ldots, m_i'', \ldots m_n)$$

och

$$\varphi(m_1, \ldots, rm_i, \ldots, m_n) = r\varphi(m_1, \ldots, m_i, \ldots, m_n),$$

där $m_i, m_i', m_i'' \in M_i$ för $i = 1, 2, \ldots, n$. Tensorprodukten $(M_1 \otimes M_2 \ldots \otimes M_n, \rho)$ skall linjärisera φ dvs diagrammet:



skall kommutera för en entydigt bestämd linjär funktion f. Paret $(M_1 \otimes M_2 \otimes \ldots \otimes M_n, \rho)$ konstrueras precis på samma sätt som i (4.7). Man kan mycket lätt bevisa isomorfismer av typen $(M_1 \otimes M_2) \otimes M_3 \cong M_1 \otimes M_2 \otimes M_3$ med hjälp av "abstract nonsense"–argument (se Övn. 2). Alla multilinjära funktioner $\varphi : M_1 \times \ldots \times M_n \to P$ bildar en R-modul som vi kommer att beteckna med $\mathrm{Mult}_R(M_1 \times \ldots \times M_n, P)$ (se (4.2)).

□

Nu skall vi definiera tensorprodukt av modulhomomorfismer:

(4.15) Proposition. *Låt $f : M \to M'$ och $g : N \to N'$ vara två R-homomorfismer. Då existerar en R-homomorfism $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ sådan att $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. $f \otimes g$ kallas* **tensorprodukten** *av f och g.*

Bevis. Betrakta diagrammet:

$$\begin{array}{ccc} M \times N & \xrightarrow{\rho} & M \otimes_R N \\ {\scriptstyle f\times g}\downarrow & & \downarrow{\scriptstyle f\otimes g} \\ M' \times N' & \xrightarrow[\rho']{} & M' \otimes_R N', \end{array}$$

där $(f \times g)(m, n) = (f(m), g(n))$ och ρ, ρ' är definierade i (4.7). Då är $\rho'(f \times g)$ en bilinjär avbildning så att $f \otimes g$ existerar i enlighet med definitionen av tensorprodukten (4.4) och har den önskade egenskapen beroende på att diagrammet kommuterar. □

(4.16) Exempel. Låt $f : V \to V'$ och $g : W \to W'$ vara linjära avbildningar av ändligt dimensionella rum (över en kropp) med respektive baser $(\boldsymbol{a}_i)$ för V, $(\boldsymbol{a}'_j)$ för V', $(\boldsymbol{b}_k)$ för W och $(\boldsymbol{b}'_l)$ för W'. Då är

$$f \otimes g : V \otimes W \to V' \otimes W'$$

varvid $(\boldsymbol{a}_i \otimes \boldsymbol{b}_k)$ är en bas för $V \otimes W$ och $(\boldsymbol{a}'_j \otimes \boldsymbol{b}'_l)$ för $V' \otimes W'$ (se (4.12)(a)). Om

$$f(\boldsymbol{a}_i) = \sum_j a_{ij}\boldsymbol{a}'_j \quad \text{och} \quad g(\boldsymbol{b}_k) = \sum_l b_{kl}\boldsymbol{b}'_l$$

(dvs $A = [a_{ij}]$ är matrisen för f, $B = [b_{kl}]$ för g) så är

$$(f \otimes g)(\boldsymbol{a}_i \otimes \boldsymbol{b}_k) = f(\boldsymbol{a}_i) \otimes g(\boldsymbol{b}_k) = (\sum a_{ij}\boldsymbol{a}'_j) \otimes (\sum b_{kl}\boldsymbol{b}'_l) = \sum a_{ij}b_{kl}(\boldsymbol{a}'_j \otimes \boldsymbol{b}'_l).$$

Detta betyder att $f \otimes g$ har matrisen $[a_{ij}b_{kl}]$. Det finns olika konventioner vid utskriften av denna matris t ex

$$\begin{bmatrix} a_{11}B & a_{12}B & \dots \\ a_{21}B & a_{22}B & \dots \\ \dots & \dots & \dots \end{bmatrix},$$

där

$$aB = \begin{matrix} ab_{11} & ab_{12} & \dots \\ ab_{21} & ab_{22} & \dots \\ \dots & \dots & \dots \end{matrix}$$

Matrisen $[a_{ij}b_{kl}]$ betecknas med $A \otimes B$ och kallas **tensorprodukten av matriserna** A **och** B (se vidare Övn. 4). Detta exempel generaliseras direkt till godtyckliga fria moduler av ändlig rang över ringar.

□

Vårt nästa resultat kommer att spela en mycket viktig roll i samband med diskussionen av begreppet tensor.

(4.17) Proposition. *Låt V, V', W, W' vara fria R-moduler av ändlig rang över R. Då gäller*

$$\mathrm{Hom}_R(V,W) \otimes_R \mathrm{Hom}_R(V',W') \cong \mathrm{Hom}_R(V \otimes_R V', W \otimes_R W'),$$

där mot $f \otimes g, f : V \to W, g : V' \to W'$ svarar $f \otimes g$ (observera skillnaden mellan de två $f \otimes g$!)

Bevis. Betrakta diagrammet

$$\begin{array}{ccc} \mathrm{Hom}_R(V,W) \times \mathrm{Hom}_R(V',W') & \xrightarrow{\rho} & \mathrm{Hom}_R(V,W) \otimes_R \mathrm{Hom}_R(V',W') \\ & \searrow^{\delta} & \downarrow \varphi \\ & & \mathrm{Hom}_R(V \otimes_R V', W \otimes_R W'), \end{array}$$

där $\delta(f,g) = f \otimes g$. δ är bilinjär (lätt att kontrollera!) så att definitionen av $\otimes_R$ ger en linjär avbildning φ som mot $f \otimes g$ ordnar $f \otimes g$. Låt nu $(\boldsymbol{a}_i), (\boldsymbol{a}'_j), (\boldsymbol{b}_k), (\boldsymbol{b}'_l)$ vara baser för respektive V, V', W, W'. Vi vet att $V \otimes_R V'$ har som en bas alla $\boldsymbol{a}_i \otimes \boldsymbol{a}'_j$, och $W \otimes_R W'$ alla $\boldsymbol{b}_k \otimes \boldsymbol{b}'_l$. Det är välbekant att $\mathrm{Hom}_R(V,W)$ har som en bas alla linjära avbildningar f_{ik} sådana att $f_{ik}(\boldsymbol{a}_i) = \boldsymbol{b}_k$ och $f_{ik}(\boldsymbol{a}_{i'}) = 0$ då $i' \neq i$. En bas för $\mathrm{Hom}_R(V',W')$ består av alla f_{jl} sådana att $f_{jl}(\boldsymbol{a}'_j) = \boldsymbol{b}'_l$ och $f_{jl}(\boldsymbol{a}'_{j'}) = 0$ då $j' \neq j$.

På liknande sätt får vi att $\mathrm{Hom}_R(V \otimes_R V', W \otimes_R W')$ har som en bas alla linjära avbildningar $f_{ij,kl}$ sådana att $f_{ij,kl}(\boldsymbol{a}_i \otimes \boldsymbol{a}'_j) = \boldsymbol{b}_k \otimes \boldsymbol{b}'_l$ och $f_{ij,kl}(\boldsymbol{a}_{i'}, \boldsymbol{a}'_{j'}) = 0$ då $i' \neq i$ eller $j' \neq j$. Men detta betyder just att $f_{ij,kl} = f_{ik} \otimes f_{jl}$ dvs φ avbildar en bas för $\mathrm{Hom}_R(V,W) \otimes_R \mathrm{Hom}_R(V',W')$ på en bas för $\mathrm{Hom}_R(V \otimes_R V', W \otimes_R W')$ dvs φ är en isomorfism. □

Vi skall avsluta detta avsnitt med några ord om tensorprodukter av algebror över kommutativa ringar.

(4.18) Definition. Man säger att A är en R-**algebra** om A är en R-modul med en R-bilinjär avbildning $A \times A \to A$ (dvs en R-linjär avbildning $A \otimes_R A \to A$). Bilden av (a_1, a_2) betecknas med $a_1 a_2$.

□

Observera att $r(a_1a_2) = (ra_1)a_2 = a_1(ra_2)$ då $r \in R$, $a_1, a_2 \in A$.

Vårt närmaste syfte är att definiera tensorprodukten av två godtyckliga R-algebror A och B. Innan vi gör detta låt oss betrakta några nya och gamla exempel på K-algebror.

(4.19) Exempel. (a) Låt A vara en godtycklig associativ ring som innehåller ringen R i sitt centrum dvs $ra = ar$ då $a \in A$ och $r \in R$[††]. A är en R-algebra då avbildningen $A \times A \to A$ ges av $(a_1, a_2) \mapsto a_1a_2$ (observera vikten av alla förutsättningar!). Som specialfall kan vi välja A som en kommutativ ring. Mera allmänt kan man betrakta en R-homomorfism $\varphi : R \to A$ sådan att $\varphi(R)$ ligger i centrum av A. Då är A en R-algebra med $ra = \varphi(r)a$ och $A \times A \to A$ som ovan. Alla efterföljande exempel är konstruerade på detta sätt.

(b) Låt $A = M_n(\mathbb{R})$. Då är A en $\mathbb{R}$-algebra. Om $X = [x_{ij}]$ är en matris och $r \in \mathbb{R}$ så definierar $rX = [rx_{ij}]$ strukturen av en $\mathbb{R}$-modul på $M_n(\mathbb{R})$. Matrisprodukten är en $\mathbb{R}$-bilinjär avbildning. Det är klart att $\mathbb{R}$ kan ersättas med en godtycklig kommutativ ring.

(c) Låt $A = \mathbb{R}^n$. Då är $\mathbb{R}^n$ en $\mathbb{R}$-algebra med $\mathbb{R}$-modulstrukturen given av $r(r_1, r_2, \ldots, r_n) = (rr_1, rr_2, \ldots, rr_n)$ ($\mathbb{R}^n$ är en ring med koordinatvis addition och multiplikation). Mera allmänt kan $\mathbb{R}$ ersättas med en godtycklig kommutativ ring.

(d) Låt G vara en grupp. Gruppringen $R[G]$ (se (2.2) (h)) är en R-algebra om man definierar $r(\sum r_g g) = \sum rr_g g$.

(e) A är en **Lie R-algebra** om A är en R-algebra och en Lie ring (dvs A är en ring sådan att $a(bc) + b(ca) + c(ab) = 0$ och $a^2 = 0$ då $a, b, c \in A$). T ex är $(\mathbb{R}^3, +, \times)$, där "$\times$"är vektorprodukten, en Lie R-algebra då $r(r_1, r_2, r_3) = (rr_1, rr_2, rr_3)$.

(f) Varje ring A är en $\mathbb{Z}$-algebra då man definierar na i enlighet med gruppstrukturen av $(A, +)$ och $A \times A \to A$ som produkten i A.

□

(4.20) Konstruktionen av algebran $A \otimes_R B$. A och B är R-moduler så att man kan konstruera R-modulen $A \otimes_R B$. Vi vill visa att man kan definiera multiplikation på $A \otimes_R B$ dvs en R–bilinjär avbildning $(A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B$ och att man kan göra det så att $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$ då $a_i \in A$, $b_i \in B$. Algebrastrukturen på A ger en linjär avbildning $m_A : A \otimes_R A \to A$ (den kommer från en R-bilinjär avbildning $A \times A \to A$) sådan att $m_A(a_1 \otimes a_2) = a_1a_2$ och på liknande sätt har vi $m_B : B \otimes_R B \to B$ med $m_B(b_1 \otimes b_2) = b_1b_2$. Låt $\sigma : B \otimes_R A \to A \otimes_R B$ vara den R-isomorfism som har egenskapen $\sigma(b \otimes a) = a \otimes b$ (se (4.13) (a)). Betrakta nu den R-linjära avbildningen (alla tensorprodukter är över R):

$$A \otimes B \otimes A \otimes B \xrightarrow{1_A \otimes \sigma \otimes 1_B} A \otimes A \otimes B \otimes B \xrightarrow{m_A \otimes m_B} A \otimes B$$

[††]Med centrum av en ring A menas $C(A) = \{x \in A : \forall_{a \in A} ax = xa\}$.

som har just egenskapen att $(a_1 \otimes b_1) \otimes (a_2 \otimes b_2) \mapsto a_1a_2 \otimes b_1b_2$. Den avbildningen svarar mot den R-bilinjära avbildningen $(A \otimes B) \times (A \otimes B) \to A \otimes B$. □

En mycket enkel konsekvens av den konstruktionen är:

(4.21) Följdsats. *Om A, B är kommutativa (associativa, bägge har etta) så är $A \otimes_R B$ kommutativ (associativ, har etta).*

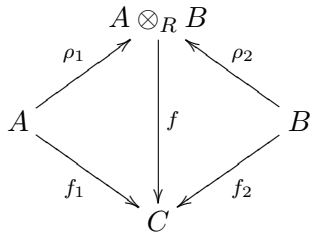
Bevis. Vi har $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2 = a_2a_1 \otimes b_2b_1 = (a_2 \otimes b_2)(a_1 \otimes b_1)$ om A, B är kommutativa. På samma sätt visas associativiteten. $1_A \otimes 1_B$ är ettan i $A \otimes_R B$. □

(4.22) Proposition (universella egenskapen hos tensorprodukter av algebror). *Låt*

$$\rho_1 : A \to A \otimes_R B \quad \textit{och} \quad \rho_2 : B \to A \otimes_R B$$

vara R-homomorfismer av kommutativa R-algebror med etta sådana att $\rho_1(a) = a \otimes 1$ och $\rho_2(b) = 1 \otimes b$.

(a) För varje kommutativ R-algebra med etta C och godtyckliga R-homomorfismer $f_1 : A \to C$ och $f_2 : B \to C$ av algebror med etta existerar en och endast en homomorfism av R-algebror $f : A \otimes_R B \to C$ sådan att diagrammet



kommuterar.

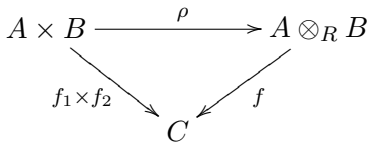
(b) Egenskapen (a) definierar $(A \otimes_R B, \rho_1, \rho_2)$ entydigt dvs om (T, ρ_1', ρ_2'), där T är en R-algebra och $\rho_1' : A \to T$, $\rho_2' : B \to T$ är homomorfismer av R-algebror med etta, har egenskapen (a) så är motsvarande R-homomorfismen f ur (a) (med $C = T$) en isomorfism.

Bevis. Först konstaterar vi att f är entydigt bestämd om den existerar. I själva verket ger kommutativiteten av diagrammet att

$$f(a \otimes b) = f((a \otimes 1)(1 \otimes b)) = f(a \otimes 1)f(1 \otimes b) = f\rho_1(a)f\rho_2(b) = f_1(a)f_2(b)$$

så att f_1 och f_2 bestämmer entydigt f på elementen $a \otimes b$ och som konsekvens på alla element i $A \otimes_R B$.

Existensen av f följer ur definitionen av tensorprodukten. För att visa den, betrakta en bilinjär avbildning $f_1 \times f_2 : A \times B \to C$, där $(f_1 \times f_2)(a, b) = f_1(a)f_2(b)$. Enligt definitionen av $\otimes$ för R-moduler existerar en linjär avbildning $f : A \otimes_R B \to C$ sådan att diagrammet



kommuterar dvs $f(a \otimes b) = f_1(a)f_2(b)$. Nu kontrollerar vi enkelt att f också är en homomorfism av R-algebror ty

$$f((a \otimes b)(a' \otimes b')) = f(aa' \otimes bb') = f_1(aa')f_2(bb') = f_1(a)f_2(b)f_1(a')f_2(b') = f(a \otimes b)f(a' \otimes b').$$

Bevis för (b) är "abstract nonsense". □

(4.23) Exempel. (a) $K[X] \otimes_K K[Y] \cong K[X, Y]$. Låt $f_1 : K[X] \to K[X, Y]$ och $f_2 : K[Y] \to K[X, Y]$ vara naturliga inbäddningar definierade av $f_1(X) = X$ och $f_2(Y) = Y$. Enligt den universella egenskapen hos tensorprodukten av algebror existerar exakt en ringhomomorfism $f : K[X] \otimes_K K[Y] \to K[X, Y]$ sådan att motsvarande diagram kommuterar dvs $f\rho_1 = f_1$ och $f\rho_2 = f_2$, där ρ_i betecknar ringhomomorfismerna från definitionen av tensorprodukten. Nu konstaterar vi omedelbart att $f(X \otimes 1) = X$ och $f(Y \otimes 1) = Y$ så att en bas $X^i \otimes Y^j$ för $K[X] \otimes_K K[Y]$ avbildas av f på en bas X^iY^j för $K[X, Y]$, vilket visar att f är bijektiv och således en ringisomorfism. Man kan lösa uppgiften på ett annat sätt genom att definiera en ringhomomorfism $g : K[X, Y] \to K[X] \otimes_K K[Y]$ så att $g(X) = X \otimes 1$ och $g(Y) = 1 \otimes Y$. Då kan man lätt kontrollera att $gf =$id och $fg =$id, vilket innebär att f (och g) är ringisomorfismer.

(b) Nu visar vi att $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(i)$. Låt $f_1 : \mathbb{Z}[i] \to \mathbb{Q}(i)$ och $f_2 : \mathbb{Q} \to \mathbb{Q}(i)$ vara de naturliga inbäddningarna. Enligt definitionen av tensorprodukten existerar en ringhomomorfism $f : \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}(i)$ sådan att $f\rho_1 = f_1$ och $f\rho_2 = f_2$, där ρ_i betecknar ringhomomorfismerna från definitionen av tensorprodukten. Vi vill visa att f är en isomorfism. Det är klart att f är surjektiv eftersom varje element i $\mathbb{Q}(i)$ kan skrivas på formen $(a + bi)/d$, där a, b, d är heltal och då är $f((a + bi) \otimes (1/d)) = (a + bi)/d$. För att visa att f är injektiv noterar vi att varje element i tensorprodukten $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Q}$ är $x = \sum(a_k + b_k i) \otimes (c_k/d_k)$ med hela a_k, b_k, c_k, d_k. Genom att skriva bråken c_k/d_k med en gemensam nämnare d och flytta varje täljare till motsvarande $a_k + ib_k$ får man $x = (a + bi) \otimes (1/d)$. Om nu $f(x) = (a + bi)/d = 0$ så är $a = b = 0$, så att $x = 0$.

Se vidare Övn. 7.

□

ÖVNINGAR

4.1. (a) Visa att $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$ då $\mathrm{SGD}(m,n) = 1$.

(b) Generalisera (a) till godtyckliga $m, n \in \mathbb{Z}$.

4.2. Låt M, N, P vara R-moduler (R kommutativ med etta). Visa att

$$(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$$

(den sista modulen är definierad enligt (4.14)(b)).

4.3. Låt M, M', N, N' vara R-moduler, $f, f_1, f_2 \in \mathrm{Hom}_R(M, M')$, $g_1, g_2 \in \mathrm{Hom}_R(N, N')$, och $r \in R$. Visa att:

$$(f_1+f_2)\otimes g = f_1\otimes g + f_2 \otimes g,\ f\otimes(g_1+g_2) = f\otimes g_1 + f\otimes g_2, (rf)\otimes g = f\otimes rg = r(f\otimes g).$$

4.4. Låt $A = [a_{ij}]_{m,n}$ och $B = [b_{ij}]_{p,q}$ vara två matriser och $A \otimes B = [a_{ij}b_{kl}]_{mp,nq}$ deras tensorprodukt (se (4.16)). Visa att:

(a) $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B$, $A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$,

(b) $rA \otimes B = r(A \otimes B) = A \otimes rB$.

Försök ge bevis som inte bygger på beräkningar!

4.5. (a) Låt $\varphi : R \to R'$ vara en ringhomomorfism och M en R-modul. Visa att $R' \otimes_R M$ kan betraktas som R'-modul med avseende på $r'(x \otimes m) = r'x \otimes m$, där $r', x \in R'$.

(b) Låt V vara R–fri med bas $e_i, i \in I$ (I en indexmängd). Visa att $R' \otimes_R V$ är R'–fri med bas $1 \otimes e_i$, $i \in I$.

Anmärkning. Om $R = \mathbb{R}$ och $R' = \mathbb{C}$ så är $\mathbb{C} \otimes_{\mathbb{R}} V$ ett vektorrum över $\mathbb{C}$ som kallas **komplexifieringen** av V.

(c) Låt A vara en R-algebra. Genom att utnyttja (a) visa att $R' \otimes_R A$ kan på ett naturligt sätt betraktas som en R'-algebra.

4.6. Låt A, B vara två kommutativa R-algebror med etta och $I \lhd A, J \lhd B$. Visa att $A/I \otimes_R B/J \cong (A \otimes_R B)/(I \otimes_R B + A \otimes_R J)$.

4.7. Visa att

(a) $R[X] \otimes_R R[Y] \cong R[X,Y]$, där R är en godtycklig kommutativ ring med etta,

(b) $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(\sqrt{2})$,

(c) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X] \cong \mathbb{C}[X]$,

(d) $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}[i] \cong \mathbb{C}$.

(e) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$,

(f) $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Kapitel 5

TENSORER OCH TENSORALGEBROR

Låt K vara en associativ och kommutativ ring med etta och V en K-modul. I praktiska tillämpningar är oftast V ett linjärt rum över en kropp K, men vanligen gäller våra resultat då V är en fri K-modul med en bas $e_1, \ldots, e_n$ (om existensen av en ändlig bas förutsätts). Detta kapitel handlar om några viktiga begrepp i multilinjär algebra som har stor betydelse i många sammanhang: olika typer av tensorer (bl a symmetriska och alternerande som ibland kallas antisymmetriska) och tensoralgebror (yttre algebror, symmetriska algebror).

(5.1) Definition. Med en **tensor** av typen (k, l) över V menar man ett element av tensorprodukten

$$T^k(V) \otimes T^l(V^*),$$

där $V^* = \mathrm{Hom}_K(V, K)$, $T^k(V) = V \otimes_K \ldots \otimes_K V$ (k stycken) samt $T^0(V) = K$.

□

(5.2) Exempel. (a) En vektor $v \in V$ är en tensor av typen $(1, 0)$.

(b) En linjär avbildning $f : V \to K$ är en tensor av typen $(0, 1)$.

(c) $f \in \mathrm{Hom}_K(V, V)$ är en tensor av typen $(1, 1)$. Vi har nämligen (se (4.17)):

$$\mathrm{Hom}_K(V, V) \cong \mathrm{Hom}_K(K, V) \otimes \mathrm{Hom}_K(V, K) \cong V \otimes V^*.$$

(d) En bilinjär form $\varphi : V \times V \to K$ är en tensor av typen $(0,2)$, ty

$$\mathrm{Bil}_K(V \times V, K) \cong \mathrm{Hom}_K(V \otimes V, K \otimes K) \cong \mathrm{Hom}_K(V, K) \otimes \mathrm{Hom}_K(V, K) \cong V^* \otimes V^*$$

(se (4.6) och (4.17)).

□

(5.3) Koordinater av tensorer. Låt $e_1, \ldots, e_n$ vara en bas för V över K och låt $\xi \in T^k(V) \otimes T^l(V^*)$ vara en (k,l)-tensor. Låt $e^1, \ldots, e^n$ vara den duala basen för V^* till basen $e_1, \ldots, e_n$ för V (observera placeringen av index!) dvs $e^i(e_j) = \delta_{ij}$. Då har vi en bas för $T^k(V) \otimes T^l(V^*)$ (se (4.12)(a)) bestående av alla produkter

$$e_{i_1} \otimes \ldots \otimes e_{i_k} \otimes e^{j_1} \otimes \ldots \otimes e^{j_l}.$$

Varje tensor ξ har entydig framställning m.a.p. denna bas:

$$\xi = \sum a^{i_1 \ldots i_k}_{j_1 \ldots j_l} e_{i_1} \otimes \ldots \otimes e_{i_k} \otimes e^{j_1} \otimes \ldots \otimes e^{j_l}$$

och $a^{i_1 \ldots i_k}_{j_1 \ldots j_l}$ är dess koordinater i K^N, där $N = n^{k+l}$. Man kan skriva ut dessa koordinater i en bestämd ordning och kalla $M_\xi = (a^{i_1 \ldots i_k}_{j_1 \ldots j_l})$ för **tensorns matris** (med avseende på den valda basen).

Placeringen av index är en väletablerad tradition som kommer från fysiken och differentialgeometrin. Man brukar utelämna $\sum$ vilket gör notationen mycket bekvämare. Fallen då $k + l = 2$ är välkända. Om $k = l = 1$ får vi tensorer

$$\xi = a^i_j e_i \otimes e^j \in V \otimes V^* \cong \mathrm{Hom}_K(V, V).$$

Matrisen $M_\xi = [a^i_j]$ är helt enkelt matrisen för den linjära avbildning $\varphi_\xi : V \to V$ som svarar mot ξ (vid isomorfismen av $V \otimes V^*$ med $\mathrm{Hom}_K(V, V)$ – se (4.17)). Om $k = 0$ och $l = 2$ får vi

$$\xi = a_{ij} e^i \otimes e^j \in V^* \otimes V^* \cong \mathrm{Bil}_K(V \times V, K)$$

och ξ svarar mot $\varphi_\xi : V \times V \to K$ (se (4.17)). □

(5.4) Vad händer med koordinater av tensorer vid ett basbyte? Fallen av $(1,0)$-tensorer (dvs vektorer), $(1,1)$-tensorer (dvs linjära avbildningar) och $(0,2)$-tensorer (dvs bilinjära former) är kända från kurser i linjär algebra. Vi skall nu diskutera det allmänna fallet. Låt $e'_1, \ldots, e'_n$ vara en ny bas för V och $e'^1, \ldots, e'^n$ den duala basen för V^*. Vi har:

$$e'_i = p^j_i e_j$$

(j är summationsindexet!), där $P = [p_i^j]$ är övergångsmatrisen från den gamla till den nya basen. Det är en enkel övning att bevisa sambandet:

$$e'^i = q_j^i e^j,$$

där $Q = [q_j^i]^t$ är inversen till P (se Övn. 15). Nu skall vi följa ännu en konvention (med ursprung i fysiken) – vi skall skriva $e_{i'}$ i stället för e'_i och $e^{i'}$ i stället för e'^i. Som konsekvens: $e_{i'} = p_{i'}^j e_j = p_{i'}^i e_i$ (bokstaven j kan bytas ut mot i) och $e^{i'} = q_i^{i'} e^i$. Vi kan också ersätta q med p därför att placeringen av primtecknet skiljer mellan P (prim nerifrån) och P^{-1} (prim uppifrån). Alltså

$$e_{i'} = p_{i'}^i e_i, \;\; e_i = p_i^{i'} e_{i'}, \;\; e^{i'} = p_i^{i'} e^i, \;\; e^i = p_{i'}^i e^{i'}.$$

Nu kan vi härleda sambandet mellan koordinaterna för en och samma tensor i olika baser:

$$\begin{aligned} \xi &= a_{j_1\dots j_l}^{i_1\dots i_k} e_{i_1} \otimes \dots \otimes e_{i_k} \otimes e^{j_1} \otimes \dots \otimes e^{j_l} = a_{j_1\dots j_l}^{i_1\dots i_k} p_{i_1}^{i'_1} e_{i'_1} \otimes \dots p_{i_k}^{i'_k} e_{i'_k} \otimes p_{j'_1}^{j_1} e^{j'_1} \otimes \dots \otimes p_{j'_l}^{j_l} e^{j'_l} \\ &= p_{i_1}^{i'_1} \dots p_{i_k}^{i'_k} p_{j'_1}^{j_1} \dots p_{j'_l}^{j_l} a_{j_1\dots j_l}^{i_1\dots i_k} e_{i'_1} \otimes \dots \otimes e_{i'_k} \otimes e^{j'_1} \otimes \dots \otimes e^{j'_l}, \end{aligned}$$

dvs

$$a_{j'_1\dots j'_l}^{i'_1\dots i'_k} = p_{i_1}^{i'_1} \dots p_{i_k}^{i'_k} a_{j_1\dots j_l}^{i_1\dots i_k} p_{j'_1}^{j_1} \dots p_{j'_l}^{j_l}. \tag{5.5}$$

Om t ex $v \in V$ är en $(1,0)$-tensor med koordinater a^i i den gamla basen så är $a^{i'} = p_i^{i'} a^i$ koordinaterna i den nya basen dvs övergången sker med hjälp av inversen till P (omvänt i förhållande till basbyte). Därför säger man att en (k,l)-tensor är k-**kontravariant**. Om $f \in V^*$ är en $(0,1)$-tensor med koordinater a_i med avseende på basen $\{e^i\}$ så är $a_{i'} = p_{i'}^i a_i$ dvs övergången sker med hjälp av matrisen P. Man säger att en (k,l)-tensor är l-**kovariant**. T ex $\xi \in V \otimes V^* \cong \mathrm{Hom}_K(V,V)$ är 1-kontravariant och 1-kovariant tensor och $a_{j'}^{i'} = p_i^{i'} a_j^i p_{j'}^j$ dvs $M'_\xi = P^{-1} M_\xi P$. Observera att referenspunkten för den terminologin är basbyte i V – samband som förmedlas av P är kovarianta, av P^{-1} kontravarianta. □

Tensorer förekommer i olika sammanhang – fysikaliska och matematiska. Det finns olika ekvivalenta varianter av tensordefinitionen. Definitionen (5.1) är koordinatfri och kort, men formuleringen ställer högre krav på matematisk apparat. Vi skall ägna en stund åt några variationer på tensorbegreppet.

(5.6) (a) **"Klassisk" definition.** Man identifierar tensorer med funktioner som mot varje bas för V över K ordnar en uppsättning av n^{k+l} element i K som transformeras lämpligt vid övergångar från en bas till en annan. Låt $\mathcal{B}(V)$ vara mängden av alla baser i V. Med en tensor av typen (k,l) menas varje funktion

$$T : \mathcal{B}(V) \to K^N, \quad \{e_i\} \mapsto (a_{j_1\dots j_l}^{i_1\dots i_k}),$$

där $N = n^{k+l}$ ($n = \dim_K V$), sådan att för två godtyckliga baser $\{e_i\}$ och $\{e'_i\}$ uppfyller motsvarande vektorer $(a^{i_1\dots i_k}_{j_1\dots j_l})$ och $(a^{i'_1\dots i'_k}_{j'_1\dots j'_l})$ sambandet (5.5). Vanligen är $K = \mathbb{R}$ eller $\mathbb{C}$.

(b) **"Pedagogisk" definition.** För att undvika tensorprodukter av moduler utnyttjar man två isomorfismer:

$$T^k(V) \otimes T^l(V^*) \cong \mathrm{Hom}_K(T^k(V) \otimes T^l(V^*), K) \cong \mathrm{Mult}_K(V \times \dots \times V \times V^* \times \dots \times V^*, K)$$

(se (3.23) och (4.17)). Med en tensor menar man nu en multilinjär funktion

$$T : V \times \dots \times V \times V^* \times \dots \times V^* \to K$$

av k stycken vektorvariabler och l stycken kovektorvariabler (en **kovektor** är ett element ur V^*). Isomorfismen ovan behöver inte gälla om V har oändlig dimension, men i praktiska sammanhang är en begränsning till ändligt dimensionella rum ofta acceptabel. Om $\{e_i\}$ är en bas för V och $\{e^i\}$ för V^* så har vi:

$$\begin{aligned} T(\mathbf{x}_1, \dots, \mathbf{x}_k, \mathbf{y}^1, \dots, \mathbf{y}^l) &= T(x_1^{i_1} e_{i_1}, \dots, x_k^{i_k} e_{i_k}, y^1_{j_1} e^{j_1}, \dots, y^l_{j_l} e^{j_l}) = \\ &= T(e_{i_1}, \dots, e_{i_k}, e^{j_1}, \dots, e^{j_l}) x_1^{i_1} \dots x_k^{i_k} y^1_{j_1} \dots y^l_{j_l} \end{aligned}$$

och $a^{j_1\dots j_l}_{i_1\dots i_k} = T(e_{i_1}, \dots, e_{i_k}, e^{j_1}, \dots, e^{j_l})$ är tensorns T koordinater. Observera dock att vektorvariabler svarar mot kovektorer och kovektorvariabler mot vektorer. T ex är $T : V^* \to K$ en vektor ty $T \in \mathrm{Hom}_K(V^*, K) = V^{**} \cong V$. Allt detta är ett resultat av Hom-verkan[††]. Denna definition av tensorer är mycket vanlig i analysböcker och har många praktiska fördelar.

(c) En annan möjlighet att definiera begreppet tensor är följande. Vi har (se (4.17)):

$$T^k(V) \otimes T^l(V^*) \cong \mathrm{Hom}_K(K, V) \otimes \dots \otimes \mathrm{Hom}_K(K, V) \otimes \mathrm{Hom}_K(V, K) \otimes \dots \otimes \mathrm{Hom}_K(V, K)$$

$$\cong \mathrm{Hom}_K(V \otimes \dots \otimes V, V \otimes \dots \otimes V) = \mathrm{Hom}_K(T^l(V), T^k(V)).$$

En tensor är helt enkelt en linjär avbildning $T^l(V) \to T^k(V)$. □

Det finns speciella typer av tensorer som har särskilt stor betydelse. Två sådana typer – symmetriska och alternerande (antisymmetriska) – definierar vi nu. Som tidigare är R en kommutativ ring med etta. V och P är godtyckliga R-moduler. Som vanligt skriver vi V^l i stället för $V \times V \times \dots \times V$ (l stycken).

(5.7) Definition. Låt $T : V^l \to P$ vara en R-multilinjär avbildning. Man säger att - T är **symmetrisk** om $T(v_{\alpha(1)}, \dots, v_{\alpha(l)}) = T(v_1, \dots, v_l)$ för varje $v_1, \dots, v_l \in V$ och varje permutation $\alpha(1), \dots, \alpha(l)$ av $1, \dots, l$. Man säger att T är **alternerande** (ibland använder man termen **antisymmetrisk**) om $T(v_1, \dots, v_l) = 0$ för varje uppsättning $v_1, \dots, v_l \in V$

[††]Vi diskuterar Hom som funktor i Kapitel 11.

som innehåller minst två lika element. Alla symmetriska R-avbildningar bildar en R-modul (en delmodul till modulen $\mathrm{Mult}_R(V^l, P)$ – se (4.14)(b)). Den kommer att betecknas med $\mathrm{Sym}_R(V^l, P)$. På liknande sätt betecknar $\mathrm{Alt}_R(V^l, P)$ modulen av alla alternerande R-avbildningar.

□

(5.8) Exempel. (a) Låt $V = Ke_1 + \ldots + Ke_n$ vara en fri K-modul med bas $e_1, \ldots, e_n$ och låt $b : V \times V \to K$ vara en symmetrisk bilinjär form. Då är b en symmetrisk avbildning. Här är

$$b(\mathbf{x}, \mathbf{y}) = b(x^i e_i, y^j e_j) = b(e_i, e_j) x^i y^j = a_{ij} x^i y^j,$$

där $a_{ij} = b(e_i, e_j) = a_{ji} = b(e_j, e_i)$.

(b) Låt $V = \mathbb{R}^n$ och $T : V^n \to \mathbb{R}$, där $T(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \det(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ (se Appendix C). Då är T alternerande.

□

(5.9) Anmärkning. (a) Om $P = K$ så är varje symmetrisk eller alternerande avbildning $T : V^l \to K$ en $(0, l)$-tensor (se (5.6)(b)). Den kallas för **symmetrisk**, respektive, **alternerande tensor**. Om $e_1, \ldots, e_n$ är en bas för V så har vi

$$a_{i_1 \ldots i_l} = T(e_{i_1}, \ldots, e_{i_l}).$$

Om T är en symmetrisk tensor så förändras inte $a_{i_1 \ldots i_l}$ vid en godtycklig permutation av $i_1, \ldots, i_l$. Om T är alternerande så är $a_{i_1 \ldots i_l} = 0$ då minst två av talen $i_1, \ldots, i_l$ är lika.

(b) Om $T : V^l \to P$ är alternerande så ger

$$0 = T(v_1, \ldots, v_i + v_{i+1}, v_i + v_{i+1}, \ldots, v_l) = T(v_1, \ldots, v_i, v_{i+1}, \ldots, v_l) + T(v_1, \ldots, v_{i+1}, v_i, \ldots, v_l)$$

dvs

$$T(v_1, \ldots, v_i, v_{i+1}, \ldots, v_l) = -T(v_1, \ldots, v_{i+1}, v_i, \ldots, v_l).$$

Alltså resulterar omkastningen av två bredvidstående argument i T i ett teckenbyte. Detta implicerar lätt att

$$T(v_{\alpha(1)}, \ldots, v_{\alpha(l)}) = \mathrm{sign}(\alpha(1), \ldots, \alpha(l)) T(v_1, \ldots, v_l) \tag{5.10}$$

för varje permutation $\alpha(1), \ldots, \alpha(l)$ av $1, \ldots, l$[††]. Antag nu att T uppfyller den sista likheten. Då får vi att $T(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_l)$ byter tecken då v_i och v_j byter plats (ett platsbyte

[††] $\mathrm{sign}(\alpha(1), \ldots, \alpha(l))$ betecknar signaturen av permutationen $\alpha(1), \ldots, \alpha(l)$ dvs $\mathrm{sign}(\alpha(1), \ldots, \alpha(l)) = 1$ om $\alpha(1), \ldots, \alpha(l)$ är en jämn permutation av talen $1, \ldots, l$ och $\mathrm{sign}(\alpha(1), \ldots, \alpha(l)) = -1$ om $\alpha(1), \ldots, \alpha(l)$ är en udda permutation av dessa tal.

är en udda permutation!). Detta innebär att

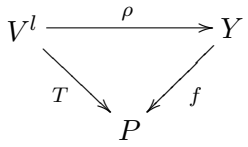
$$T(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_l) = -T(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_l)$$

dvs $2T(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_l) = 0$ då $v_i = v_j$. Den likheten behöver inte medföra att $T(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_l) = 0$ då $v_i = v_j$ (tag t ex $P = \mathbb{Z}_2$!). Om $\mathrm{char}(K) \neq 2$ dvs $-1 \neq 1$ får vi dock likheten $T(v_1, \ldots, v_l) = 0$ då minst två element bland $v_1, \ldots, v_l$ är lika. Ofta möter man (5.10) som definition av alternerande funktioner.

□

Precis som det för godtyckliga multilinjära avbildningar var möjligt att konstruera universella objekt (T, ρ) som linjäriserade dessa avbildningar är det önskvärt och möjligt att genomföra liknande konstruktioner i klassen av symmetriska och alternerande avbildningar. Vi gör det enbart för alternerande och lämnar symmetriska som Övn. 10.

(5.11) Definition. Yttre l-te potensen av en K-modul V är en K-modul Y med en alternerande avbildning $\rho : V^l \to Y$ (dvs ett par (Y, ρ)) sådana att för varje alternerandeavbildning $T : V^l \to P$ existerar en och endast en K-homomorfism $f : Y \to P$ sådan att diagrammet



kommuterar.

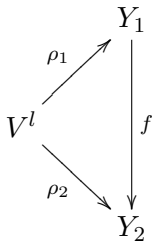
□

Precis som för tensorprodukter visar vi

(5.12) Proposition. (*a*) *Låt* $\mathrm{Ant}_K(V^l, P)$ *vara delmodulen till* $\mathrm{Mult}_K(V^l, P)$ (*se* (4.14)(*b*)) *bestående av alla alternerande avbildningar* $T : V^l \to P$. *Då är*

$$\mathrm{Ant}_K(V^l, P) \cong \mathrm{Hom}_K(Y, P).$$

(*b*) *Om* (Y_1, ρ_1) *och* (Y_2, ρ_2) *är två yttre* l*-potenser av* V *så finns det en* K*-isomorfism* $f : Y_1 \to Y_2$ *sådan att diagrammet*



kommuterar.

Bevis. För (a) är beviset exakt samma som för (4.6) (första isomorfismen). (b) bevisas med "abstract nonsense" exakt som (4.10). □

(5.13) Konstruktionen av yttre potenser. Låt V vara en K-modul och F en fri K-modul som genereras av alla uppsättningar $(v_1, \ldots, v_l), v_i \in V$. Låt F_0^{alt} vara en delmodul till F som genereras av alla uttryck:

$$(v_1, \ldots, v_i' + v_i'', \ldots, v_l) - (v_1, \ldots, v_i', \ldots, v_l) - (v_1, \ldots, v_i'', \ldots, v_l),$$
$$(v_1, \ldots, rv_i, \ldots, v_l) - r(v_1, \ldots, v_i, \ldots, v_l),$$
$$(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_l), \quad \text{där } v_i = v_j.$$

Kvotmodulen F/F_0^{alt} betecknas med $\bigwedge^l(V)$ och bilden av $(v_1, \ldots, v_l)$ i denna med $v_1 \wedge \ldots \wedge v_l$. Man definierar $\rho : V^l \to \bigwedge^l(V)$ genom $\rho(v_1, \ldots, v_l) = v_1 \wedge \ldots \wedge v_l$. Precis som i (4.7) (eller (4.14) (b)) bevisar man att paret $(\bigwedge^l(V), \rho)$ är en l-te yttre potens av V över K. □

(5.14) Anmärkning. Det finns en naturlig epimorfism $T^l(V) \to \bigwedge^l(V)$ som mot $v_1 \otimes \ldots \otimes v_l$ ordnar $v_1 \wedge \ldots \wedge v_l$. Vi vet nämligen (se (4.7) och (4.14)(b)) att $T^l(V) = F/F_0$, där F_0 genereras av elementen

$$(v_1, \ldots, v_i' + v_i'', \ldots, v_l) - (v_1, \ldots, v_i', \ldots, v_l) - (v_1, \ldots, v_i'', \ldots, v_l)$$

och

$$(v_1, \ldots, rv_i, \ldots, v_l) - r(v_1, \ldots, v_i, \ldots, v_l).$$

Detta betyder att $F_0 \subseteq F_0^{alt}$ så att vi har en epimorfism $F/F_0 \to F/F_0^{alt}$ som induceras av inbäddningen $(F_0, F) \hookrightarrow (F_0^{alt}, F)$ (se t ex Övn. 3.11). Man kan i så fall definiera $\bigwedge^l(V)$ som $T^l(V)/X$, där X genereras av alla produkter $v_1 \otimes \ldots \otimes v_l$ med minst två faktorer lika.

□

(5.15) Proposition. *Låt $f : V \to V'$ vara en K-homomorfism. Då existerar en K-homomorfism $\bigwedge^l(f) : \bigwedge^l(V) \to \bigwedge^l(V')$ sådan att $\bigwedge^l(f)(v_1 \wedge \ldots \wedge v_l) = f(v_1) \wedge \ldots \wedge f(v_l)$.*

Bevis. Betrakta diagrammet:

$$\begin{array}{ccc} V^l & \xrightarrow{f\times\cdots\times f} & V'^l \\ {\scriptstyle\rho_V}\downarrow & & \downarrow{\scriptstyle\rho_{V'}} \\ \bigwedge^l(V) & \xrightarrow[g]{} & \bigwedge^l(V') \end{array}$$

där $(f\times\ldots\times f)(v_1,\ldots,v_l)=(f(v_1),\ldots,f(v_l))$ och $\rho_V,\rho_{V'}$ är de alternerande avbildningarna ur definitionen av yttre potensen (5.11). Men $\rho_{V'}(f\times\ldots\times f)$ är alternerandeså att det finns g sådan att diagrammet kommuterar (även här (5.11)). Vi definierar $\bigwedge^l(f)=g$. Formeln för $\bigwedge^l(f)$ uttrycker just kommutativiteten av diagrammet. □

För att kunna närmare undersöka yttre potenser behöver vi tensoralgebror och yttre algebror (som också kallas Grassmannalgebror). Resten av detta kapitel ägnar vi åt dessa viktiga begrepp. Som tidigare är K en kommutativ ring med etta. R kommer att beteckna en godtycklig associativ ring med etta. Vi behöver först ett mycket allmänt begrepp:

(5.16) Definition. Man säger att en ring R är **graderad** om det finns delgrupper R_i, $i=0,1,2,\ldots$ till den additiva gruppen R sådana att $R=\oplus_{i=0}^{\infty}R_i$ och $R_iR_j\subseteq R_{i+j}$. Elementen i R_i kallas **homogena av grad** i. Om dessutom R är en K–algebra och R_i är K–moduler så säger man att R är en graderad K–algebra.

□

(5.17) Exempel. Låt $R=K[X_1,\ldots,X_n]$ och $R_i=$ alla homogena polynom i $X_1,\ldots,X_n$ av grad i och nollpolynomet (t ex $R_0=K$, $R_1=KX_1+\ldots+KX_n$, $R_2=\sum KX_iX_j$ osv).

□

(5.18) Hur kan man konstruera en graderad algebra? Antag att vi för varje $i=0,1,\ldots$ har en K-modul R_i (K en kommutativ ring) och för varje par (i,j) en K-bilinjär avbildning $R_i\times R_j\to R_{i+j}$. Om $(r_i,r_j)\in R_i\times R_j$ så betecknar vi med r_ir_j bilden av detta par i R_{i+j}. Vidare förutsätter vi att $(r_ir_j)r_k=r_i(r_jr_k)$ då $r_i\in R_i$, $r_j\in R_j$ och $r_k\in R_k$. Då är $R=\oplus_{i=0}^{\infty}R_i$ en graderad ring och även en K-algebra (se (4.18)) om man definierar multiplikationen i R så att

$$(\sum r_i)(\sum r'_j)=\sum r''_k,$$

där $r''_k=\sum_{i+j=k}r_ir'_j$. □

(5.19) Konstruktionen av tensoralgebran. Låt V vara en K-modul. Låt för varje $i>0$, $R_i=V^{\otimes i}$ ($=V\otimes\ldots\otimes V$ med i faktorer) och $R_0=V^{\otimes 0}:=K$. Modulen $V^{\otimes i}$ betecknas

ofta $T^i(V)$. Vi vet att tensorprodukten är associativ vilket ger en K-bilinjär avbildning $R_i \times R_j \to R_{i+j}$ som är associativ[††]. Den graderade K-algebran

$$T(V) = \oplus_{i=0}^{\infty} T^i(V)$$

kallas **tensoralgebran** av V över K (se (5.16)). □

(5.20) Anmärkning. Om $e_1, \ldots, e_n$ är en bas för V över K så vet vi att $T^k(V)$ har en bas bestående av alla produkter $e_{i_1} \otimes \ldots \otimes e_{i_k}$. Algebran $T(V)$ kallas ofta för **algebran av icke-kommutativa polynom** i n variabler. För att motivera den termen låt oss beteckna e_i med X_i och skriva $X_{i_1}X_{i_2}\ldots X_{i_k}$ i stället för $e_{i_1} \otimes e_{i_2} \otimes \ldots \otimes e_{i_k}$. Då kan varje element i $T^k(V)$ skrivas som en linjär kombination av $X_{i_1}X_{i_2}\ldots X_{i_k}$ (med icke-kommuterande X_i) och varje element i $T(V)$ är en summa av sådana termer.

□

För att bilda en algebra ur yttre produkter $R_i = \bigwedge^i(V)$ krävs en liten ansträngning (vi har inte någon bilinjär funktion från $\bigwedge^i(V) \times \bigwedge^j(V)$ till $\bigwedge^{i+j}(V)$).

(5.21) Definition. Låt $R = \oplus_{i=0}^{\infty} R_i$ vara en graderad ring. Man säger att I är ett **homogent** (= **graderat**) ideal i R om det finns delgrupper I_k till R_k sådana att $I = \oplus_{k=0}^{\infty} I_k$ är ett ideal i R. Om R är en graderad K–algebra (med K–moduler R_k) och I_k är K-delmoduler till R_k så säger man att I är ett homogent K-ideal i R.

□

(5.22) Exempel. Låt $R = K[X_1, \ldots, X_n]$ med gradering som i exempel (5.16). Låt $I_k = R_k$ då $k \geq 1$ och $I_0 = (0)$. Då är $I = \{\text{alla polynom } p \text{ sådana att } p(0, \ldots, 0) = 0\}$. I är homogent.

□

(5.23) Proposition. *Låt $R = \oplus_{k=0}^{\infty} R_k$ vara en graderad K-algebra och $I = \oplus_{k=0}^{\infty} I_k$ ett homogent K-ideal i R. Då är R/I en graderad K-algebra med gradering som ges av R_k/I_k (inbäddade i R/I) och multiplikation $R_k/I_k \times R_l/I_l \to R_{k+l}/I_{k+l}$ definierad genom $(\bar{r}_k, \bar{r}_l) \mapsto \overline{r_k r_l}$.*

Bevis. Eftersom paret (I_k, R_k) är inbäddat i paret (I, R), så har vi en K-homomorfism $R_k/I_k \to R/I$ med kärnan $(I \cap R_k)/I_k = (0)$ (ty $I \cap R_k = I_k$) dvs en monomorfism. Vi skall identifiera R_k/I_k med dess bild i R/I. Om $r \in R$ så är $r = \sum r_k$, $r_k \in R_k$, dvs $\bar{r} = \sum \bar{r}_k, \bar{r}_k \in R_k/I_k$ så att R/I är summan av alla R_k/I_k. Det är lätt att visa att framställningen $\bar{r} = \sum \bar{r}_k, \bar{r}_k \in R_k/I_k$ är entydig. Det återstår att kontrollera att avbildningen $(\bar{r}_k, \bar{r}_l) \mapsto \overline{r_k r_l}$ är väldefinierad och bilinjär. Men detta är trivialt. □

[††] $V^{\otimes i} \times V^{\otimes j} \to V^{\otimes(i+j)}$ får man som sammansättningen $V^{\otimes i} \times V^{\otimes j} \to V^{\otimes i} \otimes V^{\otimes j} \cong V^{\otimes(i+j)}$, där den sista isomorfismen avbildar $(v_1 \otimes \ldots \otimes v_i) \otimes (v'_1 \otimes \ldots \otimes v'_j)$ på $v_1 \otimes \ldots \otimes v_i \otimes v'_1 \otimes \ldots \otimes v'_j$.

(5.24) Konstruktionen av yttre algebran. Låt V vara en K-modul och låt $T(V) = \oplus_{k=0}^{\infty} T^k(V)$ vara tensoralgebran av V. Låt I_k vara den delmodul till $T^k(V)$ som genereras av alla $v_1 \otimes \ldots \otimes v_k$ med minst två faktorer lika. Man kontrollerar lätt att $I = \oplus_{k=0}^{\infty} I_k$ är ett K-ideal i $T(V)$ (om man multiplicerar ett element $v_1 \otimes \ldots \otimes v_k$ som har minst två lika faktorer med ett godtyckligt element ur $T(V)$ så får man en summa av termer sådana att varje term är en produkt med minst två lika faktorer). Kvotalgebran $T(V)/I$ är graderad med $T^k(V)/I_k = \bigwedge^k(V)$ enligt (5.23) (se (5.14)). Den kallas **yttre algebran** av V och betecknas $\bigwedge(V)$ footnote$\bigwedge(V)$ definierades av Hermann Grassmann (1809 – 1877) år 1844.. Alltså är $\bigwedge(V) = \oplus_{k=0}^{\infty} \bigwedge^k(V)$. Observera att $I_0 = (0)$ så att $\bigwedge^0(V) = K$. Även $I_1 = (0)$ dvs $\bigwedge^1(V) = V$.

