TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES
הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

אלגברה ב׳ 2

מערכי שעור

תש"ף

נערך על ידי

דן הרן

תוכן העניינים

ספרות מומלצת

- S. Lang, *Algebra,* Third edition, Addison-Wesley
- הרשימות של משה ירדן http://www.math.tau.ac.il/~jarden/Courses/field.pdf
- אהוד דה שליט, אלכס לובוצקי, דורון פודר, *מבנים אלגבריים* של האוניברסיטה הפתוחה

מבוא

כידוע, למשוואה ממעלה שניה $X^2 + bX + c = 0$, באשר $a, b, c \in \mathbb{Q}$, $a \neq 0$, יש פתרונות מרוכבים, אשר ניתנים על ידי הנוסחה

$$x = \pm\frac{\sqrt{b^2 - 4ac}}{2a}.$$

נוסחאות דומות, מסובכות יותר, קיימות גם עבור משוואות ממעלה 3 ו־4, מאז המאה החמש־עשרה, ואולי אפילו לפני כן. נוסחאות אלו משתמשות, חוץ ממקדמים של המשוואה, רק בארבע פעולות החשבון ובפעולות $\sqrt[2]{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \ldots$. מאז שנודעו נוסחאות אלה חיפשו מתמטיקאים נוסחה למשוואה ממעלה חמישית, אך ללא הועיל.

מאידך גיסא, פיתחו מלומדים של יוון העתיקה את השיטה של בניות גיאומטריות בעזרת סרגל ומחוגה. אך בניות אחדות לא הצליחו לבצע בדרך זו, למשל לחלק זווית נתונה לשלוש זוויות שוות או לבנות מקוביה נתונה קוביה בעלת נפח כפול.

רק בשנת 1830 מצא מתמטיקאי צרפתי צעיר אֶבָריסט גַלואה (1811–1832) דרך להוכיח שאין ולא יכולה להיות נוסחה כללית לפתורן של משוואה ממעלה 5 ומעלה. השיטה הכללית שאת יסודותיה הוא הניח, נקראת היום **תורת גלואה**. היא גם יכולה להסביר איזה בניות ניתן לעשות בעזרת סרגל ומחוגה.

תורת גלואה ושני השימושים הנ"ל הם גולת הכותרת של קורס זה. ננסה להסביר בקצרה את הרעיון מאחורי תורה זו.

יהי $K \subseteq \mathbb{C}$ שדה. כאשר מצרפים ל־K את השורשים של משוואה נתונה ממעלה 5 עם מקדמים ב־K, מקבלים קבוצה שאיננה סגורה ביחס לארבע פעולות החשבון. אם נוסיף עוד איברים כך שהקבוצה תהיה סגורה ביחס לפעולות אלה, נקבל שדה L שמכיל את K. כדי לאפיין שדה כזה, נלמד בקורס רבות על תכונות שונות של **הרחבות של שדות** $K \subseteq L$.

באופן דומה, אם קיימת נוסחה לפתרון המשוואה, כמו הנוסחה לעיל, אשר מכילה רק את ארבע פעולות החשבון והוצאת שורש, אפשר להגדיר בעזרתה שדה אחר M שמכיל את K, נוצר על ידי הביטויים בנוסחה. גם לשדה זה יש תכונות מסוימות. אבל מתברר שלא כל שדה L מהפסקה הקודמת יש לו התכונות של שדות M מהפסקה הנוכחית. לכן יש משוואות להן אין נוסחה לפתרון.

באופן דומה אפשר לייחס שדות L לבעיות בניה בעזרת סרגל ומחוגה ושדות M שמאפיינים בניות כאלה. אם יש שדה L שאינו שייך למשפחה של שדות M כאלה, אז לבעית הבניה אין פתרון.

ומהן התכונות המאפיינות את השדות האלה? משייכים לשדות חבורות (של אוטומורפיזמים של השדות) ותכונות של החבורות מאפיינות את השדות. זוהי תורת גלואה על רגל אחת.

1. חוגים, שדות.

הגדרה 1.1: **חוג** הוא קבוצה R עם שתי פעולה בינריות אסוציאטיביות: חיבור $(+)$ וכפל ($\cdot$ או בלי סימן), כך ש־R הוא חבורה חלופית ביחס לחיבור ומתקיימים חוקי הפילוג:

$$a(b+c) = ab + ac \text{ לכל } a, b \in R,$$

$$(b+c)a = ba + ca \text{ לכל } a, b \in R.$$

חוג נקרא **חילופי** אם הכפל חילופי.

הוא נקרא חוג **עם יחידה** אם יש $1 \in R$ כך ש־$a1 = a = a1$ לכל $a \in R$. (איבר כזה הוא יחיד: אם גם $1' \in R$ יחידה אז $1' = 1' \cdot 1 = 1$.)

מעתה חוג הוא חוג עם יחידה.

דוגמאות 1.2: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}[\sqrt{5}]$, $\mathrm{M}_n(F)$, באשר F שדה, חוג האפס $0 = \{0\}$ (לא בהכרח $1 \neq 0$ בחוג; אך אם $1 = 0$ אז $R = 0$, לפי למה 1.3(א) להלן).

למה 1.3: *יהי R חוג, יהיו $a, b \in R$.*

(א) $a0 = 0 = 0a$.

(ב) $(-1)a = -a$.

תרגיל 1.4: *$R^\times = \{a \in R | \ \exists s \in R, as = sa = 1\}$ היא חבורה ביחס לכפל.*

תחום (**תחום שלמות**) *הוא חוג חילופי עם $1 \neq 0$ בו מתקיים: $a \neq 0, b \neq 0 \Leftarrow ab \neq 0$ לכל $a, b \in R$.*

שדה *F הוא חוג בו $F \setminus \{0\}$ חבורה חלופית ביחס לכפל. כלומר, F חוג חילופי עם יחידה $1 \neq 0$, וכל $0 \neq a \in F$ הפיך.*

הגדרה 1.6: העתקה $\varphi\colon R \to S$ של חוגים היא **הומומורפיזם** אם היא שומרת חיבור וכפל (בפרט $\varphi(0) = 0$) וגם $\varphi(1) = 1$. **אפימורפיזם** הוא הומומורפיזם ע ועל. **איזומורפיזם** הוא הומומורפיזם חח"ע ועל. קבוצה $R_0 \subseteq R$ היא **תת־חוג** של R אם היא סגורה ביחס לפעולות המושרות מ־R, הנגדי של כל איבר ב־R_0 נמצא ב־R_0, ו־$1 \in R_0$.

תת־חוג של חוג הוא חוג בעצמו, ביחס לפעולות המושרות מ־R.

דוגמה 1.7:

(א) $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ הנתונה על ידי $k \mapsto [k]$ היא אפימורפיזם.

הערה 1.8: (א) יהי $\varphi_0\colon R_0 \to S$ הומומורפיזם. אז $S_0 = \varphi(R_0)$ הוא תת־חוג של S.

(ב) יהי S_0 תת חוג־של חוג S ויהי $\varphi_0\colon R_0 \to S_0$ איזומורפיזם. אז אפשר למצוא חוג R כך ש־R_0 הוא תת־חוג שלו ולהרחיב את φ_0 לאיזומורפיזם $\varphi\colon R \to S$.

דוגמה 1.9: חוג פולינומים (במשתנה אחד) מעל חוג כלשהו R (לא בהכרח חילופי):

$$R[X] = \{a_0X^0 + a_1X^2 + a_2X^2 + \ldots \mid 0 \text{ כמעט כולם } ,a_0, a_1, a_2, \ldots \in R\}$$

עם החיבור $\left(\sum_{i=0}^{\infty} a_iX^i\right) + \left(\sum_{i=0}^{\infty} b_iX^i\right) = \sum_{i=0}^{\infty}(a_i + b_i)X^i$
והכפל $\left(\sum_{i=0}^{\infty} a_iX^i\right)\left(\sum_{j=0}^{\infty} b_jX^j\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_ib_j\right)X^k$.

זהו חוג; $0 = \sum_{i=0}^{\infty} 0X^i$, (ו־$X = 1X^1$ וכו'). נכתוב a במקום aX^0; אז $R \subseteq R[X]$ תת־חוג.

המעלה של $f = \sum_i a_iX^i \in R[X]$: $\deg 0 = -\infty$, אם $f \neq 0$ אז $\deg f = \max\{i \mid a_i \neq 0\}$.

מתקיים $\deg(f + g) \le \max\{\deg f, \deg g\}$, $\deg(fg) \le \deg f + \deg g$, ויש שוויון אם R תחום.

באופן כללי יותר, מגדירים פולינומים במשפחה $\{X_i \mid i \in I\}$ של משתנים מעל חוג כלשהו R: תחילה נגדיר את קבוצת המונומים במשפחה זו

$$\mathcal{M} = \left\{\prod_{i\in I} X_i^{n_i} \mid \text{ שלמים, כמעט כולם אפס } n_i \ge 0\right\}$$

עם הכפל $\prod_{i\in I} X_i^{n_i} \cdot \prod_{i\in I} X_i^{n'_i} = \prod_{i\in I} X_i^{n_i+n'_i}$ עליה. ואז נגדיר

$$R[X_i \mid i \in I] = \left\{\sum_{M\in\mathcal{M}} a_M M \mid \text{ כמעט כולם אפס } ,a_M \in R\right\}$$

עם החיבור $\sum_{M\in\mathcal{M}} a_M M + \sum_{M\in\mathcal{M}} b_M M = \sum_{M\in\mathcal{M}}(a_M + b_M)M$ והכפל מושרה מהכפל על $\mathcal{M}$, כך שמתקיים חוק הפילוג. ∎

דוגמה 1.10: יהי R חוג חילופי, $a \in R$. **ההצבה** $R[X] \to R$ על ידי $f \mapsto f(a)$ היא הומומורפיזם (היחיד שהינו זהות על R ו־$X \mapsto a$).

הגדרה 1.11: יהי R חוג. תת־קבוצה I של R נקראת **אידאל** אם היא אינה ריקה, הינה סגורה תחת החיבור ו־$ax, xa \in I$ לכל $a \in R, x \in I$. (כל אידאל הוא תת חוג ללא יחידה ובפרט מכיל את 0 וסגור תחת הנגדי.)

