

### 3. Dekomposition.

**(3.1) Definition.** Lad  $M$  være en  $R$ -modul. En undermodul  $N$  i  $M$  siges da at være en *primær undermodul*, hvis der er netop ét primideal associeret til kvotientmodulen  $M/N$ . At  $\mathfrak{p}$  er det eneste primideal associeret til  $M/N$ , altså at  $\text{Ass}(M/N) = \{\mathfrak{p}\}$ , udtrykkes ved at sige, at  $N$  er en  $\mathfrak{p}$ -*primær* undermodul i  $M$ .

Betragt en endeligt frembragt  $R$ -modul  $Q \neq 0$ , og de associerede primidealer  $\mathfrak{p}_1, \dots, \mathfrak{p}_q$  for  $Q$ . Foreningsmængden af idealerne  $\mathfrak{p}_i$  er da mængden  $Z_R(Q)$  af nuldivisorer på  $Q$ :

$$Z_R(Q) = \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_q.$$

De minimale blandt idealerne  $\mathfrak{p}_i$  er netop de minimale blandt primidealene, der omfatter annullatoren for  $Q$ . Følgelig er fællesmængden af idealerne  $\mathfrak{p}_i$  lig med radikalet af annullatoren:

$$\text{Rad}(\text{Ann } Q) = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_q.$$

Fællesmængden er skarpt indeholdt i foreningsmængden med mindre  $q = 1$ . Med andre ord: Der er netop ét associeret primideal for  $Q$ , hvis og kun hvis  $Q \neq 0$  og der for enhver nuldivisor  $f$  på  $Q$  gælder, at en potens af  $f$  annullerer  $Q$ .

Når  $M$  er endeligt frembragt fås herved en karakterisering af de primære undermoduler i  $M$ . Fx fås for idealer i  $R$  følgende:

**Karakterisering.** *Idealet  $\mathfrak{q}$  er et primært ideal i  $R$ , hvis og kun hvis følgende betingelse er opfyldt:  $\mathfrak{q} \subset R$  og for alle  $f, g \in R$  gælder, at hvis  $fg \in \mathfrak{q}$  og  $g \notin \mathfrak{q}$ , så er  $f \in \text{Rad}(\mathfrak{q})$ .*

Betingelserne  $fg \in \mathfrak{q}$  og  $g \notin \mathfrak{q}$  udtrykker jo netop, at  $f$  er nuldivisor på  $R/\mathfrak{q}$ , og konklusionen,  $f \in \text{Rad}(\mathfrak{q})$ , udtrykker, at en potens af  $f$  annullerer  $R/\mathfrak{q}$ .

En undermodul  $N$  i  $M$  siges at være *irreducibel*, hvis  $N \subset M$  og  $N$  ikke kan skrives som en fællesmængde  $N = N_1 \cap N_2$ , hvor  $N \subset N_1$  og  $N \subset N_2$ .

**(3.2) Lemma.** (1) *En irreducibel undermodul er primær.*

(2) *En fællesmængde af to  $\mathfrak{p}$ -primære undermoduler er selv  $\mathfrak{p}$ -primær.*

*Bevis.* (1) Lad  $N$  være en irreducibel undermodul i  $M$ . Specielt er så  $M/N \neq 0$ . Der findes derfor associerede primidealer for  $M/N$ , jfr Sætning (2.1). Det skal nu vises, at kvotientmodulen  $M/N$  kun har ét associeret primideal. Antag, indirekte, at  $\mathfrak{p}_1$  og  $\mathfrak{p}_2$  er associerede primidealer for  $M/N$ , og at de er forskellige. For  $i = 1, 2$  har kvotienten  $M/N$  da en undermodul  $\bar{N}_i$  isomorf med  $R/\mathfrak{p}_i$ . Specielt er  $\mathfrak{p}_i$  det eneste primideal associeret til  $\bar{N}_i$ . Fællesmængden  $\bar{N}_1 \cap \bar{N}_2$  er indeholdt i  $\bar{N}_1$ . Et primideal, der er associeret til fællesmængden er derfor også associeret til  $\bar{N}_1$ , jfr Lemma (1.7), og det må følgelig være lig med  $\mathfrak{p}_1$ . Med samme begrundelse måtte det være lig med  $\mathfrak{p}_2$ . Da  $\mathfrak{p}_1 \neq \mathfrak{p}_2$  konkluderes derfor, at fællesmængden  $\bar{N}_1 \cap \bar{N}_2$  ikke har associerede primidealer. Af Sætning (2.1) følger derfor, at  $\bar{N}_1 \cap \bar{N}_2 = (0)$ .

