פרק 2:

תחילה נציג כמה מוסכמות לפרק זה.

1. $f\left(x\right)=\sum_{i=0}^{n}a_{i}x^{i}$ $g\left(x\right)=\sum_{j=0}^{m}b_{j}x^{j}$ פולינומים מעל שדה F.
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. $\xi_{0}\ldots\xi_{n}$ הם השורשים של f, ו $\eta_{0}\ldots\eta_{m}$ הם השורשים של g.

הרזולטנט

<u>משפט 2.1 (משפט הרזולטנט)</u>

יהיו f,g פולינומים מעל שדה F.

$$R_{n,m}\left(f,g\right)=a_{n}^{m}b_{m}^{n}\prod_{i=1}^{n}\prod_{j=1}^{m}\left(\xi_{i}-\eta_{j}\right)\quad.(2.1)$$

################ **פה יש בעיה**

הבעיה שזה לא מתאים להערה 1.4, לפי משוואה (2.1) מספיק שרק אחד מהמעלות קטן מ n,m ואז יש מקדם 0 וכל המכפלה מתאפסת וזה לא מתאים להגדרה לפי מטריצת סילבסטר.

מקרה טרוויאלי, כאשר $\deg\left(f\right)<n$ ו- $\deg\left(g\right)<m$, המכפלה מתאפסת, וגם $R_{n,m}\left(f,g\right)=0$ כמו שראינו בהערה 1.4.

את ההוכחה נביא מיד לאחר הדוגמא.

############################

<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

$$\xi_{1}=0,\xi_{2}=2,\xi_{3}=-2\quad\eta_{1}=-1,\eta_{2}=3$$

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-

$$\boxed{R_{m.n}\left(f,g\right)=45}$$

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

$$R_{3.2}\left(f,g\right)=\begin{vmatrix}1 & 0 & -4 & 0 & 0\\
0 & 1 & 0 & -4 & 0\\
1 & -2 & -3 & 0 & 0\\
0 & 1 & -2 & -3 & 0\\
0 & 0 & 1 & -2 & -3
\end{vmatrix}$$

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

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

לאחר שנשלים את כל התמורות 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 קבלנו את השוויון במשפט 2.1, עכשיו נעבור להוכחה.

<u>משפט 2.2 (משפט שקול למשפט הרזולטנט)</u>

יהיו f, g פולינומים מעל שדה F

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

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

מכיון שבהוכחת משפט 2.1 נשתמש בצורה השקולה משפט 2.2, אז תחילה נוכיח את שקילות המשפטים 2.2 ו 2.3

<u>טענת עזר 2.3</u>

יהיו f, g פולינומים מעל שדה F.

$$R(f,g) = (-1)^{nm} R(g,f) \quad (2.2) .$$

<u>הוכחה</u>

נפתח בדיון אינטואיטיבי:

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

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) 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.

ולכן בסה"כ הוכחנו טענה עזר 2.2.

במשוואה (2.2) נעשה שימוש בהמשך.

<u>הוכחת שקילות המשפטים 2.1 ו 2.2</u>

טענה זו נובעת כמעט ישירות מהמשפט היסודי של האלגברה.

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

<u>הוכחת I.</u>

נסמן את g כך:

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

נציב $\xi_m \ldots \xi_0$ ב g נקבל

$$g\,(\xi_i) = b_m \prod_{j=1}^{m} \left(\xi_i-\eta_j\right) \ . \quad (2.3)$$

משרשור השווינות הבא נקבל את השוויון

$$\begin{aligned}
\boxed{R\,(f,g)} &\overset{(2.1)}{\widehat{=}} a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}\left(\xi_i-\eta_j\right) \\
&= a_n^m \prod_{i=1}^{n} b_m \prod_{j=1}^{m}\left(\xi_i-\eta_j\right) \\
\text{hence } (2.3) &= \boxed{a_n^m \prod_{i=1}^{n} g\,(\xi_i)}
\end{aligned}$$

עבור f נשתמש בטענת עזר 2.3 ע"מ לקבל את השוויון.

לפי המפשט היסודי של האלגברה ניתן לרשום את f כמכפלה של גורמים לינאריים ולכן נוכל להשתמש ב I.

לפי I

$$R\,(g,f) = b_m^n \prod_{j=1}^{m} f\left(\eta_j\right)$$

ולכן

$$\begin{aligned} R(f,g) &\overset{(2.2)}{\cong} (-1)^{nm} R(g,f) \\ &= (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\eta_j) \end{aligned}$$

כנדרש.

הוכחת משפט 2.1 (משפט הרזולטנט)

לצורך הוכחת משפט הרזולטנט נצטרך שתי טענות עזר, נביא את הטענות ואת ההוכחות שלהם לפני המשפט.

טענה עזר 2.4

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

אז מתקיים

$$R_{n,m}(f+hg,g) = R_{n,m}(f,g)\ .$$

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

$$R_{n,m}(f,g+hf) = R_{n,m}(f,g)\ .$$

.