דוגמאות 1.12: הגרעין של הומומורפיזם $\varphi\colon R \to S$ של חוגים; $2\mathbb{Z} \subseteq \mathbb{Z}$; $0, R \subseteq R$. אם R חילופי, $x \in R$, אז $(x) := \{ax \mid a \in R\}$ אידאל, שנקרא **ראשי**. זהו האידאל הקטן ביותר של R אשר מכיל את x. אם $I_1, I_2 \subseteq R$ שני אידאלים ו־$c \in R$ אז גם $I_1 \cap I_2$, $I_1 + I_2 = \{x_1 + x_2 \mid x_1 \in I_1,\ x_2 \in I_2\}$, $I_1I_2 = \{\sum x_iy_j \mid x_i \in I_1,\ y_j \in I_2\}$, $cI = \{cx \mid x \in I\}$ הם אידאלים (האחרון עבור R חילופי). אידאל I של R נקרא **נָאוֹת** אם $I \neq R$. זה שקול לכך ש־I אינו מכיל הפיכים וגם לכך ש־$1 \notin I$. ∎

תרגיל 1.13: *יהי R חוג חילופי. אז R שדה אם ורק אם $R \neq 0$ ו־$0, R$ הם האידאלים היחידים של R.*

יהי I אידאל של חוג R. נגדיר על חבורת המנה R/I חיבור וכפל, לפי המייצגים: $[a] + [b] = [a + b]$, $[a][b] = [ab]$. החיבור מוגדר טוב (כפי שלומדים בתורת החבורות). הכפל מוגדר טוב: אם $[a] = [a']$, $[b] = [b']$, אז $a - a', b - b' \in I$, לכן $ab - a'b' = (a - a')b + a'(b - b') \in I$, לכן $[ab] = [a'b']$.

משפט 1.14: *R/I הוא חוג וההעתקה $\pi\colon R \to R/I$ הנתונה על ידי $a \mapsto [a]$ היא הומומורפיזם של חוגים.*

הוכחה: לפי תורת החבורות, R/I הוא חבורה חילופית ביחס לחיבור, ו־π הומומורפיזם של חבורות. מתקיים $\pi(ab) = \pi(a)\pi(b)$. מכאן קל להסיק שהכפל ב־R/I אסוציאטיבי, $\pi(1) = [1]$ הוא איבר היחידה של R/I, מתקיים הפילוג ו־π הומומורפיזם חוגים. ∎

משפט 1.15: *יהי $\varphi\colon R \to S$ הומומורפיזם של חוגים. יהי $I \subseteq \operatorname{Ker}\varphi$ אידאל של R. אז קיים הומומורפיזם יחיד $\bar{\varphi}\colon R/I \to S$ כך ש־$\varphi = \bar{\varphi} \circ \pi$. יתר על כך, $\bar{\varphi}$ חח"ע אם $I = \operatorname{Ker}\varphi$; $\bar{\varphi}$ על אם φ על.*

הוכחה: משפט זה ידוע מתורת החבורות עבור חבורות. לכן רק נותר להוכיח כי $\bar{\varphi}$ שומר גם כפל ו־$\bar{\varphi}([1]) = 1$. ואכן,

$$\bar{\varphi}([a][b]) =\bar{\varphi}(\pi(a)\pi(b)) = \bar{\varphi}(\pi(ab)) = \varphi(ab) = \varphi(a)\varphi(b) =$$
$$= \bar{\varphi}(\pi(a))\bar{\varphi}(\pi(b)) = \bar{\varphi}([a])\bar{\varphi}([b])$$

ו־$\bar{\varphi}([1]) = \bar{\varphi}(\pi(1)) = \varphi(1) = 1$. ∎

תרגיל 1.16: *$J \mapsto \pi^{-1}(J)$ היא התאמה חח"ע מקבוצת האידאלים של R/I על קבוצת האידאלים של R שמכילים את I.*

מעתה יהי R חוג קומוטטיבי ויהי I אידאל שלו.

הגדרה 1.17: (א) I **מְרַבִּי** אם $I \neq R$ ואין אידאל בין I ל־R.

(ב) I **ראשוני** אם $I \neq R$ ולכל $a, b \in R$ מתקיים $ab \in I \Leftarrow a \in I$ או $b \in I$.

למה 1.18: *(א) האידאל I הינו מרבי אם ורק אם R/I שדה.*

(ב) *האידאל I הינו ראשוני אם ורק אם R/I תחום.*

הוכחה: (א) תרגילים 1.13, 1.16.

(ב) מההגדרות. ∎

מסקנה 1.19: *אידאל מרבי הינו ראשוני.*

תרגיל 1.20: *הוכח את המסקנה הקודמת ישירות, ללא חוגי המנה.*

שדה המנות של תחום:

יהי R חוג חלקי של שדה F. אז R תחום ו־

$$K = \left\{ \frac{a}{b} \,\middle|\, a, b \in R,\ b \neq 0 \right\}$$

הינו שדה, אשר מכיל את R כתת־חוג והינו מוכל בכל תת־שדה F' של F אשר מכיל את R.

כעת יהי R תחום. נמצא שדה K כך ש־$R \subseteq K$.

(1) הגדר יחס על $R \times (R \setminus \{0\})$: $(a,b) \equiv (a',b')$ אם ורק אם $ab' = a'b$.

(2) הוכח כי $\equiv$ הוא יחס שקילות. תהי K קבוצת המנה. כתוב $\frac{a}{b}$ עבור המחלקה $[(a,b)]$.

(3) הגדר חיבור וכפל על K.

(4) הוכח שהפעולות האלה מוגדרות היטב.

(5) הוכח ש־K הוא שדה ביחס לפעולות אלה.

(6) הוכח ש־$R \to K$ המוגדרת על ידי $a \mapsto \frac{a}{1}$ הוא הומומורפיזם חח"ע.

(7) השתמש בהערה 1.8 כדי לזהות R עם תת־חוג של K.

דוגמה 1.21: יהי R תחום. אז $R[X]$ תחום. שדה המנות שלו הוא $\left\{\frac{f(X)}{g(X)} \mid f,g \in R[X],\ g \neq 0\right\}$ שדה הפונקציות הרציונליות מעל שדה מנות של R.

תרגיל 1.22: *הראה כי* $R[X,Y] \cong R[X][Y]$.

2. פריקות בתחומים.

בפרק זה יהי R תחום.

הנוסחה $\deg(fg)=\deg(f)+\deg(g)$ מבטיחה ש־$R[X]$ תחום.

טענה 2.1 (כלל הצמצום): *יהיו $a,b,p\in R$ כך ש־$0\neq p\in R$ ו־$pa=pb$. אז $a=b$.*

הוכחה: מתקיים $p(a-b)=pa-pb=0$, $p\neq 0$. לכן $a-b=0$. ∎

הגדרה 2.2: תחום R נקרא **ראשי** (PID) אם כל אידאל ב־R ראשי.

משפט 2.3: *יהי F שדה. אז $F[X]$ תחום ראשי.*

הוכחה: תזכורת – **חילוק עם שארית:** יהיו $f,g\in F[X]$, $g\neq 0$. אז יש $r,q\in F[X]$ יחידים כך ש־

$$f=gq+r,\qquad \deg r<\deg g. \tag{1}$$

יהי $0\neq I$ אידאל ב־$F[X]$. נבחר $0\neq g\in I$ ממעלה מזערית. אז $(g)\subseteq I$. נראה הכלה הפוכה. יהי $f\in I$. לפי (1), $r=f-gq\in I$, לכן ממזעריות המעלה $r=0$. לכן $f=gq\in(g)$. ∎

תרגיל 2.4: *הוכח (באופן דומה) כי $\mathbb{Z}$ תחום ראשי.*

הגדרה 2.5: יהיו $a,b\in R$.

(א) $a\mid b$ אם יש $u\in R$ כך ש־$b=au$ (אם $a\neq 0$, אז u כזה יחיד, לפי כלל הצמצום). בפרט:

(ב) a הפיך אם $a\mid 1$.

(ג) a **ראשוני** אם $a\neq 0$, a אינו הפיך ו־$a\mid a_1a_2 \Leftarrow a\mid a_2$ או $a\mid a_1$.

(ד) a **אי פריק** אם $a\neq 0$, a אינו הפיך ו־$a=a_1a_2 \Leftarrow a_2$ הפיך או a_1 הפיך .

באופן שקול:

(א') $a\mid b$ אם ורק אם $b\in(a)$ אם ורק אם $(b)\subseteq(a)$.

(ב') a הפיך אם ורק אם $(a)=R$.

(ג') a ראשוני אם ורק אם $(a)\neq 0$ אידאל ראשוני.

(ד') a אי פריק אם ורק אם (a) מרבי במשפחת האידאלים $\{(b)|\ 0\neq(b)\neq R,\ b\in R\}$. ∎

(ד) $\Leftrightarrow$ (ד'): (ד) $\Leftrightarrow$ $(a)\neq 0$, $(a)\neq R$, ואם $a=a_1a_2$, $a_2\notin R^\times$ אז $a_1\in R^\times$ $\Leftrightarrow$ (לפי (1) מטה) $R\neq(a)\neq 0$ ואם $(a)\subsetneqq(a_1)$ אז $(a_1)=R$ $\Leftrightarrow$ (ד').

מסקנה 2.6: *יהיו $0\neq a,b\in R$.*

(1) $(a)=(b)\Leftrightarrow a\mid b,\ b\mid a\Leftrightarrow b=au$, *כאשר* $u\in R^\times$. *בפרט* $(a)\subsetneqq(b)\Leftrightarrow b=au,\ u\in R\setminus R^\times$.

(2) *אם $u\in R^\times$ אז au מקיים (א)־(ד) לעיל אם ורק אם a מקיים אותם.*

(3) *אם a ראשוני אז a אי פריק.*

(4) *יהי R תחום ראשי. אז (a) מרבי $\Leftrightarrow$ a אי פריק $\Leftrightarrow$ a ראשוני $\Leftrightarrow$ (a) ראשוני.*

(5) *היחס $a \sim b$ שמוגדר על ידי $(a) = (b)$ הוא יחס שקילות על האיברים האי פריקים.*

הוכחה:

(1) נראה כי $b = au \Leftarrow a \mid b,\ b \mid a$, באשר $u \in R^\times$: לפי (א) יש $u, v \in R$ כך ש־$b = au$, $a = bv$. לכן $a = a(uv)$. מכאן $uv = 1$, כלומר, $u \in R^\times$.

