הקדמה

במבניים אלגבריים לומדים שבהינתן שני פולינומים ע"י האלגוריתים של אוקלידס ניתן למצוא את המחלק המשותף המירבי שלהם,

ע"י המחלק המשותף המירבי ניתן למצוא את השורשים המשותפים של שני הפולינומים.

בעבודה זו נרצה להוכיח דרך נוספת לדעת האם לשני פולינומים יש מחלק שורשים משותפים בדרך פשוטה יותר ללא צורך להשתמש באלגריתים של אוקלידס,

אמנם לא נקבל מהם השורשים, אבל בדרך הרבה יותר פשוטה נוכל לדעת האם יש שורשים.

ובנוסף (לא בעבודה זו) בדרך שבה נוכיח בעבודה זו ניתן להרחיב לפולינומים בכמה משתנים, כלומר ניתן לדעת האם לשני פולינומים בכמה משתנים יש שורשים משותפים.

ונציין שהאלגוריתים של אוקלידס טוב רק לפולינמים במשתנה יחיד ולא בכמה משתנים.

תחילה נזכיר בקצרה את הגדרת הדטרמיננטה לפי תמורות, ונגדיר את מטריצת סילבסטר, ובהמשך נגדיר את הרזולטנט ונוכיח את משפט הרזולטנט (פרק 2) שהוא החלק העיקרי של העבודה.

את המשפט עצמו מתי לשני פולינומים יש שורשים משותפים נוכיח בפרק 3, וכן נוכיח עוד כמה תוצאות מעניינות שנובעות מיידי ממשפט הרזולטנט.

פרק 1.

מטריצת סילבסטר

פרק זה הוא פרק קצר שבו נזכיר בקצרה את הגדרת הדטרמיננטה לפי תמורות ומטריצת סילבסטר של שני פולינומים, ובסוף הפרק נגדיר את הרזולטנט.

הגדרות אלו ילוו אותנו לאורך כל העבודה פעמים במשפטים עצמם ופעמים בהוכחות של המשפטים.

הגדרה 1.1 הגדרת הדטרמיננטה לפי תמורות[1]

תהי $A=\left(\alpha_{i,j}\right)$ מטריצה מגודל $n\times n$

$$\det\left(A\right)=\sum_{\sigma\in S_n}\operatorname{sgn}\left(\sigma\right)\sigma_{1,\sigma(1)}\sigma_{2,\sigma(2)}\cdots\sigma_{n,\sigma(n)}\,.$$

הסכום הוא על $n!$ התמורות σ של המספרים $\{1,2,\dots,n\}$, כאשר אם עבור השורה ה i ניקח את האיבר בעמודה ה j נקבל את "ההזזה" $i\to j$, ו- $\operatorname{sgn}\left(\sigma\right)=1$ אם התמורה זוגית, ו $\operatorname{sgn}\left(\sigma\right)=-1$ אם התמורה אי-זוגית.

נעבור לדוגמא:

תהי מטריצה

$$A=\begin{pmatrix}2&3&1\\4&2&3\\1&5&3\end{pmatrix}\,.$$

נחשב את $\det\left(A\right)$ לפי הגדרה 1.1.

נבחר לדוגמא את תמורת הזהות $S_3\ni\sigma=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

השורה הראשונה מייצגת את השורה במטריצה והשורה השנייה בתמורה מייצגת את העמודה במטריצה, ולכן במקרה זה נבחר מהשורה הראשונה את האיבר מהעמודה הראשונה, מהשורה השניה את האיבר בעמודה השניה, וכן הלאה.

תמורת הזהות היא זוגית ולכן $\operatorname{sgn}\left(\sigma\right)=1$, ובסה"כ מתמורת הזהות נקבל את המכפלה $2\cdot2\cdot3$.

נבחר תמורה נוספת $S_3\ni\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, במקרה זה מהשורה הראשונה נבחר את האיבר מהעמודה השלישית, מהשורה השניה את האיבר מהעמודה הראשונה, ומהשורה השלישית את האיבר בעמודה השניה.

ע"י פירוק לחילופים נקבל את $\operatorname{sgn}\left(\sigma\right)$,

$$\left(132\right)=\left(13\right)\left(21\right)\,.$$

קבלנו $\operatorname{sgn}\left(\sigma\right)=1$ ולכן בסה"כ מתמורה זו נקבל את המכפלה $1\cdot4\cdot5$.

תמורה נוספת לדוגמא $S_3\ni\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, זהו חילוף ולכן $\operatorname{sgn}\left(\sigma\right)=-1$ ובסה"כ מתמורה זו נקבל את המכפלה $-3\cdot4\cdot3$.

ולאחר חישוב כל התמורות נקבל

$$\begin{aligned}\det\left(A\right)&=\sum_{\sigma\in S_3}\operatorname{sgn}\left(\sigma\right)\sigma_{1,\sigma(1)}\sigma_{2,\sigma(2)}\cdots\sigma_{n,\sigma(n)}\\&=2\cdot2\cdot3-2\cdot3\cdot5-3\cdot4\cdot3+3\cdot3\cdot1-1\cdot2\cdot1+1\cdot4\cdot5\\&=12-30-36+9-2+20=25\,.\end{aligned}$$

הגדרה 1.2 מטריצת סילבסטר

יהיו שני פולינומים $g(x)$, $f(x)$, מעל שדה K.

נסמן $g(x)=\sum_{j=0}^{m}b_jx^j$, $f(x)=\sum_{i=0}^{n}a_ix^i$

$\mathrm{Syl}(f,g)=\mathrm{Syl}_{n,m}(f,g)$ של f,g היא מטריצה מגודל $(n+m)\times(n+m)$ המוגדרת ע"י

$$\mathrm{Syl}(f,g)=\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0\\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0\\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0\\ b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0\\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0\\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix}.$$

ב- m השורות הראשונות יש את המקדמים של f באופן הבא:

בשורה הראשונה מתחילים מהמקום הראשון עם a_n בעמודה שלאחריה a_{n-1} וכן הלאה עד a_0, בפולינום f יש n איברים ולכן בסה"כ יתמלאו n העמודות הראשונות נשארו m עמודות אותן נאכלס עם אפסים,

בשורה השניה נבצע את אותו הדבר עם שינוי קטן a_n יזוז אחד ימינה כלומר נתחיל את האיכלוס של התאים מהעמודה השניה, ואת העמודה הראשונה נאכלס באפס, ובאופן הזה נמלא את שורות המטריצה כשכל פעם מתחילים מהעמודה הבאה, עד השורה ה m שבה יהיו בהתחלה m אפסים ובסוף n איברי f.

