תורת גלואה - הוכחות נבחרות

מבנים אלגבריים (2) - 80446

מרצה: שי אברה

מתרגל: אור רז

סוכם ע״י שריה אנסבכר

סמסטר ב׳ תשפ״ד, האוניברסיטה העברית

תוכן העניינים

בהכנת סיכום זה נעזרתי רבות בספר "מבנים אלגבריים" מאת: דורון פודר, אלכס לובוצקי ואהוד דה-שליט.

* * *

סביר להניח שהסיכומים שלי מכילים טעויות רבות - אני מוצא כאלה כל יום (רשימת טעויות נפוצות),
אני מפציר בכם לעדכן אותי בכל טעות שאתם מוצאים (ממש כל טעות ללא יוצא מן הכלל);
אתם מוזמנים להגיב על המסמכים ב-Google Drive, לשלוח לי דוא"ל או למלא פנייה באתר.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 התחלה

תהא $\mathbb{E}/\mathbb{F}$ הרחבת שדות.

1.1 קצת על חבורת גלואה

למה 1.1. יהיו $\alpha\in\mathbb{E}$ ו-$f\in\mathbb{F}[x]$ כך ש-$f(\alpha)=0$, מתקיים $f(\sigma(\alpha))=0$ לכל $\sigma\in\operatorname{Gal}(\mathbb{E}/\mathbb{F})$.

הוכחה. יהיו $a_0,a_1,\ldots,a_n\in\mathbb{F}$ כך ש-$f(x)=\sum_{i=0}^{n}a_ix^i$, ויהי $\sigma\in\operatorname{Gal}(\mathbb{E}/\mathbb{F})$.

$$\Rightarrow f(\sigma(\alpha))=\sum_{i=0}^{n}a_i(\sigma(\alpha))^i=\sum_{i=0}^{n}\sigma(a_i)\cdot(\sigma(\alpha))^i=\sigma\left(\sum_{i=0}^{n}a_i\alpha^i\right)=\sigma(0)=0$$

■

מסקנה 1.2. אם $\mathbb{E}$ הוא שדה פיצול של פולינום כלשהו ב-$\mathbb{F}[x]$, אז לכל שדה הרחבה Ω של $\mathbb{E}$, ולכל $\sigma\in\operatorname{Gal}(\Omega/\mathbb{F})$ מתקיים $\sigma(\mathbb{E})=\mathbb{E}$.

מסקנה 1.3. נניח ש-$\mathbb{E}$ הוא שדה פיצול של פולינום כלשהו ב-$\mathbb{F}[x]$ ויהי $f\in\mathbb{F}[x]$ פולינום כלשהו[1].
אם קיים $\alpha\in\mathbb{E}$ כך ש-$f(\alpha)=0$, אז f מתפצל ב-$\mathbb{E}$.

♣ כלומר הפולינומים ב-$\mathbb{F}[x]$ מתחלקים לשני סוגים: אלו שאין להם ולו שורש אחד ב-$\mathbb{E}$, ואלו שמתפצלים ב-$\mathbb{E}$ - אין פולינומים שרק חלק מהשורשים שלהם ב-$\mathbb{E}$.

♣ בהמשך נקרא להרחבות כאלה <u>הרחבות נורמליות</u>.

טענה 1.4. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבה אלגברית פשוטה, ויהי $\alpha\in\mathbb{E}$ כך ש-$\mathbb{E}=\mathbb{F}(\alpha)$; לכל שורש $\beta\in\mathbb{E}$ של m_α קיים $\sigma\in\operatorname{Gal}(\mathbb{E}/\mathbb{F})$ יחיד כך ש-$\sigma(\alpha)=\beta$.

הוכחה. היחידות נובעת מהעובדה שהיוצרים של הרחבה קובעים כל אוטומורפיזם, א״כ נוכיח את הקיום.
ראינו בעבר כי לכל $\beta\in\mathbb{E}$ מתקיים:

$$\mathbb{F}(\beta)=\left\{\left.\frac{P(\beta)}{Q(\beta)}\ \right|\ P,Q\in\mathbb{F},\ \ Q(\beta)\neq 0\ \right\}$$

כאשר פעולות החיבור והכפל מוגדרות כמו בשדה שברים[2]. בדיקה פשוטה מראה שההעתקה $\frac{P(\beta)}{Q(\beta)}\mapsto\frac{P(\alpha)}{Q(\alpha)}$ (עבור $\beta\in\mathbb{E}$ כלשהו) היא אנדומורפיזם[3] המשמר את $\mathbb{F}$ (אם היא מוגדרת); הבעיות היחידות שיכולות לצוץ הן שההעתקה אינה מוכרחת להיות חח״ע, וייתכן שקיים $Q\in\mathbb{F}[x]$ כך ש-$Q(\alpha)\neq 0$ ו-$Q(\beta)=0$ - שתי הבעיות הללו נפתרות אס״ם $m_\alpha=m_\beta$. ■

---

[1] לאו דווקא זה ש-$\mathbb{E}$ הוא שדה הפיצול שלו.

[2] כלומר:

$$\frac{P_1(\beta)}{Q_1(\beta)}+\frac{P_2(\beta)}{Q_2(\beta)}:=\frac{P_1(\beta)\cdot Q_2(\beta)+P_2(\beta)\cdot Q_1(\beta)}{Q_1(\beta)\cdot Q_2(\beta)}$$
$$\frac{P_1(\beta)}{Q_1(\beta)}\cdot\frac{P_2(\beta)}{Q_2(\beta)}:=\frac{P_1(\beta)\cdot P_2(\beta)}{Q_1(\beta)\cdot Q_2(\beta)}$$

[3] תזכורת: אנדומורפיזם הוא הומומורפיזם על (במקרה הזה על $\mathbb{F}(\beta)$).

משפט 1.5. יהי $\mathbb{K}$ שדה ביניים של הרחבת שדות $\mathbb{E}/\mathbb{F}$, אם לכל $\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ מתקיים $\sigma\left(\mathbb{K}\right) = \mathbb{K}$, אז מתקיים $\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \trianglelefteq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ ובנוסף $\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \cong \mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$.

הוכחה. נניח ש-$\sigma\left(\mathbb{K}\right) = \mathbb{K}$ לכל $\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ותהא $f : \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right) \to \mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$ פונקציה המוגדרת ע"י $f\left(\sigma\right) := \sigma|_{\mathbb{K}}$ לכל $\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$.[4]
נשים לב לכך ש-f היא הומומורפיזם של חבורות, שגרעינו הוא $\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)$ ותמונתו $\mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$. מכאן ש-$\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \trianglelefteq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ועפ"י משפט האיזומורפיזם הראשון מתקיים:

$$\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \cong \mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$$

■

מסקנה 1.6. יהי $\mathbb{K}$ שדה ביניים של הרחבת שדות $\mathbb{E}/\mathbb{F}$, אם $\mathbb{K}$ הוא שדה הפיצול של פולינום כלשהו ב-$\mathbb{F}\left[x\right]$ אז $\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \trianglelefteq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ ו-$\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right) \cong \mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$.

1.2 הרחבות רדיקליות

טענה 1.7. נניח שיש ב-$\mathbb{F}$ שורש יחידה פרימיטיבי מסדר $n \in \mathbb{N}$, ויהי $\zeta \in \mathbb{F}$ כנ"ל.
קבוצת שורשי היחידה מסדר n היא הקבוצה $\left\{\zeta^k \mid n \geq k \in \mathbb{N}\right\}$, וקבוצת שורשי היחידה הפרימיטיביים מסדר n היא הקבוצה $\left\{\zeta^k \mid n \geq k \in \mathbb{N},\ \gcd\left(n,k\right) = 1\right\}$.

