תורת גלואה

עוזי וישנה

זוהי חוברת תרגילים[1] המלווה את הקורסים "תורת גלואה" בבר־אילן. החומר חולק למספר גדול של נושאים, וכל אחד מהם מוצג (במידת האפשר) בשלמותו ־ כולל ההגדרות והמשפטים היסודיים. טענות העזר והשיטות הסטנדרטיות נוסחו כתרגילים, ולחלקם ניתנת הדרכה או רמז. כל סעיף מחולק לכמה נושאים, ובכל נושא השאלות מסודרות כך שהתרגילים התאורטיים יותר קודמים.

התרגילים (כולל הטענות והמשפטים) מלווים בציון רמת הקושי שלהם: תרגילים קלים (^{1}) דורשים בדרך־כלל שליטה בהגדרות ותו לא. תרגילים טכניים מורכבים, לא רגילים או סתם קשים סומנו ב־ (^{3}). שאר התרגילים קיבלו את הציון (^{2}), ($^{2+}$) או ($^{2-}$). מספר התרגילים מספיק כדי לפתור חלק מן התרגילים בכיתה, חלק כתרגילי בית, ואת השאר לקראת המבחן. במספר סעיפים הרחבנו מעבר לרמה המכוסה בדרך כלל בקורסי המבוא. למשל, חלק מן השיטות לפירוק פולינומים 2.2, חישוב הפולינום המינימלי בעזרת מטריצות 3.2, וכן חלקים של פרק 8 ושל סעיף 9.3.

החומר תורגם באופן אוטומטי־למחצה מקובץ Oren, ואני תולה בתוכנת התרגום את כל השגיאות (גם אלו שהכנסתי במו־ידי). בשאר הבעיות אשמים השגעונות של LaTeX בעברית.

---

[1] Oct 2006, Version 3.0

תוכן עניינים

1 מבוא לשדות 7

1.1 בניה פנימית של שדות 7

1.1.1 סיפוח אברים לשדה 7

1.1.2 יוצרים של הרחבה 8

1.2 חוגי פולינומים 8

1.2.1 חוגי מנה 9

1.3 שדות כמרחבים וקטוריים 10

1.3.1 בסיס של הרחבה 10

1.3.2 מימד של הרחבה 11

1.3.3 סיפוח שורשים ריבועיים ל־ $\mathbb{Q}$ 11

1.4 פולינום מינימלי 12

1.4.1 תכונות של הפולינום המינימלי 12

1.4.2 חישוב הפולינום המינימלי 13

1.4.3 מימדים 14

2 פירוק פולינומים 15

2.1 שורשים 15

2.1.1 מספר השורשים של פולינום 15

2.1.2 שורשים רציונליים 16

2.2 שיטות כלליות לפירוק 17

2.2.1 הקריטריון של אייזנשטיין 17

2.2.2 השלמה לריבוע 19

2.2.3 פירוק לפי שורשים 19

2.3 פולינומים מעל $\mathbb{Z}_p$ 20

2.3.1 שורשים מעל $\mathbb{Z}_p$ 20

2.3.2 פירוק פולינומים מעל $\mathbb{Z}_p$ 21

2.3.3 פולינומים מעל $\mathbb{C}$ 21

2.4 משוואות ממעלה 3 ו־ 4 22

2.4.1 הצבות ליניאריות 22

2.4.2 משוואה ממעלה 3 (del Ferro, 1515) 22
2.4.3 משוואה ממעלה 4 (Ferrari, 1545) 22

3 שדות 25
3.1 המאפיין של שדה 25
3.2 הרחבות אלגבריות 25
3.2.1 חישוב פולינום מינימלי ־ ההצגה הרגולרית 26
3.2.2 תת־שדות 27
3.3 שלמים אלגבריים 28

4 בניה חיצונית של שדות 29
4.1 שורש של פולינום 29
4.2 שדות פיצול 30
4.3 הרחבות טרנסצנדנטיות 31
4.4 השדות השלמים $\mathbb{R}$ $\mathbb{C}$ 32

5 שורשי היחידה 33
5.1 הפולינומים הציקלוטומיים 33
5.1.1 איפריקות הפולינומים הציקלוטומיים 35
5.2 תכונות יסודיות של שורשי היחידה 36

6 נורמליות וספרביליות 39
6.1 הרחבות ספרביליות 39
6.1.1 פולינומים 39
6.1.2 הרחבות 40
6.1.3 שדות סופיים 40
6.2 הרחבות נורמליות 40

7 תורת גלואה 43
7.1 חבורת גלואה 43
7.1.1 תמונות של אברים 44
7.1.2 ספירת אוטומורפיזמים 44
7.1.3 חישוב חבורת גלואה 44
7.1.4 $\mathrm{Gal}(K/F)$ כחבורת תמורות 46
7.2 התאמת גלואה 46
7.2.1 H° ו־ L^* 46
7.2.2 כמה משפטים 47
7.2.3 התאמת גלואה 47
7.2.4 דוגמא: הפולינום $f(\lambda) = \lambda^4 - 3$ 48
7.2.5 תרגילים נוספים 48

7.2.6 שורשי היחידה 49
7.2.7 סגור גלואה 49
7.2.8 מכפלה טנזורית של שדות 50
7.2.9 הרחבות ביניים שהן גלואה 50
7.2.10 ההרחבה האבלית המקסימלית 50
7.3 נורמה ועקבה 50
7.3.1 תכונות יסוד 51
7.3.2 שימושים 52
7.3.3 עקבה בהרחבות ציקליות 52
7.3.4 נורמה בהרחבות ציקליות 53

8 שדות סופיים 55
8.1 תורת המבנה של שדות סופיים 55
8.1.1 קיום ויחידות 55
8.1.2 הכלות 55
8.2 אוטומורפיזם פרובניוס וחבורות גלואה 56
8.2.1 המבנה של שדה סופי 56
8.3 פולינומים מעל שדות סופיים 57
8.3.1 פולינום מינימלי 57
8.3.2 שורשי יחידה 57
8.3.3 חישוב שדות פיצול 58
8.3.4 הפולינומים האיפריקים 58
8.3.5 ספירת פולינומים איפריקים 59
8.4 פירוק לגורמים מעל שדה סופי 59
8.4.1 גורמים כפולים 59
8.4.2 פירוק לגורמים אחידים 60
8.4.3 פירוק כללי לגורמים 61
8.5 גאומטריה פרוייקטיבית 62

9 הרחבות רדיקליות 63
9.1 חבורות פתירות 63
9.1.1 חבורת הקומוטטורים 63
9.2 הרחבות רדיקליות 64
9.2.1 פולינומים שאינם פתירים על־ידי רדיקלים 64
9.3 הדיסקרימיננטה 65
9.3.1 חישוב הדיסקרימיננטה 65
9.3.2 דיסקרימיננטה של פולינומים ציקלוטומיים 66
9.3.3 פולינומים ממעלה 3 67
9.3.4 מקדמי פולינום ושורשיו 67
9.3.5 שאלות נוספות 68

10 בניות במחוגה וסרגל 69
10.1 בניות אלמנטריות 69
10.2 השדה של נקודות ניתנות לבניה 69
10.3 מספרים ניתנים לבניה 70
10.4 הבעיות של ימי קדם 71
10.4.1 בניית זוויות 71
10.4.2 בניית מצולעים משוכללים 72

פרק 1

מבוא לשדות

פרק זה עוסק במושגים הבסיסיים של תורת השדות: הגדלה של תת־שדה (על־ידי סיפוח איבר), הפולינום המינימלי של איבר בשדה, והקשר של זה למימד של הרחבת שדות. סעיף 1.2 מספק את הרקע הדרוש בחוגי פולינומים מעל שדה ־ האוקלידיות, חוגי מנה, ותכונות של פולינומים איפריקים. בשיטות לפירוק נעסוק בפרק הבא.

1.1 בניה פנימית של שדות

1.1.1 סיפוח אברים לשדה

תרגיל 1.1.1 (**) יהי K שדה. תהי $\mathcal{L}$ משפחה של תת־שדות של K. הוכח ש־ $L = \bigcap_{F\in\mathcal{L}} F$ תת־שדה של K.

יהי K שדה. אם $F \subseteq K$ תת־שדה, ו־ $\alpha \in K$, מסמנים ב־ $F(\alpha)$ את חיתוך כל תת־השדות של K המכילים את F ואת α.

תרגיל 1.1.2 (*) הוכח ש־ $F(\alpha)$ הוא השדה הקטן ביותר המכיל את F ואת α.

הגדרה 1.1.3 בדומה, $F(\alpha_1,\dots,\alpha_t)$ השדה הקטן ביותר המכיל את F ואת α_1,...,α_t.

תרגיל 1.1.4 (*) $F(\alpha)(\beta) = F(\alpha,\beta)$ (נסח מה בדיוק יש כאן להוכיח).

הגדרה 1.1.5 אם $f(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n \in F[\lambda]$ פולינום, אז $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$ ־ הצבת α במקום λ . בסעיף 1.4 נדון בכך בהרחבה.

תרגיל 1.1.6 (*) נניח $F \subseteq K$, $\alpha,\beta \in K$. $F(\alpha) \subseteq F(\beta)$ אם ורק אם $\alpha \in F(\beta)$.

תרגיל 1.1.7 (*) $F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f,g \in F[\lambda], g(\alpha) \neq 0 \right\}$. ה דרכה. צריך להוכיח שאגף ימין הוא שדה, המכיל את F ואת α, והוא מינימלי בעל תכונות אלה.

משפט 1.1.8 ()*() יהי K שדה. תת־קבוצה $F \subseteq K$ היא שדה אם היא סגורה לחיבור ולכפל, לנגדי ולהפכי.

תרגיל 1.1.9 (*) הוכח ש־ $\{a + b\sqrt{-2} : a, b \in \mathbb{Q}\}$ שדה.

משפט 1.1.10 (־)** אם $D \in \mathbb{Z}$ ו־ $\sqrt{D} \in \mathbb{Q}$, אז $\sqrt{D} \in \mathbb{Q}$.

פתרון. אם $d^2|D$ לאיזשהו $d \in \mathbb{Z}$, אפשר להחליף את D ב־ D/d^2. לפי ההנחה קיים p ראשוני כך ש־ $p|D$ ו־ p^2 אינו מחלק את D. נניח ש־ $\sqrt{D} = \frac{n}{m}$ שבר מצומצם (כלומר $(n,m) = 1$), אז $Dm^2 = n^2$, לכן $p|n^2$ ו־ $n = pn_1$. לאחר הצבה וצמצום מתברר שגם $p|m$, בסתירה להנחה שהשבר מצומצם.

1.1.2 יוצרים של הרחבה

תרגיל 1.1.11 (*+) $F \subseteq K$ הרחבה, $\alpha \in K$, $f(\lambda) \in F[\lambda]$, $\beta = f(\alpha)$. הוכח ש־ $F(\beta) \subseteq F(\alpha)$.

תרגיל 1.1.12 (+)** $\alpha, \beta \in$. הוכח ש־ $(\alpha, \beta) = (\alpha + \beta, \alpha - \beta)$.

תרגיל 1.1.13 (**) $a, b \in F$, ו־ $\sqrt{a} + \sqrt{b} \neq 0$. הוכח: $F(\sqrt{a}, \sqrt{b}) = F(\sqrt{a} + \sqrt{b})$.
הדרכה. $\sqrt{a} - \sqrt{b} = \frac{a-b}{\sqrt{a}+\sqrt{b}} \in F[\sqrt{a} + \sqrt{b}]$.

תרגיל 1.1.14 (+)** מצא $\alpha \in \mathbb{C}$ כך ש־ $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-5}, \sqrt{3})$.

תרגיל 1.1.15 (**) מצא $\alpha \in \mathbb{C}$ כך ש־ $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{-1})$.

תרגיל 1.1.16 (**) הראה ש־ $\mathbb{Q}\left(\sqrt{\frac{3+\sqrt{-7}}{2}}, \sqrt{\frac{3-\sqrt{-7}}{2}}\right) \neq \mathbb{Q}\left(\sqrt{\frac{3+\sqrt{-7}}{2}} + \sqrt{\frac{3-\sqrt{-7}}{2}}\right)$

תרגיל 1.1.17 (**) הוכח ש־ $(2^{1/3}-1)^{1/3} = (1/9)^{1/3} - (2/9)^{1/3} + (4/9)^{1/3}$. הדרכה: סמן $a = 2^{1/3}$ והכפל ב־ $a + 1$.

תרגיל 1.1.18 (**) $\alpha, \beta \in \mathbb{Q}$, ו־ $f(\lambda) = (\lambda - \alpha)(\lambda - \beta) \in \mathbb{Q}(\lambda)$. הוכח ש־ $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

1.2 חוגי פולינומים

יהי F שדה. על חוג הפולינומים מעל F מוגדרת פונקצית מעלה, $\deg(a_n\lambda^n + \ldots + a_0) = n$ אם $a_n \neq 0$.

תרגיל 1.2.1 (*) אם $0 \neq f, g \in F[\lambda]$, אז $\deg(fg) = \deg(f) + \deg(g)$.

משפט 1.2.2 (**) חוג הפולינומים עם הפונקציה $\deg$ הוא חוג אוקלידי.

תרגיל 1.2.3 **(**)** מצא את המנה והשארית בחלוקת $4\lambda^3+\lambda-6$ ב־ $3\lambda^2+1$ מעל $\mathbb{Q}$.

מסקנה 1.2.4 פולינום f ראשוני $(f|gh \to f|g \gg f|h)$ אם ורק אם הוא איפריק $(f=gh\to \deg(g)\cdot\deg(h)=0)$.

מסקנה 1.2.5 כל פולינום אפשר לכתוב כמכפלה של פולינומים איפריקים בדרך יחידה (עד כדי סדר).

מסקנה 1.2.6 כל אידיאל בחוג הפולינומים הוא ראשי (כלומר, נוצר על־ידי איבר אחד).

תרגיל 1.2.7 **(**)** יהיו $f,g\in F[\lambda]$ פולינומים. h הוא ה מחלק המשותף המקסימלי של f,g אם מתקיים אחד מבין התנאים להלן. הוכח שכולם שקולים.

א. $\langle h\rangle=\langle f,g\rangle$.

ב. h הוא הפולינום ממעלה מינימלית באידיאל $\langle f,g\rangle$.

ג. $h|f,h|g$, ולכל פולינום k, אם $k|f,k|g$ אז $k|h$.

תרגיל 1.2.8 **(**)** מצא את המחלק המשותף המקסימלי של $f(\lambda)=\lambda^3-2\lambda^2$ ושל $g(\lambda)=\lambda^3+3\lambda^2-4\lambda-12$ (כלומר ־ מצא $h\in\mathbb{Q}[\lambda]$ כך ש־ $\langle h\rangle=\langle f,g\rangle$).

תרגיל 1.2.9 **(**)** יהיו $F\subseteq K$, $f,g\in F[\lambda]$. נניח שהמחלק המשותף המקסימלי של f,g בחוג $F[\lambda]$ הוא $h\in F[\lambda]$. הוכח שהמחלק המשותף המקסימלי של f,g בחוג $K[\lambda]$ גם הוא h.

1.2.1 חוגי מנה

יהי $f(\lambda)\in F[\lambda]$ פולינום ממעלה $n=deg(f)$. חוג המנה הוא $F[\lambda]/\langle f\rangle$.

נסמן ב־ $\alpha=\lambda+\langle f\rangle$ את ההיטל של λ תחת ההיטל הטבעי $F[\lambda]\to F[\lambda]/\langle f\rangle$.

טענה ([2]). $F[\lambda]/\langle f\rangle$ הוא מרחב וקטורי מעל F, עם בסיס $\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$.

תרגיל 1.2.10 **(**)** מצא בסיס $v_0,\dots,v_3$ ל־ $F[\lambda]/\langle\lambda^4-2\lambda^2+1\rangle$ מעל F. הצג כל מכפלה v_iv_j כצירוף ליניארי של אברי הבסיס.

משפט 1.2.11 **()**(** יהי R חוג קומוטטיבי עם אידיאל I. R/I שדה אם ורק אם I אידיאל מקסימלי.

משפט ([2]). יהיו $f\in F[\lambda]$, $R=F[\lambda]/\langle f\rangle$. התנאים הבאים שקולים:

א. R שדה.

ב. R תחום שלמות.

ג. $\langle f\rangle$ אידיאל מקסימלי.

ד. f פולינום איפריק (כלומר: $f=gh\Rightarrow \deg g)\cdot\deg(h)=0$).

ה. f פולינום ראשוני (כלומר: אם $f|gh$ ו־ $1\in\langle f,g\rangle$, אז $f|h$).

תרגיל 1.2.12 (**) א. מצא את המחלק המשותף המקסימלי של $f(\lambda)=\lambda^5-5\lambda^4+5\lambda^3-25\lambda^2+4\lambda-20$ ושל $g(\lambda)=\lambda^6-6\lambda^5+5\lambda^4-16\lambda^2+96\lambda-80$ מעל $\mathbb{Q}[\lambda]$.

ב. מהו המימד של $R/\langle h(\lambda)\rangle$ מעל ?

ג. מצא בסיס $v_1,\ldots,v_?$ לחוג המנה, וכתוב את נוסחאות הכפל ($v_iv_j=\alpha_{ij}^1v_1+\ldots+\alpha_{ij}^?v_?\equiv$).

1.3 שדות כמרחבים וקטוריים

תהי $F\subseteq K$ הרחבה של שדות.

תרגיל 1.3.1 (*) K הוא מרחב וקטורי מעל F, כאשר המכפלה הסקלרית היא הכפל של K.

יהיו $F\subseteq K$ שדות, $\alpha\in K$. מגדירים $F[\alpha]=a_0+a_1\alpha+\ldots+a_n\alpha^n : a_i\in F$.

תרגיל 1.3.2 (*) $F[\alpha]$ הוא תת־חוג של K וגם תת־מרחב של K.

הגדרה 1.3.3 איבר $\alpha\in K$ נקרא אלגברי מעל F אם קיים $f(\lambda)\in F[\lambda]$ כך ש־ $f(\alpha)=0$.

תרגיל 1.3.4 (*) $\alpha\in K$ אלגברי אם ורק אם $F[\alpha]$ ממימד סופי מעל F. המימד הוא המעלה של α.

משפט 1.3.5 אם α אלגברי, אז $F(\alpha)=F[\alpha]$. במלים אחרות ־ $F[\alpha]$ שדה.

להוכחת המשפט ־ ראה סוף סעיף 1.4.

1.3.1 בסיס של הרחבה

משפט ([2]). אם $\alpha\in K$ אלגברי ממעלה n, אז $1,\alpha,\ldots,\alpha^{n-1}$ בסיס ל־ $F[\alpha]$ מעל F.

דוגמא. הבסיס של $\mathbb{Q}[\sqrt{-1}]$ מעל הוא $1,\sqrt{-1}$.

תרגיל 1.3.6 (+*)** מצא בסיס ל־ $\mathbb{Q}[\sqrt{-1},\sqrt{7}]$ מעל $\mathbb{Q}[\sqrt{7}]$.

תרגיל 1.3.7 (+*)** הבע את $\frac{1}{a+b\sqrt{D}}$ כצירוף ליניארי רציונלי של $1,\sqrt{D}$.

תרגיל 1.3.8 (־)** $\mathbb{Q}[\sqrt{3},\sqrt{5}]$ הוא שדה, עם בסיס $1,\sqrt{3},\sqrt{5},\sqrt{15}$ מעל . תן נוסחה מפורשת לחישוב $\frac{1}{a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}}$ כצירוף ליניארי של אברי הבסיס.

תרגיל 1.3.9 (**) $\alpha\in$ מקיים את המשוואה $\alpha^3+2\alpha+2=0$. חשב את $\frac{1}{\alpha^2+1}$ כצירוף ליניארי (מעל) של $1,\alpha,\alpha^2$.

תרגיל 1.3.10 (***) הוכח ש־ $\sqrt{2}\in[\sqrt{2}+2^{1/3}]$.

הדרכה. סמן $a=\sqrt{2},b=\sqrt[3]{2}$, והצג את $(a+b)^i$, $i=0,\ldots,5$, כצירופים ליניאריים של $1,a,b,ab,b^2,ab^2$. מצא את הצירוף השווה ל־ a.

1.3.2 מימד של הרחבה

המימד של ההרחבה הוא המימד של K כמרחב וקטורי מעל F. את המימד מסמנים ב־ $[K:F]$.

תרגיל 1.3.11 (**) הוכח ש־ $[\mathbb{R}:\mathbb{Q}]=\aleph=|\mathbb{R}|$.

משפט 1.3.12 (***־) יהיו $F\subseteq L$ שדות, K מרחב וקטורי מעל L. הוכח ש־ $\dim_F K=[L:F]\cdot\dim_L K$. הדרכה. אם b_j בסיס ל־ K/L ו־ a_i בסיס ל־ L/F, אז a_ib_j בסיס ל־ K/F.

תרגיל 1.3.13 (**) נניח $F\subseteq L_1,L_2\subseteq K$, $n_i=[L_i:F]$. אם n_1,n_2 זרים זה לזה, אז n_1n_2 מחלק את $[K:F]$.

תרגיל 1.3.14 (**) חשב את $[\mathbb{Q}[\sqrt{-1}]:\mathbb{Q}]$ ואת $[\mathbb{Q}[\sqrt[3]{27}]:\mathbb{Q}]$.

תרגיל 1.3.15 (**־) נסמן $\alpha=2^{1/3}$. הוכח ש־ $[\mathbb{Q}[\alpha]:\mathbb{Q}]=3$.
הדרכה. נראה ש־ $1,\alpha,\alpha^2$ בלתי תלויים מעל . אם $a+b\alpha+c\alpha^2=0$, הכפל במכנה משותף כדי לקבל $a,b,c\in\mathbb{Q}$ זרים. הוכח ש־ $a^3+2b^3+4c^3=6abc$ וכעת הראה ש־ a,b,c זוגיים, בסתירה.

1.3.3 סיפוח שורשים ריבועיים ל־ $\mathbb{Q}$

תרגיל 1.3.16 (**) נסמן $i=\sqrt{-1}$. קבע האם $\mathbb{Q}[\sqrt{1+i}]=\mathbb{Q}[\sqrt{1-i}]$.

תרגיל 1.3.17 (**־) הוכח ש־ $[\mathbb{Q}[\sqrt{6},\sqrt{14}]:\mathbb{Q}]=4$. פתרון. מספיק להוכיח ש־ $\mathbb{Q}[\sqrt{6},\sqrt{14}]\supset\mathbb{Q}[\sqrt{6}]$, משום שהממדים הם ≥ 2 בשתי ההרחבות. את ההכלה $\mathbb{Q}[\sqrt{6}]$ כבר הוכחנו. נניח ש־$\sqrt{14}\in\mathbb{Q}[\sqrt{6}]$, אז אפשר לכתוב $\sqrt{14}=a+b\sqrt{6}$ ($a,b\in$), ו־ $14=a^2+2ab\sqrt{6}+6b^2$. מכיוון ש־ $\sqrt{6}\in$, $ab=0$. לכן $\sqrt{14}\in\mathbb{Q}$ או $\sqrt{\frac{14}{6}}=\frac{1}{3}\sqrt{21}\in\mathbb{Q}$.

תרגיל 1.3.18 (***) יהיו $a_1,a_2,\dots,a_n\in\mathbb{Z}$ מספרים זרים בזוגות. הוכח ש־

$$[\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_n}]:\mathbb{Q}]=2^n$$

(*O.T. O'Meara, Introduction to Quadratic Forms, 65:16*).
הדרכה. באינדוקציה. התבונן ב־ $K=[\sqrt{a_1},\dots,\sqrt{a_{n-2}}]$. לפי ההנחה $K[\sqrt{a_{n-1}}]\supset K$ וגם $K[\sqrt{a_n}]\supset K$. המימדים בשתי ההכלות הם 2, ואם $[K[\sqrt{a_{n-1}},\sqrt{a_n}]:K]<4$, אז $K[\sqrt{a_{n-1}}]=K[\sqrt{a_n}]$.

כדי לנסח את התוצאה הכללית, נסמן $\Omega=\{-1,2,3,5,7,11,13,17,\dots\}$.

תרגיל 1.3.19 (**) $\mathbb{P}(\Omega)$ חבורה ביחס לפעולה $A\Delta B = A\cup B - A\cap B$, ו־ $A\Delta A = \phi$. לכן $\mathbb{P}(\Omega)$ מרחב וקטורי מעל $\mathbb{Z}_2$ (כאשר הכפל בסקלר הוא $1\cdot A = A$, $0\cdot A = \phi$).

תרגיל 1.3.20 (***) נגדיר $\Phi :\to \mathbb{P}(\Omega)$ לפי הפירוק לראשוניים, עם סימן. למשל, $\Phi(-30) = -1,2,3,5$, $\Phi(4) = \phi$, $\Phi(8) = 2$. אז $[\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_n}] : \mathbb{Q}] = 2^e$, כאשר $e = \dim span_{\mathbb{Z}_2}\Phi(a_1),\ldots,\Phi(a_n)$.