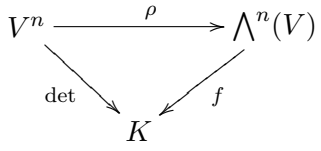
Nu kan vi beskriva $\bigwedge^k(V)$ för fria K-moduler V:

(5.25) Proposition. *Låt V vara en fri K-modul av dimension n över K med bas $e_1, \ldots, e_n$. Då är $\bigwedge^k(V)$ en fri K-modul,* $\dim_K \bigwedge^k(V) = \binom{n}{k}$ *för $0 \leq k \leq n$ och om $1 \leq k \leq n$ så bildar $e_{i_1} \wedge \ldots \wedge e_{i_k}$, där $1 \leq i_1 < \ldots < i_k \leq n$, en bas för $\bigwedge^k(V)$ över K. Dessutom är $\bigwedge^0(V) = K$ och $\bigwedge^k(V) = (0)$ då $k > n$.*

Bevis. Fallet $k = 0$ är klart ty $\bigwedge^0(V) = K$. Antag att $k > 0$. Vi vet att $e_{j_1} \otimes \ldots \otimes e_{j_k}$ (fortfarande alla $j_1, \ldots, j_k$) bildar en bas för $T^k(V)$. Alltså genererar $e_{j_1} \wedge \ldots \wedge e_{j_k}$ produkten $\bigwedge^k(V)$. Om bland $j_1, \ldots, j_k$ finns minst två index lika – detta måste vara fallet då $k > n$ – så är $e_{j_1} \wedge \ldots \wedge e_{j_k} = 0$. Alltså får vi att $\bigwedge^k(V) = 0$ då $k > n$ och vi kan förutsätta nu att $1 \leq k \leq n$ och alla $j_1, \ldots, j_k$ är olika. Vi vet att om $i_1, \ldots, i_k$ är en permutation av $j_1, \ldots, j_k$ så är

$$e_{j_1} \wedge \ldots \wedge e_{j_k} = \pm e_{i_1} \wedge \ldots \wedge e_{i_k}$$

med tecknet som beror på antalet inversioner som behövs för att överföra $j_1, \ldots, j_k$ på $i_1, \ldots, i_k$. I varje fall har vi en sådan likhet med $1 \leq i_1 < i_2 < \ldots < i_k \leq n$. Nu vill vi visa att sådana $e_{i_1} \wedge \ldots \wedge e_{i_k}$ bildar en bas för $\bigwedge^k(V)$ (deras antal är $\binom{n}{k}$). För att göra det visar vi först att $ae_1 \wedge \ldots \wedge e_n \neq 0$ om $a \neq 0$ dvs $\dim_K \bigwedge^n(V) = 1$. Betrakta diagrammet:



där $\det(v_1, \ldots, v_n)$ = determinanten av $v_1, \ldots, v_n$ m.a.p. basen $e_1, \ldots, e_n$. Eftersom "det" är alternerandeså existerar f linjär så att $f\rho = \det$. Men $\det(ae_1, \ldots, e_n) = a$, så att $f\rho(ae_1, \ldots, e_n) = f(ae_1 \wedge \ldots \wedge e_n) = a$. Alltså är $a(e_1 \wedge \ldots \wedge e_n) \neq 0$ om $a \neq 0$. Antag nu att $1 \leq k \leq n$ och att

$$\omega = \sum_{1 \leq i_1 < \ldots < i_k \leq n} a_{i_1 \ldots i_k} e_{i_1} \wedge \ldots \wedge e_{i_k} = 0.$$

Vi vill visa att alla $a_{i_1\ldots i_k} = 0$. Låt oss fixera en koefficient $a_{i_1\ldots i_k}$ och betrakta $\omega \wedge (e_{j_1} \wedge \ldots \wedge e_{j_l})$, där

$$\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset \quad \text{och} \quad \{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_l\} = \{1, \ldots, n\}.$$

Då får vi att

$$\omega \wedge (e_{j_1} \wedge \ldots \wedge e_{j_l}) = \pm a_{i_1\ldots i_k}(e_1 \wedge \ldots \wedge e_n) = 0$$

ty $\omega = 0$. (Observera att vi arbetar i $\bigwedge(V)$!). Men $ae_1 \wedge \ldots \wedge e_n \neq 0$ för $a \neq 0$ ger nu att $a_{i_1\ldots i_k} = 0$ dvs alla koefficienter av ω är $= 0$. □

Med hjälp av (5.25) kan man lätt beskriva ytteralgebran $\bigwedge(V)$ för en fri K-modul V:

(5.26) Följdsats. *Om $e_1, \ldots, e_n$ bildar en bas för V över K så bildar 1 och $e_{i_1} \wedge \ldots \wedge e_{i_k}$, där $1 \leq k \leq n$ och $1 \leq i_1 < \ldots < i_k \leq n$ en bas för $\bigwedge(V)$. Alltså är $\dim_K \bigwedge(V) = 2^n$.*

(5.27) Exempel. Låt $V = Ke_1 + Ke_2$. Då har $\bigwedge(V)$ som bas $1, e_1, e_2$ och $e_{12} := e_1 \wedge e_2$ med multiplikationstabellen:

	1	e_1	e_2	e_{12}
1	1	e_1	e_2	e_{12}
e_1	e_1	0	e_{12}	0
e_2	e_2	$-e_{12}$	0	0
e_{12}	e_{12}	0	0	0

□

Innan vi fortsätter med exempel låt oss anteckna en isomorfism som har stor betydelse då man definierar tensorer på mångfalder:

(5.28) Proposition. *Låt V vara en fri K-modul med bas $e_1, \ldots, e_n$ och låt $e^1, \ldots, e^n$ vara den duala basen för V^*. Då finns det en isomorfism $\bigwedge^k(V^*) \cong \bigwedge^k(V)^*$ sådan att mot $e^{i_1} \wedge \ldots \wedge e^{i_k}$ svarar $f_{i_1\ldots i_k} : \bigwedge^k(V) \to K$, där $f_{i_1\ldots i_k}(e_{i_1} \wedge \ldots \wedge e_{i_k}) = 1$ och $f_{i_1\ldots i_k}(e_{j_1} \wedge \ldots \wedge e_{j_k}) = 0$ då $(j_1, \ldots, j_k) \neq (i_1, \ldots, i_k)$ (vi förutsätter att $1 \leq k \leq n$).*

Bevis. Vi vet att $e^{i_1} \wedge \ldots \wedge e^{i_k}$ med $1 \leq i_1 < \ldots < i_k \leq n$ bildar en bas för $\bigwedge^k(V^*)$ och $f_{i_1\ldots i_k}$ en bas för $\bigwedge^k(V)^*$ så att påståendet är självklart. □

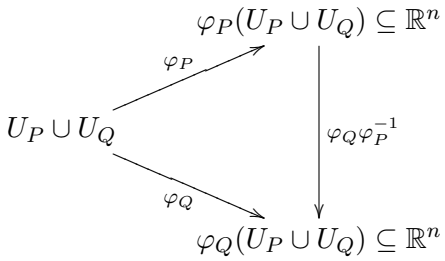
(5.29) Anmärkning. Ofta identifierar man $\bigwedge^k(V^*)$ med $\bigwedge^k(V)^*$ i enlighet med (5.28) (utan närmare kommentarer). Vi vet från tidigare att $T^k(V^*) \cong T^k(V)^*$ (se (4.17). Se vidare Övn. 12 och 13.

□

(5.30) Anmärkning. Låt M vara en C^∞-mångfald av dimension n (t ex $M = \mathbb{R}^n$ med sin naturliga analytiska struktur). Med $T_p(M)$ kommer vi att beteckna tangentrummet i punkten $P \in M$. Med ett **tensorfält på M av typen** (k, l) menar man en funktion Φ som mot varje $P \in M$ ordnar en tensor av typen (k, l) över $T_p(M)$. Låt $\frac{\partial}{\partial x_p^1}, \ldots, \frac{\partial}{\partial x_p^n}$ vara en bas för $T_p(M)$ och $dx_p^1, \ldots, dx_p^n$ den duala basen (se (3.23)) för $T_p(M)^* = \mathrm{Hom}_{\mathbb{R}}(T_p(M), \mathbb{R})$ dvs

$$(dx_P^i)(\frac{\partial}{\partial x_P^j}) = \delta_{ij}$$

(x_p^i är lokala koordinater i P dvs det finns en öppen omgivning U_P till P sådan att $\varphi_P(X) = (x_P^1(X), \ldots, x_P^n(X))$ för $X \in U_p$ är en homeomorfism av U_P med en öppen delmängd till $\mathbb{R}^n$ och om $Q \in M$ är en annan punkt med lokala koordinater x_Q^i i en omgivning U_Q så är funktionen $\varphi_Q \varphi_P^{-1}$ i det kommutativa diagrammet:



en C^∞-funktion).

Ett vektorfält ξ på M är alltså ett tensorfält av typen $(1, 0)$ (ett val av en tangentvektor $\xi(P)$ ur varje $T_P(M)$). En Riemann–metrik på M är ett tensorfält av typen $(0, 2)$ (en sådan metrik ger för varje $P \in M$ ett element ur

$$T_P(M)^* \otimes T_P(M)^* = \mathrm{Hom}_{\mathbb{R}}(T_P(M)^{\otimes 2}, \mathbb{R}) \cong \mathrm{Bil}_{\mathbb{R}}(T_P(M) \times T_P(M), \mathbb{R})$$

– mera exakt är en sådan tensor symmetrisk). En l-dimensionell differentialform

$$\omega(P) = \sum \omega_{i_1 \ldots i_l}(P) dx^{i_1} \wedge \ldots \wedge dx^{i_l}$$

är ett tensorfält av typen $(0, l)$ (Vi har

$$\omega(P) \in T_P(M)^* \otimes \ldots \otimes T_P(M)^* = \mathrm{Hom}_{\mathbb{R}}(T_P(M)^{\otimes l}, \mathbb{R}) \cong \mathrm{Mult}_{\mathbb{R}}(T_P(M)^l, \mathbb{R})$$

och ω är alternerandedvs tillhör delmodulen

$$\mathrm{Ant}_{\mathbb{R}}(T_P(M)^l, \mathbb{R}) \cong \bigwedge^l (T_P(M))^* = \bigwedge^l (T_P(M)^*)$$

– se (5.25)). Låt oss påpeka att i analytiska sammanhang är man intresserad av tensorfält Φ som tar lämplig hänsyn till den analytiska strukturen på M (t ex av kontinuerliga vektorfält $\xi(P) = \sum_{i=1}^n v_i(P) \frac{\partial}{\partial x^i}$ med kontinuerliga $v_i(P)$ på U_P) så att t ex en Riemann–metrik eller en differentialform inte enbart är ett val av en tensor utan ett sådant val att koefficientfunktionerna (t ex $\omega_{i_1 \ldots i_l}(P)$) har goda analytiska egenskaper (t ex är C^∞).

□

APPENDIX C: DETERMINANTER

Syftet med detta Appendix är att repetera begreppet determinant och utvidga dess definition till godtyckliga kommutativa ringar med etta. Vi har utnyttjat determinanter i Proposition (5.25) då vi visade satsen om dimensionen av yttre potenser av en fri modul över en kommutativ ring.

Om $v_1, v_2, \ldots, v_n$ är vektorer i $\mathbb{R}^n$ och $v_i = (a_{1i}, \ldots, a_{ni})$ så definieras determinanten av matrisen $A = [v_1, \ldots, v_n]$ vars kolonner är vektorerna v_i som

$$\det A = \sum (-1)^{sign(p_1,p_2,\ldots,p_n)} a_{1p_1} a_{2p_2} \cdots a_{np_n}, \tag{C.1}$$

där summan sträcker sig över alla permutationer $p_1, p_2, \ldots, p_n$ av $1, 2, \ldots, n$ och sign betecknar permutationens tecken. Man bevisar därefter olika egenskaper hos determinanter med utgångspunkt från denna definition.

Man konstaterar lätt att höger ledet i denna definition endast beror på ringstrukturen hos de reella talen så att det inte finns några hinder om man vill generalisera denna definition till helt godtyckliga kommutativa ringar. Antag alltså att K är en kommutativ ring med etta och att $M_n(K)$ är ringen av $(n \times n)$–matriser över K. Om $A = [a_{ij}] \in M_n(K)$ så definierar man determinanten av A med hjälp av exakt samma uttryck (C.1).

Determinanten kan uppfattas som en funktion $f : V^n \to K$, där $V = K^n$ och för godtyckliga vektorer $v_i = (a_{1i}, \ldots, a_{ni}) \in V$:

$$f(v_1, v_2, \ldots, v_n) = \det[v_1, v_2, \ldots, v_n] = \det A = \sum (-1)^{sign(p_1,p_2,\ldots,p_n)} a_{1p_1} a_{2p_2} \cdots a_{np_n}. \tag{C.2}$$

f är en multilinjär alternerande funktion dvs den är additiv:

$$f(v_1, \ldots, v_k + v_k', \ldots, v_n) = f(v_1, \ldots, v_k, \ldots, v_n) + f(v_1, \ldots, v_k', \ldots, v_n),$$

homogen:

$$f(v_1, \ldots, av_k, \ldots, v_n) = af(v_1, \ldots, v_k, \ldots, v_n)$$

då $a \in K$ och alternerande:

$$f(v_1, \ldots, v_k, v_{k+1}, \ldots, v_n) = 0$$

om $v_k = v_{k+1}$ dvs determinanten av A är lika med 0 om två (bredvidstående) kolonner i A är lika. Dessutom är $f(e_1, e_2, \ldots, e_n) = 1$ då e_i bildar standardbasen för $V = K^n$ dvs basen bestående av vektorer med exakt en etta som komponent och alla andra komponenter lika med 0.

Det visar sig att dessa egenskaper bestämmer f entydigt och utgör grunden för att härleda alla andra formella beräkningsregler för determinanter. Vi repeterar om en stund ett bevis av dessa egenskaper som gäller för determinanter definierade med hjälp av (C.2) över godtyckliga kommutativa ringar med etta. Först låt oss bevisa entydigheten av determinater:

(C.3) Proposition. *Låt $f : V^n \to K$ vara en multilinjär alternerande funktion sådan att $f(e_1, e_2, \ldots, e_n) = 1$ för en bas $e_1, e_2, \ldots, e_n$ för V över K. Om $v_i = \sum a_{ij} e_j$, så är*

$$f(v_1, \ldots, v_n) = \sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} a_{2p_2} \cdots a_{np_n},$$

där man summerar över alla permutationer $p_1, p_2, \ldots, p_n$ av talen $1, 2, \ldots, n$. Om $f' : V^n \to K$ är en annan multilinjär alternerande funktion så är $f' = af$, där $a = f'(e_1, e_2, \ldots, e_n)$.

Bevis. Vi har

$$f'(v_1, \ldots, v_n) = f'(\sum a_{1j} e_j, \ldots, \sum a_{nj} e_j) = \sum a_{1p_1} a_{2p_2} \cdots a_{np_n} f'(e_{p_1}, e_{p_2}, \ldots, e_{p_n}) =$$

$$\sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} a_{2p_2} \cdots a_{np_n} f'(e_1, e_2, \ldots, e_n),$$

där man summerar över alla permutationer $p_1, p_2, \ldots, p_n$ av $1, 2, \ldots, n$ och sign betecknar permutationens tecken. Vi utnyttjar här (5.10) och vår förutsättning att $f(e_1, e_2, \ldots, e_n) = 1$. Om $f' = f$ får man

$$f(v_1, \ldots, v_n) = \sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} a_{2p_2} \cdots a_{np_n}.$$

Alltså för en godtycklig alternerande funktion har vi $f' = af$ med $a = f'(e_1, e_2, \ldots, e_n)$. □

I grundläggande kurser i linjär algebra visas att determinant verkligen är en multilinjär alternerande funktion även om man för det mesta inte använder dessa termer. Vi skall kort repetera argumenten som visar att f som definieras av (C.2) är additiv, homogen, alternerande och $f(e_1, e_2, \ldots, e_n) = 1$ i standardbasen för $V = K^n$.

Den sista egenskapen är helt trivial – uttrycket till höger i (C.2) är 1 om $a_{ij} = 0$ då $i \neq j$ och $a_{ii} = 1$. Om $v'_k = \sum a'_{kj} e_j$ så är

$$f(v_1, \ldots, v_k + v'_k, \ldots, v_n) = \sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} \cdots (a_{kp_k} + a'_{kp_k}) \cdots a_{np_n} =$$

$$\sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} \cdots a_{kp_k} \cdots a_{np_n} + \sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} \cdots a'_{kp_k} \cdots a_{np_n} =$$

$$f(v_1, \ldots, v_k, \ldots, v_n) + f(v_1, \ldots, v'_k, \ldots, v_n),$$

vilket visar den additiva egenskapen. Vi har

$$f(v_1, \ldots, av_k, \ldots, v_n) = \sum (-1)^{sign(p_1, p_2, \ldots, p_n)} a_{1p_1} \cdots a a_{kp_k} \cdots a_{np_n} = af(v_1, \ldots, av_k, \ldots, v_n),$$

dvs funktionen f är homogen. Slutligen om t ex $v_1 = v_2$ så kan man para ihop varje term i summan till höger i (C.2) som innehåller produkten $a_{1r}a_{2s}$ med den term som innehåller produkten $a_{1s}a_{2r}$ ($r \neq s$) och som för övrigt innehåller samma faktorer a_{ip_i} då $i \geq 3$. Eftersom permutationerna $(r, s, p_3, \ldots, p_n)$ och $(s, r, p_3, \ldots, p_n)$ har motsatta tecken (de skiljer sig så när som på en transposition) så är summan av motsvarande termer i (C.2) lika med 0. På det sättet kan vi para ihop alla termer i summan (C.2) som därmed är lika med 0 (vi tar alla möjliga par (r, s) av de två första indexen åtföljda av alla möjliga permutationer $(p_3, \ldots, p_n)$ sådana att $(r, s, p_3, \ldots, p_n)$ är en permutation av $(1, 2, \ldots, n)$.

På det sättet har vi visat:

(C.4) Proposition. *Om V är en fri K–modul och $e_1, e_2, \ldots, e_n$ är en godtycklig bas så existerar en multilinjär alternerande funktion $f : V^n \to K$ sådan att $f(e_1, e_2, \ldots, e_n) = 1$. Om f och f' är två sådana funktioner så är $f' = af$, där a är en enhet i ringen K som är lika med determinanten av övergångsmatrisen från en bas $e'_1, e'_2, \ldots, e'_n$ i vilken $f'(e'_1, e'_2, \ldots, e'_n) = 1$ till basen $e_1, e_2, \ldots, e_n$. I synnerhet om $V^n = M_n(K)$ och $f(E) = 1$, där E är enhetsmatrisen, så ges f av* (C.2).

Bevis. Det återstår att visa den näst sista delen. Vi vet från (C.3) att $a = f'(e_1, e_2, \ldots, e_n)$. Av symmetriskäl är $f = a'f'$, där $a' = f'(e_1, e_2, \ldots, e_n)$. Alltså är $1 = f(e_1, e_2, \ldots, e_n) = a'f'(e_1, e_2, \ldots, e_n) = a'a$, så att a och a' är enheter i K. Det framgår av beräkningen i början av beviset för (C.3) att $a = f'(e_1, e_2, \ldots, e_n) = f'(\sum b_{1j}e'_j, \sum b_{2j}e'_j, \ldots, \sum b_{nj}e'_j) = \det[b_{ij}]$. □

Determinanter kan användas för att lösa linjära ekvationssystem. Vi bevisar en generalisering av Cramers regel som vi kommer att utnyttja vid olika tillfällen.

(C.5) Proposition. *Låt V vara en fri K–modul av rang n och $f : V^n \to K$ en alternerande multilinjär avbildning. Om $x_1v_1 + \cdots + x_nv_n = w$, där $x_i \in K$ och $v_i, w \in V$ så gäller $x_i f(v_1, \ldots, v_n) = f(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n)$. I synnerhet om $V = K^n$, och $f(v_1, \ldots, v_n) = \det[v_1, \ldots, v_n]$ är en enhet i K så är*

$$x_i = \det[v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n]/\det[v_1, \ldots, v_n].$$

Bevis. Vi har

$$f(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n) = f(v_1, \ldots, v_{i-1}, \sum_j x_j v_j, v_{i+1}, \ldots, v_n) =$$

$$x_i f(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n).$$

□

Observera att (vektor–)ekvationen $x_1v_1 + \cdots + x_nv_n = w$ kan skrivas som ett "vanligt" linjärt ekvationssystem med n ekvationer och n obekanta om $v_i, w \in K^n = V$ tolkas som kolonnvektorer. Se vidare Övn. 5.

(C.6) Anmärkning. Vi avslutar med en kommentar om determinanter av linjära avbildningar. Låt som tidigare V vara en fri K–modul av rang n med en bas $e_1, \ldots, e_n$ över K. Som vi vet definieras vanligen determinanten av en linjär avbildning $\varphi : V \to V$, $\varphi(e_j) = \sum a_{ij}e_i$, som determinanten av matrisen $M_\varphi = [a_{ij}]$. Man bevisar att determinanten av φ inte beror på basvalet (se Övn. 4). Determinanten kan definieras på ett "koordinatfritt" sätt med hjälp av yttre produkter. Eftersom $\bigwedge^n V$ är en fri modul av rang 1 och $e_1 \wedge \ldots \wedge e_n$ är dess bas, så är $\varphi(e_1 \wedge \ldots \wedge e_n) = d(e_1 \wedge \ldots \wedge e_n)$, där $d \in K$. Det är inte svårt att visa att d inte beror på basvalet och dessutom $d = \det M_\varphi$. Därför kan man definiera determinanten av φ som just $d \in K$ sådant att $\bigwedge^n \varphi(x) = dx$ för varje $x \in \bigwedge^n V$. Notera dock att förutsättningen för en sådan definition är kunskapen om att rangen av $\bigwedge^n V$ är lika med 1. Detta påstående visade vi just med hjälp av determinatbegreppet.

ÖVNINGAR

5.1. Låt $e_1, \ldots, e_n$ vara en bas för en fri modul V över en ring K.

(a) Förenkla $(e_1 + e_2) \wedge (e_1 + e_2 + e_3) + e_3 \wedge (e_1 + e_3) - (2e_2 + e_3) \wedge e_3$ och $e_1 \wedge e_2 \wedge e_3 \wedge e_4 - e_4 \wedge e_3 \wedge e_2 \wedge e_1$.

(b) Visa att

$$e_n \wedge e_{n-1} \wedge \ldots \wedge e_1 = (-1)^{\frac{n(n-1)}{2}} e_1 \wedge e_2 \wedge \ldots \wedge e_n.$$

5.2. Låt V vara ett vektorrum över en kropp K och $v_1, \ldots, v_r \in V$. Visa att $v_1, \ldots, v_r$ är linjärt beroende över K då och endast då $v_1 \wedge \ldots \wedge v_r = 0$ i $\bigwedge(V)$.

5.3. Beräkna $\det(\bigwedge^2(\varphi))$ då $\varphi : K^3 \to K^3$ (K en kropp) har matrisen $\begin{pmatrix} 1 & 0 & 2 \\ 3 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

5.4. Låt V vara en fri K–modul av rang n och låt $\varphi : V \to V$ vara en K–homomorfism.

(a) Visa att det finns exakt ett element $d \in K$ sådant att för varje $\alpha \in \bigwedge^n(V)$ är $\bigwedge^n(\varphi)(\alpha) = d\alpha$.

(b) Visa att $d = \det(\varphi)$.

Anmärkning. (a) kan antas som definition av begreppet determinant om man visar först att $\bigwedge^n(V)$ har dimension 1 över K. Se Appendix (C.6).

(c) Visa att determinanten av φ inte beror på basvalet för V.

Anmärkning. För att visa (c) kan man använda (a) eller allmänna samband mellan matriser för samma tensor i olika baser dvs (5.4).

5.5. Låt K vara en kommutativ ring med etta och V en godtycklig K-modul. Låt $v_1, \ldots, v_r \in V$ och låt $A = [a_{ij}] \in M_r(K)$ vara en matris med element i K. Visa att om $\sum a_{ij} v_i = 0$, så är $\det[a_{ij}] v_i = 0$ för $i = 1, \ldots, r$.

5.6. Ett element $\alpha \in \bigwedge(V)$ kallas r-multivektor ($r = 1$ – vektor, $r = 2$ – bivektor) om det finns vektorer $v_1, \ldots, v_r \in V$ sådana att $\alpha = v_1 \wedge \ldots \wedge v_r$. Visa att

(a) om $\dim V \leq 3$ så är varje homogent element in $\bigwedge(V) \setminus K$ en multivektor,

(b) om $\dim V = 4$ och e_1, e_2, e_3, e_4 är en bas för V över K så är $\alpha = e_1 \wedge e_2 + e_3 \wedge e_4$ inte en multivektor.

5.7. Låt W vara ett r-dimensionellt delrum till ett linjärt rum V över K. Med en **riktningsvektor** för W menar man en godtycklig r – multivektor (se Övn. 6) $v_1 \wedge \ldots \wedge v_r$, där $v_1, \ldots, v_r$ bildar en bas för W över K.

(a) Visa att om $\alpha = v_1 \wedge \ldots \wedge v_r$ och $\beta = u_1 \wedge \ldots \wedge u_r$ är två riktningsvektorer för W så är $\alpha \neq 0 \neq \beta$ och det finns $a \in K^*$ så att $\beta = a\alpha$.

(b) Visa att två olika r-dimensionella delrum till V har icke-proportionella riktningsvektorer.

(c) Låt $[\alpha]$ beteckna klassen av alla multivektorer proportionella till $\alpha \neq 0$. Visa att det finns $1-1$ motsvarighet mellan alla r-dimensionella delrum W till V och alla klasser $[\alpha]$ där $\alpha \neq 0$ är en r-multivektor.

Ledning. Utnyttja övning 2.

Anmärkning. Mängden av alla r-dimensionella delrum till V betecknas med $\mathbb{P}_r(V)$. $\mathbb{P}_1(V)$ kallas **projektiva rummet** associerat med V. Se nästa övning.

5.8. Låt $e_1, \ldots, e_n$ vara en bas för V över K och låt W vara ett r-dimensionellt delrum till W (dvs $W \in \mathbb{P}_r(V)$ – se Övn. 7). Med **Plückerkoordinaterna** för W m.a.p. $e_1, \ldots, e_n$ menas koordinaterna av en godtycklig riktningsvektor α för W ($\alpha \in \bigwedge^r(V)$) m.a.p. basen $e_{i_1} \wedge \ldots \wedge e_{i_r}$ för $\bigwedge^r(V)$ dvs om $\mathbf{x}_k = x_k^{i_k} e_{i_k}$, $k = 1, \ldots, r$ är en bas för W så är

$$\alpha = x_1^{i_1} e_{i_1} \wedge \ldots \wedge x_r^{i_r} e_{i_r} = A^{i_1 \ldots i_r} e_{i_1} \wedge \ldots \wedge e_{i_r}$$

(man summerar över alla $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$).

(a) Ge en beskrivning av Plückerkoordinaterna för W med hjälp av lämpliga determinanter. Gör det speciellt för $r = 1$ och $r = 2$, $n = 4$.

(b) Motivera att Plückerkoordinaterna för W är definierade så när som på en faktor ur K^* (dvs $A^{i'_1 \ldots i'_r} = \rho A^{i_1 \ldots i_r}, \rho \in K^*$).

(c) Låt (A^{ij}), $1 \leq i < j \leq r$ vara Plückerkoordinaterna för ett delrum $W \subset V$, där $\dim_k W = 2$ och $\dim V = 4$. Visa att $A^{12}A^{34} - A^{13}A^{24} + A^{14}A^{23} = 0$.

Anmärkning. (c) visar att inte varje uppsättning $A^{12}, A^{13}, A^{14}, A^{23}, A^{24}, A^{34}$ av 6 element ur K utgör Plückerkoordinaterna för ett 2-dimensionellt delrum till V av dimensionen 4. Plückerkoordinaterna måste uppfylla en ekvation – ett Plückersamband ur (c). Situationen är typisk för allmänna fallet: koordinaterna för r-dimensionella delrum till V svarar exakt mot lösningarna till ett ekvationssystem (proportionella lösningar identifieras). Dessa lösningar bildar en projektiv algebraisk mängd – den kallas **Grassmannmångfald**. Vi återkommer till Grassmannmångfalder i senare delen av kursen.

5.9. Låt $\varphi : V \to V$ vara en linjär avbildning av ett K-vektorrum V och låt $W \subseteq V$ vara ett ändligt dimensionellt delrum till V. Visa att om W är φ-invariant (dvs $\varphi(W) \subseteq W$) så är varje riktningsvektor för W (se Övn. 7) en egenvektor till $\bigwedge^r(\varphi)$ där $r = \dim_K W$, och omvänt, om en riktningsvektor för W är en egenvektor till $\bigwedge^r(\varphi)$ hörande till ett egenvärde $\neq 0$ så är W φ-invariant. Är förutsättningen att egenvärdet skall vara $\neq 0$ väsentlig?

5.10. (a) Formulera definitionen av den k-te symmetriska potensen $(S^k(M), \rho)$ av en R-modul M (analogt till (5.11)), bevisa dess entydighet (analogt till (5.6)) och konstruera den (analogt till (5.13)). Definiera därefter R-homomorfismen $S^k(f) : S^k(M) \to S^k(N)$ för en R-homomorfism $f : M \to N$ (analogt till (5.15)) och konstruera den symmetriska algebran $S(M) = \oplus_{k=0}^{\infty} S^k(M)$ (analogt till (5.24)).

(b) Låt $V = Ke_1 + \ldots + Ke_n$ vara ett K-vektorrum av dimensionen n över K. Visa att $S(V) \cong K[X_1, \ldots, X_n]$ (polynomringen i n variabler).

5.11. Konstruera en "egen" produkt analogt till tensorprodukter, alternerande och symmetriska och utveckla dess teori som t.ex. i Övn. 10.

5.12. Låt $T_1 : V^i \to K$ och $T_2 : V^j \to K$ vara två tensorer (se (5.1) (b)) och definiera

$$(T_1 \otimes T_2)(v_1, \ldots, v_i, v'_1, \ldots, v'_j) = T_1(v_1, \ldots, v_i) T_2(v'_1, \ldots, v'_j)$$

($T_1 \otimes T_2$ är helt enkelt sammansättningen av den naturliga avbildningen från $V^i \times V^j$ till $T^i(V) \otimes T^j(V)$ med tensorprodukten av de linjära avbildningar $T^i(V) \to K$ och $T^j(V) \to K$ som svarar mot T_1 och T_2, samt avbildningen $K \otimes_K K \to K$, där $a \otimes b \mapsto ab$). Låt $\mathcal{T}(V) = \coprod_{i=0}^{\infty} \mathrm{Mult}(V^i, K)$ med multiplikation given ovan. Visa att $\mathcal{T}(V) \cong T(V^*)$ (tensoralgebran definierad i (5.19)).

Anmärkning. Tensoralgebran definieras i många läroböcker just på detta sätt. Metoden har stora pedagogiska fördelar.

5.13. Låt V vara ett K-vektorrum (K en kropp) och låt $\mathrm{Ant}_K(V^r, K)$ vara K-modulen av alla K-linjära alternerande avbildningar $\varphi : V^r \to K$, $r \geq 1$. Vi definierar också $\mathrm{Ant}_K(V^0, K) = K$. Låt

$$\Omega(V) = \coprod_{r=0}^{\infty} \mathrm{Ant}_K(V^r, K)$$

och definiera produkten i $\Omega(V)$ så att för $\omega \in \mathrm{Ant}_K(V^r, K)$ och $\eta \in \mathrm{Ant}_K(V^s, K)$ är

$$(\omega \wedge \eta)(v_1, \ldots, v_{r+s}) = \sum_{\sigma} \mathrm{sign}(\sigma)\omega(v_{\sigma(1)}, \ldots, v_{\sigma(r)})\eta(v_{\sigma(r+1)}, \ldots, v_{\sigma(r+s)}),$$

där man summerar över alla permutationer σ sådana att $\sigma(1) < \ldots < \sigma(r)$ och $\sigma(r+1) < \ldots < \sigma(r+s)$. Visa att

(a) $\Omega(V)$ är en K-algebra graderad av $\mathrm{Ant}_K(V^r, K)$,

(b) $\Omega(V) \cong \bigwedge(V^*)$ som K-algebror.

Ledning till (b). Notera att $\mathrm{Ant}_K(V^r, K) \cong \bigwedge^r(V)^*$. Betrakta vidare isomorfismen ur (5.28) och visa att diagrammet

$$\begin{array}{ccc} \bigwedge^r(V)^* \times \bigwedge^s(V)^* & \xrightarrow{\wedge} & \bigwedge^{r+s}(V)^* \\ \downarrow & & \downarrow \\ \bigwedge^r(V^*) \times \bigwedge^s(V^*) & \xrightarrow{\wedge} & \bigwedge^{r+s}(V^*) \end{array}$$

kommuterar där "$\wedge$" i övre raden är definierad i övningen (ovan) däremot "$\wedge$" i nedre raden kommer från $\bigwedge(V^*)$. Titta på basvektorerna $f_{i_1 \ldots i_r}, f_{j_1 \ldots j_s}$ för $\bigwedge^r(V)^*$ och $\bigwedge^s(V)^*$ (se (5.28)).

Anmärkning. I många läroböcker (t ex Spivak, Calculus on Manifolds) definieras differentialformer och deras algebra med utgångspunkt från definitionen av $\Omega(V)$. Men i flera andra utgår man ifrån $\bigwedge(V^*)$ (t ex Warner, Foundations of Differentiable Manifolds).

5.14. Låt $e_1, \ldots, e_n$ vara en bas för ett K-vektorrum V, där K är en kropp och $\mathrm{char}(K) \neq 2$.

(a) Visa att $\mathrm{Bil}(V^2, K) = \mathrm{Sym}_K(V^2, K) \oplus \mathrm{Ant}_K(V^2, K)$ ($\mathrm{Sym}_K(V^2, K)$ betecknar alla symmetriska avbildningar $V \times V \to K$ som ett K-vektorrum) dvs visa att varje $(0,2)$-tensor $\xi \in V^* \otimes V^* = \mathrm{Hom}_K(V \otimes V, K) = \mathrm{Bil}(V^2, K)$ kan skrivas entydigt som summa av en symmetrisk och en alternerandetensor.

(b) Visa att $e^i \otimes e^j + e^j \otimes e^i$, med $i \leq j$ bildar en bas för $\mathrm{Sym}_K(V^2, K)$, och $e^i \otimes e^j - e^j \otimes e^i$, $i < j$ en bas för $\mathrm{Ant}_K(V^2, K)$.

Ledning. Arbeta med matrisframställningar av tensorer.

5.15. Låt $e_1, \ldots, e_n$ vara en bas för ett vektorrum V över K och $e^1, \ldots, e^n$ den duala basen för V^*. Låt $\varphi : V \to V$ vara en linjär avbildning och $\varphi^* : V^* \to V^*$ motsvarande linjära avbildning av det duala rummet dvs $\varphi^*(f) = f \circ \varphi$. Bestäm sambandet mellan matriserna för φ och φ^* i baserna $e_1, \ldots, e_n$ och $e^1, \ldots, e^n$.

5.16. Låt $R = \oplus_{i=0}^{\infty} R_i$ vara en graderad ring. Visa att ett ideal I i R är homogent då och endast då I kan genereras av homogena element.

Kapitel 6

BILINJÄRA OCH SESQUILINJÄRA FORMER

Det är ofta viktigt att välja baser för vektorrum så att koordinaterna för en given tensor är okomplicerade. Avsikten är att underlätta beräkningar och att klassificera tensorer av samma typ. Den allmänna klassifikationsuppgiften är vanligen mycket svår. I detta kapitel kommer vi att syssla med bilinjära former (dvs $(0,2)$-tensorer), och i kapitel 8, med linjära avbildningar (dvs $(1,1)$-tensorer). Flera resultat gäller då V är en fri modul med en ändlig bas över en kommutativ ring K, men vi skall förutsätta här att K är en kropp av karakteristiken $\neq 2$[††].

Låt oss påminna om att en K-bilinjär form $T : V \times V \to K$ kallas symmetrisk om $T(x,y) = T(y,x)$ för $x, y \in V$. Den kallas antisymmetrisk då $T(x,y) = -T(y,x)$ för $x, y \in V$ (se (5.8)(b)). Rent allmänt säger man att (V,T) är ett **bilinjärt rum**. Man skriver ofta $T(x,y) = (x,y)$ eller ännu kortare $T(x,y) = xy$.

(6.1) Definition. Låt $e_1, \ldots, e_n$ vara en bas för V över K. **Matrisen för en bilinjär tensor** T m.a.p. basen $e_1, \ldots, e_n$ är matrisen $M_T = [a_{ij}]$, där $a_{ij} = T(e_i, e_j)$. Denna matris är symmetrisk dvs $a_{ij} = a_{ji}$ om T är symmetrisk, och antisymmetrisk dvs $a_{ij} = -a_{ji}$ och $a_{ii} = 0$ om T är antisymmetrisk. Med **rangen** av T menas rangen av M_T. Man säger att (V,T) är **icke–urartat** om $\det M_T \neq 0$.

□

Rangen av en bilinjär tensor T beror inte på valet av basen för V. I själva verket ger ett basbyte $e_{i'} = p^i_{i'} e_i$ i V att

$$a_{i'j'} = p^i_{i'} a_{ij} p^j_{j'}$$

[††]dvs $1 + 1 \neq 0$ i K ($K = \mathbb{Z}_2$ och varje kropp som innehåller denna har karakteristiken 2).

(se (5.4)) dvs matrisen M'_T för T i den nya basen $e_{i'}$ är

$$M'_T = P^t M_T P, \tag{6.2}$$

där $P = [p^i_{i'}]$. Eftersom $\det(P) \neq 0$ så är rangen av M'_T lika med rangen av M_T.

(6.3) Bilinjära polynom. Förutom representationen av bilinjära former med hjälp av matriser betraktar man ofta representationer med hjälp av bilinjära polynom. Om $x = x^i e_i$ och $y = y^i e_i$ är vektorer i V så är

$$T(x, y) = a_{ij} x^i y^j,$$

där $a_{ij} = T(e_i, e_j)$. Polynomet $\sum a_{ij} X_i Y_j \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ kallas bilinjär form, vilket ger upphov till termen "bilinjär form" som namn på bilinjära tensorer $T : V \times V \to K$. $T(x, y)$ är polynomets värde för $X_i = x^i$ och $Y_j = y^j$.

Likheten

$$T(x, y) = \frac{T(x, y) + T(y, x)}{2} + \frac{T(x, y) - T(y, x)}{2} \tag{6.4}$$

visar att varje bilinjär form är en summa av en symmetrisk och en antisymmetrisk form dvs

$$T = T_{sym} + T_{asym},$$

där

$$T_{sym}(x, y) = \frac{1}{2}(T(x, y) + T(y, x)) \quad \text{och} \quad T_{asym}(x, y) = \frac{1}{2}(T(x, y) - T(y, x)).$$

□

Resten av detta kapitel ägnar vi åt symmetriska former. Teorin för antisymmetriska är betydligt enklare. Några viktiga resultat om antisymmetriska former finns i övningarna (se Övn. 3).

(6.5) Kvadratiska avbildningar och former. Man säger att en funktion $q : V \to K$ är kvadratisk om $q(ax) = a^2 q(x)$ för $a \in K$ och $x \in V$ samt $b(x, y) = q(x + y) - q(x) - q(y)$ är en bilinjär funktion på V. Om T är en bilinjär form så är $q(x) = T(x, x)$ ett exempel på en kvadratisk funktion på V. Alla kvadratiska funktioner på V får man på det sättet, ty $q(x) = (1/2)b(x, x)$ (observera dock vikten av förutsättningen att $\mathrm{char}(K) \neq 2$!). Enligt (6.4) kan man alltid förutsätta att i likheten $q(x) = T(x, x)$ är T symmetrisk. Vi har:

$$T(x, y) = \frac{1}{2}(T(x + y, x + y) - T(x, x) - T(y, y)) = \frac{1}{2}(q(x + y) - q(x) - q(y)) \tag{6.6}$$

så att q definierar entydigt T om T är symmetrisk. Ofta betraktar man paret (V, q) (i stället för (V, T)) som kallas **kvadratiskt rum**. Man säger att (V, q) är **icke–urartat** om (V, T)) har denna egenskap (se (6.1)). Vi har:

$$q(x) = a_{ij}x^i x^j$$

då $x = x^i e_i$ och $a_{ij} = T(e_i, e_j)$ för en bas $e_1, \ldots, e_n$ för V. Polynomet

$$q(x_1, \ldots, x_n) = \sum a_{ij} X_i X_j$$

kallas **kvadratisk form**. Det bestämmer entydigt funktionen $q(x)$ ($q(x)$ är värdet av polynomet q då $X_i = x^i$). Matrisen $M_T = [a_{ij}]$ kallas **matrisen för kvadratiska formen** q och betecknas M_q. Två kvadratiska former q_1 och q_2 kallas **ekvivalenta** om de svarar mot två baser för samma V. Detta betyder att deras matriser uppfyller sambandet (6.2). Vi kan skriva:

$$q(X_1, \ldots, X_n) = \mathbf{X}^t M_q \mathbf{X},$$

där $\mathbf{X}^t = (X_1, \ldots, X_n)$. Om q_1 och q_2 är ekvivalenta så är $M_{q_2} = P^t M_{q_1} P$ dvs

$$q_2(X_1, \ldots, X_n) = X^t M_{q_2} X = (P\mathbf{X})^t M_{q_1}(P\mathbf{X}) = q_1(p_1^i X_i, \ldots, p_n^i X_i) \tag{6.7}$$

så att q_1 övergår i q_2 vid variabelsubstitutionen $\mathbf{X} \mapsto P\mathbf{X}$. Teorin för kvadratiska former sysslar med beskrivningen av alla ekvivalensklasser av kvadratiska former över godtyckliga kroppar (och ringar). Den är rik på intressanta och ibland svåra problem. Vi skall beskriva vidare ekvivalensklasserna över $\mathbb{R}$ och $\mathbb{C}$ (se (6.11) och (6.12)). □

(6.8) Definition. Låt (V, T) vara ett symmetriskt bilinjärt rum. Låt $W \subseteq V$ vara en delmängd till V.

$$W^\perp = \{x \in V : T(x, y) = 0 \quad \text{för varje} \quad y \in W\}$$

kallas **ortogonala komplementet** till W i V. $W^\perp$ är ett delrum till V (enkel övning). Två delmängder W_1, W_2 till V kallas ortogonala om $W_1 \subseteq W_2^\perp$. Eftersom T är symmetrisk har vi även $W_2 \subseteq W_1^\perp$, vilket betecknas med $W_1 \perp W_2$ (se också Övn. 1(e)). En bas $e_1, \ldots, e_n$ för V är ortogonal då $T(e_i, e_j) = 0$ för $i \neq j$. Man skriver då $V =< e_1 > \perp \ldots \perp < e_n >$ eller $V =< a_1 > \perp \ldots \perp < a_n >$, där $a_i = a_{ii} = T(e_i, e_i) = q(e_i)$. I stället för $< a_1 > \perp \ldots \perp < a_n >$ skriver man ofta $< a_1, \ldots, a_n >$.

□

(6.9) Sats. *Låt (V,T) vara ett symmetriskt bilinjärt rum och $V \neq (0)$. Då har V en ortogonalbas.*

Bevis. Låt $q(x) = T(x,x)$. Om $q(x) = 0$ för varje $x \in V$ så är påståendet klart ty då är varje bas ortogonal (se (6.6)). Satsen är också sann då $\dim V = 1$. Vi visar satsen induktivt. Antag att $\dim V = n > 1$ och att det finns $x \in V$ med $q(x) \neq 0$. Låt $x_1 = x, x_2, \ldots, x_n$ vara en godtycklig bas för V. Bilda en ny bas:

$$x,\ x_2' = x_2 - \frac{T(x_2,x)}{q(x)}x,\ \ldots,\ x_n' = x_n - \frac{T(x_n,x)}{q(x)}x.$$

Vektorn x är ortogonal till vektorerna $x_2', \ldots, x_n'$ (kontrollera!). Rummet $Kx_2' + \ldots + Kx_n'$ har en ortogonalbas $e_2, \ldots, e_n$ enligt induktionsantagandet ty dess dimension är $n-1$. Alltså är $e_1 = x$, $e_2, \ldots, e_n$ en ortogonalbas för V över K. □

(6.10) Anmärkning. Bevismetoden för (6.9) kallas ofta Schmidts ortogonaliseringsmetod.

□

Om $e_1, \ldots, e_n$ är en ortogonalbas för (V,T) så är

$$q_T(X_1, \ldots, X_n) = a_1X_1^2 + \ldots + a_nX_n^2,$$

där $a_i = q_T(e_i)$ dvs q_T är diagonal. Vi kan välja $a_1 \ldots a_r \neq 0$ och $a_{r+1} = \ldots = a_n = 0$, där r är rangen av (V,T) (eller q_T). Ibland kan man förenkla q_T vidare beroende på egenskaperna hos kroppen K.

(6.11) Kvadratiska former över $\mathbb{C}$. Man kan ersätta en godtycklig ortogonalbas $e_1, \ldots, e_n$ sådan att $q(e_i) = a_i \neq 0$ då $1 \leq i \leq r$ och $q(e_i) = 0$ då $r < i \leq n$ med basen $(1/\sqrt{a_i})e_i$ då $1 \leq i \leq r$ och e_i då $i > r$. I denna bas har vi $q_T(X_1, \ldots, X_n) = X_1^2 + \ldots + X_r^2$. Detta betyder att två kvadratiska former över $\mathbb{C}$ är ekvivalenta då och endast då de har samma rang. Kroppen $\mathbb{C}$ kan ersättas med en godtycklig kropp sådan att $a \in K$ implicerar att $\sqrt{a} \in K$ (K kallas då "kvadratiskt sluten").

(6.12) Kvadratiska former över $\mathbb{R}$. Låt oss ordna vektorerna i en ortogonalbas $e_1, \ldots, e_n$ så att $q(e_i) = a_i > 0$ då $1 \leq i \leq p$, $q(e_i) = a_i < 0$ då $p < i \leq r$ och $q(e_i) = 0$ då $i > r$. Man kan nu välja som bas $(1/\sqrt{a_i})e_i$ då $1 \leq i \leq p$, $(1/\sqrt{-a_i})e_i$ då $p < i \leq r$ och e_i då $i > r$. I denna bas (som kallas ortonormerad i fall $n = r$) har vi:

$$q_T(X_1, \ldots, X_n) = X_1^2 + \ldots + X_p^2 - X_{p+1}^2 - \ldots - X_{p+m}^2,$$

där $p + m = r$. Vi visar om en stund att talen p och $r = p + m$ klassificerar alla kvadratiska former över $\mathbb{R}$. Mycket ofta betraktar man rangen $r = p + m$ och $s = p - m$ som kallas **formens signatur**.

(6.13) Tröghetssatsen. *Två kvadratiska former över $\mathbb{R}$ är ekvivalenta då och endast då de har samma rang och samma signatur.*

Bevis. Låt (V, T) vara ett bilinjärt rum över $\mathbb{R}$. Som vi redan vet kan man betrakta två former som svarar mot två ortogonalbaser $e_1, \ldots, e_n$ och $e'_1, \ldots e'_n$ för V:

$$X_1^2 + \ldots + X_p^2 - X_{p+1}^2 - \ldots - X_r^2 \quad \text{och} \quad X_1^2 + \ldots + X_q^2 - X_{q+1}^2 - \ldots - X_{r'}^2$$

och visa att dessa är ekvivalenta över $\mathbb{R}$ då och endast då $r = r'$ och $p = q$. Det är klart att dessa likheter ger ekvivalenta (t o m identiska) former. Det är också klart att ekvivalensen av två kvadratiska former medför att de har samma rang dvs $r' = r$ (se (6.2)). Därför måste man visa att ekvivalensen ger $p = q$. Låt

$$V^+ = \mathbb{R}e_1 + \ldots + \mathbb{R}e_p \quad \text{och} \quad V^- = \mathbb{R}e'_{q+1} + \ldots + \mathbb{R}e'_n.$$

Om $x \in V^+$, $x \neq 0$, så har vi

$$q_T(x) = (x^1)^2 + \ldots + (x^p)^2 > 0,$$

där $q_T(x) = T(x, x)$ och $x = x^i e_i$. Om $x \in V^-$, $x \neq 0$, så har vi

$$q_T(x) = -(x^{q+1})^2 - \ldots - (x^r)^2 < 0,$$

där $q_T(x) = T(x, x)$ och $x = x^i e'_i$. Alltså är $V^+ \cap V^- = (0)$ så att

$$\dim V^+ + \dim V^- \leq n.$$

Med andra ord, $p + (n - q) \leq n$ dvs $p \leq q$. Av symmetriskäl är $q \leq p$ dvs $p = q$. □

(6.14) Definition. Låt $T : V \times V \to K$ vara en bilinjär form. Man säger att en K-automorfism $\varphi : V \to V$ är en automorfism av T om $T(\varphi(x), \varphi(y)) = T(x, y)$ då $x, y \in V$. Alla automorfismer av T bildar en grupp som betecknas med $\mathrm{Aut}(T)$. Om T är symmetrisk kallas ofta $\mathrm{Aut}(T)$ för **ortogonala gruppen** av (V, T) och betecknas $O(V)$ (eller $O_n(V)$). Dess element kallas ofta för **isometrier** av (V, T). Om M_T är matrisen av T m.a.p. en bas för V så kan man beskriva $O_n(V)$ som gruppen av alla $(n \times n)$-matriser $A \in GL_n(K)$ sådana att

$$A^t M_T A = M_T$$

(se (6.2)). Om $\det M_T \neq 0$ (dvs rangen av T är n) så är $(\det A)^2 = 1$ dvs $\det A = \pm 1$. Alla automorfismer φ med $\det \varphi = 1$ (dvs matriser A ovan med $\det A = 1$) bildar en normal delgrupp $SO_n(V)$ till $O_n(V)$ – **speciella ortogonala gruppen**. Om T är antisymmetrisk kallas $\mathrm{Aut}(T)$ för **symplektiska gruppen**[††].

□

(6.15) Exempel. Låt $K = \mathbb{R}$ och $V =< 1, \ldots, 1, -1, \ldots, -1 >$ med p stycken 1, q stycken -1 och $p+q = n$. Gruppen $O_n(V)$ betecknas ofta med $O(p, q)$. Om $p = n$, $q = 0$ skriver man $O(n)$. Den sista gruppen består alltså av alla matriser $A \in GL_n(\mathbb{R})$ sådana att $A^t A = E_n$ (enhetsmatrisen), och $SO(n)$ av alla A av den typen med $\det A = 1$. Helt allmänt $A \in O(p, q)$ om

$$A^t \begin{bmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{bmatrix} A = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{bmatrix},$$

där p är antalet 1 och q är antalet -1. Låt

$$A = \left[\begin{array}{c|c} B_1 & C_1 \\ \hline C_2 & B_2 \end{array}\right],$$

där B_1 är $(p \times p)$ och B_2 är $(q \times q)$. Man kan visa att $\det B_1 \neq 0$ och $\det B_2 \neq 0$ (se Övn. 8) och att det finns en grupphomomorfism:

[††]Terminologin är inte lämplig. Termen symplektisk har två olika betydelser – se (6.22).

$$\theta : O(p,q) \to U_2 \times U_2,$$

där $U_2 = \{1, -1\}$, och

$$\theta(A) = (\frac{\det B_1}{|\det B_1|}, \frac{\det B_2}{|\det B_2|}).$$

(Det sista påståendet är inte lätt att bevisa. Ett rent algebraiskt bevis kunde vara av intresse – se Övn. 8). Låt $O^{\epsilon}_{\eta}(p,q)$ vara inversa bilden av paret $(\epsilon, \eta) \in U_2 \times U_2$. $\epsilon = +1$ respektive -1 betecknas ofta med $\uparrow$ respektive $\downarrow$, $\eta = +1$ respektive -1 med $+$ respektive $-$. T ex är $\operatorname{Ker}\theta = O^{\uparrow}_{+}(p,q)$ inversa bilden av $(1,1)$. Gruppen $U_2 \times U_2$ har 4 äkta delgrupper: $\{(1,1)\}$, $\{(1,1),(1,-1)\}$, $\{(1,1),(-1,1)\}$ och $\{(1,1), (-1,-1)\}$. Inversa bilder av dessa 4 delgrupper är normala delgruper till $O(p,q)$:

$$O^{\uparrow}_{+}(p,q),\ \ O^{\uparrow}_{+}(p,q) \cup O^{\uparrow}_{-}(p,q),\ \ O^{\uparrow}_{+}(p,q) \cup O^{\downarrow}_{+}(p,q),\ \ O^{\uparrow}_{+}(p,q) \cup O^{\downarrow}_{-}(p,q).$$

Fallet $p = 1$, $q = 3$ har en mycket stor fysikalisk betydelse och alla dessa grupper bär H. A. Lorentz namn (med olika adjektiv). Att relatera dessa grupper till andra grupper som har en bättre matematisk beskrivning (linjära, ortogonala, unitära) är en viktig uppgift. För att undersöka några samband kommer vi i nästa kapitel att introducera Cliffordalgebror. Dessa algebror är av stort intresse även i många andra sammanhang (t ex i teorin för kvadratiska former).

