האוניברסיטה הפתוחה

עבודה סמינריונית בנושא הרזולטנט

אליסף לרר

ת.ז. 308376458

מנחה: אלעד פארן

תוכן העניינים :

הקדמה

הרזולטנט של שני פולינומים הוא ביטוי פולינומי של המקדמים שלהם השווה לאפס אם ורק אם לפולינומים יש שורש משותף בשדה הפיצול שלהם. באופן שקול הרזולטנט מתאפס אם רק אם יש להם גורם משותף.

הרזולטנט מוצאת שימושים נרחבים בתורת המספרים, באופן ישיר או דרך הדסקרמיננטה, שהוא קרוב להיות הרזוטנט של פולינום והנגזרת שלו.

ניתן לחשב את הרזולטנט של שני פולינומים עם מקדמים רציונליים או פולינומיים באופן יעיל אלגורימית. זהו כלי בסיסי במדעי המחשב (algebra computational), וזה כלי מובנה ברוב המערכות האלגברה הממוחשבת. הרזולטנט גם משמש לפירוק אלגברי גלילי (decomposition algebraic cylindrical), לאינטגרציה של פונקציות רציונליות, וגם לשרטוט עקומות המוגדרות על ידי משוואה פולינומית בשני משתנים.

הרזולטנט של n פולינומים הומוגניים ב- n משתנים היא הכללה, שהוצגה על ידי מקאוליי[1], של הרזולטנט. עם בסיסי גרובנר, הוא אחד הכלים העיקריים של תורת החילוץ (theory elimination) .

בעבודה זו נפרש את ההגדרה של הרזולטנט ותכונותיו, ונוכיח את המשפטים העיקריים של תורת הרזולטנט.

בתחילה העבודה, נזכיר בקצרה את הגדרת הדטרמיננטה לפי תמורות, ונגדיר את מטריצת סילבסטר. בהמשך נגדיר את הרזולטנט ונוכיח את המשפט היסודי (פרק 2) שהוא החלק העיקרי של העבודה.

בשאלה של השורשים המשותפים של שני פולינומים נדון בפרק 3, וכן נוכיח עוד כמה תוצאות מעניינות שנובעות 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

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

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

הסכום הוא על $n!$ התמורות σ של המספרים $\{1,2,\ldots,n\}$, 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 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in S_3$

תמורת הזהות היא זוגית ולכן $\operatorname{sgn}\left(\sigma\right) = 1$, ובסה"כ מתמורת הזהות נקבל את המכפלה $2 \cdot 2 \cdot 3$.

נבחר תמורה נוספת $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) \in S_3$, ע"י פירוק לחילופים נקבל את $\operatorname{sgn}\left(\sigma\right)$,

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

קבלנו $\operatorname{sgn}\left(\sigma\right) = 1$ ולכן בסה"כ מתמורה זו נקבל את המכפלה $1 \cdot 4 \cdot 5$.

תמורה נוספת לדוגמא $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12) \in S_3$, זהו חילוף ולכן $\operatorname{sgn}\left(\sigma\right) = -1$ ובסה"כ מתמורה זו נקבל את המכפלה $-3 \cdot 4 \cdot 3$.

ולאחר חישוב כל התמורות האחרות נקבל

$$\begin{aligned} \det\left(A\right) &= \sum_{\sigma \in S_3} \operatorname{sgn}\left(\sigma\right) \alpha_{1,\sigma(1)}\alpha_{2,\sigma(2)} \cdots \alpha_{n,\sigma(n)} \\ &= 2 \cdot 2 \cdot 3 - 2 \cdot 3 \cdot 5 - 3 \cdot 4 \cdot 3 + 3 \cdot 3 \cdot 1 - 1 \cdot 2 \cdot 1 + 1 \cdot 4 \cdot 5 \\ &= 12 - 30 - 36 + 9 - 2 + 20 = 25\,. \end{aligned}$$

הגדרה 1.2 מטריצת סילבסטר

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

נסמן $f\left(x\right) = \sum_{i=0}^{n} a_i x^i$, $g\left(x\right) = \sum_{j=0}^{m} b_j x^j$

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

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

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 $\deg(f)>n$ או $\deg(f)<0$, ו $b_i=0$ אם $\deg(g)>m$ או $\deg(g)<0$.

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 $n=3$ ו- $m=2$, 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 $g(x)$, $f(x)$ ממעלה n,m בהתאמה , מעל שדה F יהיו $n,m\in\mathbb{N}$.

נגדיר את הרזולטנט שלהם

$R(f,g)=a_0b_0$ אם $n=m=0$.