דוגמא. נתבונן ב־ $K = [\sqrt{-30},\sqrt{420},\sqrt{-14},\sqrt{40},\sqrt{-84}]$:

$$span\{\{-1,2,3,5\},\{3,5,7\},\{-1,2,7\},\{2,5\},\{-1,3,7\}\} = span\{\{-1,5\},\{3,5\},\{2,5\},\{7\}\}$$

ולכן $K = [\sqrt{-5},\sqrt{15},\sqrt{10},\sqrt{7}]$, ממימד 2^4 מעל $\mathbb{Q}$.

תרגיל 1.3.21 (**) הוכח ש־ $\sqrt{6+2\sqrt{-3}} + \sqrt{6-2\sqrt{-3}} = 2\sqrt{3+2\sqrt{3}}$.

1.4 פולינום מינימלי

1.4.1 תכונות של הפולינום המינימלי

יהיו $F \subseteq K$ הרחבת שדות, $\alpha \in K$.

נסמן ב־ φ_α את פונקצית ההצבה $\lambda \mapsto \alpha, \varphi_\alpha : F[\lambda] \to K$, המוגדרת לפי $\varphi_\alpha(f) = f(\alpha)$.

תרגיל 1.4.1 (**) $\varphi_\alpha : F[\lambda] \to K$ הומומורפיזם של חוגים.

תרגיל 1.4.2 (*) $f \in Ker(\varphi_\alpha)$ אם ורק אם $f(\alpha) = 0$.

תרגיל 1.4.3 (*) אוסף הפולינומים $I = f(\lambda) \in F[\lambda] : f(\alpha) = 0$ הוא אידיאל בחוג $F[\lambda]$.

משפט 1.4.4 (*־)** יהי $f(\lambda) \in F[\lambda]$ פולינום, המקיים $f(\alpha) = 0$. התכונות הבאות שקולות.

א. f הוא היוצר של $Ker(\varphi_\alpha)$.
ב. f פולינום איפריק.
ג. אם $g(\alpha) = 0$, $g \in F[\lambda]$, אז $\deg(f) \leq \deg(g)$.
ד. אם $g(\alpha) = 0$, $g \in F[\lambda]$, אז $f|g$.
ה. $[F[\alpha] : F] = deg(f)$.

הפולינום בעל תכונות אלה נקרא הפולינום המינימלי של α.

סיכום שימושי. פולינום f הוא הפולינום המינימלי של $\alpha \in K$ מעל F אם ורק אם
א. $f \in F[\lambda]$, וגם
ב. $f(\alpha) = 0$, וגם
ג. f איפריק; או ־ $def(f) = [F[\alpha] : F]$.

דרכים להראות שפולינום מעל $\mathbb{Q}$ או מעל $\mathbb{Z}_p$ הוא איפריק נלמד בפרק הבא.

תרגיל 1.4.5 (*) יהי $\alpha \in F$. מצא את הפולינום המינימלי של α מעל F.

1.4.2 חישוב הפולינום המינימלי

תרגיל 1.4.6 (*) מצא את הפולינום המינימלי של $\sqrt{2}$ מעל $\mathbb{Q}$.

תרגיל 1.4.7 (**) מצא את הפולינום המינימלי של $\sqrt{2}+\sqrt{5}$ מעל $\mathbb{Q}$.
פתרון. נרשום $\alpha=\sqrt{2}+\sqrt{5}$. $5=\sqrt{5}^2=(\alpha-\sqrt{2})^2=\alpha^2-2\sqrt{2}\alpha+2$, ולכן $2\sqrt{2}\alpha=\alpha^2-3$. נעלה בריבוע, ונקבל $8\alpha^2=\alpha^4-6\alpha^2+9$, ולכן $f(x)=x^4-14x^2+9$ מאפס את α . הפולינום איפריק מכיוון שהוא ממעלה $[\mathbb{Q}[\alpha]:\mathbb{Q}]=4$.

תרגיל 1.4.8 (**) מצא את הפולינום המינימלי של $\rho_3=e^{\frac{2\pi i}{3}}=\cos\left(\frac{2\pi}{3}\right)+i\cdot\sin(\frac{2\pi}{3})$.
הדרכה. $\rho_3^3=1$.

תרגיל 1.4.9 (**) מצא את הפולינומים המינימליים של $\sqrt{2}+\sqrt{-1}$ ושל $\sqrt{3}+\sqrt{-3}$ מעל .

תרגיל 1.4.10 (**) מצא את הפולינומים המינימליים של $\sqrt{3}+\sqrt{2}$ מעל השדות $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$.

תרגיל 1.4.11 (**) מצא את הפולינום המינימלי של $\sqrt[3]{2}+\sqrt{2}$ מעל $\mathbb{Q}$.

תרגיל 1.4.12 (-*)** מצא פולינום מעל המתאפס ב- $\sqrt{6}+\sqrt{5}+\sqrt{3}$.

תרגיל 1.4.13 (-)** הראה שעבור $a,b\in\mathbb{Q}$, $\lambda=a^{1/3}+b^{1/3}$ מאפס את הפולינום $f(\lambda)=\lambda^9-3(a+b)\lambda^6+3(a^2-7ab+b^2)\lambda^3-(a+b)^3$.

תרגיל 1.4.14 (-*)** הראה ש- $\sqrt[n]{3}+\sqrt{2}$ מאפס פולינום ממעלה $2n$ מעל $\mathbb{Q}$. מצא את הפולינום כש- $n=5$.

תרגיל 1.4.15 (**) מצא פולינום מעל $\mathbb{Q}$ המתאפס ב- $cos(20^\circ)$. הדרכה. נוסחאות דה-מואבר.

תרגיל 1.4.16 (**) מצא פולינום מעל $\mathbb{Q}$ המתאפס ב- $tg(10^\circ)$. הדרכה. העזר בנוסחה $tg(\alpha+\beta)=\frac{tg\alpha+tg\beta}{1-tg\alpha\cdot tg\beta}$.

תרגיל 1.4.17 (**) הפולינום המינימלי של α (מעל $\mathbb{Q}$) הוא $f(\lambda)=\lambda^4-2\lambda^3+4\lambda-6$.
מצא את הפולינום המינימלי של $\beta=2\alpha+1$.

תרגיל 1.4.18 (**) הפולינום המינימלי של α הוא $f(\lambda)=\lambda^3-6\lambda^2+9\lambda+11$.
מצא את הפולינום המינימלי של $\frac{1}{1-\alpha}$.

תרגיל 1.4.19 (***) הפולינום המינימלי של α הוא $f(\lambda)=\lambda^3-6\lambda^2+9\lambda+11$. מצא את הפולינום המינימלי של $\beta=\alpha^2+1$.

1.4.3 מימדים

תרגיל 1.4.20 (**) (משפט). יהיו $F \subseteq L \subseteq K$ שדות, $\alpha \in K$. אז $[L[\alpha] : L] \leq [F[\alpha] : F]$.

תרגיל 1.4.21 (**) יהיו $F \subseteq K$ שדות, $\alpha, \beta \in K$. אז $[F[\alpha, \beta] : F] \leq [F[\alpha] : F] \cdot [F[\beta] : F]$.

תרגיל 1.4.22 (***) (משפט). יהיו $F \subseteq K$ שדות, כאשר $[K : F] < \infty$. תת־קבוצה $F \subseteq L \subseteq K$ היא שדה אם היא סגורה לחיבור, לחיסור ולכפל.

הדרכה. נשאר להראות שכל $0 \neq \alpha \in K$ הפיך. התבונן בפולינום המינימלי של αK.

מסקנה. אם $\alpha \in K$ אלגברי, אז $F[\alpha]$ שדה.

תרגיל 1.4.23 (**) הפולינומים $f(x) = x^5 + 14x^3 - 63x^2 - 105x + 721$ ו־ $g(x) = x^6 - 45x^5 + 120x^3 + 99x^2 + 18x + 36$ שניהם איפריקים מעל $\mathbb{Q}$. יהי $\alpha \in g$. הוכח ש־ $f(x)$ איפריק מעל $\mathbb{Q}[\alpha]$.

תרגיל 1.4.24 (**) תהי K/F הרחבה סופית. יהי $p(x) \in F[x]$ פולינום איפריק כך ש־ $\deg(p)$ אינו מחלק את $[K : F]$. הוכח כי K אינו מכיל שורש של $p(x)$.

פרק 2

פירוק פולינומים

הרחבות של שדות קשורות קשר הדוק לפולינומים אי־פריקים. בפרק זה נלמד לזהות פולינום אי־פריק, ולפרק פולינומים לגורמיהם האיפריקים.

תרגיל 2.0.25 (**) אם $f(\lambda) = g(\lambda) \cdot h(\lambda)$ אז לכל $F \ni a, b \neq 0$, $f(a\lambda + b) = g(a\lambda + b) \cdot h(a\lambda + b)$.
אם $f(a\lambda + b)$ איפריק מעל F אז גם $f(\lambda)$ איפריק.

2.1 שורשים

2.1.1 מספר השורשים של פולינום

תמשפט ([2]). אם $f(\lambda) \in F[\lambda]$ ו־ $a \in F$, אז $f(\lambda) = (\lambda - a)g(\lambda) + f(a)$ לאיזשהו $g(\lambda) \in F[\lambda]$.
משפט ([2]). לפולינום ממעלה n יש לכל היותר n שורשים בשדה F.
משפט ([2]). תת־חבורה סופית כפלית של שדה היא ציקלית.
הדרכה. כל אברי החבורה הם שורשים של הפולינום $\lambda^e - 1$ כאשר $e = exp(G)$.

תרגיל 2.1.1 (*) $(\lambda - a)|(f(\lambda) - f(a))$ (חילוק בחוג הפולינומים) לכל a.

תרגיל 2.1.2 (**) מצא פולינום ממעלה n עם m שורשים בדיוק (בהנחה ש־ $|F| \leq m \leq n$).

תרגיל 2.1.3 (**) יהי $f(\lambda) \in F[\lambda]$. נסמן $(\Delta f)(x, y) = \frac{f(x)-f(y)}{x-y}$ ו־ $(\Delta^2 f)(x, y, z) = ((\Delta f(x, \cdot))(y, z) = \frac{\Delta f(x,y) - \Delta f(x,z)}{y-z}$.
הוכח ש־ $\Delta f(x, y) = \Delta f(y, x)$ ו־ $(\Delta^2 f)(x_1, x_2, x_3) = (\Delta^2 f)(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3})$ לכל $\sigma \in S_3$.

תרגיל 2.1.4 (**) נסמן $f(\lambda) = 2\lambda^3 + \lambda^2$ - 16 + λ. חשב את $(\Delta f)(x,y)$ ואת $(\Delta f)(x,y,z)$.

תרגיל 2.1.5 (***) נגדיר באינדוקציה $\Delta^0 f = f$,

$$(\Delta^n f)(x_1,\ldots,x_{n+1}) = (\Delta^{n-1} f(x_1,\ldots,x_{n-1},\cdot))(x_n,x_{n+1}).$$

הוכח ש- $\Delta^n f$ היא פונקציה סימטרית לחלוטין (כלומר, אינה רגישה להחלפת סדר המשתנים).

תרגיל 2.1.6 (***) הוכח שאם $f(\lambda) = \lambda^m$, אז

$$(\Delta^n f)(x_1,\ldots,x_{n+1}) = \sum i_1 + \ldots + i_{n+1} = m - n x_1^{i_1} \ldots x_{n+1}^{i_{n+1}}$$

עבור $n < m$, $\Delta^m f = 1$, ו- $\Delta^n f = 0$ עבור $m < n$.

משפט 2.1.7 (**) יהי $f(\lambda) \in F[\lambda]$ פולינום ממעלה ≥ 3, ללא שורשים ב- F. הוכח ש- $f(\lambda)$ אי־פריק.

תרגיל 2.1.8 (**) תן דוגמא לפולינום ממעלה 4 שאין לו שורשים ב־$\mathbb{Q}$, והוא פריק.

2.1.2 שורשים רציונליים

יהי $f(\lambda) = \alpha_0 + \alpha_1\lambda + \ldots + \alpha_n\lambda^n \in \mathbb{Q}[\lambda]$ פולינום עם מקדמים שלמים.

משפט 2.1.9 (־)** . אם r/s הוא שורש רציונלי של הפולינום $f(\lambda) = a_n\lambda^n + \cdots + a_0$, כאשר $r/s \in \mathbb{Z}$ ו־r,s זרים, אז $r \mid a_0$ ו- $s \mid a_n$.

תרגיל 2.1.10 (**) במשפט לעיל, אם $a_{n-1} = 0$, אז $s^2 \mid a_n$.

תרגיל 2.1.11 (*) השורשים הרציונליים של פולינום מתוקן עם מקדמים שלמים הם כולם שלמים.

תרגיל 2.1.12 (**) הפולינומים הבאים אי־פריקים מעל :

א. $\lambda^3 - \lambda^2 + \lambda + 2$.

ב. $\lambda^2 + 3\lambda - 2$.

ג. $3\lambda^2$ - 12 + λ.

תרגיל 2.1.13 (*) ל- $\lambda^{13} - \lambda^7 + 14\lambda^2 - 7$ אין שורשים רציונליים.

תרגיל 2.1.14 (**) מצא את השורשים הרציונליים של $f(\lambda) = \lambda^4 - 24\lambda^2 + 76\lambda + 24$.

תרגיל 2.1.15 (***) מצא את השורשים הרציונליים של $g(\lambda) = 6\lambda^4 + 89\lambda^3 + 96\lambda^2 - 31\lambda - 20$.

פתרון. אם r/s שורש אז $r|20, s|6$ ולכן $\frac{\pm r}{s} \in \left\{\frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, 1, \frac{4}{3}, \frac{5}{3}, 2, \frac{5}{2}, \frac{10}{3}, 4, 5, \frac{20}{3}, 10, 20\right\}$. לאחר כמה נסיונות הצבה מגלים ש־ $f(-15) > 0 > f(-10), f(-1) > 0 > f(0) > 0 > f(-2), f(1) > 0 > f(0)$, ולכן יש פתרונות (ממשיים) בקטעים $(0, 1)$, $(-2, -1)$, $(-15, -10)$. כעת קל לאתר את השורשים $\lambda = \frac{1}{2}$, $\lambda = -\frac{4}{3}$, ולחשב את הפולינום הנותר, $\frac{f(\lambda)}{(\lambda-1/2)(\lambda+4/3)} = \lambda^2 + 14\lambda + 5$, שלו אין שורשים רציונליים.

תרגיל 2.1.16 (***) מצא את השורשים הרציונליים של הפולינום $432\lambda^5 - 396\lambda^4 - 114\lambda^3 + 114\lambda^2 - 31\lambda + 30$.

תרגיל 2.1.17 (***) מצא לפחות שורש אחד של הפולינום $\lambda^{12} + 2\lambda^{10} + \lambda^2 + 2$.

רמז. השורש אינו רציונלי.

2.2 שיטות כלליות לפירוק

תרגיל 2.2.1 (**) פרק לגורמים אי־פריקים מעל את הפולינומים $\lambda^6 - 1$ ו־ λ^4 ־1656.

תרגיל 2.2.2 (**) לפולינום $\lambda^2 - q$ אין שורש בשדה $\mathbb{Q}[\sqrt{p}]$ (כאשר p, q ראשוניים שונים).

2.2.1 הקריטריון של אייזנשטיין

משפט [3]. יהי $f(\lambda) = a_n\lambda^n + \ldots + a_0 \in [\lambda]$. אם $p|a_0, \ldots, a_{n-1}$, p^2 אינו מחלק את a_0 ו־ p אינו מחלק את a_n, אז $f(\lambda)$ איפריק מעל . פולינום כזה נקרא פולינום אייזנשטיין.

תרגיל 2.2.3 (*) הפולינומים הבאים אי־פריקים מעל :

א. $\lambda^{103} - 150\lambda^{79} + 15\lambda^{52} - 72\lambda + 6$.

ב. $\lambda^4 + 2\lambda^2 + 6$.

תרגיל 2.2.4 (**) $\lambda^4 + 2\lambda + 2$ איפריק מעל, אבל פריק מעל $\mathbb{Q}[i]$.

תרגיל 2.2.5 (+*)** האם יתכן $\mathbb{Q}[\sqrt[3]{q}] \subseteq \mathbb{Q}[\sqrt{p}]$ כאשר p, q ראשוניים ?

הצבות

פולינום החשוד באיפריקות יכול להפוך לפולינום אייזנשטיין אחרי הצבה לינארית $\lambda \mapsto a\lambda + b$. נראה שמספיק לבדוק את ההצבות $\lambda \mapsto \lambda + b$:

תרגיל 2.2.6 (־)** יהי $a \in$. אם $f(a\lambda + b)$ פולינום אייזנשטיין עבור ראשוני p, אז a זר ל־ p, וגם $f(\lambda + b)$ הוא פולינום אייזנשטיין.

תרגיל 2.2.7 (**) יהיו $b_1, b_2 \in$. אם $f(\lambda + b_1)$ פולינום אייזנשטיין עבור ראשוני p ו־ $b_1 \equiv b_2$ (dom p), אז גם $f(\lambda + b_2)$ הוא פולינום אייזנשטיין.

תרגיל 2.2.8 (**) הוכח ש־

א. $\frac{\lambda^p - 1}{\lambda - 1} = \lambda^{p-1} + \ldots + \lambda + 1$ איפריק מעל (הדרכה: הצב $\lambda = \mu + 1$).

ב. $\lambda^{p-1} - \lambda^{p-2} + \lambda^{p-3}$ ־+...+1 איפריק מעל .

תרגיל 2.2.9 (**) הוכח, בעזרת הצבה ליניארית, ש־ $f(\lambda) = \lambda^4 - 12\lambda^3 + 47\lambda^2 - 80\lambda +$ 88 איפריק מעל .

פתרון. נחשב $f(\lambda + b) = \lambda^4 + (4b - 12)\lambda^3 + (6b^2 - 36b + 47)\lambda^2 + (4b^3 - 36b^2 + 94b - 80)\lambda + f(b)$. כדי לעמוד בתנאי הקריטריון המקדמים צריכים להתחלק ב־ p. המקדם של λ^2 איזוגי, ולכן $p \neq 2$. p מחלק את $4b - 12$, ולכן $b \equiv 3(mod p)$. אפשר להציב במקדם של λ^2, ולקבל

$$-7 \equiv 6 \cdot 3^3 - 36 \cdot 3 + 47 \equiv 6b^2 - 36b + 47 \equiv 0 \pmod p$$

כלומר, $p = 7$. כעת אפשר לבחור $b = 3$, ולהציב: $f(\lambda+3) = \lambda^4 - 7\lambda^2 - 14\lambda + 28$, שהוא אכן פולינום אייזנשטיין.

תרגיל 2.2.10 (***) הוכח, בעזרת הצבה ליניארית, ש־ $f(\lambda) = \lambda^4 - 38\lambda^3 + 349\lambda^2 - 1224\lambda + 1521$ איפריק מעל .

השורש השלישי והשורש החמישי של 1

נסמן $\rho_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \cdot sin\left(\frac{2\pi}{n}\right)$. כמובן, $(\rho_n)^n = 1$.

תרגיל 2.2.11 (+*)** א. מצא את הפולינום המינימלי של ρ_3 מעל $\mathbb{Q}$. הוכח ש־ $[\mathbb{Q}[\rho_3] : \mathbb{Q}] = 2$.

ב. חשב את $\cos(\frac{2\pi}{3})$ ואת $\sin(\frac{2\pi}{3})$.

תרגיל 2.2.12 (־)** א. מצא את הפולינום המינימלי של ρ_5 מעל $\mathbb{Q}$.

ב. מצא את הפולינום המינימלי של $\rho_5 + \rho_5^{-1} = 2 \cdot \cos\left(\frac{2\pi}{5}\right)$ מעל $\mathbb{Q}$.

ג. מצא את הפולינום המינימלי של ρ_5 מעל $\mathbb{Q}[\rho_5 + \rho_5^{-1}]$.

תרגיל 2.2.13 (**) הוכח ש־ $\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$, ו־ $\sin\left(\frac{2\pi}{5}\right) = \sqrt{\frac{5+\sqrt{5}}{8}}$.

תרגיל 2.2.14 (**) חשב את $[\mathbb{Q}[\cos\frac{2\pi}{5}] : \mathbb{Q}]$, את $[\mathbb{Q}[\sin\frac{2\pi}{5}] : \mathbb{Q}]$, ואת $[\mathbb{Q}[\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5}] : \mathbb{Q}]$.

2.2.2 השלמה לריבוע

תרגיל 2.2.15 (*) אם $f(\lambda) = g(\lambda)^2 - h(\lambda)^2$, כאשר $\deg(g) \neq \deg(h)$, אז f פריק.

תרגיל 2.2.16 (**) פרק לגורמים מעל את $\lambda^4 + 6\lambda^2 + 25$.
פתרון. אפשר לכתוב $\lambda^4 + \lambda^2 + 25 = (\lambda^2 + 5)^2 - (2\lambda)^2$, ולכן $\lambda^4 + \lambda^2 + 25 = (\lambda^2 + 2\lambda + 5)(\lambda^2 - 2\lambda + 5)$.

נתבונן בפולינום $f(\lambda) = \lambda^4 - A\lambda^2 + B$ כאשר $A, B \in \mathbb{Z}$.

תרגיל 2.2.17 (**) אם $f(d) = 0$ (כאשר $d \in$) אז d שלם ו־ $d^2|B$. אם $0 < B$, אז $2\sqrt{B} < A \leq B + 1$.

תרגיל 2.2.18 (**) אם $\Delta = A^2 - 4B$ הוא ריבוע ב־, אז $f(\lambda)$ פריק.

תרגיל 2.2.19 (**) נניח שאין ל־ $f(\lambda)$ שורשים. אז $f(\lambda)$ פריק אם ורק אם קיימים $a, b \in$ כך ש־ $B = b^2$, $A = a^2 - 2b$. שים לב שבמקרה זה $a^2 = \frac{A^2-4B}{a^2-4b}$.

תרגיל 2.2.20 (**) מצא דוגמא לפולינום אי־פריק $f(\lambda)$ ממעלה 2 כך ש־ $f(\lambda^2)$ פריק (מעל).

תרגיל 2.2.21 (**) הוכח ש־ $\lambda^4 + 3\lambda^2 + 9$ הוא אי־פריק מעל.

תרגיל 2.2.22 (-*)** פרק לגורמים אי־פריקים מעל את $\lambda^6 + 27$.
הדרכה. $(\lambda^2 + 3)|(\lambda^6 + 27)$.

תרגיל 2.2.23 (-*)** פרק את $\lambda^4 + 1$ לגורמים ממעלה 2 מעל $\mathbb{Q}[\sqrt{2}]$.

תרגיל 2.2.24 (-*)** פרק את $\lambda^4 - \lambda^2 + 9$ לגורמים ממעלה 2 מעל $\mathbb{Q}[\sqrt{7}]$.

תרגיל 2.2.25 (***) פרק לגורמים אי־פריקים מעל את $\lambda^6 + 5\lambda^4 + 18\lambda + 9$.

2.2.3 פירוק לפי שורשים

נניח שלפולינום $f \in F[\lambda]$, ממעלה n, יש n שורשים $\alpha_1, \dots, \alpha_n \in K$, כאשר $F \subseteq K$. (בדרך כלל $K = \mathbb{Q}$). הפירוק של f מעל K הוא $f(\lambda) = (\lambda - \alpha_1) \dots (\lambda - \alpha_n)$.

תרגיל 2.2.26 (**) f פריק מעל F אם ורק אם קיימת תת־קבוצה $i_1, \dots, i_t$ של אינדקסים, כך ש־ $(\lambda - \alpha_{i_1}) \dots (\lambda - \alpha_{i_t}) \in F[\lambda]$.

תרגיל 2.2.27 (**) אם $\deg(f) = 4$ ואין ל־ f שורשים ב־ F, אז f פריק מעל F אם ורק אם קיימים שני שורשים α, β של f כך ש־ $\alpha + \beta, \alpha\beta \in F$.

תרגיל 2.2.28 **(***)** פרק לגורמים איפריקים מעל את $f(\lambda)=\lambda^{10}-1024$. פתרון. נסמן $\rho=\rho_{10}=e^{\frac{2\pi i}{10}}$. השורשים של $f(\lambda)$ הם $2\rho^k$, $k=0,\dots,9$.

אפשר לפרק $f(\lambda)=(\lambda-2)(\lambda+2)(\lambda^4+2\lambda^3+4\lambda^2+8\lambda+16)(\lambda^4-2\lambda^3\pm\ldots+16)$, והשורשים של הגורמים ממעלה 4 הם $2\rho^{1,3,7,9}, 2\rho^{2,4,6,8}$. אין להם שורש רציונלי, ולכן הפירוק היחיד האפשרי הוא לפולינומים ממעלה 2. אבל אם $(\lambda-2\rho^j)(\lambda-2\rho^k)\in[\lambda]$ אז $\rho^{j+k}\in$ (המקדם החופשי), ולכן $j+k\equiv 0(mod5)$. בנוסף דרוש $\rho^j+\rho^k\in$. מפירוק שני הפולינומים נובע $\frac{\sqrt{5}-1}{2=\rho^2+\rho^{-2}\in}$, סתירה.

