

פרק 2:

תחילה נציג כמה מוסכמות לפרק זה.

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

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

הרזולטנט

משפט 2.1 (משפט הרזולטנט)

יהיו f, g פולינומים מעל שדה F .

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

מקרה טריויאלי, כאשר $\deg(f) < n$ וגם $\deg(g) < m$, המכפלה מתאפסת, וזה נכון גם לפי הגדרה 1.4 כמו שראינו בהערה 1.6.

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 $3, -1$.

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 $\text{Syl}(f, g)$:

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

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:

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

"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.

משפט 2.2 (משפט שקול למשפט הרזולטנט)

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

טענת עזר 2.3

יהיו f, g פולינומים מעל שדה F .

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

הוכחה

נפתח בדיון אינטואיטיבי:

ניתן לעבור מ $\text{Syl}(f, g)$ ל $\text{Syl}(g, f)$, ע"י פעולות על שורות המטריצה, ולכן 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) תהיה במקום ה $n+1$ ואז f תהיה ב m השורות האחרונות, והשורה ה m (של המטריצה מקורית) תהיה בשורה הראשונה כלומר " g תהיה 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 $nm + n^2 - n$ חולקים את אותה זוגיות.

ולכן בסה"כ הוכחנו טענה עזר 2.2.

במשוואה (2.2) נעשה שימוש בהמשך.

הוכחת שקילות המשפטים 2.1 ו 2.2

נרצה להוכיח ש

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

ובהוכחה עצמה נוכיח את ששרשור השוויונות שווה ל $R(f, g)$

טענה זו נובעת כמעט ישירות מהמשפט היסודי של האלגברה.

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

הוכחת I.

נרשום את g כמכפלה של גורמים לינאריים :

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

נציב $\xi_0 \dots \xi_m$ ב g נקבל

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

משרשור השוויונות הבא נקבל את השוויון

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

$$\text{hence (2.3) = } \boxed{a_n^m \prod_{i=1}^n g(\xi_i)}$$

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

הערה: בהוכחת משפט הרזולטנט ללא תלות בהוכחה הנוכחית נוכיח את השוויון $R(f, g) = a_n^m \prod_{i=1}^n g(\xi_i)$ ולכן נוכל להשתמש בטענת עזר (2.3), למען הסדר הטוב לא הבאנו את ההוכחה הזו כאן אלא נשאיר אותו להוכחת משפט הרזולטנט.

נרשום את f כמכפלה של גורמים לינאריים.

לפי I

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

ולכן

$$\begin{aligned} R(f, g) &\stackrel{(2.3)}{\cong} (-1)^{nm} R(g, f) \\ &= (-1)^{nm} b_m^n \prod_{j=1}^m f(\eta_j) \end{aligned}$$

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

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

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

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

הביטוי $n - \rho$ נובע מכך שהכפל cx^ρ מזיז את איברי g 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 i הוא $b_{i-\rho}$.

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

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

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

הנחת האינדוקציה:

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

צעד האינדוקציה:

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

כנדרש.

נשים לב שתוך כדאי שרשור השוויונות קבלנו ש

$$\text{Syl}(f + hg, g) = \text{Syl}(f, g) \quad (2.4)$$

בשוויון זה נעשה שימוש בהמש.

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

טענת עזר 2.5

i. אם $\deg(g) \leq k \leq m$ אז

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

ii. אם $\deg(f) \leq k \leq n$ אז

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

הוכחה

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

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

נבחין שאם נמחק את השורה הראשונה והעמודה הראשונה נקבל את המטריצה

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

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

הוכחת II.

לפי משוואה (2.2)

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

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

ולכן

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

שוב לפי משוואה (2.2)

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

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

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

כנדרש.

הוכחת משפט הרזולטנט

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 (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 1.6.

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 2.4, נקבל

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

נחלק שוב למקרים.

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

מהנחת האינדוקציה וטענת עזר 2.5

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

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- (**) קבלנו את הטענה עבור $0 < n = \deg(f) \leq m = \deg(g)$ ו $r \neq 0$. מקרה 2. $r = 0$,

$$g = fq.$$

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

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

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.

מקרה 2

$$n = 0$$

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

והטענה מתקיימת

מקרה 3

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

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

$$f = gq + r$$

ומאותם נימוקים כמו במקרה הקודם

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

ופה נחלק שוב למקרים $r \neq 0$ נסמן $k = \deg(r) \geq 0$, ומהנחת האינדוקציה וטענת עזר 2.5 נקבל

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

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

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

ולכן בסה"כ קבלנו את 2.2.II.

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

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

ולכן

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

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

מקרה 2. $m = 0$.

$$R_{0,m}(f, g) = a_n^0 b_m^n \prod_{i=1}^n \prod_{j=1}^0 (\xi_i - \eta_j) = b_m^n$$