בכל מקרה אחר

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

הערה 1.5

לפי ההגדרה הכללית בסוף 1.2, הגדרה 1.4 עדין תקפה לכל שני פולינומים ממעלה קטנה או שווה ל- n, 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- $\operatorname{Syl}\left(f,g\right)$ 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 $a_0,\dots,a_n,b_0,\dots,b_n$, ונסמן $F=K\left(a_0,\dots,a_n,b_0,\dots,b_n\right)$.

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

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

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

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

דוגמא:

עבור $f\left(x\right)=a_2x^2+a_1x+a_0$ ו- $g\left(x\right)=b_1x+b_0$, נחשב את הדטרמיננטה של מטריצת סילבסטר

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

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

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

הוכחה

הוכחה זו מתבססת על הגדרת הדטרמיננטה לפי תמורות.

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

כלומר עבור σ_{i_1,j_1} ו- σ_{i_2,j_2} אם $i_1\neq i_2$ אז $j_1\neq j_2$ לכל j_l ו i_k עם $1\leq k$ ו $l\leq n+m$, 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 $f\left(x\right)$, ומ- n השורות האחרונות מקבלים מקדמים מהפולינום $g\left(x\right)$, ובסה"כ סכום החזקות של σ הוא m מאיברי $f\left(x\right)$ ו n מאיברי $g\left(x\right)$ כנדרש.

טענה 1.9

יהיו f,g פולינומים מעל שדה F.

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

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 המחזור

$$\left(r_1 r_2 \ldots r_m r_{m+1} \ldots r_{n+m}\right) .$$

נבצע את נמחזור הזה n פעמים. כך נקבל שהשורה הראשונה (של המטריצה המקורית) תהיה במקום ה $n+1$ "ואז f תהיה ב m השורות האחרונות", והשורה ה m (של המטריצה מקורית) תהיה 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]) וכל 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.$g\left(x\right)=\sum_{j=0}^{m}b_jx^j$ ו- $f\left(x\right)=\sum_{i=0}^{n}a_ix^i$ פולינומים מעל שדה F (F השדה שהוגדר בהערה 1.7).

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

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

<u>משפט 2.1 משפט הרזולטנט</u>

יהיו f, g פולינומים מעל שדה F.

אם $m=0$ ו $n>0$, $R\left(f,g\right)=a_0^m$.

אם $n=0$ ו $m>0$, $R\left(f,g\right)=b_0^n$.

אם $m=n=0$, $R\left(f,g\right)=a_0b_0$.

אם $n,m>0$,

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

<u>דוגמא</u>

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

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

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

נסמן

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

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

$$\left(\left(0-\left(-1\right)\right)\left(0-3\right)\right)\left(\left(2-\left(-1\right)\right)\left(2-3\right)\right)\left(\left(-2-\left(-1\right)\right)\left(-2-3\right)\right)=45$$

קבלנו ש-

$$R\left(f,g\right)=45$$

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

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

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

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

ביתר דיוק נקבל את התמורות הבאות:

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

"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, נוכיח תחילה שהוא שקול למשפט הבא.

<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 כי לפי זה ניתן לרשום את f,g כמכפלה של גורמים לינאריים מעל שדה F.

<u>הוכחת I.</u>

נרשום את g כמכפלה של גורמים לינארים:

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

נציב $\xi_0 \dots \xi_n$ ב g ונקבל

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

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 $(\eta_j - \xi_i)$ נקבל את השוויון

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

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

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

נציב $\eta_0 \ldots \eta_m$

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

ולכן שוב משרשור השוויונות הבא נקבל

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

כנדרש.

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

<u>טענה עזר 2.3</u>

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

מתקיים

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

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

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

.

<u>הוכחה</u>

ההוכחה באינדוקציה על המעלה של h, נניח ש $k \leq n - m$ ונסמן $h = \sum_{\rho=0}^{k} h_\rho x^\rho$, נוכל להניח ללא הגבלת כלליות ש $k = n - m$ ע"י הגדרת $h_\rho = 0$ לכל שאר החזקות.

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

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

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

הביטוי $n-\rho$ נובע מכך שהכפל cx^{ρ} מזיז ב g מקומות את המונומים של g ρ מקומות כי $cx^{\rho}b_jx^j = cb_jx^{j+\rho}$. לאחר הצבה $i=j+\rho$ נקבל $j=i-\rho$ כלומר המקדם של החזקה ה i הוא $b_{i-\rho}$.

כיון ש $\rho < n-m$, כל אחד מ m השורות הראשונות ב $\mathrm{Syl}\left(f+cx^{\rho}g, g\right)$ הוא סכום של אותה שורה מוכפלת ב c עם אחת השורות מ- n השורות האחרונות.