♣ אנחנו רוצים לחקור הרחבות רדיקליות, ולשם כך נעסוק תחילה במקרה הכי פשוט של הרחבה כזו: $\mathbb{F}\left(\zeta\right)/\mathbb{F}$ כאשר ζ הוא שורש יחידה פרימיטיבי מסדר n.
כדי לחקור הרחבה כזו נרצה תחילה למצוא את הפולינום המינימלי של ζ כנ"ל, אנחנו יודעים שלכל $n \geq k \in \mathbb{N}$ מתקיים $\mathbb{F}\left(\zeta\right) = \mathbb{F}\left(\zeta^k\right)$ אם"ם $\gcd\left(n,k\right) = 1$, ולכן טבעי לנחש שהפולינום המינימלי של ζ הוא:

$$\prod_{\gcd(n,k)} \left(x - \zeta^k\right)$$

להכניס כאן פולינומים ציקלוטומיים?

סימון: לכל $a \in \mathbb{F}$ נסמן ב-$\sqrt[n]{a}$ שורש של הפולינום $x^n - a$, ונסמן ב-$\mathbb{F}\left(\sqrt[n]{a}\right)$ את ההרחבה הפשוטה.

♣ בכל פעם שנשתמש בסימון זה אנו טוענים בנוסף שכל מה שאמרנו נכון לכל שורש של $x^n - a$.

למה 1.8. $\mathrm{Hom}\left(\mathbb{E}\right)$ היא קבוצה בת"ל (כתת-קבוצה של מרחב הפונקציות $\mathbb{E}^{\mathbb{E}}$ מעל $\mathbb{E}$).

בכיתה ראינו את הלמה הזו עבור $\mathrm{Aut}\left(\mathbb{E}\right)$ בלבד.

♣ למעשה הדבר היחיד שמעניין אותנו הוא ש-$\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ בת"ל, אבל ההוכחה תופסת בכל $\mathrm{Hom}\left(\mathbb{E}\right)$, אז למה לא?

הוכחה. נניח בשלילה שזוהי קבוצה תלויה ליניארית, ויהיו $a_1, a_2, \ldots, a_m \in \mathbb{E}$ כך ש-$\sum_{i=1}^{m} a_i \cdot \sigma_i = 0$,[5] ו-$m$ הוא המספר הטבעי המינימלי שעבורו קיים צר"ל כזה.[6]
יהי $c \in \mathbb{E}$ כך ש-$\sigma_1\left(c\right) \neq \sigma_m\left(c\right)$, ונשים לב לכך שלכל $x \in \mathbb{E}$ מתקיים:

$$S_1 := \sum_{i=1}^{m} a_i \cdot \sigma_i\left(c\right) \cdot \sigma_i\left(x\right) = \sum_{i=1}^{m} a_i \cdot \sigma_i\left(cx\right) = 0$$

$$S_2 := \sum_{i=1}^{m} a_i \cdot \sigma_m\left(c\right) \cdot \sigma_i\left(x\right) = \sigma_m\left(c\right) \cdot \sum_{i=1}^{m} a_i \cdot \sigma_i\left(x\right) = 0$$

[4] מההנחה נובע ש-f אכן מוגדרת היטב.
[5] להוציא את 0.
[6] בפרט $a_i \neq 0$ לכל $m \geq i \in \mathbb{N}$.

וממילא גם:

$$\sum_{i=1}^{m-1} a_i \cdot (\sigma_m (c) - \sigma_i (c)) \cdot \sigma_i (x) = \sum_{i=1}^{m} a_i \cdot (\sigma_m (c) - \sigma_i (c)) \cdot \sigma_i (x) = S_2 - S_1 = 0$$

וזאת בסתירה להגדרת m, שכן ע"פ הגדרת c מתקיים $\sigma_m (c) - \sigma_1 (c) \neq 0$, וכפי שכבר הזכרנו $a_1 \neq 0$. ■

טענה 1.9. נניח שיש ב-$\mathbb{F}$ שורש יחידה פרימיטיבי מסדר $n \in \mathbb{N}$ וש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה (**לפי ההגדרה שלי: התאמות גלואה של $\mathbb{E}/\mathbb{F}$ הופכיות זו לזו**).

אם $\text{Gal}(\mathbb{E}/\mathbb{F})$ היא חבורה ציקלית מסדר n (כלומר $\mathbb{E}/\mathbb{F}$ היא הרחבה ציקלית), אז קיים $a \in \mathbb{F}$ כך ש-$\mathbb{E} = \mathbb{F}(\sqrt[n]{a})$.

♣ כמובן שטענה זו היא הסיבה שבגללה התחלנו להתעניין בהתאמות גלואה ובמקרים שבהם הן הופכיות זו לזו (כלומר בהרחבות גלואה).

הוכחה. יהי $\zeta \in \mathbb{F}$ שורש יחידה פרימיטיבי מסדר n, ויהי $\sigma \in \text{Gal}(\mathbb{E}/\mathbb{F})$ יוצר של $\text{Gal}(\mathbb{E}/\mathbb{F})$.
מהלמה (1.8) נובע שקיים $x \in \mathbb{E}$ כך ש-$\sum_{i=0}^{n-1} \zeta^i \cdot \sigma^i (x) \neq 0$, יהי x כנ"ל ונסמן $y := \sum_{i=0}^{n-1} \zeta^i \cdot \sigma^i (x)$.
מכאן שלכל $n \geq k \in \mathbb{N}$ מתקיים:

$$\sigma^k (y) = \sum_{i=0}^{n-1} \sigma^{i+k} (\zeta^i) \cdot \sigma^{i+k} (x) = \sum_{i=0}^{n-1} \zeta^i \cdot \sigma^{i+k} (x) = \zeta^{-k} \cdot \sum_{i=0}^{n-1} \zeta^{i+k} \cdot \sigma^{i+k} (x) = \zeta^{-k} \cdot \sum_{i=0}^{n-1} \zeta^i \cdot \sigma^i (x) = \zeta^{-k} \cdot y$$

מכאן ש-$\sigma^k (y) \neq y$ ו-$\sigma^k (y^n) = y^n$ לכל $n > k \in \mathbb{N}$, ולפיכך $y^n \in \mathcal{F}(\text{Gal}(\mathbb{E}/\mathbb{F}))$ ו-$\mathcal{G}(\mathbb{F}(y)) = \{\text{Id}\}$.
מהעובדה שהעתקות גלואה הופכיות זו לזו נובע כי:

$$y \in \mathcal{F}(\text{Gal}(\mathbb{E}/\mathbb{F})) = \mathcal{F}(\mathcal{G}(\mathbb{F})) = \mathbb{F}$$
$$\mathbb{F}(y) = \mathcal{F}(\mathcal{G}(\mathbb{F}(y))) = \mathcal{F}(\{\text{Id}\}) = \mathbb{E}$$

כלומר אם נסמן $a = y^n$ נקבל ש-$\mathbb{E} = (\sqrt[n]{a})$. ■

טענה 1.10. אם יש ב-$\mathbb{F}$ שורש יחידה פרימיטיבי מסדר $n \in \mathbb{N}$, אז לכל $a \in \mathbb{F}$, החבורה $\text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ היא חבורה ציקלית, ובנוסף מתקיים:

$$\left|\text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})\right| = \min\left\{ n \geq d \in \mathbb{N} \;\middle|\; (\sqrt[n]{a})^d \in \mathbb{F} \right\} = [\mathbb{F}(\sqrt[n]{a}) : \mathbb{F}]$$

♣ אנחנו נראה בהמשך שמהשוויון $\left|\text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})\right| = [\mathbb{F}(\sqrt[n]{a}) : \mathbb{F}]$ נובע ש-$\mathbb{F}(\sqrt[n]{a})/\mathbb{F}$ היא הרחבת גלואה.

