

Notater

1. Hilbert-polynomium.

(1.1) Definition. Lad et øjeblik A være en kommutativ (additivt skrevet) gruppe (i anvendelserne er A oftest lig med \mathbb{Z}). Betragt funktioner $\varphi: \mathbb{Z} \rightarrow A$. For sådanne funktioner defineres *differensoperatoren* Δ ved

$$\Delta\varphi(n) := \varphi(n+1) - \varphi(n).$$

Differensligningen $\Delta\varphi = 0$ har som løsninger øjensynlig netop de konstante funktioner. En højreinvert til Δ er summationsoperatoren Σ . For værdier $n \geq 0$ er den defineret ved summen,

$$\Sigma\varphi(n) := \sum_{0 \leq i < n} \varphi(i).$$

Bemærk, at $\Sigma\varphi(0) = 0$. Det er klart, at for $n \geq 0$ gælder ligningen,

$$\Delta\Sigma\varphi(n) = \varphi(n).$$

Det er ikke svært at udvide definitionen af $\Sigma\varphi(n)$ til negative værdier af n således at den sidste ligning gælder for alle værdier af n .

(1.2) Observation. For et givet element a i A defineres for $i \geq 0$ funktionerne $\varphi_{i,a}$ ved

$$\varphi_{i,a}(n) := \binom{n}{i} a.$$

Funktionen $\varphi_{0,a}$ er den konstante funktion a og for $i = 1$ fås funktionen $n \mapsto na$ (her og i det følgende betegner $na = an$ den n 'te potens af a i gruppen A).

For $i > 0$ gælder ligningen $\Delta\varphi_{i,a} = \varphi_{i-1,a}$, idet binomialkoefficienterne som bekendt opfylder ligningen $\binom{n+1}{i} - \binom{n}{i} = \binom{n}{i-1}$. Heraf følger ligningen,

$$\Sigma\varphi_{i,a} = \varphi_{i+1,a}.$$

Funktionerne på ligningens to sider giver nemlig samme funktion når Δ anvendes, nemlig funktionen $\varphi_{i,a}$. Desuden har de begge værdien 0 for $n = 0$. Følgelig er de to funktioner identiske.

30. marts 2007

(1.3) Eksempel. Funktionen $\sigma_2(n) := 1^2 + 2^2 + \dots + (n-1)^2$ fås ved at anvende operatoren Σ på funktionen n^2 . Øjensynlig er $n^2 = 2\binom{n}{2} + \binom{n}{1}$. Følgelig udledes ligningen $\sigma_2(n) = 2\binom{n}{3} + \binom{n}{2}$, og altså den velkendte formel,

$$1^2 + 2^2 + \dots + n^2 = 2\binom{n+1}{3} + \binom{n+1}{2}.$$

(1.4) Definition. I det følgende vil vi kun interessere os for funktionsværdierne $\varphi(n)$ for store værdier af n . Vi vil her sige, at funktionen $\varphi: \mathbb{Z} \rightarrow A$ er en *polynomial funktion*, hvis der findes et tal $r \geq 0$, således at $\Delta^{r+1}\varphi(n) = 0$ for $n \gg 0$.

Ved *graden* af en polynomial funktion φ forstås det største tal r for hvilket funktionen $\Delta^r\varphi(n)$ for $n \gg 0$ ikke er identisk 0. Hvis $\varphi(n) = 0$ for $n \gg 0$ findes ingen sådanne tal r ; en sådan funktion tillægges graden $-\infty$.

En funktion φ er øjensynlig polynomial af grad $\leq r$, hvis og kun hvis $\Delta^{r+1}\varphi(n) = 0$ for $n \gg 0$. At φ er polynomial af grad 0 betyder, at funktionsværdien $\varphi(n)$ for store værdier af n er en konstant forskellig fra nul-elementet i A .

(1.5) Sætning. For funktioner $\varphi: \mathbb{Z} \rightarrow A$ og et givet tal $r \geq 0$ er følgende betingelser ækvivalente:

- (i) Funktionen φ er polynomial af grad $\leq r$.
- (ii) Funktionen $\Delta\varphi$ er polynomial af grad $\leq r-1$.
- (iii) Der findes $r+1$ elementer a_0, \dots, a_r i A således at

$$\varphi(n) = a_r\binom{n}{r} + \dots + a_1\binom{n}{1} + a_0 \text{ for } n \gg 0.$$

- (iv) (Når A er en undergruppe i \mathbb{C} ;) Der findes et polynomium f af grad $\leq r$ således at $\varphi(n) = f(n)$ for $n \gg 0$.