במילים אחרות ניתן לעבור מ $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(f+cx^{\rho}g, g\right)$ ע"י פעולות של הוספת קומבינציה לינארית של שורות אחרות על שורה במטריצה (שימו לב ש- $b_{n-\rho-i} = 0$ לכל $n-\rho-i > m$). אבל הוספת קומבינציה לינארית של שורות לשורה אחרת במטריצה לא משנה את הדטרמיננטה לכן

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

עתה נשלים את ההוכחה למקרה הכללי.

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

צעד האינדוקציה:

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

כנדרש.

המקרה השני $R\left(f,g\right) = \mathrm{R}\left(f,g+hf\right)$ מתקבל 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 $\deg\left(f\right) \le k \le n$ אז

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

הוכחה

ההוכחה 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 $b_m = 0$. אז

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

ניתסן להבחין שאם נמחק את השורה הראשונה והעמודה הראשונה נקבל את המטריצה

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

כאשר $\hat{g}\left(x\right)=\sum_{j=0}^{m-1}b_jx^j$, מכיון ש $b_m=0$, $\hat{g}\left(x\right)=g\left(x\right)$, לכן אם נפתח את הדטרמיננטה $R\left(f,g\right)$ לפי העמודה הראשונה נקבל:

$$\boxed{R\left(f,g\right)}=a_nR_{n,m}\left(f,\hat{g}\right)=\boxed{a_nR_{n,m-1}\left(f,g\right)}.$$

באופן כללי אם $b_i=0$ עבור כל i כך ש- $r\le i<m$ אז

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

.

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

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

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 $n+k$ ו $n-k$ חולקים 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</u>

ההוכחה באינדוקציה על הגודל של המטריצה $n+m$.

בסיס האינדוקציה:

עבור $m=n=0$ הטענה מתקיימת לפי ההגדרה של $\text{Syl}\left(f,g\right)$.

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

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

בדומה עבור $m=0$ ו $n>0$

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

עתה נניח ש- $0<m-n$

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

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

הנחת האינדוקציה:

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

מקרה 1:

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

קיימים פולינומים r ו- q עם $\deg(r) < \deg(f)$ כך ש-

$$g = qf + r\,.$$

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 $\deg(q) = m - n$, לכן נוכל להשתמש בטענת עזר 2.3: נקבל

$$R(f,g) = R(f, g - qf) = R(f,r)\;. \quad (*)$$

נחלק שוב את המקרים.

מקרה א. $r \neq 0$

נסמן $k = \deg(r) \geq 0$.

מהנחת האינדוקציה וטענת עזר 2.4,

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

כאשר 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. $r = 0$.

אז

$$g = fq\,.$$

מכיון שהנחנו ש- $n > 0$ מתקיים

$$R(f,r) = R(f,0) = 0$$

על פי מה שהוכחנו לעיל.

ולכן

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

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

מקרה 2.

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

כמו במקרה הקודם קיימים q ו r עם $\deg\left(r\right)<m$ כך ש-

$$f=gq+r$$

ומאותם נימוקים כמו במקרה הקודם

$$R\left(f,g\right)=R\left(f-gq,g\right)=R\left(r,g\right)\ .\quad(***)$$

ופה נחלק שוב את המקרים

מקרה א.$r\neq 0$

נסמן $k=\deg\left(r\right)\geq 0$, ומהנחת האינדוקציה וטענת עזר 2.4 נקבל

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

כאשר השוויון האחרון נובע מכך ש η_j הם שורשים של g, מה שגורר

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

מ $(***)$ ו $(****)$ נקבל את הנדרש.

מקרה ב.

$r=0$,

דומה מאוד לאותו מקרה בהוכחה הקודמת

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

לכן

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

כיון ש- השורשים של g הם שורשים של f, נסיק כמקודם שמכפלה הגורמים (2.1) מתאפסת ונקבל את השוויון.

פרק 3.

תוצאות ממשפט הרזולטנט

בפרק זה נמשיך עם המוסכמות שבתחילת פרק 2.

<u>טענה 3.1</u>

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

<u>הוכחה</u>

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.

<u>טענה 3.2</u>

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

<u>הוכחה</u>

צד אחד

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

אם ל- f, g יש גורם משותף ,אז יש להם שורש משותף בשדה הפיצול של fg, וממשפט 2.1 נקבל את הטענה.

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

אם $R(f,g)=0$, מטענה 3.1, ל- f, g יש שורש משותף בשדה הפיצול fg שנסמן α, אז $x-\alpha$ הוא גורם משותף של f ו- g ומכאן הטענה.

לצורך המשפט הבא נזכיר מהו מימד של מטריצה.

מימד של מטריצה הוא המימד שנפרס ע"י וקטורי השורות או העמודות של המטריצה. ונציין שבמקרה ושהשורות תלויות לינארית, המימד של המטריצה קטן מהגודל של המטריצה.

