

שדות ותורת גלואה
מערכי תרגול קורס 88-311

אוקטובר 2021, גרסה 0.27

תוכן העניינים

3	מבוא	
4	1 תרגול ראשון	
4	1.1 תזכורת מתורת החוגים	
7	1.2 קריטריון אייזנשטיין והלמה של גאוס	
7	2 תרגול שני	
9	2.1 הרחבת שדות	
11	3 תרגול שלישי	
11	3.1 חישוב פולינום מינימלי	
12	3.2 כפליות הממד	
13	4 תרגול רביעי	
13	4.1 שורשי יחידה	
15	4.2 שדות פיצול	
15	5 תרגול חמישי	
15	5.1 המשך שדות פיצול	
17	5.2 המשכה וקומפוזיטום	

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 שינויים ותוספות למערכי תרגול של איתמר שטיין ושירה גילת.
- נשתדל לכתוב **בגופן הזה** כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחבר בתשע"ט ותש"ף: תומר באואר
עדכונים בתשפ"ב: גיא בלשר

1 תרגול ראשון

1.1 תזכורת מתורת החוגים

Rng, or
non-unital ring
Additive group

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

1. $(R, +, 0)$ הוא חבורה אבלית. נקראת החבורה החיבורית של החוג.

2. (R, \cdot) הוא חבורה למחצה.

3. מתקיים פילוג (משמאל ומימין). כלומר לכל $a, b, c \in R$ מתקיים

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

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

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

Field

שדות הם חוגים מאוד טובים. הם חילופיים וכל איבר לא אפסי בהם הפיך.

הגדרה 1.3. יהי R חוג. **אידיאל** של R הוא תת-חבורה חיבורית $I \subseteq R$ שמקיימת בליעה ביחס לכפל: $IR, RI \subseteq I$.

Ideal

תזכורת 1.4. יהי F שדה. נתבונן בחוג $F[x]$.

• זהו תחום אוקלידי – ניתן לחלק פולינומים עם שארית;

• לכן, זהו תחום ראשי – כל אידיאל ב- $F[x]$ נוצר על ידי פולינום אחד. אפשר ממש למצוא את היוצר: היוצר של אידיאל $I \triangleleft F[x]$ הוא הפולינום הלא אפסי מדרגה מינימלית ששייך ל- I .

• האידיאלים המקסימליים ב- $F[x]$ הם בדיוק האידיאלים מהצורה $\langle f(x) \rangle$ כאשר $f \neq 0$ הוא פולינום אי-פריק.

• (אפשר להמשיך למספר משתנים: החוג $F[x_1, \dots, x_n]$ הוא תחום פריקות יחידה ובפרט תחום שלמות, אבל לא תחום ראשי.)

מסקנה 1.5. אם F שדה ו- $f \in F[x]$ פולינום אי-פריק, אז $F[x]/\langle f \rangle$ הוא שדה, ו- F משוכן בתוכו:

$$F \hookrightarrow F[x]/\langle f \rangle$$

לפי המסקנה האחרונה, כדי להבין שדות, עלינו להבין פולינומים אי פריקים.

תזכורת 1.6. יהי R תחום שלמות. איבר לא הפיך $a \in R$ נקרא **אי פריק** אם $a = bc$ גורר ש- b הפיך או c הפיך.

Irreducible

שאלה 1.7. 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 ממעלה 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.

טענה 1.8. לפולינום $f(x) \in F[x]$ ממעלה n מעל שדה יש לכל היותר n שורשים.

דוגמה 1.9. האם $x^n - 1$ פריק עבור $n > 1$ (נניח מעל \mathbb{Q})? כן, כי מייד רואים ש- $x = 1$ הוא שורש.

תרגיל 1.10. יהי $f(x)$ פולינום ממעלה 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 ממעלה 1 וזה אומר של- $f(x)$ יש שורש.

דוגמה 1.11. 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 1.12. 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.

