תורת גלואה - טענות בלבד

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 הרחבת שדות

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

1.1 התחלה

משפט 1.1. תהא גם $\mathbb{K}/\mathbb{E}$ הרחבת שדות (מהגדרה גם $\mathbb{K}/\mathbb{F}$ היא הרחבת שדות), אם $\mathbb{E}/\mathbb{F}$ ו/או $\mathbb{K}/\mathbb{E}$ הן הרחבות אין-סופיות אז גם $\mathbb{K}/\mathbb{F}$ היא הרחבה אין-סופית, ואם שתיהן הרחבות סופיות אז גם $\mathbb{K}/\mathbb{F}$ היא הרחבה סופית ומתקיים:

$$[\mathbb{K}:\mathbb{F}]=[\mathbb{K}:\mathbb{E}]\cdot[\mathbb{E}:\mathbb{F}]$$

טענה 1.2. תהא X קבוצת תתי-שדות של שדה $\mathbb{F}$, החיתוך של כל תתי-השדות ב-X הוא תת-שדה של $\mathbb{F}$, וזהו השדה הגדול ביותר (ביחס להכלה) שמוכל בכל תתי-השדות ב-X.

♣ נשים לב לכך שיש כאן כמה אפשרויות:

- X יכולה להיות סופית ואז קיימים תתי-שדות $F_1,F_2,\ldots,F_r\subseteq\mathbb{F}$ כך ש-$X=\{F_1,F_2,\ldots,F_r\}$, ואז החיתוך של כל תתי-השדות בה הוא הקבוצה:

$$\bigcap_{i=1}^{r}F_i$$

- X יכולה להיות אין-סופית בת-מנייה, כלומר ניתן לסדר את איבריה בסדרה אינסופית: $X=\{F_1,F_2,\ldots\}$ ואז החיתוך של כל תתי-השדות בה הוא הקבוצה:

$$\bigcap_{i=1}^{\infty}F_i$$

- X יכולה להיות אין-סופית שאינה בת-מנייה, כלומר א"א לסדר את איבריה בסדרה אינסופית, ואז החיתוך של כל תתי-השדות בה הוא הקבוצה:

$$\bigcap_{F\in X}F$$

בכל מקרה החיתוך של כל תתי-השדות ב-X הוא הקבוצה:

$$\left\{\ a\in\mathbb{F}\ \middle|\ \forall F\in X:a\in F\ \right\}$$

למה 1.3. לכל $\alpha\in\mathbb{E}$ מתקיים:

$$\mathbb{F}(\alpha)=\left\{\ \frac{P(\alpha)}{Q(\alpha)}\ \middle|\ P,Q\in\mathbb{F}[x]\,,\ Q(\alpha)\neq0\ \right\}$$

♣ עבור $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{E}$ ניתן להכליל את הלמה ע"י:

$$\mathbb{F}(\alpha_1,\alpha_2,\ldots,\alpha_n)=\left\{\ \frac{P(\alpha_1,\alpha_2,\ldots,\alpha_n)}{Q(\alpha_1,\alpha_2,\ldots,\alpha_n)}\ \middle|\ P,Q\in\mathbb{F}[x_1,x_2,\ldots,x_n]\,,\ Q(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq0\ \right\}$$

כאשר $\mathbb{F}[x_1,x_2,\ldots,x_n]$ הוא חוג הפולינומים מעל $\mathbb{F}$ ב-n משתנים, כלומר כל איבר ב-$\mathbb{F}[x_1,x_2,\ldots,x_n]$ הוא סכום סופי של מכפלות סופיות של n המשתנים הללו זה בזה, ובנוסף החיבור והכפל מוגדרים כמו שהיינו מצפים (כמובן שפורמלית מדובר במחרוזות טקסט כמו בפולינומים רגילים, אבל אתם ממש לא רוצים שאנסה לכתוב כאן את ההגדרה הזו).