תרגיל 2.2.29 **(-**)** הוכח, לפי שורשים, שהפולינום $\frac{x^4+x^3+x^2+x+1=x^5-1}{x-1}$ איפריק מעל .

תרגיל 2.2.30 **(***)** פרק לגורמים איפריקים מעל את $x^{12}-1$.

תרגיל 2.2.31 **(-**)** מצא את הפולינום המינימלי של ρ_{12} מעל $\mathbb{Q}$, מעל $\mathbb{Q}[\rho_6]$, ומעל $\mathbb{Q}[\rho_4]=\mathbb{Q}[i]$.

תרגיל 2.2.32 **(**)** הוכח ש-$x=\sqrt{a}+\sqrt{b}$ הוא שורש של $f(\lambda)=\lambda^4-2(a+b)\lambda^2+(a-b)^2$. מצא את כל שאר השורשים.

תרגיל 2.2.33 **(**)** $\lambda^4-42\lambda^2+46$ איפריק מעל $\mathbb{Q}[\sqrt{5}]$ אבל פריק מעל $\mathbb{Q}[\sqrt{10}]$.

תרגיל 2.2.34 **(**)** $\lambda^4+2\lambda+25$ איפריק מעל $K=[\sqrt{-1},\sqrt{5}]$.

תרגיל 2.2.35 **(***)** פרק, מעל $\mathbb{Q}[\sqrt{3}]$, את הפולינום λ^6-72.

תרגיל 2.2.36 **(-***)** פרק, בחוג $[a,b,c]$ את הפולינום $f(a,b,c)=a^4+b^4+c^4-2(a^2b^2+b^2c^2+c^2a^2)$ לגורמים איפריקים.

2.3 פולינומים מעל $\mathbb{Z}_p$

תרגיל 2.3.1 **(*)** $\mathbb{Z}_n$ הוא שדה אם ורק אם n ראשוני.

2.3.1 שורשים מעל $\mathbb{Z}_p$

תרגיל 2.3.2 **(**)** נ ניח ש- $d|(p-1)$. $a\in\mathbb{Z}_p$ הוא חזקת-d אם ורק אם $a^{\frac{p-1}{d}}\equiv 1(modp)$.

משפט (2). $a\in\mathbb{Z}_p$ הוא חזקת-k אם ורק אם $a^{\frac{p-1}{(k,p-1)}}\equiv 1(modp)$.

תרגיל 2.3.3 **(**)** ה ראה שלפולינום λ^6-7 אין שורשים ב- $_{193}$.

תרגיל 2.3.4 **(-**)** פ רק את הפולינום λ^6-7 לגורמים איפריקים מעל $\mathbb{Z}_{193}$.

תרגיל 2.3.5 **(*)** הוכח ש־
א. $\lambda^2+\lambda+1$ איפריק מעל $\mathbb{Z}_2$.
ב. λ^2 +1 איפריק מעל $_7$.

תרגיל 2.3.6 **(**)** פרק לגורמים איפריקים את λ^3+2 ואת $\lambda^2+\lambda-1$ מעל $\mathbb{Z}_3$.

תרגיל 2.3.7 **(**)** פרק לגורמים איפריקים את λ^3 +2 ואת $\lambda^2+\lambda-1$ מעל $\mathbb{Z}_7$.

תרגיל 2.3.8 **(**)** א. λ^3 -9 איפריק מעל $\mathbb{Z}_{31}$
ב. פרק את λ^3 -9 מעל $\mathbb{Z}_{11}$.

2.3.2 פירוק פולינומים מעל $\mathbb{Z}_p$

תרגיל 2.3.9 **(*)** רשום את כל הפולינומים ממעלה ≤ 2 מעל $\mathbb{Z}_3$.

תרגיל 2.3.10 **(**)** רשום את כל הפולינומים האיפריקים ממעלה ≤ 4 מעל $\mathbb{Z}_2$.

תרגיל 2.3.11 **(**)** פרק לגורמים איפריקים מעל $\mathbb{Z}_2$ את הפולינומים $\lambda^8+\lambda^6+\lambda^2$ +1, $\lambda^8+\lambda+1$.

תרגיל 2.3.12 **(**)** פרק לגורמים איפריקים מעל $\mathbb{Z}_5$ את $\lambda^5-\lambda+a$, לכל $a\in\mathbb{Z}_5$.

לנושא זה נחזור במשנה מרץ בפרק 8 (העוסק בשדות סופיים).

2.3.3 פולינומים מעל $\mathbb{C}$

הלמה של גאוס ([3]). נניח ש־ $f(\lambda)\in[\lambda]$ ואין למקדמים של f מחלק משותף > 1.
אם f איפריק בחוג $[\lambda]$ u אז הוא איפריק גם בחוג $[\lambda]$.
עבור ראשוני p קבוע, ההטלה $\to_p$ מסומנת $a\mapsto a$. אם $f(\lambda)=a_n\lambda^n+\ldots+a_0\in$ $[\lambda]$, אז $f(\lambda)=a_n\lambda^n+\ldots+a_0$ פולינום מעל $\mathbb{Z}_p$.

תרגיל 2.3.13 **(*)** $\deg(f)=deg(f)$ אם ורק אם המקדם העליון של f זר ל־ p.
משפט ([2]). אם המקדם העליון של $f(\lambda)\in[\lambda]$ זר ל־ p, ו־ $f(\lambda)$ איפריק מעל $\mathbb{Z}_p$, אז $f(\lambda)$ איפריק מעל $\mathbb{Q}$.

תרגיל 2.3.14 **(**)** הוכח ש־ $\lambda^6+3\lambda^4-\lambda-4$ איפריק מעל .

תרגיל 2.3.15 **(***)** הוכח ש־ $f(\lambda)=\lambda^5+462\lambda^3+243\lambda-691$ איפריק מעל .

2.4 משוואות ממעלה 3 ו־ 4

2.4.1 הצבות ליניאריות

בסעיף זה נאמר ששני פולינומים $f, g \in F[\lambda]$ שקולים אם $g(\lambda) = f(a\lambda + b)$ לאיזשהם $a, b \in F$, $a \neq 0$.

תרגיל 2.4.1 (*) היחס שהוגדר להלן הוא יחס שקילות.

טענה (^{2}). אם $f(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0$, אז המקדם של λ^{n-1} ב־ $f(\lambda - \frac{a_{n-1}}{na_n})$ הוא 0.

תרגיל 2.4.2 (*) מצא פולינום שקול ל־ $f(\lambda) = 2\lambda^3 - 9\lambda^2 + 14\lambda + 4$ שבו המקדם של λ^2 הוא אפס.

תרגיל 2.4.3 (**) $\lambda = 6$ הוא פתרון למשוואה $\lambda^3 - 14\lambda - 132 = 0$.

א. מצא פתרון למשוואה $z^3 - 9z^2 - 29z - 915 = 0$.

ב. מצא את שאר הפתרונות.

2.4.2 משוואה ממעלה 3 (del Ferro, 1515)

תהי $x^3 - bx - c = 0$ משוואה בנעלם x, מעל שדה ממאפיין $\neq 2, 3$.

נכתוב $x = \alpha + \beta$, כאשר $\alpha\beta = \frac{b}{3}$ לפי בחירה.

$$\{ \alpha^3 + \beta^3 = x^3 - 3\alpha\beta x = (b - 3\alpha\beta)x + c = c\alpha^3\beta^3 = \frac{b}{3}^3 = \frac{1}{27}b^3 \rightarrow (z-\alpha^3)(z-\beta^3) = z^2 - cz + \frac{1}{27}b^3$$

מן המשוואה הריבועית אפשר למצוא את α^3, β^3, ומהם את α, β ואת x.

תרגיל 2.4.4 (*) לכל אחד מהפרמטרים α, β יש שלושה ערכים אפשריים. מדוע אין למשוואה תשעה פתרונות?

תרגיל 2.4.5 (**) פתור את המשוואה $16x^3$ ־24x^2 ־67x־15=0.

תרגיל 2.4.6 (**) פתור את המשוואה x^3 ־3x+1=0. הבע את הפתרונות בצורה $x = 2 \cdot cos(\alpha)$.

2.4.3 משוואה ממעלה 4 (Ferrari, 1545)

תהי $x^4 - bx^2 - cx - d = 0$ משוואה בנעלם x, מעל שדה ממאפיין $\neq 2, 3$.

ננסה לפרק $x^4 + bx^2 + cx + d = (x^2 + \alpha x + \beta)(x^2 - \alpha x + \gamma)$.

מהשוואת מקדמים מתקבל

$$\{ \beta + \gamma = b + \alpha^2 \gamma - \beta = \frac{c}{\alpha} \Rightarrow \beta = \frac{1}{2}\left(b + \alpha^2 - \frac{c}{\alpha} \right), \gamma = \frac{1}{2}\left(b + \alpha^2 + \frac{c}{\alpha} \right).$$

$$d = \beta\gamma = \frac{1}{4}\left(\alpha^4 + 2b\alpha^2 + b^2 - \frac{c^2}{\alpha^2} \right) \Rightarrow \alpha^6 + 2b\alpha^4 + (b^2 - 4d)\alpha^2 - c^2 = 0$$

זוהי משוואה ממעלה 3 בנעלם α^2, ולאחר שמוצאים אותו אפשר לחשב את β, γ ולפתור את שתי המשוואות $x^2 + \alpha x + \beta = 0, x^2 - \alpha x + \gamma = 0$.

תרגיל 2.4.7 (**) תן פתרון כללי למשוואה $x^4 - (6a^2 + b^2)x^2 + 2a(4a^2 - b^2)x + 3a^2(b^2 - a^2)$.

תרגיל 2.4.8 (**) פ תור את המשוואה $x^4 - 391x^2 - 3066x - 2484 = 0$.

תרגיל 2.4.9 (**) פתור את המשוואה $x^4 - 226x^2 + 832x - 451 = 0$.

פרק 3

שדות

3.1 המאפיין של שדה

יהי F שדה. נגדיר הומומורפיזם $\Phi :\to F$ לפי $\Phi(1) = 1_F$. $Ker\Phi$ הוא אידיאל של, ולכן יש לו יוצר, אותו נסמן ב־ $charF$. $charF$ נקרא גם המאפיין של השדה.

תרגיל 3.1.1 (*) $charF$ לעולם ראשוני או 0.

תרגיל 3.1.2 (*) לשני שדות איזומורפיים יש אותו מאפיין.

תרגיל 3.1.3 (**) א. אם $charF = 0$ אז יש ל־ F תת־שדה איזומורפי ל־ $\mathbb{Q}$.
ב. אם $charF = p$ אז יש ל־ F תת־שדה איזומורפי ל־ $\mathbb{Z}_p$.

הגדרה 3.1.4 תת־השדה של F הנוצר על־ידי $1 \in F$ נקרא תת־השדה הראשוני של F.

תרגיל 3.1.5 (**) יהי F שדה סופי.
א. הוכח ש־ $p = charF \neq 0$.
ב. הוכח ש־ F הוא מרחב וקטורי מעל השדה הראשוני שלו.
ג. הסק שמספר אברי F הוא חזקה של ראשוני.

תרגיל 3.1.6 (*) אין שדה מסדר $6, 10$ או 12.

תרגיל 3.1.7 (**) מצא את המאפיין של שדה בן 371293 אברים.

3.2 הרחבות אלגבריות

הגדרה 3.2.1 תהי $K \supseteq F$ הרחבה של שדות. איבר $\alpha \in K$ נקרא איבר אלגברי מעל F אם α מאפס פולינום עם מקדמים ב־ F.

תרגיל 3.2.2 (*) $\alpha \in K$ אלגברי אם ורק אם $[F[\alpha]:F]$ סופי.

משפט ([3]). אם $F \subseteq L \subseteq K$ שדות וההרחבות $K/L, L/F$ אלגבריות, אז גם K/F אלגברית.

הדרכה. יהי $\alpha \in K$. α מאפס פולינום $g(\lambda) = \beta_n\lambda^n + \ldots + \beta_0 \in L[\lambda]$. נסמן $L_0 = F[\beta_0, \ldots, \beta_n]$, אז $L_0[\alpha]/L_0$ ממימד סופי, וגם L_0/F ממימד סופי.

תרגיל 3.2.3 (***) תהי $F \subseteq K$ הרחבה. אם $\alpha, \beta \in K$ אלגבריים מעל F, אז גם $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ אלגבריים מעל F.

תרגיל 3.2.4 (**) תהי $F \subseteq K$ הרחבה. האוסף של אברי K שהם אלגבריים מעל F הוא שדה. שדה זה נקרא הסגור האלגברי של F ב־ K.

שדה שאין לו הרחבות אלגבריות נקרא שדה סגור אלגברית.

המשפט היסודי של האלגברה. שדה המספרים המרוכבים סגור אלגברית.

הערה. למרות שמו, אין למשפט היסודי של האלגברה הוכחה "אלגברית" ־ ואין זה פלא: ההגדרה של היא אנליטית ולא אלגברית.

תרגיל 3.2.5 (**) תן דוגמא להרחבה אלגברית של ממימד אינסופי.

הצעות: הסגור האלגברי של $\mathbb{Q}$ ב־$\mathbb{C}$. השדה של גדלים הניתנים לבניה גאומטרית. $\mathbb{Q}[\sqrt{1}, \sqrt{2}, \ldots]$.

3.2.1 חישוב פולינום מינימלי ־ ההצגה הרגולרית

תרגיל 3.2.6 (**) חשב את הפולינום המינימלי של $\sqrt{5} + \sqrt{6}$ מעל .

פתרון. נניח ש־ $x = \sqrt{5} + \sqrt{6}$. אז $6 = \sqrt{6}^2 = (x - \sqrt{5})^2 = x^2 - \sqrt{5}x + 5$ ולכן $5x^2 = (\sqrt{5}x) = (x^2 - 1)^2$. מכאן ש־ x מאפס את הפולינום $\lambda^4 - 7\lambda^2 + 1$. הפולינום איפריק בגלל המימד.

תהי K/F הרחבה ממימד $n = [K:F]$. נקבע בסיס (סדור) B של K מעל F.

תרגיל 3.2.7 (*) הכפל משמאל $\Gamma_\alpha : \beta \mapsto \alpha\beta$ הוא העתקה ליניארית מהמרחב הוקטורי K לעצמו, כלומר ־ $\Gamma_\alpha \in Hom_F(K, K)$.

תרגיל 3.2.8 (**) ההצגה הרגולרית של שדה. ההתאמה $\Gamma : \alpha \mapsto \Gamma_\alpha$ היא שיכון (של חוגים) של K בתוך $Hom_F(K) \simeq M_n(F)$.

תזכורת. האיזומורפיזם $Hom_F(K) \simeq M_n(F)$ הוא התאמת העתקה ליניארית $T : K \to K$ למטריצה המייצגת: המטריצה שהעמודה ה־ i שלה היא וקטור המקדמים של $T(b_i)$ לפי הבסיס B.

תרגיל 3.2.9 (**) הפולינום המינימלי של $\alpha \in K$ שווה לפולינום המינימלי של Γ_α (שהוא מחלק של הפולינום האופייני של המטריצה המייצגת).

תרגיל 3.2.10 (**) $\alpha, \beta \in$ מקיימים α^2 =5, $\beta^2 = \beta + 3$. מצא את הפולינום המינימלי של $\alpha + \beta$ מעל $\mathbb{Q}$.

פתרון. נקבע $K = [\alpha, \beta]$, ונבחר את הבסיס $B = 1, \alpha, \beta, \alpha\beta$. המטריצות המייצגות של α, β הן $\begin{array}{cccc} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array} = [\Gamma_\beta]_B$, $\Gamma\alpha_B = \begin{array}{cccc} 0 & 5 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 1 & 0 \end{array}$. הסכום הוא $[\Gamma_{\alpha+\beta}] = \begin{array}{cccc} 0 & 5 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 1 & 5 \\ 0 & 1 & 1 & 1 \end{array} = [\Gamma_\alpha + \Gamma_\beta]$, והפולינום האופייני של $\alpha + \beta$ הוא $f(\lambda) = \lambda^4 - 2\lambda^3 - 15\lambda^2 + 16\lambda - 1$. f איפריק כי $[\mathbb{Q}[\alpha + \beta] : \mathbb{Q}] = 4$.

תרגיל 3.2.11 (**) מצא באותה שיטה את הפולינום המינימלי של $\sqrt{b} + \sqrt{a}$ מעל $\mathbb{Q}$.

תרגיל 3.2.12 (***) מצא את הפולינום המינימלי של $3^{1/3} + 2^{1/3}$ מעל $\mathbb{Q}$.

תרגיל 3.2.13 (***) α, β הם שורשים של הפולינומים $f(\lambda) = \lambda^2 - a\lambda - a', g(\lambda) = \lambda^2 - b\lambda - b'$, $a, a', b, b' \in F$. מצא פולינום (ממעלה 4) מעל F שאותו מאפס $\alpha + \beta$.

תרגיל 3.2.14 (***) לא יתכן ש־ $[K : \mathbb{Q}] = 2$ ובהצגה הרגולרית $\Gamma_\alpha = (3 \quad 20 \quad 1)$.

3.2.2 תת־שדות

תרגיל 3.2.15 (*) $[K : F] = p$ ראשוני. הוכח שאין הרחבות ביניים $K \supset L \supset F$.

תרגיל 3.2.16 (***) $K = F[\alpha]/F$ הרחבה ממימד 4, כאשר הפולינום המינימלי של α הוא $f(\lambda) = \lambda^4 - a$, $a \in F$. נמצא את כל הרחבות הביניים של K/F, בהנחה $charF \neq 2$.

א. $F[\alpha] \supset F[\alpha^2] \supset F$, שתי ההרחבות ממימד 2.

ב. אם $K \supset L \supset F$, אז $[L : F] = 2$.

ג. יהי $\beta \in L$ איבר המקיים $\beta^2 \in F$. נכתוב $\beta = u + v\alpha$, $u, v \in F[\alpha^2]$. הוכח ש־ $uv = 0$.

ד. אם $v = 0$ אז $L \subseteq F[\alpha^2]$ ולכן $L = F[\alpha^2]$.

ה. אחרת, $u = 0$. נכתוב $v = x + y\alpha^2$, $x, y \in F$. הוכח ש־ x^2 +y0 $= {}^2\alpha^4$.

ו. הראה שזו סתירה ל־ $[K : F] = 4$. ס יכום. שדה הביניים היחיד הוא $F[\alpha^2]$.

תרגיל 3.2.17 (***) $K = F[\alpha, \beta]$ הרחבה ממימד 4, כאשר $\alpha^2, \beta^2 \in F$.

א. מצא שלושה שדות ביניים $K \supset L \supset F$, והוכח שכולם שונים זה מזה.

ב. הוכח שאין עוד תת־שדות.

הדרכה. יהי $x \in K$ איבר המקיים $x^2 \in F$, היוצר שדה שאינו ברשימה. עבוד מעל תת־השדות השונים כמו בשאלה הקודמת כדי לקבל סתירה.

3.3 שלמים אלגבריים

תהי $K/\mathbb{Q}$ הרחבה.

תרגיל 3.3.1 (*) אם $f(\lambda) \in [\lambda]$, אז קיים $n \in$ כך ש־ $n \cdot f(\lambda) \in [\lambda]$.

תרגיל 3.3.2 (*) לכל $\alpha \in K$ קיים פולינום מינימלי עם מקדמים שלמים.

הגדרה 3.3.3 הגדרה. איבר $\alpha \in K$ נקרא שלם אלגברי אם יש לו פולינום מינימלי מתוקן עם מקדמים שלמים.

תרגיל 3.3.4 (*) אוסף השלמים האלגבריים של הוא חוג השלמים .

תרגיל 3.3.5 (*) $\sqrt{3}$ שלם אלגברי, אבל $\frac{\sqrt{3}-1}{2}$ לא.

תרגיל 3.3.6 (**) $D \in$. מצא תנאי הכרחי ומספיק לכך ש־ $\frac{1+\sqrt{D}}{2}$ יהיה שלם אלגברי.

תרגיל 3.3.7 (**) מצא את כל השלמים האלגבריים בשדה $\mathbb{Q}[\sqrt{5}]$.

תרגיל 3.3.8 (**) אם α שלם אלגברי ו־ $n \in \mathbb{Z}$ אז
א. $n\alpha$ שלם אלגברי.
א. $\alpha + n$ שלם אלגברי.

תרגיל 3.3.9 (**) לכל α אלגברי, קיים $n \in$ כך ש־ $n\alpha$ שלם אלגברי.
משפט. אוסף השלמים האלגבריים בשדה K סגור לחיבור ולכפל.

פרק 4

בניה חיצונית של שדות

בפרקים הקודמים פגשנו שדות מהצורה $F[\alpha]$ כאשר $\alpha \in K$ ו־ $F \subseteq K$ הרחבה נתונה. זוהי בניה של תת־שדות של K.

בפרק זה נבנה הרחבות של F בלי להעזר בהרחבות נתונות שלו.

4.1 שורש של פולינום

אם $f(\lambda) \in F[\lambda]$ איפריק, אז F_1 =F$\langle f \rangle/[\lambda]$ הוא שדה, עם שיכון $F \hookrightarrow F[\lambda]/\langle f \rangle$ לפי $a \mapsto a + \langle f \rangle$.

משפט ([2]). ה איבר $\alpha = \lambda + \langle f \rangle \in F_1$ הוא שורש של f.

משפט ([2]). אם $f(\lambda) \in F[\lambda]$ איפריק, $F \subseteq K$, ו־ $\alpha \in K$ שורש של f, אז $F_1 \simeq F[\alpha]$.

מסקנה ([2]). אם $\alpha, \beta \in K$ שורשים של f (איפריק מעל F), אז $F[\alpha] \simeq F[\beta]$.

תרגיל 4.1.1 (*) אם $f(\lambda) = (\lambda - \alpha)(\lambda - \beta) \in F[\lambda]$, אז $F[\alpha] = F[\beta]$.

תרגיל 4.1.2 (**) יהי $\alpha = 2^{1/3}$. הוכח ש־ $[\alpha\rho_3] \simeq [\alpha]$, אבל השדות שונים זה מזה. הוכח ש־ $[\alpha\rho_{3^2}] = [\alpha\rho_3]$.

תרגיל 4.1.3 (**) הפולינום $\lambda^3 - 14\lambda^2$ +96$\lambda +$ איפריק מעל, ושורשיו (ב־) הם α, β, γ. מהו הפולינום המינימלי של α מעל ? של β מעל ? של γ מעל $\mathbb{Q}[\alpha, \beta]$? מצא פולינום ממעלה 2 מעל $[\alpha]$ שאותו מאפס β.

תרגיל 4.1.4 (־)** נסמן $f(\lambda) = \lambda^3 - 7\lambda - 6$. נסמן ב־ θ את האיבר $\lambda h\langle f \rangle$ של $K = \mathbb{Q}[\lambda]/\langle f \rangle$ (כך ש־ $f(\theta) = 0$). הראה ש־ $(2\theta^2 - 3\theta - 10)^2 = 28 - 3\theta^2 =$ $(\frac{2}{5}\theta^2 + \frac{1}{5}\theta - \frac{26}{5})^2$. כיצד יתכן שיש ל־ $28 - 3\theta^2$ ארבעה שורשים שונים ? פרט את החישובים התומכים בטענותיך.

4.2 שדות פיצול

יהי $f(\lambda) \in F[\lambda]$ פולינום.

משפט ([2]). קיים שדה $F \subseteq K$ שבו f מתפצל לגורמים ליניאריים.

הדרכה. פרק את f לגורמים איפריקים. אם קיים גורם לא ליניארי, בנה שדה המכיל שורש שלו.

הגדרה 4.2.1 אם $F \subseteq K$, f מתפצל לגורמים איפריקים מעל K, אבל לא מעל אף תת־שדה שלו, אז K נקרא שדה פיצול ש ל f מעל F.

משפט ([3]). שדה פיצול קיים, והוא יחיד עד־כדי איזומורפיזם.

הדרכה. התהליך מן המשפט הקודם בונה שדה פיצול.

תרגיל 4.2.2 (**) יהי K שדה פיצול של f מעל F. הוכח ש־ $[K:F] \leq n!$ כאשר $n = deg(f)$.

משפט ([1]). יהיו $f(\lambda) \in F[\lambda]$ פולינום, $F \subseteq K$. נניח ש־ f מתפצל ב־ K, והשורשים הם $\alpha_1,\ldots,\alpha_n \in K$. אז שדה הפיצול של f הוא $F[\alpha_1,\ldots,\alpha_n]$.

תרגיל 4.2.3 (**) נניח ש־ $n = deg(f)$, ו־ $\alpha_1,\ldots,\alpha_n \in K$ כאשר $F \subseteq K$. אז שדה הפיצול של f שווה ל־ $F[\alpha_1,\ldots,\alpha_{n-1}]$.

תרגיל 4.2.4 (*) מצא את שדות הפיצול של $x^4 - 2x^2 + 1$ ושל $x^4 + 2x^2 + 1$ מעל .

תרגיל 4.2.5 (**) מצא יוצרים לשדה הפיצול של $x^4 - 12$ מעל $\mathbb{Q}$.