הדרישה ש $\deg(h) \le n-m$ במקרה הראשון (ובדומה $\deg(h) \le m-n$) הכרחית אחרת $\deg(hg) > n+m$ ולכן גם $\deg(f+hg) > n+m$ 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

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

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 $\mathrm{Syl}_{n,m}(f + cx^\rho g, g)$ הוא סכום של השורה המתאימה במטריצה $\mathrm{Syl}_{n,m}(f,g)$ עם אחד השורות מ n השורות האחרונות וקומבינציה לינארית של שורות אחרות.

במילים אחרות ניתן לעבור מ $\mathrm{Syl}_{n,m}(f,g)$ ל $\mathrm{Syl}_{n,m}(f + cx^\rho g, g)$ 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:

$$\boxed{R_{n,m}(f + (h_\rho x^\rho)g, g) = R_{n,m}(f,g)}$$

הנחת האינדוקציה :

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

צעד האינדוקציה :

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

כנדרש.

נשים לב שתוך כדאי שרשור השוויונות קבלנו ש

$$\mathrm{Syl}_{n,m}\left(f+hg,g\right)=\mathrm{Syl}_{n,m}\left(f,g\right)\quad(2.4)$$

בשוויון זה נעשה שימוש בהמש.

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

<u>טענת עזר 2.5</u>

i. אם $\deg\left(g\right)\leq k\leq m$ אז

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

ii.אם $\deg\left(f\right)\leq k\leq n$ אז

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

<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

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

נבחין 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 $\hat{g}\left(x\right)=\sum_{j=0}^{m-1}b_jx^j$ ומכיון ש $b_m=0$ אז $\hat{g}\left(x\right)=g\left(x\right)$, ולכן אם נפתח את הדטרמיננטה $R_{n,m}\left(f,g\right)$ לפי העמודה הראשונה נקבל:

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

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

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

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

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

הוכחת II.

לפי משוואה (2.2)

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

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 (2.2)

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

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

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

כנדרש.

הוכחת משפט הרזולטנט

נוכיח באינדוקציה על הגודל של המטריצה $n+m$

לפי המוסכמות בראש הפרק

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

בסיס האינדוקציה (חסר)

הנחת האינדוקציה:

נניח שמשפט הרזולטנט מתקיים לכל ערך מטריצה קטנה מ $n+m$, ובהנחה זה אנחנו כוללים שזה נכון לכל f,g שקטנות מ n,m בהתאמה לפי הערה 1.5

מקרה 1:

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

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

$$g=qf+r$$

נבחין כי

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

ולכן נקבל את השוויונות הבאים

$$\deg\left(q\right)=\deg\left(qf\right)-\deg\left(f\right)=\deg\left(g-r\right)-n=m-n$$

קבלנו ש $\deg\left(q\right)=m-n$ ולכן נוכל להשתמש בטענת עזר 2.4, נקבל

$$R_{n,m}\left(f,g\right)=R_{n,m}\left(f,g-qf\right)=R_{n,m}\left(f,r\right)$$

נחלק שוב למקרים.

מקרה 1. $r\neq 0$ נסמן $k=\deg\left(r\right)\geq 0$

מהנחת האינדוקציה וטענת עזר 2.5

$$R_{n,m}\left(f,r\right)=a_n^{m-k}R_{n,k}\left(f,r\right)=a_n^{m-k}a_n^k\prod_{i=1}^{n}r\left(\xi_i\right)=a_n^m\prod_{i=1}^{n}g\left(\xi_i\right)$$

השוויון האחרות נובע מכך ש ξ_i הם שורשים של f ולכן

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

קבלנו את הטענה עבור $0 < n = \deg(f) \leq m = \deg(g)$ ו $r \neq 0$.

עבור $r = 0$

$$g = fq$$

לפי ההנחה של מקרה זה $n > 0$ ולכן

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

ולכן

$$R_{n,,m}(f, r) = 0$$

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.

לפי טענת עזר 2

$$\begin{aligned} R_{n,,m}(f, g) &= R_{n,,m}(f, g - qf) = R_{n,,m}(f, 0) \\ &= R_{n,,m}(f, r) = 0 \end{aligned}$$

ויתר מזה

$$g(\xi_1) = f(\xi_1)\, q(\xi_1) = 0$$

כלומר ξ_1 הוא שורש של g גם ולכן ?????

מקרה 2

$n = 0$

$$\begin{aligned} R_{0.m}(f, g) &= a_n^m b_m^0 \prod_{i=1}^{0} \prod_{j=1}^{m} \left(\xi_i - \eta_j\right) \\ &= a_n^m \end{aligned}$$

והטענה מתקיימת

מקרה 3

$m = \deg(g) < n = \deg(f)$ הוכחה זה דומה למקרה 1,

וכמו כן עבור $m = 0$ הוכחה דומה עבור מקרה 2

לא נחזור על הוכחות אלו