טענה 1.4. יהי $\alpha\in\mathbb{E}$, I_α הוא אידיאל של $\mathbb{F}[x]$, ובנוסף α הוא איבר אלגברי מעל $\mathbb{F}$ אם"ם $I_\alpha\neq\{0\}$.

טענה 1.5. יהי $\alpha\in\mathbb{E}$ איבר אלגברי מעל $\mathbb{F}$; m_α הוא פולינום אי-פריק ב-$\mathbb{F}[x]$, ולכל $P\in\mathbb{F}[x]$ כך ש-$P(\alpha)=0$ מתקיים $m_\alpha\mid P$.

מסקנה 1.6. יהי $\alpha\in\mathbb{E}$ איבר אלגברי מעל $\mathbb{F}$ ויהי $P\in\mathbb{F}[x]$ פולינום מתוקן ואי-פריק, אם $P(\alpha)=0$ אז $P=m_\alpha$.

טענה 1.7. יהי $\alpha\in\mathbb{E}$ איבר אלגברי מעל $\mathbb{F}$, מתקיים $\mathbb{F}(\alpha)\cong{}^{\mathbb{F}[x]}/_{(m_\alpha)}$ ו-$[\mathbb{F}(\alpha):\mathbb{F}]=\deg_{\mathbb{F}}(m_\alpha)$.

מסקנה 1.8. יהי $\alpha\in\mathbb{E}$ איבר אלגברי מעל $\mathbb{F}$ ונסמן $n:=\deg_{\mathbb{F}}(m_\alpha)$, מתקיים $\mathbb{F}(\alpha)=\{P(\alpha)\mid P\in\mathbb{F}[x],\ \deg P<n\}$.

מסקנה 1.9. יהי $\alpha\in\mathbb{E}$, α הוא איבר אלגברי מעל $\mathbb{F}$ אס"ם ההרחבה $\mathbb{F}(\alpha)/\mathbb{F}$ סופית.

טענה 1.10. התנאים הבאים שקולים:

- ${}^{\mathbb{E}}/_{\mathbb{F}}$ היא הרחבה סופית.
- ${}^{\mathbb{E}}/_{\mathbb{F}}$ היא הרחבה אלגברית נוצרת סופית.
- קיימים $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{E}$ אלגבריים מעל $\mathbb{F}$ כך ש-$\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

מסקנה 1.11. הקבוצה $\{\alpha\in\mathbb{E}\mid \mathbb{F}$ אלגברי מעל $\alpha\}$ היא תת-שדה של $\mathbb{E}$.

מסקנה 1.12. תהא גם ${}^{\mathbb{K}}/_{\mathbb{E}}$ הרחבת שדות, אם ${}^{\mathbb{E}}/_{\mathbb{F}}$ ו-${}^{\mathbb{K}}/_{\mathbb{F}}$ הן הרחבות אלגבריות אז גם ${}^{\mathbb{K}}/_{\mathbb{E}}$ היא הרחבה אלגברית.

סימון: לכל שדה $\mathbb{F}$ נסמן ב-$\mathbb{F}(t)$ את שדה הפונקציות הרציונליות מעל $\mathbb{F}$, כלומר:

$$\mathbb{F}(t):=\left\{\ \frac{P(t)}{Q(t)}\ \middle|\ P,Q\in\mathbb{F}[x],\ \ Q\neq 0\ \right\}$$

טענה 1.13. ${}^{\mathbb{F}(t)}/_{\mathbb{F}}$ היא הרחבה פשוטה שאינה אלגברית.

1.2 שדות פיצול

משפט 1.14. יהי $f\in\mathbb{F}[x]$ פולינום אי-פריק, א"כ ${}^{\mathbb{F}[x]}/_{(f)}$ הוא שדה הרחבה של $\mathbb{F}$ ו-$x+(f)$ הוא שורש של f כפולינום מעל ${}^{\mathbb{F}[x]}/_{(f)}$.

