תורת השדות - הגדרות 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 גבי 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

יהי $\mathbb{F}$ שדה.

טענה 1.1. אם $\mathrm{char}\left(\mathbb{F}\right)\neq0$ אז $\mathrm{char}\left(\mathbb{F}\right)$ הוא מספר ראשוני.

מסקנה 1.2. $\mathbb{F}_{p}$ ניתן לשיכון בכל שדה ממציין p ראשוני, ו-$\mathbb{Q}$ ניתן לשיכון בכל שדה ממציין 0.

מסקנה 1.3. אם $\mathbb{F}$ סופי אז $\mathrm{char}\left(\mathbb{F}\right)$ הוא מספר ראשוני.

תזכורת: כל שדה הוא מרחב וקטורי מעל כל תת-שדה שלו.

מסקנה 1.4. אם $\mathbb{F}$ סופי אז קיים ראשוני p ו-$e\in\mathbb{N}$ כך ש-$\left|\mathbb{F}\right|=p^{e}$.

למה 1.5. יהי $0\neq f\in\mathbb{F}\left[x\right]$ פולינום ונסמן $n:=\deg f$, חוג המנה $\mathbb{F}[x]/(f)$ הוא מרחב וקטורי מעל $\mathbb{F}$, ו-$\left(1+\left(f\right),x+\left(f\right),\ldots,x^{n-1}+\left(f\right)\right)$ הוא בסיס שלו (בפרט $\dim\left(\mathbb{F}[x]/(f)\right)=n$).

בספר הקורס כתוב ש-f נדרש להיות מתוקן, אין לי מושג למה יש בזה צורך.

מסקנה 1.6. נניח ש-$p:=\mathrm{char}\left(\mathbb{F}\right)\neq0$, יהי $f\in\mathbb{F}\left[x\right]$ פולינום אי-פריק ונסמן $n:=\deg f$; חוג המנה $\mathbb{F}[x]/(f)$ הוא שדה סופי בגודל p^{n-1}.

טענה 1.7. אם $\mathbb{F}$ סופי אז החבורה הכפלית $\mathbb{F}^{\times}$ היא חבורה ציקלית.

תזכורת: כל שדה הוא בפרט חוג, הומומורפיזמים של שדות על שלל סוגיהם הם פשוט הומומורפיזמים של חוגים אלא שהתחום והטווח שלהם הם שדות, בפרט נאמר ששני שדות איזומורפיים זה לזה אם קיים איזומורפיזם של חוגים ביניהם.

משפט 1.8. אם $\mathbb{F}$ סופי אז קיימים p ראשוני ופולינום $f\in\mathbb{F}_{p}\left[x\right]$ אי-פריק (ב-$\mathbb{F}_{p}\left[x\right]$) כך ש-$\mathbb{F}\cong\mathbb{F}_{p}[x]/(f)$.

טענה 1.9. כל הומומורפיזם $\varphi\in\mathrm{Aut}\left(\mathbb{F}\right)$ שאינו הומומורפיזם האפס הוא חח"ע.

2 הרחבת שדות

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

משפט 2.1. 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 2.2. 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 2.3. 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 2.4. יהי $\alpha\in\mathbb{E}$, I_α הוא אידיאל של $\mathbb{F}[x]$, ובנוסף α הוא איבר אלגברי מעל $\mathbb{F}$ אס"ם $I_\alpha\neq\{0\}$.

טענה 2.5. 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 $P\mid m_\alpha$.

מסקנה 2.6. 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 2.7. 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 2.8. יהיו $\alpha,\beta\in\mathbb{E}$ איברים אלגבריים מעל $\mathbb{F}$ כך ש-$m_\alpha=m_\beta$, מתקיים $\mathbb{F}(\alpha)\cong\mathbb{F}(\beta)$.

מסקנה 2.9. 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 2.10. לכל $\alpha\in\mathbb{E}$, α הוא איבר אלגברי מעל $\mathbb{F}$ אס"ם ההרחבה $\mathbb{F}(\alpha)/\mathbb{F}$ סופית.

טענה 2.11. 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 2.12. הקבוצה $\{\alpha\in\mathbb{E}\mid \mathbb{F}$ אלגברי מעל $\alpha\}$ היא תת-שדה של $\mathbb{E}$.

מסקנה 2.13. 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:

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

טענה 2.14. ${}^{\mathbb{F}(t)}/_{\mathbb{F}}$ היא הרחבה פשוטה שאינה אלגברית.

3 שדות פיצול

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

משפט 3.1. יהי $f\in\mathbb{F}[x]$ פולינום אי-פריק, אי"כ ${}^{\mathbb{F}[x]}/_{(f)}$ הוא שדה הרחבה של $\mathbb{F}$ ו-$x+(f)$ הוא שורש של f כפולינום מעל ${}^{\mathbb{F}[x]}/_{(f)}$.

מסקנה 3.2. לכל פולינום $f\in\mathbb{F}[x]$ יש שדה פיצול, בפרט לכל פולינום $f\in\mathbb{F}[x]$ קיים שדה $\mathbb{K}$ המרחיב את $\mathbb{F}$ כך ש-f מתפצל ב-$\mathbb{K}$.

טענה 3.3. 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 3.4. 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 3.5. 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 $\text{Gal}\left({}^{\mathbb{K}}/_{\mathbb{F}}\right)$ ב-S_X.

מסקנה 3.6. יהיו $f\in\mathbb{F}[x]$ פולינום ו-$\mathbb{K}$ שדה פיצול של f, דרגת ההרחבה $[\mathbb{K}:\mathbb{F}]$ מחלקת את $(\deg f)!$.

משפט 3.7. קיימת הרחבת שדות ${}^{\mathbb{E}}/_{\mathbb{F}}$ כך ש-$\mathbb{E}$ סגור אלגברית.

מסקנה 3.8. יש ל-$\mathbb{F}$ סגור אלגברי.

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

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