1 התחלה

1.1 הגדרות

♣ ראו גם את הקובץ "על שדות".

יהי שדה.

הגדרה 1.1. המציין של (נקרא גם המאפיין של) הוא הסדר של 1 בחבורה החיבורית של כאשר סדר זה סופי, ואם אינו סופי יהיה המציין 0; בכל מקרה נסמן את המציין ב-$()$.

למה להגדיר את המציין להיות 0 ולא ∞? כך לא יהיה צורך לחלק למקרים וזה טבעי הרבה יותר.

טענה. $()$ הוא מספר ראשוני או ש-$0 = ()$.

מסקנה. $_p$ ניתן לשיכון בכל שדה ממציין p ראשוני, ו- ניתן לשיכון בכל שדה ממציין 0.

הגדרה 1.2. השדה הראשוני של הוא $_p$ אם $p := ()$ ראשוני, ואחרת יהיה השדה הראשוני של .

יהי שדה.

טענה 1.3. אם $() \neq 0$ אז $()$ הוא מספר ראשוני.

מסקנה 1.4. $_p$ ניתן לשיכון בכל שדה ממציין p ראשוני, ו- ניתן לשיכון בכל שדה ממציין 0.

מסקנה 1.5. אם סופי אז $()$ הוא מספר ראשוני.

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

מסקנה 1.6. אם סופי אז קיים ראשוני p ו-$e \in$ כך ש-$|| = p^e$.

למה 1.7. יהי $0 \neq f \in [x]$ פולינום ונסמן $n := \deg f$, חוג המנה $[x]/(f)$ הוא מרחב וקטורי מעל , ו-$\left(1 + (f), x + (f), \ldots, x^{n-1} + (f)\right)$ הוא בסיס שלו (בפרט $\dim\left([x]/(f)\right) = n$).

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

מסקנה 1.8. נניח ש-$p := () \neq 0$, יהי $f \in [x]$ פולינום אי-פריק ונסמן $n := \deg f$; חוג המנה $[x]/(f)$ הוא שדה סופי בגודל p^{n-1}.

טענה 1.9. אם סופי אז החבורה הכפלית $^\times$ 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 1.10. אם סופי אז קיימים p ראשוני ופולינום $f \in_p [x]$ אי-פריק (ב-$_p[x]$) כך ש-$_p[x]/(f) \cong$.

טענה 1.11. כל הומומורפיזם $\varphi \in ()$ שאינו הומומורפיזם האפס הוא חח"ע.

2 הרחבת שדות

2.1 הגדרות

הגדרה 2.1. יהיו שדה ו-$\subseteq$ תת-שדה, במקרה כזה נאמר ש- הוא שדה הרחבה של או ש- מרחיב את ונסמן /[1].
שדה ייקרא שדה ביניים של ההרחבה / אם הוא תת-שדה של ו- הוא תת-שדה של .

♣ פעמים רבות נכתוב "תהא / הרחבת שדות" וכדומה, וכוונתנו תהיה "יהיו ו- שדות כך ש- הוא שדה הרחבה של ".

תהא / הרחבת שדות.

סימון: אם נוצר סופית כמרחב וקטורי מעל אז נסמן ב-dim את הממד של כמ"ו מעל .

הגדרה 2.2. אם נוצר סופית כמרחב וקטורי מעל , אז דרגת ההרחבה של היא $[:] := \dim$ ונאמר ש-/ היא הרחבה סופית, אחרת נכתוב $[:] = \infty$ ונאמר ש-/ היא הרחבה אין-סופית.

טענה. תהא X קבוצת תתי-שדות של שדה , החיתוך של כל תתי-השדות ב-X הוא תת-שדה של , וזהו השדה הגדול ביותר (ביחס להכלה) שמוכל בכל תתי-השדות ב-X.

הגדרה 2.3. תהא $S \subseteq$, נסמן ב-(S) את החיתוך של כל תתי-השדות של המכילים את $\cup S$, (S) ייקרא תת-השדה של הנוצר ע"י S.

מסקנה 2.4. תהא $S \subseteq$ תת-קבוצה, מתקיימים שלושת הפסוקים הבאים:

1. (S) הוא תת-שדה של .
2. $S \subseteq (S)$.
3. לכל תת-שדה $E \subseteq$ המכיל את S מתקיים $(S) \subseteq E$.

סימון: עבור קבוצה סופית $\{s_1, s_2, \ldots, s_n\} \subseteq$ נכתוב גם $(s_1, s_2, \ldots, s_n) := (\{s_1, s_2, \ldots, s_n\})$.

