Appendix I

הוכחת טענות טכניות:

(1) קיים בסיס המקיים $[e_\alpha,e_\beta]=\pm r e_{\alpha+\beta}$

$r\in\mathbb{Z}_+$ מינימלי עבורו $0=(ad\, e_\alpha)^r e_\beta$

(2) $\mathfrak{g}_\mathbb{Z}=span_\mathbb{Z}\{e_\alpha,h_\alpha\}_{\alpha\in R}$ יציב תחת $ad(e_\beta^n/n!)$ לכל $n\in\mathbb{Z}_+$ $\beta\in R$

(3) $h,e\in\mathfrak{g}$ $[h,e]=\lambda e$

אז לכל $p\in\mathbb{C}[X]$ $p(h)e^m=e^m p(h+\lambda m)$

<u>הוכחה</u>: $he=\lambda e+eh=e(\lambda+h)$

$$he^m=hee^{m-1}=e(\lambda+h)e^{m-1}=e^m(m\lambda+h)$$

$$h^ie^m=hh^{i-1}e^m=he^m(m\lambda+h)^{i-1}=e^m(m\lambda+h)^i$$

(·) נכון לצירופים לינאריים

(4) עבור $u\in U$ $m\in\mathbb{Z}_+$ $C_{u,m}:=\binom{u}{m}$

עבור $e,f,h\in U$ $(e,f,h)=sl_2$ ~מתקיים

$$e^m/m!\; f^n/n! = \sum_{j=0}^{\min\{m,n\}} \frac{f^{n-j}}{(n-j)!}C_{h-m-n+2j,j}\frac{e^{m-j}}{(m-j)!}$$

<u>הוכחה</u>: שלב I: (·) $hf^n=f^n(h-2n)$

(·) באינדוקציה $e f^n/n! = \frac{f^n}{n!}e+\frac{f^{n-1}}{(n-1)!}(h-n+1)$

$$e f^{n+1}/(n+1)! = \frac{1}{n+1}\, e f f^n/n! = \frac{1}{n+1}(fe-h)f^n/n!$$

$$=\frac{1}{n+1}\left[f\left(f^n/n!\, e+\frac{f^{n-1}}{(n-1)!}(h-n+1)\right)-h f^n/n!\right]$$

$$=\frac{f^{n+1}}{(n+1)!}e+\frac{n}{n+1}\frac{f^n}{n!}(h-n+1)-\frac{1}{n+1}h\frac{f^n}{n!}$$

$$=f^{n+1}/(n+1)!\, e+\frac{f^n}{n!}(h-(n+1)+1)-\frac{1}{(n+1)!}\left(hf^n+(n+1)f^n-f^n(h-n+1)\right)$$

$$=f^{n+1}/(n+1)!\, e+\frac{f^n}{n!}(h-(n+1)+1)-\frac{1}{(n+1)!}\underbrace{\left(hf^n-f^n(h-2n)\right)}_{0}$$

(·) מטענה טכנית 3 $e\,C_{h+x,*}=C_{h-2+x,*}$

<u>שלב II</u>: אינדוקציה על m

הוכחת טענות טכניות:

(5) $u^{(n)} \in U(\mathfrak{g})$. הסדרה $(u^{(n)})_{n\in\mathbb{Z}_+}$ תיקרא סידרת חזקות מחולקות (Sequence of divided powers) אם $\Delta u^{(n)} = \sum_{j=0}^{n} u^{(j)} \otimes u^{(n-j)}$

(i) $x\in\mathfrak{g}$ $\quad u^{(n)} = x^n/n!$ סידרת חזקות מחולקות

<u>הוכחה:</u>

$$\Delta\left(\frac{x^n}{n!}\right) = \frac{1}{n!}(\Delta(x^n)) = \frac{1}{n!}(\Delta(x))^n$$
$$= \frac{1}{n!}(x\otimes 1 + 1\otimes x)^n = \frac{1}{n!}\sum_{j=0}^{n}\binom{n}{j}(x\otimes 1)^j(1\otimes x)^{n-j}$$
$$= \frac{1}{n!}\sum_{j=0}^{n}\binom{n}{j} x^j \otimes x^{n-j} = \sum_{j=0}^{n}\frac{x^j}{j!}\otimes\frac{x^{n-j}}{(n-j)!}$$

(ii) $x\in\mathfrak{g}$ $\quad u^{(n)} = C_{x,n}$

הוכחה: תרגיל

(6) $\{u_i^{(n)}\}_{i\le k}$ סדרות של חזקות מחולקות

עבור $(n_1,\dots,n_k) = N \in \mathbb{Z}_+^k$ $\quad U_N = u_1^{(n_1)}\cdots u_k^{(n_k)}$

נניח $\{U_N\}_{N\in\mathbb{Z}_+^k}$ בת"ל מעל $\mathbb{C}$

$V = \mathrm{Span}_{\mathbb{Z}}\{U_N\}_{N\in\mathbb{Z}_+^k}$. ($V$ קו-אלגברה) $\left(D = \mathrm{Hom}_{\mathbb{Z}}(V,\mathbb{Z})\right.$ אלגברה קומוטטיבית$\left.\right)$

נניח $(i\le k)$ $\gamma_i \in D$ כך ש $\gamma_i(U_N) = \begin{cases} 1 & U_N = u_i^{(1)} \\ 0 & \text{אחרת} \end{cases}$

נסמן $\gamma_N := \gamma_1^{n_1} * \dots * \gamma_k^{n_k}$

אזי $\gamma_N(U_M) = \mathbb{1}_{\{N=M\}}$

הוכחה: אינדוקציה ($\mathbb{Z}_+^k = G\omega$) בסיס: נכון ל $\delta_{ij}\in\mathbb{Z}_+^k$ $i\le k$

$$\gamma_{N+M}(e_k) = \gamma_N * \gamma_M(e_k)$$
$$= \underbrace{\varphi_{\mathbb{Z}}}_{\text{כפל ב } \mathbb{Z}} \circ \gamma_N\otimes\gamma_M \circ \Delta(e_k) = \varphi_{\mathbb{Z}}\, \gamma_N\otimes\gamma_M \sum_{L+J=k} e_L\otimes e_J \underset{\text{הנחה}}{=} \mathbb{1}_{\{k=N+M\}}$$

$R=R^+\cup R^-$
$\Pi\subset R$

$\mathfrak g/\mathbb C$ פשוטה למחצה $\mathfrak g = \mathfrak h \oplus \bigoplus_{\alpha\in R} \mathfrak g_\alpha$