Hvis betingelserne er opfyldt, så gælder yderligere, at koefficienterne a_i i (iii) er entydigt bestemt ved φ , og at φ har grad r , hvis og kun hvis $a_r \neq 0$.

Bevis. Det følger umiddelbart af definitionen, at (i) og (ii) er ækvivalente. I (iii) er funktionen på højresiden summen af funktionerne φ_{i,a_i} for $i = 0, \dots, r$. Af udregningen i Observation (1.2) følger, at denne sum er polynomial af grad $\leq r$. Altså vil (iii) medføre (i). Binomialkoefficienten $\binom{n}{i}$ er, som funktion af n , et polynomium af grad i . Heraf ses, at (iii) medfører (iv). Når operatoren Δ anvendes på monomiet n^r fås øjensynlig et polynomium af grad $r-1$ med ledende koefficient r . Heraf ses, at når Δ^r anvendes på et polynomium af grad r med ledende koefficient a fås konstanten $r!a$. Herefter er det klart, at (iv) medfører (i).

Vi mangler at vise, at (i) medfører (iii). Denne påstand vises ved induktion efter r . Den er sand for $r = 0$, idet begge betingelser udtrykker, at $\varphi(n)$ er konstant for $n \gg 0$. Antag $r > 0$. Funktionen $\Delta\varphi$ er polynomial af grad $\leq r-1$, så induktivt findes altså r elementer a_1, \dots, a_r i A således at de to funktioner $\Delta\varphi$ og $\varphi_{a_r,r-1} + \dots + \varphi_{a_2,1} + \varphi_{a_1,0}$ har samme værdi i n , når $n \gg 0$. Disse to funktioner fås ved at anvende operatoren Δ på funktionerne φ og $\varphi_{a_r,r} + \dots + \varphi_{a_1,1}$. Heraf ses, at når Δ anvendes på differensen,

$$\varphi - (\varphi_{a_r,r} + \dots + \varphi_{a_1,1}),$$

30. marts 2007

så fås en funktion, der er 0 for store værdier af n . Differensen selv må derfor være en konstant for store værdier af n . Betegnes denne konstant med a_0 , gælder øjensynlig den ønskede relation i (iii).

Hermed er vist, at betingelserne er ækvivalente. Entydigheden af koefficienterne (iii) vises ved et lignende induktivt argument. Endelig følger det af relationen i (iii), at $\Delta^r \varphi(n) = a_r$ for $n \gg 0$. Graden af φ er altså r (og ikke mindre end r), netop når $a_r \neq 0$. \square

(1.6) Setup. I det følgende betragtes en noethersk ring R , og polynomiumsringen $G := R[X_1, \dots, X_r]$ i r variable. Som bekendt er også G en noethersk ring. Ringen G er *graduere*t: Idet G_i er undermodulen af homogene polynomier af grad i , kan ethvert polynomium $f \in G$ skrives som summen af sine homogene led:

$$f = f_0 + f_1 + f_2 + \dots$$

(summen er naturligvis endelig: $f_i \neq 0$ gælder kun for endelig mange i).

Videre betragtes en endeligt frembragt, graduere G -modul N . At N er graduere G -modul, betyder, at der i N er givet R -undermoduler N_0, N_1, N_2, \dots således, at N som R -modul er den direkte sum af undermodulerne N_j :

$$N = N_0 \oplus N_1 \oplus N_2 \oplus \dots;$$

det betyder, at hvert element $x \in N$ entydigt kan skrives som en sum af sine *homogene* led:

$$x = x_0 + x_1 + x_2 + \dots, \quad \text{med } x_j \in N_j \text{ for } j = 0, 1, \dots,$$

og at multiplikation med en skalar, der er homogen af grad i i G , afbilder $N_j \rightarrow N_{i+j}$. Med andre ord, hvis $f \in G_i$ og $x \in N_j$, så er $fx \in N_{i+j}$.

Da N er endeligt frembragt, er N også frembragt af endelig mange homogene elementer v_α ; lad n_α være graden af v_α . Hvert polynomium f er en R -linearkombination af endelig mange *monomier* m_β . Hvis d_β er graden af monomiet m_β , så har $m_\beta v_\alpha$ graden $d_\beta + n_\alpha$. Derfor er N_n frembragt af de produkter $m_\beta v_\alpha$ for hvilke $d_\beta + n_\alpha = n$, og det giver kun endelig mange muligheder for β . Specielt er N_n en endeligt frembragt R -modul.

Vi vil interessere os for følgende betingelse:

(*) Hver af de homogene komponenter N_n har endelig længde som R -modul.