(3) נניח $a = a_1a_2$. אז $a \mid a_1a_2$, לכן, למשל, $a \mid a_1$. אבל גם $a_1 \mid a_1a_2 = a$. לפי (1), $a = a_1u$, באשר $u \in R^\times$. לפי כלל הצמצום $a_2 = u \in R^\times$.

(4) אם R ראשי, אז (ד') נותן את השקילות הראשונה; האחרונה היא (ג'). האמצעית נובעת מ־(3) ומסקנה 1.19.

∎

לפי (5) לעיל אפשר לבחור מערכת מייצגים $\{p_i\}_{i \in I}$. למשל, אם $R = F[X]$, באשר F שדה, אז $R^\times = F^\times = F \smallsetminus \{0\}$, ונקח $\{p_i\}_{i \in I}$ להיות הפולינומים האי פריקים המתוקנים.

הגדרה 2.7: תהי $\{p_i\}_{i \in I}$ מערכת מייצגים של איברים אי פריקים ב־R. יהי $0 \neq a \in R$.

(א) **פירוק** של a היא הצגה $a = u \prod_{i \in I} p_i^{m_i}$, בה $u \in R^\times$ ו־$\{m_i\}_{i \in I}$ שלמים אי שליליים, כמעט כולם 0.

(ב) R הוא **תחום פריקות** (UFD) אם לכל $0 \neq a \in R$ קים פירוק אחד ויחיד. ∎

תרגיל 2.8:

(א) *ההגדרה של תחום פריקות אינה תלויה בבחירת המייצגים $\{p_i\}_{i \in I}$.*

(ב) *אם R תחום פריקות אז a אי פריק אם ורק אם a ראשוני.*

משפט 2.9: *יהי R תחום ראשי. אז R תחום פריקות.*

הוכחה:

קיום פירוק: נקרא ל־$0 \neq a \in R$ **טוב** אם יש לו פירוק, ואחרת נקרא לו **<u>רע</u>**. נראה שכל $0 \neq a \in R$ טוב.

אם a אי פריק אז הוא טוב: יש $j \in I$ ו־$u \in R^\times$ כך ש־$a = up_j^1 \prod_{i \neq j} p_i^0$, וזהו פירוק של a.

יהי a_0 רע. לפי הפסקה הקודמת יש $a_1, a_1' \in R \smallsetminus R^\times$ כך ש־$a_0 = a_1a_1'$. לא יתכן ש־a_1, a_1' שניהם טובים, כי אז מכפלת פירוקיהם נותנת פירוק של a_0. בלי הגבלת הכלליות a_1 רע. לפי מסקנה 2.6(1) מתקיים $(a_0) \subsetneqq (a_1)$. באינדוקציה קיימת סדרה אינסופית של רעים $a_0, a_1, a_2, \ldots$ כך ש־$(a_0) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots$. קל לבדוק ש־$\bigcup_j (a_j)$ הוא אידאל של R. כיוון ש־R ראשי, יש $b \in R$ כך ש־$\bigcup_j (a_j) = (b)$. אז $b \in \bigcup_j (a_j)$ לכן יש j כך ש־$b \in (a_j)$. מכאן $(b) \subseteq \cdots \subsetneqq (a_{j+1}) \subsetneqq (a_j) \subseteq (b)$, סתירה. לכן לכל $0 \neq a \in R$ יש פירוק.

טענה: *יהי $a = u \prod_{i \in I} p_i^{m_i}$ פירוק. אז $p_j \mid a$ אם ורק אם $m_j \geq 1$.* אכן, נניח $p_j \mid a = u \prod_{i \in I,\ m_i \geq 1} p_i^{m_i}$. לפי מסקנה 2.6(4), p_j ראשוני. לכן p_j מחלק אחד הגורמים שמופיע באגף ימין. ודאי לא $p_j \mid u$ כי $p_j \notin R^\times$, לכן יש $i \in I$ כך ש־$m_i \geq 1$ ו־$p_j \mid p_i$. אז $p_i = p_jv$ עבור איזה $v \in R$. אבל p_i אי פריק, $p_j \notin R^\times$, לכן $v \in R^\times$. לכן $p_i \sim p_j$, ומכאן $i = j$, לפי בחירת I. מכאן $m_j \geq 1$.

להיפך, אם $m_j \geq 1$ אז p_j מופיע כגורם באגף ימין של פירוק, לכן מחלק את אגף שמאל.

יחידות פירוק: נניח

$$u\prod_{i\in I} p_i^{m_i} = a = v\prod_{i\in I} p_i^{n_i} \tag{3}$$

באשר $u, v \in R^\times$, $m_i, n_i \geq 0$, כמעט כולם 0. נקבע $j \in I$ ונראה $m_j = n_j$ באינדוקציה על m_j. אם $m_j = 0$, לפי הטענה גם $n_j = 0$. אם $m_j \geq 1$, לפי הטענה גם $n_j \geq 1$; אז חילוק (3) ב־p_j נותן

$$u\prod_{\substack{i\in I\\ i\neq j}} p_i^{m_i} p_j^{m_j-1} = v\prod_{\substack{i\in I\\ i\neq j}} p_i^{n_i} p_j^{n_j-1},$$

ולפי הנחת האידוקציה $m_j - 1 = n_j - 1$. לכן $m_j = n_j$.

אם כך, $\prod_{i\in I} p_i^{m_i} = \prod_{i\in I} p_i^{n_i}$. חילוק (3) בביטוי זה נותן $u = v$. ∎

מסקנה 2.10: *יהי F שדה. אז $F[X]$ ו־$\mathbb{Z}$ תחומי פריקות.*

תרגיל 2.11: *יהי R תחום פריקות. יהיו $b = v\prod_{i\in I} p_i^{n_i}$, $a = u\prod_{i\in I} p_i^{m_i}$ פירוקים. אז $a \mid b$ אם ורק אם $m_i \leq n_i$ לכל $i \in I$.*

הערה 2.12: יהיו $a_1, \ldots, a_n \in R$. אז $(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n) = \{\sum_{i=1}^n a_i b_i | \ b_i \in R\}$ הוא האידאל הקטן ביותר של R אשר מכיל את $a_1, \ldots, a_n$. (ז.א., מכיל אותם ומוכל בכל אידאל שמכיל אותם.) ∎

הגדרה 2.13: איבר $d \in R$ הוא **מחלק משותף גדול ביותר** של $a_1, \ldots, a_n \in R$ (ונכתוב $d \in \gcd(a_1, \ldots, a_n)$) אם: (1) $d \mid a_1, \ldots, a_n$; (2) ואם $d' \in R$ כך ש־$d' \mid a_1, \ldots, a_n$ אז $d' \mid d$.

ניסוח שקול: $a_1, \ldots, a_n \in (d)$, ואם $a_1, \ldots, a_n \in (d')$ אז $(d) \subseteq (d')$.

כלומר: (d), אם הוא קיים, הוא האידאל הראשי הקטן ביותר שמכיל את $(a_1, \ldots, a_n)$. ∎

למה 2.14: *יהיו $d, d', a_1, \ldots, a_n \in R$.*

(א) *אם $k < n$ אז $\gcd(a_1, \ldots, a_k, 0 \ldots, 0) = \gcd(a_1, \ldots, a_k)$ ו־$\gcd(0, \ldots, 0) = \{0\}$.*

(ב) *אם $d \in \gcd(a_1, \ldots, a_n)$ אז $d' \in \gcd(a_1, \ldots, a_n)$ אם ורק אם $(d) = (d')$.*

(ג) *אם R תחום פריקות, אז $\gcd(a_1, \ldots, a_n) \neq \emptyset$.*

ביתר דיוק, אם $a_j = u_j \prod_{i\in I} p_i^{n_{ij}}$, אז $d = \prod_{i\in I} p_i^{\min_j(n_{ij})} \in \gcd(a_1, \ldots, a_n)$.

(ד) *אם R תחום פריקות ו־$c \in R$, אז $\gcd(ca_1, \ldots, ca_n) = c\gcd(a_1, \ldots, a_n)$.*

(ה) *אם R תחום ראשי אז $d \in \gcd(a_1, \ldots, a_n)$ אם ורק אם $(d) = (a_1, \ldots, a_n)$.*

(ו) *אם R תחום ראשי ו־$d \in \gcd(a_1, \ldots, a_n)$ אז יש $b_1, \ldots, b_n \in R$ כך ש־$d = \sum_i a_i b_i$.*

הוכחה: (א) ברור.

כדי להוכיח את יתר הסעיפים, לפי (א) אפשר להניח כי $a_j \neq 0$ לכל j.

(ב) נובע מהניסוח בעזרת האידאלים.

(ג) לפי תרגיל 2.11.

(ד) בסימונים של (ג) יהי $c = v\prod_{i\in I} p_i^{m_i}$ הפירוק של c. אז $ca_j = vu_j\prod_{i\in I} p_i^{m_i+n_{ij}}$ הפירוק של ca_j. לכן לפי (ג),

$$cd = v\prod_{i\in I} p_i^{m_i+\min_j(n_{ij})} = v\prod_{i\in I} p_i^{\min_j(m_i+n_{ij})} \in \gcd(ca_1,\dots,ca_n).$$

(ה),(ו) $(d) = (a_1,\dots,a_n) = (a_1)+\dots+(a_n) = \{\sum_j a_jb_j \mid b_j \in R\}$. ∎

הערה 2.15: האלגוריתם של אוקלידס נותן את המקדמים b_j במקרה $n=2$. ∎

מעתה יהי R תחום פריקות. יהי F שדה המנות שלו. נחקור את $R[X]$.

הגדרה 2.16: פולינום $f = \sum_i a_iX^i \in R[X]$ נקרא **פרימיטיבי** אם $1 \in \gcd(a_0,a_1,\dots)$. כלומר, לפי למה 2.14(ג), לכל $p \in R$ אי פריק יש i כך ש־$p \nmid a_i$. (אם f פרימיטיבי ו־$c \in R^\times$ אז cf פרימיטיבי.) ∎

למה 2.17: *מכפלה של פולינומים פרימיטיביים היא פולינום פרימיטיבי.*

הוכחה: יהיו $f = \sum_i a_iX^i, g = \sum_j b_jX^j \in R[X]$ פרימיטיביים, ויהיו $fg = \sum_k c_kX^k$. יהי $p \in R$ אי פריק. אז יש a_i, b_j כך ש־$p \nmid a_i, b_j$; נבחר כאלה בעלי האידקסים (i,j) הקטנים ביותר. לפי תרגיל 2.8(ב), p ראשוני, ולכן $p \nmid a_ib_j$. כעת

$$c_{i+j} = (a_0b_{i+j}+\dots+a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1}+\dots+a_{i+j}b_0)$$

אינו מתחלק ב־p, כי המחובר האמצעי אינו כפולה של p ושני האחרים הינם כפולות של p. ∎

למה 2.18: *יהי* $0 \neq f(X) = \sum_i a_iX^i \in F[X]$.