(·) $h_\alpha=[e_\alpha,e_{-\alpha}]$ $\quad (e_{-\alpha}=f_\alpha) \quad$ $\dim \mathfrak g_\alpha = 1$

(·) $\alpha(h_\alpha)=2$. $\quad \alpha^\vee = H_\alpha \quad$ $h_\alpha = \frac{2H_\alpha}{(\alpha,\alpha)}$

<u>הגדרה</u>: $\mathfrak g_{\mathbb Z} = \mathrm{Span}_{\mathbb Z}\{\{h_\alpha\}_{\alpha\in R^+},\{e_\alpha\}_{\alpha\in R}\}$ ($\{e_\alpha\}$ כבטענה טכנית 1)

נניח $\Pi\subseteq R$ בסיס. $\Pi=\{\alpha_i\}_{i\in I}$ $\quad R^+=\{\beta_i\}_{i\in r}$

$\mathfrak h \xrightarrow[\text{killing}]{\sim} \mathfrak h^\vee$. $\{\alpha_i\}_{i\in I}$ בסיס ל-R מעל $\mathbb Z$

לכן $\{h_i\}_{i\in I}$ בסיס ל-$\mathrm{Span}_{\mathbb Z}\{h_\alpha\}_{\alpha\in R^+}$

סה"כ: $\{h_i\}_{i\in I}\cup\{e_\alpha\}_{\alpha\in R}$ בסיס חופשי מעל $\mathbb Z$ ל-$\mathfrak g_{\mathbb Z}$

מסקנה טכנית (1) $\mathfrak g_{\mathbb Z}$ אלגברת Lie מעל $\mathbb Z$

מסקנה טכנית (2) $\mathfrak g_{\mathbb Z}$ יציב תחת $\mathrm{ad}\, e_\alpha^n/n!$ לכל $n\in\mathbb Z_+$, $\alpha\in R$

<u>הגדרות</u>: (·) $U(\mathfrak g) \supseteq B := \langle\{e_\alpha^n/n!\}_{n\in\mathbb Z_+,\ \alpha\in R}\rangle_{\mathbb Z}$ (נוצר כאלגברה מעל $\mathbb Z$)

(·) תהי $\mathfrak n$ האלגברת Lie הנוצרת מעל $\mathbb C$ ע"י $\{e_\alpha\}_{\alpha\in R^+}$

$U(\mathfrak n)$ האלגברה האוניברסלית של $\mathfrak n$

(·) עבור $M=(m_1,\dots,m_r)\in\mathbb Z_+^r$ נגדיר $e_M = \frac{e_{\alpha_1}^{m_1}}{m_1!}\cdots\frac{e_{\alpha_r}^{m_r}}{m_r!}$ (קבענו סדר על R^+)

$\{e_M\}_{M\in\mathbb Z_+^r}$ בסיס Poincare-Birkhoff-Witt של $U(\mathfrak n)$

(·) תהי $E\subseteq U(\mathfrak g)$ תת האלגברה הנוצרת מעל $\mathbb Z$

ע"י האיברים $\{e_\alpha^n/n!\}_{n\in\mathbb Z_+,\ \alpha\in R^+}$

טענה 1: $\{e_M\}_{M\in\mathbb{Z}_+^k}$ בסיס חופשי מעל $\mathbb{Z}$ ל E

הוכחה: נגדיר $E_1=\text{span}_{\mathbb{Z}}\{e_M\}$. ברור כי מהגדרה $E_1\subseteq E$

יהי $\alpha_i\in R^+$ $n\in\mathbb{Z}_+$ $\frac{e_{\alpha_i}^n}{n!}=e_{(0,\dots,\underset{\text{מקום } i}{n},\dots,0)}$

לכן היוצרים של E ב E_1 ומספיק להוכיח כי E_1 סגור לכפל.

לכל $j\le k$ קיים $s_j\in Hom_{\mathbb{C}}(\mathfrak{g},\mathbb{C})$ כך ש

(1) $s_j(e_\alpha)=0$ לכל $\alpha\in R$

(2) $s_j(h_{\alpha_j})=1$

(3) לכל $x\in\mathfrak{g}_{\mathbb{Z}}$ $s_j(x)\in\mathbb{Z}$

ניתן להגדיר כזה עבור $i\le k$ כך ש $\alpha_i\in\Pi$

כמו כן לכל $\alpha_j\in R^+$ קיימת $\Pi_j\subseteq R$ בסיס המקיים $\alpha_j\in\Pi_j$

ובעת ניתן להגדיר את s_j על היוצרים של $\mathfrak{g}$

יהי $\rho:\mathfrak{n}\to End(\mathfrak{g})$ הצגת ה adjoint

אז $\rho:U(\mathfrak{n})\to End(\mathfrak{g})$ כלומר $\mathfrak{g}$ הוא $U(\mathfrak{n})$-מודול

נגדיר $U(\mathfrak{n})'=Hom_{\mathbb{C}}(U(\mathfrak{n}),\mathbb{C})$. עבור $j\le k$ נגדיר $\phi_j\in U(\mathfrak{n})'$

$$\phi_j(u)=s_j(u\cdot e_{-\alpha_j})$$

תכונות: $s_j(h_{\alpha_j})=\phi_j(e_{\underbrace{(0,\dots,1,\dots,0)}_{\delta_{jl}}})=1$

עבור $M\neq\delta_{jl}$ $\phi_j(e_M)=0$

לפי טענה טכנית 2 ($\mathfrak{g}_{\mathbb{Z}}$ יציב תחת $ad(\frac{e_\alpha^n}{n!})$) ותכונה (3) של s_j)

מתקיים כי $\phi_j|_E:E\to\mathbb{Z}$ (מקבל ערכים ב $\mathbb{Z}$)

עבור $N\in\mathbb{Z}_+^k$ $\phi_N=\phi_1^{n_1}*\dots*\phi_k^{n_k}$

כאשר עבור $f,g\in U(\mathfrak{n})'$ $f*g=\varphi_{\mathbb{C}}\circ f\otimes g\circ\Delta_{U(\mathfrak{n})}$

מטענה טכנית (6) $\phi_N(e_M)=\mathbb{1}_{\{N=M\}}$

המשך הוכחת טענה 1:

כעת נניח בשלילה כי E_1 אינו סגור **לכפל**.

