שדות ותורת גלואה
מערכי תרגול קורס 88-311

ספטמבר 2019, גרסה 0.15

אוניברסיטת בר-אילן

סמסטר א׳ תש״ף

תוכן העניינים

מבוא

כמה הערות טכניות לתחילת הקורס:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- החומר בחוברת הזו נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי התרגול של איתמר שטיין ושירה גילת.
- נשתדל לכתוב בגופן הזה כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית. This font
- נשמח לכל הערה על מסמך זה.

מחבר בתשע"ט ותש"ף: תומר באואר

1 תרגול ראשון

1.1 תזכורת מתורת החוגים

Rng, or non-unital ring

הגדרה 1.1. חוג בלי יחידה $(R, +, \cdot, 0)$ הוא מבנה אלגברי המקיים:

Additive group

1. $(R, +, 0)$ הוא חבורה אבלית. נקראת החבורה החיבורית של החוג.
2. $(R, \cdot)$ הוא חבורה למחצה.
3. מתקיים חוג הפילוג (משמאל ומימין). כלומר לכל $a, b, c \in R$ מתקיים

$$(a+b)c = ac + bc, \qquad a(b+c) = ab + ac$$

כאשר ההקשר ברור, נכתוב רק R במקום $(R, +, \cdot, 0)$.

Field

הגדרה 1.2. R הוא שדה אם $(R \setminus \{0\}, \cdot)$ חבורה אבלית.

שדות הם חוגים מאוד טובים. הם חילופיים וכל איבר בהם הפיך. ראינו בקורס בתורת החבורות שאם F שדה, אז חוג הפולינומים במשתנה אחד $F[x]$ הוא תחום אוקלידי, ולכן הוא תחום ראשי, ולכן הוא תחום פריקות יחידה. כל התכונות האלו יהיו מאוד שימושיות בהמשך.

נתחיל בחזרה לגבי פריקות של פולינומים מעל שדות. נסביר בהמשך למה זה רלוונטי לקורס שלנו.

Irreducible

תזכורת 1.3. יהי R תחום שלמות. איבר לא הפיך $a \in R$ נקרא אי פריק אם $a = bc$ גורר ש-b הפיך או c הפיך.

שאלה 1.4. בהינתן פולינום $f(x) \in F[x]$ איך ניתן לקבוע אם הוא אי פריק או לא?

חשוב להדגיש כל הזמן מה השדה שעובדים מעליו. למשל $x^2 - 2$ פריק מעל $\mathbb{R}$ אבל לא מעל $\mathbb{Q}$. עבורנו התכונה אי פריק היא "הבסיסית" יותר, ופולינום נקרא פריק אם הוא לא אי פריק. נציג מספר שיטות, ונתחיל בכמה אבחנות קלות:

- כל פולינום מדרגה 1 הוא אי פריק. אז המקרה הזה משעמם. מעכשיו נניח כי $\deg f(x) \geq 2$ בטענות לא טריוויאליות.
- כל פולינום שיש לו שורש בשדה F הוא פריק. הסבר: α שורש של $f(x)$ אם ורק אם $x - \alpha \mid f(x)$.
- אם ל-$f(x)$ אין שורשים בשדה F זה לא אומר שהוא אי פריק. למשל ל-$f(x) = (x^2-5)^2$ מעל $\mathbb{Q}$ אין שורשים, אבל הוא פריק.

דוגמה 1.5. האם $x^n - 1$ פריק עבור $n > 1$ (נניח מעל $\mathbb{Q}$)? כן, כי מייד רואים ש-$x = 1$ הוא שורש.

תרגיל 1.6. יהי $f(x)$ פולינום מדרגה 2 או 3. אז $f(x)$ אי פריק אם ורק אם אין ל-$f(x)$ שורשים.

פתרון. אם ל-$f(x)$ יש שורש הסברנו כבר שהוא פריק. מצד שני אם $f(x) = g(x)h(x)$ כאשר $\deg g(x), \deg h(x) \geq 1$ אז אחד מהם חייב להיות מדרגה 1 וזה אומר של-$f(x)$ יש שורש.

דוגמה 1.7. האם $x^2 - x - 1$ פריק מעל $\mathbb{Q}$? בעזרת "נוסחת השורשים" מגלים שהשורשים הם $\frac{1 \pm \sqrt{5}}{2}$ שאינם רציונליים, ולכן הפולינום אי פריק.

תרגיל 1.8. האם הפולינום $x^3 - x + 1$ פריק מעל $\mathbb{Z}_3$?

פתרון. יש בסך הכל 3 מספרים בשדה. מסתבר שאף אחד מהם לא מאפס את הפולינום ולכן הוא אי פריק.

לשמחתנו, גם אם עובדים מעל $\mathbb{Q}$ יש דרך להגיע למספר סופי של שורשים אפשריים שצריך לבדוק.

הערה 1.9. אם $f(x) \in \mathbb{Q}[x]$ אז ניתן להכפיל בבמכפלה משותפת של המכנים ולקבל פולינום עם מקדמים שלמים שהוא פריק אם ורק אם $f(x)$ פריק. לכן כשעובדים מעל $\mathbb{Q}$ ניתן תמיד להניח שהמקדמים שלמים. למשל, לעבוד עם $3x^2 + 2$ במקום עם $\frac{1}{2}x^2 + \frac{1}{3}$.

תרגיל 1.10. יהי $f(x) = a_n x^n + \cdots + a_0$ כאשר כל המקדמים שלמים, הוכיחו כי אם השבר המצומצם $\frac{q}{r}$ הוא שורש של $f(x)$ אז

$$q \mid a_0, \quad r \mid a_n$$

פתרון. לפי הנתון

$$a_n \left(\frac{q}{r}\right)^n + \cdots + a_0 = 0$$

נכפול ב-r^n ונקבל

$$a_n q^n + a_{n-1} q^{n-1} r + \cdots + a_1 q r^{n-1} + a_0 r^n = 0$$

מה שאומר ש-$q \mid a_0 r^n$ ו-$r \mid a_n q^n$, אבל בגלל ש-r ו-q זרים (הרי השבר מצומצם) אז מתקיים

$$q \mid a_0, \quad r \mid a_n$$

תרגיל 1.11. האם הפולינום $x^3 - x - 6$ אי פריק מעל $\mathbb{Q}[x]$?

פתרון. לפי התרגיל הקודם, אם $\frac{q}{r}$ פתרון (שהוא שבר מצומצם) אז

$$q \mid 6, \quad r \mid 1$$

כך שבסך הכל האפשרויות הן:

$$\frac{q}{r} \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

אם עוברים עליהן אפשר לראות ש-2 הוא שורש ולכן הפולינום פריק.

תרגיל 1.12. מצאו את הפירוק של $x^3 - x - 6$ לגורמים אי פריקים מעל $\mathbb{Q}$.

פתרון. היות ש-2 שורש של הפולינום אנחנו יודעים ש-$x - 2 \mid x^3 - x - 6$. נשתמש בחילוק פולינומים ונגלה

$$\frac{x^3 - x - 6}{x - 2} = x^2 + 2x + 3$$

ל-$x^2 + 2x + 3$ אין שורשים מעל $\mathbb{Q}$ ולכן הוא אי פריק. לסיכום הפירוק הוא

$$x^3 - x - 6 = (x - 2)(x^2 + 2x + 3)$$

כמובן ששיטה זו עובדת גם מעל שדות סופיים.

גם עבור פולינום ממעלה גבוהה מ-3 או פולינומים מעל $\mathbb{R}$ אפשר להשתמש בשיטה הזו, אבל רק כדי למצוא שורש רציונלי ולהראות פריקות. אם לא מוצאים שורש אי אפשר להגיד כלום (בינתיים).

הערה 1.13. זכרו כי לפולינום מדרגה אי זוגית מעל $\mathbb{R}$ תמיד יש שורש אחד לפחות ולכן הוא תמיד פריק.

2 תרגול שני

2.1 תזכורת נוספת מתורת החוגים

נעבור לטכניקות אחרות לבדיקת פריקות. מעכשיו נניח כי R תחום שלמות ו-F שדה השברים שלו.

משפט 2.1 (קריטריון אייזנשטיין)**.** יהי $P \lhd R$ אידאל ראשוני. יהי $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ פולינום המקיים

Eisenstein's criterion

- $a_i \in P$ לכל $i \neq n$
- $a_n \notin P$
- $a_0 \notin P^2$

אז f אי פריק ב-$F[x]$ (אין לו פירוק אמיתי מעל R). אם f פרימיטיבי ב-R (המחלק המשותף המרבי של מקדמיו הוא 1), אז f אי פריק ב-$R[x]$.

במקרה הפרטי שבו $P = \langle p \rangle$ עבור איבר ראשוני p התנאים לעיל שקולים לכך ש-p לא מחלק את a_n, מחלק את a_i עבור $i \neq n$ ו-p^2 לא מחלק את a_0.

דוגמה 2.2. $x^n - 4x + 2$ אי פריק מעל $\mathbb{Q}$ כי הוא אייזנשטיין עבור $p = 2 \in \mathbb{Z}$. לפעמים צריך להתחכם יותר.

תרגיל 2.3. האם הפולינום $x^4 + 4x^3 + 6x^2 - 1$ אי פריק מעל $\mathbb{Q}$?

כדי לפתור את התרגיל נעזר בעובדה ההבאה:

טענה 2.4. $f(x)$ אי פריק אם ורק אם $f(x+c)$ אי פריק לכל $c \in F$.

הוכחה. קל לוודא שתמיד $f(x)$ ו-$f(x+c)$ מאותה דרגה ולכן $f(x) = g(x)h(x)$ פירוק אם ורק אם $f(x+c) = g(x+c)h(x+c)$ פירוק. $\square$

פתרון. אם נשים לב שהפולינום שלנו הוא למעשה

$$(x+1)^4 - 4(x+1) + 2$$

היות ש-$x^4 - 4x + 2$ אי פריק לפי קריטריון אייזנשטיין, אז גם הפולינום שלנו אי פריק.

לשיטה הבאה שנציג צריך תזכורת נוספת:

תזכורת 2.5 (גרסה ללמה של גאוס)**.** יהי R תחום שלמות ויהי F שדה השברים שלו. יהי $f(x) \in R[x]$. אז $f(x)$ אי פריק ב-$F[x]$ אם ורק אם הוא לא ניתן לפירוק למכפלת פולינומים לא קבועים שדרגתם קטנה מ-$\deg f(x)$.

תזכורת 2.6 (גרסה ללמה של גאוס)**.** יהי $f(x)$ פולינום שכל מקדמיו שלמים. נניח שהוא פרימיטיבי. אז $f(x)$ אי פריק ב-$\mathbb{Z}[x]$ אם ורק אם הוא אי פריק ב-$\mathbb{Q}[x]$.

משפט 2.7 (שיטת הרדוקציה)**.** יהי $f(x) \in \mathbb{Z}[x]$ ויהי p ראשוני כלשהוא. נסמן ב-$\bar{f}(x)$ את הפולינום המתקבל מביצוע מודולו p למקדמי f. אם $\deg \overline{f}(x) = \deg f(x)$ ו-$\overline{f}(x)$ אי פריק אז גם $f(x)$ אי פריק.

את ההוכחה נשאיר כתרגיל מודרך לשיעורי בית. כעת נראה יישום.

תרגיל 2.8. האם הפולינום $8x^3 - 6x - 1$ אי פריק ב-$\mathbb{Q}[x]$?

פתרון. היות ש-$\gcd(8,6,1) = 1$ הפולינום אי פריק ב-$\mathbb{Q}[x]$ אם ורק אם הוא אי פריק ב-$\mathbb{Z}[x]$. ננסה להשתמש בשיטת הרדוקציה.
ננסה $p = 2$: מתקבל -1 שאינו באותה דרגה כמו f.
ננסה $p = 3$: מתקבל $2x^3 - 1$ שהוא פריק ($x = 2$ שורש).
ננסה $p = 5$: מתקבל $3x^3 - x - 1$ שהוא במקרה אי פריק (בודקים 5 אפשרויות).
לכן גם הפולינום $8x^3 - 6x - 1$ אי פריק.

נחזור לשאלה מתחילת השיעור: למה כל זה יהיה חשוב לנו? זה הרי קורס בתורת השדות!

נזכר ש-$F[x]$ הוא תחום אוקלידי, ובחוג כזה מתקיים ש-$f(x)$ אי פריק, גורר ש-$f(x)$ ראשוני, גורר ש-$\langle f(x) \rangle$ אידיאל ראשוני, גורר ש-$\langle f(x) \rangle$ אידיאל מקסימלי ולכן $F[x]/\langle f(x) \rangle$ שדה.

כלומר התחלנו עם שדה F ופולינום אי פריק מעליו, ובנינו שדה חדש (אולי גדול יותר ומעניין יותר). אנחנו נשתמש בבנייה הזאת כל הזמן במהלך הקורס, אבל היא עובדת (כלומר, מתקבל שדה) רק אם f פולינום אי פריק.

טענה 2.9. לפולינום $f(x) \in F[x]$ מדרגה n מעל שדה יש לכל היותר n שורשים.

תרגיל 2.10. מצאו את הממ"מ (gcd) מעל $\mathbb{Q}$ של הפולינומים $f(x) = x^2 - x - 3$ ו-$g(x) = x^3 - 2x^2 + 1$.

פתרון. נשתמש באלגוריתם אוקלידס (שעובד בתחום האוקלידי $\mathbb{Q}[x]$). נבצע חלוקה עם שארית:

$$x^3 - 2x^2 + 1 = (x^2 - x - 3)(x - 1) + 2x - 2$$
$$x^2 - x - 3 = (2x - 2)\frac{1}{2}x - 3$$

קיבלנו בסוף -3, שהוא הפיך. לכן $\gcd(f(x), g(x)) = 1$, כלומר הם זרים.

תרגיל 2.11. בהמשך לתרגיל הקודם. בטאו את הממ"מ כצירוף לינארי של $f(x), g(x)$.

פתרון. זה אלגוריתם אוקלידס המורחב. נבצע הצבה לאחור

$$-\frac{1}{3}(x^2 - x - 3) + (2x - 2)\frac{1}{6}x = 1$$
$$-\frac{1}{3}(x^2 - x - 3) + (x^3 - 2x^2 + 1 - (x^2 - x - 3)(x - 1))\frac{1}{6}x = 1$$

כלומר

$$\frac{1}{6}x(x^3 - 2x^2 + 1) - (\frac{1}{6}x(x - 1) + \frac{1}{3})(x^2 - x - 3) = 1$$

תרגיל 2.12. חשבו את ההופכי של $x^3 - 2x^2 + 1$ בשדה $\mathbb{Q}[x]/\langle x^2 - x - 3\rangle$.

פתרון. ראשית נזכור שהאיברים בשדה הם מהצורה

$$f(x) + \langle x^2 - x - 3\rangle$$

כלומר הכל עובד "עד כדי" חיבור כפולה של $x^2 - x - 3$. לפי התרגילים הקודמים

$$x^3 - 2x^2 + 1 + \langle x^2 - x - 3\rangle = 2x - 2 + \langle x^2 - x - 3\rangle$$

וההופכי הוא

$$\frac{1}{6}x + \langle x^2 - x - 3\rangle$$

3 תרגול שלישי

3.1 הרחבת שדות

Subfield
Field extension

הגדרה 3.1. יהי $K \subseteq F$ תת־שדה של K. במקרה זה נאמר כי K הוא הרחבה של F ונסמן זאת K/F. כן, זה אותו סימון של חוג מנה, אבל אנחנו לא נתבלבל בינהם כי שדה הוא חוג פשוט ומכאן שחוגי המנה שלו לא מעניינים.

Intermediate field

אם ישנה שרשרת של שדות $F \subseteq L \subseteq K$ נאמר כי L הוא שדה ביניים של ההרחבה K/F.

תזכורת 3.2. תהי K/F הרחבת שדות ויהי $a \in K$. הסיפוח של a ל-F הוא תת־השדה (של K) הקטן ביותר שמכיל את F ואת a. נסמן אותו $F(a)$. הרחבה כזו, באיבר אחד, נקראת גם הרחבה פשוטה. Simple extension

בדרך אחרת, השדה $F(a)$ הוא החיתוך של כל תת־השדות שמכילים גם את F וגם את a. חשוב להדגיש את התכונה הפשוטה (אך חשובה) הבאה: אם L שדה ביניים המכיל את a אז $F(a) \subseteq L$. נדגיש כי $F(a) = F$ אם ורק אם $a \in F$.