תרגיל 4.2.6 (**) מצא את שדה הפיצול של $x^5 - 2$ מעל $\mathbb{Q}$ ואת מימדו.

תרגיל 4.2.7 (**) מצא את שדה הפיצול של $\{\, x^2 + 3x^2 - 3x^3 - 2 \,\}$ מעל $\{\, \mathbb{Q}[\sqrt{-3}] \,\}$, ואת המימד.

תרגיל 4.2.8 (**) מצא את שדה הפיצול של $(x^2+3)(x^3-3)$ מעל . מצא אוסף יוצרים מינימלי (כקבוצה) להרחבה.

תרגיל 4.2.9 (**) מצא יוצרים לשדה הפיצול של $x^4 - 4$ מעל .

תרגיל 4.2.10 (**) פצל את $\lambda^8 + 4$ מעל $\mathbb{Q}$. מותר להשתמש רק במספרים רציונליים ושורשיהם הריבועיים (אסור שיופיעו $\sqrt{i}$ $\rho_8,$ וכדומה). מהו שדה הפיצול?

תרגיל 4.2.11 (-)** פצל את $\lambda^{12} - 1$ מעל $\mathbb{Q}$. מצא קבוצת יוצרים מינימלית לשדה הפיצול. מה מימדו ?

תרגיל 4.2.12 (**) חשב את מימד שדה הפיצול של $\lambda^8 - 16$ מעל $\mathbb{Q}[\sqrt{2}]$.

תרגיל 4.2.13 (***) $f(\lambda) = \lambda^4 + a\lambda^2 - b$, כאשר $a \in \mathbb{Q}$ ו־ $0 < 2b \leq a$.

א. אין ל־ f שורשים ב־ $\mathbb{Q}$.

ב. f איפריק מעל .

ג. אם $\alpha \in$ שורש של f, אז $[\mathbb{Q}[\alpha^2]:\mathbb{Q}] = 2$ ו־ $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 4$.

ד. הוכח שמימד שדה הפיצול של $f(\lambda)$ מעל הוא 8.

4.3 הרחבות טרנסצנדנטיות

יהי F שדה. את שדה השברים של חוג הפולינומים $F[\lambda]$ מסמנים $F(\lambda)$. האברים של שדה השברים הם מנות של פולינומים: $F(\lambda) = \left\{ \frac{f(\lambda)}{g(\lambda)} : f, g \in F[\lambda], g \neq 0 \right\}$.

תרגיל 4.3.1 (+)** הוכח ישירות ש־ $F(\lambda)$ הוא שדה.

תרגיל 4.3.2 (**) $F(x)(y) \simeq F(y)(x)$. שדה זה מסמנים ב־ $F(x,y)$.

תרגיל 4.3.3 (**) $F(x^2)$ (תת־השדה של $F(x)$ הנוצר על־ידי x^2) מוכל ממש ב־ $F(x)$, ואיזומורפי לו.)

תרגיל 4.3.4 (***) אם $F \subseteq K$ ו־ x טרנסנדנטי מעל K, אז $[K : F] = [K(x) : F(x)]$.

תרגיל 4.3.5 (**) חשב את המימד של $F(x,y)$ מעל $F(x^2, y^2)$.
הדרכה. חשב את המימדים ביחס להרחבת הביניים $F(x, y^2)$.

תרגיל 4.3.6 (***) חשב את המימד של $F(x,y)$ מעל $F(x^2+y^2, xy)$.

תרגיל 4.3.7 (-*)** א. הוכח ש־ $F(x-y, \frac{x}{y}) = F(x,y)$.
ב. הוכח ש־ $F(x,y) \supset F(x+y, xy)$.

תרגיל 4.3.8 (**) $[F(x) : F(x^n)] = n$.

תרגיל 4.3.9 (***) תהי $r = f/g \in F(x)$ מנה של פולינומים. הוכח שהמימד $[F(x) \colon F(r)]$ שווה ל־ $\max \deg(f), \deg(g)$. כתוב את x כמנה של פולינומים ב־ r כאשר המימד הוא 1.

תרגיל 4.3.10 (***) הוכח ש־ $G = Gal(k(x)/k) = PGL_2(k)$. הוכח ש־ $k(x)^G = k$ אם ורק אם k אינסופי.

תרגיל 4.3.11 (***) תן דוגמא נגדית: אם $F \subseteq K$ אז קיים תת־שדה $F_0 \subseteq F$ כך ש־ K/F_0 גלואה.
פתרון. קח k סופי ו־ $K = k(x) \supset F$ קטן מדי.

תרגיל 4.3.12 (***) תן דוגמא לשדה K עם שני תת־שדות $K_0, K_1 \subseteq K$ ממימד $[K:K_i]=2$, כך שהמימד של K מעל $K_0 \cap K_1$ אינסופי. **פתרון**. למשל $K = k(t)$ כאשר k ממאפיין אפס, עם $K_0 = k(t^2)$ ו־ $K_1 = k(t-t^2)$. אם נגדיר $\sigma_i : t \mapsto i - t$ אז $K_i = K^{\sigma_i}$ ולכן $K_0 \cap K_1 = K^{\sigma_0} \cap K^{\sigma_1} = K^{\langle \sigma_0, \sigma_1 \rangle}$. אבל $\sigma_0\sigma_1 : t \mapsto t+1$ ושדה השבת הוא k.

4.4 השדות השלמים $\mathbb{R}$ $\mathbb{C}$

שדה הממשיים $\mathbb{R}$ הוא השדה הסדור השלם (=כל סדרת קושי מתכנסת) המינימלי. שדה המרוכבים הוא שדה הפיצול של x^2 + 1 מעל $\mathbb{R}$. את השורשים של x^2 +1 ב־ מסמנים $i, -i$, כך ש־ $\mathbb{R}[i] =$.

תרגיל 4.4.1 (**) יהיו $a, b \in \mathbb{R}$. הוכח שקיימים $u, v \in \mathbb{R}$ כך ש־ $(u + vi)^2$ =(a+ib).

המשפט היסודי של האלגברה. השדה סגור אלגברית, כלומר ־ לכל פולינום מעל יש שורש ב־ .

תרגיל 4.4.2 (*) כל פולינום מעל מתפצל ב־ .

תרגיל 4.4.3 (**) אין ל־ $\mathbb{R}$ הרחבות ממימד איזוגי.

תרגיל 4.4.4 (**) ההרחבה היחידה ממימד 2 של $\mathbb{R}$ היא .

תרגיל 4.4.5 (**) ההרחבה היחידה ממימד סופי של $\mathbb{R}$ היא .

תרגיל 4.4.6 (**) לכל פולינום ממעלה איזוגית מעל $\mathbb{R}$ יש שורש.

תרגיל 4.4.7 (**) הפולינום $x^7 + 3x^2 + 3x + 3$ מתפרק לגורמים ממעלה ≥ 2 מעל $\mathbb{R}$.

תרגיל 4.4.8 (**) תן דוגמא לשדה $\subseteq K$ ממימד 4 מעל, כך ש־ $\mathbb{R} = K \cap \mathbb{R}$.

פרק 5

שורשי היחידה

איבר מסדר סופי בחבורה הכפלית של שדה נקרא שורש יחידה.
אם $a^n = 1$ ו־ $a^m \neq 1$ לכל $0 < m < n$, אז a הוא שורש יחידה n־פרימיטיבי.

תרגיל 5.0.9 (**) יהי $\rho = \rho_n$ שורש יחידה n־פרימיטיבי. אם d מחלק של n, שורשי היחידה ה־ (n/d)־פרימיטיביים הם $\rho^k : (k,n) = d$. בפרט, שורשי היחידה ה־n־פרימיטיביים הם $\rho^k : k \in U_n$ ($U_n = \{k : (k,n) = 1\}$ היא חבורת אוילר של n, וגודלה $|U_n| = \phi(n)$).

תרגיל 5.0.10 (*) אם $(m_1, n) = (m_2, n)$ אז $\mathbb{Q}[\rho_n^{m_1}] = \mathbb{Q}[\rho_n^{m_2}]$.

תרגיל 5.0.11 (*) שורשי היחידה ה־n־פרימיטיביים בשדה הם $e^{\frac{2\pi i k}{n}}$, $k = 0, \ldots, n-1$.

תרגיל 5.0.12 (*) $x^n - 1$ מתפרק לגורמים ליניאריים מעל $\mathbb{Q}[\rho_n]$.

5.1 הפולינומים הציקלוטומיים

תרגיל 5.1.1 (**) פרק לגורמים איפריקים מעל את $x^n - 1$ עבור $n = 1, 2, \ldots, 6$.

תרגיל 5.1.2 (*+)** יהיו $f, g \in F[\lambda]$ פולינומים. אם $g(\lambda) \,|\, f(\lambda)$ בחוג $K[\lambda]$, $F \subseteq K$, אז $g(\lambda) \,|\, f(\lambda)$ גם בחוג $F[\lambda]$.

תרגיל 5.1.3 (**) יהי $F \subseteq K$. $K[\lambda], F(\lambda) \subseteq K(\lambda)$ הם תת־חוגים. הוכח ש־ $K[\lambda] \cap F(\lambda) = F[\lambda]$.

תרגיל 5.1.4 (*+)** אם $f, g \in \mathbb{Z}[\lambda], g$ מתוקן, ו־ $\frac{f(\lambda)}{g(\lambda)} \in \mathbb{Q}[\lambda]$, אז $\frac{f(\lambda)}{g(\lambda)} \in \mathbb{Z}[\lambda]$.

תרגיל 5.1.5 (*) $\lambda^n - 1 = \prod_{i=0}^{n-1}(\lambda - \rho_n^i)$.

הגדרה 5.1.6 $\Phi_1(x) = x - 1$, ובאינדוקציה $\Phi_n(x) = \frac{x^n-1}{\prod_{d|n,d<n}\Phi_d(x)}$. דוגמא. $\Phi_2 = \frac{x^2-1}{\Phi_1}$, $\Phi_6 = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3}$.

תרגיל 5.1.7 (**) $\Phi_n(\lambda) = \prod_{(k,n)=1}(\lambda - \rho_n^k)$. הדרכה. אינדוקציה על n.

תרגיל 5.1.8 (**) $\Phi_n(\lambda) \in \mathbb{Q}[\lambda]$. הדרכה. אינדוקציה.

תרגיל 5.1.9 (-*)** $\Phi_n(\lambda) \in \mathbb{Z}[\lambda]$.

תרגיל 5.1.10 (*) $x^n - 1 = \prod_{d|n}\Phi_d$.

תרגיל 5.1.11 (***) השתמש במשפט ההיפוך של מביוס כדי להראות ש- $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$.

תרגיל 5.1.12 (**) הוכח ש- $\deg(\Phi_n) = \phi(n)$ והסק את הזהות $n = \sum_{d|n}^{\phi}(d)$, כאשר ϕ היא פונקציית אוילר.

תרגיל 5.1.13 (*) הוכח ש- $[\mathbb{Q}[\rho_n] : \mathbb{Q}] \leq \phi(n)$.

ערכים מיוחדים

תרגיל 5.1.14 (*) חשב את $\Phi_n(x)$ עבור $n = 1, 2, \dots, 10, 12, 15$.

תרגיל 5.1.15 (**) חשב את $\Phi_p(x)$ כאשר p ראשוני. הוכח ש- Φ_p איפריק מעל $\mathbb{Q}$.

תרגיל 5.1.16 (**) אם n זוגי, אז $\Phi_{2n}(x) = \Phi_n(x^2)$.

תרגיל 5.1.17 (**) אם n איזוגי, אז $\Phi_{2n}(x) = \Phi_n(-x)$.

תרגיל 5.1.18 (***) נניח $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$. נסמן $c(n) = p_1 \dots p_t$, אז $\Phi_n(x) = \Phi_{c(n)}(x^{n/c(n)})$.

תרגיל 5.1.19 (**) $\Phi_n(0) = (-1)^{d(n)}$ כאשר $d(n)$ הוא מספר המחלקים של n.

תרגיל 5.1.20 (***)
1. חשב את $\Phi_{p^t}(x)$.
2. הראה ש- $\Phi_{p^t}(1) = p$.
3. אם $n \neq p^t$, אז $\Phi_n(1) = 1$.

תרגיל 5.1.21 (***) אם $n = 2p^\alpha$ אז $\Phi_n(-1) = p$; אחרת, $\Phi_n(-1) = 1$.

5.1.1 איפריקות הפולינומים הציקלוטומיים

תרגיל 5.1.22 (*) הוכח ישירות ש־ Φ_1, Φ_2, Φ_3, Φ_4, Φ_6 איפריקים מעל $\mathbb{Q}$.

תרגיל 5.1.23 (**) הוכח ש־ Φ_5, Φ_7, Φ_{10}, Φ_{11} איפריקים מעל $\mathbb{Q}$.

תרגיל 5.1.24 (***) הוכח ש־ Φ_8, Φ_{12} איפריקים מעל $\mathbb{Q}$. הדרכה. העזר בשורשי הפולינומים, או חשב את המימד $[\mathbb{Q}[\rho_n] : \mathbb{Q}]$ ישירות.

תרגיל 5.1.25 (***) הוכח ש־ Φ_9 איפריק מעל $\mathbb{Q}$. הדרכה. מצא הצבה מתאימה, והשתמש בקריטריון אייזנשטיין.

משפט ([3]). Φ_n איפריק מעל $\mathbb{Q}$. הדרכה. יהי g הפולינום המינימלי של ρ_n מעל $\mathbb{Q}$, וכתוב $\Phi_n = gh$. הראה שקיימים שורש ρ של g וראשוני p כך ש־ ρ^p שורש של h. מכאן $g(\lambda)|h(\lambda^p)$. כל המקדמים שלמים, ומודולו p מתקיים $g|h^p$ ולכן $g|h$, ומכאן גם $g^2|\Phi_n|(x^n-1)$ מודולו p. לכן $g|(x^n-1)' = nx^{n-1}$, סתירה כי $n \equiv 0 (mod p)$.

מסקנה ([2]). $[\mathbb{Q}[\rho_n]:\mathbb{Q}] = \deg(\Phi_n) = \phi(n)$.

תרגיל 5.1.26 (***) אם n זר ל־p, אז $\Phi_n(x)$ מתפרק לגורמים אי־פריקים זרים מעל $\mathbb{Z}_p$. מאידך $\Phi_{p^t n}(x) \equiv \Phi_n(x)^{\phi(p^t)} \pmod p$.

תרגיל 5.1.27 (**) הפולינום הציקלוטומי מתפרק מעל כל תת־שדה לא־טריוויאלי של $\mathbb{Q}[\rho_n]$.

שורשי יחידה בשדות ממימד נמוך

תרגיל 5.1.28 (**) מצא את כל שורשי היחידה בשדות $\mathbb{Q}[\sqrt{d}]$ ($d \in \mathbb{Z}$).

פתרון. אם $\rho_n \in \mathbb{Q}[\sqrt{d}]$ אז $\mathbb{Q}[\rho_n] \supseteq \mathbb{Q}[\sqrt{d}]$ ולפי מימדים $\phi(n) \leq 2$. הפתרון למשוואה זו הוא $n \in \{1,2,3,4,6\}$ ולכן שורשי היחידה הם $\rho_6^k, \rho_4^{\pm 1}$, $k = 0 \dots 5$.

תרגיל 5.1.29 (־)** מצא את כל שורשי היחידה ρ_n כך ש־ $[\mathbb{Q}[\rho_n] : \mathbb{Q}] = 4$.

תרגיל 5.1.30 (***) הוכח: אם $\cos(\alpha\pi) \in \mathbb{Q}$ עבור $\alpha \in \mathbb{Q}$, אז $\cos(\alpha\pi) \in \frac{1}{2}\mathbb{Z}$.

תרגיל 5.1.31 (***) תהי K הרחבה סופית של $\mathbb{Q}$. הוכח שיש רק מספר סופי של שורשי יחידה ב־ K.

תרגיל 5.1.32 (**) הוכח שלכל $n > 1$, $\prod_{k=1}^{n-1}(1 - e^{\frac{2\pi i k}{n}}) = n$. בעזרת חישוב הערך המוחלט, הסק כי $\prod_{k=1}^{n-1} \sin(\frac{\pi k}{n}) = \frac{n}{2^{n-1}}$.

5.2 תכונות יסודיות של שורשי היחידה

תרגיל 5.2.1 (*) הראה ש־ $\mathbb{Q}[\rho_6] = \mathbb{Q}[\rho_3]$.

תרגיל 5.2.2 (**) הוכח ש־ $\mathbb{Q}[\rho_8] = \mathbb{Q}[\sqrt{2}, \sqrt{-1}]$.

תרגיל 5.2.3 (**) מצא את הפולינום המינימלי של ρ_8 מעל $\mathbb{Q}$, מעל $\mathbb{Q}[\rho_4] = [i]$ ומעל $\mathbb{Q}[\sqrt{2}]$.

תרגיל 5.2.4 (-)** כתוב את $\sqrt{-3}$ כפולינום ב־ ρ_3, ואת $\sqrt{5}$ כפולינום ב־ ρ_5. נסה לנחש הכללה של התוצאות.

תרגיל 5.2.5 (***) יהי n טבעי איזוגי. סמן $W = ((\rho_n)^{i\cdot j})_{ij=0,\dots,n-1} \in M_n$), וחשב את $W^t \cdot W$.

הוכח ש־ $\sqrt{(-1)^{\binom{n-1}{2}} n} \in \mathbb{Q}[\rho_n]$.

תרגיל 5.2.6 (**) נסמן $\rho = \rho_{12}$. מצא את המספרים השלמים $(\rho + \rho^{-1})^2$, $(\rho+\rho^5)^2$, ו־ $(\rho+\rho^7)^2$.

תרגיל 5.2.7 (**) נסמן $u_n = \rho_{2^n} + \rho_{2^n}^{-1}$. הוכח ש־ $u_{n+1}^2 = 2 + u_n$. הסק ש־

$$\underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}_{n-2 \text{ שורשים}} \in [\rho_{2^n}].$$

תרגיל 5.2.8 (**) הוכח ש־ $\underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}}_{n-1 \text{ שורשים}} \in [\rho_{3\cdot 2^n}]$ לכל $2 \leq n$.

תרגיל 5.2.9 (**) בטא את $\sqrt{2+\sqrt{3}}$ כצירוף ליניארי של $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. הדרכה. חשב את $\rho_{24} + \rho_{24}^{-1}$.

תרגיל 5.2.10 (***) חשב את הפולינום המינימלי של ρ_7 מעל $\mathbb{Q}[\sqrt{-7}]$.

הדרכה. מצפים לפולינום ממעלה 3 או 6 (במה זה תלוי?). מצא α כך שה־ gcd של $x^6+x^5+\ldots+x+1$ ושל $x^4+x^2+x+\alpha$ הוא פולינום ממעלה 3. הראה ש־ ρ_7 אכן שורש של הפולינום המתקבל על־ידי שתחשב את $(\rho_7^4+\rho_7^2+\rho_7)^2$.

תרגיל 5.2.11 (-)** מצא תת־שדה ממימד 4 של $\mathbb{Q}[\rho_{16}]$, פרט ל־ $\mathbb{Q}[\rho_8] = \mathbb{Q}[\sqrt{2}, \sqrt{-1}]$.

תרגיל 5.2.12 (**) הוכח ש־ $\rho_{16} = \frac{1}{2}\left(\sqrt{\sqrt{2}+2} + \sqrt{\sqrt{2}-2}\right)$.

תרגיל 5.2.13 (***) מצא את שדות הפיצול של x^8-2 ושל x^8-7 מעל, ואת המימדים.

פתרון. השורשים של x^n-a הם $\alpha\rho_n^k : 0 \leq k < n$, כאשר α השורש הממשי החיובי של הפולינום. שדה הפיצול של x^8-7 הוא $(\alpha^8=7)$ $[\alpha,\rho_8]=[\alpha,\alpha\rho_8,\dots,\alpha\rho_8^7]$. קל לראות ש־ $[\mathbb{Q}[\rho_8]:\mathbb{Q}]=4$ $(\phi(8)=4)$ וש־ $[\mathbb{Q}[\alpha]:\mathbb{Q}]=8$ (אייזנשטיין עם $p=7$). בנוסף, $\sqrt{2}?\in\mathbb{Q}[\alpha]$. לכן $\mathbb{Q}[\rho_8]\cap\mathbb{Q}[\alpha]=\mathbb{Q}$ והמימד הוא 32.

אם נפעיל את אותם שיקולים עבור הפולינום השני נקבל את שדה הפיצול $[\alpha,\rho_8$ u כאשר $\alpha^8=2$. אבל $\mathbb{Q}[\rho_8]=\mathbb{Q}[i,\sqrt{2}]$, ו־ $\alpha^4=\sqrt{2}$. לכן $\mathbb{Q}[\alpha,\rho_8]=\mathbb{Q}[\alpha,i]$, שדה ממימד 16.

תרגיל 5.2.14 (-*)** נסמן $\rho=\rho_{13}\in$, $a=\rho+\rho^3+\rho^9$, $b=\rho^4+\rho^{10}+\rho^{12}$, $A=a+b$.

א. הוכח ש־ $A^2+A=3$.

ב. חשב ש־ $ab=2-A$, והסק $a=\frac{A\pm\sqrt{3A-5}}{2}$.

ג. קבע את הסימנים בביטוי $cos\left(\frac{2\pi}{13}\right)+\cos\left(\frac{6\pi}{13}\right)+\cos\left(\frac{18\pi}{13}\right)=\frac{1}{2}\left(\frac{-1\pm\sqrt{13}}{2}\pm\sqrt{\frac{-13\pm3\sqrt{13}}{2}}\right)$.

פרק 6

נורמליות וספרביליות

6.1 הרחבות ספרביליות

6.1.1 פולינומים

הגדרה 6.1.1 פולינום איפריק $f(\lambda) \in F[\lambda]$ הוא פולינום ספרבילי אם בשדה הפיצול שלו, כל שורשיו שונים. פולינום הוא ספרבילי אם כל גורמיו האיפריקים הם ספרביליים.

תרגיל 6.1.2 (*) אם $F \subseteq K$ ו־ $p(x) \in F[x]$ ספרבילי מעל F, אז $p(x)$ ספרבילי גם מעל K.

הגדרה 6.1.3 (גזירה אלגברית). אם $f(\lambda) = \sum_{i=0}^{n} a_i \lambda^i \in F[\lambda]$, $f'(\lambda) = \sum_{i=1}^{n} i \cdot a_i \lambda^{i-1}$.

תרגיל 6.1.4 (*) אם $f, g \in F[\lambda]$, $(fg)' = fg' + f'g$.

תרגיל 6.1.5 (*) אם $f^2 \mid g$, אז $f|g'$, ובפרט $f|(g, g')$.

תרגיל 6.1.6 (**) נניח ש־ $f \in F[\lambda]$ ו־ $g_1, g_2 \in K[\lambda]$ כך ש־ $f = g_1 g_2$ ספרבילי. אז g_1, g_2 זרים מעל K.

תרגיל 6.1.7 (**) $charF = 0$. אם $f'|f$, אז f מהצורה $f(x) = \alpha(x - \beta)^n$.

תרגיל 6.1.8 (**) יהיו $C \subseteq D$ חוגים אוקלידיים, $f_1, f_2 \in C$. אם f_1, f_2 זרים ב־ C אז הם זרים גם ב־ D.

תרגיל 6.1.9 (+*)** יהי $f(\lambda) \in F[\lambda]$ איפריק. אז $f' \neq 0$ אם ורק אם $(f', f) = 1$ בחוג $F[\lambda]$.

משפט ([2]). יהי $f(\lambda) \in F[\lambda]$ איפריק. אז f לא ספרבילי אם ורק אם $f' = 0$.

תרגיל 6.1.10 (**) יהי $f(\lambda) \in F[\lambda]$ איפריק. $f' = 0$ אם ורק אם $f(\lambda) = g(\lambda^p)$ לאיזשהו $g(\lambda) \in F[\lambda]$, כאשר $p = charF$.

תרגיל 6.1.11 (-)** הוכח שהפולינום λ^p -t^p מעל $\mathbb{Z}_p(t^p)$ איפריק ואינו ספרבילי.

6.1.2 הרחבות

משפט ([3]). יהי F שדה שאינו סופי. אז כל הרחבה ספרבילית סופית של F נוצרת על־ידי איבר אחד. (המשפט נכון גם כאשר F סופי). יהיו $K = F[\alpha, \beta]$, ויהיו $f, g \in F[x]$ הפולינומים המינימליים של α, β. יהי L שדה פיצול של fg, כך שאפשר לכתוב ב־ L $f(x) = \prod(x - \alpha_i)$ ו־ $g(x) = \prod(x - \beta_i)$.

א. הוכח שקיים $t \in F$ כך שלכל $i, j \geq 2$ מתקיים $\alpha + t\beta \neq \alpha_i$ +tβ_j.

ב. נסמן $\gamma = \alpha + t\beta$, ו־ F_1 =F$[\gamma]$. יהי $r(x) = f(\gamma - tx)$. הוכח ש־ $(x - \beta)$ הוא המחלק המשותף המקסימלי של $r(x)$ ו־ $g(x)$ ב־ $F_1[x]$. (היכן השתמשת בספרביליות של g ?)

