פרק 3:

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

הוכחה

לפי משפט 2.1

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

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.

טענה 3.2

יהיו f,g פולינומים מעל שדה F, ל f,g יש גורם משותף אם ורק אם $R\left(f,g\right)=0$.

הוכחה

צד אחד

$\Longleftarrow$ אם ל f,g יש גורם משותף אז $R_{n,m}\left(f,g\right)=0$.

לפי ההנחה ל f,g יש גורם משותף ולכן יש להם שורש משותף ולכן הרזולטנט מתאפס, ולפי הטענה הקודמת $R_{n,m}\left(f,g\right)=0$.

$\Longrightarrow$ $R_{n,m}\left(f,g\right)=0$ אז ל f ו g יש גורם משותף.

לפי ההנחה ש $R_{n,m}\left(f,g\right)=0$ 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.

משפט 3.3

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 $n+m-\deg\left(h\right)$.

הוכחה

לפני שנכנסים לגוף ההוכחה נציין שהחלפה בין שורות המטריצה לא משנה את המימד שנפרש ע"י וקטורי השורות של המטריצה.

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

קיימים q,r כך ש $\rho=\deg\left(r\right)<m\leq n$

$$f=gq+r\Longrightarrow f-gq=r$$

ולפי טענת עזר 2.3

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

לפי ההערה בתחילת ההוכחה נוכל להסתכל על

$$R_{m,n}\left(g,r\right)$$

לפי טענת עזר 2.4 קיים β כך ש-

$$R_{m,n}\left(g,r\right)=\beta R_{m,\rho}\left(g,r\right)$$

ושוב לפי ההערה בתחילת ההוכחה המימד של $R_{m,\rho}\left(g,r\right)$ ושל $R_{\rho,m}\left(g,r\right)$ שווים.

נחזור שוב על התהליך קיימים q_2,r_2 כך ש $\rho_2=\deg\left(r_2\right)<\rho\leq m$

$$g=rq_2+r_2\Longrightarrow g-rq_2=r_2$$

ולכן

$$R_{m,\rho}\left(g,r\right)=R_{m,\rho}\left(g-rq_2,r\right)=R_{m,\rho}\left(g,r\right)$$

ולפי טענת עזר 2.4

$$R_{m,n}\left(g,r\right)=R_{m,\rho}\left(g,r\right)$$