שדות ותורת גלואה
מערכי תרגול קורס 88-311

אוקטובר 2021, גרסה 0.27

אוניברסיטת בר-אילן

סמסטר א׳ תשפ״ב

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 שינויים ותוספות למערכי תרגול 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
עדכונים בתשפ"ב: גיא בלשר

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 פילוג (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 לא אפסי בהם הפיך.

Ideal

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

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

- זהו תחום אוקלידי – ניתן לחלק פולינומים עם שארית;
- לכן, זהו תחום ראשי – כל אידאל ב-$F[x]$ נוצר על ידי פולינום אחד. אפשר ממש למצוא את היוצר: היוצר של אידאל $0\neq I\lhd F[x]$ הוא הפולינום הלא אפסי מדרגה מינימלית ששייך ל-I.
- האידאלים המקסימליים ב-$F[x]$ הם בדיוק האידאלים 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-$0\neq f\in F[x]$ 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.

Irreducible

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.

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.

הערה 1.13. 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 1.14. 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 1.15. 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:

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

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-$F = \mathbb{Q}$.

משפט 1.18 (קריטריון אייזנשטיין)**.** יהי R ‏$P \lhd R$ 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 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. □

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 $\deg \overline{f}(x) = \deg f(x)$ ו-$\overline{f}(x)$ אי פריק אז גם $f(x)$ אי פריק.

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

תרגיל 2.4. 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:

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= 0 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

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

$$\begin{aligned} b - a^2 + \frac{1}{b} &= 0 \\ \frac{a}{b} - ab &= 0 \end{aligned}$$

כלומר

$$\begin{aligned} b + \frac{1}{b} &= a^2 \\ \frac{a}{b} &= ab \end{aligned}$$

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 $a^2=\pm 2$, 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 $(\mathbb{F}_p^\times)^2\cong 2\mathbb{Z}/(p-1)\mathbb{Z}\cong\mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$, ולכן $\left[\mathbb{F}_p^\times:(\mathbb{F}_p^\times)^2\right]=2$. 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

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 בינהם כי שדה הוא חוג פשוט ומכאן שחוגי המנה שלו לא מעניינים.

Subfield
Field extension

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

Intermediate field

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**. 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 $a \in F$.

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-$\left(\sqrt{2}\right)^{-1} = \frac{1}{2}\sqrt{2}$.

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

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

הגדרה 2.14. 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 2.15. לכל שדה F מתקיים $[K:F]=1$ אם ורק אם $K=F$.

דוגמה 2.16. $[\mathbb{C}:\mathbb{R}]=2$, $[\mathbb{R}:\mathbb{Q}]=\infty$, $\left[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}\right]=2$.

משפט 2.17. יהי פולינום אי פריק f מעל F עם שורש a, אז $\deg f=[F\left(a\right):F]$.

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

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

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 2.18. 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-$b\in F[a]$.

שאלה 2.19. 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 2.20. המצבים שבהם כן כל השורשים נמצאים בהרחבה הם חשובים ונדבר עליהם בהרחבה בהמשך הקורס.

2.2 חישוב פולינום מינימלי

תרגיל 2.21. 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).