

Endelighedsbetingelser

1. Endeligt frembragte moduler.

(1.1) Endeligt frembragt modul. Lad M være en R -modul. For givne elementer v_1, \dots, v_m i M betegnes da med

$$Rv_1 + \dots + Rv_m$$

delmængden af M bestående af de elementer, der har formen

$$r_1v_1 + \dots + r_mv_m \quad \text{med } r_i \in R.$$

Øjensynlig er denne delmængde en undermodul i M , endda den mindste, der indeholder v_i 'erne. Den kaldes undermodulen *frembragt* af v_i 'erne.

Modulen M siges at være *endeligt frembragt*, hvis der i M findes endelig mange elementer v_1, \dots, v_m , som *frembringer* M , dvs opfylder at

$$M = Rv_1 + \dots + Rv_m.$$

En modul M , der er frembragt af et enkelt element, dvs har formen $M = Rv$, siges også at være en *cyklisk modul*.

(1.2) Observation. Modulen R^n er endeligt frembragt, nemlig frembragt af de n -sæt, der har 0 på alle pladser på nær et enkelt 1 på én plads. Specielt er R , som R -modul, endeligt frembragt (endda cyklisk).

For givne elementer v_1, \dots, v_m i en modul M defineres en R -lineær afbildning $R^m \rightarrow M$ ved

$$(r_1, \dots, r_m) \mapsto r_1v_1 + \dots + r_mv_m.$$

Billedet for denne afbildning er øjensynlig undermodulen frembragt af v_i 'erne. Heraf følger let, at en modul M er endeligt frembragt, hvis og kun hvis M er homomorft billede af en modul R^m for passende m , altså hvis og kun hvis M er isomorf med en kvotient R^m/K , hvor K er en undermodul i R^m .

Tilsvarende følger det, at modulen M er cyklisk, hvis og kun hvis M som modul er isomorf med en kvotient R/\mathfrak{a} , hvor \mathfrak{a} er et ideal i R .

Hvis ringen R er et legeme, er moduler over R som bekendt blot vektorrum. Et vektorrum er øjensynlig endeligt frembragt, hvis og kun hvis det er endeligdimensionalt, og det er cyklisk, hvis og kun hvis det enten er 1-dimensionalt eller består alene af 0.

(1.3) Sætning. Lad der være givet en eksakt følge af R -moduler,

$$N \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0.$$

Hvis M er endelig frembragt, så er P endelig frembragt. Hvis både N og P er endeligt frembragte, så er M endelig frembragt.

Bevis. Hvis elementer v_1, \dots, v_m frembringer M , så vil deres billeder i P frembringe P , fordi homomorfien $\psi: M \rightarrow P$ er surjektiv. Heraf følger den første påstand.

For at vise den anden påstand betragtes elementer v_1, \dots, v_n som frembringer N og elementer u_1, \dots, u_p , som frembringer P . Da ψ er surjektiv, findes elementer w_1, \dots, w_p i M , som ved ψ afbildes på u_i 'erne. Det påstås, at M er frembragt af de endelig mange elementer $\varphi v_1, \dots, \varphi v_n, w_1, \dots, w_p$. Betragt hertil et vilkårligt element x i M . Billedet af x i P er da en linearkombination af u_i 'erne, $\psi x = \sum r_i u_i$. Den tilsvarende linearkombination af w_i 'erne, $\sum r_i w_i$, har nu samme billede i P som x , og differensen,

$$x - \sum_i r_i w_i,$$

tilhører derfor kernen for ψ . Da følgen er eksakt, vil differensen altså tilhøre billedet φN . Dette billede er frembragt af φv_j 'erne, da v_j 'erne frembringer N . Differensen er derfor en linearkombination af φv_j 'erne. Heraf ses, at elementet x er en linearkombination af w_i 'erne og φv_j 'erne, som påstået. \square

(1.4) Note. Beviset for Sætningen giver mere information: Hvis P er frembragt af p elementer og N er frembragt af n elementer, så er M frembragt af $p + n$ elementer.

(1.5) Bemærkning. Den oplagte anvendelse af sætningen er på den eksakte følge hørende til en undermodul N af M ,

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

Hvis N og M/N er endeligt frembragte, så er M endeligt frembragt. Hvis M er endeligt frembragt, så er kvotienten M/N endeligt frembragt.

Bemærk, at man ikke, når M er endeligt frembragt, kan slutte at undermodulen N i M nødvendigvis er endeligt frembragt. I R , der jo som R -modul er frembragt af ét element (nemlig af et-elementet $1 \in R$), er alle idealer ikke nødvendigvis endeligt frembragte.

(1.6) Eksempel. Lad R betegne ringen af reelle talfølger (a_n) . Det er klart, at de følger (a_n) , der er 0 fra et vist trin, udgør et ideal I i R . Det er let at se, at idealet I ikke er endeligt frembragt.

(1.7) Definition. Lad M være en R -modul. Ved en (endelig) *filtration* i M forstås en følge af undermoduler,

$$0 = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = M.$$

De successive kvotienter F_i/F_{i-1} for $i = 1, \dots, n$ kaldes også *filtrationens kvotienter*. Den i 'te kvotient F_i/F_{i-1} er øjensynlig 0, netop når $F_{i-1} = F_i$. Antallet af kvotienter forskellige fra 0 er altså antallet af skarpe \subset 'er i filtrationen. Dette antal kaldes *filtrationens længde*.

(1.8) Eksempel. Antag, at M er frembragt af elementer v_1, \dots, v_m . Sæt

$$F_i := Rv_1 + \dots + Rv_i$$

for $i = 0, \dots, m$ (for $i = 0$ er $F_0 = 0$). Da udgør F_i 'erne en filtration af M . Bemærk, at kvotienten F_i/F_{i-1} er frembragt af billedet af v_i , idet der modulo F_{i-1} gælder, at $\sum_{j=1}^i r_j v_j \equiv r_i v_i$. Filtrationens kvotienter er altså cykliske.

(1.9) Observation. Ofte er det bekvemt at kunne udlede egenskaber for en modul M ud fra egenskaberne ved kvotienterne i en given filtration $0 = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = M$ af M . Lad os fx vise, at hvis kvotienterne F_i/F_{i-1} er endeligt frembragte, så er M endeligt frembragt.

Vi viser ved induktion efter i , for $i = 1, \dots, n$, at F_i er endeligt frembragt. For $i = 1$ er $F_1 = F_1/F_0$ endeligt frembragt. Til induktionsskridtet anvendes den eksakte følge,

$$0 \rightarrow F_{i-1} \rightarrow F_i \rightarrow F_i/F_{i-1} \rightarrow 0.$$

Induktivt kan det antages, at F_{i-1} er endeligt frembragt, og F_i/F_{i-1} er endeligt frembragt ifølge antagelsen. Af Sætning (1.3) følger derfor, at F_i er endeligt frembragt.

(1.10) Observation. Betragt en direkte sum af moduler, $M = M_1 \oplus \dots \oplus M_n$. Sæt

$$F_i := M_1 \oplus \dots \oplus M_i$$

for $i = 0, \dots, n$ (for $i = 0$ er $F_0 = 0$). Her kan F_i opfattes som undermodul af M : Den direkte sum M består af n -sæt, og F_i består af de n -sæt, der har 0 på pladser med index større end i . Herved udgør F_i 'erne en filtration af M . Den i 'te kvotient F_i/F_{i-1} kan identificeres med M_i . Dette følger af at der generelt for en direkte sum $F \oplus N$ gælder, at $(F \oplus N)/F = N$. Af de foregående resultater følger umiddelbart: M er endeligt frembragt, hvis og kun hvis hver „summand“ M_i er endeligt frembragt.

(1.11) Opgaver.

- U4 1. Vis, at \mathbb{Q} som \mathbb{Z} -modul ikke er endeligt frembragt.
- U4 2. Betragt delringen $R = \mathbb{Z} \oplus \mathbb{Q}X \oplus \mathbb{Q}X^2 \oplus \mathbb{Q}X^3 \oplus \dots \subseteq \mathbb{Q}[X]$. Vis, at idealet af polynomier $f \in R$ med $f(0) = 0$ ikke er endeligt frembragt.
3. Præciser hvad der menes med polynomiumsringen $R = \mathbb{Q}[X_1, X_2, X_3, \dots]$ i numerabelt mange variable. Vis, at idealet bestående af polynomier „uden“ konstantled, dvs med konstantled lig med 0, ikke er endeligt frembragt.
- U4 4. Vis, at en kommutativ gruppe (altså en \mathbb{Z} -modul) M er endelig, hvis og kun hvis M har en filtration $(0) = F_0 \subseteq \dots \subseteq F_n = M$, hvor kvotienterne F_i/F_{i-1} er endelige. Vis, at „i så fald“ er $|M| = |F_1/F_0| \cdots |F_n/F_{n-1}|$.
- U5 5. Lad der være givet en filtration $0 = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = M$ i M med cykliske kvotienter $F_i/F_{i-1} = R/\alpha_i$ for $i = 1, \dots, n$. Vis, at produktet $\alpha_1 \cdots \alpha_n$ er indeholdt i annullatoren $\text{Ann } M$.

- U6 **6.** Vis, at en R -modul M er fri, hvis og kun hvis M har en endelig filtration, hvor alle de successive kvotienter er isomorfe med R .
- 7.** Lad M være en endeligt frembragt R -modul og lad \mathfrak{a} være et ideal således, at for alle $x \neq 0$ i M er $\mathfrak{a}x \subset Rx$. Vis, at hvis $M \neq 0$, så er $\mathfrak{a}M \subset M$. [Vink: Indirekte, som i beviset for Nakayama's Lemma; brug, at en ligning $(1 - a)e = 0$, med $a \in \mathfrak{a}$ og $e \in M$ medfører, at $e = 0$.
- H3 **8.** En ring R , hvori idealerne er totalt ordnede (dvs, at for vilkårlige to idealer \mathfrak{a} og \mathfrak{b} er enten $\mathfrak{a} \subseteq \mathfrak{b}$ eller $\mathfrak{b} \subseteq \mathfrak{a}$), kaldes en valuationsring. Vis, at i en valuationsring er ethvert endeligt frembragt ideal et hovedideal.
- U9 **9.** Lad $f: M \rightarrow N$ være en homomorfi mellem moduler, der har den samme endelige længde. Vis, at følgende betingelser er ækvivalente: (i) f er surjektiv; (ii) f er injektiv; (iii) f er en isomorfi.

2. Moduler af endelig længde.

(2.1) Definition. Lad M være en R -modul. Ved *længden* af M forstås supremum af længderne af filtrationerne i M . Længden af M betegnes også $\text{long } M$. Længden kan være ∞ , nemlig hvis der findes filtrationer i M af vilkårlig stor længde. At længden er endelig betyder, at der er en øvre grænse for længden af en filtration i M , altså en øvre grænse for hvor mange skarpe inklusioner, der kan være i en filtration af M .

I enhver modul $M \neq 0$ er $(0) \subset M$ en filtration af længde 1. Nulmodulen 0 er altså den eneste modul af længde 0.

(2.2) Sætning. For en R -modul M er følgende betingelser ækvivalente:

- (i) M har længde 1.
- (ii) $M \neq 0$ og de eneste undermoduler i M er de trivielle, nemlig (0) og M .
- (iii) $M \neq 0$ og for hvert element $v \neq 0$ i M gælder $M = Rv$.
- (iv) M er modul-isomorf med en kvotient R/\mathfrak{m} , hvor \mathfrak{m} er et maksimalideal i R .

Bevis. At en modul M har længde mindst 2 betyder, at der i M findes en filtration

$$(0) \subset F_1 \subset M,$$

altså at M har en ikke-triviel undermodul. Betingelserne (i) og (ii) er derfor ækvivalente.

At (ii) \Rightarrow (iii) er klart. For hvert element $v \neq 0$ i M er Rv jo en undermodul, og $Rv \neq (0)$; hvis M kun har de trivielle undermoduler, må der altså gælde $Rv = M$. Antag omvendt, at (iii) er opfyldt. Lad $F_1 \neq (0)$ være en undermodul i M . Da $F_1 \neq (0)$, findes $v \neq 0$ i F_1 . Af $Rv \subseteq F_1 \subseteq M$ og (iii) følger nu, at $F_1 = M$. Det er således vist, at M kun har de to trivielle undermoduler, så (ii) gælder.