□

I resten av detta kapitel kommer vi att uteslutande syssla med vektorrum över $\mathbb{R}$ och $\mathbb{C}$ (se dock anmärkning (6.22)(c)).

(6.16) Definition. Låt V vara ett vektorrum över $\mathbb{C}$. Man säger att $f : V \to V$ är en **halvlinjär avbildning** om $f(x_1 + x_2) = f(x_1) + f(x_2)$ och $f(ax) = \bar{a}f(x)$ då $x, x_1, x_2 \in V$ och $a \in \mathbb{C}$. En funktion $T : V \times V \to \mathbb{C}$ kallas **sesquilinjär form** (eller $1\frac{1}{2}$**-linjär**) om T är linjär m.a.p. första variabeln och halvlinjär m.a.p. andra dvs

$$T(x_1 + x_2, y) = T(x_1, y) + T(x_2, y),\ \ T(x, y_1 + y_2) = T(x, y_1) + T(x, y_2),$$

$$T(ax, y) = aT(x, y),\ \ T(x, ay) = \bar{a}T(x, y).$$

Man säger att T är **hermitsk** om $T(y,x) = \overline{T(x,y)}$ (då är $T(x,x)$ reellt).

□

(6.17) Exempel. (a) Låt $V = \mathbb{C}^n$. Om $\mathbf{x} \in V$ så är $\mathbf{x} = \boldsymbol{x}_1 + i\boldsymbol{x}_2$ där $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{R}^n$. Låt $\bar{\boldsymbol{x}} = \boldsymbol{x}_1 - i\boldsymbol{x}_2$. Funktionen $f : \mathbb{C}^n \to \mathbb{C}^n$ där $f(\boldsymbol{x}) = \bar{\boldsymbol{x}}$ är halvlinjär.

(b) Låt V vara ett godtyckligt linjärt rum över $\mathbb{C}$ och låt $\bar{V}$ bestå av exakt samma vektorer som V. Definiera $a \circ \boldsymbol{x} = \bar{a}\boldsymbol{x}$ då $a \in \mathbb{C}$ och $\boldsymbol{x} \in \bar{V}$. $\bar{V}$ är ett vektorrum över $\mathbb{C}$ och $f : V \to \bar{V}$ där $f(\boldsymbol{x}) = \boldsymbol{x}$ är halvlinjär ty $f(\boldsymbol{x}_1 + \boldsymbol{x}_2) = f(\boldsymbol{x}_1) + f(\boldsymbol{x}_2)$ och $f(a\boldsymbol{x}) = a\boldsymbol{x} = \bar{a} \circ \boldsymbol{x} = \bar{a} \circ f(\boldsymbol{x})$[††].

(c) Låt $T : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$, där $T(\boldsymbol{x}, \boldsymbol{y}) = x_1\bar{y}_1 + x_2\bar{y}_2 + \ldots + x_n\bar{y}_n$ för $\boldsymbol{x} = (x_1, \ldots, x_n)$ och $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{C}^n$. Då är T en hermitsk form.

□

(6.18) Matrisen för en sesquilinjär form. Låt $T : V \times V \to \mathbb{C}$ vara sesquilinjär och låt $e_1, \ldots, e_n$ vara en bas för V över $\mathbb{C}$. Om $\boldsymbol{x} = x^i e_i$ och $\boldsymbol{y} = y^j e_j$ så är

$$T(\boldsymbol{x}, \boldsymbol{y}) = T(e_i, e_j) x^i \bar{y}^j.$$

Matrisen $M_T = [a_{ij}]$, där $a_{ij} = T(e_i, e_j)$ är matrisen för T m.a.p. basen $e_1, \ldots, e_n$. Vi har:

$$T(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^t M_T \bar{\boldsymbol{y}}.$$

Om $(e_{i'})$ är en ny bas för V och $e_{i'} = p^i_{i'} e_i$ så är

$$M'_T = P^t M_T \bar{P}, \tag{6.19}$$

där $P = [p^i_{i'}]$. T är hermitsk då och endast då $T(e_i, e_j) = \overline{T(e_j, e_i)}$. Matriser $A = [a_{ij}]$ med egenskapen $a_{ij} = \bar{a}_{ji}$ kallas **hermitska** (dvs $\bar{A}^t = A$). □

(6.20) Sats. *Låt $T : V \times V \to \mathbb{C}$ vara en hermitsk form. Då existerar en bas $e_1, \ldots, e_n$ för V som är ortogonal m.a.p. T dvs $T(e_i, e_j) = 0$ då $i \neq j$. Man kan välja basen så att $T(e_i, e_j) \in \{0, \pm 1\}$.*

[††]Se vidare Övning 6 i samband med "blandade tensorer".

Bevis. Man konstaterar först att $T(x,x) = 0$ för varje $x \in V$ ger $T(x,y) = 0$ för varje $x, y \in V$ (observera att likheten (6.6) inte kan utnyttjas). Vi har nämligen:

$$\begin{aligned} T(x+y, x+y) &= T(x,x) + T(x,y) + T(y,x) + T(y,y) = 0, \\ T(x+iy, x+iy) &= T(x,x) - iT(x,y) + iT(y,x) + T(y,y) = 0, \end{aligned}$$

och $T(x,x) = T(y,y) = 0$. Alltså är

$$\begin{cases} T(x,y) + T(y,x) = 0, \\ T(x,y) - T(y,x) = 0, \end{cases}$$

vilket ger $T(x,y) = T(y,x) = 0$.

Beviset att en ortogonalbas existerar är nu exakt samma som beviset av existensen av ortogonalbaser för symmetriska bilinjära former (se (6.9)). Antag nu att $e_1, \ldots, e_n$ är en ortogonalbas och $T(e_i, e_i) = a_i \in \mathbb{R}$. Vi kan ersätta e_i med $(1/\sqrt{a_i})e_i$ om $a_i > 0$ och med $(1/\sqrt{-a_i})e_i$ om $a_i < 0$. Då får vi en bas med $T(e_i, e_i) \in \{0, \pm 1\}$. Matrisen M_T för T i denna bas vid lämplig numerering av basvektorerna är

$$\begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & 0 & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & 0 & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

dvs

$$T(\boldsymbol{x}, \boldsymbol{y}) = x^1\bar{y}^1 + \ldots + x^p\bar{y}^p - x^{p+1}\bar{y}^{p+1} - \ldots - x^{p+q}\bar{y}^{p+q}.$$

□

(6.21) Definition. Låt V vara ett vektorrum över $\mathbb{R}$ och $T : V \times V \to \mathbb{R}$ en bilinjär form. Man säger att (V,T) är ett **euklidiskt** rum om T är symmetrisk och positivt definit dvs $T(x,x) > 0$ då $x \in V$, $x \neq 0$. Låt V vara ett vektorrum över $\mathbb{C}$ och $T : V \times V \to \mathbb{C}$ en sesquilinjär form. Man säger att (V,T) är ett **unitärt** rum om T är hermitsk och positivt definit dvs $T(x,x) > 0$ då $x \in V$, $x \neq 0$.

Automorfismgruppen $\mathrm{Aut}(V,T)$ då (V,T) är unitärt kallas **unitära gruppen** och betecknas $U(n)$. Om $f : V \to V$ är en automorfism av T (dvs $T(f(x), f(y)) = T(x,y)$) och A dess

matris m.a.p. en ortogonal bas för V så är $\bar{A}^t A = E$ (se (6.19)). Sådana matriser kallas **unitära**. Vi har $\det(\bar{A}^t A) = 1$ så att $|\det A| = 1$. Matriserna $A \in U(n)$ med $\det A = 1$ bildar en delgrupp till $U(n)$ som betecknas med $SU(n)$ och kallas **speciella unitära gruppen.**

□

(6.22) Anmärkning. (a) Ibland använder man termerna reell-unitär och komplex-unitär i stället för ortogonal och unitär samt beteckningarna $U_n(\mathbb{R})$ och $U_n(\mathbb{C})$ i stället för $O(n), U(n)$. Orsaken är att det finns motsvarande grupper över kvaternionalgebran $\mathbb{H}$ (se Övn. 9). Visserligen kallas dessa grupper **symplektiska**, men det finns andra grupper – automorfismgrupper av antisymmetriska former som också kallas symplektiska (och betecknas $Sp(n)$ – se Övn. 3). Dessutom är termen "ortogonal" inte särskilt relevant (se S. Langs kommentarer i "Algebra").

(b) Man kan definiera grupperna $U(p, q)$ precis som $O(p, q)$ (se (6.15)).

(c) Man kan betrakta sesquilinjära former om man har en kropp (eller ring) med involution dvs en funktion $\delta : K \to K$ sådan att $\delta(a) = \bar{a}$, där $\overline{a + b} = \bar{a} + \bar{b}$, $\overline{ab} = \bar{a}\bar{b}$ (eller $\bar{b}\bar{a}$) och $\bar{\bar{a}} = a$. Då kallas $T : V \times V \to K$, V en K-modul, sesquilinjär om T är linjär m.a.p. första variabeln och halvlinjär m.a.p. andra (dvs $T(ax, by) = aT(x, y)\bar{b}$). Allmän teori i den situationen är ganska fragmentarisk (se t ex W. Scharlau, Quadratic and Hermitian Forms, Springer, 1985, Kap. 7). Viktigaste fallet i praktiska sammanhang är $K = \mathbb{H}$ (förutom $K = \mathbb{C}$).

□

ÖVNINGAR

Alla vektorrum i övningarna nedan har ändlig dimension.

6.1. Låt $T : V \times V \to K$ vara en bilinjär form sådan att $T(x,y) = 0 \Leftrightarrow T(y,x) = 0$ (vi kommer att kalla en sådan form **svagt symmetrisk**). Man säger att (V,T) är **icke-urartat** (eller **reguljärt**) om

$$\mathrm{Ker}V := \{x \in V : T(x,V) = 0\} = \{0\}$$

($T(x,V) = 0$ betyder att $T(x,y) = 0$ för varje $y \in V$).

(a) Visa att (V,T) är icke-urartat då och endast då $\Phi : V \to V^*$ där $\Phi(v)(x) = T(v,x)$ är en isomorfism (eller $\Psi(v)(x) = T(x,v)$ är en isomorfism).

(b) Visa att (V,T) är reguljärt då och endast då $\det M_T \neq 0$ (M_T definieras i (6.1)).

(c) Visa att $V = \mathrm{Ker}V \perp V_1$, där (V_1,T) är icke-urartat (om $W \subseteq V$ är ett delrum så skriver vi (W,T), där T egentligen är restriktionen av T till W; man skriver $V = W_1 \perp W_2$ om W_1 och W_2 är delrum till V ortogonala till varandra, $V = W_1 + W_2$ och $W_1 \cap W_2 = \{0\}$ – se också (6.8)).

(d) Låt $U \subseteq V$ vara ett delrum till V och $U^\perp = \{x \in V : T(x,U) = 0\}$. Visa att om (U,T) eller (V,T) är icke-urartat så är $V/U^\perp \cong U$. Motivera att $\dim V = \dim U + \dim U^\perp$.

Ledning. Betrakta $\Phi : V \to U^*$ ur (a).

(e) Låt (U,T) vara ett icke-urartat delrum till (V,T). Visa att $V = U \perp U^\perp$.

(f) Visa att $U_1 \subseteq U_2 \subseteq V$ implicerar att $U_1^\perp \supseteq U_2^\perp$. Visa också att om (V,T) är icke-urartat så är $U^{\perp\perp} = U$.

6.2. Hyperboliska plan och rum. Låt $T : V \times V \to K$ vara en svagt symmetrisk bilinjär form (se Övn. 1). Man säger att $H \subseteq V$ är ett **hyperboliskt plan** om (H,T) är icke-urartat, $\dim_K H = 2$ och det finns $v \in H$, $v \neq 0$ och $T(v,v) = 0$. Visa att om T är symmetrisk eller antisymmetrisk så finns det en bas e_1, e_2 för H sådan att $T(e_1,e_1) = T(e_2,e_2) = 0$ och $T(e_1,e_2) = 1$.

Anmärkning. (V,T) kallas **hyperboliskt** rum om $V = H_1 \perp \ldots \perp H_k$, där H_i är hyperboliska plan ($T(x,y) = 0$ då $x \in H_i$, $y \in H_j$ för $i \neq j$).

6.3. Visa att om (V,T) är antisymmetriskt så är $V = \mathrm{Ker}V \perp V_1$, där V_1 är ett hyperboliskt rum.

Ledning. Utnyttja 1(b). Därefter visa att V_1 innehåller ett hyperboliskt plan – se Övn. 2 och konstatera att $V_1 = H \perp H^\perp$ med hjälp av 1(d). Därefter induktion m.a.p. $\dim V_1$.

Anmärkning. Om V är icke-urartat så existerar en bas $e_1, e_2, e_3, e_4, \ldots, e_{2n-1}, e_{2n}$ för

V över K sådan att M_T har i denna bas matrisen

$$\begin{bmatrix} 0 & 1 & & & & \\ -1 & 0 & & & 0 & \\ & & 0 & 1 & & \\ & & -1 & 0 & & \\ & & & \ddots & & \\ & 0 & & & 0 & 1 \\ & & & & -1 & 0 \end{bmatrix},$$

ty hyperboliska plan har matriser $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ (se Övn. 2). Ofta ordnar man basvektorerna så att matrisen har formen

$$\begin{bmatrix} 0 & E_k \\ -E_k & 0 \end{bmatrix},$$

där E_k är $(k \times k)$-enhetsmatrisen (dvs man ordnar: $e_1, e_3, \ldots, e_{2n-1}, e_2, e_4, \ldots, e_{2n}$). Om $\boldsymbol{x} = x^i e_i$ och $\boldsymbol{y} = y^i e_i$ så är

$$T(\boldsymbol{x}, \boldsymbol{y}) = (x^1 y^2 - x^2 y^1) + (x^3 y^4 - x^4 y^3) + \ldots + (x^{2n-1} y^{2n} - x^{2n} y^{2n-1}).$$

Automorfismgrupper av icke-urartade antisymmetriska rum (V, T) kallas **symplektiska grupper**. Om $\dim_K(V) = 2n$, så betecknas gruppen med $Sp_{2n}(K)$ (se (6.22) och Övn. 9 angående terminologin).

6.4. Låt $T : V \times V \to K$ vara sesquilinjär ($K = \mathbb{C}$, men se (6.22)(c)). Visa att $\Phi : V \to V^*$, där $\Phi(v)(x) = T(x, v)$ är en halvlinjär avbildning (V^* duala rummet till V), och $\Psi : V \to V'$, där $\Psi(v)(x) = T(v, x)$ är en linjär avbildning från V till det linjära rummet V' av alla halvlinjära funktionaler på V. Visa att om T är svagt-symmetrisk (dvs $T(x, y) = 0 \Leftrightarrow T(y, x) = 0$ – se Övn. 1) och icke-urartad (dvs $\{x \in V : T(x, V) = 0\} = (0)$ – se Övn. 1), så är Φ och Ψ isomorfismer.

6.5. Låt $T : V \times V \to K$ vara svagt-symmetrisk och icke-urartad (se Övn. 1 och 4) bilinjär eller sesquilinjär och låt $f : V \to V$ vara en linjär avbildning.

(a) Visa att det finns en entydigt bestämd linjär avbildning $g : V \to V$ sådan att $T(f(x), y) = T(x, g(y))$ för varje $x, y \in V$.

Anmärkning. g kallas **adjungerad** till f. Man säger att f är T-symmetrisk om $g = f$. Om f är T–symmetrisk och (V, T) är euklidiskt så kallas f **symmetrisk**, och om (V, T) är unitärt kallas f **hermitsk**.

(b) Låt (V, T) vara euklidiskt. Visa att $f : V \to V$ är symmetrisk $\Leftrightarrow$ M_f är symmetrisk i varje ortonormal bas för V (dvs $M_f^t = M_f$).

(c) Låt (V, T) vara unitärt. Visa att $f : V \to V$ är hermitsk $\Leftrightarrow$ M_f är hermitsk i varje ortonormal bas för V (dvs $\bar{M}_f^t = M_f$).

6.6. Låt V vara ett vektorrum över $\mathbb{C}$. Med en generaliserad tensor av typen $(k, \bar{k}, l, \bar{l})$ över V menas en funktion:

$$T : V^k \times V^{\bar{k}} \times V^{*l} \times V^{*\bar{l}} \to \mathbb{C}$$

som är linjär med avseende på de första k variablerna ur V och de första l variablerna ur V^* och halvlinjär med avseende på de övriga variablerna. Låt $e_1, \dots, e_n$ vara en bas för V över $\mathbb{C}$ och $e^1, \dots e^n$ den duala basen för V^*. Koordinaterna för T m.a.p. dessa baser definieras på samma sätt som för vanliga tensorer (se (5.5)(b)) och betecknas:

$$a^{j_1 \dots j_l \bar{j}_{l+1} \dots \bar{j}_{l+\bar{l}}}_{i_1 \dots i_k \bar{i}_{k+1} \dots \bar{i}_{k+\bar{k}}}.$$

Låt $V' = \{f : V \to \mathbb{C},\ f \text{ halvlinjär}\}$ och låt $\bar{V}$ vara det konjugerade rummet till V (se (6.17) (b): $V = \bar{V}$ som abelska grupper, men $a \circ v = \bar{a}v$ då $a \in \mathbb{C}$, $v \in V$). Visa att $f : \bar{V} \to \mathbb{C}$ är linjär då $f \in V'$. Motivera att en generaliserad tensor T kan betraktas som multilinjär funktion:

$$T : V^k \times \bar{V}^{\bar{k}} \times V^{*l} \times \bar{V}^{*\bar{l}} \to \mathbb{C}.$$

6.7. Låt V vara ett vektorrum över en kropp K och låt T vara en tensor över V av typen $(1,0)$ eller $(0,1)$. Bestäm "kanoniska" former för T (i likhet med ortogonala baser för symmetriska eller hermitska former).

6.8. (a) Låt $A \in O(p,q)$ (se (6.15)) och

$$A = \left[\begin{array}{c|c} B_1 & C_1 \\ \hline C_2 & B_2 \end{array}\right],$$

(se (6.15)). Visa att $\det B_1 \cdot \det B_2 \neq 0$.

(b) Visa att $\theta : O(1,3) \to U_2 \times U_2$, där

$$\theta(A) = \left(\frac{\det B_1}{|\det B_1|}, \frac{\det B_2}{|\det B_2|}\right)$$

är en homomorfism (se (6.15)).

6.9. Låt $\mathbb{H}$ vara kvaternionalgebran över $\mathbb{R}$ dvs

$$\mathbb{H} = \left\{ \left[\begin{array}{cc} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{array}\right], z_1, z_2 \in \mathbb{C} \quad \right\}$$

med matrisaddition och matrismultiplikation. Visa att $\theta(x) = \bar{x}$, där

$$\bar{x} = \left[\begin{array}{cc} \bar{z}_1 & -z_2 \\ \bar{z}_2 & z_1 \end{array}\right]$$

är en antiinvolution av $\mathbb{H}$ (dvs $\overline{x+y} = \bar{x} + \bar{y}$, $\overline{xy} = \bar{y}\bar{x}$ och $\bar{\bar{x}} = x$).

Anmärkning. Låt $V = \mathbb{H}^n$ och $T : V \times V \to \mathbb{H}$ där $T(\boldsymbol{x}, \boldsymbol{y}) = \sum x_i \bar{y}_i$. Gruppen av alla automorfismer av T dvs $\varphi : V \to V$ sådana att $T(\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})) = T(\boldsymbol{x}, \boldsymbol{y})$ kallas **symplektiska gruppen** och betecknas ofta $Sp(n)$. Det vore bättre att skriva $U_n(\mathbb{H})$ och kalla gruppen för kvaternion-unitära (se t ex kommentaren i S. Langs bok "Algebra", (6.22) och Övn. 3).

6.10. (a) Låt $T : V \times V \to \mathbb{C}$ vara sesquilinjär. Visa att om $T(y,x) = -T(x,y)$ så är $T(x,y) = 0$ för varje $x, y \in V$.

Ledning. Utnyttja beviset för (6.20).

(b) Låt $T : V \times V \to \mathbb{C}$ vara sesquilinär. Visa att om $T(y,x) = -\overline{T(x,y)}$ så är $iT(x,y)$ hermitsk.

Anmärkning. (a) och (b) visar att begreppet "antihermitsk" enkelt kan relateras till "hermitsk".

6.11. Visa att

$$U(2) = \{\begin{bmatrix} z_1 & z_2 \\ -\lambda\bar{z}_2 & \lambda\bar{z}_1 \end{bmatrix} : z_1, z_2, \lambda \in \mathbb{C}, \quad |z_1|^2 + |z_2|^2 = 1, \quad |\lambda| = 1\},$$

och

$$SU(2) = \{\begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix} : z_1, z_2 \in \mathbb{C}, \quad |z_1|^2 + |z_2|^2 = 1\}.$$

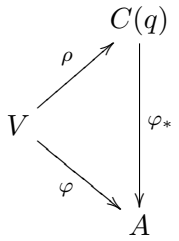
6.12. Visa att varje ändlig uppsättning av parvis ortogonala vektorer i ett vektorrum med en symmetrisk bilinjär form är linjärt oberoende.

Kapitel 7

CLIFFORDALGEBROR

Varje kvadratiskt rum (V, q) definierar på ett naturligt sätt en algebra som innehåller V och sådan att $x^2 = q(x)$ då $x \in V$. Denna algebra, som först konstruerades av William Clifford (1845 – 1879), spelar en mycket viktig roll i teorin för kvadratiska former. Men man möter också Cliffordalgebror i analys, topologi och det finns flera exempel på deras tillämpningar i fysik. Dessa tillämpningar baseras på det faktum att enheterna i Cliffordalgebran av ett kvadratiskt rum (V, q) kan relateras till isometrigruppen av rummet. På detta sätt kan man utnyttja rik algebrastruktur för att studera isometrigrupper av kvadratiska rum. I detta kapitel diskuteras Cliffordalgebror och deras tillämpningar på klassiska isometrigrupper (bl a ortogonala, unitära, spinorgrupper osv).

(7.1) Definition. Låt (V, q) vara ett kvadratiskt rum över en kropp K. Med en **Cliffordalgebra** av (V, q) menar man en K-algebra $C(q)$ sådan att det finns en injektiv linjär avbildning $\rho : V \to C(q)$ med $\rho(v)^2 = q(v) \cdot 1$, där 1 är ettan i $C(q)$, och följande villkor är uppfyllt: Om $\varphi : V \to A$ är en K-linjär avbildning av V i en K-algebra A sådan att $\varphi(v)^2 = q(v) \cdot 1_A$ så existerar exakt en algebrahomomorfism $\varphi_* : C(q) \to A$ sådan att diagrammet:



kommuterar.

□

Det är klart att om $C(q)$ existerar så är den entydigt bestämd så när som på en K-isomorfism ("abstract nonsense"). För att förenkla beteckningarna kommer vi att identifiera $v \in V$ med dess bild $\rho(v)$ i $C(q)$ (dvs vi kommer att skriva v i stället för $\rho(v)$). Låt oss påminna om att

$$b(x, y) = q(x + y) - q(x) - q(y)$$

är en bilinjär form på V.

(7.2) Sats. *Låt (V, q) vara ett kvadratiskt rum och $\dim_K V = n$. Då existerar $C(q)$ och $\dim_K C(q) = 2^n$. $C(q)$ har som bas över K:*

$$1 \quad \textit{och} \quad e_{i_1} \dots e_{i_k},$$

där $1 \le i_1 < \ldots < i_k \le n$ då $e_1, \ldots, e_n$ är en ortogonalbas[††] för (V, b). Om $q(e_i) = a_i$, så är $e_i^2 = a_i$ och $e_i e_j = -e_j e_i$ då $i \neq j$.

Bevis. Låt $\varphi : V \to A$ uppfylla $\bar{x}^2 = q(x)$, där $\bar{x} = \varphi(x)$ (vi utelämnar 1_A i $q(x) \cdot 1_A$). Då är

$$\bar{x}\bar{y} + \bar{y}\bar{x} = b(x, y),$$

för $x, y \in V$. Vi har nämligen:

$$q(x + y) = q(x) + b(x, y) + q(y) = \bar{x}^2 + b(x, y) + \bar{y}^2$$

och

$$q(x + y) = (\overline{x + y})^2 = (\bar{x} + \bar{y})^2 = \bar{x}^2 + \bar{x}\bar{y} + \bar{y}\bar{x} + \bar{y}^2.$$

Låt nu $e_1, \ldots, e_n$ vara en ortogonalbas för (V, b) över K med $q(e_i) = a_i$. Då är

$$\bar{e}_i^2 = q(e_i) = a_i \quad \text{och} \quad \bar{e}_i\bar{e}_j + \bar{e}_j\bar{e}_i = b(e_i, e_j) = 0 \quad \text{då} \quad i \neq j.$$

Detta betyder att varje produkt $\bar{e}_{i_1} \dots \bar{e}_{i_k}$ kan skrivas om till en produkt med $1 \le i_1 < \ldots < i_k \le n$ följd av en lämplig koefficient ur K (genom en upprepad användning av $\bar{e}_i^2 = a_i$

[††]Man kan visa att dessa element bildar en bas för $C(q)$ för en helt godtycklig bas för V – ej nödvändigt ortogonal. Förutsättningen att basen för V är ortogonal ger enkla beräkningsregler för basen i $C(q)$.

och $\bar{e}_j\bar{e}_i = -\bar{e}_i\bar{e}_j$). Låt $I = \{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ och låt $e_I = \bar{e}_{i_1} \ldots \bar{e}_{i_k}$. Genom en upprepad användning av $\bar{e}_i^2 = a_i$ och $\bar{e}_j\bar{e}_i = -\bar{e}_i\bar{e}_j$ får vi också att:

$$e_I e_J = \beta(I, J) \prod_{k \in I \cap J} a_k e_{I \div J}, \tag{7.3}$$

där $\beta(I, J) = \prod(i, j)$ med $i \in I$, $j \in J$ och

$$(i, j) = \begin{cases} 1 & \text{om} \quad i \leq j, \\ -1 & \text{om} \quad i > j, \end{cases}$$

samt $I \div J = (I \cup J) - (I \cap J)$[††]. Vi antar dessutom att $\beta(\emptyset, J) = \beta(I, \emptyset) = 1$. Observera att

$$\beta(I_1 \div I_2, J) = \beta(I_1, J)\beta(I_2, J) \quad \text{och} \quad \beta(I, J_1 \div J_2) = \beta(I, J_1)\beta(I, J_2). \tag{7.4}$$

Nu kan vi definiera $C(q)$. Först låt $C(q)$ vara ett vektorrum med 2^n basvektorer e_I för $I \subseteq \{1, 2, \ldots, n\}$ (dvs $C(q)$ är en fri K-modul med 2^n basvektorer). Därefter förvandlar vi $C(q)$ till en K-algebra genom att definiera produkt av två godtyckliga element ur $C(q)$ (se (7.3)):

$$\sum x_I e_I \cdot \sum y_J e_J = \sum x_I y_J \beta(I, J) \prod_{k \in I \cap J} a_k e_{I \div J},$$

där $x_I, y_J \in K$. På det sättet får vi en K-algebra. Den har som etta $e_\emptyset$ ty

$$e_\emptyset e_I = \beta(\emptyset, I) e_{\emptyset \div I} = e_I = e_I e_\emptyset.$$

Vi identifierar $e_1, \ldots, e_n$ med $e_{\{1\}}, \ldots, e_{\{n\}}$ och på det sättet får vi $V \subset C(q)$. Vi har

$$e_i^2 = e_i e_i = \beta(\{i\}, \{i\}) a_i e_{\{i\} \div \{i\}} = a_i$$

och

[††] $I \div J$ kallas symmetriska differensen av I och J. Alla delmängder till en given mängd X bildar en (kommutativ och associativ) ring (Boolesk ring) om man tar $A \div B$ som addition och $A \cap B$ som multiplikation. Neutrala elementet för addition är $\emptyset$. Observera att $A \div A = \emptyset$.

$$e_j e_i + e_i e_j = \beta(\{j\},\{i\})e_{\{j\}\div\{i\}} + \beta(\{i\},\{j\})e_{\{i\}\div\{j\}} = 0$$

då $i \neq j$. Alltså är $e_i^2 = a_i$ (vi skriver $e_\emptyset = 1$ och identifierar $a \in K$ med $a\cdot 1$ så att $K \subseteq C(q)$), och $e_j e_i = -e_i e_j$. Om $x = \sum x_i e_i \in V$ så är

$$x^2 = (x_1e_1 + \ldots + x_ne_n)^2 = x_1^2e_1^2 + \ldots + x_n^2e_n^2 + \sum x_ix_j(e_ie_j + e_je_i) = a_1x_1^2 + \ldots + a_nx_n^2,$$

dvs $x^2 = q(x)$. Slutligen kontrollerar vi att algebran $C(q)$ är associativ:

$$(e_Ie_J)e_K = \beta(I,J)\prod_{r\in I\cap J} a_r e_{I\div J}e_K = \beta(I,J)\beta(I\div J,K)\prod_{r\in I\cap J} a_r \prod_{r\in(I\div J)\cap K} a_r e_{(I\div J)\div K}$$

och

$$e_I(e_Je_K) = e_I\beta(J,K)\prod_{r\in J\cap K} a_r e_{J\div K} = \beta(J,K)\beta(I,J\div K)\prod_{r\in J\cap K} a_r \prod_{r\in I\cap(J\div K)} a_r e_{I\div(J\div K)}.$$

Men $(I\div J)\div K = I\div(J\div K)$, $\beta(I,J)\beta(I\div J,K) = \beta(J,K)\beta(I,J\div K)$ (se (7.4)) och

$$\prod_{r\in I\cap J} a_r \prod_{r\in(I\div J)\cap K} a_r = \prod_{r\in J\cap K} a_r \prod_{r\in I\cap(J\div K)} a_r$$

ty bägge är lika med $\prod_r a_r$, där $r \in (I\cap J)\cup(I\cap K)\cup(J\cap K)$.

Om nu $\varphi : V \to A$ är K-linjär och $\varphi(x)^2 = q(x)$ då $x \in V$ så kan man definiera $\varphi_* : C(q) \to A$ så att $\varphi_*(e_I) = \varphi(e_{i_1})\ldots\varphi(e_{i_r})$, där $I = \{i_1,\ldots,i_r\}$. Men formeln (7.3) gäller i A så att φ_* är en algebrahomomorfism (det räcker att kontrollera likheten $\varphi_*(e_Ie_J) = \varphi_*(e_I)\varphi_*(e_J)$ för basvektorerna och denna likhet är självklar). Å andra sidan, om man har en algebrahomomorfism $\psi : C(q) \to A$ sådan att $\psi(x) = \varphi(x)$ för $x \in V$, så är $\psi(e_i) = \varphi_*(e_i) = \varphi(e_i)$, vilket ger $\psi(x) = \varphi_*(x)$ för varje $x \in C(q)$ därför att $C(q)$ genereras av e_i (som algebra). Detta visar att φ_* är entydig. □

(7.5) Exempel. (a) Låt $q(X,Y) = aX^2 + bY^2$, $a,b \in K$. Cliffordalgebran $C(q)$ har dimension 4 och har som bas $1, e_1, e_2, e_1e_2$ varvid $e_1^2 = a$, $e_2^2 = b$ och $e_1e_2 = -e_2e_1$. Låt $e_1 = i$, $e_2 = j$ och $e_1e_2 = k$. Då är $i^2 = a$, $j^2 = b$, $k^2 = -ab$, $ij = -ji = k$, $jk = -kj = -bi$, $ki = -ik = -aj$. Algebran $C(q)$ betecknas ofta med $(a,b)_K$ och kallas för en **generaliserad kvaternionalgebra** över K. Om $a = 1$, $b = -1$ får vi algebran $(1,-1)_K$ bestående

av $a + bi + cj + dk$ med $i^2 = 1$, $j^2 = -1$, $ij = -ji = k$. Denna algebra är isomorf med matrisalgebran $M_2(K)$ om K är en kropp av karakteristiken $\neq 2$. För att bevisa detta låt

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Matriserna E, X, Y, XY bildar en bas för $M_2(K)$ och $X^2 = E$, $Y^2 = -E$, $XY = -YX$. Detta betyder att multiplikationstabellen för I, X, Y, XY är identisk med multiplikationstabellen för $1, i, j, ij$. Med andra ord får man en isomorfism mellan $(1, -1)_K$ och $M_2(K)$ då man ordnar $a + bi + cj + dk$ mot $aE + bX + cY + dXY$.

Om $K = \mathbb{R}$ och $a = b = -1$ får vi algebran vars element är $a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$ och $i^2 = j^2 = -1$, $ij = -ji = k$, dvs $(-1, -1)_{\mathbb{R}} = \mathbb{H}$ består av de vanliga kvaternionerna. Algebran $\mathbb{H}$ kallas algebran av **Hamiltonkvaternioner**. William Rowen Hamilton (1805 –1865) definierade kvaternioner år 1844. Man visar lätt, som ovan för $M_2(K)$, att den är isomorf med algebran av alla matriser

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

där $z_1, z_2 \in \mathbb{C}$ om man väljer:

$$I = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

och ordnar $a + bi + cj + dk$ mot $aE + bI + cJ + dIJ$ (observera att $I^2 = J^2 = -E$ och $IJ = -JI$).

(b) Låt $q(x) = aX^2$, $a \neq 0$. Cliffordalgebran $C(q)$ har dimension 2 och består av $x + ye$, där $e^2 = a$, dvs $C(q) = K[\sqrt{a}]$.

□

(7.6) Automorfismer av (V, q) och $C(q)$. Om $\varphi : V \to V$ är en isometri av (V, q) dvs $q(\varphi(x)) = q(x)$ för $x \in V$, så inducerar φ en automorfism av $C(q)$. Detta följer direkt ur universella egenskapen hos $C(q)$. I diagrammet:

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C(q) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_*} \\ V & \xrightarrow{\rho} & C(q) \end{array}$$

har sammansättningen $\rho\varphi$ egenskapen: $(\rho\varphi)(v)^2 = \rho(\varphi(v))^2 = q(\varphi(v)) = q(v)$. Alltså existerar exakt en algebrahomomorfism φ_* sådan att diagrammet kommuterar. φ_* är en automorfism ty φ har inversen φ^{-1} så att även φ_* har inversen φ_*^{-1} (motivera detta påstående med hjälp av definitionen av Cliffordalgebran!).

(7.7) Huvudinvolutionen av $C(q)$. Tag $\varphi(x) = -x$ i (7.6). Då får man $\varphi_* : C(q) \to C(q)$ med $\varphi_*(x) = -x$ för $x \in V$ (mera exakt: x tillhörande bilden av V i $C(q)$). Vi skall beteckna den automorfismen av $C(q)$ med δ. Den kallas **huvudinvolutionen** av $C(q)$. Definiera:

$$\begin{aligned} C_0(q) &= \{x \in C(q) : \delta(x) = x\}, \\ C_1(q) &= \{x \in C(q) : \delta(x) = -x\}. \end{aligned}$$

□

(7.8) Proposition. *(a)* $C(q) = C_0(q) \oplus C_1(q)$,

(b) $C_i(q)C_j(q) \subseteq C_{i\oplus j}(q)$, *där* $i \oplus j$ *är summan modulo 2.*

Bevis. (a) Vi har $e_I \in C_0(q)$ då $|I|$ jämnt och $e_I \in C_1(q)$ då $|I|$ udda. Om $x \in C(q)$ så har x entydig framställning

$$x = \sum_{|I| \text{ jämnt}} a_I e_I + \sum_{|I| \text{ udda}} a_I e_I.$$

(b) Följer direkt ur definitionen av $C_0(q)$ och $C_1(q)$. □

Enligt (7.8)(b) är $C_0(q)C_0(q) \subseteq C_0(q)$ så att $C_0(q)$ är en delalgebra till $C(q)$.

(7.9) Definition. $C_0(q)$ kallas **jämna Cliffordalgebran** av (V, q).

□

(7.10) Exempel. (a) $q(x, y) = aX^2 + bY^2$, $ab \neq 0$. $C_0(q)$ genereras av $1, e_1e_2$ med $(e_1e_2)^2 = -ab$ dvs $C_0(q) = K[\sqrt{-ab}]$.

(b) $q(X, Y, Z) = aX^2 + bY^2 + cZ^2$, $abc \neq 0$. $C_0(q)$ genereras av $1, e_1e_2, e_2e_3, e_3e_1$. Låt $e_1e_2 = i$, $e_2e_3 = j$. Då är $i^2 = -ab$, $j^2 = -bc$ och $ij = -ji$. Alltså är $C_0(q) = (-ab, -bc)_K$ dvs en generaliserad kvaternionalgebra (se (7.5)(a)).

□

(7.11) Huvudantiinvolutionen av $C(q)$. Det finns en viktig antiinvolution $x \mapsto x^*$ på $C(q)$ ($(x+y)^* = x^* + y^*, (xy)^* = y^*x^*$ och $x^{**} = x$). Man kan få den ur (7.6) eller genom en direkt definition:

$$e_I^* = (e_{i_1} \cdots e_{i_k})^* = e_{i_k} \cdots e_{i_1} \quad \text{och} \quad 1^* = 1.$$

Man kontrollerar lätt att villkoren är uppfyllda då man definierar $x^* = (\sum a_I e_I)^* = \sum a_I e_I^*$ (se också Övn. 2).

Vi skall anteckna några enkla och användbara räknelagar för basvektorerna e_I för $C(q)$:

(7.12) Proposition. *Låt (V, q) vara ett icke–urartat kvadratiskt rum. Då gäller:*

(a) $e_I e_J e_I^{-1} = (-1)^{|I||J|-|I\cap J|} e_J$ om e_I^{-1} existerar.

(b) Om $x \in C_0(q)$ och $xv = vx$ för varje $v \in V$ så $x \in K$.

(c) Om $x \in C_1(q)$ och $xv = -vx$ för varje $v \in V$ så $x = 0$.

Bevis. (a) Om $e_I = e_{i_1} \dots e_{i_k}$ så $e_I^{-1} = (q(e_{i_1}) \cdots q(e_{i_k}))^{-1} e_{i_k} \cdots e_{i_1}$. Nu räcker det att flytta $e_{i_1}, \dots, e_{i_k}$ till vänster i produkten $e_I e_J e_I^{-1}$ ("passera" e_J) med hänsyn tagen till $e_i e_j = -e_j e_i$ då $i \neq j$ och $e_i^2 = q(e_i)$.

(b) Enligt (a) har vi $e_i e_I = \epsilon_I e_I e_i$, där

$$\epsilon_I = \begin{cases} 1 & \text{då} \quad i \notin I, \\ -1 & \text{då} \quad i \in I, \end{cases}$$

om $|I|$ är jämnt. Om $x = \sum a_I e_I \in C_0(q)$ och $xe_i = e_i x$ så

$$e_i x = \sum a_I e_i e_I = \sum a_I \epsilon_I e_I e_i = \sum a_I e_I e_i.$$

Detta ger $a_I = 0$ då $i \in I$ (för varje $I \neq \emptyset$ finns $i \in I$) så att $x = a_\emptyset e_\emptyset \in K$ ($e_\emptyset = 1$).

(c) Visas på samma sätt som (b). □

Se vidare Övn. 3 i samband med resultat om centrum av $C(q)$ och $C_0(q)$. Viktiga tillämpningar på Cliffordalgebror bygger på samband mellan enheterna i $C(q)$ och automorfismgruppen $O(q)$ av (V, q). Gruppen av alla enheter i $C(q)$ betecknas som vanligt med $C(q)^*$. Denna grupp består av alla $\varepsilon \in C(q)$ sådana att $\varepsilon\eta = \eta\varepsilon = 1$ for ett element $\eta \in C(q)$.

(7.13) Proposition. *Antag att $\alpha \in C(q)^*$ och $\alpha x \alpha^{-1} \in V$ för $x \in V$. Då är funktionen $\sigma_\alpha(x) = \alpha x \alpha^{-1}$ en isometri av (V, q).*

Bevis. $q(\alpha x \alpha^{-1}) = \alpha x \alpha^{-1} \alpha x \alpha^{-1} = \alpha q(x) \alpha^{-1} = q(x)$ (observera att $q(x) \in K$ kommuterar med alla element i $C(q)$.) □

(7.14) Exempel. Låt $v \in V$ och $q(v) \neq 0$. Då är $v^{-1} = q(v)^{-1} v$ inversen till v i $C(q)$ (ty $vv^{-1} = vq(v)^{-1}v = v^2 \cdot q(v)^{-1} = 1$). I detta fall har vi

$$\begin{aligned} \sigma_v(x) &= vxv^{-1} = vxvq(v)^{-1} = (vx + xv)vq(v)^{-1} - x = \\ &= b(x,v)vq(v)^{-1} - x = -(x - \frac{b(x,v)}{q(v)}v) = -\tau_v(x), \end{aligned}$$

där $b(x, y) = q(x + y) - q(x) - q(y)$ (vilket ger $vx + xv = b(x, v)$) och

$$\tau_v(x) = x - \frac{b(x,v)}{q(v)}v.$$

Funktionen $\tau_v : V \to V$ är speglingen i hyperplanet vinkelrät mot v, ty $\tau_v(v) = -v$ ($b(v, v) = 2q(v)$), och om $x \perp v$ (dvs $b(x, v) = 0$) så är $\tau_v(x) = x$.

□

Vi tar upp som en övning (se Övn. 12) följande viktiga sats:

(7.15) Sats. *Varje isometri σ av (V, q) är en sammansättning av speglingar.*

(7.16) Anmärkning. Man kan visa (se Övn. 7) att om $\alpha \in C(q)^*$ och $\delta(\alpha) x \alpha^{-1} \in V$ då $x \in V$ så är $\rho_\alpha(x) = \delta(\alpha) x \alpha^{-1}$ en isometri av (V, q). Gruppen Γ av alla sådana α (det är lätt att se att de bildar en grupp) kallas **Cliffordgruppen** och är ofta viktigare än gruppen av α sådana att $\alpha V \alpha^{-1} \subseteq V$ ur (7.13).

□

(7.17) Sats. *Låt $S\Gamma(q) = \{\alpha \in C_0(q)^* : \alpha v \alpha^{-1} \in V \quad då \ v \in V\}$. Då är $S\Gamma(q)/K^* \cong SO(q)$.*

Bevis. Det är klart att $S\Gamma(q)$ är en grupp. Vi har en grupphomomorfism:

$$\varphi : S\Gamma(q) \to O(q)$$

given av $\varphi(\alpha) = \sigma_\alpha$, där $\sigma_\alpha(v) = \alpha v \alpha^{-1}$ (se (7.13)). Vi har

$$\mathrm{Ker}\varphi = \{\alpha \in S\Gamma(q) : \forall_{v\in V}\sigma_\alpha(v) = v\} = \{\alpha \in S\Gamma(q) : \forall_{v\in V}\alpha v = v\alpha\} = K^*$$

enligt (7.12). Vi måste visa att $\mathrm{Im}\varphi = SO(q)$. Låt $\sigma \in SO(q)$. Då är $\sigma = \tau_{u_1} \circ \ldots \circ \tau_{u_k}$, där τ_{u_i} är speglingar (se (7.15) och (7.14)). k måste vara jämnt ty $\det\sigma = 1$ och $\det\tau_{u_i} = -1$ (se Övn. 10). Låt $\alpha = u_1 \cdots u_k$. Då är $\alpha \in C_0(q)$ och $\varphi(\alpha) = \sigma_\alpha = \tau_{u_1} \circ \cdots \circ \tau_{u_k}$ (ty $\alpha x \alpha^{-1} = u_1 \cdots u_k x u_1^{-1}$ – se (7.14)). Detta visar att $SO(q) \subseteq \mathrm{Im}\varphi$.

Antag att det finns $\alpha \in S\Gamma(q)$ sådan att $\varphi(\alpha) \notin SO(q)$. Då är $\det\varphi(\alpha) = -1$. Men $\varphi(\alpha) = \sigma_\alpha = \tau_{u_1} \circ \cdots \circ \tau_{u_l}$ med l udda. Låt $\beta = u_1 \cdots u_l$. Vi har

$$\sigma_\beta = -\tau_{u_1} \circ \cdots \circ \tau_{u_l} = -\sigma_\alpha$$

dvs $\beta v \beta^{-1} = -\alpha v \alpha^{-1}$, vilket är ekvivalent med $\alpha^{-1}\beta v = -v\alpha^{-1}\beta$ för varje $v \in V$. Enligt (7.12) är $\alpha^{-1}\beta = 0$ – en motsägelse. Detta visar att $\mathrm{Im}\varphi = SO(q)$. □

(7.18) Exempel. Vi visar att $SU(2)/ < -E > \cong SO(3)$, där E är enhetsmatrisen. Vi ger också en beskrivning av isomorfismen. Betrakta Cliffordalgebran $C(q)$ av $(\mathbb{R}^3, q)$, där $q = X^2 + Y^2 + Z^2$. Vi vet redan att $C_0(q) = (-1,-1)_\mathbb{R}$ är kvaternionalgebran $\mathbb{H}$ över $\mathbb{R}$ (se (7.10)(b)). För varje $\alpha \in C_0(q)^* = C_0(q) \setminus \{0\}$ gäller det att $\alpha v \alpha^{-1} \in V = \mathbb{R}^3 = \mathbb{R}e_1 + \mathbb{R}e_2 + \mathbb{R}e_3$ då $v \in V$ och e_1, e_2, e_3 bildar standardbasen för $\mathbb{R}^3$. Man kontrollerar detta direkt genom att utnyttja likheten:

$$\alpha^{-1} = \bar{\alpha} \cdot \frac{1}{N(\alpha)},$$

där $\alpha = a + bi + cj + dk$, $(i = e_1e_2,\ j = e_2e_3,\ k = ij = -ji)$, $\bar{\alpha} = a - bi - cj - dk$ och $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$. Det räcker att visa $\alpha e_i \bar{\alpha} \in V$, vilket är mycket lätt att göra. Alltså är $S\Gamma(q) = C_0(q)^*$ och enligt (7.17) är $C_0(q)^*/\mathbb{R}^* \cong SO(3)$ varvid $\alpha \in C_0(q)^*$ avbildas på σ_α där $\alpha_\alpha(x) = \alpha x \alpha^{-1}$. $C_0(q) = \mathbb{H}$ består av alla matriser

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

och $\mathbb{R}$ är inbäddad som alla diagonalmatriser

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}, r \in \mathbb{R}.$$

Alltså är $SU(2) \subseteq C_0(q)^*$, ty $SU(2)$ består av alla matriser

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

med $|z_1|^2 + |z_2|^2 = 1$ (se Övn. 6.11). Homomorfismen:

$$SU(2) \hookrightarrow C_0(q)^* \to C_0(q)^*/\mathbb{R}^* \cong SO(3)$$

har kärnan bestående av reella diagonalmatriser i $SU(2)$. Dessa är

$$\begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$$

med $r^2 = 1$ dvs $\pm E$. Bilden av $SU(2)$ är $SU(2)\mathbb{R}^*/\mathbb{R}^*$. Men varje matris i $C_0(q)^*$ har formen:

$$\begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} z_1/r & z_2/r \\ -\bar{z}_2/r & \bar{z}_1/r \end{bmatrix},$$

där $r^2 = |z_1|^2 + |z_2|^2$, $r \in \mathbb{R}$, och

$$\frac{1}{r} \begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix} \in SU(2).$$

Detta visar att $C_0(q)^* = SU(2)\mathbb{R}^*$ dvs bilden av $SU(2)$ är $SU(2)\mathbb{R}^*/\mathbb{R}^* = C_0(q)^*/\mathbb{R}^* \cong SO(3)$. Alltså är $SU(2)/ < -E > \cong SO(3)$.

□

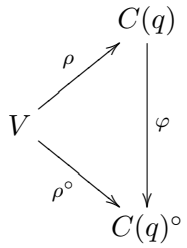
Vi skall visa andra liknande isomorfismer i samband med övningar (se Övn. 4).

ÖVNINGAR

7.1. Låt (V, q) vara ett kvadratiskt rum över K och låt $T(V)$ vara tensoralgebran av V över K. Visa att $C(q) \cong T(V)/(x \otimes x - q(x))$, där $(x \otimes x - q(x))$ betecknar idealet i $T(V)$ som genereras av alla $x \otimes x - q(x) \in T(V)$ med $x \in V$.

Ledning. Utnyttja universella egenskapen hos $C(q)$ och en naturlig algebrahomomorfism $T(V) \to C(q)$.

7.2. Låt A vara en K-algebra och låt A° vara den algebra som har samma element som A, med samma addition som i A, men med en ny multiplikation "$\circ$": $a \circ b = ba$, där $a, b \in A^\circ$ och produkten till höger är i A. A° kallas **duala algebran** till A. Låt $C(q)$ vara Cliffordalgebran av (V, q). Då har man:



där $\rho^\circ(v) = v$. Alltså är $(\rho^\circ(v))^2 = q(v)$. Detta innebär att det finns φ i diagrammet som gör att det kommuterar. Motivera att φ är huvudantiinvolutionen på $C(q)$ (se (7.11)).

7.3. Låt (V, q) vara ett kvadratiskt rum över $K, e_1, \ldots e_n$ en ortogonalbas för V över K och $\alpha = e_1 \ldots e_n \in C(q)$. Låt $Z(A)$ beteckna centrum av en K-algebra A (dvs $Z(A) = \{\alpha \in A : \forall_{x \in A}\ \alpha x = x\alpha\}$) Visa att

(a) om $\dim V$ är jämn så är $Z(C(q)) = K$, $Z(C_0(q)) = K[\alpha]$,

(b) om $\dim V$ är udda så är $Z(C(q)) = K[\alpha]$, $Z(C_0(q)) = K$.

7.4. Genom att använda samma teknik som i (7.18) visa att

(a) $O^\uparrow_+(1,2) \cong SL(2,\mathbb{R})/ < -E >$,

(b) $O^\uparrow_+(1,3) \cong SL(2,\mathbb{C})/ < -E >$.

7.5. Låt (V, q) vara ett kvadratiskt rum. Visa att följande delmängder till $C(q)$ bildar grupper med avseende på multiplikation:

(a) $\Gamma(q) = \{\alpha \in C(q)^* : \delta(\alpha) V \alpha^{-1} = V\}$ (Cliffordgruppen av (V, q)),

(b) $S\Gamma(q) = \Gamma(q) \cap C_0(q)$ (speciella Cliffordgruppen av (V, q)),

(c) $G(q) = \{\alpha \in C(q)^* : \alpha = v_1 \ldots v_i, \quad v_i \in V \text{ och } q(v_i) \neq 0\}$,

(d) $SG(q) = G(q) \cap C_0(q)$,

(e) $\mathrm{Pin}(q) = \{\alpha \in G(q) : \alpha\alpha^* = 1\}$ (pinorgruppen av (V, q)),

(f) $\mathrm{Spin}(q) = \mathrm{Pin}(q) \cap C_0(q)$ (spinorgruppen av (V, q)).

7.6. Låt A vara en ändligt dimensionell K-algebra och låt $x \in A$. Visa att om det finns $y \in A$ så att $xy = 1$ så är även $yx = 1$ (på samma sätt $yx = 1 \Rightarrow xy = 1$).

7.7. (a) Visa att $\varphi : \Gamma(q) \to \mathrm{Aut}_K(V)$, där $\varphi(\alpha) =: \sigma_\alpha$, $\sigma_\alpha(x) = \delta(\alpha)x\alpha^{-1}$ är en grupphomomorfism och att $\mathrm{Ker}\varphi = K^*$.

(b) Visa att $N : \Gamma(q) \to K^*$, där $N(\alpha) = \alpha\bar{\alpha}$ är en grupphomomorfism.

Ledning. Visa att $\alpha\bar{\alpha} \in \mathrm{Ker}\varphi$.