באותו האופן נאכלס את n השורות האחרונות עם איברי הפולינום g, בשורה ה $m+1$ את העמודה הראשונה נאכלס עם g_m, את העמודה השניה עם g_{m-1} וכך נמשיך עד העמודה ה m, ואת שאר העמודות נאכלס באפסים, בשורה ה $m+2$ נתחיל בעמודה השניה עם g_m ואת העמודה הראשונה נאכלס באפס, ונמשיך באופן הזה כמו עם f.

נביא הגדרה נוספת כללית יותר.

יהיו f,g פולינומים ממעלה n,m בהתאמה $\mathrm{Syl}_{n,m}(f,g)$ מוגדרת באופן הבא, האיבר במיקום (i,j) שווה ל a_{n+i-j} כאשר $1\le i\le m$ ו- b_{i-j} אם $m+1\le i\le m+n$, $a_i=0$ אם $i>n$ או $i<0$, $b_i=0$ אם $i>m$ או $i<0$.

דוגמא:

נגדיר $f(x)=a_3x^3+a_2x^2+a_1x+a_0$, $g(x)=b_2x^2+b_1x+b_0$.

במקרה זה $n=3$ $m=2$, ולכן

$$\mathrm{Syl}_{2,3}(f,g)=\begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0\\ 0 & a_3 & a_2 & a_1 & a_0\\ b_2 & b_1 & b_0 & 0 & 0\\ 0 & b_2 & b_1 & b_0 & 0\\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix}.$$

הבחנה 1.3

אם אחד הפולינומים f או g, ממעלה 0 אז $\mathrm{Syl}(f,g)$ היא מטריצה משולשת.

הגדרה 1.4 הגדרת הרזולטנט

יהיו שני פולינומים $g(x)$, $f(x)$, מעל שדה F.

נגדיר את הרזולטנט שלהם להיות

יהיו $n,m\in\mathbb{N}$

$R(f,g)=a_0b_0$ אם $n=m=0$,

בכל מקרה אחר

$$R\left(f,g\right)=\det\left(\mathrm{Syl}_{n,m}\left(f,g\right)\right)\ .$$

הערה 1.5

לפי הגדרה 1.4 $R\left(f,g\right)$ נקבע באופן חח"ע לפי f,g.

נרחיב את ההגדרה 1.4 לכל שני פולינומים ממעלה קטנה מ- n,m, עבור f נשלים עד למעלה n עם מקדמים 0 , ובאותו אופן עבור g נשלים עד למעלה m עם מקדמים 0.

ובאופן הזה הגדרה 1.4 נכונה לכל שני פולינומים ממעלה קטנה או שווה ל- n,m.

ביתר פירוט :

אם $\deg\left(\left(f\right)\right)\leq k<m$ נגדיר $\hat{f}\left(x\right)=\sum_{i=0}^{k}a_i\cdot x^i+\sum_{i=k+1}^{n}0\cdot x^i$ כאשר a_i הם המקדמים של הפולינום f, ולכן $f=\hat{f}$.
ובאותו אופן נעשה עם הפולינום g אם $\deg\left(g\right)<m$.

באופן כללי נמשיך להשתמש בסימון $R\left(f,g\right)$, במקרים שנרצה להתייחס למימד בצורה מפורשת נציין זאת ע"י $R_{n,m}\left(f,g\right)$.

הבחנה 1.6

נבחין שבמקרה שגם $\deg\left(f\right)<n$ וגם $\deg\left(g\right)<m$, ב$\mathrm{Syl}\left(f,g\right)$ נקבל עמודת אפסים ולכן $R_{n,m}\left(f,g\right)=0$.

הערה 1.7

עבור שני פולינומים f,g מעל שדה K

נוסיף לשדה F את המשתנים $a_0,\ldots,a_n,b_0,\ldots,b_n$, ונסמן $F=K\left(a_0,\ldots,a_n,b_0,\ldots,b_n\right)$.

אם נסמן $g\left(x\right)=\sum_{j=0}^{m}b_jx^j$ $f\left(x\right)=\sum_{i=0}^{n}a_ix^i$, אז f ו g הם פולינומים מעל F.

ואז$\deg\left(\mathrm{Syl}\left(f,g\right)\right)$ היא בעצמה איבר של F כלומר פולינום מעל השדה K במשתנים $a_0,\ldots,a_n,b_0,\ldots,b_n$.

ולכן נוכל להתייחס $\det\left(\mathrm{Syl}\left(f,g\right)\right)$ כפולינום במשתנים אלו.

מכאן ולהבא כשנזכיר את השדה F כוונתנו ל- F כפי שהיא מוגדרת בהערה 1.7.

דוגמא:

עבור $f\left(x\right)=a_2x^2+a_1x+a_0$ $g\left(x\right)=b_1x+b_0$,

נחשב את הדטרמיננטה של מטריצת סילבסטר

$$\begin{aligned}R\left(f,g\right)&=\det\left(\mathrm{Syl}_{2,1}\left(f,g\right)\right)\\&=\det\begin{pmatrix}a_2&a_1&a_0\\b_1&b_0&0\\0&b_1&b_0\end{pmatrix}=a_0b_1^2+a_2b_0^2-b_0a_1b_1\ .\end{aligned}$$

קיבלנו איבר בשדה F, שהוא פולינום ב 5 משתנים בלתי תלויים a_2,a_1,a_0,b_1b_0 מעל השדה K.

משפט 1.8

יהיו $g\left(x\right)=\sum_{j=0}^{m}b_jx^j$, $f\left(x\right)=\sum_{i=0}^{n}a_ix^i$ פולינומים מעל שדה F.

$R\left(f,g\right)$ הוא פולינום הומוגני עם מקדמים שלמים במקדמים a_i,b_i, כאשר עבור $a_0\ldots a_n$ המעלה היא m, ועבור $b_0\ldots b_m$ המעלה היא n.

הוכחה

הוכחה זו מתבססת על הגדרת הדטרמיננטה לפי תמורות.

נחזור ל $\mathrm{Syl}\left(f,g\right)$, זוהי מטריצה מסדר $n+m\times n+m$, נתבונן באיבר כלשהוא בסכום הנתון בהגדרה 1.1 נבחר $\sigma\in S_{n+m}$, המחובר בסכום מתקבל ע"י כפל בין איברי המטריצה כך שכל שורה וכל עמודה מופיעה בדיוק פעם אחת.