אזי קיימים $N,M\in\mathbb{Z}_+^2$ $e_N e_M \notin E_1$

(אם אינו סגור לכפל אז אינו סגור לכפל של איברי בסיס)

מעל $\mathbb{C}$ ניתן לכתוב $e_N e_M = \sum_{p\in\mathbb{Z}_+^2} c_p e_p$

$e_N e_M \notin E_1$ לכן קיים $c_p\notin\mathbb{Z}$. תהי L מינימלי בסדר הלקסיקוגרפי כך ש $c_L\notin\mathbb{Z}$

נפעיל את ϕ_L על המשוואה ונקבל כי

$c_L=\phi_L(e_N e_M)\notin\mathbb{Z}$ סתירה לכך ש $e_N e_M\in E$

ו ϕ_L נותנת ערכים שלמים על E.

(ס) נשים לב כי בחרנו סדר שרירותי על R^+
(חשיבות: הישרנו בין תכונות הקשורות בסדר ואלו שלא)

<u>הגדרה</u>: עבור $K\in\mathbb{Z}_+^l$ נגדיר $h_K = C_{h_1,k_1}\cdot\ldots\cdot C_{h_l,k_l}$

כאשר $C_{x,n}=\binom{x}{n}$

$\{h_K\}_{K\in\mathbb{Z}_+^l}$ בסיס מעל $\mathbb{C}$ ל $U(\mathfrak{h})$ (PBW)

מטענה לכנית 5(ii) $\mathrm{Span}_{\mathbb{Z}}\{h_K\}$ יוצר אלגברת Hopf מעל $\mathbb{Z}$

כלומר $\Delta(\mathrm{Span}_{\mathbb{Z}}\{h_K\})\subseteq \mathrm{Span}_{\mathbb{Z}}\{h_K\}\otimes\mathrm{Span}_{\mathbb{Z}}\{h_K\}$

כמו כן (Appendix II) לכל $k\in\mathbb{Z}_+$ $m_i\in\mathbb{Z}$

$C_{h_i-m_i,k}\in \mathrm{Span}_{\mathbb{Z}}\{h_K\}$

(ס) <u>הגדרה</u> תהי $\mathcal{N}_-$ האלגברת Lie הנוצרת מעל $\mathbb{C}$

ע"י $\{e_\alpha\}_{\alpha\in R^-}$.

$R^-=\{\beta_1,\ldots,\beta_t\}$ $f_M = \frac{e_{\beta_1}^{m_1}}{m_1!}\cdots\frac{e_{\beta_t}^{m_t}}{m_t!}$. $\{f_M\}$ בסיס

חופשי מעל $\mathbb{Z}$ ל E_- כאשר $E_-=\langle\{e_\alpha^n/n!\}_{\alpha\in R^-,\, n\in\mathbb{Z}_+}\rangle_{\mathbb{Z}}$

הגדרה: $Q\subseteq R$ תיקרא סגורה אם לכל $\alpha,\beta\in Q$

$$\alpha+\beta\in R \longrightarrow \alpha+\beta\in Q$$

טענה 2: תהי $Q\subseteq R$ סגורה כך ש- $Q\cap -Q=\emptyset$, $Q=\{\beta_i\}_{i\le k}$

נסמן $E_Q=\langle \{e_\beta^n/n! \mid \beta\in Q,\ n\in\mathbb{Z}_+\}\rangle_{\mathbb{Z}}$ האלגברה הנוצרת מעל $\mathbb{Z}$

אזי $\{q_M\}_{M\in\mathbb{Z}_+^k}$ בסיס חופשי מעל $\mathbb{Z}$ ל- E_Q

כאשר $q_M= e_{\beta_1}^{m_1}/m_1! \cdots e_{\beta_k}^{m_k}/m_k!$

הוכחה: נגדיר $span_{\mathbb{C}}\{e_\beta\}_{\beta\in Q}=\mathfrak{n}_Q$

מהנחות על Q (סגורה, $Q\cap -Q=\emptyset$) $\mathfrak{n}_Q\le\mathfrak{g}$ תת אלגברת Lie

$E_Q\subseteq U(\mathfrak{n}_Q)$. $\{q_M\}$ בסיס ל- $U(\mathfrak{n}_Q)$ מעל $\mathbb{C}$.

עבור $i\le k$ $u\in E_Q$ נגדיר

$$\phi_i(u)=S_{\beta_i}(u\cdot e_{-\beta_i})$$

מסיימים כמו בטענה 1

טענה 3: יהיו $\alpha,\beta\in R$ בת"ל. $m,n\in\mathbb{Z}_+$ $Q=(\mathbb{Z}_+\alpha+\mathbb{Z}_+\beta)\cap R$

אזי $e_\alpha^n/n!\cdot e_\beta^m/m! = e_\beta^m/m!\cdot e_\alpha^n/n! + \sum_{|M|<n+m} r_M q_M$ עבור $r_M\in\mathbb{Z}$

הוכחה: נגדיר $u:= e_\alpha^n/n!\, e_\beta^m/m! - e_\beta^m/m!\, e_\alpha^n/n!$

$$0=\bar{u}\in U^{n+m}(E_Q)/U^{n+m-1}(E_Q) \qquad \text{(P-B-W)}$$

מטענה 2 $r_M\in\mathbb{Z}$

מסקנה מטענה 3: $Q\subseteq R$ סגורה $Q\cap -Q=\emptyset$

נניח $\{\beta_i\}_{i\le k}$ $\{\alpha_i\}_{i\le k}$ שתי מניות של Q $\left(\{q_N^\alpha\}\{q_N^\beta\}\right)$ (המסמנים המתאימים)

עבור $v\in E_Q$ $v= c\cdot\prod_{i\le n}\beta_{m_i}^{n_i}$ ($c\in\mathbb{C}^\times$) נגדיר $l(v)=\sum n_i$ הדרגה של v

אזי לכל $M\in\mathbb{Z}_+^k$ קיים $M'\in\mathbb{Z}_+^k$ כך ש-

(1) $|M'|=|M|$

(2) $q_M^\alpha = q_{M'}^\beta + \sum_{|N|<|M|} r_M\, q_N^\beta$

שמחה ברקאי Lie Algebras חלק I ⑤

<u>משפט:</u> $\{f_N h_k e_M\}_{\substack{N,M\in\mathbb{Z}_+^t \\ k\in\mathbb{Z}_+^l}}$ בסיס חופשי מעל $\mathbb{Z}$ של B

<u>הוכחה:</u> $\{f_N h_k e_M\}$ בסיס P-B-W מעל $\mathbb{C}$ של B

נגדיר $U_\mathbb{Z} = span_\mathbb{Z}\{f_N h_k e_M\}$ (קבענו סדר על R^-, R^+)

<u>שלב I:</u> נראה כי $U_\mathbb{Z}\subseteq B$.

