שדות ותורת גלואה
מערכי תרגול קורס 88-311

אוקטובר 2018, גרסה 0.3

אוניברסיטת בר-אילן

סמסטר א' תשע"ט

תוכן העניינים

מבוא **3**

1 תרגול ראשון **4**
1.1 תזכורת מתורת החוגים 4

2 תרגול שני **7**
2.1 בנייה בסרגל ומחוגה 7
2.2 תזכורת נוספת מתורת החוגים 9

3 תרגול שלישי **10**
3.1 הרחבת שדות 10
3.2 שורשי יחידה 12

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 בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי התרגול של איתמר שטיין ושירה גילת.
- This font נשתדל לכתוב בגופן הזה כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחבר בתשע"ט: 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 $(R\setminus\{0\},\cdot)$ הוא 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 $F[x]$ הם 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 $a\in R$ לא הפיך 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 ש-$\deg f(x)\geq 2$.
- 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 $n>1$ (ננית מעל $\mathbb{Q}$)? כן, כי מייד רואים ש-$x=1$ הוא שורש.

תרגיל 1.6. יהי $f(x)$ פולינום מדרגה 2 או 3 אזי $f(x)$ 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 $\mathbb{Q}$? פותרים, 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 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 1.10. יהי $f(x)=a_nx^n+\cdots+a_0$ 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

$$a_nq^n+a_{n-1}q^{n-1}r+\cdots+a_1qr^{n-1}+a_0r^n=0$$

מה שאומר ש-$q \mid a_0r^n$ ו-$r \mid a_nq^n$, 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:

$$\frac{q}{r} \in \{\pm1, \pm2, \pm3, \pm6\}$$

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.

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

Eisenstein's criterion

משפט 1.14 (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

- $a_i \in P$ 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 המירבי 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 1.15. x^n-4x+2 אי פריק מעל $\mathbb{Q}$ כי הוא אייזנשטיין עבור $p = 2 \in \mathbb{Z}$. לפעמים צריך להתחכם יותר.

תרגיל 1.16. האם הפולינום $x^4+4x^3+6x^2-1$ אי פריק מעל $\mathbb{Q}$?

כדי לפתור את התרגיל נעזר בעובדה ההבאה:

טענה 1.17. $f(x)$ 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. □

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 1.18 (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 1.19 (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 1.20 (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 1.21. 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 1.22. לפולינום $f(x) \in F[x]$ מדרגה n מעל שדה יש לכל היותר n שורשים.

2 תרגול שני

2.1 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 2.1. המספר $a \in \mathbb{R}$ הוא מספר בר־בנייה אם $(a,0)$ בת־בנייה. מספר מרוכב $a+ib \in \mathbb{C}$ ניתן לבנייה אם a ו־b ניתנים לבנייה.

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 הקורס.

תרגיל 2.2. 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 2.3. נניח כי a, b בני־בנייה. הראו כי $a+b$ בר־בנייה.

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

תרגיל 2.4. 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 הוצאת שורש ריבועי.

2.2 תזכורת נוספת מתורת החוגים

עד סוף התרגול נעשה תרגילים שיכינו אותנו להמשך הקורס.

תרגיל 2.5. 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 2.6. בהמשך לתרגיל הקודם. בטאו את ה gcd 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 2.7. 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

הגדרה 3.1. 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 בינהם 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 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.

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.

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 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:

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:

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

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).

3.2 שורשי יחידה

הגדרה 3.19. יהי F שדה. איבר $\rho\in F$ נקרא שורש יחידה פרימיטיבי מדרגה n אם הסדר (הכפלי) שלו הוא n. כלומר $\rho^n=1$ וגם $\rho^i\neq 1$ לכל $1\leq i<n$.

דוגמה 3.20. ב-$\mathbb{C}$ לכל $n\in\mathbb{N}$ יש שורש יחידה פרמיטיבי, למשל $\rho_n=e^{2\pi i/n}$.

הערה 3.21. אם ρ שורש יחידה פרימיטיבי מדרגה n, אז ρ^k הוא שורש יחידה פרימיטיבי אם ורק אם $(n,k)=1$.

תרגיל 3.22. 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 $x^n - 1 = \prod_{i=1}^{n} (x - \rho^i)$.

דוגמה 3.23. 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 3.24. יהי p ראשוני ויהי ρ_p שורש יחידה פרמיטיבי מדרגה p. אז הפולינום המינימלי שלו הוא

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

כלומר $[\mathbb{Q}[\rho_p] : \mathbb{Q}] = p - 1$.

תרגיל 3.25. 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 3.26. 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 3.27. בהמשך לתרגיל הקודם, מצאו פולינום מינימלי של ρ.

פתרון. אנחנו יודעים ש $\rho^{12}=1$ כלומר הוא שורש של $x^{12}-1$. אבל זה כמובן פריק. נתחיל לפרק

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

ρ שורש של x^6+1. לפי הנוסחה $a^3+b^3=(a+b)(a^2-ab+b^2)$ נפרק ונקבל

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

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 3.28. בהמשך הקורס תלמדו את הפירוק המלא של הפולינום x^n-1.