Ifølge Noether's anden Isomorfisætning svarer undermodulerne  $\bar{N}_i$  i  $M/N$  til undermoduler  $N_i \supseteq N$ . Af det viste følger at  $N_1 \cap N_2 = N$ . Yderligere er  $N_i \supset N$ , da  $\bar{N}_i \neq 0$ . Da  $N$  var irreducibel, har antagelsen således ført til en modstrid, som ønsket.

(2) Lad  $N = N_1 \cap N_2$  være en fællesmængde af  $\mathfrak{p}$ -primære moduler  $N_1$  og  $N_2$ . Det er klart, at  $M/N \neq 0$ , så det skal vises, at  $\mathfrak{p}$  er det eneste associerede primideal for  $M/N$ . Lad hertil  $\mathfrak{q}$  være et associeret primideal for  $M/N$ . Betragt homomorfien

$$M \rightarrow M/N_1 \oplus M/N_2, \quad (*)$$

der til et element i  $M$  knytter parret af restklasser modulo  $N_1$  og modulo  $N_2$ . Kernen for denne homomorfi er øjensynlig fællesmængden  $N_1 \cap N_2$ , altså  $N$ , så ifølge Isomorfisætningen er kvotienten  $M/N$  isomorf med en undermodul af den direkte sum på højresiden i (\*). Primidealet  $\mathfrak{q}$  er derfor associeret til en undermodel af den direkte sum, og dermed også associeret til den direkte sum, jfr (1.7.2). Af den anden inklusion i (1.7.2), anvendt på en af summanderne i den direkte sum, følger, at et primideal associeret til summen må være associeret til en af summanderne  $M/N_i$ . Ifølge forudsætningen er  $\mathfrak{p}$  det eneste primideal associeret til  $M/N_i$ . Altså må  $\mathfrak{q}$  være lig med  $\mathfrak{p}$ , som ønsket.  $\square$

**(3.3) Eksempel.** (1) Et primideal  $\mathfrak{p}$  er en  $\mathfrak{p}$ -primær undermodul i  $R$ . Som vist i Eksempel (1.6) er nemlig  $\text{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ .

(2) Lad  $\mathfrak{m}$  være et maksimalideal. Enhver potens  $\mathfrak{m}^m$ , hvor  $m \geq 1$ , og mere generelt, ethvert ideal  $\mathfrak{a}$  således at

$$\mathfrak{m}^m \subseteq \mathfrak{a} \subseteq \mathfrak{m},$$

vil da være et  $\mathfrak{m}$ -primært ideal i  $R$ . Ifølge Eksempel (1.6) består støtten for  $R/\mathfrak{a}$  nemlig af de primidealer  $\mathfrak{p}$ , som omfatter  $\mathfrak{a}$ . Af  $\mathfrak{a} \subseteq \mathfrak{p}$  følger, at potensen  $\mathfrak{m}^m$  er indeholdt i  $\mathfrak{p}$ . Da  $\mathfrak{p}$  er et primideal, følger det videre, at en af faktorerne i produktet  $\mathfrak{m}^m$ , dvs  $\mathfrak{m}$ , er indeholdt i  $\mathfrak{p}$ . Da  $\mathfrak{m}$  er et maksimalideal følger det endelig, at  $\mathfrak{p} = \mathfrak{m}$ . Det er således godtgjort, at støtten for  $R/\mathfrak{a}$  består af det ene primideal  $\mathfrak{m}$ . Og så er  $\mathfrak{m}$  også det eneste associerede primideal til  $R/\mathfrak{a}$  ifølge Sætning (2.1).