הוכחה. נסמן:

$$m := \min\left\{ n \geq d \in \mathbb{N} \;\middle|\; (\sqrt[n]{a})^d \in \mathbb{F} \right\}$$

יהי $\zeta \in \mathbb{F}$ שורש יחידה פרימיטיבי מסדר $m \in \mathbb{N}$, נשים לב לכך שלכל $m \geq k \in \mathbb{N}$ מתקיים $(\sqrt[n]{a} \cdot \zeta^k)^m - a = 0$, ולכן מהלמה (1.1) נובע שלכל $\sigma \in \text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ קיים $m \geq k \in \mathbb{N}$ יחיד כך ש-$\sigma(\sqrt[n]{a}) = \sqrt[n]{a} \cdot \zeta^k$; א"כ תהא $f : \text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F}) \to \mathbb{Z}_m$ פונקציה המחזירה לכל $\sigma \in \text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ את אותו k יחיד.
מכיוון ש-$\mathbb{F}(\sqrt[n]{a})/\mathbb{F}$ היא הרחבה פשוטה ש-$\sqrt[n]{a}$ הוא יוצר שלה, נדע גם שלא קיימים $\sigma, \tau \in \text{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ כך ש-$\sigma \neq \tau$ ו-$\sigma(\sqrt[n]{a}) = \tau(\sqrt[n]{a})$, כלומר f חח"ע.
כעת נשים לב לכך ש-f היא גם הומומורפיזם של חבורות, כלומר f הוא שיכון של $\text{Gal}(\mathbb{E}/\mathbb{F})$ ב-$\mathbb{Z}_m$, ומכאן ש-$\text{Gal}(\mathbb{E}/\mathbb{F})$ היא חבורה ציקלית ו-$|\text{Gal}(\mathbb{E}/\mathbb{F})| \leq m$.
מצד שני לכל $m \geq d, e \in \mathbb{N}$ מתקיים $d = e \iff \zeta^d = \zeta^e \iff \sqrt[n]{a} \cdot \zeta^d = \sqrt[n]{a} \cdot \zeta^e$, ולכן מהטענה הקודמת (1.4) ומהעובדה ש-$(\sqrt[n]{a} \cdot \zeta^k)^m - a = 0$ לכל $m \geq k \in \mathbb{N}$ נובע ש-$|\text{Gal}(\mathbb{E}/\mathbb{F})| \geq m$.
העובדה ש-$[\mathbb{F}(\sqrt[n]{a}) : \mathbb{F}] = m$ נובעת מהיות $\left\{ (\sqrt[n]{a})^k \;\middle|\; m \geq k \in \mathbb{N} \right\}$ בסיס של $\mathbb{F}(\sqrt[n]{a})$ מעל $\mathbb{F}$. ■

מסקנה 1.11. נניח שיש ב-$\mathbb{F}$ שורש יחידה פרימיטיבי מסדר $n \in \mathbb{N}$ וש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה (**לפי ההגדרה שלי: התאמות גלואה של $\mathbb{E}/\mathbb{F}$ הופכיות זו לזו**). $\mathbb{E}/\mathbb{F}$ היא הרחבה ציקלית אם"ם קיימים $a \in \mathbb{F}$ ו-$n \in \mathbb{N}$ כך ש-$\mathbb{E} = \mathbb{F}(\sqrt[n]{a})$, ובמקרה כזה $|\text{Gal}(\mathbb{E}/\mathbb{F})| = n$ (כלומר $\text{Gal}(\mathbb{E}/\mathbb{F}) \cong \mathbb{Z}_n$).

משפט 1.12. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה (**לפי ההגדרה שלי: התאמות גלואה של $\mathbb{E}/\mathbb{F}$ הופכיות זו לזו**), ויהי $\mathbb{K}$ שדה ביניים של $\mathbb{E}/\mathbb{F}$.
מתקיים $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \trianglelefteq \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ אם"ם לכל $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ מתקיים $\sigma(\mathbb{K}) = \mathbb{K}$, ובמקרה כזה מתקיים גם $\mathrm{Gal}(\mathbb{E}/\mathbb{F})/\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

הוכחה.

- $\Leftarrow$
נניח שקיים $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ כך ש-$\sigma(\mathbb{K}) \neq \mathbb{K}$, ויהיו $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ ו-$k \in \mathbb{K}$ כך ש-$\sigma(k) \notin \mathbb{K}$.[7]
מהיות $\mathbb{E}/\mathbb{F}$ הרחבת גלואה נובע ששדה השבת של $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ הוא בדיוק $\mathbb{K}$,[8] כלומר קיים $\tau \in \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ כך ש-$\tau(\sigma(k)) \neq \sigma(k)$, יהי τ כנ"ל.
$$\Rightarrow \left(\sigma^{-1} \circ \tau \circ \sigma\right)(k) = \sigma^{-1}(\tau(\sigma(k))) \neq \sigma^{-1}(\sigma(k)) = k$$
$$\Rightarrow \sigma^{-1} \circ \tau \circ \sigma \notin \mathrm{Gal}(\mathbb{E}/\mathbb{K})$$
ומכאן ש-$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \ntrianglelefteq \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. הוכחנו שאם קיים $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ כך ש-$\sigma(\mathbb{K}) \neq \mathbb{K}$ אז $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \ntrianglelefteq \mathrm{Gal}(\mathbb{E}/\mathbb{K})$, ולכן אם $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \trianglelefteq \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ אז לכל $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ מתקיים $\sigma(\mathbb{K}) = \mathbb{K}$.

- $\Rightarrow$
מקרה פרטי של משפט 1.5.

■

משפט 1.13. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה רדיקלית, ויהיו $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{E}$ ו-$n_1, n_2, \ldots, n_r \in \mathbb{N}$ כך ש-$\mathbb{E} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ ו-$(\alpha_i)^{n_i} \in \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ לכל $r \geq i \in \mathbb{N}$.
נסמן $N := \mathrm{lcm}(n_1, n_2, \ldots, n_r)$; אם קיים שדה Ω המרחיב את $\mathbb{F}$ שבו יש שורש יחידה פרימיטיבי מסדר N, אז $\mathbb{E}/\mathbb{F}$ היא הרחבה פתירה.

הוכחה. יהי Ω שדה הרחבה של $\mathbb{F}$ כך שקיים $\zeta \in \Omega$ המהווה שורש יחידה פרימיטיבי מסדר N, ויהי $\zeta \in \Omega$ כנ"ל.
נסמן $\mathbb{K} := \mathbb{F}(\zeta)$ ו-$\mathbb{L} := \mathbb{E}(\zeta)$ (א"כ $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r, \zeta)$).

- ראשית נוכיח ש-$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ היא חבורה פתירה.
נסמן $\mathbb{K}_i := \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_i)$ ו-$\beta_i := (\alpha_i)^{n_i}$ לכל $r \geq i \in \mathbb{N}$, כמו כן נסמן $\mathbb{K}_0 := \mathbb{K}$.
מהגדרת N, ומהעובדה שיש ב-$\mathbb{K}$ שורש פרימיטיבי מסדר N, נובע שלכל $r \geq i \in \mathbb{N}$ ולכל $i \geq j \in \mathbb{N}$, הפולינום $x^{n_j} - \beta_j$ מתפצל ב-$\mathbb{K}_i$.
מכאן שע"פ למה 1.1: לכל $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, לכל $r \geq i \in \mathbb{N}$ ולכל $i \geq j \in \mathbb{N}$, מתקיים $\sigma(\alpha_j) \in \mathbb{K}_i$, ולכן גם $\sigma(\mathbb{K}_i) = \mathbb{K}_i$.
ממשפט 1.5 נקבל שלכל $r \geq i \in \mathbb{N}$, מתקיים:
$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}_i) \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$
$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}_{i-1})/\mathrm{Gal}(\mathbb{L}/\mathbb{K}_i) \cong \mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i-1})$$
ומכיוון שע"פ טענה 1.10 החבורה $\mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i-1})$ היא חבורה ציקלית לכל $r \geq i \in \mathbb{N}$, נדע של-$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ יש סדרה נורמלית בעלת גורמים ציקליים, כלומר $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ פתירה.

