INLEDNING TILL KOMMUTATIV ALGEBRA

J. Brzezinski

MATEMATISKA VETENSKAPER
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
GÖTEBORG 2004

FÖRORD

Dessa föreläsningsanteckningar är en del av en något omarbetad version av en algebrakurs för doktorander som återkommer vartannat år sedan 1979. Kursen handlar om kommutativ algebra med tanke på algebraisk geometri (algebraiska mångfalder i affina och projektiva rum, algebraiska kurvor) och algebraisk talteori (algebraiska heltal, p-adiska tal, diofantiska ekvationer). Dessa två områden har en central ställning och är relaterade till forskningsverksamheten vid institutionen.

Denna kurs tillsamans med kursen "Linjär och multilinjär algebra" har dock en mera universell ambition – den vänder sig till alla som kan komma i kontakt med algebraiska metoder i samband med sin aktuella eller framtida forskning. Därför är ett av dess syften att ge en allmän, något översiktlig, orientering om algebra och dess valda områden med tanke på dem vars matematiska intressen ligger eller kommer att ligga på andra håll. Samtidigt vill man också ge en tillräcklig grund för vidare studier inom algebra för alla de som i samband med sitt forskningsarbete kommer att behöva djupare kunskaper i ämnet.

Kunskaper i algebra förmedlas i ett fåtal kurser inom grundutbildningen. Därför har denna kurs en mycket grundläggande karaktär. Den är tillgänglig för alla som besitter förkunskaper motsvarande GU–kursen "Algebraiska strukturer" (eller den gamla kursen "Grupper, ringar och kroppar"). Men den börjar med en detaljerad (men snabb) repetition av alla nödvändiga förkunskaper. Därför kan den följas av alla som har intresse i algebran och som är beredda att repetera eller komplettera sina förkunskaper under en relativt kort tid. Kapitel 3 handlar om moduler över ringar. Därefter diskuteras lokaliseringar av ringar, ringutvidgningar, Noetherska ringar, dimension av ringar, Dedekindringar och kompletteringar av ringar. Dessa begrepp betraktas i anslutning till några grundläggande begrepp i algebraisk geometri och algebraisk talteori. Kompendiet avslutas med två kapitel av en mera allmän karaktär – ett om kategorier och ett om homologisk algebra.

Kursen är en fördjupnigskurs i grundutbildningen och ingår också som andra delen i en grundkurs i algebra för doktorander. Den är i princip en oberoende fortsättning på den kurs i "Linjär och multilinjär algebra" som gavs tidigare under denna termin.

Dessa föreläsningsanteckningar består av 12 kapitel ur den tidigare algebrakursen för doktorander som har omarbetats och kompletterats för att anpassa innehållet till kursens nya roll i grundutbildningen.

J.B.

Göteborg
Oktober, 2004

KOMPENDIETS STRUKTUR

Kapitel **1** har marginell betydelse för kursen. Det har inkluderats beroende på ett par hänvisningar i Kapitel **2** (och tekniska överväganden när det gäller numreringen).

Kapitel **2** och **3** är grunden för alla efterföljande kapitel och utgör också en del av kursen i linjär och multilinjär algebra som gavs under första delen av terminen.

Kapitel **4** − **9** bör läsas i linjär ordning.

Kapitel **10** har något översiktlig karaktär och bygger på kapitel **4** − **9**. Flera bevis utelämnas.

Kapitel **11** bygger enbart på kapitel **2** och **3**, men några exempel hänvisar till övriga kapitel.

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. Lie tillämpade gruppteorin på problem i matematisk analys – bl a associerade han grupper med differentialekvationer. Teorin för Liegrupper, som samtidigt är grupper och analytiska mångfalder, har mycket stor betydelse både inom matematiken och 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

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

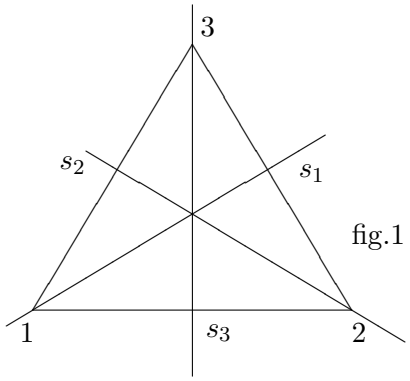


fig.1

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, $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = e'$.

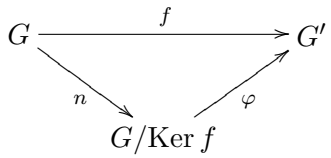
(b) Vi har $g' \in g(\mathrm{Ker}f) \Leftrightarrow g^{-1}g' \in \mathrm{Ker}f \Leftrightarrow f(g^{-1}g') = e' \Leftrightarrow f(g') = f(g)$ dvs sidoklassen $g(\mathrm{Ker}f)$ består av alla element i G vars bild i G' är $f(g)$. Nu definierar vi $\varphi : G/\mathrm{Ker}f \to \mathrm{Im}f$ genom att 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.

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 $\bar{x} \mapsto e^{2\pi inx}$, där n är ett heltal och $\bar{x} \in \mathbb{R}^+/\mathbb{Z}$;

(c) varje karaktär av $\mathbb{Z}$ (med diskret topologi) är $n \mapsto e^{2\pi inx}$, 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 många viktiga matematiska objekt. 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 "$\cdot$" (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 multiplikation 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.

(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

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

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

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

$R = \mathbb{C}[[X]]$ 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 **huvudideal** (eller **principalideal**). En kommutativ ring R i vilken varje ideal är ett huvudideal 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. Denna ring kallas ofta **restklassringen** av R modulo I.

(2.13)^l Konstruktionen av restklassringar. 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 $0+(n), 1+(n), \ldots, n-1+(n)$ (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

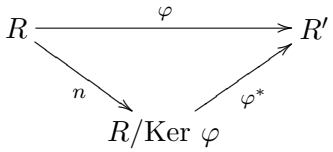
$$\operatorname{Ker}\varphi = \{p \in R[X] : p(i) = 0\} = (X^2+1).$$

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 **primideal** 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 ett primideal.*

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 ett primideal 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).

□

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. Affina algebraiska mängder. Låt K vara en kropp. Med en **algebraisk mängd** V i K^n menar man mängden av alla lösningar $\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n$ till ett ekvationssystem $p_i(X_1, \ldots, X_n) = 0$, där $p_i \in K[X_1, \ldots, X_n]$ för $i \in J$ (en indexmängd) dvs

$$(*) \qquad V = \{\boldsymbol{a} = (a_1, \ldots, a_n) \in K^n : \forall_{i \in J} p_i(a_1, \ldots, a_n) = 0\}.$$

Vi skall också skriva $V = \mathcal{Z}((p_i)_{i \in J})$ och $p(\boldsymbol{a})$ i stället för $p(a_1, \ldots, a_n)$.

(a) Låt I vara idealet i $K[X_1, \ldots, X_n]$ genererat av alla p_i, $i \in J$. Motivera att $V = \mathcal{Z}(I) = \{\boldsymbol{a} \in K^n : \forall_{p \in I} p(\boldsymbol{a}) = 0\}$.

Anmärkning. Hilberts bassats (se även (2.8)(c)) säger att det finns ett ändligt antal polynom sådana att $I = (p_1, \ldots, p_m)$ dvs varje algebraisk mängd i K^n kan beskrivas som lösningsmängden till ett ändligt ekvationssystem.

(b) Låt $\mathcal{J}(V) = \{p \in K[X_1, \ldots, X_n] : \forall_{\boldsymbol{a} \in V} p(\boldsymbol{a}) = 0\}$. Visa att $\mathcal{J}(V)$ är ett ideal i $K[X_1, \ldots, X_n]$ och $\mathcal{J}(V) \supseteq I$ (I ur (a)).

Anmärkning. $\mathcal{J}(V)$ kallas **idealet av den algebraiska mängden** V. Restklassringen

$$K[X_1, X_2, \ldots, X_n]/\mathcal{J}(V)$$

betecknas med $K[V]$ och kallas **ringen av de reguljära funktionerna** på V (lägg märke till att $p + \mathcal{J}(V) = q + \mathcal{J}(V) \Leftrightarrow \forall_{\boldsymbol{a} \in V} p(\boldsymbol{a}) = q(\boldsymbol{a})$ dvs p, q ger samma polynomfunktion på V).

(c) Låt $V = \mathcal{Z}(I)$. Ge ett exempel då $\mathcal{J}(V) \supset I$.

(d) Visa att unionen av två (eller ett ändligt antal) algebraiska mängder och snittet av en godtycklig familj av algebraiska mängder är algebraiska mängder. Motivera också att $\emptyset$ och K^n är algebraiska.

Anmärkning. Detta visar att algebraiska mängder definierar en topologi i K^n. Den kallas **Zariskis topologi** (efter Oscar Zariski).

(e) Låt V_1, V_2 vara delmängder till K^n och I_1, I_2 ideal i $K[X_1, \ldots, X_n]$. Visa att

$$V_1 \subseteq V_2 \Rightarrow \mathcal{J}(V_1) \supseteq \mathcal{J}(V_2), \quad I_1 \subseteq I_2 \Rightarrow \mathcal{Z}(I_1) \supseteq \mathcal{Z}(I_2)$$

samt

$$\mathcal{J}\mathcal{Z}(I) \supseteq I, \quad \mathcal{Z}\mathcal{J}(V) \supseteq V.$$

Därefter motivera att $\mathcal{Z}\mathcal{J}\mathcal{Z}(I) = \mathcal{Z}(I)$ och $\mathcal{J}\mathcal{Z}\mathcal{J}(V) = \mathcal{J}(V)$. (Lägg märke till att om $V = \mathcal{Z}(I)$ så är $\mathcal{Z}\mathcal{J}(V) = V$).

(f) En algebraisk mängd $V \subseteq K^n$ kallas **irreducibel** om V inte är unionen av två äkta algebraiska delmängder. Visa att V är irreducibel då och endast då $\mathcal{J}(V)$ är ett primideal.

(g) Låt V vara en algebraisk mängd i K^n, där K är en algebraiskt sluten kropp dvs för varje $p \in K[X]$, $\deg p \geq 1$ existerar $\alpha \in K$ så att $p(\alpha) = 0$ (t ex $K = \mathbb{C}$). Visa att $\mathcal{J}(V)$ är maximalt då och endast då V består av en punkt i K^n.

Ledning. Här måste man använda Hilberts Nullstellensatz – se (2.26) (c). Den formen av satsen kallas svag. Den starka formen säger att för varje ideal I är $\mathcal{J}\mathcal{Z}(I) = \{p \in K[X_1, \ldots, X_N] : p^m \in I \text{ för något } m \geq 1\}$. Hilberts Nullstellensatz visas senare.

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). 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).

□

(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).

□

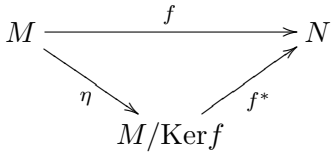
(3.10) Proposition. *Om $f : M \to N$ är en R-homomorfism så är* $\mathrm{Ker}f$ *en delmodul till M och* $\mathrm{Im}f$ *är en delmodul till N. (Om $R = K$ är en kropp så är nollrummet till f ett delrum till M och värderummet till f är ett delrum till N.)*

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 $f : M \to N$ 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 $f : M \to N$ är en R-homomorfism så existerar exakt en monomorfism $f^* : M/\mathrm{Ker}f \to N$ sådan att diagrammet:



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

□

(3.13) Proposition. *En R-homomorfism $f : M \to N$ 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 $r \in R$.

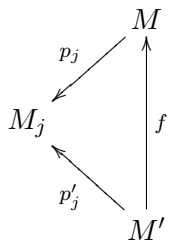
3.6. Låt I_1, I_2 vara två ideal i en ring med etta R sådana att det finns en R-isomorfism av R-moduler R/I_1 och R/I_2. Visa att $I_1 = I_2$. (Observera att R/I betraktas som R-modul i enlighet med (3.2)(d)).

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.

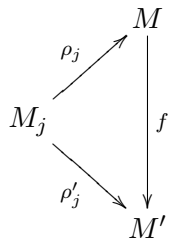
3.8. Låt $M' \xrightarrow{f} M \xrightarrow{g} M'$ vara en sekvens av R-moduler och R-homomorfismer sådana att $gf = id_{M'}$. Visa att $M = \mathrm{Im}f \oplus \mathrm{Ker}g$.

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

$$\begin{array}{ccc} M & \xrightarrow{\ f\ } & N \\ \downarrow & & \downarrow \\ M/M' & \xrightarrow[\ f^*\ ]{} & N/N' \end{array}$$

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.

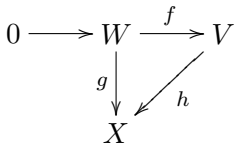
(d) $K = \mathbb{R}$, $V =$ alla periodiska följder $(a_1, a_2, \ldots), a_i \in \mathbb{R}$, av alla ändliga perioder.

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)).

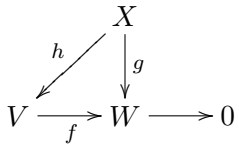
3.27. Låt K vara en kropp, V, W, X linjära rum över K.

(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.

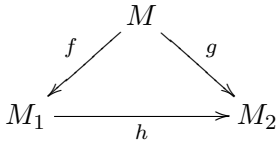
Anmärkning. (a) säger att varje K-vektorrum X är **injektivt**, däremot (b) att det är **projektivt**. Definitionerna av projektiva och injektiva moduler givna i (a) och (b) (då K är en ring) diskuterar vi senare.

(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

LOKALISERING OCH LOKALA RINGAR

Konstruktionen av de rationella talen från heltalen är ett specialfall av en allmän konstruktion i algebran som mot en ring ordnar nära relaterade ringar – dess lokaliseringar – med enklare idealstruktur. För att undersöka en ring studerar man dess lokaliseringar som ofta tillåter en bättre beskrivning. Ibland får man som ett resultat av lokaliseringen lokala ringar – ringar med exakt ett maximalideal. Geometriskt innebär lokalisering att man övergår från funktioner definierade på en öppen delmängd till en mångfald till de funktioner som är definierade i en omgivning till en punkt tillhörande den öppna mängden. Detta kapitel ägnas åt lokaliseringsproceduren och en beskrivning av några enkla egenskaper hos lokala ringar. Vi ger också ett antal exempel på lokala ringar av aritmetisk och geometrisk karaktär. Alla ringar i detta kapitel är kommutativa med etta eller nollringen med endast ett element 0.

(4.1) Definition. Med en **multiplikativ mängd** i en ring R menar man en delmängd S till R sådan att $1 \in S$ och om $s_1, s_2 \in S$ så $s_1 s_2 \in S$.

□

(4.2) Exempel. (a) Låt R vara ett integritetsområde och $S = R \setminus \{0\}$.

(b) Mera allmänt, låt $\mathfrak{p}$ vara ett primideal i R och $S = R \setminus \mathfrak{p}$ (i (a) är $\mathfrak{p} = (0)$).

(c) Låt R vara en ring och S mängden av icke-nolldelare i R (dvs $s \in S$ då och endast då $sx = 0$ med $x \in R$ implicerar att $x = 0$).

(d) Låt $f \in R$ och $S = \{f^n, n \geq 0\}$ (vi antar att $f^0 = 1$).

□

(4.3) Lokalisering av en ring med avseende på en multiplikativ mängd. Låt R vara en ring och S en multiplikativ mängd i R. Betrakta alla par (r, s), där $r \in R$ och $s \in S$ (tänk på alla bråk $\frac{r}{s}$, där r, s är heltal och $s \neq 0$!). Definiera följande relation på mängden av alla sådana par:

$$(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow s(s_2 r_1 - s_1 r_2) = 0 \quad \text{för något } s \in S$$

(förekomsten av faktorn s motiveras om en stund). Relationen "$\sim$" är en ekvivalensrelation. Det är klart att den är reflexiv och symmetrisk. För transitiviteten antag att $(r_1, s_1) \sim (r_2, s_2)$ dvs $s(s_2 r_1 - s_1 r_2) = 0$, och $(r_2, s_2) \sim (r_3, s_3)$ dvs $s'(s_3 r_2 - s_2 r_3) = 0$. Då är $ss's_2(s_3 r_1 - s_1 r_3) = 0$[†]. Kalla nu ekvivalensklassen av paret (r, s) för bråk och beteckna den med $\frac{r}{s}$. Definiera:

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}, \\ \frac{r_1}{s_1}\frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2}. \end{aligned}$$

Man kontrollerar lätt att dessa operationer (addition och multiplikation av bråk) är väldefinierade (dvs oberoende av representationen av ett bråk) och att de ger en ringstruktur i mängden av alla bråk. Den ringen betecknas med R_S eller $S^{-1}R$ och kallas **lokaliseringen av R med avseende på S.** □

(4.4) Anmärkning. Funktionen $f(r) = \frac{r}{1}$ är en ringhomomorfism $f : R \to R_S$, men den behöver inte vara injektiv (se Övn. 1 (b)).

□

(4.5) Proposition. *Låt R vara ett integritetsområde och $S = R \setminus \{0\}$. Då är R_S en kropp och homomorfismen $f : R \to R_S$, där $f(r) = \frac{r}{1}$, är en injektion. Kroppen R_S kallas oftast* **kvotkroppen** *av R* [††].

Bevis. Att R_S är en kropp följer direkt ur definitionen ty varje bråk $\frac{r}{s}$ med $r \neq 0$ och $s \neq 0$ är inverterbart ($\frac{s}{r}$ är också ett tillåtet bråk). Om $f(r) = \frac{r}{1} = 0$ så är $sr = 0$ för något $s \in S = R \setminus \{0\}$ dvs $r = 0$ ty R är ett integritetsområde. □

Låt oss betrakta några exempel på lokaliseringar:

(4.6) Exempel. (a) Låt $R = \mathbb{Z}$ och $S = \mathbb{Z} \setminus (p)$, där p är ett primtal. Då är

$$\mathbb{Z}_S = \{\frac{m}{n} \in \mathbb{Q} : p \nmid n\}.$$

Man skriver ofta $\mathbb{Z}_S = \mathbb{Z}_{(p)}$.

[†]Försök bevisa transitiviteten utan faktorerna s och s'! Det är inte möjligt att göra därför att det kan finnas nolldelare i R, vilket ej är fallet vid konstruktionen av $\mathbb{Q}$ ur $\mathbb{Z}$.

[††]Fast den borde snarare kallas "bråkkroppen" av R.

(b) Mera allmänt låt R vara en ring och $S = R \setminus \mathfrak{p}$, där $\mathfrak{p}$ är ett primideal i R. I detta fall skriver man $R_S = R_{\mathfrak{p}} = \{\frac{r}{s} : r \in R \quad \text{och} \quad s \notin \mathfrak{p}\}$.

(c) Som ett specialfall av (b) låt $R = \mathbb{C}[X, Y]$ och låt $\mathfrak{p} = (X - a, Y - b)$ vara ett maximalideal i R. Här är

$$\mathbb{C}[X, Y]_{\mathfrak{p}} = \{\frac{p(X, Y)}{q(X, Y)} : q(X, Y) \notin \mathfrak{p}\} = \{\frac{p(X, Y)}{q(X, Y)} : q(a, b) \neq 0\}$$

ringen av de rationella funktionerna i X och Y som är definierade i punkten $(a, b) \in \mathbb{C}$. Den ringen betecknas ofta $\mathbb{C}[X, Y]_{(a,b)}$ och kallas den lokala ringen av (a, b) på $\mathbb{C}^2$ (vi generaliserar detta exempel senare i (4.22)).

(d) Om R är en ring, $f \in R$ och $S = \{f^n, n \geq 0\}$ (se (4.2)(d)) så betecknas R_S med R_f. T.ex. $\mathbb{Z}_2 = \{\frac{m}{2^n} : m, n \in \mathbb{Z},\ n \geq 0\} = \mathbb{Z}[\frac{1}{2}]$, $\mathbb{C}[X, Y]_X = \{\frac{p(X,Y)}{X^n} : n \geq 0, p \in \mathbb{C}[X, Y]\}$.

□

Idealstrukturen i lokaliseringen av en ring är vanligen enklare än i den ursprungliga ringen. Ibland får man s.k. lokala ringar:

(4.7) Definition. Man säger att R är en **lokal ring** om R innehåller endast ett maximalideal $\mathfrak{m}$. Kvoten $R/\mathfrak{m}$ kallas **residukroppen** av R.

□

(4.8) Exempel. (a) Varje kropp är en lokal ring – maximalidealet är $\mathfrak{m} = (0)$.

(b) Om R är en ring och $\mathfrak{p}$ är ett primideal i R så är $R_{\mathfrak{p}}$ en lokal ring. Vi har nämligen

$$R_{\mathfrak{p}} = \{\frac{r}{s} : r \in R,\ s \in R \setminus \mathfrak{p}\}.$$

Ringen $R_{\mathfrak{p}}$ innehåller idealet $\mathfrak{p}R_{\mathfrak{p}} = \{\frac{r}{s} : r \in \mathfrak{p} \quad \text{och} \quad s \in R \setminus \mathfrak{p}\}$ (kontrollera att detta är ett äkta ideal!). Om I är ett äkta ideal i $R_{\mathfrak{p}}$ så är $I \subseteq \mathfrak{p}R_{\mathfrak{p}}$. I själva verket ger $I \nsubseteq \mathfrak{p}R_{\mathfrak{p}}$ att det finns $\frac{r}{s} \in I$ med $r \notin \mathfrak{p}$ och $s \notin \mathfrak{p}$, dvs $\frac{s}{r} \in R_{\mathfrak{p}}$. Detta ger $1 = \frac{r}{s} \cdot \frac{s}{r} \in I$ vilket betyder att $I = R_{\mathfrak{p}}$. Alltså är $\mathfrak{p}R_{\mathfrak{p}}$ det största äkta idealet i $R_{\mathfrak{p}}$.

(c) Låt U vara ett område i det komplexa planet, $\mathcal{A}(U)$ ringen av alla analytiska funktioner i U (ett integritetsområde!) och $\mathcal{M}(U)$ kvotkroppen av $\mathcal{A}(U)$ dvs kroppen av alla meromorfa funktioner i U. Låt $P \in U$ och låt

$$\mathcal{O}_{P,U} = \{f \in \mathcal{M}(U) : P \quad \text{är inte en pol till } f\}.$$

Man kontrollerar enkelt att $\mathcal{O}_{P,U}$ är en lokal ring vars maximalideal är

$$\mathfrak{m}_{P,U} = \{f \in \mathcal{M}(U) : f(P) = 0\}.$$

$\mathcal{O}_{P,U}$ kallas den lokala ringen av P på U. För vidare generaliseringar se Övn. 14. Observera att $\mathcal{O}_{P,U} = \mathcal{A}(U)_{\mathfrak{p}}$, där $\mathfrak{p} = \{f \in \mathcal{A}(U) : f(P) = 0\}$.

(d) Ringen $\mathbb{C}[[X]]$ av de formella potensserier i variabeln X (se (2.6)(b)) är en lokal ring. Dess enda maximalideal består av alla potensserier $a_0 + a_1X + a_2X^2 + \ldots$ med $a_0 = 0$ (se Övn. 4). Även den delring till $\mathbb{C}[[X]]$ som består av alla potensserier med konvergensradie > 0 är en lokal ring (se t ex H. Cartan, Th. Élem. des Funct. Anal., Chap. 1 – men det är lätt att visa på egen hand).

□

(4.9) Proposition. *Låt R vara en ring. Följande villkor är ekvivalenta:*

(*a*) *R är en lokal ring;*

(*b*) *Om r_1, r_2 är ej inverterbara element i R så är också $r_1 + r_2$ ej inverterbart;*

(*c*) *Alla ej inverterbara element i R bildar ett ideal.*

Bevis. (a) ⇒ (b) Låt $\mathfrak{m}$ vara maximalidealet i R och låt r_1, r_2 vara ej inverterbara element i R. Idealen (r_1) och (r_2) är äkta så att de ligger i maximalideal. Alltså är $(r_1), (r_2) \subseteq \mathfrak{m}$ därför att det endast finns ett maximalideal. Detta visar att $r_1 + r_2$ inte är inverterbart ty $r_1 + r_2 \in \mathfrak{m}$.

(b) ⇒ (c) Om r inte är inverterbart och $x \in R$ så är också rx ej inverterbart (ty $rxy = 1$ säger att r är inverterbart). Detta och (b) implicerar (c).

(c) ⇒ (a) Låt $\mathfrak{m}$ vara idealet av alla ej inverterbara element. Om I är ett ideal i R och $I \nsubseteq \mathfrak{m}$ så finns $x \in I \setminus \mathfrak{m}$. Då är x inverterbart så att $I = R$. Alltså är $\mathfrak{m}$ det största äkta idealet i R ($1 \notin \mathfrak{m}$). Således är $\mathfrak{m}$ det enda maximalidealet i R. □

(4.10) Följdsats. *Om R är en ring och $\mathfrak{m}$ ett äkta ideal i R sådant att $x \in R \setminus \mathfrak{m}$ implicerar att x är inverterbart, så är R lokal och $\mathfrak{m}$ dess maximalideal.*

Bevis. Se bevis av (c) $\Rightarrow$ (a) i (4.9). □

Nu skall vi diskutera lokaliseringar av moduler över ringar.

(4.11) Definition. Låt R vara en ring, S en multiplikativ mängd i R och M en R-modul. Med **lokaliseringen** M_S av M med avseende på S menar man den R_S-modul som konstrueras på följande sätt: Betrakta alla par (m, s), där $m \in M$ och $s \in S$. Låt $s_1, s_2 \in S$, $m_1, m_2 \in M$. Definiera

$$(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow s(s_2 m_1 - s_1 m_2) = 0 \quad \text{för något} \quad s \in S.$$

Man kontrollerar lätt att "$\sim$" är en ekvivalensrelation (se (4.3)). Låt $\frac{m}{s}$ vara ekvivalensklassen av (m, s). Definiera

$$\begin{aligned} \frac{m_1}{s_1} + \frac{m_2}{s_2} &= \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}, \\ \frac{r}{s'} \cdot \frac{m}{s} &= \frac{rm}{s's}, \end{aligned}$$

där $r \in R$ och $s, s' \in S$. Man visar att dessa operationer är korrekt definierade och att man får en R_S-modul. Den betecknas med M_S.

Om $f : M \to N$ är en R-homomorfism, så definierar $f_S : M_S \to N_S$, där $f_S(\frac{m}{s}) = \frac{f(m)}{s}$ en R_S-homomorism (kontrollera att f_S är väldefinierad dvs att definitionen inte beror på representationen av bråket $\frac{m}{s}$).

□

(4.12) Anmärkning. Definitionen (4.11) visar att vi får en kovariant funktor (se (11.4))

$$F_S : \mathrm{Mod}(R) \to \mathrm{Mod}(R_S)$$

sådan att $F_S(M) = M_S$ och $F_S(f) = f_S$ då $f : M \to N$. Den kallas **lokaliseringsfunktorn**. Se vidare Övn. 8.

□

(4.13) Proposition. *Lokaliseringsfunktorn är exakt dvs om $M' \xrightarrow{f} M \xrightarrow{g} M''$ är en exakt sekvens av R-moduler så är $M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$ en exakt sekvens av R_S-moduler.*

Bevis. Vi har $g_S f_S(\frac{m'}{s}) = \frac{gf(m')}{s} = 0$ så att $g_S f_S = 0$ dvs $\mathrm{Im} f_S \subseteq \mathrm{Ker} g_S$. Antag att $\frac{m}{s} \in \mathrm{Ker} g_S$ så att $g_S(\frac{m}{s}) = \frac{g(m)}{s} = 0$ dvs $s'g(m) = 0$ för något $s' \in S$. Detta betyder att $g(s'm) = 0$ dvs $s'm \in \mathrm{Ker} g = \mathrm{Im} f$. Alltså är $s'm = f(m')$ så att $\frac{m}{s} = \frac{f(m')}{ss'}$ dvs $\frac{m}{s} \in \mathrm{Im} f_S$.
□

(4.14) Anmärkning. Ur (4.13) följer det att om $N \subseteq M, N$ en delmodul, så kan N_S betraktas som en delmodul till M_S (ty en injektion $0 \to N \to M$ ger att $0 \to N_S \to M_S$ är en injektion). Speciellt om I är ett ideal i R så är I_S ett ideal i R_S.

□

Vi skall beskriva sambandet mellan ideal i R och R_S:

(4.15) Proposition. *Låt S vara en multiplikativ mängd i R och $f_S : R \to R_S$ homomorfismen $f_S(r) = \frac{r}{1}$ för $r \in R$. Låt I vara ett ideal i R och I' ett ideal i R_S. Då gäller:*

(a) $I_S = R_S$ då och endast då $I \cap S \neq \emptyset$,

(b) $f_S^{-1}(I_S) = I$ då och endast då för varje $s \in S$ och $x \in R$ implicerar $sx \in I$ att $x \in I$,

(c) $(f_S^{-1}(I'))_S = I'$.

Bevis. (a) Om $s \in I \cap S$ så är $\frac{s}{1} \in I_S$ och $\frac{1}{s} \in I_S$ så att $1 \in I_S$. Alltså är $I_S = R_S$. Om $I_S = R_S$ så $\frac{1}{1} = \frac{i}{s}$, där $i \in I$, dvs $s'(s - i) = 0$ för $s' \in S$. Alltså är $s's \in I \cap S \neq \emptyset$.

(b) Om $f_S^{-1}(I_S) = I$ och $sx \in I$ så är $\frac{x}{1} = \frac{sx}{s} \in I_S$, vilket ger att $x \in f_S^{-1}(I_S) = I$. Omvänt: Om villkoret $sx \in I \Rightarrow x \in I$ är uppfyllt och $x \in f_S^{-1}(I_S)$ så är $\frac{x}{1} = \frac{i}{s}$, dvs $s'(sx - i) = 0$ för ett $s' \in S$. Den likheten ger $(s's)x \in I$, vilket implicerar $x \in I$. Alltså är $f_S^{-1}(I_S) \subseteq I$. Den motsatta inklusionen är självklar ($I \subseteq f_S^{-1}(I_S)$ ty $f_S(I) \subseteq I_S$).

(c) Lämnas som övning (Övn. 7). □

(4.16) Definition. Mängden av alla primideal i en ring R betecknas med Spec$R$ och kallas **spektrum** av R.

□

(4.17) Proposition. *Det finns en en-entydig motsvarighet mellan alla primideal $\mathfrak{p}$ i R sådana att $\mathfrak{p} \cap S = \emptyset$, och alla primideal i R_S, som ges av $\mathfrak{p} \mapsto \mathfrak{p}_S$.*

Bevis. Först noterar vi att om $\mathfrak{p}$ är ett primideal i R och $\mathfrak{p} \cap S = \emptyset$ så är $\mathfrak{p}_S$ ett primideal i R_S ($\mathfrak{p}_S$ är äkta enligt (4.15)(a)). Låt $U_S = \{\mathfrak{p} \in \text{Spec}R : \mathfrak{p} \cap S = \emptyset\}$. Vi har två funktioner:

$$U_S \to \text{Spec}R_S, \quad \text{där} \quad \mathfrak{p} \mapsto \mathfrak{p}_S,$$

och

$$\mathrm{Spec}R_S \to U_S, \quad \text{där} \quad \mathfrak{p}' \mapsto f_S^{-1}(\mathfrak{p}')$$

(den andra avbildar primideal på primideal ty vid varje homomorfism $f : R \to R'$ är inversa bilden $f^{-1}(\mathfrak{p}')$ av ett primideal $\mathfrak{p}'$ i R' ett primideal i R – se (2.9)).

Nu säger (4.15) (b) och (c) att den ena av dessa två funktioner är inversen till den andra, ty $f_S^{-1}(\mathfrak{p}_S) = \mathfrak{p}$ då $\mathfrak{p} \cap S = \emptyset$ (villkoret $sx \in \mathfrak{p}$ och $s \notin \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ är uppfyllt ty $\mathfrak{p}$ är ett primideal) och $(f_S^{-1}(\mathfrak{p}'))_S = \mathfrak{p}'$. Alltså etablerar dessa funktioner en en-entydig motsvarighet mellan alla $\mathfrak{p} \in \mathrm{Spec}R$ sådana att $\mathfrak{p} \cap S = \emptyset$ och alla $\mathfrak{p}' \in \mathrm{Spec}R_S$. □

Vanligen är det enklare att undersöka ringar R och R-moduler M genom att studera deras lokaliseringar $R_\mathfrak{p}$ och $M_\mathfrak{p}$ för $\mathfrak{p} \in \mathrm{Spec}R$. Man försöker bevisa "globala" egenskaper hos R och M genom att studera "lokala" egenskaper hos $R_\mathfrak{p}$ och $M_\mathfrak{p}$ för $\mathfrak{p} \in \mathrm{Spec}R$. Här följer några exempel.