**(3.4) Primærdekomposition.** Lad  $N$  være en undermodul i modulen  $M$ . Ved en *primærdekomposition* af  $N$  forstås en fremstilling af  $N$  som en fællesmængde,

$$N = N_1 \cap \dots \cap N_q,$$

hvor  $N_j$ 'erne er primære undermoduler. Antag, at  $N_j$  er  $\mathfrak{p}_j$ -primær. Dekompositionen siges da at være *uforkortelig*, hvis  $\mathfrak{p}_j$ 'erne er forskellige og ingen af  $N_j$ 'erne i fællesmængden er overflødige.

Det følger af Lemma (3.2), at man ud fra en primærdekomposition af  $N$  kan opnå en uforkortelig dekomposition: Først erstattes for hvert primideal  $\mathfrak{p}$  de  $N_j$ 'er, der er  $\mathfrak{p}$ -primære, med deres fællesmængde, og dernæst bortkastes overflødige  $N_j$ 'er.

**(3.5) Dekompositionssætning.** *Lad  $M$  være en endeligt frembragt  $R$ -modul. Da har hver undermodul  $N$  en primærdekomposition,*

$$N = N_1 \cap \dots \cap N_q. \quad (3.5.1)$$

30. marts 2007

Antag, at en sådan dekomposition er uforkortelig, og at  $N_j$  er  $\mathfrak{p}_j$ -primær. Da er  $\mathfrak{p}_j$ 'erne netop primidealerne associerede til  $M/N$ . Yderligere gælder, at de undermoduler  $N_j$ , for hvilke  $\mathfrak{p}_j$  er et minimalt primideal for  $M/N$ , er entydigt bestemte, idet  $N_j$  er kernen for den sammensatte homomorfi  $M \rightarrow M/N \rightarrow (M/N)_{\mathfrak{p}_j}$ .

*Bevis.* For at vise eksistensen af fremstillingen er det ifølge Lemma (3.2) nok at vise, at enhver undermodul  $N$  er en endelig fællesmængde af irreducible undermoduler. Denne påstand vises ved noethersk induktion: Antag, indirekte, at påstanden er gal, og betragt mængden  $\mathcal{S}$  af de undermoduler i  $N$ , der ikke er en endelig fællesmængde af irreducible undermoduler. Ifølge antagelsen er  $\mathcal{S}$  ikke tom. Da  $M$  er endeligt frembragt over en noethersk ring, er  $M$  noethersk. Følgelig findes i  $\mathcal{S}$  en undermodul  $N$ , der er maksimal blandt undermodulerne i  $\mathcal{S}$ . Undermodulen  $N$  tilhører  $\mathcal{S}$ , og specielt kan den derfor ikke være irreducibel. Yderligere er  $N \subset M$ , idet  $M$  har en fremstilling af den ønskede form, nemlig som fællesmængde af ingen irreducible moduler. Da  $N \subset M$  og  $N$  ikke er irreducibel, er  $N$  en fællesmængde,  $N = N_1 \cap N_2$ , af undermoduler  $N_i \supset N$ . Da  $N$  var maksimal blandt undermodulerne i  $\mathcal{S}$ , kan ingen af undermodulerne  $N_i$  tilhøre  $\mathcal{S}$ . Følgelig er begge undermoduler  $N_1$  og  $N_2$  en endelig fællesmængde af irreducible undermoduler, og så er fællesmængden  $N$  det også, i modstrid med at  $N$  var element i  $\mathcal{S}$ .

Antag nu, at fremstillingen (3.5.1) er uforkortelig. Betragt homomorfin,

$$M/N \rightarrow M/N_1 \oplus \cdots \oplus M/N_q, \quad (*)$$

der afbilder restklassen af  $x$  modulo  $N$  i  $q$ -sættet hvis  $j$ 'te koordinat er restklassen af  $x$  modulo  $N_j$ . Denne homomorfi er veldefineret, da  $N \subseteq N_j$ , og den er injektiv, da  $N$  er fællesmængden af  $N_j$ 'erne. Lad  $\mathfrak{p}$  være et primideal associeret med  $M/N$ . Af Lemma (1.7) følger nu først, at  $\mathfrak{p}$  er associeret med den direkte sum på højresiden af (\*), og dernæst at  $\mathfrak{p}$  er associeret med en af addenderne  $M/N_j$ . Da  $M/N_j$  er  $\mathfrak{p}_j$ -primær, er  $\mathfrak{p}_j$  det eneste primideal associeret med  $M/N_j$ . Altså er  $\mathfrak{p}$  lig med et af  $\mathfrak{p}_j$ 'erne.