דוגמה 3.3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. הסבר: צריך רק לוודא שהוא סגור לכפל לחיבור ולהופכי ואז זה תת־שדה של $\mathbb{R}$. מצד שני, ברור שכל שדה שמכיל את $\mathbb{Q}$ ו-$\sqrt{2}$ מכיל גם את השדה מסגירות לחיבור ולכפל. שימו לב כי $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ מפני ש-$\left(\sqrt{2}\right)^{-1} = \frac{1}{2}\sqrt{2}$.

תרגיל 3.4. הוכיחו כי $\sqrt{6} \notin \mathbb{Q}[\sqrt{2}]$.

פתרון. נניח בשלילה ש-$\sqrt{6} \in \mathbb{Q}[\sqrt{2}]$. אז קיימים $a, b \in \mathbb{Q}$ עבורם

$$\sqrt{6} = a + b\sqrt{2}$$

לא ייתכן ש-$b = 0$ כי $\sqrt{6}$ לא רציונלי, ולא ייתכן ש-$a = 0$ כי $\sqrt{3}$ לא רציונלי. נעלה משוואה זו בריבוע ונקבל

$$6 = a^2 + 2\sqrt{2}ab + 2b^2$$

כלומר

$$\sqrt{2} = \frac{6 - a^2 - 2b^2}{2ab}$$

מותר לחלק כי כבר הוכחנו $ab \neq 0$. קיבלנו ש-$\sqrt{2}$ רציונלי, וזו סתירה.

הערה 3.5. כמו שאפשר לספח איבר אחד, אפשר לספח קבוצת איברים, והעיקרון דומה.

תרגיל 3.6. האם $\sqrt{2}i \in \mathbb{Q}[\sqrt{2} + i]$?

פתרון. על פניו אפשר לחשוד שלא, כמו בתרגיל הקודם. אבל בעצם

$$(\sqrt{2} + i)^2 = 2 + 2\sqrt{2}i - 1 = 1 + 2\sqrt{2}i$$

נחסר 1 ונחלק ב-2 (פעולות שמשאירות אותנו בתוך השדה) ונקבל כי

$$\sqrt{2}i \in \mathbb{Q}[\sqrt{2} + i]$$

הגדרה 3.7. תהי K/F הרחבת שדות. בפרט K הוא מרחב וקטורי מעל F. הממד של K/F הוא הממד של K מעל F ומסמנים אותו $[K : F] = \dim_F K$. לא להתבלבל עם הסימון הזהה של אינדקס שראינו בתורת החבורות. Dimension

דוגמה 3.8. לכל שדה F מתקיים $[K : F] = 1$ אם ורק אם $K = F$.

דוגמה 3.9. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2$.

משפט 3.10. יהי f פולינום אי פריק מעל F עם שורש a, אז $\deg f = [F(a) : F]$.

במילים אחרות, אם K/F הרחבת שדות ו-$a \in K$ אלגברי מעל F, אז

$$F[x]/\langle f(x)\rangle \cong F[a] \cong F(a)$$

כאשר $f(x)$ הוא פולינום מינימלי של a. שימו לב שאם $b \in K$ שורש אחר של $f(x)$, אז $f(x)$ הוא פולינום מינימלי גם של b ומתקיים $F[a] \cong F[b]$. גם הכיוון ההפוך נכון:

טענה 3.11. אם K/F הרחבת שדות כך ש-$K \cong F[a]$, אז $K = F[b]$ עבור איזשהו $b \in K$ שהוא שורש של פולינום מינימלי של a. זה כמובן לא אומר ש-$b \in F[a]$.

תזכורת 3.12 (כפליות הממד)**.** אם $F \subseteq L \subseteq K$, אז

$$[K : L][L : F] = [K : F]$$

תרגיל 3.13. תהי $F \subseteq K$ הרחבת שדות ויהיו $a, b \in K \backslash F$. נניח כי

$$[F(a) : F] = n, \quad [F(b) : F] = m$$

הוכיחו כי $[F(a,b) : F] \leq nm$.

פתרון. הנתון $[F(a) : F] = n$ אומר לנו שהפולינום המינימלי $m_a \in F[x]$ של a מעל F הוא מדרגה n. אבל m_a הוא גם פולינום מעל $F(b)$ שמאפס את a. לכן הפולינום המינימלי של a מעל $F(b)$ מחלק את m_a ולכן הוא מדרגה קטנה (או שווה) ממנו. לכן

$$[F(a,b) : F(b)] \leq n$$

ומכאן נקבל בעזרת כפליות הממד:

$$[F(a,b) : F(b)] = [F(a,b) : F(b)]\,[F(b) : F] \leq nm$$

תרגיל 3.14. בהמשך לתרגיל הקודם, הראו שאם $(n,m) = 1$ אז $[F(a,b) : F] = nm$.

פתרון. נשים לב כי

$$[F(a,b) : F] = [F(a,b) : F(a)][F(a) : F] = n[F(a,b) : F(a)]$$

$$[F(a,b) : F] = [F(a,b) : F(b)][F(b) : F] = m[F(a,b) : F(b)]$$

כלומר $n, m \mid [F(a,b) : F]$. לפי תורת המספרים האלמנטרית

$$nm = [n,m] \mid [F(a,b) : F]$$

כי n, m זרים, ולכן $[F(a,b) : F] = nm$.

דוגמה 3.15. $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 6$

שאלה 3.16. תהי $F(a)$ הרחבה של F ונניח ש-f הוא הפולינום המינימלי של a (מעל F). האם כל השורשים של f נמצאים ב-$F(a)$?

פתרון. לפעמים כן (למשל $\mathbb{Q}(\sqrt{2})$) אבל זה לא תמיד קורה. למשל ניקח את $\mathbb{Q}(\sqrt[3]{2})$. ברור כי $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ ושהפולינום המינימלי של $\sqrt[3]{2}$ הוא x^3-2, אבל שאר השורשים שלו הם מרוכבים ולכן לא נמצאים ב-$\mathbb{Q}(\sqrt[3]{2})$.

הערה 3.17. המצבים שבהם כן כל השורשים נמצאים בהרחבה הם חשובים ונדבר עליהם בהרחבה בהמשך הקורס.

תרגיל 3.18. נתון כי הפולינום המינימלי של a (מעל $\mathbb{Q}$) הוא $x^3-6x^2+9x+11$ מצאו את הפולינום המינימלי של $\frac{1}{a}$.

פתרון. נציב a בפולינום ונשים לב כי

$$a^3-6a^2+9a+11=0$$

ולכן

$$1-\frac{6}{a}+\frac{9}{a^2}+\frac{11}{a^3}=0$$

כלומר הפולינום $11x^3+9x-6x+1$ מאפס את $\frac{1}{a}$. אין לפולינום שורשים ב-$\mathbb{Q}$ (אם b היה שורש אז $\frac{1}{b}$ שורש של הפולינום המקורי בסתירה לאי פריקות). לכן הוא הפולינום המינימלי (צריך לחלק ב-11 כדי להפוך אותו למתוקן).

4 תרגול רביעי

4.1 שורשי יחידה

הגדרה 4.1. יהי F שדה. איבר $\rho \in F$ נקרא שורש יחידה פרימיטיבי (או קדום) מדרגה n אם הסדר שלו ב-F^* הוא n. כלומר $\rho^n=1$ וגם $\rho^i \neq 1$ לכל $1 \leq i < n$.

Primitive root of unity

דוגמה 4.2. ב-$\mathbb{C}$ לכל $n \in \mathbb{N}$ יש שורש יחידה פרמיטיבי, למשל $\rho_n=e^{2\pi i/n}$.

הערה 4.3. אם ρ שורש יחידה פרימיטיבי מדרגה n, אז ρ^k הוא שורש יחידה פרימיטיבי מדרגה n אם ורק אם $(n,k)=1$.

תרגיל 4.4. יהי $\rho \in F$ שורש יחידה פרמיטיבי מדרגה n. הוכיחו כי $1,\rho,\ldots,\rho^{n-1}$ כולם שונים זה מזה, והראו כי

$$x^n-1=\prod_{i=1}^{n}\left(x-\rho^i\right)$$

פתרון. נניח כי $\rho^i=\rho^j$ כאשר $i \leq j$. אז $\rho^{j-i}=1$. אבל $0 \leq j-i < n$, ולכן בהכרח $j=i$, כי ρ הוא שורש יחידה פרמיטיבי מדרגה n.

נשים לב ש-ρ^i הוא שורש של x^n-1 לכל i. מכיוון שהם שונים, אלו הם כל השורשים של x^n-1, כי זה פולינום מעל שדה מדרגה n. לכן $x^n-1=\prod_{i=1}^{n}\left(x-\rho^i\right)$.

דוגמה 4.5. יהי ρ שורש יחידה פרימיטיבי מדרגה n. אז

$$\mathbb{Q}(\rho) = \left\{a_0 + a_1\rho \cdots + a_{n-1}\rho^{n-1} \,\middle|\, a_i \in \mathbb{Q}\right\}$$

דוגמה 4.6. יהי p ראשוני ויהי ρ_p שורש יחידה פרמיטיבי מדרגה p. אז הוא בוודאי מאפס את $x^p - 1$. נחפש גורם אי פריק של פולינום זה:

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

שהוא הפולינום המינימלי של ρ_p כי למזלנו פתרנו את תרגילי הבית בתורת החוגים שבהם הוכחנו שהוא אי פריק. לכן $[\mathbb{Q}(\rho_p) : \mathbb{Q}] = p - 1$.

תרגיל 4.7. נסמן $\rho = e^{\frac{\pi i}{6}}$, שהוא שורש יחידה פרמיטיבי מדרגה 12. הוכיחו כי

$$\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{3}, i)$$

פתרון. נשים לב ש-$\rho = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. אז ברור ש-$\mathbb{Q}(\rho) \subseteq \mathbb{Q}(\sqrt{3}, i)$. מצד שני $\rho^3 = i$ ולכן $i \in \mathbb{Q}(\rho)$ וגם

$$\sqrt{3} = 2(\rho - \frac{i}{2}) \in \mathbb{Q}(\rho)$$

ולכן יש שוויון.

תרגיל 4.8. בהמשך לתרגיל הקודם, חשבו את $[\mathbb{Q}(\rho) : \mathbb{Q}]$.

פתרון. קל לראות ש-$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ וש-$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$ ולכן

$$[\mathbb{Q}(\rho) : \mathbb{Q}] = 4$$

תרגיל 4.9. בהמשך לתרגיל הקודם, מצאו פולינום מינימלי של ρ.

פתרון. אנחנו יודעים כי $\rho^{12} = 1$. כלומר מדובר בשורש של $x^{12} - 1$. אבל זה כמובן פריק. נתחיל לפרק

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

ונשים לב כי ρ שורש של $x^6 + 1$. לפי הנוסחה $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$ נקבל

$$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

מפני ש-ρ אינו שורש של $x^2 + 1$, אז הוא צריך להיות שורש של $x^4 - x^2 + 1$. זה פולינום אי פריק כי אנחנו כבר יודעים ש-$[\mathbb{Q}(\rho) : \mathbb{Q}] = 4$. למעשה יש לנו דרך חדשה להוכיח שפולינום הוא אי פריק.

הערה 4.10. בהמשך הקורס נלמד על הפירוק המלא של $x^n - 1$.

4.2 שדות פיצול

הגדרה 4.11. יהי $f \in F[x]$. הפולינום f מתפצל ב-F אם אפשר לפרק אותו למכפלה של גורמים לינאריים. אם f מתפצל בהרחבת שדות E/F, נאמר ש-E הוא שדה מפצל של f. Split
E Splits f

דוגמה 4.12. $\mathbb{Q}[\sqrt{2}]$ מפצל את x^2-2 מעל $\mathbb{Q}$. באופן דומה $\mathbb{Q}[\sqrt{\Delta}]$ מפצל את ax^2+bx+c כאשר Δ היא הדיסקרימיננטה. אפשר לפצל כמה פולינומים בבת אחת, למשל $\mathbb{C}$ הוא שדה מפצל של כל פולינום מעל $\mathbb{Q}$.

הגדרה 4.13. יהי $f \in F[x]$. נאמר ש-E/F הוא שדה פיצול של f אם הוא שדה מפצל מינימלי. כלומר אין שדה ביניים (לא טריוויאלי) שהוא שדה מפצל. Splitting field

משפט 4.14. יהי $f \in F[x]$. כל שדות הפיצול של f מעל F איזומורפיים.

תרגיל 4.15. מצאו את שדה הפיצול של x^5-2 מעל $\mathbb{Q}$ ואת הממד שלו.

פתרון. נסמן $\rho = e^{2\pi i/5}$. אז השורשים של הפולינום הם

$$\sqrt[5]{2}, \sqrt[5]{2}\rho, \dots, \sqrt[5]{2}\rho^4$$

ולכן שדה הפיצול הוא $E = \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}\rho, \dots, \sqrt[5]{2}\rho^4)$. קל לבדוק כי

$$\mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}\rho, \dots, \sqrt[5]{2}\rho^4) = \mathbb{Q}(\sqrt[5]{2}, \rho)$$

וקל לחשב $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$. כמו כן, נשים לב כי x^5-1 מאפס את ρ. אבל הפולינום הזה אינו הפולינום המינימלי כי הוא פריק. אנחנו כבר יודעים כי

$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$$

ושהגורם $x^4+x^3+x^2+x+1$ הוא אי פריק. לכן $[\mathbb{Q}(\rho) : \mathbb{Q}] = 4$. מפני ש-$\gcd(4,5)=1$, אז לפי תרגיל משבוע שעבר (או מתרגיל הבית), נקבל $[E : \mathbb{Q}] = 20$.

תרגיל 4.16. מצאו את שדה הפיצול של x^4-4x^2-1 מעל $\mathbb{Q}$.

פתרון. צריך בסך הכל למצוא את השורשים. מציבים $t = x^2$ ופותרים. מגלים שהשורשים הם

$$\pm\sqrt{2+\sqrt{5}}, \pm\sqrt{2-\sqrt{5}}$$

ולכן שדה הפיצול הוא $\mathbb{Q}(\sqrt{2+\sqrt{5}}, \sqrt{2-\sqrt{5}})$.

תרגיל 4.17. הוכיחו כי $f(x) = x^4-4x^2-1$ הוא אי פריק מעל $\mathbb{Q}$.

פתרון. דרך א': ברור של-$f(x)$ אין שורשים ב-$\mathbb{Q}$ (כי מצאנו את השורשים). אז נשאר לוודא שהוא לא מתפרק למכפלת פולינומים ממעלה 2. אבל אנחנו כבר יודעים

$$x^4-4x^2-1=(x-\sqrt{2+\sqrt{5}})(x+\sqrt{2+\sqrt{5}})(x-\sqrt{2-\sqrt{5}})(x+\sqrt{2-\sqrt{5}})$$

וקל לבדוק שכל מכפלה של שני גורמים מכאן אינה פולינום מעל $\mathbb{Q}$.

דרך ב': כמו בתרגיל הבית מוכיחים ש-$[\mathbb{Q}(\sqrt{2+\sqrt{5}}):\mathbb{Q}]=4$. לכן הפולינום המינימלי של $\sqrt{2+\sqrt{5}}$ הוא ממעלה 4, לכן x^4-4x^2-1 מינימלי ולכן אי פריק.

תרגיל 4.18. כמה תת־שדות יש ל-$\mathbb{C}$ שאיזומורפיים ל-$\mathbb{Q}(\sqrt{2+\sqrt{5}})$?