Betingelserne (ii) og (iii) er således ækvivalente. Er de opfyldt, må M specielt være cyklisk ifølge (iii), altså isomorf med en kvotient R/\mathfrak{m} , hvor \mathfrak{m} er et ideal i R . Det er derfor nok at vise for en kvotient $M = R/\mathfrak{m}$, at (ii) er opfyldt, hvis og kun hvis \mathfrak{m} er et maximalideal. Denne sidste påstand følger umiddelbart af Noether's anden Isomorfisætning: undermodulerne i kvotienten R/\mathfrak{m} svarer bijektivt til undermoduler (dvs idealer) $\mathfrak{a} \supseteq \mathfrak{m}$. \square

(2.3) Definition. En modul M , der opfylder de ækvivalente betingelser i Sætning (2.2), kaldes en *simpel modul*.

Lad M være en modul, og betragt i M en filtration med skarpe inklusioner,

$$(0) = F_0 \subset F_1 \subset \cdots \subset F_n = M.$$

Undermoduler F mellem F_{i-1} og F_i , dvs som opfylder $F_{i-1} \subseteq F \subseteq F_i$, svarer ifølge Noether's anden Isomorfisætning til undermoduler af kvotienten F_i/F_{i-1} . Af betingelsen (2.2)(ii) følger derfor, at kvotienten F_i/F_{i-1} er en simpel modul, hvis og kun hvis der ikke findes undermoduler F , som ligger „ægte“ mellem F_{i-1} og F_i . Med andre ord: filtrationen er *uforfinelig*, hvis og kun hvis alle kvotienterne F_i/F_{i-1} er simple moduler.

Hvis modulen M har endelig længde, så findes naturligvis en sådan uforfinelig filtration i M . Vi skal senere se, at det omvendte også gælder.

30. marts 2007

(2.4) Sætning. Lad der være givet en eksakt følge af moduler,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Da gælder formelen,

$$\text{long } M = \text{long } M' + \text{long } M''.$$

Bevis. Vi kan antage, at M' er en undermodul i M og at $M'' = M/M'$ er den tilhørende kvotientmodul. Vi viser ligheden ved at vise de to uligheder.

„ \geq “: Betragt to vilkårlige filtrationer i M' og M'' ,

$$(0) \subseteq F'_1 \subseteq \cdots \subseteq F'_{n-1} \subseteq M', \quad (0) \subseteq F''_1 \subseteq \cdots \subseteq F''_{m-1} \subseteq M'',$$

og lad k' og k'' betegne længderne af filtrationerne. Ifølge Noether's anden Isomorfiætning svarer undermodulerne F''_i af kvotienten M'' til undermoduler F_i af M , således at $F_i \supseteq M'$. I M fås således en filtration,

$$(0) \subseteq F'_1 \subseteq \cdots \subseteq F'_{n-1} \subseteq M' \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq M.$$

I denne filtration er der ialt $k' + k''$ skarpe inklusioner, så filtrationens længde er $k' + k''$. Altså er $k' + k'' \leq \text{long } M$. Da filtrationerne i M' og M'' var vilkårlige, følger det endelig, at

$$\text{long } M \geq \text{long } M' + \text{long } M''.$$

„ \leq “: For at vise den omvendte ulighed betragtes en vilkårlig filtration i M ,

$$(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M.$$

Sæt $F'_i := F_i \cap M'$, og lad F''_i betegne billedet af F_i i kvotienten M/M' . Da udgør modulerne F'_i en filtration i undermodulen M' , og modulerne F''_i udgør en filtration i kvotientmodulen M/M' , og F'_i er kernen for den surjektive homomorfi $F_i \rightarrow F''_i$. Af Slangelemmaet får vi så eksakte følger,

$$0 \longrightarrow F'_i/F'_{i-1} \longrightarrow F_i/F_{i-1} \longrightarrow F''_i/F''_{i-1} \longrightarrow 0. \quad (*)$$

Lad nu k, k', k'' være længderne af filtrationerne i M , i M' og i M/M' . I (*) er den midterste modul altså forskellig fra 0 for k værdier af $i = 1, \dots, n$. Af eksaktheden følger derfor, at for hver af disse k værdier af i er mindst én af de to moduler, F'_i/F'_{i-1} og F''_i/F''_{i-1} , forskellig fra 0. Den første er forskellig fra 0 for k' værdier af i , den anden er forskellig fra 0 for k'' værdier af i . Heraf fås uligheden,

$$k \leq k' + k''.$$

Ifølge definitionen er $k' \leq \text{long } M'$ og $k'' \leq \text{long } M''$. Uligheden ovenfor medfører derfor, at $k \leq \text{long } M' + \text{long } M''$. Da k var længden af en vilkårlig filtration i M , følger det endelig, at

$$\text{long } M \leq \text{long } M' + \text{long } M''.$$

Herved er den omvendte ulighed, og dermed den søgte formel, bevist. □

(2.5) Korollar. (1) For en undermodul N i M gælder formelen,

$$\text{long } M = \text{long } N + \text{long } M/N.$$

(2) For en filtration $0 = F_0 \subseteq \dots \subseteq F_n = M$ gælder formelen,

$$\text{long } M = \sum \text{long } F_i/F_{i-1}.$$

(3) For en direkte sum $M = M_1 \oplus \dots \oplus M_n$ gælder formelen,

$$\text{long } M = \sum \text{long } M_i.$$

Bevis. (1) Da følgen $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ er eksakt, følger (1) umiddelbart af sætningen. Påstand (2) følger ved induktion efter n af sætningen ved hjælp af den eksakte følge,

$$0 \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow F_n/F_{n-1} \longrightarrow 0.$$

Endelig følger (3) af (2) ved at betragte filtrationen defineret ved $F_i := M_1 \oplus \dots \oplus M_i$. \square

(2.6) Bemærkning. Bemærk, at de anførte formler gælder, når der på oplagt måde regnes med ∞ . Fx er det således en del af udsagnet i (2.5)(1), at modulen M har endelig længde, hvis og kun hvis både N og M/N har endelig længde.

(2.7) Korollar. Modulen M har endelig længde, hvis og kun hvis der i M findes en uforfinelig filtration,

$$(0) = F_0 \subset F_1 \subset \dots \subset F_n = M. \quad (*)$$

Alle uforfinelige filtrationer har samme længde, nemlig længden af M .

Bevis. Hvis M har endelig længde, så findes øjensynlig en uforfinelig filtration (*) med $n = \text{long } M$. Antag omvendt, at (*) er en uforfinelig filtration. Da er alle kvotienterne F_i/F_{i-1} simple moduler, dvs af længde 1. Tallet n er filtrationens længde. Af Korollar (2.5)(2) følger, at $\text{long } M = n$. Hermed er påstandene bevist. \square

(2.8) Eksempel. De simple \mathbb{Z} -moduler er kvotienterne $\mathbb{Z}/(p)$ for et primtal p . De er specielt endelige. Heraf følger let, at en \mathbb{Z} -modul M har endelig længde, hvis og kun hvis M er endelig. Antag, at M har længde n . I en uforfinelig filtration af M forekommer så kvotienterne \mathbb{Z}/p_i for n ikke nødvendigvis forskellige primtal p_i . Det følger let, at der så gælder $|M| = p_1 \cdot \dots \cdot p_n$.

De simple $\mathbb{C}[X]$ -moduler er kvotienterne $\mathbb{C}[X]/(X - \alpha)$ for $\alpha \in \mathbb{C}$. De er specielt 1-dimensionale som vektorrum over \mathbb{C} . Heraf følger let, at en $\mathbb{C}[X]$ -modul M har endelig længde, hvis og kun hvis M har endelig dimension som vektorrum over \mathbb{C} , og at der faktisk gælder ligheden $\text{long } M = \dim_{\mathbb{C}} M$.

(2.9) Opgaver.

- U4 1. Hvor langt er et vektorrum?
- U4 2. Angiv i \mathbb{Z} som \mathbb{Z} -modul en filtration af længde 999.
3. Vis, at enhver modul af endelig længde er endeligt frembragt.
- U4 4. Vis, hvis ringen R som R -modul har endelig længde, så har enhver endeligt frembragt R -modul også endelig længde.
- U8 5. Lad $0 \rightarrow M_n \rightarrow \dots \rightarrow M_1 \rightarrow M_0 \rightarrow 0$ være en exakt følge af moduler af endelig længde. Vis, at $\sum (-1)^i \text{long } M_i = 0$.
6. Vis, at en $\mathbb{R}[X]$ -modul M har endelig længde, hvis og kun hvis M har endelig dimension som vektorrum over \mathbb{R} .
7. Lad \mathfrak{m} være et fast maksimalideal i R . For hver uforfinelig filtration i en modul M kan vi spørge om antallet af gange den simple modul R/\mathfrak{m} forekommer blandt filtrationens kvotienter. Lad $\text{long}_{\mathfrak{m}} M$ betegne det største antal gange R/\mathfrak{m} forekommer som simpel kvotient i en uforfinelig filtration af M . Vis, at $\text{long}_{\mathfrak{m}} R/\mathfrak{m} = 1$, og at $\text{long } R/\mathfrak{n} = 0$, når \mathfrak{n} er et maksimalideal, $\mathfrak{n} \neq \mathfrak{m}$. Vis, for en undermodul M' af M , at $\text{long}_{\mathfrak{m}} M = \text{long}_{\mathfrak{m}} M' + \text{long}_{\mathfrak{m}} M/M'$. Vis, at i enhver filtration af M forekommer R/\mathfrak{m} som simpel kvotient præcis $\text{long}_{\mathfrak{m}} M$ gange.
- H2 8. Antag, at R er et PID, og at $a = p_1^{v_1} \cdots p_r^{v_r}$ er en primopløsning. Bestem længden af R -modulen $R/(a)$.
- U5 9. Antag, at R er et PID og ikke et legeme. Lad M være en endeligt frembragt R -modul. Vis, at M har endelig længde, hvis og kun hvis $\text{Ann } M \neq (0)$.
- H3 10. Lad M være en endeligt frembragt modul over en noethersk ring R . Vis, at M har endelig længde, hvis og kun hvis der findes endelig mange maksimalidealer $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ (ikke nødvendigvis forskellige) i R således, at $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$.
Hvad udsiger resultatet, hvis R er lokal?

3. Lidt om noetherske ringe og moduler.

(3.1) Sætning. For en modul M er følgende betingelser ækvivalente:

- (i) Enhver undermodul i M er endeligt frembragt.
- (ii) I enhver stigende kæde af undermoduler i M ,

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots,$$

gælder lighed fra et vist trin.

- (iii) I enhver ikke-tom mængde S af undermoduler i M findes en undermodul, der er maksimal blandt undermodulerne i S .

Bevis. (i) \Rightarrow (ii): Betragt en kæde af undermoduler som i (ii), og dan foreningsmængden,

$$N := \bigcup_i M_i.$$

Foreningsmængden N er stabil under addition. Lad nemlig x og y være elementer i N . Da findes i, j så at $x \in M_i$ og $y \in M_j$. Det kan antages, at $i \leq j$. Men så er $M_i \subseteq M_j$, og undermodulen M_j vil altså indeholde både x og y og dermed også summen $x + y$. Følgelig tilhører $x + y$ foreningsmængden N .

Det er klart, at nul-elementet tilhører N , og det er let at vise, at N er stabil under multiplikation med skalar. Da N også er stabil under addition, er N derfor en undermodul. Ifølge antagelsen (i) er N endeligt frembragt. Der findes altså endelig mange elementer v_1, \dots, v_m i N så at

$$N = Rv_1 + \dots + Rv_m.$$

Hver af frembringerne v_k tilhører en af undermodulerne M_i . Af disse endelig mange M_i 'er er en, fx M_n , den største. Da hver af frembringerne v_k tilhører M_n , gælder

$$N = Rv_1 + \dots + Rv_m \subseteq M_n \subseteq M_{n+1} \subseteq \dots \subseteq \bigcup M_i = N.$$

Det følger, at lighed gælder overalt i inklusionerne ovenfor. Specielt gælder altså at $M_n = M_{n+1} = \dots$, hvormed (ii) er bevist.