[1] אין שום קשר לחוג מנה, זהו סימון בלבד שאינו קשור בשום צורה שהיא.

הגדרה 2.5. יהי $\subseteq$ תת-שדה, נאמר שתת-קבוצה $S \subseteq$ היא קבוצת יוצרים של מעל אם $(S) =$.

הגדרה 2.6. / תיקרא הרחבה נוצרת סופית אם קיימת קבוצה סופית $S \subseteq$ כך ש-$(S) =$, ותיקרא הרחבה פשוטה אם קיים $\alpha \in$ כך ש-$(\alpha) =$ (α כזה ייקרא יוצר פרימיטיבי של מעל).

למה. לכל $\alpha \in$ מתקיים:

$$(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} \;\middle|\; P, Q \in [x]\,,\ \ Q(\alpha) \neq 0 \right\}$$

הגדרה 2.7. איבר $\alpha \in$ ייקרא אלגברי מעל אם קיים $0 \neq P \in [x]$ כך ש-$P(\alpha) = 0$, אחרת ייקרא טרנסצנדנטי.
/ תיקרא הרחבה אלגברית אם כל איברי אלגבריים מעל , אחרת תיקרא טרנסצנדנטית.

♣ העובדה שאיבר $\alpha \in$ הוא אלגברי מעל אומרת שלמרות שבלמה האחרונה אין מגבלה על דרגת הפולינומים, בפועל יש כזו מפני שתמיד אפשר לחלק (עם שארית) את הפולינומים בפולינום שמאפס את α ולקחת רק את השארית.

סימון: לכל $\alpha \in I$ נסמן $I_\alpha := \{P \in [x] : P(\alpha) = 0\}$.

טענה. I_α הוא אידיאל של $[x]$, ו-α הוא איבר אלגברי מעל אם"ם $I_\alpha \neq \{0\}$.

הגדרה 2.8. יהי $\alpha \in$ איבר אלגברי מעל , הפולינום המינימלי של α מעל הוא הפולינום המתוקן היוצר את האידיאל I_α, פולינום זה יסומן ב-m_α וכמו כן הדרגה של α מעל תוגדר ע"י $\deg(\alpha) := \deg(m_\alpha)$.

תהא / הרחבת שדות.

משפט 2.9. תהא גם / הרחבת שדות (מהגדרה גם / היא הרחבת שדות), אם / ו/או / הן הרחבות אין-סופיות אז גם / היא הרחבה אין-סופית, ואם שתיהן הרחבות סופיות אז גם / היא הרחבה סופית ומתקיים:

$$[:] = [:] \cdot [:]$$

טענה 2.10. תהא X קבוצת תתי-שדות של שדה , החיתוך של כל תתי-השדות ב-X הוא תת-שדה של , 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 $F_1, F_2, \ldots, F_r \subseteq$ 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:

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

למה 2.11. לכל $\alpha \in$ מתקיים:

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

♣ עבור $\alpha_1, \alpha_2, \ldots, \alpha_n \in$ ניתן להכליל את הלמה ע״י:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \ \frac{P(\alpha_1, \alpha_2, \ldots, \alpha_n)}{Q(\alpha_1, \alpha_2, \ldots, \alpha_n)} \ \middle| \ P, Q \in [x_1, x_2, \ldots, x_n] \, , \ \ Q(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0 \ \right\}$$

כאשר $[x_1, x_2, \ldots, x_n]$ הוא חוג הפולינומים מעל ב-n משתנים, כלומר כל איבר ב-$[x_1, x_2, \ldots, x_n]$ 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 2.12. יהי $\alpha \in$, I_α הוא אידיאל של $[x]$, ובנוסף α הוא איבר אלגברי מעל אם״ם $I_\alpha \neq \{0\}$.

טענה 2.13. יהי $\alpha \in$ איבר אלגברי מעל ; m_α הוא פולינום אי-פריק ב-$[x]$, ולכל $P \in [x]$ כך ש-$P(\alpha) = 0$ מתקיים $m_\alpha \mid P$.

מסקנה 2.14. יהי $\alpha \in$ איבר אלגברי מעל ויהי $P \in [x]$ פולינום מתוקן ואי-פריק, אם $P(\alpha) = 0$ אז $P = m_\alpha$.

טענה 2.15. יהי $\alpha \in$ איבר אלגברי מעל , מתקיים $(\alpha) \cong {}^{[x]}/_{(m_\alpha)}$ ו-$[(\alpha) :] = \deg(m_\alpha)$.