פתרון. אם $K\subseteq\mathbb{C}$ הוא שדה ויש $\varphi\colon\mathbb{Q}(\sqrt{2+\sqrt{5}})\to K$ איזומורפיזם, אז φ מקבע את $\mathbb{Q}$. כמו כן $\varphi(\sqrt{2+\sqrt{5}})$ בהכרח נשלח לשורש של x^4-4x^2-1 שזה פולינום עם 4 שורשים (שונים) בסך הכל. מכאן מסיקים שכל אחד מבין

$$\mathbb{Q}(\sqrt{2+\sqrt{5}}),\mathbb{Q}(-\sqrt{2+\sqrt{5}}),\mathbb{Q}(\sqrt{2-\sqrt{5}}),\mathbb{Q}(-\sqrt{2-\sqrt{5}})$$

מוכל ב-K. לכן הוא צריך להיות שווה ל-K משיקולי ממד. כעת נשים לב שהשניים הימניים והשמאליים למעשה שווים. אז יש רק שני תת־שדות והם $\mathbb{Q}(\sqrt{2-\sqrt{5}})$ ו-$\mathbb{Q}(\sqrt{2+\sqrt{5}})$. אלו שדות איזומורפיים אבל שונים, כי אחד מרוכב והשני ממשי.

תרגיל 4.19. נסמן $E=\mathbb{Q}(\sqrt{2+\sqrt{5}},\sqrt{2-\sqrt{5}})$. חשבו את הממד שלו מעל $\mathbb{Q}$.

פתרון. כבר ראינו $[\mathbb{Q}(\sqrt{2+\sqrt{5}}):\mathbb{Q}]=4$, ונשאר לבדוק מהו $[E:\mathbb{Q}(\sqrt{2+\sqrt{5}})]$. ברור שזה לא 1 כי

$$\sqrt{2-\sqrt{5}}\notin\mathbb{Q}(\sqrt{2+\sqrt{5}})$$

שהוא מספר מרוכב ואילו $\mathbb{Q}(\sqrt{2+\sqrt{5}})$ ממשי. מצד שני, נשים לב ש-$\sqrt{5}\in\mathbb{Q}(\sqrt{2+\sqrt{5}})$ ולכן

$$x^2-2+\sqrt{5}$$

פולינום מאפס של $\sqrt{2-\sqrt{5}}$ מעל $\mathbb{Q}(\sqrt{2+\sqrt{5}})$. לכן $[E:\mathbb{Q}(\sqrt{2+\sqrt{5}})]=2$ וקיבלנו ש-$[E:\mathbb{Q}]=8$.

תרגיל 4.20. יהי F שדה ממאפיין p. נתבונן בפולינום $f(x)=x^p-x-a$. יהי α שורש של $f(x)$. מצאו את שדה הפיצול של α מעל F.

פתרון. נשים לב כי לכל $k\in\{0,1,\dots,p-1\}$ מתקיים

$$f(\alpha+k)=(\alpha+k)^p-(\alpha+k)-a=\alpha^p+k^p-\alpha-k-a=0$$

מפני ש-$(\alpha+k)^p=\alpha^p+k^p$. כלומר $\{\alpha+k\}_{k=0}^{p-1}$ הם כל השורשים של f, כי הוא מדרגה p. לכן שדה הפיצול הוא

$$F[\alpha]=F[\alpha,\alpha+1,\dots,\alpha+p-1]$$

טענה 4.21. לכל פולינום $f \in F[x]$ יש שדה מפצל שממדו אינו עולה על $(\deg f)!$.

דוגמה 4.22. בתרגיל 4.20, אם $f(x)$ אי פריק, אז $[F[\alpha]:F]=p$ וזה יכול להיות ממש קטן מ-$p!$.

5 תרגול חמישי

5.1 פולינומים ספרבילים

הגדרה 5.1. פולינום $f(x)$ המתפצל בשדה E נקרא ספרבילי (פָּרִיד) אם בפירוק שלו אין גורם כפול מן הצורה $(x-\alpha)^2$. בצורה פחות מדוייקת, אפשר לומר שכל השורשים של $f(x)$ שונים זה מזה בשדה הפיצול שלו, ולמעשה אין תלות ב-E. Separable

דוגמה 5.2. נתבונן ב-$F=\mathbb{F}_2(t)$ שהוא שדה השברים של החוג $\mathbb{F}_2[t]$. הפולינום $f(x)=x^2-t$ הוא אי פריק ואי ספרבילי. רואים זאת לפי החישוב

$$x^2-t=(x-\sqrt{t})(x+\sqrt{t})=(x+\sqrt{t})^2$$

כי השדה הוא ממאפיין 2, והוא אי פריק כי $\sqrt{t}\notin F$.

הערה 5.3. דרך אפקטיבית לזהות פולינום ספרבילי היא לפי הקריטריון: $f(x)$ ספרבילי אם ורק אם $\gcd(f(x),f'(x))=1$.
בפרט, אם $f(x)$ אי פריק, אז הוא ספרבילי אם ורק אם $f'\neq 0$.

תרגיל 5.4. האם הפולינום $x^4-8x+16\in\mathbb{Q}[x]$ ספרבילי?

פתרון. הנגזרת היא $4x^3-8$. צריך לבדוק האם הם זרים. נשתמש באלגוריתם אוקלידס כאשר קודם נחלק ב-4 (שהוא הפיך) ונמשיך עם x^3-2:

$$x^4-8x+16=x(x^3-2)-6x+16$$

נחלק ב--6 ונמשיך עם $x-\frac{8}{3}$:

$$(x^3-2)=(x^2+\frac{8}{3}x+\frac{64}{9})(x-\frac{8}{3})+\frac{512}{27}$$

ולכן הפולינום זרים. כלומר הפולינום $x^4-8x+16$ ספרבילי.

תרגיל 5.5. האם הפולינום x^4-8x^2+16 ספרבילי?

פתרון. קל לפתור על ידי חישוב השורשים ישירות, אבל נשתמש בנגזרת במקום. הנגזרת היא $4x^3-16x$ ונשתמש באלגוריתם אוקלידס עם x^3-4x. נחשב

$$x^4-8x^2+16=x(x^3-4x)-4x^2+16$$

ומפני ש-$x^3-4x=x(x^2-4)$, כלומר לפולינום ולנגזרתו יש גורם משותף x^2-4, נקבל כי x^2-4x^2+16 לא ספרבילי.

Separable extension

הגדרה 5.6. הרחבת שדות K/F תקרא ספרבילית (פְּרִידָה) אם הפולינום המינימלי של כל $a \in K$ מעל F הוא ספרבילי.

דוגמה 5.7. אם F שדה ממאפיין $p > 0$, אז $F(t)/F$ אינה ספרבילית כי $x^p - t$ לא ספרבילי.

תרגיל 5.8. תהי K/F הרחבת שדות ספרבילית, ויהי L שדה ביניים. הוכיחו כי גם L/F וגם K/L ספרביליות.

פתרון. ברור ש-L/F ספרבילית, כי כל איבר ב-L הוא איבר של K. עבור K/L, יהי $a \in K$ ויהי $m_{a,F}$ הפולינום המינימלי של a מעל F. אז $m_{a,L}|m_{a,F}$ ולכן ל-$m_{a,L}$ אין שורשים כפולים. לכן K/L ספרבילית.

6 תרגול שישי

תרגיל 6.1. יהיו $f, g\colon F(a_1, \ldots, a_n) \to K$ שני הומומורפיזמים שמקיימים

$$f(x) = g(x) \quad \forall x \in F$$
$$f(a_i) = g(a_i) \quad 1 \le i \le n$$

הוכיחו כי $f = g$.

פתרון. הקבוצה $\{x \in F(a_1, \ldots, a_n) \mid f(x) = g(x)\}$ היא תת־שדה של $F(a_1, \ldots, a_n)$ (קל לבדוק) והיא מכילה את $F, a_1, \ldots, a_n$. לכן היא כל $F(a_1, \ldots, a_n)$, ונסיק $f = g$.

Extension of an embedding

הגדרה 6.2. תהי K/F הרחבת שדות, ויהי $\varphi\colon F \to E$ שיכון (למה כל הומומורפיזם של שדות הוא שיכון?). שיכון $\overline{\varphi}\colon K \to E$ נקרא המשכה של φ אם הצמצום של $\overline{\varphi}$ ל-F שווה ל-φ.

תרגיל 6.3. תהי K/F הרחבת שדות. יהי $g(x) \in F[x]$ אי פריק ויהיו a, b שני שורשים של g. הוכיחו כי יש איזומורפיזם

$$f\colon F(a) \to F(b)$$

המקיים כי $f(a) = b$ וכן $f(\alpha) = \alpha$ לכל $\alpha \in F$.

פתרון. נסתכל על העתקת ההכלה $i : F \hookrightarrow F(b)$. אפשר להרחיב אותה להעתקה

$$\hat{i}\colon F[x] \to F(b)$$

כך ש-$f(x) = b$ לפי הגדרת פולינומים. כמובן שכעת זו העתקה על. נשים לב שהגרעין הוא $\langle g(x) \rangle$ (כי $g(x)$ פולינום מינימלי של a). לפי משפט האיזומורפיזם הראשון

$$f\colon F[x]/\langle g(x) \rangle \to F(b)$$

הוא איזומורפיזם ובאופן דומה ניתן לבנות איזומורפיזם $g\colon F[x]/\langle g(x) \rangle \to F(a)$. האיזומורפיזם שאנחנו מחפשים הוא gf^{-1}.

תזכורת 6.4. תהי K/F הרחבת שדות ויהיו $a,b\in K$ איברים עם פולינומים מינימליים m_a,m_b מעל F, בהתאמה. נסמן ב-E_a,E_b את שדות הפיצול של m_a,m_b. אז כל איזומורפיזם

$$f\colon F(a)\to F(b)$$

שמקבע את איברי F (כלומר $f(\alpha)=\alpha$ לכל $\alpha\in F$) ניתן להרחיב לאיזומורפיזם $f\colon E_a\to E_b$.

תרגיל 6.5. יהי $g(x)\in F[x]$ פולינום אי פריק עם שדה פיצול E. ויהיו a,b שני שורשים של $g(x)$. הוכיחו כי יש איזומורפיזם $f\colon E\to E$ שמקבע את איברי F ומקיים $f(a)=b$.

פתרון. לפי תרגיל קודם יש איזומורפיזם $f\colon F(a)\to F(b)$ שמקבע את איברי F ושולח $f(a)=b$ לפי התזכורת אפשר להרחיב אותו לכל E.

הגדרה 6.6. אם $F,L\subseteq K$, אז הקומפוזיטום של F ו-L הוא תת־השדה המינימלי שמכיל את F,L ומסומן בדרך כלל FL או $F\vee L$. Compositum

תרגיל 6.7. יהיו $F\subseteq K\subseteq E$ שדות כך ש-E שדה פיצול של פולינום $f(x)\in F[x]$ כלשהו ו-K מכיל שורש a של $f(x)$. הוכיחו כי ניתן למצוא $K_1,\dots,K_r$ תת־שדות של E שכולם איזומורפיים ל-K כך שמתקיים

$$E=K_1\vee K_2\vee\cdots\vee K_r$$

פתרון. נסמן ב-$b_1,\dots,b_r$ את שורשי F. ראינו כבר שיש איזומורפיזמים

$$f_i\colon F(a)\to F(b_i)$$

ואפשר להרחיב אותם $f_i\colon E\to E$. נסמן $K_i=f_i(K)$ לכל i. אז כמובן $K_i\cong K$, ולכל i מתקיים $K_i\subseteq E$ ולכן

$$K_1\vee K_2\vee\cdots\vee K_r\subseteq E$$

מצד שני כל השורשים של f שייכים ל-$K_1\vee K_2\vee\cdots\vee K_r$ ולכן $E\subseteq B_1\vee B_2\vee\cdots\vee B_k$, כדרוש.

6.1 חבורת גלואה

הגדרה 6.8. אוטומורפיזם של הרחבת שדות K/F הוא אוטומורפיזם $\varphi\colon K\to K$ המקבע את איברי F. כלומר $\varphi(a)=a$ לכל $a\in F$. באופן שקול, זו העתקה לינארית של מרחבים וקטוריים מעל F. Automorphism

דוגמה 6.9. כל אנדומורפיזם $\varphi\in\mathrm{End}(K)$ הוא אוטומורפיזם של ההרחבה K מעל תת־השדה הראשוני של K.

הגדרה 6.10. תהי K/F הרחבת שדות. חבורת גָּלוּאָה $\mathrm{Gal}(K/F)$ היא החבורה של כל האוטומורפיזמים של K/F עם פעולת ההרכבה. זו תת־חבורה של $\mathrm{Aut}(K)$. Galois group

סימונים נוספים עבור $\mathrm{Gal}(K/F)$ הם $G(K/F)$, $G_{K/F}$ ו-$\mathrm{Aut}(K/F)$.

הדבר המרכזי שנעשה בקורס הזה הוא (לנסות) ללמוד הרחבות שדות באמצעות חבורות גלואה.

דוגמה 6.11. תהי $F/\mathbb{Q}$ הרחבת שדות. אז $\mathrm{Gal}(F/\mathbb{Q})$ היא למעשה $\mathrm{Aut}(F)$, לפי דוגמה 6.9. למשל ראינו (כנראה בתורת החוגים) כי $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$ ולכן זו חבורת גלואה של ההרחבה $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

באופן דומה $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{id}\}$ כי כל אוטומורפיזם של $\mathbb{R}$ מעביר מספר חיובי למספר חיובי (כי $\varphi(a^2) = \varphi(a)^2$), ומכאן שהוא שומר על יחס הסדר ב-$\mathbb{R}$. לכן כל אוטומורפיזם של $\mathbb{R}$ הוא העתקת הזהות.

תרגיל 6.12 (בהרצאה)**.** יהי $f(x) \in F[x]$ ויהי $\sigma \in \mathrm{Gal}(K/F)$. הוכיחו שלכל שורש $a \in K$ של f, גם $\sigma(a)$ הוא שורש.

פתרון. אם $f(x) = c_0x^n + \ldots + c_n$, אז

$$c_0a^n + \ldots + c_n = 0$$

מפעילים σ על המשוואה הזו ומקבלים את הדרוש כי σ מקבע את כל המקדמים.

7 תרגול שביעי

7.1 מבוא לחישוב חבורות גלואה

תרגיל 7.1. חשבו את $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

פתרון. נסמן $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ונשים לב שזהו שדה הפיצול של $(x^2-2)(x^2-3)$. כל אוטומורפיזם של E נקבע לחלוטין לפי תמונות $\sqrt{2}$ ו-$\sqrt{3}$. שימו לב כי $\sqrt{2}$ חייב להשלח לשורשים של הפולינום המינימלי שלו x^2-2 שהם $\pm\sqrt{2}$. הפולינום המינימלי של $\sqrt{3}$ מעל $\mathbb{Q}(\sqrt{2})$ הוא עדין x^2-3 ולכן $\sqrt{3}$ ישלח ל-$\pm\sqrt{3}$. ישנם ארבעה שורשים שנזהה אותם עם המספרים

$$1 \leftrightarrow \sqrt{2}, \quad 2 \leftrightarrow -\sqrt{2}, \quad 3 \leftrightarrow \sqrt{3}, \quad 4 \leftrightarrow -\sqrt{3}$$

ונוכל לשכן את $\mathrm{Gal}(E/\mathbb{Q})$ ב-S_4 בעזרת זיהוי זה. ישנן ארבע אפשרויות:

האוטומורפיזם $\mathrm{id} \in \mathrm{Gal}(E/\mathbb{Q})$ השולח כל שורש לעצמו. הוא מתאים לתמורת הזהות $\mathrm{id} \in S_4$.

האוטומורפיזם השולח $\sqrt{2} \mapsto -\sqrt{2}$ ו-$\sqrt{3} \mapsto \sqrt{3}$ מתאים לתמורה $(1\ 2)$.

האוטומורפיזם השולח $\sqrt{2} \mapsto \sqrt{2}$ ו-$\sqrt{3} \mapsto -\sqrt{3}$ מתאים לתמורה $(3\ 4)$.

האוטומורפיזם השולח $\sqrt{2} \mapsto -\sqrt{2}$ ו-$\sqrt{3} \mapsto -\sqrt{3}$ מתאים לתמורה $(1\ 2)(3\ 4)$.