ג. הסק כי $\beta \in F_1$ ו־ $F[\alpha, \beta] = K = F_1$ =F$[\gamma]$.

תרגיל 6.1.12 (-)** יהיו F שדה ממאפיין $p \neq 0$, $\alpha \in F$. הוכח שהפולינום המינימלי של α הוא ספרבילי אם ורק אם $F[\alpha^p] = F[\alpha]$.

6.1.3 שדות סופיים

יהיו F שדה ממאפיין $p \neq 0$, $\alpha \in F$.

תרגיל 6.1.13 (*) אם $\alpha = \beta^p$ כאשר $\beta \in F$, אז $\lambda^p - \alpha = (\lambda - \beta)^p$.

תרגיל 6.1.14 (**) אם $\alpha^{1/p}$; $F \in \#???$, אז $f(\lambda) = \lambda^p - \alpha$ איפריק, וההרחבה F/$F[\alpha^{1/p}]$ לא ספרבילית.

הדרכה. נניח ש־ $f(\lambda) = g(\lambda)h(\lambda)$, ויהי β שורש של g בשדה פיצול E של f. הוכח ש־ $g(\lambda) = (\lambda - \beta)^k$ לאיזשהו k. השתמש במקדם של x^{k-1}.

תרגיל 6.1.15 (**) אם F סופי, אז $\alpha^{1/p} \in F$.

הדרכה. a איבר בחבורה הכפלית של F שהיא מסדר $|F| - 1$.

תרגיל 6.1.16 (**) פולינום איפריק מעל שדה סופי הוא ספרבילי.

6.2 הרחבות נורמליות

הגדרה 6.2.1 הרחבה K/F היא נורמלית אם הפולינום המינימלי מעל F של כל איבר ב־ K, מתפצל ב־ K.

תרגיל 6.2.2 (**) כל הרחבה ממימד 2 היא נורמלית.

משפט ([3]). K/F נורמלית אם ורק אם K הוא שדה פיצול לאיזשהו פולינום מעל F.

תרגיל 6.2.3 (*+)** יהיו $K \supset L \supset F$ שדות, כך ש־ K/F הרחבה נורמלית. הראה שגם K/L נורמלית.

תרגיל 6.2.4 (**) נ ורמליות אינה תכונה טרנזיטיבית. נסמן $L = \mathbb{Q}[\sqrt{2}]$, $K = \mathbb{Q}[\sqrt{1+\sqrt{2}}]$. הראה ש־ $L/\mathbb{Q}$ ו־ K/L הרחבות נורמליות, אבל $K/\mathbb{Q}$ אינה נורמלית.

הדרכה. הראה ש־ $K \in \sqrt{1-\sqrt{2}}$.

תרגיל 6.2.5 (**) $\mathbb{Q}[2^{1/4}]/\mathbb{Q}$ אינה הרחבה נורמלית.

הגדרה 6.2.6 הרחבה K/F היא הרחבה ספרבילית אם הפולינום המינימלי של כל איבר $\alpha \in K$ ספרבילי.

הגדרה 6.2.7 K/F הרחבת גלואה אם היא נורמלית וספרבילית.

משפט ([3]). K/F היא הרחבת גלואה אם ורק אם K שדה פיצול לאיזשהו פולינום ספרבילי מעל F.

תרגיל 6.2.8 (**) תן דוגמא להרחבה נורמלית, שאינה ספרבילית. הצעה. קח $F =_p (t)$.

תרגיל 6.2.9 (**) F שדה ממאפיין $p \neq 0$, t טרנצנדנטי מעל F, ו־ $K = F(t)$. ניקח $E = K[t^{1/p}]$, שדה הפיצול של λ^p ־t. חשב את $Gal(E/K)$. האם E/K הרחבה נורמלית (הוכח ישירות). האם היא הרחבת גלואה?

תרגיל 6.2.10 (***) הראה שלכל הרחבת גלואה K/F קיים בסיס נורמלי (כלומר, בסיס מהצורה $\sigma(a)$ כאשר $a \in K$ קבוע).

פרק 7

תורת גלואה

תרגיל 7.0.11 (*) אם $\varphi : F \to K$ הומומורפיזם של חוגים, F, K שדות, אז φ חח"ע.

תרגיל 7.0.12 (*) אם $\varphi : R \to R$ אנדומורפיזם של חוגים, ו־ $\varphi^n = Id_R$ לאיזשהו R, אז φ אוטומורפיזם.

הגדרה 7.0.13 איזומורפיזם מהשדה לעצמו נקרא אוטומורפיזם.

תרגיל 7.0.14 (*) אוסף כל האוטומורפיזמים של שדה הוא חבורה (ביחס לפעולת ההרכבה).

7.1 חבורת גלואה

תהי $F \subseteq K$ הרחבה של שדות.

הגדרה 7.1.1 אוטומורפיזם של ההרחבה K/F הוא אוטומורפיזם $\sigma : K \to K$, כך ש־ $\sigma(a) = a$ לכל $a \in F$.

תרגיל 7.1.2 (**) אוסף האוטומורפיזמים של ההרחבה הוא חבורה.

תרגיל 7.1.3 (*) יהי F_0 השדה הראשוני של F. אז כל אוטומורפיזם של F הוא אוטומורפיזם של F/F_0.

הגדרה 7.1.4 חבורת גלואה של הרחבה - $Gal(K/F) = \{\sigma : K \to K, \sigma|_F = id_F\}$.

תרגיל 7.1.5 (**) אם K/F ממימד סופי ו־ $\sigma : K \to K$ הומומורפיזם השומר על אברי F, אז $\sigma \in Gal(K/F)$.

תרגיל 7.1.6 (+*) אם $F \subseteq L \subseteq K$, אז $Gal(K/L) \leq Gal(K/F)$.

7.1.1 תמונות של איברים

תרגיל 7.1.7 (-*)** $Gal(\mathbb{R}/\mathbb{Q})=\{1\}$. הדרכה: כל אוטומורפיזם הוא אוטומורפיזם של השדה הסדור.

תרגיל 7.1.8 (*) יהיו $f(\lambda)\in F[\lambda]$, $\alpha\in K$, $\sigma\in Gal(K/F)$. אז $\sigma f(\alpha)=f(\sigma\alpha)$.
יהי $\alpha\in K$ איבר שהפולינום המינימלי שלו מעל F הוא $f(\lambda)\in F[\lambda]$.
משפט (^{2}). לכל $\sigma\in Gal(K/F)$, $\sigma(\alpha)$ הוא שורש של f ב־ K.

תרגיל 7.1.9 (**) $\sqrt{D}?\in$. הוכח שאם $a+b\sqrt{m}$ שורש של $f(\lambda)\in[\lambda]$, אז גם $a-b\sqrt{\lambda}$ שורש.

תרגיל 7.1.10 (**) חבורת גלואה של $\mathbb{Q}[\sqrt[3]{5}]/\mathbb{Q}$ היא טריוויאלית.

תרגיל 7.1.11 (**) נניח ש־ $K=F[\alpha_1,\ldots,\alpha_t]$. אם $\sigma,\sigma'\in Gal(K/F)$ מקיימים $\sigma(\alpha_i)=\sigma'(\alpha_i)$, אז $\sigma=\sigma'$.
(במלים אחרות, התמונה של קבוצת יוצרים קובעת את האוטומורפיזם).

תרגיל 7.1.12 (**) חשב את חבורת גלואה של $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.
פתרון. אם $\sigma\in G=Gal([\sqrt{2}]/)$ אז $\sigma:\sqrt{2}\mapsto\pm\sqrt{2}$, ולכן $|G|\leq 2$. $\sqrt{2}\mapsto\sqrt{2}$ הוא הזהות, ואת האוטומורפיזם השני אפשר לבדוק ישירות. מתקבל $G\simeq_2$.

תרגיל 7.1.13 (**) חשב את חבורות גלואה של $\mathbb{Q}[\sqrt{2},\sqrt{3}]/?$ ושל $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}[\sqrt{3}]$.

7.1.2 ספירת אוטומורפיזמים

התוצאות. $|\mathrm{Gal}(K/F)|\leq[K:F]$, שוויון אם"ם זוהי הרחבת פיצול. הרחבה היא נורמלית אם"ם $F=K^G$.
משפט (^{2}). יהי $K=F[\alpha]$ כאשר $f(\lambda)\in F[\lambda]$ הפולינום המינימלי של α . אז $|\mathrm{Gal}(K/F)|$ שווה למספר השורשים של f ב־ K.
מסקנה (^{2}). אם K שדה הפיצול של $f(\lambda)\in F[\lambda]$ איפריק, ו־ K נוצר על־ידי שורש של f, אז $|\mathrm{Gal}(K/F)|=[K:F]$.
משפט (^{3}). לכל הרחבה K/F, $|\mathrm{Gal}(K/F)|\leq[K:F]$. אם ההרחבה K/F נורמלית וספרבילית, קיים שוויון.
הדרכה. אינדוקציה על המימד, בעזרת המשפט על המקרה $K=F[\alpha]$.

7.1.3 חישוב חבורת גלואה

תרגיל 7.1.14 () פשר להחליף חישוב של חבורת גלואה גדולה בחישוב מספר חבורות גלואה קטנות יותר (היוצרות את החבורה הגדולה).

תרגיל 7.1.15 () תהי K/F הרחבת גלואה, ויהיו $F \subseteq L_1,\dots,L_t \subseteq K$ תת־שדות. נסמן ב־ $G_i = Gal(K/L_i)$ את חבורות גלואה המתאימות (שכולן תת־חבורות של $G = Gal(K/F)$). הוכח ש־ $G = \langle G_1,\dots,G_t\rangle$ אם ורק אם $L_1 \cap \dots \cap L_t = F$.

תרגיל 7.1.16 (**) כתוב במפורש את כל האוטומורפיזמים של $F[2^{1/3}]$ מעל F, עבור:
א. $F = [\rho_3]$.
ב. $F =$.
ג. $F = [2^{1/6}]$.

תרגיל 7.1.17 (**) נסמן $f(\lambda) = \lambda^3$ ־2, $\alpha = 2^{1/3}$ (שורש של f). חשב את חבורת גלואה של $[\alpha]/\mathbb{Q}$ ושל שדה הפיצול של f מעל .

תרגיל 7.1.18 (**) מצא את חבורת גלואה של שדה הפיצול של $x^4 - 3x^2 + 4$ מעל .

תרגיל 7.1.19 (**) $\rho_n \in F$. הוכח שחבורת גלואה של x^n ־a היא אבלית.

תרגיל 7.1.20 (**) חשב את חבורות גלואה הבאות: $Gal(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$, $Gal(\mathbb{Q}[\sqrt{2}+\sqrt{3}]/\mathbb{Q})$.

תרגיל 7.1.21 (**) יהיו $p_1,\dots,p_n$ ראשוניים שונים. מצא את חבורת גלואה של

$$\mathbb{Q}[\sqrt{p_1},\dots,\sqrt{p_n}]/\mathbb{Q}.$$

תרגיל 7.1.22 () א. נסמן $f(\lambda) = \lambda^4 + 3$. חשב את שדה הפיצול של $f(\lambda)$ מעל ואת מימדו.

הדרכה. נסמן $\alpha = 3^{1/4}$ ו־ $\rho = \rho_8$. שורשי הפולינום הם $\rho\alpha, \rho^3\alpha, \rho^5\alpha, \rho^7\alpha$ ושדה הפיצול $K = [\rho^2, \rho\alpha]$. הוכח ש־ $\mathbb{Q}[\sqrt{-1}, \sqrt{3}], [\rho\alpha] \subseteq K$ הם תת־שדות ממימד 4. הוכח ש־ $[K : [\rho\alpha]] \le 2$. הוכח ש־ $[\rho\alpha] \neq \mathbb{Q}[\sqrt{-1}, \sqrt{3}]$. הסק ש־ $[K : \mathbb{Q}] = 8$.

ב. חשב את חבורת גלואה $Gal(K/)$.

פתרון. ההרחבה $K/[\rho\alpha]$ נוצרת על־ידי ρ^2 ומימדה 2. חבורת האוטומורפיזמים נוצרת על־ידי $\tau : \rho^2 \to -\rho^2$ ואיזומורפית ל־ $\mathbb{Z}_2$. ההרחבה $K/\mathbb{Q}[\rho^2]$ נוצרת על־ידי $\rho\alpha$ והחבורה נוצרת על־ידי $\sigma : \rho\alpha \to \rho^3\alpha$, ואיזומורפית ל־ $\mathbb{Z}_4$. בנוסף $\tau\sigma\tau^{-1} = \sigma^{-1}$ ולכן $Gal(K/) \simeq D_4$.

ג. הוכח ש־ $K \cap \mathbb{R} = [\sqrt{3}]$.

ד. הוכח ש־ $\rho? \in K$. פתרון. א חרת $\sqrt{2} = \rho + \rho^{-1} \in K$ והרי גם $\sqrt{2} \in \mathbb{R}$, סתירה לסעיף ג'.

ה. חשב את מימד ההרחבה $L = [\rho, \alpha]/\mathbb{Q}$ ואת חבורת גלואה. הוכח ש־ L הוא שדה פיצול של $x^8 - 9$.

הדרכה. $[L:K] \leq 2$ ו־ $K \neq L$. לכן המימד הוא 16. את החבורה אפשר לחשב באופן דומה לסעיף ב: היא נוצרת על־ידי : η_2 , $(\alpha \to \alpha\rho \to \rho^3)$: η_1 , $(\alpha \to \rho\alpha\rho \to \rho)$: μ $(\alpha \to \alpha\rho \to -\rho)$. מצא יחסים המספיקים לתאור החבורה.

ו. הוכח שהצמוד המרוכב $z \mapsto z$ הוא אוטומורפיזם של L, והצג אותו כמכפלה של היוצרים.

ז. חשב את התמונה של K תחת הצמוד המרוכב, והראה שהשדה המתקבל K שונה מ־ K. הסק ש־ $z \mapsto z$ אינו אוטומורפיזם של K. חשב את $K \cap K$. חשב את $L \cap \mathbb{R}$.

7.1.4 $\mathrm{Gal}(K/F)$ כחבורת תמורות

יהי K שדה הפיצול של $f(\lambda) \in F[\lambda]$.

תרגיל 7.1.23 (*) יהיו $\alpha_1, \ldots, \alpha_n$ השורשים של f ב־ K. נגדיר העתקה $Gal(K/F) \to S_n$ לפי $\alpha_{\sigma(i)} = \sigma(\alpha_i)$. הוכח שזהו שיכון.

תרגיל 7.1.24 (**) תת־החבורה $Gal(K/F)$ של S_n היא טרנזיטיבית (כלומר, $\forall i \forall j \exists \sigma$: $\sigma(i) = j$).

תרגיל 7.1.25 (**) כתוב במפורש את השיכון של $Gal(\mathbb{Q}[2^{1/5}, \rho_5]/\mathbb{Q})$ ב־ S_5.

7.2 התאמת גלואה

7.2.1 H° ו־ L^*

תהי K/F הרחבת שדות, ותהי $G = \mathrm{Gal}(K/F)$ חבורת גלואה.

הגדרה 7.2.1 תהי $H \leq G$ תת־חבורה. $H^\circ = K^H = \alpha \in K : \sigma \in H \to \sigma(\alpha) = \alpha$ - השדה הקבוע של H.

תרגיל 7.2.2 (*) K^H הוא שדה ביניים של K/F : $F \subseteq K^H \subseteq K$. בפרט, $F \subseteq K^G$.

תרגיל 7.2.3 (*) אם $H_1 \subseteq H_2$ אז $H_2^\circ \subseteq H_1^\circ$.

יהי $F \subseteq L \subseteq K$ שדה ביניים.

הגדרה 7.2.4 $L^* = Gal(K/L) = \sigma \in G : \alpha \in L \to \sigma(\alpha) = \alpha$ - החבורה הקובעת את L.

תרגיל 7.2.5 (*) $Gal(K/L)$ תת־חבורה של G.

תרגיל 7.2.6 (*) אם $L_1 \subseteq L_2$ אז $L_2^* \subseteq L_1^*$.

תרגיל 7.2.7 (*) א. לכל $H \leq G$, $H \subseteq H^{\circ *}$ (בניסוח אחר: $H \leq Gal(K/K^H)$.
ב. לכל $F \subseteq L \subseteq K$, $L \subseteq L^{*\circ}$).

תרגיל 7.2.8 (**) $H^{\circ * \circ} = H^\circ$, $L^{*\circ *} = L^*$.

7.2.2 כמה משפטים

תרגיל 7.2.9 (*) אם $G = Gal(K/F)$, אז $Gal(K/K^G) = G$.

משפט ([3]). אם K/F הרחבה נורמלית וספרבילית, אז $K^{Gal(K/F)}$ =F

הדרכה. אם $F_1 = K^{Gal(K/F)}$ אז $[K : F_1] = Gal(K/F_1) = |Gal(K/F)| =$ $[K : F]$.

הלמה של $Artin$ ([3]). לכל חבורה G של אוטומורפיזמים של K, מתקיים $[K : K^G] \leq |G|$.

הדרכה. נניח $G = \sigma_1, \ldots, \sigma_n$, ו־ $a_1, \ldots, a_m \in K$, $n < m$. קח פתרון (מעל E) למשוואות $\forall i : \sum_{j=1^{m\sigma_i(a_j)x_j=0}}$, והראה שאפשר לקבל ממנו פתרון עם $x_j \in K^G$ – ולכן a_j תלויים מעל K^G.

משפט ([2]). לכל חבורה G של אוטומורפיזמים, $Gal(K/K^G) = G$, וההרחבה K/K^G הרחבת גלואה.

7.2.3 התאמת גלואה

משפט ([3]). תהי K/F הרחבת גלואה. אז ההתאמה $H \to K^H$ הפוכה להתאמה $L \to \mathrm{Gal}(K/L)$, ושתיהן חד־חד־ערכיות ועל. בנוסף, ההתאמות שומרות על –

א. אינדקסים: $[K : K^H] = |H|$, $[G : H] = [K^H : F]$.

ב. היפוך סדר: $H_1 \subseteq H_2 \to K^{H_2} \subseteq K^{H_1}$.

ג. נורמליות: K^H/F הרחבה נורמלית אם ורק אם $H \triangleleft G$.

משפט ([2]). אם $H \triangleleft G$, אז $\mathrm{Gal}(K^H/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/K^H)$.

תרגיל 7.2.10 (-)** אם K/F הרחבה סופית, אז קיימת הרחבה $F \subseteq K \subseteq E$ כך ש־ $[E : F] \leq [K : F]!$, ו־ E/F הרחבת גלואה.

תרגיל 7.2.11 (**) אם K/F הרחבה ממימד סופי, אז יש רק מספר סופי של שדות ביניים $F \subseteq L \subseteq K$.

תרגיל 7.2.12 (**) מצא את חבורת גלואה, ועבור כל תת־חבורה שלה מצא את תת־השדה המתאים:

א. $\mathbb{Q}[\sqrt[3]{3}]/\mathbb{Q}$.

ב. $\mathbb{Q}[\rho_{12}]/\mathbb{Q}$.

ג. $\mathbb{Q}[\rho_9]/\mathbb{Q}$.

תרגיל 7.2.13 (**) מצא שבעה תת־שדות שונים של $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{-1}]$.

7.2.4 דוגמא: הפולינום $f(\lambda) = \lambda^4 - 3$

נסמן ב־ α את השורש הממשי $\alpha = \sqrt[4]{3}$.

תרגיל 7.2.14 (*) פצל את הפולינום $f(\lambda)$ מעל . הוכח ששדה הפיצול של $f(\lambda)$ הוא $K = [\alpha, i]$.

תרגיל 7.2.15 (+*) $[K : \mathbb{Q}] = 8$.

נסמן ב־ σ, τ את האוטומורפיזמים של K המוגדרים על־ידי $\sigma : \left\{ \begin{array}{c} \alpha \to i\alpha \\ i \to i \end{array} \right\}$, $\tau : \left\{ \begin{array}{c} \alpha \to \alpha \\ i \to -i \end{array} \right\}$.

תרגיל 7.2.16 (**) הוכח ש־ $Gal(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

תרגיל 7.2.17 (*) הראה ש־ $\sigma^4 = \tau^2 = (\sigma\tau)^2 = id_K$, והסק ש־ $Gal(K/\mathbb{Q}) \simeq D_4$.

תרגיל 7.2.18 (**) מצא את השדה $K^{\sigma\tau}$.

תרגיל 7.2.19 (**) מצא את כל הרחבות הביניים $K \supset L \supset$ כך ש־ $L/\mathbb{Q}$ נורמלית.

7.2.5 תרגילים נוספים

תרגיל 7.2.20 () מצא את חבורת גלואה של שדה הפיצול של $x^3 - 2$ מעל $\mathbb{Q}$. מצא את כל תת החבורות של G ועבור כל תת־חבורה את שדה השבת שלה.

תרגיל 7.2.21 (**) חשב את חבורות גלואה של ההרחבות הבאות: $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt[3]{5}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$. בכל המקרים חשב את שדות השבת של כל תת־החבורות של חבורת גלואה. באילו מקרים K/F, K/K^H ו־ K^H/F הרחבות גלואה?

תרגיל 7.2.22 (**) יהי F שדה ממאפיין $\neq 2$. נניח ש־ $Gal(K/F) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. תאר את סריג שדות הביניים של K/F, ומצא יוצרים לכל הרחבה בסריג.

תרגיל 7.2.23 (**) חשב את שדה הפיצול של $f(\lambda) = \lambda^4 - a\lambda^2 + b^2$, כאשר $a, b \in F$. מצא את חבורת גלואה, ואת כל שדות הביניים.

הדרכה. פצל את $y^2 - ay + b^2$ בשדה $F[\sqrt{D}]$. הראה שמימד שדה הפיצול מעל $F[\sqrt{D}]$ הוא 2 ולא 4.

תרגיל 7.2.24 (**) חשב את חבורת גלואה G של $x^4 - 3x^2 + 4$. מצא את תת־החבורות של G ואת שדות השבת שלהם.

הדרכה. בדוק את הריבוע של $1 + \sqrt{-7}$.

תרגיל 7.2.25 (־)** חשב את התאמת גלואה עבור הפולינום $\lambda^6 + 3$. הדרכה. מימד שדה הפיצול הוא 6. מדוע ?

7.2.6 שורשי היחידה

תרגיל 7.2.26 (++*) מצא את חבורת גלואה של $\mathbb{Q}[\rho_9]/\mathbb{Q}[\rho_3]$.

תרגיל 7.2.27 (**) נסמן $\rho = \rho_n$. לכל אוטומורפיזם $\sigma : \mathbb{Q}[\rho] \to \mathbb{Q}[\rho]$ קיים $d \in U_n$ כך ש- $\forall m : \sigma(\rho^m) = \rho^{md}$.

משפט (^{2}). חבורת גלואה $Gal(\mathbb{Q}[\rho_n]/\mathbb{Q})$ איזומורפית לחבורת אוילר U_n.

תרגיל 7.2.28 (***) אם $n = p^m$, $p \neq 2$ אז חבורת אוילר של n היא ציקלית, $U_n \simeq \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p-1}$.

תרגיל 7.2.29 (***) אם $n = 2^m$, $3 \leq m$, אז $U_n = \langle 5, -1 \rangle \simeq \mathbb{Z}_{n/4} \times \mathbb{Z}_2$.

תרגיל 7.2.30 (**) אם $(n,m) = 1$ אז $U_{nm} \simeq U_n \times U_m$.

תרגיל 7.2.31 (+*) הוכח ש- $U_{360} \simeq \mathbb{Z}_{12} \times (\mathbb{Z}_2)^3$.

תרגיל 7.2.32 (**) מצא שדה פיצול K לפולינום $\lambda^{12} - 1$ מעל $\mathbb{Q}$, וחשב את חבורת גלואה של ההרחבה ואת תת־השדות שלה.

תרגיל 7.2.33 (**) הוכח ש- $Gal(\mathbb{Q}[\rho_7]/\mathbb{Q}) = \langle \rho_7 \mapsto \rho_7^3 \rangle$. הראה שתת־השדות של $\mathbb{Q}[\rho_7]$ הם $\mathbb{Q}[\rho + \rho^{-1}]$ ו- $\mathbb{Q}[\rho + \rho^2 + \rho^4]$. הצג את $\rho + \rho^2 + \rho^4$ בצורה $\sqrt{d}$, $d \in \mathbb{Z}$.

תרגיל 7.2.34 (***) נסמן $\rho = \rho_{24}$.

א. הוכח ש- $\rho = \frac{\sqrt{2}}{4}\left((1+\sqrt{3}) + (-1+\sqrt{3})i\right)$. הדרכה: חשב את ρ^2,ρ^3.

ב. הסק ש- $cos(15°) = \frac{\sqrt{6}+\sqrt{2}}{4}$, $sin(15°) = \frac{\sqrt{6}-\sqrt{2}}{4}$.

ג. הוכח ש- $\mathbb{Q}[\rho_{24}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{-1}]$.