(א) *קיימים* $c \in F^\times$ *ו־* $p(X) \in R[X]$ *פרימיטיבי כך ש־* $f = cp$.

(ב) *אם גם* $f = c'p'$, *באשר* $c' \in F^\times$ *ו־* $p'(X) \in R[X]$ *פרימיטיבי אז* $c'/c \in R^\times$.

(ג) *נניח כי* $f \in R[X]$ *ויהי* c *כמו ב־(א). אז* $c \in R$. *ביתר דיוק,* $c \in \gcd(a_0,a_1,\dots)$.

הוכחה: (א) יש $0 \neq a \in R$ כך ש־$af \in R[X]$. בפרט $a \in F^\times$. לכן בלי הגבלת הכלליות $f \in R[X]$. יהי $c \in \gcd(a_0,a_1,\dots)$. לפי למה 2.14(ד), $1 \in \gcd(\frac{a_0}{c},\frac{a_1}{c},\dots)$, לכן $p = \frac{a_0}{c} + \frac{a_1}{c}X + \dots \in R[X]$ פרימיטיבי. מתקיים $f = cp$.

(ב) אם $cp = c'p'$, צריך להוכיח כי $\frac{c'}{c} \in R^\times$. בלי הגבלת הכלליות $c, c' \in R$. נקח gcd של המקדמים של שני האגפים ונקבל $(c) = (c')$, ולכן $\frac{c'}{c} \in R^\times$, לפי מסקנה 2.6(1).

(ג) הוכחנו ב־(א) שאפשר לבחור $c \in \gcd(a_0,a_1,\dots) \subseteq R$. לפי (ב), בחירה אחרת c' מקיימת $\frac{c'}{c} \in R^\times$, לכן גם $c' = (\frac{c'}{c})c \in R$, ואפילו $(c) = (c')$. בפרט, $c' \in \gcd(a_0,a_1,\dots)$. ∎

מסקנה 2.19 (הלמה של גאוס): *יהיו $f_1, f_2 \in F[X]$ מתוקנים כך ש־$f_1 f_2 \in R[X]$. אז $f_1, f_2 \in R[X]$.*

הוכחה: נכתוב $f_i = c_i^{-1} p_i$, באשר $c_i \in F^\times$ ו־$p_i \in R[X]$ פרימיטיבי. כיוון ש־f_i מתוקן, c_i המקדם העליון של p_i. לכן $c_i \in R$. מתקיים $f_1 f_2 = (c_1 c_2)^{-1}(p_1 p_2)$. לפי למה 2.17, $p_1 p_2$ פרימיטיבי, לכן לפי למה 2.18(ג), $(c_1 c_2)^{-1} \in R$. לכן $c_1 c_2 \in R^\times$. מכאן $c_1, c_2 \in R^\times$, ולכן $f_1, f_2 \in R[X]$. ∎

למה 2.20: *(א)* $(R[X])^\times = R^\times$.

(ב) *יהי $0 \neq a \in R$. אז a אי פריק ב־$R[X]$ אם ורק אם a אי פריק ב־R.*

(ג) *יהי $f \in R[X]$ ממעלה ≥ 1. אז f אי פריק ב־$R[X]$ אם ורק אם f פרימיטיבי ואי פריק ב־$F[X]$.*

הוכחה: קודם נוכיח

טענה: *יהיו $0 \neq a \in R$, $f_1, f_2 \in R[X]$ כך ש־$a = f_1 f_2$. אז $f_1, f_2 \in R \setminus \{0\}$.*

אכן, $f_i \neq 0$ לכן $\deg f_i \geq 0$. אבל $\deg f_1 + \deg f_2 = \deg(a) = 0$, לכן $\deg f_i = 0$, $i = 1, 2$.

(א) לפי הטענה עם $a = 1$, $(R[X])^\times \subseteq R^\times$. ההכלה ההפוכה ברורה.

(ב) נניח $a = f_1 f_2$. אם $f_i \in R$ אז גם $f_i \in R[X]$. להיפך, אם $f_i \in R[X]$ אז, לפי הטענה, $f_i \in R$. לפי (א), $f_i \in R^\times \Leftrightarrow f_i \in (R[X])^\times$. מכאן המסקנה.

(ג) נניח כי f אי פריק ב־$R[X]$. לפי למה 2.18(ג), $f = cp$ באשר $0 \neq c \in R$, $p \in R[X]$ פרימיטיבי. כיוון ש־p אינו הפיך ב־$R[X]$, בהכרח c הפיך, כלומר, $c \in (R[X])^\times = R^\times$. לכן f פרימיטיבי.

יהיו $f_1, f_2 \in F[X]$ כך ש־$f = f_1 f_2$. אז $f_i = c_i p_i$ באשר $c_i \in F^\times$, $p_i \in R[X]$ פרימיטיבי, $i = 1, 2$. כעת $f = c_1 c_2 p_1 p_2$, ו־$p_1 p_2$ פרימיטיבי לפי למה 2.17, לכן $c_1 c_2 \in R$, לפי למה 2.18(ג). כיוון ש־f אי פריק ב־$R[X]$ ו־$\deg(p_1 p_2) \geq 1$, $c_1 c_2 \in R^\times$. כיוון ש־f אי פריק ב־$R[X]$, גם $p_1 p_2$ כזה. לכן p_1 (או p_2) הפיך ב־$R[X]$. בפרט הוא הפיך ב־$F[X]$. מכאן ש־$f_1 = c_1 p_1$ הפיך ב־$F[X]$.

להיפך, נניח כי $f \in R[X]$ פרימיטיבי ואי פריק ב־$F[X]$. יהיו $f_1, f_2 \in R[X]$ כך ש־$f = f_1 f_2$. אז, למשל, f_1 הפיך ב־$F[X]$, כלומר, $\deg f_1 = 0$. אז $f_1 \in R$ והוא מחלק את המקדמים של f ב־R. אך f פרימיטיבי, לכן $f_1 \in R^\times$. לכן f אי פריק ב־$R[X]$. ∎

משפט 2.21: *אם R תחום פריקות אז $R[X]$ תחום פריקות.*

הוכחה: תהי $\{r_i\}_{i \in I}$ מערכת מייצגים של איברים אי פריקים ב־R ותהי $\{f_j\}_{j \in J}$ קבוצת הפולינומים האי פריקים המתוקנים ב־$F[X]$ ממעלה ≥ 1. אז לכל $j \in J$ יש $c_j \in F^\times$ ו־$p_j \in R[X]$ פרימיטיבי כך ש־$f_j = c_j p_j$. נקבע אותם.

טענה: $\Gamma = \{r_i\}_{i \in I} \cup \{p_j\}_{j \in J}$ היא מערכת מייצגים של איברים אי פריקים ב־$R[X]$.

צריך להוכיח שלכל $f \in R[X]$ אי פריק יש $g \in \Gamma$ יחיד כך ש־$f = ug$ עבור איזה $u \in (R[X])^\times = R^\times$.

זה ברור אם $\deg f = 0$, כלומר, אם $f \in R$. אם $\deg f > 0$ אז

(1) $f \neq u r_i$ לכל $i \in I$ ולכל $u \in R^\times$.

(2) f אי פריק ב־$F[X]$, לכן יש $j \in J$ ו־$c \in F^{\times}$ כך ש־$f = cf_j$. אז $f = up_j$, באשר $u = cc_j \in F^{\times}$. אך גם f וגם p_j פרימיטיביים, לכן $u \in R^{\times}$. יתר על כן, j כזה הוא יחיד: אם $f = up_j$, באשר $u \in R^{\times}$, $j \in J$, אז $f = uc_j^{-1} f_j$, באשר $uc_j^{-1} \in F^{\times}$, ויש j יחיד כזה.

בכך הוכחה הטענה.

יהי $0 \neq f \in R[X]$. כיוון ש־$F[X]$ הוא תחום פריקות, לכל $j \in J$ יש $m_j \geq 0$ יחיד (וכמעט כולם אפס) ו־$c \in F^{\times}$, כך ש־$f = c \prod_{j \in J} f_j^{m_j}$. אז $f = c' \prod_{j \in J} p_j^{m_j}$, באשר $c' = \prod_{j \in J} c_j^{m_j} c \in F^{\times}$. אבל $\prod_{j \in J} p_j^{m_j}$ פרימיטיבי, לכן לפי למה 2.18(ג), $c' \in R$. כמובן, $c' \neq 0$. לכן לכל $i \in I$ יש $n_i \geq 0$ יחיד (וכמעט כולם אפס) כך ש־$c' = u \prod_{i \in I} r_i^{n_i}$ עבור איזה $u \in R^{\times}$. לכן יש $n_i, m_j \geq 0$ יחידים כך ש־$f = u \prod_{i \in I} r_i^{n_i} \prod_{j \in J} p_j^{m_j}$ עבור איזה $u \in R^{\times}$. ∎

מסקנה 2.22: *אם R תחום פריקות, אז $R[X_1, \ldots, X_n]$ תחום פריקות.*

הוכחה: באינדוקציה על n, כיוון ש־ $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ∎

תרגיל 2.23: *יהי F שדה. הראה שתחום הפריקות $F[X_1, X_2]$ אינו חוג ראשי.*

תרגיל 2.24 (בוחן איזנשטיין): *יהי R תחום פריקות ויהי F שדה המנות שלו. יהי $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ממעלה n ונניח שיש ראשוני $p \in R$ כך ש־ $p \nmid a_n$, $p \mid a_i$, עבור $0 \leq i < n$, ו־$p^2 \nmid a_0$. אז f אי פריק ב־$F[X]$.*

3. פולינומים סימטריים

יהי A חוג חילופי עם יחידה ויהי $R = A[X_1, \dots, X_n]$.

החבורה הסימטרית S_n פועלת על R באופן הבא:

$$\sigma\Big(\sum_{m=(m_1,\dots,m_n)} a_m X_1^{m_1} \cdots X_n^{m_n} \Big) = \sum_{m=(m_1,\dots,m_n)} a_m \, X_{\sigma(1)}^{m_1} \cdots X_{\sigma(n)}^{m_n}.$$

כלומר, אם $\sigma, \tau \in S_n$ ו־$f \in R$ אז $\sigma\big(\tau(f)\big) = (\sigma\tau)(f)$ ו־$1(f) = f$.