בסך הכל $\mathrm{Gal}(E/\mathbb{Q}) \cong V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ כאשר V היא חבורת הארבעה של קליין. לצורך חינוכי עתידי נשים לב כי סריג תת־החבורות של V הוא

$$\begin{tikzcd}
 & V \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle(1\ 2)\rangle \arrow[dr, dash] & \langle(1\ 2)(3\ 4)\rangle \arrow[d, dash] & \langle(3\ 4)\rangle \arrow[dl, dash] \\
 & \{\mathrm{id}\} &
\end{tikzcd}$$

ואילו סריג תת־השדות של E הוא

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

תרגיל 7.2. חשבו את $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

פתרון (בהרצאה). הפולינום המינימלי של $\sqrt[3]{2}$ הוא x^3-2. יהי $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. גם $\varphi(\sqrt[3]{2})$ הוא גם שורש של x^3-2. אבל $\varphi(\sqrt[3]{2})$ הוא מספר ממשי ולכן בהכרח $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. למה זה שימושי? כעת נשתמש בטענה שכבר הוכחנו בעבר. אם

$$\varphi, \psi \colon F(a_1,\dots,a_n) \to F(a_1,\dots,a_n)$$

הם הומומורפיזמים שמסכימים על F ועל האיברים $\{a_1,\dots,a_n\}$, אז $\varphi=\psi$. במונחים החדשים, המשמעות היא ששני איברים בחבורת גלואה של $F(a_1,\dots,a_n)/F$ שמסכימים על $\{a_1,\dots,a_n\}$ הם שווים. במקרה שלנו, מפני ש-$\varphi(\sqrt[3]{2}) = \mathrm{id}(\sqrt[3]{2})$ נקבל ש-$\varphi = \mathrm{id}$, ולכן $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$ היא החבורה הטריוויאלית.

תרגיל 7.3. חשבו את $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\rho)/\mathbb{Q})$ כאשר ρ הוא שורש יחידה פרימיטיבי מסדר 3.

פתרון. מפני ש-$\mathbb{Q}(\sqrt[3]{2}\rho)$ ו-$\mathbb{Q}(\sqrt[3]{2})$ הן הרחבות איזומורפיות של $\mathbb{Q}$, אז גם כאן חבורת גלואה היא טריוויאלית.

תרגיל 7.4. חשבו את $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$.

פתרון. הפולינום המינימלי של $\sqrt[4]{2}$ מעל $\mathbb{Q}(\sqrt{2})$ הוא כמובן $x^2-\sqrt{2}$. אם φ בחבורת גלואה, אז לפי מה שראינו קודם $\varphi(\sqrt[4]{2}) = \pm\sqrt[4]{2}$. אם $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}$, אז כבר הסקנו כי $\varphi = \mathrm{id}$ שהוא בוודאי איבר בחבורת גלואה.

עבור האפשרות $\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}$ צריך להזהר! בשלב הזה אנחנו לא יודעים בכלל אם קיימת φ שמקיימת את הנ"ל. השוו לתרגיל הקודם בו גילינו עם שיקול הממשיות שאין φ המקיימת $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\rho$. מפני שזו בסך הכל הרחבה מסדר 2 אנחנו יודעים שאפשר לכתוב איברים של $\mathbb{Q}(\sqrt[4]{2})$ בצורה $a + b\sqrt[4]{2}$ כאשר $a, b \in \mathbb{Q}(\sqrt{2})$. אם אכן קיימת φ כזו, אז בהכרח מתקיים

$$\varphi(a + b\sqrt[4]{2}) = a - b\sqrt[4]{2}$$

ניתן לבדוק את כל הדרישות ולראות שזה אכן אוטומורפיזם המקבע את $\mathbb{Q}(\sqrt{2})$. לכן בחבורת גלואה יש שני איברים בדיוק, ויש רק חבורה אחת (עד כדי איזומורפיזם) בעלת שני איברים והיא $\mathbb{Z}_2$.

כמו שניתן לראות, אפילו בדוגמאות פשוטות לא ממש קל לראות מה היא חבורת גלואה. אנחנו צריכים כלים יותר מתוחכמים. נתחיל ממשהו שכבר הוכחנו: לפי תרגיל 6.5 אם $g(x) \in F[x]$ פולינום אי פריק עם שדה פיצול E ו-a, b הם שני שורשים של $g(x)$, אז יש איזומורפיזם $f\colon E \to E$ שמקבע את איברי F ומקיים $f(a) = b$. בשפה עדכנית קיים $\varphi \in \mathrm{Gal}(E/F)$ כך ש-$\varphi(a) = b$.

עם הטענה הזאת אפשר לפשט את הפתרון של השאלה הקודמת, מפני ש-$\mathbb{Q}(\sqrt[4]{2})$ הוא שדה הפיצול של $x^2 - \sqrt{2}$. היינו יכולים לדעת מייד שקיים φ כך ש-$\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}$ ולא היה צריך להתאמץ בשביל זה.

אזהרה! שימו לב שמשפט זה (ועוד אחרים שנראה) עובדים רק עבור חבורת גלואה של שדה פיצול. בדוגמה בחישוב $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ אין φ כך ש-$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\rho$, ובאמת $\mathbb{Q}(\sqrt[3]{2})$ אינו שדה הפיצול של $x^3 - 2$ (בהמשך הקורס נוכיח שהוא לא שדה פיצול של שום פולינום). כלי מועיל נוסף הוא המשפט הבא:

תרגיל 7.5. יהי $f(x) \in F[x]$ פולינום עם שדה פיצול E. נניח שהשורשים של f ב-E הם $a_1, \ldots, a_n$. הוכיחו כי $\mathrm{Gal}(E/F)$ משוכנת בתוך S_n.

פתרון (בהרצאה). תהי $\varphi \in \mathrm{Gal}(E/F)$. כבר ראינו שלכל i מתקיים

$$\varphi(a_i) \in \{a_1, \cdots, a_n\}$$

ולכן הצמצום של φ ל-$A = \{a_1, \cdots, a_n\}$ הוא פונקציה המוגדרת היטב. מפני ש-φ חד־חד ערכית, גם הצמצום שלה חד־חד ערכי. לכן יש לנו איבר של $S_A \cong S_n$, שנסמן אותו π_φ. כעת נותר להוכיח כי ההתאמה

$$\begin{aligned} \Phi\colon\ \mathrm{Gal}(E/F) &\to S_A \\ \varphi &\mapsto \pi_\varphi \end{aligned}$$

היא שיכון של חבורות. ראשית נשים לב שאם $\Phi(\varphi) = \pi_\varphi = \pi_{\varphi'} = \Phi(\varphi')$, אז φ ו-φ' מסכימים על כל שורשי הפולינום וראינו כבר ש-$\varphi = \varphi'$. כלומר Φ היא אכן חד־חד ערכית. נותר לבדוק שהיא הומומורפיזם, נשים לב כי

$$\Phi(\varphi\varphi') = \Phi(\varphi)\Phi(\varphi') = \pi_\varphi\pi_{\varphi'} = \pi_{\varphi\varphi'}$$

וקל לראות שמתקיים $\pi_\varphi\pi_{\varphi'} = \pi_{\varphi\varphi'}$. לא במקרה זה מזכיר את השיכון ממשפט קיילי.

הערה 7.6. את הטענה האחרונה אפשר לנסח גם בצורה הבאה: חבורת גלואה פועלת על קבוצת השורשים של $f(x)$. כל פעולה של חבורה על קבוצה מגדירה הומומורפיזם לחבורה סימטרית.

אם ל-$f(x)$ יש פירוק $f = f_1 f_2 \dots f_r$ ונסמן $K = F[\alpha_1, \dots, \alpha_n]$ כאשר α_i הם כל השורשים של $f(x)$. כל אוטומורפיזם $\sigma \in \mathrm{Gal}(K/F)$ משרה תמורה על השורשים ויש שיכון

$$\mathrm{Gal}(K/F) \hookrightarrow S_{\deg f_1} \times S_{\deg f_2} \times \cdots \times S_{\deg f_r}$$

עכשיו נתחיל להשתמש בכלים שראינו ונפתור מקרה יותר מסובך.

תרגיל 7.7. חשבו את $\mathrm{Gal}(E/\mathbb{Q})$ כאשר E הוא שדה הפיצול של הפולינום $x^3 - 2$.

פתרון (בהרצאה). ראשית נשים לב ששורשי הפולינום הם $\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^3$ כאשר ρ שורש יחידה פרימיטיבי מסדר 3. לכן חבורת גלואה היא תת־חבורה של S_3, וזה מידע משמעותי. קל לזהות שני איברים של חבורת גלואה: ברור שהעתקת הזהות id שם, וכך גם ההומומורפיזם ההצמדה $z \mapsto \overline{z}$ הוא אוטומורפיזם של E (ששונה מ-id) ומקבע את $\mathbb{Q}$. נתבונן כיצד הצמדה פועלת על השורשים:

$$\sqrt[3]{2} \to \sqrt[3]{2}, \qquad \sqrt[3]{2}\rho \to \sqrt[3]{2}\rho^2, \qquad \sqrt[3]{2}\rho^2 \to \sqrt[3]{2}\rho$$

לכן היא מתאימה לתמורה $(2\ 3) \in S_3$ כאשר זיהינו את השורשים עם $1, 2, 3$. עכשיו נשים לב כי

$$E = \mathbb{Q}(\sqrt[3]{2}, \rho)$$

ולכן איברי החבורה נקבעים לפי התמונה שלהם ב-$\sqrt[3]{2}, \rho$. לפי משפט קודם, קיים אוטומורפיזם $\varphi \in \mathrm{Gal}(E/\mathbb{Q})$ המקיים

$$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\rho$$

אבל לא ברור כל כך מה עושה לשאר השורשים. נשים לב שהפולינום המינימלי של ρ הוא $x^2 + x + 1$ והשורשים שלו הם ρ, ρ^2. לכן $\varphi(\rho) \in \{\rho, \rho^2\}$. נבדוק את שתי האפשרויות: אם $\varphi(\rho) = \rho$, אז התמורה ש-φ מבצעת על השורשים היא $(1, 2)$. כך שבחבורת גלואה יש גם את $(1\ 2)$ וגם את $(2\ 3)$ אבל שתי התמורות האלה יוצרות את כל S_3 ולכן $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

אם דווקא $\varphi(\rho) = \rho^2$ אז התמורה על השורשים יוצאת $(1\ 2\ 3)$. שוב, התמורות $(1\ 2\ 3), (2\ 3)$ יוצרות את כל S_3 ולכן גם באפשרות הזאת $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

נעיר שחבורת גלואה באמת מכילה את שתי האפשרויות שבחנו, אבל זה לא כל כך ברור. עצם העובדה ש-ρ, ρ^2 הם שורשים של פולינום לא מכריח שתהיה φ שמקיימת $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\rho$, וגם $\varphi(\rho) = \rho$ או $\varphi(\rho) = \rho^2$.

8 תרגול שמיני

8.1 הרחבות נורמליות והרחבות גלואה

נמשיך עם תרגילים הנוגעים לחישוב חבורת גלואה. אבל קודם נזכיר כלים נוספים שראיתם בהרצאה.

טענה 8.1. לכל הרחבה סופית K/F מתקיים $|\operatorname{Gal}(K/F)| \le [K:F]$.

תזכורת 8.2. הרחבת שדות K/F נקראת נורמלית אם K הוא שדה פיצול של פולינום כלשהו ב-F. באופן שקול, לכל $a \in K$ הפולינום המינימלי מעל F מתפצל ב-K (ולכן כל השורשים שלו שייכים ל-K). Normal

דוגמה 8.3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ היא דוגמה קלאסית להרחבה לא נורמלית וספרבילית כי לא כל השורשים של x^3-2 שייכים ב-$\mathbb{Q}(\sqrt[3]{2})$. לעומת זאת $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ נורמלית וספרבילית כי $\mathbb{Q}(\sqrt{2})$ הוא שדה הפיצול של x^2-2.

ההרחבה $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ היא נורמלית כי t הוא השורש (היחיד) של $x^p - t^p$ שבמאפיין p שווה ל-$(x-t)^p$. בדוגמה 5.7 ראינו שזו הרחבה לא ספרבילית.

תזכורת 8.4. הרחבת שדות K/F נקראת הרחבת גלואה אם היא נורמלית וספרבילית. זה שקול לכך ש-K הוא שדה פיצול של פולינום ספרבילי מעל F. מה שטוב בהרחבות גלואה זה ש-K/F הרחבת גלואה אם ורק אם Galois extension

$$|\operatorname{Gal}(K/F)| = [K:F]$$

דוגמה 8.5. נחשב שוב את $\operatorname{Gal}(E/\mathbb{Q})$ כאשר E הוא שדה הפיצול של הפולינום x^3-2. ראשית נשים לב ששורשי הפולינום הם $\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^3$ כאשר ρ שורש יחידה פרימיטיבי מסדר 3. לכן חבורת גלואה היא (איזומורפית ל)תת־חבורה של S_3. בנוסף זאת הרחבת גלואה וקל לבדוק כי $[E:\mathbb{Q}]=6$. לכן חבורת גלואה היא מסדר 6 ובהכרח היא S_3.

תרגיל 8.6. יהי $f(x) \in \mathbb{Q}[x]$ פולינום מדרגה p ראשוני עם $p-2$ שורשים ממשיים ו-2 שורשים מרוכבים שאינם ממשיים (שורשים אלה בהכרח צמודים). יהי E שדה הפיצול שלו. הוכיחו כי

$$\operatorname{Gal}(E/F) \cong S_p$$

פתרון. כבר ראינו שחבורת גלואה משוכנת בתוך S_p. בנוסף ברור כי

$$p \mid [E:\mathbb{Q}] = |\operatorname{Gal}(E/\mathbb{Q})|$$

לפי משפט קושי זה אומר שיש בחבורת גלואה איבר σ מסדר p. איבר כזה חייב להיות מחזור באורך p. כמו כן, הצמדה מרוכבת היא איבר בחבורת גלואה. היא מחליפה בין שני השורשים המרוכבים ומקבעת את השאר. לכן השיכון ל-S_p שולח אותה לחילוף. ניתן להניח, אחרי תמורה על האינדקסים, כי החילוף הוא $(1\ 2)$. בחזקה מתאימה של המחזור σ נקבל $\sigma^k(1)=2$. על ידי שינוי שאר האינדקסים אפשר להניח כי המחזור הוא $(1\ 2 \dots p)$. כלומר חילוף ומחזור באורך p יוצרים את כל S_p ולכן $\operatorname{Gal}(E/F) \cong S_p$.

תרגיל 8.7. יהי $f(x) \in \mathbb{Q}[x]$ פולינום אי פריק ויהי $E/\mathbb{Q}$ שדה הפיצול שלו. הוכיחו שאם $\operatorname{Gal}(E/\mathbb{Q}) \cong Q_8$, אז בהכרח $\deg f(x) \ge 8$.

פתרון. אם $\deg f(x) < 8$, אז $\mathrm{Gal}(E/\mathbb{Q})$ משוכנת ב-S_n עבור $n < 8$. בתרגיל בית בתורת החבורות הראנו שאין שיכון כזה של Q_8 בעזרת פעולה של חבורה. נוכיח זאת שוב למקרה הפרטי הנוכחי.

נניח בשלילה כי Q_8 איזומורפית לתת־חבורה של S_7 (זה מכסה גם את המקרים של $S_2, \dots, S_6$). אזי היא פועלת על הקבוצה $X = \{1, \dots, 7\}$. יהי $x \in X$. אז

$$[Q_8 : \mathrm{stab}(x)] = \frac{|Q_8|}{|\mathrm{stab}(x)|} = |\mathrm{orb}(x)| \leq 7$$

ולכן $|\mathrm{stab}(x)| > 1$. נזכר שכל תת־חבורה לא טריוויאלית של Q_8 מכילה את -1 ולכן $-1 \in \mathrm{stab}(x)$ לכל $x \in X$. כלומר -1 פועל בצורה טריוויאלית על X, וזו סתירה כי אין איבר לא טריוויאלי ב-S_7 שפועל טריוויאלית על X. משפט קיילי מספק שיכון של Q_8 ל-S_8.

תרגיל 8.8 (לבית). נביט בהרחבה $F \subseteq K \subseteq E$ ונניח כי E/F נורמלית. האם K/F נורמלית? האם E/K נורמלית?

פתרון. K/F לא חייבת להיות נורמלית. למשל $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ ו-E הוא שדה הפיצול של $x^3 - 2$.