(ii) \Rightarrow (i): Antag, indirekte, at der i M findes en undermodul N , der ikke er endeligt frembragt. Vælg et element v_1 i N (fx $v_1 = 0$), og sæt $M_1 := Rv_1$. Da $v_1 \in N$, er $M_1 \subseteq N$, og da N specielt ikke er frembragt af ét element, gælder endda

$$M_1 \subset N.$$

Vælg nu v_2 i overskudsmængden $N \setminus M_1$, og sæt $M_2 := M_1 + Rv_2$. Øjensynlig er $M_1 \subseteq M_2$, og da M_2 indeholder v_2 , som var valgt i komplementærmængden til M_1 , gælder endda

30. marts 2007

$M_1 \subset M_2$. Videre er M_2 frembragt af v_1 og v_2 , som begge var valgt i N ; følgelig er $M_2 \subseteq N$. Da N specielt ikke kan være frembragt af to elementer, fås endda

$$M_1 \subset M_2 \subset N.$$

Vælg nu v_3 i overskudsmængden $N \setminus M_2$, og sæt $M_3 := M_2 + Rv_3$. Idet processen fortsættes induktivt, fås en uendelig følge af undermoduler,

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

(der alle er skarpt indeholdt i N). Da dette er i modstrid med antagelsen (ii), er det indirekte bevis fuldført.

(ii) \iff (iii): Dette resultat gælder for enhver partielt ordnet mængde, og har intet at gøre med at vi her betragter undermoduler af en modul. Beviset overlades til læseren. \square

(3.2) Noethersk modul. En modul M , der opfylder de ækvivalente betingelser (i), (ii), (iii) i Sætning (3.1), kaldes en *noethersk modul*.

Bemærk forskellen og ligheden i definitionen af „noethersk“ og „endelig længde“. At M er noethersk betyder at i en given kæde af undermoduler,

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots,$$

kan der kun være endelig mange skarpe inklusioner. At M har endelig længde betyder at der er en på forhånd given øvre grænse for antallet af skarpe inklusioner.

(3.3) Sætning. Lad N være en undermodul i modulen M . Da er M noethersk, hvis og kun hvis både undermodulen N og kvotientmodulen M/N er noetherske.

Bevis. Antag først, at N og M/N er noetherske. Vi efterviser, at M opfylder betingelsen (3.1)(i). Lad altså K være en undermodul i M . Billedet K'' af K i M/N er da en undermodul i M/N . Altså er K'' endeligt frembragt, da M/N er noethersk. Fællesmængden $K' := K \cap N$ er en undermodul i N . Altså er K' endeligt frembragt, da N er noethersk. Restriktion af den kanoniske afbildning $M \rightarrow M/N$ til undermodulen K giver en eksakt følge,

$$0 \longrightarrow K' \longrightarrow K \longrightarrow K'' \longrightarrow 0.$$

Af Sætning (1.3) følger derfor, at K er endeligt frembragt. Da K var en vilkårlig undermodul i M , er M således noethersk.

Antag omvendt, at M er noethersk. Enhver undermodul K i N er da specielt en undermodul i M , og derfor endeligt frembragt, da M er noethersk. Altså er N noethersk. Betragt dernæst en undermodul L i M/N . Ifølge Noether's anden Isomorfisætning er L så homomorft billede af en undermodul K af M (endda med $K \supseteq N$). Da M er noethersk er K endeligt frembragt, og det homomorfe billede L er derfor ligeledes endeligt frembragt, jfr Sætning (1.3). Altså er M/N noethersk. \square

30. marts 2007

(3.4) Korollar. (1) For en eksakt følge $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ gælder, at M er noethersk, hvis og kun hvis M' og M'' er noetherske.

(2) For en filtration $(0) = F_0 \subseteq \cdots \subseteq F_n = M$ gælder, at M er noethersk, hvis og kun hvis alle kvotienterne F_i/F_{i-1} er noetherske.

(3) For en direkte sum $M = M_1 \oplus \cdots \oplus M_n$ gælder, at M er noethersk, hvis og kun hvis alle addenderne M_i er noetherske.

Bevis. Ifølge Isomorfisætningen er (1) blot en oversættelse af Sætningen. Påstand (2) følger ved induktion af (1), ved hjælp af den eksakte følge,

$$0 \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow F_n/F_{n-1} \longrightarrow 0.$$

Endelig følger (3) af (2) ved at betragte filtrationen i den direkte sum defineret ved $F_i := M_1 \oplus \cdots \oplus M_i$. □

(3.5) Definition. Ringen R kaldes en *noethersk ring*, hvis den er noethersk som R -modul. Undermodulerne i modulen R er netop idealerne i ringen R , så R er en noethersk ring, netop hvis ethvert ideal i R er endeligt frembragt.

(3.6) Sætning. Antag, at ringen R er noethersk. Enhver endeligt frembragt R -modul er da noethersk. Desuden er enhver kvotientring af R en noethersk ring.

Bevis. Modulen R^n er en direkte sum $R^n = R \oplus \cdots \oplus R$ med n addender. Af Korollar (3.4)(3) følger derfor, at R^n er en noethersk modul. Lad nu M være en endeligt frembragt R -modul. Da er M homomorft billede af R^n for passende n . Af Korollar (3.4)(1) følger derfor specielt, at M er noethersk.

Den sidste påstand følger af at idealerne i en kvotientring R/\mathfrak{a} netop er undermodulerne i kvotientmodulen R/\mathfrak{a} . □

(3.7) Eksempel. Enhver endelig ring er noethersk. Ethvert legeme er en noethersk ring. Enhver hovedidealring er noethersk. Specielt: ringen \mathbb{Z} og polynomiumsringen $k[X]$ over et legeme k er noetherske ringe.

(3.8) Hilbert's Basissætning. Lad R være en noethersk ring. Da er også polynomiumsringen $R[X]$ en noethersk ring.

Bevis. Vi viser, at polynomiumsringen $R[X]$ har egenskaben (3.1)(i). Betragt derfor et ideal \mathfrak{A} i $R[X]$. Lad $\mathfrak{l} = \mathfrak{l}(\mathfrak{A})$ betegne mængden bestående af de ledende koefficienter for polynomierne i \mathfrak{A} , samt elementet 0. Elementet $a \in R$ tilhører så \mathfrak{l} , hvis og kun hvis der i idealet \mathfrak{A} findes et polynomium af formen

$$aX^n + \cdots,$$

hvor „ \cdots “ står for en sum af led af lavere grad end det første.

Vi viser først, at delmængden \mathfrak{l} er et ideal i R . Det er klart, at 0 tilhører \mathfrak{l} . Videre følger af $a \in \mathfrak{l}$ og $r \in R$ at $ra \in \mathfrak{l}$, thi hvis $aX^n + \cdots$ tilhører \mathfrak{A} , så vil også polynomiet

$$raX^n + \cdots = r(aX^n + \cdots)$$

tilhøre \mathfrak{A} . Antag endelig, at $a, b \in \mathfrak{l}$. Der findes altså i \mathfrak{A} polynomier af formen $aX^n + \dots$ og $bX^m + \dots$. Det kan fx antages, at $n \geq m$. Da \mathfrak{A} er et ideal følger det, at også polynomiet

$$(a + b)X^n + \dots = (aX^n + \dots) + X^{n-m}(bX^m + \dots)$$

vil tilhøre \mathfrak{A} . Altså er også $a + b$ element i \mathfrak{l} . Hermed er vist, at \mathfrak{l} er et ideal i R .

Da R er noethersk, er idealet \mathfrak{l} endeligt frembragt. Der findes altså endelig mange polynomier,

$$P_i = a_i X^{n_i} + \dots,$$

hvis ledende koefficienter a_i frembringer \mathfrak{l} . Lad nu n_0 være den største af graderne n_i , og lad $\mathfrak{A}_{<n_0}$ betegne mængden af polynomier, der tilhører \mathfrak{A} og har grad mindre end n_0 . Det er klart, at $\mathfrak{A}_{<n_0}$ er en R -modul, nemlig en undermodul i R -modulen $R[X]_{<n_0}$ bestående af alle polynomier af grad mindre end n_0 . Den sidste R -modul er endeligt frembragt, nemlig frembragt af de n_0 monomier $1, X, \dots, X^{n_0-1}$. Da R er noethersk, følger det af Sætning (3.6) at $R[X]_{<n_0}$ er noethersk som R -modul. I undermodulen $\mathfrak{A}_{<n_0}$ findes derfor endelig mange polynomier Q_j , som frembringer $\mathfrak{A}_{<n_0}$ som R -modul.

Det påstås nu, at idealet \mathfrak{A} i $R[X]$ er frembragt af de endelig mange polynomier P_i og Q_j . Lad \mathfrak{B} betegne idealet frembragt af disse polynomier. Da polynomierne er valgt i \mathfrak{A} , er $\mathfrak{B} \subseteq \mathfrak{A}$. Omvendt skal det altså vises for hvert F i \mathfrak{A} , at F tilhører \mathfrak{B} . Denne påstand vises ved induktion efter graden n af F .

Hvis $n < n_0$ er påstanden klar, thi så tilhører F delmængden $\mathfrak{A}_{<n_0}$, og F er derfor endda en R -linearkombination af Q_j 'erne.

Hvis $n \geq n_0$ betragtes den ledende koefficient a i F . Da $F \in \mathfrak{A}$, er $a \in \mathfrak{l}$. Følgelig er a en R -linearkombination af a_i 'erne,

$$a = \sum r_i a_i.$$

Nu var $P_i = a_i X^{n_i} + \dots$ og $n \geq n_0 \geq n_i$, så linearkombinationen,

$$G := \sum r_i X^{n-n_i} P_i,$$

har grad n og ledende koefficient a . Linearkombinationen G har altså samme grad og samme ledende koefficient som F . Differensen $F - G$ har derfor lavere grad end F . Da G er en linearkombination af P_i 'erne, vil G tilhøre \mathfrak{B} . Videre er $F - G$ et polynomium i \mathfrak{A} og af lavere grad end F , så ifølge induktionsforudsætningen vil $F - G$ tilhøre \mathfrak{B} . Men så vil også $F = G + (F - G)$ tilhøre \mathfrak{B} , som påstået. Hermed er Sætningen bevist. \square

(3.9) Korollar. *Polynomiumsringen $k[X_1, \dots, X_r]$ i r variable, hvor k er et legeme eller $k = \mathbb{Z}$, er en noethersk ring.*

Bevis. Påstanden gælder generelt, når k er noethersk. Den vises ved induktion. Basissætningen giver både starten, $r = 1$, og induktionsskridtet, idet

$$R[X_1, \dots, X_r] = R[X_1, \dots, X_{r-1}][X_r].$$

\square

(3.10) Note. Det er Korollar (3.9) for et legeme k , der er den oprindelige „basissætning“. Resultatet udsiger, at hvert ideal i $k[X_1, \dots, X_r]$ er frembragt af endelig mange polynomier, dvs har en endelig „basis“.

(3.11) Opgaver.