7.8. (a) Enligt (7.17) har man $S\Gamma(q)/K^* \cong SO(q)$. Visa att $\Gamma(q)/K^* \cong O(q)$, där isomorfismen induceras av φ ur Övn. 7(a).

(b) Visa att $N : \Gamma(q) \to K^*$ inducerar en homomorfism $\theta : \Gamma(q)/K^* \to K^*/K^{*2}$ (dvs $\theta : O(q) \to K^*/K^{*2}$). Motivera att $\theta(\tau_\alpha) = q(\alpha)K^{*2}$ och allmänt $\theta(\tau_{\alpha_1} \circ \ldots \circ \tau_{\alpha_k}) = q(\alpha_1)\ldots q(\alpha_k)K^*$ ($\theta(\sigma_\alpha) = \alpha\bar{\alpha} = N(\alpha)$ modulo K^*).

Anmärkning. θ kallas **spinornormen.**

(c) Låt $\Theta(q) = \{\sigma \in O(q) : \theta(\sigma) \in K^{*2}\}$. Visa att det finns surjektiva grupphomomorfismer $\mathrm{Pin}(q) \to \Theta(q)$ och $\mathrm{Spin}(q) \to S\Theta(q)$ med kärnan $\{\pm 1\}$, där $S\Theta(q) = \Theta(q) \cap C_0(q)$.

7.9. Låt (V, q) vara ett Euklidiskt rum över $\mathbb{R}$. Visa att det finns en surjektiv homomorfism $\mathrm{Spin}(q) \to SO(q)$ med kärnan $\{\pm 1\}$ inducerad av surjektionen $S\Gamma(q) \to SO(q)$.

7.10. Låt $\tau : V \to V$ vara en spegling (se (7.14)). Visa att $\det \tau = -1$.

7.11. Låt (V, q) vara ett hyperboliskt rum (se Övn. 6.2) och låt $q(x) = T(x, x)$, där $T : V \times V \to K$ är symmetrisk och bilinjär. Låt $e_1, \ldots, e_m$, $f_1, \ldots, f_m$ vara en bas för V sådan att $q(e_i) = q(f_i) = 0$ och $T(e_i, f_i) = 1$ (dvs V är ett hyperboliskt rum). Visa att:

(a) $C(q)e$, där $e = e_1 \ldots e_m$, är ett vänsterideal i $C(q)$ och $\dim_K C(q)e = 2^m$.

(b) $C(q) \cong \mathrm{End}_K(C(q)e)$ och en isomorfism ges av $\Phi(\alpha)(x) = \alpha x$ då $\alpha \in C(q)$ och $x \in C(q)e$.

(c) $C(q) \cong \bigwedge(U)$, där $U = Ke_1 + \ldots + Ke_m$.

Anmärkning. Elementen i $C(q)e$ kallas **spinorer** och isomormofismen i (b) kallar man för **spinorrepresentationen** av $C(q)$. Varje element i $C(q)$ representeras med hjälp av den isomorfismen som en $(2^m \times 2^m)$-matris. En liknande konstruktion gäller då $V = H \perp < a >$, där H är ett hyperboliskt rum.

(d) Låt $V =< 1 > \perp < -1 > \perp < -1 > \perp < -1 >$ över $\mathbb{C}$ och låt $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ vara en ortogonalbas sådan att $q(\alpha_1) = 1$, $q(\alpha_i) = -1$ för $i = 2, 3, 4$. Bestäm en bas e_1, e_2, f_1, f_2 för V som ovan och bestäm spinorrepresentationen av $\alpha_1, \alpha_2, \alpha_3, \alpha_r \in C(q)$. (Man får s.k. **Diracmatriser**).

7.12. Låt (V, q) vara ett icke-urartat kvadratiskt rum (se Övn. 6.1). Visa att:

(a) Om $v_1, v_2 \in V$, $q(v_1) = q(v_2)$ och $q(v_1 - v_2) \neq 0$ så $\tau_{v_1 - v_2}(v_1) = v_2$ (se (7.14)).

(b) Om $v_1, v_2 \in V$, $q(v_1) = q(v_2) \neq 0$ så existerar en isometri $\sigma : V \to V$ sådan att $\sigma(v_1) = v_2$ varvid σ är en symmetri eller sammansättning av två symmetrier.

Ledning. $q(v_1 + v_2) + q(v_1 - v_2) \neq 0$.

(c) Visa att varje isometri $\sigma : V \to V$ är en sammansättning av symmetrier.

Ledning. Välj $v \in V$ med $q(v) \neq 0$ och tillämpa (b) på $v_1 = v, v_2 = \sigma(v)$. Betrakta $V_1 \subset V$ där $V =< v > \perp V_1$ och använd induktion m.a.p. $\dim V$.

Anmärkning. (c) är en försvagad version av Cartan-Dieudonné sats som säger att σ är en sammansättning av högst $\dim V$ symmetrier. Vår bevismetod ger att σ är en sammansättning av högst $2 \dim V$ symmetrier.

Kapitel 8

MODULER ÖVER HUVUDIDEALOMRÅDEN

I detta kapitel förutsätter vi att R är ett huvudidealområde med etta. Vårt syfte är att beskriva alla ändligt genererade R-moduler. Som två viktiga specialfall får vi huvudsatsen om ändligt genererade abelska grupper (8.15) och satser om normalformer för matriser som t.ex. Jordans normalform i (8.23).

Vi skall börja med fria R-moduler. Låt oss påminna om att rangen av en fri R-modul F är kardinaliteten av en godtycklig bas för F över R. Vi skall beteckna rangen av F över R med $\mathrm{rg}_R F$.

(8.1) Sats. *(a) Om F är en fri R-modul och M är dess delmodul så är också M fri och $\mathrm{rg}_R M \leq \mathrm{rg}_R F$.*

(b) Om F är ändligt genererad fri över R så existerar en bas $e_1, \ldots, e_n$ för F över R och $d_1, \ldots, d_r \in R$ sådana att $d_1 e_1, \ldots, d_r e_r$ bildar en bas för M över R. Vidare kan $d_1, \ldots, d_r$ väljas så att $d_1 | \ldots | d_r$.

(c) Idealen $(d_1) \supseteq \cdots \supseteq (d_r)$ är entydigt bestämda av F och M.

Bevis. Låt $a \in R$, $a \neq 0$. Med $l(a)$ betecknar vi antalet irreducibla faktorer i faktoruppdelningen av a i produkt av irreducibla element i R. Som vi vet existerar sådana uppdelningar i R och antalet irreducibla faktorer är oberoende av valet av uppdelningen (ty R är ett huvudidealområde). Notera att $l(a) = 0$ då och endast då a är en enhet i R. $l(a)$ är inte definierad då $a = 0$.

(a) Vi skall begränsa oss till fallet då F är ändligt genererad och visa satsen induktivt med avseende på $\mathrm{rg}_R F$. Om $F = (0)$ så är påståendet klart. Antag att satsen gäller då $\mathrm{rg}_R F < n$

och låt $e_1, \ldots, e_n$ vara en bas för F över R. Om $M = (0)$ så är allt klart. Antag att $M \neq (0)$ och låt $m \in M$, $m \neq 0$. Då är

$$m = a_1 e_1 + \cdots + a_n e_n,$$

där ej alla a_i är 0. Genom att eventuellt numrera om basvektorerna kan vi förutsätta att $a_1 \neq 0$. Låt oss välja $m^0 \in M$ så att

$$m^0 = a_1^0 e_1 + \cdots + a_n^0 e_n$$

och $l(a_1^0) = \min(l(a_1))$ då $m \in M$ och $a_1 \neq 0$. Vi påstår att om $m \in M$ och $m = a_1 e_1 + \cdots + a_n e_n$ så $a_1^0 | a_1$. Låt $d = SGD(a_1^0, a_1)$ (se Övn. 2.27). Då existerar x_1^0, $x_1 \in R$ sådana att

$$d = x_1^0 a_1^0 + x_1 a_1.$$

Vi har $x_1^0 m^0 + x_1 m = d e_1 + \cdots$ så $l(d) \geq l(a_1^0)$ enligt valet av a_1^0. Men $d | a_1^0$, vilket ger att $l(d) \leq l(a_1^0)$. Alltså har d och a_1^0 samma irreducibla faktorer (så när som på associering) och således $a_1^0 | a_1$.

Låt nu $F_0 = Re_2 + \cdots + Re_n$ och $M_0 = F_0 \cap M$. Vi påstår att

$$M = Rm^0 \oplus M_0.$$

Om $m \in M$ är ett godtyckligt element i M som ovan så är $a_1 = q a_1^0$, där $q \in R$, så att $m - qm^0 \in M_0$. Detta visar att $M = Rm^0 + M_0$. Om $m \in Rm^0 \cap M_0$ så är

$$m = a(a_1^0 e_1 + \cdots + a_n^0 e_n) = a_2 e_2 + \cdots + a_n e_n,$$

där $a \in R$, vilket ger $m = 0$ ty $a a_1^0 = 0$ och $a_1^0 \neq 0$ implicerar $a = 0$. Nu följer påståendet ur vårt induktiva antagande ty M_0 är en delmodul till den fria R-modulen F_0 vars rang över R är $n - 1$.

Notera att vi har visat lite mera än bara påståendet i (a). Vårt bevis visar att F har en bas $e_1, e_2, \ldots, e_n$ sådan att

$$\begin{aligned} f_1 &= a_{11} e_1 + a_{12} e_2 + \cdots + a_{1r} e_r + \cdots + a_{1n} e_n, \\ f_2 &= \qquad a_{22} e_2 + \cdots + a_{2r} e_r + \cdots + a_{2n} e_n, \\ &\cdots\cdots \\ f_r &= \qquad\qquad\qquad a_{rr} e_r + \cdots + a_{rn} e_n \end{aligned} \tag{8.2}$$

bildar en bas för M över R, där $f_1 = m^0$ (dvs $a_{1i} = a_i^0$). Vi förstärker detta påstående ytterligare i beviset av andra delen av satsen.

(b) Vi skall också använda oss av induktion med avseende på $\mathrm{rg}_R F$, men den här gången startar vi med $n = 1$. I detta fall är F och R isomorfa som R–moduler. Låt en isomorfism avbilda 1 i R på e i F dvs $F = Re$. M är isomorf med en delmodul till R dvs ett ideal I i R. Men $I = Rd$ är ett huvudideal så att $M = Rde$. (Observera att fallet $n = 1$ också följer från (8.2)). Antag nu att påståendet gäller då $\mathrm{rg}_R F < n$ och $n \geq 2$.

Låt oss nu välja $m^0 \in M$, $m^0 \neq 0$, så att

$$m^0 = a_1^0 e_1 + \cdots + a_n^0 e_n$$

och $l(a_1^0) = \min(l(a_1))$ då $m = a_1 e_1 + \cdots + a_n e_n$ löper över alla element i M och $e_1, \ldots, e_n$ över alla möjliga baser för F över R. På samma sätt som i (a) får vi $a_1^0 | a_1$. Nu visar vi att även $a_1^0 | a_i$ för alla i. Låt oss först visa att $a_1^0 | a_i^0$ dvs

$(*)$ om $m^0 = a_1^0 e_1 + \cdots + a_n^0 e_n$ och $l(a_1^0)$ är minimalt (som ovan) så $a_1^0 | a_i^0$.

Vi kan förutsätta att $i = 2$ genom att eventuellt numrera om basvektorerna $e_2, \ldots, e_n$. Låt $d = SGD(a_1^0, a_2^0)$. Då är $d = a_1^0 x_1 + a_2^0 x_2$, där $x_1, x_2 \in R$. Betrakta en ny bas för F över R bestående av $e_1', e_2', \ldots, e_n'$ sådana att

$$\begin{aligned} e_1 &= x_1 e_1' - b_1 e_2', \\ e_2 &= x_2 e_1' + b_2 e_2', \end{aligned}$$

samt $e_i = e_i'$ då $i > 2$, där $b_1 = a_2^0/d$ och $b_2 = a_1^0/d$. Det är klart att $e_1', e_2', \ldots, e_n'$ bildar en bas ty determinanten av övergångsmatrisen från dessa vektorer till $e_1, e_2, \ldots, e_n$ är $b_2 x_1 + b_1 x_2 = d^{-1}(a_1^0 x_1 + a_2^0 x_2) = 1$. I den nya basen är

$$m^0 = a_1^0 e_1 + a_2^0 e_2 + \cdots + a_n^0 e_n = (a_1^0 x_1 + a_2^0 x_2) e_1' + \cdots = d e_1' + \cdots$$

så att $l(d) \geq l(a_1^0)$ enligt valet av a_1^0. Men $d | a_1^0$ ger nu $l(d) = l(a_1^0)$, vilket betyder att a_1^0 och d är associerade (skiljer sig så när som på en enhet). Detta visar att $a_1^0 | a_2^0$ och allmänt $a_1^0 | a_i^0$ för $i \geq 1$. Nu kan vi ersätta e_1 med vektorn $(1/a_1^0) m^0$, ty denna vektor tillsammans med $e_2, \ldots, e_n$ bildar också en bas för F över R. Enligt (8.2) existerar en bas för F, som vi också betecknar med $e_1 = (1/a_1^0) m^0, e_2, \ldots, e_n$, sådan att

$$\begin{aligned} f_1 &= a_1^0 e_1, \\ f_2 &= \quad a_{22} e_2 + \cdots + a_{2r} e_r + \cdots + a_{2n} e_n, \\ &\cdots\cdots \\ f_r &= \quad\quad\quad\quad\quad\quad a_{rr} e_r + \cdots + a_{rn} e_n, \end{aligned}$$

där $a_{ij} \in R$, är en bas för M. Men $f_1 + f_i = a_1^0 e_1 + a_{ii} e_i + \cdots + a_{in} e_n \in M$ så att $a_1^0 | a_{ij}$ enligt $(*)$. Om nu $m \in M$ så är m en linjärkombination av $f_1, f_2, \ldots, f_r$. Alltså är alla koordinater för m i basen $e_1, e_2, \ldots, e_n$ delbara med a_1^0. Notera också att vi kan ersätta $e_1, e_2, \ldots, e_n$ med en annan bas för F över R och då är koordinaterna för m i denna bas fortfarande delbara med a_1^0. Definiera nu $d_1 = a_1^0$. Som i (a) får vi att

$$M = R m^0 \oplus M_0,$$

där $m^0 = f_1 = d_1 e_1, M_0 = F_0 \cap M$ och $F_0 = R e_2 + \cdots + R e_n$ har rangen $n - 1$ över R. Induktionen ger att F_0 har en bas, som vi fortfarande betecknar med $e_2, \ldots, e_n$, sådan att $d_2 e_2, \ldots, d_r e_r$ är en bas för M_0 över R och $d_2 | \ldots | d_r$. Vi vet redan att $d_1 | d_2$, vilket betyder att $e_1, e_2, \ldots, e_n$ är en önskad bas för F över R och $d_1 e_2, d_2 e_2, \ldots, d_r e_r$ för M över R.

(c) Det återstår att visa entydigheten av idealen $(d_1), \ldots, (d_r)$. Detta påstående visas lite senare i (8.10) (se också Övn. 1). □

Nu går vi från fria moduler till godtyckliga ändligt genererade moduler över R. Först behöver vi några enkla och allmänna begrepp.

(8.3) Definition. Låt M vara en R-modul. Ett element $m \in M$ kallas **torsionselement** om det finns $a \in R$, $a \neq 0$, så att $am = 0$. M kallas **torsionsmodul** om varje element i M är ett torsionselement. Man betecknar med M_t mängden av alla torsionselement i M.

□

Observera att om $R = \mathbb{Z}$ och M är en $\mathbb{Z}$-modul (dvs en abelsk grupp) så består M_t av alla element i M som har en ändlig ordning. Rent allmänt har vi:

(8.4) Proposition. *Om M är en R-modul så är M_t en delmodul till M. Om $f : M \to M'$ är en isomorfism så ger restriktionen av f till M_t en isomorfism mellan M_t och M'_t.*

Bevis. Enkel övning. □

Alla moduler över huvudidealområden är uppbyggda av så kallade cykliska moduler.

(8.5) Definition. Man säger att en R-modul M är **cyklisk** om det finns $m \in M$ så att $M = Rm$.

□

Begreppet cyklisk modul generaliserar begreppet cyklisk grupp. Låt oss repetera att om G är en cyklisk grupp så är $G \cong \mathbb{Z}$ eller $G \cong \mathbb{Z}/(n)$, där $n \neq 0$. Mera allmänt gäller följande beskrivning av cykliska moduler:

(8.6) Proposition. *En cyklisk R-modul $M = Rm$ är antingen fri och då $M \cong R$, eller $M \cong R/(d)$, där $d \in R$ och $d \neq 0$. I det sista fallet är M en torsionsmodul och $dM = (0)$.*

Bevis. Betrakta surjektionen $\varphi : R \to M$, där $\varphi(r) = rm$. Låt $\mathrm{Ker}\varphi = (d)$. Då är $M \cong R/(d)$. Om $d = 0$ så är $M \cong R$ en fri R-modul. Om $d \neq 0$ så är M en torsionsmodul och det är klart att $d(rm) = r(dm) = r\varphi(d) = 0$. □

Låt M vara en R-modul. Då kallas

$$\mathrm{Ann}_R(M) = \{x \in R : xM = (0)\} \tag{8.7}$$

för **annulatorn** av M. $\mathrm{Ann}_R(M)$ är ett ideal i R (se Övn. 3.4). Om $M = R/(d)$ så är $\mathrm{Ann}_R(M) = (d)$.

Nu är vi beredda att visa vår andra sats i detta kapitel. Satsen ger en nästan fullständig beskrivning av ändligt genererade R-moduler. Men vi kommer att få en ännu mera detaljerad bild i Sats (8.14).

(8.8) Sats. *Låt M vara en ändligt genererad R-modul över ett huvudidealområde R. Då är*

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^s,$$

där $d_1|\ldots|d_r$ och $s \geq 0$. Idealen $(d_r) \subseteq \ldots \subseteq (d_1) \neq R$ samt r och s är entydigt definierade av isomorfiklassen av M, dvs om

$$M' \cong R/(d_1') \oplus \cdots \oplus R/(d_{r'}') \oplus R^{s'}$$

och $M \cong M'$ så är $r = r'$, $s = s'$ och $(d_i) = (d_i')$ för $i = 1, \ldots, r$.

Bevis. För att visa existensen låt $M = Rm_1 + \cdots + Rm_n$. Betrakta en fri R-modul $F = Re_1' + \cdots + Re_n'$ och surjektionen $\varphi : F \to M$, där $\varphi(e_i') = m_i$. Låt $F_0 = \text{Ker } \varphi$ så att $M = F/F_0$. Enligt (8.1)(a) är F_0 fri. Låt $e_1, \ldots, e_n$ vara en bas för F över R sådan att $F_0 = Rd_1e_1 + \cdots + Rd_re_r$, där $d_1|\ldots|d_r$ och $r \leq n$ (se (8.1) (b)). Låt $s = n - r$.

Definiera nu

$$\psi : F \longrightarrow R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^s$$

så att $\psi(\sum a_ie_i) = (\bar{a}_1, \ldots, \bar{a}_n)$, där $\bar{a}_i$ är restklassen av a_i i $R/(d_i)$ då $1 \leq i \leq r$ och $\bar{a}_i = a_i$ då $r < i \leq n$. Man finner lätt att Ker $\psi = F_0$ så att

$$M \cong F/F_0 \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^s$$

Om d_i är en enhet så är $R/(d_i) = (0)$. Vi kan stryka alla sådana d_i och numrera om de återstående så att d_1 inte är en enhet. Detta visar det första påståendet i satsen.

Observera att

$$M_t \cong R/(d_1) \oplus \cdots \oplus R/(d_r)$$

därför att $a(\bar{a}_1, \ldots, \bar{a}_n) = (0, \ldots, 0)$ med $a \neq 0$ implicerar att $\bar{a}_i = a_i = 0$ då $r < i \leq n$, däremot $d_r(\bar{a}_1, \ldots, \bar{a}_r, 0, \ldots, 0) = (0, \ldots, 0)$ ty $d_i|d_r$ då $1 \leq i \leq r$. Man inser lätt att

$$\text{Ann}_R(M_t) = \{x \in R : xM_t = 0\} = (d_r).$$

För att visa entydigheten av $(d_1), \ldots, (d_r)$ och s låt oss börja med två triviala observationer. Om $M = M_1 \oplus M_2$, där M_1, M_2 är R-moduler och $a \in R$ så är $aM = aM_1 \oplus aM_2$. Varje R-isomorfism $f : M \to M'$ inducerar en R-isomorfism $f : aM \to aM'$ (vi använder här samma beteckning för f och f begränsad till aM).

Tag $a = d_rd_{r'}'$. Isomorfismen $M \cong M'$ inducerar $aM \cong aM'$. Men $aR/(d_i) = 0$ och $aR/(d_j') = 0$ för $i = 1, \ldots, r$ och $j = 1, \ldots, r'$ ty $d_i|a$ och $d_j'|a$. Alltså är $aR^s \cong aR^{s'}$. Men $aR \cong R$ så

att $R^s \cong R^{s'}$, vilket ger $s = s'$ enligt (3.20) (två baser för samma fria R-modul har samma kardinalitet).

Isomorfismen $M \cong M'$ ger också $M_t \cong M'_t$ dvs

$$M_t \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \cong R/(d'_1) \oplus \cdots \oplus R/(d'_{r'}) \cong M'_t$$

Observera att $\mathrm{Ann}_R(M_t) = \mathrm{Ann}_R(M'_t) = (d_r) = (d'_{r'})$, ty isomorfa moduler har identiska annulatorer. Vi skall visa induktivt med avseende på antalet irreducibla primfaktorer i d_r (dvs med avseende på $l(d_r) = l(d'_{r'})$ – se början av beviset för (8.1)) att $r = r'$ och $(d_i) = (d'_i)$.

Om $(d_r) = (d'_{r'}) = (p)$, där p är ett irreducibelt element i R så måste

$$(d_1) = \ldots = (d_r) = (d'_1) = \ldots = (d'_{r'}) = (p)$$

ty $d_i, d'_i | d_r$ och de är inte enheter. Alltså är

$$M_t \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{r \text{ termer}} \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{r' \text{ termer}} \cong M'_t.$$

Men $R/(p)$ är en kropp (ty (p) är maximalt i R) så att M_t och M'_t är isomorfa vektorrum. Därför måste deras dimensioner över $R/(p)$ vara lika dvs $r = r'$.

Antag nu att påståendet gäller för torsionsmoduler vars annulatorer genereras av element med antalet irreducibla faktorer som är $< l(d_r) = l(d'_{r'})$, där $(d_r) = (d'_{r'})$ är annulatorn av M_t (och M'_t). Först påstår vi att d_1 och d'_1 måste ha en gemensam irreducibel faktor. Om det inte är fallet, så existerar irreducibla faktorer p och p' sådana att $p | d_1$ och $p \nmid d'_1$ samt $p' | d'_1$ och $p' \nmid d_1$. Då har vi:

$$pM_t \cong R/(d_1/p) \oplus \cdots \oplus R/(d_r/p) \cong R/(d'_1) \oplus \cdots \oplus R/(d'_{r'}/p) \cong pM'_t,$$

och

$$p'M_t \cong R/(d_1) \oplus \cdots \oplus R/(d_r/p') \cong R/(d'_1/p') \oplus \cdots \oplus R/(d'_r/p') \cong p'M'_t,$$

ty

$$p(R/(d)) \cong (pR + dR)/(d) \cong \begin{cases} R/(d/p) & \text{då} \quad pR + dR = pR \quad \text{dvs} \quad p|d, \\ R/(d) & \text{då} \quad pR + dR = R \quad \text{dvs} \quad p \nmid d. \end{cases}$$

Men $\mathrm{Ann}_R(pM_t) = (d_r/p)$ och $\mathrm{Ann}_R(p'M_t) = (d_r/p')$ (observera att $pp' | d_r = d'_{r'}$) så att vårt induktiva antagande ger att $(d_1/p) = (d'_1)$ och $(d'_1/p') = (d_1)$. Alltså är $(pp') = R$, vilket är orimligt. Detta visar att det finns p så att $p|d_1$ och $p|d'_1$. Betrakta nu modulerna pM_t och pM'_t. Vi får

$$pM_t \cong R/(d_1/p) \oplus \cdots \oplus R/(d_r/p) \cong R/(d'_1/p) \oplus \cdots \oplus r/(d'_{r'}/p) \cong pM'_t$$

och $\mathrm{Ann}_R(pM_t) = (d_r/p)$ innehåller färre primfaktorer än $\mathrm{Ann}_R(M_t)$. Alltså är $r = r'$ och $(d_i/p) = (d'_i/p)$ dvs $(d_i) = (d'_i)$ för $i = 1, \ldots, r$. □

Låt oss anteckna två mycket viktiga följdsatser av den sista satsen.

(8.9) Följdsats. *Låt M vara en ändligt genererad R-modul över ett huvudidealområde R. Då är*

$$M \cong M_t \oplus F,$$

där F är en fri R-modul.

Bevis. Påståendet sammanfaller med första delen av (8.8). □

Nu kan vi också ge ett bevis av entydigheten i (8.1)(c):

(8.10) Följdsats. *Idealen $(d_1) \subseteq \ldots \subseteq (d_r)$ i sats (8.1)(c) är entydigt definierade av M och F.*

Bevis. Om $e_1, \ldots, e_n$ och $e'_1, \ldots e'_n$ är baser för F över R sådana att

$$M = Rd_1e_1 + \cdots + Rd_re_r \quad \text{och} \quad M = Rd'_1e'_1 + \cdots + Rd'_re'_r,$$

så är

$$F/F_0 \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^s \cong R/(d'_1) \oplus \cdots \oplus R/(d'_r) \oplus R^s$$

(se början av beviset för (8.8)). Alltså är $(d_i) = (d'_i)$ för $i = 1, \ldots r$ enligt (8.8). □

Nu skall vi göra sista steget och beskriva alla cykliska torsionsmoduler $R/(d)$. I detta syfte visar vi först ett mycket allmänt resultat:

(8.11) Kinesiska restsatsen. *Låt R vara en ring med etta, $I_1, \ldots I_n$ ideal i R sådana att $I_k + I_l = R$ då $k \neq l$. För varje uppsättning $x_1, \ldots, x_n \in R$ existerar då $x \in R$ så att $x \equiv x_i \pmod{I_i}$ (dvs $x - x_i \in I_i$ då $i = 1, \ldots, n$).*

Bevis. Induktion. Om $n = 2$, så är

$$1 = r_1 + r_2, \;\; r_1 \in I_1, r_2 \in I_2.$$

Välj då $x = x_2r_1 + x_1r_2$. Låt oss nu anta att satsen gäller för $n-1$ ideal och betrakta n ideal. För varje k existerar $r_1^{(k)} \in I_1$ och $r_k \in I_k$, $k \geq 2$, sådana att

$$r_1^{(k)} + r_k = 1$$

(ty $I_1 + I_k = R$). Produkten $\prod_{k=2}^n (r_1^{(k)} + r_k) = 1$ tillhör idealet $I_1 + \prod_{k=2}^n I_k$ dvs

$$I_1 + \prod_{k=2}^{n} I_k = R.$$

Enligt fallet $n = 2$ existerar $y_1 \in R$ sådant att

$$y_1 \equiv 1 \pmod{I_1} \quad \text{och} \quad y_1 \equiv 0 \pmod{\prod_{k=2}^{n} I_k},$$

vilket ger $y_1 \equiv 0 \pmod{I_k}$, $k \neq 1$. Av symmetriskäl finns det också $y_2, \ldots, y_n$ sådana att

$$y_l \equiv 1 \pmod{I_l} \quad \text{och} \quad y_l \equiv 0 \pmod{I_k} \quad \text{då} \quad k \neq l$$

för $l = 2, \ldots, n$ (och tidigare även $l = 1$). Nu väljer vi $x = x_1y_1 + \cdots + x_ny_n$ och kontrollerar lätt att $x \equiv x_i \pmod{I_i}$ för $i = 1, \ldots, n$. □

(8.12) Anmärkning. Om $R = \mathbb{Z}$ så är (8.11) den "ursprungliga versionen" av Kinesiska restsatsen. Den säger att om $m_1, \ldots, m_n$ är heltal som är parvis relativt prima och $r_1, \ldots, r_n$ är givna heltal så existerar ett heltal x sådant att resten vid division av x med m_i är r_i (dvs $x \equiv r_i \pmod{m_i}$).

□

(8.13) Proposition. *Låt $R/(d)$ vara en cyklisk R-modul, och $d = p_1^{k_1} \ldots p_n^{k_n}$, där p_i är olika irreducibla element i R. Då är*

$$R/(d) \cong R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_n^{k_n}).$$

Bevis. Låt φ vara homomorfismen $R \to R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_n^{k_n})$, där $r \mapsto (\bar{r}, \ldots, \bar{r})$ och $\bar{r}$ på i-te platsen betecknar bilden av r vid den naturliga surjektionen $R \to R/(p_i^{k_i})$. Vi har Ker $\varphi = \{r \in R : r \equiv 0 \pmod{p_i^{k_i}} \text{ för } i = 1, \ldots, n\} = (d)$. Enligt Kinesiska restsatsen är φ en surjektion ty för godtyckliga element $\bar{r}_i \in R/(p_i^{k_i})$, $r_i \in R$ existerar $r \in R$ sådant att $r \equiv r_i \pmod{p_i^{k_i}}$ dvs $\bar{r} = \bar{r}_i$. Detta betyder att

$$r \mapsto (\bar{r}, \ldots, \bar{r}) = (\bar{r}_1, \ldots, \bar{r}_n)$$

(möjligheten att tillämpa Kinesiska restsatsen följer ur det faktum att idealen $(p_i^{k_i})$ är relativt prima dvs $(p_i^{k_i}) + (p_j^{k_j}) = R$, ty $\mathrm{SGD}(p_i^{k_i}, p_j^{k_j}) = 1$). □

Nu kan vi bevisa huvudsatsen om torsionsmoduler över huvudidealområden. Om p är ett irreducibelt element i R och M är en R-modul så definierar vi

$$M(p) = \{m \in M : \exists_{k \geq 0}\ p^k m = 0\}.$$

(8.14) Sats. *Om $M \neq (0)$ är en ändligt genererad torsionsmodul över R så är*

$$M = \bigoplus M(p),$$

där (p) löper över alla primideal sådana att $(p) \supseteq \mathrm{Ann}_R(M)$, och varje $M(p)$ är en direkt summa av cykliska moduler $R/(p^k)$ med entydigt bestämda exponenter k.

Bevis. Först uppdelar vi M i enlighet med (8.8):

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_r)$$

där $d_1 | \ldots | d_r$ och $R/(d_i) \neq 0$ är torsionsmoduler. Låt

$$\begin{aligned} d_r &= p_1^{k_{r1}} \cdots p_t^{k_{rt}}, \\ &\cdots\cdots \\ d_1 &= p_1^{k_{11}} \cdots p_t^{k_{1t}}, \end{aligned}$$

där $k_{11} \leq \ldots \leq k_{r1}, \ldots, k_{1t} \leq \ldots \leq k_{rt}$, $p_1, \ldots, p_t$ är olika irreducibla element i R. Nu tillämpar vi (8.13) på var och en av modulerna $R/(d_i)$ och samlar ihop de cykliska modulerna $R/(p_i^{k_{ij}})$ dvs:

$$M(p_i) \cong R/(p_i^{k_{1i}}) \oplus \cdots \oplus R/(p_i^{k_{ri}})$$

och

$$M \cong M(p_1) \oplus \cdots \oplus M(p_t).$$

Påståendet om entydigheten av termerna $R/(p_i^{k_{ij}})$ följer direkt ur entydigheten av faktoruppdelningar i R samt (8.8). Lägg märke till att $\mathrm{Ann}_R(M) = (d_r)$.

□

Vi skall tillämpa (8.14) i två specialfall – ändligt genererade abelska grupper och kanoniska former av linjära avbildningar. Vi börjar med abelska grupper.

Om $R = \mathbb{Z}$ och G är en ändligt genererad abelsk grupp (= en ändligt genererad $\mathbb{Z}$-modul) då ger (8.8) uppdelningen $G = G_t \oplus F$, där G_t är torsionsdelmodulen till G och F är en fri $\mathbb{Z}$-modul (en direkt summa av oändliga cykliska grupper). Enligt (8.14) är G_t en direkt summa av ändliga cykliska grupper $\mathbb{Z}/(p^k)$ vars ordningar är entydigt bestämda potenser av primtal. Alltså har vi följande resultat:

(8.15) Sats. *Låt G vara en ändligt genererad abelsk grupp. Då är G en direkt summa av cykliska grupper vars ordningar är primtalspotenser och oändliga cykliska grupper (om G är oändlig) dvs*

$$G \cong \mathbb{Z}/(p_1^{k_1}) \oplus \cdots \oplus \mathbb{Z}/(p_m^{k_m}) \oplus \mathbb{Z}^s,$$

där p_i är primtal (som inte behöver vara olika). Ordningarna $p_i^{k_i}$ av de ändliga cykliska grupperna samt antalet s av oändliga cykliska grupper i framställningen av G är entydigt bestämda.

Nu skall vi diskutera kanoniska former av linjära avbildningar – rationella former och Jordans normalform.

Låt K vara en kropp och låt $\varphi : V \to V$ vara en linjär avbildning. Låt oss påminna om att V kan betraktas som $K[X]$-modul då man definierar $K[X] \times V \to V$ genom $(p(X), v) \mapsto p(\varphi)(v)$ för ett godtyckligt polynom $p \in K[X]$. Rent formellt får vi den strukturen på följande sätt:

V är en modul över ringen $\mathrm{End}_K(V)$ då $(\varphi, v) \mapsto \varphi(v)$ (se också Övn. 3.2). Man har en ringhomomorfism:

$$\Phi : K[X] \longrightarrow \mathrm{End}_K(V)$$

sådan att $\Phi(p(X)) = p(\varphi)$. Nu är som vanligt varje $\mathrm{End}_K(V)$-modul en $K[X]$-modul då verkan av $K[X]$ förmedlas av Φ (om $\Phi : R \to R'$ är en ringhomomorfism och M' är en R'-modul så är M' en R-modul då $rm' = \Phi(r)m$ för $m' \in M'$). Om V är ett ändligt dimensionellt vektorrum över K, så är V en ändligt genererad $K[X]$-modul och vi kan tillämpa på V vår allmänna teori för moduler över huvudidealområden (här $R = K[X]$). Låt oss sammanfatta våra observationer:

(8.16) Proposition. *Låt K vara en kropp och låt $\varphi : V \to V$ vara en linjär avbildning av ett ändligt dimensionellt vektorrum V över K. Då är V en ändligt genererad torsionsmodul över $K[X]$ om man definierar $p(X)v = p(\varphi)(v)$ för $p \in K[X]$ och $v \in V$. Om*

$$\Phi : K[X] \to \mathrm{End}_K(V),$$

där $\Phi(p(X)) = p(\varphi)$, så är $Ker\,\Phi = \mathrm{Ann}_{K[X]}(V)$.

Bevis. $\dim_K \mathrm{End}_K(V) = n^2$, där $n = \dim_K V$. Alltså är $id, \varphi, \ldots, \varphi^{n^2}$ linjärt beroende över K ty deras antal är större än dimensionen. Detta visar att det finns ett icke-trivialt polynom $p \in K[X]$ så att $p(\varphi) = 0$ dvs $p(X) \in \mathrm{Ann}_{K[X]}(V)$. Alltså är V en torsionsmodul. Det är klart att $\mathrm{Ker}\Phi = \mathrm{Ann}_{K[X]}(V)$ (se (8.7)). □

(8.17) Definition. Med **minimalpolynomet** av $\varphi : V \to V$ menas ett polynom $p \in K[X]$ av lägsta möjliga grad med högsta koefficienten 1 sådant att $p(\varphi) = 0$. Med andra ord, p är en generator av $\mathrm{Ann}_{K[X]}(V)$ och har högsta koefficienten 1.

□

Enligt (8.14) och (8.16) är

$$V \cong K[X]/(p_1^{k_1}) \oplus \cdots \oplus K[X]/(p_r^{k_r}), \tag{8.18}$$

där p_i är irreducibla faktorer av minimalpolynomet för $\varphi : V \to V$ (så att $(p_i) \supseteq \mathrm{Ann}_{K[X]}(V)$) och k_i är entydigt definierade av V. Observera att p_i i (8.18) behöver inte vara olika. En sådan framställning kan användas för att välja en bas för V i vilken φ har en "okomplicerad" matris. Rent allmänt är modulerna i (8.18) av typen

$$K[X]/(p),$$

där $p = a_0 + a_1X + \cdots + a_{k-1}X^{k-1} + X^k$ (p ej nödvändigt irreducibelt). Avbildningen $\varphi : V \to V$ bestäms till höger i (8.18) av multiplikation med X ty $Xv = \varphi(v)$. Låt oss som

bas i $K[X]/(p)$ välja alla monom $1, x, \ldots, x^{k-1}$, där x betecknar restklassen av X. Då är matrisen för multiplikation med X (dvs för φ) given av:

$$\begin{array}{llllll} \varphi(1) & = x \cdot 1 & = & x & & \\ \varphi(x) & = x \cdot x & = & & x^2 & \\ \ldots & \ldots & & & & \\ \varphi(x^{k-2}) & = x \cdot x^{k-2} & = & & & x^{k-1} \\ \varphi(x^{k-1}) & = x \cdot x^{k-1} & = -a_0 & -a_1 x & -a_2 x^2 - & \cdots - a_{k-1} x^{k-1} \end{array}$$

dvs matrisen för φ i denna bas är:

(8.19)
$$M_p = \begin{bmatrix} 0 & 0 & 0 & \ldots & -a_0 \\ 1 & 0 & 0 & \ldots & -a_1 \\ 0 & 1 & 0 & \ldots & -a_2 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & -a_{k-1} \end{bmatrix}$$

(8.20) Proposition. *Om φ är en linjär avbildning av ett vektorrum V över en kropp K så existerar en bas för V över K sådan att matrisen för φ är uppbyggt av block av typen* (8.19) *dvs*

$$M_\varphi = \begin{bmatrix} M_{p_1} & & & \\ & M_{p_2} & & 0 \\ & & \ddots & \\ 0 & & & M_{p_k} \end{bmatrix}$$

Antalet block och deras storlek bestäms av uppdelningen (8.18)*.*

Bevis. Man väljer en bas för varje term i summan (8.18) i enlighet med diskussionen ovan då $p = p_i^{k_i}$ för $i = 1, \ldots, r$. Matrisen för φ i den bas som består av alla baser för termerna har den önskade formen. □

Den form av matriser för linjära avbildningar som ges i (8.20) kallas **rationell normalform** eller **Frobenius**[††] **normalform**. Varje linjär avbildning av ett ändligt dimensionellt rum över en godtycklig kropp har en sådan form i en lämplig bas. Vårt nästa resultat ger en ännu enklare form, men under mera restriktiva förutsättningar.

(8.21) Jordans normalform. Antag nu att kroppen K är algebraiskt sluten. T ex kan vi anta att $K = \mathbb{C}$, men våra resultat gäller under betydligt mildare förutsättningar (se vidare (8.25)). Uppdelningen (8.18) har nu formen:

[††]G. Frobenius (1849 – 1917), framstående tysk matematiker

$$V \cong K[X]/(X-\lambda_1)^{k_1} \oplus \cdots \oplus K[X]/(X-\lambda_r)^{k_r}, \tag{8.22}$$

därför att irreducibla polynom i $K[X]$ har grad 1. Som tidigare vill vi välja en bas för varje term i direkta summan till höger och därefter konstruera en bas för V. Betrakta en av termerna

$$K[X]/(X-\lambda)^k.$$

I stället för basen $1, x, \ldots, x^{k-1}$ väljer vi nu $1, x-\lambda, \ldots, (x-\lambda)^{k-1}$. I denna bas är

$$\begin{array}{llll}
\varphi(1) & = x\cdot 1 & = \lambda + & (x-\lambda) \\
\varphi(x-\lambda) & = x(x-\lambda) & = & \lambda(x-\lambda) + (x-\lambda)^2 \\
\ldots\ldots & & & \\
\varphi((x-\lambda)^{k-2}) & = x(x-\lambda)^{k-2} & = & \lambda(x-\lambda)^{k-2} + (x-\lambda)^{k-1} \\
\varphi((x-\lambda)^{k-1}) & = x(x-\lambda)^{k-1} & = & \lambda(x-\lambda)^{k-1}
\end{array}$$

(man utnyttjar här likheterna $x = x-\lambda+\lambda$ och $(x-\lambda)^k = 0$) dvs matrisen för φ är:

$$M_{\lambda,k} = \begin{bmatrix} \lambda & 0 & \ldots & 0 & 0 \\ 1 & \lambda & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & \lambda & 0 \\ 0 & 0 & \ldots & 1 & \lambda \end{bmatrix} \tag{8.23}$$

Nu kan vi bilda en bas för V som består av alla baser för termerna $K[X]/(X-\lambda_i)^{k_i}$ i (8.22). Alltså får vi

(8.24) Sats. *Om φ är en linjär avbildning av ett vektorrum V över en algebraiskt sluten kropp K så existerar en bas för V över K sådan att matrisen för φ är uppbyggt av block av typen* (8.23) *dvs*

$$M_\varphi = \begin{bmatrix} M_{\lambda_1,k_1} & & & \\ & M_{\lambda_2,k_2} & & 0 \\ & & \ddots & \\ 0 & & & M_{\lambda_r,k_r} \end{bmatrix}$$

Antalet block och deras storlek bestäms av uppdelningen (8.22) *och λ_i är egenvärdena till φ.*

Bevis. Existensen av basen för V med önskade egenskaper följer ur diskussionen ovan. Det faktum att λ_i är egenvärden till φ är klart ty $\det(M_\varphi - XE) = 0$ har som sina lösningar just λ_i (E betecknar en lämplig enhetsmatris). □

(8.25) Anmärkning. Samma resultat gäller då kroppen K är sådan att alla polynom p_i har grad 1, vilket betyder att alla egenvärden till φ ligger i K.

□

ÖVNINGAR

8.1. En kvadratisk matris P med element ur R kallas **unimodulär** om $\det P \in R^*$. Man säger att två $(m \times n)$-matriser A och A' är **ekvivalenta** över R om det finns två unimodulära matriser P och Q sådana att $A' = PAQ$. En största gemensam delare till determinanter av alla $(r \times r)$-delmatriser till A, där $r \leq \min(m, n)$, (om det finns sådana $\neq 0$), kallas **r:te determinantfaktorn** till A. Vi skall beteckna en sådan delare med $D_r(A)$. $D_r(A)$ är definierad så när som på en enhet i R (dvs så när som på associering).

(a) Visa att varje $(m \times n)$-matris A med element ur en Euklidisk ring R är ekvivalent med en matris

$$(*) \qquad \begin{bmatrix} d_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix},$$

där $d_j \in R$ och $d_1 | \dots | d_r \neq 0$. Om A samtidigt är ekvivalent med

$$(*) \qquad \begin{bmatrix} d'_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & d'_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \dots & d'_{r'} & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix},$$

där $d'_j \in R$ och $d'_1 | \dots | d'_{r'} \neq 0$, så är $r = r'$ och d_i är associerat med d'_i (dvs $(d_i) = (d'_i)$ för $i = 1, \dots, r$).

Ledning. Låt F_0 vara delmodulen till $F = R^n$ som generas av raderna i A. Utnyttja beviset av (8.1)(a) för att visa existensen av $(*)$, och (8.1)(c) för att visa entydigheten (så när som på associering). Matrisen $(*)$ kallas ibland för **Smiths normalform** av A.

(b) Visa att två $(m \times n)$-matriser med element ur R är ekvivalenta över R då och endast då deras motsvarande determinantfaktorer är associerade.

Ledning. Observera att determinantfaktorerna för $(*)$ är $D_1 = d_1, D_2 = d_1 d_2, \dots, D_r = d_1 d_2 \cdots d_r$. För att visa att ekvivalenta matriser har associerade determinantfaktorer kan man behöva följande sats av Cauchy-Binet. För en godtycklig $(m \times n)$-matris X och $1 \leq i_1 < \dots < i_k \leq m$, $1 \leq j_1 < \dots < j_k \leq n$ betecknar vi med

$$X^{i_1, \dots, i_k}_{j_1, \dots, j_k}$$

den delmatris av X som består av elementen i raderna $i_1, \dots, i_k$ och kolonnerna $j_1, \dots, j_k$. Låt A vara en $(p \times q)$-matris och B en $(q \times r)$-matris. Låt vidare $C = AB$. Då gäller

likheten

$$\det C^{i_1,\dots,i_k}_{j_1,\dots,j_k} = \sum_{s_1,\dots,s_k} \det A^{i_1,\dots,i_k}_{s_1,\dots,s_k} \det B^{s_1,\dots,s_k}_{j_1,\dots,j_k},$$

där summationen sker över alla $1 \le s_1 < \dots < s_k \le q$. Om $A' = PAQ$ så visar Cauchy-Binet sats att $D_k(A)|D_k(PA)|D_k(PAQ) = D_k(A')$. Likheten $P^{-1}A'Q^{-1} = A$ ger $D_k(A')|D_k(A)$.

Anmärkning. $d_1, d_2, \dots, d_r$ (eller idealen $(d_1) \supseteq (d_2) \supseteq \dots \supseteq (d_r)$) kallas för **invariantfaktorerna** av A. Det följer direkt ur första meningen i ledningen att determinantfaktorerna bestämmer invariantfaktorerna och omvänt. Resultaten i denna övning gäller över godtyckliga huvudidealringar, men bevisen är litet mera komplicerade än för euklidiska ringar.

8.2. Bestäm Smiths normalform för $A - XE$ över $\mathbb{C}[X]$ och Jordans normalform av A för följande matriser A:

(a) $\begin{bmatrix} 0 & -3 & -5 \\ 3 & 6 & 7 \\ -1 & -1 & 0 \end{bmatrix}$, (b) $\begin{bmatrix} 4 & 3 & 4 \\ -1 & 2 & 1 \\ 0 & -1 & 0 \end{bmatrix}$,

(c) $\begin{bmatrix} 1 & 3 & 3 & 3 \\ 0 & -3 & -4 & -4 \\ 0 & 8 & 9 & 8 \\ 0 & -4 & -4 & -3 \end{bmatrix}$, (d) $\begin{bmatrix} 12 & 0 & -3 & 2 \\ -18 & 1 & 5 & -3 \\ 33 & -1 & -9 & 5 \\ -15 & 1 & 5 & -1 \end{bmatrix}$.

8.3. Låt A vara en $(m \times n)$-matris med element ur ett huvudidealområde R. Om d_i för $i = 1, \dots r$ är invariantfaktorer till A (se Övn. 1) och

$$d_i = p_1^{k_{i1}} \dots p_s^{k_{is}},$$

där p_j för $j = 1, \dots s$ är irreducibla element i R så kallas $p_j^{k_{ij}}$ med $k_{ij} > 0$ för **elementära delare** till A. Det är klart att elementära delare till A bestäms entydigt (så när som på associering) av determinantfaktorerna (och invariantfaktorerna) till A.

(a) Låt A och B vara två matriser med element ur R. Visa att de elementära delarna till matrisen

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

är alla elementära delare till A och alla elementära delare till B.

Ledning. Låt F_0 vara den delmodul till $F = R^n$ som genereras av matrisens A rader. Representera modulen F/F_0 som direkt summa av cykliska moduler i enlighet med (8.14). Identifiera de elementära delarna till A med annulatorerna till dessa cykliska moduler. Gör samma sak med matrisen B. Utnyttja entydigheten i (8.14).

(b) Beräkna determinantfaktorerna, invariantfaktorerna och elementära delare till $M_{\lambda,k} - XE$ då

$$M_{\lambda,k} = \begin{bmatrix} \lambda & 0 & \dots & 0 & 0 \\ 1 & \lambda & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & \lambda & 0 \\ 0 & 0 & \dots & 1 & \lambda \end{bmatrix}$$

är Jordans cell. Gör liknande beräkningar för $A - XE$ då A är en godtycklig matris i Jordans normalform som i (8.24). Motivera att de elementära delarna till $A - XE$ bestämmer den matrisen (och således A) entydigt så när som på Jordans celler ordningsföljd.

8.4. Låt A och B vara $(n \times n)$-matriser med element ur en oändlig kropp K. Visa att A och B är konjugerade över K (dvs det finns en icke-singulär matris P sådan att $B = P^{-1}AP$) då och endast då motsvarande karakteristiska matriserna $A - XE$ och $B - XE$ är ekvivalenta som matriser över $K[X]$ (E är $(n \times n)$-enhetsmatrisen).

8.5. Bestäm Smiths normalform över $\mathbb{Z}$ för matriserna i Övn. 2.

8.6. Låt K vara en kropp med en involution $x \mapsto \bar{x}$ ($\bar{x} = x$ för varje x är möjligt). Låt $T : V \times V \to K$ vara en hermitsk avbildning m a p den givna involutionen. Låt $f : V \to V$ vara en linjär avbildning. Man säger att **spektralegenskapen** gäller för (T, f) om det finns en ortogonalbas för (V, T) bestående av egenvektorer till f. Antag att alla egenvärden till f tillhör K (t.ex. är $\mathbb{C}$ algebraiskt sluten). Visa:

(a) **Spektralsatsen för symmetriska avbildningar.** Om $K = \mathbb{R}$, $\bar{x} = x$, då $x \in \mathbb{R}, T$ är positivt definit och f är symmetrisk (dvs $T(f(x), y) = T(x, f(y))$ så har (T, f) spektralegenskapen.

(b) **Spektralsatsen för hermitska avbildningar.** Om $K = \mathbb{C}$, $x \mapsto \bar{x}$ är konjugeringen, T är positivt definit och f är hermitsk (dvs $T(f(x), y) = T(x, f(y))$ så har (T, f) spektralegenskapen.

(c) **Spektralsatsen för normala avbildningar.** Om $K = \mathbb{C}$, $x \mapsto \bar{x}$ är konjugeringen, och T är positivt definit så har paret (T, f) spektralegenskapen då och endast då $ff^* = f^*f$ där $T(f(x), y) = T(x, f^*(y))$ för varje $x, y \in V$ (se Övn. 6.5). (f med egenskapen $ff^* = f^*f$ kallas **normal**).

Ledning. "⇒" Om $f(\alpha_k) = (a_k + ib_k)\alpha_k$, definiera $f_1(\alpha_k) = a_k\alpha_k$, $f_2(\alpha_k) = b_k\alpha_k$. Kontrollera att $f^* = f_1 - if_2$.

"⇐" Först visar vi att om $f, g : V \to V$ och $fg = gf$, där V är ett vektorrum över $\mathbb{C}$ så existerar en egenvektor v gemensam för både f och g.

Lösning. Låt v_0 vara en egenvektor till f och låt λ vara motsvarande egenvärde (v_0 finns ty $\mathbb{C}$ är algebraiskt sluten). Låt $V_\lambda = \{v \in V : f(v) = \lambda v\}$. V_λ är ett delrum till V. Om $u \in V_\lambda$ så är $f(g(u)) = g(f(u)) = g(\lambda u) = \lambda g(u)$. Alltså är g är en linjär avbildning av V_λ så att det finns en egenvektor v till g i V_λ. Då är v både en egenvektor till f och g.

Nu visar vi "⇐" induktivt m.a.p. $\dim V$. Om $\dim V = 1$ så är allt klart. Antag att $\dim V > 1$ och välj en egenvektor e_1 till både f och f^*. Låt $W = \mathbb{C}e_1$. Betrakta $W^\perp = \{\boldsymbol{x} \in V : T(\boldsymbol{x}, e_1) = 0\}$. $W^\perp$ är ett delrum till V som är invariant med avseende på både f och f^*:

$$\boldsymbol{x} \in W^\perp \Rightarrow T(f(\boldsymbol{x}), e_1) = T(\boldsymbol{x}, f^*(e_1)) = T(\boldsymbol{x}, \lambda_1 e_1) = 0 \Rightarrow f(\boldsymbol{x}) \in W^\perp$$

På samma sätt får man att $f^*(\boldsymbol{x}) \in W^\perp$. Men $\dim W^\perp = \dim V - 1$ så att $W^\perp$ har en bas $e_1, \ldots e_n$ bestående av egenvektor till f (och f^*) sådan att $T(e_i, e_j) = 0$ då $i \neq j$, $2 \leq i, j \leq n$. Alltså bildar $e_1, \ldots, e_n$ en önskad bas.