אבל E/K כן. אם E הוא שדה הפיצול של $f(x)$ מעל F הוא גם שדה הפיצול של $f(x)$ מעל K.

תרגיל 8.9. מצאו הרחבה $E/\mathbb{Q}$ כך שחבורת גלואה שלה היא $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

פתרון. נבחר $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. זהו שדה פיצול של $(x^2-2)(x^2-3)(x^2-5)$ ולכן זו הרחבת גלואה. קל לראות שהממד הוא 8 ולכן החבורה בגודל המתאים. בנוסף, כל איבר φ בחבורת גלואה חייב לקיים

$$\varphi(\sqrt{2}) = \pm\sqrt{2}, \qquad \varphi(\sqrt{3}) = \pm\sqrt{3}, \qquad \varphi(\sqrt{5}) = \pm\sqrt{5}$$

כלומר כל האיברים מסדר 1 או 2. חבורה זו חייבת להיות החבורה המבוקשת. שימו לב שלעומת Q_8 את החבורה הזו אפשר לשכן ב-S_6. האם זו חבורת גלואה של פולינום אי פריק ממעלה 6 מעל $\mathbb{Q}$?

תרגיל 8.10. שימוש לחבורת גלואה: תהי K/F הרחבת גלואה עם חבורת גלואה G. ויהי $a \in K$. נסמן

$$\mathrm{orb}(a) = \{\varphi(a) \mid \varphi \in G\}$$

שהוא המסלול של a תחת הפעולה של חבורת גלואה (הנקודה היא שזו קבוצה ולכן אין חזרות). הוכיחו כי הפולינום המינימלי של a הוא Orbit

$$m_a(x) = \prod_{b \in \mathrm{orb}(a)} (x - b)$$

פתרון. מצד אחד $\varphi(a)$ תמיד שורש של הפולינום המינימלי של a ולכן

$$\prod_{b\in\mathrm{orb}(a)}(x-b)\mid m_a$$

כמו כן נזכר כי m_a ספרבילי ולכן אין לו שורשים כפולים. כעת נשאר להוכיח שאין ל-m_a שורשים נוספים. נשים לב ש-K מפצל את m_a ולכן לכל שורש c של m_a יש $\varphi\in G$ כך ש-$\varphi(a)=c$ (טרנזיטיביות על השורשים של פולינום אי פריק וכו'). לכן כל שורש c של m_a שייך ל-$\mathrm{orb}(a)$.

מסקנה 8.11. מתקיים $[F[a]:F]=\deg m_a=|\mathrm{orb}(a)|$.

תרגיל 8.12. נביט על ההרחבה $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. מצאו את הפולינום המינימלי של $a=\sqrt{2}-3\sqrt{3}+2\sqrt{6}$ (לפחות כפירוק לשורשים) ואת $[\mathbb{Q}[a]:\mathbb{Q}]$.

פתרון. נשתמש במשפט הקודם. נזכר שחבורת גלואה של ההרחבה היא $\mathbb{Z}_2\times\mathbb{Z}_2$. נסמן את האיברים שלה $\{\mathrm{id},\theta,\tau,\theta\tau\}$ כאשר

$$\theta(\sqrt{2})=-\sqrt{2},\qquad\theta(\sqrt{3})=\sqrt{3}$$
$$\tau(\sqrt{2})=\sqrt{2},\qquad\tau(\sqrt{3})=-\sqrt{3}$$

נמצא את המסלול של a:

$$\mathrm{id}(a)=\sqrt{2}-3\sqrt{3}+2\sqrt{6}$$
$$\theta(a)=-\sqrt{2}-3\sqrt{3}-2\sqrt{6}$$
$$\tau(a)=\sqrt{2}+3\sqrt{3}-2\sqrt{6}$$
$$\theta\tau(a)=-\sqrt{2}-3\sqrt{3}+2\sqrt{6}$$

הם כולם שונים כי כזכור $1,\sqrt{2},\sqrt{3},\sqrt{6}$ הוא בסיס עבור המרחב הוקטורי $\mathbb{Q}(\sqrt{2},\sqrt{3})$ מעל $\mathbb{Q}$. לכן הפולינום המינימלי הוא $(x-a)(x-\theta(a))(x-\tau(a))(x-\theta\tau(a))$ שמעלתו היא $[\mathbb{Q}[a]:\mathbb{Q}]=4$.

הערה 8.13. שווה לציין את הנקודה הבאה: נניח נרצה לדעת מהו הפולינום המינימלי של $\sqrt{6}$, ולהשתמש בשיטה לעיל. היינו מגלים ש-$\mathrm{orb}(\sqrt{6})=\{\pm\sqrt{6}\}$, ולכן הפולינום המינימלי הוא x^2-6 כפי שאנחנו כבר יודעים.

9 תרגול תשיעי

9.1 התאמת גלואה

בהנתן שדה K ותת־שדה שלו F הגדרנו את חבורת גלואה $\mathrm{Gal}(K/F)$. אפשר גם ללכת בכיוון ההפוך:

הגדרה 9.1. יהי K שדה, ותהי G חבורה של אוטומורפיזמים של K. תת־השדה

$$K^G = \{a \in K \,|\, \forall \sigma \in G : \sigma(a) = a\}$$

נקרא שדה השבת של G. Fixed field

הערה 9.2. שתי ההעתקות האלו הופכות סדר: אם $F \subseteq L \subseteq K$, אז $\mathrm{Gal}(K/L) \le \mathrm{Gal}(K/F)$. כמו כן אם $H \le G$, אז $K^G \subseteq K^H$. בהרצאה תלמדו מה קורה כשממשיכים להפעיל את ההעתקות האלו יותר מפעם אחת.

תרגיל 9.3. תהי E/F הרחבת שדות עם חבורת גלואה $G = \mathrm{Gal}(E/F)$. תהי תת־חבורה $H \le G$ הנוצרת על ידי $\varphi_1, \ldots, \varphi_k$. הוכיחו כי $E^H = E^{\{\varphi_1,\ldots,\varphi_k\}}$.

פתרון. ההכלה $E^H \subseteq E^{\{\varphi_1,\ldots,\varphi_k\}}$ טריויאלית. מצד שני ברור שאברים המקובעים על ידי $\{\varphi_1, \ldots, \varphi_k\}$ מקובעים גם על ידי כל דבר שהם יוצרים, ולכן $E^H = E^{\{\varphi_1,\ldots,\varphi_k\}}$, כנדרש.

טענה 9.4. תהי E/F הרחבת שדות. התנאים הבאים שקולים:

1. E/F הרחבת גלואה (כלומר נורמלית וספרבילית).
2. E/F שדה פיצול של פולינום ספרבילי.
3. $E^{\mathrm{Gal}(E/F)} = F$.
4. $E^H = F$ עבור תת־חבורה $H \le \mathrm{Aut}(E)$ סופית.
5. $|\,\mathrm{Gal}(E/F)| = [E : F]$.

הערה 9.5. המשפט שהוא כנראה הכי חשוב בקורס, המשפט היסודי של תורת גלואה: תהי E/F הרחבת גלואה. יש אנטי-איזומורפיזם של סריגים בין סריג תת־החבורות של $\mathrm{Gal}(E/F)$ לבין סריג תת־השדות של E/F. בהינתן שדה ביניים L החבורה המתאימה היא $\mathrm{Gal}(E/L)$, ובהינתן תת־חבורה $H \le G$ תת־שדה המתאים הוא E^H. Fundamental theorem of Galois theory

התאמת גלואה מגיעה עם לא מעט מסקנות: הסדרים והאינדקסים מתאימים, כלומר $|H| = [E : E^H]$ וגם $[E : L] = |\,\mathrm{Gal}(E/L)|$. ההרחבה L/F היא גלואה אם ורק אם $\mathrm{Gal}(E/L)$ נורמלית, ובנוסף Galois correspondence

$$\mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/L) \cong \mathrm{Gal}(L/F)$$

ובפרט כל אוטומורפיזם של L/F ניתן להמשיך לאוטומורפיזם של E/F.

תרגיל 9.6. חשבו את $\mathrm{Gal}(E/\mathbb{Q})$ כאשר E הוא שדה הפיצול של הפולינום $f(x) = x^4 - 2$.

פתרון. הפולינום $f(x)$ הוא ספרבילי כי הוא אי פריק מעל שדה ממאפיין אפס, ולכן $E/\mathbb{Q}$ הרחבת גלואה. נסמן את השורשים של $f(x)=(x^2-\sqrt{2})(x^2+\sqrt{2})$ במספרים

$$1 \leftrightarrow \alpha \coloneqq \sqrt[4]{2}, \qquad 2 \leftrightarrow -\alpha, \qquad 3 \leftrightarrow \alpha i, \qquad 4 \leftrightarrow -\alpha i$$

נוותר על הבדיקה שמוכיחה כי $E=\mathbb{Q}[\alpha,i]$, ונשים לב כי $[E:\mathbb{Q}]=8$. לכן $\mathrm{Gal}(E/\mathbb{Q})$ איזומורפית לתת־חבורה מסדר 8 של S_4, ובהכרח $\mathrm{Gal}(E/\mathbb{Q})\cong D_4$.

כל אוטומורפיזם ב־$\mathrm{Gal}(E/\mathbb{Q})$ נקבע לפי תמונת α (שחייב להשלח לשורש של x^4-2) ותמונת i (שחייב להשלח ל־$\pm i$). שימו לב שהפולינום המינימלי של i מעל $\mathbb{Q}[\alpha]$ הוא עדין x^2+1, שיעזור בבדיקה האם אוטומורפיזם מסוים קיים בכלל. אצלנו כל אחת מ־$4\cdot 2=8$ ההצבות האפשרויות לתמונות α, i תגדיר אוטומורפיזם:

תמורת השורשים	תמונת i	תמונת α	אוטומורפיזם
$\mathrm{id}\in S_4$	i	α	id_E
$(1\,3\,2\,4)$	i	αi	σ
$(1\,2)(3\,4)$	i	$-\alpha$	σ^2
$(1\,4\,2\,3)$	i	$-\alpha i$	σ^3
$(1\,2)$	$-i$	$-\alpha$	τ
$(1\,3)(2\,4)$	$-i$	αi	$\tau\sigma$
$(3\,4)$	$-i$	α	$\tau\sigma^2$
$(1\,4)(2\,3)$	$-i$	$-\alpha i$	$\tau\sigma^3$

איך חישבנו את הטבלה? למשל

$$\sigma^2(\alpha)=\sigma(\alpha i)=\sigma(\alpha)\sigma(i)=\alpha i i=-\alpha$$

ולמציאת התמורה מחשבים את הפעולה על השורשים. שימו לב כי $\tau\sigma^2$ היא הצמדה מרוכבת. בסך הכל קיבלנו כי $\mathrm{Gal}(E/\mathbb{Q})=\langle\sigma,\tau\rangle\le S_4$. סריג תת־החבורות של D_4 הוא

$$\begin{tikzcd}
 & & D_4 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \langle\tau,\sigma^2\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle\sigma\rangle \arrow[d, dash] & \langle\tau\sigma,\sigma^2\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\tau\rangle \arrow[drr, dash] & \langle\tau\sigma^2\rangle \arrow[dr, dash] & \langle\sigma^2\rangle \arrow[d, dash] & \langle\tau\sigma\rangle \arrow[dl, dash] & \langle\tau\sigma^3\rangle \arrow[dll, dash] \\
 & & \{\mathrm{id}\} & &
\end{tikzcd}$$

כעת נמצא את סריג תת־השדות של $E/\mathbb{Q}$. למצוא חלק מתת־השדות זה קל, אך כדי להיות בטוחים שמצאנו את כולם ואין כפילויות, נצטרך כלים תיאורטיים נוספים שלא

ידרשו שום ניחושים. תחילה אפשר למצוא תת־שדות מוכרים כמו $\mathbb{Q}[i]$. ברור ש-$\mathbb{Q}[i]$ שונה מ-$\mathbb{Q}[\alpha]$ הממשי, שבתורו שונה מ-E. להמשך נצטרך את התאמת גלואה וחישוב המסלולים שראינו קודם. בסך הכל נקבל

$$\begin{tikzcd}
 & & E = \mathbb{Q}[\alpha, i] \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}[\alpha i] \arrow[dr, dash] & \mathbb{Q}[\alpha] \arrow[d, dash] & \mathbb{Q}[\sqrt{2}, i] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}[(1+i)\alpha] \arrow[d, dash] & \mathbb{Q}[(1-i)\alpha] \arrow[dl, dash] \\
 & \mathbb{Q}[\sqrt{2}] \arrow[dr, dash] & \mathbb{Q}[i] \arrow[d, dash] & \mathbb{Q}[\sqrt{2}i] \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

למציאת $E^{\langle \tau\sigma^2 \rangle}$ נשים לב כי $\tau\sigma^2(\alpha) = \alpha$ ולכן $\mathbb{Q}[\alpha] \subseteq E^{\langle \tau\sigma^2 \rangle}$. מפני שהממדים של שני השדות האלו הוא 4, נסיק שיש שוויון $\mathbb{Q}[\alpha] = E^{\langle \tau\sigma^2 \rangle}$. למציאת $E^{\langle \tau,\sigma^2 \rangle}$ נשים לב כי $\tau(\alpha^2) = \sigma^2(\alpha^2) = \alpha^2$. לכן $\mathbb{Q}[\alpha^2] \subseteq E^{\langle \tau,\sigma^2 \rangle}$ ומפני ששוב הממדים שווים 2, נסיק שוויון.

במסלול של α תחת $\tau\sigma$ נמצאים $\{\alpha, \alpha i\}$ ולכן האיבר $\alpha + \alpha i = (1+i)\alpha$ נשמר תחת הפעולה של $\tau\sigma$. תת־השדה $\mathbb{Q}[(1+i)\alpha]$ הוא ממימד 4 ולכן שונה מ-$\mathbb{Q}[\sqrt{2}i]$. עבור חבורות גלואה קטנות אפשר למצוא כך את כל שדות הביניים.

תזכורת 9.7. אם $F \subseteq K, L \subseteq E$, אז הקומפוזיטום של K ו-L הוא תת־השדה המינימלי שמכיל את K, L ומסומן בדרך כלל LK או $L \vee K$. אם $K = F[\alpha_1, \ldots, \alpha_n]$, אז $L \vee K = L[\alpha_1, \ldots, \alpha_n]$.

Restriction

הגדרה 9.8. תהי E/F הרחבת גלואה ו-$F \subseteq K \subseteq E$ שדה ביניים כך שההרחבה K/F גם היא גלואה. אז העתקת הצמצום

$$\begin{aligned} \operatorname{res}^E_K \colon\ \operatorname{Gal}(E/F) &\to \operatorname{Gal}(K/F) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

היא הומומורפיזם של חבורות. החידוש הוא בכך שהצמצום מוגדר היטב (זה שהוא הומומורפיזם זה ברור).

תרגיל 9.9. תהינה K/F ו-L/F הרחבות סופיות, ונניח K/F גלואה. הוכיחו:

1. $L \vee K/L$ הרחבת גלואה.
2. ישנו שיכון $\varphi\colon \operatorname{Gal}(L \vee K/L) \to \operatorname{Gal}(K/F)$ לפי $\varphi(\sigma) = \sigma|_K$.
3. $\operatorname{Im}\varphi = \operatorname{Gal}(K/K \cap L)$, ואם $K \cap L = F$, אז $\operatorname{Gal}(L \vee K/L) \cong \operatorname{Gal}(K/F)$.

פתרון. למעשה ראינו חלק מהוכחות תרגיל זה בעבר.

1. בתרגיל בית הוכחתם שאם K/F שדה פיצול של פולינום ספרבילי $f(x)$, אז $L\vee K/L$ שדה פיצול של אותו פולינום. בפירוט: אפשר לסמן $K=F[\alpha_1,\dots,\alpha_n]$. שדה הפיצול של $f(x)$ מעל L הוא $L[\alpha_1,\dots,\alpha_n]$. ברור כי $L\subseteq L\vee K$ ובנוסף $\alpha_i\in K\subseteq L\vee K$ לכל i, ולכן $L[\alpha_1,\dots,\alpha_n]\subseteq L\vee K$. מצד שני $L,K\subseteq L[\alpha_1,\dots,\alpha_n]$. לכן $L\vee K=L[\alpha_1,\dots,\alpha_n]$. כלומר $L\vee K$ הוא שדה פיצול של פולינום ספרבילי מעל L, ולכן זו הרחבת גלואה.