Da hvert N_n er endeligt frembragt som R -modul, er betingelsen (*) fx opfyldt, når ringen R har endelig længde.

Observation. Betingelsen (*) er opfyldt, når blot hver af de endelig mange cykliske undermoduler Rv_α af N_{n_α} har endelig længde. For hvert monomium m_β i G definerer multiplikation med m_β nemlig en surjektiv homomorfi af Rv_α på $Rm_\beta v_\alpha$. Hvis alle undermodulerne Rv_α har endelig længde, så følger det, at også undermodulerne $Rm_\beta v_\alpha$ har endelig længde, og da N_n var en sum af endelig mange sådanne undermoduler, har også N_n endelig længde.

(1.7) Sætning. Antag setup'et i (1.6), og at betingelsen (*) er opfyldt. Da er funktionen,

$$\lambda_N(n) := \text{long } N_n,$$

en polynomial funktion med værdier i \mathbb{Z} af grad mindre end r (hvor r var antallet af variable i polynomiumsringen G).

Bevis. Sætningen vises ved induktion efter r . For $r = 0$, er $G = G_0 = R$ og $G_i = 0$ for $i \neq 0$. Der er kun ét homogent monomium i G , nemlig konstanten 1, og den største grad af et produkt $m_\beta v_\alpha$ er derfor den største grad af frembringerne v_α . Derfor er $N_n = 0$, når n er større end denne grad. For $n \gg 0$ er altså $\lambda_N(n) = 0$, og følgelig er λ_N polynomial af grad ≤ -1 .

Antag, at $r \geq 1$, og betragt multiplikation med skalarer X_r i modulen N . Denne multiplikation er en lineær afbildning af N ind i N , og den er homogen af grad 1. Lad K være kernen og lad L være kokernen. Da er K og L graduerede moduler, idet K_n blot er kernen for multiplikationen $X_r: N_n \rightarrow N_{n+1}$ og L_n defineres som kokernen for denne multiplikation. Vi har da for hvert n en eksakt følge,

$$0 \rightarrow K_n \rightarrow N_n \xrightarrow{X_r} N_{n+1} \rightarrow L_n \rightarrow 0.$$

Modulen L er en kvotient af N , og derfor endeligt frembragt. Da G som nævnt er noethersk, er også undermodulen K i N endeligt frembragt. Videre er K_n , som undermodul af N_n , og L_n , som kvotientmodul af N_{n+1} , af endelig længde som R -moduler. Modulerne K og L opfylder altså betingelsen (*). Af den eksakte følge sluttes videre, at den alternerende sum af de indgående modulers længde er lig med 0. Da $\text{long } N_{n+1} - \text{long } N_n = \lambda_N(n+1) - \lambda_N(n) = \Delta\lambda_N(n)$, gælder altså ligningen,

$$\Delta\lambda_N = \lambda_L - \lambda_K. \quad (1.7.1)$$

De to moduler L og K annulleres af skalarer X_r , og de kan derfor opfattes som moduler over kvotientringen $G/X_r G$, som vi kan identificere med polynomiumsringen $R[X_1, \dots, X_{r-1}]$ i $r-1$ variable. Modulerne L og K , som moduler over G/GX_r , opfylder altså forudsætningen med $r-1$ i stedet for r . Induktivt sluttes derfor, at de to funktioner på højresiden af (1.7.1) er polynomiale af grad mindre end $r-1$. Altså er $\Delta\lambda_N$ polynomial af grad mindre end $r-1$. Af Sætning (1.5) følger så, at λ_N er polynomial af grad mindre end r , som påstået. \square

(1.8) Definition. Antag, at betingelserne i Sætning (1.7) er opfyldt. Funktionen λ_N er da polynomial af en grad d , der er mindre end eller lig med $r-1$. Antag først, at $d = -\infty$. I dette tilfælde er altså $\text{long } N_n = 0$ for $n \gg 0$, altså $N_n = 0$ for $n \gg 0$. Da også $N_n = 0$ for $n \ll 0$ (dette følger af at N er endeligt frembragt), er altså kun endelig mange N_n 'er forskellige fra 0. Modulen N er den direkte sum af N_n 'erne, så N har derfor endelig længde som R -modul. Omvendt er det klart, at hvis N har endelig længde som R -modul, så er kun endelig mange N_n 'er forskellige fra 0. Betingelsen $d = -\infty$ gælder altså hvis og kun hvis N har endelig længde som R -modul.