- כעת נוכיח ש-$\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ היא חבורה פתירה.
ע"פ למה 1.1 לכל $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ מתקיים $\sigma(\mathbb{K}) = \mathbb{K}$,[9] ולכן ממשפט 1.5 נקבל ש-$\mathrm{Gal}(\mathbb{L}/\mathbb{F}) \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ ו-$\mathrm{Gal}(\mathbb{L}/\mathbb{F})/\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{K}/\mathbb{F})$, מכאן שאם נצליח להוכיח ש-$\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ פתירה הרי שבכך נוכיח כי $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ פתירה. ואמנם, ההרחבה $\mathbb{K}/\mathbb{F}$ היא הרחבה ציקלוטומית ולכן $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ היא חבורה אבלית (**צריך להוכיח זאת**) ובפרט פתירה.

---

[7] מהיות σ אוטומורפיזם נובע ש-$[\sigma(\mathbb{K}) : \mathbb{F}] = [\mathbb{K} : \mathbb{F}]$, ולכן אם $\sigma(\mathbb{K}) \neq \mathbb{K}$ אז $\sigma(\mathbb{K}) \nsubseteq \mathbb{K}$.
[8] $\mathbb{K} = \mathcal{F}(\mathcal{G}(\mathbb{K})) = \mathcal{F}(\mathrm{Gal}(\mathbb{E}/\mathbb{K})) = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{K})}$.
[9] $\sigma(\zeta)$ מוכרח להיות שורש של הפולינום $x^N - 1$, ומצד שני הוא מוכרח להיות יוצר של חבורת שורשי הפולינום, כלומר שורש פרימיטיבי.

- לבסוף נוכיח שההרחבה $\mathbb{E}/\mathbb{F}$ פתירה.
$\mathbb{E}$ הוא שדה הפיצול של הפולינום $\prod_{i=1}^{r}(x-\alpha_i)$, ולכן ע״פ מסקנה 1.6 מתקיים $\text{Gal}(\mathbb{L}/\mathbb{F}) \trianglelefteq \text{Gal}(\mathbb{L}/\mathbb{E})$ וגם $\text{Gal}(\mathbb{L}/\mathbb{F})/\text{Gal}(\mathbb{L}/\mathbb{E}) \cong \text{Gal}(\mathbb{E}/\mathbb{F})$.
כזכור הוכחנו בשלב הקודם של ההוכחה ש-$\text{Gal}(\mathbb{L}/\mathbb{F})$ פתירה, ולפיכך נובע מהשורה הקודמת ש-$\text{Gal}(\mathbb{E}/\mathbb{F})$ פתירה.

■

למה 1.14. נניח ש-$\mathbb{E}$ הוא שדה הפיצול של פולינום מהצורה $x^n - a$ עבור $a \in \mathbb{F}$ ו-$n \in \mathbb{N}$.
אם יש ב-$\mathbb{E}$ שורש יחידה פרימיטיבי מסדר n, אז $\mathbb{E}/\mathbb{F}$ היא הרחבה פתירה.

איפה אנחנו משתמשים בלמה הזו???

הוכחה. נניח שב-$\mathbb{E}$ יש שורש יחידה פרימיטיבי מסדר $n \in \mathbb{N}$, וקיים $a \in \mathbb{F}$ כך ש-$\mathbb{E}$ הוא שדה הפיצול של הפולינום $x^n - a$.
יהי $a \in \mathbb{F}$ כנ״ל, יהי $\zeta \in \mathbb{E}$ שורש יחידה פרימיטיבי מסדר n, ונסמן $\mathbb{K} := \mathbb{F}(\zeta)$, א״כ החבורה $\text{Gal}(\mathbb{E}/\mathbb{K})$ היא חבורה ציקלית (טענה 1.9).
$\mathbb{K}$ הוא שדה הפיצול של הפולינום $x^n - 1$, ולכן ע״פ המסקנה (1.6) מתקיים $\text{Gal}(\mathbb{E}/\mathbb{K}) \trianglelefteq \text{Gal}(\mathbb{E}/\mathbb{F})$ ו-$\text{Gal}(\mathbb{K}/\mathbb{F}) \cong \text{Gal}(\mathbb{E}/\mathbb{F})/\text{Gal}(\mathbb{E}/\mathbb{K})$, מכאן שאם נצליח להוכיח ש-$\text{Gal}(\mathbb{K}/\mathbb{F})$ פתירה נוכיח בזה שגם $\text{Gal}(\mathbb{E}/\mathbb{F})$ פתירה. ואכן, ההרחבה $\mathbb{K}/\mathbb{F}$ היא הרחבה ציקלוטומית ולכן $\text{Gal}(\mathbb{K}/\mathbb{F})$ היא חבורה אבלית (**צריך להוכיח זאת**) ובפרט פתירה. ■

משפט 1.15. נניח ש-$\mathbb{E}$ הוא שדה הפיצול של פולינום $f \in \mathbb{F}[x]$, ונניח שקיים שדה Ω המרחיב את $\mathbb{F}$ שבו יש שורש יחידה פרימיטיבי מסדר $[\mathbb{E}:\mathbb{F}]$.
f ניתן לפתרון באמצעות רדיקלים אס״ם f פתיר (כלומר חבורת גלואה שלו פתירה).

♣ כמובן שהמשפט הזה הוא הסיבה לכך שאנחנו קוראים לחבורות פתירות בשם זה.

1.3 התאמות גלואה

טענה 1.16. לכל שתי תתי-חבורות $H_1, H_2 \leqslant \text{Gal}(\mathbb{E}/\mathbb{F})$ כך ש-$H_2 \leqslant H_1$ מתקיים $\mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$, וכמו כן לכל שני שדות ביניים $\mathbb{K}_1, \mathbb{K}_2 \subseteq \mathbb{E}$ של ההרחבה $\mathbb{E}/\mathbb{F}$ כך ש-$\mathbb{K}_2 \subseteq \mathbb{K}_1$ מתקיים $\mathcal{G}(\mathbb{K}_1) \supseteq \mathcal{G}(\mathbb{K}_2)$.

טענה 1.17. לכל תת-חבורה $H \leqslant \text{Gal}(\mathbb{E}/\mathbb{F})$ מתקיים $H \subseteq \mathcal{G}(\mathcal{F}(H))$, ולכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\mathbb{K} \subseteq \mathcal{F}(\mathcal{G}(\mathbb{K}))$.

♣ אנחנו נראה בהמשך שאם H סופית אז $H = \mathcal{G}(\mathcal{F}(H))$, אך לעומת זאת לא תמיד מתקיים $\mathbb{K} = \mathcal{F}(\mathcal{G}(\mathbb{K}))$.

להביא דוגמה לכך שלא בהכרח מתקיים שוויון $\mathbb{K} \subseteq \mathcal{F}(\mathcal{G}(\mathbb{K}))$.

משפט 1.18. תהא $H \leqslant \text{Gal}(\mathbb{E}/\mathbb{F})$ תת-חבורה סופית, מתקיים $|H| = [\mathbb{E}:\mathcal{F}(H)]$ (בפרט $\mathbb{E}$ נוצר סופית כמרחב וקטורי מעל $\mathcal{F}(H)$).

הוכחה. יהיו $\sigma_1, \sigma_2, \ldots, \sigma_m$ כל האוטומורפיזמים השונים ב-H, ותהא $(a_1, a_2, \ldots, a_n)$ סדרה בת״ל ב-$\mathbb{E}$ כמ״ו מעל $\mathcal{F}(H)$ (כאשר אם $\mathbb{E}$ נ״ס כמ״ו מעל $\mathcal{F}(H)$ אזי נדרוש ש-$n = [\mathbb{E}:\mathcal{F}(H)]$). נתבונן במטריצה:

$$A := \begin{bmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \cdots & \sigma_1(a_n) \\ \sigma_2(a_1) & \sigma_2(a_2) & \cdots & \sigma_2(a_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(a_1) & \sigma_m(a_2) & \cdots & \sigma_m(a_n) \end{bmatrix}$$

- נניח בשלילה ש-$m < n$, מכאן שהעמודות של A תלויות ליניארית מעל $\mathbb{E}$. נסמן ב-r את הטבעי המינימלי שעבורו כל r עמודות מבין $r+1$ העמודות הראשונות הן בת״ל מעל $\mathbb{E}$.
יהיו $x_1, x_2, \ldots, x_{r+1} \in \mathbb{E}$ שכולם שונים מ-0 ו-$x_{r+1} = 1$, כך שמתקיים (לכל $m \geq i \in \mathbb{N}$):

$$\sum_{j=1}^{r+1} x_j \cdot \sigma_i(a_j) = 0$$

מהמינימליות של r נובע שאכן קיימים $x_1, x_2, \ldots, x_{r+1}$ כאלה.