Observera att (c) ger ett bevis av (b) (och även (a) om man tar $K = \mathbb{R}$ och $\bar{x} = x$).

8.7. Låt $\varphi : V \to V$ vara en linjär avbildning, där V är ett vektorrum över en kropp som innehåller alla egenvärden till φ. Visa att det finns en bas i vilken matrisen för φ är diagonal då och endast då minimalpolynomet för φ saknar multipla nollställen.

8.8. (a) Låt $\varphi : V \to V$ vara en linjär avbildning, där V är ett vektorrum över en kropp K. Låt $V \cong K[X]/(q_1) \oplus \ldots \oplus K[X]/(q_r)$, där $q_1 | \ldots | q_r$. Visa att minimalpolynomet för φ är lika med q_r, och karakteristiska polynomet för φ, dvs $P_\varphi(X) = \det(\varphi - XE)$, är lika med $q_1 \cdots q_r$.

Ledning. Börja med $V \cong K[X]/(q)$ och utnyttja den rationella normalformen för φ (se (8.20)).

(b) Utnyttja det faktum att minimalpolynomet för φ är en delare till karakteristiska polynomet för att visa Cayley-Hamiltons sats: Om $P_\varphi(X)$ är karakteristiska polynomet för φ så är $P_\varphi(\varphi) = 0$ (med andra ord är $P_\varphi(A) = 0$, där A är matrisen för φ i en bas för V över K).

(c) Ge ett direkt bevis av Cayley-Hamiltons sats i enlighet med följande idéer: Låt $e_1, \ldots, e_n$ vara en bas för V över K. Låt $\varphi(e_i) = \sum a_{ij} e_j$. Betrakta V som $K[X]$-modul och motivera att $\sum (a_{ij} - \delta_{ij} X) e_j = 0$ i V (δ_{ij} är Kroneckers δ dvs $\delta_{ij} = 0$ om $i \neq j$ och $\delta_{ii} = 1$). Utnyttja determinant enligt övning 5.5.

Kapitel 9

KORT OM GRUPPREPRESENTATIONER

Linjära grupprepresentationer har många viktiga tillämpningar. De ger en beskrivning av gruppelementen med hjälp av matriser och skapar därmed en effektiv möjlighet att studera gruppstrukturen. I de fall då en grupp verkar på ett rum, kan gruppens representationer ge nyttiga upplysningar om rummets egenskaper. Texten som följer ger en mycket kort introduktion till grupprepresentationer. Vi begränsar oss till några enkla satser om matrisrepresentationer av ändliga grupper och exemplifierar dessa satser genom att beskriva alla icke-ekvivalenta representationer i några specialfall.

För enkelhets skull förutsätter vi att alla kroppar, över vilka man representerar grupper med hjälp av matriser, är talkroppar, dvs delkroppar till kroppen av de komplexa talen $\mathbb{C}$. Varje gång då vi säger att K är en kropp menar vi alltså att $K \subseteq \mathbb{C}$. Kroppen av de reella talen betecknas här med $\mathbb{R}$. Med $GL_n(K)$ betecknas gruppen av alla inverterbara $n \times n$ – matriser med element ur K. Om A är en sådan matris så betecknar A^t dess transponat.

Definitioner och exempel.

Låt K vara en kropp och låt V vara ett n-dimensionellt vektorrum över K ($n \geq 1$). Vi skall beteckna med $GL(V)$ alla inverterbara linjära avbildningar $\varphi : V \to V$. $GL(V)$ är en grupp med avseende på sammansättning av funktioner. Låt G vara en grupp.

(9.1) Definition. Med en (linjär) representation av G över K menar man en godtycklig grupphomomorfism

$$T : G \longrightarrow GL(V).$$

Dimensionen av V över K kallar man för dimensionen av representationen T.

□

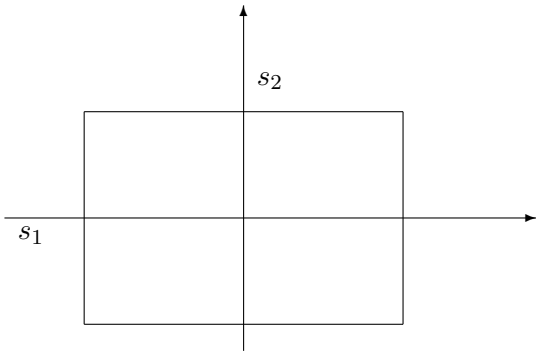
Definitionen säger att för varje $g \in G$ är $T(g) : V \to V$ en inverterbar linjär avbildning och

$$T(g_1 g_2) = T(g_1)T(g_2)$$

då $g_1, g_2 \in G$. Observera att $T(g^{-1}) = T(g)^{-1}$ och $T(e) = I$, där e är det neutrala elementet i G och I den identiska avbildningen av V (dvs det neutrala elementet i $GL(V)$).

Låt oss betrakta några exempel.

(9.2) Exempel. (a) Låt G vara symmetrigruppen för en rektangel:



G består av identiteten I, två speglingar s_1 och s_2 i axlarna x och y samt vridningen v vinkeln 180°. Om $V = \mathbb{R}^2$ så har man en representation

$$T : G \longrightarrow GL(\mathbb{R}^2)$$

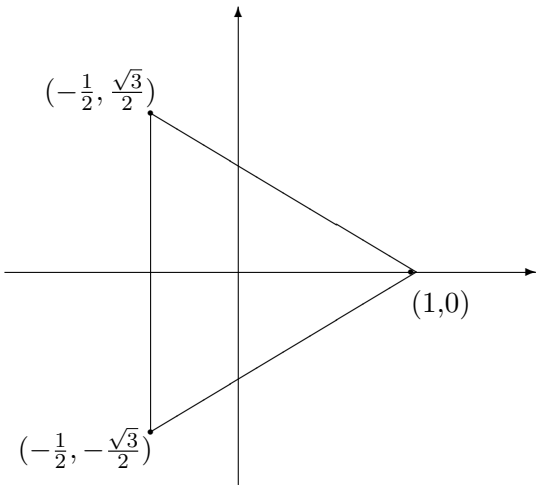
som mot varje gruppelement g ordnar motsvarande transformation av planet $\mathbb{R}^2$. För att beskriva dessa avbildningar med hjälp av matriser låt oss välja standardbasen $e_1^t = (1, 0)$, $e_2^t = (0, 1)$. I denna bas har vi

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad s_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad s_2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad v = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

(b) På liknande sätt kan man beskriva symmetrigrupper för andra månghörningar t ex symmetrigruppen för en liksidig triangel eller symmetrigruppen för en kvadrat. Låt oss göra det

för en liksidig triangel. Gruppen $G = D_3$ består av alla kongruensavbildningar av planet som bevarar en liksidig triangel. Det finns 6 sådana kongruensavbildningar – 3 vridningar och 3 speglingar. Genom att välja $V = \mathbb{R}^2$ får vi en gruppprepresentation

$$T : D_3 \to GL(\mathbb{R}^2).$$



Låt oss i planet $\mathbb{R}^2$ fixera standardbasen som i (a) och uttrycka dessa avbildningar som matriser med avseende på denna bas:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad v_1 = \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix},$$

$$s_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad s_2 = \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{bmatrix}, \quad s_3 = \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix}.$$

(c) Låt G vara en godtycklig ändlig grupp av ordning $|G| = n$. G har en så kallad **reguljär representation** i vektorrummet $V = K^n$ över en godtycklig kropp K. Denna representation definieras på följande sätt: Låt $G = \{g_1, \ldots, g_n\}$, där $g_1 = e$ är det neutrala elementet. Låt $e_{g_i} = (0, \ldots, 1, \ldots, 0)$ med 1 på i :te platsen. Definiera

$$T : G \longrightarrow GL(K^n)$$

genom $T(g)(e_{g_i}) = e_{gg_i}$. Man kontrollerar lätt att

$$T(gg')(e_{g_i}) = e_{gg'g_i} = T(g)(e_{g'g_i}) = T(g)(T(g')(e_{g_i})) = T(g)T(g')(e_{g_i}),$$

dvs $T(gg') = T(g)T(g')$.

□

Det finns två andra begrepp som är ekvivalenta med begreppet linjär representation och som ofta är mycket användbara. Låt oss introducera dessa begrepp: matrisrepresentationer av G och G-moduler.

(9.3) Matrisrepresentationer. Låt $T : G \to GL(V)$ vara en gruppprepresentation. Om man väljer en bas $\mathbf{b} = (b_1, \ldots, b_n)$ för V över K så ger varje $T(g)$ motsvarande matris $T_{\mathbf{b}}(g) = [a_{ij}(g)]$, där

$$T(g)(b_i) = \sum a_{ji}(g)b_j.$$

Avbildningen $g \mapsto T_{\mathbf{b}}(g) = [a_{ij}(g)]$ är en grupphomomorphism:

$$T_{\mathbf{b}} : G \longrightarrow GL_n(K).$$

Rent allmänt säger man att en **matrisrepresentation** av G över K är en grupphomomorfism

$$T : G \to GL_n(K). \tag{9.4}$$

som mot $g \in G$ ordnar en matris $T(g)$. Ibland kommer vi att skriva $[T(g)]$ för att understrycka att bilden av g är en matris.

Det finns inte någon väsentlig skillnad mellan begreppen linjär gruppprepresentation i definitionen (9.1) och matrisrepresentationen i (9.4). Om en matrisrepresentation (9.4) är given så har man en linjär gruppprepresentation (som vi betecknar med samma bokstav T):

$$T : G \longrightarrow GL(K^n),$$

där $T(g)$ är den linjära avbildning som i standardbasen $e_1^t = (1, 0, \ldots, 0)$,..., $e_n^t = (0, 0, \ldots, 1)$ ges av likheten

$$T(g)(e_i) = [T(g)]e_i.$$

I fortsättningen kommer vi att fritt växla mellan $T : G \to GL(K^n)$ och $T : G \to GL_n(K)$, men definitionen (1.1) har en stor fördel som vi kommer att utnyttja ganska ofta – den är koordinatfri dvs den är inte beroende av basvalet för K^n över K.

(9.5) Moduler. Man kan också tolka gruppprepresentationer som G-**moduler** – ett begrepp som endast oväsentligt skiljer sig från begreppet modul över gruppringen $K[G]$ av G över K. Gruppringar definierade vi i Kapitel 2 (se (2.2) (h)). Först definierar vi begreppet G–modul över K och därefter förklarar sambandet med $K[G]$–moduler. Med en G-**modul** V över K menar man ett vektorrum V över K sådant att det finns en funktion

$$G \times V \longrightarrow V$$

som mot $(g, v) \in G \times V$ ordnar $gv \in V$ så att

$$\begin{array}{rcl} (g_1g_2)v & = & g_1(g_2v), \\ ev & = & v, \\ g(v_1 + v_2) & = & gv_1 + gv_2, \\ g(av) & = & a(gv) \end{array} \tag{9.6}$$

för godtyckliga $g, g_1, g_2 \in G$, $v, v_1, v_2 \in V$ och $a \in K$. Det är klart att varje representation $T : G \to GL(V)$ förvandlar V till en G-modul då man definierar

$$gv = T(g)(v)$$

(kontrollera likheterna (9.6) som en övning). Omvänt definierar en G-modul V en linjär representation $T : G \to GL(V)$ så att

$$T(g)(v) = gv.$$

Då är $T(g)$ en linjär avbildning ty

$$T(g)(v_1 + v_2) = g(v_1 + v_2) = gv_1 + gv_2 = T(g)(v_1) + T(g)(v_2)$$

och

$$T(g)(av) = g(av) = a(gv) = aT(g)(v).$$

Dessutom är

$$T(g_1g_2)(v) = (g_1g_2)v = g_1(g_2v) = T(g_1)(g_2v) = T(g_1)(T(g_2)(v)) = T(g_1)T(g_2)(v)$$

så att $T(g_1g_2) = T(g_1)T(g_2)$. $T(g)$ har som invers $T(g^{-1})$ ty

$$(T(g)T(g^{-1})(v) = T(gg^{-1})(v) = T(e)(v) = v,$$

dvs $T(g)T(g^{-1}) = I$.

Sambandet mellan G–moduler över K och $K[G]$–moduler är mycket enkelt – varje G–modul V över K är en $K[G]$–modul och omvänt. Låt oss först påminna om att elementen i $K[G]$ är alla summor $\sum_{g\in G} a_g g$, där $a_g \in K$. Dessa summor adderas och multipliceras på ett naturligt sätt (se (2.2) (h)). Om V är en G–modul så är V en $K[G]$–modul om för $x = \sum a_g g \in K[G]$ är $xv = \sum a_g gv$. Omvänt om V är en $K[G]$–modul så är det klart att produkter gv är definierade för varje $g \in G$ och $v \in V$ eftersom $g \in K[G]$.

□

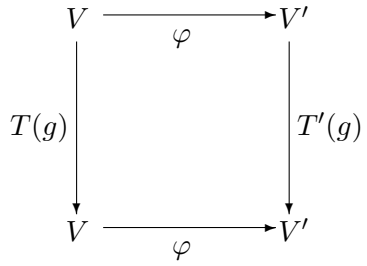
Irreducibla representationer.

En och samma grupp kan ha flera olika representationer. En av våra huvuduppgifter är att kunna hitta alla representationer och klassificera dessa. För att genomföra den uppgiften är det nödvändigt att precisera vad man menar med olika representationer.

(9.7) Definition. Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara två representationer i vektorrum över samma kropp K. Man säger att T och T' är isomorfa (eller ekvivalenta) om det finns en isomorfism $\varphi : V \to V'$ sådan att $T'(g)\varphi = \varphi T(g)$ för varje $g \in G$.

□

Man kan uttrycka definitionen i form av ett kommuterande diagram:



Det är intresant och viktigt att formulera isomorfismbegreppet i termer av matrisrepresentationer och moduler. Låt oss göra det i bägge fallen.

(9.8) Isomorfism av matrisrepresentationer. Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara två isomorfa representationer och låt $\varphi : V \to V'$ definiera deras isomorfism. Låt $e_1, \ldots, e_n$ vara en bas för V över K och $e'_1, \ldots, e'_n$ en bas för V' över K. Om matrisen för φ med avseende på dessa baser är $B = [b_{ij}]$ dvs

$$\varphi(e_i) = \sum_j b_{ji} e'_j$$

och $[a_{ij}(g)]$ är matrisen för $T(g)$ i basen $e_1, \ldots, e_n$ samt $[a'_{ij}(g)]$ är matrisen för $T'(g)$ i basen $e'_1, \ldots, e'_n$ så ger diagrammet ovan det välbekanta sambandet

$$[a'_{ij}(g)]B = B[a_{ij}(g)],$$

dvs

$$[a'_{ij}(g)] = B[a_{ij}(g)]B^{-1}.$$

Om två matrisrepresentationer skiljer sig på detta sätt så kallas de också för isomorfa (eller ekvivalenta).

(9.9) Isomorfism av moduler. Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara isomorfa representationer av G. Då är V och V' G-moduler enligt (9.5). Det faktum att $\varphi : V \to V'$ är en isomorfism mellan dessa representationer betyder att $\varphi(gv) = g\varphi(v)$ för varje $g \in G$ och $v \in V$. Detta innebär helt enkelt att $K[G]$ moduler V och V' (se (9.5)) är isomorfa.

Låt oss observera att man, mera allmänt, kan betrakta linjära avbildningar $\varphi : V \to V'$ av G-moduler sådana att $\varphi(gv) = g\varphi(v)$ för varje $g \in G$ och $v \in V$. Man säger då att φ är

en **homomorfism** av G-moduler, vilket helt naturligt är en homomorfism av $K[G]$–moduler $\varphi : V \to V'$.

Följande resultat är mycket enkelt att bevisa och egentligen är ett specialfall av (3.10):

(9.10) Proposition. *Låt $\varphi : V \to V'$ vara en homomorfism av G-moduler. Då är kärnan*

$$\operatorname{Ker}\varphi = \{v \in V : \varphi(v) = 0\}$$

en G-delmodul till V, och bilden

$$\operatorname{Im}\varphi = \{v' \in V' : \exists_{v \in V} v' = \varphi(v)\}$$

en G-delmodul till V'.

Bevis. $\varphi(v) = 0$ ger att $\varphi(gv) = g\varphi(v) = 0$, dvs $v \in \operatorname{Ker}\varphi$ ger $gv \in \operatorname{Ker}\varphi$. $v' = \varphi(v)$ ger $gv' = \varphi(gv)$, dvs $v' \in \operatorname{Im}\varphi$ ger $gv' \in \operatorname{Im}\varphi$. □

Vanligen vill man hitta alla icke-isomorfa (dvs ej ekvivalenta) gruppprepresentationer. Den uppgiften är inte så enkel. Först och främst vill man hitta de enklaste representationerna. Med sådana menar man **irreducibla representationer**.

(9.11) Definition. Man säger att en gruppprepresentation $T : G \to GL(V)$ är **reducibel** om det finns ett äkta delrum W till V (dvs $W \neq (0), V$) sådant att $T(g)(W) \subseteq W$ för varje $g \in G$. Man säger då att W är ett T-**invariant** (eller G-**invariant**) delrum till V. I sådant fall har man en representation $T' : G \to GL(W)$, där $T'(g)(w) = T(g)(w)$ för $w \in W$. T' kallas då en **delrepresentation** till T. En representation som inte är reducibel kallas **irreducibel**.

□

(9.12) Exempel. (a) Betrakta representationen i (9.2) (a). Man ser direkt att delrummen $\mathbb{R}e_1$ och $\mathbb{R}e_2$ är G-invarianta så att representationen är reducibel.

(b) Representationen ur (9.2) (b) är irreducibel. Antag nämligen att det finns ett G-invariant delrum W till V sådant att $(0) \subset W \subset V$. Man har dim $W = 1$ ty dim $V = 2$. Alltså är $W = \mathbb{R}e$ för någon vektor e som måste vara en gemensam egenvektor till alla 6 matriser i G. En mycket enkel räkning visar att det inte finns någon sådan vektor (räkna egenvektorer till t ex v_1 och s_1 !).

□

Som tidigare begrepp, låt oss uttrycka reducibiliteten i termer av matrisrepresentationer och moduler.

(9.13) Reducibla och irreducibla matrisrepresentationer. Låt $T : G \to GL(V)$ vara en representation och låt W vara ett T-invariant delrum till V. Låt oss välja en bas $e_1, \ldots, e_n$ för V över K så att $e_1, \ldots, e_r$ bildar en bas för W över K. De matriser $A(g) = [a_{ij}(g)]$ som svarar mot $T(g)$ i basen $e_1, \ldots, e_n$ har då följande form

$$A(g) = \begin{bmatrix} a_{11}(g) & \ldots & a_{1r}(g) & * & \ldots & * \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{r1}(g) & \ldots & a_{rr}(g) & * & \ldots & * \\ 0 & \ldots & 0 & * & \ldots & * \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & * & \ldots & * \end{bmatrix}.$$

Ibland har man två T-invarianta delrum W_1 och W_2 till V sådana att $V = W_1 \oplus W_2$ är en **direkt summa**, dvs varje vektor $v \in V$ kan skrivas entydigt som summa $v = w_1 + w_2$, där $w_1 \in W_1$ och $w_2 \in W_2$. Om representationen T säger man också att den är en **direkt summa** av sina delrepresentationer motsvarande W_1 och W_2. I detta fall får man matriser:

$$A(g) = \begin{bmatrix} a_{11}(g) & \ldots & a_{1r}(g) & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{r1}(g) & \ldots & a_{rr}(g) & 0 & \ldots & 0 \\ 0 & \ldots & 0 & a_{r+1\,r+1}(g) & \ldots & a_{r+1\,n}(g) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_{n\,r+1}(g) & \ldots & a_{nn}(g) \end{bmatrix}$$

om man väljer som bas för V en bas bestående av basvektorer för W_1 och W_2.

(9.14) Reducibla och irreducibla moduler. Låt oss uttrycka reducibiliteten i termer av G-moduler. Om $T : G \to GL(V)$ är reducibel och W är ett delrum till V sådant att $T(g)(W) \subseteq W$ så är det klart att W är en G-delmodul till G-modulen V (ty $gw = T(g)(w) \in W$ för varje $g \in G$ och $w \in W$). Alltså är V irreducibelt precis då V saknar äkta G-delmoduler (eller $K[G]$–delmoduler), dvs delmoduler skilda från (0) eller V. En modul med denna egenskap kallas **enkel** och eftersom den termen är mera allmän (man definierar enkla moduler över helt godtyckliga ringar, medan begreppet irreducibel representation är snarare relaterat till gruppringar) så vore det motiverat att kalla irreducibla representationer för enkla. Traditionen är dock annan. Man studerar också irreducibla moduler, men då menar man moduler som inte kan skrivas som direkt summa av två äkta delmoduler. Faktum är att för gruppringar av ändliga grupper över talkroppar (och mera allmänt kroppar vars karakteristik inte delar gruppens ordning) sammanfaller dessa två begrepp. Detta följer direkt från (9.15).

Ett mycket viktigt resultat i representationsteorin säger att varje representation av en ändlig grupp över en kropp är en direkt summa av irreducibla representationer. I termer av moduler innebär detta resultat att varje ändligt genererad modul över en gruppring är en direkt summa av enkla moduler. Sådana moduler kallas **halvenkla**. Maschkes sats som vi bevisar nedan (se (9.16)) säger just att över en gruppring är varje ändligt genererad modul halvenkel. Vi kommer att formulera och bevisa detta resultat i termer av G-moduler. Först visar vi ett mycket väsentligt hjälpresultat.

(9.15) Proposition. *Låt V vara ett vektorrum över en kropp K och G en ändlig grupp. Om V är en G-modul och W är en G-delmodul till V så existerar en G-delmodul W' till V sådan att $V = W \oplus W'$.*

Bevis. Låt $e_1, \ldots, e_r$ vara en bas för W över K och låt oss komplettera denna bas till en bas $e_1, \ldots, e_r, \ldots, e_n$ för V över K. Det finns en linjär avbildning $f : V \to W$ sådan att $f(e_i) = e_i$ då $1 \leq i \leq r$ och $f(e_i) = 0$ då $r < i \leq n$ (observera att f begränsad till W är identiteten på W). Betrakta en ny linjär avbildning $\varphi : V \to W$ som definieras på följande sätt:

$$\varphi(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} f(gv).$$

Vi påstår att φ är en homomorfism av G-moduler dvs $\varphi(g_0 v) = g_0 \varphi(v)$ för varje $g_0 \in G$ och $v \in V$. I själva verket har vi

$$\varphi(g_0 v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} f(g g_0 v) = \frac{1}{|G|} \sum_{h \in G} g_0 h^{-1} f(hv) = g_0 \varphi(v),$$

där $h = g g_0$ ger alla element i G då g löper över alla element i G. Nu kontrollerar vi lätt att $\varphi(v) = v$ då $v \in W$ ty $g^{-1} f(gv) = g^{-1} gv = v$ för varje $g \in G$ och $v \in W$. Som vi vet är $W' = \operatorname{Ker} \varphi$ en G-delmodul till V (se (9.10)). Vi skall slutligen kontrollera att

$$V = W \oplus W'.$$

Om $v \in V$ så är $v = \varphi(v) + (v - \varphi(v))$ varvid $\varphi(v) \in W$ och $v - \varphi(v) \in W'$ ty $\varphi(v - \varphi(v)) = \varphi(v) - \varphi(v) = 0$. Detta visar att $V = W + W'$. Men $W \cap W' = (0)$ ty $w \in W \cap W'$ ger att $\varphi(v) = v = 0$. Alltså är $V = W \oplus W'$. □

(9.16) Maschkes sats. *Låt G vara en ändlig grupp. Då är varje G-modul en direkt summa av irreducibla G-moduler, dvs om ett ändligt dimensionellt rum V över K är en G-modul så är $V = W_1 \oplus \cdots \oplus W_r$, där W_i är irreducibla G-moduler.*

Bevis. Vi bevisar satsen med induktion med avseende på dimensionen av V över K. Om $\dim V = 1$ eller, mera allmänt, V är irreducibel så är påståendet klart. Annars har man en irreducibel G-delmodul W_1 till V (t ex en delmodul $\neq (0)$ av minsta möjliga dimension). Enligt (9.15) är $V = W_1 \oplus W'$ för en G-delmodul W'. Nu kan vi använda oss av induktion ty $\dim W' < \dim V$. □

Något senare visar vi att om V är given så är de irreducibla modulerna W_i i Maschkes sats entydigt definierade så när som på en isomorfism av G-moduler. Mera exakt visar vi att om $V = W_1 \oplus \dots W_r$ och $V = W_1' \oplus \dots W_{r'}'$, där W_i och W_i' är irreducibla G-moduler så är $r = r'$ och $W_i \cong W_i'$ vid lämplig numrering av delmodulerna. Vår huvuduppgift är att hitta alla W_i. Tyvärr är denna uppgift mycket svår, men vi kommer att bevisa några satser som ger en möjlighet att hantera relativt okomplicerade grupper.

Schurs Lemma.

Ett mycket viktigt resultat som vi kommer att använda ofta i fortsättningen är Schurs Lemma:

(9.17) Schurs Lemma. *Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara irreducibla grupprepresentationer av G och låt $\varphi : V \to V'$ vara en linjär avbildning sådan att $T'(g)\varphi = \varphi T(g)$ för varje $g \in G$. Då är φ en isomorfism (och således är representationerna isomorfa) eller $\varphi = 0$.*

Bevis. Låt

$$W = \mathrm{Ker}\varphi = \{x \in V : \varphi(x) = 0\}.$$

W är ett G-invariant delrum till V (se (9.10)). Men T är irreducibelt så att $W = V$ eller $W = (0)$. I första fallet är $\varphi = 0$. I andra fallet är φ injektiv. Vi visar att φ även är surjektiv. $\varphi(V)$ är ett G-invariant delrum till V' (se (9.10)). Alltså är $\varphi(V) = V'$ ty T' är irreducibelt och $\varphi(V) \neq (0)$. Detta visar att φ är en isomorfism i det andra fallet. □

Vi skall anteckna två enkla och mycket viktiga följdsatser av Schurs Lemma:

(9.18) Följdsats. *Låt $T : G \to GL(V)$ vara en irreducibel grupprepresentation av G över $\mathbb{C}$. Om $\varphi : V \to V$ är en linjär avbildning sådan att $\varphi T(g) = T(g)\varphi$ för varje $g \in G$ så existerar $\lambda \in \mathbb{C}$ så att $\varphi(v) = \lambda v$ för varje $v \in V$.*

Bevis. Låt λ vara ett egenvärde till φ. Då har man

$$(\varphi - \lambda I)T(g) = T(g)(\varphi - \lambda I)$$

Alltså är $\varphi - \lambda I = 0$ enligt Schurs Lemma ty $\det(\varphi - \lambda I) = 0$. Detta betyder att $\varphi(v) = \lambda v$ för varje $v \in V$. □

(9.19) Följdsats. *Låt $T : G \to GL(V)$ vara en irreducibel representation av en abelsk grupp G över $\mathbb{C}$. Då är* $\dim V = 1$ (*dvs T som matrisrepresentation är en grupphomomorfism $T : G \to K^*$*).

Bevis. För varje $x \in G$ kommuterar $\varphi = T(x)$ med alla $T(g)$, $g \in G$. Alltså säger (9.18) att det finns $\lambda_x \in \mathbb{C}$ så att $\varphi(v) = \lambda_x v$ för varje $v \in V$. Detta innebär att varje delrum W till V är invariant med avseende på alla $\varphi = T(x)$. Men V är irreducibelt så att den enda möjligheten är att V saknar icke-triviala delrum, dvs $\dim V = 1$. □

(9.20) Anmärkning. Låt oss formulera Schurs Lemma i matrisform. Om $\mathbf{e} = (e_1, \ldots, e_n)$ är en bas för V och $\mathbf{e}' = (e'_1, \ldots, e'_{n'})$ en bas för V' så har vi motsvarande matriser $T_{\mathbf{e}}(g) = [a_{ij}(g)]$, $T'_{\mathbf{e}'}(g) = [a'_{ij}(g)]$, och $M_\varphi = [b_{ij}]$, där M_φ är matrisen för φ med avseende på baserna $\mathbf{e}$ och $\mathbf{e}'$. Då säger Schurs Lemma att likheten

$$T'_{\mathbf{e}'}(g) M_\varphi = M_\varphi T_{\mathbf{e}}(g)$$

implicerar att M_φ är kvadratisk med $\det M_\varphi \neq 0$ eller $M_\varphi = \mathbf{0}$ ($\mathbf{0}$ är nollmatrisen). Den första följdsatsen säger att om $T = T'$ och representationerna är över de komplexa talen $\mathbb{C}$ så är $M_\varphi = \lambda E$, där E betecknar $n \times n$-enhetsmatrisen.

□

Funktioner på ändliga grupper. Karaktärer.

Alla funktioner

$$\varphi : G \to K$$

bildar ett vektorrum över K under addition

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g)$$

och multiplikation med skalärer

$$(a\varphi)(g) = a\varphi(g).$$

Vi skall beteckna detta vektorrum med K^G. Det är klart att $\dim_K K^G = |G|$, ty en bas för rummet K^G består av alla funktioner φ_g, $g \in G$, sådana att

$$\varphi_g(x) = \begin{cases} 1 & \text{då} \quad x = g, \\ 0 & \text{då} \quad x \neq g. \end{cases}$$

Vi har $\varphi = \sum_{g \in G} \varphi(g)\varphi_g$ för varje funktion $\varphi \in K^G$[††].

På rummet K^G definieras en bilinjär symmetrisk form:

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1}). \tag{9.21}$$

Man kontrollerar mycket lätt att formen (φ, ψ) verkligen är bilinjär och symmetrisk, dvs

$$(\varphi_1 + \varphi_2, \psi) = (\varphi_1, \psi) + (\varphi_2, \psi), \quad (\varphi, \psi_1 + \psi_2) = (\varphi, \psi_1) + (\varphi, \psi_2),$$

$$(a\varphi, \psi) = a(\varphi, \psi), \quad (\varphi, a\psi) = a(\varphi, \psi),$$

och

$$(\varphi, \psi) = (\psi, \varphi),$$

ty

$$(\psi, \varphi) = \frac{1}{|G|} \sum_{g \in G} \psi(g)\varphi(g^{-1}) = \frac{1}{|G|} \sum_{h \in G} \varphi(h)\psi(h^{-1}),$$

där $h = g^{-1}$.

(9.22) Exempel. Låt $T : G \to GL(V)$ vara en grupprepresentation och låt $\mathbf{e} = (e_1, \ldots, e_n)$ vara en bas för V över K. Om

[††] K^G har också en ringstruktur och med denna är identisk med gruppringen $K[G]$ (se (2.2)(h)), men vi utnyttjar inte denna struktur här. Funktionsrummet K^G studeras också för oändliga grupper (se Övn. 8).

$$T(g)(e_i) = \sum_j a_{ji}(g)e_j,$$

så har vi n^2 funktioner $g \mapsto a_{ij}(g)$.

□

En mycket viktig klass av funktioner på grupper utgör så kallade karaktärer. Innan vi definierar detta begrepp, låt oss repetera kort begreppet spår för en linjär avbildning.

Låt $\varphi : V \to V$ vara en K-linjär avbildning av ett vektorrum över en kropp K. Låt $\mathbf{e} = (e_1, \ldots, e_n)$ och $\mathbf{e}' = (e'_1, \ldots, e'_n)$ vara två baser för V över K och låt $P = [p_{ij}]$ vara övergångsmatrisen från $\mathbf{e}$ till $\mathbf{e}'$ dvs $e'_i = \sum p_{ji}e_j$. Om M_φ är matrisen för φ i den första basen, och M'_φ i den andra, så har man

$$M'_\varphi = P^{-1}M_\varphi P.$$

Med **karakteristiska polynomet** för φ menas

$$\mathrm{char}(\varphi) = \det(xI - M_\varphi)$$

.

Detta polynom är oberoende av basvalet för φ ty

$$\det(xI - M'_\varphi) = \det(xI - P^{-1}M_\varphi P) = \det(P^{-1}(xI - M_\varphi)P) = \det(xI - M_\varphi).$$

Om $M_\varphi = [a_{ij}]$ så är

$$\det(xI - M_\varphi) = x^n - (\sum a_{ii})x^{n-1} + \cdots.$$

Koefficienten $\sum a_{ii}$ kallas för **spåret** av φ och är naturligtvis oberoende av basvalet för V över K. Spåret betecknas med $Tr(\varphi)$. Spåret är alltså summan av diagonalelementen i matrisen för φ i en godtycklig bas. Rent allmänt definieras spåret av en matris A som summan av dess diagonalelement. Det är klart att

$$Tr(\varphi + \psi) = Tr(\varphi) + Tr(\psi) \quad \text{och} \quad Tr(a\varphi) = aTr(\varphi)$$

om φ och ψ är linjära avbildningar av V samt $a \in K$. I termer av matriser säger dessa likheter att

$$Tr(A+B) = Tr(A) + Tr(B) \quad \text{och} \quad Tr(aA) = aTr(A)$$

då A och B är kvadratiska matriser av samma storlek. Vi har också (se Övn. 11)

$$Tr(\varphi\psi) = Tr(\psi\varphi)$$

och

$$Tr(AB) = Tr(BA).$$

(9.23) Definition. Låt $T : G \to GL(V)$ vara en representation av G över K. Med karaktären χ_T av T menas funktionen

$$\chi_T(g) = Tr(T(g)).$$

Karaktären χ_T kommer vi också att beteckna med χ_V.

□

(9.24) Exempel. Låt $T : G \to GL(V)$ vara den reguljära representationen (se (9.2)(c)) och χ_{reg} dess karaktär. Då är

$$\chi_{reg}(g) = \begin{cases} |G| & \text{om } g = e \\ 0 & \text{om } g \neq e \end{cases}$$

(Försök föreställa Dig hur matriserna för $T_{reg}(g)$ ser ut då $g = e$ och $g \neq e$.)

□

Vårt närmaste syfte är ett bevis av följande viktiga hjälpresultat:

(9.25) Proposition. *Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara irreducibla representationer av G. Låt $\mathbf{e} = (e_1, \dots, e_n)$ vara en bas för V över K och $\mathbf{e}' = (e'_1, \dots, e'_{n'})$ en bas för V' över K. Om $T_{\mathbf{e}}(g) = A(g) = [a_{ij}(g)]$ och $T'_{\mathbf{e}'}(g) = A'(g) = [a'_{ij}(g)]$ så är*

(a) $(a_{ij}, a'_{kl}) = \frac{1}{|G|}\sum_{x\in G} a_{ij}(x)a'_{kl}(x^{-1}) = 0$ *om T och T' inte är isomorfa,*

(b) $(a_{ij}, a_{kl}) = \frac{1}{|G|}\sum_{x\in G} a_{ij}(x)a_{kl}(x^{-1}) = \delta_{il}\delta_{jk}\frac{1}{\dim V}$ *om T och T' är isomorfa, $V = V'$ och $K = \mathbb{C}$.*

Bevis. Låt $P = [p_{ij}]$ vara en godtycklig $n' \times n$ – matris med element i kroppen K. Betrakta matrisen

$$Q = \sum_{x\in G} A'(x)PA(x^{-1}).$$

För ett godtyckligt element $g \in G$ har man

$$A(g)Q = \sum_{x\in G} A(gx)PA'(x^{-1}) = \sum_{y\in G} A(y)PA'(y^{-1}g) = (\sum_{y\in G} A(y)PA'(y^{-1}))A'(g) = QA'(g),$$

där $y = gx$. Om T och T' inte är isomorfa så ger (9.20) att $Q = \mathbf{0}$. Alltså är

$$\sum_{x\in G}\sum_{j,k} a_{ij}(x)p_{jk}a'_{kl}(x^{-1}) = 0.$$

När man väljer matrisen P så att endast ett element p_{jk} är 1 och alla andra är lika med 0 så får man

$$\sum_{x\in G} a_{ij}(x)a'_{kl}(x^{-1}) = 0,$$

vilket bevisar (a).

Om nu $T = T'$ (dvs $A(g) = A'(g)$ för varje $g \in G$) så gäller enligt (9.20) att $Q = \lambda I$ för ett tal $\lambda \in K$. Alltså har vi

$$\sum_{x\in G} A(x)PA(x^{-1}) = \lambda I. \tag{9.26}$$

Låt oss räkna ut spåret av matriserna till höger och till vänster i den sista likheten. Då får vi

$$Tr(\sum_{x\in G} A(x)PA(x^{-1})) = \sum_{x\in G} Tr(A(x)PA(x^{-1})) = \sum_{x\in G} Tr(P) = Tr(\lambda I),$$

ty $Tr(A(x)PA(x^{-1})) = Tr(A(x^{-1})A(x)P) = Tr(A(x^{-1}x)P) = Tr(P)$. Alltså är

$$Tr(P)|G| = \lambda \dim V.$$

.

Likheten (9.26) säger att för godtyckliga i, l är

$$\sum_{x\in G}\sum_{j,k} a_{ij}(x)p_{jk}a_{kl}(x^{-1}) = \delta_{il}\lambda.$$

Låt oss igen välja matrisen P så att endast ett element p_{jk} är 1 och alla andra 0. Då är $Tr(P) = \delta_{jk}$ så att

$$\frac{1}{|G|}\sum_{x\in G} a_{ij}(x)a_{kl}(x^{-1}) = \delta_{il}\delta_{jk}\frac{1}{\dim V}.$$

□

Nu kan vi visa **ortogonalitetsrelationer för karaktärer**

(9.27) Sats. *Låt χ och χ' vara karaktärer av två olika (dvs inte isomorfa) irreducibla representationer av G över $\mathbb{C}$. Då gäller det att $(\chi, \chi') = 0$ och $(\chi, \chi) = 1$.*

Bevis. Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara irreducibla representationer av G med karaktärer χ och χ'. Låt $\mathbf{e} = (e_1, \ldots, e_n)$ vara en bas för V över K och $\mathbf{e}' = (e'_1, \ldots, e'_{n'})$ en bas för V' över K. Låt $T_{\mathbf{e}}(g) = [a_{ij}(g)]$ och $T'_{\mathbf{e}'}(g) = [a'_{ij}(g)]$. Vi har (se (9.21)):

$$(\chi, \chi') = \frac{1}{|G|}\sum_{x\in G}\chi(x)\chi'(x^{-1}) = \frac{1}{|G|}\sum_{x\in G}(\sum_i a_{ii}(x))(\sum_j a'_{jj}(x^{-1}))$$

$$= \frac{1}{|G|}\sum_{i,j}\sum_{x\in G} a_{ii}(x)a'_{jj}(x^{-1}) = 0$$

enligt (9.25)(a). Vidare har vi enligt (9.25)(b)

$$(\chi,\chi)=\frac{1}{|G|}\sum_{x\in G}\chi(x)\chi(x^{-1})=\frac{1}{|G|}\sum_{x\in G}(\sum_i a_{ii}(x))(\sum_j a_{jj}(x^{-1}))$$

$$=\frac{1}{|G|}\sum_{i,j}\sum_{x\in G}a_{ii}(x)a_{jj}(x^{-1})=\sum_{i,j}\delta_{ij}\frac{1}{\dim V}=1$$

ty $\delta_{ij}=0$ då $i\neq j$ och i löper från 1 till $n=\dim V$. □

Hur kan man beräkna (χ,χ') då χ och χ' är godtyckliga karaktärer? Svaret följer lätt ur följande enkla observation:

(9.28) Proposition. *Om $T:G\to GL(V)$ är en representation av G och $W_1,W_2\subseteq V$ är G-invarianta delrum till V (se (9.11)) sådana att $V=W_1\oplus W_2$ så är $\chi_V=\chi_{W_1}+\chi_{W_2}$.*

Bevis. Om $e_1,\dots,e_r$ är en bas för W_1 och $e_{r+1},\dots,e_n$ en bas för W_2 så ser man direkt att spåret av $T(g)$ är summan av spåren av restriktionerna av $T(g)$ till W_1 och W_2 (se eventuellt (9.13)). □

En enkel induktion ger nu en generalisering av (9.29):

(9.29) Följdsats. *Om $T:G\to GL(V)$ är en representation och $V=W_1\oplus\cdots\oplus W_r$, där W_i är irreducibla G-delmoduler med karaktärer χ_i så är $\chi_V=\chi_1+\cdots+\chi_r$.*

□

Rent teoretiskt har vi nu en möjlighet att beräkna (χ,χ') genom att uppdela χ och χ' i summor av karaktärer som svarar mot irreducibla representationer. Därefter kan vi utnyttja sats (9.27) samt det faktum att (χ,χ') är en bilinjär form med avseende på sina variabler. Låt oss anteckna en mycket viktig konsekvens av den observationen och sats (9.27):

(9.30) Följdsats. *Om χ är karaktären av en godtycklig representation av G över $\mathbb{C}$ så är $(\chi,\chi)\neq 0$.*

Bevis. Om χ är karaktären av en godtycklig representation $T:G\to GL(V)$ så är $V=W_1\oplus\cdots\oplus W_r$, där W_i är irreducibla G-moduler med karaktärer χ_i. Enligt (9.29) är $\chi=\chi_1+\cdots+\chi_r$ så att $(\chi,\chi)\neq 0$ enligt (9.27) (man inser lätt att $(\chi,\chi)\geq r$). □

Grupprepresentationer och karaktärer.

I detta avsnitt visar vi en mycket viktig sats som säger att karaktärerna svarar en-entydigt mot olika representationer av samma grupp. Därefter formulärar vi och bevisar en rad viktiga följdsatser till denna sats. Men först behöver vi ett enkelt hjälpresultat.

Låt $T : G \to GL(V)$ vara en representation av G över K och låt $L \supseteq K$ vara en kroppsutvidgning. I den situationen kan man utvidga representationen T till en representation T_L av G över L på följande sätt. Låt V_L vara ett linjärt rum som har samma dimension över L som V har över K. Låt $\mathbf{e} = (e_1, \ldots, e_n)$ vara en bas för V över K, och $\mathbf{f} = (f_1, \ldots, f_n)$ en bas för V_L över L. Om

$$T(g)(e_i) = \sum_j a_{ji}(g)e_j$$

så definierar vi

$$T_L(g)(f_i) = \sum_j a_{ji}(g)f_j.$$

På det sättet får vi en ny representation $T_L : G \to GL(V_L)$[†] som man ofta kallar för **utvidgningen av T till L**. Låt oss observera att även om T är irreducibel så kan det visa sig att T_L är reducibel (se vidare Övn. 1).

Följande observation är helt självklar (se (9.23)):

(9.31) Proposition. *Låt $T : G \to GL(V)$ vara en representation av G över K och låt $L \supseteq K$ vara en kroppsutvidgning. Om $T_L : G \to GL(V_L)$ är utvidgningen av T till L så är $\chi_T = \chi_{T_L}$.*

(9.32) Följdsats. *Låt $T : G \to GL(V)$ vara en representation av G över K med karaktären χ. Då är $(\chi, \chi) \neq 0$.*

Bevis. Låt oss utvidga representationen T till $\mathbb{C}$. Som vi vet är karaktären av den representationen fortfarande lika med χ och enligt (9.31) är $(\chi, \chi) \neq 0$. □

(9.33) Sats. *Låt $T : G \to GL(V)$ och $T' : G \to GL(V')$ vara två representationer av G i vektorrum V och V' över K. Representationerna T och T' är isomorfa då och endast då deras karaktärer är lika dvs $\chi_T(g) = \chi_{T'}(g)$ för varje $g \in G$.*

[†]rummet V_L betecknas ofta med $V \otimes_K L$.

Bevis. Antag först att T och T' är isomorfa dvs det finns en isomorfism $\varphi : V \to V'$ sådan att $T'(g)\varphi = \varphi T(g)$ för varje $g \in G$. Då är $T'(g) = \varphi T(g)\varphi^{-1}$ och således

$$\chi_{T'}(g) = Tr(\varphi T(g)\varphi^{-1}) = Tr(\varphi^{-1}\varphi T(g)) = Tr(T(g)) = \chi_T(g).$$

Låt oss nu anta att $\chi_T = \chi_{T'}$. Låt $V = W_1 \oplus \cdots \oplus W_r$ och $V' = W_1' \oplus \cdots \oplus W_{r'}'$ vara uppdelningar av V och V' i direkta summor av irreducibla G-moduler W_i och W_j' med motsvarande karaktärer χ_i och χ_j'. Vi vill visa att $r = r'$ och $W_i \cong W_i'$ vid lämplig numrering av modulerna.

Enligt (9.30) har man $\chi_T = \chi_1 + \cdots + \chi_r$ och $\chi_T' = \chi_1' + \cdots + \chi_{r'}$. Vi skall använda oss av induktion med avseende på sammanlagda antalet direkta summander $r + r'$. Om $r + r' = 2$, dvs $V = W_1$ och $V' = W_1'$, så innebär likheten $\chi_1 = \chi_1'$ att $V \cong V'$ ty $V \ncong V'$ ger enligt (9.27) att $(\chi_T, \chi_{T'}) = 0$, vilket strider mot att $(\chi_T, \chi_{T'}) = (\chi_T, \chi_T) \neq 0$.

Antag nu att $r + r' > 2$ och att χ_1' inte finns bland $\chi_1, \ldots, \chi_r$. Då är

$$(\chi_T, \chi_1') = \sum_{i=1}^{r} (\chi_i, \chi_1') = 0 \quad \text{och} \quad (\chi_{T'}, \chi_1') = \sum_{i=1}^{r'} (\chi_i', \chi_1') \neq 0.$$

Den motsägelsen visar att χ_1' måste finnas bland $\chi_1, \ldots, \chi_r$. Låt oss numrera om karaktärerna så att $\chi_1 = \chi_1'$. Då får vi att $W_1 \cong W_1'$ som G-moduler och $\chi_2 + \cdots + \chi_r = \chi_2' + \cdots + \chi_{r'}$ (observera att $r + r' > 2$ ger att $r > 1$ och $r' > 1$ ty $r = 1$ eller $r' = 1$ skulle innebära att W_1 eller W_1' hade varit reducibel). Nu kan vi tillämpa vårt induktiva antagande på G-modulerna $W_2 \oplus \cdots \oplus W_r$ och $W_2' \oplus \cdots \oplus W_{r'}$ (med antalet av irreducibla summander $r + r' - 2$). Vi får $r - 1 = r' - 1$ och $W_2 \cong W_2', \ldots, W_r \cong W_r'$ vid lämplig numrering av summanderna. □

Låt $V = W_1 \oplus \cdots \oplus W_r$, där W_i är irreducibla G-moduler. Bland modulerna W_i kan finnas isomorfa. Om W är irreducibelt och exakt m bland modulerna W_i är isomorfa med W så säger man att W har **multipliciteten** m i V.

(9.34) Följdsats. *Låt $T : G \to GL(V)$ vara en representation av G över $\mathbb{C}$ med karaktären χ, och låt $T_0 : G \to GL(V_0)$ vara en irreducibel representation av G över $\mathbb{C}$ med karaktären χ_0. Då är multipliciteten av V_0 i V lika med (χ, χ_0).*

Bevis. Låt $V = W_1 \oplus \cdots \oplus W_r$, där W_i är irreducibla G-delmoduler med karaktärer χ_i. Om V_0 är isomorf med m summanderna bland W_i så är $(\chi, \chi_0) = m$ ty $(\chi_i, \chi_0) = 1$ då V_0 och W_i är isomorfa och $(\chi_i, \chi_0) = 0$ om de inte är isomorfa (se (9.27)). □

(9.35) Följdsats. *Varje irreducibel representation $T_0 : G \to GL(V_0)$ är en delrepresentation till den reguljära representationen av G med multipliciteten $\chi_0(e)$, där χ_0 är karaktären av T_0 och n_0 är dess dimension. Om χ_{reg} är karaktären av den reguljära representationen så är*

$$\chi_{reg} = \sum_i \chi_i(e)\chi_i,$$

där χ_i löper över karaktärerna av alla irreducibla representationer av G.

Bevis. Vi har

$$(\chi_{reg}, \chi_0) = \frac{1}{|G|} \sum_{g \in G} \chi_{reg}(g)\chi_0(g^{-1}) = \chi_0(e) = n_0$$

så att påståendet följer ur (9.34) med den reguljära representationen $T : G \to GL(K^n)$, där $n = |G|$. □

Följande viktiga resultat är en direkt konsekvens av (9.35):

(9.36) Följdsats. *Varje ändlig grupp har endast ändligt många icke-isomorfa irreducibla representationer över K.*

□

(9.37) Proposition. *Låt G vara en ändlig grupp och låt $n_1, \ldots, n_r$ vara dimensionerna av alla irreducibla representationer av G över $\mathbb{C}$ med karaktärerna $\chi_1, \ldots, \chi_r$. Då gäller*

$$|G| = n_1^2 + \cdots + n_r^2$$

och för varje $g \in G$, $g \neq e$,

$$n_1\chi_1(g) + \cdots + n_r\chi_r(g) = 0.$$

Bevis. Enligt (9.35) är

$$\chi_{reg}(e) = |G| = \sum_i \chi_i(e)\chi_i(e) = \sum_i n_i^2,$$

och för varje $g \in G$, $g \neq e$, är

$$0 = \chi_{reg}(g) = \sum_i \chi_i(e)\chi_i(g) = \sum_i n_i\chi_i(g).$$

□

(9.38) Anmärkning. Man kan visa att dimensionerna n_i av de irreducibla representationerna av G är alla delare till ordningen $|G|$. Tyvärr kräver beviset av den satsen några nya begrepp som vi inte kan introducera i denna text. Men resultatet följer relativt enkelt ur (9.42) om man vet att karaktärernas värden $\chi(g)$ är algebraiska heltal, dvs komplexa tal som satisfierar algebraiska ekvationer med heltaliga koefficienter och högsta koefficienten lika med 1.

□

(9.39) Exempel. Vi skall beskriva alla irreducibla representationer av symmetrigruppen D_3 för en liksidig triangel. Vi har $|D_3| = 6$. D_3 är inte abelsk så att det finns irreducibla representationer av dimension > 1 (se (9.2)(b) och Övn. 4). Den enda möjligheten är alltså uppdelningen

$$6 = 1^2 + 1^2 + 2^2$$

(se (9.37)) så att D_3 har två irreducibla representationer av dimensionen 1 och en irreducibel representation av dimensionen 2. Det är lätt att hitta alla dessa representationer. Den 2-dimensionella representationen T ges i (9.2)(b). Man visar att den är irreducibel i (9.12)(b). En av de två 1-dimensionella representationerna är den triviala $T_1 : D_3 \to GL(\mathbb{C}) = \mathbb{C}^*$, där $T_1(g) = 1$ för varje $g \in G$. Den andra representationen av dimensionen 1 är $T_2(g) = \det(T(g))$, där T är den 2-dimensionella irreducibla representationen. Representationerna T_1 och T_2 är inte isomorfa ty deras karaktärer är olika (dvs T_1 och T_2 är olika som funktioner).

(b) Låt $G = \mathbf{Z}/n\mathbf{Z}$. G är en abelsk grupp, så att alla irreducibla representationer har dimensionen 1 (se (9.19)). Deras antal är således n i enlighet med (9.37). Dessa representationer ges av $T_j : G \to GL(\mathbb{C}) = \mathbb{C}^*$ för $j = 0, 1, \ldots, n-1$, där

$$T_j([k]_n) = e^{\frac{2\pi ikj}{n}}.$$

Man kontrollerar lätt att varje T_j är en grupphomomorfism. Olika T_j definierar icke-isomorfa representationer därför att de har olika karaktärer (helt enkelt är de olika t ex då $g = [1]_n$).

Om G är en godtycklig ändlig abelsk grupp, så kan man uppdela G i en direkt summa av cykliska grupper och därefter beskriva alla irreducibla representationer G, dvs alla grupphomomorfismer $G \to \mathbb{C}^*$.

□

Vi möter flera andra exempel på en beskrivning av alla irreducibla representationer av olika grupper i samband med övningar.

Antalet irreducibla representationer.

I detta avsnitt kommer vi att förklara hur gruppstrukturen är relaterad till antalet av irreducibla representationer. Karaktärerna spelar också här en mycket viktig roll.