30. marts 2007

Antag dernæst, at $d \geq 0$. Af Sætning (1.5), anvendt med $A = \mathbb{Z}$, følger så, at der findes $d + 1$ hele tal e_0, \dots, e_d , så at

$$\text{long } N_n = e_d \binom{n}{d} + \dots + e_1 \binom{n}{1} + e_0 \text{ for } n \gg 0. \quad (1.8.1)$$

Polynomiet på højresiden af ovenstående ligning kaldes for *Hilbert-polynomiet* hørende til den givne modul N , og det betegnes χ_N . Graden af Hilbert-polynomiet, altså tallet d , kaldes også den *homogene dimension* af N , og koefficienten e_d kaldes *multipliciteten* af N . Bemærk, at multipliciteten e_d er positiv. Multipliciteten er nemlig forskellig fra 0, og var den negativ ville højresiden i (1.8.1) være negativ når $n \gg 0$, i modstrid med at venstresiden i (1.8.1) er en længde, og dermed ikke-negativ.

(1.9) Bemærkning. Betragt, under forudsætningerne i Sætning (1.7), den akkumulerede sum,

$$\sigma_N(n) := \sum_{i < n} \text{long } N_i,$$

Den herved definerede funktion σ_N opfylder øjensynlig $\Delta\sigma_N = \lambda_N$. Da λ_N er polynomial af grad $\leq r - 1$, er σ_N polynomial af grad $\leq r$. Hvis $d \geq 0$, så har σ_N graden $d + 1$. Hvis $d = -\infty$, så er kun endelig mange N_n forskellige fra 0, så når n er stor er $\sigma_N(n) = \text{long } N$, jfr diskussionen i (1.8). I dette tilfælde, dvs når N har endelig længde som R -modul, er altså graden af σ_N lig med 0 når $N \neq 0$ og lig med $-\infty$ når $N = 0$. Bemærk, at vi (når $N \neq 0$) har følgende ligning for den akkumulerede funktion (med en konstant l):

$$\sum_{i < n} \text{long } N_i = e_d \binom{n}{d+1} + \dots + e_0 \binom{n}{1} + l \quad \text{når } n \gg 0$$

(1.10) Sætning. Antag, at N opfylder betingelserne i Sætning (1.7). Lad N' være en homogen undermodul i N , og lad $N'' = N/N'$ være den tilhørende kvotientmodul. Da vil også N' og N'' opfylde betingelserne, og for Hilbert-polynomierne gælder ligningen,

$$\chi_N = \chi_{N'} + \chi_{N''}.$$

Bevis. Da G som nævnt er noethersk, er undermodulen N' endeligt frembragt, og trivielt er kvotienten N'' endeligt frembragt. For hvert n findes en eksakt følge,

$$0 \rightarrow N'_n \rightarrow N_n \rightarrow N''_n \rightarrow 0.$$

Specielt følger heraf, at N'_n og N''_n har endelig længde. Altså er betingelsen (*) opfyldt for både N' og N'' . Af den eksakte følge fås ligningen,

$$\lambda_N(n) = \lambda_{N'}(n) + \lambda_{N''}(n).$$

Differensfunktionen $\lambda_{N'} + \lambda_{N''} - \lambda_N$ er altså 0. Funktionerne λ stemmer for store værdier af n overens med de tilsvarende polynomier χ . Værdien i n af differenspolynomiet $\chi_{N'} + \chi_{N''} - \chi_N$ er altså lig med 0, når $n \gg 0$. Heraf følger, at differenspolynomiet er lig med 0 for alle n , hvormed den søgte ligning er bevist. \square

30. marts 2007

(1.11) Bemærkning. Som nævnt (1.6) er betingelsen (*) opfyldt, når ringen R selv har endelig længde. Den mest oplagte anvendelse er på polynomiumsringen $G = k[X_1, \dots, X_r]$, hvor $R = k$ er et legeme. Længden af en k -modul V er vektorrumdimensionen, som vi betegner $\text{rk } V$. Til enhver endeligt frembragt, graderet G -modul N vil Hilbertpolynomiet χ_N altså opfylde, at $\text{rk } N_n = \chi_N(n)$ for $n \gg 0$. Graden af χ_N og koefficienterne e_0, \dots, e_d er invarianter for modulen N ; de spiller en vigtig rolle i algebraisk geometri.

Betragt fx $N = G$. Her består N_n af de homogene polynomier af grad n . Monomierne af grad n er en k -basis, og der er $\binom{n+r-1}{r-1}$ sådanne polynomier (idet vi antager $r \geq 1$). Altså gælder ligningen,

$$\text{rk } G_n = \binom{n+r-1}{r-1} \quad \text{for } n \geq 0.$$

Her er højresiden et polynomium af grad $r-1$, og dette polynomium er altså Hilbert polynomiet χ_G . Det er ikke svært at skrive dette polynomium som linearkombination af polynomierne $\binom{n}{i}$ for $i = 1, \dots, r-1$, og det er i hvert fald klart, at multipliciteten er $e_{r-1} = 1$.