$\{f_N\},\{e_M\}\subseteq B$ לכן מספיק להראות כי לכל i ולכל $n\in\mathbb{Z}_+$

$C_{h_i,n}\in B$

הוכחה באינדוקציה על n: $n=0$ $C_{h_i,n}=1\in B$

נניח כי לכל $k<n$ $C_{h_i,k}\in B$

לפי טענה טכנית (4) $\frac{e^n}{n!}\frac{f^n}{n!} = C_{h,n} + \sum_{k=0}^{n-1}\frac{f^{n-k}}{(n-k)!}C_{h-2n+2k,k}\frac{e^{n-k}}{(n-k)!}$

הנחה + Appendix II $\Rightarrow$ המחובר השני $\sum_{k=0}^{n-1}(\ -\ )$ ב-B

$\Rightarrow$ $C_{h,n}\in B$ $\Rightarrow$ $U_\mathbb{Z}\subseteq B$

<u>שלב II:</u> נראה כי $U_\mathbb{Z}\cdot U_\mathbb{Z}\subseteq U_\mathbb{Z}$. (יספיק כי היוצרים של B ב-$U_\mathbb{Z}$)

(·) $U_\mathbb{Z}\cdot E\subseteq U_\mathbb{Z}$ מטענה 1

(·) $U_\mathbb{Z}\cdot C_{h,n}\subseteq U_\mathbb{Z}$ מטענה טכנית (3)

לכן נותר להראות כי $U_\mathbb{Z}\cdot E_-\subseteq U_\mathbb{Z}$

(·) תהי $\{\alpha_i\}_{1\le i\le l}$ מניה כלשהו של R. $v = c\prod e_{\alpha_i}^{n_i}$ עבור $c\in\mathbb{C}$ $l(v)=\sum n_i$

תהי $u\in U_\mathbb{Z}$ $v\in E_-$ נוכיח באינדוקציה על $l(u\cdot v)$

כי $u\cdot v\in U_\mathbb{Z}$

(·) מספיק להוכיח עבור $u=e_M$ $M\in\mathbb{Z}_+^t$ (כי $f_N h_k f_M h_L\subseteq U_\mathbb{Z}$ מטענה טכנית (3))

(·) מספיק להוכיח עבור $v=f_N$

בסיס האינדוקציה $|N|+|M|=0$ $\Rightarrow$ $e_M=1$ $f_N=1$
ואין מה להוכיח

צעד האינדוקציה: יהיו $M,N\in\mathbb{Z}_+^k$ נניח כי לכל $M',N'\in\mathbb{Z}_+^k$

$$e_{M'}f_{N'}\in U_{\mathbb{Z}} \longleftarrow |M'|+|N'|<|M|+|N|$$

הטענה נובעת כעת מטענה טכנית (4) + מסקנה מטענה (3). וכרגע:

(0) נניח קודם כי $f_N=f_\alpha^n/n!=f^n/n!$ עבור $\alpha\in R^-$. נסדר $R^+=(\tilde\alpha_1,\dots,\tilde\alpha_{k-1},-\alpha)$

$\tilde e_{M'}=e_{\tilde\alpha_1}^{m_1'}/m_1'!\cdots e_{\tilde\alpha_{k-1}}^{m_{k-1}'}/m_{k-1}'!\cdot e_{-\alpha}^{m_k'}/m_k'!$. ממסקנה לטענה 3 נוכל לכתוב $e_M=\tilde e_{M'}+\sum_{|N|<|M|}r_N\tilde e_N$, $|M'|=|M|$

$$e_M f^n/n! = \tilde e_{M'}f^n/n! + \underbrace{\sum_{|N|<|M|}r_N\tilde e_N f^n/n!}_{\text{ב-}U_{\mathbb{Z}}\text{ מהנחת האינדוקציה}}$$

נגדיר $S=\mathbb{Z}_+^{k-1}\times\{0\}$. מטענה טכנית (4) נוכל להניח כי $M'\in S$

(הדרכה איך נוצרת משימוש בטענה טכנית (4))

$$i=\max\{i\mid m_i'\neq 0\} \qquad \tilde M=(m_1',\dots,m_{i-1}',0,\dots,0)$$

$$\tilde e_{M'}f^n/n! = \tilde e_{\tilde M}\, e_{\tilde\alpha_i}^{m_i'}/m_i'!\; f^n/n! \underset{\substack{\text{טענה 3}\\ T=\mathbb{Z}\alpha+\mathbb{Z}_+\tilde\alpha_i}}{=} \tilde e_{\tilde M}\, f^n/n!\; e_{\tilde\alpha_i}^{m_i'}/m_i'! + \tilde e_{\tilde M}\Big(\sum_{|N|<n+m_i} r_N t_N\Big)$$

ובכך נוכל להשתמש בהנחת האינדוקציה על שני המחוברים

(0) ממסקנה מטענה (3), טענה טכנית (4)

מתקיים $e_M f^n/n! = \sum_{|N|\le m+n} r_N w_N f^n/n!\, e_N$ $w_N\in U(T_I)$, $r_N\in\mathbb{Z}$

כלומר [illegible] סלינו בדרך

זה מוכיח את הטענה עבור $v\in E_-$ איבר כללי.

סה"כ $U_{\mathbb{Z}}\cdot U_{\mathbb{Z}}\subseteq U_{\mathbb{Z}}$

$\Leftarrow$ $B\subseteq U_{\mathbb{Z}}$ $\boxed{\text{מ.ש.ל}}$

תהי (ρ,V) הצגה סופית של $\mathfrak{g}$

$\mathfrak{h}$ פועלת אלכסונית על V

$$V=\bigoplus_{\lambda\in\mathfrak{h}^\vee} V_\lambda$$

אוסף המשקלות של V (יסומן $\Delta(V)$) $=\{\lambda\in\mathfrak{h}^\vee \mid V_\lambda\neq\{0\}\}$

(·) לכל $\lambda\in\Delta(V)$ $h\in\mathfrak{h}$ $\lambda(h)\in\mathbb{Z}$

(·) $\mathfrak{g}_\alpha(V_\lambda)\subseteq V_{\lambda+\alpha}$ $(\alpha\in R)$

$\Pi\subseteq R$ בסיס (מגדיר R^+,R^-)

נגדיר $Bor(\Pi)=\mathfrak{h}\oplus\bigoplus_{\alpha\in R^+}\mathfrak{g}_\alpha$ $N(\Pi)=\bigoplus_{\alpha\in R^+}\mathfrak{g}_\alpha$

(·) $N(\Pi), Bor(\Pi)\leq\mathfrak{g}$ תתי אלגבראות Lie

$$[Bor(\Pi),Bor(\Pi)]=N(\Pi)$$

$N(\Pi)$ נילפוטנטי $\Leftarrow$ $Bor(\Pi)$ פתירה

לכן ממשפט Lie קיים $\lambda\in\Delta(V)$ $0\neq v^+\in V_\lambda$ כך שלכל $\alpha\in R^+$ $g_\alpha v^+=0$.