2. נתון כי K/F גלואה, ובפרט נורמלית. ראינו כי הצמצום מוגדר היטב במקרה כזה ולכן לכל $\sigma\in\operatorname{Gal}(L\vee K/L)$ נקבל $\sigma|_K\in\operatorname{Gal}(K/F)$. בפרט לכל $\sigma\in\operatorname{Gal}(L\vee K/L)\subseteq\operatorname{Gal}(L\vee K/F)$ מתקיים $\sigma|_K\in\operatorname{Gal}(K/F)$ ולכן φ מוגדר היטב. נבדוק שזהו שיכון.
תחילה נבדוק כי φ הומומורפיזם. לכל $\sigma_1,\sigma_2\in\operatorname{Gal}(L\vee K/L)$ מתקיים
$$\varphi(\sigma_1\sigma_2)=(\sigma_1\sigma_2)|_K\underset{(*)}{=}\sigma_1|_K\circ\sigma_2|_K=\varphi(\sigma_1)\varphi(\sigma_2)$$
כאשר המעבר $(*)$ נובע מכך ש-$\sigma_2(K)=K$. כדי לבדוק ש-φ חח"ע נמצא את הגרעין
$$\operatorname{Ker}\varphi=\{\sigma\in\operatorname{Gal}(L\vee K/L)\,|\,\varphi(\sigma)=\mathrm{id}_K\}$$
כלומר $\sigma\in\operatorname{Ker}\varphi$ אם ורק אם $\varphi(\sigma)=\sigma|_K$ משמר את איברי K ונרצה להראות כי σ משמר את L. אבל σ משמר את K כי $\sigma|_K=\mathrm{id}_K$ ומשמר את L כי $\sigma\in\operatorname{Gal}(L\vee K/L)$. לכן σ משמר את $L\vee K$. מכאן שהגרעין טריוויאלי.

3. נשים לב שמתקיים
$$\begin{aligned}K^{\operatorname{Im}\varphi}&=\{k\in K\,|\,\forall\sigma\in\operatorname{Gal}(L\vee K/L),(\varphi(\sigma))(k)=k\}\\&=\{k\in K\,|\,\forall\sigma\in\operatorname{Gal}(L\vee K/L),\,\sigma|_K(k)=k\}\end{aligned}$$
ולכן $K^{\operatorname{Im}\varphi}=K\cap(L\vee K)^{\operatorname{Gal}(L\vee K/L)}=K\cap L$. כלומר $\operatorname{Im}\varphi=K\cap L$. בנוסף, אם $K\cap L=F$ נקבל איזומורפיזם $\operatorname{Gal}(L\vee K/L)\cong\operatorname{Gal}(K/F)$.

מסקנה 9.10. מהתאמת גלואה נקבל
$$[L\vee K:F]=\frac{[K:F][L:F]}{[K\cap L:F]}$$

9.2 סגור גלואה

הגדרה 9.11. תהי K/F הרחבת שדות ספרבילית סופית. סְגוֹר גלואה (זה גם הסגור הנורמלי) שלה הוא הרחבת השדות E/K המינימלית שהיא גלואה. Galois closure

הערה 9.12. אם K/F גלואה, אז בוודאי שסגור גלואה הוא $E=K$. אחרת, נסמן $K=F[\alpha_1,\dots,\alpha_n]$ וכדי למצוא את סגור גלואה נספח ל-K את כל שורשי הפולינומים המינימליים של $\alpha_1,\dots,\alpha_n$. מכאן שסגור גלואה קיים, והוא יחיד עד כדי איזומורפיזם.

תרגיל 9.13. מצאו את סגור גלואה של $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$.

פתרון. ראינו כבר שההרחבה הזו אינה נורמלית. הפולינום המינימלי של $\sqrt[3]{2}$ הוא x^3-2. אזי סגור גלואה יהיה

$$E=\mathbb{Q}[\sqrt[3]{2},\sqrt[3]{2}\rho,\sqrt[3]{2}\rho^2]=\mathbb{Q}[\sqrt[3]{2},\rho]$$

כאשר ρ הוא שורש יחידה פרימיטיבי מסדר 3.

תרגיל 9.14. מצאו את סגור גלואה של $\mathbb{Q}[\sqrt[3]{5},\sqrt[3]{7}]/\mathbb{Q}$.

פתרון. גם ההרחבה הזו אינה נורמלית, בדומה לתרגיל הקודם. הפולינום המינימלי של $\sqrt[3]{5}$ הוא x^3-5 ושניים משורשיו מרוכבים למרות שההרחבה ממשית. שוב נסמן ב-ρ שורש יחידה פרימיטיבי מסדר 3, ונקבל שסגור גלואה המבוקש הוא

$$E=\mathbb{Q}[\sqrt[3]{5},\sqrt[3]{5}\rho,\sqrt[3]{5}\rho^2,\sqrt[3]{7},\sqrt[3]{7}\rho,\sqrt[3]{7}\rho^2]=\mathbb{Q}[\sqrt[3]{5},\sqrt[3]{7},\rho]$$

10 תרגול עשירי

10.1 שדות סופיים

תזכורת 10.1. בתורת החבורות למדנו שהסדר של חבורה סופית הוא כנראה המידע הכי חשוב לגביה. בשדות סופיים, הסדר של השדה הוא הדבר היחיד שחשוב, ברוב המקרים.

יהי p מספר ראשוני. כל שדה סופי חייב כמובן להיות ממאפיין חיובי, נניח p. לכל חזקה $q=p^k$ קיים שדה $\mathbb{F}_q$ מסדר q (או בסימון $\mathrm{GF}(q)$) והוא יחיד עד כדי איזומורפיזם.

תרגיל 10.2. הוכיחו שבשדה $\mathbb{F}_q$ מתקיים $a^q=a$ לכל $a\in\mathbb{F}_q$ וגם

$$x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$$

פתרון. אם $a=0$ זה ברור. אחרת, $a\in\mathbb{F}_q^*$, ואנו יודעים שזו חבורה מסדר $q-1$. לפי מסקנה ממשפט לגראנז' נקבל $a^{q-1}=1$. נכפול ב-a ונקבל $a^q=a$. המשמעות היא שכל איברי $\mathbb{F}_q$ הם שורשים של הפולינום x^q-x, ולכן המכפלה $\prod_{a\in\mathbb{F}_q}(x-a)$ מחלקת אותו. מפני שהדרגות של שני הפולינומים האלו שווה, ושניהם מתוקנים, אז הם בהכרח שווים.

הערה 10.3. כמסקנה מהתרגיל, השדה $\mathbb{F}_q$ הוא שדה הפיצול של הפולינום $x^q - x \in \mathbb{F}_p[x]$. בנוסף, החבורה הכפלית שלו $\mathbb{F}_q^*$ היא ציקלית (כמו כל חבורה סופית של כל שדה), והחבורה החיבורית שלו היא אלמנטרית, כלומר $\mathbb{F}_q \cong (\mathbb{Z}/p\mathbb{Z})^k$ כחבורות, שהרי זה מרחב וקטורי ממימד k מעל $\mathbb{F}_p$. כל הרחבה של שדות סופיים היא גלואה. חבורת גלואה היא תמיד ציקלית, למשל $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/k\mathbb{Z}$, והיא נוצרת על ידי אוטומורפיזם פרובניוס $x \mapsto x^p$.

תרגיל 10.4. בנו במפורט שדה בן $2^3 = 8$ איברים.

פתרון. זה צריך להיות שדה ממאפיין 2, שהוא שדה הפיצול של $x^8 - x$. נפרק

$$x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

נמשיך ונפרק $x^6 + \ldots + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$ לפי קצת ניסוי וטעייה. נשים לב ששני הפולינומים אי פריקים מעל $\mathbb{F}_2$. השדה שלנו איזומורפי ל-$\mathbb{F}_2[x]/(x^3 + x + 1)$. כלומר בניה מפורשת של איבר $\mathbb{F}_8$ הוא $a + bx + cx^2 \in \mathbb{F}_2[x]$ כאשר $x^3 = -1 - x$.

תרגיל 10.5. יהי F אחד מן השדות $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$. מצאו את ממד שדה הפיצול של $x^3 - 2$ מעל F. תארו את הפעולה של האוטומורפיזמים היוצרים את חבורת גלואה בכל מקרה.

פתרון. נסמן ב-α שורש של הפולינום בשדה הפיצול. נזכור ש-$F(\alpha)/F$ נורמלית ולכן זה שדה הפיצול (ולכן $F(\alpha)$ מכיל את כל שורשי הפולינום). נותר רק לקבוע מה הסדר של $F(\alpha)$.

עבור $F = \mathbb{F}_3$, הפולינום מתפרק $x^3 - 2 = (x-2)^3$. לכן שדה הפיצול הוא $\mathbb{F}_3$ עצמו וחבורת גלואה טריויאלית.

עבור $F = \mathbb{F}_5$, הפולינום מתפרק $x^3 - 2 = (x-3)(x^2 + 3x + 4)$ והפולינום $x^2 + 3x + 4$ הוא אי פריק (למשל לפי הצבה) ולכן זאת הרחבה ממימד 2. כלומר שדה הפיצול הוא $\mathbb{F}_{25}$, וחבורת גלואה היא $\mathbb{Z}/2\mathbb{Z}$. איברי השדה הם מן הצורה $a + bx \in \mathbb{F}_5[x]$ כאשר $x^2 = -3x - 4$. לכן אוטומורפיזם פרובניוס $\varphi\colon x \mapsto x^5$ פועל לפי

$$\begin{aligned}\varphi(a+bx) &= a + bx^5 = a + bx(-3x-4)(-3x-4) = \\ &= a + bx(4x^2 + 4x + 1) = a + bx(-12x - 16 + 4x + 1) \\ &= a + bx(-8x) = a + 2bx^2 = a + 2b + 4bx\end{aligned}$$

עבור $F = \mathbb{F}_7$, הפולינום $x^3 - 2$ הוא אי פריק כי אם יש שורש α מעל ב-$\mathbb{F}_7$ אז אותו שורש צריך לקיים

$$\alpha^6 = 4$$

אבל לפי משפט לגראנז' בתורת החבורות אנחנו יודעים ש-$\alpha^6 = 1$. אפשר לעשות גם בדיקה יותר ארוכה ולהציב כל איבר של $\mathbb{F}_7$. לכן $\mathbb{F}_{7^3} \cong \mathbb{F}_7[x]/\langle x^3 - 2\rangle$ הוא שדה הפיצול המבוקש. חבורת גלואה שלו היא $\mathbb{Z}/3\mathbb{Z}$. איברי השדה הם מן הצורה $a + bx + cx^2 \in \mathbb{F}_7[x]$ כאשר $x^3 = 2$. לכן אוטומורפיזם פרובניוס $x \mapsto x^7$ פועל לפי

$$\varphi(a + bx + cx^2) = a + bx^7 + cx^{14}$$

ומפני ש-$x^7 = xx^3x^3 = 4x$, נקבל $x^{14} = 16x^2 = 2x^2$, ולכן בסך הכל

$$\varphi(a+bx+cx^2) = 1 + 4bx + 2cx^2$$

תרגיל 10.6. הוכיחו כי $\mathbb{F}_q$ משוכן ב-$\mathbb{F}_t$ אם ורק אם $t = q^r$ עבור r כלשהו. בפרט, עבור p ראשוני, $\mathbb{F}_{p^n}$ הוא תת־שדה של $\mathbb{F}_{p^m}$ אם ורק אם $n|m$.

פתרון. נתחיל בדוגמאות של סריג תת־השדות של $\mathbb{F}_{p^{24}}$ ושל $\mathbb{F}_{p^{27}}$:

$$\begin{tikzcd}[arrows=dash]
\mathbb{F}_{p^{27}} \arrow[d] \\
\mathbb{F}_{p^{9}} \arrow[d] \\
\mathbb{F}_{p^{3}} \arrow[d] \\
\mathbb{F}_{p}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[arrows=dash]
& \mathbb{F}_{p^{24}} \arrow[dl] \arrow[dr] & \\
\mathbb{F}_{p^{8}} \arrow[d] & & \mathbb{F}_{p^{12}} \arrow[d] \arrow[dll] \\
\mathbb{F}_{p^{4}} \arrow[d] & & \mathbb{F}_{p^{6}} \arrow[d] \arrow[dll] \\
\mathbb{F}_{p^{2}} \arrow[dr] & & \mathbb{F}_{p^{3}} \arrow[dl] \\
& \mathbb{F}_{p} &
\end{tikzcd}$$

בכיוון אחד, נניח כי $\mathbb{F}_q$ הוא תת־שדה של $\mathbb{F}_t$. אזי $\mathbb{F}_t$ מרחב וקטורי מעל $\mathbb{F}_q$, ולכן $t = q^r$ עבור r כלשהו.

בכיוון השני, נניח $t = q^r$, ונראה כי ל-$\mathbb{F}_t$ יש תת־שדה מסדר q. החבורה $\mathrm{Gal}(\mathbb{F}_t/\mathbb{F}_p)$ ציקלית, ולפי התאמת גלואה יש לה תת־חבורה (יחידה) מכל סדר שמחלק אותה, והיא מתאימה לתת־שדה מכל חזקה של p, בפרט q. באופן מפורש, מתקיים

$$\begin{aligned} x^t - x &= x\left(x^{q^r-1}-1\right) = x\left(x^{q-1}-1\right)\left(x^{q^r-q}+x^{q^r-2q}+\cdots+x^q+1\right) = \\ &= \left(x^q-x\right)\left(x^{q^r-q}+x^{q^r-2q}+\cdots+x^q+1\right) \end{aligned}$$

ולכן ישנו חילוק פולינומים $(x^q-x)\,|\,(x^t-x)$. לפי תרגיל 10.2, הפולינום x^t-x מתפצל לגורמים לינאריים שונים מעל $\mathbb{F}_t$, ולכן גם x^q-x מתפצל לגורמים לינאריים שונים. כלומר בקבוצה $K = \{x \in \mathbb{F}_t \,|\, x^q = x\}$ יש בדיוק q איברים שונים, וזה יהיה תת־השדה הדרוש של $\mathbb{F}_t$. מספיק להראות סגירות לכפל וחיבור: אם $x, y \in K$, אז $x^q = x$ וגם $y^q = y$. נניח $q = p^n$, ולכן

$$\begin{aligned} (x+y)^q &= (x+y)^{p^n} = x^{p^n} + y^{p^n} = x^q + y^q = x + y \\ (xy)^q &= x^q y^q = xy \end{aligned}$$

וקיבלנו $x+y, xy \in K$. כלומר K תת־שדה של $\mathbb{F}_t$ מסדר q.

תזכורת 10.7. הפולינום $x^{p^k} - x \in \mathbb{F}_p[x]$ הוא מכפלת כל הפולינומים האי פריקים (המתוקנים) שמעלתם מחלקת את k. טענה זו מאפשרת לנו למצוא באופן רקורסיבי את כל הפולינומים האי פריקים מעל $\mathbb{F}_p$ במעלה נתונה.

בפרט, אפשר להסיק שלכל $k, m \in \mathbb{N}$ קיים פולינום אי פריק ממעל m מעל $\mathbb{F}_{p^k}$, כי קיים שדה מסדר p^{km}.

מסקנה 10.8. כל פולינום אי פריק מעל שדה סופי הוא ספרבילי. ראינו שזה לא נכון לשדות אינסופיים ממאפיין חיובי.

תרגיל 10.9 (ממבחן). מצאו כמה פולינומים אי פריקים ממעלה 4 יש מעל $\mathbb{F}_2$.