- U4 **1.** Vis, at enhver kvadratisk talring R er noethersk. [Vink: Udnyt, at som \mathbb{Z} -modul er $R = \mathbb{Z}^2$, og at hvert ideal i R altså er en undergruppe af \mathbb{Z}^2 .]
- U4 **2.** Lad \mathfrak{a} være et ideal i en noethersk ring R , og sæt $\mathfrak{r} = \text{Rad } \mathfrak{a}$. Vis, at der findes et $N \in \mathbb{N}$ således, at $\mathfrak{r}^N \subseteq \mathfrak{a}$.
- U4 **3.** Lad R være et noethersk integritetsområde. Vis, at „irreducible opløsninger eksisterer“. Med andre ord: Vis, at hvert element $r \in R$, der ikke er 0 eller en enhed, kan skrives som produkt af irreducible elementer.
- U4 **4.** Vis, at hvis et ideal \mathfrak{a} ikke er et primideal, så findes idealer \mathfrak{b} og \mathfrak{c} med $\mathfrak{a} \subset \mathfrak{b}$ og $\mathfrak{a} \subset \mathfrak{c}$ og $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$. Vis, at i en noethersk ring R vil hvert ideal indeholde et produkt af primideal; mere præcist: til hvert ideal \mathfrak{a} findes primideal $\mathfrak{p}_i \supseteq \mathfrak{a}$ for $i = 1, \dots, s$ således, at $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{a}$.
- U5 **5.** Antag, at R er noethersk. Vis, at (0) er et produkt af primideal: $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$. Vis, at hvert primideal $\mathfrak{p} \subset R$ indeholder et \mathfrak{p}_i . Specielt er de minimale blandt idealerne \mathfrak{p}_i netop de minimale blandt primidealene i R . Vis, at $\text{Rad}(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$.
Vis for hvert ideal \mathfrak{a} , at der i mængden af primideal \mathfrak{p} med $\mathfrak{p} \supseteq \mathfrak{a}$ findes endelig mange minimale elementer. Vis, at hvis $\mathfrak{q}_1, \dots, \mathfrak{q}_q$ er disse minimale elementer, så er $\text{Rad}(\mathfrak{a}) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_q$.
- U5 **6.** Et ideal \mathfrak{q} kaldes *irreducibelt*, hvis \mathfrak{q} er et ægte ideal og \mathfrak{q} ikke kan skrives som fællemængde $\mathfrak{q} = \mathfrak{a} \cap \mathfrak{b}$ af idealer, der er effektivt større end \mathfrak{q} . Vis, at et primideal er irreducibelt. Vis, at de irreducible idealer i \mathbb{Z} er (0) og hovedidealene (p^n) frembragt af en primtalspotens. Vis, at i en noethersk ring er hvert ideal \mathfrak{a} en fællesmængde, $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, af irreducible idealer \mathfrak{q}_i . (Her medregnes fællesmængden af ingen idealer som fremstillingen af R .)
- U5 **7.** Lad M være en endeligt frembragt R -modul. Vis, at M er en noethersk modul, hvis og kun hvis kvotientringen $R/\text{Ann } M$ er en noethersk ring.
- U6 **8.** Antag, at M er en noethersk R -modul. Vis, for en vilkårlig multiplikativ delmængde S af R , at $S^{-1}M$ er en noethersk $S^{-1}R$ -modul. [Vink: Enhver undermodul af $S^{-1}M$ har som bekendt formen $S^{-1}N$ med en undermodul $N \subseteq M$.]
- H2 **9.** Vis for hvert n -sæt $\alpha = (\alpha_1, \dots, \alpha_n)$ i k^n , at idealet $\mathfrak{m}_\alpha := (X_1 - \alpha_1, \dots, X_n - \alpha_n)$ består af de polynomier $f \in k[X_1, \dots, X_n]$ for hvilke $f(\alpha_1, \dots, \alpha_n) = 0$. Vis, når k er et legeme, at \mathfrak{m}_α er et maksimalideal.
- H2 **10.** Antag, at k er et uendeligt legeme. Vis, at hvis $f \in k[X_1, \dots, X_n]$ ikke er nul-polynomiet, så findes et $\alpha = (\alpha_1, \dots, \alpha_n) \in k^n$ med $f(\alpha) \neq 0$.
- 11.** En partielt ordnet mængde (\mathcal{M}, \leq) kaldes *noethersk ordnet*, hvis der i enhver stigende kæde $x_1 \leq x_2 \leq x_3 \leq \cdots$ gælder „=“ fra et vist trin. Formuler en ækvivalent „maksimalitetsbetingelse“. Ordningen kaldes *artinsk*, hvis den modsatte ordning er noethersk. Antag, at ordningen er både noethersk og artinsk. Vis, at så findes der i \mathcal{M} en kæde $x_0 < x_1 < \cdots < x_{n-1} < x_n$, som er *uforfinelig* i den forstand, at x_0 er minimalt element i \mathcal{M} ,

x_n er maksimalt element i \mathcal{M} og for hvert i findes der intet element x med $x_{i-1} < x < x_i$. I almindelighed kan man ikke slutte, at der så er en øvre grænse for antallet af elementer i en uforfinelig kæde. Hvilket resultat kan man udlede, når \mathcal{M} er mængden af undermoduler af en given modul M ?

U5 **12.** Betragt R -homomorfier $\varphi: M \rightarrow N$ og $\psi: N \rightarrow P$. Vis, at $\text{Ker } \varphi \subseteq \text{Ker } \psi\varphi$ og at ψ inducerer en surjektiv homomorfi $\varphi(M) \rightarrow \psi\varphi(M)$. Vis, at $\text{Ker } \varphi = \text{Ker } \psi\varphi$, hvis og kun hvis den inducerede homomorfi er en isomorfi $\psi: \varphi(M) \rightarrow \psi\varphi(M)$.

Vis, at hvis M er noethersk, så er enhver surjektiv homomorfi $M \rightarrow M$ automatisk en isomorfi.

U5 **13.** Vis, at enhver noethersk modul $M \neq 0$ har en simpel kvotientmodul.

14. To af de egenskaber, der karakteriserer noetherske moduler ved deres undermoduler, hedder, henholdsvis, „den opstigende kædes egenskab“, og „maksimalitetsegenskaben“. Præciser hvilke! Formuler tilsvarende „den nedstigende kædes egenskab“ og „minimalitetsegenskaben“, og vis at de to sidste egenskaber er ækvivalente. En modul, der har de to egenskaber, kaldes *artinsk*. Vis, at enhver artinsk modul har en simpel undermodul.

15. Vis, at en R -modul M har endelig længde, hvis og kun hvis M er både noethersk og artinsk.

16. Lad p være et primtal, og lad $C_{p^\infty} \subset \mathbb{C}^*$ være foreningsmængden af undergrupperne:

$$C_1 \subset C_p \subset C_{p^2} \subset \dots, \quad (*)$$

Vis, at C_{p^∞} er en gruppe, og at undergrupperne i (*) er de eneste ægte undergrupper af C_{p^∞} . Vis, at C_{p^∞} er artinsk som \mathbb{Z} -modul.

17. Vis, for et primtal p , at $M := \mathbb{Z}[1/p]/\mathbb{Z}$ er artinsk som \mathbb{Z} -modul. [Vink 1: Vis, at undergrupperne $\mathbb{Z}(1/p)^n/\mathbb{Z}$ for $n = 0, 1, 2, \dots$ er de eneste ægte undergrupper af M . Eller Vink 2: Vis, at M er relateret til gruppen C_{p^∞} .]

18. Antag, at nul-idealet er et produkt af maksimalidealers, $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. Vis, at så er følgende betingelser ækvivalente: (i) R er noethersk; (ii) R er artinsk; (iii) R har endelig længde. [Vink: I filtrationen af R bestemt ved $F_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$ har hver af de successive kvotienter formen F/mF ; specielt er hver kvotient en modul over en kvotientring R/\mathfrak{m} , altså et vektorrum. Brug nu, at for vektorrum er de tre betingelser trivielt ækvivalente.]

19. Vis, at R (som modul over sig selv) er artinsk, hvis og kun hvis R har endelig længde. [Vink: Antag, at R er artinsk. Det er nok at vise, at (0) er produkt af maksimalidealers. Vælg \mathfrak{d} minimalt blandt de idealers, der er produkter af maksimalidealers, og sæt $\mathfrak{a} = \text{Ann } \mathfrak{d}$. Så er \mathfrak{a} det største ideal med $\mathfrak{a}\mathfrak{d} = 0$. Antag, indirekte, at $\mathfrak{d} \neq (0)$. Så er $1 \notin \mathfrak{a}$, og kvotienten R/\mathfrak{a} er ikke nul. Slut heraf, at R/\mathfrak{a} har en simpel undermodul, svarende til et ideal \mathfrak{b} med $\mathfrak{a} \subset \mathfrak{b}$ og $\mathfrak{b}/\mathfrak{a} = R/\mathfrak{m}$. Nu er $\mathfrak{m}\mathfrak{b} \subseteq \mathfrak{a}$, og dermed er $\mathfrak{m}\mathfrak{b}\mathfrak{d} = 0$. Øjensynlig er $\mathfrak{m}\mathfrak{d} \subseteq \mathfrak{d}$ er produkt af maksimal idealers, så valget af \mathfrak{d} sikrer, at $\mathfrak{m}\mathfrak{d} = \mathfrak{d}$. Altså er $\mathfrak{b}\mathfrak{d} = (0)$, men da $\mathfrak{a} \subset \mathfrak{b}$ er det er i modstrid med definitionen af \mathfrak{a} .

20. Vis, at en endeligt frembragt R -modul er artinsk, hvis og kun hvis den har endelig længde.

- U6 **21.** Lad M være en R -modul, og betragt den direkte sum $R \oplus M$. Vis, at med kompositionen $(r, x)(s, y) = (rs, ry + sx)$ som multiplikation er $R \oplus M$ en kommutativ ring. (Tænker man på (r, x) som $r + x$, er multiplikationen bestemt ved $xy = 0$.) Antag, at $R = k$ er et legeme. Vis, at $k \oplus M$ en lokal ring med kun ét primideal. Hvornår er $k \oplus M$ noethersk?, – artinsk?, – af endelig længde?

4. Endeligt frembragte algebraer. Hele udvidelser.

(4.1) Algebra og delalgebra. Lad der være givet en ringhomomorfi $\theta: R \rightarrow A$. Ringen A organiseres da som R -modul med multiplikationen defineret ved

$$ra := \theta(r)a \quad \text{for } r \in R, a \in A.$$

Når ringhomomorfien θ er givet, siges A også at være en *algebra over R* eller en R -algebra. Specielt: hvis R er en delring af A , så kan A opfattes som algebra over R .

Når A er en R -algebra kan enhver delring $B \subseteq A$, som omfatter $\theta(R)$, selv opfattes som R -algebra. En sådan delring kaldes også en *delalgebra* af A .

(4.2) Lemma. *Lad A være en R -algebra, og lad M være en A -modul. Hvis M er endeligt frembragt som A -modul og A er endeligt frembragt som R -modul, så er M endeligt frembragt som R -modul.*

Bevis. Den givne A -modul M opfattes naturligt som R -modul, idet produktet rx for $r \in R$ og $x \in M$ defineres ved $rx := \theta(r)x$.

Antag nu, at n elementer e_1, \dots, e_n i M frembringer M som A -modul, og at p elementer v_1, \dots, v_p i A frembringer A som R -modul. Det påstås, at de np elementer $v_i e_j$ i M frembringer M som R -modul. Lad nemlig x være element i M . Da har x en fremstilling,

$$x = a_1 e_1 + \dots + a_n e_n, \quad (*)$$

som A -linearkombination af e_j 'erne. Koefficienterne a_j tilhører A , og hver koefficient a_j har derfor en fremstilling som R -linearkombination af v_i 'erne. Indsættes for hvert a_j i (*) en sådan fremstilling, fås en fremstilling af x som R -linearkombination af $v_i e_j$ 'erne, som ønsket. \square

(4.3) Endeligt frembragt algebra. Lad A være en R -algebra. For givne elementer a_1, \dots, a_m i A betegnes da med

$$R[a_1, \dots, a_m]$$

delmængden af A bestående af de elementer, der er R -linearkombinationer af endelig mange af de endelige produkter,

$$a_1^{i_1} a_2^{i_2} \dots a_m^{i_m}.$$

Øjensynlig er denne delmængde en delring af A , endda den mindste, der indeholder billedringen $\theta(R)$ og alle a_i 'erne. Specielt er delmængden selv en R -algebra; den kaldes *delalgebraen frembragt af a_i 'erne*.

En given R -algebra A siges at være *endeligt frembragt* (mere udførligt: *endeligt frembragt som R -algebra*), hvis der i A findes endelig mange elementer a_1, \dots, a_m , som frembringer algebraen A , dvs opfylder at

$$A = R[a_1, \dots, a_m].$$

Algebraen A er specielt en R -modul, men det skal understreges, at en endeligt frembragt algebra ikke nødvendigvis er endeligt frembragt som R -modul.

(4.4) Definition. Polynomiumsringen $R[X_1, \dots, X_m]$ er en R -algebra, idet R kan opfattes som delringen bestående af de konstante polynomier. Polynomiumsringen er endeligt frembragt som R -algebra, nemlig frembragt af de variable X_1, \dots, X_m .

For givne elementer a_1, \dots, a_m i en R -algebra A defineres en R -lineær ringhomomorfi $R[X_1, \dots, X_m] \rightarrow A$ ved

$$\sum r_{i_1, \dots, i_m} X_1^{i_1} \cdots X_m^{i_m} \mapsto \sum r_{i_1, \dots, i_m} a_1^{i_1} \cdots a_m^{i_m}.$$

Billedet af et polynomium $P \in R[X_1, \dots, X_m]$ ved denne afbildning betegnes også

$$P(a_1, \dots, a_m),$$

og det siges at fremkomme ved at *indsætte* a_1, \dots, a_m i P . Billedet for denne ringhomomorfi er øjensynlig delalgebraen frembragt af a_i 'erne. Billedet af det konstante polynomium $r \in R$ er elementet $r 1_A = \theta(r)$ i A ; hvis misforståelser er udelukkede skrives blot r for dette element i A .