(9.40) Definition. En funktion $\varphi : G \to \mathbb{C}$ kallas $\mathbb{C}$ central om $\varphi(gxg^{-1}) = \varphi(x)$ för godtyckliga $g, x \in G$.

□

Som exempel på centrala funktioner på G låt oss nämna karaktärerna. I själva verket har man

$$\chi(gxg^{-1}) = Tr(T(gxg^{-1})) = Tr(T(g)T(x)T(g^{-1})) =$$

$$Tr(T(g^{-1})T(g)T(x)) = Tr(T(x)) = \chi(x).$$

ty för godtyckliga linjära avbildningar φ, ψ gäller det att $Tr(\varphi\psi) = Tr(\psi\varphi)$.

Låt oss påmina om att två element x och x' i en grupp G kallas **konjugerade** om det finns $g \in G$ så att $x' = gxg^{-1}$. Denna relation mellan gruppens element är en ekvivalensrelation. Vi skall beteckna med $C_1, \ldots, C_s$ dess ekvivalensklasser (dvs klasser av konjugerade element i G). Den sista definitionen säger att med en central funktion φ på G menas en funktion som har samma värde på varje konjugatklass C_i. Vi skall beteckna detta värde med $\varphi(C_i)$. De centrala funktionerna på G är helt enkelt alla funktioner på konjugatklasserna.

Det är klart att alla centrala funktioner på G bildar ett delrum till rummet $\mathbb{C}^G$ av alla funktioner på G. Vi skall beteckna detta delrum med $Z[G]$[†] . Rummet $\mathbb{C}^G$ är försett med symmetrisk bilinjär form (φ, ψ). Följande observation är nästan självklar:

(9.41) Proposition. $\dim_{\mathbb{C}} Z[G] = s$, *där* s *är antalet konjugatklasser i* G.

Bevis. Låt $C_1, \ldots, C_s$ beteckna alla konjugatklasser i G. Låt φ_i för $i = 1, \ldots, s$ vara centrala funktioner på G sådana att

[†] "Z" kommer från tyskans "Zentrum".

$$\varphi_i(x) = \begin{cases} 1 & \text{om } x \in C_i, \\ 0 & \text{om } x \notin C_i. \end{cases}$$

Om nu φ är en godtycklig central funktion på G så har vi

$$\varphi = \sum_{i=1}^{s} \varphi(C_i)\varphi_i,$$

dvs φ_i genererar $Z[G]$. Det är också klart att φ_i är linjärt oberoende över $\mathbb{C}$ ty likheten

$$\sum_{i=1}^{s} a_i\varphi_i = 0$$

ger efter insättningen av ett element $x \in C_i$ att $a_i = 0$. □

Vårt närmaste syfte är ett bevis för att antalet irreducibla representationer av G över $\mathbb{C}$ är lika med antalet konjugatklasser i G. Vi tänker visa att karaktärerna av irreducibla representationer av G bildar en bas i rummet $Z[G]$, vilket ger att antalet sådana karaktärer är lika med rummets dimension som enligt (9.41) sammanfaller med antalet konjugatklasser. Vi behöver ett hjälpresultat:

(9.42) Lemma. *Låt f vara en central funktion på G och låt $T : G \to GL(V)$ vara en irreducibel representation av G över $\mathbb{C}$ med karaktären χ. Definiera $\varphi : V \to V$ med hjälp av formeln:*

$$\varphi = \sum_{g\in G} f(g^{-1})T(g).$$

Då är $\varphi(v) = \lambda v$ för $v \in V$ och

$$\lambda = \frac{|G|}{\dim V}(f, \chi).$$

Bevis. Låt $g_0 \in G$ vara ett godtyckligt element i G. Då har vi

$$T(g_0^{-1})\varphi T(g_0) = \sum_{g\in G} f(g^{-1})T(g_0^{-1}gg_0) = \sum_{h\in G} f(g_0h^{-1}g_0^{-1})T(h) = \sum_{h\in G} f(h^{-1})T(h) = \varphi,$$

där $h = g_0^{-1}gg_0$ löper över alla element i G då g gör detta. Alltså är $\varphi T(g_0) = T(g_0)\varphi$ för varje $g_0 \in G$. Enligt Schurs Lemma (se (9.18)) är $\varphi(v) = \lambda v$ för ett komplext tal λ, dvs $\varphi = \lambda I$, där I är den identiska avbildningen av V. Nu räknar vi spåren till höger och till vänster i likheten

$$\lambda I = \sum_{g\in G} f(g^{-1})T(g).$$

Vi får

$$\lambda \dim V = \sum_{g\in G} f(g^{-1})\chi(g) = |G|(f,\chi),$$

vilket bevisar (9.42). □

Nu kan vi visa vårt huvudresultat i detta avsnitt:

(9.43) Sats. *Låt $\chi_1, \ldots, \chi_r$ vara alla olika irreducibla karaktärer över $\mathbb{C}$ av en ändlig grupp G. Då bildar dessa karaktärer en bas i rummet $Z[G]$ (ortonormal med avseende på $(\ ,\ )$).*

Bevis. Låt X beteckna delrummet till $Z[G]$ genererat av karaktärerna av G. Vi vet att varje karaktär är en summa av χ_i. Dessa karaktärer bildar en ortonormal bas i X med avseende på den bilinjära formen (φ, ψ) enligt (9.27). Därför är dessa karaktärer linjärt oberoende över $\mathbb{C}$ (se Övn. 6.12). Vektorerna χ_i kan kompletteras till en ortogonal bas för hela rummet $Z[G]$. Antag att det finns i denna bas en vektor $f \in Z[G]$ utöver χ_i. För varje representation $T : G \to GL(V)$ definiera

$$\varphi_T = \sum_{g\in G} f(g^{-1})T(g).$$

Om T är irreducibel och har karaktären χ (en av χ_i) så ger (9.42) att $\varphi_T = 0$ ty

$$\lambda = \frac{|G|}{\dim V}(f,\chi) = 0.$$

Om T inte är irreducibel så är $V = W_1 \oplus \cdots \oplus W_r$, där W_i är irreducibla. För varje delrepresentation $T_i = T_{|W_i}$ gäller det att $\varphi_{T_i} = 0$, dvs $\varphi_T = 0$ på W_i. Alltså är $\varphi_T = 0$ på hela V. Låt oss som T välja den reguljära representationen T_{reg} (se (9.2)(c)) och låt e_{g_1} vara den basvektor som svarar mot det neutrala elementet $g_1 = e$ i G. Vi får

$$0 = \varphi_{T_{reg}}(e_{g_1}) = \sum_{g\in G} f(g^{-1})T_{reg}(g)(e_{g_1}) = \sum_{g\in G} f(g^{-1})e_{gg_1} = \sum_{g\in G} f(g^{-1})e_g.$$

Men e_g är linjärt oberoende (se (9.2)(c)) så att $f(g^{-1}) = 0$ för varje $g \in G$. Detta visar att $f = 0$, vilket strider mot förutsättningen att f var en av basvektorerna. Vi konstaterar att karaktärerna χ_i själva utgör en bas i $Z[G]$. Satsen är bevisad. □

ÖVNINGAR

9.1. Låt G vara gruppen av alla vridningar av en kvadrat ($|G| = 4$).

(a) Skriv ut en matrisrepresentation av G över $\mathbb{R}$ som en grupp av linjära avbildningar av planet $\mathbb{R}^2$.

(b) Är representationen i (a) irreducibel över $\mathbb{R}$?

(c) Motivera att matrisrepresentationen i (a) utvidgad till $\mathbb{C}$ (dvs betraktad som bestående av matriser i $GL_2(\mathbb{C})$) är reducibel. Välj en bas i $\mathbb{C}^2$ så att G representeras av diagonala matriser.

9.2. Låt U vara gruppen av alla vridningar av cirkeln $x^2 + y^2 = 1$ i $\mathbb{R}^2$. Låt $\bar{\theta}$ beteckna vridningen vinkeln θ, där $0 \leq \theta < 2\pi$.

(a) Visa att

$$T(\bar{\theta}) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

är en matrisrepresentation av U över $\mathbb{R}$.

(b) Betrakta matriserna i (a) som representation av U över $\mathbb{C}$ och visa att den utvidgade representationen är reducibel över $\mathbb{C}$.

9.3. Låt $G = S_n$ vara den symmetriska gruppen av graden n, dvs gruppen av alla bijektiva funktioner $\sigma : X \to X$, där $X = \{1, \ldots, n\}$. Låt $V = K^n$ och låt $e_i = (0, \ldots, 1, \ldots, 0)$ med 1 på i-te platsen.

(a) Visa att $T : S_n \to GL(K^n)$ är en linjär representation om man definierar

$$T(\sigma)(e_i) = e_{\sigma(i)}.$$

(b) Låt U bestå av alla vektorer $(x_1, \ldots, x_n)$ sådana att $\sum_i x_i = 0$. Visa att U är ett T-invariant delrum till K^n. Visa också att delrummet U är irreducibelt.

(c) Visa att delrummet $W = Ke$, där $e = e_1 + \cdots + e_n$ är T-invariant. Vad är det för linjär representation av G som definieras av W?

9.4. (a) Låt G vara en ändlig grupp. Visa att varje irreducibel representation av G över $\mathbb{C}$ har dimensionen 1 då och endast då gruppen G är abelsk.

(b) Är påståendet i (a) sant då man ersätter $\mathbb{C}$ med $\mathbb{R}$?

9.5. Låt $\operatorname{Ker} T = \{g \in G : T(g) = I\}$, där $T : G \to GL(V)$ är en representation av en grupp över en kropp K. Låt N en normal delgrupp till G. Visa att det finns en naturlig motsvarighet mellan alla representationer av G/N över K och alla representationer T av G över K sådana att $N \subseteq \operatorname{Ker} T$.

9.6. Låt $\chi : G \to K^*$ och $T : G \to GL(V)$ vara representationer av en grupp G. Motivera att även χT, där $(\chi T)(g) = \chi(g)T(g)$, är en representation av G. Ge exempel som visar att T och χT kan, men behöver ej, vara olika (icke-isomorfa).

9.7. Ge en beskrivning av alla irreducibla representationer över $\mathbb{C}$ av följande grupper:

(a) Kleinfyragrupp dvs $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$,

(b) Kvadratgruppen D_4, dvs symmetrigruppen för en kvadrat (observera att $|D_4| = 8$).

(c) Symmetrigruppen för en regelbunden tetraeder S_4 (här är $|S_4| = 24$).

Ledningar. (b) Man inser lätt att det finns exakt en irreducibel representation av dimensionen 2 genom att studera uppdelningar av 8 i summor av kvadrater (observera att gruppen inte är abelsk!).

(c) Den naturliga representationen av alla kongruensavbildningar av tetraedern i rymden ger en irreducibel representation T_3 av dimensionen 3. Genom att utnyttja Övn. 6 och karaktären $\chi(g) = \det T_3(g)$ får man en annan irreducibel representation av dimensionen 3. Vidare innehåller S_4 en normal delgrupp V_4 bestående av alla jämna permutationer av ordningen ≤ 2. Motivera att $S_4/V_4 \cong D_3$ och utnyttja (9.2)(b) för att konstruera en irreducibel representation av dimensionen 2. Det är lätt att hitta alla representationer av dimensionen 1.

9.8. Låt G vara en grupp och låt X vara en mängd. Låt $G \times X \to X$, där $(g, x) \mapsto gx$, vara en verkan av G på X, dvs $(g_1g_2)x = g_1(g_2x)$ och $ex = x$ då $g_1, g_2, g \in G$, $x \in X$ samt e är det neutrala elementet i G. Låt K vara en kropp och låt $V = K^X = \{f : X \to K\}$. V är ett vektorrum över K med vanlig addition $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ samt multiplikation med skalärer $(af)(x) = af(x)$ då $x \in X$ och $a \in K$. Motivera att $T : G \to GL(V)$, där

$$[T(g)(f)](x) = f(g^{-1}x)$$

är en representation av G i V över K.

Anmärkning. Situationen i denna övning är mycket vanlig och mycket viktig. Observera att om G verkar från höger, dvs $X \times G \to X$ så definieras T så att

$$[T(g)(f)](x) = f(xg).$$

Vad händer om man i stället för $f(g^{-1}x)$ tar $f(gx)$?

9.9. Alla vridningar av en kub bildar en grupp G (isomorf med S_4). Betrakta rummet V av alla funktioner $f : X \to \mathbb{C}$, där X är mängden av 6 sidor av kuben. Låt T vara representationen av G konstruerad i enlighet med Övn. 8. Är denna representation irreducibel ? Skriv ut 3 matriser $T(g)$ vid ett val av en bas för V.

9.10. Man säger att en representation $T : G \to GL(V)$ över $K = \mathbb{R}$ (resp. $\mathbb{C}$) är **ortogonal** (resp. **unitär**) om det finns $b : V \times V \to K$, där b definierar V som euklidiskt (resp. unitärt) rum över K så att $b(T(g)(x), T(g)(y)) = b(x, y)$ då $x, y \in V$ och $g \in G$. Visa att varje representation T är ortogonal (resp. unitär) om G är ändlig.

Ledning. Välj $b_0 : V \times V \to K$ så att $b_0(x, x) > 0$ då $x \in V$, $x \neq 0$. Definiera $b(x, y) = \sum_{g \in G} b_0(T(g)(x), T(g)(y))$.

9.11. Låt φ och ψ vara linjära avbildningar av ett linjärt rum V över en kropp K. Visa att $Tr(\varphi\psi) = Tr(\psi\varphi)$.

9.12. Låt G vara en grupp och K en kropp.

(a) Visa att endimensionella representationer av G är i 1-1 motsvarighet med alla grupphomomorfismer $\chi : G \to K^*$ (olika grupphomomorfismer ger olika dvs icke-isomorfa grupprepresentationer).

(b) Låt G vara ändlig. Visa att antalet icke-isomorfa endimensionella representationer är lika med ordningen av gruppen G/G', där G' är kommutatorgruppen av G (se Övn. 1.17).

9.13. Låt G vara en grupp, K en kropp och V_1, V_2 två $K[G]$-moduler. Visa att man kan definiera $V_1 \otimes_K V_2$ som $K[G]$-modul genom formeln $g(v_1 \otimes v_2) = gv_1 \otimes gv_2$.

Kapitel 10

GRUPPREPRESENTATIONER OCH LIEALGEBROR

Beskrivningen av alla gruppprepresentationer för en oändlig grupp är oftast mycket svårare än i det ändliga fallet. Samtidigt spelar sådana gruppprepresentationer en mycket stor roll både i rent matematiska sammanhang och i samband med olika tillämpningar. Låt oss bara nämna att t ex Fourierserier kan på ett naturligt sätt relateras till linjära representationer av cirkelgruppen (alla vridningar av en cirkel), representationer av SU-grupper spelar en mycket viktig roll i elementärpartiklarnas fysik, representationer av Galoisgrupper av de algebraiska talen och GL-grupper över de reella talen och de p-adiska talen utgör vitala delar av talteorin. Teorin för linjära gruppprepresentationer av oändliga grupper är starkt beroende av en ofta avancerad analytisk och topologisk apparat. Därför begränsar vi oss här till några allmänna begrepp och försöker förklara hur algebraiska strukturer – särskilt Liealgebror – träder in i samband med studier av gruppprepresentationer av oändliga grupper.

Låt G vara en grupp och $\Phi : G \to GL_K(V)$ en representation av G i ett ändligt dimensionellt vektorrum V över en kropp K. Oftast är man intresserad av matrisgrupper bestående av element ur matrisringar $M_n(K)$, där K är en fullständig kropp som t ex $\mathbb{R}, \mathbb{C}$ eller

$\widehat{\mathbb{Q}}_p$ (se (14.14)). Om $|\ |$ är en norm på K så kan man definiera en norm på $M_n(K)$:

$$\|A\| = \sum |a_{ij}|^2, \tag{10.1}$$

där $A = [a_{ij}] \in M_n(K)$. Man kontrollerar lätt att $\|\ \|$ uppfyller de vanliga villkoren:

(a) $\|A\| \geq 0$ och $\|A\| = 0 \Leftrightarrow A = 0$,
(b) $\|A\| = \| - A\|$,
(c) $\|A + B\| \leq \|A\| + \|B\|$,
(d) $\|AB\| \leq \|A\|\|B\|$.

Funktionen $d(A,B) = \|A - B\|$ för $A, B \in M_n(K)$ definierar en topologisk (här metrisk) struktur på $G \subset M_n(K)$. I sådana fall betraktar man kontinuerliga representationer $\Phi : G \to GL(K^N)$† dvs sådana att funktionen Φ är kontinuerlig m.a.p. konvergensen definierad av $\| \ \|$.

För representationer av ändliga grupper spelar K-algebran $K[G]$ av alla funktioner $\varphi : G \to K$ en stor roll. För oändliga grupper är dock formeln för multiplikation:

$$(\varphi\psi)(g) = \sum_{hh'=g} \varphi(h)\psi(h')$$

meningslös. Man kan begränsa sig till funktioner φ med $\varphi(g) = 0$ för nästan alla g, men en sådan ring $K[G]$ förlorar då sin viktigaste egenskap att varje irreducibel G-representation är en direkt summand i den reguljära, dvs den som definieras av $K[G]$-modulen $K[G]$. Därför ersätter man $K[G]$ med andra algebraiska objekt relaterade till G. En metod är att betrakta ringar bestående av rikligare funktionsklasser på G. En annan metod, som kan tillämpas då G är en Liegrupp (en grupp med analytisk struktur som är rikare än rent topologisk – se (10.5)), är att använda en mycket effektiv apparat av Liealgebror. Vi skall diskutera kort dessa två metoder.

(10.2) Rummet $\mathbf{K^G}$. Låt K^G vara K-vektorrummet av alla funktioner $\varphi : G \to K$ med addition $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$ och multiplikation med sklärer $(a\varphi)(g) = a\varphi(g)$ för $a \in K$, $g \in G$. Låt

$$\Phi : G \to GL(K^G),$$

där

$$[\Phi(g)(\varphi)](h) = \varphi(g^{-1}h)$$

för $\varphi \in K^G$, $h, g \in G$. Man kontrollerar lätt at $\Phi(g_1g_2) = \Phi(g_1)\Phi(g_2)$. (Observera att $[\Phi(g)(\varphi)](h) = \varphi(gh)$ skulle leda till $\Phi(g_2)\Phi(g_1)$!). Representationen Φ kallas helt allmänt för **reguljär**. Om G är ändlig kan man definiera ringstrukturen på K^G så att $K^G \cong K[G]$ (se (2.2)(h)).

Varken $K[G]$ eller K^G tar hänsyn till den topologiska strukturen på G (om G har en sådan). Vanligen väljer man lämpliga delrum till K^G. Om t ex G är en topologisk grupp (t ex $\mathbb{R}^+, \mathbb{C}^+, \mathbb{R}^*, \mathbb{C}^*$, $T = \{z \in \mathbb{C} : |z| = 1\}$ med naturlig topologisk struktur) och μ är ett mått (t ex Lebesguemåttet), så betraktar man rummet $L^2(G,\mu) \subset K^G$ bestående av alla funktioner $\varphi : G \to \mathbb{R}$ (eller $\mathbb{C}$) sådana att φ är mätbar m.a.p. μ och $\int_G |\varphi(g)|^2 d\mu < \infty$ (mera exakt består $L^2(G,\mu)$ av ekvivalensklasser av sådana funktioner där två funktioner identifieras då de är lika nästan överallt på G). Som bekant är $L^2(G,\mu)$ ett Hilbertrum med skalärprodukten:

†Om $V = K^N$ skriver vi $GL(K^N)$ i stället för $GL_K(K^N)$.

$$(\varphi, \psi) = \int_G \varphi(g)\overline{\psi(g)}d\mu.$$

Man betraktar kontinuerliga representationer $\Phi : G \to GL_K(V)$, där $V = \mathbb{R}^n, \mathbb{C}^n$ (dvs sådana att funktionen $G \times V \to V$, där $(g, v) \mapsto \Phi(g)(v)$ är kontinuerlig). Man säger att V är **enkel** om det inte finns icke-triviala delmoduler $W \subset V$ sådana att W är slutet som ett delrum till V och $G \times W \to W$ är kontinuerlig (se (9.14)).

Om G är en kompakt grupp (i vårt fall då $G \subset M_n(K)$ och topologin definieras av $\| \ \|$ betyder det att mängden G är sluten och begränsad) får man en teori som liknar representationsteorin för ändliga grupper. Bl a får man att varje enkel G-representation är en direkt summand i $L^2(G, \mu)$. Om G är abelsk så är varje enkel representation av dimension 1, och $L^2(G, \mu)$ är en direkt summa (i topologisk mening) av alla och olika enkla G-moduler (jfr (9.16)).

(10.3) Exempel. Låt $G = T = \{z \in \mathbb{C} : |z| = 1\} \cong \mathbb{R}/2\pi\mathbb{Z}$. Man kan också beskriva T som gruppen av alla matriser

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in M_2(\mathbb{R})$$

$\theta \in [0, 2\pi[$. T är en kompakt topologisk grupp (med topologin inducerad från $\mathbb{R}$ – man kan tolka T som $[0, 2\pi]$ med 0 och 2π identifierade). T kallas ofta **torus**. Betrakta på T måttet $\mu = \frac{d\theta}{2\pi}$, där $d\theta$ är Lebesguemåttet på $\mathbb{R}$. Det finns en-entydig motsvarighet mellan alla funktioner $\varphi : T \to \mathbb{C}$ och alla funktioner $\varphi : \mathbb{R} \to \mathbb{C}$ sådana att $\varphi(x + 2\pi) = \varphi(x)$, $x \in \mathbb{R}$. Betrakta rummet $L^2(T, \mu)$. T är abelsk så att alla irreducibla (= enkla) representationer av T har dimension 1. Man kan lätt skriva ut sådana representationer – men det är mycket svårare att visa att det inte finns några andra:

$$\Phi_n : T \to \mathbb{C}^*, \ \ \Phi_n(\theta) = e^{in\theta}, \ n = 0, \pm 1, \pm 2, \pm 3, \ldots.$$

Φ_n definierar en T-modul[†]: $M_n = \mathbb{C}$, där $T \times \mathbb{C} \to \mathbb{C}$ ges av $(\theta, z) \mapsto ze^{in\theta}$. Nu vet vi att $L^2(T, \mu)$ är en direkt summa av alla M_n, dvs om $\varphi \in L^2(T, \mu)$ så finns det en entydig uppdelning

$$\varphi = \sum \varphi_n,$$

[†]Om G är en grupp så säger man att en abelsk grupp M är en G-modul om det finns en funktion $G \times M \to M$ som mot $(g, m) \in G \times M$ ordnar $gm \in M$ varvid $em = m, (g_1g_2)m = g_1(g_2m), g(m_1 + m_2) = gm_1 + gm_2$. Om M är en R-modul och $g(rm) = r(gm)$ för varje $r \in R$ så kan M betraktas som en $R[G]$-modul på ett naturligt sätt. Omvänt kan varje $R[G]$-modul betraktas som en G-modul som satisfierar den sista likheten.

där $\varphi_n \in M_n$, dvs $\varphi_n = z_n e^{in\theta}$ och serien konvergerar till φ i $L^2(T,\mu)$ m.a.p. $\|\varphi\| = \int_T |\varphi(g)|^2 d\mu$. Detta påstående om $L^2(T,\mu)$ är alltså den välkända satsen om Fourierserier.

□

(10.4) Exempel. Låt

$$G = SU_2 = \left\{ \begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix} : z_1,\, z_2 \in \mathbb{C} \quad \text{och} \quad |z_1|^2 + |z_2|^2 = 1 \right\}.$$

Låt $M_n = \{\sum_{i+j=n} a_{ij} x^i y^j,\, a_{ij} \in \mathbb{C},\, 0 \le i,\, j \le n\}$, dvs M_n är vektorrummet av alla polynom av grad n i x, y. Definiera:

$$[\Phi_n(A)p](x,y) = p(a_{11}x + a_{21}y, a_{12}x + a_{22}y),$$

där

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in G,$$

och $p \in M_n$. Det är lätt att kontrollera att $\Phi_n : SU_2 \to GL(M_n)$ är en representation (observera att $M_n \cong \mathbb{C}^{n+1}$). Man visar att Φ_n ger alla irreducibla representationer av SU_2 (så när som på isomorfism). Ett bevis av dessa påståenden brukar man genomföra med hjälp av Liealgebran av SU_2 (se vidare (10.20)(c)). M_n är direkta summander i $L^2(G,\mu)$ med lämpliga multipliciteter. Vi avstår från att definiera måttet μ och multipliciteterna.

□

Gruppprepresenttioner av topologiska grupper (kompakta och lokalt-kompakta dvs sådana att varje punkt har en omgivning vars slutna höljet är kompakt t ex $\mathbb{R}^+$, $\mathbb{C}^+$, $GL(n,\mathbb{R})$ osv.) är mycket rika och deras presentation kräver minst lika mycket topologi och analys som algebra. I ännu större grad är teorin för Liegrupper och deras representationer mera en del av analys än algebra. Icke desto mindre ägnar vi lite tid åt att diskutera samband mellan Liegrupper och motsvarande Liealgebror.

(10.5) Definition. Man säger att G är en **Liegrupp** om G är en grupp, G är en C^∞-mångfald (se (5.28)) och funktionerna $G \times G \to G$, där $(g_1, g_2) \mapsto g_1 g_2$ och $G \to G$, där $g \mapsto g^{-1}$ är C^∞-funktioner (kortare: $G \times G \to G$, där $(g_1, g_2) \mapsto g_1 g_2^{-1}$ är en C^∞-funktion).

□

(10.6) Exempel. (a) Låt G vara gruppen av alla matriser

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}, \quad a, b \in \mathbb{R},\ a \neq 0,$$

med avseende på matrismultiplikation. Om man ordnar mot en sådan matris punkten $(a, b) \in \mathbb{R}^2$ får man en bijektion av G på en öppen delmängd till $\mathbb{R}^2$. På detta sätt definierar man på G strukturen av en C^∞-mångfald (med en enda karta $U = G$ och $\varphi_0 : U \to \mathbb{R}^2$). G är en Liegrupp därför att operationen $(A, B) \mapsto AB^{-1}$ är C^∞:

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_2^{-1} & -a_2^{-1}b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1a_2^{-1} & -a_1a_2^{-1}b_2 + b_1 \\ 0 & 1 \end{bmatrix}$$

så att avbildningen $\varphi : G \times G \longrightarrow G$ ges av

$$((a_1, b_1), (a_2, b_2)) \mapsto (\varphi_1(a_1, b_1, a_2, b_2),\ \varphi_2(a_1, b_1, a_2, b_2)),$$

där $\varphi_1(a_1, b_1, a_2, b_2) = a_1a_2^{-1}$ och $\varphi_2(a_1, b_1, a_2, b_2) = -a_1a_2^{-1}b_2 + b_1$.

(b) $GL(n, \mathbb{R})$ och $GL(n, \mathbb{C})$ är Liegrupper. $A \in GL(n, \mathbb{R})$ kan identifieras med följden $(a_{ij}) \in \mathbb{R}^{n^2}$, där $\det[a_{ij}] \neq 0$. På detta sätt är $\mathrm{GL}(n, \mathbb{R})$ en öppen delmängd till $\mathbb{R}^{n^2}$ och kan betraktas som mångfald med hjälp av en enda karta $U = GL(n, \mathbb{R}) \subset \mathbb{R}^{n^2}$. Avbildningen $(A, B) \mapsto AB^{-1}$ är C^∞, vilket följer direkt ur formlerna för matrismultiplikation och invers (jfr (a)). När det gäller $GL(n, \mathbb{C})$ identifierar man dess element med punkter i $\mathbb{R}^{2n^2}$.

(c) Automorfismgrupper av kvadratiska former över $\mathbb{R}$ och $\mathbb{C}$ ($O(n), O(p, q), U(n), U(p, q)$ osv – se Kap. 6) är alla Liegrupper, men bevisen att de är C^∞-mångfalder är inte helt självklara. Konstruktioner av kartor är inte lika enkla som i (a) och (b). Vi ger en ganska enkel och allmän metod i Övn. 5, men en mera naturlig plats för den aspekten är analys. Så snart man har C^∞-strukturen på dessa grupper konstaterar man utan några problem att de är Liegrupper dvs att gruppoperationerna är C^∞-funktioner.

□

I den diskussion som följer kommer vi att begränsa oss till Liegrupper G bestående av matriser (reella eller komplexa) med multiplikation som gruppoperation[†]. För en matris X kommer vi att beteckna med $(X)_{ij}$ dess element. Låt $A \in M_n(\mathbb{R})$. Man visar lätt (se Övn. 1(a)) att för varje (i, j) är serien:

$$(I)_{ij} + (A)_{ij} + \frac{1}{2!}(A^2)_{ij} + \frac{1}{3!}(A^3)_{ij} + \dots$$

[†]T ex är $\mathbb{R}^+$ isomorf med alla matriser $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, $a \in \mathbb{R}$ m a p multiplikation.

konvergent. Man definierar e^A som matrisen med dessa element dvs

$$e^A = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \ldots. \tag{10.7}$$

Man visar att

$$e^A e^B = e^{A+B} \quad \text{om} \quad AB = BA \tag{10.8}$$

(se Övn. 1(b)). Härifrån följer direkt att $\det e^A \neq 0$ ty $e^A e^{-A} = e^0 = I$ (0 betecknar en nollmatris) så att $\det(e^A \cdot e^{-A} = 1)$.

(10.9) Definition. Med en **kurva** i G menar man varje kontinuerlig funktion

$$\gamma :]a, b[\to G.$$

Man säger att γ är **glatt** om för varje $u \in]a, b[$ existerar derivatan $\gamma'(u) \in M_n(\mathbb{R})$[††]. Man säger då att $\gamma'(u)$ är **tangentvektorn** till γ i punkten $g = \gamma(u) \in G$.

□

(10.10) Exempel. Låt $G = GL(n, \mathbb{R})$ och låt $\gamma_A(u) = e^{Au}$, $A \in M_n(\mathbb{R})$, $u \in \mathbb{R}$. Då är $\gamma_A : \mathbb{R} \to G$ en glatt kurva: $\gamma'_A(u) = Ae^{Au}$ och $\gamma'_A(0) = A$. Observera att i detta fall är $\gamma_A(u_1 + u_2) = \gamma_A(u_1)\gamma_A(u_2)$ (se (10.8)). En kurva av typen $\varphi : \mathbb{R} \to G$, där φ är en grupphomomorfism dvs $\varphi(u_1 + u_2) = \varphi(u_1)\varphi(u_2)$, kallas **enparameter delgrupp** till G. Sådana φ spelar en mycket viktig roll i teorin för Liegrupper. Om $G = GL(n, \mathbb{R})$ så är alltid $\varphi(u) = e^{Au}$ för en lämplig $A \in M_n(\mathbb{R})$.

Om $\gamma, \delta :]a, b[\to G$ är två kurvor definierar man deras produkt:

$$(\gamma\delta)(u) = \gamma(u)\delta(u) \in G.$$

Om γ och δ är glatta så är även $\gamma\delta$ glatt och

$$(\gamma\delta)'(u) = \gamma'(u)\delta(u) + \gamma(u)\delta'(u).$$

[††]Observera att $\gamma :]a, b[\to \mathbb{R}^{n^2}$ och $\gamma'(u) = [\gamma'_{ij}(u)]$ då $\gamma(u) = [\gamma_{ij}(u)]$.

I själva verket har vi $\gamma(u) = [\gamma_{ij}(u)], \delta(u) = [\delta_{ij}(u)]$ och $(\gamma\delta)_{ij}(u) = \sum \gamma_{ik}(u)\delta_{kj}(u)$ så att $(\gamma\delta)'_{ij}(u) = \sum \gamma'_{ik}(u)\delta_{kj}(u) + \sum \gamma_{ik}(u)\delta'_{kj}(u)$.

□

Vi vill undersöka kurvor som går genom neutrala elementet $e \in G$ (dvs $e = I$ enhetsmatrisen). För enkelhets skull antar vi att $0 \in]a, b[$ och $\gamma(0) = e$ för sådana kurvor.

(10.11) Proposition. *Låt T_e vara mängden av alla tangentvektorer $\gamma'(0)$ till alla kurvor $\gamma :]a, b[\to G$ med $\gamma(0) = e$. Då är T_e ett vektorrum över $\mathbb{R}$.*

Bevis. Om $\gamma'(0), \delta'(0) \in T_e$ så är $\gamma\delta(0) = \gamma(0)\delta(0) = e$ och

$$(\gamma\delta)'(0) = \gamma'(0) + \delta'(0) \in T_e.$$

Om $\gamma'(0) \in T_e$ och $r \in \mathbb{R}$ så är $\delta(u) = \gamma(ru)$ en kurva sådan att $\delta(0) = \gamma(0) = e$ och $\delta'(0) = r\gamma'(0) \in T_e$. □

(10.12) Definition. T_e kallas **tangentrummet** till G i punkten e. $\dim_{\mathbb{R}} T_e$ kallas **dimensionen** av G.

□

Tangentrummet har en rik algebraisk struktur – Liealgebrastrukturen. Låt oss repetera relevanta definitioner ur Kapitel 2:

(10.13) Definition. En ring R kallas en **Liering** om

$$a(bc) + b(ca) + c(ab) + 0 \quad \text{(Jacobi identiteten) och } a^2 = 0$$

för godtyckliga $a, b, c \in R$. L kallas **abelsk** om $ab = 0$ för godtyckliga $a, b \in L$. Om R är en Liering och samtidigt en K-algebra så säger man att R är en Liealgebra över K (se (4.18)). Observera att $(a + b)^2 = 0$ ger $ab = -ba$.

□

(10.14) Exempel. Låt R vara en godtycklig associativ ring. Låt

$$[a, b] = ab - ba \quad \text{då} \quad a, b \in R.$$

Man kontrollerar lätt att $(R, +, [\ ,\ ])$ är en Liering. Mera allmänt om $(R', +)$ är en delgrupp till $(R, +)$ sådan att $a, b \in R'$ implicerar att $[a, b] \in R'$ så är $(R', +, [\ ,\ ])$ en Liering (observera att $(R', +, \cdot)$ behöver inte vara en delring till $(R, +, \cdot)$). Nästan alla viktiga exempel på Lieringar (Liealgebror) kan konstrueras på detta sätt. Låt t ex $R = M_n(K)$, där K är en kommutativ ring, och låt $R' = \{A \in M_n(K) : Tr(A) = 0\}$. Då är $(R', +, [\ ,\ ])$ en Liering därför att $Tr(A + B) = Tr(A) + Tr(B)$ och $Tr(AB - BA) = 0$ så att $A, B \in R'$ ger att $A + B$, $[A, B] \in R'$.

□

(10.15) Anmärkning. Det finns en djupt rotad tradition att beteckna multiplikation ab i Lieringar med $[ab]$. Den förklaras av exemplet ovan. I alla satser om Lieringar som visades i Kapitel 2 (och betecknades där med "l") använde vi den vanliga beteckningen ab för produkt i en ring. Med beteckningar ovan säger Jacobi identiteten att

$$[a[bc]] + [b[ca]] + [c[ab]] = 0.$$

□

För att bevisa att T_e är en Liealgebra behöver vi ett resultat vars bevis måste utelämnas (se t ex J. Milnor, Morse Theory, Lemma 2.4. I exempel (10.18)(c) visar vi detta resultat i ett mycket viktigt specialfall).

(10.16) Sats. *Om G är en Liegrupp och $A \in T_e$ så $e^{uA} \in G$ för varje $u \in \mathbb{R}$ (dvs A definierar en enparameter delgrupp $\gamma_A : \mathbb{R} \to G$, $\gamma_A(u) = e^{uA}$ – se* (10.10)).

(10.17) Sats. *Låt G vara en Liegrupp. Då är T_e en Liealgebra då produkten av $A, B \in T_e$ definieras som $[A, B] = AB - BA$. T_e kallas Liealgebran av gruppen G (den kommer att betecknas med $\mathfrak{g}$).*

Bevis. Man måste visa att $[A, B] \in T_e$ – allt annat är klart (se exempel (10.10)). Först observerar man att kurvan; $\varphi : \mathbb{R} \to G$ där

$$\varphi(u) = e^{uA}e^{uB}e^{-uA}e^{-uB}$$

har egenskapen $\varphi(0) = e$, $\varphi'(0) = 0$, $\varphi''(0) = [A, B]$. I själva verket är:

$$\begin{aligned}\varphi(u) &= [I + Au + \frac{1}{2!}(Au)^2 + \ldots][I + Bu + \frac{1}{2!}(Bu)^2 + \ldots] \times \\ &\quad [I - Au + \frac{1}{2!}(Au)^2 + \ldots][I - Bu + \frac{1}{2!}(Bu)^2 + \ldots] =\end{aligned}$$

$$[I + (A+B)u + \frac{1}{2!}(A^2 + 2AB + B^2)u^2 + \ldots] \times$$
$$[I - (A+B)u + \frac{1}{2!}(A^2 + 2AB + B^2)u^2 + \ldots] =$$
$$I + [A,B]u^2 + \ldots.$$

Definiera nu:

$$\gamma(s) = \begin{cases} \varphi(\sqrt{s}) & \text{då} \quad s \geq 0, \\ \varphi(-\sqrt{-s}) & \text{då} \quad s \leq 0. \end{cases}$$

Man får en kurva $\gamma : \mathbb{R} \to G$ med egenskapen $\gamma'(0) = [A,B] \in T_e$. □

(10.18) Exempel. (a) Låt $G = GL(n,\mathbb{R})$. Det är klart att $e^{uA} \in G$ t.o.m. för varje $A \in M_n(\mathbb{R})$ och $u \in \mathbb{R}$ – se texten under (10.8). Tangentrummet i $e = I$ består av alla $A \in M_n(\mathbb{R})$ ty för kurvan $\varphi_A(u) = e^{uA}$ har vi $\varphi_A(0) = I$ och $\varphi'_A(0) = A$ dvs $\mathfrak{g} = M_n(\mathbb{R})$. Standardbeteckningen för denna algebra är $gl(n,\mathbb{R})$.

(b) Låt $G = SL(n,\mathbb{R})$. Liealgebran $sl(n,\mathbb{R})$ av $SL(n,\mathbb{R})$ består av alla $A \in M_n(\mathbb{R})$ sådana att $Tr(A) = 0$. För at bevisa detta på påstående noterar vi först att

$$\det e^A = e^{Tr(A)}$$

(se Övn. 1(d)). $A \in T_e$ ger att $e^A \in G$ (se (10.15)) så att $1 = \det e^A = e^{Tr(A)}$ dvs $Tr(A) = 0$.

Omvänt, om $Tr(A) = 0$ så är $\det e^{uA} = e^{Tr(uA)} = 1$, dvs $\varphi_A(u) = e^{uA}$ är en kurva i G med $\varphi_A(0) = I$ och $\varphi'_A(0) = A$ dvs $A \in T_e$, $(e = I)$. Alltså är $T_e = sl(n,\mathbb{R})$.

(c) Låt $D \in M_n(\mathbb{R})$ och låt $G = \{A \in M_n(\mathbb{R} : A^t D A = D\}$ – t ex $G = O(n), O(p,q)$ osv med motsvarande val av D. Vi påstår att Liealgebran av G, eller rättare sagt, Liealgebran av den sammanhängande komponenten av e i G[†] är

$$\mathfrak{g} = \{A \in M_n(\mathbb{R}) : A^t D + DA = 0\}.$$

T ex är $so(n) = \{A \in M_n(\mathbb{R}) : A + A^t = 0\}$. Om $A \in T_e$, så existerar en kurva $\gamma :]a,b[\to G$ sådan att $\gamma(0) = e$ och $\gamma'(0) = A$. Alltså är $\gamma(u)^t D \gamma(u) = D$. Derivering av den likheten i punkten $u = 0$ ger $\gamma'(0)^t D \gamma(0) + \gamma(0)^t D \gamma'(0) = 0$ dvs $A^t D + DA = 0$. Omvänt, låt $A^t D + DA = 0$ dvs $A^t D = -DA$. Induktionen ger att

$$(A^t)^n D = (-1)^n D A^n.$$

[†]Med den sammanhängande komponenten av e i G menas mängden av alla $g \in G$ sådana att det finns en kurva $\gamma :]0,1[\to G$ med $\gamma(0) = e$ och $\gamma(1) = g$.

Multiplicera den likheten med $\frac{u^n}{n!}$ och summera! Resultatet är

$$(e^{uA})^t D = De^{-uA}$$

dvs $(e^{uA})^t De^{uA} = D$ så att $\varphi_A(u) = e^{uA} \in G$. Som tidigare får man $\varphi'_A(0) = A$ dvs $A \in T_e$. Alltså är $T_e = \mathfrak{g}$.

□

På samma sätt hanterar man $G = \{A \in M_n(\mathbb{C}) : A^t D\bar{A} = D\}$ (t ex $G = U(n)$). Observera att Liealgebran av G enbart beror på den sammanhängande komponenten av e i G.

För vissa kroppar (t ex $\mathbb{R}, \mathbb{C}, \widehat{\mathbb{Q}}_p$) är sambandet mellan Liegrupper och motsvarande Liealgebror mycket nära. Principen är den att en och samma Liealgebra svarar mot Liegrupper relaterande på ett enkelt sätt till en speciell Liegrupp. Gruppprepresentationer av dessa Liegrupper svarar mot moduler över motsvarande Liealgebran. Klassifikation av grupppresentationer är då ekvivalent med klassifikation av moduler över Liealgebran – den sista uppgiften är i stort sett rent algebraisk. Vi skall definiera först moduler över Liealgebror och därefter visa hur gruppprepresentationer leder till moduler. Klassifikationsproblemen för Liealgebror och för moduler över dessa utgör innehållet i en mycket omfattande teori som räcker gott och väl för en helt separat kurs. Sambanden mellan Liegrupper och Liealgebror ligger mycket närmare analys än algebra.

(10.19) Definition. Låt L vara en Liealgebra över K och låt V vara ett K-vektorrum. Låt $gl_K(V)$ beteckna Liealgebran associerad med (den associativa) ringen $\mathrm{End}_K(V)$ i enlighet med (10.14). Man säger att V är en L-**modul** om det finns en Liealgebra-homomorfism $\Phi : L \to gl_K(V)$. Detta betyder att:

(a) $\Phi(x_1 + x_2) = \Phi(x_1) + \Phi(x_2)$,
(b) $\Phi([x_1x_2]) = [\Phi(x_1), \Phi(x_2)]$,
(c) $\Phi(ax) = a\Phi(x)$,

då $x, x_1, x_2 \in L$, $a \in K$. Man säger också att Φ är en K-**representation** av L. Observera att om man definierar $L \times V \to V$ genom $(x, v) \mapsto \Phi(x)(v) =: xv$ så säger villkoren (a) – (c) att

(a′) $(x_1 + x_2)v = x_1v + x_2v$,
(b′) $[x_1x_2]v = x_1(x_2v) - x_2(x_1v)$,
(c′) $(ax)v = a(xv)$.

Lägg märke till att $\Phi(x) \in \mathrm{End}_K(V)$. Sådana begrepp som homomorfism, isomorfism, irreducibel (dvs enkel) modul osv definieras exakt på samma sätt som för moduler över godtyckliga ringar.

□

(10.20) Exempel. (a) Varje ideal i L är en L-modul (om I är ett ideal så är $\Phi(x)(i) = [xi]$ då $x \in L$, $i \in I$). Observera att det inte finns någon skillnad mellan vänster- och högerideal ty $[xy] = -[yx]$ tillhör I samtidigt.

(b) Låt L vara en Liealgebra och låt $V = L$. Definiera $\Phi : L \to gl(L)$ så att $\Phi(x)(y) = [xy]$. Φ betecknas oftast med ad så att $(ad\, x)(y) = [xy]$ och kallas den **adjungerade representationen**. L förvandlas med hjälp av ad till en modul över sig själv. Observera att (b) är ett specialfall av (a) då $I = L$.

(c) Vi skall betrakta ett specialfall av (b). Låt $L = su(2)$ vara Liealgebran av $SU(2)$. I enlighet med (10.18)(c) består $su(2)$ av alla $A \in M_2(\mathbb{C})$ sådana att $\bar{A}^t + A = 0$, dvs alla antihermitska matriser. En bas för $su(2)$ över $\mathbb{R}$ består av

$$S_1 = \frac{1}{2}\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad S_2 = \frac{1}{2}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad S_3 = \frac{1}{2}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

varvid $[S_1, S_2] = S_3$, $[S_2, S_3] = S_1$, $[S_3, S_1] = S_2$. Observera att $\dim_{\mathbb{R}} su(2) = 3$ och $su(2)$ är isomorf med Liealgebran av alla vektorer i $\mathbb{R}^3$ med vektorprodukt "$\times$" som multiplikation. Betrakta representationen ad på $su(2)$. Matriserna av adS_i, $i = 1, 2, 3$, med avseende på basen S_1, S_2, S_3 (i denna ordning) är

$$M_{adS_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \quad M_{adS_2} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \quad M_{adS_3} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Dessa tre matriser är linjärt oberoende och bildar en bas för alla 3×3 antisymmetriska matriser. Alla sådana matriser bildar Liealgebran av $SO(3)$ (se (10.18)(c)). Alltså definierar ad en isomorfism $ad : su(2) \cong so(3)$. Vi skall snart förklara den isomorfismen utifrån en allmän teori och det faktum att $SU(2)/\{\pm I\} \cong SO(3)$ enligt (7.18).

□

(10.21) Från grupprepresentationer av Liegrupper till moduler över Liealgebror. Låt $\Phi : G \to GL(\mathbb{R}^N)$ vara en kontinuerlig representation av en Liegrupp G. Låt $\mathfrak{g}$ vara Liealgebran av G. Om $A \in \mathfrak{g} = T_e$ så betraktar man kurvan $u \mapsto \Phi(e^{uA}) = e^{uA'}$. Nu definierar man $\varphi : \mathfrak{g} \to gl_{\mathbb{R}}(\mathbb{R}^N)$ så att $\varphi(A) = A'$. Man kontrollerar att φ är en homomorfism av Liealgebror så att $\mathbb{R}^n$ förvandlas till en $\mathfrak{g}$-modul (vi utelämnar beviset). φ kallas ibland för derivatan av Φ och betecknas med $d\Phi$. Motsvarigheten mellan representationer av G och representationer av dess Liealgebra $\mathfrak{g}$ fungerar bra enbart för vissa klasser av Liegrupper. □

(10.22) Definition. Man säger att G är **sammanhängande** om för varje $g \in G$ existerar en kurva $\gamma : [0, 1] \to G$ sådan att $\gamma(0) = e$ och $\gamma(1) = g$. Alla kurvor $\gamma : [0, 1] \to G$ med

$\gamma(0) = \gamma(1) = e$ bildar en grupp $\Omega(G)$ om $(\gamma_1\gamma_2)(u) = \gamma_1(u)\gamma_2(u)$ (kontrollera!). G kallas **enkelt sammanhängande** om $\Omega(G)$ är sammanhängande[†] (för exempel se (10.24)).

□

(10.23) Vi sammanfattar några viktiga resultat om samband mellan representationer av Liegrupper och moduler över motsvarande Liealgebror.

(a) Det finns en $1-1$ motsvarighet mellan isomorfiklasser av kontinuerliga och ändligt dimensionella gruppprepresentationer av en sammanhängande och enkelt sammanhängande Liegrupp G och isomorfiklasser av ändligt dimensionella moduler över motsvarande Liealgebra. Motsvarigheten ges av (10.21).

(b) Låt G vara en sammanhängande och enkelt sammanhängande Liegrupp med Liealgebran $\mathfrak{g}$. Varje sammanhängande Liegrupp med Liealgebran isomorf med $\mathfrak{g}$ är isomorf med G/D, där D är en diskret och central normaldelgrupp till G[††]. Alla gruppprepresentationer av G/D får man ur alla gruppprepresentationer $\Phi : G \to GL(V)$ sådana att $D \subseteq \mathrm{Ker}\Phi$ (jfr Övn. 16.6 och ta hänsyn till kontinuiteten).

(c) Om G är en sammanhängande Liegrupp så existerar så när som på isomorfism exakt en sammanhängande och enkelt sammnhängande Liegrupp $\widetilde{G}$ och en surjektion $\widetilde{G} \to G$. Liealgebror av G och $\widetilde{G}$ är isomorfa. □

Dessa resultat visar att en studie av sammanhängande Liegrupper (t ex över $\mathbb{R}$ eller $\mathbb{C}$) kan genomföras så att man först klassificerar alla Liealgebror, därefter konstruerar alla sammanhängande och enkelt sammanhängande Liegrupper med dessa algebror som Liealgebror och slutligen beskriver alla diskreta och centrala normala delgrupper till dessa Liegrupper.

Man kan också försöka beskriva alla gruppprepresentationer av sammanhängande Liegrupper G genom att konstruera Liealgebran $\mathfrak{g}$, gruppen $\widetilde{G}$ ur (10.23)(c) och en diskret central och normal delgrupp D så att $G \cong \widetilde{G}/D$. Därefter ger gruppprepresentationerna $\Phi : \widetilde{G} \to GL(V)$ med $D \subseteq \mathrm{Ker}\Phi$ alla gruppprepresentationer av G.

Den strategin fungerar bra i vissa fall t ex för grupper med Liealgebror av små dimensioner och för s k halvenkla grupper över vissa kroppar (t ex $\mathbb{R}$ eller $\mathbb{C}$). Vi skall ägna några ord åt dessa fall.

(10.24) Liealgebror av små dimensioner. Låt L vara en Liealgebra över en kropp K.

(a) Om $\dim_K L = 1$ så är $L = Ke$ med $[ee] = 0$. Om $K = \mathbb{R}$ så är L Liealgebran av $G = \mathbb{R}^+$.

(b) Om $\dim_K L = 2$ så $L = Ke_1 + Ke_2$. Om $[e_1e_2] = 0$ så är $[xy] = 0$ för godtyckliga $x, y \in L$

[†] $\Omega(G)$ har en naturlig topologisk struktur definierad av $\|\gamma_1 - \gamma_2\| = \sup_u \|\gamma_1(u) - \gamma_2(u)\|$.

[††] Diskret betyder att för varje $g \in D$ existerar en omgivning U i G så att $U \cap D = \{g\}$. Central betyder att $D \subseteq Z(G)$ där $Z(G) = \{x \in G : \forall_{g\in G} gx = xg\}$.

dvs L är en abelsk Liealgebra. Om $[e_1e_2] \neq 0$ så är $L^2 := [LL] = Ke$ för något $e \in L$, $e \neq 0$. Man kan välja en bas e_1, e_2 så att $[e_1e_2] = e_1$. Alltså får man två icke-isomorfa Liealgebror.

Om $K = \mathbb{R}$ svarar dessa två Liealgebror mot följande sammnhängande och enkelt sammanhängande Liegrupper: $G = \mathbb{R}^2$ (med addition) ger $\mathfrak{g}$ med $\mathfrak{g}^2 = 0$.

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{R},\, a > 0 \right\}$$

(med matrismultiplikation) ger $\mathfrak{g}$ med $\dim_{\mathbb{R}} \mathfrak{g}^2 = 1$ (se exempel (10.6)).

(c) Om $\dim_K L = 3$ är den allmänna klassifikationen relativt invecklad.

Fall 1. $\dim_K L^2 = 0$ dvs $[xy] = 0$ då $x, y \in L$. Då är L abelsk.

Fall 2. $\dim_K L^2 = 1$. Då är $[xy] = T(x, y)e$ där $e \in L$, $e \neq 0$ och $T(x, y) \in K$. $T(x, y)$ är en antisymmetrisk bilinjär form på L ($T : L \times L \to K$). Det finns två delfall:

Fall 2a. $T(x, e) = 0$ för varje $x \in L$. Då kan man välja en bas x, y, z för L över K med $[xy] = z$, $[xz] = [yz] = 0$ ($z = e$).

Fall 2b. Det finns $x \in L$ så att $T(x, e) = 1$. Då kan man välja en bas x, y, z så att $[xy] = [zy] = 0$ och $[xz] = z$ ($z = e$) (enkel övning).