פתרון. אנחנו נמצא את הפולינומים האי פריקים ממעלה 1 מעל $\mathbb{F}_2$, אז את אלו ממעלה 2 ולבסוף את אלו ממעלה 4. למה זה טוב? שהרי מכפלת כל הפולינומים האלו היא

$$x^{2^4} - x = x^{16} - x$$

במעלה 1 הפולינומים מחלקים את $x^{2^1} - x = x(x-1)$ ולכן ישנם שני פולינומים אי פריקים ממעלה 1. במעלה 2 הפולינומים מחלקים את

$$x^{2^2} - x = x(x-1)(x^2+x+1)$$

ולכן ישנו פולינום יחיד ממעלה 2 שהוא אי פריק. במעלה 4 הפולינומים מחלקים את

$$x^{2^4} - x = x(x-1)(x^2+x+1)\Pi_4$$

כאשר Π_4 היא מכפלת הפולינומים האי פריקים ממעלה 4. ברור כי $\deg \Pi_4 = 12$ ולכן ישנם בדיוק שלושה פולינומים אי פריקים ממעלה 4.

תרגיל 10.10. בהמשך לתרגיל הקודם, מצאו כמה פולינומים אי פריקים ממעלה 8 יש מעל $\mathbb{F}_2$.

פתרון. מכפלת כל הפולינומים האי פריקים ממעלה בדיוק 8 מעל $\mathbb{F}_2$ היא

$$(x^{2^8} - x)/(x^{2^4} - x)$$

שהיא ממעלה $240 = 16 - 256$. לכן יש $\frac{240}{8} = 30$ פולינומים אי פריקים ממעלה 8 מעל $\mathbb{F}_2$.

11 תרגול אחד עשר

11.1 פולינומים ציקלוטומיים

הגדרה 11.1. הפולינום הציקלוטומי ה-n-י הוא הפולינום המינימלי של שורש יחידה מסדר n מעל $\mathbb{Q}$. Cyclotomic polynomial

שם התואר ציקלוטומי מקורו ביוונית ופירושו "חותך מעגל". משה ירדן מציע במילונו את התרגום פולינום חַשְׁרוּרִי (נגזר מחִשּׁוּר, שהוא מוט המחבר מרכז אוֹפַן לחישוקו).

הערה 11.2. הפולינומים הציקלוטומיים מקיימים את הנוסחה הרקורסיבית

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

דרגת הפולינום היא $\deg \Phi_n = \varphi(n)$ כאשר φ היא פונקציית אוילר. יהי ρ_n שורש יחידה פרימיטיבי מסדר n. בהרצאה כבר הגדרתם את השדה הציקלוטומי $\mathbb{Q}(\rho_n)$ והוכחתם כי $\mathrm{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q}) \cong U_n$. Cyclotomic field

דוגמה 11.3. נחשב כמה מהפולינומים הציקלוטומיים הראשונים:

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = \frac{x^2-1}{x-1} = x+1$$
$$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$$
$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = x^2+1$$

דוגמה 11.4. יהי p ראשוני. כבר ראינו בדוגמה 4.6 כי

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

תרגיל 11.5. חשבו את Φ_{15}.

פתרון. חישבנו ש-$\Phi_1(x) = x - 1$ ו-$\Phi_p(x)$ עבור $p = 3$ או $p = 5$ מוכרים לנו:

$$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$$
$$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$$

ולכן

$$\Phi_{15} = \frac{x^{15}-1}{\Phi_1\Phi_3\Phi_5} = \frac{x^{15}-1}{(x^5-1)\Phi_3} = \frac{x^{10}+x^5+1}{\Phi_3} = x^8-x^7+x^5-x^4+x^3-x+1$$

כאשר בשוויון האחרון נעזרנו בחילוק פולינומים.

תרגיל 11.6. חשבו את Φ_{16}.

פתרון. נשים לב כי $x^{16}-1=(x^8-1)(x^8+1)$. השורשים של Φ_{16} הם שורשי יחידה מסדר 16 ולכן אינם מאפסים את x^8-1. לכן $\gcd(\Phi_{16}, x^8-1) = 1$. לפי הגדרה גם מתקיים $\Phi_{16}|x^{16}-1$ ולכן בהכרח $\Phi_{16}|x^8+1$. אבל $\deg\Phi_{16} = \varphi(16) = 8$ ונסיק $\Phi_{16} = x^8+1$.

הערה 11.7. בחוג $\mathbb{Q}[x]$, לכל n מתקיים $\prod_{k=0}^{n-1}(x-\rho_n^k) = x^n-1$, כי אלו שני פולינומים מתוקנים מאותה מעלה ועם אותם שורשים. השורשים של $\Phi_n(x)$ הם ρ_n^k כאשר $k < n$ טבעי וזר ל-n, ואלו בדיוק כל שורשי היחידה הפרימיטיביים מסדר n.

בהרצאה ראיתם כי $\Phi_n(x) \in \mathbb{Z}[x]$ ושהוא אי פריק מעל $\mathbb{Q}$. לכן ניתן להתבונן ב-$\Phi_n(x)$ מעל שדה סופי, שם הוא לעיתים פריק. למשל מעל $\mathbb{F}_2$:

$$\Phi_7(x) = x^6+\cdots+x+1 = (x^3+x+1)(x^3+x^2+1)$$

תרגיל 11.8. תהי $E/\mathbb{Q}$ הרחבת גלואה סופית, שלא מכילה שדות ביניים שהם הרחבות אבליות (כלומר שחבורות גלואה שלהם הן אבליות). הוכיחו כי

$$\mathrm{Gal}(E[\rho_n]/E) \cong U_n$$

פתרון. לפי הטענות בתרגיל 9.9 נסיק

$$\mathrm{Gal}(E[\rho_n]/E) \cong \mathrm{Gal}(\mathbb{Q}[\rho_n]/E \cap \mathbb{Q}[\rho_n])$$

ונטען כי $E \cap \mathbb{Q}[\rho_n] = \mathbb{Q}$. הרי זה שדה ביניים של $\mathbb{Q}[\rho_n]/\mathbb{Q}$, ולכן יש לו חבורת גלואה אבלית (כל תת־חבורה של חבורה אבלית היא אבלית). כלומר זה שדה ביניים של $E/\mathbb{Q}$ עם חבורת גלואה אבלית, ולפי הנתון זה בהכרח רק $\mathbb{Q}$.

תרגיל 11.9 (ממבחן)**.** יהי $K = \mathbb{Q}(\rho_9)$ השדה הציקלוטומי התשיעי.

1. חשבו את $[K : \mathbb{Q}]$ ומצאו את $\mathrm{Gal}(K/\mathbb{Q})$.
2. חשבו את $[K : \mathbb{Q}(\rho_9 + \rho_9^{-1})]$.
3. מצאו את הפולינום המינימלי של $\rho_9 + \rho_9^{-1}$.

פתרון. בכל מקרה נרצה למצוא $\Phi_9(x)$. לפי נוסחת הנסיגה

$$x^9 - x = \Phi_1(x)\Phi_3(x)\Phi_9(x)$$

ולכן

$$\Phi_9(x) = \frac{x^9 - x}{(x-1)(x^2+x+1)} = x^6 + x^3 + 1$$

שלפי שאלת הרשות בתרגיל הבית זה גם בדיוק $\Phi_3(x^3)$.

1. לפי החישוב $[K : \mathbb{Q}] = \deg \Phi_9(x) = \varphi(9) = 6$. חבורת גלואה היא
$$\mathrm{Gal}(K/\mathbb{Q}) \cong U_9 = \{1, 2, 4, 5, 7, 8\}$$
שהיא חבורה אבלית מסדר 6, ולכן בהכרח איזומורפית ל-$\mathbb{Z}/6\mathbb{Z}$.

2. נסמן $\alpha = \rho_9 + \rho_9^{-1}$. השדה $\mathbb{Q}(\alpha)$ הוא שדה ביניים, ונציג אותו כשדה שבת K^H. לפי התאמת גלואה $[K : \mathbb{Q}(\alpha)] = |H|$. איבר ב-$\mathrm{Gal}(K/\mathbb{Q})$ נקבע לפי תמונת ρ_9 והוא מהצורה $\sigma_k(\rho_9) = \rho_9^k$ עבור $k \in U_9$. נבדוק מי מהם שומר על $\mathbb{Q}(\alpha)$. מספיק לבדוק מי מקבע את α:
$$\begin{aligned} \sigma_1(\alpha) &= \mathrm{id}(\alpha) = \alpha & \sigma_5(\alpha) &= \rho_9^5 + \rho_9^4 \neq \alpha \\ \sigma_2(\alpha) &= \rho_9^2 + \rho_9^7 \neq \alpha & \sigma_7(\alpha) &= \rho_9^7 + \rho_9^2 \neq \alpha \\ \sigma_4(\alpha) &= \rho_9^4 + \rho_9^5 \neq \alpha & \sigma_8(\alpha) &= \rho_9^8 + \rho_9 = \alpha \end{aligned}$$
ולכן $H = \langle \sigma_8 \rangle \cong \langle 8 \rangle \leq U_9$, שהיא מסדר 2 ולכן זה ממד ההרחבה.

3. דרגת הפולינום המינימלי היא $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, ומוצאים שלפי התאמת גלואה היא $[U_9 : \langle 8 \rangle] = 3$. נעזר בתזכורת, שלפיה אפשר לחשב את המסלול של α כדי למצוא את הפולינום המינימלי:
$$(x - (\rho_9 + \rho_9^8))(x - (\rho_9^2 + \rho_9^7))(x - (\rho_9^4 + \rho_9^5)) = x^3 - 3x + 1$$

12 תרגול שניים עשר

12.1 הנורמה והעקבה

תזכורת 12.1. תהי K/F הרחבת גלואה עם חבורת גלואה G. כל איבר $\alpha \in K$ מאפס את הפולינום

$$f_\alpha(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \sigma(\alpha))$$

המקדם החופשי והמקדם השני של פולינום זה הם מספיק חשובים כדי שניתן להם שם משלהם.

הגדרה 12.2. הנורמה של α היא Norm

$$\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) \in F$$

ולעיתים נקצר את הסימון ל-$\mathrm{N}(\alpha)$. העקבה של α היא Trace

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) \in F$$

ולעיתים נקצר את הסימון ל-$\mathrm{Tr}(\alpha)$.

יש הגדרות כלליות יותר שמתאימות לכל הרחבת שדות K/F סופית. נזכר כי K הוא מרחב וקטורי ממימד $n = [K : F]$ מעל F. חוג האנדומורפיזמים של K הוא

$$\mathrm{End}_F(K) := \mathrm{Hom}_F(K, K) \cong M_n(F)$$

וישנו שיכון של חוגים $K \hookrightarrow \mathrm{End}_F(K)$ לפי $\alpha \mapsto l_\alpha$ כאשר l_α היא ההעתקה הלינארית $l_\alpha \colon K \to K$ המוגדרת לפי $l_\alpha(k) = \alpha k$. מסתבר שללא תלות בבחירת הבסיס לשיכון $K \hookrightarrow M_n(F)$, הנורמה היא הדטרמיננטה של l_α, והעקבה היא העקבה שלה. העקבה מאפשרת להוכיח שאיברים מסוימים לא שייכים לשדה, והנורמה מאפשרת להוכיח שאיבר מסוים אינו חזקה.

דוגמה 12.3. יהי $D \in \mathbb{Z}$ חופשי מריבועים. עבור שדה המספרים הריבועי $\mathbb{Q}[\sqrt{D}]$ שפגשנו בקורס תורת החוגים נקבל כצפוי

$$\mathrm{N}_{\mathbb{Q}[\sqrt{D}]/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - Db^2 \qquad \mathrm{Tr}_{\mathbb{Q}[\sqrt{D}]/\mathbb{Q}}(a + b\sqrt{D}) = 2a$$

וזה מתאים לשיכון $M_2(\mathbb{Q}) \ni \left(\begin{smallmatrix} a & b \\ Db & a \end{smallmatrix}\right) \mapsfrom a + b\sqrt{D}$ עם בחירת הבסיס $\{1, \sqrt{D}\}$.

בתרגיל הבית תוכיחו שהנורמה כפלית והעקבה חיבורית. זה נובע מכך שאיברי $\mathrm{Gal}(K/F)$ הם הומומורפיזמים של חוגים. בנוסף תוכיחו שהן טרנזיטיביות, כלומר בהנתן שדה ביניים $F \subseteq L \subseteq K$ מתקיים

$$\mathrm{N}_{K/F} = \mathrm{N}_{L/F} \circ \mathrm{N}_{K/L} \qquad \mathrm{Tr}_{K/F} = \mathrm{Tr}_{L/F} \circ \mathrm{Tr}_{K/L}$$

הגדרה 12.4. תהי K/F הרחבה גלואה. בסיס מן הצורה $\{\sigma(\alpha)\,|\,\sigma\in\mathrm{Gal}(K/F)\}$ עבור $\alpha\in K$ קבוע נקרא בסיס נורמלי.

Normal basis

משפט 12.5. לכל הרחבת גלואה סופית K/F קיים בסיס נורמלי.

בפרט, עבור $\alpha\in K$ המגדיר בסיס נורמלי, מתקיים $K=F[\alpha]$. נסמן $n=[K:F]$ וראינו ש-$K=F[\alpha]$ אם ורק אם $|\mathrm{orb}(\alpha)|=n$.

דוגמה 12.6. שימו לב שאם $|\mathrm{orb}(\alpha)|=n$, אז לא בהכרח $\{\sigma(\alpha)\}$ מהווה בסיס נורמלי. למשל, נתבונן בהרחבה $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$ שהיא גלואה. מתקיים $\mathbb{Q}[\sqrt{2},\sqrt{3}]=\mathbb{Q}[\sqrt{2}+\sqrt{3}]$, אבל המסלול

$$\mathrm{orb}(\sqrt{2}+\sqrt{3})=\left\{\sqrt{2}+\sqrt{3},-\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3},-\sqrt{2}-\sqrt{3}\right\}$$

מכיל איברים תלויים לינארית כמו

$$(-\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})=0$$

לעומת זאת לכל $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\in\mathbb{Q}[\sqrt{2},\sqrt{3}]$ עם a,b,c,d כולם שונים מאפס נקבל בסיס נורמלי.

טענה 12.7. תהי K/F הרחבת גלואה סופית ונסמן $G=\mathrm{Gal}(K/F)$. יהי $\alpha\in K$ המגדיר בסיס נורמלי. אז לכל $H\le G$ מתקיים

$$K^H=F\left[\sum_{\sigma\in H}\sigma(\alpha)\right]=F[\mathrm{Tr}_{K/K^H}(\alpha)]$$

הוכחה. תת־החבורה H פועלת על עצמה טרנזיטיבית לפי ההצגה הרגולרית (משפט קיילי). לכן $\sum_{\sigma\in H}\sigma(\alpha)\in K^H$, ונסיק

$$F\left[\sum_{\sigma\in H}\sigma(\alpha)\right]\subseteq K^H$$

כמו כן $\left[F\left[\sum_{\sigma\in H}\sigma(\alpha)\right]:F\right]\le[K^H:F]$, ולכן אם נראה אי שוויון בכיוון השני, סיימנו לפי השוואת ממדים. אבל $\left[F\left[\sum_{\sigma\in H}\sigma(\alpha)\right]:F\right]$ שווה גודל המסלול של $\sum_{\sigma\in H}\sigma(\alpha)$, ובנוסף לפי התאמת גלואה $[K^H:F]=[G:H]$.

נסמן $r=[G:H]$, ולכן מספיק להוכיח שיש לפחות r איברים במסלול של $\sum_{\sigma\in H}\sigma(\alpha)$. נסמן

$$G/H=\{\sigma_1H,\dots,\sigma_rH\}$$

וברור ש-$\sigma_iH\ne\sigma_jH$ עבור $i\ne j$. לכל $i\in\{1,\dots,r\}$ מתקיים

$$\sigma_i\left(\sum_{\sigma\in H}\sigma(\alpha)\right)=\sum_{\sigma\in H}\sigma_i(\sigma(\alpha))=\sum_{\sigma\in\sigma_iH}\sigma(\alpha)$$

ולכן $\left\{\sum_{\sigma\in\sigma_i H}\sigma(\alpha)\,\middle|\, i\in\{1,\ldots,r\}\right\} \subseteq \operatorname{orb}\left\{\sum_{\sigma\in H}\sigma(\alpha)\right\}$ היא תת־קבוצה של המסלול שכל איבריה שונים זה מזה, כי מדובר בסכומים של איברים שונים מהבסיס הנורמלי. לכן גודל המסלול הוא לפחות r, כדרוש. $\square$

תרגיל 12.8. תהי K/F הרחבת גלואה ממימד 2 עם חבורת גלואה $\mathrm{Gal}(K/F)=\langle\sigma\rangle$, ויהי $\alpha\in K$. הוכיחו כי $\{\alpha,\sigma(\alpha)\}$ הוא בסיס נורמלי אם ורק אם $\alpha\notin F$ ו-$\mathrm{Tr}(\alpha)\neq 0$.