Givne elementer a_1, \dots, a_m i A siges at være *algebraisk uafhængige* over R , eller *transcendente* over R , hvis homomorfien defineret ved indsættelse er injektiv. Hvis homomorfien ikke er injektiv, kaldes elementerne *algebraisk afhængige* over R .

(4.5) Observation. Af definitionerne følger let, at en R -algebra A er endeligt frembragt over R , hvis og kun hvis A er homomorft billede af en polynomiumsring $R[X_1, \dots, X_m]$ for passende m , altså hvis og kun hvis A er isomorf med en kvotient $R[X_1, \dots, X_m]/\mathfrak{A}$, hvor \mathfrak{A} er et ideal.

Specielt følger det, at en algebra, der er endeligt frembragt over en noethersk ring R , selv er en noethersk ring.

(4.6) Sætning. Lad A være en R -algebra. For hvert element a i A er følgende betingelser ækvivalente:

- (i) Der findes et normeret polynomium P i $R[X]$ så at $P(a) = 0$. Med andre ord: der findes i A en relation af formen $a^n + r_1 a^{n-1} + \cdots + r_n = 0$, hvor r_i 'erne tilhører R .
- (ii) Delalgebraen $R[a]$ af A er endeligt frembragt som R -modul.
- (iii) Der findes en delalgebra B af A , som er endeligt frembragt som R -modul og indeholder a .

Bevis. (i) \Rightarrow (ii). Antag, at a tilfredsstillen en ligning,

$$a^n + r_1 a^{n-1} + \cdots + r_n = 0, \quad (*)$$

hvor r_i 'erne tilhører R . Det påstås, at elementerne $1, a, \dots, a^{n-1}$ frembringer $R[a]$ som R -modul. Det er øjensynlig nok at vise, at hver potens a^p er en R -linear kombination af $1, \dots, a^{n-1}$. Dette vises ved induktion efter p . For $p < n$ er det klart. Antag, at påstanden gælder for a^p , dvs at der gælder en ligning,

$$a^p = s_n + s_{n-1}a + \cdots + s_1 a^{n-1},$$

30. marts 2007

hvor s_1, \dots, s_n tilhører R . Multipliseres denne ligning med a fås ligningen

$$a^{p+1} = (s_n a + s_{n-1} a^2 + \dots + s_2 a^{n-1}) + s_1 a^n. \quad (**)$$

Af (*) ses, at $a^n = -r_n - r_{n-1}a - \dots - r_1 a^{n-1}$. Specielt er a^n en R -linearkombination af $1, \dots, a^{n-1}$. Erstattes a^n på højresiden af (**) med denne linearkombination fås en fremstilling af a^{p+1} som R -linearkombination af $1, \dots, a^{n-1}$, som ønsket.

(ii) \Rightarrow (iii). Hvis (ii) gælder, så kan $B := R[a]$ øjensynlig anvendes i (iii).

(iii) \Rightarrow (i). Antag, at B er en delalgebra af A , frembragt som R -modul af elementer b_1, \dots, b_m , og at $a \in B$. Da B er en delring og $a \in B$, gælder for hvert b i B , at produktet ab tilhører B ; produktet ab har altså en fremstilling som en R -linearkombination af b_i 'erne. Skrives koefficienterne i en sådan fremstilling som en søjlematrix α , fås altså en matrixligning af formen,

$$ab = (b_1, \dots, b_m)\alpha.$$

Specielt fås for $i = 1, \dots, m$ en sådan ligning for $b = b_i$, og disse ligninger kan under ét skrives som en matrixligning,

$$a(b_1, \dots, b_m) = (b_1, \dots, b_m)\alpha,$$

hvor α nu er en $m \times m$ -matrix med koefficienter i R . Den sidste matrixligning kan omformes til ligningen,

$$(b_1, \dots, b_m)(a1_m - \alpha) = 0,$$

hvor 1_m betegner enhedsmatricen. Betrag nu determinanten $d := \det(a1_m - \alpha)$ i A . Af matrixligningen følger ved hjælp af Cramer's formler, at $(b_1, \dots, b_m)d = 0$. Determinanten d annullerer derfor alle b_i 'erne, og dermed også enhver linearkombination af b_i 'erne. Da B er frembragt som R -modul af b_i 'erne, vil d annullere ethvert element i B . Specielt vil d annullere et-elementet 1_A , som jo tilhører B . Følgelig er $d = 0$. Da matricen α har koefficienter i R , er det på den anden side klart, at $d = \det(a1_m - \alpha)$ har formen,

$$d = a^m + r_1 a^{m-1} + \dots + r_m,$$

hvor r_1, \dots, r_m tilhører R . Ligningen $d = 0$ viser derfor, at betingelsen (i) er opfyldt.

Hermed er Sætningen bevist. □

(4.7) Definition. Lad A være en R -algebra, givet ved ringhomomorfien $\theta: R \rightarrow A$. Et element a i A , som opfylder de ækvivalente betingelser i Sætning (4.6), siges at være *helt over* R . Hvis alle elementer i A er hele over R , siges afbildningen θ at være en *hel homomorfi*, og algebraen A siges at være *hel over* R .

Øjensynlig er A hel over R , netop når A er hel over delringen $\theta(R)$.

Hvis R -algebraen A er endeligt frembragt som R -modul, da er A hel over R , dvs hvert element a i A er helt over R . Som delalgebra B i betingelsen (4.6)(iii) kan nemlig i så fald bruges $B = A$.

30. marts 2007

(4.8) Korollar. *Lad A være en R -algebra. Elementer a_1, \dots, a_m i A er da hele over R , hvis og kun hvis delalgebraen $R[a_1, \dots, a_m]$ er endeligt frembragt som R -modul.*

Bevis. Delalgebraen $R[a_1, \dots, a_m]$ indeholder a_i 'erne. Af betingelsen (4.6)(iii) følger derfor, at hvis delalgebraen er endelig over R , så er hvert af a_i 'erne hele over R .

Den omvendte implikation vises ved induktion efter m . For $m = 1$ følger påstanden direkte af definitionen, jfr betingelsen (4.6)(ii). Antag nu, at elementer a_1, \dots, a_{m+1} i A er hele over R , og at påstanden gælder for m elementer. Sæt $B := R[a_1, \dots, a_m]$. Øjensynlig er $R[a_1, \dots, a_m, a_{m+1}] = B[a_{m+1}]$, og det skal vises, at denne algebra er endeligt frembragt som R -modul. Da a_{m+1} er hel over R , er a_{m+1} også hel over B . Følgelig er $B[a_{m+1}]$ endeligt frembragt som B -modul. Af induktionsforudsætningen følger, at B er endeligt frembragt som R -modul. Af Lemma (4.2) følger nu, at $B[a_{m+1}]$ er endeligt frembragt som R -modul, som ønsket. \square

(4.9) Korollar. *Sum og produkt af hele elementer a, b i A er igen hele. Elementerne i A , som er hele over R , udgør en delalgebra af A .*

Bevis. Ifølge det foregående korollar er $R[a, b]$ endelig over R . Da både summen $a + b$ og produktet ab tilhører $R[a, b]$, følger det af betingelsen (4.6)(iii), at $a + b$ og ab er hele over R . Heraf følger videre den sidste påstand, idet elementerne i $\theta(R)$ er hele over R ; elementet $a := \theta(r)$ i A opfylder jo ligningen $a - r1_A = 0$. \square

(4.10) Korollar. *Antag, at A er hel over R . Lad $A \rightarrow C$ være en ringhomomorfi. Hvert element i C , der er helt over A , vil da også være helt over R . Hvis homomorfien $A \rightarrow C$ er hel, da er også den sammensatte homomorfi $R \rightarrow C$ hel.*

Bevis. Betragt i C et element c , der er helt over A . Det skal vises, at c er hel over R . Da c er hel over A , findes en relation,

$$c^n + a_1 c^{n-1} + \dots + a_n = 0,$$

hvor a_i 'erne tilhører A . Af denne relation fremgår, at c er hel over delalgebraen $B := R[a_1, \dots, a_n]$ af A . Altså er $B[c]$ endeligt frembragt som B -modul. Da A er hel over R og B er en delring af A , er B hel over R . Af Korollar (4.8) følger derfor, at B er endeligt frembragt som R -modul. Altså følger det af Lemma (4.2), at algebraen $B[c]$ er endeligt frembragt som R -modul. Da c tilhører denne delalgebra af C , er c hel over R . Hermed er Korollarets første påstand bevist.

Den sidste påstand følger trivielt af den første. \square

(4.11) Sætning. *Lad R være en faktoriel ring. Enhver brøk i brøkleget for R , som er hel over R , vil da tilhøre R .*

Bevis. Betragt en brøk r/s , hvor $s \neq 0$. Da R er faktoriel, kan r, s vælges primiske. Antag, at r/s er hel over R . Der findes altså i brøkleget en relation,

$$(r/s)^n + r_1 (r/s)^{n-1} + \dots + r_n = 0.$$

Multipliseres med s^n fås en ligning i R ,

$$s(-r_1r^{n-1} - r_2r^{n-2}s - \dots - r_ns^{n-1}) = r^n.$$

Af denne ligning følger, at enhver primdivisor i s er divisor i r^n og dermed i r . Følgelig har s ingen primdivisorer, og s er derfor invertibel i R . Altså er $r/s = rs^{-1}$ element i R . \square

(4.12) Note. Sætningen ovenfor generaliserer en del af følgende sætning kendt fra gymnasiet: Hvis et polynomium med hele koefficienter har en rational rod skrevet som uforkortelig brøk r/s , så går r op i konstantleddet og s går op i højstegrads-koefficienten.

(4.13) Noether's Normaliseringslemma. Lad k være et legeme og lad $A \neq 0$ være en algebra over k frembragt af m elementer a_1, \dots, a_m . Da findes i A et sæt af $t \leq m$ elementer x_1, \dots, x_t , der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delalgebraen $k[x_1, \dots, x_t]$.

Bevis. Påstanden vises ved induktion efter m . For $m = 0$ (forudsætningen er her, at $k \rightarrow A$ er surjektiv) er påstanden triviel.

Antag nu at $m > 0$, og at påstanden er vist for algebraer frembragt af færre end m elementer. Hvis de givne elementer a_1, \dots, a_m er algebraisk uafhængige, er påstanden triviel: vi kan bruge $t = m$ og $x_i = a_i$ for $i = 1, \dots, m$. Antag derfor, at a_i 'erne er algebraisk afhængige, dvs at der findes en relation,

$$\sum r_{i_1, \dots, i_m} a_1^{i_1} \cdots a_m^{i_m} = 0, \quad (*)$$

hvor koefficienterne r_{i_1, \dots, i_m} tilhører k , og hvor ikke alle koefficienterne er 0. Lad nu g_1, \dots, g_{m-1} være et sæt af $m - 1$ positive eksponenter, og sæt

$$b_i := a_i - a_m^{g_i} \quad \text{for } i = 1, \dots, m - 1.$$

Det er nok at vise, at hvis g_j 'erne vælges passende, så er a_m hel over delalgebraen $B := k[b_1, \dots, b_{m-1}]$. Antag nemlig, at a_m er hel over B . Da er $B[a_m]$ endeligt frembragt som B -modul. For $i = 1, \dots, m - 1$ er $a_i = b_i + a_m^{g_i}$, og altså er $a_i \in B[a_m]$. Da A er frembragt som k -algebra af a_i 'erne, følger det at $A = B[a_m]$. Altså er A endeligt frembragt som B -modul. Videre følger det af induktionsforudsætningen, at der findes $t \leq m - 1$ elementer i B , der er algebraisk uafhængige over k , og således at B er endeligt frembragt som modul over $k[x_1, \dots, x_t]$. Af Lemma (4.2) følger, at A er endeligt frembragt som modul over $k[x_1, \dots, x_t]$, og så er påstanden vist for algebraen A .

