תורת גלואה - 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 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.

הגדרה 1.1. $\mathbb{E}/\mathbb{F}$ תיקרא הרחבה רדיקלית פשוטה אם קיימים $\alpha \in \mathbb{E}$ ו-$n \in \mathbb{N}$ כך ש-$\mathbb{E} = \mathbb{F}(\alpha)$ ו-$\alpha^n \in \mathbb{F}$.
כמו כן, $\mathbb{E}/\mathbb{F}$ תיקרא הרחבה רדיקלית אם קיימים $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{E}$ 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 $r \geq i \in \mathbb{N}$.

♣ מטרתנו היא לקבוע מתי ניתן לפתור פולינום נתון באמצעות חיבור, חיסור, כפל, חילוק והוצאת שורש; הצורה הפורמלית לומר זאת היא שהפולינום מתפצל בשדה הרחבה רדיקלית.

♣ מטרה נוספת היא לקבוע מתי יש נוסחה קבועה לפתרון כל הפולינומים ממעלה כלשהי מעל שדה נתון.

הגדרה 1.2.

- נאמר שפולינום $f \in \mathbb{F}[x]$ ניתן לפתרון באמצעות רדיקלים אם קיימת הרחבות שדות רדיקלית $\mathbb{K}/\mathbb{F}$ כך ש-f מתפצל ב-$\mathbb{K}$.
- כמו כן נאמר שפולינום $f \in \mathbb{F}[x]$ הוא פתיר אם $\mathrm{Gal}(\mathbb{E}_f/\mathbb{F})$ היא חבורה פתירה, כאשר $\mathbb{E}_f$ הוא שדה הפיצול של f.

מסקנה 1.3. יהי $f \in \mathbb{F}[x]$ פולינום ונסמן ב-$\mathbb{E}_f$ את שדה הפיצול שלו, מתקיים f ניתן לפתרון באמצעות רדיקלים אם"ם $\mathbb{E}_f/\mathbb{F}$ היא הרחבה רדיקלית.

הגדרה 1.4. איבר $\zeta \in \mathbb{F}$ ייקרא שורש יחידה מסדר $n \in \mathbb{N}$, אם $\zeta^n = 1$, כמו כן ייקרא שורש יחידה פרימיטיבי מסדר n אם (בנוסף) $\zeta^k \neq 1$ לכל $n > k \in \mathbb{N}$.

הגדרה 1.5. חבורת גלואה[1]
חבורת גלואה של ההרחבה $\mathbb{E}/\mathbb{F}$ היא $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) := \{\varphi \in \mathrm{Aut}(\mathbb{E}) : \varphi|_{\mathbb{F}} = \mathrm{Id}_{\mathbb{F}}\}$ (פעולת החבורה היא הרכבה כמובן).

הערה: במקומות אחרים קוראים לקבוצה $\{\varphi \in \mathrm{Aut}(\mathbb{E}) : \varphi|_{\mathbb{F}} = \mathrm{Id}_{\mathbb{F}}\}$ חבורת האוטומורפיזמים של ההרחבה $\mathbb{E}/\mathbb{F}$ ומסמנים אותה ב-$\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, את השם "חבורת גלואה" ואת הסימון $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ הם שומרים למקרה שבו $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה (אנחנו נגדיר מהי הרחבת גלואה בהמשך).

למה 1.6. לכל תת-חבורה $H \leqslant \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, הקבוצה $\{x \in \mathbb{E} \mid \forall \sigma \in H \ \ \sigma(x) = x\}$ היא שדה המכיל את $\mathbb{F}$.

הגדרה 1.7. לכל תת-חבורה $H \leqslant \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ נסמן $\mathbb{E}^H := \{x \in \mathbb{E} \mid \forall \sigma \in H \ \ \sigma(x) = x\}$, $\mathbb{E}^H$ ייקרא שדה השבת של H.

הגדרה 1.8. התאמות גלואה
התאמות גלואה של ההרחבה $\mathbb{E}/\mathbb{F}$ הן שתי הפונקציות הבאות:

- $\mathcal{F} : \{H \mid H \leqslant \mathrm{Gal}(\mathbb{E}/\mathbb{F})\} \to \{\mathbb{K} \mid \mathbb{E}/\mathbb{K}$ הוא שדה ביניים של $\mathbb{K}\}$ המוגדרת ע"י (לכל $H \leqslant \mathrm{Gal}(\mathbb{E}/\mathbb{F})$):
$$\mathcal{F}(H) := \mathbb{E}^H = \{x \in \mathbb{E} \mid \forall \sigma \in H \ \ \sigma(x) = x\}$$
- $\mathcal{G} : \{\mathbb{K} \mid \mathbb{E}/\mathbb{F}$ הוא שדה ביניים של $\mathbb{K}\} \to \{H \mid H \leqslant \mathrm{Gal}(\mathbb{E}/\mathbb{F})\}$ המוגדרת ע"י (לכל שדה ביניים $\mathbb{K}$ של $\mathbb{E}/\mathbb{F}$):
$$\mathcal{G}(\mathbb{K}) := \mathrm{Gal}(\mathbb{E}/\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{E}) \mid \forall x \in \mathbb{K} \ \ \sigma(x) = x\}$$