פתרון. נניח כי $\{\alpha,\sigma(\alpha)\}$ הוא בסיס נורמלי. נניח בשלילה כי $\alpha\in F$. אבל אז $\sigma(\alpha)=\alpha$, ולכן יש תלות לינארית $\alpha-\sigma(\alpha)=0$. כלומר $\{\alpha,\sigma(\alpha)\}$ בכלל לא בסיס. לכן $\alpha\notin F$. באופן דומה, אם

$$\mathrm{Tr}(\alpha)=\alpha+\sigma(\alpha)=0$$

נקבל תלות לינארית. לכן $\mathrm{Tr}(\alpha)\neq 0$.

בכיוון השני, נניח $\alpha\notin F$ ו-$\mathrm{Tr}(\alpha)\neq 0$. הפולינום המינימלי של α הוא ממעלה 2 (אחרת $\alpha\in F$), ולכן קיימים $a,b\in F$ כך שהפולינום המינימלי הוא x^2-ax+b. כלומר $\mathrm{Tr}(\alpha)=a\neq 0$. כמו כן

$$a=\mathrm{Tr}(\alpha)=\alpha+\sigma(\alpha)$$

ולכן $\sigma(\alpha)=a-\alpha$. כדי להוכיח ש-$\{\alpha,\sigma(\alpha)\}$ הוא בסיס נורמלי, מספיק להראות ששני האיברים האלו בלתי תלויים לינארית (משפט "שלישי חינם", כי גודל הבסיס כממד ההרחבה). יהי

$$r_1\alpha+r_2(a-\alpha)=0$$

צירוף לינארי מתאפס עבור $r_1,r_2\in F$. אזי $(r_1-r_2)\alpha=-r_2 a$. אבל $r_2,a\in F$ ולכן $-r_2 a\in F$. לכן גם אגף שמאל שייך ל-F. אבל $\alpha\notin F$ ואילו $r_1-r_2\in F$. לכן $(r_1-r_2)\alpha\in F$ אם ורק אם $r_1=r_2$. לכן

$$(r_1-r_2)\alpha=0=-r_2 a$$

ומפני ש-$a\neq 0$ נסיק $r_1=r_2=0$ כי F תחום שלמות (ודוגמה לגרסה החיבורית של משפט 90 של הילברט).

משפט 12.9 (משפט 90 של הילברט). תהי K/F הרחבה ציקלית, יהי σ יוצר של $\mathrm{Gal}(K/F)$ ויהי $a\in K$. אזי $\mathrm{N}_{K/F}(a)=1$ אם ורק אם קיים $b\in K^*$ כך ש-$a=b\sigma^{-1}(b)$.

13 תרגול שלושה עשר

13.1 בנייה בסרגל ומחוגה

נתאר "משחק" הנדסי במישור. לפעמים נחליף בין $\mathbb{R}^2$ ובין המישור המרוכב מבלי לשים לב. החוקים שלו הם כאלה: אם נחשוב על כל הנקודות, הישרים והמעגלים במישור אז יש כאלה שאנחנו יכולים לבנות וכאלה שאנחנו לא יכולים לבנות. מה אנחנו יכולים לבנות? מותר להשתמש במספר סופי של הצעדים הבאים:

- בהינתן שתי נקודות P, Q בנות־בנייה, אפשר להעביר את הקו הישר העובר בינהן. זה שימוש בסרגל, שהוא לא מסומן בשנתות וארוך כרצוננו (ויש לו צד אחד).
- בהינתן שתי נקודות P, Q בנות־בנייה, אפשר להעביר את המעגל שמרכזו ב-P ועובר דרך Q. זה שימוש במְחוּגָה, שגם היא רחבה כרצוננו.
- בהינתן ישרים ומעגלים בני־בנייה, אפשר לבנות את נקודות החיתוך שלהם.

כדי להתחיל אנו מקבלים שתי נקודות שמקובל להכריז עליהן בתור $(0, 0)$ ו-$(1, 0)$. כבר בעולם העתיק ידעו לפתור בעיות בנייה רבות, בינהן:

- מציאת אמצע של קטע.
- הורדת אנך לישר דרך נקודה נתונה.
- לחצות זוית, הנתונה בין שני ישרים לא מקבילים.
- בניית מעגל שמרכזו בנקודה נתונה ורדיוסו באורך קטע נתון.
- בניית מחומש משוכלל, ובעיות יותר קשות.

הגדרה 13.1. המספר $a \in \mathbb{R}$ הוא מספר בר־בנייה אם $(a, 0)$ בת־בנייה. מספר מרוכב $a + ib \in \mathbb{C}$ הוא בר־בנייה אם a ו-b בני־בנייה.

Constructible number

מסתבר שאת כל השאלות האלה אפשר לתרגם לשאלה לגבי האם מספרים ניתנים לבנייה. למשל אפשר להוכיח שמצולע משוכלל עם n צלעות ניתן לבנייה אם ורק אם $\cos \frac{2\pi}{n}$ הוא בר־בנייה. שימו לב כי $\cos \alpha$ בר־בנייה אם ורק אם $\sin \alpha$ בר־בנייה אם ורק אם $e^{i\alpha}$ בר־בנייה. אנו נאפיין מספרים בני־בנייה בהמשך.

תרגיל 13.2. יהיו P, Q נקודות נתונות. בנה את נקודת אמצע הקטע.

פתרון. נשרטט מעגל שמרכזו ב-P ורדיוסו באורך PQ. נשרטט מעגל שמרכזו ב-Q ורדיוסו באורך PQ. מעגלים אלו נחתכים בשתי נקודות A, B. כעת נעביר את הקו הישר AB. החיתוך של AB עם הישר PQ זו הנקודה הדרושה.

תרגיל 13.3. נניח כי a, b בני־בנייה. הראו כי $a + b$ בר־בנייה.

פתרון. נבנה מעגל ברדיוס b שמרכזו ב-$(a, 0)$. הוא חותך את ציר ה-x ב-$(a + b, 0)$.

תרגיל 13.4. יהי $a > 0$ מספר בר־בנייה. הוכיחו כי $\sqrt{a}$ בר־בנייה.

פתרון. בהרצאה ראיתם שהמספרים בני־הבנייה סגורים לחיבור, נגדי וכפל במספר רציונלי. לכן גם $\frac{a+1}{2}$ ו-$\frac{|a-1|}{2}$ בני־בנייה. נעביר מעגל שמרכזו ב-$A = \left(\frac{|a-1|}{2}, 0\right)$ ברדיוס $\frac{a+1}{2}$. נסמן נקודת חיתוך של המעגל עם ציר ה-y ב-B וכן את $O = (0, 0)$. המשולש AOB הוא ישר זווית ולפי משפט פיתגורס אורך הצלע OB היא

$$\sqrt{\left(\frac{a+1}{2}\right)^2 - \left(\frac{|a-1|}{2}\right)^2} = \sqrt{a}$$

המספרים בני־הבנייה סגורים לחיבור, כפל, הופכי (שונה מאפס) והוצאת שורש ריבועי. למעשה הם מהווים תת־שדה של המרוכבים, שהוא תת־השדה הקטן ביותר של המרוכבים הכולל את i עם התכונה של סגירות להוצאת שורש ריבועי.

13.2 הרחבות פתירות ופתרון על ידי שורשים

Repeated quadratic extension (or quadratically defined)

הגדרה 13.5. הרחבת שדות K/F היא הרחבה ריבועית חוזרת (גם מוגדרת ריבועית או 2-רדיקלית) אם יש שדות ביניים

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K$$

כך ש-$[F_{i+1} : F_i] = 2$ לכל i.

טענה 13.6. מספר $a \in \mathbb{R}$ הוא בר־בנייה אם ורק אם קיימת הרחבה ריבועית חוזרת $K/\mathbb{Q}$ כך ש-$a \in K$. בפרט, דרגת הפולינום המינימלי $[\mathbb{Q}(a) : \mathbb{Q}]$ של מספר בר־בנייה היא חזקת 2 (אך לא להפך).

בנוסף, אם $K/\mathbb{Q}$ הרחבת גלואה, אז היא ריבועית חוזרת אם ורק אם $\mathrm{Gal}(K/\mathbb{Q})$ היא חבורת-2.

תרגיל 13.7 (ממבחן)**.** האם $e^{2\pi i/7}$ הוא בר־בנייה?

פתרון. זהו שורש יחידה פרימיטיבי מסדר 7. הפולינום המינימלי שלו הוא

$$\frac{x^7-1}{x-1} = x^6 + \cdots + x + 1$$

הוא מדרגה 6, שאינה חזקת 2. לכן הוא לא בר־בנייה.

תרגיל 13.8. האם ניתן באמצעות סרגל ומחוגה לחלק זוית לשבע?

פתרון. בהינתן זוית θ מבקשים לדעת האם ניתן לבנות את $\frac{\theta}{7}$. כמסקנה משאלה בתרגיל הבית השני זה שקול לבניית משובע משוכלל. אבל זה אומר שנוכל לבנות גם את $e^{2\pi i/7}$, בסתירה לתרגיל הקודם.

תרגיל 13.9. יהי p ראשוני מהצורה $2^n + 1$. הוכיחו כי ρ_p הוא בר־בנייה.

פתרון. ההרחבה $\mathbb{Q}(\rho_p)/\mathbb{Q}$ היא גלואה וחבורת גלואה שלה איזומורפית ל-U_p. הסדר של החבורה הוא

$$|U_p| = 2^n + 1 - 1 = 2^n$$

ולכן ρ_p הוא בר־בנייה. בפרט, ניתן לבנות משולש משוכלל, מחומש משוכלל, את $e^{2\pi i/17}$ ואת $e^{2\pi i/257}$.

תרגיל 13.10. תהי הרחבת גלואה E/F עם שני שדות ביניים K_1, K_2 כך שההרחבות K_1/F ו-K_2/F הן מחזקת 2. האם גם ההרחבה $K_1 \vee K_2/F$ מחזקת 2?

פתרון. לא! בהרצאה ראיתם כי קיימת הרחבה כך ש-$\mathrm{Gal}(E/F) \cong S_4$, למשל כאשר $F = \mathbb{Q}$. נבחר את שדות הביניים בעזרת התאמת גלואה

$$K_1 = E^{H_1} \qquad\qquad K_2 = E^{H_2}$$

כאשר תת־החבורה H_1 כוללת את כל התמורות שמקבעות את 1, ותת־החבורה H_2 כוללת את כל התמורות שמקבעות את 2. לפי התאמת גלואה $[K_i : F] = [G : H_i]$. אבל $H_1 \cong H_2 \cong S_3$, ולכן

$$[K_i : F] = [S_4 : S_3] = 4$$

שזו חזקת 2. תת־החבורה $H_1 \cap H_2$ כוללת את כל התמורות שמקבעות את $\{1, 2\}$ ולכן איזומורפית ל-S_2. לכן

$$[K_1 \vee K_2 : F] = [E^{H_1 \cap H_2} : F] = [S_4 : H_1 \cap H_2] = 12$$

אבל 12 אינו חזקת 2, ולכן $K_1 \vee K_2/F$ אינה הרחבה ריבועית חוזרת.

תרגיל 13.11. האם קיימת הרחבת גלואה K/F עם חבורת גלואה S_n?

פתרון. נתבונן בשדה $K = \mathbb{Q}(x_1, \ldots, x_n)$. אז S_n היא תת־חבורה של חבורת גלואה לפי הפעולה "הטבעית"

$$\pi(x_i) = x_{\pi(i)}$$

לכל $\pi \in S_n$. נסמן את שדה השבת $F = \mathbb{Q}(x_1, \ldots, x_n)^{S_n}$. אז ההרחבה K/F היא גלואה. וראינו כי

$$\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(x_1, \ldots, x_n)^{S_n}) \cong S_n$$

היא חבורת גלואה שלה, כדרוש.

תזכורת 13.12. יהי $f(x) \in \mathbb{Q}[x]$ פולינום עם שדה פיצול E. אז $f(x)$ פתיר על ידי רדיקלים אם ורק $\mathrm{Gal}(E/\mathbb{Q})$ היא פתירה. אולי גם ראיתם היא פתירה אם ורק אם $E/\mathbb{Q}$ היא מוגדרת רדיקלית.

שאלה 13.13. האם הפולינום $f(x) = 5x^5 - 100x + 10 \in \mathbb{Q}[x]$ פתיר על ידי רדיקלים?

פתרון. ראשית נשים לב שהפולינום אי פריק לפי קריטריון אייזנשטיין עבור $p = 2$. ננסה למצוא את חבורת גלואה $\mathrm{Gal}(E/\mathbb{Q})$. הנגזרת של $f(x)$ היא

$$f'(x) = 25x^4 - 100$$

והיא מתאפסת כאשר $x^4 = 4$. כלומר $x = \pm\sqrt{2}$. נשים לב כי

$$f(\sqrt{2}) < 0 \qquad\qquad f(-\sqrt{2}) > 0$$

לפי הצבה ישירה. מחישוב $f''(x) = 100x^3$ נשים לב כי $\sqrt{2}$ היא נקודת מינימום ו-$-\sqrt{2}$ היא נקודת מקסימום. מכל המידע הזה נסיק ש-$f(x)$ חותך את ציר x שלוש פעמים ולכן יש לו שלושה שורשים ממשיים ו-2 מרוכבים. לפי תרגיל 8.6 שעשינו בעבר חבורת גלואה היא S_5, שהיא לא פתירה (הרי A_5 שהיא פשוטה ולא אבלית מופיעה בסדרת הנגזרות של S_5). לכן $f(x)$ לא פתיר על ידי רדיקלים.

תרגיל 13.14. תהי E/F הרחבת גלואה עם חבורת גלואה פתירה. הוכיחו כי יש לה שדה ביניים K כך ש-$[K:F]=p$ ראשוני.

פתרון. מפני ש-$G=\mathrm{Gal}(E/F)$ פתירה, אז יש תת־חבורה נורמלית $H \lhd G$ כך ש-G/H היא חבורה אבלית פשוטה, דהיינו $\mathbb{Z}_p$ עבור p ראשוני. נגדיר $K=E^H$. לפי התאמת גלואה נקבל

$$[K:F]=[E^H:E^G]=[G:H]=p$$

כדרוש. שימו לב שאם G לא פתירה, אז הטענה לא נכונה, וישנן חבורות סופיות ללא תת־חבורה מאינדקס ראשוני.

שאלה 13.15. האם הפולינום $f(x)=x^6-3x^3+6\in\mathbb{Q}[x]$ פתיר על ידי רדיקלים?

פתרון. השורשים של $f(x)$ מתקבלים מפתרון משוואה ריבועית במשתנה $y=x^3$:

$$y_{1,2}=\frac{3\pm\sqrt{-15}}{2}$$

לכן ניתן לפרק את $f(x)$ למכפלת פולינומים מעל הרחבה רדיקלית

$$f(x)=\left(x^3-\frac{3+\sqrt{-15}}{2}\right)\left(x^3-\frac{3-\sqrt{-15}}{2}\right)=f_1(x)f_2(x)$$

וכל אחד מן הגורמים $f_i(x)$ הוא ממעלה 3. נזכר שמעל $\mathbb{Q}$ (או כל שדה ממאפיין 0) כל פולינום ממעלה לכל היותר 4 הוא פתיר על ידי רדיקלים (שהרי חבורת גלואה של שדה הפיצול שלו משוכנת ב-S_4, שהיא פתירה). יהיו K_1,K_2 שדות הפיצול של $f_1(x),f_2(x)$, בהתאמה. אז ההרחבות $K_1,K_2/F$ פתירות, ולכן גם $K_1\vee K_2/F$, שהוא שדה הפיצול של F, יהיה הרחבה פתירה. לכן $f(x)$ פתיר על ידי רדיקלים.