Vi viser nu, at g_j 'erne kan vælges passende. Ifølge definitionen er $a_i = b_i + a_m^{g_i}$ for $i = 1, \dots, m - 1$. Indsættes disse ligninger i ligningen (*) fremkommer på venstresiden en sum af udtryk af formen,

$$r_{i_1, \dots, i_m} (b_1 + a_m^{g_1})^{i_1} \cdots (b_{m-1} + a_m^{g_{m-1}})^{i_{m-1}} a_m^{i_m}.$$

I dette udtryk kan vi udføre multiplikationerne (binomialformlen), og ordne efter potenser af a_m . Hver potens af a_m kommer da med en koefficient, der afhænger af b_j 'erne. Disse

30. marts 2007

koefficienter tilhører altså delalgebraen B . Den højeste exponent til a_m er øjensynlig $g_1 i_1 + \dots + g_{m-1} i_{m-1} + i_m$, og den hertil hørende koefficient er blot r_{i_1, \dots, i_m} . Udtrykket har altså formen

$$r_{i_1, \dots, i_m} a_m^{g_1 i_1 + \dots + g_{m-1} i_{m-1} + i_m} + \dots, \quad (**)$$

hvor de tre prikker står for en B -linearkombination af potenser af a_m med lavere exponent end den første.

I den givne relation (*) er r_{i_1, \dots, i_m} 'erne kun forskellige fra 0 for endelig mange sæt i_1, \dots, i_m . Svarende til disse endelig mange sæt i_1, \dots, i_m vælger vi nu g_j 'erne, så at de tilhørende exponenter $i_1 g_1 + \dots + i_{m-1} g_{m-1} + i_m$ er indbyrdes forskellige. At et sådant valg er muligt kan indses således: Vi betragter kun endelig mange sæt i_1, \dots, i_m , så der findes et naturligt tal g som er skarpt større end hvert af de optrædende i_v 'er. Med dette g vælger vi $g_j := g^{m-j}$. De tilhørende exponenter er da

$$i_1 g^{m-1} + \dots + i_{m-1} g + i_m g^0.$$

Exponenterne svarende til de endelig mange sæt i_1, \dots, i_m er da indbyrdes forskellige, thi da $i_v \leq g - 1$ er sættet simpelthen cifrene, når exponenten skrives i g -talssystemet.

Med dette valg af g_j 'erne opnås det ønskede. For de endelig mange sæt i_1, \dots, i_m , for hvilke $r_{i_1, \dots, i_m} \neq 0$, er de tilsvarende exponenter $i_1 g^m + \dots + i_{m-1} g + i_m g^0$ nu forskellige, så blandt dem findes en, der er størst. Lad N være den største exponent, og lad r være den tilhørende koefficient. Blandt udtrykkene (**) forekommer så udtrykket $r a_m^N + \dots$, og i alle andre udtryk forekommer a_m med en eksponent mindre end N . Ved addition af udtrykkene (**) og udnyttelse af ligningen (*) får vi derfor en relation,

$$r a_m^N + \dots = 0,$$

hvor de tre prikker står for en B -linearkombination af potenser af a_m med exponent mindre end N . Ifølge valget er $r \neq 0$. Da k er et legeme, kan relationen derfor multipliceres med r^{-1} . Det følger af den fremkomne relation, at a_m er hel over B . Hermed er det ønskede opnået, og Normaliseringslemma'et bevist. \square

(4.14) Lemma. *Lad A være et integritetsområde, og antag, at A er hel over en delring R . Da er A et legeme, hvis og kun hvis R er et legeme.*

Bevis. Antag først, at A er et legeme. Det skal så vises for hvert element $r \neq 0$ i R , at r er et invertibelt element i R . Da A er et legeme, har r et inverst element a i A . Ifølge antagelsen er elementet a helt over R . Der findes altså en relation i A ,

$$a^m + r_1 a^{m-1} + \dots + r_m = 0,$$

hvor r_i 'erne tilhører R . Multiplicer denne relation med r^m . Da $ra = 1$ fås følgende ligninger,

$$0 = 1 + r r_1 + r^2 r_2 + \dots + r^m r_m = 1 + r(r_1 + \dots + r_m r^{m-1}).$$

30. marts 2007

Heraf aflæses, at summen i parentesen, bortset fra fortegnet, er det inverse til r . Da summen tilhører R , aflæses specielt, at det inverse til r er element i R .

Antag dernæst, at R er et legeme. Lad a være et element forskelligt fra 0 i A . Det skal vises, at a er invertibelt i A . Multiplikation med a definerer en R -lineær afbildning $x \mapsto ax$ af $R[a]$ ind i sig selv. Da A er et integritetsområde er multiplikationsafbildningen injektiv. Videre er a hel over R , og $R[a]$ er derfor endeligt frembragt som R -modul. Med andre ord er $R[a]$ et endeligdimensionalt vektorrum over legemet R . Følgelig er den injektive multiplikationsafbildning bijektiv. Et-elementet 1 i $R[a]$ vil derfor tilhøre billedet. Der findes altså et element x i $R[a]$, så at $ax = 1$. Altså er elementet a invertibelt i A . \square

(4.15) Hilbert's Nulpunktssætning, version 1. Lad k være et legeme, og lad A være en endeligt frembragt algebra over k . Antag, at A er et legeme. Da er A et endeligdimensionalt vektorrum over k .

Bevis. Ifølge Noether's Normaliseringslemma findes i A elementer x_1, \dots, x_t , der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delringen $k[x_1, \dots, x_t]$. Da A er et legeme, følger det af Lemma (4.14), at også denne delring er et legeme. Da elementerne x_1, \dots, x_t er algebraisk uafhængige over k , er delringen isomorf med polynomiumsringen over k i t variable. Øjensynlig er en sådan polynomiumsring kun et legeme, hvis $t = 0$. Delringen er altså blot k . Algebraen A er altså endeligt frembragt som modul over legemet k . Med andre ord: A er endeligdimensional over k . \square

(4.16) Opgaver.

1. Lad R være et integritetsområde med brøklegerne K , og antag, at K er dellegeme af et legeme L . Hvis $\alpha \in L$ er algebraisk over K , betegnes med $f_{\alpha/K}$ det *minimale polynomium* for α , dvs det normerede polynomium af lavest grad i $K[X]$, der har α som rod. Antag, at R er helt afsluttet i K . Vis, at α er hel over R , hvis og kun hvis α er algebraisk over K og $f_{\alpha/K}$ har koefficienter i R .

2. Gennemfør følgende bevis for Noether's Normaliseringslemma. Lad $A := k[a_1, \dots, a_m]$ være den givne algebra. Antag, at der findes en egentlig relation $F(a_1, \dots, a_m) = 0$, hvor F ikke er nul-polynomiet. Betragt et sæt af $m - 1$ skalarer $\lambda_1, \dots, \lambda_{m-1} \in k$, og sæt

$$b_i := a_i - \lambda_i a_m \quad \text{for } i = 1, \dots, m - 1.$$

Det skal vises, at skalarerne kan vælges sådan, at a_m er hel over $k[b_1, \dots, b_{m-1}]$ (thi så bliver $k[a_1, \dots, a_m]$ hel over $k[b_1, \dots, b_{m-1}]$). Lad d være graden af F , og altså $F = F_d + \dots + F_1 + F_0$, hvor F_i er homogen af grad d . Vi har $a_i = b_i + \lambda_i a_m$, og altså ligningen,

$$F(b_1 + \lambda_1 a_m, \dots, b_{m-1} + \lambda_{m-1} a_m, a_m) = 0.$$

Ordnes efter potenser af a_m fås en ligning af grad højst d i a_m , og koefficienten til a_m^d kommer fra F_d . Det bliver en skalar:

$$0 = F(b_1 + \lambda_1 a_m, \dots, b_{m-1} + \lambda_{m-1} a_m, a_m) = F_d(\lambda_1, \dots, \lambda_{m-1}, 1) a_m^d + \dots$$

30. marts 2007

Nu var $F_d(X_1, \dots, X_m)$ homogent og ikke nul-polynomiet, og så er $F_d(X_1, \dots, X_{m-1}, 1)$ ikke nul-polynomiet. Vælg nu skalarerne sådan, at koefficienten $F_d(\lambda_1, \dots, \lambda_{m-1}, 1) \neq 0$. Division med denne koefficient giver så en „helheds“-relation for a_m over $k[b_1, \dots, b_{m-1}]$.

Den væsentlige fordel ved dette bevis er, at den givne algebra bliver hel over algebraisk uafhængige elementer, der er *linearkombinationer* af de givne a_1, \dots, a_m . Ulempen er, at beviset kun fungerer, når legemet k er undeligt. Hvorfor denne sidste indskrænkning?

U9 **3.** Lad k være et legeme, og lad $A := k^{\mathbb{N}}$ være ringen af alle følger $\alpha_1, \alpha_2, \dots$ med $\alpha_i \in k$. Vis, at de følger, der er konstante fra et vist trin, udgør en delring R af A . For en følge (α_i) i R betegnes med α_∞ følgens konstante værdi α_j for $j \gg 0$. Vis, for hvert $i = 1, 2, \dots, \infty$, at følgerne $\alpha \in R$ med $\alpha_i = 0$ udgør et maksimalideal \mathfrak{m}_i i R , og at disse idealer er samtlige primideal i R . [Vink: Lad \mathfrak{p} være et primideal i R . Betragt, for $i = 1, 2, \dots$, hovedidealet (δ_i) i R (hvor δ_i er Kronecker's delta, $\delta_{ij} = 1$ når $j = i$ og $\delta_{ij} = 0$ når $j \neq i$). Udnyt, at $(\delta_i)\mathfrak{m}_i = (0) \subseteq \mathfrak{p}$.]

Vis, at de følger, der kun antager endelig mange værdier, udgør en delring R' af A [Så $R' = A$, hvis k er et endeligt legeme]. Vis, at R' er den hele afslutning af R i A . Kan du bestemme et maksimalideal i R' , der ligger over \mathfrak{m}_i ? – Også for $i = \infty$?

U9 **4.** Betragt i polynomiumsringen $k[T]$ (k er et legeme) polynomierne $x = T^2$ og $y = T^3$, og delalgebraen $k[x, y]$ af $k[T]$. Vis, at kernen for den naturlige homomorfi $k[X, Y] \rightarrow k[x, y]$ (bestemt ved $f \mapsto f(x, y)$) er idealet $\mathfrak{p} := (X^3 - Y^2)$. [Vink: Regn modulo det sidste ideal, dvs at man i monomier kan erstatte X^3 med Y^2 (og omvendt). For hvert $f \in k[X, Y]$ har vi så en kongruens, $f \equiv f_0(X) + f_1(X)Y$ med polynomier $f_0, f_1 \in k[X]$. Det er klart, at \mathfrak{p} er indeholdt i kernen. Antag omvendt, at f tilhører kernen. Så følger det, at $f_0(x) + f_1(x)y = 0$, altså $f_0(T^2) + f_1(T^2)T^3 = 0$, og så må f_0 og f_1 være nul, og altså $f \equiv 0$, dvs $f \in (X^3 - Y^2)$.]

5. *Betragt i polynomiumsringen $k[T]$ (k er et legeme) polynomierne $x = T^2$, $y = T^3$ og $z = T^4$, og delalgebraen $k[x, y, z]$ af $k[T]$. Vis, at kernen for den naturlige homomorfi $k[X, Y, Z] \rightarrow k[x, y, z]$ er idealet $\mathfrak{p} := (Y^2 - XZ, X^3 - YZ, X^2Y - Z^2)$. [Vink: Regn modulo det sidste ideal, og vis, at for hvert $f \in k[X, Y, Z]$ er der en kongruens

$$f \equiv X^2 f_1(Z) + XY f_2(Z) + X f_3(Z) + Y f_4(Z) + f_5(Z) \pmod{\mathfrak{p}}.$$

Det er klart, at kernen omfatter \mathfrak{p} . Omvendt, hvis f ligger i kernen, så fås $T^6 f_1(T^5) + T^7 f_2(T^5) + T^3 f_3(T^5) + T^4 f_4(T^5) + f_5(T^5)$, og heraf følger $f_1 = f_2 = f_3 = f_4 = f_5 = 0$, og altså $f \in \mathfrak{p}$.]