הגדרה 3.1: פולינום $f \in R$ נקרא **סימטרי** אם $\sigma(f) = f$ לכל $\sigma \in S_n$.

הערה 3.2: (א) יהי $\sigma \in S_n$. ההעתקה $f \mapsto \sigma(f)$ היא הומומורפיזם $R \to R$. היא אפילו אוטומורפיזם, כי יש לה העתקה הפוכה, $f \mapsto \sigma^{-1}(f)$.

(ב) קבוצת הפולינומים הסימטריים היא תת־חוג של R אשר מכיל את A.

דוגמה 3.3: (א) הפולינומים הבאים סימטריים; נקראים **הפולינומים הסימטריים היסודיים**.

$$s_1 = \sum_i X_i,$$
$$s_2 = \sum_{i<j} X_i X_j = \sum_{\substack{\{i,j\} \\ |\{i,j\}|=2}} X_i X_j,$$
$$s_3 = \sum_{i<j<k} X_i X_j X_k = \sum_{\substack{\{i,j,k\} \\ |\{i,j,k\}|=3}} X_i X_j X_k,$$
$$\dots$$
$$s_n = X_1 X_2 \cdots X_n.$$

(ב) הפולינומים $X_1^m + \cdots + X_n^m$, $\prod_{i<j} (X_i - X_j)^2$ הם סימטריים.

(ג) פולינום קבוע הוא סימטרי. סכום ומכפלה של פולינומים סימטריים הוא פולינום סימטרי. באופן כללי יותר: יהי $g \in R$ כלשהו, אז $g(s_1, \dots, s_n)$ פולינום סימטרי. ∎

הערה 3.4: יהיו $\alpha_1, \dots, \alpha_n \in A$. אז

$$(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) =$$
$$X^n - s_1(\alpha_1, \dots, \alpha_n) X^{n-1} + s_2(\alpha_1, \dots, \alpha_n) X^{n-2} + \cdots + (-1)^n s_n(\alpha_1, \dots, \alpha_n).$$

הגדרה 3.5: יהי $f \in R$. נגדיר **מעלה** $\deg(f)$ **ומשקל** $w(f)$ של f: אם $0 \neq a \in A$,

$$\deg(a X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n}) = m_1 + m_2 + \cdots + m_n$$
$$w(a X_1^{m_1} X_2^{m_2} \cdots X_n^{m_n}) = m_1 + 2m_2 + \cdots + n m_n$$

ואם $f \neq 0$, המעלה $\deg(f)$ (המשקל $w(f)$) של f הוא מקסימום המעלות (המשקלים) של המונומים שונים מ־0 של f. לבסוף, $w(0) = \deg(0) = -\infty$.

הערה 3.6: הגדרות אלה אינן תלויות ב־n: אם $n \leq N$, אז $A[X_1, \dots, X_N] \supseteq A[X_1, \dots, X_n] = R \ni f$; אבל $\deg(f)$ ו־$w(f)$ אינם תלויים ב־n, N. ∎

טענה 3.7: *יהי* $g \in R$. *אז* $\deg g(s_1, \dots, s_n) \leq w(g)$.

הוכחה: כל מונום $a_m X_1^{m_1} \cdots X_n^{m_n}$ ב־g (עם $a_m \neq 0$) מקיים $m_1 + 2m_2 + \cdots + nm_n \leq w(g)$. אבל $a_m s_1^{m_1} \cdots s_n^{m_n}$ הוא סכום של מונומים ממעלה $m_1 + 2m_2 + \cdots + nm_n \leq w(g)$, ו־$g(s_1, \dots, s_n)$ הוא סכום של כל המונומים האלה כאשר עוברים על כל המונומים של g. ∎

משפט 3.8: *יהי* $f \in R$ *סימטרי ממעלה* d. *אז יש* $g \in R$ *כך ש־*$w(g) \leq d$ *ו־*$f = g(s_1, \dots, s_n)$.

הוכחה: באינדוקציה על n. עבור $n = 1$ נקח $g = f$, כי $s_1 = X_1$. אז $w(g) = \deg g = d$.

נניח כי המשפט נכון עבור $n - 1$ משתנים. נסמן $R_0 = A[X_1, \dots, X_{n-1}] \subseteq R$. לכל $f \in R$ נגדיר $(f)_0 = f(X_1, \dots, X_{n-1}, 0) \in R_0$. כלומר, אם $f = \sum_m a_m X_1^{m_1} \cdots X_{n-1}^{m_{n-1}} X_n^{m_n}$ אז $(f)_0 = \sum_{\substack{m \\ m_n=0}} a_m X_1^{m_1} \cdots X_{n-1}^{m_{n-1}}$. מתקיים (בדוק!)

(א) $f \mapsto (f)_0$ הוא הומומורפיזם חוגים $R \to R_0$.

(ב) $\big(\sigma(f)\big)_0 = \sigma\big((f)_0\big)$ לכל $\sigma \in S_{n-1} \subseteq S_n$ (החבורה S_{n-1} פועלת על אברי R_0).

(ג) אם $f \in R$ סימטרי אז גם $(f)_0 \in R_0$ סימטרי.

(ד) $(s_1)_0, (s_2)_0, \dots, (s_{n-1})_0$ הם הפולינומים הסימטריים היסודיים ב־$X_1, \dots, X_{n-1}$ ו־$(s_n)_0 = 0$.

נמשיך באינדוקציה על $d = \deg f$.

אם $d \leq 0$, אז $f \in A$ ונקח $g = f$. נניח שהמשפט נכון לפולינומים ממעלה $< d$. באינדוקציה על n (לא d) יש $g_0 \in R_0$ כך שמתקיים (השוויון הימני לפי (א) לעיל)

$$(f)_0 = g_0\big((s_1)_0, \dots, (s_{n-1})_0\big) = \big(g_0(s_1, \dots, s_{n-1})\big)_0, \qquad (1)$$
$$w(g_0) \leq \deg(f)_0 \leq \deg f = d.$$

לפי דוגמה 3.3(ג), $g_0(s_1, \dots, s_{n-1})$ סימטרי. לפי טענה 3.7, $\deg g_0(s_1, \dots, s_{n-1}) \leq w(g_0) \leq d$. לכן

$$\hat{f} := f - g_0(s_1, \dots, s_{n-1}) \in R$$

סימטרי, ממעלה $\leq d$. לפי (1), $\hat{f}(X_1, \dots, X_{n-1}, 0) = (\hat{f})_0 = 0$, לכן $X_n \mid \hat{f}$. כיוון ש־$\hat{f}$ סימטרי, גם $X_1, \dots, X_{n-1} \mid \hat{f}$. ולכן $X_1 \cdots X_n \mid \hat{f}$. לכן $\hat{f} = s_n f_1$, עבור איזה $f_1 \in R$, אשר הינו בהכרח סימטרי (כי אם $\sigma \in S_n$ אז $s_n \sigma(f_1) = s_n f_1$, ולכן $\sigma(f_1) = f_1$), ממעלה $\leq d - n < d$. באינדוקציה על d קיים $g_1 \in R$ כך ש־$f_1 = g_1(s_1, \dots, s_n)$, ו־$w(g_1) \leq d - n$.

לכן

$$f = g_0(s_1,\dots,s_{n-1}) + s_n g_1(s_1,\dots,s_n) = (g_0 + X_n g_1)(s_1,\dots,s_n)$$

ו־$w(g_0 + X_n g_1) \le d$ ∎

משפט 3.9: *יהי* $g \in R$ *כך ש־*$g(s_1,\dots,s_n) = 0$*. אז* $g = 0$.

הוכחה: באינדוקציה על n. עבור $n = 1$ – ברור. נמשיך באינדוקציה על $\deg g$. אם $\deg g \le 0$ – ברור. כעת

$$0 = \big(g(s_1,\dots,s_n)\big)_0 = g\big((s_1)_0,\dots,(s_{n-1})_0,0\big) = (g)_0\big((s_1)_0,\dots,(s_{n-1})_0\big),$$

לכן לפי הנחת האינדוקציה על n, $(g)_0 = g(X_1,\dots,X_{n-1},0) = 0$. לכן, אם נכתוב את g כפולינום ב־X_n מעל R_0, אז $g = X_n g_1$ עבור איזה $g_1 \in R$. לכן $s_n g_1(s_1,\dots,s_n) = 0$, ולכן $g_1(s_1,\dots,s_n) = 0$. אבל $\deg g_1 < \deg g$, לכן $g_1 = 0$. מכאן $g = X_n g_1 = 0$. ∎

משפט 3.10: *יהי* $f \in R$ *סימטרי ממעלה* d*. אז יש* $g \in R$ *יחיד כך ש־*$f = g(s_1,\dots,s_n)$*. יתר על כן,* $w(g) = d$.

הוכחה: לפי משפט 3.8 קיים g כזה. לפי משפט 3.9 הוא יחיד. לפי משפט 3.8, $w(g) \le d$. לבסוף, לפי טענה 3.7, $d = \deg f = \deg g(s_1,\dots,s_n) \le w(g) \le d$. ולכן $w(g) = d$. ∎

4. הרחבות סופיות ואלגבריות

יהי K שדה.