Betragt omvendt et af primidealerne  $\mathfrak{p}_k$ . Lad  $M_k$  være fællesmængden af de  $N_j$ 'er, hvor  $N_k$  ikke medtages, og lad  $Q$  være kvotientmodulen  $Q := M_k/N$ . Af Noether's anden Isomorfisætning følger, at  $Q = M_k/N$  er isomorf med en undermodul i  $M/N$ . På den anden side er øjensynlig  $N = M_k \cap N_k$ , så af Noether's første Isomorfisætning følger, at  $Q = M_k/(M_k \cap N_k)$  er isomorf med en undermodul i  $M/N_k$ . Af Lemma (1.7) fås derfor inklusionerne,

$$\text{Ass } Q \subseteq \text{Ass}(M/N), \quad \text{Ass } Q \subseteq \text{Ass}(M/N_k).$$

Modulen  $M/N_k$  er  $\mathfrak{p}_k$ -primær, så mængden på højresiden af den sidste inklusion indeholder ét element, nemlig primidealet  $\mathfrak{p}_k$ . Modulen  $M_k$  opfylder at  $M_k \supset N$ , thi ellers var jo  $N_k$  overflødig i fremstillingen (3.5.1). Kvotienten  $Q = M_k/N$  er derfor forskellig fra 0, og  $\text{Ass } Q$  er derfor ikke tom ifølge Sætning (2.1). Den anden inklusion ovenfor medfører derfor, at  $\text{Ass } Q$  består alene af primidealet  $\mathfrak{p}_k$ . Den første inklusion ovenfor medfører derfor, at  $\mathfrak{p}_k$  er associeret til  $M/N$ .

Hermed er det vist, at  $\mathfrak{p}_j$ 'erne er de associerede primidealer til  $M/N$ .

30. marts 2007

For at bevise den sidste del af entydighedsudsagnet betragtes først en vilkårlig endeligt frembragt modul  $Q$ , med den egenskab at  $\text{Ass } Q$  består af netop et primideal  $\mathfrak{p}$ . Det påstås, at den kanoniske homomorfi,

$$Q \rightarrow Q_{\mathfrak{p}},$$

da er injektiv. Antag nemlig, at  $y$  er et element forskelligt fra 0 i homomorfiens kerne. Da brøken  $y/1$  er lig med 0 i  $M_{\mathfrak{q}}$ , er  $\text{Ann}(y)$  ikke indeholdt i  $\mathfrak{q}$ . Men det er i modstrid med at  $\text{Ann}(y)$  er indeholdt i et associeret primideal ifølge Sætning (2.1) og  $\mathfrak{q}$  er det eneste associerede primideal for  $Q$ .

Lad nu  $\mathfrak{p}_j$  være et minimalt primideal for  $M/N$ . Betragt homomorfi, der fremkommer af (\*) ved lokalisering i  $\mathfrak{p}_j$ . For  $k \neq j$  består støtten for  $M/N_k$  af de primidealer, der omfatter  $\mathfrak{p}_k$ , og  $\mathfrak{p}_j$  er ikke et sådant primideal, da  $\mathfrak{p}_j$  er minimalt blandt  $\mathfrak{p}_k$ 'erne. Altså er  $(M/N_k)_{\mathfrak{p}_j} = 0$  for  $k \neq j$ . Den lokaliserede homomorfi er derfor følgende homomorfi,