יהי $m \geq k \in \mathbb{N}$, לכל $m \geq i \in \mathbb{N}$ קיים $m \geq l \in \mathbb{N}$ יחיד כך שמתקיים:

$$0 = \sum_{j=1}^{r+1} \sigma_k(x_j) \cdot (\sigma_k \circ \sigma_i)(a_j) = \sum_{j=1}^{r+1} \sigma_k(x_j) \cdot \sigma_l(a_j)$$

שכן הרכבת σ_k היא תמורה על $\mathrm{Gal}\left(\mathbb{E}/\mathcal{F}(H)\right)$. מכאן שלכל $m \geq i \in \mathbb{N}$ מתקיים:

$$\sum_{j=1}^{r+1} \sigma_k(x_j) \cdot \sigma_i(a_j) = 0$$

וממילא גם:

$$\begin{aligned} 0 &= \sum_{j=1}^{r+1} (\sigma_k(x_j) - x_j) \cdot \sigma_i(a_j) = \sum_{j=1}^{r} (\sigma_k(x_j) - x_j) \cdot \sigma_i(a_j) + (\sigma_k(1) - 1) \cdot \sigma_i(a_j) \\ &= \sum_{j=1}^{r} (\sigma_k(x_j) - x_j) \cdot \sigma_i(a_j) + (1-1) \cdot \sigma_i(a_j) = \sum_{j=1}^{r} (\sigma_k(x_j) - x_j) \cdot \sigma_i(a_j) \end{aligned}$$

ולכן מההנחה ש-r העמודות הראשונות של A בת"ל נובע ש-$\sigma_k(x_j) = x_j$ לכל $r \geq j \in \mathbb{N}$.
k הנ"ל היה שרירותי, ולכן לכל $\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathcal{F}(H)\right)$ ולכל $r \geq j \in \mathbb{N}$ מתקיים $\sigma(x_j) = x_j$, כלומר $x_1, x_2, \ldots, x_r \in \mathcal{F}(H)$.
אבל $\mathrm{Id}_{\mathbb{E}} \in \mathrm{Gal}\left(\mathbb{E}/\mathcal{F}(H)\right)$ ולכן:

$$0 = \sum_{j=1}^{r+1} x_j \cdot \mathrm{Id}_{\mathbb{E}}(a_j) = \sum_{j=1}^{r+1} x_j \cdot a_j$$

בסתירה לכך ש-$(a_1, a_2, \ldots, a_n)$ היא סדרה בת"ל ו-$x_1 \neq 0$, מכאן שהנחת השלילה אינה נכונה ומתקיים $n \leq m$.

- יהי $y \in \mathbb{E}^m$ כך ש-$A^t \cdot y = 0$, מכאן שלכל $n \geq j \in \mathbb{N}$ מתקיים:

$$\sum_{i=1}^{m} y_i \cdot \sigma_i(a_j) = 0$$

כעת יהי $v \in \mathbb{E}$, ויהיו $c_1, c_2, \ldots, c_n \in \mathcal{F}(H)$ כך ש-$v = \sum_{j=1}^{n} c_j \cdot a_j$ (ראינו ש-$(a_1, a_2, \ldots, a_n)$ בסיס).

$$\begin{aligned} \Rightarrow \sum_{i=1}^{m} y_i \cdot \sigma_i(v) &= \sum_{i=1}^{m} y_i \cdot \sigma_i\left(\sum_{j=1}^{n} c_j \cdot a_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} \cdot y_i \cdot \sigma_i(c_j) \cdot \sigma_k(a_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} y_i \cdot c_j \cdot \sigma_k(a_j) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m} y_i \cdot c_j \cdot \sigma_k(a_j) = \sum_{j=1}^{n} c_j \cdot \sum_{i=1}^{m} y_i \cdot \sigma_k(a_j) = \sum_{j=1}^{n} c_j \cdot 0 = 0 \end{aligned}$$

מהיות v שרירותי נובע כי $\sum_{i=1}^{m} y_i \cdot \sigma_i = 0$, ולכן מלמה 1.8 נובע ש-$y = 0$.
מכאן שהשורות של A בת"ל ובפרט $m \geq n$.

■

נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבה סופית.

מסקנה 1.19. מתקיימים ארבעת הפסוקים הבאים:

1. $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| \leq [\mathbb{E}:\mathbb{F}]$.
2. $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = [\mathbb{E}:\mathbb{F}]$ אם"ם $\mathbb{F} = \mathcal{F}\left(\mathcal{G}\left(\mathbb{F}\right)\right)$.
3. לכל תת-חבורה $H \leq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ מתקיים $H = \mathcal{G}\left(\mathcal{F}\left(H\right)\right)$.
4. $\mathcal{F}$ חח"ע ו-$\mathcal{G}$ על.

♣ א"כ יש לנו כיוון כיצד לענות על השאלה שלנו: כדי ש-$\mathcal{F}$ ו-$\mathcal{G}$ תהיינה הופכיות זו לזו אנחנו צריכים למצוא מתי מתקיים $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = [\mathbb{E}:\mathbb{K}]$ לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$.

את סעיף 3 (ואת סעיף 4 הנובע ממנו) ראינו רק במקרה שבו $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה, וזאת למרות שהוא נכון לכל הרחבה.

♣ לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$, המקיים את תנאי משפט 1.5, מתקיים:
$$\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = \left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| \cdot \left|\mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)\right|$$
לו היה הדבר נכון לכל שדה ביניים היינו יכולים להוכיח שאם $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = [\mathbb{E}:\mathbb{F}]$ אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = [\mathbb{E}:\mathbb{K}]$.
אלא שלא תמיד מתקיימים תנאי המשפט, ולכן הדבר היחיד שאנחנו יכולים לומר הוא שאם $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = [\mathbb{E}:\mathbb{F}]$, אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים[10]:
$$\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = \left|\left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E} \mid \sigma\mid_{\mathbb{F}} = \mathrm{Id}_{\mathbb{F}}\right\}\right|$$
למרות זאת, במשפט הבא אנחנו נראה שאמירה זו מספיקה כדי להוכיח את השוויון המבוקש לכל שדה ביניים.

משפט 1.20. אם $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = [\mathbb{E}:\mathbb{F}]$, אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = [\mathbb{E}:\mathbb{K}]$.

ראינו את המשפט הזה בשלב מאוחר מאוד של הקורס, ואת ההוכחה שאביא כעת לא ראינו כלל.