הגדרה 4.1: תת־קבוצה $K_0 \subseteq K$ היא **תת־שדה** של K, אם היא סגורה תחת החיבור, הכפל וההופכי, ומכילה את 1 (היחידה של K) ואת -1. אז K_0 שדה. נאמר אז גם כי K **הרחבה של** K_0 או ש־K/K_0 **הרחבת שדות**. אז K הוא גם מרחב וקטורי מעל K_0. **המעלה** של K/K_0 היא $[K : K_0] = \dim_{K_0} K$ (מספר טבעי או ∞). ∎

הערה 4.2: תהי $A \subseteq K$ קבוצה. אז קיים התת־חוג (התת־שדה) הקטן ביותר של K שמכיל את A. אכן, זהו החיתוך של כל התת־חוגים (תת־שדות) של K שמכילים את A. ∎

הגדרה 4.3: **התת־חוג** (**התת־שדה**) **הראשוני** של K הוא התת־חוג (התת־שדה) הקטן ביותר של K. ∎

הערה 4.4: על התת־חוג (התת־שדה) הראשוני. נגדיר $\varphi\colon \mathbb{Z} \to K$ על ידי

$$\varphi(n) = n1_K = \begin{cases} 0_K & n = 0 \text{ אם} \\ \overbrace{1_K + \cdots + 1_K}^{n} & n > 0 \text{ אם} \\ \overbrace{(-1_K) + \cdots + (-1_K)}^{-n} & n < 0 \text{ אם} \end{cases}$$

קל לראות ש־φ הומומורפיזם ו־$\varphi(\mathbb{Z})$ מוכל בכל תת חוג של K. לכן $\varphi(\mathbb{Z})$ הוא החוג הראשוני של K ושדה המנות שלו $\mathbb{F}$ הוא התת־שדה הראשוני שלו. כיוון ש־$\mathbb{Z}$ ראשי, יש $p \in \mathbb{Z}$ כך ש־$\operatorname{Ker}\varphi = (p) = p\mathbb{Z}$. בלי הגבלת הכלליות $p \geq 0$. אז p נקרא **האיפיון** $\operatorname{char}(K)$ של K. נבדיל בין שני מקרים:

(א) $p = 0$. אז $\varphi(\mathbb{Z}) \cong \mathbb{Z}$, ולכן $\mathbb{F} \cong \mathbb{Q}$. נאמר ש־$\mathbb{Z}$ ($\mathbb{Q}$) הוא החוג (השדה) הראשוני של K.

(ב) $p > 0$. אז $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ תחום, לכן p ראשוני, ולכן $\mathbb{Z}/p\mathbb{Z}$ שדה. אז $\mathbb{F} = \varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. נאמר ש־$\mathbb{F}_p$ הוא החוג וגם השדה הראשוני של K.

מסקנה 4.5: *$\operatorname{char}(K)$ הוא אפס או ראשוני.*

הגדרה 4.6: שתי הרחבות L_1, L_2 של K **איזומורפיות מעל** K ($L_1 \cong_K L_2$) אם יש איזומורפיזם $\theta\colon L_1 \to L_2$ כך ש־$\theta(a) = a$ לכל $a \in K$. ∎

הערה 4.7: סימון. תהי L/K הרחבת שדות ותהי $S \subseteq L$ קבוצה. **החוג** (**השדה**) **הנוצר על ידי** S **מעל** K הוא התת־חוג (התת־שדה) הקטן ביותר של L שמכיל את K ואת S. יסומן $K[S]$ ($K(S)$). מתקיים

$$K[S] = \{f(z_1, \ldots, z_m) |\ f \in K[X_1, \ldots, X_m],\ m \in \mathbb{N}, z_1, \ldots, z_m \in S\},$$
$$K(S) = \Big\{\frac{f(z_1, \ldots, z_m)}{g(z_1, \ldots, z_m)}\Big|\ f, g \in K[X_1, \ldots, X_m],\ m \in \mathbb{N}, z_1, \ldots, z_m \in S, \ g(z_1, \ldots, z_m) \neq 0\Big\}.$$

אם $S=\{\alpha_1,\dots,\alpha_n\}$, נכתוב $K[\alpha_1,\dots,\alpha_n]$ במקום $K[S]$ ו־$K(\alpha_1,\dots,\alpha_n)$ במקום $K(S)$. מתקיים $K[\alpha]=\{f(\alpha)|\ f\in K[X]\}$, $K(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}|\ f,g\in K[X],\ g(\alpha)\neq 0\right\}$.

נאמר ש־L/K **נוצרת סופית** אם יש $\alpha_1,\dots,\alpha_n\in L$ כך ש־$L=K(\alpha_1,\dots,\alpha_n)$.

נאמר ש־L/K **פשוטה** אם יש $\alpha\in L$ כך ש־$L=K(\alpha)$.

דוגמה 4.8: $\mathbb{Q}(\pi,e)/\mathbb{Q}$ נוצרת סופית, $\mathbb{C}/\mathbb{R}$ פשוטה , כי $\mathbb{C}=\mathbb{R}(\sqrt{-1})$.

משפט 4.9: *יהי $p\in K[X]$ אי פריק.*

(א) *יהי $L=K[X]/(p)$ ותהי $x\in L$ מחלקת השקילות של X. אז L שדה שמכיל את K ומתקיים $L=K[x]=K(x)$ ו־$p(x)=0$.*

(ב) *אם $K(\alpha)$ הרחבה פשוטה של K כך ש־$p(\alpha)=0$, אז קיים הומומורפיזם־K יחיד $\theta\colon K(x)\to K(\alpha)$ המעתיק את x על α; הוא איזומורפיזם.*

הוכחה: (א) לפי מסקנה 2.6(4), (p) אידאל מרבי. לפי למה 1.18(א), חוג המנה L הוא שדה. הרכבת ההומומורפיזמים $K\to K[X]\to L$ היא מונומורפיזם (כל הומומורפיזם משדה לתוך חוג $L\neq 0$, אשר מעתיק 1 על 1 הוא חח"ע, כי גרעינו הוא אידאל של השדה שאינו מכיל את 1 ולכן הוא 0), לכן אפשר לזהות בעזרתו את K עם תת־שדה של L. מתקיים $K[x]\subseteq K(x)\subseteq L$. אך אם $g=\sum_i a_iX^i\in K[X]$, אז $g(x)=\sum_i a_ix^i=\sum_i a_i(X+(p))^i=\sum_i a_iX^i+(p)=g+(p)$, ולכן

$$L=\{g+(p)|\ g\in K[X]\}=\{g(x)|\ g\in K[X]\}=K[x].$$

מכאן $L=K[x]=K(x)$ ו־$p(x)=p+(p)=(p)=0$.

(ב) **היחידות:** לפי הערה 4.7, $K[x]=\{g(x)|\ g\in K[X]\}$. אם θ כנ"ל, אז לכל $g=\sum_i a_iX^i\in K[X]$ מתקיים $\theta(g(x))=\theta(\sum_i a_ix^i)=\sum_i\theta(a_i)\theta(x)^i=\sum_i a_i\alpha^i=g(\alpha)$ ומכאן היחידות.

קיום: ההצבה $\alpha\mapsto X$ מגדירה הומומורפיזם־K $\varphi\colon K[X]\to K(\alpha)$ על ידי $\varphi(f)=f(\alpha)$. בפרט $\varphi(X)=\alpha$. מתקיים $\varphi(p)=p(\alpha)=0$, לכן $(p)\subseteq\ker\varphi$. לפי משפט האיזומורפיזם הראשון φ משרה הומומורפיזם $\theta\colon L=K[X]/(p)\to K(\alpha)$ אשר מעתיק את x על α. כיוון ש־L שדה, θ חח"ע. תמונתו היא שדה שמכיל את K ואת α, לכן התמונה היא $K(\alpha)$. לכן θ איזומורפיזם. ∎

הגדרה 4.10: תהי L/K הרחבת שדות. איבר $\alpha\in L$ נקרא **אלגברי מעל** K אם יש $0\neq f\in K[X]$ כך ש־$f(\alpha)=0$; אחרת α נקרא **טרנסצנדנטי**. הרחבה L/K נקראת **אלגברית** אם כל $\alpha\in L$ אלגברי מעל K.

ההצבה $\varphi_\alpha\colon K[X]\to L$ הנתונה על ידי $f\mapsto f(\alpha)$ היא הומומורפיזם חוגים. לכן α אלגברי אם ורק אם $\operatorname{Ker}\varphi_\alpha\neq 0$. ∎

משפט 4.11 (הרחבה אלגברית פשוטה): *תהי L/K הרחבת שדות ויהי $\alpha\in L$ אלגברי מעל K.*

(א) *יש $p\in K[X]$ מתוקן יחיד כך ש־$\operatorname{Ker}\varphi_\alpha=(p)$. הוא ייקרא **הפולינום האי פריק של** α ויסומן $\operatorname{irr}(\alpha,K)$.*

(ב) *p אי פריק.*

(ג) *יהי $f \in K[X]$. אז $f(\alpha) = 0$ אם ורק אם $p \mid f$.*

(ד) *$K(\alpha) = K[\alpha]$.*

(ה) *$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in K\}$, כאשר $n = \deg p$.*

(ו) *$[K(\alpha) : K] = n = \deg p$. ביתר דיוק, $1, \alpha, \ldots, \alpha^{n-1}$ הוא בסיס של $K(\alpha)$ מעל K.*

(ז) *אם $K(\beta)$ הרחבה של K כך ש־$p(\beta) = 0$ אז קיים איזומורפיזם־K יחיד $\rho\colon K(\alpha) \to K(\beta)$ המעתיק α על β.*

הוכחה: (א) $0 \neq \operatorname{Ker}\varphi_\alpha \subseteq K[X]$ אידאל. לפי משפט 2.3 יש $p \in K[X]$ כך ש־$\operatorname{Ker}\varphi_\alpha = (p)$. לפי מסקנה 2.6(1), $(p) = (p')$ אם ורק אם $p' = up$, כאשר $u \in (K[X])^\times = K^\times$. לכן בה"כ p מתוקן וכזה הוא יחיד.

(ב) $K[X]/(p) \cong K[\alpha]$ תחום. לכן לפי למה 1.18, (p) אידאל ראשוני. לפי מסקנה 2.6(4), p אי פריק.

(ג) $f(\alpha) = 0$ אם ורק אם $f \in \operatorname{Ker}\varphi_\alpha = (p)$ אם ורק אם $p \mid f$.

(ד) לפי המשפט הקודם יש איזומורפיזם־K $\theta\colon K[X]/(p) \to K(\alpha)$ אשר מעתיק את $x = X + (p)$ על α. אבל $K(\alpha) = \theta(K[X]/(p)) = \theta(\{g(x) \mid g \in K[X]\}) = \{g(\alpha) \mid g \in K[X]\} = K[\alpha]$.

(ה) $\supseteq$ ברור. להיפך, אם $\beta \in K[\alpha]$ אז $\beta = f(\alpha)$, כאשר $f \in K[X]$. אז $f = pq + r$ כאשר $q, r \in K[X]$ ו־$\deg r < n$. לכן $\beta = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, לכן β באגף ימין.