(4.18) Proposition. *Låt M vara en R-modul. Då är följande villkor ekvivalenta:*

(*a*) $M = (0)$,

(*b*) $M_\mathfrak{p} = 0$ *för varje primideal* $\mathfrak{p}$ *i* R,

(*c*) $M_\mathfrak{m} = 0$ *för varje maximalideal* $\mathfrak{m}$ *i* R.

Bevis. Implikationerna (a) ⇒ (b) ⇒ (c) är självklara. Låt $m \in M$. Betrakta idealet $\mathrm{Ann}(m) = \{r \in R : rm = 0\}$ (se Övn. 3.4). Antag att $\mathrm{Ann}(m)$ är ett äkta ideal. Då existerar ett maximalideal $\mathfrak{m}$ sådant att $\mathrm{Ann}(m) \subseteq \mathfrak{m}$. Men $\frac{m}{1} = 0$ i $M_\mathfrak{m}$ så att det finns $s \in R \setminus \mathfrak{m}$ sådant att $sm = 0$. Alltså har vi en motsägelse ty $s \in \mathrm{Ann}(m) \subseteq \mathfrak{m}$ och $s \notin \mathfrak{m}$. Detta betyder att $\mathrm{Ann}(m) = R$, vilket ger att $1m = m = 0$, ty $1 \in \mathrm{Ann}(m)$. Alltså är $M = 0$. □

(4.19) Följdsats. *Låt $f : M \to N$ vara en R-homomorfism av R-moduler sådan att för varje primideal $\mathfrak{p} \in SpecR$ är $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ en injektion (resp. surjektion). Då är f en injektion (resp. surjektion).*

Bevis. Betrakta den exakta sekvensen $0 \to \mathrm{Ker}f \to M \xrightarrow{f} N$. Om $\mathfrak{p} \in \mathrm{Spec}R$ så är också sekvensen

$$0 \to (\mathrm{Ker}f)_\mathfrak{p} \to M_\mathfrak{p} \xrightarrow{f_\mathfrak{p}} N_\mathfrak{p}$$

exakt (se (4.13)). Om nu $f_\mathfrak{p}$ är en injektion för varje $\mathfrak{p}$, så är $(\mathrm{Ker}f)_\mathfrak{p} = 0$ för varje $\mathfrak{p} \in \mathrm{Spec}R$. Alltså är $\mathrm{Ker}f = 0$ enligt (4.18) dvs f är en injektion. På liknande sätt visas fallet med surjektion. □

(4.20) Proposition. *Låt R vara ett integritesområde med kvotkroppen K. Då är $R = \bigcap R_{\mathfrak{m}}$, där $\mathfrak{m}$ löper över alla maximalideal i R ($R_{\mathfrak{m}} = \{\frac{r}{s} : r \in R,\, s \in R \setminus \mathfrak{m}\}$ är en delring till K).*

Bevis. Det är klart att $R \subseteq R_{\mathfrak{m}}$. Antag att $x \in \bigcap R_{\mathfrak{m}}$. Låt $D_x = \{r \in R : rx \in R\}$. D_x är ett ideal i R (kontrollera!). Antag att D_x är ett äkta ideal. Då är $D_x \subseteq \mathfrak{m}$, där $\mathfrak{m}$ är ett maximalideal. Men $x \in R_{\mathfrak{m}}$ så att $x = \frac{r}{s}$, där $r \in R$ och $s \in R \setminus \mathfrak{m}$. Samtidigt betyder $sx = r \in R$ att $s \in D_x \subseteq \mathfrak{m}$ vilket ger en motsägelse. Alltså är $D_x = R$ så att $1 \in D_x$. Detta ger $x \in R$. □

(4.21) Exempel. Låt V vara en algebraisk varietet (= en irreducibel algebraisk mängd – se Övn. 2.22) i $\mathbb{C}^n$. Låt $\mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_n]$ vara ringen av de reguljära funktionerna på V (dvs $\mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[X_1, \ldots, X_n]/\mathcal{I}(V)$). Enligt Hilberts Nullstellensatz är alla maximalideal i $\mathbb{C}[V]$ av formen $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, där $(a_1, \ldots, a_n) \in V$. Likheten $\mathbb{C}[V] = \bigcap \mathbb{C}[V]_{\mathfrak{m}}$ säger att varje rationell funktion på V (dvs en funktion tillhörande kvotkroppen $\mathbb{C}(V)$ av $\mathbb{C}[V]$) som är reguljär i varje punkt av V (dvs för varje punkt $\boldsymbol{a} \in V$ finns en omgivning sådan att för $\boldsymbol{x}$ tillhörande omgivningen är $f(\boldsymbol{x}) = \frac{p(\boldsymbol{x})}{q(\boldsymbol{x})}$, där $p, q \in \mathbb{C}[X_1, \ldots, X_n]$ och $g(\boldsymbol{a}) \neq 0$) måste vara reguljär på hela V dvs $f \in \mathbb{C}[V]$. Man skriver ibland $\mathbb{C}[V]_{\mathfrak{m}} = \mathcal{O}_{P,V}$, där $P = (a_1, \ldots, a_n)$, och kallar $\mathcal{O}_{P,V}$ den lokala ringen för P på V.

□

Vi avslutar detta kapitel med några ord om nilradikalen och Jacobsonradikalen av en ring.

Vi repeterar (se Övn. 2.21):

(4.22) Definition. Med **nilradikalen** $\mathcal{N}(R)$ av en ring R menar man idealet i R som består av alla nilpotenta element i R dvs $\mathcal{N}(R) = \{r \in R : \exists_{n>0} r^n = 0\}$.

□

(4.23) Proposition. *$\mathcal{N}(R)$ är snittet av alla primideal i R.*

Bevis. Se Övn. 2.21 och Övn. 11. □

(4.24) Definition. Med **Jacobsonradikalen** $J(R)$ av R menar man snittet av alla maximalideal i R.

□

(4.25) Proposition. *$x \in J(R) \Leftrightarrow 1 + rx$ är inverterbart i R för varje $r \in R$.*

Bevis. "⇒" Om $1 + rx$ inte är inverterbart så finns det ett maximalideal $\mathfrak{m}$ sådant att $(1 + rx) \subseteq \mathfrak{m}$. Men $x \in J(R) \subseteq \mathfrak{m}$ så att $1 \in \mathfrak{m}$ – en motsägelse.

"⇐" Om $x \notin J(R)$ så finns det ett maximalideal $\mathfrak{m}$ sådant att $x \notin \mathfrak{m}$. Då är $\mathfrak{m} + Rx = R$ (ty $\mathfrak{m} + Rx$ är ett ideal som innehåller $\mathfrak{m}$). Alltså är $1 = m + rx$ för ett $m \in \mathfrak{m}$ och $r \in R$. Detta innebär att $m = 1 + (-r)x \in \mathfrak{m}$ inte är inverterbart. □

(4.26) Exempel. (a) $\mathcal{N}(\mathbb{Z}) = J(\mathbb{Z}) = (0)$; $\mathcal{N}(K[X_1, \ldots, X_n]) = J(K[X_1, \ldots, X_n]) = (0)$.

(b) Om R är en lokal ring med maximalidealet $\mathfrak{m}$ och om R saknar nilpotenta element (t ex R ett integritetsområde) så är $\mathcal{N}(R) = (0)$ och $J(R) = \mathfrak{m}$ (t ex R en lokalisering av ett integritetsområde med avseende på ett primideal).

□

(4.27) Nakayamas Lemma. *Låt M vara en ändligt genererad R-modul och I ett ideal i R sådant att $I \subseteq J(R)$. Om $IM = M$ så är $M = 0$.*

Bevis. Antag att $M \neq 0$ och låt $M = Rm_1 + \ldots + Rm_k$, där $m_1, \ldots, m_k$ är en minimal uppsättning av generatorer för M. Vi har $m_k \in M = IM$ så att

$$m_k = r_1 m_1 + \ldots + r_k m_k,\ r_1, \ldots, r_k \in I,$$

vilket ger $(1 - r_k)m_k = r_1 m_1 + \ldots + r_{k-1} m_{k-1}$ (uttrycket tolkas som 0 då $k = 1$). Enligt (4.25) är $1 - r_k$ inverterbart i R (ty $r_k \in J(R)$) så att

$$m_k = \sum_{i=1}^{k-1} \frac{r_i}{1 - r_k} m_i$$

dvs generatorn m_k kan elimineras. Detta strider mot antagandet att $m_1, \ldots, m_k$ var en minimal uppsättning av generatorer för M. Alltså är $M = 0$. □

(4.28) Följdsats. *Låt M vara en ändligt genererad R-modul och N en delmodul till M sådan att $M = N + IM$ för ett ideal $I \subseteq J(R)$. Då är $M = N$* [†].

Bevis. Vi har $I(M/N) = (IM + N)/N = M/N$. Alltså är $M/N = (0)$ dvs $M = N$. □

(4.29) Proposition. *Låt R vara en lokal ring med maximalidealet $\mathfrak{m}$ och M en ändligt genererad R-modul. Om $m_1, \ldots, m_k \in M$ är sådana att $\bar{m}_1, \ldots, \bar{m}_k$ bildar en bas för $M/\mathfrak{m}M$ över $R/\mathfrak{m}$ (se* (3.14)*) så genererar $m_1, \ldots, m_k$ R-modulen M.*

Bevis. Låt $N = Rm_1 + \ldots + Rm_k \subseteq M$. Då är bilden av N vid den naturliga surjektionen $M \to M/\mathfrak{m}M$ lika med $M/\mathfrak{m}M$. Alltså är $N + \mathfrak{m}M = M$ ($N + \mathfrak{m}M$ innehåller kärnan $\mathfrak{m}M$ och har samma bild som M). Enligt (4.28) är $N = M$. □

[†] Ofta kallas den följdsatsen för Nakayamas Lemma.

ÖVNINGAR

4.1. Beskriv lokaliseringarna:

(a) $(\mathbb{Z}/(4))_S$, där $S = \{1, 3\}$; (b) $(\mathbb{Z}/(6))_{\mathfrak{p}}$, där $\mathfrak{p}$ är ett primideal i $\mathbb{Z}/(6)$.

4.2. Låt R vara en lokal ring och $\mathfrak{m}$ dess maximalideal. Visa att homomorfismen $f : R \to R_{\mathfrak{m}}$, där $f(r) = \frac{r}{1}$, är en isomorfism.

4.3. Låt M vara en ändligt genererad R-modul och S en multiplikativ mängd i R. Visa att $M_S = 0$ då och endast då det finns $s \in S$ sådant att $sM = 0$ (speciellt är det så då S innehåller 0).

4.4. Visa att $\mathbb{C}[[X]]$ är en lokal ring och mera allmänt $K[[X_1, \ldots, X_n]]$, då K är en kropp.

4.5. Låt S vara en multiplikativ mängd i R och M, N två R-moduler. Visa att:

(a) $R_S \otimes_R M \cong M_S$, där $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$,

(b) $M_S \otimes_{R_S} N_S \cong (M \otimes_R N)_S$, där $\frac{m}{s} \otimes \frac{n}{s'} \mapsto \frac{m \otimes n}{ss'}$.

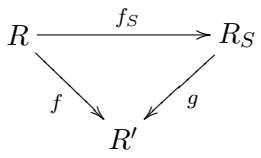
4.6. Är följande påståenden sanna?

(a) För varje $\mathfrak{p} \in \mathrm{Spec}R$ saknar $R_{\mathfrak{p}}$ nilpotenta element $\Leftrightarrow$ R saknar nilpotenta element.

(b) För varje $\mathfrak{p} \in \mathrm{Spec}R$ saknar $R_{\mathfrak{p}}$ nolldelare $\Leftrightarrow$ R saknar nolldelare.

4.7. Visa (4.15)(c).

4.8. Låt R vara en ring och S en multiplikativ mängd i R. Visa att paret (R_S, f_S), där $f_S : R \to R_S$ ges av $f_S(r) = \frac{r}{1}$ har följande universella egenskap: För varje ring R' och varje homomorfism $f : R \to R'$ sådan att $f(s)$ har invers i R' då $s \in S$ finns det exakt en ringhomomorfism $g : R_S \to R'$ så att diagrammet



kommuterar.

4.9. Låt $f \in R$. Visa att $R_f \cong R[X]/(fX - 1)$ (R_f definierades i (4.6)(d)).

4.10. Visa att förutsättningen i Nakayamas lemma om att M är en ändligt genererad modul är väsentlig.

4.11. Låt I vara ett ideal i en ring R.

(a) Visa att $\sqrt{I} = \{r \in R : \exists_n r^n \in I\}$ är ett ideal i R. Det kallas **radikalen** av I.

(b) Visa att $\sqrt{I} = \bigcap \mathfrak{p}$, där $\mathfrak{p}$ löper över alla primideal som innehåller I.

Anmärkning. Om $I = (0)$ så är $\sqrt{(0)} = \mathcal{N}(R)$. (b) generaliserar (4.24).

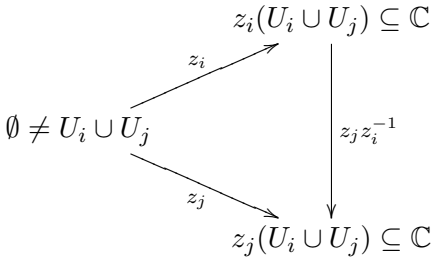
4.12. Låt K vara en kropp och R dess delring sådan att för varje $a \in K$ är $a \in R$ eller $1/a \in R$. Visa att R är en lokal ring. Ge exempel på sådana R!

Anmärkning. En ring R med den egenskapen kallas **valuationsring**.

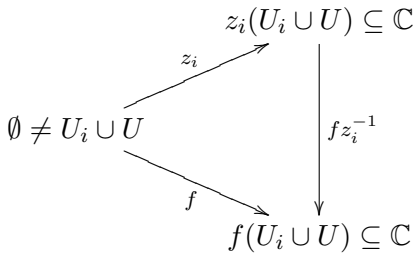
4.13. Visa att för varje maximalideal $\mathfrak{m}$ i R är $R/\mathfrak{m}^n$ en lokal ring (n ett naturligt tal ≥ 1).

Ledning. Om I, I' är ideal i R och $\mathfrak{p}$ är ett primideal så implicerar $II' \subseteq \mathfrak{p}$ att $I \subseteq \mathfrak{p}$ eller $I' \subseteq \mathfrak{p}$ (visa det som en delövning).

4.14. Låt M vara en analytisk mångfald av komplex dimension 1 (dvs M är ett Hausdorffrum med en öppen övertäckning $\{U_i\}_{i\in I}$ sådan att för varje $i \in I$ finns det en homeomorfism z_i av U_i med en öppen delmängd av $\mathbb{C}$ och



för varje par (i, j) är funktionen $z_j z_i^{-1}$ i diagrammet ovan analytisk och har derivatan $\neq 0$ i varje punkt av $z_i(U_i \cap U_j)$). Låt U vara en öppen delmängd till M och $f : U \to \mathbb{C}$ en reguljär funktion på U (dvs för varje $i \in I$ om $U_i \cap U \neq \emptyset$ så är funktionen $f z_i^{-1}$ analytisk på $z_i(U_i \cap U)$ eller med andra ord $f = g(z_i)$, där $g = f z_i^{-1}$ är analytisk i $z_i(U_i \cap U)$).



Låt $P \in M$ och betrakta alla par (U, f), där U är en öppen omgivning till P och f är reguljär på U. Man säger att (U_1, f_1) och (U_2, f_2) är ekvivalenta om det finns $U \subseteq U_1 \cap U_2$, U en öppen omgivning till P, sådan att $f_1|U = f_2|U$. Ekvivalensklasser av den ekvivalensrelationen (kontrollera!) betecknas också (U, f). Visa att dessa ekvivalensklasser bildar en lokal ring om man definierar:

$$\begin{aligned}(U_1, f_1) + (U_2, f_2) &= (U_1 \cap U_2, f_1 + f_2),\\ (U_1, f_1)(U_2, f_2) &= (U_1 \cap U_2, f_1 f_2).\end{aligned}$$

Den ringen betecknas ofta $\mathcal{O}_{P,M}$ och kallas **den lokala ringen av punkten P på M** (eller **groddar av reguljära funktioner i P**). Beskriv maximalidealet i $\mathcal{O}_{P,M}$.

Anmärkning. Ringen $\mathcal{O}_{P,M}$ i fallet då $M = U$ ur (4.8) (c) behöver inte vara lika med $\mathcal{O}_{P,U}$ som definierades där.

4.15. Låt R vara en ring.

(a) Visa att man definierar en topologi på Spec$R$ genom att som slutna mängder förklarar

$$V(I) = \{\mathfrak{p} \in \text{Spec}R : \mathfrak{p} \supseteq I\}$$

för alla ideal I i R. Den kallas för **Zariskis topologi** på Spec$R$.

(b) Visa att om $f \in R$ så är

$$D(f) = \{\mathfrak{p} \in \text{Spec}R : f \notin \mathfrak{p}\}$$

en öppen mängd och att sådana mängder bildar en bas för Zariskis topologi.

4.16. Låt A vara en kommutativ K-algebra med etta och M en A-modul. Med **derivering** $D : A \to M$ (över K) menas en K-homomorfism sådan att $D(ab) = aD(b) + D(a)b$ för $a, b \in A$. För enkelhetens skull antag att $K \subseteq A$. Visa att:

(a) $D(x) = 0$ då $x \in K$,

(b) Alla K-deriveringar D bildar en A-modul $\text{Der}_K(A, M)$ då man definierar $(D_1 + D_2)(x) = D_1(x) + D_2(x)$ och $(aD)(x) = aD(x)$,

(c) Om K är en kropp, A är en lokal ring med maximalidealet $\mathfrak{m}$, och den naturliga sammansättningen $K \hookrightarrow A \to A/\mathfrak{m}$ är en isomorfism så är

$$\text{Der}_K(A, K) \cong \text{Hom}_A(\mathfrak{m}/\mathfrak{m}^2, K).$$

Ledning. (c) För $D : A \to K$ betrakta restriktionen av D till $\mathfrak{m}$ och visa att den avbildar $\mathfrak{m}^2$ på 0. Visa vidare att D inducerar en A-homomorfism

$$\mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m} = K.$$

Omvänt, om $\varphi : \mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m} = K$ är en A-homomorfism, definiera $D(a) = \varphi(\overline{a_1})$, där $a = a_1 + \lambda$, $a_1 \in \mathfrak{m}$ och $\lambda \in K$ (en framställning av a på formen $a_1 + \lambda$ existerar och är entydig).

Anmärkning. Låt M vara en analytisk mångfald och $P \in M$. Med tangentrummet till M i P menas $\text{Der}_{\mathbb{R}}(\mathcal{O}_{P,M}, \mathbb{R}) =: T_{P,M}$. (c) visar att $T_{P,M} \cong \text{Hom}_{\mathbb{R}}(\mathfrak{m}_P/\mathfrak{m}_P^2, \mathbb{R})$, där $\mathfrak{m}_P$ är maximalidealet i den lokala ringen $\mathcal{O}_{P,M}$ av P på M.

Kapitel 5

RINGUTVIDGNINGAR

Ett par bestående av en ring och dess delring kallas ringutvidgning. Oftast är man intresserad hur olika ringegenskaper beter sig vid övergången från den ena ringen till den andra. Vi diskuterar här utvigningar av tre typer: Ändliga, av ändlig typ och hela. De har stor betydelse i efterföljande kapitel då vi visar både deras aritmetiska och geometriska tillämpningar. Alla ringar i detta kapitel är kommutativa med etta. De skall betecknas här med A, B, C osv.

(5.1) Definition. Om A, B är ringar och $B \supseteq A$ så säger man att B är en **utvidgning** av A. Man säger att ringutvidgningen $B \supseteq A$ är **ändlig** om B är en ändligt genererad A-modul dvs $B = Ax_1 + \ldots + Ax_n$, där $x_i \in B$. Man säger att $B \supseteq A$ är av **ändlig typ** om B är en ändligt genererad A-algebra dvs $B = A[x_1, \ldots, x_n]$, där $x_i \in B$ (dvs varje element i B kan skrivas på formen $p(x_1, \ldots, x_n)$ där $p \in A[X_1, \ldots, X_n]$).

□

(5.2) Exempel. (a) $\mathbb{Z}[i] = \{a+bi,\ a, b \in \mathbb{Z}\}$ är en ändlig utvidgning av $\mathbb{Z}$ (med $x_1 = 1$, $x_2 = i$).

(b) Om $K \subseteq L$, där K, L är kroppar och L har en ändlig bas över K så är L en ändlig utvidgning av K ($L = Kx_1 + \ldots + Kx_n$ om $x_1, \ldots, x_n$ bildar en bas av L över K).

(c) Polynomringen $K[X_1, \ldots, X_n]$ är en utvidgning av ändlig typ över K (K en godtycklig kommutativ ring). Men den utvidgningen är inte ändlig (varför?).

(d) Polynomringen $K[X_1, \ldots, X_n, \ldots]$ i ett uppräkneligt antal variabler över K (K som ovan) är inte av ändlig typ över K (Övn. 1).

□

(5.3) Proposition. *Låt $C \supseteq B \supseteq A$ vara tre ringar. Om $B \supseteq A$ och $C \supseteq B$ är ändliga (av ändlig typ) så är också $C \supseteq A$ ändlig (av ändlig typ).*

Bevis. Om $B = \sum_{i=1}^{r} Ax_i$, $C = \sum_{j=1}^{s} By_j$ och $c \in C$ så är $c = \sum_j b_j y_j = \sum_j (\sum_i a_{ij} x_i) y_j$. Alltså är $C = \sum_{i,j} Ax_i y_j$ ändlig över A. Om $B = A[x_1, \ldots, x_r]$ och $C = B[y_1, \ldots, y_s]$ så är $C = A[x_1, \ldots, x_r, y_1, \ldots, y_s]$ dvs C är av ändlig typ över A. □

(5.4) Definition. Låt $B \supseteq A$. Man säger att $x \in B$ är ett **helt element** över A om x uppfyller en ekvation med koefficienter i A och med högsta koefficienten 1 dvs om

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, \quad \text{där} \quad a_i \in A.$$

Man säger att utvidgningen $B \supseteq A$ är **hel** om varje element $x \in B$ är helt över A.

□

(5.5) Exempel. (a) $\mathbb{Z}[i] \supset \mathbb{Z}$ är en hel utvidgning ty talet $x = a + bi$, $a, b \in \mathbb{Z}$ uppfyller ekvationen $x^2 - 2ax + (a^2 + b^2) = 0$.

(b) Utvidgningen $\mathbb{Q} \supseteq \mathbb{Z}$ är inte hel. Talet $1/2$ är inte helt över $\mathbb{Z}$ (visa det och se vidare (5.12)(c)).

(c) Om $L \supseteq K$ är en ändlig kroppsutvidgning dvs L har en ändlig dimension över K, säg $\dim_K L = n$, så är varje element $x \in L$ helt över K dvs $L \supseteq K$ är en hel utvidgning. I själva verket är $1, x, \ldots, x^n$ linjärt beroende över K (ty deras antal är $(n+1)$). Alltså finns det $a_0, a_1, \ldots, a_n \in K$ som inte alla är lika med 0 så att $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Samtidigt kan vi förutsätta att högsta koefficienten (framför högsta potensen av x med koefficient $\neq 0$) är lika med 1. I fall $L \supseteq K$ är en kroppsutvidgning säger man vanligen att $x \in L$ är **algebraiskt** över K (i stället för "helt") och man kallar utvidgningen $L \supseteq K$ **algebraisk** (i stället för "hel") om varje element i L är algebraiskt över K. Utvidgningen $\mathbb{R} \supset \mathbb{Q}$ är inte algebraisk. Talen e, π är exempel på icke-algebraiska element över $\mathbb{Q}$ (bevis är inte enkla). Om $L \supseteq K$ är en kroppsutvidgning och $x \in L$ inte är algebraiskt över K så kallar man x **transcendent** över K. Transcendenta element diskuterar vi i Kapitel 7.

□

(5.6) Proposition. *Låt $A \subseteq B$ vara en hel utvidgning, där A och B är integritetsområden. Då är A en kropp då och endast då B är en kropp.*

Bevis. "⇒" Låt A vara en kropp och $y \in B$, $y \neq 0$. Låt

$$y^n + a_{n-1}y^{n-1} + \ldots + a_0 = 0,\ a_i \in A$$

med minsta möjliga n. Då är $a_0 \neq 0$, ty om $a_0 = 0$, så har vi $y(y^{n-1}+a_{n-1}y^{n-2}+\ldots+a_1) = 0$ och $y \neq 0$ implicerar att y uppfyller en ekvation av grad $(n-1)$ (ty B saknar nolldelare). Alltså är $(-1/a_0)(y^{n-1} + a_{n-1}y^{n-2} + \ldots + a_1)$ inversen till y i B.

"$\Leftarrow$" Låt B vara en kropp och $x \in A$, $x \neq 0$. Då har vi $x^{-1} \in B$ (ty B är en kropp) och

$$(x^{-1})^m + a'_{m-1}(x^{-1})^{m-1} + \ldots + a'_0 = 0,\ a'_i \in A.$$

Genom att multiplicera ekvationen med x^{m-1} får vi $x^{-1} = -(a'_0x^{m-1} + \ldots + a'_{m-1}) \in A$. □

(5.7) Proposition. *Låt $A \subseteq C$ vara en ringutvidgning och $x \in C$. Då är följande villkor ekvivalenta:*

(*a*) *x är helt över A,*

(*b*) *$A[x] \supseteq A$ är en ändlig utvidgning,*

(*c*) *det finns en ändlig utvidgning $B \supseteq A$ sådan att $x \in B$ och $B \subseteq C$.*

Bevis. (a) $\Rightarrow$ (b) Låt $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, $a_i \in A$. $A[x]$ genereras av alla potenser x^k, $k = 0, 1, 2, \ldots$ Vi påstår att $A[x] = A + Ax + \ldots + Ax^{n-1}$ dvs att $1, x, \ldots, x^{n-1}$ räcker. Detta visas enkelt med induktion: $x^0 = 1 \in A[x]$. Antag att $x^k \in A[x]$ dvs

$$x^k = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}.$$

Då är

$$x^{k+1} = b_0x + b_1x^2 + \cdots + b_{n-1}x^n = b_0x + b_1x^2 + \ldots + b_{n-1}[-(a_0 + \cdots + a_{n-1}x^{n-1})] \in A[x].$$

(b) $\Rightarrow$ (c) Tag $B = A[x]$.

(c) $\Rightarrow$ (a) Låt $B = Ax_1 + \cdots + Ax_n$ och $x \in B$. Då är

$$\begin{cases} xx_1 = a_{11}x_1 + \ldots + a_{1n}x_n, \\ \cdots\cdots \\ xx_n = a_{n1}x_1 + \ldots + a_{nn}x_n, \end{cases}$$

dvs

$$\begin{cases} (a_{11}-x)x_1+\ldots+a_{1n}x_n=0, \\ \cdots\cdots \\ a_{n1}x_1+\ldots+(a_{nn}-x)x_n=0. \end{cases}$$

Låt $M=[a_{ij}]$ och låt E vara $(n\times n)$-enhetsmatrisen. Genom en vanlig elimination får vi att $[\det(M-xE)]x_i=0$ för $i=1,2,\ldots,n$. Alltså är $[\det(M-xE)]B=0$, vilket implicerar att $\det(M-xE)=0$ (välj $1\in B$!). Likheten $\det(M-xE)=0$ ger en ekvation av typen $x^n+a_{n-1}x^{n-1}+\ldots+a_0=0$ med $a_i\in A$ dvs x är helt över A. □

(5.8) Följdsats. *Om $B\supseteq A$ är en ändlig utvidgning så är den hel.*

Bevis. (c) ⇒ (a) i (5.7). □

Omvändningen av (5.8) gäller inte (se Övn. 3). Men vi har:

(5.9) Proposition. *Om $B=A[x_1,\ldots,x_n]$, där x_i är hela över A så är utvidgningen $B\supseteq A$ ändlig (och som konsekvens av (5.8) är den hel).*

Bevis. Induktion. Om $n=1$ så gäller påståendet enligt (5.7). Låt $n>1$ och $B'=A[x_1,\ldots,x_{n-1}]$. Då är $B=B'[x_n]$. Utvidgningarna $B\supseteq B'$ och $B'\supseteq A$ är hela ty $B\supseteq A$ är hel. Alltså är både $B\supseteq B'$ och $B'\supseteq A$ ändliga enligt fallet $n=1$ och induktionsantagandet. Nu följer ur (5.3) att även $B\supseteq A$ är ändlig. □

(5.10) Proposition. *Låt $A\subseteq C$ vara en ringutvidgning. Alla element i C som är hela över A bildar en ring.*

Bevis. Låt $x,y\in C$ vara hela över A. Då är $A[x,y]$ en hel utvidgning av A enligt (5.9). Alltså är $x\pm y$, $xy\in A[x,y]$ hela över A. □

(5.11) Definition. Ringen av alla hela element över A i en utvidgning $A\subseteq C$ kallas **hela höljet** till A i C. A kallas **helt sluten** i C om dess hela höljet i C är A. A kallas **helt sluten** om A är ett integritetsområde och A är helt sluten i sin kvotkropp.

□

(5.12) Exempel. (a) Låt $A=\mathbb{Q}$, $C=\mathbb{C}$. Hela höljet till $\mathbb{Q}$ i $\mathbb{C}$ består av alla algebraiska tal. De bildar en kropp $\overline{\mathbb{Q}}$ (se (5.6)!) som kallas kroppen av **de algebraiska talen**.

(b) Låt $A = \mathbb{Z}$, $C = \mathbb{C}$. Hela höljet till $\mathbb{Z}$ i $\mathbb{C}$ består av alla algebraiska heltal. De bildar en ring som kallas ringen av **de algebraiska heltalen**.

(c) Låt $A = \mathbb{Z}$, $C = \mathbb{Q}$. Ringen $\mathbb{Z}$ är helt sluten (dvs helt sluten i sin kvotkropp $\mathbb{Q}$). Det är nämligen så att ett rationellt tal är helt över $\mathbb{Z}$ då och endast då det är ett heltal. För att visa det låt $x = \frac{p}{q}$, där $p, q \in \mathbb{Z}$, $x = 0$ och $\mathrm{SDG}(p, q) = 1$. Om

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_0 = 0,\ a_i \in \mathbb{Z},$$

så är $p^n + a_{n-1}p^{n-1}q + \ldots + a_0 q^n = 0$, vilket implicerar att $q|p$. Villkoret $\mathrm{SGD}(p, q) = 1$ ger då $q = \pm 1$, vilket betyder att $x = \pm p \in \mathbb{Z}$. För en generalisering se Övn. 5 (samma bevis går igenom för varje ring med entydig primfaktoruppdelning – t ex varje PID och varje polynomring $K[X_1, \ldots, X_n]$, där K är en kropp).

(d) Hela höljet till $\mathbb{Z}$ i $\mathbb{Q}(i) = \{a + bi,\ a, b \in \mathbb{Q}\}$ är ringen av de Gaussiska heltalen $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$ – se Övn. 6.

□

(5.13) Anmärkning. En kropp K kallas **algebraiskt sluten** om varje icke-konstant polynom med koefficienter i K har minst ett nollställe i K (och som konsekvens kan uppdelas i produkt av förstagradsfaktorer i $K[X]$). Exempel på sådana kroppar är $\mathbb{C}$ och $\overline{\mathbb{Q}}$ (se Övn. 4). Lägg märke till att en kropp alltid är helt sluten i enlighet med definitionen (5.11) (ty kvotkroppen av en kropp är samma kropp). Man kan säga att en kropp är algebraiskt sluten om det inte finns icke-triviala algebraiska (= hela) utvidgningar av den. Låt oss notera att varje kropp kan inbäddas i en algebraiskt sluten kropp varvid för varje kropp K existerar en kropp $\overline{K}$ sådan att $\overline{K}$ är algebraiskt sluten och algebraiskt över K. Om $\overline{K}$ och $\overline{K}'$ är två sådana kroppar så existerar en K-isomorfism $f : \overline{K} \to \overline{K}'$ (dvs en isomorfism av kroppar sådan att $f(x) = x$ då $x \in K$). Vi kommer inte att bevisa dessa påståenden (se t ex Langs book "Algebra", chap. VII, §2).