Algebrorna i 2a och 2b är inte isomorfa (övning) – den första är isomorf med alla matriser

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$$

(med "+" och [,]), däremot den andra är en direkt summa $(Kx + Kz) + Ky$, där $Kx + Kz$ är Liealgebran ur (b) som inte är abelsk och Ky är algebran ur (a).

Fall 3. $\dim_K L^2 = 2$ – vi lämnar detta fall som Övning 2.

Fall 4. $\dim_K L^2 = 3$ dvs $L^2 = L$. Den allmänna klassifikationen är ekvivalent med klassifikationen av alla bilinjära symmetriska former i 3 variabler med koefficienter i K – ett ganska invecklat problem (se t ex I. Kaplansky, Liealgebras and locally compact groups, 1971). Vi begränsar oss till $K = \mathbb{R}$. Det finns två icke-isomorfa Liealgebror: $L_1 = \mathbb{R}x + \mathbb{R}y + \mathbb{R}z$ med $[xy] = z, [yz] = y$ – se exempel (10.20)(c), och $L_2 = \mathbb{R}x + \mathbb{R}y + \mathbb{R}z$ med $[xy] = 2y$, $[xz] = -2z$, $[yz] = x$.

Den andra algebran är isomorf med algebran av alla 2×2 – matriser med spåret lika med 0. En isomorfism ges då

$$x \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad y \mapsto \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad z \mapsto \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

L_1 är Liealgebran $su(2)$ av $SU(2)$ – se exempel (10.20)(c), och L_2 är Liealgebran av $SL(2,\mathbb{R})$ (se (10.18)(b). Observera dock att $SL_2(\mathbb{R})$ inte är enkelt sammanhängande och $sl_2(\mathbb{R})$ (se (10.23)(c)) inte kan realiseras som en delgrupp till $GL(n,\mathbb{C})$ för något n – bevis är inte enkelt). □

Vi skall avsluta med några kommentarer om halvenkla Liealgebror och motsvarande grupper. Som för associativa algebror definierar man enkla, och därefter, halvenkla Liealgebror.

(10.25) Definition. En Liealgebra L kallas **enkel** om $L^2 \neq 0$ och L saknar ideal $\neq 0, L$. Man säger att L är **halvenkel** om $L \cong L_1 \oplus \ldots \oplus L_t$ där L_i är enkla Liealgebror. Man säger att en sammanhängande Liegrupp är halvenkel om dess Liealgebra är halvenkel (jfr (9.14).

□

(10.26) Anmärkning. Det finns många ekvivalenta villkor för en Liealgebra att vara halvenkel. Ett villkor är särskilt viktigt. Låt $\kappa(x,y) = Tr(adx \cdot ady)$, där $x, y \in L$ (se (10.20)(b)). Då är κ en symmetrisk bilinjär form på L som kallas **Killingformen**. Man visar att L är halvenkel då och endast då denna form är icke-urartad (dvs $\kappa(x,L) = 0$ ger $x = 0$ – se Övn. 6.1). Halvenkelhelt av en Liegrupp kan karakteriseras med hjälp av gruppegenskaper (se t ex J.-P. Serre, Lie algebras and Lie groups, Benjamin, 1965 och 1987).

□

Klassifikationen av halvenkla Liealgebror är väl utarbetad. Låt oss nämna resultatet för $K = \mathbb{C}$.

(10.27) Enkla algebror över $\mathbb{C}$. Varje enkel Liealgebra över $\mathbb{C}$ är isomorf med någon av:

(a) A_n – algebran av alla komplexa $(n+1) \times (n+1)$ matriser med spåret 0 för $n = 1, 2, \ldots$.

(b) B_n – algebran av alla komplexa $(2n+1) \times (2n+1)$ antisymmetriska matriser för $n = 2, 3, \ldots$ $(B_1 \cong A_1)$.

(c) C_n – algebran av alla komplexa $(2n) \times (2n)$ matriser X som uppfyller $X^t D_{2n} + D_{2n} X = 0$, där

$$D_{2n} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix},$$

I_n är $n \times n$-enhetsmatrisen, för $n = 3, 4, \ldots$ ($C_1 \cong A_1$, $C_2 \cong B_2$).

(d) D_n – algebran av alla komplexa $(2n) \times (2n)$ antisymmetriska matriser för $n = 4, 5, \ldots$ (D_1 är abelsk, $D_2 \cong A_1 \oplus A_1$, $D_3 \cong A_3$).

(e) En av 5 ytterligare algebror som betecknas med G_2, F_4, E_6, E_7, E_8. □

Om $K = \mathbb{R}$ finns det 12 oändliga serier (som (a)–(d)) och 23 specialfall (som (e)). Samma klassifikation som över $\mathbb{C}$ får man över varje algebraiskt sluten kropp av karakteristiken 0.

ÖVNINGAR

10.1. Låt $A \in M_n(\mathbb{R})$. Visa att:

(a) serien

$$e^A = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \dots$$

konvergerar (se (10.7)),

(b) $e^A e^B = e^{A+B}$ då $A, B \in M_n(\mathbb{R})$ och $AB = BA$,

(c) $\det e^{C^{-1}AC} = \det e^A$ då $C \in GL(n, \mathbb{R})$,

(d) $\det e^A = e^{Tr(A)}$.

Ledningar. a) Låt $n = \max |a_{ij}|$, där $A = [a_{ij}]$. Uppskatta $\max |(A^n)_{ij}|$ med hjälp av m och n, där $(A^n)_{ij}$ är (i, j)-te elementet i A^n.

(d) Låt $D = C^{-1}AC$, där D är Jordans matris motsvarande A (se Kap. 8). Utnyttja (c) och det faktum att $Tr(C^{-1}AC) = Tr(A)$. Likheten (d) för matrisen D är enkel.

10.2. Låt L vara en Liealgebra över K med $\dim_K L = 3$ och $\dim_K L^2 = 2$. Visa att:

(a) L^2 som Liealgebra är abelsk.

Ledning: Antag att $L^2 = Kx + Ky$ med $[x, y] = y$. Komplettera x, y till en bas x, y, z för L över K. Betrakta $ad(z) : L^2 \to L^2$.

(b) Låt $L^2 = Kx + Ky$, $[x, y] = 0$ och låt A vara matrisen för $ad(z)$ i basen x, y för L^2. Visa att $\det A \neq 0$.

(c) Låt

$$[A] = \{B \in M_2(K) : \exists_{C \in GL(2,K),\, c \in K^*}\ cA = C^{-1}BC\}.$$

Visa att det finns 1 - 1 motsvarighet mellan isomorfiklasser av Liealgebror L över K med $\dim_K L = 3$, $\dim_K L^2 = 2$ och klasserna $[A]$, $A \in GL(2, K)$.

10.3. (a) Låt L vara Liealgebran ur (10.24)(b) Fall 1. Visa at den svarar mot $G = (\mathbb{R}^3, +)$.

(b) Låt L vara Liealgebran ur (10.24)(b) Fall 2 (a). Visa att den svarar mot Liegruppen av alla matriser

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

under multiplikation (jfr (10.6)(a)).

(b) Låt L vara Liealgebran ur (10.34)(b) Fall 2(b). Visa att den svarar mot Liegruppen $G_1 \times G_2$, där $G_1 = (\mathbb{R}, +)$, G_2 är gruppen ur (10.6)(a) med villkoret $a > 0$.

10.4. Låt $M_n(\mathbb{R})^\circ = \{A \in M_n(\mathbb{R}) : \det(E+A) \neq 0\}$. Kalla $A^\# = (E-A)(E+A)^{-1}$ för **Cayleybilden** av A då $A \in M_n(\mathbb{R})^\circ$. Visa att $A^\# \in M_n(\mathbb{R})^\circ$, $A^{\#\#} = A$ och motivera att funktionen $A \mapsto A^\#$ ger en homeomorfism av den öppna delmängden $M_n(\mathbb{R})^\circ$ till $M_n(\mathbb{R})$ med sig själv. Låt $G = O(n)$ (ortogonala gruppen över $\mathbb{R}$ av $(n \times n)$-matriser).

(a) Visa att om $A \in O(n)$, $A \in M_n(\mathbb{R})^\circ$ och $B = A^\#$ (se Övn. 4) så $A + B^t = 0$.

(b) Visa att om $B + B^t = 0$ så $B \in M_n(\mathbb{R})^\circ$ och $B^\# \in O(n)$.

(c) Motivera att $A \mapsto A^\#$ ger en homeomorfism av omgivningen $O(n)^\circ = O(n) \cap M_n(\mathbb{R})^\circ$ till E (enhetsmatrisen) med $\frac{n(n-1)}{2}$ – dimensionella rummet av alla antisymmetriska matriser i $M_n(\mathbb{R})$.

(d) Visa att man får en Liegruppstruktur på $O(n)$ genom att man mot omgivningen $O(n)^\circ C = \{AC : A \in O(n)^\circ\}$ av matrisen $C \in O(n)$ ordna Cayleybilderna $A^\#$ (kartorna på $O(n)$ är alltså $O(n)^\circ C$, $C \in O(n)$).

Anmärkning. På liknande sätt kan man introducera Liegruppstrukturen på många klassiska grupper. Mera naturligt genomför man den uppgiften med lite mera analys – se t ex F. W. Warner, Foundations of Differentiable Manifolds and Lie Groups, Theorem 3.34 och ett par efterföljande sidor.

Kapitel 11

KATEGORIER OCH FUNKTORER

Begreppen "kategori" och "funktor" är grunden för alla matematiska teorier och har en stor metodologisk betydelse[†]. Många begrepp som vi har diskuterat i tidigare kapitel finner sin naturliga plats som specialfall av mycket allmänna matematiska konstruktioner. Kategoriteorin bidrar till en bättre förståelse av dessa konstruktioner och gör det möjligt att jämföra olika matematiska begrepp. Vi återkommer till kategorier i nästa kapitel som ägnas åt en orientering om homologisk algebra.

(11.1) Definition. En **kategori** $\mathcal{C}$ är

(a) en klass av objekt $\mathcal{O}b(\mathcal{C})$

sådan att:

(b) för två godtyckliga objekt $M, N \in \mathcal{O}b(\mathcal{C})$ finns det en mängd $\mathrm{Mor}_{\mathcal{C}}(M, N)$ (eller kortare: $\mathrm{Mor}(M, N), (M, N)$) som kallas mängden av morfismer från M till N varvid

$$\mathrm{Mor}(M, N) \cap \mathrm{Mor}(M', N') = \emptyset$$

om $M \neq M'$ eller $N \neq N'$. Om $f \in \mathrm{Mor}(M, N)$ så skriver man $f : M \to N$ eller $M \xrightarrow{f} N$.

(c) För godtyckliga tre objekt $M, N, P \in \mathcal{O}b(\mathcal{C})$ finns det en avbildning

$$\mathrm{Mor}(M, N) \times \mathrm{Mor}(N, P) \to \mathrm{Mor}(M, P)$$

[†]Vill man bekanta sig lite mera med kategorier, kan man göra det med hjälp av t.ex. S. MacLanes bok "Categories for the Working Mathematician".

som mot $f : M \to N$ och $g : N \to P$ ordnar $g \circ f : M \to P$ (ibland skriver man gf) med följande egenskaper:

(c)$_1$ $(h \circ g) \circ f = h \circ (g \circ f)$ om $M \xrightarrow{f} N \xrightarrow{g} P \xrightarrow{h} R$,

(c)$_2$ för varje $M \in \mathcal{O}b(\mathcal{C})$ finns en morfism $1_M \in \mathrm{Mor}(M, M)$ sådan att $1_M \circ f = f$ då $f : M' \to M$ för ett objekt M', och $g \circ 1_M = g$ då $g : M \to M''$ för ett objekt M''.

□

(11.2) Exempel. Kategorin ${}_R\mathcal{M}$ (eller $\mathcal{M}od(R)$ då R är en kommutativ ring) av alla vänster-R-moduler (objekt) med $\mathrm{Mor}(M, N) = \mathrm{Hom}_R(M, N)$. Som ett viktigt speciallfall får vi kategorin $\mathcal{A}b$ av abelska grupper (då $R = \mathbb{Z}$). Ett annat viktigt fall är $\mathcal{V}ect_K$ – kategorin av vektorrum över en kropp K.

(b) Kategorin $\mathcal{R}ing$ vars objekt är ringar och $\mathrm{Mor}(R, R')$ är mängden av alla ringhomomorfismer av R i R'.

(c) Kategorin $\mathcal{T}op$ vars objekt är topologiska rum och $\mathrm{Mor}(X, X')$ är mängden av alla kontinuerliga avbildningar av X i X'.

(d) Kategorin $\mathcal{S}et$ (eller $\mathcal{E}ns$) av mängder i vilken morfismer $\mathrm{Mor}(X, X')$ är alla avbildningar av X i X'.

(e) Kategorin $\mathcal{G}r$ vars objekt är alla grupper och morfismer $\mathrm{Mor}(G, G')$ är alla grupphomomorfismer $f : G \to G'$.

(f) Kategorin $\mathcal{N}vs_\infty$ av alla normerade vektorrum (som objekt) och morfismer $\mathrm{Mor}(V, V')$ är alla begränsade linjära operatorer dvs $\varphi : V \to V'$ sådana att

$$\|\varphi\| = \sup_{\|x\| \leq 1} \|\varphi(x)\| < \infty.$$

(g) Kategorin $\mathcal{B}an_\infty$ av Banachrum med morfismer som i (f) (dvs morfismer är alla kontinuerliga linjära operatorer).

□

(11.3) Anmärkning. I fall då är det klart vilka morfismer man menar i en kategori beskriver man den genom dess objekt (t ex kategorin av alla R-moduler över en kommutativ ring – underförstått: Med homomorfismer av R-moduler som morfismer).

□

(11.4) Definition. Låt $\mathcal{C}, \mathcal{C}'$ vara två kategorier. Man säger att F är en **kovariant funktor** från $\mathcal{C}$ till $\mathcal{C}'$ och man skriver $F : \mathcal{C} \to \mathcal{C}'$ om för varje objekt $M \in \mathcal{O}b(\mathcal{C})$ finns $F(M) \in \mathcal{O}b(\mathcal{C}')$ och för varje morfism $f : M \to N$ finns en morfism $F(f) : F(M) \to F(N)$ så att

(a) $F(1_M) = 1_{F(M)}$ för varje $M \in \mathcal{O}b(\mathcal{C})$,

(b) $F(g \circ f) = F(g) \circ F(f)$ då $M \xrightarrow{f} N \xrightarrow{g} P$.

Man säger att F är en **kontravariant funktor** om för $f : M \to N$ är $F(f) : F(N) \to F(M)$ och i stället för (b) gäller $F(g \circ f) = F(f) \circ F(g)$.

□

(11.5) Exempel. (a) Definiera $F : \mathcal{M}od(R) \to \mathcal{M}od(R)$ genom $F(N) = \mathrm{Hom}_R(M, N)$, där M är en fixerad modul och för $\psi : N \to N'$,

$$F(\psi) = \bar{\psi} : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'),$$

där $\bar{\psi}(f) = \psi \circ f$ för $f : M \to N$. Då är F en kovariant funktor (se Övn. 10, 11, 13).

(b) I samma situation som i (a) låt $G : \mathcal{M}od(R) \to \mathcal{M}od(R)$ ges av $G(M) = \mathrm{Hom}_R(M, N)$ med N fixerad och för $\varphi : M' \to M$,

$$G(\varphi) = \bar{\varphi} : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N),$$

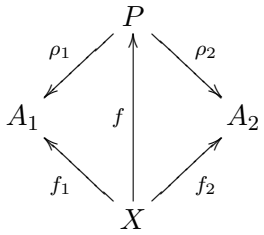
där $\bar{\varphi}(f) = f \circ \varphi$ för $f : M \to N$. G är en kontravariant funktor. Ett mycket viktigt specialfall får vi då $N = R$. Då är $G(M) = \mathrm{Hom}_R(M, R) = M^*$ den duala modulen (se Övn. 10, 11,13).

□

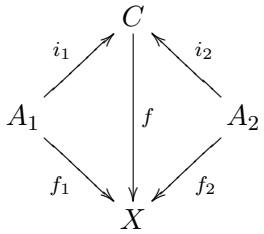
Det finns en lång lista av mycket viktiga och allmänna begrepp som kan definieras i kategorier under mer eller mindre restriktiva förutsättningar. Bland dessa begrepp kan nämnas som särskilt viktiga sådana som isomorfism, monomorfism, epimorfism, kärna, bild, kokärna, kobild, produkt, koprodukt, fibrerad och kofibrerad produkt, direkta och inversa limes, representerbar funktor och flera andra. Vi skall ägna övningar åt några av dessa begrepp. Som vårt första exempel betraktar vi begreppen produkt och koprodukt.

(11.6) Definition. Låt $\mathcal{C}$ vara en kategori. Man säger att (P, ρ_1, ρ_2) är en **produkt** av objekt $A_1, A_2 \in \mathcal{O}b(\mathcal{C})$, där $P \in \mathcal{O}b(\mathcal{C})$, $\rho_1 : P \to A_1$, $\rho_2 : P \to A_2$, om för varje objekt X i $\mathcal{C}$

och godtyckliga morfismer $f_1 : X \to A_1, f_2 : X \to A_2$ i $\mathcal{C}$ existerar en och endast en morfism $f : X \to P$ sådan att diagrammet



kommuterar. Man säger att (C, i_1, i_2) är en **koprodukt** av objekt $A_1, A_2 \in \mathcal{O}b(\mathcal{C})$, där $C \in \mathcal{O}b(\mathcal{C})$, $i_1 : A_1 \to C$, $i_2 : A_2 \to C$, om för varje objekt X i $\mathcal{C}$ och godtyckliga morfismer $f_1 : A_1 \to X$, $f_2 : A_2 \to X$ i $\mathcal{C}$ existerar en och endast en morfism $f : C \to X$ sådan att diagrammet



kommuterar. (Definitionen av "kobegreppet" får man genom att vända på alla pilar i definitionen av "begreppet").

□

(11.7) Exempel. Produkter existerar för godtyckliga par av objekt i $\mathcal{S}et$, $\mathcal{M}od(R)$, $\mathcal{R}ing$, $\mathcal{G}r$. I alla dessa fall ges produkten av A_1 och A_2 som den vanliga produkten $A_1 \times A_2$ med de naturliga projektionerna $\rho_i(a_1, a_2) = a_i$ då $i = 1, 2$. Koprodukter existerar i $\mathcal{S}et, Mod(R)$ och $\mathcal{G}r$ (i $\mathcal{G}r$ är konstruktionen något invecklad). För kommutativa och associativa R-algebror med etta är $A \otimes_R B$ koprodukten med $i_A : A \to A \otimes_R B$, där $a \mapsto a \otimes 1_B$, och $i_B : B \to A \otimes_R B$, där $b \mapsto 1_A \otimes b$ (se (4.22)). Se vidare Övn. 7.

□

Många matematiska begrepp kända från algebra, analys eller geometri kan formuleras i termer av kategorier. En sådan formulering kräver att begreppen kan definieras med hjälp av morfismer dvs "pilar". I själva verket definierar varje objekt en utvald morfism – den identiska, som fullständigt karakteriserar detta objekt (varje objekt har exakt en identisk morfism och olika objekt har olika sådana morfismer). Definitioner av matematiska begrepp i termer av

kategorier kräver ibland en förmåga att befria sig från ovidkommande detaljer i begreppets definition inom en konkret teori. Detta ger ofta en bättre förståelse av begreppen och en möjlighet till att jämföra olika begreppskonstruktioner. En nackdel kan vara att det krävs en viss vana för att inte avskräckas av pilarnas djungel. Låt oss fortsätta med några ytterligare exempel.

(11.8) Monomorfismer och epimorfismer. Om M och N är mängder så säger man att $f : M \to N$ är injektiv om $f(m) = f(m')$ ger $m = m'$ då $m, m' \in M$. Hur kan man formulera denna egenskap i termer av godtyckliga kategorier? Man utnyttjar här följande observation. Låt X vara en mängd och låt $g : X \to M$ och $h : X \to M$ vara två funktioner. Om f är injektiv så ger likheten $f \circ g = f \circ h$ att $g = h$ ty $f(g(m)) = f(h(m))$ ger $g(m) = h(m)$ för varje $m \in M$. Men även omvänt, om $f \circ g = f \circ h$ implicerar $g = h$ så måste f vara injektiv (se Övn. 4). Nu är det klart att en sådan tolkning av injektiviteten kan överföras till godtyckliga kategorier. Man säger att en morfism $f : M \to N$ i en kategori $\mathcal{C}$ är en **monomorfism** om för varje diagram i $\mathcal{C}$

$$X \underset{h}{\overset{g}{\rightrightarrows}} M \xrightarrow{f} N$$

implicerar $f \circ g = f \circ h$ att $g = h$. Man kan också uttrycka det så att funktionen:

$$_Xf : \mathrm{Mor}(X, M) \longrightarrow \mathrm{Mor}(X, N),$$

där $_Xf(g) = f \circ g$ för $g \in \mathrm{Mor}(X, M)$, är injektiv för varje $X \in Ob(\mathcal{C})$. Man kan lätt formulera motsvarande begrepp som svarar mot surjektiviteten. Man säger att $f : M \to N$ är en **epimorfism** om för varje diagram i $\mathcal{C}$.

$$M \xrightarrow{f} N \underset{h}{\overset{g}{\rightrightarrows}} X$$

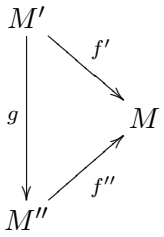
implicerar $g \circ f = h \circ f$ att $g = h$. Ett annat sätt att uttrycka den definitionen är en översättning till morfismmängder. $f : M \to N$ är en epimorfism om för varje objekt X i $\mathcal{C}$ är funktionen

$$f_X : \mathrm{Mor}(N, X) \to \mathrm{Mor}(M, X),$$

där $f_X(g) = g \circ f$ för $g \in \mathrm{Mor}(N, X)$, injektiv. Se vidare Övn. 4 när det gäller relationer mellan injektiva funktioner och monomorfismer samt surjektiva funktioner och epimorfismer.

(11.9) Isomorfismer och bijektiva funktioner. Med en isomorfism mellan två objekt M och N i en kategori $\mathcal{C}$ vars objekt har en mängdstruktur (t ex i $\mathcal{S}et$, $\mathcal{A}b$, $\mathcal{G}r$ eller $\mathcal{R}ing$) menar man vanligen en bijektiv funktion $f : M \to N$ som satisfierar ytterligare förutsättningar beroende på $\mathcal{C}$. I vanliga fall åtföljs en isomorfism f av sin invers $g : N \to M$, där $g \circ f = id_M$ och $f \circ g = id_N$. Nu kan vi konstatera att den sista egenskapen har en "kategorisk karaktär". I många viktiga fall implicerar existensen av g att f är både injektiv och surjektiv dvs bijektiv. I en godtycklig kategori $\mathcal{C}$ säger man att en morfism $f : M \to N$ är en **isomorfism** om det existerar $g : N \to M$ så att $g \circ f = id_M$ och $f \circ g = id_N$. Se vidare Övn. 4 som visar att man måste vara mycket försiktig när det gäller den intuitiva bakgrunden till denna definition.

(11.10) Delobjekt. Med hjälp av monomorfismer kan man definiera begreppet delobjekt till ett objekt $M \in \mathcal{O}b(\mathcal{C})$. Intuitivt är ett delobjekt till M en monomorfism $f' : M' \to M$. Men man vill gärna identifiera två monomorfismer f' och f'':



om det finns en isomorfism $g : M' \to M''$ så att diagrammet kommuterar dvs $f'' \circ g = f'$. Därför säger man att ett **delobjekt** till M är en ekvivalensklass av monomorfismer där två monomorfismer $f' : M' \to M$ och $f'' : M'' \to M$ är ekvivalenta om det existerar en isomorfism $g : M' \to M''$ sådan att $f'' \circ g = f'$. Vanligen säger man att $f' : M' \to M$ är ett delobjekt till M och då menar man ekvivalensklassen av f'.

Duala begreppet till delobjekt är kvotobjekt. Det är helt klart hur man definierar detta begrepp, men vi gör det ändå. Ett **kvotobjekt** av M är en ekvivalensklass av epimorfismer från M, där två epimorfismer $g' : M \to M'$ och $g'' : M \to M''$ anses ekvivalenta om det existerar en isomorfism $g : M' \to M''$ sådan att $g \circ f' = f''$. □

För att kunna utveckla en tillräcklig djup teori som är fri från "patologiska exempel" och samtidigt har intressanta modeller krävs det ofta något starkare förutsättningar om kategorier. Två klasser av kategorier är särskilt viktiga – additiva och abelska.

(11.11) Definition. Man säger att en kategori $\mathcal{C}$ är **additiv** om för godtyckliga objekt $M, N \in \mathcal{O}b(\mathcal{C})$ är $\mathrm{Mor}(M, N)$ en abelsk grupp så att

(a) för $M, N, P \in \mathcal{O}b(\mathcal{C})$ är avbildningen

$$\mathrm{Mor}(M, N) \times \mathrm{Mor}(N, P) \to \mathrm{Mor}(M, P)$$

bilinjär,

(b) det finns ett objekt $O \in \mathcal{O}b(\mathcal{C})$ sådant att för varje objekt $M \in \mathcal{O}b(\mathcal{C})$ har mängderna $\mathrm{Mor}(O, M)$ och $\mathrm{Mor}(M, O)$ exakt ett element,

(c) för godtyckliga $M, N \in \mathcal{O}b(\mathcal{C})$ existerar produkt och koprodukt.

I additiva kategorier brukar man beteckna $\mathrm{Mor}(M, N)$ med $\mathrm{Hom}(M, N)$. Den enda morfismen i $\mathrm{Hom}(M, O)$ eller $\mathrm{Hom}(O, M)$) brukar betecknas med 0 (utan större fara för missförstånd).

En funktor $F : \mathcal{C} \to \mathcal{C}'$, där $\mathcal{C}'$ också är additiv, kallas för en **additiv funktor** om för varje par av objekt $M, N \in \mathcal{C}$ är avbildningen $F : \mathrm{Hom}_{\mathcal{C}}(M, N) \to \mathrm{Hom}_{\mathcal{C}'}(F(M), F(N))$ en grupphomomorfism.

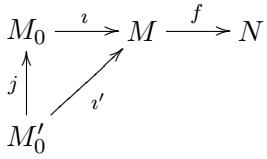
□

(11.12) Exempel. Kategorin $\mathcal{M}od(R)$ i (11.2) (a) är additiv. Funktorerna i exempel (11.5) (a) och (b) är additiva.

□

I additiva kategorier kan man definiera begreppen kärna (kokärna) och bild (kobild) till en godtycklig morfism $f : M \to N$. Man kan också definiera begreppet exakt sekvens. Låt oss definiera dessa begrepp (i samband med definitionerna tänk alltid på moduler och modulhomomorfismer).

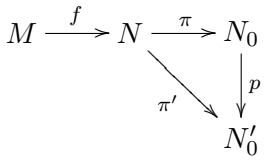
(11.13) Definition. Låt $f : M \to N$ vara en morfism i en additiv kategori $\mathcal{C}$. Med **kärnan** $\mathrm{Ker} f$ till f menas ett delobjekt $\imath : M_0 \to M$ (mera exakt, ekvivalensklassen av $\imath$ – se (11.10)) med följande egenskaper:



(a) $f \circ \imath = 0$,

(b) om $\imath' : M_0' \to M$ är en morfism sådan att $f \circ \imath' = 0$ så existerar en morfism $j : M_0' \to M_0$ så att $\imath \circ j = \imath'$.

Begreppet kokärna definieras på motsvarande sätt då "pilarna till M" ersätts med "pilarna från N" dvs ett kvotobjekt $\pi : N \to N_0$ kallas **kokärnan** $\mathrm{Coker} f$ till f om följande villkor gäller:



(a) $\pi \circ f = 0$,

(b) om $\pi' : N \to N_0'$ är en morfism sådan att $\pi' \circ f = 0$ så existerar en morfism $p : N_0 \to N_0'$ så att $p \circ \pi = \pi'$.

□

Ett annat sätt att definiera dessa begrepp (som inkluderar egenskaper av delobjekt, respektive, kvotobjekt) är följande. $\imath : M_0 \to M$ är kärnan till f om för varje objekt X i $\mathcal{C}$ är följden av de abelska grupperna:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(X, M_0) \to \mathrm{Hom}_{\mathcal{C}}(X, M) \to \mathrm{Hom}_{\mathcal{C}}(X, N)$$

exakt (jfr (11.8) och se (3.25) för definitionen av en exakt följd av abelska grupper). På liknande sätt är $\pi : N \to N_0$ kokärnan till f om för varje objekt X i $\mathcal{C}$ är följden av de abelska grupperna:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(N_0, X) \to \mathrm{Hom}_{\mathcal{C}}(N, X) \to \mathrm{Hom}_{\mathcal{C}}(M, X)$$

exakt (jfr (11.8)).

Begeppen bild och kobild kan definieras med hjälp av begreppen kärna och kokärna. Om $f : M \to N$ är en homomorfism av moduler över en ring (t ex av två vektorrum över en kropp) så är $\mathrm{Ker} f = \{m \in M : f(m) = 0\}$ (i (11.10) är $\mathrm{Ker} f$ delobjektet $\imath : \mathrm{Ker} f \to M$, där $\imath$ är identiteten på $\mathrm{Ker} f$). Kokärnan är epimorfismen $\pi : N \to N/\mathrm{Im} f$, där $\mathrm{Im} f$ är bilden av f (kontrollera att detta stämmer med (11.10)). Den omständigheten visar samtidigt hur man kan definiera bilden till f. Det är klart att bilden är kärnan till π. Detta är grunden för följande definition.

(11.14) Definition. Med **bilden** av en morfism $f : M \to N$ i en additiv kategori $\mathcal{C}$ menar man kärnan till $\pi : N \to N_0$, där π är kokärnan till f. Duallt säger man att **kobilden** till f är kokärnan till $\imath : M_0 \to M$, där $\imath$ är kärnan till f.

□

Det är helt klart att kärnor, kokärnor, bilder och kobilder inte behöver existera i helt godtyckliga additiva kategorier (se vidare Övn. 5). Därför ställer man ytterligare krav på additiva kategorier för att tillförsäkra sig om existensen av dessa genom att införa abelska kategorier. Men låt oss poängtera att additiva kategorier som inte är abelska också har en mycket stor betydelse. För att definiera abelska kategorier låt oss först undersöka ett viktigt samband mellan bilden och kobilden. För moduler över ringar existerar en viktig sekvens:

$$\mathrm{Ker}f \longrightarrow M \longrightarrow \mathrm{Coim}f \xrightarrow{f^*} \mathrm{Im}f \longrightarrow N \longrightarrow \mathrm{Coker}f$$

då $f : M \to N$ är en homomorfism. Morfismen f^* avbildar sidoklassen $m + \mathrm{Ker}f$ i $\mathrm{Coim}f = M/\mathrm{Ker}f$ på $f(m)$ och "huvudsatsen om modulhomomorfismer" säger att f^* är en isomorfism (se (3.11) och även (1.38)). Vad kan man säga om existensen av f^* i godtyckliga additiva kategorier?

(11.15) Proposition. *Låt $f : M \to N$ vara en morfism i en additiv kategori $\mathcal{C}$ och anta att både* $\mathrm{Im}f$ *och* $\mathrm{Coim}f$ *existerar (alltså existerar också* $\mathrm{Ker}f$ *och* $\mathrm{Coker}f$*). Om*

$$\pi : M \to \mathrm{Coim}f \quad \textit{och} \quad \imath : \mathrm{Im}f \to N$$

är respektive kobilden och bilden av f så existerar exakt en morfism $f^* : \mathrm{Coim}f \to \mathrm{Im}f$ sådan att i diagrammet

$$M \xrightarrow{\pi} \mathrm{Coim}f \xrightarrow{f^*} \mathrm{Im}f \xrightarrow{\imath} N$$

är $f = \imath \circ f^* \circ \pi$.

Bevis. Enligt (11.13) har man följande diagram:

$$\begin{array}{ccccccc} \mathrm{Ker}f & \xrightarrow{\imath_0} & M & \xrightarrow{\pi} & \mathrm{Coim}f = \mathrm{Coker}\,\imath_0 & & \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \pi'} & & & \\ \mathrm{Coker}f & \xleftarrow{\pi_0} & N & \xleftarrow{\imath} & \mathrm{Im}f = \mathrm{Ker}\,\pi_0 & & \end{array}$$

Entydigheten av f^* följer på följande sätt. Antag att det även finns $g : \mathrm{Coim}f \to \mathrm{Im}f$ så att $\imath \circ g \circ \pi = \imath \circ f^* \circ \pi$. Men $\imath$ är en monomorfism så att $g \circ \pi = f^* \circ \pi$, och π är en epimorfism så att $g = f^*$.

För att visa existensen av f^* observerar vi först att $f \circ \imath_0 = 0$. Enligt definitionen av $\mathrm{Coker}\imath_0$ existerar en morfism $\pi' : \mathrm{Coker}\imath_0 \to N$ sådan att $\pi' \circ \pi = f$. Men $\pi_0 \circ \pi' = 0$ ty

$\pi_0 \circ \pi' \circ \pi = \pi_0 \circ f = 0$ (enligt definitionen av π_0) och π är en epimorfism så att $\pi_0 \circ \pi' \circ \pi = 0$ ger $\pi_0 \circ \pi' = 0$. Definitionen av $\imath$ ger nu existensen av f^* med egenskapen $\imath \circ f^* = \pi'$. Alltså är $\imath \circ f^* \circ \pi = \pi' \circ \pi = f$. □

Resonemanget ovan är mycket typiskt för bevisföring i termer av kategorier. Det kräver inte någon större fyndighet, men man måste vara helt vaken för att dra lämpliga pilar och inte förväxla deras riktningar. Nu kan vi definiera abelska kategorier.

(11.16) Definition. Man säger att en additiv kategori $\mathcal{C}$ är **abelsk** om

a) varje morfism i $\mathcal{C}$ har kärna och kokärna,

b) varje morfism i $\mathcal{C}$ som är monomorfism och epimorfism är en isomorfism,

c) för varje morfism f är morfismen $f^* : \mathrm{Coim}f \to \mathrm{Im}f$ (se (11.15)) en isomorfism.

□

Som exempel på abelsk kategori låt oss nämna $\mathcal{M}od(R)$.

Abelska kategorier gör det möjligt att utveckla begreppsapparat känd för moduler över ringar. I själva verket finns resultat som visar att många bevis i sådana kategorier kan genomföras då man i stället för objekt och morfismer betraktar moduler och modul homomorfismer över ringar. För att precisera den tanken låt oss betrakta exakta sekvenser och exakta funktorer.

(11.17) Definition. Man säger att en sekvens av objekt och morfismer i en abelsk kategori $\mathcal{C}$:

$$(*) \qquad M' \xrightarrow{f} M \xrightarrow{g} M''$$

är **exakt** om $\mathrm{Im}f = \mathrm{Ker}g$. En kovariant funktor $F : \mathcal{C} \to \mathcal{C}'$, där $\mathcal{C}'$ också är en abelsk kategori, kallas **exakt** om den är additiv och för varje exakt sekvens $(*)$ är sekvensen

$$F(M') \to F(M) \to F(M'')$$

exakt. Man säger att F är **vänsterexakt** om för varje exakt sekvens

$$0 \to M' \to M \to M''$$

är sekvensen

$$0 \to F(M') \to F(M) \to F(M'')$$

exakt, och **högerexakt** om för varje exakt sekvens

$$M' \to M \to M'' \to 0$$

är sekvensen

$$F(M') \to F(M) \to F(M'') \to 0$$

exakt.

□

Dualt definierar man exakta, vänsterexakta och högerexakta kontravarianta funktorer. En funktor som är både höger- och vänsterexakt är exakt (enkel övning).

(11.18) Exempel. Funktorerna $M \mapsto \mathrm{Hom}_R(M, N)$ och $N \mapsto \mathrm{Hom}_R(M, N)$ är vänsterexakta (se Övn. 10, 11, 13) och funktorn $M \mapsto M \otimes_R N$ är högerexakt (se Övn. 14).

□

Nu kan vi beskriva samband mellan abelska kategorier och kategorier av moduler över ringar. Följande sats visades av Freyd, Grothendieck och Lubkin:

(11.19) Inbäddningssatsen för abelska kategorier. *Låt $\mathcal{C}$ vara en abelsk kategori vars objekt bildar en mängd. Då existerar en exakt funktor $F : \mathcal{C} \to \mathcal{M}od(\mathbb{Z})$ som är injektiv på både objekt och morfismer.*

Detta resultat förbättrades av Mitchell[†] som visade att man kan välja en ring R så att det existerar en funktor $F : \mathcal{C} \to \mathcal{M}od(R)$ som är **full** vilket betyder att för godtyckliga objekt M och N i $\mathcal{C}$ är avbildningen $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(F(M), F(N))$ en isomorfism (och inte bara en monomorfism som i (11.19)). Vi skall dra en praktisk nytta av dessa resultat i Kapitel 18 då vi diskuterar kort homologisk algebra. Som påpekas av H. Bass i hans bok "Algebraic K-theory" påminner förhållandet mellan abelska kategorier och kategorier av moduler över ringar om förhållandet mellan grupper och deras representationer i form av t ex matrisgrupper. Med andra ord är teorin för "abstrakta" abelska kategorier ofta nödvändig trots att det finns vissa möjligheter att representera dem som delkategorier till kategorier av moduler över ringar.

[†]Inbäddningssatsen samt dess generalisering visas i B. Mitchells bok "Theory of Categories", Academic Press, 1965.

ÖVNINGAR

11.1. Visa att $\mathcal{C}$ är en kategori med lämpligt definierad avbildning

$$\mathrm{Mor}(A,B)\times\mathrm{Mor}(B,C)\to\mathrm{Mor}(A,C)$$

då:

(a) $\mathcal{O}b(\mathcal{C})=\{1,2,3,\ldots\}$,

$$\mathrm{Mor}(i,j)=\begin{cases} i\to j & \text{om} \quad i|j,\\ \emptyset & \text{om} \quad i\nmid j.\end{cases}$$

(b) $\mathcal{O}b(\mathcal{C})=$ alla delmängder till en mängd X,

$$\mathrm{Mor}(A,B)=\begin{cases} A\to B & \text{då} \quad A\subseteq B,\\ \emptyset & \text{då} \quad A\not\subseteq B.\end{cases}$$

(c) Generalisera (a) och (b).

(d) $\mathcal{O}b(\mathcal{C})=$ en grupp G, $\mathrm{Mor}(G,G)=$ alla element i G. Visa här att en kategori med ett enda objekt G sådant att $\mathrm{Mor}(G,G)$ enbart består av isomorfismer har den egenskapen att $\mathrm{Mor}(G,G)$ är en grupp.

(e) $\mathcal{O}b(\mathcal{C})=$ alla ringar med etta, $\mathrm{Mor}(R,R')=$ alla homomorfismer sådana att ettan 1_R går på ettan $1_{R'}$.

(f) $\mathcal{O}b(\mathcal{C})=\{1,2,3,\ldots\}$, $\mathrm{Mor}(i,j)=$ alla (j,i)-matriser med element ur en kropp K.

11.2. Låt $\mathcal{C}$ vara en kategori. Man säger att ett objekt O i $\mathcal{O}b(\mathcal{C})$ är **initialt** om för varje objekt A i $\mathcal{C}$ finns exakt en morfism $O\to A$. Duala begreppet kallas **ändobjekt**[†]

(a) Bestäm initialobjekt och ändobjekt (om de existerar) i $\mathcal{S}et$, $\mathcal{M}od(R)$ samt kategorierna ur Övn. 1.

(b) Visa att initialobjekt och ändobjekt är entydigt bestämda så när som på isomorfism om de existerar.

(c) Motivera att $V\otimes_K W$, $V\wedge V$ och symmetrisk produkt kan tolkas som initiala objekt i lämpliga kategorier (V,W är K-vektorrum över en kropp K).

11.3. Låt $\mathcal{C}$ vara en kategori.

(a) Låt M vara ett fixerat objekt i $\mathcal{C}$. Motivera att ${}_Mh:\mathcal{C}\to\mathcal{S}et$ är en kovariant funktor om ${}_Mh(X)=\mathrm{Mor}(M,X)$ och ${}_Mh(\varphi)(f)=\varphi\circ f$, där $M\xrightarrow{f}X\xrightarrow{\varphi}X'$.

(b) Låt N vara ett fixerat objekt i $\mathcal{C}$. Motivera att $h_N:\mathcal{C}\to\mathcal{S}et$ är en kontravariant funktor om $h_N(X)=\mathrm{Mor}(X,N)$ och $h_N(\psi)(f)=f\circ\psi$, där $X'\xrightarrow{\psi}X\xrightarrow{f}N$.

11.4. Låt $\mathcal{C}$ vara en kategori.

(a) Visa att i kategorierna $\mathcal{S}et$, $\mathcal{M}od(R)$, $\mathcal{R}ing$ är en morfism en monomorfism då och endast då den är injektiv som funktion (dvs olika element går på olika).

[†]På engelska kallas dessa objekt: "universally repelling" och "universally attracting".

(b) Visa att i kategorierna $\mathcal{S}et$, $\mathcal{M}od(R)$ är en morfism en epimorfism då och endast då den är surjektiv (dvs "på"). Visa att det inte är sant i kategorin av kommutativa ringar med etta (där morfismer avbildar ettan på ettan).

(c) Visa att en isomorfism är både epi- och monomorfism.

(d) Ge ett exempel på en kategori vars objekt är (vissa) mängder och som har den egenskapen att det finns i den kategorin morfismer som är mono utan att vara injektiva samt epi utan att vara surjektiva.

Svar. Låt $\mathcal{C}$ bestå av två objekt, A, B som är två olika mängder med $\mathrm{Mor}(A,A) = \{1_A\}$, $\mathrm{Mor}(B,B) = \{1_B\}$, $\mathrm{Mor}(A,B) = \{\varphi\}$, där φ är varken injektion eller surjektion, $\mathrm{Mor}(B,A) = \emptyset$.

(e) Låt $\mathcal{B}an_{\mathbb{R}}$ vara kategorin av Banachrum över $\mathbb{R}$ med morfismer $\mathrm{Mor}(V,W) =$ alla kontinuerliga linjära avbildningar. Visa att i den kategorin finns morfismer som är både mono och epi utan att vara iso.

11.5. Låt $\mathcal{C}$ vara kategorin av ändligt genererade fria $\mathbb{Z}$-moduler med modulhomomorfismer som morfismer. Är den kategorin additiv? Är den abelsk?

11.6. Låt $F : \mathcal{C} \to \mathcal{C}'$, $G : \mathcal{C} \to \mathcal{C}'$ vara två kovarianta funktorer. Man säger att F och G är **isomorfa** om det för varje objekt X i $\mathcal{C}$ finns en isomorfism $\alpha_X : F(X) \to G(X)$ så att för varje morfism $f : X \to X'$ i $\mathcal{C}$ kommuterar diagrammet

$$\begin{array}{ccc} F(X) & \xrightarrow{\alpha_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(X') & \xrightarrow{\alpha_{X'}} & G(X') \end{array}$$

Visa att funktorerna $F, G : \mathcal{M}od(R) \to \mathcal{M}od(R)$, där $F(X) = X \otimes_R R/I$ och $G(X) = X/IX$ (I ett fixerat R-ideal) är isomorfa (för $f : X \to X'$ är $F(f) = f \otimes id$, och $G(f) = f^*$, där $f^* : X/IX \to X'/IX'$ induceras av f).

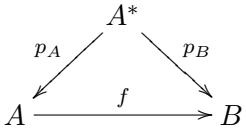
11.7. Man säger att en kovariant funktor $F : \mathcal{C} \to \mathcal{S}et$ är **representerbar** om det finns ett objekt $A_F \in \mathcal{O}b(\mathcal{C})$ sådant att funktorerna F och h_{A_F} (se Övn. 3 – ${}_{A_F}h(x) = \mathrm{Mor}(A_F, X)$) är isomorfa (se Övn. 6). En kontravariant funktor $F : \mathcal{C} \to \mathcal{S}et$ är **representerbar** om det finns ett objekt $A_F \in \mathcal{O}b(\mathcal{C})$ sådant att funktorerna F och h_{A_F} (se Övn. 3 – $h_{A_F}(X) = \mathrm{Mor}(X, A_F)$) är isomorfa.

(a) Visa att om M, N är två R-moduler och $F : \mathcal{M}od(R) \to \mathcal{S}et$ definieras som $F(X) = \mathrm{Bil}_R(M \times N, X)$ och $F(\varphi) : \mathrm{Bil}_R(M \times N, X) \to \mathrm{Bil}_R(M \times N, X')$ för $\varphi : X \to X'$, där $F(f)$ är sammansättningen $M \times N \to X \to X'$ så är F representerbar av $M \otimes_R N$ (mera exakt säger mana att F representeras av A_F och ρ_F, där ρ_F är bilden av 1_{A_F} vid isomorfism $\mathrm{Mor}(A_F, A_F) \cong F(A_F)$).

(b) Visa att om M, N är två R-moduler och $F : \mathcal{M}od(R) \to \mathcal{S}et$ definieras som $F(X) = \mathrm{Hom}_R(X, M_1) \times \mathrm{Hom}_R(X, M_2)$ (definiera lämpligt $F(X') \to F(X)$ då $\varphi : X \to X'$ är given i $\mathcal{M}od(R)$) så är F representerbar av $M_1 \times M_2$ (direkta produkten av M_1 och M_2). Jfr Övn. 3.9.

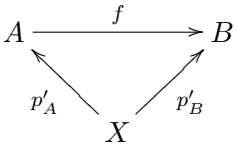
11.8. Låt $\mathcal{C}$ vara en kategori och $\mathcal{T}$ en liten delkategori till $\mathcal{C}$ (dvs $\mathcal{T}$ är en kategori vars objekt bildar en mängd $\mathcal{O}b(\mathcal{T}) \subseteq \mathcal{O}b(\mathcal{C})$, och för varje par $A, B \in \mathcal{O}b(\mathcal{T})$ är $\mathrm{Mor}_{\mathcal{T}}(A,B) \subseteq \mathrm{Mor}_{\mathcal{C}}(A,B)$). Med **inversa limes** $\varprojlim \mathcal{T}$ menar man ett objekt $A^* \in \mathcal{O}b(\mathcal{C})$ och morfismer $p_A : A^* \to A$ för varje $A \in \mathcal{O}b(\mathcal{T})$ sådana att följande villkor är uppfyllda:

(i)

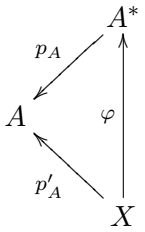


kommuterar för varje $f \in \mathrm{Mor}_{\mathcal{T}}(A,B)$.

(ii) Om $X \in \mathcal{O}b(\mathcal{C})$ och $p'_A : X \to A$ är morfismer i $\mathcal{C}$ sådana att



kommuterar för varje $f \in \mathrm{Mor}_{\mathcal{T}}(A,B)$ så existerar exakt en morfism $\varphi : X \to A^*$ sådan att



kommuterar för varje $A \in \mathcal{O}b(\mathcal{T})$.

Duala begreppet (man vänder på alla pilar) kallas **direkta limes** och betecknas $\varinjlim \mathcal{T}$

(a) Vad är $\varprojlim \mathcal{T}$ och $\varinjlim \mathcal{T}$ då $\mathcal{T}$ saknar morfismer $\neq i_A$ för $A \in \mathcal{O}b(\mathcal{T})$?

Svar. $\varprojlim \mathcal{T} = \prod_{A \in \mathcal{O}b(\mathcal{T})} A$ är produkten av alla objekt A i $\mathcal{T}$, $\varinjlim \mathcal{T} = \coprod_{A \in \mathcal{O}b(\mathcal{T})} A$ är koprodukten av alla objekt A i $\mathcal{T}$.

(b) Bestäm $\varinjlim$ och $\varprojlim$ för kategorier i Övn. 1 (a), (b) (om dessa existerar).

(c) Låt $\mathcal{T}$ vara en kategori, $\mathcal{O}b(\mathcal{T}) = \{A, B, C\}$, $\mathrm{Mor}(A,C) = \{f : A \to C\}$ och $\mathrm{Mor}(B,C) = \{g : B \to C\}$, $\mathrm{Mor}(X,X) = \{i_x\}$ för $X \in \mathcal{O}b(\mathcal{T})$). $\varprojlim \mathcal{T}$ kallas **pull-back** eller **fibrerad produkt** av A och B över C. Den betecknas $A \times_C B$. Ge en beskrivning av $A \times_C B$ då $\mathcal{C} = \mathcal{S}et$, $\mathcal{M}od(R)$.

Anmärkning. Duala begreppet kallas **push-out** eller **kofibrerad produkt** och betecknas $A \coprod_C B$.

(d)* Ge en beskrivning av $\varinjlim$ och $\varprojlim$ för $\mathcal{C} = \mathcal{S}et$.

Ledning. Man hittar dessa beskrivningar i många läroböcker om man inte vill bevisa (d) på egen hand.

11.9. Låt R vara en ring och M, M_i, $i \in I$, N_j, $j \in J$, R-moduler. Visa att:

(a) $\mathrm{Hom}_R(\coprod_i M_i, N) \cong \prod_i \mathrm{Hom}_R(M_i, N)$,

(b) $\mathrm{Hom}_R(M, \prod_j N_j) \cong \prod_j \mathrm{Hom}_R(M, N_j)$,

(c) $(\coprod_i M_i) \otimes N \cong \coprod_i (M_i \otimes N)$,

Ledning. Man kan lösa problemet genom att använda "abstract nonsense" och definitionerna av $\coprod, \prod$.

11.10. Ge exempel på en kategori i vilken produkt och koprodukt inte existerar för en lämplig uppsättning av objekt.

11.11. Visa att funktorerna (a) $M \mapsto \mathrm{Hom}_R(M, N)$ och (b) $N \mapsto \mathrm{Hom}_R(M, N)$ är vänsterexakta (se (11.5) och (11.8)).

Lösning av (a): Antag att $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ är exakt. Man skall visa att även

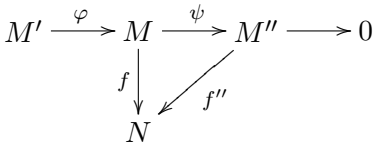
$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(M, N) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(M', N)$$

är exakt.

Steg 1. $\mathrm{Ker}\,\bar{\psi} = (0)$ dvs om $\bar{\psi}(f'') = 0$ så är $f'' = 0$, där $f'' : M'' \to N$. Betrakta $M \xrightarrow{\psi} M'' \xrightarrow{f''} N$. Villkoret $\bar{\psi}(f'') = f'' \circ \psi = 0$ betyder att $(f'' \circ \psi)(m) = f''(\psi(m)) = 0$ för varje $m \in M$. Men varje element $m'' \in M''$ kan skrivas på formen $m'' = \psi(m)$ (ty ψ är epi) så att $f''(m'') = 0$ för alla $m'' \in M''$ dvs $f'' = 0$.

Steg 2. $\mathrm{Im}\bar{\psi} \subseteq \mathrm{Ker}\bar{\varphi}$ dvs $\bar{\varphi} \circ \bar{\psi} = 0$ (se (3.26)(d)). Men $(\bar{\varphi} \circ \bar{\psi})(f'') = f'' \circ \psi \circ \varphi = 0$ för varje $f'' : M'' \to N$, ty $\psi \circ \varphi = 0$ (se (3.26)(d)).

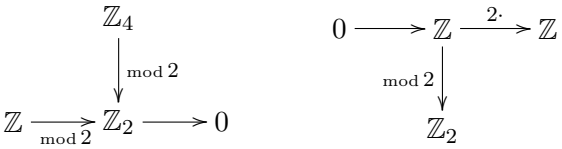
Steg 3. $\mathrm{Im}\bar{\psi} \supseteq \mathrm{Ker}\bar{\varphi}$. Betrakta diagrammet:



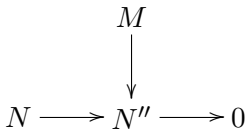
där $f \circ \varphi = 0$. Vi måste visa att om $\bar{\varphi}(f) = f \circ \varphi = 0$ så finns det f'' så att $\psi(f'') = f'' \circ \psi = f$. Villkoret $f \in \mathrm{Ker}\bar{\varphi}$ betyder $\bar{\varphi}(f) = f \circ \varphi = 0$ dvs $\mathrm{Ker}\psi = \mathrm{Im}\varphi \subseteq \mathrm{Ker}f$. Existensen av f'' följer nu direkt ur Övn. 3.30 (vi ger dock ett kort bevis här: om $m'' \in M''$ så är $m'' = \psi(m)$, där $m \in M$ och man definierar $f''(m'') = f(m)$. Den definitionen är korrekt, ty $m'' = \psi(m_1)$ ger $m - m_1 \in \mathrm{Ker}\psi \subseteq \mathrm{Ker}f$ dvs $f(m) = f(m_1)$).