טענה 1.15. לכל פולינום $f\in\mathbb{F}[x]$ יש שדה פיצול, כלומר קיים שדה $\mathbb{K}$ המרחיב את $\mathbb{F}$ כך ש-f מתפצל ב-$\mathbb{K}$.

טענה 1.16. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{K}$ שדה פיצול של f, ויהיו $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{K}$ כל השורשים של f; מתקיים $\mathbb{K}=\mathbb{F}(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

מסקנה 1.17. לכל $f_1,f_2,\ldots,f_n\in\mathbb{F}[x]$, קיימת הרחבת שדות סופית ${}^{\mathbb{K}}/_{\mathbb{F}}$ כך שכל הפולינומים הנ"ל מתפצלים ב-$\mathbb{K}$.

משפט 1.18. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{K}$ שדה פיצול של f,ויהיו $\alpha_1,\alpha_2,\ldots,\alpha_n\in\mathbb{K}$ כל השורשים של f, ונסמן $X:=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$; קיים שיכון של $\mathrm{Gal}({}^{\mathbb{K}}/_{\mathbb{F}})$ ב-S_X.

מסקנה 1.19. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{K}$ שדה פיצול של f, דרגת ההרחבה $[\mathbb{K}:\mathbb{F}]$ מחלקת את $(\deg f)!$.

1.3 סגור אלגברי

משפט 1.20. קיימת הרחבת שדות ${}^{\mathbb{E}}/_{\mathbb{F}}$ כך ש-$\mathbb{E}$ סגור אלגברית.

מסקנה 1.21. יש ל-$\mathbb{F}$ סגור אלגברי.

♣ לא הוכחנו זאת, אך לכל שדה יש שדה סגור אלגברית מינימלי (ביחס לשיכון) יחיד (עד כדי איזומורפיזם).

סימון: לכל שדה $\mathbb{F}$ נסמן את אותו שדה סגור אלגברית מינימלי ב-$\overline{\mathbb{F}}$ ונקרא לו הסגור האלגברי של $\mathbb{F}$.

1.4 הרחבות רדיקליות

אין טענות בסעיף זה.

2 חבורת גלואה והתאמות גלואה

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

טענה 2.1. לכל שתי תתי-חבורות $H_1, H_2 \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ כך ש-$H_1 \leqslant H_2$ מתקיים $\mathcal{F}\left(H_1\right) \supseteq \mathcal{F}\left(H_2\right)$, וכמו כן לכל שני שדות ביניים $\mathbb{K}_1, \mathbb{K}_2 \subseteq \mathbb{E}$ של ההרחבה $\mathbb{E}/\mathbb{F}$ כך ש-$\mathbb{K}_1 \subseteq \mathbb{K}_2$ מתקיים ו-$\mathcal{G}\left(\mathbb{K}_1\right) \supseteq \mathcal{G}\left(\mathbb{K}_2\right)$.

טענה 2.2. לכל תת-חבורה $H \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ מתקיים $H \subseteq \mathcal{G}\left(\mathcal{F}\left(H\right)\right)$, ולכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\mathbb{K} \subseteq \mathcal{F}\left(\mathcal{G}\left(\mathbb{K}\right)\right)$.

למה 2.3. $\mathrm{Hom}\left(\mathbb{E}\right)$ היא קבוצה בת״ל מעל $\mathbb{E}$ (כתת קבוצה של מרחב הפונקציות $\mathbb{E}^{\mathbb{E}}$).