□

Vi kan komplettera (5.3) med en parallell egenskap hos hela utvidgningar:

(5.14) Proposition. *Låt $C \supseteq B \supseteq A$ vara tre ringar. Om $C \supseteq B$ och $B \supseteq A$ är hela så är också utvidgningen $C \supseteq A$ hel.*

Bevis. Låt $x \in C$. Då är

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0, \quad \text{där} \quad b_i \in B.$$

Låt $B' = A[b_0, \ldots, b_{n-1}]$. Utvidgningarna $B' \supseteq A$ och $B'[x] \supseteq B'$ är ändliga enligt (5.9). Alltså är $B'[x] \supseteq A$ ändlig enligt (5.3) och således hel enligt (5.8). Men $x \in B'[x]$, vilket betyder att x är helt över A. □

(5.15) Följdsats. *Låt $A \subseteq C$. Om B är hela höljet till A i C så är B helt sluten i C.*

Bevis. B är ringen av alla hela element över A i C. Om $x \in C$ och är helt över B så har vi $A \subseteq B \subseteq B[x]$, där $A \subseteq B$ och $B \subseteq B[x]$ är hela. Alltså är $A \subseteq B[x]$ hel så att x är helt över A. Detta betyder att $x \in B$. □

Vi skall avsluta detta kapitel med ett resultat som säger vad som händer med olika typer av utvidgningar vid homomorfismer och lokaliseringar:

(5.16) Proposition. *Låt $B \supseteq A$ vara en ringutvidgning.*

(*a*) *Om $\varphi : B \to B'$ är en surjektion av ringar och $A' = \varphi(A)$ så är $B' \supseteq A'$ ändlig* (*av ändlig typ, hel*) *om $B \supseteq A$ är ändlig* (*av ändlig typ, hel*).

(*b*) *Om S är en multiplikativ mängd i A så är $B_S \supseteq A_S$ ändlig* (*av ändlig typ, hel*) *om $B \supseteq A$ är ändlig* (*av ändlig typ, hel*).

Bevis. (a) Om $B = Ax_1 + \ldots + Ax_n$ så är $B' = A'\varphi(x_1) + \ldots + A'\varphi(x_n)$. Om $B = A[x_1, \ldots, x_n]$ så är $B' = A'[\varphi(x_1), \ldots, \varphi(x_n)]$. Om $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ så är $\varphi(x)^n + \varphi(a_{n-1})\varphi(x)^{n-1} + \ldots + \varphi(a_0) = 0$, vilket visar att $\varphi(x)$ är helt över A'.

(b) Om $B = Ax_1 + \ldots + Ax_n$ så är $B_S = A_S\frac{x_1}{1} + \ldots A_S\frac{x_n}{1}$. Om $B = A[x_1, \ldots, x_n]$ så är $B_S = A_S[\frac{x_1}{1}, \ldots, \frac{x_n}{1}]$. Om $\frac{x}{s} \in B_S$, där $x \in B$ och $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, så är $(\frac{x}{s})^n + \frac{a_{n-1}}{s}(\frac{x}{s})^{n-1} + \ldots + \frac{a_0}{s^n} = 0$, vilket visar att $\frac{x}{s}$ är helt över A_S. □

ÖVNINGAR

5.1. Vilka av följande ringutvidgningar är av ändlig typ, ändliga, hela?

(a) $\mathbb{Q} \supset \mathbb{Z}$; (b) $\mathbb{Z}[\frac{1}{2}] \supset \mathbb{Z}$; (c) $\mathbb{Z}_{(2)} \supset \mathbb{Z}$;

(d) $\mathbb{R}[x, y] \supset \mathbb{R}[x]$, där $x^2 + y^2 = 1$ och x är variabeln;

(e) $\mathbb{R}[X_1, \ldots, X_n, \ldots] \supset \mathbb{R}$ (antalet variabler är uppräkneligt).

5.2. Låt $A \subseteq B$ vara en hel utvidgning och $x \in A$ ett inverterbart element i B. Visa att $x^{-1} \in A$.

5.3. Ge ett exempel på en hel utvidgning $B \supseteq A$ som inte är ändlig.

5.4. Låt $\overline{\mathbb{Q}}$ beteckna de algebraiska talen (dvs alla algebraiska element i $\mathbb{C}$ över $\mathbb{Q}$). Visa att $\overline{\mathbb{Q}}$ är en algebraiskt sluten kropp. Generalisera till ett påstående som gäller i det fall då K är en kropp och L är en algebraiskt sluten kropp som innehåller K.

5.5. Låt A vara ett integritesområde. Man säger att A har **entydig faktoruppdelning** (A är UFD[†]) om varje icke–inverterbart nollskilt element $a \in A$ kan entydigt skrivas som produkt av irreducibla element i följande mening: Om

$$a = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s,$$

där p_i, q_j är irreducibla element, så är $r = s$ och $Ap_i = Aq_i$ vid lämplig numrering av faktorerna (ett element $p \in A$ kallas **irreducibelt** om likheten $p = ab$, där $a, b \in A$ implicerar att exakt en av faktorerna a, b är inverterbart i A). Visa att om A är UFD så är A helt sluten (se (5.11)).

5.6. Låt $L \supseteq \mathbb{Q}$ vara en ändligt kroppsutvidgning. Hela höljet till $\mathbb{Z}$ i L (dvs alla tal i L hela över $\mathbb{Z}$) kallas ringen av **algebraiska heltalen i** L. Låt $L = \mathbb{Q}(\sqrt{d})$, där d är kvadratfritt och $d \neq 1$. Visa att de algebraiska heltalen i L är alla tal $a + b\omega$, $a, b \in \mathbb{Z}$, där $\omega = \sqrt{d}$ om $d \equiv 2$ eller $3 \pmod 4$ och $\omega = \frac{1+\sqrt{d}}{2}$ då $d \equiv 1 \pmod 4$ (t ex är alla heltal i $\mathbb{Q}(i)$ av formen $a + bi$, $a, b \in \mathbb{Z}$, ty $d = -1 \equiv 3 \pmod 4$).

5.7. En homomorfsim av ringar $f : A \to B$ kallas ändlig (av ändlig typ, hel) om utvidgningen $f(A) \subseteq B$ är ändlig (av ändlig typ, hel). Visa att sammansättningen av två ändliga homomorfismer är en ändlig homomorfism. Visa samma påstående för homomorfismer av ändlig typ och för hela homomorfismer.

5.8. Låt $L \supseteq K$ vara en kroppsutvidgning och $x \in L$ ett algebraiskt element över K. Med ett **minimalpolynom** för x över K menas ett polynom $p(X) \in K[X]$ med högsta koefficienten 1 vars grad är den lägsta bland graderna av alla polynom som har x som ett nollställe. Visa att:

(a) $p(X)$ är entydigt bestämt och irreducibelt i $K[X]$,

(b) $K[x] = K + Kx + \ldots + Kx^{n-1}$, där $n = \text{grad}p(X)$ och $\dim_K K[x] = n$.

Ledning. Visa att $K[x] \cong K[X]/(p(X))$. Observera att $K[x] = K(x)$ är den minsta delkropp till L som innehåller K och x.

[†]Från "unique factorization domain

5.9. Låt $M \supseteq L \supseteq K$ vara kroppsutvidgningar. Visa att $\dim_K M = (\dim_L M)(\dim_K L)$ (ofta skriver man $\dim_K M = [M : K]$ osv).

5.10. Låt $B \supseteq A$ vara en ringutvidgning och $x \in B$. Visa att om det finns en A-modul M sådan att M är ändligt genererad över A, $\mathrm{Ann}(M) = (0)$ (se Övn. 3.4) och $xM \subseteq M$ så är x helt över A.

5.11. Låt S vara en multiplikativ mängd i en helt sluten ring A. Visa att även lokaliseringen A_S är helt sluten.

Kapitel 6

NOETHERSKA RINGAR OCH MODULER

Med en noethersk ring menar man en ring i vilken varje ideal kan genereras av ändligt många element. Bland dessa ringar finns både restklassringar av polynomringar viktiga i algebraisk geometri och ringar av heltal i algebraiska talkroppar viktiga i talteori. Noetherska ringar hade studerats långt innan deras formella definition tillkom i ett mycket inflytelserikt arbete av Emmy Noether från 1921. E. Noether visade hur ringegenskaper kunde användas för att härleda geometriska egenskaper hos algebraiska mångfalder. På det sättet öppnade hon vägen till en mycket produktiv inriktning inom algebran som förbinder ringteori med algebraisk geometri.

Låt R vara en ring med etta och låt M vara en vänster R-modul.

(6.1) Definition. Man säger att M är en **noethersk** R-modul om varje delmodul till M är ändligt genererad.

□

Innan vi ger exempel på noetherska moduler visar vi några ekvivalenta egenskaper som karakteriserar sådana moduler.

(6.2) Proposition. *Om M är en vänster R-modul så är följande villkor ekvivalenta:*

(a) *M är noethersk,*

(b) *varje växande kedja*

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M_k \subseteq \ldots$$

av delmoduler till M är stationär dvs det finns ett index n så att $M_n = M_{n+1} = \ldots$,

(c) varje icke-tom familj av delmoduler till M innehåller ett maximalt element med avseende på inklusion.

Bevis. (a) $\Rightarrow$ (b) Låt $\bigcup_{i=1}^{\infty} M_i$ vara unionen av alla moduler $M_1 \subseteq M_2 \subseteq \ldots \subseteq M_k \subseteq \ldots$. Unionen är en delmodul till M så att

$$\bigcup_{i=1}^{\infty} M_i = (m_1, \ldots, m_k),$$

där $m_j \in M$. Varje m_j tillhör någon av modulerna i kedjan så att det finns ett index n sådant att alla m_j tillhör M_n. Då är $\bigcup_{i=1}^{\infty} M_i = M_n$, vilket ger $M_n = M_{n+1} = \ldots$.

(b) $\Rightarrow$ (c) Låt $\mathcal{S}$ vara en icke-tom familj av delmoduler till M. Antag att $\mathcal{S}$ inte innehåller något maximalt element med avseende på inklusion. Välj en godtycklig modul $M_1 \in \mathcal{S}$. M_1 är inte maximalt i $\mathcal{S}$ så att det finns $M_2 \in \mathcal{S}$ med $M_1 \subset M_2$. M_2 är inte maximalt i $\mathcal{S}$ så vi kan välja $M_3 \in \mathcal{S}$ med $M_1 \subset M_2 \subset M_3$ osv. På så sätt kan vi konstruera en oändlig icke-stationär kedja av delmoduler till M vilket strider mot (b).

(c) $\Rightarrow$ (a) Låt N vara en delmodul till M och låt $\mathcal{S}$ vara familjen av alla ändligt genererade delmoduler till N. Låt $(n_1, \ldots, n_k) \subseteq N$ vara ett maximalt element i $\mathcal{S}$. Om $(n_1, \ldots, n_k) \neq N$ så existerar $n \in N \setminus (n_1, \ldots, n_k)$. Men då är $(n_1, \ldots, n_k, n)$ en delmodul till N tillhörande $\mathcal{S}$ som är större än $(n_1, \ldots, n_k)$. Detta strider mot valet av $(n_1, \ldots, n_k)$ i $\mathcal{S}$ och ger en motsägelse. Alltså är $N = (n_1, \ldots, n_k)$ ändligt genererad vilket visar att M är noethersk. $\square$

Vårt nästa resultat är ofta mycket användbart:

(6.3) Proposition. *Låt N vara en delmodul till en R-modul M. M är noethersk då och endast då N och M/N är noetherska.*

Bevis. "$\Rightarrow$" Varje delmodul till N är ändligt genererad som en delmodul till M. Varje delmodul till M/N är ändligt genererad ty dess urbild vid den naturliga surjektionen $M \to M/N$ är en delmodul till M och som sådan är den ändligt genererad (varje delmodul till M/N är bilden av sin urbild i M vid den naturliga surjektionen så att den genereras av bilderna av urbildens generatorer).

"$\Leftarrow$" Först visar vi att om $L \subseteq L'$ är två delmoduler till M sådana att

$$N \cap L = N \cap L' \quad \text{och} \quad N + L = N + L'$$

så är $L = L'$. Tag $l' \in L'$. Då är $l' = n + l$, där $l \in L$ och $n \in N$. Alltså är $l' - l = n \in N \cap L' = N \cap L \subseteq L$ så att $l' \in L$. Detta visar att $L' \subseteq L$. Enligt förutsättningen är $L \subseteq L'$ så att $L' = L$.

Låt nu

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M_k \subseteq \ldots$$

vara en växande kedja av delmoduler till M. Kedjorna

$$N \cap M_1 \subseteq N \cap M_2 \subseteq \ldots \subseteq N \cap M_k \subseteq \ldots$$

och

$$(N + M_1)/N \subseteq (N + M_2)/N \subseteq \ldots \subseteq (N + M_k)/N \subseteq \ldots$$

är stationära ty N och M/N är noetherska. Alltså existerar ett index n sådant att

$$N \cap M_n = N \cap M_{n+1} = \ldots \quad \text{och} \quad (N + M_n)/N = (N + M_{n+1})/N = \ldots$$

dvs

$$N + M_n = N + M_{n+1} = \ldots$$

Men enligt vår observation i början av beviset betyder dessa likheter att $M_n = M_{n+1} = \ldots$ så att M också är noethersk. □

(6.4) Anmärkning. Proposition (6.3) kan också formuleras så att i en exakt sekvens av R-moduler

$$0 \to M' \to M \to M'' \to 0$$

är M noethersk då och endast då M' och M'' är noetherska.

□

(6.5) Följdsats. *Om M_i, $i = 1, \ldots, n$, är noetherska R-moduler så är även $M_1 \oplus \ldots \oplus M_n$ en noethersk R-modul.*

Bevis. Om $M = M_1 \oplus M_2$ så innehåller M en noethersk delmodul $N = M_1$ sådan att $M/N \cong M_2$ också är noethersk. Alltså är M noethersk enligt (6.3) (eller (6.4)). En enkel induktion visar nu resultatet då $n > 2$. □

Nu kan vi definiera noetherska ringar och ge exempel på noetherska moduler:

(6.6) Definition. Man säger att en ring R är **vänsternoethersk** om R är noethersk som vänster R-modul.

□

Definitionen säger att R är noethersk om varje vänsterideal i R är ändligt genererat.

(6.7) Anmärkning. Det finns exempel som visar att en ring kan vara vänsternoethersk utan att vara högernoethersk. Våra intressen kommer dock att koncentreras till kommutativa noetherska ringar då det inte finns en distinktion mellan dessa begrepp.

□

(6.8) Proposition. *Om $f : R \to R'$ är en surjektiv ringhomomorfism och R är noethersk så är R' noethersk.*

Bevis. $R' \cong R/\mathrm{Ker}f$ kan betraktas som en kvotmodul av R-modulen R. Alltså följer påståendet ur (6.3). □

(6.9) Exempel. (a) Varje huvudidealring är noethersk.

(b) Vi visar snart Hilberts bassats som säger att polynomringarna $K[X_1, \ldots, X_n]$, där K är en kropp (eller mera allmänt en godtycklig noethersk ring) är noetherska (se (6.11)). Detta i kombination med (6.1) ger att varje restklassring $K[X_1, \ldots, X_n]/I$ modulo ett ideal I i $K[X_1, \ldots, X_n]$ är noethersk.

□

Exempel på noetherska moduler följer lätt ur följande resultat:

(6.10) Proposition. *Om R är en noethersk och M är en ändligt genererad R-modul så är M noethersk.*

Bevis. Om $M = Rm_1 + \ldots + Rm_n$ så existerar en surjektion $f : R^n \to M$ sådan att $f((r_1, \ldots, r_n)) = r_1m_1 + \ldots + r_nm_n$. Alltså är M isomorf med en kvotmodul av R^n. Detta visar att M är noethersk enligt (6.3) ty R^n är noethersk enligt (6.5). □

Vårt nästa resultat är en mycket berömd sats som visades 1890 av D. Hilbert:

(6.11) Hilberts bassats. *Om R är en kommutativ noethersk ring så är också polynomringen $R[X]$ noethersk.*

Bevis. Antag att $R[X]$ inte är noethersk och låt $\mathfrak{I}$ vara ett ideal i $R[X]$ som inte är ändligt genererat. Välj ett nollskilt polynom $p_1 \in \mathfrak{I}$ av minsta möjliga grad och konstruera en

sekvens av polynom $p_1, p_2, \ldots p_k, \ldots$ så att $p_{k+1} \in \mathfrak{I}$ och p_{k+1} har minsta möjliga grad bland alla polynom i $\mathfrak{I}$ som inte tillhör $\mathfrak{I}_k = (p_1, \ldots, p_k)$ för $k = 1, 2, \ldots$. Låt a_k vara högsta koefficienten i p_k och betrakta idealkedjan i R:

$$(a_1) \subseteq (a_1, a_2) \subseteq \ldots \subseteq (a_1, a_2, \ldots, a_k) \subseteq \ldots.$$

Enligt förutsättningen existerar n så att $(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n, a_{n+1}) = \ldots$, vilket visar att $a_{n+1} = r_1 a_1 + \ldots + r_n a_n$, där $r_i \in R$. Låt $\operatorname{grad}(p_k) = d_k$. Observera att $d_1 \leq \ldots \leq d_k \leq \ldots$. Betrakta polynomet

$$p = p_{n+1} - r_1 X^{d_{n+1}-d_1} p_1 - \ldots - r_n X^{d_{n+1}-d_n} p_n.$$

Det är klart att $p \in \mathfrak{I}$ och $p \notin \mathfrak{I}_n$ (ty $p_{n+1} \notin \mathfrak{I}_n$ och $p_k \in \mathfrak{I}_n$ då $1 \leq k \leq n$). Men p är inte nollpolynomet och graden av p är lägre än graden av p_{n+1}, vilket ger en motsägelse. Detta visar att en icke-stationär växande idealkedja i $R[X]$ inte kan existera dvs $R[X]$ är noethersk. □

(6.12) Följdsats. *Om $R \subseteq S$ är en ringutvidgning av ändlig typ och R är noethersk så är också S noethersk. I synnerhet är polynomringen $R[X_1, \ldots, X_n]$ noethersk.*

Bevis. Förutsättningen säger att $S = R[x_1, \ldots, x_n]$ är isomorf med restklassringen av polynomringen $R[X_1, \ldots, X_n]$ (vid den surjektiva homomorfism som avbildar X_i på x_i). Med utgångspunkt från Hilberts bassats ger en enkel induktion att $R[X_1, \ldots, X_n]$ är noethersk. Alltså är också $R[x_1, \ldots, x_n]$ noethersk enligt (6.8). □

ÖVNINGAR

6.1. Vilka av följande ringar är noetherska:

(a) Polynomringen $K[X_1, X_2, \ldots, X_n, \ldots]$ i variablerna $X_1, X_2, \ldots, X_n \ldots$.

(b) Ringen av alla hela analytiska funktioner $\mathcal{A}(\mathbb{C})$.

(c) Ringen av alla potensserier $a_0 + a_1 z + a_2 z^2 + \ldots$ med konvergensradie > 0, $a_i \in \mathbb{C}$.

(d) Produkten $\prod_{i \in I} R_i$, där R_i är noetherska ringar.

6.2. Är det sant att

(a) om $R[X]$ är en noethersk ring så är R noethersk?

(b) om $R_{\mathfrak{p}}$ är noethersk för varje $\mathfrak{p} \in \mathrm{Spec} R$ så är R noethersk?

6.3. Visa att om R är noethersk och S är en multiplikativ delmängd till R så är också R_S noethersk (se (4.3)).

6.4. Visa att om R är en kommutativ noethersk ring så är potensserieringen $R[[X]]$ också noethersk.

Ledning. Låt $\mathfrak{I}$ vara ett ideal i $R[X]$. Betrakta idealkedjan i R:

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_k \subseteq \ldots,$$

där I_k genereras av koefficienterna för X^k i alla potensserier $a_k X^k + a_{k+1} X^{k+1} + \ldots$ tillhörande $\mathfrak{I}$. Välj n så att $I_n = I_{n+1} = \ldots$ och låt $p_{ki} = a_{ki} X^k + \ldots$ vara alla potensserier vars koefficienter a_{ki} genererar I_k för $k = 1, \ldots, n$. Visa att p_{ki} genererar $\mathfrak{I}$.

6.5. Låt $\mathcal{N}(R)$ vara nilradikalen (se (4.23)) av en noethersk ring R. Visa att det finns $n > 0$ sådant att $\mathcal{N}(R)^n = (0)$. Visa att förutsättningen att R är noethersk är väsentlig.

6.6. Ett primideal i en ring kallas minimalt om det inte innehåller något annat primideal (t ex (0) i ett integritetsomrdåde).

(a) Visa att varje primideal i en godtycklig ring innehåller ett minimalt primideal.

(b) Visa att antalet minimala primideal i en noethersk ring är ändligt.

(c) Visa att radikalen av ett godtyckligt ideal i en noethersk ring är snittet av ett ändligt antal primideal (se Övn. 2.21).

(d) Ge exempel på en ring med oändligt många minimala primideal.

6.7. Ge exempel på en icke-noethersk lokal ring med endast ett primideal.

6.8. (a) Låt R vara en ring och $r \in R$. Låt $I = (x_1, \ldots, x_n)$ vara ett ideal i R och låt m vara ett heltal ≥ 1. Visa att $r \in I^m$ då och endast då det finns ett homogent polynom $F_m \in R[X_1, \ldots, X_n]$ av grad m sådant att $r = F_m(x_1, \ldots, x_n)$.

(b)* Bevisa **Krulls Sats**: Om R är noethersk och I är ett ideal i R så gäller det att

$$a \in \bigcap_{m=1}^{\infty} I^m \Leftrightarrow a \in aI.$$

(c) Härled ur (b): Om R är noethersk och lokal med maximalidealet $\mathfrak{m}$ så är

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0).$$

(d) Härled ur (b): Om R är ett noetherskt integritetsområde och I är ett ideal i R så är

$$\bigcap_{n=1}^{\infty} I^n = (0).$$

6.9. Man säger att R är en **Artinring** om varje avtagande kedja

$$I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots$$

av ideal i R är stationär dvs det finns n_0 sådant att för $n \geq n_0$ är $I_n = I_{n+1} = \ldots$. Låt R vara en Artinring. Visa att

(a) varje primideal i R är maximalt och antalet maximalideal är ändligt,

(b) det finns $r > 0$ så att $\mathcal{N}(R)^r = (0)$ ($\mathcal{N}(R)$ = nilradikalen = Jacobson-radikalen av R),

(c)* R är en Artinring då och endast då R är noethersk och varje primideal i R är maximalt.

Ledning. (a) Låt $\mathfrak{p}$ vara ett primideal i R. Betrakta $R/\mathfrak{p}$ som också är en Artinring och visa att $R/\mathfrak{p}$ är en kropp (tag $x \in R/\mathfrak{p}$, $x \neq 0$ och betrakta kedjan $(x) \supseteq (x^2) \supseteq \ldots$).

(b) Betrakta kedjan $N \supseteq N^2 \supseteq \ldots$, där $N = \mathcal{N}(R)$. Låt $N^r = N^{r+1} = \ldots$. Tag $M = N^r$ i Nakayamas Lemma!

(c) "⇒" Enligt (b) är $(0) = \mathfrak{n}_1 \ldots \mathfrak{n}_k$, där $\mathfrak{n}_i$ är maximalideal i R, ty $\mathcal{N}(R) = \bigcap \mathfrak{m}_i \supseteq \mathfrak{m}_1 \ldots \mathfrak{m}_k$, där $\mathfrak{m}_i$ är alla maximalideal i R (observera att faktorerna $\mathfrak{n}_i$ behöver inte vara olika). Betrakta kedjan $R \supset \mathfrak{n}_1 \supseteq \mathfrak{n}_1\mathfrak{n}_2 \supseteq \ldots \supseteq \mathfrak{n}_1 \ldots \mathfrak{n}_k = (0)$ och utnyttja det faktum att $(\mathfrak{n}_1 \ldots \mathfrak{n}_i)/(\mathfrak{n}_1 \ldots \mathfrak{n}_i\mathfrak{n}_{i+1})$ är ett vektorrum över kroppen $R/\mathfrak{n}_{i+1}$. Utnyttja (6.3).

"⇐" Betrakta $\mathcal{N}(R) = \bigcap \mathfrak{m}_i$, $\mathfrak{m}_i$ maximala enligt förutsättningen och Övn. 6 (c). Utnyttja därefter Övn. 5 och betrakta samma kedja av ideal som i beviset av "⇒".

Kapitel 7

DIMENSION AV RINGAR

Alla ringar i detta kapitel är kommutativa med etta.

(7.1) Exempel.

$$\begin{aligned} V_0 &= \{(x,y,x) \in \mathbb{C}^3 : x^2+y^2=1\}, \\ V_1 &= \{(x,y,z) \in \mathbb{C}^3 : x^2+y^2=1 \quad \text{och} \quad x=1\} \\ V_2 &= \{(x,y,z) \in \mathbb{C}^3 : x^2+y^2=1,\, x=1 \quad \text{och} \quad z=0\} \end{aligned}$$

är tre algebraiska mängder i $\mathbb{C}^3$: en cylinder, dess

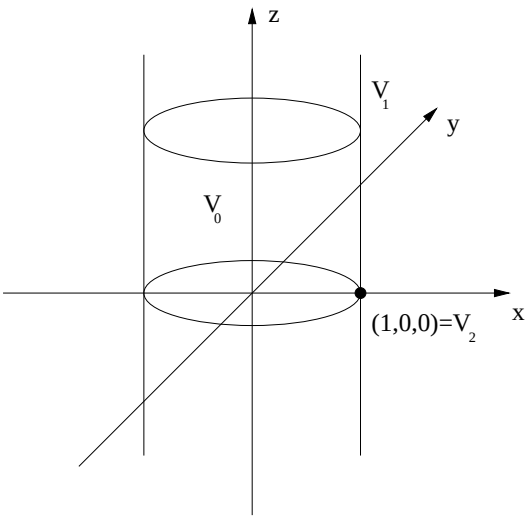


Figure 7.1:

generatris och en punkt på den (se Fig. 7.1 där vi ritar $V_i \cap \mathbb{R}^3$).

Intuitivt har de dimensionerna: 2,1,0. V_0 är mängden av alla nollställen till idealet $\mathfrak{p}_0 = (X^2+Y^2-1)$ i $\mathbb{C}[X,Y,Z]$, V_1 till idealet $\mathfrak{p}_1 = (X-1,Y)$, och V_2 till idealet $\mathfrak{p}_2 = (X-1,Y,Z)$ (se Övn. 2.21). Dessa ideal är primideal och $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$. Vi skall visa senare att

$$\mathcal{I}(V_0) = \{p \in \mathbb{C}[X,Y,Z] : \forall_{v\in V_0} p(v) = 0\} = (X^2+Y^2-1) = \mathfrak{p}_0.$$

Alltså är ringen av de regulära funktionerna på V_0:

$$\mathbb{C}[V_0] = \mathbb{C}[X,Y,Z]/\mathcal{I}(V_0) = \mathbb{C}[x,y,z],$$

där x,y,z är restklasser av X,Y,Z och $x^2+y^2=1$. Kedjan $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$ ger i $\mathbb{C}[x,y,z]$ kedjan $(0) = \bar{\mathfrak{p}}_0 \subset \bar{\mathfrak{p}}_1 \subset \bar{\mathfrak{p}}_2$. Vi visar senare att det inte finns längre kedjor av primideal i $\mathbb{C}[V_0]$, vilket svarar just mot den intuitiva föreställningen om dimensionen av en cylinder som tillåter exakt två typer av irreducibla algebraiska delmängder av lägre dimension (dessa svarar mot två primideal som tillsammans med nollidealet bildar en maximal kedja av primideal i $\mathbb{C}[V_0]$). □

I detta kapitel skall vi precisera alla påståenden i Exempel (7.1).

(7.2) Definition. Låt R vara en ring. Med **Krulldimensionen**[†] (eller kortare **dimensionen**) $\dim R$ av R menar man maximum av sådana k att det finns en kedja

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k$$

av primideal i R. Man säger att k är längden av kedjan.

□

(7.3) Exempel. (a) Om K är en kropp så är $\dim K = 0$. Omvänt, om K är ett integritetsområde och $\dim K = 0$, så är K en kropp, ty (0) är ett maximalideal då.

(b) $\dim \mathbb{Z} = 1$, ty $(0) \subset (p)$, där p är ett primtal, är en kedja av primideal och det finns inte längre kedjor av den typen. På samma sätt är $\dim K[X] = 1$, då K är en kropp. Mera allmänt om R är ett huvudidealområde (PID) som inte är en kropp, så är $\dim R = 1$. I själva verket är (0) ett primideal och om $\mathfrak{p} = (p) \neq (0)$ är ett primideal så är $\mathfrak{p}$ maximalt (se Övn. 2.11). Alltså har varje maximal kedja av primideal i R längden 1.

(c) $\dim \mathbb{Z}[i] = 1$ enligt (b), ty $\mathbb{Z}[i]$ är PID. Men detta påstående är ett specialfall av likheten $\dim \mathbb{Z}[\sqrt{d}] = 1$, d ett heltal, som följer ur (7.4). Vi visar där att om $R' \subseteq R$ är en hel utvidgning så är $\dim R' = \dim R$ (här är $R' = \mathbb{Z}[\sqrt{d}]$, $R = \mathbb{Z}$).

(d) Vi skall visa senare att $\dim K[x,y] = 1$ om $p(x,y) = 0$, där $p(X,Y)$ är ett irreducibelt polynom, vilket svarar mot den intuitiva uppfattningen om dimensionen av en algebraisk kurva (ekvationen $p(X,Y) = 0$ beskriver en sådan i $\bar{K}^2$ och $K[x,y]$ är ringen av de regulära

[†]Efter Wolfgang Krull (1899-1970).

funktionerna på den). Vi skall också visa att $\dim \mathbb{C}[x,y,z] = 2$, där $x^2 + y^2 = 1$ (se Exempel (7.24)) – den likheten säger att en cylinder har dimensionen 2.

(e) I (7.9) visar vi att $\dim K[X_1, \ldots, X_n] = n$ ($K[X_1, \ldots, X_n]$ är ringen av de regulära funktionerna på den algebraiska mängden $\bar{K}^n$ så att resultatet bekräftar den geometriska intuitionen).

□

(7.4) Sats. *Om $R' \supseteq R$ är en hel utvidgning så är $\dim R' = \dim R$. Mera exakt: Om $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_n$ är en kedja av primideal i R' så är $\mathfrak{p}'_0 \cap R \subset \mathfrak{p}'_1 \cap R \subset \ldots \subset \mathfrak{p}'_n \cap R$ en kedja av primideal i R och för varje kedja $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ av primideal i R existerar en kedja $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_n$ av primideal i R' sådan att $\mathfrak{p}_i = \mathfrak{p}'_i \cap R$ för $i = 1, 2, \ldots, n$.*

Bevis för den satsen kommer att följa ur några hjälpresultat:

(7.5) Proposition. *Låt $R' \supseteq R$ vara en hel utvidgning. Låt $\mathfrak{p}' \subset R'$ och $\mathfrak{p} \subset R$ vara primideal sådana att $\mathfrak{p} = R \cap \mathfrak{p}'$. Då är $\mathfrak{p}$ maximalt då och endast då $\mathfrak{p}'$ är maximalt.*

Bevis. Betrakta den naturliga surjektionen $R' \to R'/\mathfrak{p}'$. Bilden av R är $R/(\mathfrak{p}' \cap R) = R/\mathfrak{p}$. Utvidgningen $R/\mathfrak{p} \subseteq R'/\mathfrak{p}'$ är hel (se (5.16)(a)) så att $R/\mathfrak{p}$ är en kropp då och endast då $R'/\mathfrak{p}'$ är en kropp (se (5.6)) dvs $\mathfrak{p}$ är ett maximalideal då och endast då $\mathfrak{p}'$ är sådant. □

(7.6) Proposition. *Låt $R' \supseteq R$ vara en hel utvidgning och $\mathfrak{p}'_1 \subseteq \mathfrak{p}'_2$ två primideal i R'. Om $\mathfrak{p}'_1 \cap R = \mathfrak{p}'_2 \cap R =: \mathfrak{p}$ så är $\mathfrak{p}'_1 = \mathfrak{p}'_2$.*

Bevis. Betrakta den multiplikativa mängden $S = R \setminus \mathfrak{p}$ (notera att $\mathfrak{p}$ är ett primideal i R!) och lokaliseringarna $R_S \subseteq R'_S$. Idealen $(\mathfrak{p}'_1)_S$ och $(\mathfrak{p}'_2)_S$ är äkta primideal i R'_S ty $S \cap \mathfrak{p}'_1 = S \cap \mathfrak{p}'_2 = \emptyset$ (se (4.17)). Alltså är $(\mathfrak{p}'_1)_S \cap R_S = (\mathfrak{p}'_2)_S \cap R_S = \mathfrak{p}_S$, ty $(\mathfrak{p}'_i)_S \cap R_S \supseteq \mathfrak{p}_S$ och $\mathfrak{p}_S$ är maximalidealet i den lokala ringen R_S ($= R_\mathfrak{p}$) (se (4.8)(b)). Eftersom utvidgningen $R_S \subseteq R'_S$ är hel (se (5.16)(b)), får vi enligt (7.5) att $(\mathfrak{p}'_1)_S$ och $(\mathfrak{p}'_2)_S$ är maximalideal i R'_S. Alltså implicerar inklusionen $\mathfrak{p}'_1 \subseteq \mathfrak{p}'_2$ att $(\mathfrak{p}'_1)_S = (\mathfrak{p}'_2)_S$. Detta ger $\mathfrak{p}'_1 = \mathfrak{p}'_2$ enligt (4.17). □

(7.7) Proposition. *Låt $R' \supseteq R$ vara en hel utvidgning.*

(a) Om $\mathfrak{p}$ är ett primideal i R så existerar ett primideal $\mathfrak{p}'$ i R' sådant att $\mathfrak{p}' \cap R = \mathfrak{p}$.