כלומר עבור $\sigma_{i_1,j_1},\sigma_{i_2,j_2}$ אם $i_1\neq i_2$ אז $j_1\neq j_2$ לכל i_k,j_l, $1\leq k,l\leq n+m$, ולכן בסה"כ מספר האיברים במכפלה הינו כמספר השורות (או העמודות) וזה בדיוק $n+m$.

לפי הגדרה 1.2 מ- m השורות הראשונות מקבלים מקדמים של הפולינום $f(x)$, ומ- n השורות האחרונות מקבלים מקדמים מהפולינום $g(x)$, ובסה"כ סכום החזקות של האיבר σ הוא m מאיברי $f(x)$ ו n מאיברי $g(x)$.

כנדרש.

טענה 1.9

יהיו f, g פולינומים מעל שדה F.

$$R_{n,m}(f,g) = (-1)^{nm} R_{m,n}(g,f) \quad (1.1) \ .$$

הוכחה

נפתח בדיון אינטואיטיבי:

ניתן לעבור מ $\mathrm{Syl}(f,g)$ ל $\mathrm{Syl}(g,f)$, ע"י פעולות על שורות המטריצה, ולכן נבדוק מה יהיה המחיר לעבור מ $\mathrm{Syl}(f,g)$ ל $\mathrm{Syl}(g,f)$.

נזכור שהחלפת שורות בין שורות המטריצה מחליפה את הסימן של הדטרמיננטה, ולכן נרצה לבדוק כמה החלפות בין השורות נדרש ע"מ להפוך בין f, g וזה יהיה הסימן המבוקש.

נעבור להוכחה.

ההחלפה בין השורות תיעשה באופן הבא:

את השורה הראשונה נעביר להיות בשורה השניה את השניה לשלישית וכן הלאה עד האחרונה. את האחרונה נעביר להיות השורה הראשונה.

בכתיב תמורות נקבל את המעגל

$$(r_1 r_2 \dots r_m r_{m+1} \dots r_{n+m}) \ .$$

נבצע את המעגל הזה n פעמים. כך נקבל שהשורה הראשונה (של המטריצה המקורית) תיהיה במקום ה $n+1$ "ואז f תיהיה ב m השורות האחרונות", והשורה ה m (של המטריצה מקורית) תיהיה בשורה הראשונה כלומר "g תיהיה ב n השורות הראשונות" (מספר השורות הוא $n+m$).

החתימה של מחזור באורך l הוא $l-1$ (הוכחת טענה זו חורגת ממסגרת המאמר הזה[2]) ולכן כל מחזור כזה הוא באורך $l = n+m-1$.

נבצע n מחזורים כאלו ע"מ להחליף בין f ל g ולכן בסה"כ נקבל שהסימן הוא

$$\left[(-1)^{(m+n-1)}\right]^n = (-1)^{(nm+n^2-n)} = (-1)^{nm} \ .$$

השוויון האחרות מתקיים כיון ש- $n^2 - n = n(n-1)$ תמיד מספר זוגי כי n זוגי או $n-1$ זוגי, ולכן $nm + n^2 - n$ ו mn חולקים את אותה זוגיות.

פרק 2.

הרזולטנט

תחילה נציג כמה מוסכמות לפרק זה.

1. $g(x)=\sum_{j=0}^{m}b_jx^j$ $f(x)=\sum_{i=0}^{n}a_ix^i$ פולינומים מעל שדה F (F השדה שהוגדר בהערה 1.7.

2. ללא הגבלת כלליות ניתן להניח ש F הוא שדה הפיצול של $f\cdot g$, כלומר F מכיל את כל השורשים של f ו- g.

3. $\xi_n \dots \xi_0$ הם השורשים של f, ו $\eta_m \dots \eta_0$ הם השורשים של g.

משפט 2.1 משפט הרזולטנט

יהיו f,g פולינומים מעל שדה F.

אם $m=0$ ו $n>0$, $R(f,g)=a_0^m$.

אם $n=0$ ו $m>0$, $R(f,g)=b_0^n$.

אם $m=n=0$, $R(f,g)=a_0b_0$.

אם $n,m>0$

$$R_{n,m}(f,g)=a_n^mb_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}\left(\xi_i-\eta_j\right) \quad (2.1)$$

דוגמא

$f(x)=x\left(x^2-4\right)=x(x+2)(x-2)=x^3-4x$

$g(x)=(x+1)(x-3)=x^2-2x-3$

נבחין כי השורשים של f הם $0,2,-2$ והשורשים של g הם $-1,3$.

נסמן

$$\xi_1=0,\xi_2=2,\xi_3=-2 \quad \eta_1=-1,\eta_2=3$$

נציב במשוואה (2.1) כאשר $a_n^m=1^2, b_m^n=1^3$.

$$((0-(-1))(0-3))((2-(-1))(2-3))((-2-(-1))(-2-3))=45$$

קבלנו ש-

$$R(f,g)=45$$

נחשב לפי הגדרה 1.1 את $\mathrm{Syl}(f,g)$:

$$R(f,g)=\begin{vmatrix}1&0&-4&0&0\\0&1&0&-4&0\\1&-2&-3&0&0\\0&1&-2&-3&0\\0&0&1&-2&-3\end{vmatrix}$$

נבחין שמהשורה הראשונה תמיד נבחר את העמודה הראשונה או השלישית אחרת המכפלה תתאפס.

ומאותו הטעם מהשורה החמישית נבחר את האיבר החמישי ולכן התמורות יהיו מהצורה

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & & & & 5 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & & & & 5 \end{pmatrix}$$

לאחר שנשלים את כל התמורות נקבל את התמורות הבאות :

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}}_{\operatorname{sgn}(\sigma)=1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}}_{\operatorname{sgn}(\sigma)=-1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}}_{\operatorname{sgn}(\sigma)=1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}}_{\operatorname{sgn}(\sigma)=-1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}}_{\operatorname{sgn}(\sigma)=1} .$$

"את הסימן רשמנו מתחת לתמורה".

לאחר חישוב של המכפלות המתאימות נקבל

$$(-27) - (-36) + (48) - (-36) + (-48) = 45$$

כלומר במקרה זה מתקיים משפט 2.1.