$$(M/N)_{\mathfrak{p}_j} \rightarrow (M/N_j)_{\mathfrak{p}_j}. \quad (**)$$

Homomorfi (\*) var injektiv, så det følger af Isomorfisætning for Brøkmoduler, at den lokaliserede homomorfi (\*\*) er injektiv. På den anden side følger det af påstanden ovenfor, anvendt på  $Q := M/N_j$  og  $\mathfrak{p} := \mathfrak{p}_j$ , at homomorfi  $M/N_j \rightarrow (M/N_j)_{\mathfrak{p}_j}$  er injektiv. Det er klart, at følgende diagram er kommutativt,

$$\begin{array}{ccc} M & \longrightarrow & M/N_j \\ \downarrow & & \downarrow \\ (M/N)_{\mathfrak{p}_j} & \longrightarrow & (M/N_j)_{\mathfrak{p}_j}. \end{array}$$

De to homomorfier der ender i  $(M/N_j)_{\mathfrak{p}_j}$  er ifølge det viste injektive. De to homomorfier der begynder i  $M$  har derfor samme kerne. Heraf følger øjensynlig Sætningens påstand om entydigheden af  $N_j$ .  $\square$

**(3.6) Eksempel.** (1) Lad  $\mathfrak{a}$  være en fællesmængde af primidealer,

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q. \quad (3.6.1)$$

Det følger af Eksempel (3.3)(1), at fremstillingen (3.6.1) er en primærdekomposition. Antag, at der ikke er inklusioner mellem  $\mathfrak{p}_j$ 'erne, altså at intet  $\mathfrak{p}_j$  er indeholdt i et af de øvrige. Da er dekompositionen uforkortelig, thi  $\mathfrak{p}_j$ 'erne er specielt forskellige, og var et af  $\mathfrak{p}_j$ 'erne, fx  $\mathfrak{p}_k$ , overflødig, så ville primidealet  $\mathfrak{p}_k$  indeholde fællesmængden af de øvrige, og heraf følger som bekendt, at  $\mathfrak{p}_k$  ville indeholde et af de øvrige. Det følger af Dekompositionssætningen, at  $\mathfrak{p}_j$ 'erne er de associerede primidealer til  $R/\mathfrak{a}$ .

(2) Lad  $\mathfrak{m}_1, \dots, \mathfrak{m}_q$  være forskellige maksimalidealer i  $R$ , og betragt en fællesmængde,

$$\mathfrak{a} = \mathfrak{m}_1^{m_1} \cap \cdots \cap \mathfrak{m}_q^{m_q}, \quad (3.6.2)$$

hvor eksponenterne  $m_j$  er positive. Da er (3.6.2) en uforkortelig primærdekomposition af  $\mathfrak{a}$ . Det følger nemlig først af Eksempel (3.3)(2), at idealet  $\mathfrak{m}_j^{m_j}$  er  $m_j$ -primært. Videre er

30. marts 2007

ingen af idealerne  $\mathfrak{m}_j^{m_j}$  overflødige i fællesmængden. Antag nemlig, indirekte, at fx  $\mathfrak{m}_1^{m_1}$  er overflødig. Da vil  $\mathfrak{m}_1^{m_1}$  indeholde fællesmængden af de øvrige  $\mathfrak{m}_j^{m_j}$ 'er. Specielt vil primidealet  $\mathfrak{m}_1$  indeholde denne fællesmængde. Som bekendt følger heraf, at  $\mathfrak{m}_1$  indeholder et af idealerne  $\mathfrak{m}_j^{m_j}$  for  $j > 1$ , og videre, at  $\mathfrak{m}_1$  indeholder  $\mathfrak{m}_j$ . Dette er en modstrid, da  $\mathfrak{m}_j$  er et maksimalideal og  $\mathfrak{m}_1 \neq \mathfrak{m}_j$ .

Af Dekompositionssætningen fremgår nu, at  $\mathfrak{m}_j$ 'erne er de associerede primidealer til  $R/\mathfrak{a}$ . Af korollaret til Filtrations-sætningen følger videre, at  $R/\mathfrak{a}$  har endelig længde.