Betragt videre et homogent polynomium f forskelligt fra 0, af grad h . Lad N være kvotienten G/Gf . Multiplikation med f giver da for alle n en eksakt følge,

$$0 \rightarrow G_{n-h} \xrightarrow{f} G_n \rightarrow N_n \rightarrow 0.$$

(Idet vi sætter $G_n := 0$ for $n < 0$.) Altså er $\lambda_N(n) = \lambda_G(n) - \lambda_G(n-h)$. For $n \geq h$ slutter vi, at $\lambda_N(n) = \chi_G(n) - \chi_G(n-h)$. Her er højresiden $\chi_G(n) - \chi_G(n-h)$ et polynomium for alle n , og dette polynomium er derfor Hilbert-polynomiet χ_N . Altså er

$$\chi_{G/fG}(n) = \binom{n+r-1}{r-1} - \binom{n-h+r-1}{r-1}.$$

Det er klart, at Hilbert-polynomiet $\chi_{G/fG}$ har grad $r-2$ (her antager vi at $r \geq 2$), og at multipliciteten er graden h af polynomiet f .

(1.12) Opgaver.

- U9 1. Eftervis formelen $\binom{n+r}{p} = \sum_{i+j=p} \binom{n}{i} \binom{r}{j}$. [Vink: brug binomialformlen på $(1+x)^{n+r} = (1+x)^n(1+x)^r$.] Udtryk binomialkoefficienten $\binom{n+r}{r}$ som linearkombination af binomialkoefficienterne $\binom{n}{i}$ for $i = 0, 1, \dots, r$.

2. Samuel-Polynomialium.

(2.1) Setup. Betragt en noethersk ring R , et ideal \mathfrak{a} i R , og en endeligt frembragt R -modul M . Rees-ringen \tilde{R} og Rees-modulen \tilde{M} er de direkte summer,

$$\begin{aligned}\tilde{R} &= R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots, \\ \tilde{M} &= M \oplus \mathfrak{a}M \oplus \mathfrak{a}^2M \oplus \cdots.\end{aligned}$$

Rees-ringen \tilde{R} er en gradueret ring. Det er bekvemt at tænke på den som delringen af polynomiumsringen $R[T]$ bestående af de polynomier, hvor koefficienten til T^i tilhører \mathfrak{a}^i for alle i . Alternativt er \tilde{R} frembragt som R -algebra af alle homogene førstegrads-polynomier aT med $a \in \mathfrak{a}$. Hvis idealet \mathfrak{a} er frembragt af r elementer, $\mathfrak{a} = (a_1, \dots, a_r)$, så er \tilde{R} frembragt som R -algebra af elementerne a_1T, \dots, a_rT , der er homogene af grad 1. Når et sådant frembringersystem for \mathfrak{a} er givet, kan vi opfatte \tilde{R} som en kvotient af polynomiumsringen $G = R[X_1, \dots, X_r]$ modulo et homogent ideal.

Rees-modulen er en gradueret \tilde{R} -modul. Hvis (v_α) er et endeligt frembringersystem for M , så vil v_α 'erne, opfattet som homogene elementer af grad 0 i $\tilde{M}_0 = M$, udgøre et frembringersystem for \tilde{M} som \tilde{R} -modul.

Betragt nu undermodulen $\mathfrak{a}\tilde{M}$ i \tilde{M} . Elementerne i \mathfrak{a} opfattes her som homogene skalarer af grad 0 i \tilde{R} , så $\mathfrak{a}\tilde{M}$ er den homogene undermodul,

$$\mathfrak{a}\tilde{M} = \mathfrak{a}M \oplus \mathfrak{a}^2M \oplus \mathfrak{a}^3M \oplus \cdots.$$

Kvotientmodulen $\tilde{M}/\mathfrak{a}\tilde{M}$ er derfor den graduerede modul,

$$\tilde{M}/\mathfrak{a}\tilde{M} = M/\mathfrak{a}M \oplus \mathfrak{a}M/\mathfrak{a}^2M \oplus \mathfrak{a}^2M/\mathfrak{a}^3M \oplus \cdots.$$

Den betegnes også udførligt $\text{Gr}_\mathfrak{a}(M)$. Da \tilde{R} -modulen \tilde{M} er endeligt frembragt af v_α 'erne, vil restklasserne af v_α 'erne i $\text{Gr}_\mathfrak{a}(M)_0 = M/\mathfrak{a}M$ være et \tilde{R} -frembringersystem for kvotienten $\text{Gr}_\mathfrak{a}(M)$.