ד. מצא את הפולינום המינימלי של ρ_{24} מעל $\mathbb{Q}[\sqrt{-1}]$ ומעל $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

ה. נסמן ב- σ_2 את האוטומורפיזם המוגדר לפי $\sigma_2 : \sqrt{-1} \to \sqrt{-1}\sqrt{2} \to -\sqrt{2}\sqrt{3} \to \sqrt{3}$, ובדומה σ_3 ו- σ_{-1}.

הראה ש- $\sigma_{-1}(\rho) = \rho^{23}$, $\sigma_2(\rho) = \rho^{13}$, $\sigma_3(\rho) = \rho^{17}$.

ו. בנה איזומורפיזם $Gal(\mathbb{Q}[\rho_{24}]/\mathbb{Q}) \cong U_{24}$.

7.2.7 סגור גלואה

הגדרה. תהי K/F הרחבה ספרבילית. שדה הפיתול E של הפולינום המינימלי של יוצר של K/F נקרא 'סגור גלואה' של K/F.

1. E הוא השדה המינימלי המכיל את K שהוא גלואה מעל F.
2. אז הליבה של $\mathrm{Gal}(E/K)$ בתוך $\mathrm{Gal}(E/F)$ היא 1.

תרגיל 7.2.35 (-*)** חשב את המימד של סגור גלואה E של $\mathbb{Q}[\sqrt{5+\sqrt{7}}]$ מעל $\mathbb{Q}$, והראה ש- $\mathbb{Q}[\sqrt{2}, \sqrt{7}] \subseteq E$.

7.2.8 מכפלה טנזורית של שדות

הגדרת $K\otimes_F L$ לפי יוצר והרחבת סקלרים. זהו שדה אם ורק אם $K\cap L=F$.

תרגיל 7.2.36 (***) נניח ש־ $L=L_1\otimes_F L_2$. הוכח שאם L_1/F ו־ L_2/F הן הרחבות גלואה, אז L/F הרחבת גלואה ו־ $Gal(L/F)\cong Gal(L_1/F)\times Gal(L_2/F)$.

תרגיל 7.2.37 (***) מצא דוגמא של $L=L_1\otimes_F L_2$, כך ש־ L גלואה מעל L_1 ו־L_2 (ולכן גם מעל F), ו־ L_1 גלואה מעל F, אבל L_2 לא גלואה מעל F.

7.2.9 הרחבות ביניים שהן גלואה

תהי E/F הרחבת גלואה.

תרגיל 7.2.38 (+)** הראה שלכל $F\subseteq K\subseteq E$ קיים תת־שדה מינימלי M כך ש־ K/M גלואה; היינו, K/M' גלואה אם ורק אם $M\subseteq M'$.

תרגיל 7.2.39 (**) הוכח שאם K גלואה מעל L_1 ומעל L_2, אז K גלואה מעל $L_1\cap L_2$.

תרגיל 7.2.40 (**) נניח ש־ $F=L_1\cap L_2$. אם $L_1\otimes_F L_2$ הוא גלואה מעל L_1 ומעל L_2, הוכח ש־ $L_1\otimes_F L_2$ גלואה מעל F.

7.2.10 ההרחבה האבלית המקסימלית

משפט ([2]). תהי K/F הרחבת גלואה. אז קיים תת־שדה מקסימלי $F\subseteq L\subseteq K$ כך שחבורת גלואה $\mathrm{Gal}(L/F)$ אבלית (שדה זה נקרא ההרחבה האבלית המקסימלית של F בתוך K).

הדרכה. תהי $G=\mathrm{Gal}(K/F)$. הוכח ש־ $L=K^{G'}$ הוא השדה המבוקש (כאשר G' חבורת הקומוטטורים).

תרגיל 7.2.41 (+*) הוכח ש־ $Gal(L/F)=G/G'$.

תרגיל 7.2.42 (-)** מצא את ההרחבה האבלית המקסימלית של $\mathbb{Q}$ בתוך שדה הפיצול של x^4-7.

תרגיל 7.2.43 (-*)** ההרחבה האבלית המקסימלית של $\mathbb{Q}$ בתוך $L=\mathbb{Q}[3^{1/4},\rho_8]$ היא $\mathbb{Q}[\sqrt{-1},\sqrt{2},\sqrt{3}]$.

7.3 נורמה ועקבה

תהי K/F הרחבת גלואה, ותהי $G=\{\sigma_1,\dots,\sigma_n\}=\mathrm{Gal}(K/F)$ חבורת גלואה. (סדר האברים אינו חשוב).

7.3.1 תכונות יסוד

הגדרה 7.3.1 הנורמה - $N_{K/F}(\beta) = \sigma_1(\beta)\cdots\sigma_n(\beta)$.

תרגיל 7.3.2 (*) $N_{K/F}$ היא פונקציה שומרת כפל $K \to F$.

תרגיל 7.3.3 (*) אם $a \in F$, $N_{K/F}(a) = a^{[K:F]}$.

הגדרה 7.3.4 העקבה (*trace*) - $Tr_{K/F}(\beta) = \sigma_1(\beta) + \cdots + \sigma_n(\beta)$.

תרגיל 7.3.5 (*) $Tr_{K/F}$ היא פונקציה שומרת חיבור $K \to F$.

תרגיל 7.3.6 (*) אם $a \in F$, $N_{K/F}(a) = [K:F]\cdot a$.

תרגיל 7.3.7 (**) תהי $K = F[\alpha]/F$ הרחבת גלואה, כאשר הפולינום המינימלי של α הוא $f(\lambda) = \sum a_i\lambda^i$. הוכח ש- $Tr_{K/F}(\alpha) = -a_1$, $N_{K/F}(\alpha) = (-1)^n a_n$.

תרגיל 7.3.8 (*) יהי $d \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Q}$. הוכח ש- $N_{\mathbb{Q}[\sqrt{D}]/\mathbb{Q}}(a+b\sqrt{D}) = a^2 - Db^2$; $Tr_{\mathbb{Q}[\sqrt{D}]/\mathbb{Q}}(a+b\sqrt{D}) = 2a$.

תרגיל 7.3.9 (**) חשב במפורש את $N(a+b\alpha+c\alpha^2)$ עבור ההעתקה $N:[\rho_3],\alpha] \to [\rho_3]$, כאשר $\alpha = \sqrt[3]{6}$.

תרגיל 7.3.10 (**) חשב את $N_{[\rho_n]/}(\rho_n)$ ואת $Tr_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(\rho_n)$ עבור $n = 1,\dots,12$.

תרגיל 7.3.11 (-)** הוכח ש- $N_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(\rho_n) = 1$ לכל $2 < n$.

תרגיל 7.3.12 (***) הוכח ש- $\mu(n)= Tr_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(\rho_n)$ לכל n, כאשר μ היא פונקצית מביוס. הדרכה. הגדר $F(n) = \sum_{i=0}^{n-1}\rho^i$ ו- $f(n) = Tr(\rho_n)$. חשב את F והוכח ש- $F(n) = \sum_{d|n}^{f}(d)$.

תרגיל 7.3.13 (-*)** חשב את $N_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(1-\rho_n)$. הדרכה. הראה ש- $f(x) = \Phi_n(1-x)$ הוא הפולינום המינימלי של $1-\rho_n$, ולכן $N_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(1-\rho_n) = (-1)^{\phi(n)}f(0)$.

תרגיל 7.3.14 (-)** חשב את $N_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(1+\rho_n)$ כאשר n איזוגי. הדרכה. כתוב את $1+\rho_n$ כמנה.

תרגיל 7.3.15 (+*)** נניח ש- K/F הרחבת גלואה, וש- $K = F[a]$. הבחן שאם $Tr_{K/F}$ a)=0), אז הוקטורים $\sigma(a)_{\sigma\in Gal(K/F)}$ תלויים ליניארית מעל F. הראה שאם הוקטורים $\sigma(a)$ תלויים ליניארית ו- $Tr_{K/F}(a) \neq 0$, אז בכל צירוף $\sum \alpha_\sigma\cdot\sigma(a) = 0$ עם $\alpha_\sigma \in F$, מתקיים $\sum \alpha_\sigma = 0$.

תרגיל 7.3.16 (**) תהי K/F הרחבת גלואה. הראה ש- $x \mapsto tr(\alpha x)$ הוא פונקציונל ליניארי לכל $\alpha \in K$. הוכח ש- $tr(\alpha_1 x),\dots,tr(\alpha_k x)$ בת"ל אם $\alpha_1,\dots,\alpha_k$ בת"ל.

7.3.2 שימושים

תרגיל 7.3.17 (**) חשב את $\sqrt{30\sqrt{-6}-141}$ (כאיבר ב- $\mathbb{Q}[\sqrt{-6}]$).

פתרון. נניח ש- $30\sqrt{-6}-141=(a+b\sqrt{-6})^2$. נחשב נורמה בשני האגפים.

$$25281=141^2+6\cdot 30^2=N(30\sqrt{-6}-141)=N(a+b\sqrt{-6})^2$$

ולכן $159=\sqrt{25281}=a^2+6b^2$. אפשר להניח ש- $a,b\in$ (מדוע?). כעת $3|a^2$ ולכן $3|a$. נכתוב $a=3a_1$, אז $3a_1^2+2b^2=53$ ולפי בדיקה $(a_1,b)=(\pm 1,\pm 5)$. אכן, $(3+5\sqrt{-6})^2=30\sqrt{-6}-141$.

תרגיל 7.3.18 (**) חשב את $[\mathbb{Q}[\sqrt{1+\sqrt{2}}]:\mathbb{Q}]$.

תרגיל 7.3.19 (-*)** חשב את מימד שדה הפיצול של $\lambda^4-2\lambda^2+289$ מעל $\mathbb{Q}$.

תרגיל 7.3.20 (**) העזר בחישוב נורמה כדי למצוא את $\sqrt[3]{5-134\sqrt{-2}}$ בשדה $\mathbb{Q}[\sqrt{-2}]$.

תרגיל 7.3.21 (**) פתור את מערכת המשוואות $\{\, x^3-9xy^2=-260x^2y-y^3=21 \,\}$
.

הדרכה. זהה את הבעיה האמיתית.

תרגיל 7.3.22 (***) הוכח שהקבוצה $\in x^2-6xy+2y^2 : x,y$ סגורה לכפל (בדוק זאת על-ידי כמה דוגמאות).

הדרכה. מצא θ כך ש- $[\mathbb{Q}[\theta]:\mathbb{Q}]=2$, ו- $N_{[\theta]/}(x+y\theta)=x^2-6xy+2y^2$. הסבר מדוע זה עונה לשאלה (מהי התכונה שצריך לקיים θ ?).

תרגיל 7.3.23 (**) נתון ש- $13^2-6\cdot 13+6^2=107, 15^2-11\cdot 15+11^2=181$. מצא מספרים שלמים n,m כך ש- $n^2-nm+m^2=19367$. רמז. $107\cdot 181=19367$.

תרגיל 7.3.24 (-*)** הבע את $(3+2^{1/3}-6\cdot 2^{2/3})^{-1}$ כצירוף ליניארי מעל של $1,2^{1/3},2^{2/3}$.
הדרכה. עבוד בשדה $\mathbb{Q}[2^{1/3},\rho_3]$.

תרגיל 7.3.25 (-*)** נסמן $U_a=\sum_{j\equiv a(mod 3)}\frac{x^j}{j!}$. הוכח ש- $U_0^3+U_1^3+U_2^3-3U_0U_1U_2=1$. הדרכה. יהי $K=[\rho_3]((x))$ - השדה של טורי חזקות ב- x מעל השדה $[\rho_3]$. האוטומורפיזם $\sigma : x\mapsto \omega x$ מקיים $U_a\mapsto \rho^a U_a$, ו- $e^x=U_0+U_1+U_2$. חשב את $N_\sigma(U_0+U_1+U_2)$ בשתי דרכים.

7.3.3 עקבה בהרחבות ציקליות

הרחבת גלואה עם חבורת גלואה ציקלית נקראת הרחבה ציקלית.

תרגיל 7.3.26 (*) הראה שאם $Gal(K/F)$ ציקלית אז $Tr_{K/F}(\sigma(v)-v)=0$.

תרגיל 7.3.27 (-)** (משפט 90 של הילברט לעקבה). אם K/F הרחבה ציקלית עם $Gal(K/F)=\langle\sigma\rangle$, ו־ $Tr_{K/F}(u)=0$, אז קיים $v\in K$ כך ש־ $u=\sigma(v)-v$. ה דרכה. הלמה של $Artin$.

תרגיל 7.3.28 (***) (משפט $Artin-Schreier$). אם K/F הרחבה ציקלית ממימד p, $charF=p$, אז $K=F[\alpha]$ כאשר הפולינום המינימלי של α מהצורה $\lambda^p-\lambda-\theta=0, \theta\in F$. הדרכה. $Tr(1)=0$.

תרגיל 7.3.29 (**) הראה ש־ α כנ"ל הוא יחיד עד־כדי כפל ב־ $i\in\mathbb{Z}_p^*$ ותוספת של קבוע (איבר של F).

תרגיל 7.3.30 (-*)** K/F הרחבה ציקלית ממימד $p=charF$. נניח ש־ $K=F[\alpha]$ כאשר הפולינום המינימלי של α הוא $\lambda^p-a\lambda-b$. הראה ש־ $a^{1/(p-1)}\in F$. הדרכה. חשב את $(\sigma\alpha-\alpha)^p$.

7.3.4 נורמה בהרחבות ציקליות

תרגיל 7.3.31 (*) הראה שאם $Gal(K/F)=\langle\sigma\rangle$ אז $N_{K/F}(\frac{\sigma(v)}{v})=1$.

תרגיל 7.3.32 (***) (משפט 90 של הילברט). אם K/F הרחבה ציקלית עם $Gal(K/F)=\langle\sigma\rangle$, ו־ $N_{K/F}(u)=1$, אז קיים $v\in K$ כך ש־ $u=\sigma(v)v^{-1}$.
הדרכה. בחר $a_i=(u\dots\sigma^{i-1}(u))^{-1}$, ו־ $v=\sum a_i\sigma^i(y)$ עבור y כזה ש־ $v\neq 0$ (מדוע קיים?).

תרגיל 7.3.33 (**) יהי $\rho=\rho_p$, כאשר p ראשוני. הבחן שההרחבה $\mathbb{Q}[\rho_p]/\mathbb{Q}$ ציקלית; נסמן ב־ σ יוצר של חבורת גלואה. הראה ש־ $N_{\mathbb{Q}[\rho_n]/\mathbb{Q}}(\rho)=1$. מצא v כך ש־ $\sigma(v)=\rho v$.

תרגיל 7.3.34 (**) תהי K/F הרחבה ציקלית ממימד n, ויהי $a\in K^\times$. הראה ש־ $N(\frac{a^n}{N(a)})=1$, ומצא y כך ש־ $\frac{\sigma(y)}{y}=\frac{a^n}{N(a)}$.

תרגיל 7.3.35 (**) הוכח שהנורמה של כל איבר בהרחבה סופית של $\mathbb{Z}_2$ היא 1.

תרגיל 7.3.36 (***) $F\subseteq L\subseteq K$ שרשרת שדות, כך ש־ $Gal(K/F)=\langle\sigma\rangle$ מסדר nm, $\rho_m\in F$, $[K:L]=m$. הוכח ש־ ρ_m הוא נורמה ב־ L/F (כלומר ־ קיים $\mu\in L$ כך ש־ $N_{L/F}(\mu)=\rho_m$). **הדרכה.** לפי משפט $K=L[\alpha]$ עבור $\alpha\in K$ המקיים $\sigma^m(\alpha)=\rho_m\alpha$ (מדוע?). חשוב על $\sigma(\alpha)\alpha^{-1}$.

מסקנה. לא קיימת הרחבה $K/\mathbb{Q}$ ציקלית מסדר 4, עם תת־שדה $\mathbb{Q}[i]\subseteq K$.

תרגיל 7.3.37 (***) נסח והוכח את התרגיל לעיל במקרה $n=m=2$.

תרגיל 7.3.38 (***) תהי K/F הרחבה ציקלית ממימד n, ונניח ש־ $\rho_m \in F$. הוכח שעבור $a \in K$, השדה $K[\sqrt[m]{a}]$ הוא הרחבה ציקלית של F אם ורק אם $\sigma(a)a^{-1}$ הוא חזקת m ב־K.

נניח $n = m$. הוכח שעבור $a \in K$, השדה $K[\sqrt[m]{a}]$ הוא הרחבת גלואה עם החבורה $\mathbb{Z}/n \times \mathbb{Z}/n$ של F אם ורק אם $a \in F^{\times}K^{\times n}$.

תרגיל 7.3.39 (***) (לא ניתן להכליל את משפט 90 של $Hilbert$ להרחבות שאינן גלואה) . תהי K/F הרחבת גלואה, עם $\sigma \in G = Gal(K/F)$. תהי $H \leq G$ תת־חבורה כך ש־ $\langle H, \sigma\rangle = G$, ויהי $L = K^H$ השדה המתאים. יהי $a \in L$, עם $N_\sigma(a) = 1$ (הבחן שבדרך־כלל σ אינו אוטומורפיזם של $L : \sigma(K^H) = K^{\sigma H \sigma^{-1}}$). נניח שקיים $u \in L$ כך ש־ $a = \sigma(u)/u$. הוכח ש־ a שייך לתת־שדה של L שהוא נורמלי מעל F.

הדרכה. (משפט 90 של $Hilbert$ מבטיח שקיים $k \in K$ כך ש־ $a = \sigma(k)/k$). נסמן $H^\sigma = \langle \sigma^i H \sigma^{-i}\rangle$: תת־החבורה הנורמלית המינימלית של G המכילה את H, σ, ו־ L_0 =K$^{H^\sigma}$. הוכח ש־ $u \in L_0$, ואז ש־ $a \in L_0$.

פרק 8

שדות סופיים

8.1 תורת המבנה של שדות סופיים

8.1.1 קיום ויחידות

משפט (^{2j}). אם F שדה סופי אז $|F| = p^n$ כאשר $p = charF$ ראשוני.

תרגיל 8.1.1 (*) אם F שדה סופי אז כל $\alpha \in F$ הוא שורש של הפולינום $f(\lambda) = \lambda^{|F|} - \lambda$.

תרגיל 8.1.2 (**) אם F שדה סופי, $|F| = p^n$, אז F הוא שדה הפיצול של הפולינום $\lambda^{|F|} - \lambda$ מעל $\mathbb{Z}_p$.

משפט (^{2}). שדה הפיצול של $f(\lambda) = \lambda^{p^n} - \lambda$ מעל $\mathbb{Z}_p$ הוא שדה מסדר p^n.

הדרכה. יהי F שדה הפיצול. אוסף השורשים של $f(\lambda)$ הוא תת־שדה של F, שגודלו p^n.

הגדרה 8.1.3 את השדה מסדר $q = p^n$ נסמן ב־ $\mathbb{F}_q$.

8.1.2 הכלות

תרגיל 8.1.4 (*) אם $F \subseteq \mathbb{F}_{p^n}$, אז $F = \mathbb{F}_{p^m}$ כאשר $m|n$.

תרגיל 8.1.5 (**) נניח ש־ $m|n$.

א. $(p^m - 1)|(p^n$ ־1).

ב. $(\lambda^{p^m-1} - 1)|(\lambda^{p^n-1} - 1)$, ולכן גם $(\lambda^{p^m} - \lambda)|(\lambda^{p^n} - \lambda)$.

ג. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

הדרכה. הוכח $(t^m - 1)|(t^n - 1)$ והצב כדי להוכיח את סעיפים א,ב.

תרגיל 8.1.6 (*) רשום את סריג תת־השדות של $\mathbb{F}_{3^{24}}$.

8.2 אוטומורפיזם פרובניוס וחבורות גלואה

תרגיל 8.2.1 (**) יהי F שדה ממאפיין p (לאו דווקא סופי).

א. $F^p = a^p : a \in F$ תת־שדה של F.

ב. $a \mapsto a^p$ הוא איזומורפיזם $F \simeq F^p$.

ג. ההרחבה F/F^p אינה ספרבילית (אלא אם $F^p = F$).

ד. אם F סופי אז $F^p = F$.

תרגיל 8.2.2 (**) סגור אלגברי של שדה הוא אינסופי.

הגדרה 8.2.3 האוטומורפיזם של פרובניוס מוגדר על $\mathbb{F}_{p^n}$ לפי $\sigma : a \mapsto a^p$.

תרגיל 8.2.4 (+)** תת־השדה של $\mathbb{F}_{p^n}$ הקבוע על־ידי σ^m הוא מסדר p^m.

תרגיל 8.2.5 (*+) אם $m|n$, אז $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \sigma^m \rangle$, חבורה ציקלית מסדר $n/m = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$.

מסקנה ([1]). כל הרחבה של שדות סופיים היא הרחבת גלואה (עם חבורת גלואה ציקלית).

תרגיל 8.2.6 (**) אם $f(\lambda) \in \mathbb{F}_{p^m}$ איפריק, אז מימד שדה הפיצול מעל $\mathbb{F}_{p^m}$ הוא $\deg(f)$.

8.2.1 המבנה של שדה סופי

תרגיל 8.2.7 (*) $(\mathbb{F}_{p^n}, +) \simeq_p^n$.

תרגיל 8.2.8 (*) $(\mathbb{F}_{p^n})^*$ ציקלית מסדר $p^n - 1$.

תרגיל 8.2.9 (**) $F =_2 [\alpha | \alpha^3 = \alpha + 1]$ שדה מסדר 8. כתוב את לוח החיבור ולוח הכפל שלו.

תרגיל 8.2.10 (**) מצא את הפולינומים המינימליים מעל השדה הראשוני של כל האברים ב־ $\mathbb{F}_8, \mathbb{F}_{25}$.

תרגיל 8.2.11 (***) יהי $p \neq 2$ ראשוני.

א. $-1 \in \binom{*}{p}^2$ אם ורק אם $p \equiv 1(mod4)$.

ב. $2 \in \binom{*}{p}^2$ אם ורק אם $p \equiv \pm 1(mod8)$.

ג. $3 \in \binom{*}{p}^2$ אם ורק אם $p \equiv 1(mod6)$. הדרכה. חשוב על ρ_3.

ד. מצא את התנאים השקולים לכך ש־ $3, 6, -3, -6$ יהיו ריבועים בשדה $\mathbb{Z}_p$.

תרגיל 8.2.12 (**) n טבעי, p ראשוני. כמה שורשים יש לפולינום $x^n - 1$ מעל $\mathbb{Z}_p$?

תרגיל 8.2.13 (***) (דוגמא נגדית ל־ "אם $f(\lambda) \in \mathbb{Q}[\lambda]$ פריק מעל כל $\mathbb{Z}_p$, אז הוא פריק ב־ $\mathbb{Q}[\lambda]$) ": הוכח ש־ $\lambda^4 + 1$ איפריק מעל, אבל הוא פריק מעל כל $\mathbb{Z}_p$.

הדרכה. אם $p \neq 2$, אז ב־ $(\mathbb{F}_{p^2})^*$ קיים איבר מסדר 8.

?

8.3 פולינומים מעל שדות סופיים

8.3.1 פולינום מינימלי

תרגיל 8.3.1 (**) נסמן $f(\lambda) = \lambda^3 + \lambda^2 + 1$ מעל $\mathbb{Z}_2$.

א. $f(\lambda)$ איפריק מעל $\mathbb{Z}_2$.

ב. $K =_2 [\lambda]/\langle f\rangle$ שדה בן 8 אברים. נסמן $\alpha = \lambda + \langle f\rangle \in K$, כך ש־ $K = F[\alpha]$.

ג. מהם תת־השדות של K ? מצא יוצר לחבורה הכפלית K^*.

ד. מצא את השורשים של $f(\lambda)$ ב־ K ופצל את הפולינום.

ה. הוכח (בלי לחשב) שגם הפולינום $g(\lambda) = \lambda^3 + \lambda + 1$ מתפצל ב־ K, ואז מצא את השורשים שלו.

ו. $x^2 + x + 1$ איפריק מעל K (ולכן $K[\mu]/\langle \mu^2 + \mu + 1\rangle$ שדה מסדר 64).

ז. אם $(n, 3) = 1$, אז f איפריק מעל $\mathbb{F}_{2^n}$, ואם $3|n$ אז f מתפצל מעל $\mathbb{F}_{2^n}$.

תרגיל 8.3.2 (**) $K \supseteq \mathbb{Z}_3$, והפולינום המינימלי $f(\lambda)$ של $\alpha \in K$ מעל $\mathbb{Z}_3$ הוא מדרגה 6.

א. מצא את כל השורשים של f ב־ K.

ב. כתוב את הפולינום המינימלי של α מעל תת־השדה מסדר 3^2 ומעל תת־השדה מסדר 3^3.

ג. מה הפולינום המינימלי מעל $\mathbb{F}_{3^5}$? מעל $\mathbb{F}_{3^{10}}$?

תרגיל 8.3.3 (־*)** יהי $0 \neq a \in \mathbb{Z}_5$. נסמן $f(\lambda) = \lambda^4$ +a$\lambda - 1 \in \mathbb{Z}_5[\lambda]$.