U9 **6.** Lad $\theta: R \rightarrow R'$ være en ringhomomorfi, og lad S være en multiplikativ delmængde af R . Brøkmodulet $S^{-1}R'$ kan som bekendt identificeres med brøkringen $\theta(S)^{-1}R'$, og homomorfin $S^{-1}R \rightarrow S^{-1}R'$ er en ringhomomorfi. Vis, at hvis R' er hel over R , så er $S^{-1}R'$ hel over $S^{-1}R$.

5. Transcendensgrad.

I denne paragraf betragtes et fast integritetsområde A , og det antages, at ringen R er en delring af A . Specielt er R så et integritetsområde, og A er en R -algebra.

(5.1) Definition. Af definitionen (4.4) fremgår, at et enkelt element a i A er algebraisk afhængigt over R , hvis og kun hvis der findes en relation,

$$r_m a^m + \cdots + r_1 a + r_0 = 0, \quad (5.1.1)$$

hvor r_i 'erne tilhører R , og hvor mindst ét af r_i 'erne er forskelligt fra 0. Er dette opfyldt siges a også at være *algebraisk over R* .

Delmængden af A bestående af de elementer a , der er algebraiske over R , betegnes \bar{R} , og den kaldes den *algebraiske afslutning* af R i A . Bemærk, at betegnelsen \bar{R} er ufuldstændig, idet denne delmængde afhænger af både R og A .

(5.2) Observation. Hvis delringen R er et legeme, så er et element a i A algebraisk over R , hvis og kun hvis a er hel over R . At a er hel over R betyder jo, at der findes en relation af formen (5.1.1), hvor $r_m = 1$. Et helt element er således algebraisk. Omvendt, hvis R er et legeme og a tilfredsstillende en ligning af formen (5.1.1), hvor $r_m \neq 0$, så kan denne ligning multipliceres med r_m^{-1} , hvorved der opnås en ligning med $r_m = 1$.

Hvis brøkleget K for R er indeholdt i A , så er et element a algebraisk over R , hvis og kun hvis a er algebraisk (og dermed hel) over K . Er der nemlig givet en ligning (5.1.1), hvor koefficienterne r_i er brøker i K , så kan ligningen multipliceres med en fælles nævner for disse brøker, og herved opnås en ligning, hvor koefficienterne tilhører R .

(5.3) Lemma. (1) Den algebraiske afslutning \bar{R} i A er en delring af A . Hvis A eller R er et legeme, så er \bar{R} et legeme.

(2) Lad B være en delring af A således at $R \subseteq B \subseteq A$, og således at hvert element i B er algebraisk over R . Hvert element $a \in A$, som er algebraisk over B , er da algebraisk over R .

Bevis. (1) Antag først, at R er et legeme. Delmængden \bar{R} af A består da af de elementer, der er hele over R . Af Korollar (4.9) følger derfor, at \bar{R} er en delring af A . Da denne delring er hel over legemet R følger det af Lemma (4.14), at \bar{R} er et legeme. Hermed er (1) vist når R er et legeme.

I det almindelige tilfælde betegnes med Q brøkleget for A . Legemet Q vil da indeholde brøkleget K for R , og vi har inklusioner,

$$\begin{array}{ccc} A & \subseteq & Q \\ \cup & & \cup \\ R & \subseteq & K. \end{array}$$

Lad \bar{K} betegne den algebraiske afslutning af K i Q . Ifølge det allerede viste er \bar{K} da et legeme. Da K er brøkleget for R , består \bar{K} af de elementer i Q , der er algebraiske over R . Heraf følger først, at $\bar{R} = A \cap \bar{K}$, hvoraf fremgår, at \bar{R} er en delring af A . Hvis A er

30. marts 2007

et legeme, og altså $A = Q$, så følger det videre, at $\bar{R} = \bar{K}$ er et legeme. Hermed er alle påstandene i (1) bevist.

Beviset for (2) er tilsvarende: Af antagelsen følger, at elementet a er helt over brøkleget for B , og at brøkleget for B er helt over K . Af Korollar (4.10) følger, at a er helt over K . Følgelig er a algebraisk over R . \square

(5.4) Lemma. *Lad der være givet et sæt af endelig mange elementer a_1, \dots, a_m i A . Da er a_i 'erne algebraisk afhængige over R , hvis og kun hvis et af a_i 'erne er algebraisk over delalgebraen frembragt af de øvrige.*

Bevis. Elementet a_m er algebraisk over delalgebraen $R[a_1, \dots, a_{m-1}]$ netop hvis der findes en relation,

$$P_N(a_1, \dots, a_{m-1})a_m^N + P_{N-1}(a_1, \dots, a_{m-1})a_m^{N-1} + \dots + P_0(a_1, \dots, a_{m-1}) = 0, \quad (*)$$

hvor koefficienterne fås ved indsættelse af a_1, \dots, a_{m-1} i polynomier P_j i $m - 1$ variable, og hvor en af koefficienterne $P_j(a_1, \dots, a_{m-1})$ er forskellig fra 0. Venstresiden i (*) fås øjensynlig ved at indsætte a_1, \dots, a_m i polynomiet

$$P := P_N X_m^N + P_{N-1} X_m^{N-1} + \dots + P_0. \quad (**)$$

Nu følger „hvis“ umiddelbart: Er fx (*) opfyldt, og $P_j(a_1, \dots, a_{m-1}) \neq 0$, så er $P \neq 0$; af $P(a_1, \dots, a_m) = 0$ følger derfor, at a_i 'erne er algebraisk afhængige.

„Kun hvis“ vises ved induktion efter m . Det er trivielt for $m = 1$, idet delalgebraen frembragt af den tomme mængde blot er R . Antag, at $m > 1$ og at påstanden gælder for $m - 1$ elementer. Betragt m elementer a_1, \dots, a_m , som er algebraisk afhængige. Hvis de $m - 1$ elementer a_1, \dots, a_{m-1} er algebraisk afhængige, så fås den ønskede konklusion af induktionsforudsætningen. Antag derfor, at de $m - 1$ første a_i 'er er algebraisk uafhængige. Da alle a_i 'erne er algebraisk afhængige, findes et polynomium $P \neq 0$ så at $P(a_1, \dots, a_m) = 0$. Skriv nu polynomiet P på formen (**). Så er ligningen (*) opfyldt. Yderligere er en af koefficienterne $P_j(a_1, \dots, a_{m-1})$ forskellig fra nul, idet P ellers ville være nul-polynomiet. Altså er a_m algebraisk over delalgebraen frembragt af de første $m - 1$ af a_i 'erne. \square

(5.5) Definition. Lad V være en delmængde af A . Da siges V at have endelig *algebraisk dimension* over R , hvis der findes endelig mange elementer a_1, \dots, a_n i A , så at hvert element i V er algebraisk over delringen $R[a_1, \dots, a_n]$, dvs så at

$$V \subseteq \overline{R[a_1, \dots, a_n]}. \quad (5.5.1)$$

Hvis relationen (5.5.1) er opfyldt, siges a_i 'erne at være et *algebraisk frembringingsystem* for V over R . Det mindste (endelige) antal a_i 'er, der kan frembringe V , vil vi betegne $\dim_R^{\text{alg}} V$. Hvis V ikke har endelig algebraisk dimension sættes $\dim_R^{\text{alg}} V := \infty$.

Ved *transcendensgraden* for V over R forstås det største antal af algebraisk uafhængige (over R) elementer, der kan udtages fra V . Transcendensgraden betegnes $\text{tdeg}_R V$. Mere

præcist, transcendensgraden er ∞ , hvis der kan udtages vilkårligt store (endelige) delmængder af V , som er algebraisk uafhængige over R . Hvis transcendensgraden ikke er uendelig, findes et største antal af elementer i V , der er algebraisk uafhængige over R , og dette største antal betegnes $\text{tdeg}_R V$.

Ved en (endelig) *transcendensbasis* for V over R forstås et endeligt sæt af elementer v_1, \dots, v_t i V , som er algebraisk uafhængige over R og som frembringer V algebraisk over R .

Af definitionen følger, at enhver delmængde V af A , der er indeholdt i en endelig frembragt R -delalgebra, har endelig algebraisk dimension over R .

Bemærk videre, at en delmængde V har transcendensgrad 0, hvis og kun hvis hvert element i V er algebraisk over R , og at dette indtræffer hvis og kun hvis den algebraiske dimension af V er lig med 0. I dette tilfælde er den tomme mængde en transcendensbasis for V over R .

(5.6) Lemma. *Lad V være en delmængde af A , og lad der være givet et endeligt sæt af elementer v_1, \dots, v_t i V . Følgende betingelser (over R) er da ækvivalente:*

- (i) *Sættet v_1, \dots, v_t er et minimalt algebraisk frembringersystem for V , dvs et frembringersystem hvori intet v_i kan undværes.*
- (ii) *Sættet v_1, \dots, v_t er et maksimalt algebraisk uafhængigt system i V , dvs et algebraisk uafhængigt system, der ikke kan udvides med et element fra V til et større algebraisk uafhængigt system.*
- (iii) *Sættet v_1, \dots, v_t er en transcendensbasis for V .*

Bevis. „(i) \Rightarrow (iii)“: Antag, at v_i 'erne er et minimalt algebraisk frembringersystem. For at vise, at de udgør en transcendensbasis, skal vises, at de er algebraisk uafhængige. Antag, indirekte, at v_i 'erne er algebraisk afhængige. Det følger da af Lemma (5.4), at et af v_i 'erne, fx v_t , er algebraisk over delalgebraen frembragt af de øvrige. Lad B betegne denne delalgebra. Da er

$$R[v_1, \dots, v_t] = R[v_1, \dots, v_{t-1}][v_t] = B[v_t].$$

Da v_t er algebraisk over B følger det Lemma (5.3)(1), at alle elementer i $B[v_t]$ er algebraiske over B . Af Lemma (5.3)(2) følger derfor, at $\overline{B[v_t]} = \overline{B}$. Med andre betegnelser,

$$V \subseteq \overline{R[v_1, \dots, v_t]} = \overline{R[v_1, \dots, v_{t-1}]}.$$

Men dette strider mod at v_1, \dots, v_t var et minimalt frembringersystem for V .

„(iii) \Rightarrow (i)“: Antag, at v_i 'erne er en transcendensbasis for V . Da er de specielt et algebraisk frembringersystem for V , og det skal vises, at dette frembringersystem er minimalt. Antag, indirekte, at et af v_i 'erne, fx v_t , kan undværes. Da gælder inklusionen $V \subseteq \overline{R[v_1, \dots, v_{t-1}]}$. Nu er v_t element i V , og følgelig er v_t element i relationens højreside. Ifølge Lemma (5.4) er dette i modstrid med at v_i 'erne er algebraisk uafhængige.

Beviset for „(ii) \iff (iii)“ er analogt, og overlades til læseren. □

(5.7) Bemærkning. Af Lemma'et følger, at en delmængde V af A har en (endelig) transcendensbasis, hvis enten V har endelig transcendensgrad, eller hvis der findes endelig mange

30. marts 2007

elementer i V , der udgør et algebraisk frembringersystem for V over R . I det første tilfælde kan vi nemlig begynde med den tomme mængde, som er en algebraisk uafhængig delmængde af V , og så supplere successivt med elementer fra V indtil vi opnår en maximal algebraisk uafhængig delmængde af V ; forudsætningen medfører, at denne proces stopper efter endelig mange skridt. I det andet tilfælde kan vi begynde med en endelig delmængde af V , som udgør et algebraisk frembringersystem, og så successivt bortkaste v_i 'er, som kan undværes. Efter endelig mange skridt fås et minimalt algebraisk frembringersystem for V .

(5.8) Lemma. *Lad V være en delmængde af A , og antag at V har en endelig transcendentbasis over R med t elementer. Da gælder ulighederne,*

$$\dim_R^{\text{alg}} V \leq t \leq \text{tdeg}_R V.$$

Bevis. Lad v_1, \dots, v_t være en transcendentbasis for V over R . Da er v_i 'erne specielt et algebraisk frembringersystem for V , så antallet, t , af v_i 'er er større end eller lig med det minimale antal elementer, der kan frembringe V . Videre er v_i 'erne et algebraisk uafhængigt sæt fra V , så antallet af v_i 'er er mindre end eller lig med det maksimale antal (evt ∞) der kan være i et algebraisk uafhængigt sæt udtaget fra V .