(2.2) Definition. Antag, at kvotienten $M/\mathfrak{a}M$ har endelig længde. Som bekendt har en R -modul endelig længde, hvis og kun hvis alle primidealer i støtten er maximalidealer. Støtten for M består af de primidealer, der omfatter annullatoren $\text{Ann } M$, og støtten for $M/\mathfrak{a}M$ er delmængden heraf bestående af de primidealer, som desuden omfatter \mathfrak{a} . Antagelsen er altså, at alle sådanne primidealer, dvs alle primidealer der indeholder $\mathfrak{a} + \text{Ann } M$, er maksimalidealer. Specielt er antagelsen opfyldt, hvis R/\mathfrak{a} har endelig længde.

Det påstås, hvis vi opfatter \tilde{R} som en kvotient af polynomiumsringen $G = R[X_1, \dots, X_r]$, så er betingelsen (*) i (1.6), med $N := \text{Gr}_\mathfrak{a}(M)$ som G -modul, opfyldt. Dette følger af, at N som nævnt er frembragt af de endelig mange restklasser i $N_0 = M/\mathfrak{a}M$ af v_α modulo $\mathfrak{a}M$, og N_0 har derfor ifølge antagelsen endelig længde. Af Sætning (1.7) fås derfor følgende:

Resultat. For alle n har kvotienten $\mathfrak{a}^n M / \mathfrak{a}^{n+1} M$ endelig længde, og funktionen,

$$n \mapsto \text{long } \mathfrak{a}^n M / \mathfrak{a}^{n+1} M,$$

er *polynomial af grad mindre end r* , og dermed af grad mindre end det minimale antal elementer, der frembringer idealet \mathfrak{a} .

Betragt nu den akkumulerede sum af længderne $\sum_{i < n} \text{long } \mathfrak{a}^i M / \mathfrak{a}^{i+1} M$, ligesom i Bemærkning (1.9). De enkelte moduler $\mathfrak{a}^i M / \mathfrak{a}^{i+1} M$ er de successive kvotienter i filtrationen af $M / \mathfrak{a}^n M$ defineret ved kæden,

$$\mathfrak{a}^n M \subseteq \dots \subseteq \mathfrak{a} M \subseteq M.$$

Summen af længderne er derfor lig med længden af $M / \mathfrak{a}^n M$. Som bemærket i (1.9) fås derfor følgende:

Sætning. For alle n har kvotienten $M / \mathfrak{a}^n M$ endelig længde, og funktionen,

$$\sigma_{\mathfrak{a}, M}(n) = \text{long } M / \mathfrak{a}^n M,$$

er *polynomial af grad mindre end eller lig med det minimale antal elementer, der frembringer idealet \mathfrak{a}* .

Polynomiet hørende til den polynomiale funktion $\sigma = \sigma_{\mathfrak{a}, M}$ kaldes *Hilbert-Samuel-polynomiet* eller blot *Samuel-polynomiet*, og vi vil betegne det $\chi_{\mathfrak{a}, M}$. Graden af Samuel-polynomiet betegnes $d = d_{\mathfrak{a}}(M)$. Hvis $M = \mathfrak{a}M$, er øjensynlig $\sigma(n) = 0$ for alle n . I dette tilfælde er Samuel-polynomiet altså nul-polynomiet og $d = -\infty$. Antag, at $\mathfrak{a}M \subset M$. Funktionen $\sigma(n)$ er øjensynlig voksende, så det følger, at $\sigma(n) > 0$ for alle $n \geq 1$. Samuel-polynomiet er derfor ikke nul-polynomiet, og graden d er derfor større end eller lig med 0. Af Sætning (1.5) følger, at der findes $d + 1$ hele tal e_0, \dots, e_d således at

$$\text{long } M / \mathfrak{a}^n M = e_d \binom{n}{d} + \dots + e_1 \binom{n}{1} + e_0 \quad \text{for } n \gg 0.$$

Med $e = e_{\mathfrak{a}}(M)$ betegnes koefficienten e_d . Den er positiv, idet polynomiet for $n \gg 0$ har ikke-negative værdier.