(b) Om $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ är primideal i R så existerar en kedja $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_n$ av primideal i R' sådan att $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$ för $i = 1, 2, \ldots, n$.

Bevis. (a) Låt $S = R \setminus \mathfrak{p}$. Betrakta det kommutativa diagrammet:

$$\begin{array}{ccc} R & \xrightarrow{i} & R' \\ {\scriptstyle f_S}\downarrow & & \downarrow{\scriptstyle f'_S} \\ R_S & \xrightarrow[i_S]{} & R'_S \end{array}$$

där i, i_S är inbäddningarna och f_S, f'_S de naturliga homomorfismerna ($r \mapsto \frac{r}{1}$, $r' \mapsto \frac{r'}{1}$). Låt $\mathfrak{m}'$ vara ett maximalideal i R'_S. Då är $\mathfrak{m} = R_S \cap \mathfrak{m}'$ maximalidealet $\mathfrak{p}_S$ i den lokala ringen $R_S (= R_\mathfrak{p})$ enligt (7.5) ty utvidgningen $R_S \subseteq R'_S$ är hel. Låt $\mathfrak{p}' = f'^{-1}_S(\mathfrak{m}')$. Då är $\mathfrak{p}'$ ett primideal i R' (som inversa bilden av ett primideal) och ur kommutativiteten av diagrammet följer direkt att $\mathfrak{p}' \cap R = f_S^{-1}(\mathfrak{p}_S) = \mathfrak{p}$.

(b) Induktion. Fallet $n = 0$ följer ur (a). Antag att (b) är sant för varje kedja av längden $< n$. Låt $\mathfrak{p}'_0 \subset \ldots \subset \mathfrak{p}'_{n-1}$ vara primideal i R' sådana att $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$ för $i = 0, 1, \ldots, n-1$. Betrakta den naturliga surjektionen $R' \to R'/\mathfrak{p}'_{n-1} =: \bar{R}'$. Bilden av R är $R/(\mathfrak{p}'_{n-1} \cap R) = R/\mathfrak{p}_{n-1} =: \bar{R}$. $\mathfrak{p}_n/\mathfrak{p}_{n-1} =: \bar{\mathfrak{p}}_n$ är ett nollskilt primideal i $\bar{R}$ och utvidgningen $\bar{R} \subseteq \bar{R}'$ är hel enligt (5.16)(a). Enligt (a) existerar ett primideal $\bar{\mathfrak{p}}'_n$ i $\bar{R}'$ sådant att $\bar{\mathfrak{p}}_n = \bar{\mathfrak{p}}'_n \cap \bar{R}$. Inversa bilden av $\bar{\mathfrak{p}}'_n$ i R' är ett primideal $\mathfrak{p}'_n$ sådant att $\mathfrak{p}'_n \supset \mathfrak{p}'_{n-1}$ och $\mathfrak{p}'_n \cap R = \mathfrak{p}_n$. □

(7.8) Bevis av (7.4). Om $\mathfrak{p}'_0 \subset \mathfrak{p}'_1 \subset \ldots \subset \mathfrak{p}'_n$ är en kedja av primideal i R' så är $\mathfrak{p}'_0 \cap R \subset \mathfrak{p}'_1 \cap R \subset \ldots \subset \mathfrak{p}'_n \cap R$ en kedja av primideal i R enligt (7.6). Alltså är $\dim R \geq \dim R'$. Om $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$ är en kedja av primideal i R så existerar en kedja $\mathfrak{p}'_0 \subset \ldots \subset \mathfrak{p}'_n$ av primideal i R' (och till och med $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$, $i = 1, \ldots, n$) enligt (7.7) (b). Alltså är $\dim R' \geq \dim R$.

Nu visar vi en annan viktig sats om Krulldimensionen av ringar:

(7.9) Sats. $\dim K[X_1, \ldots, X_n] = n$ *om* K *är en kropp.*

Bevis. Det är klart att $\dim K[X_1, \ldots, X_n] \geq n$ ty

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \ldots \subset (X_1, X_2, \ldots, X_n)$$

är en kedja av längden n av primideal i $K[X_1, \ldots, X_n]$. Vi skall visa med induktion m.a.p. n att $\dim K[X_1, \ldots, X_n] \leq n$. Om $n = 1$ så är påståendet klart (se (7.3)(b)). Antag att påståendet gäller för varje K då antalet variabler är $< n$. Låt

$$(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_k$$

vara en kedja av primideal i $K[X_1, \ldots, X_n]$ med $k \geq n \geq 2$. Betrakta de multiplikativa mängderna $S_i = K[X_i] \setminus (0)$ för $i = 1, \ldots, n$. Vi påstår att det finns $i \in \{1, 2, \ldots, n\}$ sådant att $S_i \cap \mathfrak{p}_{k-1} = \emptyset$. Detta följer ur:

(7.10) Lemma. *Om $\mathfrak{p}$ är ett primideal i $K[X_1, \ldots, X_n]$ sådant att $S_i \cap \mathfrak{p} \neq \emptyset$ för varje $i \in \{1, \ldots, n\}$ så är $\mathfrak{p}$ maximalt.*

Bevis. Låt $K[X_1, \ldots, X_n]/\mathfrak{p} =: K[x_1, \ldots, x_n]$. Utvidgningen $K[x_1, \ldots, x_n] \supseteq K$ är hel ty för varje i finns det ett icke-konstant polynom $p(X_i) \in \mathfrak{p}$ så att $p(x_i) = 0$ dvs x_i är algebraiskt (= hel) över kroppen K. Alltså är $K[x_1, \ldots, x_n]$ en kropp enligt (5.9) och (5.6), vilket betyder att $\mathfrak{p}$ är maximalt. □

Nu vet vi att det finns i sådant att $S_i \cap \mathfrak{p}_{k-1} = \emptyset$ ty $\mathfrak{p}_{k-1}$ är inte maximalt. Låt $S_i = S$ och betrakta kedjan (se (4.17))

$$(0) = (\mathfrak{p}_0)_S \subset (\mathfrak{p}_1)_S \subset \ldots \subset (\mathfrak{p}_{k-1})_S$$

i $K[X_1, \ldots, X_n]_S = K(X_i)[X_1, \ldots, \hat{X}_i, \ldots, X_n]$= polynomringen i alla variabler $X_1, \ldots, X_n$ utom X_i med koefficienter i kroppen $K(X_i)$. Enligt induktionsantagandet är $k - 1 \leq n - 1$ så att $k \leq n$. □

För att kunna beräkna dimensionen av ringar av typen $K[V]$, där V är en delmångfald i $\bar{K}^n$ (som t ex i (7.3) (d)) måste vi diskutera begreppet transcendent dimension.

(7.11) Definition. Låt $K \subseteq L$ vara en kroppsutvidgning. Man säger att $x_1, \ldots, x_n \in L$ är **algebraiskt beroende över** K om det finns ett icke konstant polynom p i polynomringen $K[X_1, \ldots, X_n]$ sådant att $p(x_1, \ldots, x_n) = 0$. Om ett sådant polynom inte existerar så säger man att $x_1, \ldots, x_n$ är **algebraiskt oberoende över** K. En delmängd $\mathcal{B}$ till L kallas algebraiskt oberoende över K om varje ändlig uppsättning av element i $\mathcal{B}$ är algebraiskt oberoende över K.

□

Observera att begreppet linjärt (o)beroende definieras på liknande sätt med hjälp av linjära polynom $p(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n$, $a_i \in K$. Precis som för linjära fallet kommer vi att definiera begreppen bas och dimension.

(7.12) Anmärkning. Det faktum att elementen $x_1, \ldots, x_r \in L \supseteq K$ är algebraiskt oberoende över K kan man också uttrycka så att ringen $K[x_1, \ldots, x_r]$ är isomorf med polynomringen $K[X_1, \ldots, X_r]$. I själva verket har vi en surjektion:

$$\varphi : K[X_1, \ldots, X_r] \to K[x_1, \ldots, x_r],$$

där $\varphi(X_i) = x_i$. Betrakta kärnan $\mathrm{Ker}\varphi = \{p \in K[X_1, \ldots, X_r] : p(x_1, \ldots, x_r) = 0\}$. Om $x_1, \ldots, x_r$ algebraiskt oberoende och $p \in \mathrm{Ker}\varphi$ så är $p \equiv 0$ dvs $\mathrm{Ker}\varphi = (0)$, vilket betyder att φ är en injektion. Alltså är $K[X_1, \ldots, X_r] \cong K[x_1, \ldots, x_r]$. En isomorfism mellan dessa ringar implicerar att $x_1, \ldots, x_r$ är algebraiskt oberoende – det är en direkt konsekvens av (7.11).

□

(7.13) Definition. Man säger att $\mathcal{B} \subset L$ är en **transcendent bas** för L över K om $\mathcal{B}$ är en algebraiskt oberoende delmängd till L som är maximal med avssende på den egenskapen, dvs $\mathcal{B}$ är algebraiskt oberoende och för varje $x \in L$ om $x \notin \mathcal{B}$ så är $\mathcal{B} \cup \{x\}$ algebraiskt beroende.

□

Definitionen kan också formuleras så att $\mathcal{B}$ är en transcendent bas för L över K om $\mathcal{B}$ är algebraiskt oberoende över K och utvidgningen $L \supseteq K(\mathcal{B})$ är algebraisk.

(7.14) Sats. *För varje kroppsutvidgning $K \subseteq L$ som inte är algebraisk existerar en transcendent bas över K och två sådana baser har samma kardinalitet.*

Bevis. Existensen av transcendenta baser visas på exakt samma sätt som existensen av linjära med hjälp av Zorns Lemma. Med andra ord betraktar man över K alla algebraiskt oberoende delmängder $\mathcal{B}$ till L, ordnade med inklusion. Sådana delmängder existerar därför att L enligt förutsättningen innehåller transcendenta element så att man kan välja $\mathcal{B} = \{x\}$ med ett transcendent $x \in L$. Om $\mathcal{B}_1 \subseteq \ldots \subseteq \mathcal{B}_n \subseteq \ldots$ är en växande kedja av algebraiskt oberoende delmängder till L så är också $\bigcup_{i=1}^{\infty} \mathcal{B}_i$ algebraiskt oberoende. Enligt Zorns Lemma existerar en maximal över K algebraiskt oberoende delmängd till L.

Det andra påståendet i satsen visar vi under förutsättningen att L har en ändlig transcendent bas. Detta är det fall som är viktigt i fortsättningen. Mera exakt visar vi att om $\mathcal{B} = \{x_1, \ldots, x_n\}$ är en transcendent bas och $y_1, \ldots, y_m \in L$ är algebraiskt oberoende så är $m \leq n$. Det är då klart att alla transcendenta baser för L över K måste vara ändliga och bestå av n element.

Vi visar påstående med hjälp av induktion med avseende på n då K är en godtycklig delkropp till L.

Om $n = 1$ så är utvidgningen $L \supseteq K(x_1)$ algebraisk så att y_1 satisfierar en polynomekvation $\neq 0$ med koefficienter i $K(x_1)$. Detta betyder att $p(y_1, x_1) = 0$ för ett icke-trivialt polynom p med koefficienter i K som innehåller både x_1 och y_1 (därför att x_1 och y_1 inte är algebraiska över K). Alltså är utvidgningarna

$$L \supseteq K(y_1, x_1) \supseteq K(y_1)$$

algebraiska dvs $L \supseteq K(y_1)$ är algebraiskt. Detta visar att uppsättningen $y_1, \ldots, y_m$ endast innehåller ett element dvs $m = 1$.

Antag nu att påståendet gäller då antalet element i $\mathcal{B}$ är $< n$, där $n > 1$. Eftersom $L \supseteq K(x_1, \ldots, x_n)$ är en algebraisk utvidgning så är y_1 lösningen till en icke-trivial ekvation med koefficienter i $K(x_1, \ldots, x_n)$. Precis som ovan ger detta en polynomekvation $p(y_1, x_1, \ldots, x_n) = 0$, där p är ett icke-trivialt polynom med koefficienter i K. Polynomet p måste innehålla y_1 (ty $x_1, \ldots, x_n$ är algebraiskt oberoende) och något av $x_1, \ldots, x_n$ (ty y_1 är

algebraiskt oberoende dvs transcendent över K). Anta (efter en eventuell omnumrering) att x_1 ingår i p. Då får vi att utvidgningarna:

$$L \supseteq K(y_1, x_1, \ldots, x_n) \supseteq K(y_1, x_2, \ldots, x_n)$$

är algebraiska. Alltså är $x_2, \ldots, x_n$ en transcendent bas för L över $K(y_1)$. Elementen $y_2, \ldots, y_m \in L$ är algebraiskt oberoende över $K(y_1)$. Enligt induktionsantagandet är $m-1 \leq n-1$ så att $m \leq n$. □

(7.15) Definition. Om $K \subseteq L$ är en kroppsutvidgning med en ändlig transcendent bas $\mathcal{B}$ så kallas kardinaliteten av $\mathcal{B}$ för **transcendent dimension** (eller **transcendensgraden**) av L över K. Vi skall beteckna den dimensionen med $\text{tr.d.}_K L$.

□

(7.16) Anmärkning. Observera att om L är ändligt genererad som kropp över K dvs $L = K(x_1, \ldots, x_n)$, där $x_i \in L$, så är existensen av en transcendent bas banal. Man kan helt enkelt succesivt välja en maximal uppsättning av algebraiskt oberoende element bland $x_1, \ldots, x_n$. En sådan uppsättning bildar en transcendent bas (se (7.13) och (5.9)).

□

(7.17) Noethers normaliseringssats. *Låt $L \supseteq K$ vara en ändligt genererad kroppsutvidgning av transcendensgraden $r \geq 1$. Om $L = K(x_1, \ldots, x_n)$ så existerar $y_1, \ldots, y_r \in K[x_1, \ldots, x_n]$ sådana att utvidgningen*

$$K[y_1, \ldots, y_r] \subseteq K[x_1, \ldots, x_n]$$

är hel (och $y_1, \ldots, y_r$ bildar en transcendent bas för L över K).

Bevis. Vi skall använda oss av induktion med avseende på n. Om $n = 1$ så är $r = 1$ och man väljer $y_1 = x_1$. Antag att satsen gäller då antalet generatorer är $< n$, där $n > 1$. Om $x_1, \ldots, x_n$ är algebraiskt oberoende så kan vi välja $y_i = x_i$ för $i = 1, \ldots, n$. Om dessa element är algebraiskt beroende så har vi

$$(*) \qquad \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = 0,$$

där $a_{i_1 \ldots i_n} \in K^*$. Vi vill välja ett generatorsystem $x_1', \ldots, x_n'$ för L över K så att

$$K[x_1, \ldots, x_n] = K[x_1', \ldots, x_n']$$

och x_n' är helt över $K[x_1', \ldots, x_{n-1}']$. Detta i kombination med induktionsantagandet ger att det finns $y_1, \ldots, y_r$ sådana att

$$K[y_1, \ldots, y_r] \subseteq K[x_1', \ldots, x_{n-1}'] \subseteq K[x_1', \ldots, x_{n-1}', x_n'] = K[x_1, \ldots, x_n]$$

är hela utvidgningar. Låt oss välja

$$x_1' = x_1 - x_n^{k_1}, \ldots, x_{n-1}' = x_{n-1} - x_n^{k_{n-1}},\ x_n' = x_n$$

med $k_1, \ldots, k_{n-1}$ som vi definierar snart. Det är klart att $K[x_1, \ldots, x_n] = K[x_1', \ldots, x_n']$. Likheten $(*)$ kan man skriva om på följande sätt

$$(**) \qquad \sum a_{i_1 \ldots i_n} x_n'^{i_1 k_1 + \ldots + i_{n-1} k_{n-1} + i_n} + p(x_1', \ldots, x_n') = 0,$$

där $p \in K[X_1, \ldots, X_n]$ och $p(0, \ldots, 0, x_n') = 0$. Nu väljer vi ett naturligt tal b som är större än alla exponenter $i_1, \ldots, i_n$ och $k_1 = b^{n-1}, \ldots, k_{n-1} = b$. Då är alla naturliga tal

$$i_1 b^{n-1} + \ldots + i_{n-1} b + i_n$$

olika ($i_1, \ldots, i_n$ är "siffror" i talsystemet med bas b). Alltså säger ekvationen $(**)$ att x_n' är helt över $K[x_1', \ldots, x_{n-1}']$. □

(7.18) Proposition. *Låt R vara en K-algebra utan nolldelare av ändlig typ över K och låt L vara kvotkroppen av R. Då är* $\dim R = tr.d._K L$.

Bevis. Låt $R = K[x_1, \ldots, x_n]$ och låt $\mathrm{tr.d.}_K L = r$. Låt $y_1, \ldots, y_r \in R$ vara algebraiskt oberoende element sådana att $K[x_1, \ldots, x_n]$ är en hel utvidgning av $K[y_1, \ldots, y_r]$ (existensen av $y_1, \ldots, y_r$ följer ur Noethers normaliseringssats). Då är

$$\dim K[x_1, \ldots, x_n] = \dim K[y_1, \ldots, y_r] = r,$$

varvid första likheten följer ur sats (7.4) (ty $K[x_1, \ldots, x_n] \supseteq K[y_1, \ldots, y_r]$ är hel) och den andra ur sats (7.9) (ty $K[y_1, \ldots, y_r]$ är polynomringen i r variabler enligt (7.12)) □.

(7.19) Exempel. Vi återkommer till Exempel (7.3) (d). Låt

$$R = K[x, y, z] = K[X, Y, Z]/(X^2 + Y^2 - 1).$$

Då är $\dim R = 2$. Först konstaterar vi att x, z är algebraiskt oberoende över K – om $p(x, z) = 0$, där $p(X, Z)$ är ett polynom $\neq 0$, så har vi $p(X, Z) \in (X^2 + Y^2 - 1)$ dvs $p(X, Z) = (X^2 + Y^2 - 1)q(X, Y, Z)$. Men den likheten är omöjlig ty $p(X, Z)$ innehåller inte variabeln Y, däremot till höger har vi ett polynom vars grad m.a.p. Y är minst 2. Men y är algebraiskt beroende av x, z (ty $x^2 + y^2 = 1$) så att $\mathrm{tr.d}_K K(x, y, z) = 2$. Enligt (7.18) är $\dim R = 2$. På samma sätt, om $K[x, y] = K[X, Y]/(p(X, Y))$, där p är ett irreducibelt polynom, så är $\dim K[x, y] = 1$, ty x eller y måste vara transcendent över K. För att visa det observera att om $p(X, Y)$ innehåller Y så är x algebraiskt oberoende (dvs transcendent) – om $q(x) = 0$ så har vi $q(X) \in (p(X, Y))$ dvs $q(X) = p(X, Y)r(X, Y)$ – en motsägelse! Det är klart att x och y är algebraiskt beroende. Alltså är $\mathrm{tr.d.}_K K(x, y) = 1$, dvs $\dim K[x, y] = 1$.

□

(7.20) Definition. Låt $V \subseteq \bar{K}^n$ vara en irreducibel algebraisk mängd. Med **dimensionen** $\dim V$ av V menar man

$$\dim K[V] = \dim K[X_1, \ldots, X_n]/\mathcal{I}(V),$$

där $\mathcal{I}(V) = \{p \in K[X_1, \ldots, X_n] : \forall_{\boldsymbol{x} \in V} p(\boldsymbol{x}) = 0\}$ (se Övn. 2.22).

□

(7.21) Hilberts Nullstellensatz. *Låt $p_1, \ldots, p_r \in K[X_1, \ldots, X_n]$, där K är en algebraiskt sluten kropp. Om $p \in K[X_1, \ldots, X_n]$ är ett polynom sådant att $p(\boldsymbol{x}) = 0$ för varje lösning $\boldsymbol{x} \in K^n$ till systemet $p_1 = 0, \ldots, p_r = 0$, så finns det $N > 0$ sådant att*

$$p^N = p_1 q_1 + \ldots + p_r q_r, \quad \text{där} \quad q_1, \ldots, q_r \in K[X_1, \ldots, X_n].$$

Med andra ord, om $I \lhd K[X_1, \ldots, X_n]$ så är $\mathcal{IZ}(I) = \sqrt{I}$ † (här är $I = (p_1, \ldots, p_r)$).

Vi skall först visa:

(7.22) Hilberts Nullstellensatz i svag form. *Om $\mathfrak{m}$ är ett maximalideal i polynomringen $K[X_1, ..., X_n]$, där K är algebraiskt sluten, så är $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ för något $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$.*

Bevis. Betrakta kroppen $K[X_1, \ldots, X_n]/\mathfrak{m} =: K[x_1, \ldots, x_n]$. Vi påstår att $x_1, \ldots, x_n$ är algebraiska över K. Om inte, så finns det bland $x_1, \ldots, x_n$ minst ett transcendent element dvs $\text{tr.d.}_K K(x_1, \ldots, x_n) = r \geq 1$. Enligt Noethers normaliseringssats finns det $y_1, \ldots, y_r \in K[x_1, \ldots, x_n]$ sådana att utvidgningen $K[x_1, \ldots, x_n] \supset K[y_1, \ldots, y_r]$ är hel. Men $K[x_1, ..., x_n]$ är en kropp så att $K[y_1, \ldots, y_r]$ också är en kropp enligt (5.6). Detta är dock omöjligt ty $r \geq 1$ och $K[y_1, \ldots, y_r]$ är en polynomring i r variabler. Detta visar att $x_1, \ldots, x_n$ är algebraiska över K. Men K är algebraiskt sluten så att $x_i \in K$. Alltså är $X_i - x_i \in \mathfrak{m}$ så att $\mathfrak{m} \supseteq (X_1 - x_1, \ldots, X_n - x_n)$. Men $(X_1 - x_1, \ldots, X_n - x_n)$ är ett maximalideal dvs $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ ty $\mathfrak{m}$ är också maximalt. □

(7.23) Bevis av (7.21). Betrakta $K[X_1, \ldots, X_n, T]$ och polynomen $p_1, \ldots, p_r, 1 - Tp$ i denna polynomring. Systemet $p_1 = 0, \ldots, p_r = 0, 1 - Tp = 0$ saknar lösningar $(\boldsymbol{x}, t) \in K^{n+1}$, ty $p_1(\boldsymbol{x}) = 0, \ldots, p_r(\boldsymbol{x}) = 0$ ger $p(\boldsymbol{x}) = 0$ dvs $1 = 0$. Alltså måste $(p_1, \ldots, p_r, 1 - Tp) = K[X_1, \ldots, X_n, T]$ ty ett äkta ideal $(p_1, \ldots, p_r, 1 - Tp)$ ligger i ett maximalideal $(X_1 - x_1, \ldots, X_n - x_n, T - t)$ enligt (7.22) så att $(\boldsymbol{x}, t) = (x_1, \ldots, x_n, t)$ är en lösning till $p_1 = \ldots = p_r = 1 - Tp = 0$. Därför

$$1 = q_1'(X_1, \ldots, X_n, T)p_1 + \ldots + q_r'(X_1, \ldots, X_n, T)p_r + q'(X_1 \ldots, X_n, T)(1 - Tp).$$

Låt oss sätta in $T = \frac{1}{p}$ och multiplicera likheten med en tillräckligt hög potens av p. Då får vi

$$p^N = q_1(X_1, \ldots, X_n)p_1 + \ldots + q_r(X_1, \ldots, X_n)p_r$$

för lämpliga polynom $q_i \in K[X_1, \ldots, X_n]$. □

† $\sqrt{I}$ definieras i övn. 4.11

(7.24) Exempel. I Exempel (7.1) hade vi $V = V_0 = \{(x, y, z) \in \mathbb{C}^3 : x^2 + y^2 = 1\}$. Låt $\mathfrak{p} = (X^2 + Y^2 - 1)$. Vi har $V = \mathcal{Z}(\mathfrak{p})$. Alltså är $\mathcal{I}(V) = \mathcal{I}\mathcal{Z}(\mathfrak{p}) = \sqrt{\mathfrak{p}}$ enligt Nullstellensatz. Men $\mathfrak{p}$ är ett primideal så att $\sqrt{\mathfrak{p}} = \mathfrak{p}$ och det betyder att $\mathfrak{I}(V) = (X^2 + Y^2 - 1)$.

□

ÖVNINGAR

7.1. Bestäm $\dim R$ för följande ringar R:

(a) $R = \mathbb{Z}[\sqrt{d_1}, \ldots, \sqrt{d_n}]$, $d_1, \ldots, d_n$ heltal;

(b) $R = \mathbb{Z}/(n)$, n ett heltal;

(c) $R = K[X]/(p)$, p ett polynom;

(d) $R = K[X_1, \ldots, X_n]/(p)$, p ett irreducibelt polynom.

7.2. Låt R vara en ring och S en multiplikativ mängd i R. Visa att $\dim R_S \leq \dim R$.

7.3. Låt R vara en ring och I ett ideal i R. Visa att $\dim R/I \leq \dim R$.

7.4. Visa att om $K[x_1, \ldots, x_n]$ är en kropp så är $x_1, \ldots, x_n$ algebraiska över kroppen K.

Anmärkning och ledning. Detta påstående kallas ofta för den svaga formen av Nullstellensatz. Utnyttja samma argument som i beviset av (7.18)!

7.5. Låt K vara en kropp och $\mathfrak{m}$ ett maximalideal i $K[X_1, \ldots, X_n]$. Visa att det finns en kedja $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n$ av primideal i $K[X_1, \ldots, X_n]$ sådan att $\mathfrak{p}_n = \mathfrak{m}$.

7.6. Låt $V = \{(t, t^2, t^3) \in \mathbb{C}^3, t \in \mathbb{C}\}$. Visa att V är en irreducibel algebraisk mängd. Bestäm $\mathcal{I}(V)$ och $\dim V$.

7.7. Låt $V = \mathcal{Z}(X^2 + Y^2 - Z^2, Z - X) \subset \mathbb{C}^3$. Bestäm $\mathcal{I}(V)$ och $\dim V$.

7.8. Låt $f_1, g_1, \ldots, g_r \in K[V]$ vara regulära funktioner på en algebraisk mångfald, $V \subseteq K^n$, K en algebraiskt sluten kropp. Visa att om $f(v) = 0$ för varje $v \in V$ sådan att $g_1(v) = \ldots = g_r(v) = 0$ så existerar $N > 0$ så att $f^N \in (g_1, \ldots, g_r)$.

Anmärkning. Det är en version av Nullstellensatz ($V \subseteq K^n$ i stället för $V = K^n$) – den följer lätt ur (7.17).

Kapitel 8

DEDEKINDRINGAR

Ringar av algebraiska heltal studerades mycket intensivt under 1800-talet speciellt i samband med olika försök att bevisa Fermats stora sats. Bristen på entydigheten av primfaktoruppdelningar i flertalet ringar av den typen ledde E. Kummer till en teori som med hjälp av "idealtal" kunde återinföra entydiga faktoruppdelningar fast för helt nya objekt relaterade till sådana ringar. Med hjälp av denna teori lyckades Kummer att bevisa Fermats stora sats för alla exponenter ≤ 100. Senare förenklades Kummers "idealtal" av R. Dedekind som introducerade begreppet ideal och definierade den klass av ringar i vilken varje ideal $\neq (0)$ är en entydig produkt av primideal. Sådana ringar bär idag Dedekinds namn. De har en mycket stor betydelse både i talteori och i algebraisk geometri. Vi skall ägna detta kapitel åt Dedekindringar samt deras aritmetiska och geometriska aspekter.

(8.1) Definition. Man säger att ett integritetsområde R är en **Dedekindring** om R är noethersk, helt sluten och har Krulldimensionen 1 (dvs varje nollskilt primideal i R är maximalt).

□

(8.2) Exempel. (a) $\mathbb{Z}$ och $K[X]$ (K en kropp) är Dedekindringar. Mera allmänt är varje huvudidealområde, som inte är en kropp, en Dedekindring – det är noetherskt, helt slutet[†] och har Krulldimensionen 1 (se (7.3)(b)).

(b) $\mathbb{Z}[i]$ är en Dedekindring. Här fungerar samma argument som i (a) (ty $\mathbb{Z}[i]$ är en huvudidealring), men detta exempel är ett specialfall av en allmän sats (se (8.16)) som säger att om R är en Dedekindring, K dess kvotkropp och $L \supseteq K$ en ändlig och separabel (se (8.20)) kroppsutvidgning så är hela höljet R' till R i L en Dedekindring (här är $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ och $R' = \mathbb{Z}[i]$). Speciellt om $L \supseteq \mathbb{Q}$ är en algebraisk talkropp (av ändlig dimension över $\mathbb{Q}$) så bildar alla algebraiska heltal i L en Dedekindring.

[†]Tidigare konstaterade vi att en ring med entydig faktoruppdelning är helt sluten (se (5.12)(c)). Varje huvudidealområde har den egenskapen (se Övn. 8).

(c) Senare visar vi att om $V = \{(a,b) \in \mathbb{C}^2 : F(a,b) = 0\}$ är en irreducibel kurva i $\mathbb{C}^2$, där F är ett irreducibelt polynom i $\mathbb{C}[X,Y]$, så är V icke-singulär då och endast då $\mathbb{C}[V] = \mathbb{C}[X,Y]/(F)$ är en Dedekindring (se (8.13)). T ex om $y^2 = x^3 - x$ (en elliptisk kurva) så är ringen $\mathbb{C}[x,y]$ en Dedekindring (det är lätt att kontrollera att kurvan är icke-singulär – se (8.11)).

(d) Om R är en Dedekind ring och $\mathfrak{p}$ ett primideal i $R, \mathfrak{p} \neq (0)$, så är $R_\mathfrak{p}$ en lokal Dedekindring (t ex $\mathbb{Z}_{(p)} = \{\frac{m}{n} : m,n \in \mathbb{Z}, p \nmid n\}$). Ringen $R_\mathfrak{p}$ är lokal, noethersk (se Övn. 6.3), helt sluten (se Övn. 5.11) och $\dim R_\mathfrak{p} = 1$, ty $(0) \subset \mathfrak{p}R_\mathfrak{p}$ är den längsta (och den enda) kedjan av primideal i $R_\mathfrak{p}$.

□

Låt oss först undersöka lokala Dedekindringar.

(8.3) Proposition. *Låt R vara ett lokalt integritetsområde. Då är R en Dedekindring då och endast då R är en huvudidealring.*

Bevis. Det är klart att varje huvudidealring är en Dedekindring (se (8.2)(a)). Antag att R är en Dedekindring och $\mathfrak{m}$ maximalidealet i R. Låt K vara kvotkroppen av R och låt

$$\mathfrak{m}' = \{x \in K : x\mathfrak{m} \subseteq R\}.$$

Man kontrollerar lätt att $\mathfrak{m}'$ är en R-modul sådan att $\mathfrak{m}' \supseteq R$. Det är klart att

$$\mathfrak{m} \subseteq \mathfrak{m}'\mathfrak{m} \subseteq R$$

och att $\mathfrak{m}'\mathfrak{m}$ är ett ideal i R. Men $\mathfrak{m}$ är ett maximalideal så att $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ eller $\mathfrak{m}'\mathfrak{m} = R$. Vi visar att $\mathfrak{m}'\mathfrak{m} = R$. För att göra det låt oss först konstatera att $\mathfrak{m}' \supset R$. Välj nämligen $r \in \mathfrak{m}$, $r \neq 0$, och betrakta den multiplikativa mängden $S_r = \{r^n,\, n \geq 0\}$. Lokaliseringen R_{S_r} är en delring till K som innehåller R. Primidealen i R_{S_r} är lokaliseringarna av primidealen i R. Men $r \in \mathfrak{m}$ så att $\mathfrak{m}_{S_r} = R_{S_r}$ dvs R_{S_r} har enbart ett maximalideal – nollidealet. Alltså är R_{S_r} en kropp dvs $R_{S_r} = K$ (ty kvotkroppen av varje lokalisering av R är K). Fixera nu ett element $m_0 \in \mathfrak{m}$, $m_0 \neq 0$, och välj som r olika generatorer $r_1, \ldots, r_k$ för $\mathfrak{m}$ (om $\mathfrak{m} = Rr_1 + \ldots + Rr_k$). Då är

$$\frac{1}{m_0} = \frac{r_i'}{r_i^{n_i}},$$

dvs $r_i^{n_i} = r_i' m_0 \in Rm_0$ för ett $r_i' \in R$ och ett lämpligt n_i. Alltså kan man välja N så att $\mathfrak{m}^N \subseteq Rm_0$ (t ex $N = k \cdot \max(n_i)$). Välj nu N minimalt med den egenskapen, dvs sådant att $\mathfrak{m}^N \subseteq Rm_0$ och $\mathfrak{m}^{N-1} \not\subseteq Rm_0$. Låt $x \in \mathfrak{m}^{N-1} \setminus Rm_0$. Då är $\mathfrak{m}x \subseteq Rm_0$, vilket ger att $\frac{x}{m_0} \in \mathfrak{m}'$. Men $\frac{x}{m_0} \notin R$ ty $x \notin Rm_0$. Detta visar att $\mathfrak{m}' \supset R$.

