האוניברסיטה הפתוחה

עבודה סמינריונית בנושא הרזולטנט

אליסף לרר

ת.ז. 308376458

מנחה: אלעד פארן

תוכן העניינים :

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

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

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

נעבור לדוגמא:

תהי מטריצה

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

נחשב את $\det(A)$ לפי הגדרה 1.1.

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

השורה הראשונה מייצגת את השורה במטריצה והשורה השניה 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 $\operatorname{sgn}(\sigma)=1$, 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 $\operatorname{sgn}(\sigma)$,

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

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

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

לאחר חישוב כל התמורות נקבל

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

הגדרה 1.2 מטריצת סילבסטר

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

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

$\mathrm{Syl}(f,g) = \mathrm{Syl}_{n,m}(f,g)$ 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 ב[illegible] $\mathrm{Syl}_{n,m}$[illegible]$g)$ מה[illegible] מוגדר[illegible] באופן הבא, [illegible] 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 $n = 3$ $m = 2$, לכן

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

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 $f(x), g(x)$, מעל שדה F.

נגדיר את הרזולטנט שלהם ל[illegible]

יהיו $n, m \in \mathbb{N}$

$R(f,g) = a_0 b_0$ אם $n = m = 0$,

בכלל 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.

~~נכתוב 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 $m<k\le\deg\left(\left(f\right)\right)$ 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 $\hat{f}=f$.~~
~~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 $a_0,\dots,a_n,b_0,\dots,b_n$, ונסמן $F=K\left(a_0,\dots,a_n,b_0,\dots,b_n\right)$.

אם נסמן $g\left(x\right)=\sum_{j=0}^{m}b_jx^j$,$f\left(x\right)=\sum_{i=0}^{n}a_ix^i$, 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 $a_0,\dots,a_n,b_0,\dots,b_n$.

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 $a_0\dots a_n$ המעלה היא m, ועבור $b_0\dots b_m$ המעלה היא n.

הוכחה

הוכחה זו מתבססת על הגדרת הדטרמיננטה לפי תמורות.

נחזור ל $\mathrm{Syl}\left(f,g\right)$, 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 שמכל שורה וכל עמודה מופיעה בדיוק פעם אחת.

כלומר עבור σ_{i_2,j_2} ,σ_{i_1,j_1} אם $i_1\ne i_2$ אז $j_1\ne j_2$ לכל i_k,j_l, $1\le k,l\le n+m$, 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 האיבר~~ 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 $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(g,f\right)$, ע"י פעולות על שורות המטריצה, ולכן נבדוק מה יהיה המחיר לעבור מ $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(g,f\right)$.

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

$$\left(r_1r_2\dots r_mr_{m+1}\dots r_{n+m}\right)\ .$$

נבצע את המעגל הזה n פעמים. כך נקבל שהשורה הראשונה (של המטריצה המקורית) תיהיה [illegible]ם 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

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

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

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 $g\cdot f$, כלומר F מכיל את כל השורשים של f ו- g.
3. $\xi_0\ldots\xi_n$ הם השורשים של f, ו $\eta_0\ldots\eta_m$ 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 $n,m>0$

טוב!

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

דוגמא

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

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

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

נסמן

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

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

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

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 :

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

~~"את הסימן ? שממנו 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 כי

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

נה

<u>הוכחת I.</u>

נרשום את g כמכפלה של גורמים ליניארים :

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

נציב $\xi_n \dots \xi_0$ ב g נקבל

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

משרשור השווינות הבא נקבל את השוויון

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

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

לא הבנתי

2.1

הוכחת II

תחילה נבחין ש~~ע"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

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

נציב $\eta_0 \dots \eta_m$

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

ולכן שוב משרשור השוויונות הבא נקבל

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

(2.1) **לא הבנתי**

כנדרש.

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

טענת עזר 2.3

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

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

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

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

.

~~הדרישה ש $\deg(h) \le n - m$ במקרה הראשון (ובדומה $\deg(h) \le m - n$) הכרחית, נניח ש- $\deg(h) > n - m$ ולכן $\deg(gh) >$ $n - m + m = n$ ולכן גם $\deg(f + hg) > n$ 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.

ρ

מכיון ש $n < m$, 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 $cx^\rho b_j x^j = cb_j x^{j+\rho}$, לאחר הצבה $i = j+\rho$ נקבל $j = i-\rho$ כלומר המקדם של החזקה ה i הוא $b_{i-\rho}$.

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

במילים אחרות ניתן לעבור מ $\operatorname{Syl}(f,g)$ ל $\operatorname{Syl}\left(f + cx^\rho g, g\right)$ 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, לכן

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

אותה

הנחת האינדוקציה:

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

צעד האינדוקציה:

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

כנדרש.

צריך לבדוק האם אני משתמש בזה ואם זה לא שובר לא הוכחה בהמשך

wrong

נשים לב שמתוך כך שבשביל השוויונות קבלנו ש

$$\operatorname{Syl}(f+hg,g) = \operatorname{Syl}(f,g) \quad (2.2)$$

בשוויון זה נעשה שימוש בהמשך.