λ נקרא המשקל המורם (Highest weight)

v^+ נקרא וקטור מקסימלי או וקטור ממשקל מורם

<u>טענה</u>: $V=\mathfrak{g}v^+$ $R^+=\{\alpha_i\}_{i\le r}$ $\Pi=\{\alpha_i\}_{i\le\ell}$ $v^+\in V_\lambda$

(א) $V=\mathrm{span}_{\mathbb{C}}\{f_M\cdot v^+\}_{M\in\mathbb{Z}_+^r}$

(ב) המשקלות של V הם מהצורה $\mu=\lambda-\sum_{i\le\ell}k_i\alpha_i$

(ג) לכל $\mu\in\mathfrak{h}^\vee$ $\dim V_\mu<\infty$ וכן $\dim V_\lambda=1$

<u>הוכחה</u>: (א) $\{f_M h_L e_N\}$ בסיס ל $\mathfrak{g}$

$$f_M h_L e_N\cdot v^+=f_M k v^+$$

(ב) ל $f_M v^+$ משקל $\lambda-\sum_{i\le r}m_i\alpha_i$

וניתן להביאו לצורה הרצויה

(ג) לכל $0\neq M\in\mathbb{Z}_+^r$ $\sum m_i\alpha_i\neq0$ $\Leftarrow$ $f_M v^+\notin V_\lambda$

$\Leftarrow$ $\dim V_\lambda=1$

עבור $\lambda-\mu\in R$ "המסלולים" (המכוונים) מ λ ל $\lambda-\mu$ סופיים

כי R סופית

שמחה ברקאי — Lie Algebras — חלק ב (פ)

$V \in U(\mathfrak{g})$-Mod ממימד סופי (הצגה סופית של $\mathfrak{g}$)

משקלות $\Delta(V)$

סריג $V_{\mathbb{Z}} \subseteq V$ ($V_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{C} = V$) יקרא טוב (Admissible)

אם $B(V_{\mathbb{Z}}) \subseteq V_{\mathbb{Z}}$

משפט: (א) נסמן $V_{\mathbb{Z}}^{\mu} = V_{\mathbb{Z}} \cap V^{\mu}$ ($\mu \in \Delta(V)$)

לכל סריג טוב $V_{\mathbb{Z}}$ מתקיים $V_{\mathbb{Z}} = \bigoplus_{\mu \in \Delta(\mu)} V_{\mathbb{Z}}^{\mu}$

(ב) קיים סריג טוב $V_{\mathbb{Z}} \subseteq V$

הוכחה: (א) עבור $\mu \in \Delta(V)$ נגדיר $d(\mu) = (\mu(h_1), \dots, \mu(h_\ell)) \in \mathbb{Z}^\ell$

יהי $\lambda \in \Delta(V)$ קיים $f \in \mathbb{C}[X_1, \dots, X_\ell]$ $f(\mathbb{Z}^\ell) \subseteq \mathbb{Z}$

$f(d(\lambda)) = 1$, $f(d(\mu)) = 0$ לכל $\mu \neq \lambda$ ($\Delta(V)$ סופית)

(טענה 2 Appendix II)

$u_\lambda := f(h_1, \dots, h_\ell)$. $u_\lambda \in U(\mathfrak{h}_{\mathbb{Z}})$ (טענה 1 Appendix II)

[עבור $h_k \in U(\mathfrak{h}_{\mathbb{Z}})$ $h_k(\lambda) = \binom{\lambda(h_1)}{k_1} \cdots \binom{\lambda(h_\ell)}{k_\ell}$ הראינו, זו הפסוקה ש $\mathfrak{h}_{\mathbb{Z}}$ של $U(\mathfrak{h}_{\mathbb{Z}})$]

. $\sum_{\mu \in \Delta(\mu)} u_\mu = Id_V$ (u_μ הטלה לרכיב V^μ)

עבור $w \in V_{\mathbb{Z}}$. $w_\mu = u_\mu \cdot w \in V_{\mathbb{Z}}$ (סגירות תחת B) $w = \sum_{\mu \in \Delta(V)} w_\mu$

לכן $V_{\mathbb{Z}} = \bigoplus_{\mu \in \Delta(V)} V_{\mathbb{Z}}^{\mu}$ (ראינו כי ההטלות הם איברים ב B)

(ב) $\mathfrak{g}$ פשוטה למחצה לכן כל הצגה סופית היא

סכום של הצגות אי פריקות.

לכן ניתן להניח V אי פריקה.

$v^+ \in V$ וקטור מירבי, ממשקל מירבי λ

נגדיר $V_{\mathbb{Z}} = Bv^+$. $Bv^+ = f_M \mathbb{Z} v^+ \Leftarrow Bv^+ \cap V^\lambda \subseteq \mathbb{Z} v^+$

[הסבר: $\{f_M h_L e_N\}$ בסיס של B $\underbrace{\prod_{i \le \ell} \binom{\lambda(h_i)}{k_i}}_{\mathbb{Z}} v^+ = h_k v^+$]

לכל $|M| = \sum_{i \le t} m_i > 0$ $f_M v^+ = 0$ (כי יש מספר סופי של שורשים)

$\Leftarrow$ $V_{\mathbb{Z}}$ נ.ס. $V_{\mathbb{Z}} = Bv^+ \supseteq BBv^+ = B(V_{\mathbb{Z}})$

<u>המשך:</u> נותר להראות כי $V_{\mathbb{Z}}$ סריג

נניח $c_1,\dots,c_k\in\mathbb{Q}$ בלתי תלויים לינארית מעל $\mathbb{Z}$

$v_1,\dots,v_k\in V_{\mathbb{Z}}$

צריך להראות כי אם $\sum c_i v_i=0$ אז לכל $i\le k$ $v_i=0$.