Nu kan vi visa att $\mathfrak{m}'\mathfrak{m} = R$. Om den likheten inte gäller så är $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. Alltså får vi att för varje $x \in \mathfrak{m}'$ gäller $x\mathfrak{m} \subseteq \mathfrak{m}$. Men $\mathfrak{m}$ är ändligt genererad R-modul, vilket ger att x är helt över R (se bevis för (5.7)). Alltså $x \in R$ ty R är helt sluten. Detta visar att $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ implicerar att $\mathfrak{m}' \subseteq R$ – en motsägelse.

Nu visar vi att $\mathfrak{m}$ är ett huvudideal. Vi har

$$1 = x_1y_1 + \ldots + x_ry_r,$$

där $x_i \in \mathfrak{m}$ och $y_i \in \mathfrak{m}'$. Men $x_iy_i \in R$ så att någon av termerna x_iy_i måste vara en enhet. Låt t ex $u = x_1y_1 \in R^*$. Då är $1 = xy$, där $x = x_1u^{-1} \in \mathfrak{m}$ och $y = y_1 \in \mathfrak{m}'$. Elementet $x \in \mathfrak{m}$ genererar $\mathfrak{m}$. I själva verket har vi $Rx \subseteq \mathfrak{m}$ och om $m \in \mathfrak{m}$ så är $m = x(ym) \in Rx$ ty $ym \in R$.

Det återstår att visa att alla ideal i R är principala. Detta följer ur följande resultat som avslutar beviset av (8.3):

(8.4) Lemma. *Låt R vara ett lokalt integritetsområde med maximalidealet $\mathfrak{m}$. Om R är noethersk,* $\dim R = 1$ *och $\mathfrak{m}$ är ett huvudideal så är R ett huvudidealområde (och således en Dedekindring).*

Bevis. Låt $\mathfrak{m} = (t)$. Först visar vi att $\cap_{k=0}^{\infty}\mathfrak{m}^k = (0)$ ($\mathfrak{m}^0 = R$). Om $x \in \cap_{k=0}^{\infty}\mathfrak{m}^k$, $x \neq 0$, så är $x = t^kx_k$, $x_k \in R$, för $k = 0, 1, \ldots$. Vi har

$$(x_0) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots$$

så att det finns N med $(x_N) = (x_{N+1}) = \ldots$ (ty R är noethersk). Då är $x_{N+1} = \varepsilon x_N$, $\varepsilon \in R^*$, så att $t^Nx_N = t^{N+1}x_{N+1} = t^{N+1}\varepsilon x_N$ ger $1 = t\varepsilon$ – en motsägelse.

Låt $r \in R$, $r \neq 0$. Då är $r \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ för något k, dvs $r = t^k\eta$, $\eta \in R^*$. Alltså är $(r) = (t^k) = \mathfrak{m}^k$. Om nu I är ett ideal i R så är $I = Rr_1 + \ldots + Rr_n = \mathfrak{m}^{k_1} + \ldots + \mathfrak{m}^{k_n} = \mathfrak{m}^k$, där $k = \min_i(k_i)$, dvs $I = (t^k)$ är ett huvudideal. □ □

Nu kan vi bevisa den viktigaste egenskapen hos Dedekindringarna – existensen och entydigheten av faktoruppdelningar av ideal i produkt av primideal. Först en definition:

(8.5) Definition. Låt R vara ett integritetsområde med kvotkroppen K. Man säger att en R-modul $M \subseteq K$ är ett **bråkideal** om det finns ett ideal $I \subseteq R$ och $a \in K^*$ så att $M = aI$.

□

Om t.ex. $R = \mathbb{Z}$ och $a = \frac{1}{2}$ så är $\frac{1}{2}\mathbb{Z}$ ett bråkideal.

(8.6) Sats. *Om R är en Dedekindring så kan varje icke-trivialt ideal I i R (dvs $I \neq (0), R$) skrivas som en entydig produkt av primideal så när som faktorernas ordningsföljd. Alla nollskilda bråkideal i K bildar en grupp med avseende på multiplikation av bråkidealen.*

Bevis. Låt $I \subseteq R$, $I \neq 0$. Definiera

$$I' = \{x \in K : xI \subseteq R\},$$

där K är kvotkroppen till R. Man konstaterar lätt att I' är en R-modul, $I' \supseteq R$ och $I \subseteq II' \subseteq R$. Om nu $a \in I$, $a \neq 0$ så är $aI' \subseteq R$ och aI' är ett R-ideal. Alltså är I' ett bråkideal ($aI' = J \Rightarrow I' = (1/a)J$, med ett ideal J i R).

Först visar vi att $II' = R$. Antag motsatsen. Då existerar ett maximalideal $\mathfrak{m}$ sådant att $II' \subseteq \mathfrak{m} \subset R$. Lokaliseringen ger:

$$(II')_{\mathfrak{m}} \subseteq \mathfrak{m}R_{\mathfrak{m}} \subset R_{\mathfrak{m}}.$$

Men $(II')_{\mathfrak{m}} = I_{\mathfrak{m}}I'_{\mathfrak{m}}$ (enkel övning!) och $R_{\mathfrak{m}}$ är en huvudidealring enligt (8.3). Alltså är $I_{\mathfrak{m}} = aR_{\mathfrak{m}}$ och $I'_{\mathfrak{m}} = \{x \in K : xI_{\mathfrak{m}} \subseteq R_{\mathfrak{m}}\} = (1/a)R_{\mathfrak{m}}$ dvs $I_{\mathfrak{m}}I'_{\mathfrak{m}} = R_{\mathfrak{m}}$, vilket strider mot vårt antagande. Detta visar att $II' = R$.

Nu visar vi lätt att R-bråkidealen bildar en grupp: multiplikation av två bråkideal $M_1 = a_1I_1, M_2 = a_2I_2$, där I_1, I_2 är ideal i R, ger ett bråkideal $M_1M_2 = a_1a_2I_1I_2$, en sådan multiplikation är associativ, idealet R är neutralt, och inversen till $M = aI$, med I ett ideal i R, är $M' = (1/a)I'$. Man skriver $M' = M^{-1}$.

Låt oss nu visa att varje icke-trivialt ideal i R är en produkt av primideal. Antag att det finns ett ideal $I \subset R$, $I \neq (0)$ som saknar en sådan framställning. Låt I vara maximalt i mängden av alla ideal utan framställning (existensen av I följer ur förutsättningen att R är noethersk). I är inte ett maximalideal ty ett sådant är ett primideal. Alltså är $I \subset J \subset R$ för ett R-ideal J. Men $I = J(J^{-1}I) \subseteq J^{-1}I$ och $I \subset J$ ger att $J^{-1}I \subset J^{-1}J = R$. Både J och $J^{-1}I \neq I$ kan skrivas som produkter av primideal, vilket betyder att även I är en sådan produkt. Vi får en motsägelse som bevisar existensen av faktoruppdelningar. Det återstår entydigheten. Låt

$$(*) \qquad \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{p}'_1\mathfrak{p}'_2 \dots \mathfrak{p}'_s.$$

Alltså är $\mathfrak{p}'_1\mathfrak{p}'_2 \dots \mathfrak{p}'_s \subseteq \mathfrak{p}_r$, vilket ger att $\mathfrak{p}'_i \subseteq \mathfrak{p}_r$ för något i ($\mathfrak{ab} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ eller $\mathfrak{b} \subseteq \mathfrak{p}$ för godtyckliga R-ideal $\mathfrak{a}$ och $\mathfrak{b}$ då $\mathfrak{p}$ är ett primideal). Men både $\mathfrak{p}'_i$ och $\mathfrak{p}_r$ är maximalideal så att $\mathfrak{p}'_i = \mathfrak{p}_r$. Vi kan numrera om idealen och förutsätta att $i = s$, dvs $\mathfrak{p}'_s = \mathfrak{p}_r$. Likheten $(*)$ kan nu multipliceras med $\mathfrak{p}_r^{-1}$. Då är:

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{r-1} = \mathfrak{p}'_1\mathfrak{p}'_2 \dots \mathfrak{p}'_{s-1}.$$

Ett induktivt argument ger nu $r - 1 = s - 1$ och $\mathfrak{p}_i = \mathfrak{p}'_i$ vid lämplig numrering av idealen. □

(8.7) Definition. En lokal Dedekindring kallas **diskret valuationsring** (DVR).

□

(8.8) Anmärkning. Om R är en DVR och K dess kvotkropp så är gruppen av alla R – bråkideal i K isomorf med $\mathbb{Z}$. Vi vet nämligen att bråkidealen är alla potenser $\mathfrak{m}^n$, där $\mathfrak{m}$ är maximalidealet i R och $n \in \mathbb{Z}$. När man ordnar mot $\mathfrak{m}^n$ exponenten $n \in \mathbb{Z}$ så får man en isomorfism. Man har följande kedja av R-ideal

$$\dots \mathfrak{m}^n \subset \mathfrak{m}^{n-1} \subset \dots \subset \mathfrak{m} \subset \mathfrak{m}^0 = R,$$

och $\bigcap_{n=0}^{\infty} \mathfrak{m}^n = (0)$ (se (8.4)). Alltså kan man definiera en funktion $v : R \setminus \{0\} \to \mathbb{Z}$, så att $v(t) = n$ då och endast då $t \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. En sådan funktion kallas **diskret valuation** på R. Vi skall närmare undersöka diskreta valuationer i nästa kapitel. Observera att enligt (8.3) är en diskret valuationsring ett huvudidealområde.

□

Låt oss ägna några ord åt faktoruppdelningar av element och faktoruppdelningar av ideal i ringar.

(8.9) Definition. Låt R vara ett integritetsområde. Ett element $p \in R$, 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** (UFD) 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**.

□

(8.10) Exempel. (a) Varje huvudidealområde är UFD (se vidare Övn. 7). Varje polynomring $K[X_1, \dots, X_n]$, K en kropp, är UFD. Mera allmänt kan man bevisa (se Övn. 17) 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

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

Talen 3, $2 \pm \sqrt{-5}$ är irreducibla (se (8.9)). 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. Men $\mathbb{Z}[\sqrt{-5}]$ är en Dedekindring (se (8.2)(b) och Övn. 5.6). Detta betyder att man räddar entydig uppdelning genom att övergå till ideal. Låt oss exemplifiera (8.6).

Betrakta $\mathfrak{p}_1 = (3, 2 + \sqrt{-5})$ och $\mathfrak{p}_2 = (3, 2 - \sqrt{-5})$. $\mathfrak{p}_1$ och $\mathfrak{p}_2$ är primideal (övning!). Vi har

$$\mathfrak{p}_1^2 = (2 + \sqrt{-5}), \quad \mathfrak{p}_2^2 = (2 - \sqrt{-5}), \quad \mathfrak{p}_1\mathfrak{p}_2 = (3).$$

Alltså är (9)=(3)(3)=$(\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_1\mathfrak{p}_2) = \mathfrak{p}_1^2\mathfrak{p}_2^2$ och (9)=$(2 + \sqrt{5})(2 - \sqrt{-5}) = \mathfrak{p}_1^2\mathfrak{p}_2^2$, vilket är just det förväntade resultatet. I början kallades ideal för "idealtal"† och "adjungerades" till ringen som extra element.

†Begreppet introducerades av E. Kummer (1810-1893) i samband med hans arbeten om Fermats stora sats.

(c) Alla algebraiska heltal i $\mathbb{Q}(\sqrt{d})$, d kvadratfritt heltal, bildar en Dedekindring $\mathbb{Z}[\omega_d]$, där $\omega_d = \sqrt{d}$ då $d \equiv 2, 3 \pmod 4$ och $\omega_d = \frac{1+\sqrt{d}}{2}$ då $d \equiv 1 \pmod 4$ (se Övn. 10.6 och exempel (8.2)(b)). Om $d < 0$, så är $\mathbb{Z}[\omega_d]$ UFD endast då $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$[††]. Om $d > 0$ så är det inte känt om det finns oändligt många d sådana att $\mathbb{Z}[\omega_d]$ är UFD (men man kan förmoda att det är så – det finns t.ex. 38 sådana då $d < 100$). Denna förmodan formulerades redan av C. F. Gauss.

□

Vi skall fortsätta med exempel på Dedekindringar – nu av geometrisk karaktär.

(8.11) Exempel. Låt K vara en kropp, F ett irreducibelt polynom i $K[X, Y]$ och $V = \{(a, b) \in \bar{K}^2 : F(a, b) = 0\}$ en kurva i $\bar{K}^2$. Man säger att punkten $(a, b) \in V$ är icke-singulär om $\frac{\partial F}{\partial X}(a, b) \neq 0$ eller $\frac{\partial F}{\partial Y}(a, b) \neq 0$. Vi repeterar att $K[V] = K[X, Y]/(F) =: K[x, y]$ är noethersk (se (6.12)) och $\dim K[x, y] = 1$ (se (7.19)). Mot punkten (a, b) svarar idealet $\mathfrak{m} = \mathfrak{m}_{(a,b)} = (x - a, y - b)$ i $K[x, y]$. Den lokala ringen för denna punkt på kurvan är $\mathcal{O}_{(a,b)} := K[x, y]_{\mathfrak{m}}$.

□

(8.12) Proposition. *$(a, b) \in V$ är icke-singulär då och endast då $\mathcal{O}_{(a,b)}$ är DVR.*

Bevis. "⇒" Låt $F'_x(a, b) \neq 0$ (vi skriver F'_x och F'_y i stället för F'_X och F'_Y). Vi skall visa att maximalidealet i $\mathcal{O}_{(a,b)} = K[x, y]_{\mathfrak{m}}$, där $\mathfrak{m} = (x - a, y - b)$, är genererat av $y - b$. Då följer ur (8.4) att $\mathcal{O}_{(a,b)}$ är DVR, ty den ringen är noethersk (som en lokalisering av en noethersk ring) och har dimensionen 1 (ty $\dim K[x, y] = 1$). Betrakta Taylorutvecklingen i $K[X, Y]$:

$$F(X, Y) = F(a, b) + F'_x(a, b)(X - a) + F'_y(a, b)(Y - b) + (X - a)^2 G(X, Y) + (Y - b)H(X, Y)$$

för lämpliga $G, H \in K[X, Y]$. I $K[x, y]$ övergår den likheten i

$$0 = F'_x(a, b)(x - a) + F'_y(a, b)(y - b) + (x - a)^2 G(x, y) + (y - b)H(x, y).$$

Alltså har vi $x - a = \alpha(y - b)$, där

$$\alpha = -\frac{F'_y(a, b) + H(x, y)}{F'_x(a, b) + (x - a)G(x, y)} \in \mathcal{O}_{(a,b)},$$

ty täljaren och nämnaren är i $K[x, y]$ och nämnaren ligger inte i $(x - a, y - b)$ (om $F'_x(a, b) + (x - a)G(x, y) \in (x - a, y - b)$, så $F'_x(a, b) \in (x - a, y - b)$ – en motsägelse ty $F'_x(a, b) \neq 0$).

[††]Detta påstående var en hypotes av C. F. Gauss tills H. Stark visade det 1967. Ett tidigare bevis av K. Heegner (50-talet) var oklart, men dess brister var inte så stora (som det visade sig drygt 10 år efter dess publikation).

Det betyder att $(x-a, y-b) = (y-b)$ ty $x-a$ i $\mathcal{O}_{(a,b)}$ kan uttryckas med hjälp av $y-b$. Idealet $(x-a, y-b)$ i $\mathcal{O}_{(a,b)}$ är alltså ett huvudideal.

"$\Leftarrow$". Låt $\mathcal{O}_{(a,b)}$ vara DVR. Då är idealet $\mathfrak{m}\mathcal{O}_{(a,b)} = (x-a, y-b)$ ett huvudideal. Man kan generera det med hjälp av $x-a$ eller $y-b$, ty enligt (8.8) har vi $(x-a) \subseteq (y-b)$ eller tvärtom. Antag att $(x-a) \subseteq (y-b) = (x-a, y-b)$. Då är

$$x - a = \frac{g(x,y)}{h(x,y)}(y-b), \quad g, h \in K[x,y],\ h(a,b) \neq 0.$$

Den likheten i $\mathcal{O}_{(a,b)}$ kommer från en likhet i $K[X,Y]$:

$$(X-a)h(X,Y) = g(X,Y)(Y-b) + F(X,Y)\cdot q(X,Y), \quad q \in K[X,Y].$$

Derivera den likheten med avseende på X och sätt in $(X,Y) = (a,b)$. Då är:

$$h(a,b) = F'_x(a,b)q(a,b)$$

(ty $F(a,b) = 0$). Alltså är $F'_x(a,b) \neq 0$ eftersom $h(a,b) \neq 0$. Beviset är avslutat. □

Antag nu att K är algebraiskt sluten. Då är varje maximalideal i $K[x,y]$ av formen $(x-a, y-b)$, där $(a,b) \in V$ (Nullstellensatz!) och $K[x,y] = \bigcap \mathcal{O}_{(a,b)}$, där (a,b) löper över alla punkter tillhörande V enligt (4.21). Alltså får vi:

(8.13) Proposition. *Låt K vara en algebraiskt sluten kropp och V en irreducibel kurva i K^2. V är icke-singulär (dvs alla punkter av V är icke-singulära) då och endast då $K[V]$ är en Dedekindring.*

Bevis. Om $K[V]$ är en Dedekindring och $\mathfrak{m} = (x-a, y-b)$, $(a,b) \in V$, så är den lokala ringen $K[V]_{\mathfrak{m}} = \mathcal{O}_{(a,b)}$ en DVR enligt (8.2)(d) så att (a,b) är icke-singulär enligt (8.12).

Om V är icke-singulär så är varje lokal ring $\mathcal{O}_{(a,b)}$ en DVR enligt (8.12) och som sådan är den helt sluten (se övn. 10.5 och observera att en diskret valuationsring är ett huvudidealområde i enlighet med (8.3)). Då är också $K[V] = \bigcap \mathcal{O}_{(a,b)}$ (se (4.21)) helt sluten. Vi vet redan att $K[V]$ är noethersk och $\dim K[V] = 1$ så att $K[V]$ är en Dedekindring. □

Som ett konkret exempel låt $y^2 = x^3 + ax + b$, där $a, b \in \mathbb{C}$ och $x^3 + ax + b = 0$ saknar multipla nollställen. En kurva av den typen kallas elliptisk (vi skall diskutera den terminologin senare i Kapitel 10). Man kontrollerar lätt att en sådan kurva är icke-singulär. Alltså är ringen $\mathbb{C}[x,y]$ en Dedekindring.

Nu skall vi diskutera ett begrepp som har en central betydelse i både talteori och i algebraisk geometri.

(8.14) Definition. Låt R vara en Dedekindring, K dess kvotkropp och $\mathcal{F}(R)$ gruppen av alla R-bråkideal i K. Låt $\mathcal{P}(R)$ vara gruppen av alla principala bråkideal dvs alla R-moduler

av formen $R\alpha$, $\alpha \in K^*$. Kvotgruppen $\mathcal{F}(R)/\mathcal{P}(R)$ kallas **klassgruppen** av R och betecknas $Cl(R)$.

□

(8.15) Exempel. (a) Om R är ett huvudidealområde så är $Cl(R) = (1)$. T ex är $Cl(\mathbb{Z}) = (1)$, $Cl(K[X]) = (1)$, $Cl(\mathbb{Z}[i]) = (1)$.

(b) Man kan visa att $Cl(\mathbb{Z}[\sqrt{-5}])$ innehåller två element: (1) och klassen av idealet $(3, 2 + \sqrt{-5})$. Tyvärr kan vi inte bevisa detta påstående här (det visas t ex i kursen "Algebraisk talteori").

(c) Helt allmänt visar man i algebraisk talteori att klassgruppen är ändlig om R är ringen av de algebraiska heltalen i en ändlig utvidgning $L \supseteq \mathbb{Q}$. För sådana ringar R är $Cl(R) = (1)$ då och endast då R är UFD (se Övn. 9). Därför är det t.ex. inte känt om det finns oändligt många kvadratiska utvidgningar $\mathbb{Q}(\sqrt{d}) \supset \mathbb{Q}$ sådana att $Cl(\mathbb{Z}[\omega_d]) = (1)$ då $d > 0$ (se (8.10)(c)). Undersökningar av $Cl(R)$ utgör ett av centralproblemen i algebraisk talteori (se vidare Övn. 12). Klassgruppen är också ändlig då $R = K[V]$ är ringen av de regulära funktionerna på en icke-singulär kurva V över en ändlig kropp K, t.ex. då $R = \mathbb{Z}_p[X, Y]/(X^3 + Y^3 - 1)$, $p \neq 3$ (en Fermatkurva). Se vidare Övn. 12.

□

Vi skall avsluta detta kapitel med ett resultat som ger en beskrivning av en stor klass av Dedekindringar (se t.ex. (8.2) (b)):

(8.16) Sats. *Låt R vara en Dedekindring, K dess kvotkropp och $L \supseteq K$ en ändlig och separabel kroppsutvidgning. Då är hela höljet R' till R i L en Dedekindring.*

Först skall vi förklara termen separabel kroppsutvidgning.

(8.17) Definition. Låt V vara ett ändligtdimensionellt vektorrum över en kropp K och $\varphi : V \to V$ en linjär avbildning. Med **spåret** $T(\varphi)$ av φ menar man summan av diagonalelementen i matrisen för φ med avseende på en godtycklig bas för V[†].

□

(8.18) Definition. Låt $L \supseteq K$ vara en ändlig kroppsutvidgning och $\alpha \in L$. Med **spåret** $T_{L/K}(\alpha)$ av α menar man spåret av den linjära avbildningen $x \mapsto \alpha x$, $x \in L$. Med **normen**

[†]Om $e_1, \ldots, e_n$ är en bas för V och $M_\varphi = [a_{ij}]$ matrisen för φ m.a.p. denna bas så är $-T(\varphi)$ koefficienten framför x^{n-1} i det karakteristiska polynomet $\det(XE_n - M_\varphi) = X^n - \sum a_{ii}X^{n-1} + \ldots + (-1)^n \det A$ (E_n – enhetsmatrisen). Karakteristiska polynomet är oberoende av basvalet för V.

$N_{L/K}(\alpha)$ av α menas determinanten av samma avbildning. Om $M_\alpha = [a_{ij}]$ är matrisen för $x \mapsto \alpha x$, $x \in L$, så kallar man polynomet $p_\alpha(X) = \det(XE_n - M_\alpha)$ för karakteristiska polynomet för α över K ($n = \dim_K L$).

□

(8.19) Proposition. *Låt $L \supseteq K$ vara en ändlig kroppsutvidgning och $n = \dim_K L$. Om $\alpha, \beta \in L$ och $a \in K$ så är*

(*a*) $T(\alpha + \beta) = T(\alpha) + T(\beta), \quad T(\alpha\beta) = T(\beta\alpha), \quad T(a\alpha) = aT(\alpha),$

(*b*) $N(\alpha\beta) = N(\alpha)N(\beta), \quad N(a\alpha) = a^n N(\alpha).$

Bevis. Följer direkt ur (8.18). □

(8.20) Definition. En ändlig kroppsutvidgning $L \supseteq K$ kallas **separabel** om det finns $\alpha \in L$ så att $T(\alpha) \neq 0$. En godtycklig algebraisk utvidgning $L \supseteq K$ kallas separabel om varje ändlig utvidgning av K i L är separabel.

□

(8.21) Exempel. (a) Om K har karakteristiken 0 så är varje utvidgning $L \supseteq K$ separabel, ty $1 \in L$ har spåret $T(1) = n1$, där $n = \dim_K L$.

(b) Utvidgningen $\mathbb{F}_2(X) \supset \mathbb{F}_2(X^2)$, där $\mathbb{F}_2 = \mathbb{Z}/(2)$, är icke-separabel, ty varje element $\alpha \in \mathbb{F}_2(X)$ kan skrivas på formen $\alpha = \varphi(X^2) + \psi(X^2)X$, där φ, ψ är rationella funktioner i X^2 (observera att $1, X$ bildar en bas för utvidgningen). Nu har vi

$$\begin{aligned} \alpha \cdot 1 &= \varphi(X^2) + \psi(X^2)X, \\ \alpha \cdot X &= \psi(X^2)X^2 + \varphi(X^2)X, \end{aligned}$$

så att matrisen för α är

$$M_\alpha = \begin{bmatrix} \varphi(X^2) & \psi(X^2) \\ \psi(X^2) & \varphi(X^2) \end{bmatrix}$$

med spåret $T(\alpha) = \varphi(X^2) + \varphi(X^2) = 2\varphi(X^2) = 0$.

□

Separabla utvidgningar har följande viktiga egenskap:

(8.22) Proposition. *Låt $L \supseteq K$ vara en ändlig separabel utvidgning och $e_1, \ldots, e_n$ en bas för L över K. Då finns det en bas $f_1, \ldots, f_n$ för L över K sådan att $T(e_i f_j) = \delta_{ij}$ (Kroneckers symbol).*

Bevis. Helt allmänt, om V är ett vektorrum med en bas $e_1, \ldots, e_n$ och $b : V \times V \to K$ är en symmetrisk bilinjär avbildning (= en bilinjär symmetrisk form) sådan att $b(v, V) = 0$ implicerar $v = 0$, så existerar en bas $f_1, \ldots, f_n$ sådan att $b(e_i, f_j) = \delta_{ij}$. Basen $f_1, \ldots, f_n$ är entydigt bestämd av $e_1, \ldots, e_n$ och b och kallas för den **duala basen** till $e_1, \ldots, e_n$. Vi visar detta påstående om en stund. Låt oss konstatera att $b(x, y) = T(xy)$ är just en sådan avbildning. Vi har nämligen:

$$\begin{aligned} b(x_1 + x_2, y) &= T((x_1 + x_2)y) = T(x_1y) + T(x_2y) = b(x_1, y) + b(x_2, y), \\ b(x, y) &= T(xy) = b(y, x), \\ b(ax, y) &= T(axy) = aT(xy) = ab(x, y), \end{aligned}$$

då $a \in K$. Vidare har vi att likheten $b(x, L) = T(xL) = 0$ med $x \neq 0$ implicerar att $T(L) = 0$, ty $xL = L$. Om nu $L \supseteq K$ är separabel och $b(x, L) = T(xL) = 0$ så måste $x = 0$ ty $T(1) \neq 0$.

Nu kan vi visa existensen av den duala basen. Låt $\varphi : V \to V^*$ vara avbildningen $\varphi(v)(w) = b(v, w)$, där V^* är duala rummet till V. φ är linjär och

$$\mathrm{Ker}\varphi = \{v \in V : \varphi(v) = 0\} = \{v \in V : \forall_{w \in V} b(v, w) = 0\} = (0)$$

enligt förutsättningen. Men $\dim V = \dim V^*$ så att φ som en injektion är en isomorfism. Låt $f_1, \ldots, f_n$ vara sådana vektorer i V att $\varphi(f_1), \ldots, \varphi(f_n)$ bildar den duala basen för V^* i förhållande till basen $e_1, \ldots, e_n$ för V dvs $\varphi(f_i)(e_j) = b(f_i, e_j) = \delta_{ij}$. □

(8.23) Proposition. *Låt R vara ett integritetsområde, K dess kvotkropp och $L \supseteq K$ en ändlig kroppsutvidgning. Låt $\alpha \in L$.*

(a) Det finns $r \in R$, $r \neq 0$ så att $r\alpha$ är helt över R.

(b) Om α är helt över R och R är helt sluten så har minimipolynomet för α över K alla sina koefficienter i R.

(c) Karakteristiska polynomet för α över K är en potens av minimipolynomet för α över K. Speciellt är $T(\alpha)$, $N(\alpha) \in R$ om α är helt över R och R är helt sluten.

Bevis. (a) α är algebraiskt över K så att

$$r_n\alpha^n + r_{n-1}\alpha^{n-1} + \ldots + r_0 = 0, \quad \text{där} \quad r_i \in R \quad \text{och} \quad r_n \neq 0,$$

ty K är kvotkroppen av R. Nu är $(r_n\alpha)^n + r_{n-1}(r_n\alpha)^{n-1} + \ldots + r_0 r_n^{n-1} = 0$ dvs $r_n\alpha$ är helt över R.

(b) Låt $\bar{L}$ vara en algebraiskt sluten kropp som innehåller L. Låt α vara ett nollställe till

$$p(X) = X^N + a_{N-1}X^{N-1} + \ldots + a_0, \quad a_i \in R$$

och låt $m(X) = X^n + r_{n-1}X^{n-1} + \ldots + r_0$ vara minimalpolynomet för α över K (här har man $r_i \in K$, men vi vill visa att $r_i \in R$!). Vi vet att $m(X)$ är en delare till $p(X)$ så att varje nollställe till $m(X)$ är ett nollställe till $p(X)$. Alltså är alla nollställen till $m(X)$ hela som element i $\bar{L}$. Koefficienterna r_i är summor av produkter av dessa nollställen så att de också är hela över R (se (5.10)). Men $r_i \in K$ och R är helt sluten i K så att $r_i \in R$.

(c) Låt $X^n + r_{n-1}X^{n-1} + \ldots + r_0 = 0$ vara minimipolynomet för α över K. Vi vet att $1, \alpha, \ldots, \alpha^{n-1}$ bildar en bas för $K(\alpha)$ över K (se Övn. 10.8). Låt $e_1, \ldots, e_m$ vara en bas för L över $K(\alpha)$. Produkterna $\alpha^i e_j$ bildar en bas för L över K (se Övn. 10.9). I denna bas har $x \mapsto \alpha x$, $x \in L$, matrisen:

$$M_\alpha = \begin{bmatrix} \boxed{\text{A}} & & & \\ & \boxed{\text{A}} & 0 & \\ & & \ddots & \\ & 0 & & \boxed{\text{A}} \end{bmatrix},$$

där antalet A på diagonalen är m och

$$A = \begin{bmatrix} 0 & 0 & \ldots & -r_0 \\ 1 & 0 & \ldots & -r_1 \\ 0 & 1 & \ldots & -r_2 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & -r_{n-1} \end{bmatrix}$$

ty

$$\begin{cases} \alpha \cdot 1 = & \alpha & \\ \alpha \cdot \alpha = & & \alpha^2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \alpha \cdot \alpha^{n-1} = -r_0 - r_1\alpha - r_2\alpha^2 - \ldots - r_{n-1}\alpha^{n-1} & & \end{cases}$$

Alltså är $\det(XE_{mn} - M_\alpha) = [\det(XE_n - A)]^m$. Determinanten till vänster är karakteristiska polynomet för $\alpha \in L$ över K, däremot den till höger är det minimala polynomet för α över K, ty $\det(XE_n - A) = X^n + r_{n-1}X^{n-1} + \ldots + r_0$ (en enkel övning). Vi har alltså $T(\alpha) = -mr_{n-1}$ och $N(\alpha) = \pm r_0^m$ så att $T(\alpha)$, $N(\alpha) \in R$ om α är helt över R och R är helt sluten (se (b)). □

(8.24) Bevis för (8.16). R' har Krulldimensionen 1 enligt (7.4) och är helt sluten enligt (5.15). Vi måste visa att R' är noethersk. Låt $e_1, \ldots, e_n$ vara en bas för L över K. Vi kan förutsätta enligt (8.23) (a) att $e_1, \ldots, e_n \in R'$, ty det finns $r \neq 0$ sådant att $r \in R$ och $re_i \in R'$ (välj ett r som passar alla e_i!). Låt $f_1, \ldots, f_n$ vara den duala basen till $e_1, \ldots, e_n$ med avseende på spåret T (se (8.23)). Vi vill visa att $R' \subseteq Rf_1 + \ldots + Rf_n$ dvs att R' är en delmodul till en ändlig R-modul. Då är R' noethersk (se (6.3)) dvs varje ideal i R' har en ändlig bas (ty varje ideal i R' är en R-modul). Låt $r' \in R'$ och $r' = \sum a_i f_i$, där $a_i \in L$. Då är $T(r'e_j) = T(\sum_i a_i f_i e_j) = a_j$. Men $r'e_j \in R'$ så att $a_j = T(r'e_j) \in R$ enligt (8.23) (c), dvs $r' \in Rf_1 + \ldots + Rf_n$. □

ÖVNINGAR

8.1. Visa att 21 har två olika uppdelningar i produkt av irreducibla tal i $\mathbb{Z}[\sqrt{-5}]$: $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Bestäm primideal $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ sådana att $(3)=\mathfrak{p}_1\mathfrak{p}_2$, $(7)=\mathfrak{p}_3\mathfrak{p}_4, (1 + 2\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, (1 - 2\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4$.