11.12. Visa att funktorerna $N \mapsto \mathrm{Hom}_R(M, N)$ och $M \mapsto \mathrm{Hom}_R(M, N)$ inte är höger exakta

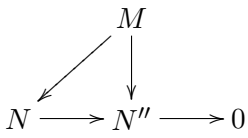
Ledning. Betrakta diagrammen:



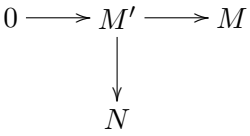
Anmärkning. Funktorn $N \mapsto \mathrm{Hom}_R(M, N)$ är högerexakt då och endast då varje diagram



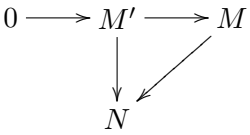
kan kompletteras till ett kommutativt diagram



Modulen M kallas då **projektiv** (se Övn. 3.21 (b)). Funktorn $M \mapsto \mathrm{Hom}_R(M, N)$ är högerexakt då och endast då varje diagram

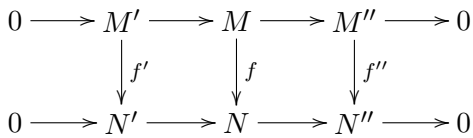


kan kompletteras till ett kommutativt diagram



Då säger man att N är **injektiv**. Vi återkommer till projektiva och injektiva moduler i Kapitel 18.

11.13. Man säger att sekvenserna $0 \to M' \to M \to M'' \to 0$ och $0 \to N' \to N \to N'' \to 0$ av R-moduler och R-homomorfismer är isomorfa om diagrammet



är kommutativt och f', f, f'' är R-isomorfismer. Visa att om en rad i detta diagram är exakt så är också den andra.

11.14. Låt $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ vara en sekvens av R-moduler och R-homomorfismer.

(a) Visa att om sekvensen

$$\mathrm{Hom}_R(M'', N) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(M, N) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(M', N) \longrightarrow 0$$

är exakt för varje R-modul N så är sekvensen

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

exakt (se (11.5)(b)).

(b) Visa motsvarande egenskap hos funktorn $N \mapsto \mathrm{Hom}_R(M, N)$.

Lösning av (a): Antag att Hom-sekvensen är exakt för varje N.

Steg 1. ψ är epi. Betrakta diagrammet $M \xrightarrow{\psi} M'' \xrightarrow{f''} M''/\mathrm{Im}\psi$, där f'' är den naturliga surjektionen ($N = M''/\mathrm{Im}\psi$). Vi har $\bar{\psi}(f'') = f'' \circ \psi = 0$. Alltså är $f'' = 0$, ty $\bar{\psi}$ är mono. Detta betyder at $M''/\mathrm{Im}\psi = 0$ dvs $\mathrm{Im}\psi = M''$ så att ψ är epi.

Steg 2. $\mathrm{Im}\varphi \subseteq \mathrm{Ker}\psi$. Här måste vi visa att $\psi \circ \varphi = 0$. Vi vet att $(\bar{\varphi} \circ \bar{\psi})(f'') = f'' \circ \psi \circ \varphi = 0$ för varje $f'' : M'' \to N$. Tag $N = M''$ och $f'' = id_{M''}$. Då är sammansättningen

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \xrightarrow{id_{M''}} M''$$

lika med 0 dvs $\psi \circ \varphi = 0$.

Steg 3. $\mathrm{Im}\varphi \subseteq \mathrm{Ker}\psi$. Betrakta diagrammet

$$\begin{array}{ccccccc} M' & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle f''} & & & \\ & & M/\mathrm{Im}\varphi & & & & \end{array}$$

där f är den naturliga surjektionen ($N = M/\mathrm{Im}\varphi$). Vi har $\bar{\varphi}(f) = f \circ \varphi = 0$ dvs $f \in \mathrm{Ker}\bar{\varphi} = \mathrm{Im}\bar{\psi}$ så att det finns f'' sådan att $f = f'' \circ \psi$. Alltså är $\mathrm{Im}\varphi = \mathrm{Ker}f = \mathrm{Ker}(f'' \circ \psi) \supseteq \mathrm{Ker}\psi$.

11.15. Visa att $M \mapsto M \otimes_R N$ är högerexakt dvs om $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ är exakt så är

$$M' \otimes_R N \xrightarrow{f \otimes id_N} M \otimes_R N \xrightarrow{g \otimes id_N} M'' \otimes_R N \longrightarrow 0$$

exakt. Visa också att denna funktor inte är vänsterexakt.

Lösning: Definiera $F : \mathcal{M}od(R) \to \mathcal{M}od(R)$ och $G : \mathcal{M}od(R) \to \mathcal{M}od(R)$ så att

$$F(X) = \mathrm{Hom}_R(X, \mathrm{Hom}_R(N, P)) \quad \text{och} \quad G(X) = \mathrm{Hom}_R(X \otimes_R N, P),$$

där P är en fixerad R-modul [†]. Nu vet vi enligt Övn. 11 att sekvensen

$$0 \longrightarrow F(M'') \longrightarrow F(M) \longrightarrow F(M')$$

är exakt. I enlighet med (4.6) har vi ett kommutativt diagram i vilket kolonnerna är isomorfismer:

$$\begin{array}{ccccccc} 0 & \longrightarrow & F(M'') & \xrightarrow{F(g)} & F(M) & \xrightarrow{F(f)} & F(M') \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & G(M'') & \xrightarrow{G(g)} & G(M) & \xrightarrow{G(f)} & G(M') \end{array}$$

Alltså är också andra raden exakt (se Övn. 13). Enligt Övn. 14 är sekvensen

$$M' \otimes_R N \xrightarrow{f\otimes id_N} M \otimes_R N \xrightarrow{g\otimes id_N} M'' \otimes_R N \longrightarrow 0$$

exakt ty P är godtycklig.

Anmärkning. Man kan bevisa påståendet direkt utan att använda Övn. 14.

Ledning. För att visa att $M \mapsto M \otimes_R N$ inte är vänsterexakt välj $R = \mathbb{Z}$, $M' = M = \mathbb{Z}$ och $f(n) = 2n$.

[†]Mot $X' \xrightarrow{f} X$ svarar $G(f) : \mathrm{Hom}_R(X \otimes_R N, P) \longrightarrow \mathrm{Hom}_R(X' \otimes_R N, P)$, där $G(f) = \mathrm{Hom}_R(f \otimes id_N, , id_P)$ – det är "självklart".

Kapitel 12

KORT OM HOMOLOGISK ALGEBRA

Vi skall ägna detta kapitel åt en kort diskussion av homologisk algebra. Homologisk algebra ger en mycket kraftfull teknisk apparat för studier av många viktiga matematiska objekt som t.ex. mångfalder av olika typer (algebraiska, analytiska, aritmetiska, topologiska) och olika algebraiska strukturer (grupper, ringar, associativa algebror, Liealgebror osv). Homologi och kohomologigrupper konstruerades i olika förklädnader under 1900-talet (egentligen finns de redan i Hilberts arbeten om "syzygies" från 1890). Topologiska konstruktioner spelade en avgörande roll i utvecklingen av den allmänna teori som skapades under 1940-talet huvudsakligen av S. Eilenberg och S. MacLane. År 1956 publicerades H. Cartan och S. Eilenbergs bok "Homological Algebra" som lade grunden för modern homologisk algebra. Ett år senare publicerade A. Grothendieck en viktig artikel "Sur quelques points d'algebre homologique" som väsentligt utvidgade möjligheter att använda homologisk apparat till stora klasser av kategorier.

Vi kommer att begränsa oss till kategorier av moduler över ringar, men i själva verket fungerar nästan alla formella konstruktioner som presenteras här i godtyckliga abelska kategorier. R kommer att beteckna en associativ ring med etta och ${}_R\mathcal{M}$ kategorin av vänster R-moduler.

(12.1) Definition. Med ett **komplex** i ${}_R\mathcal{M}$ menar man en följd:

$$(\mathbf{M}, \mathbf{d}) \qquad \cdots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \longrightarrow \cdots$$

av R-moduler M_n och R-homomorfismer d_n sådan att $d_n d_{n+1} = 0$ för varje $n \in \mathbb{Z}$. Man säger att $\mathbf{M}$ är **begränsat från höger** om det finns N så att $M_n = 0$ då $n \geq N$, och **begränsat från vänster** om det finns N' så att $M_n = 0$ då $n \leq N'$. Ett komplex kallas **begränsat** (eller **ändligt**) om det är begränsat från både höger och vänster. Vanligen skriver man inte

ut de oändliga avsnitt av komplex som består av enbart nollmoduler. Ibland kommer vi att utelämna $\mathbf{d}$ i beteckningen $(\mathbf{M}, \mathbf{d})$ av ett komplex.

Man säger att $\mathbf{f} : \mathbf{M} \to \mathbf{M}'$ är en morfism (av komplex) om $\mathbf{f} = (f_n)$, där för varje n är $f_n : M_n \to M'_n$ en R-homomorfism och alla kvadrater i diagrammet:

$$(*) \qquad \begin{array}{ccccccccc} \cdots & \longrightarrow & M_{n+1} & \xrightarrow{d_{n+1}} & M_n & \xrightarrow{d_n} & M_{n-1} & \xrightarrow{d_{n-1}} & \cdots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \longrightarrow & M'_{n+1} & \xrightarrow{d'_{n+1}} & M'_n & \xrightarrow{d'_n} & M'_{n-1} & \xrightarrow{d'_{n-1}} & \cdots \end{array}$$

kommuterar dvs $f_{n-1}d_n = d'_n f_n$ för varje $n \in \mathbb{Z}$. Komplex och deras morfismer bildar en kategori som vi kommer att beteckna med ${}_R\mathcal{C}omp$

□

Likheten $d_n d_{n+1} = 0$ är ekvivalent med Im $d_{n+1} \subseteq$ Ker d_n. Detta motiverar följande definition:

(12.2) Definition. Med n:te **homologigruppen** av komplexet $(\mathbf{M}, \mathbf{d})$ menar man gruppen:

$$H_n(\mathbf{M}) = \text{Ker } d_n / \text{Im } d_{n+1}.$$

□

Observera att $H_n(\mathbf{M})$ mäter avvikelsen av sekvensen

$$M_{n+1} \to M_n \to M_{n-1}$$

från att vara exakt.

Om $\mathbf{f} : \mathbf{M} \to \mathbf{M}'$ är en morfism av komplex, dvs diagrammet $(*)$ är kommutativt så är $f_n(\text{Ker}\, d_n) \subseteq \text{Ker}\, d'_n$ och $f_n(\text{Im}\, d_{n+1}) \subseteq \text{Im}\, d'_{n+1}$ (se Övn. 3.31). Alltså inducerar f_n en homomorfism

$$(12.3) \qquad f_n^* : H_n(\mathbf{M}) \longrightarrow H_n(\mathbf{M}'),$$

där $f_n^*(m_n + \text{Im } d_{n+1}) = f_n(m_n) + \text{Im } d'_{n+1}$ då $m_n \in M_n$.

(12.4) Anmärkning. (a) Homologigrupper kan betraktas som funktorer från kategorin av komplex över R till kategorin av abelska grupper:

$$H_n :_R \mathcal{C}omp \longrightarrow \mathcal{A}b,$$

där mot $\mathbf{M}$ svarar $H_n(\mathbf{M})$, och mot $\mathbf{f} : \mathbf{M} \to \mathbf{M}'$ svarar $H_n(\mathbf{f})$. Vi lämnar som enkel övning en kontroll att H_n verkligen är en kovariant funktor.

(b) Ibland är det mera naturligt att ha växande index i riktningen mot höger. I sådana fall brukar man skriva index uppifrån så att ett komplex antecknas som:

$$(\mathbf{M}, \mathbf{d}) \qquad \cdots \longrightarrow M^{n-1} \xrightarrow{d_{n-1}} M^n \xrightarrow{d_n} M^{n+1} \longrightarrow \cdots$$

Homologigrupper betecknas då $H^n(\mathbf{M})$.

□

Komplex och deras homologigrupper förekommer i många situationer. Låt $\mathcal{C}$ vara en kategori. Ofta studerar man $\mathcal{C}$ (dvs objekt och morfismer i $\mathcal{C}$) genom att man konstruerar en sekvens av funktorer $H_n : \mathcal{C} \to \mathcal{A}b$. Abelska grupper $H_n(X)$ då $X \in \mathcal{O}b\mathcal{C}$ är ofta viktiga invarianter som ibland karakteriserar X (bestämmer X så när som på isomorfism) eller är exakt samma för vissa intressanta klasser av objekt i $\mathcal{C}$. $H_n(X)$ brukar kallas för homologigrupper av X om H_n är kovariant, och kohomologigrupper av X om H_n är kontravariant. I det sista fallet skriver man vanligen H^n i stället för H_n.

(12.5) Exempel. (a) Låt $\mathcal{T}op$ vara kategorin av topologiska rum och låt X vara ett topologiskt rum i $\mathcal{T}op$. Låt

$$\Delta_n = \{(t_0, \ldots, t_n) \in \mathbb{R}^{n+1} : t_i \geq 0 \quad \text{och} \quad \sum t_i = 1\}.$$

Δ_n kallas för n-dimensionellt **standard simplex**. Låt $S_n(X)$ vara den fria abelska grupp (dvs fri $\mathbb{Z}$-modul) som genereras av alla kontinuerliga funktioner $f : \Delta_n \to X$. Alltså genereras $S_0(X)$ av alla punkter i X, och $S_1(X)$ av alla kurvor i X. $S_n(X)$ bildar ett komplex

$$\cdots \to S_n(X) \xrightarrow{\partial_n} S_{n-1}(X) \to \cdots \to S_1(X) \to S_0(X) \to 0.$$

som definieras på följande sätt: Det finns kontinuerliga funktioner $d_n^i : \Delta_{n-1} \to \Delta_n$, där $d_n^i(t_0, \ldots, t_{n-1}) = (t_0, \ldots, t_{i-1}, 0, t_i, \ldots, t_{n-1}) \in \Delta_n$ $(0 \leq i \leq n,\ n \geq 1)$. Varje kontinuerlig funktion $f : \Delta_n \to X$ definierar en kontinuerlig funktion $fd_n^i : \Delta_{n-1} \to X$. Därefter definierar man

$$\partial_n(f) = \sum_i (-1)^i (f d_n^i).$$

Man kontrollerar ganska enkelt att $\partial_{n-1}\partial_n = 0$ så att man får ett komplex. Homologigrupper av detta komplex betecknas med $H_n(X, \mathbb{Z})$ och kallas **singulära homologigrupper** av X. Varje kontinuerlig funktion $\varphi : X \to Y$ (en morfism i $\mathcal{T}op$) definierar

$$H_n(X, \mathbb{Z}) \to H_n(Y, \mathbb{Z})$$

(ty $\Delta_n \xrightarrow{f} X \xrightarrow{\varphi} Y$ ger $S_n(X) \to S_n(Y)$ och man får en homomorfism av komplexet motsvarande X i komplexet motsvarande Y).

(b) Låt M vara en C^∞-mångfald av dimension n (se (5.30)). Låt $D^k(M)$ beteckna $\mathbb{R}$-modulen av alla k-differentialformer ω på M (dvs för varje $P \in M$ existerar en omgivning U_p sådan att

$$\omega|_{U_p} = \sum a_{i_1 \ldots i_k} dx^{i_1} \wedge \ldots \wedge dx^{i_k},$$

där $a_{i_1 \ldots i_k}$ är en funktion reguljär på U_p). Man definierar ett komplex:

$$D^0(M) \to D^1(M) \to \cdots \to D^k(M) \xrightarrow{d^k} D^{k+1}(M) \to \ldots,$$

där

$$d^k_{U_p}\omega = \sum_{i_1 < \ldots < i_k} \sum_{j=1}^{n} \frac{\partial a_{i_1 \ldots i_k}}{\partial x^j} dx^j \wedge dx^{i_1} \wedge \ldots \wedge dx^{i_k}.$$

Man kontrollerar lätt att $d^{k+1}d^k = 0$, vilket betyder att man har ett komplex. Homologigrupper av detta komplex kallas **de Rhams kohomologigrupper** av M och betecknas $H^k(M, d)$. Observera att $H^k(M, d) = Z^k(M, d)/B^k(M, d)$, där

$$Z^k(M, d) = \{\omega \in D^k(M) : d^k\omega = 0\}$$

och

$$B^k(M, d) = \{\omega \in D^k(M) : \exists\, \tau \in D^{k-1}(M),\ \omega = d^{k-1}\tau\}.$$

En morfism $\varphi : M \to N$ definierar en morfism av komplex $D^k(N) \to D^k(M)$ för $k = 0, 1, \ldots$ (den exakta definitionen utelämnas här. Observera dock att φ inducerar en kovariant

avbildning av tangentrum så att differentialformer avbildas i motsatt riktning i förhållande till funktionaler på tangentrum). Man får en sekvens av kontravarianta funktorer $M \mapsto H^n(M,d)$, $\varphi \mapsto H^n(\varphi,d)$ (här är $H^n(M,d)$ ett vektorrum över $\mathbb{R}$).

□

En typisk situation i samband med studier av homologigrupper är att man har en sekvens av komplex relaterade till olika nära besläktade objekt som t ex en mångfald, en delmångfald och komplementet till delmångfalden (eller en modul, en delmodul och motsvarande kvotmodul). I sådana fall betraktar man vanligen exakta sekvenser av komplex:

(12.6) Definition. Man säger att en sekvens av komplex

$$0 \to \mathbf{M}' \to \mathbf{M} \to \mathbf{M}'' \to 0$$

är exakt om för varje $n \in \mathbb{Z}$ är sekvensen

$$0 \to M'_n \to M_n \to M''_n \to 0$$

exakt.

□

Följande resultat om en lång exakt sekvens av homologigrupper som svarar mot en kort exakt följd av komplex är mycket viktigt i homologisk algebra:

(12.7) Sats. *Om* $0 \longrightarrow \mathbf{M}' \xrightarrow{\mathbf{f}} \mathbf{M} \xrightarrow{\mathbf{g}} \mathbf{M}'' \longrightarrow 0$ *är en kort exakt följd av komplex så existerar en lång exakt följd av homologigrupper:*

$$\cdots \longrightarrow H_{n+1}(\mathbf{M}') \xrightarrow{H_n(\mathbf{f})} H_n(\mathbf{M}) \xrightarrow{H_n(\mathbf{g})} H_n(\mathbf{M}'') \xrightarrow{\delta_n} H_{n-1}(\mathbf{M}') \longrightarrow \cdots$$

Bevis. Den korta exakta följden av komplex är följden av moduler och deras homomorfismer:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_{n+1} & \xrightarrow{f_{n+1}} & M_{n+1} & \xrightarrow{g_{n+1}} & M''_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{n+1}} & & \downarrow{\scriptstyle d_{n+1}} & & \downarrow{\scriptstyle d''_{n+1}} & & \\
0 & \longrightarrow & M'_{n} & \xrightarrow{f_{n}} & M_{n} & \xrightarrow{g_{n}} & M''_{n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{n}} & & \downarrow{\scriptstyle d_{n}} & & \downarrow{\scriptstyle d''_{n}} & & \\
0 & \longrightarrow & M'_{n-1} & \xrightarrow{f_{n-1}} & M_{n-1} & \xrightarrow{g_{n-1}} & M''_{n-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{n-1}} & & \downarrow{\scriptstyle d_{n-1}} & & \downarrow{\scriptstyle d''_{n-1}} & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Morfismerna $\mathbf{f} : \mathbf{M}' \to \mathbf{M}$ och $\mathbf{g} : \mathbf{M} \to \mathbf{M}''$ definierar homomorfismerna

$$H_n(\mathbf{f}) : H_n(\mathbf{M}') \to H_n(\mathbf{M}) \quad \text{och} \quad H_n(\mathbf{g}) : H_n(\mathbf{M}) \to H_n(\mathbf{M}'')$$

i enlighet med (12.3). Man måste definiera homomorfismerna:

$$\partial_n : H_n(\mathbf{M}'') \to H_{n-1}(\mathbf{M}')$$

så att den långa sekvensen blir exakt. Konstruktionen av ∂_n är ett specialfall av ett mycket användbart resultat som, beroende på dess stora betydelse, vi formulerar separat:

(12.8) "Snake Lemma". *Låt*

$$\begin{array}{ccccccc}
 & & M'_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & M''_1 \longrightarrow 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} \\
0 & \longrightarrow & M'_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & M''_2
\end{array}$$

vara ett kommutativt diagram med exakta rader. Då är sekvensen

$$\mathrm{Ker}d' \xrightarrow{f_1^*} \mathrm{Ker}d \xrightarrow{g_1^*} \mathrm{Ker}d'' \xrightarrow{\partial} \mathrm{Coker}d' \xrightarrow{f_2^*} \mathrm{Coker}d \xrightarrow{g_2^*} \mathrm{Coker}d''$$

exakt om f_i^*, g_i^* induceras av respektive f_i, g_i och

$$\partial(m''_1) = f_2^{-1} d g_1^{-1}(m''_1) + Im\ d'$$

för $m_1'' \in \mathrm{Ker} d''$ där med $g_1^{-1}(m_1'')$ menas en godtycklig urbild av m_1''.

Först visar vi att "Snake Lemma" verkligen implicerar vår långa exakta sekvens. I detta syfte skriver vi om ett avsnitt av sekvensen $0 \to \mathbf{M}' \to \mathbf{M} \to \mathbf{M}'' \to 0$ på följande sätt:

$$\begin{array}{ccccccc} & & M_n'/\mathrm{Im} d_{n+1}' & \xrightarrow{\bar{f}_n} & M_n/\mathrm{Im} d_{n+1} & \xrightarrow{\bar{g}_n} & M_n''/\mathrm{Im} d_{n+1}'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle \bar{d}_n'} & & \downarrow{\scriptstyle \bar{d}_n} & & \downarrow{\scriptstyle \bar{d}_n''} \\ 0 \longrightarrow & \mathrm{Ker} d_{n-1}' & \xrightarrow{\bar{f}_{n-1}} & \mathrm{Ker} d_{n-1} & \xrightarrow{\bar{g}_{n-1}} & \mathrm{Ker} d_{n-1}'' & \end{array}$$

Här induceras avbildningarna med "streck" av motsvarande avbildningar utan "streck" på ett naturligt sätt. Man ser lätt att

$$\mathrm{Ker}\ \bar{d}_n = \mathrm{Ker}\ d_n/\mathrm{Im}\ d_{n+1} = H_n(\mathbf{M}) \quad \text{och} \quad \mathrm{Coker}\ \bar{d}_n = \mathrm{Ker}\ d_{n-1}/\mathrm{Im}\ d_n = H_{n-1}(\mathbf{M}).$$

Motsvarande likheter gäller för $\bar{d}_n'$ och $\bar{d}_n''$. Man kontrollerar utan svårigheter att raderna är exakta. "Snake Lemma" applicerat på diagrammet ovan bevisar direkt satsen. □

(12.9) Bevis av "Snake Lemma". Att kontrollera alla detaljer är ganska tråkigt. Men det är något som man borde göra en gång (dock ej fler!). Eftersom vi redan hade liknande resonemang i Kapitel 11 (se Övn. 11.11 och 11.14) ger vi här ett något fragmentariskt bevis.

Exaktheten av följderna

$$\mathrm{Ker}\ d' \xrightarrow{f_1^*} \mathrm{Ker}\ d \xrightarrow{g_1^*} \mathrm{Ker}\ d''$$

och

$$\mathrm{Coker}\ d' \xrightarrow{f_2^*} \mathrm{Coker}\ d \xrightarrow{g_2^*} \mathrm{Coker}\ d''$$

följer ur Övn. 3.31. När det gäller ∂ måste man visa att definitionen av $\partial(m_1'')$ är korrekt ty valet av urbilder $g_1^{-1}(m_1'')$ är inte entydigt.

Låt oss komma överens om att x_1', x_i, x_i'' betecknar godtyckliga element ur M_i', M_i, M_i'' (x kan ersättas med en godtycklig symbol).

Först visar vi att ∂ är korrekt definierad. För $m_1'' \in \mathrm{Ker}\ d''$ väljer man en godtycklig urbild m_1 dvs $g_1(m_1) = m_1''$. Vi har då $d(m_1) \in \mathrm{Im}\ f_2 = \mathrm{Ker}\ g_2$ (ty $g_2 d(m_1) = d'' g_1(m_1) = d''(m_1'') = 0$). Alltså finns det m_2' så att $f_2(m_2') = d(m_1)$ så att vi verkligen kan definiera $\partial(m_1'') = m_2' + \mathrm{Im}\ d'$. Men vi måste visa att valet av m_1 inte påverkar den definitionen. Antag att även $g_1(\bar{m}_1) = m_1''$. Då är $g_1(m_1 - \bar{m}_1) = 0$, vilket ger $m_1 - \bar{m}_1 = f_1(m_1')$, ty $\mathrm{Ker}\ g_1 = \mathrm{Im}\ f_1$. Alltså är $d(m_1 - \bar{m}_1)$ bilden av $d'(m_1')$ på grund av diagrammets kommutativitet. Om nu

$$d(m_1) = f_2(m_2') \quad \text{och} \quad d(\bar{m}_1) = f_2(\bar{m}_2'),$$

så är

$$m_2' - \bar{m}_2' = d'(m_1') \in \text{Im } d',$$

ty f_2 är injektiv. Alltså är $m_2' + \text{Im } d' = \bar{m}_2' + \text{Im } d'$, vilket visar att definitionen av ∂ är korrekt.

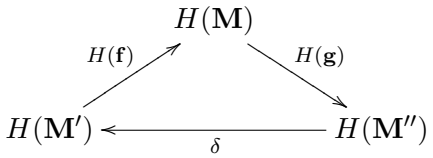
Det återstår att visa exaktheten i Ker d'' och Coker d'. Det faktum att Im $g_1^* \subseteq$ Ker ∂ och Im $\partial \subseteq$ Ker f_2^* följer direkt ty det är lätt att kontrollera likheterna $\partial g_1^* = 0$ och $f_2^* \partial = 0$. Som avslutning låt oss visa att Ker $\partial \subseteq$ Im g_1^* (resten av detaljerna lämnar vi som övning).

Låt $m_1'' \in$ Ker ∂ dvs $m_1'' = g_1(m_1)$, där $d(m_1) = f_2(m_2')$ och $m_2' \in$ Im d' (ty $\partial(m_1'') = m_2' + \text{Im}d' = \text{Im}d'$). Vi vill visa att $m_1'' \in$ Im g_1^* dvs $m_1'' = g_1(\bar{m}_1)$, där $\bar{m}_1 \in$ Ker d. Men $m_2' = d'(m_1')$ så att kommutativiteten ger

$$d(m_1) = f_2(m_2') = f_2 d'(m_1') = df_1(m_1'),$$

vilket betyder att $d(m_1 - f_1(m_1')) = 0$. Alltså $\bar{m}_1 = m_1 - f_1(m_1') \in \text{Ker}d$ och samtidigt $g_1(\bar{m}_1) = g_1(m_1 - f_1(m_1')) = g_1(m_1) = m_1''$, ty $g_1 f_1 = 0$. Detta visar vårt påstående. □

(12.10) Anmärkning. Ofta är det mycket fördelaktigt att uppfatta ett komplex $(\mathbf{M}, \mathbf{d})$ som modulen $\mathbf{M} = \bigoplus M_n$ $(n \in \mathbb{Z})$ med $\mathbf{d} : \mathbf{M} \to \mathbf{M}$ som är homogent av grad -1 dvs $\mathbf{d}(M_n) \subseteq M_{n-1}$ och $\mathbf{dd} = 0$. En sådan definition generaliseras direkt till $\mathbf{d}$ av grad p dvs $\mathbf{d}(M_n) \subseteq M_{n+p}$ och $\mathbf{dd} = 0$. I synnerhet kan en vanlig direkt summa $\mathbf{M} = \bigoplus M_n$ uppfattas som komplex med $\mathbf{d} = 0$ av godtycklig grad p. Man kan definiera en morfism $\mathbf{f} : (\mathbf{M}, \mathbf{d}) \to (\mathbf{M}', \mathbf{d}')$, där $\mathbf{d}$ och $\mathbf{d}'$ har samma grad p, som en modulhomomorfism med $\mathbf{f}(M_n) \subseteq M'_{n+q}$ och $\mathbf{fd} = \mathbf{d'f}$ för varje n och ett fixerat heltal q. I sådana termer kan sats (18.7) formuleras mycket enkelt. Man kan säga att till varje kort exakt följd av komplex $0 \to \mathbf{M}' \xrightarrow{\mathbf{f}} \mathbf{M} \xrightarrow{\mathbf{g}} \mathbf{M}'' \to 0$ existerar en exakt triangel



där $H(\mathbf{M}) = \bigoplus H_n(\mathbf{M})$ är komplex med $\mathbf{d} = 0$ av grad -1 (med samma tolkning av $H(\mathbf{M}')$ och $H(\mathbf{M}'')$), och ∂ är en morfism av grad -1 dvs

$$\partial(H_n(\mathbf{M}')) \subseteq H_{n-1}(\mathbf{M}'').$$

□

Olika konstruktioner av (ko)homologigrupper kan ofta betraktas som specialfall av en mycket allmän konstruktion av deriverade funktorer – man utgår ifrån en funktor $\mathcal{F}$ som sammanfaller med H^0 (H_0). De övriga H^n (H_n) är "deriverade" funktorer av $\mathcal{F}$. Vi skall beskriva den konstruktionen mycket allmänt, men först måste vi komplettera våra kunskaper om två mycket viktiga klasser av moduler över ringar – projektiva och injektiva moduler.

Vi repeterar (se Övn. 3.27 och Övn. 11.12):

(12.11) Definition. En R-modul P kallas (R–)**projektiv** om funktorn $X \mapsto \mathrm{Hom}_R(P, X)$ är exakt. En R-modul I kallas (R–)**injektiv** om funktorn $X \mapsto \mathrm{Hom}_R(X, I)$ är exakt.

□

(12.12) Anmärkning. Vi vet att funktorn "Hom" är vänsterexakt (se Övn. 11.11), vilket betyder att om $0 \to M' \to M \to M'' \to 0$ är exakt så är sekvenserna

$$0 \to \mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M'')$$

och

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$$

exakta för varje R-modul N. P är projektiv om den första sekvensen är exakt från höger då $N = P$, dvs om varje diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

kan kompletteras till ett kommutativt diagram:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow & \downarrow & & \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

På liknande sätt är I injektiv om den andra sekvensen är exakt från höger då $N = I$ dvs om varje diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow & & \\ & & I & & \end{array}$$

kan kompletteras till ett kommutativt diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow & \swarrow & \\ & & I & & \end{array}$$

□

(12.13) Exempel. (a) Varje fri R-modul F är projektiv. Låt $\{e_i\}$ vara en bas för F över R. Betrakta diagrammet:

$$\begin{array}{ccccc} & & F & & \\ & \swarrow^{f} & \downarrow{\scriptstyle h} & & \\ M & \xrightarrow[g]{} & M'' & \longrightarrow & 0 \end{array}$$

Låt oss välja $m_i \in M$ så att $g(m_i) = h(e_i)$ (det är möjligt ty g är surjektiv). Definiera f så att $f(e_i) = m_i$ (se (3.18)). Då kommuterar diagrammet dvs $gf = h$.

(b) En ändligt genererad R-modul P är projektiv då och endast då det finns en R-modul P' sådan att $P \oplus P' \cong R^n$ för något n (se Övn. 1). Låt nu $R = \mathbb{Z}/(6)$. R kan betraktas som R-modul och som sådan är den projektiv (den är fri). Men $\mathbb{Z}(6) = \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ (se t.ex. (1.49)). Alltså är både $\mathbb{Z}/(2)$ och $\mathbb{Z}/(3)$ projektiva $\mathbb{Z}/(6)$-moduler. Men de är inte fria ty en fri R-modul har minst 6 element.

(c) Låt K vara en kropp och V en godtycklig K-modul. Då är V injektiv (och projektiv enligt (a)). Betrakta diagrammet:

$$\begin{array}{ccccc} 0 & \longrightarrow & W' & \xrightarrow{i} & W \\ & & \downarrow{\scriptstyle g} & \swarrow_{f} & \\ & & V & & \end{array}$$

Låt $\{e_i\}_{i\in I'}$ vara en bas för W' och $\{e_i\}_{i\in I}$, där $I \supseteq I'$, en bas för W över K. Definiera nu f

så att $f(e_i) = g(e_i)$ då $i \in I'$, och $f(e_i) = 0$ då $i \in I \setminus I'$. Då definierar f (entydigt) en linjär avbildning $f : W \to V$ (se (3.18)) sådan att $fi = g$.

(d) Det är mycket svårare att ge exempel på injektiva moduler över godtyckliga ringar. Vi noterar utan bevis att om R är en Dedekindring så är M en injektiv R-modul då och endast då M är R-delbar[†], dvs till varje $m \in M$ och till varje $r \in R$, $r \neq 0$, existerar $x \in M$ så att $rx = m$. På det sättet ser vi lätt att kvotkroppen K av en Dedekindring är R-injektiv (t ex är $\mathbb{Q}$ en $\mathbb{Z}$-injektiv modul).

□

(12.14) Proposition. *Låt R vara en ring och M en R-modul. Då existerar*

(*a*) *en projektiv upplösning av M dvs ett exakt komplex*

$$\ldots \to P_1 \to P_0 \to M \to 0,$$

där P_i är projektiva,

(*b*) *en injektiv upplösning av M dvs ett exakt komplex*

$$0 \to M \to I_0 \to I_1 \to \ldots,$$

där I_i är injektiva.

Bevis. (a) Först observerar vi att för varje R-modul M existerar en projektiv (t o m fri) R-modul P och en epimorfism $P \to M \to 0$. Det räcker att välja P som den fria modul som genereras av alla $\{e_m\}_{m \in M}$ (en bas för P) och definiera $P \to M$ genom $e_m \mapsto m$ (se (3.18)). Nu konstruerar vi en projektiv upplösning. Först betraktar vi en exakt sekvens:

$$0 \longrightarrow \text{Ker } d_0 \longrightarrow P_0 \xrightarrow{d_0} M \longrightarrow 0.$$

där P_0 är en fri R-modul (se ovan). Välj nu en fri R-modul P_1 och en epimorfism $P_1 \to \text{Ker } d_0 \to 0$. Då är sekvensen

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0$$

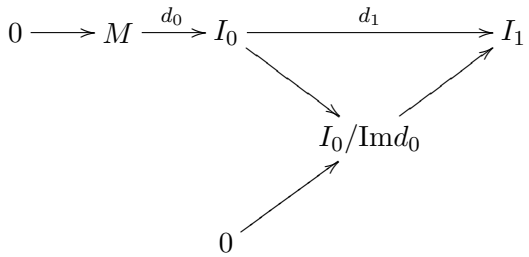
[†]Den egenskapen karakteriserar Dedekindringar.

exakt om d_1 är sammansättningen $P_1 \to \text{Ker } d_0 \to P_0$. Nu betraktar vi en fri R-modul P_2, en epimorfism $P_2 \to \text{Ker } d_1 \to 0$ och förlänger sekvensen med $P_2 \xrightarrow{d_2} P_1$, som är sammansättningen av $P_2 \to \text{Ker } d_1 \to P_1$ osv.

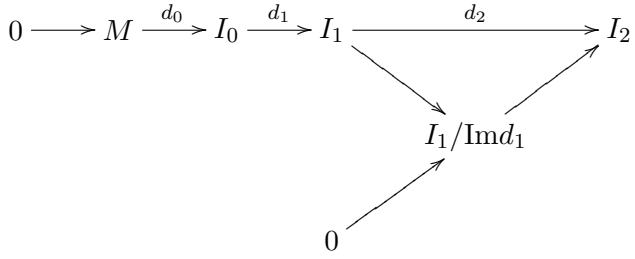
(b) Först måste vi veta att för varje R-modul M existerar en injektiv R-modul I och en monomorfism $0 \to M \to I$. Även om beviset inte är särskilt svårt måste vi avstå från att ge det här. Med detta påstående är resten enkel. Man startar med den exakta sekvensen

$$0 \longrightarrow M \xrightarrow{d_0} I_0 \longrightarrow I_0/\text{Im}d_0 \longrightarrow 0$$

i vilken I_0 är injektiv. Betrakta nu en monomorfism $0 \to I_0/\text{Im } d_0 \to I_1$, där I_1 är R-injektiv och definiera d_1 ur diagrammet



som sammansättningen av $I_0 \to I_0/\text{Im } d_0 \to I_1$. Därefter betrakta:



med d_2 som sammansättningen av $I_1 \to I_1/\text{Im } d_1 \to I_2$, där I_2 är injektiv och $0 \to I_1/\text{Im } d_1 \to I_2$ är en monomorfism, osv. □

Nu är vi beredda att definiera deriverade funktorer.

Låt R vara en ring och ${}_R\mathcal{M}$ kategorin av vänster R-moduler. Låt $\mathcal{F} :_R \mathcal{M} \to \mathcal{A}b$ vara en kovariant vänsterexakt och additiv funktor (se (11.11) och (11.17)). Låt M vara en R-modul och

$$0 \to M \to I_0 \to I_1 \to I_2 \to \cdots$$

en injektiv upplösning av M. Betrakta komplexet $\mathbf{I}$:

$$0 \to I_0 \to I_1 \to I_2 \to \cdots$$

Högerderiverade funktorer $R^n\mathcal{F}$ av $\mathcal{F}$ definieras som:

$$(R^n\mathcal{F})(M) = H^n(\mathcal{F}(\mathbf{I}))$$

dvs $(R^n\mathcal{F})(M)$ är n-te homologigruppen av komplexet:

$$0 \to \mathcal{F}(I_0) \to \mathcal{F}(I_1) \to \mathcal{F}(I_2) \to \dots$$

Det följer direkt ur konstruktionen att $(R^0\mathcal{F})(M) = H^0(\mathcal{F}(\mathbf{I})) = \mathcal{F}(M)$ därför att $0 \to M \to I_0$ är exakt och $\mathcal{F}$ är vänsterexakt så att $0 \to \mathcal{F}(M) \to \mathcal{F}(I_0) \to \mathcal{F}(I_1)$ är exakt, dvs $\mathcal{F}(M)$ är kärnan till $\mathcal{F}(I_0) \to \mathcal{F}(I_1)$. Man visar (ganska jobbigt) att $(R^n\mathcal{F})(M)$ är oberoende av valet av $\mathbf{I}$ (så när som på en isomorfism). Vidare låt $\varphi : M \to M'$ vara en R-homomorfism och låt oss välja injektiva upplösningar:

$$0 \longrightarrow M \longrightarrow I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \cdots$$

och

$$0 \longrightarrow M' \longrightarrow I'_0 \longrightarrow I'_1 \longrightarrow I'_2 \longrightarrow \cdots$$

Enligt definitionen av injektiva moduler existerar homomorfismer $I_k \to I'_k$ för $k = 0,\, 1, 2, \dots$ som mam konstruerar succesivt. På detta sätt får man en morfism av den injektiva upplösningen av M i den injektiva upplösningen av M' dvs ett kommutativt diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \longrightarrow & I_0 & \longrightarrow & I_1 & \longrightarrow & I_2 \longrightarrow \cdots \\
 & & {\scriptstyle\varphi}\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & M' & \longrightarrow & I'_0 & \longrightarrow & I'_1 & \longrightarrow & I'_2 \longrightarrow \cdots
\end{array}$$

och, som konsekvens, homomorfismerna $(R^n\mathcal{F})(M) \to (R^n\mathcal{F})(M')$. Om

$$0 \to M' \to M \to M'' \to 0$$

är exakt så väljer man injektiva upplösningar $\mathbf{I}', \mathbf{I}, \mathbf{I}''$ av M', M och M'' på ett sådant sätt att man får en exakt sekvens av komplex $0 \to \mathbf{I}' \to \mathbf{I} \to \mathbf{I}'' \to 0$, vilket enligt (18.7) ger en lång exakt sekvens:

$$\begin{aligned} 0 \quad \to \quad & (R^0\mathcal{F})(M') \to (R^0\mathcal{F})(M) \to (R^0\mathcal{F})(M'') \to (R^1\mathcal{F})(M') \to \dots \\ & \dots \to (R^n\mathcal{F})(M) \to (R^n\mathcal{F})(M'') \to (R^{n+1}\mathcal{F})(M') \to \dots \end{aligned}$$

Om $\mathcal{F}$ är högerexakt (som t.ex. $\otimes$) konstruerar man i stället vänsterderiverade funktorer $L_n\mathcal{F}$ med hjälp av projektiva upplösningar[†]. För kontravarianta $\mathcal{F}$ förfar man på samma sätt, men projektiva och injektiva upplösningar ersätter varandra (se t ex J.J. Rotman, "An introduction to homological algebra").

(12.15) Exempel. (a) Låt G vara en grupp, $R = \mathbb{Z}[G]$ gruppringen av G över $\mathbb{Z}$. Låt $\mathcal{F} :_R \mathcal{M} \to \mathcal{A}b$ vara funktorn:

$$\mathcal{F}(M) = M^G = \{m \in M : \forall_{g\in G}\, gm = m\}$$

och för $f : M \to M'$, $\mathcal{F}(f) : \mathcal{F}(M) \to \mathcal{F}(M')$, där $\mathcal{F}(f)$ är restriktionen av f till $\mathcal{F}(M) = M^G$ ($m \in M^G \Rightarrow f(m) \in M'^G$ ty $gf(m) = f(gm) = f(m)$ då $g \in G$). Funktorn $\mathcal{F}$ är kovariant och vänsterexakt, ty $0 \to M' \to M \to M'' \to 0$ exakt ger att

$$0 \to M'^G \to M^G \to M''^G$$

är exakt (enkel övning). Högerderiverade funktorer av $\mathcal{F}$ betecknas med $H^n(G, M)$ och kallas **kohomologigrupper av** G med koefficienter i M. Deras betydelse är mycket stor. Observera att $M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ (enkel övning).

(b) Låt ${}_R\mathcal{M}$ vara kategorin av vänster R-moduler över en ring R. Betrakta funktorn $\mathcal{F}(N) = \mathrm{Hom}_R(M, N)$, där M är en fixerad R-modul. $\mathcal{F}$ är kovariant och vänsterexakt. Högerderiverade funktorer av $\mathcal{F}$ betecknas med $\mathrm{Ext}^n_R(M, N)$. Om $\mathcal{G}(M) = \mathrm{Hom}_R(M, N)$ med N fixerad så får man en kontravariant vänsterexakt funktor. I enlighet med den allmänna konstruktionen har denna funktor sina högerderiverade funktorer $R^n\mathcal{G}$ (som konstrueras med hjälp av projektiva upplösningar). Dessa betecknas också med $\mathrm{Ext}^n_R(M, N)$. Man visar att bägge konstruktionerna med utgångspunkt från $\mathcal{F}$ eller $\mathcal{G}$ leder till isomorfa funktorer av 2 variabler. Observera också att $H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ i exempel (a) ty

$$H^0(G, M) = \mathrm{Ext}^0_{\mathbb{Z}[G]}(\mathbb{Z}, M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) = M^G,$$

[†]Höger- och vänsterderiverade funktorer kan konstrueras även om $\mathcal{F}$ inte är höger- eller vänsterexakt. Men då kan sambandet mellan dessa funktorer och $\mathcal{F}$ vara mycket svagt.

där $\mathbb{Z}$ betraktas som $\mathbb{Z}[G]$-modul med trivial verkan av G dvs $gn = n$ då $g \in G$ och $n \in \mathbb{Z}$.

(c) Låt $M_0 \subseteq M$ vara R-moduler och låt $f_0 : M_0 \to N$ vara en R-homomorfism. Antag att man vill veta om det är möjligt att utvidga f_0 till M, dvs om det finns en R-homomorfism $f : M \to N$ så att $f|_{M_0} = f_0$. Betrakta den exakta sekvensen

$$0 \to M_0 \xrightarrow{i} M \to M/M_0.$$

Vi vet att

$$0 \longrightarrow \mathrm{Hom}_R(M/M_0, N) \longrightarrow \mathrm{Hom}_R(M, N) \xrightarrow{i_*} \mathrm{Hom}_R(M_0, N)$$

är exakt (se (11.17) och Övn. 11.10). Låt oss förlänga den sekvensen med epimorfismen av $\mathrm{Hom}_R(M_0, N)$ på $\mathrm{Hom}_R(M_0, N)/\mathrm{Im}\ i_* =: E$ dvs

$$0 \longrightarrow \mathrm{Hom}_R(M/M_0, N) \longrightarrow \mathrm{Hom}_R(M, N) \xrightarrow{i_*} \mathrm{Hom}_R(M_0, N) \xrightarrow{\alpha} E \longrightarrow 0.$$

Modulen E är intressant ty $\alpha(f_0) = 0$ då och endast då $f_0 \in \mathrm{Im}\ i_*$ dvs $f_0 = fi$ för något $f : M \to N$

$$\begin{array}{ccccc} 0 & \longrightarrow & M_0 & \xrightarrow{i} & M \\ & & \downarrow{\scriptstyle f_0} & \swarrow{\scriptstyle f} & \\ & & N & & \end{array}$$

vilket betyder att $\alpha(f_0) = 0 \Leftrightarrow f_0$ kan utvidgas till $f : M \to N$. Om t ex $E = 0$ så kan man utvidga varje f_0. Om man fixerar M_0 och M så kan man betrakta E som en funktor av N (morfismer $N_1 \to N_2$ definierar enkelt $E(N_1) \to E(N_2)$). Denna funktor är mycket nära relaterad till Ext^1_R. Den exakta sekvensen $0 \to M_0 \to M \to M/M_0 \to 0$ ger den långa exakta sekvensen:

$$0 \longrightarrow \mathrm{Hom}_R(M/M_0, N) \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M_0, N) \longrightarrow$$

$$\longrightarrow \mathrm{Ext}^1_R(M/M_0, N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow \cdots$$

Nu ser vi att moduler E kan beskrivas som kärnan till avbildningen $\mathrm{Ext}^1_R(M/M_0, N) \to \mathrm{Ext}^1_R(M, N)$. Beteckningen "Ext" ("extension") kommer just från sambandet mellan Ext-funktorerna och olika typer av utvidgningar av homomorfismer.

□

Även singulära homologigrupper av topologiska rum och de Rham kohomologigrupper kan konstrueras som deriverade funktorer (se t.ex. Warner's bok "Foundations of Differentiable Manifolds").

ÖVNINGAR

12.1. Visa att en ändligt genererad R-modul P är projektiv då och endast då det finns en R-modul P' sådana att $P \oplus P' \cong R^n$ för något n ($R^n = R \oplus \ldots \oplus R$ med n termer R).

12.2. Man säger att en exakt sekvens $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ är **splittrad** om det finns en R-homomorfism $j : M'' \to M$ så att $gj = 1_{M''}$. Visa att följande villkor är ekvivalenta för $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$:

(a) det finns $j : M'' \to M$ så att $gj = 1_{M''}$ (dvs sekvensen är splittrad i enlighet med definitionen ovan),

(b) det finns $p : M \to M'$ så att $pf = 1_{M'}$,

(c) det finns $M_0 \subset M$ så att $M = \mathrm{Im}\, f \oplus M_0$ ($\mathrm{Im} = \mathrm{Ker}$ ty sekvensen är exakt).

12.3. (a) Visa att P är en projektiv R-modul då och endast då varje exakt sekvens $0 \to M' \to M \to P \to 0$ är splittrad.

(b) Visa att I är injektiv R-modul då och endast då varje exakt sekvens $0 \to I \to M \to M'' \to 0$ är splittrad.

12.4. Man säger att en R-modul F är **flat** om funktorn $X \to F \otimes_R X$ är exakt.

(a) Visa att varje fri modul är flat.

(b) Visa med hjälp av (a) och t.ex. Övn. 1 att varje projektiv R-modul är flat.

12.5. Låt $\mathcal{C}$ vara en delkategori till ${}_R\mathcal{M}$ sådan att $M = (0)$ är i $\mathcal{C}$ och låt G vara en abelsk grupp. Antag att mot varje M i $\mathcal{C}$ svarar ett element $\varphi(M) \in G$ så att $\varphi((0)) = 0$ (det neutrala elementet i G) och för varje exakt sekvens i ${}_R\mathcal{M}$

$$0 \to M' \to M \to M'' \to 0,$$

där M, M', M'' är objekt i $\mathcal{C}$, gäller det att $\varphi(M) = \varphi(M') + \varphi(M'')$. En sådan funktion φ kallas ibland för en **Euler-Poincaré funktion** på $\mathcal{C}$.

(a) Visa att om M och M' är isomorfa R-moduler som båda tillhör $\mathcal{C}$ så är $\varphi(M) = \varphi(M')$.

(b) Låt $R = K$ vara en kropp och låt $\mathcal{C}$ bestå av ändligt-dimensionella vektorrum. Definiera $\varphi(M) = \dim_K M$ för M i $\mathcal{C}$. Visa att φ är en Euler-Poincaré funktion på $\mathcal{C}$.

(c) Låt $R = \mathbb{Z}$ och låt $\mathcal{C}$ bestå av alla ändliga abelska grupper. Definiera $\varphi(M) = |M|$ (antalet element i M) då M är i $\mathcal{C}$. Visa att φ är en Euler-Poincaré funktion på $\mathcal{C}$.

(d) Visa att det finns en abelsk grupp G^* och en Euler-Poincaré funktion på $\mathcal{C}$ som antar sina värden i G^* sådana att för varje Euler-Poincaré funktion på $\mathcal{C}$ med värden i en abelsk grupp G existerar exakt en grupphomomorfism $f : G^* \to G$ sådan att $f(\varphi^*(M)) = \varphi(M)$ för varje M i $\mathcal{C}$. Gruppen G^* betecknas med $K_0(\mathcal{C})$ och kallas Grothendieckgruppen av $\mathcal{C}$.

Ledning. Definiera G^* som kvoten F/F_0, där F är den fria abelska grupp genererad av isomorfiklasser $[M]$ för M i $\mathcal{C}$, och F_0 är delgruppen genererad av $[M] - [M'] - [M'']$ för alla exakta sekvenser i ${}_RM$

$$0 \to M' \to M \to M'' \to 0,$$

där M, M', M'' är i $\mathcal{C}$.

12.6. Låt φ vara en Euler-Poincaré funktion på $\mathcal{C}$ som i Övn. 5. Låt

$$(\mathbf{M}, \mathbf{d}) \qquad \ldots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \longrightarrow \ldots$$

vara ett komplex i $\mathcal{M}_R$ sådant att M_n och $H_n(\mathbf{M})$ tillhör $\mathcal{C}$ och är 0 för nästan alla n. Med **Euler-karakteristiken** av $\mathbf{M}$ med avseende på φ menas

$$\chi_\varphi(\mathbf{M}) = \sum (-1)^i \varphi(H_i(\mathbf{M})).$$

Antag att för varje exakt sekvens $0 \to M' \to M \to M'' \to 0$ i $\mathcal{M}_R$ gäller det att om M är i $\mathcal{C}$ så är M' och M'' i $\mathcal{C}$. Visa att

$$\chi_\varphi(\mathbf{M}) = \sum (-1)^i \varphi(M_i).$$

Anmärkning. $K_0(\,)$ kan betraktas som funktor från $\mathcal{C}$ till abelska grupper. Man konstruerar också sekvenser av funktorer $K_i(\,)$ för $i \geq 0$. Liksom homologifunktorer spelar dessa funktorer en mycket viktig roll i olika delar av matematiken. En mycket bra introduktion till algebraiska aspekter av K-teorin utgör boken av J. Milnor, Introduction to Algebraic K – theory.