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

הוכחה. נניח בשלילה שזוהי קבוצה תלויה ליניארית, ויהיו $a_1, a_2, \ldots, a_m \in \mathbb{N}$ כך ש-$\sum_{i=1}^{m} a_i \cdot \sigma_i = 0$, ו-$m$ הוא המספר הטבעי[1] המינימלי שעבורו קיים צר״ל כזה.[2]

יהי $c \in \mathbb{E}$ כך ש-$\sigma_1\left(c\right) \neq \sigma_m\left(c\right)$, ומכאן שלכל $x \in \mathbb{E}$ מתקיים:

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

ולכן גם:

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

וממילא גם:

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

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

למה 2.4. תהא $H \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ תת-חבורה סופית, ויהיו $\sigma_1, \sigma_2, \ldots, \sigma_m$ כל האוטומורפיזמים השונים ב-H.

יהי $\left(a_1, a_2, \ldots, a_n\right)$ בסיס של $\mathcal{F}\left(H\right)$ כמ״ו מעל $\mathbb{F}$[3], המטריצה:

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

היא מטריצה הפיכה, ובפרט ריבועית.

מסקנה 2.5. תהא $H \leqslant \mathrm{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ תת-חבורה סופית, מתקיים $\left|H\right| = \left[\mathbb{E} : \mathcal{F}\left(H\right)\right]$.

בכיתה ראינו את הלמה והמסקנה הנ״ל בשלב מאוחר יותר של הקורס, למרות שהוכחתם אינה דורשת יותר מאלגברה ליניארית.

[1] להוציא את 0.
[2] בפרט $a_i \neq 0$ לכל $m \geq i \in \mathbb{N}$.
[3] **מי אמר שהוא נוצר סופית?**

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

מסקנה 2.6. מתקיימים ארבעת הפסוקים הבאים:

1. $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|\leq\left[\mathbb{E}:\mathbb{F}\right]$.
2. $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=\left[\mathbb{E}:\mathbb{F}\right]$ אס"ם $\mathbb{F}=\mathcal{F}\left(\mathcal{G}\left(\mathbb{F}\right)\right)$.
3. לכל תת-חבורה $H\leq\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ 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 $\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|=\left[\mathbb{E}:\mathbb{K}\right]$ 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.

משפט 2.7. אם $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=\left[\mathbb{E}:\mathbb{F}\right]$, אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|=\left[\mathbb{E}:\mathbb{K}\right]$.

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

♣ ובכן, היינו רוצים לומר שהגודל של חבורת גלואה הוא כפלי כמו דרגת ההרחבה, כלומר שבהינתן $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=\left[\mathbb{E}:\mathbb{F}\right]$ לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים:

$$\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|\cdot\left|\text{Gal}\left(\mathbb{K}/\mathbb{F}\right)\right|$$

ולכן נרצה שע"פ משפט האיזומורפיזם הראשון יתקיים $\text{Gal}\left(\mathbb{K}/\mathbb{F}\right)\cong{}^{\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)}/_{\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)}$: ההעתקה $\sigma\mapsto\sigma|_{\mathbb{K}}$ היא הומומורפיזם שגרעינו הוא $\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)$, אבל תמונתו היא $\text{Gal}\left(\mathbb{K}/\mathbb{F}\right)$ אס"ם $\sigma\left(\mathbb{K}\right)=\mathbb{K}$ לכל $\sigma\in\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ ואין זה מוכרח ש-$\sigma\left(\mathbb{K}\right)=\mathbb{K}$ לכל $\sigma\in\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$. א"כ משפט האיזומורפיזם הראשון נותן לנו רק את העובדה שמתקיים:

$$^{\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)}/_{\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)}\cong\left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E}\mid\sigma\mid_{\mathbb{F}}=\text{Id}_{\mathbb{F}}\right\}$$

הוכחה. נניח ש-$\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|=\left[\mathbb{E}:\mathbb{F}\right]$ ונסמן $I:=\left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E}\mid\sigma\mid_{\mathbb{F}}=\text{Id}_{\mathbb{F}}\right\}$.