8.2. Vilka av följande ringar är Dedekindringar:

(a) $\mathbb{Z}[\sqrt{-6}]$; (c) $\mathbb{C}[X, Y]/(X^2 - Y^3)$;
(b) $\mathbb{Z}[2i]$; (d) $\mathbb{Z}[\sqrt{-2}]$.

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

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

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

(c) 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:

(i) $\mathbb{Z}$, (ii) $K[X], K$ en kropp, (iii) $\mathbb{Z}[i]$, (iv) $\mathbb{Z}[\sqrt{2}]$, (v) $\mathbb{Z}[\sqrt{-2}]$.

Anmärkning. Det är inte svårt att visa att bland ringarna $\mathbb{Z}[\omega_d]$ med $d < 0$ (se (8.10)(c)) finns det enbart 5 som är euklidiska. De ges av $d = -1, -2, -3, -7, -11$ och är euklidiska med avseende på den vanliga normen $N(a + b\omega_d) = |a + b\omega_d|^2$. Om $d > 0$ så är $\mathbb{Z}[\omega_d]$ euklidisk med avseende på normen $N(a + b\omega_d) = |(a + b\omega_d)(a + b\bar{\omega}_d)|$ (se (8.18) och (8.10) (c)) endast då $d =$ 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73. Det är inte känt om $\mathbb{Z}[\omega_d]$ kan vara euklidisk för andra $d > 0$ (med avseende på en lämplig funktion N). Man förmodar att det är så för t.ex. $\mathbb{Z}[\sqrt{14}]$. En euklidisk ring är UFD (bevis som för $\mathbb{Z}$), men UFD behöver inte vara euklidisk (ett exempel: $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ – se (8.10)(c)).

(d) Visa att varje euklidisk ring är ett huvudidealområde.

8.4. Om R är euklidisk och $a \in R$ så är a inverterbart då och endast då $N(a) = 1$.

8.5. Låt R vara ett noethersk integritetsområde. Visa att varje element $r \in R \setminus R^*$, $r \neq 0$, är en produkt av irreducibla element (irreducibla element definieras i (8.9)).

8.6. Låt $\overline{\mathbb{Z}}$ vara ringen av alla algebraiska heltal (= alla komplexa tal hela över $\mathbb{Z}$). Visa att $\overline{\mathbb{Z}}$ saknar irreducibla element trots att det finns ej inverterbara element i $\overline{\mathbb{Z}}$ (motivera det!). Motivera att $\overline{\mathbb{Z}}$ inte är noethersk (utnyttja Övn. 5).

8.7. Låt R vara ett integritetsområde. Ett icke-inverterbart nollskilt 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 ett primtal då och endast då idealet (p) är ett primideal.

(a) Visa att ett primelement är irreducibelt (se (8.9)) 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.

8.8. Utnyttja Övn. 5 och 7 (c) för att visa att om R är PID så är R UFD.

8.9. Visa att en Dedekindring är UFD då och endast då den är PID.

8.10. 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 $\mathrm{SGD}(0, 0) = 0$.)

8.11. Låt $I_1 \subseteq I_2$ vara två ideal i en Dedekindring R. Visa att det finns exakt ett ideal I i R sådant att $I_1 = I_2 I$.

8.12. Låt $a \in R$, $a \neq 0$, R en Dedekindring. Visa att antalet primideal $\mathfrak{p}$ i R sådana att $\mathfrak{p} \supseteq (a)$ är ändligt.

8.13. Bestäm alla heltalslösningar till följande ekvationer:

(a) $y^2 = x^3 - 1$, (b) $y^2 = x^3 - 2$,
(c) $y^2 = x^3 - 3$, (d) $y^2 = x^3 - 10$.

Ledning. Utnyttja det faktum att $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$ är UFD och att klassgruppen för $\mathbb{Z}[\sqrt{-10}]$ har 2 element.

8.14. Låt $R = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$. R är en euklidisk ring (se Övn. 3).

(a) Bestäm alla enheter i R.

(b) Visa att $(1 - \omega)$ är ett maximalt ideal i R och $R/(1 - \omega) \cong \mathbb{Z}/(3)$.

(c)* Visa att ekvationen $x^3 + y^3 = z^3$ saknar heltalslösningar med $xyz \neq 0$. (se t.ex. K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory).

8.15. (a) Låt p vara ett primtal. Visa att ekvationen $x^2 + 1 = 0$ har en lösning i kroppen $\mathbb{Z}/(p)$ då och endast då $p = 2$ eller $p \equiv 1 \pmod 4$

(b) Visa att $(1 - i)$ är ett primideal i $\mathbb{Z}[i]$ och $(2)=(1 - i)^2$. Om $p \equiv 1 \pmod 4$ så är $(p) = (a + bi)(a - bi)$, där $(a + bi)$ och $(a - bi)$ är två olika primideal i $\mathbb{Z}[i]$. Om $p \equiv 3 \pmod 4$ så är (p) ett primideal i $\mathbb{Z}[i]$.

Ledning. I (a) utnyttja Fermats lilla sats: $x^p = x$ i $\mathbb{Z}/(p)$. I (b) utnyttja det att $\mathbb{Z}[i]$ är en huvudidealring och (a).

8.16. Låt $K[X, Y]/(F) = K[x, y]$, där $F(X, Y) = Y^2 - X^3 - aX - b$, vara ringen av de regulära funktionerna på den elliptiska kurvan $F = 0$ ($X^3 + aX + b = 0$ saknar multipla nollställen). Visa att $K[x, y]$ är en Dedekindring (char $K \neq 2, 3$).

Ledning. Visa att varje element av kroppen $K(x, y)$ kan skrivas på formen $\varphi(x)+\psi(x)y$, där $\varphi, \psi \in K(x)$ är rationella funktioner. Visa vidare att $K[x, y]$ är helt sluten genom

att visa att $\varphi + \psi y$ är helt över $K[x, y]$ då och endast då $\varphi, \psi \in K[x]$. (Observera at x är transcendent över K).

8.17. Låt K vara en kropp av karakteristiken $\neq 2, 3$ och $R = K[x, y]$, där $x^3 + y^3 = 1$ ringen av de regulära funktionerna på $X^3 + Y^3 = 1$. Låt $L = K(x, y)$ vara kvotkroppen av R, $z = \frac{36(x-y)}{x+y}$ och $t = \frac{12}{x+y}$. Visa att

(a) $K(x, y) = K(z, t)$ och $t^3 = z^2 + 432$;

(b) $K[z, t] \subset K[x, y]$ och $K[x, y]$ är lokaliseringen av $K[x, t]$ med avseende på den multiplikativa mängden $S = \{t^n,\ n \geq 0\}$;

(c) Motivera att $K[x, y]$ är en Dedekindring.

Anmärkning. Observera att $X^3 + Y^3 = 1$ saknar rationella lösningar då och endast då $T^3 = Z^2 + 432$ saknar rationella lösningar. Existensen av rationella lösningar till $X^3 + Y^3 = 1$ är ekvivalent med existensen av heltalslösningar till $a^3 + b^3 = c^3$ med $abc \neq 0$. Notera att $T^3 = Z^2 + 432$ är en elliptisk kurva.

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

Kapitel 9

KOMPLETTERINGAR AV RINGAR

Komplettering av en ring är en mycket viktig konstruktion som generaliserar övergången från de rationella talen till de reella. Man betraktar ringar med topologiska strukturer givna av normer. En norm definierar konvergenta följder som på ett naturligt sätt bildar en ny ring. Kompletteringen får man genom att identifiera konvergenta följder som skiljer sig så när som på en följd konvergent mot 0. De rationella talen kan kompletteras på flera olika sätt – det vanliga absolutbeloppet ger de reella talen, men dessutom får man mycket viktiga p-adiska talkroppar då man kompletterar de rationella talen med avseende på alla normer som svarar mot olika primtal p. Kompletteringen av en ring ger en ny ring som har enklare engenskaper än den urspungliga. Ofta studerar man dessa kompletteringar för att med hjälp av deras egenskaper kunna få en bättre kunskap om den givna ringen. Alla ringar i detta kapitel är kommutativa med etta.

(9.1) Definition. Man säger att en funktion $\| \| : R \to \mathbb{R}$ är en **kvasinorm** på en ring R om för godtyckliga $x, y \in R$ gäller:

(a) $\|x\| \geq 0$,
(b) $\|x\| = \| - x\|$,
(c) $\|x + y\| \leq \|x\| + \|y\|$,
(d) $\|xy\| \leq \|x\|\|y\|$.

Man säger att $\| \|$ är en **norm** om dessutom:

(a′) $\|x\| = 0 \Leftrightarrow x = 0$,
(d′) $\|xy\| = \|x\|\|y\|$.

Vi skall alltid förutsätta att det finns $x_0 \in R$ så att $\|x_0\| \neq 0$.

□

(9.2) Exempel. (a) Låt R vara en delring till $\mathbb{C}$ och $\|x\| = |x|$ då $x \in R$ (det vanliga absolutbeloppet).

(b) Låt p vara ett fixt primtal. Varje rationellt tal $x \in \mathbb{Q}$, $x \neq 0$, kan skrivas entydigt på formen

$$x = p^k \frac{m}{n}, \quad \text{där} \quad p \nmid mn.$$

Låt $v_p(x) = k$. Funktionen v_p kallas den p-**adiska valuationen**. Låt nu

$$\|x\|_p = \rho^{v_p(x)} \quad \text{då} \quad x \neq 0 \quad \text{och} \quad \|0\|_p = 0,$$

där $0 < \rho < 1$ (oftast antar man att $\rho = \frac{1}{p}$). Vi får en norm på $\mathbb{Q}$ (en enkel övning). I detta fall har vi i stället för (c):

$$\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p).$$

En norm som har den egenskapen kallas **icke-arkimedisk** (se vidare (9.5)).

(c) Som motsvarighet till (b) i fall då $R = K[X]$, låt p vara ett irreducibelt polynom i $K[X]$. Varje rationell funktion $\varphi \in K(x)$, $\varphi \neq 0$, kan entydigt skrivas på formen:

$$\varphi = p^k \frac{m}{n}, \quad \text{där} \quad p \nmid mn,$$

$k \in \mathbb{Z}$ och $m, n \in K[X]$. Låt $v_p(\varphi) = k$ och

$$\|\varphi\|_p = \rho^{v_p(\varphi)}, \quad \text{då} \quad \varphi \neq 0 \quad \text{och} \quad \|0\|_p = 0,$$

där $0 < \rho < 1$. Som i (b) får vi att $\| \, \|_p$ är icke-arkimedisk norm (på $K(X)$).

(d) Låt R vara en godtycklig ring och I ett ideal i R. Låt $I^* = \bigcap_{n=0}^{\infty} I^n$ ($I^0 = R$). Om $r \in I^*$ definierar vi $\|r\| = 0$. Om $r \notin I^*$ så existerar n sådant att $r \in I^n \setminus I^{n+1}$. Låt $\|r\| = \rho^n$, där $0 < \rho < 1$. Man kontrollerar lätt att villkoren (a) – (d) i (9.1) är uppfyllda. Kvasinormen i detta exempel kallar man för I-**adisk**.

(e) Låt $\| \, \|$ vara en norm på ett integritetsområde R och låt K vara kvotkroppen av R. Om man definierar

$$\left\| \frac{r_1}{r_2} \right\| = \frac{\|r_1\|}{\|r_2\|} \quad \text{då} \quad r_2 \neq 0,$$

så får man en norm på K (kontrollera att definitionen är korrekt!). Lägg märke till att normerna i både (b) och (c) får man ur den (p)-adiska normen på $\mathbb{Z}$ respektive $K[X]$ (se (d)) med hjälp av den konstruktionen.

(f) Låt R vara en Banachalgebra med norm $\| \|$. Då är villkoren (a) – (d) i (9.1) uppfyllda.

(g) Låt $R = V$ vara ett normerat linjärt rum över $\mathbb{R}$ eller $\mathbb{C}$ med norm $\| \|$. Man kan betrakta R som ring om $xy = 0$ då $x, y \in R$. Villkoren (a) – (d) i (9.1) är uppfyllda.

□

(9.3) Anmärkning. (a) Om $\| \|$ är en norm på en ring med etta R så är $\|1\| = 1$. Vi har $\|1\| = \|1\|\|1\|$ och $\|1\| \neq 0$ ger $\|1\| = 1$. Om $\|1\| = 0$ så är $\|x\| = \|x \cdot 1\| = \|x\| \cdot \|1\| = 0$ för varje $x \in R$, vilket strider mot förutsättningen att det finns $x_0 \in R$ med $\|x_0\| \neq 0$.

(b) Om $\| \|$ är en kvasinorm på R så är $J = \{x \in R : \|x\| = 0\}$ ett R-ideal (Övn. 1). Funktionen $\|\bar{x}\| := \|x\|$, där $\bar{x} = x + J$, är en väldefinierad kvasinorm på R/J som dessutom uppfyller villkoret (9.1)(a′).

(c) Om $\| \|$ är en norm på en ring R så kan man definiera en topologisk struktur på R vars bas består av alla omgivningar $U_{r,\varepsilon} = \{x \in R : \|x - r\| < \varepsilon\}$. Se vidare Övn. 8.

□

(9.4) Proposition. *Om $\| \|$ är en kvasinorm på R så är $|\|x\| - \|y\|| \leq \|x - y\|$.*

Bevis. $\|x\| = \|x - y + y\| \leq \|x - y\| + \|y\|$ och $\|y\| \leq \|y - x\| + \|x\|$. Men $\|x - y\| = \|y - x\|$ enligt (9.1)(b). □

(9.5) Definition. Man säger att en kvasinorm $\| \|$ på R är **icke-arkimedisk** eller **ultrametrisk** om i stället för (9.1)(c) gäller det att $\|x + y\| \leq \max(\|x\|, \|y\|)$ (se (9.2) (b), (c), (d)). Om $R' \subseteq R$ och $\|r'\| = 1$ då $r' \in R'$ så säger man att $\| \|$ är **trivial** på R'.

□

(9.6) Ostrowskis sats. *Normerna $\|x\| = |x|^\alpha$, $0 < \alpha \leq 1$, och de p-adiska normerna $\|x\|_p$ är alla icke-triviala normer på $\mathbb{Q}$.* □

För ett bevis se t ex N. Koblitz "p-adic Numbers, p-adic Analysis and Zeta-Functions".

(9.7) Anmärkning. Ett resultat som svarar mot (9.6) för $K(X)$ (och är enklare – se Övn. 4) säger att alla icke-triviala normer på $K(X)$ som är triviala på K ges av de p-adiska normerna $\| \|_p$ ur Exempel (9.2)(c) samt normen

$$\|\varphi\|_\infty = \rho^{v_\infty(\varphi)}, \quad \text{då} \quad \varphi \neq 0 \quad \text{och} \quad \|0\|_\infty = 0,$$

där $0 < \rho < 1$ och $v_\infty(\varphi) = \text{grad}(n) - \text{grad}(m)$, för $\varphi(X) = \frac{m(X)}{n(X)}$. Om $R = K[\frac{1}{X}]$, så är $\| \|_\infty$ den norm som definieras av idealet $(\frac{1}{X}) = I \subset R$ i enlighet med (9.2)(d) och därefter förlängs till kvotkroppen $K(\frac{1}{X}) = K(X)$ i enlighet med (9.2)(e). Vi skall återkomma till detta exempel senare (se Kap. 19).

□

(9.8) Definition. En **valuation** är en funktion $v : R \setminus (0) \to \mathbb{R}$ sådan att

(a) $v(xy) = v(x) + v(y)$,
(b) $v(x + y) \geq \min(v(x), v(y))$.

□

För exempel se (9.2)(b) och (c). Varje valuation definierar normer:

$$\|x\|_v = \rho^{v(x)}, \quad \text{då } x \neq 0 \text{ och } \|0\|_v = 0,$$

där $0 < \rho < 1$ (notera att $v(\pm 1) = 0$ så att $v(x) = v(-x)$). Valuationen v kallas **diskret** om $v(x)$ genererar en diskret delgrupp till $\mathbb{R}^+$ – en sådan grupp är isomorf med $\mathbb{Z}^+$ och består av alla multipler nr_0 av ett reellt tal $r_0 > 0$ (se Övn. 5). Motsvarande norm $\| \|_v$ kallas också diskret. Vi skall vanligen förutsätta att $r_0 = 1$ så att $v(x) = n$ för ett heltal n.

(9.9) Exempel. Låt R vara en diskret valuationsring, K dess kvotkropp och $\mathfrak{m} = (\pi)$ maximalidealet i R. Om $x \neq 0$, $x \in R$, så är $(x) = (\pi^n)$ för något n så att $x = \pi^n \varepsilon$, $\varepsilon \in R^*$. Låt $v(x) = n$. Vi får en diskret valuation på R. Om nu $x \in K$ så är $x = \pi^n \varepsilon$, där $n \in \mathbb{Z}$ (tag en kvot av två element ur R) och $v(x) = n$ definierar en diskret valuation på K. Lägg märke till att $v(x) \geq 0 \Leftrightarrow x \in R$ och $v(x) > 0 \Leftrightarrow x \in \mathfrak{m}$. Dessutom följer ur $x \notin R$ att $1/x \in \mathfrak{m}$.

□

(9.10) Proposition. *Låt $\| \|$ vara en icke-arkimedisk norm på en kropp K. Då är*

$$R = \{x \in K : \|x\| \leq 1\}$$

en lokal ring med kvotkroppen K och

$$\mathfrak{m} = \{x \in K : \|x\| < 1\}$$

dess maximalideal. Om $\| \|$ är en diskret norm (dvs definierad av en diskret valuation – se (9.8)) så är R en diskret valuationsring.

Bevis. Vi har $\|x \pm y\| \leq \max(\|x\|, \|y\|) \leq 1$ och $\|xy\| = \|x\|\|y\| \leq 1$ om $x, y \in R$, så att R är en ring. Om $x, y \in \mathfrak{m}$, så är $\|x \pm y\| < 1$ och om $r \in R$ så är $\|rx\| = \|r\|\|x\| < 1$, dvs $\mathfrak{m}$ är ett ideal. Om $r \in R \setminus \mathfrak{m}$, dvs $\|r\| = 1$, så är också $\|r^{-1}\| = 1$, ty $\|r\| \cdot \|r^{-1}\| = \|1\| = 1$. Alltså $r^{-1} \in R$ dvs alla element ur $R \setminus \mathfrak{m}$ är inverterbara. Detta betyder att R är en lokal ring (se (4.9)). Om $r \notin R$ så är $\|r\| > 1$ dvs $\|\frac{1}{r}\| < 1$. Alltså är K kvotkroppen av R. Låt nu $\| \ \|$ vara en diskret norm och v motsvarande valuation med värdemängden $\mathbb{Z}^+$ (dvs $\|x\| = \rho^{v(x)}$). Låt $\pi \in \mathfrak{m}$ vara ett element sådant att $v(\pi) = 1$. Om $x \in R$ och $v(x) = n$ så är $v(x\pi^{-n}) = v(x) - nv(\pi) = 0$ dvs $x\pi^{-n} = \varepsilon \in R^*$. Alltså är $x = \varepsilon\pi^{v(x)}$. Om nu $I \neq (0)$ är ett godtyckligt ideal i R så kan vi välja $x_0 \in I$ så att $v(x_0)$ är minimalt. Då är $I = (x_0) = (\pi^{v(x_0)})$, ty om $x \in I$ så är $(x) = (\pi^{v(x)}) \subseteq (\pi^{v(x_0)}) = I$ eftersom $v(x) \geq v(x_0)$. Detta visar att R är en huvudidealring (och som en lokal ring en diskret valuationsring). □

(9.11) Komplettering av en ring. Låt $(R, \| \ \|)$ vara en ring med en kvasinorm. Låt $C(R)$ vara mängden av alla följder $\{r_n\}_{n=0}^{\infty}$, $r_n \in R$, som uppfyller Cauchys villkor dvs sådana att

$$\forall_{\varepsilon>0}\exists_N\forall_{n,n'>N} \|r_n - r_{n'}\| < \varepsilon.$$

Man kontrollerar utan svårigheter att $C(R)$ är en ring med avseende på addition $\{r_n\}+\{r'_n\} = \{r_n + r'_n\}$ och multiplikation $\{r_n\}\{r_n\} = \{r_n r'_n\}$. Låt I vara mängden av alla 0-följder i $C(R)$ dvs sådana följder att

$$\forall_{\varepsilon>0}\exists_N\forall_{n>N} \|r_n\| < \varepsilon.$$

Man kontrollerar lätt att I är ett ideal i $C(R)$. Låt $\widehat{R} = C(R)/I$. Låt $\overline{\{r_n\}} \in \widehat{R}$ och definiera

$$\|\overline{\{r_n\}}\| = \lim_{n\to\infty} \|r_n\|.$$

Observera att $\{\|r_n\|\}$ uppfyller Cauchys villkor ty $|\|r_n\| - \|r_{n'}\|| \leq \|r_n - r_{n'}\| < \varepsilon$ då $n, n' > N$ enligt (9.4). Definitionen av $\|\overline{\{r_n\}}\|$ är korrekt. I själva verket ger $\overline{\{r_n\}} = \overline{\{r'_n\}}$ att $\{r_n - r'_n\} \in I$ dvs $\lim_{n\to\infty} \|r_n - r'_n\| = 0$. Men $|\|r_n\| - \|r'_n\|| \leq \|r_n - r'_n\|$ så att $\lim_{n\to\infty} \|r_n\| = \lim_{n\to\infty} \|r'_n\|$. Man kontrollerar enkelt att $\| \ \|$ är en kvasinorm på $\widehat{R}$, dvs att villkoren (9.1)(a) – (d) är uppfyllda (observera att en norm på R ger en norm på $\widehat{R}$).

Ringen $\widehat{R}$ med kvasinormen $\| \ \|$ kallar man för **kompletteringen av R med avseende på** $\| \ \|$. Vi har en naturlig homomorfism

$$\iota : R \to \widehat{R},$$

där $\iota(r) = \overline{\{r_n\}}$ med $r_n = r$ för alla n. Bilden av r skall vi beteckna med $\{r\}$. Homomorfismen ι behöver inte vara injektiv. Vi har $\iota(r) = 0 \Leftrightarrow \{r\} \in I \Leftrightarrow \|r\| = 0$. Alltså om $\|r\| = 0 \Leftrightarrow r = 0$

så är ι injektiv. I varje fall har vi $\|r\| = \|\{r\}\|$ så att kvasinormen på $\widehat{R}$ förlänger den på R. □

Vårt nästa resultat visar att kompletteringen ger en fullständig ring dvs $\widehat{\widehat{R}} = \widehat{R}$.

(9.12) Proposition. *Kompletteringen $(\widehat{R}, \|\ \|)$ av $(R, \|\ \|)$ är en fullständig ring dvs om $\{\rho_k\}_{k=1}^{\infty}, \rho_k \in \widehat{R}$, är en följd som uppfyller Cauchys villkor så är den konvergent dvs det finns $\rho \in \widehat{R}$ så att $\lim_{k\to\infty} \rho_k = \rho$. Dessutom är R tät i $\widehat{R}$ dvs varje element i $\widehat{R}$ är ett gränsvärde av en följd bestående av element i R.*

Bevis. Först observerar vi att om $\rho \in \widehat{R}$, $\rho = \overline{\{r_n\}}$ så är $\rho = \lim_{k\to\infty}\{r_k\}_{n=1}^{\infty}$ (observera att $\{r_k\}_{n=1}^{\infty}$ betecknar en följd som har alla termer lika med r_k). I själva verket har vi

$$\|\rho - \{r_k\}_{n=1}^{\infty}\| = \|\overline{\{r_n - r_k\}}\| = \lim_{n\to\infty} \|r_n - r_k\|.$$

Alltså är $\lim_{k\to\infty} \|\rho - \{r_k\}_{n=1}^{\infty}\| = \lim_{k\to\infty} \lim_{n\to\infty} \|r_n - r_k\| = 0$ ty $\{r_n\}_{n=1}^{\infty}$ uppfyller Cauchys villkor. Detta visar att R är tät i $\widehat{R}$. Antag nu att $\rho_k = \overline{\{r_{nk}\}}_{n=0}^{\infty}$, $r_{nk} \in R$. Vi vet att $\rho_k = \lim_{n\to\infty}\{r_{nk}\}$. Låt oss välja $r_k \in R$ så att $\|\rho_k - \{r_k\}\| < \frac{1}{k}$ (t ex kan r_k väljas som r_{nk} för ett lämpligt n). Följden $\{\rho_k\}$ uppfyller Cauchys villkor så att följden $\{r_k\}_{k=1}^{\infty}$ gör det också. Låt $\rho = \overline{\{r_k\}}$. Nu är $\lim_{k\to\infty} \rho_k = \rho$ ty $\|\rho_k - \rho\| \le \|\rho_k - \{r_k\}\| + \|\{r_k\} - \rho\| \to 0$ därför att $\|\rho_k - \{r_k\}\| < \frac{1}{k}$ och $\lim_{k\to\infty}\{r_k\} = \rho$. □

Låt oss också bevisa följande viktiga observation:

(9.13) Proposition. *Om $\|\ \|$ är en norm på en kropp K så är också $\widehat{K}$ en kropp.*

Bevis. Vi måste visa att om $\rho \in \widehat{K}$ och $\rho \neq 0$ så existerar ρ^{-1}. Låt $\rho = \overline{\{r_n\}}$, $r_n \in K$. Vi kan förutsätta att $r_n \neq 0$ för alla n, ty det finns n_0 så att $r_n \neq 0$ då $n \ge n_0$ och man kan ersätta alla r_n för $n < n_0$ med $r_n = 1$ – om $\{r_n\}$ och $\{r'_n\}$ skiljer sig för ett ändligt antal n så är $\{r_n - r'_n\}$ en 0-följd. Nu påstår vi att $\{\frac{1}{r_n}\}$ är en Cauchy följd. Vi har:

$$\left\| \frac{1}{r_n} - \frac{1}{r_{n'}} \right\| = \frac{\|r_n - r_{n'}\|}{\|r_n\|\|r_{n'}\|} \le \frac{\varepsilon}{E^2},$$

där $\|r_n\| \ge E > 0$ och $\|r_n - r_{n'}\| < \varepsilon$ då $n, n' > N$ ($\lim \|r_n\|$ existerar och är > 0 samt alla $r_n \neq 0$). Det är klart att $\rho^{-1} = \overline{\{\frac{1}{r_n}\}}$ ty $\rho\rho^{-1} = \{1\}$. □

Två efterföljande resultat ger en möjlighet till att beskriva kompletteringar av ringar och kroppar i vissa specialfall. Vi skall använda dessa resultat för att beskriva kompletteringar av $\mathbb{Z}, \mathbb{Q}, K[X]$ och $K(X)$.

(9.14) Proposition. *Låt R vara en fullständig diskret valuationsring med maximalidealet $\mathfrak{m} = (\pi)$. Låt $A \subseteq R$ vara en mängd sådan att $a + \mathfrak{m}, a \in A$, ger alla och olika sidoklasser till $\mathfrak{m}$ i R. Då kan varje element $r \in R$ entydigt skrivas på formen:*

$$r = a_0 + a_1\pi + a_2\pi^2 + \dots,$$

där $a_i \in A$, dvs $r = \lim_{n\to\infty} s_n$, $s_n = a_0 + a_1\pi + \ldots + a_n\pi^n$.

Bevis. Låt $r \in a_0 + \mathfrak{m}$. Då är $r - a_0 = \pi r_1$ dvs $r = a_0 + \pi r_1$. Vidare induktivt: Om $r = a_0 + a_1\pi + \ldots + a_{n-1}\pi^{n-1} + r_n\pi^n$, $r_n \in R$, så är $r_n \in a_n + \mathfrak{m}$, dvs $r_n - a_n = \pi r_{n+1}$, vilket ger $r = a_0 + a_1\pi + \ldots + a_{n-1}\pi^{n-1} + a_n\pi^n + r_{n+1}\pi^{n+1}$. Det är klart att $\{s_n\}$ konvergerar mot r, ty $r - s_n = r_{n+1}\pi^{n+1}$ så att $v(r - s_n) \geq n + 1$ (eller: $\|r - s_n\| \leq \rho^{n+1}$, där $0 < \rho < 1$).

Entydigheten. Antag att $r = a_0 + a_1\pi + \ldots + a_n\pi^n + \ldots = a'_0 + a'_1\pi + \ldots + a'_n\pi^n + \ldots$ så att $s_n + \pi^{n+1}r_{n+1} = s'_n + \pi^{n+1}r'_{n+1}$, där $r_{n+1}, r'_{n+1} \in R$. Antag att $a_0 = a'_0, \ldots, a_{n-1} = a'_{n-1}$. Då är $a_n\pi^n + \pi^{n+1}r_{n+1} = a'_n\pi^n + \pi^{n+1}r'_{n+1}$, vilket ger $a_n + \pi r_{n+1} = a'_n + \pi r'_{n+1}$. Alltså är $a_n - a'_n \in \mathfrak{m}$ så att $a_n + \mathfrak{m} = a'_n + \mathfrak{m}$. Enligt definitionen av A får vi $a_n = a'_n$. □

(9.15) Proposition. *Låt K vara en kropp med en icke-arkimedisk norm $\| \|$ och låt $(\widehat{K}, \| \|)$ vara kompletteringen av $(K, \| \|)$. Låt*

$$R = \{x \in K : \|x\| \leq 1\}, \;\; \mathfrak{m} = \{x \in K : \|x\| < 1\},$$

och

$$\widehat{R} = \{x \in \widehat{K} : \|x\| \leq 1\}, \;\; \widehat{\mathfrak{m}} = \{x \in \widehat{K} : \|x\| < 1\}.$$

Då är $\widehat{R} = \{\overline{\{r_n\}} \in \widehat{K} : r_n \in R\}$ och den naturliga injektionen $R \to \widehat{R}$ inducerar en isomorfism $R/\mathfrak{m} \cong \widehat{R}/\widehat{\mathfrak{m}}$ (se (9.10)).

Bevis. Om $\rho \in \widehat{K}$ och $\rho = \overline{\{r_n\}}$, där $r_n \in R$ så är $\|\rho\| = \lim_{n\to\infty} \|r_n\| \leq 1$ dvs $\rho \in \widehat{R}$. Omvänt. Låt $\rho \in \widehat{R}$ dvs $\rho = \overline{\{x_n\}}$, $x_n \in K$ och $\|\rho\| \leq 1$. Då existerar n_0 så att $\|x_n\| \leq 1$ då $n \geq n_0$. I själva verket är $\|\{x_n\}\| = \|\{x_n\} - \rho + \rho\| \leq \max(\|\{x_n\} - \rho\|, \|\rho\|) \leq 1$ då $n \geq n_0$ ty $\|\{x_n\} - \rho\| \to 0$ då $n \to \infty$. (jfr bevis för (9.12)). Alltså är $\rho = \overline{\{r_n\}}$, där $r_n = 0$, $n < n_0$ och $r_n = x_n$ då $n \geq n_0$ så att första påståendet är bevisat.