1.13. הערה. אם $f(x) \in \mathbb{Q}[x]$ אז ניתן להכפיל במכפלה 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 1.14. יהי $f(x) = a_n x^n + \dots + a_0$ 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

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

נכפול ב- r^n ונקבל

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

מה שאומר ש- $a_0 r^n \mid a_n q^n - 1$ ו- $r \mid a_n q^n - 1$, אבל בגלל ש- r ו- q זרים (הרי השבר מצומצם) אז מתקיים

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

תרגיל 1.15. 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 1.16. 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 1.17. זכרו כי לפולינום ממעלה אי זוגית מעל \mathbb{R} תמיד יש שורש אחד לפחות ולכן הוא תמיד פריק.

1.2 קריטריון אייזנשטיין והלמה של גאוס

נעבור לטכניקות אחרות לבדיקת פריקות. מעכשיו נניח כי R תחום שלמות ו- F שדה השברים שלו. הדוגמה שבדרך כלל תשמש אותנו היא $R = \mathbb{Z}$ ו- $F = \mathbb{Q}$.

Eisenstein's
criterion

משפט 1.18 (קריטריון אייזנשטיין). יהי $P \triangleleft R$ אידיאל ראשוני. יהי $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ פולינום המקיים

$$i \neq n \quad a_i \in P \bullet$$

$$a_n \notin P \bullet$$

$$a_0 \notin P^2 \bullet$$

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

תרגיל 1.20. האם הפולינום $x^4 + 4x^3 + 6x^2 - 1$ אי פריק מעל \mathbb{Q} ?

כדי לפתור את התרגיל נעזר בעובדה ההבאה:

טענה 1.21. $f(x)$ 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 מעלה 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.

2 תרגול שני

לשיטה הבאה שנציג צריך תזכורת נוספת:

תזכורת 2.1 (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 שמעלתם קטנה מ- $\deg f(x)$.

תזכורת 2.2 (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 2.3 (שיטת הרדוקציה). יהי $f(x) \in \mathbb{Z}[x]$ ויהי p ראשוני כלשהו. נסמן ב- $\bar{f}(x)$ את הפולינום המתקבל מביצוע מודולו p למקדמי f . אם $\deg \bar{f}(x) = \deg f(x)$ ו- $\bar{f}(x)$ אי פריק אז גם $f(x)$ אי פריק.

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

תרגיל 2.4. 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 מעלה 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.

תרגיל 2.5. הפולינום $f(x) = x^4 + 1$ הוא אי-פריק מעל \mathbb{Q} . הראו שלכל p ראשוני, f פריק ב- \mathbb{F}_p .

פתרון. ראשית, כדי להוכיח ש- $f(x)$ אי-פריק מעל \mathbb{Q} , נשים לב כי

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

שהוא אי-פריק לפי אייזנשטיין עם $p = 2$.

כעת נעבור ל- \mathbb{F}_p . נראה שאפשר למצוא פירוק מהצורה

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

נשווה מקדמים:

$$a + c = 0$$

$$b + ac + d = 0$$

$$ad + bc = 0$$

$$bd = 1$$

אם נציב את המשוואה הראשונה ואת המשוואה האחרונה בשתי המשוואות האמצעיות, נקבל

$$b - a^2 + \frac{1}{b} = 0$$

$$\frac{a}{b} - ab = 0$$

כלומר

$$b + \frac{1}{b} = a^2$$

$$\frac{a}{b} = ab$$

נחלק לשני מקרים:

- אם $a = 0$, נרצה שיתקיים $b^2 + 1 = 0$ (כלומר $\sqrt{-1} \in \mathbb{F}_p$).
- אם $a \neq 0$, נרצה שיתקיים $b^2 = 1$, כלומר $b = \pm 1$. נציב במשוואה הראשונה ונקבל $a^2 = \pm 2 \in \mathbb{F}_p$, כלומר רוצים $\sqrt{\pm 2} \in \mathbb{F}_p$.