(3) Antag, at ringen  $R$  er faktoriel, og betragt et element  $f$  med primopløsningen  $f = p_1^{m_1} \cdots p_q^{m_q}$  (hvor altså  $p_j$ 'erne er irreducibile og ikke associerede, og  $m_j$ 'erne positive). Ved brug af den entydige primopløsning ses det let, at

$$(f) = (p_1^{m_1}) \cap \cdots \cap (p_q^{m_q}). \quad (3.6.3)$$

Af Eksempel (3.3)(3) følger, at fremstillingen ovenfor er en uforkortelig primærdekomposition af hovedidealet  $(f)$ .

(4) Lad  $\mathfrak{m}$  være et maksimalideal og lad  $\mathfrak{p}$  være et primideal forskelligt fra  $\mathfrak{m}$  og således at  $\mathfrak{p} \not\subseteq \mathfrak{m}^2$ . Betragt fællesmængden,

$$\mathfrak{a} = \mathfrak{p} \cap \mathfrak{m}^2. \quad (3.6.4)$$

Det ses ganske som under (1) eller (2), at (3.6.4) er en uforkortelig primærdekomposition. Primidealene  $\mathfrak{m}$  og  $\mathfrak{p}$  er altså de associerede primidealer til  $R/\mathfrak{a}$ . Hvis  $\mathfrak{p} \subseteq \mathfrak{m}$  (og dette er ikke udelukket), så er  $\mathfrak{p}$  det eneste minimale primideal for  $R/\mathfrak{a}$  og  $\mathfrak{m}$  er et indlejret primideal.

**(3.7) Bemærkning.** Dekompositionssætningen kan specielt anvendes på et ideal  $\mathfrak{a}$  i  $R$ . Som konsekvens fås en uforkortelig primærdekomposition,

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_q,$$

hvor idealet  $\mathfrak{q}_j$  er  $\mathfrak{p}_j$ -primært. De minimale primidealer  $\mathfrak{p}$  for  $R/\mathfrak{a}$  er de minimale blandt primidealene, der omfatter  $\mathfrak{a}$ , jfr Eksempel (1.6). Hvis  $\mathfrak{p}_j$  er et sådant primideal, så er  $\mathfrak{q}_j$  entydigt bestemt, nemlig som kernen for den sammensatte homomorfi  $R \rightarrow R/\mathfrak{a} \rightarrow (R/\mathfrak{a})_{\mathfrak{p}_j}$ . Her er kvotienten  $(R/\mathfrak{a})_{\mathfrak{p}_j}$  ifølge Lokaliseringsprincippet lig med  $R_{\mathfrak{p}_j}/\mathfrak{a}R_{\mathfrak{p}_j}$ . Heraf ses, at  $\mathfrak{q}_j$  er kontraktionen af ekstensionen  $\mathfrak{a}R_{\mathfrak{p}_j}$ .

Specielt ses, at hvis  $\mathfrak{q}$  er et  $\mathfrak{p}$ -primært ideal, så er homomorfien  $R/\mathfrak{q} \rightarrow R_{\mathfrak{p}}/\mathfrak{q}R_{\mathfrak{p}}$  injektiv. Hvis  $\mathfrak{p} = \mathfrak{m}$  er et maksimalideal, følger det endda af Korollar (2.5), at denne homomorfi er en isomorfi. Specielt fremhæves for en potens  $\mathfrak{m}^i$ , at lokalisering i  $\mathfrak{m}$  inducerer en isomorfi,

$$R/\mathfrak{m}^i \xrightarrow{\sim} R_{\mathfrak{m}}/\mathfrak{m}^i R_{\mathfrak{m}}.$$