♣ כלומר $\mathcal{F}$ ו-$\mathcal{G}$ הן פונקציות בין תתי-החבורות של חבורת גלואה של ההרחבה, לבין קבוצת שדות הביניים של ההרחבה: $\mathcal{F}$ מתאימה לכל תת-חבורה את שדה הביניים הגדול ביותר שנשמר תחת פעולתה, ו-$\mathcal{G}$ מתאימה לכל שדה ביניים את תת-החבורה הגדולה ביותר שהשדה נשמר תחתיה. השאלה שנעסוק בה תהיה מתי $\mathcal{F}$ ו-$\mathcal{G}$ הופכיות זו לזו, כלומר מתי יש התאמה חח"ע ועל בין שדות הביניים של הרחבת שדות לבין תתי-החבורות של חבורת גלואה. או אז נוכל להשתמש בכלים החזקים שפיתחנו בקורס הקודם כדי לחקור את שדות הביניים, ולקבוע מתי ניתן לפתור את הפולינום שיצר את ההרחבה.

[1] ערך בוויקיפדיה: אוריסט גלואה.

צריך להסביר שהאוטומורפיזמים מאפשרים לנו לחקור את הקשרים האלגבריים בין שורשי הפולינום היוצר את ההרחבה מבלי "ללכלך את הידיים".

מסקנה 1.9. מתקיים $\mathcal{F}(\{\mathrm{Id}\}) = \mathbb{E}$, $\mathcal{G}(\mathbb{E}) = \{\mathrm{Id}\}$ ו-$\mathcal{G}(\mathbb{F}) = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

♣ אין זה מוכרח שיתקיים $\mathcal{F}(\mathrm{Gal}(\mathbb{E}/\mathbb{F})) = \mathbb{F}$, כך לדוגמה לכל $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$ מתקיים $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$ ולכן $\mathcal{F}\left(\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)\right) = \mathbb{Q}\left(\sqrt[3]{2}\right)$.

הגדרה 1.10. נאמר ש-$\mathbb{E}/\mathbb{F}$ היא <u>הרחבת גלואה</u> אם $\mathcal{F}$ ו-$\mathcal{G}$ הופכיות זו לזו.
כמו כן, אם $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה נאמר ש-$\mathbb{E}/\mathbb{F}$ היא <u>הרחבה ציקלית/אבלית/פתירה</u> אם $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ היא חבורה ציקלית/אבלית/פתירה.

בכיתה הגדרנו שהרחבת גלואה היא הרחבה נורמלית וספרבילית, אנחנו נראה בהמשך שאלה הן הגדרות שקולות.

מסקנה 1.11. $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אם"ם לכל שדה ביניים $\mathbb{K}$ גם $\mathbb{E}/\mathbb{K}$ היא הרחבת גלואה.

2 הרחבות ספרביליות והרחבות נורמליות

יהי $\mathbb{F}$ שדה.

2.1 הרחבות ספרביליות

הגדרה 2.1. נאמר שפולינום $f \in \mathbb{F}[x]$ הוא <u>ספרבילי</u> אם בשדה הפיצול שלו הוא מתפרק לגורמים ליניאריים שונים, כלומר הריבוי של כל אחד משורשיו הוא 1.
בהינתן הרחבת שדות $\mathbb{E}/\mathbb{F}$ נאמר שאיבר $\alpha \in \mathbb{F}$ הוא <u>ספרבילי</u> אם m_α ספרבילי, וכמו כן נאמר ש-$\mathbb{E}/\mathbb{F}$ היא <u>הרחבה ספרבילית</u> אם כל $\alpha \in \mathbb{E}$ ספרבילי.

סימון: יהיו Ω שדה סגור אלגברית ו-$\varphi : \mathbb{F} \hookrightarrow \Omega$ שיכון, לכל הרחבה סופית $\mathbb{E}/\mathbb{F}$ נסמן $I_{\varphi,\Omega}(\mathbb{E}/\mathbb{F}) := \{\hat{\varphi} : \mathbb{E} \hookrightarrow \Omega \mid \hat{\varphi}|_{\mathbb{F}} = \varphi\}$ ו-$i_{\varphi,\Omega}(\mathbb{E}/\mathbb{F}) := |I_{\varphi,\Omega}(\mathbb{E}/\mathbb{F})|$, כלומר $i_{\varphi,\Omega}(\mathbb{E}/\mathbb{F})$ הוא מספר השיכונים של $\mathbb{E}$ ב-Ω המרחיבים את φ.

סימון: לכל פולינום $f := \sum_{i=0}^{n} a_i \cdot x^i \in \Omega$ נסמן $\varphi(f) := \sum_{i=0}^{n} \varphi(a_i) \cdot x^i \in \Omega$.

למה. יהיו Ω שדה סגור אלגברית ו-$\varphi : \mathbb{F} \hookrightarrow \Omega$ שיכון; לכל $\alpha \in \Omega$, $i_{\varphi,\Omega}(\mathbb{F}(\alpha)/\mathbb{F})$ שווה למספר השורשים השונים של $\varphi(m_\alpha)$ ב-Ω.