Hermed er ulighederne bevist. □

(5.9) Udskiftningssætningen. *Lad V være en delmængde af A . Lad a_1, \dots, a_l være et sæt af elementer i A , som frembringer V algebraisk over R , og lad v_1, \dots, v_t være et sæt af elementer i V , som er algebraisk uafhængige over R . Da er $l \geq t$, og der findes $l - t$ af a_i 'erne som sammen med v_j 'erne frembringer V algebraisk over R .*

Bevis. Sætningen vises ved induktion efter t . For $t = 0$ er påstanden triviel (og indholdsløs). Antag, at $t \geq 1$, og at påstanden gælder for $t - 1$ elementer v_j . Da de $t - 1$ første v_j 'er er algebraisk uafhængige over R , gælder påstanden altså for v_1, \dots, v_{t-1} . Følgelig er $l \geq t - 1$, og vi kan udskifte $t - 1$ af a_i 'erne med disse v_j 'er. Vi kan antage, at det er de første $t - 1$ af a_i 'erne der kan udskiftes, dvs at elementerne $v_1, \dots, v_{t-1}, a_t, \dots, a_l$ frembringer V algebraisk over R . [I dette skridt ved vi kun, at $l \geq t - 1$; det er altså ikke udelukket, at $l = t - 1$, i hvilket tilfælde følgen a_t, \dots, a_l er tom.] Altså er $V \subseteq \overline{R[v_1, \dots, v_{t-1}, a_t, \dots, a_l]}$. Da $v_t \in V$ gælder derfor specielt, at

$$v_t \in \overline{R[v_1, \dots, v_{t-1}, a_t, \dots, a_l]}.$$

Af Lemma (5.4) følger nu, at elementerne $v_1, \dots, v_{t-1}, a_t, \dots, a_l, v_t$ er algebraisk afhængige over R . Der findes altså en ikke-triviel algebraisk relation mellem disse elementer. Da elementerne v_1, \dots, v_t er forudsat algebraisk uafhængige, må et af elementerne a_t, \dots, a_l forekomme i denne relation. Specielt følger det, at $t \leq l$. Det kan antages, at det er a_t , der forekommer i relationen, og så får vi, at

$$a_t \in \overline{R[v_1, \dots, v_t, a_{t+1}, \dots, a_l]}.$$

Under brug af Lemma (5.3)(2) fås følgende inklusioner,

$$V \subseteq \overline{R[v_1, \dots, v_{t-1}, a_t, \dots, a_l]} \subseteq \overline{R[v_1, \dots, v_t, a_{t+1}, \dots, a_l]}.$$

Altså er $v_1, \dots, v_t, a_{t+1}, \dots, a_l$ et algebraisk frembringersystem for V over R .

Hermed er påstanden vist for t elementer, hvorved induktionsbeviset er fuldført. □

(5.10) Hovedsætning. For enhver delmængde V af A gælder ligningen,

$$\text{tdeg}_R V = \dim_R^{\text{alg}} V.$$

Hvis V har endelig transcendensgrad t over R , så findes der endelige transcendensbaser for V over R , og alle sådanne baser indeholder t elementer.

Bevis. Uligheden $\dim_R^{\text{alg}} V \leq \text{tdeg}_R V$ gælder, thi hvis højresiden er uendelig gælder den trivielt, og hvis højresiden er endelig, så findes der en transcendensbasis for V , og så følger uligheden af Lemma (5.8).

Ligeledes gælder uligheden $\text{tdeg}_R V \leq \dim_R^{\text{alg}} V$. Hvis højresiden er uendelig gælder uligheden nemlig trivielt. Hvis højresiden er endelig, findes et algebraisk frembringersystem a_1, \dots, a_l for V over R med $l = \dim_R^{\text{alg}} V$. Af Udskiftningssætningen (5.9) følger, at der for hvert algebraisk uafhængigt sæt i V med t elementer gælder $t \leq l$. Altså er $\text{tdeg}_R V \leq l$, hvormed den påståede ulighed er vist.

Altså gælder ligningen anført i sætningen. Sætningens sidste påstand følger nu umiddelbart af Lemma (5.8). \square

(5.11) Bemærkning. Begreberne og sætningerne i dette afsnit anvendes ofte i en situation hvor A og/eller R er legemer.

Antag først, at integritetsområdet A er et legeme. For enhver delring B af A vil da også brøkleget for B være indeholdt i A . For givne elementer a_1, \dots, a_m i A betegnes med

$$R(a_1, \dots, a_m)$$

brøkleget for delalgebraen $R[a_1, \dots, a_m]$. Øjensynlig er dette dellegeme af A det mindste, der indeholder R og alle a_i 'erne; det kaldes *dellegemet frembragt af R og a_i 'erne*.

Det givne legeme A siges at være *endeligt frembragt som legeme* over R , hvis der i A findes endelig mange elementer a_1, \dots, a_m , som *frembringer legemet A* , dvs opfylder at

$$A = R(a_1, \dots, a_m).$$

I denne situation har altså enhver delmængde V af A en endelig transcendensbasis over R , nødvendigvis med højst m elementer.

Betragt dernæst tilfældet, hvor A er et integritetsområde, endeligt frembragt som algebra over et legeme k af elementer a_1, \dots, a_m . Da er $A = k[a_1, \dots, a_m]$, og for brøkleget af A kan anvendes betegnelsen $k(a_1, \dots, a_m)$. Algebraen A er homomorft billede af en polynomiumsring, altså af formen $A = k[X_1, \dots, X_m]/\mathfrak{P}$, og idealet \mathfrak{P} er et primideal i polynomiusringen, da A er forudsat at være et integritetsområde. Resultaterne i dette kapitel har altså speciel anvendelse på sådanne kvotienter af polynomiumsringen over et legeme k . Ifølge Noether's Normaliseringslemma er en sådan algebra A hel over en delring af formen $k[x_1, \dots, x_t]$, hvor x_i 'erne er algebraisk uafhængige over k . Ifølge definitionen udgør x_i 'erne en transcendensbasis for A over k . Specielt er antallet t entydigt bestemt, nemlig som $t = \text{tdeg}_k A$.

(5.12) Sætning. Antag, at A er et integritetsområde, og at legemet k er en delring af A . Lad \mathfrak{p} være et primideal i A . Da gælder uligheden,

$$\text{tdeg}_k(A/\mathfrak{p}) \leq \text{tdeg}_k A.$$

Hvis $\text{tdeg}_k A < \infty$ og lighed gælder i uligheden ovenfor, da er $\mathfrak{p} = (0)$.

Bevis. Lad $a \mapsto \hat{a}$ betegne den kanoniske (surjektive) homomorfi $A \rightarrow A/\mathfrak{p}$. Betragt i A elementet $P(a_1, \dots, a_t)$, der fås ved at indsættelse af a_i 'er i et polynomium P . Det er klart, at billedet i A/\mathfrak{p} af dette element fås ved at indsætte \hat{a}_i 'erne i P . Det følger, at hvis \hat{a}_i 'erne er algebraisk uafhængige over k , så er a_i 'erne algebraisk uafhængige over k . Heraf følger den påståede ulighed umiddelbart.

Antag nu, at $\text{tdeg}_k A < \infty$ og at lighed gælder i uligheden. Vi kan da vælge a_i 'erne, med $t := \text{tdeg}_k(A/\mathfrak{p})$, så at \hat{a}_i 'erne udgør en transcendensbasis for A/\mathfrak{p} . Da er a_i 'erne algebraisk uafhængige over k . Specielt afbildes delringen $B := k[a_1, \dots, a_t]$ derfor isomorft på sit billede $k[\hat{a}_1, \dots, \hat{a}_t]$ i A/\mathfrak{p} . Da $t = \text{tdeg}_k A$, er a_i 'erne en transcendensbasis for A over k , og hvert element i A er derfor algebraisk over B . Lad nu a være et element forskelligt fra 0 i A . Der findes da en ligning,

$$b_m a^m + \dots + b_1 a + b_0 = 0, \quad (*)$$

hvor koefficienterne b_i tilhører B , og hvor ikke alle b_i 'er er lig med 0. I denne relation kan vi antage, at b_0 er forskellig fra 0. Er nemlig b_i den første koefficient forskellig fra 0, så kan a^i sættes uden for parentes på venstresiden; da $a \neq 0$, er parentesen lig med 0, og dette er så en ligning af den ønskede form.

Ligningen (*) medfører følgende ligning i A/\mathfrak{p} :

$$\hat{b}_m \hat{a}^m + \dots + \hat{b}_1 \hat{a} + \hat{b}_0 = 0$$

Nu var afbildningen $b \mapsto \hat{b}$ injektiv på B , og da vi har antaget $b_0 \neq 0$, følger det af den sidste ligning, at $\hat{a} \neq 0$.

Vi har vist, at for $a \neq 0$ er $\hat{a} \neq 0$. Altså er afbildningen $A \rightarrow A/\mathfrak{p}$ injektiv. Og det betyder, at kernen \mathfrak{p} er lig med (0) . \square

(5.13) Bemærkning. Nogle af resultaterne i denne paragraf kan generaliseres til tilfældet, hvor algebraen A ikke er et integritetsområde. Lad os her betragte en endeligt frembragt algebra $A = k[a_1, \dots, a_n]$ over et legeme k ; det forudsættes ikke, at A er et integritetsområde. Definitionen af transcendensgrad, $\text{tdeg}_k A$, som det største antal algebraisk uafhængige elementer fra A , kan overføres uændret. Bemærk, at hvis x_1, \dots, x_d er algebraisk uafhængige elementer i A , så er delalgebraen $k[x_1, \dots, x_d]$ isomorf med polynomiumsringen over k i d variable; specielt er delalgebraen et integritetsområde.

Sætning. Antag, at algebraen $A = k[x_1, \dots, x_n]$ er hel over en delalgebra $B = k[x_1, \dots, x_t]$ frembragt af t algebraisk uafhængige elementer. Da er $t = \text{tdeg}_k A$.

Bevis. Det skal vises, at hvis y_1, \dots, y_d er d algebraisk uafhængige elementer i A , så er $d \leq t$. Lad $C := k[y_1, \dots, y_d]$. Vi viser først, at der findes et primideal $\mathfrak{p} \subseteq A$ således, at $C \cap \mathfrak{p} = (0)$. Betragt hertil idealet $\tau = \text{Rad}(0)$ i A bestående af alle nilpotente elementer. Da A er noethersk, er τ en endelig fællesmængde af primidealer, $\tau = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_N$. Snit med C . Da C er et integritetsområde, er 0 det eneste nilpotente element i C . Derfor er $C \cap \tau = (0)$. Følgelig får vi ligningen,

$$(0) = (C \cap \mathfrak{p}_1) \cap \dots \cap (C \cap \mathfrak{p}_N).$$

Højresiden er en fællesmængde af primidealer og venstresiden er et primideal. Heraf følger let, at venstresiden er et af primidealene på højresiden. Med et af primidealene \mathfrak{p}_i som \mathfrak{p} , har vi altså den ønskede ligning $C \cap \mathfrak{p} = (0)$.

Ligningen $C \cap \mathfrak{p} = (0)$ viser, at den sammensatte homomorfi $C \rightarrow A \rightarrow A/\mathfrak{p}$ er injektiv. Det betyder, at elementerne y_1, \dots, y_d afbildes på d algebraisk uafhængige elementer i A/\mathfrak{p} . Derfor gælder uligheden

$$d \leq \text{tdeg}_k(A/\mathfrak{p}).$$

På den anden side kan vi betragte den sammensatte homomorfi $B \rightarrow A \rightarrow A/\mathfrak{p}$. Billedet er en delalgebra \overline{B} af A/\mathfrak{p} , og da A er hel over B følger det, at A/\mathfrak{p} er hel over \overline{B} . Specielt er A/\mathfrak{p} algebraisk over \overline{B} ; de to integritetsområder har derfor samme transcendensgrad over k . Nu har vi ulighederne,

$$t = \text{tdeg}_k B \geq \text{tdeg}_k \overline{B} = \text{tdeg}_k A/\mathfrak{p}.$$

Tilsammen får vi den søgte ulighed $d \leq t$. □

(5.14) Opgaver.

1. Lad B være en delring af A således at $R \subseteq B \subseteq A$. Vis formelen,

$$\text{tdeg}_R A = \text{tdeg}_B A + \text{tdeg}_R B.$$