<u>משפט 3.3</u>

יהיו f, g פולינומים בשדה F.

נסמן ב- $h=\mathrm{GCD}(f,g)$ את המחלק המשותף המירבי של f, g. אזי 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, לפעמיים נתייחס רק לגודל של אחד מהם כשהכוונה לשניהם.

<u>הוכחה</u>

לפני שנכנסים לגוף ההוכחה נציין:

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

(2) . $\mathrm{Syl}(f,g)$ ו- $\mathrm{Syl}(g,f)$ שוות פרט לסדר של השורות, ולכן המימד שלהן שווה, מכאן, נוכל להניח ללא הגבלת הכלליות ש- $m\le n$.

(3) . קיימים q ו- r עם $\deg(r)<m$ כך ש- $f=qg+r$. בהוכחת 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 של הוספת קומבינציה לינארית של שורות לשורה אחרת במטריצה. 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 $\text{Syl}\left(f,g\right)$.

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

<u>שלב 1.</u>

קיים q ו- r עם $k=\deg\left(r\right)<m$, כך ש-

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

מאידך,

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

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

<u>שלב 2</u>

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

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

בעמודה הראשונה יש רק איבר יחיד b_m, לכן וקטור זה שייך למימד שנפרש ע"י וקטורי העמודות, 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 $\text{Syl}_{n,m}\left(r,g\right)$ ו $\text{Syl}_{n-1,m}\left(r,g\right)$ שווים, כאשר $\text{Syl}_{n-1,m}\left(r,g\right)$ 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 $\text{Syl}_{n-1,m}\left(r,g\right)$, וכך נמשיך עד שנקבל את המטריצה $\text{Syl}_{k,m}\left(r,g\right)$, ולפי ההסבר בשלב 2 המימד של המשלים של המטריצות המתקבלות ע"י מחיקה העמודה והשורה המתאימות לא משתנה.

סיכום ביניים:

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

<u>שלב 4</u>

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

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

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

<u>שלב 5</u>

משלבים 3 ו 2 המימדים של המשלימים של $\text{Syl}_{n,m}\left(f,g\right),\text{Syl}_{k,m}\left(r,g\right),\text{Syl}_{k_0,k}\left(r_0,r\right),\text{Syl}_{k_1,k_0}\left(r_1,r_0\right)\ldots,\text{Syl}_{k_{d-1},l}\left(0,h\right)$ 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, לכן המימד של המשלים של $\mathrm{Syl}_{k_{d-1},l}(0,h)$ הוא $l=\deg(h)$,

זה מוכיח שהמימד 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

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

נוכיח ש-

$$pf+qg=\sum_j\gamma_jx^j$$

ובזה נסיים את ההוכחה.

נחקור את הביטוי

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

לשם כך 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

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

נבצע החלפת אינדקסים $j = m + n - l$, לכל $0 \leq j \leq n + m$ בפרט $0 \leq l \leq n + m$

מתקיים

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

אם $m > l$, מכיון שלכל $k > l$, $\alpha_k = 0$, מתקיים

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

אם $m < l$, מכיון שלכל $k \geq m$, $\alpha_k = 0$(כי $\deg(p) = m - 1$). לכן

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

ובאותו אופן מתקיים

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

קבלנו ש

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

עתה נחשב את המכפלה

$$\begin{aligned}
\boxed{pf+qg} &= \sum_{\tau}\alpha_\tau x^\tau \sum_k a_k x^k + \sum_\tau \beta_\tau x^\tau \sum_k b_k x^k \\
&= \sum_l \sum_{k+\tau=l} \alpha_\tau a_k x^l + \sum_l \sum_{k+\tau=l} \beta_\tau b_k x^l \\
&= \sum_l \sum_{k=0}^{l} \alpha_k a_{l-k} x^l + \sum_l \sum_{k=0}^{l} \beta_k b_{l-k} x^l \\
&= \sum_l \left(\sum_{k=0}^{l} \alpha_k a_{l-k} + \sum_{k=0}^{l} \beta_k b_{l-k} \right) x^l \\
&= \boxed{\sum_k \gamma_j x^k}
\end{aligned}$$

ואכן קבלנו את השוויון הנדרש.

ביבליוגרפיה

[1]. Macaulay, F. S. (1902), "Some Formulæ in Elimination", Proc. London Math. Soc., 35: 3–27, doi: 10.1112/plms/s1-35.1.3.

[2]. Bourbaki, N. (1998). "Algebra I: Chapters 1-3", 6.1 p. 65 (example), Hermann, Publishers in Arts and Sciences, Addison-Wesley..