כדי להוכיח את משפט 2.1, נשתמש בצורה שקולה משפט 2.2, ומכיון שכך תחילה נוכיח את משפט 2.2 ולאחר מיכן נפנה להוכחה של משפטים 2.1 ו 2.2.

<u>משפט 2.2</u>

יהיו f, g פולינומים מעל שדה F

I. $R(f,g) = a_n^m \prod_{i=1}^n g(\xi_i)$.

II. $R(f,g) = (-1)^{nm} b_m^n \prod_{j=1}^m f(\eta_j)$.

<u>הוכחת משפט 2.2</u>

טענה זו נובעת כמעט ישירות מהמשפט היסודי של האלגברה.

נציין שלפי המשפט היסודי של האלגברה מעל שדה F ניתן לרשום את f, g כמכפלה של גורמים לינאריים.

<u>הוכחת I.</u>

נרשום את g כמכפלה של גורמים לינארים :

$$g(x) = b_m \prod_{j=1}^m (x - \eta_j) \ .$$

נציב $\xi_n \dots \xi_0$ ב g נקבל

$$g(\xi_i) = b_m \prod_{j=1}^m (\xi_i - \eta_j) \ . \ (*)$$

משרשור השווינות הבא נקבל את השוויון

$$a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (\xi_i - \eta_j) = a_n^m \prod_{i=1}^n b_m \prod_{j=1}^m (\xi_i - \eta_j)$$

$$\text{hence } (*) = \boxed{a_n^m \prod_{i=1}^n g(\xi_i)}.$$

הוכחת II

תחילה נבחין שע"י הוצאת -1 מהביטוי $\left(\eta_j-\xi_i\right)$ נקבל את השוויון

$$a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \left(\xi_i-\eta_j\right) = \left(-1\right)^{nm} b_m^n a_n^m \prod_{j=1}^{m} \prod_{i=1}^{n} \left(\eta_j-\xi_i\right) \ .$$

מכאן נוכל להמשיך כמו בהוכחה של I. נרשום את f כמכפלה של גורמים לינאריים

$$f\left(x\right) = a_n \prod_{i=1}^{n} \left(x-\xi_i\right) \ . \ (**) \ .$$

נציב $\eta_0 \dots \eta_m$

$$f\left(\eta_j\right) = a_n \prod_{i=1}^{n} \left(\eta_j-\xi_i\right) \ .$$

ולכן שוב משרשור השוויונות הבא נקבל

$$\begin{aligned} a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} \left(\xi_i-\eta_j\right) &= \left(-1\right)^{nm} b_m^n a_n^m \prod_{j=1}^{m} \prod_{i=1}^{n} \left(\eta_j-\xi_i\right) \\ &= \left(-1\right)^{nm} b_m^n \prod_{j=1}^{m} a_n \prod_{i=1}^{n} \left(\eta_j-\xi_i\right) \\ \text{hence } (**) &= \boxed{\left(-1\right)^{nm} b_m^n \prod_{j=1}^{m} f\left(\eta_j\right)} . \end{aligned}$$

כנדרש.

נעבור עכשיו להוכחת משפטים 2.1 ו 2.2, תחילה נוכיח שתי טענות עזר שנצטרך להם בהוכחה.

טענה עזר 2.3

יהיו f, g פולינומים ממעלה m, n בהתאמה כך שמתקיים $m \le n$, ויהי h פולינום כך ש $\deg\left(h\right) \le n-m$.

מתקיים

$$R\left(f+hg, g\right) = R\left(f, g\right) \ .$$

באופן סימטרי אם $n \le m$ אז עבור h כך ש $\deg\left(h\right) \le m-n$ מתקיים

$$R\left(f, g+hf\right) = R\left(f, g\right) \ .$$

.

הדרישה ש $\deg\left(h\right) \le n-m$ במקרה הראשון (ובדומה $\deg\left(h\right) \le m-n$) הכרחית, נניח ש- $\deg\left(h\right) > n-m$ ולכן $\deg\left(gh\right) >$ $n-m+m=n$ ולכן גם $\deg\left(f+hg\right) > n$ ואז השוויון לא יוכל להתקיים.

הוכחה

נוכיח באינדוקציה על המעלה של h, נניח ש $k \le n-m$ ונסמן $h = \sum_{l=\rho}^{k} h_\rho x^\rho$.

תחילה נוכיח שהמשפט מתקיים עבור מונום יחיד cx^ρ עם $\rho \in \mathbb{Z}$, ובפרט הוא מתקיים עבור $h_\rho x^\rho$.

נוכל להניח ללא הגבלת כלליות ש $k = n-m$ ע"י הגדרת $h_\rho = 0$ לכל שאר החזקות.

מכיון ש $m<n$, לפי הגדרת מטריצת סילבסטר נקבל

$$\begin{pmatrix} a_n+cb_{n-\rho} & a_{n-1}+cb_{n-\rho-1} & a_{n-2}+cb_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n+h_\rho b_{n-\rho} & a_{n-1}+cb_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1+cb_1 & a_0+cb_0 & 0 \\ 0 & 0 & 0 & \dots & a_2+cb_2 & a_1+cb_1 & a_0+cb_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix} = R_{,}\left(f+\left(cx^\rho\right)g,g\right)$$

הביטוי $n-\rho$ נובע מכך שהכפל cx^ρ מזיז את איברי g ρ מקומות כי $cx^\rho b_j x^j = cb_j x^{j+\rho}$, ולאחר הצבה $i=j+\rho$ נקבל $j=i-\rho$ כלומר המקדם של החזקה ה i הוא $b_{i-\rho}$.

מכך ש $\rho<n-m$, כל אחד מ m השורות הראשונות ב $\mathrm{Syl}\left(f+cx^\rho g,g\right)$ הוא סכום של השורה המתאימה במטריצה $\mathrm{Syl}\left(f,g\right)$ עם אחד השורות מ n השורות האחרונות וקומבינציה לינארית של שורות אחרות.

במילים אחרות ניתן לעבור מ $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(f+cx^\rho g,g\right)$ ע"י פעולות על השורות של המטריצה וקומבינציה לינארית של שורות אחרות. אבל הוספת קומבינציה לינארית של שורות לשורה אחרת במטריצה לא משנה את הדטרמיננטה ולכן:

$$\boxed{R_{,}\left(f+\left(h_\rho x^\rho\right)g,g\right)=R\left(f,g\right)}$$

הנחת האינדוקציה:

נניח שהטענה נכונה עבור פולינום ממעלה $k-1$ ונוכיח עבור פולינום ממעלה k.