Låt nu $\rho = \overline{\{r_n\}} \in \widehat{R}$ och $r_n \in R$. Välj $r \in R$ så att $\|\rho - \{r\}\| < 1$ (jfr bevis (9.12)). Definiera $\varphi : \widehat{R} \to R/\mathfrak{m}$ så att $\varphi(\rho) = r + \mathfrak{m}$. Definitionen är korrekt ty om $\|\rho - \overline{\{r'\}}\| < 1$ så är $\|r - r'\| = \|r - \rho + \rho - r'\| \leq \max(\|r - \rho\|, \|\rho - r'\|) < 1$ dvs $r - r' \in \mathfrak{m}$. Om $\|\rho_1 - \overline{\{r_1\}}\| < 1$ och $\|\rho_2 - \overline{\{r_2\}}\| < 1$ så är $\|\rho_1 + \rho_2 - \overline{\{r_1 + r_2\}}\| < 1$ och $\|\rho_1\rho_2 - \overline{\{r_1r_2\}}\| < 1$ (enkla uppskattningar av $\| \|$) så att $\varphi : \widehat{R} \to R/\mathfrak{m}$ är en ringhomomorfism. Det är klart att φ är surjektiv (välj $\rho = \overline{\{r\}}$). $R/\mathfrak{m}$ är en kropp så att Kerφ är ett maximalideal i frn lokala ringen $\widehat{R}$ (se (9.10)). Alltså är Ker$\varphi = \widehat{\mathfrak{m}}$ (se (9.10)), vilket ger $\widehat{R}/\widehat{\mathfrak{m}} \cong R/\mathfrak{m}$. □

(9.16) Exempel. (a) Om $\|x\| = |x|$ då $x \in \mathbb{Q}$ så är $\widehat{\mathbb{Q}} = \mathbb{R}$.

(b) Låt $\| \, \|_p$ vara den p-adiska normen på $\mathbb{Q}$. Kompletteringen av $\mathbb{Q}$ med avseende på $\|x\|_p$ kallas kroppen av **de p-adiska talen** och kommer att betecknas med $\widehat{\mathbb{Q}}_p$. $\widehat{\mathbb{Z}}_p = \{x \in \widehat{\mathbb{Q}}_p : \|x\|_p \leq 1\}$ kallas ringen av **de p-adiska heltalen**. $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : \|x\|_p \leq 1\}$ är lokaliseringen av $\mathbb{Z}$ med avseende på (p) och $\widehat{\mathbb{Z}}_p = \{x \in \widehat{\mathbb{Q}}_p : \|x\|_p \leq 1\}$ är kompletteringen av $\mathbb{Z}_{(p)}$. Ringen $\widehat{\mathbb{Z}}_p$ är en diskret valuationsring (se (9.10)) och p (mera exakt $\overline{\{p\}}$) genererar dess maximalideal (se bevis (9.10)). Man har $\widehat{\mathbb{Z}}_p/(p) \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/(p)$ så att $0, 1, \ldots, p-1$ kan väljas som representanterna av alla sidoklasser. Enligt (9.14) får vi att elementen i $\widehat{\mathbb{Z}}_p$ är

$$a_0 + a_1 p + a_2 p^2 + \ldots, \quad \text{där} \quad a_i \in \{0, 1, \ldots, p-1\}.$$

Observera att varje element i $\widehat{\mathbb{Z}}_p$ kan också beskrivas som $\rho = \overline{\{r_n\}}$ där $r_n \in \mathbb{Z}$ med $r_n = a_0 + a_1 p + \ldots + a_n p^n$ (den sista slutsatsen får man i efterhand men det är mycket lätt att visa direkt att för varje $x \in \mathbb{Z}_{(p)}$ (dvs $x = \frac{m}{n}$, $p \nmid n$) och $\varepsilon > 0$ finns det $a \in \mathbb{Z}$ så att $\|x - a\|_p < \varepsilon$). Gruppen $\widehat{\mathbb{Z}}_p^*$ av alla enheter i $\widehat{\mathbb{Z}}_p$ består av $\varepsilon = a_0 + a_1 p + a_2 p^2 + \ldots$ sådana att $a_0 \neq 0$ och varje nollskilt element i $\widehat{\mathbb{Z}}_p$ kan skriva entydigt som produkt εp^n, där $\varepsilon \in \widehat{\mathbb{Z}}_p^*$ och $n \geq 0$. Alltså kan varje nollskilt element i $\widehat{\mathbb{Q}}_p$ skrivas entydigt på formen εp^n, där $\varepsilon \in \widehat{\mathbb{Z}}_p^*$ och $n = 0, \pm 1, \pm 2, \ldots$.

(c) På liknande sätt får vi att kompletteringena av $\mathbb{C}[X]$ med avseende på $\| \, \|_p$, där $p = X$, är ringen $\mathbb{C}[[X]]$ av formella potensserierna. Kompletteringen av $\mathbb{C}(X)$ är kvotkroppen av $\mathbb{C}[[X]]$ som betecknas med $\mathbb{C}((X))$ – det är kroppen av formella Laurentserier (se Övn. 11).

□

ÖVNINGAR

9.1. Låt $\| \|$ vara en kvasinorm på R och $I = \{x \in R : \|x\| = 0\}$.

(a) Visa att I är ett ideal i R.

(b) Visa att om man definierar $\|\bar{x}\| = \|x\|$, där $\bar{x} = x + I$, så får man en väldefinierad kvasinorm på R/I som uppfyller (9.1)(a′).

9.2. Låt $\| \|$ vara en icke-arkimedisk norm på R. Låt $x, y \in R$ och antag att $\|x\| \neq \|y\|$. Visa att $\|x + y\| = \max(\|x\|, \|y\|)$.

9.3. (a) Visa att $(3, 34, 334, 3334, \ldots)$ är lika med $2/3$ i $\widehat{\mathbb{Z}}_5$.

(b) Bestäm den 2-adiska utvecklingen av $2/3$. Är detta ett heltal i $\widehat{\mathbb{Q}}_2$?

(c) Bestäm de första 4 siffrorna av $\sqrt{-1}$ i $\widehat{\mathbb{Q}}_{13}$.

9.4. Låt v vara en icke-trivial valuation på $K(X)$ som är trivial på K (dvs $v(a) = 0$ då $a \in K^*$). Visa att v är diskret och under förutsättningen att $v(K(X)^*) = \mathbb{Z}^+$ visa att v sammanfaller med en av valuationerna v_p, v_∞ ur (9.17).

Ledning. Låt $R_v = \{\varphi \in K(X) : v(\varphi) \geq 0\}, \mathfrak{m}_v = \{\varphi \in K(X) : v(\varphi) > 0\}$. Motivera att R_v är en lokal ring med maximalidealet $\mathfrak{m}_v$ (se (9.10)). Antag först att $v(X) \geq 0$. Då är $R_v \supset K[X]$. Låt $\mathfrak{m}_v \cap K[X] = (p)$. Visa att $R_v = K[X]_{(p)}$ och $v(p) = 1$. Antag därefter att $v(X) < 0$. Visa att $R_v \supset K[\frac{1}{X}]$ och motivera att $R_v = K[\frac{1}{X}]_{(\frac{1}{X})}$ så att $v = v_\infty$.

9.5. En delgrupp $G \neq (0)$ till $\mathbb{R}^+$ kallas diskret om för varje $g \in G$ existerar ett intervall (a, b) sådant att $(a, b) \cap G = \{g\}$. Visa att G är en oändlig cyklisk grupp (dvs $G = \{nr_0,\ n \in \mathbb{Z}, r_0 \neq 0\}$).

9.6. Låt $\| \|$ vara en norm på en ring R. Låt vidare R^* vara en ring som är fullständig m.a.p. en norm $\| \|'$. Antag att $R^* \supseteq R$ och $\|r\|' = \|r\|$ då $r \in R$. Visa att om R är tät i R^* (dvs varje element i R^* är ett gränsvärde av en följd $\{r_n\}$, $r_n \in R$ m.a.p. $\| \|'$) så är $(R^*, \| \|')$ R-isomorf med $(\widehat{R}, \| \|)$ dvs det finns en isomorfism $\varphi : R^* \to \widehat{R}$ sådan att $\varphi(r) = r$ då $r \in R$ och $\|r\|' = \|\varphi(r)\|$ då $r \in R^*$.

9.7. Betrakta en kommutativ ring R som topologiskt rum med topologin definierad av en norm $\| \|$ (se (9.3)(c)), och $R \times R$ som topologiskt rum med produkttopologin. Visa att addition och multiplikation i R är kontinuerliga som funktioner från $R \times R$ till R.

9.8. (a) Visa att $\mathbb{Z}$ är tät i $\mathbb{Z}_{(p)}$ m.a.p. normen $\| \|_p$ (dvs till varje $\frac{m}{n} \in \mathbb{Z}_{(p)}$ och $\varepsilon > 0$ existerar ett heltal a så att $\|\frac{m}{n} - a\|_p < \varepsilon$).

(b) Genom att utnyttja (a) visa att $\mathbb{Z}$ är tät i $\widehat{\mathbb{Z}}_p$

9.9. Visa att kroppen av de p-adiska talen $\mathbb{Q}_p$ är lokalt kompakt, men inte kompakt.

9.10. Låt v_x vara valuationen av $K(X)$ definierad av polynomet X i $K[X]$ (se (7.17)) och $K(X)^\wedge$ kompletteringen av $K(X)$ med avseende på en norm definierad av v_X. Visa att $K[X]^\wedge = K[[X]]$ och $K(X)^\wedge = K((X))$ är kroppen av de formella Laurent potensserier (= kvotkroppen av $K[[X]]$).

Ledning. Visa att $K[X]$ är tät i $K[X]_{(X)}$ (m.a.p. $\| \|_X$). Utnyttja därefter Övn. 7 för att visa att $K[X]$ är tät i $\widehat{R} = \{\varphi \in K(X)^\wedge : \|\varphi\|_X \leq 1\}$. Motivera att $\widehat{R}/m \cong K$ ($\mathfrak{m} = \{\varphi \in K(X)^\wedge : \|\varphi\|_X < 1\}$ och utnyttja (9.15).

9.11. Visa direkt att $K[[X]]$ med normen $\|\varphi\| = \rho^k$ om $\varphi = a_k X^k + a_{k+1}X^{k+1} + \ldots$, $a_k \neq 0$ ($0 < \rho < 1$) är kompletteringen av $K[X]$ med avseende på $\| \|$ (begränsad till $K[X] \subset K[[X]]$).

9.12. Låt $R \subseteq R'$ och låt $\| \|$ vara en kvasinorm på R'. Visa att $\widehat{R}$ kan betraktas som en delring till $\widehat{R}'$ (definiera en naturlig injektion).

9.13. Låt R vara en ring med kvasinorm $| |$ och M en R-modul. Man säger att $\| \|$ är en kvasinorm på R-modulen M om $\|m\| > 0$, $\|m_1 + m_2\| \leq \|m_1\| + \|m_2\|$, $\|m\| = \| - m\|$ och $\|rm\| \leq |r|\|m\|$ då $m, m_1, m_2 \in M$, $r \in R$.

(a) Definiera kompletteringen $\widehat{M}$ m.a.p. $\| \|$ (konstruktionen liknar konstruktionen av $\widehat{R}$).

(b) Visa att $\widehat{M}$ är en $\widehat{R}$-modul då man definierar $\overline{\{r_n\}}\ \overline{\{m_n\}} = \overline{\{r_n m_n\}}$, där $\overline{\{r_n\}} \in \widehat{R}$ och $\overline{\{m_n\}} \in \widehat{M}$ är klasser av Cauchy-följder (man måste visa att definitionen är korrekt).

9.14. Låt I vara ett ideal i R och låt M vara en R-modul. Man definierar den I-adiska normen av M på följande sätt: Låt $M^* = \bigcap_{n=0}^{\infty} I^n M$ och $0 < \rho < 1$.) Om $m \in M^*$ låt $\|m\| = 0$. Om $m \notin M$ så existerar n så att $m \in I^n M \setminus I^{n+1}M$. Då definierar man $\|m\| = \rho^n$.

(a) Visa att $\| \|$ är en kvasinorm på R-modulen M då R betraktas med den I-adiska normen (se (9.2)(d)).

(b) Låt $f : M \to N$ vara en homomorfism av R-moduler. Visa att f definierar en $\widehat{R}$-homomorfism $\widehat{f} : \widehat{M} \to \widehat{N}$.

Anmärkning. Man får enligt (a) och (b) en funktor från R-moduler till $\widehat{R}$-moduler. Man kan visa att i fall $0 \to M' \to M \to M'' \to 0$ är en exakt följd av ändligt genererade R-moduler över en noethersk ring så är följden

$$0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$$

också exakt. Men bevis av den egenskapen är inte lika enkelt som för lokalisering (se (9.13)). Man kan visa att om R är noethersk så är $\widehat{R}$ noethersk (I-adisk komplettering). Detta bevis är också väsentligt svårare än beviset att lokalisering av en noethersk ring är noethersk.

9.15. Låt R_1, R_2 vara två diskreta valuationsringar sådana att $R_1 \subseteq R_2$ och $\mathfrak{m}_1 = R_2 \cap \mathfrak{m}_2$, där $\mathfrak{m}_i$ är maximalidealet i R_i. Visa att $R_1 = R_2$.

Kapitel 10

ALGEBRAISKA MÄNGDER I PROJEKTIVA RUM

Redan i kapitel 2 introducerade vi affina algebraiska mängder som därefter kunde användas för att berika olika algebraiska begrepp med geometrisk tolkning. Algebraisk geometri, som är en mycket central del av algebran, studerar algebraiska mängder (dvs lösningsmängder till polynomekvationer) med hjälp av mycket varierande metoder. Den mest fundamentala metod som något sporadiskt användes redan av I. Newton och L. Euler, men etablerades av G. Monge i slutet av 1700–talet är att komplettera affina algebraiska mängder med "oändliga" punkter i projektiva rum. En sådan utvidgning av en affin algebraisk mängd till en projektiv innebär att man får ett fullständigt objekt (även i topologisk mening) vars egenskaper är mycket lättare att beskriva. Vi har valt här en något ovanlig metod att motivera behovet av projektivisering genom ett viktigt samband mellan punkter på affina kurvor och valuationer av deras funktionskroppar. Kapitlet har en preliminär och översiktlig karaktär. Flera bevis har utelämnats. I appendix förklarar vi hur projektiva mångfalder förhåller sig till det allmänna mångfaldsbegreppet.

(10.1) Exempel. Vi vet att alla normer av $\mathbb{C}(X)$ triviala på $\mathbb{C}$ ges av $\| \ \|_p$ och $\| \ \|_\infty$ (se (9.2)(c) och (9.7)). De kan beskrivas på följande sätt:

$$\|\varphi\|_p = \rho^{v_p(\varphi)} \quad \text{då } \varphi \neq 0 \quad \text{och} \quad \|0\|_p = 0 \quad (0 < \rho < 1),$$

där $(p) = (X - a)$ är ett maximalideal i $\mathbb{C}[X]$ och för

$$\varphi = (X-a)^k \frac{g}{h}, \quad \text{där} \quad g(a) \neq 0 \neq h(a)$$

är $v_p(\varphi) = k$, dvs k är multipliciteten av a som ett nollställe eller en pol till φ samt

$$\|\varphi\|_\infty = \rho^{v_\infty(\varphi)} \quad \text{då} \quad \varphi \neq 0 \quad \text{och} \quad \|0\|_\infty = 0 \quad (0 < \rho < 1),$$

där $v_\infty(\varphi) = \deg(h) - \deg(g)$ om $\varphi = \frac{g}{h}$. Valuationerna v_p svarar en-entydigt mot olika komplexa tal $a \in \mathbb{C}$. Hur kan man förklara närvaron av v_∞? Vi har

$$\varphi(X) = \frac{a_n X^n + \cdots + a_0}{b_m X^m + \cdots + b_0} = \left(\frac{1}{X}\right)^{n-m} \frac{a_n + a_{n-1}(\frac{1}{X}) + \cdots + a_0(\frac{1}{X})^n}{b_m + b_{m-1}(\frac{1}{X}) + \cdots + b_0(\frac{1}{X})^m}$$

och $v_\infty(\varphi) = n - m$ dvs $v_\infty(\varphi)$ säger om multipliciteten av ∞ som ett nollställe eller en pol till φ. På det sättet får vi att alla valuationer på $\mathbb{C}(X)$ svarar en-entydigt mot alla punkter på Riemannsfären (= det utvidgade komplexa planet $\mathbb{C} \cup \{\infty\}$)[†].

Om man t ex betraktar parabeln $V = \{(x, y) \in \mathbb{C}^2 : y = x^2\}$, ringen av de reguljära funktionerna på denna $\mathbb{C}[V] = \mathbb{C}[x, y] = \mathbb{C}[x]$ (ty $y = x^2$) och dess kvotkropp $\mathbb{C}(V) = \mathbb{C}(x)$ så får man exakt samma situation: alla punkter på V definierar alla valuationer av $\mathbb{C}(V)$ utom en – punkten (a, a^2) svarar mot idealet $(x - a) \subset \mathbb{C}[x]$ som definierar den diskreta valuationsringen $\mathbb{C}[X]_{(X-a)}$. Vi saknar en valuation v_∞. Detta visar att det borde finnas en punkt till på parabeln. Hur kan man definiera den punkten? Den naturliga lösningen (som svarar mot kompletteringen av $\mathbb{C}$ med ∞) visar sig vara övergången till projektiva rum (observera att parabeln ligger i $\mathbb{C}^2$ ej i $\mathbb{C}$!).

□

(10.2) Definition. Låt K vara en kropp. Med **projektiva rummet** $\mathbb{P}^n(K)$ menar man mängden av ekvivalensklasser av alla uppsättningar $(x_0, \ldots, x_n)$, $x_i \in K$, sådana att inte alla $x_i = 0$ och $(x_0, \ldots, x_n)$ är ekvivalent med $(x'_0, \ldots, x'_n)$ då och endast då det finns $a \in K$, $a \neq 0$, så att $x'_i = ax_i$. Ekvivalensklasser kallas **punkter** och kommer att betecknas med $(x_0; x_1; \ldots; x_n)$. x_i kallas **projektiva koordinater**.

Om $F(X_0, \ldots, X_n)$ är ett homogent polynom så säger man att $(x_0; \ldots; x_n)$ är ett nollställe till F (en lösning till $F = 0$) om $F(x_0, \ldots, x_n) = 0$ (lägg märke till at $F(ax_0, \ldots, ax_n) = a^{\deg F} F(x_0, \ldots, x_n)$ så att definitionen enbart beror på punkten).

Med en **projektiv algebraisk mångfald** V i $\mathbb{P}^n(K)$ menar man mängden av alla punkter $(x_0; \ldots; x_n) \in \mathbb{P}^n(K)$ som uppfyller ett homogent ekvationssystem $F_i = 0$, $i \in I$ (I är en indexmängd).

□

[†]Egentligen får man en en-entydig motsvarighet mellan alla diskreta valuationsringar i $\mathbb{C}(X)$ som innehåller $\mathbb{C}$ och punkterna på Riemannsfären. Två icke-arkimediska normer kallas ekvivalenta om deras lokala ringar är identiska (se (9.10)). Olika ρ, $0 < \rho < 1$, definierar olika $\| \ \|$, men samma valuationsring $R = \{\varphi \in \mathbb{C}(V) : \|\varphi\| \leq 1\}$.

(10.3) Exempel. (a) Betrakta $\mathbb{P}^2(K)$. Alla punkter $(x_0; x_1; x_2)$ med $x_0 \neq 0$ kan representeras av $(1, \frac{x_1}{x_0}, \frac{x_2}{x_0})$. Om $\frac{x_1}{x_0} = x$, $\frac{x_2}{x_0} = y$, så svarar punkten $(1, x, y)$ mot punkten $(x, y) \in K^2$, och omvänt, mot $(x, y) \in K^2$ svarar punkten $(1, x, y) \in \mathbb{P}^2(K)$. På det sättet kan K^2 betraktas som en delmängd till $\mathbb{P}^2(K)$. Det finns 3 naturliga delmängder: $U_i = \{(x_0; x_1; x_2); x_i \neq 0\}$, $i = 0, 1, 2$. Dessa tre mängder täcker hela $\mathbb{P}^2(K)$. Varje U_i kan identifieras med K^2. Samma sak gäller $\mathbb{P}^n(K)$ som kan täckas av $(n + 1)$ mängder $U_i = \{(x_0; \ldots; x_n) : x_i \neq 0\}$ för $i = 0, 1, \ldots, n$ och punkterna i U_i svarar en–entydigt mot punkterna i K^n.

(b) Betrakta den projektiva linjen $\mathbb{P}^1(\mathbb{C})$ över $\mathbb{C}$. Här har vi $\mathbb{P}^1(\mathbb{C}) = U_0 \cup U_1$, där U_0 består av alla punkter $(1, \frac{x_1}{x_0})$ med $x_0 \neq 0$, och U_1 av alla $(\frac{x_0}{x_1}, 1)$ med $x_1 \neq 0$. Om $x = \frac{x_1}{x_0}$ så kan U_0 identifieras med $\mathbb{C}^1$ (genom $(1, \frac{x_1}{x_0}) \mapsto x$). Det finns endast en punkt i U_1 som inte finns i U_0 – punkten $(0, 1)$ ("punkten ∞"). $\mathbb{P}^1(\mathbb{C})$ kan uppfattas som Riemannsfären. Dess punkter svarar en–entydigt mot alla valuationer av $\mathbb{C}(X)$ som är triviala på $\mathbb{C}$.

(c) Låt (A^{ij}) vara Plückerkoordinaterna av ett r-dimensionellt delrum till ett vektorrum V över en kropp K, där $\dim_K V = n$. Enligt Övn. 5.6 och 5.7 svarar (A^{ij}) mot punkter i ett projektivt rum (vars dimension är $\binom{n}{r} - 1$). T ex får man för $n = 4, r = 2$, $(A^{12}; A^{13}; A^{14}; A^{23}; A^{24}; A^{34}) \in \mathbb{P}^5(K)$. Dessa punkter bildar en projektiv mångfald med ekvationen $X^{12}X^{34} - X^{13}X^{24} + X^{14}X^{23} = 0$ (se Övn. 5.7 (c)) (lösningarna svarar en–entydigt mot linjer i $\mathbb{P}^3(K)$). För godtyckliga r, n får man projektiva mångfalder – de kallas **Grassmannmångfalder**.

(d) Låt $V = \{(x, y) \in \mathbb{C} : y = x^2\}$. Parabeln V i $\mathbb{C}^2$ definierar en punktmängd i $\mathbb{P}^2(\mathbb{C})$. Man kan inbädda parabeln i $\mathbb{P}^2(\mathbb{C})$ som mängden av alla punkter $(1, x, y)$ med $y = x^2$. Det finns ett irreducibelt homogent polynom $F(X_0, X_1, X_2)$ som har bland sina nollställen alla punkter $(1, x, y)$, $y = x^2$. Det är lätt att hitta ett sådant: $X_0X_2 - X_2^1 = 0$ (det är entydigt bestämt så när som på en faktor ur $\mathbb{C}^*$ – se (e) nedan). Nu frågar vi om alla punkter som uppfyller ekvationen $X_0X_2 - X_2^1 = 0$. Om $x_0 \neq 0$ så kan vi välja $x_0 = 1$ och vi har alla punkter $(1, x_1, x_2)$ med $x_2 = x_1^2$. Om $x_0 = 0$ så måste $x_1 = 0$. Vi väljer då t ex $x_2 = 1$ dvs punkten $(0, 0, 1)$ – "punkten i ∞" på parabeln (den "saknade" punkten i samband med vår diskussion av normer i början av detta kapitel).

(e) Låt K vara en algebraiskt sluten kropp och $V = \{(x, y) \in K^2 : F(x, y) = 0\}$, där F är ett irreducibelt polynom i $K[X, Y]$. V är en irreducibel kurva i K^2 som kan inbäddas i $\mathbb{P}^2(K)$ genom $(x, y) \mapsto (1, x, y)$. Man hittar det irreducibla homogena polynom $\bar{F}$ som bland sina nollställen har alla nollställen till $F(X, Y) = 0$ på följande sätt:

$$\bar{F}(X_0.X_1, X_2) = X_0^{\deg F} F\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right).$$

Kurvan $\bar{V} = \{(x_0; x_1; x_2) \in \mathbb{P}^2(K) : \bar{F}(x_0, x_1, x_2) = 0\}$ kallas **projektiva höljet** till V. $\bar{F}$ är entydigt bestämt av F så när som på en faktor ur K^* (bevis är enkelt – man kan t ex utnyttja Nullstellensatz). T ex definierar den elliptiska kurvan $Y^2 = X^3 + aX + b$ i $\mathbb{C}^2$ kurvan $X_0X_2^2 = X_1^3 + aX_0^2X_1 + bX_0^3$ i $\mathbb{P}^2(\mathbb{C})$ – den enda punkt som skiljer dessa kurvor är $(0, 0, 1)$.

Den affina kurvan $X^3 + Y^3 = 1$ i $\mathbb{C}^2$ definierar $X_1^3 + X_2^3 = X_0^3$ i $\mathbb{P}^2(\mathbb{C})$ med 3 nya punkter: $(0, 1, \varepsilon)$, där $\varepsilon^3 = -1$.

□

Det faktum att det finns en en–entydig motsvarighet mellan alla punkter på Riemannsfären och alla valuationsringar i $\mathbb{C}(X)$ som innehåller $\mathbb{C}$ är ett specialfall av följande resultat:

(10.4) Sats. *Låt $V = \{(x, y) \in \mathbb{C}^2 : F(x, y) = 0\}$ vara ett irreducibelt kurva och $\bar{V}$ dess projektiva hölje i $\mathbb{P}^2(\mathbb{C})$ som är icke-singulär (dvs kurvorna $U_i \cap V$, $i = 0, 1, 2$ är icke-singulära – se (8.11)). Då finns det en en–entydig motsvarighet mellan alla punkter på $\bar{V}$ och alla diskreta valuationsringar med kvotkroppen $\mathbb{C}(V)$ som innehåller $\mathbb{C}$.*

(10.5) Anmärkning. Ekvationen $F(x, y) = 0$ definierar y som en algebraisk funktion av x. Den kompakta Riemannyta som svarar mot den funktionen är just $\bar{V}$ (se vidare (10.6)(b)).

□

Bevis. Låt $\mathbb{C}[x, y] = \mathbb{C}[X, Y]/(F(X, Y))$ vara ringen av de reguljära funktionerna på V och låt $\mathbb{C} \subset R \subset \mathbb{C}(x, y)$, där R är en diskret valuationsring. Antag först att $x, y \in R$ så att $R \supseteq \mathbb{C}[x, y]$. Låt $\mathfrak{m}$ vara maximalidealet i R. Då är $\mathfrak{m} \cap \mathbb{C}[x, y] \neq (0)$ ty $\mathfrak{m} \cap \mathbb{C}[x, y] = (0)$ ger att alla nollskillda element i $\mathbb{C}[x, y]$ har inverser i R (R är lokal!) så att $\mathbb{C}(x, y) \subseteq R$ – en motsägelse. Men $\dim \mathbb{C}[x, y] = 1$ (se (7.15)) så att $\mathfrak{m} \cap \mathbb{C}[x, y]$ är ett maximalideal i $\mathbb{C}[x, y]$. Enligt Nullstellensatz är $\mathfrak{m} \cap \mathbb{C}[x, y] = (x - a, y - b)$ för lämpliga $a, b \in \mathbb{C}$ så att $(X - a, Y - b) \supseteq (F(X, Y))$ i $\mathbb{C}[X, Y]$ dvs $F(a, b) = 0$. Nu är det lätt att bevisa likheten $R = \mathbb{C}[x, y]_{\mathfrak{m}_{(a,b)}}$, där $\mathfrak{m}_{(a,b)} = \mathfrak{m} \cap \mathbb{C}[x, y]$ (se Övn. 9.16). Detta visar att varje R med $x, y \in R$ definierar entydigt en punkt $(a, b) \in V$.

Betrakta nu ekvationen $\bar{F}(x_0, x_1, x_2) = 0$ för $\bar{V} \subseteq \mathbb{P}^2(\mathbb{C})$. Punkterna på V svarar en–entydigt mot punkterna på $\bar{V} \cap U_0$ och $F(X, Y) = \bar{F}(1, X, Y)$ (se (10.3)(e)). Vi skall identifiera V med $\bar{V} \cap U_0$ (dvs identifiera (x, y) med $(1, x, y)$) och betrakta $F(X, Y) = \bar{F}(1, X, Y) = 0$ som ekvationen för $\bar{V} \cap U_0$.

Betrakta nu $\bar{V} \cap U_1$. Den kurvan har ekvationen $F_1(X, Y) = \bar{F}(X, 1, Y)$ då punkten $(x, 1, y) \in \bar{V} \cap U_1$ identifieras med (x, y) ($(x, 1, y) \in \bar{V} \cap U_1 \Leftrightarrow \bar{F}(x, 1, y) = F_1(x, y) = 0$). Kurvan $F_1(X, Y) = 0$ är irreducibel (som övning visa att polynomet F_1 är irreducibelt i $\mathbb{C}[X, Y]$ därför att F är irreducibelt). Ringen av de reguljära funktionerna på denna kurva är $\mathbb{C}[\bar{V} \cap U_1] = \mathbb{C}[X, Y]/(F_1) \cong \mathbb{C}[\frac{1}{x}, \frac{y}{x}]$ (observera att $F_1(\frac{1}{x}, \frac{y}{x}) = \bar{F}(\frac{1}{x}, 1, \frac{y}{x}) = (\frac{1}{x})^{\deg F} F(x, y) = 0$. Därefter betrakta homomorfismen $\mathbb{C}[X, Y] \xrightarrow{\varphi} \mathbb{C}(x, y)$, där $X \mapsto x$ och $Y \mapsto y$.). Enligt resonemanget i början av beviset svarar punkterna på $\bar{V} \cap U_1$ en–entydigt mot alla diskreta valuationsringar R sådana att $\mathbb{C}[\bar{V} \cap U_1] \subset R \subset \mathbb{C}(\frac{1}{x}, \frac{y}{x}) = \mathbb{C}(x, y)$.

På liknande sätt betraktar man $\bar{V} \cap U_2$ som är en kurva med ekvationen $F_2(X, Y) = \bar{F}(X, Y, 1)$. Den är irreducibel och $\mathbb{C}[\bar{V} \cap U_2] = \mathbb{C}[X, Y]/(F_2) \cong \mathbb{C}[\frac{x}{y}, \frac{1}{y}]$. Punkterna på $\bar{V} \cap U_2$ svarar en–

entydigt mot alla diskreta valuationsringar R sådana att $\mathbb{C}[\bar{V} \cap U_2] \subset R \subset \mathbb{C}(\frac{x}{y}, \frac{1}{y}) = \mathbb{C}(x, y)$.

Nu observerar vi följande viktiga egenskap: R måste innehålla x, y eller $\frac{1}{x}, \frac{y}{x}$ eller $\frac{x}{y}, \frac{1}{y}$ dvs R definierar exakt en punkt på $\bar{V}$. Om man antar att t.ex. $x \notin R$ så $1/x \in R$ (se (9.9)). Om $y \in R$ så är $\frac{1}{x}, \frac{y}{x} \in R$. Om även $y \notin R$ så $1/y \in R$. Men $\frac{x}{y} \in R$ eller $\frac{y}{x} \in R$ så att R innehåller $\frac{1}{x}, \frac{y}{x}$ eller $\frac{1}{y}, \frac{x}{y}$.