(ו) לפי (ה), $1, \alpha, \ldots, \alpha^{n-1}$ פורשים את $K(\alpha)$ מעל K. נראה שהם בלתי תלויים לינארית. יהיו $a_0, a_1, \ldots, a_{n-1} \in K$ כך ש־$a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1} = 0$, אז $f = a_0 + a_1X + \cdots a_{n-1}X^{n-1}$ מקיים $f(\alpha) = 0$. לפי (ג), $p \mid f$. אבל $\deg f < \deg p$ לכן $f = 0$. מכאן $a_0 = a_1 = \cdots = a_{n-1} = 0$.

(ז) לפי המשפט הקודם יש איזומורפיזמי־K יחידים $\rho\colon K[X]/(p) \to K(\beta)$, $\theta\colon K[X]/(p) \to K(\alpha)$, שמעתיקים את $x = X + (p)$ על α, β, בהתאמה. אז $\rho \circ \theta^{-1}$ האיזומורפיזם המבוקש והוא יחיד כזה. ∎

משפט 4.12 (הרחבה טרנסצנדנטית פשוטה): *תהי L/K הרחבת שדות ויהי $\alpha \in L$ טרנסצנדנטי מעל K.*

(א) *$K[X] \cong_K K[\alpha]$ על ידי $f(X) \mapsto f(\alpha)$.*

(ב) *$K(X) \cong_K K(\alpha)$ על ידי $\frac{f(X)}{g(X)} \mapsto \frac{f(\alpha)}{g(\alpha)}$.*

(ג) *$[K(\alpha) : K] = \infty$. ביתר דיוק, $1, \alpha, \alpha^2, \ldots$ בסיס של $K[\alpha]$ מעל K.*

(ד) *$K[\alpha] \subsetneqq K(\alpha)$.*

הוכחה: (א) φ_α הומומורפיזם. גרעינו 0, לכן הוא חח"ע. תמונתו $K[\alpha] = \{f(\alpha) \mid f \in K[X]\}$.

(ב) האיזומורפיזם $K[X] \to K[\alpha]$ של חוגים ניתן להרחבה לאיזומורפיזם של שדות המנות שלהם.

(ג) ברור ש־$1, \alpha, \alpha^2, \ldots$ פורשים $K[\alpha]$ מעל K. אם יש $n \in \mathbb{N}$ ו־$a_0, a_1, \ldots, a_n \in K$ כך ש־$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^n = 0$, אז $f = a_0 + a_1X + \cdots a_nX^n$ מקיים $f(\alpha) = 0$. לכן $f = 0$.

(ד) לפי (א) ו־(ב), כיוון ש־$K[X] \subsetneqq K(X)$. ∎

מסקנה 4.13: *תהי L/K הרחבה ויהי $\alpha \in L$. אז α אלגברי מעל K אם ורק אם $[K(\alpha) : K] < \infty$.*

משפט 4.14: *יהיו $K \subseteq L \subseteq M$ שדות. אז $[M:K] = [M:L]\cdot[L:K]$. ביתר דיוק, אם $\{x_i\}_{i\in I}$ בסיס של L מעל K ו־$\{y_j\}_{j\in J}$ בסיס של M מעל L אז $\{x_iy_j\}_{(i,j)\in I\times J}$ בסיס של M מעל K.*

הוכחה: **הקבוצה פורשת**: יהי $z \in M$. אז יש $a_j \in L$, כמעט כולם 0, כך ש־$z = \sum_{j\in J} a_jy_j$. לכל $j \in J$ יש $b_{ij} \in K$, כמעט כולם 0, כך ש־$a_j = \sum_{i\in I} b_{ij}x_i$; אם $a_j = 0$, בה"כ $b_{ij} = 0$ לכל i. אז

$$z = \sum_{j\in J}\sum_{i\in I} b_{ij}x_iy_j.$$

ו־$b_{ij} = 0$ עבור כמעט על i, j.

הקבוצה בלתי תלויה לינארית מעל K: יהיו $b_{ij} \in K$, כמעט כולם 0, כך ש־ $\sum_{j\in J}\sum_{i\in I} b_{ij}x_iy_j = 0$, כלומר $\sum_{j\in J}(\sum_{i\in I} b_{ij}x_i)y_j = 0$. כיוון ש־$y_j$ בלתי תלויים לינארית מעל L ו־$\sum_{i\in I} b_{ij}x_i \in L$ לכל $j \in J$, מתקיים $\sum_{i\in I} b_{ij}x_i = 0$ לכל j. נקבע j. כיוון ש־x_i בלתי תלויים לינארית מעל K, מתקיים $b_{ij} = 0$ לכל i.
∎

מסקנה 4.15: *תהי L/K הרחבה.*

(א) *אם $[L:K] < \infty$ אז כל $\alpha \in L$ אלגברי מעל K.*

(ב) *$[L:K] < \infty$ אם ורק אם קיימים $\alpha_1,\dots,\alpha_n \in L$ אלגבריים מעל K כך ש־$L = K(\alpha_1,\dots,\alpha_n)$.*

הוכחה: (א) $K \subseteq K(\alpha) \subseteq L$ ו־$[L:K] = [L:K(\alpha)]\cdot[K(\alpha):K]$, לכן $[K(\alpha):K] \le [L:K] < \infty$. לפי מסקנה 4.13, α אלגברי מעל K.

(ב) $\Leftarrow$: יהי $\alpha_1,\dots,\alpha_n$ בסיס של L מעל K. אז $L = K(\alpha_1,\dots,\alpha_n)$. לפי (א), $\alpha_1,\dots,\alpha_n$ אלגבריים מעל K.

$\Rightarrow$: עבור $0 \le i \le n$ נגדיר $L_i = K(\alpha_1,\dots,\alpha_i)$. אז $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = L$. לכל $i \ge 1$ מתקיים $L_i = L_{i-1}(\alpha_i)$, ו־α_i אלגברי מעל K ולכן גם מעל L_{i-1}, לכן $[L_i : L_{i-1}] < \infty$. לפי נוסחת המכפלה, $[L:K] < \infty$. ∎

מסקנה 4.16: *תהי L/K הרחבת שדות ויהיו $\alpha_1, \alpha_2 \in L$ אלגבריים מעל K. אז $\alpha_1 \pm \alpha_2, \alpha_1\alpha_2, \frac{\alpha_1}{\alpha_2}$ אלגבריים מעל K. (המנה מוגדרת רק אם $\alpha_2 \neq 0$.)*

הוכחה: מושארת כתרגיל. (נסה להשתכנע שהוכחה ישירה מההגדרה אינה פשוטה בכלל.) ∎

הגדרה 4.17: אם $L_1,\dots,L_r \subseteq L$ שדות, אז **הצירוף** $L_1\cdots L_r$ של $L_1,\dots,L_r$ בתוך L הוא התת־שדה הקטן ביותר של L שמכיל את $L_1,\dots,L_r$. למשל, $K(\alpha_1)\cdots K(\alpha_r) = K(\alpha_1,\dots,\alpha_r)$. ∎

משפט 4.18: *יהיו $K \subseteq L, F \subseteq M$ שדות.*

(א) *M/K סופית אם ורק אם L/K, M/L סופיות.*

(ב) *אם L/K סופית, אז LF/F סופית.*

(ג) אם L/K, F/K סופיות אז LF/K סופית

כנ"ל עם "אלגברי" במקום "סופי".

הוכחה: (ג) נובע באופן פורמלי (בשני המקרים) מתוך (א),(ב).

הרחבות סופיות:

(א) $[M:K]=[M:L]\cdot[L:K]$.

(ב) נשתמש פעמיים בבוחן של מסקנה 4.15(ב): קיימים $\alpha_1,\dots,\alpha_n\in L$ אלגבריים מעל K כך ש־$L=K(\alpha_1,\dots,\alpha_n)$. אז $LF=F(\alpha_1,\dots,\alpha_n)$. אבל $\alpha_1,\dots,\alpha_n$ אלגבריים גם מעל F, לכן $[LF:F]<\infty$.

הרחבות אלגבריות:

(א) $\Leftarrow$: ברור.

$\Rightarrow$: יהי $\alpha\in M$. יהיו $\alpha_1,\dots,\alpha_n\in L$ המקדמים של $\mathrm{irr}(\alpha,L)\in L[X]$. אז α אלגברי מעל $K(\alpha_1,\dots,\alpha_n)$, ו־$\alpha_1,\dots,\alpha_n$ אלגבריים מעל K. לכן

$$[K(\alpha,\alpha_1,\dots,\alpha_n):K]=[K(\alpha_1,\dots,\alpha_n)(\alpha):K(\alpha_1,\dots,\alpha_n)]\cdot[K(\alpha_1,\dots,\alpha_n):K]<\infty.$$

לכן לפי מסקנה 4.15(א), α אלגברי מעל K.

(ב) אם $S,S'\subseteq L$ קבוצות סופיות, אז $F(S),F(S')\subseteq F(S\cup S')$. לכן $F'=\bigcup_{S\subseteq L}$ סופית $F(S)$ תת־שדה של LF (בדוק!). הוא מכיל את F וכל איבר של L, לכן $F'=LF$. לכן די להוכיח לכל $S=\{\alpha_1,\dots,\alpha_n\}\subseteq L$ סופית כי $F(S)$ אלגברית מעל F. אבל $\mathrm{irr}(\alpha_i,K)\in K[X]\subseteq F[X]$, לכל $1\le i\le n$, לכן $\alpha_1,\dots,\alpha_n$ אלגבריים מעל F. לפי מסקנה 4.15(ב), $[F(S):F]<\infty$, לכן לפי מסקנה 4.15(ב), $F(S)$ אלגברית מעל F. ∎

תרגיל 4.19: *תהי L/K אלגברית ויהי $\sigma\colon L\to L$ הומומורפיזם־K. אז σ אוטומורפיזם של L.*

הדרכה: הנח קודם ש־L/K סופית.

תרגיל 4.20: *יהיו $K\subseteq L, F\subseteq M$ שדות, L/K סופית. הוכח: $[LF:F]\le[L:K]$.*

5. הסגור האלגברי

יהי K שדה.

למה 5.1: *יהיו $\alpha \in K$, $f \in K[X]$. אז $f(\alpha) = 0$ אם ורק אם $f \mid (X-\alpha)$ ב־$K[X]$.*

הוכחה: נניח $f(\alpha) = 0$. יש $q, r \in K[X]$ כך ש־$f = (X-\alpha)q + r$, $\deg r < 1$, כלומר, $r \in K$. אז $r = r(\alpha) = f(\alpha) = 0$. לכן $f = (X-\alpha)q$.