$$\Rightarrow{}^{\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)}/_{\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)}\cong\left\{\sigma:\mathbb{K}\hookrightarrow\mathbb{E}\mid\sigma\mid_{\mathbb{F}}=\text{Id}_{\mathbb{F}}\right\}$$

$$\Rightarrow\left|I\right|=\left|{}^{\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)}/_{\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)}\right|=\frac{\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right|}{\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|}=\frac{\left[\mathbb{E}:\mathbb{F}\right]}{\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|}$$

ולכן גם:

$$\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|=\frac{\left[\mathbb{E}:\mathbb{F}\right]}{\left|I\right|}=\frac{\left[\mathbb{E}:\mathbb{K}\right]\cdot\left[\mathbb{K}:\mathbb{F}\right]}{\left|I\right|}$$

וע"פ המסקנה האחרונה (2.6) נקבל:

$$\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|=\left[\mathbb{E}:\mathbb{K}\right]\iff\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right|\geq\left[\mathbb{E}:\mathbb{K}\right]\iff\left|I\right|\geq\left[\mathbb{K}:\mathbb{F}\right]$$

א"כ נוכיח ש-$\left|I\right|\geq\left[\mathbb{K}:\mathbb{F}\right]$.

יהי $\left(a_{1},a_{2},\ldots,a_{l}\right)$ בסיס של $\mathbb{K}$ כמ"ו מעל $\mathbb{F}$, ויהיו $b_{1},b_{2},\ldots,b_{k}\in\mathbb{E}$ כך ש-$\left(a_{1},a_{2},\ldots,a_{l};b_{1},b_{2},\ldots,b_{k}\right)$ בסיס של $\mathbb{E}$ כמ"ו מעל $\mathbb{F}$.

נסמן $n:=l+k=\left[\mathbb{E}:\mathbb{F}\right]$, יהיו $\sigma_{1},\sigma_{2},\ldots,\sigma_{m}$ כל האוטומורפיזמים השונים ב-$\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ונסמן:

$$A:=\left[\begin{array}{ccc|ccc}
\sigma_{1}\left(a_{1}\right) & \cdots & \sigma_{1}\left(a_{l}\right) & \sigma_{1}\left(b_{1}\right) & \cdots & \sigma_{1}\left(b_{k}\right)\\
\sigma_{2}\left(a_{1}\right) & \cdots & \sigma_{2}\left(a_{l}\right) & \sigma_{2}\left(b_{1}\right) & \cdots & \sigma_{2}\left(b_{k}\right)\\
\sigma_{3}\left(a_{1}\right) & \cdots & \sigma_{3}\left(a_{l}\right) & \sigma_{3}\left(b_{1}\right) & \cdots & \sigma_{3}\left(b_{k}\right)\\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\
\sigma_{m}\left(a_{1}\right) & \cdots & \sigma_{m}\left(a_{l}\right) & \sigma_{m}\left(b_{1}\right) & \cdots & \sigma_{m}\left(b_{k}\right)
\end{array}\right]$$

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 ע״פ למה 2.4 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. ■

למה 2.8. יהיו $f \in \mathbb{F}[x]$ פולינום ו-$\alpha \in \mathbb{F}$ שורש של f, לכל $\sigma \in \text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ גם $\sigma(\alpha)$ הוא שורש של f.

משפט 2.9. 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 $\sigma \in \text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ יחיד כך ש-$\sigma(\alpha) = \beta$.

מסקנה 2.10. נניח ש-$\mathbb{E}/\mathbb{F}$ היא הרחבה אלגברית פשוטה, ויהי $\alpha \in \mathbb{E}$ כך ש-$\mathbb{E} = \mathbb{F}(\alpha)$; מתקיים $|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)| = [\mathbb{E} : \mathbb{F}]$ אם״ם m_α מתפצל ב-$\mathbb{E}$ לגורמים ליניאריים שונים.

מסקנה 2.11. אם $|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)| = [\mathbb{E} : \mathbb{F}]$ אז $\mathbb{E}$ הוא שדה פיצול של פולינום $f \in \mathbb{E}[x]$ המתפצל ב-$\mathbb{E}$ לגורמים ליניאריים שונים.