#### 4. Valuationsringe og Dedekindringe.

**(4.1) Lemma.** *Antag, at  $R$  er et (noethersk) integritetsområde. Da har hvert element  $a$  i  $R$ , som ikke er nul eller en enhed, en irreducibel opløsning, dvs der findes en fremstilling af  $a$  som et produkt af irreducible elementer,*

$$a = q_1 \cdots q_n. \quad (*)$$

*Bevis.* Beviset er indirekte, ved noethersk induktion. Antag, at der findes elementer  $b$ , som ikke er nul og ikke er enheder og ikke kan skrives som produkt af irreducible elementer. Lad  $\mathcal{S}$  betegne mængden af hovedideal ( $b$ ) frembragt af sådanne elementer  $b$ . Der findes da i  $\mathcal{S}$  et hovedideal ( $b$ ), der er maksimalt blandt hovedidealene i  $\mathcal{S}$ . Elementet  $b$  kan specielt ikke være irreducibelt, og det er forskelligt fra nul og ikke en enhed. Følgelig er  $b$  et produkt  $b = b_1 b_2$ , hvor faktorerne  $b_i$  ikke er enheder. Nu er  $(b) \subset (b_2)$ . Ellers ville lighed nemlig gælde, og så ville  $b_2$  kunne skrives  $b_2 = ab = ab_1 b_2$ ; da nul-reglen gælder, ville det følge, at  $1 = ab_1$ , i modstrid med at  $b_1$  ikke er en enhed. Tilsvarende er  $(b) \subset (b_1)$ .

Af  $(b) \subset (b_i)$  følger, at hovedidealene ( $b_i$ ) ikke tilhører  $\mathcal{S}$ . Heraf følger videre, at  $b_i$  er et produkt af irreducible elementer. Men det er i modstrid med at  $b = b_1 b_2$  og  $b$  ikke er et produkt af irreducible elementer.  $\square$

**(4.2) Sætning.** *Lad  $R$  være en lokal (noethersk) ring med maksimalidealet  $\mathfrak{m}$ . Antag, at  $R$  er et integritetsområde, men ikke et legeme. Da er følgende betingelser ækvivalente:*

- (i) *Maksimalidealet  $\mathfrak{m}$  er et hovedideal.*
- (ii) *Idealerne i  $R$  er totalt ordnede ved inklusion.*
- (iii) *Ringens  $R$  er et hovedidealområde.*

*Bevis.* „(i) $\Rightarrow$ (ii)“. Antag, at  $\mathfrak{m} = (p)$  er hovedidealet frembragt af et element  $p$  i  $R$ . Da  $R$  ikke er et legeme, er  $p \neq 0$ . Videre er  $(p)$  et maksimalideal, og dermed et primideal. Altså er  $p$  et primelement. Specielt er  $p$  et irreducibelt element. Det påstås, at  $p$ , på nær multiplikation med en enhed, er det eneste irreducible element. Betragt nemlig et irreducibelt element  $q$ . Specielt er  $q$  da ikke en enhed, og følgelig er  $q$  element i den lokale rings maksimalideal. Med andre ord er  $q \in (p)$ , så  $q$  kan skrives  $q = rp$ . Da  $q$  er irreducibelt, er  $r$  en enhed.

Det følger af Lemma (4.1), at hvert element  $a$ , som ikke er nul og som ikke er en enhed, har en fremstilling som produkt af irreducible elementer. Af det allerede viste følger, at denne fremstilling har formen,

$$a = up^n, \quad (4.2.1)$$

hvor  $u$  er en enhed og  $n \geq 1$ . For enhederne i  $R$  fås en fremstilling (4.2.1) med  $n = 0$ .

Det påstås nu, at samtlige idealer i  $R$  er følgende:

$$(0) \subset \cdots \subset (p^{n+1}) \subset (p^n) \subset \cdots \subset (p) \subset (1).$$

Af denne påstand følger øjensynlig (ii). For at vise påstanden betragtes et vilkårligt ideal  $\mathfrak{a} \neq (0)$  i  $R$ . Der findes da elementer  $a$  i  $\mathfrak{a}$  som er forskellige fra 0. Vælg nu blandt alle

30. marts 2007

sådanne elementer  $a$  et, for hvilket fremstillingen (4.2.1) har det mindst mulige  $n$ . Da  $a$  er valgt i  $\mathfrak{a}$ , er  $p^n = u^{-1}a$  element i  $\mathfrak{a}$ . Følgelig er

$$(p^n) \subseteq \mathfrak{a}.$$

Omvendt har ethvert element  $b \neq 0$  i  $\mathfrak{a}$  en fremstilling af formen (4.2.1), dvs af formen  $b = vp^m$ ; valget af  $n$  sikrer, at  $m \geq n$ , og så er  $b = vp^{m-n}p^n$  element i  $(p^n)$ . Altså er  $\mathfrak{a} = (p^n)$ . Hermed er den ønskede påstand, og specielt betingelsen (ii) eftervist.