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

<u>טענת עזר 2.4</u>

I. אם $\deg(g) \le k \le m$ אז

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

II. אם $\deg(f)\le k\le n$ אז

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

הוכחה

ה 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

b_m

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

נבחין שאם נמחק את השורה הראשונה והעמודה הראשונה נקבל את המטריצה

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

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

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

~~בשביל לסיים את ההוכחה נגדיר את g לכל $\deg(g)\le j\le m$ להיות עם מקדם 0, ונקבל~~

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

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

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

הוכחת II.

לפי 1.9

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

לפי I והתנאי ש $\deg(f) < k < n$ נקבל

~~ולכן~~

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

שוב לפי משוואה 1.9

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

נציב ונקבל

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

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

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

כנדרש.

הוכחת משפט 2.1 ~~ו 2.2~~

~~נוכיח~~ באינדוקציה על הגודל של המטריצה $n + m$

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

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

(*)

בסיס האינדוקציה:

עבור $m = n = 0$ הטענה מתקיימת.

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

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

בדומה עבור $m = 0$ ו $n > 0$

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

(*)

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

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

לכן 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 ונקבל

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

נחלק שוב ~~למקרים~~.

מקרה א. $r\neq0$, נסמן $k=\deg(r)\geq0$,

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 האחרון 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 הראשונית של מקרה זה $n>0$ ולכן~~

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

~~"0" בשוויון האחרון הכוונה למטריצת האפס~~

ולכן

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

גם

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.

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

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

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

מאותם נימוקים כמו במקרה הקודם

$$(***)\ R(f,g)=R(f-gq,g)=R(r,g)$$

ופה נחלק שוב ~~למקרים~~.

מקרה א.

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

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

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

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

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

מקרה ב.

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

~~$\mathrm{Syl}(r,g)=\mathrm{Syl}(0,g)=$ "0".~~

ולכן

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

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

עד כאן הייתי כבר ==========================

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

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

זה 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

$\Leftarrow$ 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~~ α ~~$x-$ גורם משותף מ f,g.~~

~~וקבלנו את הטענה.~~

לצורך המשפט הבא נזכיר מהו מימד של מטריצה.

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

במקרה 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 $\deg(h)$.

הערה: 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). $\mathrm{Syl}(f,g)$ ו $\mathrm{Syl}(g,f)$ שווים פרט לסדר של השורות, ולכן המימד ~~שנפרש על ידם~~ שווה, ~~לכן~~ ללא הגבלת כלליות נוכל להניח ש $n\le m$.

(3). קיימים r,q ~~כך ש~~ $m>\deg(r)$ ~~המקיימים~~ $f=qg+r$, 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 ~~על שורות המטריצה~~ ולכן המימד שלהם שווה.

רעיון ההוכחה:

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

~~נתחיל...~~

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

<u>שלב 1.</u>

עם ~~כך ש~~ כך ש ~~המתקיימים~~ $k=\deg(r)<m$ ~~כך ש~~ r ~~וקיים~~ ו- q קיים

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

$$\deg(q)=\deg(qg)-\deg(g)=n-m\,.$$

מתקיימים תנאי משפט 2.3, לכן לפי (2) הממד של $\mathrm{Syl}_{n,m}(f,g)$ ו $\mathrm{Syl}_{n,m}(r,g)$ ~~שווה~~.

<u>שלב 2</u>

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

$$\mathrm{Syl}_{n,m}(r,g)=\begin{pmatrix}
0 & \cdots & 0 & v_{n-k-1} & v_{n-k-2} & v_{n-k-3} & \cdots & 0 & 0 & 0\\
0 & 0 & \cdots & 0 & v_{n-k-1} & v_{n-k-2} & \cdots & 0 & 0 & 0\\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & v_1 & v_0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & v_2 & v_1 & v_0\\
b_m & b_{m-1} & b_{m-2} & b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & 0\\
0 & b_m & b_{m-1} & 0 & b_m & b_{m-1} & \cdots & 0 & 0 & 0\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & b_1 & b_0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0
\end{pmatrix}.$$

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

סיכום ביניים:

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

<u>שלב 4</u>

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

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

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

<u>שלב 5</u>

משלבים 3 ו 2 המימדים של המשלימים של $\mathrm{Syl}_{n,m}(f,g)\,,\mathrm{Syl}_{k,m}(r,g)\,,\mathrm{Syl}_{k_0,k}(r_0,r)\,,\mathrm{Syl}_{k_1,k_0}(r_1,r_0)\ldots,\mathrm{Syl}_{k_{d-1},l}(0,h)$ שווים.

ולכן נשאר לבדוק מהו המימד של המשלים של $\text{Syl}_{k_{d-1},l}(0,h)$. לפי הגדרת מטריצת סילבסטר, למטריצה $\text{Syl}_{k_{d-1},l}(0,h)$ יש l שורות אפסים ו $d-1$ שורות בת"ל, ולכן המימד של המשלים של $\text{Syl}_{k_{d-1},l}(0,h)$ הוא ~~l~~, ~~וזה בדיוק $\deg(h)$, ולכן~~ המימד של $\text{Syl}_{n,m}(f,g)$ 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

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

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

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

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

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~~, $0 \le l \le n + m$

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

אם

~~עבור המקרה~~ $m > l$,

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

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

אם

~~עבור המקרה~~ $m < l$,

מכיון שלכל $k \ge m$, $\alpha_k = 0$ (~~מכיוון ש~~ כי $\deg(p) = m - 1$) ~~מתקיים~~. לכן

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

באותו 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,