הוכחה. נוכיח את המסקנה באינדוקציה על מספר היוצרים של ההרחבה (הנחנו שהיא סופית), את בסיס האינדוקציה ראינו במסקנה הקודמת (2.10), לכן נעבור היישר לצעד האינדוקציה.
נניח שלכל הרחבת שדות סופית $\mathbb{L}/\mathbb{K}$ כך ש-$[\mathbb{L} : \mathbb{K}] < [\mathbb{E} : \mathbb{F}]$, אם $|\text{Gal}\left(\mathbb{L}/\mathbb{K}\right)| = [\mathbb{L} : \mathbb{K}]$ אז $\mathbb{L}$ הוא שדה פיצול של פולינום $f \in \mathbb{L}[x]$ המתפצל ב-$\mathbb{L}$ לגורמים ליניאריים שונים.
יהיו $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{E} \setminus \mathbb{F}$ כך ש-$\mathbb{E} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, מכאן ש-$[\mathbb{E} : \mathbb{F}(\alpha_1)] < [\mathbb{E} : \mathbb{F}]$.
ממשפט 2.7 נובע שאם $|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)| = [\mathbb{E} : \mathbb{F}]$ אז $|\text{Gal}\left(\mathbb{E}/\mathbb{F}(\alpha_1)\right)| = [\mathbb{E} : \mathbb{F}(\alpha_1)]$, ולכן ע״פ הנחת האינדוקציה נקבל ש $\mathbb{E}$ הוא שדה פיצול של פולינום $f \in \mathbb{E}[x]$ המתפצל ב-$\mathbb{E}$ לגורמים ליניאריים שונים. ■

3 הרחבות ספרביליות והרחבות נורמליות

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

3.1 הרחבות ספרביליות

למה 3.1. לכל $\alpha\in\Omega$, מספר השורשים השונים של $\varphi\left(m_{\alpha}\right)$ ב-Ω הוא $i_{\varphi,\Omega}\left({}^{\mathbb{F}(\alpha)}/_{\mathbb{F}}\right)$.

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

למה 3.2. 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 3.3. 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 3.4. 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 3.5. לכל הרחבה סופית ${}^{\mathbb{E}}/_{\mathbb{F}}$ מתקיים $i\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)\leq[\mathbb{E}:\mathbb{F}]$, ובנוסף מתקיים $i\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)=[\mathbb{E}:\mathbb{F}]$ אס"ם ההרחבה ${}^{\mathbb{E}}/_{\mathbb{F}}$ ספרבילית.

מסקנה 3.6. 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 3.7. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{E}$ שדה פיצול של f, אם f ספרבילי אז גם ההרחבה ${}^{\mathbb{E}}/_{\mathbb{F}}$ ספרבילית.

טענה 3.8. 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 $\mathbb{F}$.

3.2 הרחבות נורמליות

טענה 3.9. יהי $\mathbb{K}$ שדה ביניים של ${}^{\mathbb{E}}/_{\mathbb{K}}$, אם $\sigma(\mathbb{K})=\mathbb{K}$ לכל $\sigma\in\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)$ אז $\mathrm{Gal}\left({}^{\mathbb{K}}/_{\mathbb{F}}\right)\cong{}^{\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)}/_{\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{K}}\right)}$.

טענה 3.10. יהי $\mathbb{K}$ שדה ביניים של ${}^{\mathbb{E}}/_{\mathbb{F}}$, אם ${}^{\mathbb{K}}/_{\mathbb{F}}$ היא הרחבה נורמלית אז לכל $\sigma\in\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)$ מתקיים $\sigma(\mathbb{K})=\mathbb{K}$,
ועי"פ הטענה הקודמת (3.9) נקבל שגם $\mathrm{Gal}\left({}^{\mathbb{K}}/_{\mathbb{F}}\right)\cong{}^{\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)}/_{\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{K}}\right)}$.