צעד האינדוקציה:

$$\begin{aligned} \boxed{R_{,}\left(f+hg,g\right)} &= \det\left(\mathrm{Syl}\left(f+\left(\sum_{l=1}^{k}h_l x^l\right)g,g\right)\right) \\ &= \det\left(\mathrm{Syl}\left(f+\left(\sum_{l=1}^{k-1}h_l x^l\right)g+\left(h_k x^k\right)g,g\right)\right) \\ \text{step induction} &= \det\left(\mathrm{Syl}\left(f+\left(h_k x^k\right)g,g\right)\right) \\ \text{case base} &= \det\left(\mathrm{Syl}\left(f,g\right)\right) \\ &= \boxed{R\left(f,g\right)} \end{aligned}$$

כנדרש.

נשים לב שתוך כדאי שרשור השוויונות קבלנו ש

$$\mathrm{Syl}\left(f+hg,g\right)=\mathrm{Syl}\left(f,g\right) \quad (2.2)$$

בשוויון זה נעשה שימוש בהמשך.

עבור המקרה השני $R_{,}\left(f,g+hf\right)=R\left(f,g\right)$ נקבל את השוויון באותו האופן.

<u>טענת עזר 2.4</u>

I. אם $\deg\left(g\right)\le k\le m$ אז

$$R_{n,m}\left(f,g\right)=a_n^{m-k}R_{n,k}\left(f,g\right)\ .$$

II. אם $\deg(f) \leq k \leq n$ אז

$$R_{n,m}(f,g) = (-1)^{(n-k)m} b_m^{n-k} R_{k,m}(f,g)\ .$$

<u>הוכחה</u>

הוכחה מתבססת על כך שאם המקדם של החזקה הגבוהה ביותר הוא 0 אז התת מטריצת המתקבלת ע"י מחיקת השורה הראשונה והעמודה הראשונה היא מטריצת סילבסטר,

כלומר נניח ש $g_m = 0$. אז

$$\operatorname{Syl}(f,g) = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0 \\ 0 & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ 0 & 0 & b_{m-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix}.$$

נבחין שאם נמחק את השורה הראשונה והעמודה הראשונה נקבל את המטריצה

$$\operatorname{Syl}(f,\hat{g}) = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0 \\ b_{m-1} & b_{m-2} & b_{m-3} & \dots & 0 & 0 & 0 \\ 0 & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix}.$$

כאשר $\hat{g}(x) = \sum_{j=0}^{m-1} b_j x^j$ ומכיון ש $b_m = 0$ אז $\hat{g}(x) = g(x)$, ולכן אם נפתח את הדטרמיננטה $R(f,g)$ לפי העמודה הראשונה נקבל:

$$\boxed{R(f,g)} = a_n R_{n,m}(f,\hat{g}) = \boxed{a_n R_{n,m-1}(f,g)}.$$

בשביל לסיים את ההוכחה נגדיר את g לכל $\deg(g) \leq j \leq m$ להיום עם מקדם 0, ונקבל

$$\begin{aligned} R(f,g) &= a_n R_{n,m-1}(f,g) \\ &= a_n a_n R_{n,m-2}(f,g) \\ &= \left(\underbrace{a_n a_n \dots a_n}_{r\,\text{times}} \right) R_{n,m-r}(f,g) \\ &= a_n^r R_{n,m-r}(f,g) \end{aligned}$$

כאשר $m-r-1$ הוא המקדם הראשון שאינו 0 .

נסמן $k=m-r$ ונקבל $R\left(f,g\right)=a_n^{m-k}R_{n,k}\left(f,g\right)$ כנדרש.

הוכחת .II

לפי 1.9

$$R\left(f,g\right)=\left(-1\right)^{nm}R_{m,n}\left(g,f\right)$$

לפי I והתנאי ש $\deg\left(f\right)<k<n$ נקבל

ולכן

$$\left(-1\right)^{nm}R_{m,n}\left(g,f\right)=\left(-1\right)^{nm}b_m^{n-k}R_{m,k}\left(g,f\right)\ .$$

שוב לפי משוואה 1.9

$$R_{m,k}\left(g,f\right)=\left(-1\right)^{km}R_{k,m}\left(f,g\right)$$

נציב ונקבל

$$\begin{aligned}\left(-1\right)^{nm}R_{m,n}\left(g,f\right)&=\left(-1\right)^{nm}b_m^{n-k}\left(-1\right)^{km}R_{k,m}\left(f,g\right)\\&=\left(-1\right)^{m(n+k)}b_m^{n-k}R_{k,m}\left(f,g\right)\ .\end{aligned}$$

ומכיון של $m+n+k$ ו $n-k$ אותה זוגיות נקבל לאחר כל השוויונות

$$\boxed{R\left(f,g\right)=\left(-1\right)^{m(n-k)}b_m^{n-k}R_{k,m}\left(f,g\right)}$$

כנדרש.

<u>הוכחת משפט 2.1 ו 2.2</u>

נוכיח באינדוקציה על הגודל של המטריצה $n+m$

לפי המוסכמות בראש הפרק והמשפט היסודי של האלגברה נוכל לרשום את f,g כמכפלה של גורמים לינאריים

$$f\left(x\right)=a_n\prod_{i=1}^{n}\left(x-\xi_i\right)\quad g\left(x\right)=b_m\prod_{j=1}^{m}\left(x-\eta_j\right)\ .$$

בסיס האינדוקציה:

עבור $m=n=0$ הטענה מתקיימת.

עבור המקרה $n=0$ ו $m>0$ לפי הבחנה 1.3

$$R\left(f,g\right)=b_0^n\ .$$

ובדומה עבור $m=0$ ו $n>0$

$$R\left(f,g\right)=a_0^m\ .$$

הנחת האינדוקציה:

נניח שמשפט 2.1 נכון לכל ערך מטריצה קטנה מ $n+m$.

מקרה 1:

$0<n=\deg(f)\leq m=\deg(g)$.

קיימים פולינומים q,r כך ש $\deg(r)<\deg(f)$ ומתקיים

$$g=qf+r$$

נבחין כי

$$\deg(g-r)=\deg(qf)$$

ולכן נקבל את השוויונות הבאים

$$\deg(q)=\deg(qf)-\deg(f)=\deg(g-r)-n=m-n\,.$$

קבלנו ש $\deg(q)=m-n$ ולכן נוכל להשתמש בטענת עזר 2.3, נקבל

$$(*)\ \ R(f,g)=R_{,}(f,g-qf)=R_{,}(f,r)\ \ .$$

נחלק שוב למקרים.

