פרק 2.

הרזולטנט

תחילה נציג כמה מוסכמות לפרק זה.

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

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

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

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

נציב $\eta_0\ldots\eta_m$

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

ולכן שוב משרשור השוויונות הבא נקבל

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

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 $m\leq n$, ויהי h פולינום כך ש $\deg\left(h\right)\leq n-m$.

מתקיים

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

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

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

.

הדרישה ש $\deg\left(h\right)\leq n-m$ במקרה הראשון (ובדומה $\deg\left(h\right)\leq m-n$) 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 $k\leq n-m$ 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 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:

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

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 $\deg(f) \le k \le n$ 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

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

נבחין שאם נמחק את השורה הראשונה והעמודה הראשונה נקבל את המטריצה

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

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 $\deg(g) \le j \le m$ 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 $R(f,g) = a_n^{m-k} R_{n,k}(f,g)$ 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

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

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

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

כנדרש.

<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

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

בסיס האינדוקציה:

עבור $m = n = 0$ הטענה מתקיימת.

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

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

ובדומה 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

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

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

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

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

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

"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..