(2.3) Bemærkning. Antag, at $M / \mathfrak{a}M$ har endelig længde. Af resultaterne i (2.2) følger, at graden $d_{\mathfrak{a}}(M)$ er mindre end eller lig med det mindste antal elementer der frembringer idealet \mathfrak{a} . Modulen M er en modul over kvotientringen $\bar{R} := R / \text{Ann } M$. Lad $\bar{\mathfrak{a}}$ betegne billedet af \mathfrak{a} i kvotientringen \bar{R} . Det er klart, at længden af kvotienten $M / \mathfrak{a}^n M$, der definerer funktionen $\sigma_{\mathfrak{a}, M}$, ikke ændres, hvis M opfattes som \bar{R} -modul og \mathfrak{a} erstattes med $\bar{\mathfrak{a}}$. Heraf følger, at $d_{\mathfrak{a}, M}$ er mindre end eller lig med det mindste antal elementer, der frembringer idealet $\bar{\mathfrak{a}}$ i \bar{R} .

30. marts 2007

(2.4) Eksempel. Betragt $R = \mathbb{Z}$, og lad $\mathfrak{a} = (a)$ være hovedidealet frembragt af et positivt helt tal a . Da er $\mathbb{Z}/(a)$ en endelig ring, og specielt af endelig længde, så resultatet i (2.2) kan anvendes på enhver endeligt frembragt kommutativ gruppe M . Da idealet er frembragt af ét element får Samuel-polynomiet $\chi_{(a),M}$ grad højst 1. Lad $a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ være primopløsningen af a . Længden af $\mathbb{Z}/(a)$ er da summen $\alpha := \alpha_1 + \cdots + \alpha_t$, og mere generelt, længden af $\mathbb{Z}/(a)^n$ er lig med αn . Samuel-polynomiet $\chi_{(a),\mathbb{Z}}$ er altså førstegradspolynomiet αn , og $e_{(a)}(\mathbb{Z}) = \alpha$. Betragt videre en cyklisk gruppe $M = \mathbb{Z}/(q^\varepsilon)$, hvor q er et primtal. Hvis q er forskelligt fra p_i 'erne, vil multiplikation med a være bijektiv på M . Er derimod q lig med et af p_i 'erne, vil multiplikation med a^n på M være nul-afbildningen når $n \gg 0$. I det første tilfælde er $\text{long } M/a^n M = 0$ for alle n , så Samuel-polynomiet er nulpolynomiet. I det andet tilfælde er $\text{long } M/a^n M = \text{long } M = \varepsilon$ når $n \gg 0$, så Samuel-polynomiet er det konstante polynomium ε .

(2.5) Sætning. Antag, at $M/\mathfrak{a}M$ har endelig længde. Lad M' være en undermodul i M og lad $M'' = M/M'$ være den tilhørende kvotientmodul. Da har begge kvotienter $M'/\mathfrak{a}M'$ og $M''/\mathfrak{a}M''$ endelig længde. Videre gælder ligningen,

$$d_{\mathfrak{a}}(M) = \max\{d_{\mathfrak{a}}(M'), d_{\mathfrak{a}}(M'')\}. \quad (2.5.1)$$

Endelig gælder, at funktionen,

$$\sigma_{\mathfrak{a},M'} + \sigma_{\mathfrak{a},M''} - \sigma_{\mathfrak{a},M}, \quad (2.5.2)$$

overalt er ikke-negativ, og den er polynomial af en grad, der er $\leq d_{\mathfrak{a}}(M') - 1$ og dermed $\leq d_{\mathfrak{a}}(M) - 1$.

Bevis. At $M/\mathfrak{a}M$ har endelig længde er som nævnt enbetydende med at alle primidealer, som omfatter $\mathfrak{a} + \text{Ann } M$ er maksimalidealer. For både undermodulen M' og kvotientmodulen M'' gælder, at annihilatoren omfatter $\text{Ann } M$. Heraf slutes, at både $M'/\mathfrak{a}^n M'$ og $M''/\mathfrak{a}^n M''$ har endelig længde.

Funktionerne $\sigma_{M'}(n) = \text{long } M'/\mathfrak{a}^n M'$ og $\sigma_{M''}(n) = \text{long } M''/\mathfrak{a}^n M''$ er altså polynomiale. Lad d' og d'' betegne deres grader, og lad δ betegne funktionen i (2.5.2), altså

$$\delta(n) = \sigma_{M'}(n) + \sigma_{M''}(n) - \sigma_M(n). \quad (2.5.3)$$

Da er δ en polynomial funktion, idet de tre indgående funktioner σ i (2.5.2) er polynomiale. Nu findes som bekendt for hvert n en eksakt følge,

$$M'/\mathfrak{a}^n M' \rightarrow M/\mathfrak{a}^n M \rightarrow M''/\mathfrak{a}^n M'' \rightarrow 0.$$