מקרה א. $r\neq 0$ נסמן $k=\deg(r)\geq 0$,

מהנחת האינדוקציה וטענת עזר 2.4

$$(**)\ \ R_{n,m}(f,r)\overset{2.5}{=}a_n^{m-k}R_{n,k}(f,r)\overset{\text{base induction}}{=}a_n^{m-k}a_n^k\prod_{i=1}^{n}r(\xi_i)=a_n^m\prod_{i=1}^{n}g(\xi_i)$$

השוויון האחרות נובע מכך ש ξ_i הם שורשים של f ולכן

$$\boxed{g(\xi_i)}=\underbrace{q(\xi_i)\,f(\xi_i)}_{=0}+r(\xi_i)=\boxed{r(\xi_i)}\,.$$

מ $(*)$ ו- $(**)$ נקבל את הנדרש.

מקרה ב. $r=0$,

$$g=fq\,.$$

לפי ההנחה הראשונה של מקרה זה $n>0$ ולכן

$$\text{Syl}(f,r)=\text{Syl}(f,0)="0"\,.$$

"0" בשוויון האחרון הכוונה למטריצת האפס.

ולכן

$$R\left(f,g\right)=0\,.$$

מצד שני כיון ש f מחלק את g אז השורשים של f הם שורשים של g גם כן, ולכן בנוסחה 2.1 קיימים ξ_i ו η_j כך ש $\xi_i=\eta_j$ ולכן המכפלה מתאפסת, ומתקיים השוויון הנדרש.

מקרה 2.

$.m=\deg\left(g\right)<n=\deg\left(f\right)$

כמו במקרה הקודם קיימים q,r כך ש $\deg\left(r\right)<m$ ומתקיים

$$f=gq+r$$

ומאותם נימוקים כמו במקרה הקודם

$$(***)\ R\left(f,g\right)=R_{,}\left(f-gq,g\right)=R_{,}\left(r,g\right)$$

ופה נחלק שוב למקרים

מקרה א.

$r\neq0$ נסמן $k=\deg\left(r\right)\geq0$, ומהנחת האינדוקציה וטענת עזר 2.4 נקבל

$$\begin{aligned}(****)\ \boxed{R_{n,m}\left(r,g\right)} &= \left(-1\right)^{(n-k)m}b_m^{n-k}R_{k,m}\left(r,g\right)\\ \text{base induction}\rightarrow &= \left(\left(-1\right)^{(n-k)m}b_m^{n-k}\right)\left(\left(-1\right)^{km}b_m^{k}\prod_{j=1}^{m}r\left(\eta_j\right)\right)\\ &= \left(-1\right)^{nm}b_m^{n}\prod_{j=1}^{m}r\left(\eta_j\right)\\ &= \boxed{\left(-1\right)^{nm}b_m^{n}\prod_{j=1}^{m}f\left(\eta_j\right)}\end{aligned}$$

ושוב השוויון האחרון נובע מכך ש η_j הם שורשים של g ולכן

$$f\left(\eta_j\right)=\underbrace{g\left(\eta_j\right)q\left(\eta_j\right)}_{=0}+r\left(\eta_j\right)$$

ושוב מ $(***)$ ו $(****)$ נקבל את הנדרש.

מקרה ב.

$r=0$, דומה מאוד לאותו מקרה בהוכחה הקודמת

$$\text{Syl}\left(r,g\right)=\text{Syl}\left(0,g\right)=\text{"0"}\,.$$

ולכן

$$R_{n,m}\left(0,g\right)=0$$

וכמו כן השורשים של g הם שורשים של f ג"כ ולכן המכפלה (2.1) מתאפסת ונקבל את השוויון..

פרק 3.

תוצאות ממשפט הרזולטנט

בפרק זה נמשיך עם המוסכמות שבתחילת פרק 2.

טענה 3.1

יהיו f,g פולינומים מעל שדה F ל f,g יש שורש משותף אם ורק אם $R(f,g)=0$.

הוכחה

לפי משפט 2.1

$$R(f,g)=0 \Longleftrightarrow a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}\left(\xi_i-\eta_j\right)=0\,.$$

וזה מתקיים אם ורק אם קיימים ξ_i ו η_j כך ש $\xi_i=\eta_j$, כלומר אם ורק אם ל f ו- g יש שורש משותף.

טענה 3.2

יהיו f,g פולינומים מעל שדה F, ל f,g יש גורם משותף אם ורק אם $R(f,g)=0$.

הוכחה

צד אחד

$\Longleftarrow$ אם ל f,g יש גורם משותף אז $R(f,g)=0$.

לפי ההנחה ל f,g יש גורם משותף ולכן יש להם שורש משותף וממשפט 2.1 נקבל את הטענה.

$\Longrightarrow$ $R(f,g)=0$ אז ל f ו g יש גורם משותף.

לפי ההנחה ש $R(f,g)=0$ מטענה 3.1 ל f,g יש שורש משותף נסמן α, נוכל נוציא את $x-\alpha$ גורם משותף מ f,g.

וקבלנו את הטענה.

לצורך המשפט הבא נזכיר מהו מימד של מטריצה.

מימד של מטריצה הוא המימד שנפרס ע"י וקטורי השורות או העמודות של המטריצה.

ובמקרה שהשורות תלויות לינארית אז המימד שנפרש ע"י המטריצה קטן מהגודל של המטריצה.

משפט 3.3

יהיו f,g פולינומים בשדה F.

נסמן ב- $h=\mathrm{GCD}(f,g)$ את המחלק המשותף המירבי של f,g .

המעלה של המימד של $\mathrm{Syl}(f,g)$ הוא $n+m-\deg(h)$, ובאופן שקול המעלה של המימד של המשלים של $\mathrm{Syl}(f,g)$ הוא $\deg(h)$.

<u>הערה:</u> מכיון שגודל המימד של מטריצה וגודל המימד של המשלים תלויים אחד בשני, לפעמים נתייחס רק לגודל של אחד מהם כשהכוונה לשניהם.

הוכחה

לפני שנכנסים לגוף ההוכחה נציין:

(1) . החלפה בין שורות המטריצה לא משנה את המימד שנפרש ע"י וקטורי השורות (או העמודות) של המטריצה.