הוכחה. נניח ש-$\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = [\mathbb{E}:\mathbb{F}]$ ונסמן $I := \left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E} \mid \sigma\mid_{\mathbb{F}} = \mathrm{Id}_{\mathbb{F}}\right\}$.
$$\Rightarrow |I| = \left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = \frac{\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|}{\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|} = \frac{[\mathbb{E}:\mathbb{F}]}{\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|}$$
ולכן גם:
$$\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = \frac{[\mathbb{E}:\mathbb{F}]}{|I|} = \frac{[\mathbb{E}:\mathbb{K}]\cdot[\mathbb{K}:\mathbb{F}]}{|I|}$$
וע"פ המסקנה האחרונה (1.19) נקבל:
$$\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = [\mathbb{E}:\mathbb{K}] \iff \left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| \geq [\mathbb{E}:\mathbb{K}] \iff |I| \geq [\mathbb{K}:\mathbb{F}]$$
א"כ נוכיח ש-$|I| \geq [\mathbb{K}:\mathbb{F}]$.
יהי $(a_1,a_2,\ldots,a_l)$ בסיס של $\mathbb{K}$ כמ"ו מעל $\mathbb{F}$, ויהיו $b_1,b_2,\ldots,b_k \in \mathbb{E}$ כך ש-$(a_1,a_2,\ldots,a_l;b_1,b_2,\ldots,b_k)$ בסיס של $\mathbb{E}$ כמ"ו מעל $\mathbb{F}$.

---

[10] ההעתקה $\sigma \mapsto \sigma|_{\mathbb{K}}$ מוגדרת היטב על קבוצת המחלקות $\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)$, היא חח"ע, ותמונתה היא $\left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E} \mid \sigma\mid_{\mathbb{F}} = \mathrm{Id}_{\mathbb{F}}\right\}$.

נסמן $n:=l+k=[\mathbb{E}:\mathbb{F}]$, יהיו $\sigma_1,\sigma_2,\ldots,\sigma_m$ כל האוטומורפיזמים השונים ב-$\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ונסמן:

$$A:=\left[\begin{array}{ccc|ccc}\sigma_1(a_1) & \cdots & \sigma_1(a_l) & \sigma_1(b_1) & \cdots & \sigma_1(b_k)\\ \sigma_2(a_1) & \cdots & \sigma_2(a_l) & \sigma_2(b_1) & \cdots & \sigma_2(b_k)\\ \sigma_3(a_1) & \cdots & \sigma_3(a_l) & \sigma_3(b_1) & \cdots & \sigma_3(b_k)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ \sigma_m(a_1) & \cdots & \sigma_m(a_l) & \sigma_m(b_1) & \cdots & \sigma_m(b_k)\end{array}\right]$$

מהעובדה ש-$a_i\in\mathbb{K}$ לכל $l\geq i\in\mathbb{N}$, ומהעובדה שכל איבר ב-I הוא צמצום של איבר $\sigma\in\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ ל-$\mathbb{K}$, נובע שניתן לבצע פעולות שורה אלמנטריות על A, ולקבל בבלוק השמאלי בדיוק $|I|$ שורות שאינן שורות אפסים.

אבל כפי שראינו בהוכחה של משפט 1.18 A היא מטריצה הפיכה, ולכן גם כל מטריצה שמתקבלת ממנה ע״י פעולות שורה אלמנטריות גם היא הפיכה, ומכאן שבהכרח מספר העמודות בבלוק השמאלי קטן או שווה למספר השורות שאינן שורות אפסים בבלוק זה, כלומר $[\mathbb{K}:\mathbb{F}]=l\leq|I|$ כנדרש. ■

מסקנה 1.21. $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אס״ם $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=[\mathbb{E}:\mathbb{F}]$.

מסקנה 1.22. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבה אלגברית פשוטה, ויהי $\alpha\in\mathbb{E}$ כך ש-$\mathbb{E}=\mathbb{F}(\alpha)$.
$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אס״ם m_α מתפצל ב-$\mathbb{E}$ לגורמים ליניאריים שונים.

2 הרחבות ספרביליות והרחבות נורמליות

תהא $\mathbb{E}/\mathbb{F}$ הרחבת שדות סופית, יהי Ω שדה סגור אלגברית, ויהי $\varphi:\mathbb{F}\hookrightarrow\Omega$ שיכון.

2.1 הרחבות ספרביליות

למה 2.1. לכל $\alpha\in\Omega$, מספר השורשים השונים של $\varphi(m_\alpha)$ ב-Ω הוא $i_{\varphi,\Omega}\left(\mathbb{F}(\alpha)/\mathbb{F}\right)$.

♣ בפרט עבור $\varphi=\text{Id}$ נקבל ש-$i_{\varphi,\Omega}\left(\mathbb{F}(\alpha)/\mathbb{F}\right)$ שווה למספר השורשים השונים של m_α.

למה 2.2. יהיו Ω_1 ו-Ω_2 שדות סגורים אלגברית, ויהיו $\varphi_1:\mathbb{F}\hookrightarrow\Omega_1$ ו-$\varphi_2:\mathbb{F}\hookrightarrow\Omega_2$ שיכונים.
לכל פולינום $f\in\mathbb{F}[x]$, מספר השורשים השונים של $\varphi_1(f)$ ב-Ω_1 שווה למספר השורשים השונים של $\varphi_2(f)$ ב-Ω_2.

משפט 2.3. יהיו Ω_1 ו-Ω_2 שדות סגורים אלגברית, ויהיו $\varphi_1:\mathbb{F}\hookrightarrow\Omega_1$ ו-$\varphi_2:\mathbb{F}\hookrightarrow\Omega_2$ שיכונים, מתקיימים שלושת הפסוקים הבאים:

1. $i_{\varphi_1,\Omega_1}\left(\mathbb{E}/\mathbb{F}\right)=i_{\varphi_2,\Omega_2}\left(\mathbb{E}/\mathbb{F}\right)$
2. $i_{\varphi_1,\Omega_1}\left(\mathbb{E}/\mathbb{F}\right)\geq 1$
3. לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $i_{\varphi_1,\Omega_1}\left(\mathbb{E}/\mathbb{F}\right)=i_{\varphi_1,\Omega_1}\left(\mathbb{E}/\mathbb{K}\right)\cdot i_{\varphi_1,\Omega_1}\left(\mathbb{K}/\mathbb{F}\right)$.

סימון: לכל הרחבה סופית $\mathbb{E}/\mathbb{F}$ נסמן $i\left(\mathbb{E}/\mathbb{F}\right):=i_{\varphi,\Omega}\left(\mathbb{E}/\mathbb{F}\right)$ עבור שדה סגור אלגברית Ω ושיכון $\varphi:\mathbb{F}\hookrightarrow\Omega$, ונקרא ל-$i\left(\mathbb{E}/\mathbb{F}\right)$ דרגת הספרביליות של ההרחבה $\mathbb{E}/\mathbb{F}$.

♣ דרגת הספרביליות נקראת כך משום שהיא מודדת עד כמה כל הרחבה פשוטה ב״מגדל״ ההרחבות שיוצר את $\mathbb{E}/\mathbb{F}$ היא ספרבילית (כמה שורשים שונים יש לפולינום המינימלי של יוצר ההרחבה).

משפט 2.4. יחידות שדה הפיצול

יהי $f\in\mathbb{F}[x]$ ויהיו $\mathbb{E}_1$ ו-$\mathbb{E}_2$ שדות פיצול של f, מתקיים $\mathbb{E}_1\cong\mathbb{E}_2$; כלומר שדה פיצול של פולינום הוא יחיד עד כדי איזומורפיזם.

משפט 2.5. לכל הרחבה סופית $\mathbb{E}/\mathbb{F}$ מתקיים $i\left(\mathbb{E}/\mathbb{F}\right)\le\left[\mathbb{E}:\mathbb{F}\right]$, ובנוסף מתקיים $i\left(\mathbb{E}/\mathbb{F}\right)=\left[\mathbb{E}:\mathbb{F}\right]$ אס״ם ההרחבה $\mathbb{E}/\mathbb{F}$ ספרבילית.

מסקנה 2.6. תהיינה $\mathbb{K}/\mathbb{F}$ ו-$\mathbb{E}/\mathbb{K}$ הרחבות סופיות, $\mathbb{E}/\mathbb{F}$ ספרבילית אס״ם $\mathbb{K}/\mathbb{F}$ ו-$\mathbb{E}/\mathbb{K}$ ספרביליות.

