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 ל f,g יש שורש משותף אם ורק אם $R\left(f,g\right)=0$.

<u>הוכחה</u>

לפי משפט 2.1

$$R\left(f,g\right)=0\Longleftrightarrow a_{n}^{m}b_{m}^{n}\prod_{i=1}^{n}\prod_{j=1}^{m}\left(\xi_{i}-\eta_{j}\right)=0\,.$$

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, ל f,g יש גורם משותף אם ורק אם $R\left(f,g\right)=0$.

<u>הוכחה</u>

צד אחד

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

לפי ההנחה ל f,g יש גורם משותף ולכן יש להם שורש משותף וממשפט 2.1 נקבל את הטענה.

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

לפי ההנחה ש $R\left(f,g\right)=0$ מטענה 3.1 ל f,g יש שורש משותף נסמן α, נוכל נוציא את $x-\alpha$ גורם משותף מ f,g.

וקבלנו את הטענה.

לצורך המשפט הבא נזכיר מהו מימד של מטריצה.

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

ובמקרה שהשורות תלויות לינארית אז המימד שנפרש ע"י המטריצה קטן מהגודל של המטריצה.

<u>משפט 3.3</u>

יהיו f,g פולינומים בשדה F.

נסמן ב- $h=\mathrm{GCD}\left(f,g\right)$ את המחלק המשותף המירבי של f,g .

המעלה של המימד של $\mathrm{Syl}\left(f,g\right)$ הוא $n+m-\deg\left(h\right)$, ובאופן שקול המעלה של המימד של המשלים של $\mathrm{Syl}\left(f,g\right)$ הוא $\deg\left(h\right)$.

<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) . $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(g,f\right)$ שוות פרט לסדר של השורות, ולכן המימד שנפרש על ידם שווה, ולכן ללא הגבלת כלליות נוכל להניח ש $m\leq n$.

(3) . קיימים r,q כך ש $\deg\left(r\right)<m$ המקיימים $f=qg+r$, ובהוכחת טענת עזר 2.3 ראינו שאפשר לעבור מ $\mathrm{Syl}\left(f,g\right)$ ל $\mathrm{Syl}\left(f+\left(-qg\right),g\right)=\mathrm{Syl}\left(r,g\right)$ ע"י פעולות על שורות המטריצה 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 $\mathrm{Syl}\left(f,g\right)$.

נתחיל...

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

<u>שלב 1.</u>

קיים q וקיים r כך ש $k=\deg\left(r\right)<m$ ומתקיים

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

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

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

<u>שלב 2</u>

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

$$\mathrm{Syl}_{n,m}\left(r,g\right)=\begin{pmatrix} 0 & \cdots & 0 & \upsilon_{n-k-1} & \upsilon_{n-k-2} & \upsilon_{n-k-3} & \cdots & 0 & 0 & 0\\ 0 & 0 & \cdots & 0 & \upsilon_{n-k-1} & \upsilon_{n-k-2} & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & \upsilon_1 & \upsilon_0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & \upsilon_2 & \upsilon_1 & \upsilon_0\\ b_m & b_{m-1} & b_{m-2} & b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & 0\\ 0 & b_m & b_{m-1} & 0 & b_m & b_{m-1} & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & b_1 & b_0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0 \end{pmatrix}$$

בעמודה הראשונה יש רק איבר יחיד b_m ולכן 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 שהמימד של המשלים של $\mathrm{Syl}_{n,m}\left(r,g\right)$ ו $\mathrm{Syl}_{n-1,m}\left(r,g\right)$ שווים, כאשר $\mathrm{Syl}_{n-1,m}\left(r,g\right)$ 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 $\mathrm{Syl}_{n-1,m}\left(r,g\right)$, וכך נמשיך עד שנקבל את המטריצה $\mathrm{Syl}_{k,m}\left(r,g\right)$, ולפי ההסבר בשלב 2 המימד של המשלים של המטריצות המתקבלות ע"י מחיקה העמודה והשורה המתאימה לה לא משתנה.

סיכום ביניים:

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

<u>שלב 4</u>

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

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

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

<u>שלב 5</u>

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

וזה בדיוק $\deg(h)$, ולכן המימד 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

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

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 $0\le l\le n+m$

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

עבור המקרה $m>l$

מכיון שלכל $k>l$, $\alpha_k=0$ מתקיים

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

עבור המקרה $m<l$

מכיון שלכל $k\ge m$, $\alpha_k=0$ מכיון ש $\deg(p)=m-1$ מתקיים

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

ובאותו אופן מתקיים

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

קבלנו ש

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

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 $l = k$ $k = i$.