(2) . $\mathrm{Syl}(f,g)$ ל $\mathrm{Syl}(g,f)$ שוות פרט לסדר של השורות, ולכן המימד שנפרש על ידם שווה, ולכן ללא הגבלת כלליות נוכל להניח ש $m\le n$.

(3) . קיימים r,q כך ש $\deg(r)<m$ המקיימים $f=qg+r$, ובהוכחת טענת עזר 2.3 ראינו שאפשר לעבור מ $\mathrm{Syl}(f,g)$ ל $\mathrm{Syl}(f+(-qg),g)=\mathrm{Syl}(r,g)$ ע"י פעולות על שורות המטריצה ולכן המימד שלהם שווה.

רעיון ההוכחה:

נמצא את h לפי האלגוריתים של אוקלידס, ותוך כדי התהליך נקטין את גודל המטריצות ונוכיח שהמימד של המשלים של המטריצות המתקבלות לא משתנה, וכך (כפי שנראה בהוכחה עצמה) נמצא את המימד של המשלים של $\mathrm{Syl}\left(f,g\right)$.

נתחיל...

נחלק את ההוכחה לשלבים כדי להקל על הקורא להבין את ההוכחה.

<u>שלב 1.</u>

קיים q וקיים r כך ש $k=\deg\left(r\right)<m$ ומתקיים

$$f=qg+r\,.$$

$$\deg\left(q\right)=\deg\left(qg\right)-\deg\left(g\right)=n-m$$

מתקיים תנאי משפט 2.3 ולכן לפי (2) המימד של $\mathrm{Syl}_{n,m}\left(f,g\right)$ ו $\mathrm{Syl}_{n,m}\left(r,g\right)$ שווה.

<u>שלב 2</u>

נסמן $r=\sum_{l=0}^{n}\upsilon_{l}x^{l}$, ונתבונן ב $\mathrm{Syl}_{n,m}\left(r,g\right)$, נבחין של- r יש $n-k$ מקדמים שהם אפסים ולכן $\mathrm{Syl}_{n,m}\left(r,g\right)$ מהצורה :

$$\mathrm{Syl}_{n,m}\left(r,g\right)=\begin{pmatrix}0 & \cdots & 0 & \upsilon_{n-k-1} & \upsilon_{n-k-2} & \upsilon_{n-k-3} & \ldots & 0 & 0 & 0\\ 0 & 0 & \cdots & 0 & \upsilon_{n-k-1} & \upsilon_{n-k-2} & \ldots & 0 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & \upsilon_{1} & \upsilon_{0} & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & \upsilon_{2} & \upsilon_{1} & \upsilon_{0}\\ b_{m} & b_{m-1} & b_{m-2} & b_{m} & b_{m-1} & b_{m-2} & \ldots & 0 & 0 & 0\\ 0 & b_{m} & b_{m-1} & 0 & b_{m} & b_{m-1} & \ldots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & b_{1} & b_{0} & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & b_{2} & b_{1} & b_{0}\end{pmatrix}$$

בעמודה הראשונה יש רק איבר יחיד b_m ולכן וקטור זה שייך למימד שנפרש ע"י וקטורי העמודות (או השורות), ולכן מחיקת העמודה הראשונה והשורה ה $m+1$ (השורה שבה יש את האיבר שאינו אפס בעמודה הראשונה) לא תשפיע על המימד של המשלים.

נובע מכך שהמימד של המשלים של $\mathrm{Syl}_{n,m}\left(r,g\right)$ ו $\mathrm{Syl}_{n-1,m}\left(r,g\right)$ שווים, כאשר $\mathrm{Syl}_{n-1,m}\left(r,g\right)$ היא המטריצה שהתקבלה אחרי המחיקה של השורה והעמודה המתאימה.

<u>שלב 3</u>

נחזור שוב על שלב 2 (במקרה ש $n-k>1$), על המטריצה $\mathrm{Syl}_{n-1,m}\left(r,g\right)$, וכך נמשיך עד שנקבל את המטריצה $\mathrm{Syl}_{k,m}\left(r,g\right)$, ולפי ההסבר בשלב 2 המימד של המשלים של המטריצות המתקבלות ע"י מחיקה העמודה והשורה המתאימה לה לא משתנה.

סיכום ביניים :

המימד של המשלים של $\mathrm{Syl}_{n,m}\left(f,g\right)$ ו $\mathrm{Syl}_{n,m}\left(r,g\right)$ ו $\mathrm{Syl}_{k,m}\left(r,g\right)$ שווים, כאשר r הוא השארית של החלוקה של f ב g.

<u>שלב 4</u>

לפי (2) המימד של $\mathrm{Syl}_{k,m}\left(r,g\right)$ ו $\mathrm{Syl}_{m,k}\left(g,r\right)$.

נבצע את שלבים $3-1$ על $\mathrm{Syl}_{m,k}\left(g,r\right)$, עם r_0 $k_0=\deg\left(r_0\right)<k$ ו- q_0 המקיימים $g=rq_0+r_0$.

נמשיך שוב ושוב את שלבים $3-1$(כלומר נבצע את האלגוריתים של אוקלידס) עד שנקבל r_d כך ש- $r_{d-2}=q_{d}r_{d-1}+r_{d}$ כאשר $r_d=0$, ומהאלגוריתים של אוקלידס $r_{d-1}=h$.

<u>שלב 5</u>

משלבים 3 ו 2 המימדים של המשלימים של $\mathrm{Syl}_{n,m}\left(f,g\right),\mathrm{Syl}_{k,m}\left(r,g\right),\mathrm{Syl}_{k_{0},k}\left(r_{0},r\right),\mathrm{Syl}_{k_{1},k_{0}}\left(r_{1},r_{0}\right)\ldots,\mathrm{Syl}_{k_{d-1},l}\left(0,h\right)$ שווים.

ולכן נשאר לבדוק מהו המימד של המשלים של $\mathrm{Syl}_{k_{d-1},l}(0,h)$ לפי הגדרת מטריצת סילבסטר למטריצה $\mathrm{Syl}_{k_{d-1},l}(0,h)$ יש l שורות אפסים ו $d-1$ שורות בת"ל ולכן המימד של המשלים של $\mathrm{Syl}_{k_{d-1},l}(0,h)$ הוא l,

וזה בדיוק $\deg(h)$, ולכן המימד של $\mathrm{Syl}_{n,m}(f,g)$ הוא $n+m-\deg(h)$.

משפט 3.4

יהיו f,g פולינומים מעל שדה F.