מספיק לבדוק עבור $v_1,\dots,v_k\in V_{\mathbb{Z}}^{\mu}$ $\left(V_{\mathbb{Z}}=\oplus V_{\mathbb{Z}}^{\mu}\right)$

נניח $\sum_{i\le k} c_i v_i=0$ $v_1\neq 0$ ($\{c_i\}$ בת"ל מעל $\mathbb{Z}$. $\{v_i\}\subseteq V_{\mathbb{Z}}^{\mu}$)

(ההצגה א' פריקה לכן) קיים $p\in E=\left\langle\left\{e_\alpha^n/n! \;\middle|\; \begin{smallmatrix} n\in\mathbb{Z}^+\\ \alpha\in R^+\end{smallmatrix}\right\}\right\rangle$ ממשקל $\mu-\lambda$ כך ש $pv_1\neq 0$

לכל $i\le k$ $pv_i\in V^{\lambda}$ לכן $pv_i\in Bv^+\cap V^{\lambda}\underset{\text{עמוד קודם}}{=}\mathbb{Z}v^+$

נוכל לסמן $pv_i=m_i v^+$ $m_i\in\mathbb{Z}$.

$pv_1\neq 0 \Leftarrow m_1\neq 0$

$$0=p(0)=p\left(\sum_{i\le k} c_i v_i\right)=\left(\sum_{i\le k} c_i m_i\right)v$$

$\Leftarrow$ $\sum_{i\le k} c_i m_i=0$. $m_1\neq 0$ ולכן קיבלנו תלות לינארית

של $\{c_i\}$ מעל $\mathbb{Z}$, בסתירה להנחה

סה"כ $Bv^+=V_{\mathbb{Z}}$ סריג טוב

$\boxed{\text{//}}$

מסקנות: (-) $[e_\alpha,e_\beta]=\pm r\, e_{\alpha+\beta}$ $r=\min_n\{(\mathrm{ad}\, e_{-\alpha})^n e_\beta=0\}$

(·) לכל $\alpha\in R$ $n\in\mathbb{Z}_+$ $(\mathrm{ad}\, e_\alpha^n/n!)\,\mathfrak{g}_\mathbb{Z}\subseteq\mathfrak{g}_\mathbb{Z}$

הגדרה: $\alpha,\beta\in R$ יהיו $r,q\in\mathbb{Z}_+$ מקסימליים כך ש-
$\beta-r\alpha,\ \beta+q\alpha\in R$. $\beta-r\alpha,\dots,\beta+(q-1)\alpha,\beta+q\alpha$ נקראו השרשרת
של α דרך β.

למה 1: R מערכת שורשים. $\alpha,\beta\in R$ $\|\alpha\|\le\|\beta\|$

אם $(\alpha,\beta)>0$ אז $\alpha-\beta\in R$

($\Leftarrow$ $(\alpha,\beta)<0$ $\longrightarrow$ $\alpha+\beta\in R$)

הוכחה: $(\alpha,\beta)>0 \longleftrightarrow \langle\alpha,\beta\rangle>0 = \frac{2(\alpha,\beta)}{(\beta,\beta)}$

$$\langle\alpha,\beta\rangle=1 \Leftarrow \begin{cases} \|\alpha\|\le\|\beta\| \Rightarrow \langle\alpha,\beta\rangle\in\{-1,0,1\} \\ (\alpha,\beta)>0 \Rightarrow \langle\alpha,\beta\rangle>0 \end{cases}$$

$$R\ni s_\beta(\alpha)=\alpha-\langle\alpha,\beta\rangle\beta=\alpha-\beta$$

למה 2: $\beta-r\alpha,\dots,\beta+q\alpha$ השרשרת של α דרך β

אז לכל $-r\le n\le q$ $\beta+n\alpha\in R$

הוכחה: אחרת קיימים $p<s$ $\beta+p\alpha\in R$ $\beta+(p+1)\alpha\notin R$

$\beta+s\alpha\in R$ $\beta+(s-1)\alpha\notin R$

מלמה 1 $(\alpha,\beta+p\alpha)\ge0$ $(\alpha,\beta+s\alpha)\le0$

$\Leftarrow$ $(\alpha,(p-s)\alpha)\ge0$ $=\overset{<0}{(p-s)}\overset{>0}{(\alpha,\alpha)}$ סתירה.

(·) השרשרת של α דרך β s_α אינווריאנטית.

יתר על כן (s_α הופכת סדר) $\beta-\langle\beta,\alpha\rangle\alpha-q\alpha=s_\alpha(\beta+q\alpha)=\beta-r\alpha$

$\Leftarrow r-q=\langle\beta,\alpha\rangle=\beta(h_\alpha)$. . $|\langle\beta,\alpha\rangle|\le3$ כי אורך השרשרת חסום ע"י 4

למה 3: $\alpha,\beta\in R$ בת"ל. $\beta-r\alpha,\dots,\beta+q\alpha$ השרשרת של α דרך β

(א) $|\{\|\beta-n\alpha\| \mid -r\le n\le q\}|\le2$

(ב) אם $\alpha+\beta\in R$ אז $r+1=q\frac{(\alpha+\beta,\alpha+\beta)}{(\beta,\beta)}$

<u>הוכחת למה 3</u>: (א) $Rank((\mathbb{Z}\alpha+\mathbb{Z}\beta)\cap R)=2$

(ב) (ניתן לבדוק באופן ישיר עבור מערכת ש Rank 2)

$$r+1-q\frac{(\alpha+\beta,\alpha+\beta)}{(\beta,\beta)}=q+\langle\beta,\alpha\rangle+1-q\frac{(\alpha+\beta,\alpha+\beta)}{(\beta,\beta)}=\underbrace{(\langle\beta,\alpha\rangle+1)}_{A}\underbrace{\left(1-q\frac{(\alpha,\alpha)}{(\beta,\beta)}\right)}_{B}$$

<u>מקרה I</u>: $(\alpha,\alpha)\geq(\beta,\beta) \Rightarrow |\langle\alpha,\beta\rangle|\geq|\langle\beta,\alpha\rangle| \Rightarrow \langle\beta,\alpha\rangle\in\{-1,0,1\}$

אם $\langle\beta,\alpha\rangle=-1$ אז $A=0$

אחרת $\langle\beta,\alpha\rangle\geq0 \Rightarrow (\beta,\alpha)\geq0 \Rightarrow (\beta+\alpha,\beta+\alpha)>\max\{(\alpha,\alpha),(\beta,\beta)\}$

מסעיף (א) $(\alpha,\alpha)=(\beta,\beta)$

$(\beta+2\alpha,\beta+2\alpha)>(\beta+\alpha,\beta+\alpha)>(\alpha,\alpha) \Rightarrow \beta+2\alpha\notin R \Rightarrow q=1 \Rightarrow B=0$

<u>מקרה II</u>: $(\beta,\beta)>(\alpha,\alpha)$ $(\alpha+\beta,\alpha+\beta)\in\{(\alpha,\alpha),(\beta,\beta)\} \Rightarrow (\alpha,\beta)<0$

$(\beta-\alpha,\beta-\alpha)>(\beta,\beta)>(\alpha,\alpha) \Rightarrow \beta-\alpha\notin R \Rightarrow r=0$

$|\langle\alpha,\beta\rangle|<|\langle\beta,\alpha\rangle| \Rightarrow \langle\alpha,\beta\rangle\in\{-1,0,1\}$

$(\alpha,\beta)<0 \Rightarrow \langle\alpha,\beta\rangle<0 \Rightarrow \langle\alpha,\beta\rangle=-1$.