לכן עלינו להראות שלכל p , לפחות אחד מבין $-1, 2, -2$ הוא ריבוע מודולו p . בתרגיל הבית תוכיחו כי $\mathbb{F}_p^\times = \langle g \rangle$ היא חבורה ציקלית, כלומר $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$; לכן $(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$ ולכן $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$. נתבונן במחלקות המתאימות ל- $-1, 2, -2$ ב- $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$; אם -1 ו- 2 אינם ריבועים, אז שניהם מתאימים למחלקה הלא טריוויאלית, ולכן מכפלתם (-2) תתאים למחלקה הטריוויאלית, כלומר -2 כן יהיה ריבוע מודולו p .

2.1 הרחבת שדות

Subfield
Field extension

Intermediate
field

הגדרה 2.6. יהי $F \subseteq K$ 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 ביניהם כי שדה הוא חוג פשוט ומכאן שחוגי המנה שלו לא מעניינים.
אם ישנה שרשרת של שדות $F \subseteq L \subseteq K$ נאמר כי L הוא שדה ביניים של ההרחבה K/F .

תזכורת 2.7. ראינו בתרגול הקודם דרך לבנות הרחבת שדות מתוך השדה F : אם $f \in F[x]$ פולינום אי-פריק, אז $F[x]/\langle f \rangle$ הוא שדה שמכיל את f . אם $\deg f = n$, הוכחתם בתרגיל הבית כי $\{1, x, \dots, x^{n-1}\}$ הוא בסיס של $F[x]/\langle f \rangle$ כמרחב וקטורי מעל F .

תרגיל 2.8. בשדה $\mathbb{Q}[x]/\langle x^3 - x^2 + 1 \rangle$, חשבו את ההופכי של $x^2 - 1$ כצירוף לינארי של $1, x, x^2$.

פתרון. נסמן $f(x) = x^3 - x^2 + 1$ ו- $g(x) = x^2 - 1$. כדי לחשב את ההופכי, ניעזר באלגוריתם אוקלידס המורחב למצוא $a(x), b(x) \in \mathbb{Q}[x]$ שעבורם

$$a(x) \cdot f(x) + b(x) \cdot g(x) = 1$$

נחלק עם שארית:

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

ולכן

$$x = 1 \cdot (x^3 - x^2 + 1) - (x - 1) \cdot (x^2 - 1) = f(x) - (x - 1)g(x)$$

לשלב הבא,

$$x^2 - 1 = x \cdot x - 1$$

ולכן

$$1 = x \cdot x - 1 \cdot (x^2 - 1) = x \cdot (f(x) - (x - 1)g(x)) - g(x) = x \cdot f(x) + (-x^2 + x - 1)g(x)$$

בסך הכל $a(x) = x$ ו- $b(x) = -x^2 + x - 1$. לכן ההופכי של $x^2 - 1$ בשדה $\mathbb{Q}[x]/\langle x^3 - x^2 + 1 \rangle$ הוא $-x^2 + x - 1$.

תזכורת 2.9. תהי K/F הרחבת שדות ויהי $a \in K$.

• מגדירים $F[a] = \{f(a) \mid f \in F[x]\} = \{\sum_{i=0}^n \alpha_i a^i \mid \alpha_i \in F\}$. זהו תת-חוג של F .

• 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**. 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 $a \in F$.

Simple extension

Algebraic

Transcendental

אם a הוא **אלגברי** מעל F , כלומר שורש של איזשהו פולינום לא אפסי עם מקדמים ב- F , אז $F[a]$ הוא שדה ומתקיים $F[a] = F(a)$; אחרת, אומרים ש- a הוא **טרנסצנדנטי** מעל F , ואז $F[a] \cong F[x]$ ו- $F(a) \cong F(x)$.