יהי $v=(\alpha_{m-1},\dots,\alpha_0,\beta_{n-1},\dots,\beta_0)$ וקטור שורה מדרגה $m+n$.

מתקיים

$$v\mathrm{Syl}_{n,m}(f,g)=0\,.$$

אם ורק אם $pf+qg=0$ כאשר $q=\beta_{n-1}x^{n-1}+\dots+\beta_0x^0$ ו- $p=\alpha_{m-1}x^{m-1}+\dots+\alpha_0x^0$.

הוכחה

נתבונן במכפלה $\gamma=v\mathrm{Syl}_{n,m}(f,g)$

$$\gamma=(\alpha_{m-1},\dots,\alpha_0,\beta_{n-1},\dots,\beta_0)\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0\\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0\\ 0 & 0 & 0 & \dots & a_2 & a_1 & a_0\\ b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0\\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0\\ 0 & 0 & 0 & \dots & b_2 & b_1 & b_0 \end{pmatrix}$$

$$=\left(\underbrace{\alpha_{m-1}a_n+\beta_{n-1}b_m}_{\gamma_1},\underbrace{\alpha_{m-1}a_{n-1}+\alpha_{m-2}a_n+\beta_{n-1}b_{m-1}+\beta_{n-2}b_m}_{\gamma_2},\dots,\underbrace{\alpha_0a_0+\beta_0b_0}_{\gamma_{n+m}}\right)$$

הרכיב ה j של γ מתקבל ע"י המכפלה

$$\gamma_j=(\alpha_{m-1},\dots,\alpha_0,\beta_{n-1},\dots,\beta_0)\begin{pmatrix} a_{n+1-j}\\ \vdots\\ a_{n+m-j}\\ b_{m+1-j}\\ \vdots\\ b_{n+m-j}\end{pmatrix}\,.$$

כאשר $1\le j\le n+m$,

נרשום γ_j כסכום של טורים, הטור הראשון הוא $\sum_{i=1}^{m}\alpha_{m-i}a_{n+i-j}$, ובטור השני האינדקס מתחיל $m+1$ ולכן נסמן $i=i-m$, ונקבל $\sum_{m+1}^{n+m}\beta_{n+m-i}b_{i-j}$

ולכן בסה"כ

$$\gamma_j=\sum_{i=1}^{m}\alpha_{m-i}a_{n+i-j}+\sum_{m+1}^{n+m}\beta_{n+m-i}b_{i-j}\,.$$

נתבונן באינדקסים של המקדמים,

נוכיח ש

$$pf+qg=\sum_j \gamma_j x^j$$

ובזה נסיים את ההוכחה.

נחקור את הביטוי

$$\gamma_j=\sum_{i=1}^{m}\alpha_{m-i}a_{n+i-j}+\sum_{i=m+1}^{n+m}\beta_{n+m-i}b_{i-j}$$

נחשב כל אחד מהמחוברים בנפרד

נבצע החלפת אינדקסים $i=m-k$

$$\sum_{i=1}^{m}\alpha_{m-i}a_{n+i-j}=\sum_{k=0}^{m-1}\alpha_k a_{n+m-k-j}=\sum_{k=0}^{m}\alpha_k a_{n+m-k-j}$$

(השוויון האחרון נובע מכך ש $\alpha_m=0$).

בדומה עבור הביטוי השני נבצע את ההחלפת האינדקסים $i=m+n-k$

$$\sum_{i=m+1}^{n+m}\beta_{n+m-i}b_{i-j}=\sum_{k=0}^{n-1}\beta_k b_{m+n-k-j}=\sum_{k=0}^{n}\beta_k b_{m+n-k-j}$$

(השוויון האחרון נובע מכך ש $\beta_n=0$).

בסה"כ קבלנו כי

$$\gamma_j=\sum_{k=0}^{m}\alpha_k a_{n+m-k-j}+\sum_{k=0}^{n}\beta_k b_{m+n-k-j}$$

נבצע החלפת אינדקסים $j=m+n-l$, $0\le j\le n+m$ ולכן $0\le l\le n+m$

$$\sum_{k=0}^{m}\alpha_k a_{n+m-k-j}+\sum_{k=0}^{n}\beta_k b_{m+n-k-j}=\sum_{k=0}^{m}\alpha_k a_{l-k}+\sum_{k=0}^{n}\beta_k b_{l-k}\,.$$

עבור המקרה $m>l$

מכיון שלכל $k>l$, $\alpha_k=0$ מתקיים

$$\sum_{k=0}^{m}\alpha_k a_{l-k}=\sum_{k=0}^{l}\alpha_k a_{l-k}\,.$$

עבור המקרה $m<l$

מכיון שלכל $k\ge m$, $\alpha_k=0$ מכיון ש $\deg(p)=m-1$ מתקיים

$$\sum_{k=0}^{m}\alpha_k a_{l-k}=\sum_{k=0}^{l}\alpha_k a_{l-k}\,.$$

ובאותו אופן מתקיים

$$\sum_{k=0}^{n}\beta_k b_{l-k}=\sum_{k=0}^{l}\beta_k b_{l-k}$$

קבלנו ש

$$\gamma_j=\sum_{k=0}^{l}\alpha_k a_{l-k}+\sum_{k=0}^{l}\beta_k b_{l-k}\ \ (*)$$

נחשב את המכפלה

$$\begin{aligned}
\boxed{fp+gq} &= \sum_i a_i x^i \sum_\tau \alpha_\tau x^\tau + \sum_i b_i x^i \sum_\tau \beta_\tau x^\tau \\
&= \sum_k \sum_{i+\tau=k} a_i \alpha_\tau x^k + \sum_k \sum_{i+\tau=k} b_i \beta_\tau x^k \\
&= \sum_k \sum_{i=0}^{k} a_i \alpha_{k-i} x^k + \sum_k \sum_{i=0}^{k} b_i \beta_{k-i} x^k \\
&= \sum_k \left(\sum_{i=0}^{k} a_i \alpha_{k-i} + \sum_{i=0}^{k} b_i \beta_{k-i}\right) x^k \\
(*) &= \boxed{\sum_k \gamma_k x^k}
\end{aligned}$$

$(*)$ מתקבל ע"י החלפת האינדקס $k=i$ $l=k$.

[1] . Publications. .Dover Analysis Tensor of .Applications (1957) McConnell

[2]. Prentice-Hall ed.), (3rd Applications with Algebra Abstract in Course First A ,(2006) J. Joseph Rotman,