Da homomorfien $M/\mathfrak{a}^n M \rightarrow M''/\mathfrak{a}^n M''$ er surjektiv, slutes at $0 \leq \sigma_{M''}(n) \leq \sigma_M(n)$. Heraf ses, at der for graderne gælder uligheden $d'' \leq d$. I den eksakte følge er kernen for den første homomorfi undermodulen i $M'/\mathfrak{a}^n M'$ bestemt ved $K_n/\mathfrak{a}^n M'$, hvor

$$K_n := M' \cap \mathfrak{a}^n M.$$

Af den eksakte følge suppleret med denne kerne sluttes, at den alternerende sum af længderne af de indgående moduler er lig med 0. Denne relation kan skrives

$$\delta(n) = \sigma_{M'} + \sigma_{M''}(n) - \sigma_M(n) = \text{long } K_n/\alpha^n M'.$$

Heraf følger først, at $\delta(n) \geq 0$, som påstået. Øjensynlig er $\alpha^n M' \subseteq K_n$. Af Artin–Rees' Lemma følger, at der findes et naturligt tal h , således at der for alle $n \geq h$ gælder $K_n \subseteq \alpha^{n-h} M'$. For $n \geq h$ er altså

$$\alpha^n M' \subseteq K_n \subseteq \alpha^{n-h} M' \subseteq M',$$

og heraf fås uligheden,

$$\begin{aligned} \delta(n) &= \text{long } K_n/\alpha^n M' = \text{long } M'/\alpha^n M' - \text{long } M'/K_n \\ &\leq \text{long } M'/\alpha^n M' - \text{long } M'/\alpha^{n-h} M' = \sigma_{M'}(n) - \sigma_{M'}(n-h). \end{aligned}$$

Da funktionen $\sigma_{M'}$ er polynomial af grad d' sluttes, at differensen $\sigma_{M'}(n) - \sigma_{M'}(n-h)$, som funktion af n , er polynomial af grad $d' - 1$. Denne differens majoriserer $\delta(n)$, og da $\delta(n) \geq 0$ følger det, at δ er polynomial af grad $\leq d' - 1$. Ligningen (2.5.3) er, når $n \gg 0$, en ligning mellem polynomier. Venstresiden har grad $\leq d' - 1$. Polynomierne på højresiden har grader d' , d'' og d , og vi har vist, at $d'' \leq d$. Det ses, at ligningen kun kan være opfyldt, når $d = \max\{d', d''\}$ (og yderligere ses når $d \geq 0$, at koefficienterne e' , e'' og e til d -tegradsleddene på højresiden må opfylde, at $e' + e'' = e$).

Hermed er sætningens påstande eftervist. \square

(2.6) Korollar. Antag, at $M/\alpha M$ har endelig længde. Da gælder for enhver homomorfi $f: M \rightarrow M$, at differensen,

$$\sigma_{\alpha, \text{Coker } f} - \sigma_{\alpha, \text{Ker } f},$$

er polynomial af grad $\leq d_{\alpha}(M) - 1$. Specielt gælder, hvis homomorfien f er injektiv, at $d_{\alpha}(\text{Coker } f) \leq d_{\alpha}(M) - 1$.

Bevis. Korollaret fås ved at anvende sætningens sidste del først med $M' := \text{Ker } f$ og $M'' := f(M)$ og dernæst med $M' := f(M)$ og $M'' := \text{Coker } f$. Korollarets sidste påstand er blot specialtilfældet, hvor $\text{Ker } f = 0$. \square

(2.7) Bemærkning. Antag, at R/α har endelig længde. Sætningen kan da anvendes på enhver (endeligt frembragt) R -modul M , og specielt på $M = R$. Yderligere er

$$d_{\alpha}(M) \leq d_{\alpha}(R),$$

thi da M er endeligt frembragt, er M homomorft billede af en fri modul R' , og gentagen anvendelse af Sætning (2.5) giver relationerne $d_{\alpha}(M) \leq d_{\alpha}(R') = d_{\alpha}(R)$.

(2.8) Opgaver.

- H4 1. Bestem for $R = \mathbb{Z}$ og $\alpha = (24)$ Hilbert–Samuel-polynomiet $\chi_{\alpha, M}$ for $M = \mathbb{Z}$. – Og for $M = \mathbb{Z}/9\mathbb{Z}$, og $M = \mathbb{Z}/10\mathbb{Z}$ og $M = \mathbb{Z}/11\mathbb{Z}$.