טענה 3.11. מתקיים $\left|\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)\right|\leq i\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)$; ובנוסף, מתקיים $\left|\mathrm{Gal}\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)\right|=i\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)$ אס"ם לכל שדה סגור אלגברית Ω המכיל את $\mathbb{E}$, ולכל שיכון $\tau:\mathbb{E}\hookrightarrow\Omega$, מתקיים $\tau(\mathbb{E})=\mathbb{E}$.

משפט 3.12. התנאים הבאים שקולים:

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

מסקנה 3.13. יהי $\mathbb{K}$ שדה ביניים, $\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית אס״ם גם $\mathbb{E}/\mathbb{K}$ נורמלית.

4 הרחבות גלואה

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

4.1 המשפט היסודי של תורת גלואה

למה 4.1. לכל $H \leqslant \text{Gal}\left(\mathbb{E}/\mathbb{H}\right)$ ו-$\sigma \in \text{Gal}\left(\mathbb{E}/\mathbb{H}\right)$ מתקיים $\sigma\left(\mathcal{F}\left(H\right)\right) = \mathcal{F}\left(\sigma H \sigma^{-1}\right)$.

למה 4.2. 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 $\sigma \in \text{Gal}\left(\mathbb{E}/\mathbb{F}\right)$, ובמקרה כזה מתקיים $\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)/\text{Gal}\left(\mathbb{E}/\mathbb{K}\right) \cong \text{Gal}\left(\mathbb{K}/\mathbb{F}\right)$.

משפט 4.3. המשפט היסודי של תורת גלואה

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

1. $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה.
2. $\mathbb{E}$ הוא שדה פיצול של פולינום ספרבילי $f \in \mathbb{F}\left[x\right]$ כלשהו.
3. $\left|\text{Gal}\left(\mathbb{E}/\mathbb{F}\right)\right| = \left[\mathbb{E} : \mathbb{F}\right]$.
4. לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left|\text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right| = \left[\mathbb{E} : \mathbb{K}\right]$.
5. $\mathcal{F}$ ו-$\mathcal{G}$ הופכיות זו לזו.

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

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

לא ראינו את השקילות של סעיפים 4 ו-5 לסעיפים האחרים (לפחות לא באופן מפורש), אלא ראינו רק שסעיפים 1-3 (ששקולים זה לזה) גוררים את 4 ו-5.

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

מסקנה 4.4. אם $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אז לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$ מתקיים $\left[\mathbb{K} : \mathbb{F}\right] = \left[\text{Gal}\left(\mathbb{E}/\mathbb{F}\right) : \text{Gal}\left(\mathbb{E}/\mathbb{K}\right)\right]$.

4.2 מתי פולינום נתון הוא ספרבילי?

משפט 4.5. לכל שני פולינומים $f, g \in \mathbb{F}\left[x\right]$ מתקיים $\left(f+g\right)' = f' + g'$ ו-$\left(f \cdot g\right)' = f' \cdot g + f \cdot g'$.

מסקנה 4.6. יהיו $f \in \mathbb{F}\left[x\right]$ 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:
$$f\left(x\right) = \prod_{i=1}^{r}\left(x - \alpha_i\right)^{e_r}$$
מתקיים גם:
$$f'\left(x\right) = \sum_{i=1}^{r} e_i \cdot \frac{f\left(x\right)}{x - \alpha_i}$$

מסקנה 4.7. יהי $f \in \mathbb{F}[x]$, הריבוי האלגברי של שורש $\alpha \in \mathbb{F}$ גדול מ-1 אס"ם $x - \alpha \mid f'$.

למה 4.8. 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 4.9. יהי $f \in \mathbb{F}[x]$ פולינום, f ספרבילי אס"ם $\gcd(f, f') = 1$.

מסקנה 4.10. 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 4.11.

- 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 4.12.

- 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 4.13. 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[4].