למה. יהיו Ω שדה סגור אלגברית ו-$\varphi_1, \varphi_2 : \mathbb{F} \hookrightarrow \Omega$ שיכונים; לכל פולינום $f \in \mathbb{F}[x]$, מספר השורשים השונים של $\varphi_1(f)$ שווה למספר השורשים השונים של $\varphi_2(f)$.

משפט. תהיינה $\mathbb{K}/\mathbb{F}$ ו-$\mathbb{E}/\mathbb{K}$ הרחבות שדות, 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.
אם $\mathbb{E}/\mathbb{F}$ היא הרחבה סופית אז מתקיימים שלושת הפסוקים הבאים:

1. $i_{\varphi_1,\Omega_1}(\mathbb{E}/\mathbb{F}) = i_{\varphi_2,\Omega_2}(\mathbb{E}/\mathbb{F})$
2. $i_{\varphi_1,\Omega_1}(\mathbb{E}/\mathbb{F}) \geq 1$
3. $i_{\varphi_1,\Omega_1}(\mathbb{E}/\mathbb{F}) = i_{\varphi_1,\Omega_1}(\mathbb{E}/\mathbb{K}) \cdot i_{\varphi_1,\Omega_1}(\mathbb{K}/\mathbb{F})$

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

2.2 הרחבות נורמליות

הגדרה 2.2. תהא $\mathbb{E}/\mathbb{F}$ הרחבת שדות, נאמר ש-$\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית אם לכל פולינום אי-פריק $f \in \mathbb{F}[x]$, כך שיש ל-f שורש ב-$\mathbb{E}$, f מתפצל ב-$\mathbb{E}$.

מסקנה 2.3. תהא $\mathbb{E}/\mathbb{F}$ הרחבת שדות, $\mathbb{E}/\mathbb{F}$ היא הרחבה נורמלית אם"ם לכל $\alpha \in \mathbb{E}$ הפולינום המינימלי של α מעל $\mathbb{F}$ מתפצל ב-$\mathbb{E}$.

3 הרחבות גלואה

3.1 המשפט היסודי של תורת גלואה

הגדרה 3.1. נאמר שהרחבת שדות $\mathbb{E}/\mathbb{F}$ היא הרחבת גלואה אם היא נורמלית וספרבילית.

3.2 מתי פולינום נתון הוא ספרבילי?

הגדרה 3.2. נאמר ש-$\mathbb{F}$ הוא שדה משוכלל אם כל הרחבה אלגברית שלו היא ספרבילית.

הערה: במקומות אחרים אומרים על שדה כזה שהוא מושלם.

הגדרה 3.3. יהי $f(x) := \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{F}[x]$ פולינום, פולינום הנגזרת של f הוא הפולינום $f'(x) := \sum_{i=0}^{n-1} (i+1) \cdot a_{i+1} \cdot x^i$.

♣ נשים לב: כש-i מופיע בחזקה (x^i) הוא איבר ב-$\mathbb{N}_0$, ואילו כאשר הוא מופיע במקדמי הפולינום ($(i+1) \cdot a_{i+1}$) הוא איבר ב-$\mathbb{F}$, בפרט ייתכן שמקדמים יתאפסו (אם $\operatorname{char}(\mathbb{F})$ ראשוני) וכתוצאה מכך יתקיים $\deg f' < \deg f - 1$.

סימון: יהי $\mathbb{E}$ שדה הרחבה של $\mathbb{F}$, הסגור הספרבילי של $\mathbb{F}$ בתוך $\mathbb{E}$ הוא הקבוצה $\mathbb{F}_{\mathbb{E}}^{\text{sep}} := \{\alpha \in \mathbb{E} \mid \mathbb{F} \text{ ספרבילי מעל } \alpha\}$.

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

4 נספח: בניות בסרגל ובמחוגה

יש לכתוב פרק זה

5 שאריות

הגדרה 5.1. הדיסקרימיננטה

יהיו $f \in \mathbb{F}[x]$ פולינום ו-$\mathbb{E}$ שדה הפיצול של f, ויהיו $c \in \mathbb{E}$, $\alpha_1, \alpha_2, \ldots, \alpha_{\deg f}$ כך שמתקיים:

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

<u>הדיסקרימיננטה</u> של f היא:

$$\Delta f = \prod_{i<j\leq \deg f} (\alpha_i - \alpha_j)$$

מה???

למה 5.2. לכל $n \in \mathbb{N}$ ולכל $a \in \mathbb{F}$, שדה הפיצול של $x^n - a \in \mathbb{Q}[x]$ הוא $\mathbb{Q}\left(\sqrt[n]{a}, \operatorname{cis}\left(\frac{2\pi}{n}\right)\right)$.

הגדרה 5.3. לכל $n \in \mathbb{N}$, השדה $\mathbb{Q}\left(\operatorname{cis}\left(\frac{2\pi}{n}\right)\right)$ ייקרא <u>השדה הציקלוטומי</u> מדרגה n.