מעמוד קודם $\langle\beta,\alpha\rangle=r-q=-q$

$$q=-\langle\beta,\alpha\rangle=\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\beta\rangle}=\frac{(\beta,\beta)}{(\alpha,\alpha)} \Rightarrow B=0$$

<u>למה 4</u>: $\alpha,\beta\in R$ ב.ת.ל. $\beta-r\alpha,\dots,\beta+q\alpha$ המחרוזת של α דרך β

$x_\beta\in\mathfrak{g}_{[\beta]}$ אז $[e_{-\alpha},[e_\alpha,x_\beta]]=q(r+1)x_\beta$

<u>הוכחה</u>: אם $\alpha+\beta\notin R$ אז $[e_\alpha,x_\beta]=0$ וגם $q=0$. כמו כן ניתן להניח כי $x_\beta\neq0$.

$$\bigoplus_{-r\leq n\leq q}\mathfrak{g}_{[\beta+n\alpha]}\in sl_2^\alpha\text{-Mod} \qquad \left(sl_2^\alpha=\langle e_\alpha,\overset{f_\alpha}{\overset{\shortparallel}{e_{-\alpha}}},h_\alpha\rangle\right)$$

ממימד $r+q+1$

המשקל הגבוה ביותר הוא $r+q$ $\left((\beta+q\alpha)(h_\alpha)=\beta(h_\alpha)+2q=r-q+2q=r+q\right)$

$v_{r+q}\neq0$ וקטור ממשקל $r+q$

$c\in F^\times$ $x_\beta=cv_q$. $e_\alpha v_q=((r+q)-q+1)v_{q-1}$, $e_{-\alpha}(v_{q-1})=qv_q$

$\Rightarrow e_{-\alpha}(e_\alpha v_q)=(r+1)qv_q \Rightarrow [e_{-\alpha},[e_\alpha,x_\beta]]=e_{-\alpha}(e_\alpha x_\beta)=(r+1)qx_\beta$

טענה 1: ניתן לבחור $e_\alpha \in \mathfrak{g}[\alpha]$ לכל $\alpha \in R$

כך שיתקיימו התנאים הבאים

(1) $[e_\alpha, e_{-\alpha}] = h_\alpha$ לכל $\alpha \in R$

(2) $\alpha, \beta, \alpha+\beta \in R$ $\quad [e_\alpha, e_\beta] = C_{\alpha,\beta} e_{\alpha+\beta}$

ומתקיים $-C_{\alpha,\beta} = C_{-\alpha,-\beta}$

(3) $C_{\alpha,\beta}^2 = (r+1)^2$ כאשר $\beta - r\alpha, \dots, \beta + q\alpha$

השרשרת של α דרך β

הוכחה: (1) קיים $\sigma \in Aut(\mathfrak{g})$ כך ש $\sigma(\mathfrak{g}[\alpha]) = \mathfrak{g}[-\alpha]$

$\sigma|_{\mathfrak{h}} = -Id_{\mathfrak{h}}$

לכל $x_\alpha \in \mathfrak{g}[\alpha]$ נסמן $x_{-\alpha} := \sigma(x_\alpha) \in \mathfrak{g}[-\alpha]$

$K(\mathfrak{g}[\alpha], \mathfrak{g}[-\alpha]) \neq 0$

לכן $K(x_\alpha, x_{-\alpha}) = a \in \mathbb{C}$ $\quad$ ($\dim_{\mathbb{C}} \mathfrak{g}[\alpha] = 1$ כי)

נבחר $c = \left(\frac{2}{(\alpha,\alpha)} \cdot \frac{1}{a}\right)^{\frac{1}{2}} \in \mathbb{C}^\times$

$K(cx_\alpha, cx_{-\alpha}) = c^2 a = \frac{2}{(\alpha,\alpha)} \frac{1}{a} \cdot a = \frac{2}{(\alpha,\alpha)}$

$[cx_\alpha, cx_{-\alpha}] = K(cx_\alpha, cx_{-\alpha}) \cdot H_\alpha = \frac{2H_\alpha}{(\alpha,\alpha)} = h_\alpha$

נגדיר $e_\alpha = cx_\alpha$ $\quad e_{-\alpha} = cx_{-\alpha}$

(2) $\alpha, \beta, \alpha+\beta \in R$. $\quad [e_\alpha, e_\beta] = C_{\alpha,\beta} e_{\alpha+\beta}$

($e_{\alpha+\beta}$ הוגדר ב (1))

$-C_{\alpha,\beta} e_{-\alpha-\beta} = \sigma(C_{\alpha,\beta} e_{\alpha+\beta}) = [e_{-\alpha}, e_{-\beta}] = C_{-\alpha,-\beta} e_{-\alpha-\beta}$

$\Leftarrow \quad C_{-\alpha,-\beta} = -C_{\alpha,\beta}$

(3) $\alpha, \beta, \alpha+\beta \in R$ $\Leftarrow$ α, β בת"ל. $\Leftarrow$ H_α, H_β בת"ל.