דוגמה 2.10. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. 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- $(\sqrt{2})^{-1} = \frac{1}{2}\sqrt{2}$.

תרגיל 2.11. 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 2.12. כמו שאפשר לספח איבר אחד, אפשר לספח קבוצת איברים, והעיקרון דומה.

תרגיל 2.13. 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

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

3 תרגול שלישי

Dimension

3.1 הגדרה 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 הזה של אינדקס שראינו בתורת החבורות.

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

3.3 דוגמה $[C : R] = 2, [R : Q] = \infty, [Q[\sqrt{2}] : Q] = 2$.

3.4 משפט יהי פולינום אי פריק f 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:

3.5 טענה 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- $b \in F[a]$.

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

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

3.1 חישוב פולינום מינימלי

3.8 תרגיל מהו הפולינום המינימלי של $\sqrt{2} + \sqrt{3}$ מעל Q ? מעל $Q(\sqrt{2})$?

פתרון. נסמן $a = \sqrt{2} + \sqrt{3}$. מעל $Q(\sqrt{2})$,

$$a - \sqrt{2} = \sqrt{3} \implies a^2 - 2\sqrt{2}a + 2 = 3 \implies a^2 - 2\sqrt{2}a - 1 = 0$$

נטען כי $f(x) = x^2 - 2\sqrt{2}x - 1$ הוא הפולינום המינימלי של a מעל $Q(\sqrt{2})$. אכן, $\sqrt{2} + \sqrt{3} \notin Q(\sqrt{2})$, ולכן הפולינום המינימלי לא יכול להיות לינארי. לכן הוא מדרגה 2, אבל $f(x)$ מדרגה 2 ולכן הוא המינימלי. מעל Q , נשים לב כי

$$a^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$$

ולכן $a^2 - 5 = 2\sqrt{6}$ נעלה בריבוע ונקבל

$$a^4 - 10a^2 + 25 = 24 \implies a^4 - 10a^2 + 1 = 0$$

נטען כי $g(x) = x^4 - 10x^2 + 1$ הוא הפולינום המינימלי של $\sqrt{2} + \sqrt{3}$. אכן, הוא מאפס אותו; כדי להראות אי-פריקות, ניזכר שמתרגיל הבית מתקיים $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, וניתן לוודא כי $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. לכן הדרגה של הפולינום המינימלי של $\sqrt{2} + \sqrt{3}$ מעל \mathbb{Q} צריכה להיות 4, ולכן זהו $g(x)$.

תרגיל 3.9. 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).

3.2 כפליות הממד

תזכורת 3.10 (כפליות הממד). אם $F \subseteq L \subseteq K$, אז

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

תרגיל 3.11. תהי $F \subseteq K$ הרחבת שדות ויהיו $a, b \in K \setminus F$. 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 ממעלה 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 ממעלה קטנה (או שווה) ממנו. לכן

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

ומכאן נקבל בעזרת כפליות הממד:

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

תרגיל 3.12. 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 $n, m \mid [F(a, b) : F]$.

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

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

דוגמה 3.13. $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{11}) : \mathbb{Q}] = 6$ כי $(2, 3) = 1$.

תרגיל 3.14. תהי K/F הרחבה סופית, ויהי $p \in F[x]$ פולינום אי-פריק (מעל F) כך ש- $\deg p \nmid [K : F]$. הוכיחו כי ל- p אין שורש ב- K .

הוכחה. נניח בשלילה שיש שורש $\alpha \in K$ של p . לכן $F \subseteq F(\alpha) \subseteq K$. ממשפט 3.4, $\deg p = [F(\alpha) : F] \mid [K : F]$. אבל מכפלויות המימד נקבל $[K : F] \nmid \deg p$. בסתירה לנתון. \square

הערה 3.15. ייתכן שמעל F הפולינום p יהפוך להיות פריק, גם אם אין לו שורש. למשל, אם ניקח $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$ ו- $p(x) = x^4 - 2$. $p(x) = (x^2 + \sqrt{2})(x^2 - \sqrt{2})$ כי מעל K אבל פריק מעל \mathbb{Q} לפי אייזנשטיין עם $p = 2$.