מסקנה 4.14. כל שדה סופי הוא שדה משוכלל.

טענה 4.15. לכל שדה הרחבה $\mathbb{E}$ של $\mathbb{F}$, גם $\mathbb{F}_{\mathbb{E}}^{\text{sep}}$ הוא שדה הרחבה של $\mathbb{F}$.

משפט 4.16. תהא ${}^{\mathbb{E}}/_{\mathbb{F}}$ הרחבה סופית, מתקיים $\left[\mathbb{F}_{\mathbb{E}}^{\text{sep}} : \mathbb{F}\right] = i\left({}^{\mathbb{E}}/_{\mathbb{F}}\right)$.

[4] ערך בוויקיפדיה: פרדיננד גאורג פרובניוס.

5 מסקנות מתורת גלואה

5.1 המשפט היסודי של האלגברה

טענה 5.1. 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 5.2. 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 5.3. לכל הרחבת גלואה סופית $\mathbb{E}/\mathbb{R}$ קיים $n \in \mathbb{N}_0$ כך ש-$[\mathbb{E} : \mathbb{R}] = 2^n$.

טענה 5.4. 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: לכל חבורה סופית G, ולכל $p \in \mathbb{N}$ ראשוני כך ש-p מחלק את $|G|$, קיימת תת-חבורה

5.2 שדות סופיים

יהי $p \in \mathbb{N}$ ראשוני.

טענה 5.5. הפולינום $x^{p^n} - x \in \mathbb{F}_p[x]$ ספרבילי לכל $n \in \mathbb{N}$.

משפט 5.6. 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 5.7. לכל $n \in \mathbb{N}$ קיים פולינום אי-פריק $f \in \mathbb{F}_p[x]$ כך ש-$\deg f = n$.

משפט 5.8. לכל $n, d \in \mathbb{N}$ כך ש-$d \mid n$, יש ל-$\mathbb{F}_{p^n}$ תת-שדה יחיד בגודל $\mathbb{F}_{p^d}$.

למה 5.9. הפולינום $x^p - t \in \mathbb{F}_p(t)[x]$[5] אי-פריק מעל $\mathbb{F}_p(t)$ ובעל שורש יחיד ב-$\overline{\mathbb{F}_p(t)}$.

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

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

מסקנה 5.10. 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-$\left|\mathrm{Gal}\left(\mathbb{F}_p\left(\sqrt[p]{t}\right)/\mathbb{F}_p\right)\right| = 1$.

מסקנה 5.11. ההרחבה $\mathbb{F}_p\left(\sqrt[p]{t}\right)/\mathbb{F}_p$ היא הרחבה אלגברית שאינה ספרבילית.

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

6 נספח: בניות בסרגל ובמחוגה

יש לכתוב פרק זה

7 שאריות

משפט 7.1. נניח ש-$\operatorname{char}(\mathbb{F})=0$, 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 $\sigma\in\operatorname{Gal}\left(\mathbb{E}/\mathbb{F}\right)$ אז $a\in\mathbb{F}$.

טענה 7.2. נניח ש-$\operatorname{char}(\mathbb{F})=0$ ויהי $f\in\mathbb{F}[x]$ פולינום מדרגה n, מתקיים $\pm\sqrt{\Delta f}\in\mathbb{F}$ אס״ם $\operatorname{Gal}\left(\mathbb{E}/\mathbb{F}\right)\leqslant A_n$.

טענה 7.3. יהי $\mathbb{F}$ שדה ראשוני, $\operatorname{Aut}(\mathbb{F})$ היא החבורה הטריוויאלית.

מסקנה 7.4. יהי $\mathbb{F}$ שדה ראשוני, לכל הרחבת שדות $\mathbb{E}/\mathbb{F}$ מתקיים $\operatorname{Aut}(\mathbb{E})=\operatorname{Gal}\left(\mathbb{E}/\mathbb{F}\right)$.