א. הוכח ש־ $f(\lambda)$ איפריק.

ב. יהיו K שדה הפיצול של f מעל $_5$ (כך ש־ $|K| = 5^4$), ו־ $\alpha \in K$ שורש של f. מצא את כל השורשים.

ג. חשב את הפולינום המינימלי של α מעל השדה בגודל 5^2.

8.3.2 שורשי יחידה

תרגיל 8.3.4 (־)** יהיו p ראשוני ו־ n זר ל־p. הוכח שהשורשים של $\lambda^n - 1$ בשדה הפיצול מעל $\mathbb{Z}_p$ יוצרים שדה ממימד $ord_{U_n}(p)$. הסק שאם $F = \mathbb{F}_{p^\alpha}$, שדה הפיצול של $\lambda^n - 1$ מעל F הוא ממימד $\frac{s}{(s,\alpha)}$ מעל F , כאשר $s = ord_{U_n}(p)$.

תרגיל 8.3.5 (***) הפולינום $\Phi_n(x)$ איפריק מעל $\mathbb{F}_{p^\alpha}$ אם ורק אם p יוצר של החבורה הכפלית U_n ו־ $(\alpha, \phi(n)) = 1$.

הדרכה. התחל במקרה $\alpha = 1$. חשוב על השדה הנוצר על־ידי שורש של הפולינום.

תרגיל 8.3.6 (־)** הוכח שהפולינום $\frac{x^n-1}{x-1}$ איפריק מעל $\mathbb{F}_p$ אם ורק אם n ראשוני ו־p יוצר של החבורה הכפלית U_n.

תרגיל 8.3.7 (**) פרק לגורמים ראשוניים את $\Phi_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)}$ מעל השדות $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_9$, $\mathbb{F}_7$.

תרגיל 8.3.8 (**) הפולינום x^2+1 אי-פריק מעל $\mathbb{F}_p$ עבור $p=2^{17}-1$. יהי i שורש שלו. חשב את הסדר של $1\pm i$ בחבורה הכפלית של $\mathbb{F}_{p^2}$.

תרגיל 8.3.9 (-*)** (העזר ב) מסעיף. א. הראה שקיים שורש יחידה מסדר 13 בשדה הרחבה מתאים של $\mathbb{Z}_3$, המקיים $\rho^3=\rho^2+\rho+1$.
ב. הוכח שקיים שורש יחידה מסדר 7 באותו שדה, המקיים $\rho_{13}=\rho_7+\rho_7^{-1}$.

8.3.3 חישוב שדות פיצול

תרגיל 8.3.10 (*) הראה שבשדה הפיצול של λ^3-2 מעל $\mathbb{Z}_7$ יש 343 איברים.

תרגיל 8.3.11 (**) מצא שדה פיצול לפולינום $\lambda^{12}-1$ מעל $\mathbb{Z}_{19}$. מצא את כל שורשי הפולינום.

תרגיל 8.3.12 (**) מצא שדה פיצול של λ^6-3 מעל $\mathbb{Z}_5$. מהי מימדו מעל $\mathbb{Z}_5$?

תרגיל 8.3.13 (**) מצא את מימד שדה הפיצול של λ^6-8 מעל $\mathbb{Z}_{13}$. פצל את הפולינום, אם $\alpha^2=2$ בשדה הפיצול.

תרגיל 8.3.14 (**) יהי α שורש של $f(\lambda)=\lambda^3-2\lambda+1$ בשדה הפיצול מעל $\mathbb{Z}_3$. מצא את שאר השורשים.

8.3.4 הפולינומים האי-פריקים

תרגיל 8.3.15 (+*) פרק את $\lambda^8-\lambda$ לגורמים אי-פריקים מעל $\mathbb{Z}_2$.

תרגיל 8.3.16 (+*) פרק את $\lambda^{16}-\lambda$ לגורמים אי-פריקים מעל $\mathbb{Z}_2$.

תרגיל 8.3.17 (**) אם $f(\lambda)\in\mathbb{Z}_p[\lambda]$ אי-פריק ממעלה n, אז $f(\lambda)|(\lambda^{p^n}-\lambda)$.

תרגיל 8.3.18 (**) f גורם אי-פריק של $\lambda^{p^n}-\lambda$ מעל $\mathbb{Z}_p$ אם ורק אם $\deg(f)|n$.

תרגיל 8.3.19 (**) $\lambda^{p^n}-\lambda$ שווה למכפלת כל הפולינומים האי-פריקים מעל $\mathbb{Z}_p$ שמעלתם מחלקת את n.

תרגיל 8.3.20 (**) הסק מתכונות של $\lambda^{p^n}-\lambda$ שכל פולינום אי-פריק מעל שדה סופי הוא ספרבילי.

תרגיל 8.3.21 (-*)** $\alpha,2\alpha$ הם שורשים של פולינום אי-פריק f מעל $\mathbb{Z}_{31}$.
א. מצא את מעלת הפולינום.
ב. מצא את כל המקדמים של f, פרט ל- $f(0)$. הדרכה: התחל בחישוב $f(0)$.

תרגיל 8.3.22 (***) נניח ש- n הוא חזקת 2. הוכח שכל גורם אי-פריק של $f(x)=1+x^{n-1}+x^n$ מעל $\mathbb{Z}/2$, הוא ממעלה זוגית. [הדרכה. הראה ש- $(1+\alpha)^n=\frac{1}{1+\alpha}$ כאשר α שורש של הפולינום.]

8.3.5 ספירת פולינומים אי‍פריקים

תרגיל 8.3.23 (**) הראה שיש בדיוק $\frac{p^2-p}{2}$ פולינומים אי‍פריקים מתוקנים ממעלה 2 מעל $\mathbb{Z}_p$.

תרגיל 8.3.24 (***) נסמן ב־ $I_q(n)$ את מספר הפולינומים המתוקנים האי‍פריקים ממעלה n מעל $\mathbb{F}_q$. הוכח ש־ $I_q(n)=\frac{1}{n}\sum_{d|n}\frac{\mu(n}{d)}q^d$, כאשר μ פונקצית מביוס.

הדרכה. מספר האברים שלהם פולינום מינימלי מסדר n שווה ל־ $n\cdot I_q(n)$, ולפי מבנה תת־השדות $q^n=\sum_{d|n} d\cdot I_q(d)$. לפי נוסחת ההיפוך של מביוס, $n\cdot I_q(n) = \sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$.

תרגיל 8.3.25 (**) הראה שמספר הפולינומים המתוקנים האי‍פריקים ממעלה r, r ראשוני, מעל $\mathbb{F}_q$ הוא $\frac{q^r-q}{r}$.

תרגיל 8.3.26 (*) חשב את I_2 (n) עבור $n=2,3,4$.

תרגיל 8.3.27 (***) מצא, עבור כל ראשוני p, פולינום אי‍פריק ממעלה 2, ופולינום אי‍פריק ממעלה 3 מעל $\mathbb{Z}_p$.

תרגיל 8.3.28 (**) בנה במפורש שדה בן 625 אברים.

משפט ([2]). קיים פולינום אי‍פריק ממעלה n מעל $\mathbb{F}_q$ לכל $n, q=p^\alpha$ שלמים.

פתרון. $I_q(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d > \frac{1}{n}\left(q^n-\sum_{d|n,d<n}q^d\right) > \frac{1}{n}\left(q^n-n\cdot q^{n/2}\right) = \frac{q^{n/2}}{n}(q^{n/2}-n)$. אם $q>2$ אז $q>3^{2/3}\geq(n^{1/n})^2$. אחרת $q^{n/2}>n$ רק כאשר $n\geq 5$. עבור $n=2,3,4$ אפשר לחשב ישירות.

תרגיל 8.3.29 (+*)** הסיכוי של שני פולינומים אקראיים ממעלה $\leq n$ מעל $\mathbb{F}_q$ להיות זרים הוא $1-1/q$.

8.4 פירוק לגורמים מעל שדה סופי

בסעיף זה נציג אלגוריתם יעיל לפירוק פולינום f מעל שדה סופי לגורמיו הראשוניים. נאמר שפולינום הוא **אחיד** אם גורמיו האי‍פריקים שווי מעלה.

נקבע $F=\mathbb{F}_q$ ממאפיין p.

8.4.1 גורמים כפולים

תרגיל 8.4.1 (*) נניח ש־ $f=\sum a_i\lambda^i\in F[\lambda]$ ו־ $f'=0$. הראה ש־ $f=g^p$ עבור g יחיד והסבר כיצד למצוא אותו.

תרגיל 8.4.2 (*) אם $f=g^t$ כאשר $1<t$ ו־ $f'\neq 0$, אז (f,f') הוא גורם לא טריוויאלי של f.

תרגיל 8.4.3 (**) פרק לגורמים איפריקים את $f(\lambda) = \lambda^7 + \lambda^6 - \lambda^5 - \lambda^4 - \lambda^2 + \lambda - 1$ מעל $\mathbb{Z}_3$.

תרגיל 8.4.4 (**) פרק לגורמים איפריקים את $f(\lambda) = \lambda^5 + \lambda^4 + \lambda^3 + 3\lambda^2 - \lambda - 1$ מעל $\mathbb{Z}_5$.

8.4.2 פירוק לגורמים אחידים

תרגיל 8.4.5 (***) 1. מצא את הפולינום המינימלי המתוקן $f(x)$ של $\alpha = \sqrt{2} + \sqrt{3}$ מעל $\mathbb{Q}$. בדוק ש־ $f(x) \in \mathbb{Z}[x]$.

2. כתוב את הפירוק של f מעל כל תת־שדה של $K = \mathbb{Q}[\alpha]$.

3. הוכח ש־ $f(x)$ פריק מעל כל שדה סופי (הדרכה: מודולו כל מספר ראשוני, 2, 3 או 6 הוא שארית ריבועית).

האלגוריתם הכללי שיתואר בהמשך מפרק גם פולינומים שאינם אחידים, כך שבמובן מסויים הפירוק לגורמים אחידים מיותר. פירוק זה מוצג כאן בכל זאת משום שהוא פשוט יותר ומהיר יותר מן האלגוריתם הכללי.

נניח ש־ $f = f_1 \dots f_t$ הפירוק לגורמים איפריקים שונים של f מעל F.

תרגיל 8.4.6 (**) הראה ש־ $(\lambda^{p^m} - \lambda, f)$ שווה למכפלת הגורמים f_i ממעלה המחלקת את m.

תרגיל 8.4.7 (***) מצא דרך לחשב את הפירוק של f לגורמים אחידים, על־ידי חישוב $(\lambda^{p^m} - \lambda, f)$ עבור ערכי m שונים.

תרגיל 8.4.8 (**) הוכח ש־ $(\lambda^{p^n} - \lambda, \lambda^{p^m} - \lambda) = \lambda^{p^{(n,m)}} - \lambda$.

תרגיל 8.4.9 (***) פרק בצורה לא טריוויאלית את $f(\lambda) = \lambda^7 - 2\lambda^2 + 2$ מעל $\mathbb{Z}_7$. פתרון. $(f, \lambda^7 - \lambda) = 1$, ולכן אין ל־ f שורשים. $\lambda^{49} - \lambda \equiv (2\lambda^2 - 2)^7 - \lambda \equiv 2\lambda^{14} - 2 - \lambda \equiv 2(2\lambda^2 - 2)^2 - 2 - \lambda = \lambda^4 - 2\lambda^2 - \lambda - 1 \pmod{f(\lambda)}$ ובהמשך התהליך מגלים ש־ $gcd(f, \lambda^{49} - \lambda) = \lambda^2 - 3\lambda + 1$. זהו מחלק לא־טריוויאלי של f.

תרגיל 8.4.10 (**) פרק לגורמים אחידים את $\lambda^{11} + \lambda^{10} + \lambda^9 + \lambda^8 + \lambda^6 + \lambda^4 + \lambda^3 + 1$ מעל $\mathbb{Z}_2$.

משפט [3]. יהי $f(\lambda) \in F[\lambda]$ איפריק ממעלה n, כאשר F סופי. תהי K/F הרחבה ממימד m, $m|n$. אז f הוא אחיד מעל K : f שווה למכפלת m פולינומים איפריקים זרים מעל K, כולם ממעלה n/m.

הדרכה. יהי $f = g_1 \dots g_t$ הפירוק של f לגורמים איפריקים מעל K. יהיו L שדה הפיצול של f מעל F, ו־ L_i שדה הפיצול של g_i מעל K. יהי α_i שורש של g_i. הוכח ש־ $L_i \subseteq K[\alpha_i] \subseteq F[\alpha_i] = L \subseteq K[\alpha_i]$, ולכן L_i =L והמימד $[L_i : K] = deg(g_i)$ קבוע ושווה ל־ $\deg(f)/[K:F]$.

תרגיל 8.4.11 (**) בתנאי המשפט, מה קורה אם m אינו מחלק את n?

תרגיל 8.4.12 (***) יהי $f(x) \in \mathbb{F}_q[x]$ פולינום ממעלה המתחלקת ב־ m. הוכח ש־ f הוא נורמה של פולינום בהרחבה $\mathbb{F}_{q^m}(x)/\mathbb{F}_q(x)$.

תרגיל 8.4.13 (***) $\lambda^4+2\lambda+4$ אי־פריק מעל $\mathbb{Z}_5$. פרק את הפולינום מעל $\mathbb{F}_{25} = \mathbb{Z}_5[\sqrt{2}]$.

8.4.3 פירוק כללי לגורמים

נניח ש־ $f = f_1 \ldots f_t$ פירוק של f לגורמים שונים מעל $F = \mathbb{F}_q$.

תרגיל 8.4.14 (**) הראה ש־ $F[\lambda]/\langle f\rangle \simeq F[\lambda]/\langle f_1\rangle \times \ldots \times F[\lambda]/\langle f_t\rangle$ מכפלה של שדות.

הדרכה. הפולינומים f_i זרים בזוגות. העזר במשפט השאריות הסיני.

תרגיל 8.4.15 (**) ההעתקה $\sigma : \alpha \mapsto \alpha^q$ היא הומומורפיזם של $F[\lambda]/\langle f\rangle$ אל עצמו.

הגדרה 8.4.16 אם $a \in F$ אז $a + \langle f\rangle$ היא נקודת שבת טריוויאלית של σ.

תרגיל 8.4.17 (*) אם $t = 1$, אז נקודות השבת היחידות של σ הן טריוויאליות.

תרגיל 8.4.18 (-*)** מספר נקודות השבת של σ הוא בדיוק q^t.

תרגיל 8.4.19 (***) אם $(g + \langle f\rangle)^q = g + \langle f\rangle$ נקודת שבת לא־טריוויאלית, אז $f = \prod_{a\in F}(f, g-a)$ הוא פירוק לא טריוויאלי של f.

תרגיל 8.4.20 (**) פרק את הפולינום $f(\lambda) = \lambda^5 - \lambda^4 + \lambda - 1$ מעל $\mathbb{Z}_3$, בהנתן נקודת השבת $g = \lambda^3 + \lambda$.

תרגיל 8.4.21 (**) פרק את הפולינום $f(\lambda) = \lambda^8 + \lambda^4 + \lambda^2 + \lambda + 1$ מעל $\mathbb{Z}_2$, בהנתן נקודת השבת $g = \lambda^6 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2$.

תרגיל 8.4.22 (**) נניח ש־ $\deg(f) = n$. אפשר לחשב את המטריצה (a_{ij}) שעבורה $\lambda^{q^i} - \lambda^i \equiv \sum_{j=0}^{n-1} a_{ij}\lambda^j (mod f)$. הראה ש־ $g = \sum b_j\lambda^j$ היא נקודת שבת של σ אם ורק אם $(a_{ij}) \cdot (b_j) = 0$. הסק ש־ $rank(a_{ij}) = n - t$.

תרגיל 8.4.23 (**) פרק את $\lambda^{12} - 1$ לגורמים אי־פריקים מעל $\mathbb{Z}_5$ ומעל $\mathbb{Z}_5[\sqrt{2}]$. הדרכה. $\lambda^4 - 1 = (\lambda^{12} - 1, \lambda^5 - \lambda)$, וזו מכפלת הגורמים ממעלה 1. $\lambda^{25} - \lambda = \lambda(\lambda^{12} - 1)(\lambda^{12} + 1)$, ולכן כל הגורמים של $\lambda^{12} - 1$ הם ממעלה 1 או 2: ארבעה ממעלה 1, וארבעה ממעלה 2. לפי הפירוק הידוע של Φ_{12} מעל נשאר לפרק את $\lambda^4 - \lambda^2 + 1$ מעל $\mathbb{Z}_5$. שים לב שהפולינום מתפצל מעל $\mathbb{Z}_5[\sqrt{2}]$.

תרגיל 8.4.24 (**) מצא את נקודות השבת של σ עבור $f = \lambda^6 + \lambda^4 + \lambda + 1$ מעל $\mathbb{Z}_2$. העזר בהן כדי לפרק את f.

תרגיל 8.4.25 (**) מצא את נקודות השבת של σ עבור $f = \lambda^5 + \lambda^2 - \lambda + 1$ מעל $\mathbb{Z}_3$.

8.5 גאומטריה פרוייקטיבית

מכל שדה סופי אפשר לבנות גאומטריה פרוייקטיבית. בסעיף זה נציג את האקסיומות והמשפטים היסודיים, ונתאר את שיטת הבניה.

הגדרה 8.5.1 גאומטריה היא זוג סדור $(X, \bullet?)$, $\bullet Omega \subseteq P(X)$. אברי X נקראים נקודות, ואברי • Omega ישרים.

הגדרה. גאומטריה פרוייקטיבית היא גאומטריה המקיימת את האקסיומות הבאות:

(A1) (כל שני ישרים נחתכים).

(A2) (דרך כל שתי נקודות עובר ישר יחיד).

(A3) (אין שני ישרים המכסים את המישור X כולו).

תרגיל 8.5.2 (*) הוכח שכל שני ישרים נחתכים בנקודה אחת.

תרגיל 8.5.3 (+*) הוכח שהדוגמאות הבאות מקיימות את אקסיומות $(A1), (A2)$, אבל לא את $(A3)$:

משפט (^{2}). נניח ש־ X סופית. על כל שני ישרים יש אותו מספר נקודות (נאמר $n+1$).

משפט (^{2}). במקרה זה, דרך כל נקודה עוברים בדיוק $n+1$ ישרים.

תרגיל 8.5.4 (**) בגאומטריה פרוייקטיבית סופית יש n^2 +n+1 נקודות ו־ n^2 +n+1 ישרים.

תרגיל 8.5.5 (**) הוכח שהגאומטריה הפרוייקטיבית היחידה עם $n = 2$ היא הגאומטריה הבאה:

תרגיל 8.5.6 (***) צייר גאומטריה פרוייקטיבית עם $n = 3$.

תרגיל 8.5.7 (-)** יהי F שדה. הוכח שקבוצת תת־המרחבים ממימד 1 של F^3 כנקודות, עם קבוצת תת־המרחבים ממימד 2 של F^3 כישרים (ויחס החילה הרגיל) היא גאומטריה פרוייקטיבית. בדוק את קיום משפטי הספירה במקרה ש־ $q = |F|$.

פרק 9

הרחבות רדיקליות

9.1 חבורות פתירות

הגדרה. חבורה G היא פתירה אם קיימת שרשרת של תת־חבורות

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G,$$

כך ש־ G_{i+1}/G_i ציקלית מסדר ראשוני. שרשרת כזו נקראת סדרת הרכב.

תרגיל 9.1.1 (**) G פתירה אם ורק אם קיימת שרשרת כנ"ל עם מנות אבליות.

משפט ([3]). בכל סדרות ההרכב של חבורה G המנות G_{i+1}/G_i שוות עד־כדי החלפת סדר.

תרגיל 9.1.2 (**) מצא את כל סדרות ההרכב של S_4. חשב את מנות הסדרה.

משפט ([2]). אם $N \lhd G$, אז G פתירה אם ורק אם $N, G/N$ שתיהן פתירות.

תרגיל 9.1.3 (**) אם $H \leq G$ ו־ G פתירה, אז גם H פתירה.

תרגיל 9.1.4 (**) החבורות S_n, $n \leq 5$, אינן פתירות.

תרגיל 9.1.5 (**) הראה שתת־החבורות היחידות של S_5 שאינן פתירות הן A_5, S_5.

9.1.1 חבורת הקומוטטורים

הגדרה. G' ־ חבורת הקומוטטורים של G ־ היא תת־החבורה הנוצרת על־ידי האברים מהצורה $[a,b] = aba^{-1}b^{-1}$.

תרגיל 9.1.6 (**) $G' \lhd G$ ו־ G/G' אבלית.

תרגיל 9.1.7 (**) אם $\varphi : G \to A$ אפימורפיזם אז A אבלית אם ורק אם $G' \subseteq Ker(\varphi)$.

משפט ([2−]). G פתירה אם ורק אם הסדרה $\ldots \leq G^{(3)} \leq G" \leq G' \leq G$ מסתיימת ב־ $G^{(n)} = 1$.

9.2 הרחבות רדיקליות

הגדרה. הרחבה $F[\alpha]/F$, כאשר הפולינום המינימלי של α הוא $\lambda^n - a$, נקראת הרחבה שורשית.

בסעיף 2.4 ראינו שבהנתן שורשי יחידה מהסדר המתאים, אפשר לפצל פולינום ממעלה 3 או 4 על־ידי הוצאות שורש. כלומר, שדה הפיצול של פולינום ממעלה 3 או 4 הוא קצה של שרשרת הרחבות שורשיות הפותחת ב־ .

תרגיל 9.2.1 (**) אם $[K:F]=2$ ו־ $charF \neq 2$, אז ההרחבה שורשית. הראה שהטענה אינה נכונה אם מוותרים על $charF \neq 2$ (התבונן בשדות מסדרים $2,4$).

יהי n טבעי, ו־ F שדה ממאפיין זר ל־ n, עם שורשי יחידה מסדר n.

תרגיל 9.2.2 (**) תהי $F[\alpha]/F$ הרחבה שורשית. הוכח ש־ $Gal(E/F) \simeq_n$ (כלומר ־ ההרחבה ציקלית).

תרגיל 9.2.3 (־)** נניח ש־ $E \subseteq F$, $\alpha \in E$, $\alpha^n \in F$.

א. אם α^m ;$?F$ לכל $1 \le m < n$, אז $\lambda^n - \alpha^n$ איפריק מעל F.

ב. אם $[F[\alpha]:F]=n$, אז $\lambda^n - \alpha^n$ איפריק מעל F (ולכן ההרחבה $F[\alpha]/F$ שורשית).

הדרכה. לפי שורשים.

משפט ([3]). אם K/F הרחבה ציקלית מסדר n, אז K/F שורשית.

הדרכה. משפט 90 של $Hilbert$.

הגדרה. פולינום $f(\lambda) \in F[\lambda]$ הוא פתיר על־ידי רדיקלים א ם הוא מתפצל בשדה K, כך שקיימת שרשרת $F = K_0 \supset K_1 \supset \ldots \supset K_n = K$ שבה K_{i+1}/K_i שורשית.

משפט ([3]). פ ולינום $f(\lambda) \in F[\lambda]$ פתיר על־ידי רדיקלים אם ורק אם החבורה $Gal(f)$ פתירה.

9.2.1 פולינומים שאינם פתירים על־ידי רדיקלים

תרגיל 9.2.4 (**) אם p ראשוני, $\sigma \in S_p$ מסדר p ו־ $\tau = (ij)$ חילוף, אז $\langle \sigma, \tau \rangle = S_p$.

תרגיל 9.2.5 (**) אם לפולינום $f(\lambda) \in \mathbb{Q}[\lambda]$ יש בדיוק שני שורשים שאינם מרוכבים, אז $Gal(f)$ כוללת חילוף.

תרגיל 9.2.6 (**) אם $\deg(f)$ ראשוני, אז $Gal(f)$ כולל איבר מסדר $\deg(f)$.

תרגיל 9.2.7 (**) חבורת גלואה של הפולינום $f(\lambda) = \lambda^5$ ־10002 $+ \lambda$ היא החבורה הסימטרית S_5, ולכן f אינו פתיר על־ידי רדיקלים.

9.3 הדיסקרימיננטה

הגדרה. יהי $f(\lambda) \in F[\lambda]$ פולינום איפריק, עם שדה פיצול $K = F[\alpha_1, \ldots, \alpha_n]$, כאשר α_i השורשים של f. הדיסקרימיננטה של f מוגדרת כ־ $\Delta(f) = \prod_{i<j}{}^{(\alpha_i - \alpha_j)}$. נניח ש־ $charF \neq 2$.

תרגיל 9.3.1 (*) חשב את הדיסקרימיננטה של פולינום ממעלה שניה, $\Delta(a\lambda^2 + b\lambda + c)$.

תרגיל 9.3.2 (*) סדר השורשים אינו משנה את $\Delta(f)^2$.

תרגיל 9.3.3 (**) $\Delta(f)^2 \in F$. הדרכה: $\sigma(\Delta) = \pm\Delta$ לכל $\sigma \in Gal(K/F)$.

משפט ($^{2-}$). $Gal(K/F) \subseteq A_n$ אם ורק אם $\Delta(f) \in F$.