4 תרגול רביעי

4.1 שורשי יחידה

Primitive root of unity

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

דוגמה 4.2. ב- \mathbb{C} לכל $n \in \mathbb{N}$ יש שורש יחידה פרימיטיבי, 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 פרימיטיבי מדרגה n . הוכיחו כי $1, \rho, \dots, \rho^{n-1}$ כולם שונים זה מזה, והראו כי

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

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 ממעלה n . לכן $x^n - 1 = \prod_{i=1}^n (x - \rho^i)$.

דוגמה 4.5. יהי שורש יחידה פרמיטיבי מדרגה n . אז

$$\mathbb{Q}(\rho) = \{a_0 + a_1\rho + \dots + a_{n-1}\rho^{n-1} \mid a_i \in \mathbb{Q}\}$$

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:

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

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 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 3.12 (או מתרגיל הבית), נקבל $[E : \mathbb{Q}] = 20$.

5 תרגול חמישי

5.1 המשך שדות פיצול

תרגיל 5.1. 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 5.2. 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 5.3. כמה תת-שדות יש ל- \mathbb{C} שאיזומורפיים ל- $\mathbb{Q}(\sqrt{2 + \sqrt{5}})$?

פתרון. אם $K \subseteq \mathbb{C}$ הוא שדה ויש $\varphi: \mathbb{Q}(\sqrt{2 + \sqrt{5}}) \rightarrow K$ 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 5.4. 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 5.5. 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 ממעלה p . לכן שדה הפיצול הוא

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

טענה 5.6. לכל פולינום $f \in F[x]$ יש שדה מפצל שממדו אינו עולה על $(\deg f)!$.
דוגמה 5.7. בתרגיל 5.5, אם $f(x)$ אי פריק, אז $[F[\alpha] : F] = p$ וזה יכול להיות ממש קטן מ- $p!$.

5.2 המשכה וקומפוזיטום

תרגיל 5.8. יהיו $f, g: F(a_1, \dots, a_n) \rightarrow K$ שני הומומורפיזמים שמקיימים

$$\begin{aligned} f(x) &= g(x) \quad \forall x \in F \\ f(a_i) &= g(a_i) \quad 1 \leq i \leq n \end{aligned}$$

הוכיחו כי $f = g$.

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

הגדרה 5.9. תהי K/F הרחבת שדות, ויהי $\varphi: F \rightarrow E$ שיכון (למה כל הומומורפיזם של שדות הוא שיכון?). שיכון $\bar{\varphi}: K \rightarrow E$ נקרא **המשכה** של φ אם הצמצום של $\bar{\varphi}$ ל- F שווה ל- φ .

Extension of an embedding

תרגיל 5.10. תהי K/F הרחבת שדות. יהי $g(x) \in F[x]$ אי פריק ויהיו a, b שני שורשים של g . הוכיחו כי יש איזומורפיזם

$$f: F(a) \rightarrow F(b)$$

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

$$\hat{i}: F[x] \rightarrow F(b)$$

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

$$f: F[x]/\langle g(x) \rangle \rightarrow F(b)$$

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

תזכורת 5.11. 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

$$f: F(a) \rightarrow F(b)$$

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

תרגיל 5.12. 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 $f: E \rightarrow E$ שמקבע את איברי F ומקיים $f(a) = b$.

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

Compositum

הגדרה 5.13. אם $F, L \subseteq K$, אז **הקומפוזיטום** של F ו- L הוא תת-השדה המינימלי שמכיל את F, L ומסומן בדרך כלל FL או $F \vee L$.

תרגיל 5.14. 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

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

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

$$f_i: F(a) \rightarrow F(b_i)$$

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

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

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