מסקנה 2.16. יהיו $\alpha, \beta \in$ איברים אלגבריים מעל כך ש-$m_\alpha = m_\beta$, מתקיים $(\alpha) \cong (\beta)$.

מסקנה 2.17. יהי $\alpha \in$ איבר אלגברי מעל ונסמן $n := \deg(m_\alpha)$, מתקיים $(\alpha) = \{P(\alpha) \mid P \in [x],\ \deg P < n\}$.

מסקנה 2.18. לכל $\alpha \in$, α הוא איבר אלגברי מעל אם"ם ההרחבה (α) / סופית.

טענה 2.19. התנאים הבאים שקולים:

- / היא הרחבה סופית.
- / היא הרחבה אלגברית נוצרת סופית.
- קיימים $\alpha_1, \alpha_2, \ldots, \alpha_n \in$ אלגבריים מעל כך ש-$= (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

מסקנה 2.20. הקבוצה $\{\alpha \in |$ אלגברי מעל $\alpha\}$ היא תת-שדה של .

מסקנה 2.21. תהא גם / הרחבת שדות, אם / ו-/ הן הרחבות אלגבריות אז גם / היא הרחבה אלגברית.

סימון: לכל שדה נסמן ב-(t) את שדה הפונקציות הרציונליות מעל , כלומר:

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

טענה 2.22. ${}^{(t)}/$ היא הרחבה פשוטה שאינה אלגברית.

3 שדות פיצול

3.1 הגדרות

תהא / הרחבת שדות.

הגדרה 3.1. נאמר שפולינום $f \in [x]$ מתפצל בשדה הרחבה אם ניתן להציגו כמכפלה של גורמים ליניאריים ב-$[x]$, כלומר אם קיימים $a, \deg f, c \in$ כך שמתקיים:

$$f(x) = c \cdot \prod_{i=1}^{\deg f} (x - \alpha_i)$$

הגדרה 3.2. נאמר ששדה הרחבה הוא שדה פיצול של פולינום $f \in [x]$, אם f מתפצל ב-, ובנוסף הוא שדה הביניים היחיד של / שבו f מתפצל.

♣ אנחנו נראה בהמשך שלכל פולינום יש שדה פיצול, ובהמשך נראה גם ששדה פיצול הוא יחיד עד כדי איזומורפיזם, א"כ מוצדק לדבר עליו בה"א הידיעה.

הגדרה 3.3. נאמר ש- הוא שדה סגור אלגברית אם לכל פולינום $f \in [x]$ כך ש-$\deg f \geq 1$ יש שורש ב-.

הגדרה 3.4. נאמר ששדה הרחבה הוא סגור אלגברי של אם / היא הרחבה אלגברית ו- סגור אלגברית.

משפט. קיימת הרחבת שדות / כך ש- סגור אלגברית.

♣ מכאן שלכל שדה יש סגור אלגברי.

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

סימון: לכל שדה נסמן את אותו שדה סגור אלגברית מינימלי ב- ונקרא לו הסגור האלגברי של .

תהא / הרחבת שדות.

משפט 3.5. יהי $f \in [x]$ פולינום אי-פריק, א״כ $[x]/(f)$ הוא שדה הרחבה של ו-$x + (f)$ הוא שורש של f כפולינום מעל $[x]/(f)$.

מסקנה 3.6. לכל פולינום $f \in [x]$ יש שדה פיצול, בפרט לכל פולינום $f \in [x]$ קיים שדה המרחיב את כך ש-f מתפצל ב-.

טענה 3.7. יהיו $f \in [x]$ פולינום ו- שדה פיצול של f, ויהיו $\alpha, n \in$ כל השורשים של f; מתקיים $:= (\alpha, n)$.

מסקנה 3.8. לכל $f, n \in [x]$, קיימת הרחבת שדות סופית / כך שכל הפולינומים הנ״ל מתפצלים ב-.

משפט 3.9. יהיו $f \in [x]$ פולינום ו- שדה פיצול של f,ויהיו $\alpha, n \in$ כל השורשים של f, ונסמן $X := \{\alpha, n\}$; קיים שיכון של $(/)$ ב-S_X.

מסקנה 3.10. יהיו $f \in [x]$ פולינום ו- שדה פיצול של f, דרגת ההרחבה $[:]$ מחלקת את $(\deg f)!$.

משפט 3.11. קיימת הרחבת שדות / כך ש- סגור אלגברית.

מסקנה 3.12. יש ל- סגור אלגברי.

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

סימון: לכל שדה נסמן את אותו שדה סגור אלגברית מינימלי ב- ונקרא לו הסגור האלגברי של .