Omvänt, om $P \in \bar{V}$ så tillhör P unionen $(\bar{V} \cap U_0) \cup (\bar{V} \cap U_1) \cup (\bar{V} \cap U_2)$ dvs P definierar ett maximalideal i (minst) en av ringarna $\mathbb{C}[x, y]$, $\mathbb{C}[\frac{1}{x}, \frac{y}{x}]$ eller $\mathbb{C}[\frac{x}{y}, \frac{1}{y}]$. Lokalisering ger då en diskret valuationsring $R = \mathcal{O}_p$ med kvotkroppen $\mathbb{C}(x, y)$ (se (8.12)). Observera att R är oberoende av vilken av de tre ringarna man lokaliserar om P tillhör olika snitt $\bar{V} \cap U_i$) ($P = (a_0, a_1, a_2)$ ger $(x - \frac{a_1}{a_0}y - \frac{a_2}{a_0})$ i $\mathbb{C}[x, y]$ då $a_0 \neq 0$. $(\frac{1}{x} - \frac{a_0}{a_1}, \frac{y}{x} - \frac{a_2}{a_1})$ i $\mathbb{C}[\frac{1}{x}, \frac{y}{x}]$ då $a_1 \neq 0$ och $(\frac{x}{y} - \frac{a_1}{a_2}, \frac{1}{y} - \frac{a_0}{a_2})$ i $\mathbb{C}[\frac{x}{y}, \frac{1}{y}]$ då $a_2 \neq 0$. Om t ex $a_0 a_1 \neq 0$ så får man $\mathbb{C}[x, y]_{(x-a, y-b)} = \mathbb{C}[\frac{1}{x}, \frac{y}{x}]_{(\frac{1}{x} - \frac{1}{a}, \frac{y}{x} - \frac{b}{a})}$, där $a = \frac{a_1}{a_0}$, $b = \frac{a_2}{a_0}$.) □

Hittills har vi enbart diskuterat irreducibla plana kurvor dvs kurvor som kan beskrivas i $\mathbb{C}^2$ med hjälp av en irreducibel ekvation $F(X, Y) = 0$ eller motsvarande $\bar{F}(X_0, X_1, X_2) = 0$ i $\mathbb{P}^2(\mathbb{C})$ (se (10.3)(e)). Mera allmänt, låt $V \subseteq \mathbb{C}^n$ vara en irreducibel algebraisk mångfald. Man säger att V är en kurva om $\dim \mathbb{C}[V] = 1$, yta då $\dim \mathbb{C}[V] = 2$ osv. En övergång från affina rum $\mathbb{C}^n$ till projektiva $\mathbb{P}^n(\mathbb{C})$ är lika naturlig i alla dimensioner – man ersätter ekvationerna $F_i(Y_1, \ldots, Y_n) = 0$, $i \in I$, för V med

$$\bar{F}_i(X_0, \ldots, X_n) = X_0^{\deg F_i} F_i(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) = 0.$$

Dessa ekvationer beskriver

$$\bar{V} = \{(x_0, \ldots, x_n) \in \mathbb{P}^n(\mathbb{C}) : \bar{F}_i(x_0, \ldots, x_n) = 0 \quad \text{för varje } i \in I\}.$$

$\bar{V}$ har en övertäckning med mängderna $\bar{V} \cap U_i$, $i = 0, 1, \ldots, n$ (se (10.3)(a)). Om $P \in \bar{V}$ och $P \in \bar{V} \cap U_i$ så har man den lokala ringen av P på $\bar{V}$: $\mathcal{O}_p = \mathbb{C}[V \cap U_i]_{\mathfrak{m}_p}$, där $\mathfrak{m}_p$ är maximalidealet motsvarande punkten P i $\mathbb{C}[V \cap U_i]$. $\mathcal{O}_p$ är oberoende av i som vi såg i beviset för (10.4) (om P tillhör olika övertäckningsmängder). Man säger att en algebraisk kurva $\bar{V} \subseteq \mathbb{P}^n(\mathbb{C})$ är icke-singulär om varje punkt $P \in \bar{V}$ är icke-singulär dvs $\mathcal{O}_p$ är en diskret valuationsring. Sats (10.4) gäller fortfarande (bevis förändras oväsentligt): $\mathcal{O}_p$ ger precis alla diskreta valuationsringar som innehåller $\mathbb{C}$ och har kvotkroppen $\mathbb{C}(\bar{V}) := \mathbb{C}(\bar{V} \cap U_i)$ (samma $\mathbb{C}(\bar{V})$ oberoende av i – se beviset för (10.4)).

(10.6) Anmärkning. (a) En algebraisk kurva $V = \{(x, y) \in \mathbb{C}^2 : F(x, y) = 0\}$ kan betraktas som en yta över $\mathbb{R}$ – ekvationen $F(x, y) = 0$, $x = a + bi$, $y = c + di$, $a, b, c, d \in \mathbb{R}$, kan ersättas med två ekvationer $F_1(a, b, c, d) = 0$ och $F_2(a, b, c, d) = 0$, där F_1, F_2 är polynom med reella

koefficienter. Dessa beskriver en yta i $\mathbb{R}^4$ (lokalt kan man uttrycka lösningarna med hjälp av två parametrar).

(b) Låt $V = \{(x,y) \in \mathbb{C}^2 : F(x,y) = 0\}$ vara en godtycklig irreducibel kurva. Det finns då en kurva $V^* \subseteq \mathbb{P}^N(\mathbb{C})$ (för ett lämpligt N) sådan att $\mathbb{C}(V^*) = \mathbb{C}(V)$ och V^* är icke-singulär. En algebraisk konstruktion av V^* bygger på att ringarna $\mathbb{C}[\bar{V} \cap U_i], i = 0,1,2$, ersätts man med deras hela höljen i $\mathbb{C}(V)$ (dessa är Dedekindringar enligt (8.16)). En analytisk konstruktion av V^*, som är Riemannytan[†] av den algebraiska funktionen $F(x,y) = a_n(x)y^n + \cdots + a_0(x) = 0$, $a_i(X) \in \mathbb{C}[X]$, bygger på analytisk fortsättning: om $(x_0,y_0) \in \mathbb{C}^2$ är sådan att $F(x_0,y_0) = 0$ och $\frac{\partial F}{\partial y}(x_0,y_0) \neq 0$ så existerar ett område $U_{x_0} \subseteq \mathbb{C}$ och en analytisk funktion $x \mapsto g(x)$, $x \in U_{x_0}$ sådan att $F(x,g(x)) = 0$ i U_{x_0}. Man konstruerar därefter Riemannytan av F genom analytisk fortsättning av paret (U_{x_0}, g). Man får då även en naturlig projektion $V^* \to \mathbb{P}^1(\mathbb{C})$, där $(U_{x_0}, g) \mapsto x_0$ som mycket naturligt kan beskrivas i termerna av den ändliga kroppsutvidgningen $K(x) \subseteq K(x,y)$, där y uppfyller $F(x,y) = 0$ (och motsvarande ringutvidgningar $K[x] \subseteq$ hela höljet till $K[x]$ i $K(x,y)$, $K\,[\frac{1}{x}] \subseteq$ hela höljet till $K[\frac{1}{x}]$ i $K(x,y)$).

□

För orienteringens skull avslutar vi detta kapitel med några satser om algebraiska kurvor. Dessa satser kräver betydligt större utrymme för att kunna presenteras med fullständiga bevis.

(10.7) Definition. Låt V vara en icke-singulär irreducibel algebraisk kurva i $\mathbb{P}^2(\mathbb{C})$. Med en **divisor** på V menar man ett godtyckligt element i den fria abelska gruppen Div (V) som genereras av alla $P \in V$ dvs $D \in$ Div (V) om

$$D = \sum n_P P,$$

där $n_p \in \mathbb{Z}$, $n_p = 0$ för nästan alla $P \in V$. Med **graden** av D menar man:

$$\deg\,(D) = \sum n_p.$$

Om $D = \sum n_P P$ och $D' = \sum n'_P P$ så skriver man $D \geq D'$ om $n_p \geq n'_p$ för varje $P \in V$. Låt v_p beteckna den (diskreta) valuation som svarar mot ringen $\mathcal{O}_p \subset \mathbb{C}(V)$ (se (9.9)). Om $\varphi \in \mathbb{C}(V)$ definierar man **divisorn av** φ:

$$(\varphi) = \sum v_p(\varphi) P.$$

Man skriver $(\varphi)_0 = \sum v_P(\varphi)P$, $v_P(\varphi) > 0$ och $(\varphi)_\infty = -\sum v_P(\varphi)P$, $v_P(\varphi) < 0$. Man säger att $(\varphi)_0$ är **divisorn av nollställen** av φ och $(\varphi)_\infty$ är **divisorn av poler** av φ.

□

[†] $V^* \subseteq \mathbb{P}^n(\mathbb{C})$ är en analytisk mångfald – se Övn. 9.14 för begreppet analytisk mångfald.

Det är klart att

$$(\varphi\psi) = (\varphi) + (\psi) \quad \text{och} \quad (\frac{1}{\varphi}) = -(\varphi), \tag{10.8}$$

ty $v_P(\varphi\psi) = v_P(\varphi) + v_P(\psi)$ och $v_P(1/\varphi) = -v_P(\varphi)$ (se (9.8)). Divisorer (φ) bildar en delgrupp till Div (V). De kallas **huvuddivisorer**.

(10.9) Sats. *Låt $\varphi \in \mathbb{C}(V)$, $\varphi \notin \mathbb{C}$. Då är deg $(\varphi)_0$ = deg $(\varphi)_\infty = [\mathbb{C}(V) : \mathbb{C}(\varphi)]$ så att deg $(\varphi) = 0$.*

(10.10) Definition. Man säger att $D_1, D_2 \in$ Div (V) är **linjärt ekvivalenta** om $D_1 - D_2 = (\varphi)$, där $\varphi \in \mathbb{C}(V)$. Kvotgruppen Div (V) modulo huvuddivisorer kallas gruppen av **divisorklasser** och betecknas med $Cl(V)$ (jfr med (8.14)).

Varje divisor D definierar ett mycket viktigt vektorrum över $\mathbb{C}$:

$$\mathcal{L}(D) = \{\varphi \in \mathbb{C}(V) : (\varphi) + D \geq 0\} \cup \{0\}.$$

□

(10.11) Sats. *$\mathcal{L}(D)$ är ett vektorrum av ändlig dimension över $\mathbb{C}$.*

Dimensionen av $\mathcal{L}(D)$ betecknas med $\ell(D)$. Man definierar $\dim \mathcal{L}(D) = 0$ då $\mathcal{L}(D) = \{0\}$. Det faktum att $\mathcal{L}(D)$ är ett vektorrum visas mycket lätt, däremot är det svårare att visa att dimensionen av detta rum är ändligt.

(10.12) Exempel. Låt $V = \mathbb{P}^1(\mathbb{C}) = U_0 \cup U_1$. Här är $\mathbb{C}(V) = \mathbb{C}(X) \supset \mathbb{C}$ och punkterna $P \in V$ svarar mot alla valuationsringar R sådana att $\mathbb{C} \subset R \subset \mathbb{C}(X)$ (se (9.17)). Vi skall skriva P_a då $P = (1, a) \in \mathbb{P}^1(\mathbb{C})$ och P_∞ då $P = (0, 1)$ och beteckna motsvarande valuationer med v_a, v_∞. Om $\varphi = \frac{x^2+1}{x-1}$ så är

$$(\varphi) = P_i + P_{-i} - P_1 - P_\infty$$

($v_\infty(\varphi) = \deg(x-1) - \deg(x^2-1) = -1$). Låt $D = 2P_\infty$. Då är

$$\mathcal{L}(D) = \{\varphi \in \mathbb{C}(V) : (\varphi) + 2P_\infty \geq 0\} \cup \{0\}.$$

Detta betyder att om $\varphi(x) = \frac{p(x)}{q(x)}$, SGD $(p,q) = 1$ så $v_a(\varphi) \geq 0$ för varje $a \in \mathbb{C}$ och $v_\infty(\varphi) \geq -2$. Alltså saknar φ poler $\neq \infty$ dvs $q = 1$ och grad $p \leq 2$ så att $\varphi = ax^2 + bx + c, a, b, c \in \mathbb{C}$. Detta visar att $\ell(D) = 3$. Mera allmänt är $\ell(D) = \deg D + 1$ då $D = dP_\infty$ med $d \geq 0$. Det är också klart att $\ell(D) = 0$ då $d > 0$ (ty $v_P(\varphi) > 0$ för varje P är omöjligt så att $\mathcal{L}(D) = (0)$).

□

(10.13) Riemanns olikhet. *Låt V vara en icke-singulär irreducibel kurva över $\mathbb{C}$. Då existerar ett heltal $g \geq 0$ sådant att*

$$\ell(D) - \deg D \geq -g + 1$$

för varje divisor $D \in \mathrm{Div}\,(V)$ och det finns D_0 så att likheten gäller. Talet g kallas **genus** *av V.*

(10.14) Exempel. Låt $V = \mathbb{P}^2(\mathbb{C})$ och $D = \sum n_i P_{a_i} - \sum m_j Q_{b_j}$, $m_j, n_i > 0$, $a_i, b_j \in \mathbb{C} \cup \{\infty\}$. Om $\sum n_i = \sum m_j$, dvs deg $D = 0$, så existerar $\varphi \in \mathbb{C}(V)$ så att $(\varphi) = D$, ty

$$\varphi = \frac{\prod (x - a_i)^{n_i}}{\prod (x - b_j)^{m_j}}, \text{ där } a_i, b_j \neq \infty$$

har som sin divisor D. Om D är en godtycklig divisor så är

$$D = D^0 + dP_\infty = (\varphi) + dP_\infty$$

för en funktion $\varphi \in \mathbb{C}(V)$ då $d = \deg D$ (således är deg $D^0 = 0$). Helt allmänt gäller

$$\deg (D_1) = \deg (D_2) \quad \text{och} \quad \ell(D_1) = \ell(D_2)$$

då $D_1 - D_2 = (\varphi)$ för $\varphi \in \mathbb{C}(V)$ (en enkel övning). Alltså är

$$\ell(D) - \deg (D) = \ell(dP_\infty) - \deg (dP_\infty) = \begin{cases} (d+1) - d = 1 & \text{då} \quad d \geq 0, \\ -d & \text{då} \quad d < 0. \end{cases}$$

Detta visar att $\min(\ell(D) - \deg(D)) = 1 = -g + 1$ så att $g = 0$ då $V = \mathbb{P}^1(\mathbb{C})$. Omvänt, låt V vara en irreducibel icke-singulär kurva över $\mathbb{C}$ av genus $g = 0$. Låt $D = P$. Då är $\ell(D) - \deg(D) \geq 1$ dvs $\ell(D) \geq 2$. Låt $\varphi \in \mathcal{L}(D)$, $\varphi \notin \mathbb{C}$ (φ finns ty $\ell(D) \geq 2$). Då är $(\varphi) + P \geq 0$ så att $(\varphi) = Q - P$. Nu är $[\mathbb{C}(V) : \mathbb{C}(\varphi)] = \deg(\varphi)_0 = 1$ enligt (10.10). Alltså är $\mathbb{C}(V) = \mathbb{C}(\varphi)$. Detta visar att V och $\mathbb{P}^1(\mathbb{C})$ har isomorfa kroppar av rationella funktioner. Detta är ekvivalent med $V \cong \mathbb{P}^1(\mathbb{C})$ (vi har inte definierat isomorfibegreppet för mångfalder. Se dock appendix C).

□

(10.15) Anmärkning. (a) Riemann-Rochs sats beskriver skillnaden mellan vänster- och höger led i Riemanns olikhet. Den säger att:

$$\ell(D) - \deg(D) = -g + 1 + \ell(K - D),$$

där K är en särskild divisor på V som kallas **kanonisk** (mera exakt är dess klass i $Cl(V)$ kanonisk).

(b) Genus av elliptiska kurvor (med ekvationer $y^2 = x^2 + ax + b$ i $\mathbb{C}^2$ – se texten efter (8.13)) är 1, och omvänt, varje V av genus 1 har $\mathbb{C}(V) = \mathbb{C}(x, y)$, där x, y uppfyller

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{C}.$$

(c) Man betraktar differentialformer på V ($\omega = \varphi d\psi, \varphi, \psi \in \mathbb{C}(V)$) och ordnar en divisor mot varje sådan form. Dessa divisorer bildar just den kanoniska klassen K (var och en kan väljas som K i (a)). Ur Riemann-Rochs sats med $D = 0$ får man $g = \ell(K)$, ty $\ell(D) = 1$ och $\deg(D) = 0$ då $D = 0$. g är dimensionen av rummet av alla differentialformer $\omega = \varphi\omega_0$ sådana att $(\omega) = (\varphi\omega_0) = (\varphi) + (\omega_0) \geq 0$ (där $(\omega_0) = K$) dvs sådana som saknar poler på V.

□

APPENDIX C: NÅGRA ORD OM MÅNGFALDSBEGREPPET

Vårt syfte här är att placera begreppet mångfald i allmännare perspektiv. Tidigare betraktade vi analytiska mångfalder (se Kap. 5), affina algebraiska mångfalder (se Övn. 2.20) och projektiva mångfalder. Det finns en möjlighet att betrakta dessa begrepp som specialfall av en allmän konstruktion. Den kräver begreppet ringat rum.

(C.1) Definition. Låt X vara ett topologisk rum och låt U_X vara kategorin av alla öppna delmängder till X (se övn. 11.1 (b) – objekt är öppna delmängder $U \subseteq X$, och Mor (U, V) har ett element om $U \subseteq V$ och är tom då $U \not\subseteq V$). Med en **prekärve** på X menas en kontravariant funktor $\mathcal{F}$ från U_X till en kategori $\mathcal{C}$. Ofta är $\mathcal{C}$ kategorin av abelska grupper eller kommutativa ringar med etta. Bilden av $s \in \mathcal{F}(V)$ vid $\mathcal{F}(V) \to \mathcal{F}(U)$ betecknas med $s|U$. □

(C.2) Exempel. (a) Låt $X = \mathbb{R}$ med naturlig topologi och låt $\mathcal{F}(V) =$ alla kontinuerliga funktioner $f : V \to \mathbb{R}$. Om $U \subseteq V$ definierar man $\mathcal{F}(V) \to \mathcal{F}(U)$ som restriktion: $f \in \mathcal{F}(V)$ avbildas på $f|_U$. $\mathcal{F}(V)$ är en kommutativ ring med etta och restriktionerna är ringhomomorfismer.

(b) Låt V vara en öppen mängd i $\mathbb{R}^n$ och låt $\mathcal{F}(V) =$ alla funktioner $f : V \to \mathbb{R}$ av klass C^k (C^∞, analytiska). $\mathcal{F}(V)$ är en kommutativ ring med etta och för $U \subseteq V$ är den naturliga restriktionen av $f \in \mathcal{F}(V)$ till U en ringhomomorfism $\mathcal{F}(V) \to \mathcal{F}(U)$. □

(C.3) Definition. Man säger att en prekärve $\mathcal{F}$ på X är en **kärve** om det för varje öppen mängd $U \subseteq X$ och för varje övertäckning $U = \cup_{i \in I} U_i$ med öppna mängder U_i är följande villkor uppfyllt: Om $s_i \in \mathcal{F}(U_i)$ är givna så att $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ för $i, j \in I$ så existerar exakt ett $s \in \mathcal{F}(U)$ så att $s|_{U_i} = s_i$ för varje $i \in I$.

Om $\mathcal{F}$ är en kärve av ringar på X så säger man att $(X, \mathcal{F})$ är ett **ringat rum**. Man skriver då ofta $\mathcal{F} = \mathcal{O}_X$.

Två ringade rum $(X, \mathcal{F})$ och $(Y, \mathcal{G})$ är **isomorfa** om det finns en homeomorfism $\varphi : X \to Y$ och för varje öppen mängd $V \subseteq X$ en ringisomorfism

$$\varphi_V : \mathcal{F}(V) \to \mathcal{G}(\varphi(V))$$

så att alla diagram:

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(\varphi(V)) \\ \downarrow & & \downarrow \\ \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(\varphi(U)) \end{array}$$

kommuterar då $U \subseteq V$. □

(C.4) Exempel. Prekärvarna i (C.2) är självklart kärvar.

Nu kan man definiera en reell mångfald M (av en lämplig klass) som ett ringat rum $(M, \mathcal{F})$ sådant att för varje $P \in M$ finns en omgivning $U_P \subseteq M$ och $(U_P, \mathcal{F}|_{U_P}) \cong (U, \mathcal{O}_U)$, där $U \subseteq \mathbb{R}^n$ och $\mathcal{O}_U$ är kärven ur exemplet (C.2) (b). På liknande sätt kan man definiera komplexa mångfalder. En sådan definitionen är ekvivalent med vår tidigare definition i Kap. 4 – $\mathcal{F}(U)$ där är ringen av alla reguljära funktioner på U.

Definitionen av algebraiska mångfalder formuleras på liknande sätt. Först och främst konstaterar vi att en irreducibel algebraisk mångfald $V \subseteq \mathbb{C}^n$ kan rekonstrueras ur $\mathbb{C}[V] = \mathbb{C}[X_1, \ldots, X_n]/\mathcal{I}(V)$ med hjälp av Spec $\mathbb{C}[V]$ = mängden av alla primideal i $\mathbb{C}[V]$ – enligt Nullstellensatz svarar punkterna $(a_1, \ldots, a_n) \in V$ en–entydigt mot alla maximalideal $(x_1 - a_1, \ldots, x_n - a_n)$ i $\mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_n]$. Spec $\mathbb{C}[V]$ innehåller dessutom ideal som svarar mot alla andra delmångfalder till V : $W \subseteq V \Rightarrow \mathcal{I}(W) \supseteq \mathcal{I}(V)$ så att $\mathcal{I}(W)/\mathcal{I}(V)$ är ett primideal i $\mathbb{C}[X_1, \ldots, X_n]/\mathcal{I}(V) = \mathbb{C}[V]$. Spec $\mathbb{C}[V]$ har en topologi – Zariskis topologi (se Övn. 4.15). Vidare kan vi förse Spec $\mathbb{C}[V]$ med en lämplig kärve enligt konstruktionen nedan.

Mera allmänt låt R vara en godtycklig kommutativ ring (med etta) utan nolldelare (den sista förutsättningen är för att förenkla definitionerna som annars är rent tekniskt mera invecklade – konstruktionen gäller för godtyckliga kommutativa ringar). Låt K vara kvotkroppen av R. Om $U \subseteq$ Spec R så definierar man $\mathcal{F}(U) = \cap_{\mathfrak{p} \in U} R_{\mathfrak{p}}$. Det är självklart att $\mathcal{F}$ är en kärve. Paret $(\text{Spec}R, \mathcal{O}_R)$ där $\mathcal{O}_R = \mathcal{F}$ kallas **affint schema**. Man säger att ett ringat rum $(X, \mathcal{O}_X)$ är ett **schema** om för varje $P \in X$ existerar en omgivning U_P så att $(U_P, \mathcal{O}_X|_{U_P}) \cong (\text{Spec } R, \mathcal{O}_R)$ för en ring R (som beror på P). Notera att $\mathcal{O}_R(U)$ = ringen av alla "rationella funktioner" som är definierade i alla punkter av U (tag $R = \mathbb{C}[V]$ och analysera vad detta innebär! Se (4.21).).

Kurvor $V \subseteq \mathbb{P}^2(\mathbb{C})$ (eller hela projektiva rummet $\mathbb{P}^2(\mathbb{C})$) är exempel på scheman som inte är affina. V har övertäckningen $V \cap U_i$, $i = 0, 1, 2$, där $V \cap U_i$ är en kurva i $\mathbb{C}^2$. Man har en kärve på varje $V \cap U_i$ som konstrueras ur $\mathbb{C}[V \cap U_i]$ och detta ger en kärve på V genom en enkel "klistring" som i bevis för (10.4) och (10.6).

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 $\varphi : M' \to M$,

$$G(\varphi) = \bar{\varphi} : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N),$$

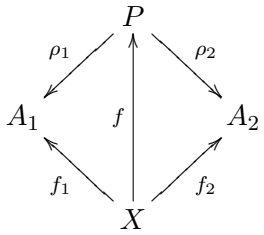
där $\bar{\varphi}(f) = f \circ \varphi$ för $f : M \to N$. G är en kontravariant funktor. Ett mycket viktigt specialfall får vi då $N = R$. Då är $G(M) = \mathrm{Hom}_R(M, R) = M^*$ den duala modulen (se Övn. 10, 11,13).

□

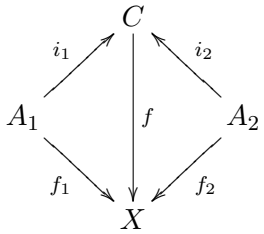
Det finns en lång lista av mycket viktiga och allmänna begrepp som kan definieras i kategorier under mer eller mindre restriktiva förutsättningar. Bland dessa begrepp kan nämnas som särskilt viktiga sådana som isomorfism, monomorfism, epimorfism, kärna, bild, kokärna, kobild, produkt, koprodukt, fibrerad 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) i kompendiet "Linjär och multilinjär algebra"). 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 $\mathcal{C}$.

$$M \xrightarrow{f} N \underset{h}{\overset{g}{\rightrightarrows}} X$$

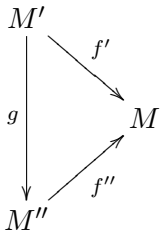
implicerar $g \circ f = h \circ f$ att $g = h$. Ett annat sätt att uttrycka den definitionen är en översättning till morfismmängder. $f : M \to N$ är en epimorfism om för varje objekt X i $\mathcal{C}$ är funktionen

$$f_X : \mathrm{Mor}(N, X) \to \mathrm{Mor}(M, X),$$

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).

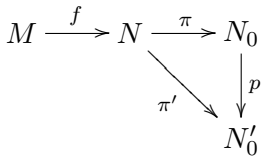
(11.13) Definition. Låt $f : M \to N$ vara en morfism i en additiv kategori $\mathcal{C}$. Med **kärnan** $\mathrm{Ker} f$ till f menas ett delobjekt $\imath : M_0 \to M$ (mera exakt, ekvivalensklassen av $\imath$ – se (11.10)) med följande egenskaper:

$$\begin{array}{ccccc} M_0 & \xrightarrow{\imath} & M & \xrightarrow{f} & N \\ \uparrow{\scriptstyle j} & \nearrow{\scriptstyle \imath'} & & & \\ M_0' & & & & \end{array}$$

(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 12 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).

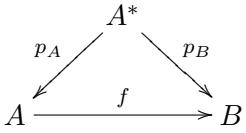
11.7. Man säger att en kovariant funktor $F : \mathcal{C} \to \mathcal{S}et$ är **representerbar** om det finns ett objekt $A_F \in \mathcal{O}b(\mathcal{C})$ sådant att funktorerna F och h_{A_F} (se Övn. 3 – ${}_{A_F}h(x) = \mathrm{Mor}(A_F, X)$) är isomorfa (se Övn. 6). En kontravariant funktor $F : \mathcal{C} \to \mathcal{S}et$ 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.

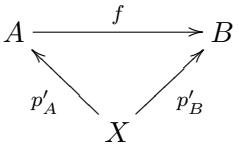
11.8. Låt $\mathcal{C}$ vara en kategori och $\mathcal{T}$ en liten delkategori till $\mathcal{C}$ (dvs $\mathcal{T}$ är en kategori vars objekt bildar en mängd $\mathcal{O}b(\mathcal{T}) \subseteq \mathcal{O}b(\mathcal{C})$, och för varje par $A, B \in \mathcal{O}b(\mathcal{T})$ är $\mathrm{Mor}_{\mathcal{T}}(A,B) \subseteq \mathrm{Mor}_{\mathcal{C}}(A,B)$). 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)

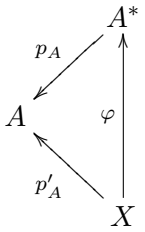


kommuterar för varje $f \in \mathrm{Mor}_{\mathcal{T}}(A,B)$.

(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

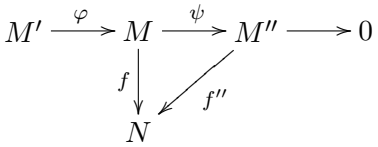
$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(M, N) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(M', N)$$

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)).

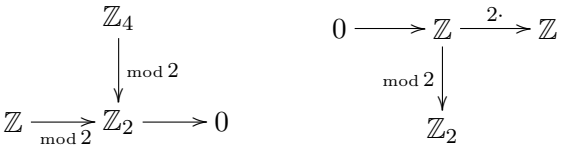
Steg 3. $\mathrm{Im}\bar{\psi} \supseteq \mathrm{Ker}\bar{\varphi}$. Betrakta diagrammet:



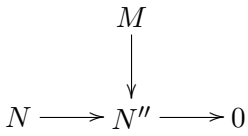
där $f \circ \varphi = 0$. Vi måste visa att om $\bar{\varphi}(f) = f \circ \varphi = 0$ så finns det f'' så att $\psi(f'') = f'' \circ \psi = f$. Villkoret $f \in \mathrm{Ker}\bar{\varphi}$ betyder $\bar{\varphi}(f) = f \circ \varphi = 0$ dvs $\mathrm{Ker}\psi = \mathrm{Im}\varphi \subseteq \mathrm{Ker}f$. 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

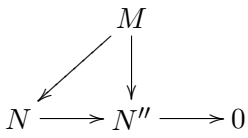
Ledning. Betrakta diagrammen:



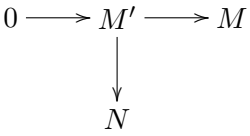
Anmärkning. Funktorn $N \mapsto \mathrm{Hom}_R(M, N)$ är högerexakt då och endast då varje diagram



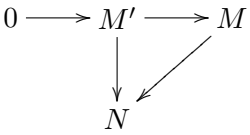
kan kompletteras till ett kommutativt diagram



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

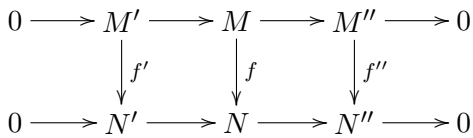


kan kompletteras till ett kommutativt diagram



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 t ex (5.30) i kompendiet "Linjär och multilinjär algebra"). 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.

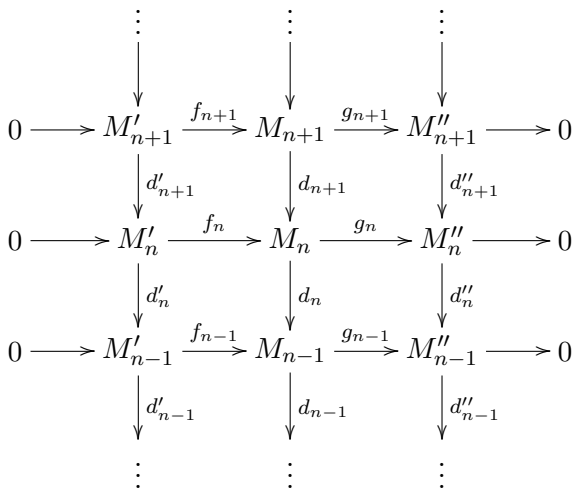
□

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:



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:

$$\begin{array}{ccccccccc} & & M_n'/\mathrm{Im} d_{n+1}' & \xrightarrow{\bar{f}_n} & M_n/\mathrm{Im} d_{n+1} & \xrightarrow{\bar{g}_n} & M_n''/\mathrm{Im} d_{n+1}'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \bar{d}_n'} & & \downarrow{\scriptstyle \bar{d}_n} & & \downarrow{\scriptstyle \bar{d}_n''} & & \\ 0 & \longrightarrow & \mathrm{Ker} d_{n-1}' & \xrightarrow{\bar{f}_{n-1}} & \mathrm{Ker} d_{n-1} & \xrightarrow{\bar{g}_{n-1}} & \mathrm{Ker} d_{n-1}'' & & \end{array}$$

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.

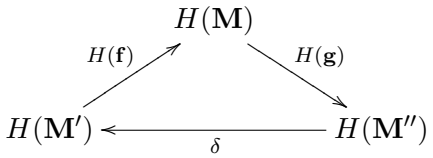
Det återstår att visa exaktheten i Ker d'' och Coker d'. Det faktum att Im $g_1^* \subseteq$ Ker ∂ och Im $\partial \subseteq$ Ker f_2^* följer direkt ty det är lätt att kontrollera likheterna $\partial g_1^* = 0$ och $f_2^* \partial = 0$. Som avslutning låt oss visa att Ker $\partial \subseteq$ Im g_1^* (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:

$$\begin{array}{ccccc} 0 & \longrightarrow & W' & \xrightarrow{i} & W \\ & & {\scriptstyle g}\downarrow & \swarrow_{f} & \\ & & V & & \end{array}$$

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

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0$$

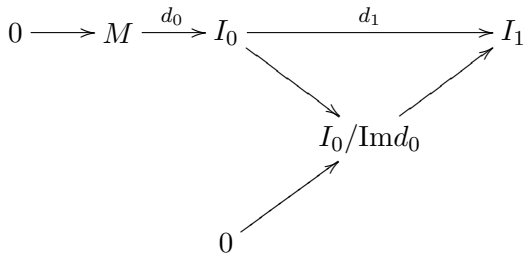
[†]Den egenskapen karakteriserar Dedekindringar.

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.

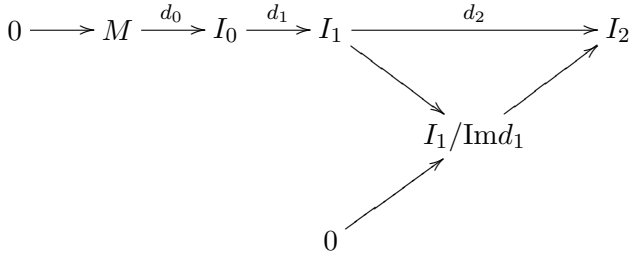
(b) Först måste vi veta att för varje R-modul M existerar en injektiv R-modul I och en monomorfism $0 \to M \to I$. Även om beviset inte är särskilt svårt måste vi avstå från att ge det här. Med detta påstående är resten enkel. Man startar med den exakta sekvensen

$$0 \longrightarrow M \xrightarrow{d_0} I_0 \longrightarrow I_0/\text{Im}d_0 \longrightarrow 0$$

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:

$$0 \to \mathcal{F}(I_0) \to \mathcal{F}(I_1) \to \mathcal{F}(I_2) \to \ldots$$

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 $k = 0,\, 1, 2, \ldots$ 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.