$H_{\alpha+\beta} = H_\alpha + H_\beta$

$\mathfrak{h} \xrightarrow{\tilde{K}} \mathfrak{h}^\vee$, $\quad H_\alpha \mapsto \alpha$

$[[e_\alpha, e_\beta], -[e_{-\alpha}, e_{-\beta}]] = [C_{\alpha\beta} e_{\alpha+\beta}, C_{\alpha\beta} e_{-\alpha-\beta}] = C_{\alpha,\beta}^2 \frac{2H_{\alpha+\beta}}{(\alpha+\beta, \alpha+\beta)}$

($\alpha - r'\beta, \dots, \alpha + q'\beta$ השרשרת של β דרך α)

לאחר פתיחת צד שמאל נקבל $q'(r'+1)[e_\alpha, e_{-\alpha}] + q(r+1)[e_\beta, e_{-\beta}]$

נשווה את המקדמים של H_β ונקבל

$C_{\alpha,\beta}^2 = (r+1) q \frac{(\alpha+\beta, \alpha+\beta)}{(\beta,\beta)}$

מלמה 3(ב) $C_{\alpha,\beta}^2 = (r+1)^2$

כאשר r מקיים $(\mathrm{ad}\, e_{-\alpha})^r e_\beta \neq 0$ $\quad (\mathrm{ad}\, e_{-\alpha})^{r+1} e_\beta = 0$

(d) Appendix I   Lie Algebras   שמחה ברקאי

<u>טענה 2</u>: $\{h_\alpha, e_\alpha\}_{\alpha\in R}$ בבסיס 1

$\mathfrak{g}_{\mathbb{Z}} = \mathrm{span}_{\mathbb{Z}}\{h_\alpha, e_\alpha\}_{\alpha\in R}$. אזי $\mathfrak{g}_{\mathbb{Z}}$ יציב תחת $ad(e_\alpha^n/n!)$

עבור כל $\alpha\in R$ $n\in\mathbb{Z}_+$

<u>הוכחה</u>: $\{\alpha_i\}_{i\le \ell} = \Pi \subseteq R$

(·) $$(ad\, e_\alpha)(h_i) = -\underbrace{\alpha(h_i)}_{\in\mathbb{Z}} e_\alpha \in \mathfrak{g}_{\mathbb{Z}}$$

לכל $n>1$ $$(ad\, e_\alpha^n/n!)\, h_i = 0$$

(·) לכן מתקיים $$(ad(e_\alpha^n/n!))e_\alpha = 0 \in \mathfrak{g}_{\mathbb{Z}}$$

(·) $$(ad\, e_\alpha)\, e_{-\alpha} = h_\alpha \in \mathfrak{g}_{\mathbb{Z}}$$

$$(ad\, e_\alpha^2/2)\, e_{-\alpha} = -\tfrac{1}{2}[h_\alpha, e_\alpha] = -e_\alpha \in \mathfrak{g}_{\mathbb{Z}}$$

לכל $n>2$ $$(ad\, e_\alpha^n/n!)\, e_{-\alpha} = 0$$

(·) $\beta\notin\{\pm\alpha\}$. $\beta - r\alpha, \dots, \beta + q\alpha$ השרשרת של α דרך β

$$(ad\, e_\alpha)\, e_{\beta+n\alpha} = \pm(r+n+1)\, e_{\beta+(n+1)\alpha}$$

$$(ad\, e_\alpha^m/m!)\, e_\beta = \underbrace{\pm\frac{(r+1)\cdots(r+m)}{m!}}_{\pm\binom{r+m}{m}\in\mathbb{Z}}\, e_{\beta+m\alpha} \in \mathfrak{g}_{\mathbb{Z}}$$

$\boxtimes$

$$R = \{ P\in \mathbb{C}[x_1,\dots,x_\ell] \mid P(\mathbb{Z}^\ell)\subseteq \mathbb{Z} \}$$

<u>טענה 1</u>: $$R = \mathrm{Span}_{\mathbb{Z}} \left\{ \binom{x_i}{m_i} \right\}_{\substack{i\le \ell \\ m_i\in\mathbb{Z}_+}}$$

(קל לראות כי $\left\{\binom{x_i}{m_i}\right\}_{\substack{i\le\ell\\ m_i\in\mathbb{Z}_+}}$ חופשית מעל $\mathbb{Z}$)

<u>הוכחה</u>: באינדוקציה על ℓ וחזקת x_ℓ

$f\in R$. אם f קבוע $f\equiv c\in\mathbb{Z}$

$$f = c\binom{x_\ell}{0}$$

אחרת: $f(x_1,\dots,x_\ell)=\sum_{k=0}^{r} f_k(x_1,\dots,x_{\ell-1})\binom{x_\ell}{r}$ כאשר r=דרגת x_ℓ ב-f

$f_k\in \mathbb{C}[x_1,\dots,x_{\ell-1}]$

$$f(x_1,\dots,x_\ell+1)=\sum_{k=0}^{r} f_k(x_1,\dots,x_{\ell-1})\binom{x_\ell+1}{r}$$

$$g(x_1,\dots,x_\ell) = \underbrace{f(x_1,\dots,x_\ell+1)-f(x_1,\dots,x_\ell)}_{R \text{ איבר ב}} = \sum_{k=0}^{r} f_k(x_1,\dots,x_{\ell-1})\left[\binom{x_\ell+1}{r}-\binom{x_\ell}{r}\right]$$

$$= \sum_{k=0}^{r} f_k(x_1,\dots,x_{\ell-1})\binom{x_\ell}{r-1}$$

[כאשר $\binom{x_\ell}{n}=0$ לכל $n\in\mathbb{Z}_{<0}$]

$$\underbrace{g(x_1,\dots,x_\ell+1)-g(x_1,\dots,x_\ell)}_{R \text{ איבר ב}} = \sum_{k=0}^{r} f_k(\;-\;)\binom{x_\ell}{r-2}$$

נמשיך בתהליך זה r פעמים ונקבל

$$h(x_1,\dots,x_\ell+1)-h(x_1,\dots,x_\ell) = f_r\binom{x_\ell}{0} = f_r$$

אז $f_r\in R$

כעת משתמשים בהנחת האינדוקציה על $f - f_r\binom{x_\ell}{r}$ ∎

<u>טענה 2</u>: $d\in\mathbb{Z}^\ell$ $\quad S\subseteq \mathbb{Z}^\ell\setminus\{d\}$ סופית

קיים פולינום $f\in R$ כך ש $f(d)=1$ $\quad f(S)=0$

<u>הוכחה</u>: $d=(d_1,\dots,d_\ell)$ עבור $k\in\mathbb{Z}_+$

$f_k(x_1,\dots,x_\ell) = \prod_{i\le \ell}\binom{x_i-d_i+k}{k}\binom{-x_i+d_i+k}{k}$. לכל $k\in\mathbb{Z}_+$ $\quad f_k(d)=1$

לכל $\Delta\in\mathbb{Z}^\ell$; אם $0<\|d-\Delta\|_\infty<k$ $\quad f_k(\Delta)=0$

S סופית לכן קיים $k>>0$ $\quad f_k(S)=0$