„(ii) $\Rightarrow$ (iii)“. Antag, at idealerne i  $R$  er totalt ordnede. Heraf følger først, at ethvert ideal  $(a, b)$  frembragt af 2 elementer er et hovedideal. Af hovedidealene  $(a)$  og  $(b)$  vil nemlig et, fx  $(b)$ , omfatte det andet, og af  $(a) \subseteq (b)$  følger, at summen  $(a, b) = (a) + (b)$  er lig med  $(b)$ . I almindelighed er  $(a_1, \dots, a_n) = (a_1, \dots, a_{n-1}) + (a_n)$ , så ved induktion følger, at hvert endeligt frembragt ideal er et hovedideal. Da  $R$  er noethersk, er betingelsen (iii) altså opfyldt.

Implikationen „(iii) $\Rightarrow$ (i)“ er trivial. Hermed er ækvivalensen bevist.  $\square$

**(4.3) Definition.** En lokal (noethersk) ring, som er et integritetsområde og ikke et legeme og opfylder de ækvivalente betingelser i Sætning (4.2), kaldes en (*diskret*) *valuationsring*.

**(4.4) Note.** Betingelsen (ii) har mening for enhver ikke nødvendigvis noethersk ring, og en ring, der opfylder denne betingelse, kaldes ofte en valuationsring. Adjektivet „diskret“ går essentielt på forudsætningen om at ringen i Definition (4.3), ligesom ellers i dette kapitel, forudsættes at være noethersk.

**(4.5) Bemærkning.** Antag, at  $R$  er lokal, med maksimalidealet  $\mathfrak{m}$ , og lad  $k := R/\mathfrak{m}$  betegne restklasselegemet. Kvotienten  $\mathfrak{m}^i/\mathfrak{m}^{i+1}$  er da en modul over kvotientringen  $R/\mathfrak{m}$ , dvs et vektorrum over  $k$ . Hvis  $R$  er en valuationsring, så er

$$\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} = 1 \text{ for alle } i,$$

thi potensen  $\mathfrak{m}^i$  er hovedidealet  $(p^i)$ , og det er klart, at  $r \mapsto rp^i$  inducerer en isomorfi af  $R/(p)$  på  $(p^i)/(p^{i+1})$ . Det følger i øvrigt af Nakayama's Lemma, at dimensionen  $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}$  er lig med det minimale antal frembringere for idealet  $\mathfrak{m}^i$ . Betingelsen (i) Sætning (4.2) kan således udtrykkes ved ligningen  $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ .

**(4.6) Eksempel.** Antag, at  $R$  er en faktoriel ring. For hvert irreducibelt element  $p$  er hovedidealet  $(p)$  da et primideal. Brøkringen  $R_{(p)}$ , der fås ved lokalisering i primidealet  $(p)$ , er en valuationsring, thi maksimalidealet i brøkringen er ekstensionen af hovedidealet  $(p)$ , og det er derfor et hovedideal. Betingelsen (4.2)(i) er således opfyldt.

Specielt gælder for hvert primtal  $p$ , at den lokale ring  $\mathbb{Z}_{(p)}$ , der består af rationale tal af formen  $a/s$ , hvor  $s$  ikke er delelig med  $p$ , er en valuationsring.

*Potensrækkeringen*  $R[[X]]$  består af uendelige følger  $f = (a_0, a_1, a_2, \dots)$  organiseret som ring med addition og multiplikation svarende til det, der kendes for polynomier. Ofte skrives  $f = a_0 + a_1X + a_2X^2 + \dots$ , hvor man bedst kan opfatte  $X^i$  som en „pladsholder“. Det er ikke svært at vise, at potensrækkeringen  $k[[X]]$  med koefficienter i et legeme  $k$  er en valuationsring.