מסקנה 2.7. יהיו $f\in\mathbb{F}\left[x\right]$ פולינום ו-$\mathbb{E}$ שדה פיצול של f, אם f ספרבילי אז גם ההרחבה $\mathbb{E}/\mathbb{F}$ ספרבילית.

טענה 2.8. תהא $\mathbb{E}/\mathbb{F}$ הרחבה סופית, התנאים הבאים שקולים:

1. $\mathbb{E}/\mathbb{F}$ היא הרחבה ספרבילית.
2. לכל קבוצת יוצרים של $\mathbb{E}$ מעל $\mathbb{F}$ - כל איבריה ספרביליים מעל $\mathbb{F}$.
3. קיימת קבוצת יוצרים של $\mathbb{E}$ מעל $\mathbb{F}$ שכל איבריה ספרביליים מעל $\mathbb{F}$.

2.2 הרחבות נורמליות

טענה 2.9. יהי $\mathbb{K}$ שדה ביניים של $\mathbb{E}/\mathbb{F}$, אם $\mathbb{K}/\mathbb{F}$ היא הרחבה נורמלית אז לכל $\sigma\in\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ מתקיים $\sigma\left(\mathbb{K}\right)=\mathbb{K}$, וע״פ משפט 1.5 מתקיים גם $\text{Gal}\left(\mathbb{K}/\mathbb{F}\right)\cong\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)$.

טענה 2.10. מתקיים $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|\le i\left(\mathbb{E}/\mathbb{F}\right)$; ובנוסף, מתקיים $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=i\left(\mathbb{E}/\mathbb{F}\right)$ אס״ם לכל שדה סגור אלגברית Ω המכיל את $\mathbb{E}$, ולכל שיכון $\tau:\mathbb{E}\hookrightarrow\Omega$, מתקיים $\tau\left(\mathbb{E}\right)=\mathbb{E}$.

משפט 2.11. התנאים הבאים שקולים:

1. $\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית.
2. $\mathbb{E}$ הוא שדה פיצול של פולינום $f\in\mathbb{F}\left[x\right]$ כלשהו.
3. $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=i\left(\mathbb{E}/\mathbb{F}\right)$.

מסקנה 2.12. יהי $\mathbb{K}$ שדה ביניים, $\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית אס״ם גם $\mathbb{E}/\mathbb{K}$ נורמלית.

♣ נשים לב: בניגוד לספרביליות לא מתקיים כאן שאם $\mathbb{E}/\mathbb{K}$ ו-$\mathbb{K}/\mathbb{F}$ נורמליות אז $\mathbb{E}/\mathbb{F}$ נורמלית. לדוגמה: ההרחבות $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ו-$\mathbb{Q}(\sqrt{2},\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ הן הרחבות נורמלית שכן $\mathbb{Q}\left(\sqrt{2}\right)$ הוא שדה הפיצול של x^2-2 ו-$\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right)$ הוא שדה הפיצול של $x^2-\sqrt{2}$, אבל למרות זאת ההרחבה $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})/\mathbb{Q}$ אינה נורמלית שכן לפולינום x^4-2 יש שורש ב-$\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right)$ אך הוא אינו מתפצל ב-$\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2}\right)$.

3 הרחבות גלואה

תהא $\mathbb{E}/\mathbb{F}$ הרחבת שדות.

3.1 המשפט היסודי של תורת גלואה

למה 3.1. לכל $H \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{H}\right)$ ו-$\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathbb{H}\right)$ מתקיים $\sigma\left(\mathcal{F}\left(H\right)\right) = \mathcal{F}\left(\sigma H \sigma^{-1}\right)$.

למה 3.2. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה ויהי $\mathbb{K}$ שדה ביניים של $\mathbb{E}/\mathbb{F}$, ההרחבה $\mathbb{K}/\mathbb{F}$ היא הרחבת גלואה אס"ם $\sigma\left(\mathbb{K}\right) = \mathbb{K}$ לכל $\sigma \in \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ובמקרה כזה מתקיים $\mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right) \cong {}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}/_{\mathrm{Gal}(\mathbb{E}/\mathbb{K})}$.

משפט 3.3. המשפט היסודי של תורת גלואה

- נניח ש-$\mathbb{E}/\mathbb{F}$ סופית, התנאים הבאים שקולים:

1. $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה (**לפי ההגדרה שלי: $\mathcal{F}$ ו-$\mathcal{G}$ הופכיות זו לזו**).
2. $\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית וספרבילית (**זו ההגדרה שראינו בכיתה לכך ש-$\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה**).
3. $\mathbb{E}$ הוא שדה פיצול של פולינום ספרבילי $f \in \mathbb{F}\left[x\right]$ כלשהו.
4. $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = \left[\mathbb{E} : \mathbb{F}\right]$.
5. לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left|\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = \left[\mathbb{E} : \mathbb{K}\right]$.

- בנוסף, אם $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אז מתקיים:

1. לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\mathcal{G}\left(\mathbb{K}\right) \trianglelefteq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ ($\mathcal{G}\left(\mathbb{K}\right)$ נורמלית) אס"ם $\mathbb{K}/\mathbb{F}$ היא הרחבה נורמלית, ובמקרה כזה מתקיים גם:
$$ {}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}/_{\mathrm{Gal}(\mathbb{E}/\mathbb{K})} \cong \mathrm{Gal}\left(\mathbb{K}/\mathbb{F}\right)$$
2. לכל תת-חבורה $H \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ מתקיים $H \trianglelefteq \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ (H נורמלית) אס"ם $\mathcal{F}(H)/\mathbb{F}$ היא הרחבה נורמלית, ובמקרה כזה מתקיים גם:
$$ {}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}/_{\mathrm{Gal}(\mathbb{E}/\mathcal{F}(H))} \cong \mathrm{Gal}\left(\mathcal{F}(H)/\mathbb{F}\right)$$

לא ראינו את השקילות של סעיפים 1 ו-5 לסעיפים האחרים (לפחות לא באופן מפורש), אלא ראינו רק שסעיפים 2-4 (ששקולים זה לזה) גוררים את 1 ו-5.

♣ א"כ מצאנו את מה שחיפשנו, השאלה היא רק מתי פולינום נתון הוא פולינום ספרבילי ובזה נעסוק בסעיף הבא.

מסקנה 3.4. אם $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left[\mathbb{K} : \mathbb{F}\right] = \left[\mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right) : \mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right]$.

3.2 מתי פולינום נתון הוא ספרבילי?

משפט 3.5. לכל שני פולינומים $f,g\in\mathbb{F}[x]$ מתקיים $(f+g)'=f'+g'$ ו-$(f\cdot g)'=f'\cdot g+f\cdot g'$.

מסקנה 3.6. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{E}$ שדה פיצול של f, יהיו $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{E}$ כל השורשים השונים של f, ויהיו $e_1,e_2,\ldots,e_r\in\mathbb{N}$ כך שמתקיים:

$$f(x)=\prod_{i=1}^{r}(x-\alpha_i)^{e_r}$$

מתקיים גם:

$$f'(x)=\sum_{i=1}^{r}e_i\cdot\frac{f(x)}{x-\alpha_i}$$

מסקנה 3.7. יהי $f\in\mathbb{F}[x]$, הריבוי האלגברי של שורש $\alpha\in\mathbb{F}$ גדול מ-1 אס"ם $x-\alpha\mid f'$.

למה 3.8. לכל שני פולינומים $f,g\in\mathbb{F}[x]$, המחלק המשותף המקסימלי שלהם מעל $\mathbb{F}$ הוא גם המחלק המשותף המקסימלי מעל כל שדה הרחבה של $\mathbb{F}$.

טענה 3.9. יהי $f\in\mathbb{F}[x]$ פולינום, f ספרבילי אס"ם $\gcd(f,f')=1$.

מסקנה 3.10. יהי $f\in\mathbb{F}[x]$ פולינום אי-פריק ונחלק למקרים:

- אם $\text{char}(\mathbb{F})=0$ אז f ספרבילי.
- אם $p:=\text{char}(\mathbb{F})$ ראשוני ולא קיים $g\in\mathbb{F}[x]$ כך ש-$f(x)=g(x^p)$ אז f ספרבילי.