מסקנה (^{2}). יהיו $f(\lambda) \in F[\lambda]$ איפריק, $def(f) = 3$, K שדה הפיצול. $Gal(K/F) \simeq_3$ אם $\Delta(f) \in F$, ו־ $Gal(K/F) \simeq S_3$ אחרת.

תרגיל 9.3.4 (**) חשב את $\Delta(\lambda^3$ -גן.

9.3.1 חישוב הדיסקרימיננטה

נסמן

$$V(\alpha_1, \ldots, \alpha_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

- מטריצת van der monde של השורשים.

תרגיל 9.3.5 (**) $\Delta = |V(\alpha_1, \ldots, \alpha_n)|$.

נסמן $u_k = Tr(\alpha_1^k = \alpha_1^k + \ldots + \alpha_n^k$.

תרגיל 9.3.6 (*) $u_0 = n$.

תרגיל 9.3.7 (*) $u_k \in F$.

תרגיל 9.3.8 (**) הוכח ש־ $\Delta^2 = \left(u_{i+j} \right)_{i,j=0 \ldots n-1}$. הדרכה. חשב את VV^t.

אם נדע לחשב את $u_0, \ldots, u_{2n-2}$ נוכל לחשב את Δ^2.

נסמן $s_1 = \sum \alpha_i$, $s_2 = \sum_{i<j} \alpha_i \alpha_j$, ובאופן כללי $s_k = \sum_{i_1 < \ldots < i_k} \alpha_{i_1} \ldots \alpha_{i_k}$.

בפרט $s_n = \alpha_1 \ldots \alpha_n$, $s_0 = 1$.

תרגיל 9.3.9 (**) $f(\lambda) = (\lambda - \alpha_1) \ldots (\lambda - \alpha_n) = \lambda^n - s_1\lambda^{n-1} + s_2\lambda^{n-2} - \ldots + (-1)^n s_n$. כלומר - s_k מופיעים כמקדמים בפולינום. (בפרט $s_k \in F$).

זהויות ניוטון (^{3j}). $u_k = s_1u_{k-1} - s_2u_{k-2} + s_3u_{k-3} - \ldots + (-1)^k ks_k$
$s_1u_{k-1} - s_2u_{k-2} + s_3u_{k-3} - \ldots + (-1)^n s_n u_{k-n}$.
דוגמא. נניח $f(\lambda) = \lambda^2 + b\lambda + c$, $n = 2$. אז $s_0 = 1$, $s_1 = -b$, $s_2 = c$. לכן $u_0 = 2$, $u_1 = -b$, $u_2 = b^2 - 2c$. מכאן אפשר לחשב:

$$\Delta(f)^2 = \det\begin{pmatrix} u_0 & u_1 \\ u_1 & u_2 \end{pmatrix} = \det\begin{pmatrix} 2 & -b \\ -b & b^2-2c \end{pmatrix} = b^2 - 4c.$$

תרגיל 9.3.10 (**) הוכח שעבור $f(\lambda) = \lambda^3 - b\lambda + c$, $\Delta(f)^2 = 4b^3 - 27c^2$.

תרגיל 9.3.11 (***) הוכח שעבור $f(\lambda) = \lambda^4 + b\lambda^2 + c\lambda + d$, $\Delta(f)^2 = -4b^3d + b^2c^2 + 18bcd - 4c^3 - 27d^2$.

תרגיל 9.3.12 (***) יהיו $F = [\rho_n]$, $f(\lambda) = \lambda^n - 2$. נסמן $\alpha = 2^{1/n}$.

א. הוכח שעבור פולינום זה, $u_k = Tr(\alpha_i^k) = 0$ לכל $k? \equiv 0(modn)$, $u_0 = n$, $u_n = 2n$.

ב. הסק ש־ $\Delta^2 = |n \quad 0 \quad \ldots \quad 00 \quad 0 \quad \ldots \quad 2n \ldots \quad \ldots \quad \ldots \quad \ldots 0 \quad 2n \quad \ldots \quad 0| =$ $(-1)^{\binom{n}{2}}2^{n-1}n^n$.

ג. אם n איזוגי, אז $\sqrt{(-1)^{\binom{n}{2}}n} \in \mathbb{Q}[\rho_n]$. הדרכה. $\sqrt{(-1)^{\binom{n}{2}}n} \in F[\alpha]$, אבל $[F[\alpha] : F]$ איזוגי.

9.3.2 דיסקרימיננטה של פולינומים ציקלוטומיים

תרגיל 9.3.13 (**) חשב, לפי ההגדרה, את $\Delta(\Phi_5)$, את $\Delta(\Phi_{12})$ ואת $\Delta(\Phi_8)$.

תרגיל 9.3.14 (+**)** נסמן $\delta(n) = (-1)^{\binom{\varphi(n)}{2}}(\Delta(\Phi_n))^2$. הוכח את הנוסחאות הבאות.

1. לכל n,

$$\delta(n) = \prod_{i \in U_n, i \neq 1} \Phi_{n/(i-1,n)}(1)^{\varphi(n)/\varphi(n/(i-1,n))} = (-1)^{\varphi(n)/2} n^{\varphi(n)} / \prod_{p|n} p^{\varphi(n)/(p-1)}.$$

2. אם $n = p^\alpha$, $\delta(n) = p^{\alpha\cdot\varphi(n) - n/p}$.

3. אם n, m זרים, $\delta(nm) = \delta(n)^{\varphi(m)}\delta(m)^{\varphi(n)}$.

4. אם $n = P_1 \ldots P_t$ כאשר P_i זרים, אז $\delta(n) = \prod_{i=1..t}^{\delta}(P_i)^{\varphi(n/P_i)}$.

הדרכה. אפשר להוכיח את סעיפים ב,ג ישירות, ולהסיק מהם את סעיף א. אפשרות אחרת היא לחשב את $\delta(n) = \prod_{k \in U_n}\prod_{i \in U_n} i \neq 1(\rho^k - \rho^{ik})$ ישירות, בעזרת $\prod_{k \in U_n}(\lambda - (\rho_m)k(modm)) = \Phi_m(\lambda)^{\varphi(n)/\varphi(m)}$ ($m|n$). זכור ש־ $\Phi_m(1) =$ 1, אלא אם $m = p^\alpha$ שאז $\Phi_m(1) = p$.

תרגיל 9.3.15 (**) $\Delta(\Phi_n)\in\mathbb{Z}$, אלא אם $n=p^\alpha$ כאשר $p\neq 2$ ראשוני.

תרגיל 9.3.16 (**) $\sqrt{(-1)^{\frac{p-1}{2}}p}\in\mathbb{Z}[\rho_p]$.

9.3.3 פולינומים ממעלה 3

נתבונן בפולינום איפריק $f(\lambda)=\lambda^3+a\lambda+b\in F[\lambda]$, ששורשיו בשדה הפיצול K הם $\alpha_1,\alpha_2,\alpha_3$.

תרגיל 9.3.17 (-**) $K=F[\sqrt{D},\alpha_1]$.

תרגיל 9.3.18 (**) מצא את חבורת גלואה של $\lambda^3-\lambda-1$ מעל $\mathbb{Q}$ ומעל $\mathbb{Q}[\sqrt{-23}]$.

תרגיל 9.3.19 (-***) יהי α שורש של הפולינום $f(\lambda)=\lambda^3-5\lambda+2$. הצג את $\mathbb{Q}[\rho_3]$,$\mathbb{Q}[\alpha]/\mathbb{Q}[\rho_3]$ כהרחבה שורשית.

תרגיל 9.3.20 (-***) האם ההרחבה $\mathbb{R}(x)/\mathbb{R}(x^3-ax)$ יכולה להיות נורמלית? הוכח.

9.3.4 מקדמי פולינום ושורשיו

זוהי הכללה של נוסחאות ויאטה.

תרגיל 9.3.21 (**) נסמן את שורשי הפולינום $\lambda^3-14\lambda^2+6\lambda-9$ ב־ α,β,γ.

א. בנה פולינום מעל $\mathbb{Q}$, ששורשיו הם α^2, β^2,γ^2.
ב. בנה פולינום ששורשיו α^{-1}, β^{-1},γ^{-1}.
ג. בנה פולינום ששורשיו $\alpha+\beta,\beta+\gamma,\gamma+\alpha$.

תרגיל 9.3.22 (-**) $\sigma\in Gal(\mathbb{Q}[\theta]/\mathbb{Q})$ מעביר $\sigma:\theta\to 1-2\theta^2$, כאשר $\theta^3=a\theta+b$. חשב את a,b.

הדרכה. חשב את $Tr(\theta)$ בשתי דרכים.

תרגיל 9.3.23 (-***) יהי $f(x)$ פולינום ממשי ממעלה n שהמקדמים של x^{n-1},x^{n-2} בו הם אפס. הראה שהפולינום אינו יכול להתפצל מעל $\mathbb{R}$.

תרגיל 9.3.24 (***) חבורה $G\leq S_n$ פועלת על שדה הפונקציות $K=F(\alpha_1,\dots,\alpha_n)$ על־ידי חילוף אינדקסים. הוכח ש־ $Gal(K/K^G)\simeq G$, כך שכל חבורה סופית היא חבורת גלואה של איזשהו פולינום. בפרט S_n היא חבורת גלואה של $(\lambda-\alpha_1)\cdots(\lambda-\alpha_n)$ ומכיוון שאינה פתירה, לא קיים אלגוריתם הפותר פולינומים ממעלה n בעזרת פעולות של שדה והוצאות שורש, אם $5\leq n$.

9.3.5 שאלות נוספות

תרגיל 9.3.25 (***) (משה נוימן). נאמר ש־ E/F היא הרחבה שורשית חזקה (מסדר n), אם ההרחבה שורשית ו־ F כולל את שורשי היחידה מסדר n.

א. הוכח שכל הרחבה שורשית חזקה אפשר לעדן לשרשרת של הרחבות שורשיות חזקות מסדר ראשוני.

ב. נניח ש־ $E_0 \subset E_1 \subset \ldots \subset E_t$ שרשרת של הרחבות שורשיות חזקות, כך ש־ $E_0 = \mathbb{Q}$ ו־ $\rho_p \in E_t$. הוכח ש־ $[E_t : \mathbb{Q}]$ מתחלק ב־ p^*, כאשר p^* מוגדר כמכפלה המשותפת המינימלית של $q^\alpha \cdot q^*$ לכל חזקת ראשוני $q^\alpha | (p-1)$.
(למשל $2^* = 1, 5^* = 4, 11^* = [2,20] = 20, 89^* = [8 \cdot 2^*, 11 \cdot 11^*] = [8, 11 \cdot 20] = 440$).

ג. הראה ש־ $\mathbb{Q} \subset \mathbb{Q}[\rho_5]$ ניתנת לעידון לשרשרת של הרחבות שורשיות חזקות, אבל $\mathbb{Q} \subset \mathbb{Q}[\rho_{11}]$ לא.

ד. הראה שגם $\mathbb{Q} \subset \mathbb{Q}[\rho_7]$ לא ניתנת לעידון כזה, ומצא את מימד השדה המינימלי שמכיל את ρ_7 וכן ניתן לעידון מסוג זה.

פרק 10

בניות במחוגה וסרגל

10.1 בניות אלמנטריות

האקסיומות.

סרגל. בהנתן נקודות A, B, אפשר להעביר את הישר העובר דרכן.

מחוגה. בהנתן נקודות A, B, C, אפשר להעביר את המעגל שמרכזו A ורדיוסו $|BC|$.

חיתוך. בהנתן שני ישרים, ישר ומעגל, או שני מעגלים, הנחתכים, אפשר לסמן את נקודות החיתוך.

0 ו־ 1. נתונות שתי נקודות במישור, הקרויות 0 ו־ 1.

משפט (^{2}). במחוגה וסרגל אפשר:

א. להעלות אנך לישר l החוצה את הקטע AB שעל הישר.

ב. להקצות קטע באורך $|AB|$ על ישר l, שאחת מנקודות הקצה שלו היא $C \in l$.

ג. להוריד אנך לישר l, העובר דרך נקודה A שמחוץ לו.

ד. להעלות אנך לישר l העובר דרך נקודה A שעליו.

משפט (^{2}). בהנתן קטעים באורכים $1, x, y$, אפשר לבנות את הקטעים שאורכם $x^{-1}, x \cdot y, x + y$, $\sqrt{x}$.

תרגיל 10.1.1 (*) נתון קטע יחידה. בנה את הקטע שאורכו $\frac{1}{3+\sqrt{5}}$ ־ תאר במפורט את שלבי הבנייה.

תרגיל 10.1.2 (**) הראה כיצד לחצות זווית.

10.2 השדה של נקודות ניתנות לבניה

נזהה בין הנקודות במישור $\mathbb{R}^2$ לבין האברים של השדה המרוכב .

הגדרה. מספר $z \in$ ניתן לבניה אם אפשר לסמן את הנקודה המתאימה לו על־פי האקסיומות.

תרגיל 10.2.1 (**) הוכח שהמספר $z = x + iy$ ניתן לבניה אם ורק אם אפשר לבנות קטעים באורכים x, y.

משפט $(^{3})$. אם אפשר לבנות את $z, w \in$, אז אפשר לבנות גם את $z + w, z \cdot w, z^{-1}$, $\sqrt{z}$.

הערה. שים לב להבדל העקרוני בין ההוכחות כאן לבין ההוכחות במקרה של קטעים ממשיים.

מסקנה. אוסף האברים הניתנים לבניה של הוא תת־שדה, הסגור להוצאת שורש.

10.3 מספרים ניתנים לבניה

משפט $(^{2})$. $z \in$ ניתן לבניה אם ורק אם קיים תת־שדה $K \subseteq$ כך ש־ $z \in K$, וקיימת שרשרת של הרחבות ריבועיות $K = K_n \supset \ldots \supset K_1 \supset K_0 =$, $[K_{i+1} : K_i] = 2$.

הדרכה. חשוב על שלבי הבניה.

תרגיל $(^{1h})$. אם $\alpha \in$ ניתן לבניה, אז כל אברי $\mathbb{Q}[\alpha]$ ניתנים לבניה.

תרגיל $(^{2-})$. נניח ש־ $\alpha \in$ ניתן לבניה. המספר המינימלי של הוצאות שורש הדרוש לבניית α הוא n אם מימד ההרחבה $\mathbb{Q}[i][\alpha]/\mathbb{Q}[i]$ שווה ל־ 2^n.

הדרכה. ברור שמספר הוצאות השורש אינו יכול לרדת מ־ n. יהי $\alpha \in K$ שדה, כך שקיימת שרשרת הרחבות ריבועיות מ־ $[i]$ ל־ $K[i]$. חתוך את השרשרת עם $\mathbb{Q}[i, \alpha]$.

תרגיל 10.3.1 (**) כמה הוצאות שורש צריך כדי לבנות את $\alpha = \sqrt{3+\sqrt{2}} - \sqrt{3-\sqrt{2}}$?

תרגיל $(^{3j})$. מצא את חבורת גלואה של $\mathbb{Q}[\sqrt{3+\sqrt{2}}, \sqrt{3-\sqrt{2}}]/\mathbb{Q}$ ואת כל תת־השדות.

תרגיל 10.3.2 (**) אם K/F הרחבת גלואה ממימד $[K : F] = 2^n$, אז קיימת שרשרת של הרחבות ריבועיות מ־ F ל־ K.

הדרכה. כל חבורה מסדר 2^n היא נילפוטנטית (מספיק לדעת שיש לה מרכז לא־טריוויאלי).

תרגיל $(^{3j})$. נניח שחבורת גלואה של פולינום f מדרגה 4 היא S_4, ויהי α שורש של f. הראה ש־ α אינו ניתן לבניה (למרות ש־ $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$). דוגמא לאיבר כזה: $\alpha = \frac{1}{2}\left(\sqrt{-\frac{u^3+2}{u}} - u\right)$, כאשר $u = \sqrt{\sqrt[3]{\frac{2+\sqrt{2}}{4}} + \sqrt[3]{\frac{2-\sqrt{2}}{4}}}$, הוא בעל פולינום מינימלי $\alpha^4 - \alpha + \frac{3}{8} = 0$.

תרגיל 10.3.3 (***) יהי f הפולינום המינימלי של $\alpha \in$ שהוא ניתן לבניה.

א. כל האברים בשדה הפיצול של f ניתנים לבניה.

ב. חבורת גלואה של f היא מסדר 2^n.

ג. נניח ש־ α ניתן לבניה ב־ m הוצאות שורש. הוכח ש־ $n \leq 2^m - 1$.

תרגיל 10.3.4 (**) אם $[\mathbb{Q}[z] : \mathbb{Q}]$ אינו חזקה של 2, אז z אינו ניתן לבניה.

תרגיל 10.3.5 (**) יהי $f(\lambda) \in [\lambda]$ פולינום עם חבורת גלואה S_4, ויהי $\alpha \in$ שורש של f, כך ש־ $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$. הוכח ש־ α אינו ניתן לבניה.

הדרכה. לתת־החבורה היחידה מאינדקס 2 של S_4 אין תת־חבורות מאינדקס 2.

תרגיל 10.3.6 (**) הראה כיצד לבנות מחומש משוכלל.

משפט (*Bayer-Fluckiger, Parimala, 1995*). אם F/k ממימד חזקת־2, אז קיימת הרחבה L ממימד אי־זוגי של k כך ש־ FL/L ניתן לבניה (מאותו ממד).

10.4 הבעיות של ימי קדם

המתמטיקאים של יוון העתיקה השאירו אחריהם חמש שאלות פתוחות.

($A1$) מצא שליש של זווית נתונה.

($A2$) בנה קוביה שנפחה כפול משל קוביה נתונה.

($A3$) בנה מצולע משוכלל בן 7 צלעות.

($A4$) בנה ריבוע ששטחו שווה לזה של עיגול נתון.

($A5$) הוכח את אקסיומת המקבילים של אוקלידס בעזרת שאר האקסיומות (הנראות טבעיות יותר).

בתרגילים הבאים נראה שאת ארבע הבעיות הראשונות לא ניתן לפתור. את אי־התלות של אקסיומת המקבילים בשאר האקסיומות הוכיחו, באופן בלתי תלוי, בוליי, לובצ'בסקי וגאוס באמצע המאה ה־*19*, כשבנו גאומטריות לא־אוקלידיות.

תרגיל 10.4.1 (**) המספר $2^{1/3}$ אינו ניתן לבניה, ולכן בעיה ($A2$) אינה פתירה.

תרגיל 10.4.2 (*) ידוע ש־π אינו אלגברי מעל $\mathbb{Q}$. הוכח ש־ $\sqrt{\pi}$ אינו ניתן לבניה, ולכן בעיה ($A4$) אינה פתירה.

10.4.1 בניית זוויות

תרגיל 10.4.3 (*) אפשר לבנות זווית $\theta \Leftrightarrow e^{i\theta}$ ניתן לבניה $\Leftrightarrow$ אפשר לבנות את $\cos\theta$.

תרגיל 10.4.4 (**) הראה ש־ $\cos\theta$ הוא שורש של הפולינום $4\lambda^3 - 3\lambda - \cos(3\theta)$ מעל $\mathbb{Q}[\cos(3\theta)]$.

תרגיל 10.4.5 (***) נסמן $P_n(\lambda) = \sum_{j=0}^{[n/2]} \left((-1)^j \sum_{k=j}^{[n/2]} \binom{n}{2k}\binom{k}{j} \right) \lambda^{n-2j}$. הוכח ש־ $cos(n\theta) = P_n(cos\theta)$.

הדרכה. כללי דה־מואבר: $cos(n\theta) + i \cdot sin(n\theta) = e^{ni\theta} = (e^{i\theta})^n = (cos\theta + i \cdot sin\theta)^n$.

תרגיל 10.4.6 (***) הגדר פולינומים Q_n עבור $sin\theta$, ומצא נוסחאות רקורסיביות ל־ $(P_n(\lambda), Q_n(\mu))$.

תרגיל 10.4.7 (***) נסמן $T_1(x) = x$, $R_1(x) = 1$, $T_{n+1} = T_n + xR_n$, $R_{n+1} = R_n - xT_n$.

א. הוכח ש־ $tg(n\alpha) = T_n(tg\alpha)/R_n(tg\alpha)$.

ב. הראה ש־ $T_{n+1} + xR_{n+1} \equiv 2(T_n + xR_n) \pmod{x^2+1}$, ולכן x^2+1 אינו מחלק את $T_n + xR_n$.

ג. הוכח שהפולינומים T_n, R_n זרים.

ד. מצא פולינום רציונלי המתאפס ב־ $tg(°)$.

תרגיל 10.4.8 (*) בנה זווית של $60°$.

תרגיל 10.4.9 (**) מצא את הפולינום המינימלי של $cos(20°)$ מעל, והסק שהזווית $20°$ אינה ניתנת לבניה. בפרט, בעיה $(A1)$ אינה פתירה.

תרגיל 10.4.10 (**) מצא את הפולינום המינימלי של $cos(10°)$ מעל $\mathbb{Q}$.

תרגיל 10.4.11 (***) מצא את הפולינום המינימלי של $cos(18°)$ מעל $\mathbb{Q}$.

10.4.2 בניית מצולעים משוכללים

תרגיל 10.4.12 (*) אפשר לבנות מצולע משוכלל בן n צלעות $\Leftrightarrow$ ρ_n ניתן לבניה $\Leftrightarrow$ $\cos\left(\frac{2\pi}{n}\right)$ ניתן לבניה.

תרגיל 10.4.13 (**) א. אם ρ_n ניתן לבניה אז גם ρ_{2n} ניתן לבניה.

ב. אם ρ_n,ρ_m ניתנים לבניה, ו־ $(n,m) = 1$, אז גם ρ_{nm} ניתן לבניה.

ג. אם ρ_n ניתן לבניה ו־ $m|n$ אז גם ρ_m ניתן לבניה.

תרגיל (^{2}): כתוב שרשרת של הרחבות ריבועיות מ־ ל־ $[\rho_{15}]$.

תרגיל 10.4.14 (**) מצא את הפולינום המינימלי של ρ_7 והראה שלא ניתן לבנות מצולע משוכלל בן שבע צלעות. הסק שלא ניתן לבנות גם מצולע בן 14 צלעות.

תרגיל 10.4.15 (**) אפשר לבנות את ρ_p, p ראשוני, אם ורק אם $p = 2^m+1$.

תרגיל 10.4.16 (**) אם 2^m+1 ראשוני אז $m = 2^k$, כלומר, $p = 2^{2^k}+1$.

תרגיל 10.4.17 (**) אם $p^2 \mid n$ עבור ראשוני $p > 2$, אז לא ניתן לבנות את ρ_n. לכן המצולעים המשוכללים היחידים שניתן לבנות הם בני $n = 2^k p_1 \dots p_t$ צלעות, כאשר $p_1, \dots, p_t$ ראשוניים שונים, כולם מהצורה $F_k = 2^{2^k}+1$ (מספרי פרמה).

תרגיל 10.4.18 (**) הראה שאפשר לבנות מצולעים בעלי $3, 5, 17, 257, 65537$ צלעות. מצא עוד 26 מספרים אי־זוגיים בעלי תכונה זו.

תרגיל (^{3j}). הראה, ללא עזרת מחשב, ש־ $641|F_5$.

הערה. נכון ל־ 2006, לא ידועים מספרים ראשוניים מהצורה F_k פרט ל־ F_0, F_1, F_2, F_3, F_4. ידוע הפירוק לגורמים של $F_5, F_6, \ldots, F_{10}$, וידועים מחלקים של עוד כמה מספרי פרמה. על כמה מספרים ידוע שאינם ראשוניים למרות שלא ידוע מחלק שלהם.

תרגילים לא ממויינים.

תהי K/F הרחבה סופית. יהי E שדה המכיל את הסגור הנורמלי של K מעל F. סמן ב־ $[K:F]_s$ את מספר השיכונים של K ב־ E שצמצומם ל־ F הוא הזהות. הוכח ש־ K/F נורמלית אם ורק אם $|\mathrm{Gal}(K/F)| = [K:F]_s$.

(מכיוון שכל שיכון של K ב־ E שולח את K לסגור הנורמלי שלו, $[K:F]_s$ אינו תלוי בשדה E. אם K/F נורמלית אז K הוא הסגור הנורמלי של K מעל $F\ldots$)

חשב את המימדים הבאים. $[\mathbb{Q}[\sqrt{2}+\sqrt[3]{5}]:\mathbb{Q}]$, $[\mathbb{Q}[\sqrt{2},\sqrt[3]{5}]:\mathbb{Q}]$, $[\mathbb{Q}[\sqrt[3]{5}]:\mathbb{Q}]$, $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]$.

α מקיים את הפולינום המינימלי $f(x) = x^3+2x-6x+1$, ו־ $\beta = \alpha^2+3\alpha-7$. בטא את α כפולינום ממעלה 2 ב־ β.

הוכח. הפולינום $f(x) = x^3-3x+14$ איפריק מעל ובעל שורש ממשי אחד. יהי E שדה הפיצול של f. מה המימד $[E:\mathbb{Q}]$? מהי חבורת גלואה ?