מסקנה 3.11.

- אם $\text{char}(\mathbb{F})=0$ אז כל הרחבה אלגברית $\mathbb{E}/\mathbb{F}$ היא ספרבילית.
- אם $p:=\text{char}(\mathbb{F})$ ראשוני אז כל הרחבה סופית $\mathbb{E}/\mathbb{F}$ כך ש-p אינו מחלק את $[\mathbb{E}:\mathbb{F}]$ היא הרחבה ספרבילית.

משפט 3.12.

- אם $\text{char}(\mathbb{F})=0$ אז $\mathbb{F}$ הוא שדה משוכלל.
- אם $p:=\text{char}(\mathbb{F})$ ראשוני אז $\mathbb{F}$ הוא שדה משוכלל אס"ם ההעתקה $x\mapsto x^p$ היא על.

למה 3.13. נניח ש-$p:=\text{char}(\mathbb{F})$ ראשוני, הפונקציה $\varphi:\mathbb{F}\to\mathbb{F}$ המוגדרת ע"י $\varphi(x):=x^p$ לכל $x\in\mathbb{F}$ היא שיכון (של חוגים).

♣ שיכון זה נקרא ההומומורפיזם של פרובניוס[11].

מסקנה 3.14. כל שדה סופי הוא שדה משוכלל.

טענה 3.15. לכל שדה הרחבה $\mathbb{E}$ של $\mathbb{F}$, גם $\mathbb{F}_{\mathbb{E}}^{\text{sep}}$ הוא שדה הרחבה של $\mathbb{F}$.

משפט 3.16. תהא $\mathbb{E}/\mathbb{F}$ הרחבה סופית, מתקיים $i(\mathbb{E}/\mathbb{F})=[\mathbb{F}_{\mathbb{E}}^{\text{sep}}:\mathbb{F}]$.

[11] ערך בוויקיפדיה: פרדיננד גאורג פרובניוס.

4 מסקנות מתורת גלואה

4.1 המשפט היסודי של האלגברה

טענה 4.1. אם כל פולינום $f \in \mathbb{R}[x]$ מתפצל ב-$\mathbb{C}$ אז גם כל פולינום $f \in \mathbb{C}[x]$ מתפצל ב-$\mathbb{C}$.

תזכורת: ראינו באינפי' 1 שלכל פולינום $f \in \mathbb{R}[x]$, אם הדרגה $\deg f$ אי-זוגית אז קיים $x \in \mathbb{R}$ כך ש-$f(x) = 0$.

מסקנה 4.2. לכל פולינום אי-פריק $f \in \mathbb{R}[x]$ הדרגה $\deg f$ זוגית, ומכאן שלכל הרחבה סופית לא טריוויאלית $\mathbb{E}/\mathbb{R}$ דרגת ההרחבה $[\mathbb{E} : \mathbb{R}]$ זוגית.

טענה 4.3. לכל הרחבת גלואה סופית $\mathbb{E}/\mathbb{R}$ קיים $n \in \mathbb{N}_0$ כך ש-$[\mathbb{E} : \mathbb{R}] = 2^n$.

טענה 4.4. לכל פולינום אי-פריק $f \in \mathbb{C}[x]$ מתקיים $\deg f \neq 2$, מכאן שלכל הרחבה סופית $\mathbb{E}/\mathbb{C}$ מתקיים $[\mathbb{E} : \mathbb{C}] \neq 2$.

תזכורת: תהא G חבורה סופית, יהי $p \in \mathbb{N}$ ראשוני ונסמן $n := \max\left\{k \in \mathbb{N}_0 : |G| \text{ מחלק את } p^k\right\}$.
ראינו בקורס הקודם שבמקרה כזה לכל $n \geq k \in \mathbb{N}_0$ קיימת תת-חבורה $H \leqslant G$ כך ש-$|H| = p^k$.

מסקנה 4.5. לא קיימת הרחבת גלואה סופית $\mathbb{E}/\mathbb{C}$ כך ש-$[\mathbb{E} : \mathbb{C}] = 2^n$ עבור $n \in \mathbb{N}$ כלשהו.

משפט 4.6. המשפט היסודי של האלגברה
כל פולינום $f \in \mathbb{C}[x]$ מתפצל ב-$\mathbb{C}$, כלומר $\mathbb{C}$ סגור אלגברית.

4.2 שדות סופיים

יהי $p \in \mathbb{N}$ ראשוני.

טענה 4.7. הפולינום $x^{p^n} - x \in \mathbb{F}_p[x]$ ספרבילי לכל $n \in \mathbb{N}$.

משפט 4.8. לכל $n \in \mathbb{N}$ קיים שדה בגודל p^n, ושדה זה הוא יחיד עד כדי איזומורפיזם.

סימון: ולכל $n \in \mathbb{N}$ נסמן את השדה הנ"ל ב-$\mathbb{F}_{p^n}$.

מסקנה 4.9. לכל $n \in \mathbb{N}$, ההרחבה $\mathbb{F}_{p^n}/\mathbb{F}_p$ היא הרחבת גלואה מדרגה n.

משפט 4.10. יהי $n \in \mathbb{N}$, קיימת התאמה חח"ע ועל בין המחלקים של n לבין תתי-השדות של $\mathbb{F}_{p^n}$, בפרט: לכל $d \in \mathbb{N}$, $\mathbb{F}_{p^d}$ הוא תת-שדה של $\mathbb{F}_{p^n}$ אס"ם $d \mid n$.

למה 4.11. הפולינום [12]$x^p - t \in \mathbb{F}_p(t)[x]$ אי-פריק מעל $\mathbb{F}_p(t)$ ובעל שורש יחיד ב-$\overline{\mathbb{F}_p(t)}$.

מסקנה 4.12. נתבונן בהרחבה $\mathbb{F}_p(t)/\mathbb{F}_p$, מתקיים $\left[\mathbb{F}_p\left(\sqrt[p]{t}\right) : \mathbb{F}_p\right] = p$ ו-$\left|\text{Gal}\left(\mathbb{F}_p\left(\sqrt[p]{t}\right)/\mathbb{F}_p\right)\right| = 1$.

מסקנה 4.13. ההרחבה $\mathbb{F}_p\left(\sqrt[p]{t}\right)/\mathbb{F}_p$ היא הרחבה אלגברית שאינה ספרבילית.

[12] $\mathbb{F}_p(t)[x]$ הוא חוג הפולינומים מעל שדה הפונקציות הרציונליות $\mathbb{F}_p(t)$

5 נספח: בניות בסרגל ובמחוגה

יש לכתוב פרק זה

6 שאריות

משפט 6.1. נניח ש-$\mathrm{char}(\mathbb{F})=0$, ויהיו $f\in\mathbb{F}[x]$ פולינום, $\mathbb{E}$ שדה הפיצול של $\mathbb{F}$ ו-$a\in\mathbb{E}$; אם $\sigma(a)\in\mathbb{F}$ לכל $\sigma\in\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ אז $a\in\mathbb{F}$.

טענה 6.2. נניח ש-$\mathrm{char}(\mathbb{F})=0$ ויהי $f\in\mathbb{F}[x]$ פולינום מדרגה n, מתקיים $\pm\sqrt{\Delta f}\in\mathbb{F}$ אס״ם $\mathrm{Gal}(\mathbb{E}/\mathbb{F})\leqslant A_n$.

טענה 6.3. יהי $\mathbb{F}$ שדה ראשוני, $\mathrm{Aut}(\mathbb{F})$ היא החבורה הטריוויאלית.

מסקנה 6.4. יהי $\mathbb{F}$ שדה ראשוני, לכל הרחבת שדות $\mathbb{E}/\mathbb{F}$ מתקיים $\mathrm{Aut}(\mathbb{E})=\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.