אם $f = (X-\alpha)g$ אז $f(\alpha) = (\alpha-\alpha)g(\alpha) = 0$. ∎

מסקנה 5.2: *לכל $0 \neq f \in K[X]$ יש לכל היותר $\deg f$ שורשים שונים ב־K.*

הוכחה: ל־f יש לכל היותר $\deg f$ גורמים אי פריקים ממעלה 1. ∎

תרגיל 5.3: *תהי E/K הרחבה אלגברית. אז $|E| \leq \kappa := \max(|K|, \aleph_0)$.*

הוכחה: קבוצת הפולינומים המתוקנים ממעלה n מעל K היא בעלת עוצמה $|K|^n$. לכן קבוצת הפולינומים המתוקנים מעל K היא בעלת עוצמה κ. לכל $f \in K[X]$ מתוקן תהי $R(f)$ קבוצת שורשיו ב־E. אז $R(f)$ סופית. אך $E = \bigcup_f R(f)$. לכן $|E| \leq \kappa \cdot \aleph_0 = \kappa$. ∎

הגדרה 5.4: (א) שדה L **סגור אלגברית** אם לכל $f \in L[X]$ ממעלה ≥ 1 יש שורש ב־L.

(ב) שדה L הנו **סגור אלגברי** של K אם הוא סגור אלגברית ו־L/K הרחבה אלגברית. ∎

למה 5.5: *שדה K סגור אלגברית אם ורק אם אין לו הרחבה אלגברית L/K, $L \neq K$.*

הוכחה: $\Leftarrow$: תהי L/K אלגברית; נראה ש־$L = K$. יהי $\beta \in L$. אז $f = \mathrm{irr}(\beta, K) \in K[X]$ יש לו שורש $\alpha \in K$, לכן $f \mid X-\alpha$. אבל f אי פריק, לכן $f = X - \alpha$. מכאן $\beta = \alpha \in K$.

$\Rightarrow$: יהי $f \in K[X]$ ממעלה ≥ 1. יש לו גורם אי פריק מתוקן $p \in K[X]$ ממעלה ≥ 1. יש L/K אלגברית בה יש ל־p שורש. זהו גם שורש של f. אבל $L = K$, לכן ל־f יש שורש ב־K. ∎

משפט 5.6: *(א) ל־K יש סגור אלגברי $\tilde{K}$.*

(ב) *אם $\tilde{K}'$ סגור אלגברי (נוסף) של K אז $\tilde{K} \cong_K \tilde{K}'$.*

(ג) *תהי $\tilde{K}/K$ הרחבה אלגברית ויהי C שדה סגור אלגברית. אז כל שיכון שדות $K \to C$ ניתן להרחבה לשיכון $\tilde{K} \to C$.*

הוכחה: (א) תהי M קבוצה שמכילה את K, כך ש־$|K|, \aleph_0 < |M|$.

אם L קבוצה, $K \subseteq L \subseteq M$, אז כל פונקציה $f\colon L \times L \to L \times L$ מגדירה שתי פעולות בינריות, (נקרא לבן חיבור וכפל) על L: $f(a,b) = (a+b, ab)$. אם L שדה ביחס לפעולות אלה ו־K תת־שדה שלו, נאמר כי (L, f) **שדה בתוך** M.

נתבונן במשפחה Λ של שדות (L, f) בתוך M עבורם (L, f) הרחבה *אלגברית* של K. אז $\Lambda \neq \emptyset$, כי $K \in \Lambda$. נגדיר יחס סדר חלקי על Λ: $(L, f) \prec (L', f')$ אם (L', f') הרחבה של (L, f) (כלומר, $L \subseteq L'$

ו־$f = f'|_{L\times L}$; בדוק שזהו אכן יחס סדר חלקי). אם $\{(L_i, f_i)\}_{i\in I}$ שרשרת בתוך Λ אז יש לה חסם מלעיל $(\bigcup_{i\in I} L_i, \bigcup_{i\in I} f_i)$. לכן לפי הלמה של צורן יש לה איבר מרבי $(\tilde{K}, f)$. נראה ש־$(\tilde{K}, f)$ סגור אלגברית.

אכן, אחרת יש $p(X) \in \tilde{K}[X]$ ממעלה ≥ 1 שאין לו שורש ב־$\tilde{K}$. בלי הגבלת הכלליות p אי פריק, אחרת נחליף אותו בגורם אי פריק שלו. לפי משפט 4.9 יש ל־$\tilde{K}$ הרחבה $L' \cong_{\tilde{K}} \tilde{K}[X]/(p)$ בה יש ל־p שורש; בפרט $\tilde{K} \subsetneqq L'$. אז L' הרחבה אלגברית של $\tilde{K}$, ולכן של K. לפי תרגיל 5.3, $|\tilde{K}|, |L'| < |M|$, לכן $|L' \smallsetminus \tilde{K}| \leq |L'| < |M| = |M \smallsetminus \tilde{K}|$. לכן בלי הגבלת הכלליות $L' \subseteq M$. כעת עבור f' מתאימה, $(L', f') \in \Lambda$, $(\tilde{K}, f) \prec (L', f')$, אבל $(\tilde{K}, f) \neq (L', f')$, סתירה למרביות.

(ג) בלי הגבלת הכלליות $\tilde{K}$ סגור אלגברי של K. אכן, לפי (א) יש ל־$\tilde{K}$ סגור אלגברי $\hat{K}$. אז $\hat{K}/K$ אלגברית, לכן $\hat{K}$ סגור אלגברי של K. אם נצליח להרחיב $K \to C$ ל־$\theta\colon \hat{K} \to C$ אז $\theta|_{\tilde{K}}\colon \tilde{K} \to C$ הוא כמבוקש.

תהי Λ' משפחת הזוגות (L, θ), באשר $K \subseteq L \subseteq \tilde{K}$ שדה ביניים ו־$\theta\colon L \to C$ שיכון שמרחיב את $K \to C$. נגדיר יחס סדר חלקי על Λ': $(L, \theta) \prec (L', \theta')$ אם L' הרחבה של L ו־θ' הרחבה של θ. (שוב, זהו יחס סדר חלקי.)

אם $\{(L_i, \theta_i)\}_{i\in I}$ שרשרת בתוך Λ' אז יש לה חסם מלעיל $(\bigcup_{i\in I} L_i, \bigcup_{i\in I} \theta_i)$. לכן לפי הלמה של צורן יש ב־Λ' איבר מרבי (L, θ). נראה ש־L סגור אלגברית. אז, היות ו־$\tilde{K}/K$ אלגברית, גם $\tilde{K}/L$ אלגברית, ולכן לפי למה 5.5, $L = \tilde{K}$. בכך יוכח (ג).

אחרת, כמו בחלק (א), יש $p(X) \in L[X]$ אי פריק שאין לו שורש ב־L. האיזומורפיזם $\theta\colon L \to \theta(L)$ ניתן להרחבה לאיזומורפיזם $L[X] \to \theta(L)[X]$, שמעתיק את p על פולינום אי פריק $\theta(p)$ ולכן משרה איזומורפיזם $\hat{\theta}$ בתרשים למטה. כיוון ש־$\tilde{K}, C$ סגורים אלגברית, יש ל־p שורש α ב־$\tilde{K}$ ול־$\theta(p)$ שורש β ב־C. לפי משפט 4.11(ז) יש איזומורפיזמים ρ, λ בתרשים. אז הרכבת ההעתקות בשורה העליונה של התרשים היא שיכון $\theta'\colon L(\alpha) \to C$ שמרחיב את θ ולכן $(L, \theta) \prec (L(\alpha), \theta')$, סתירה למרביות.

$$\begin{tikzcd}
L(\alpha) \arrow[r, "\lambda"'] & L[X]/(p) \arrow[r, "\hat{\theta}"'] & \theta(L)[X]/(\theta(p)) \arrow[r, "\rho"'] & \theta(L)(\beta) \arrow[r, "\text{הכלה}"'] & C \\
L \arrow[u] \arrow[r, equal] & L \arrow[u] \arrow[r, "\theta"'] & \theta(L) \arrow[u] \arrow[r, equal] & \theta(L) \arrow[u] \arrow[r, "\text{הכלה}"'] & C \arrow[u, equal]
\end{tikzcd}$$

(ב) יהי $K \to \tilde{K}'$ ההכלה. לפי (ג) יש שיכון־K $\theta\colon \tilde{K} \to \tilde{K}'$. אז $\tilde{K} \cong_K \theta(\tilde{K})$, ולכן $\theta(\tilde{K})$ גם סגור אלגברי של K. אבל $\tilde{K}'/K$ אלגברית, לכן גם $\tilde{K}'/\theta(\tilde{K})$, לכן $\tilde{K}' = \theta(\tilde{K})$, לפי למה 5.5. ∎

מסקנה 5.7: *יהי $\tilde{K}$ סגור אלגברי של שדה K, יהי $K \subseteq L \subseteq \tilde{K}$ שדה, ויהי $\sigma\colon L \to \tilde{K}$ שיכון־K. אז σ ניתן להרחבה לאוטומורפיזם־K של $\tilde{K}$.*

הוכחה: לפי (ג), σ ניתן להרחבה לשיכון־K $\sigma\colon \tilde{K} \to \tilde{K}$. לפי תרגיל 4.19, $\sigma(\tilde{K}) = \tilde{K}$. ∎

למה 5.8: *תהי F/K הרחבת שדות. אז יש לכל היותר סגור אלגברי אחד של K מוכל בתוך F; אם F סגור אלגברית אז יש בדיוק אחד.*

הוכחה: יהי $L = \{\alpha \in F |\ K$ אלגברי מעל $\alpha\}$. לפי מסקנה 4.16, L הינו שדה, לכן L הרחבה אלגברית של K.
אם $L' \subseteq F$ סגור אלגברי של K אז $L' \subseteq L$. לפי למה 5.5, $L' = L$.

אם F סגור אלגברית, יהי $f \in L[X]$ ממעלה ≥ 1. אז $f \in F[X]$, לכן יש לו שורש $\alpha \in F$. אבל α אלגברי מעל L, לכן מעל K ולכן $\alpha \in L$. מכאן ש־L הוא סגור אלגברי של K. ∎

תרגיל 5.9: *(א) אם L שדה סגור אלגברית, אז כל $f \in L[X]$ ממעלה $n \geq 1$* **מתפצל מעל** *L, כלומר, מתפרק לגורמים לינאריים ב־$L[X]$: $f = c(X-\alpha_1)\cdots(X-\alpha_n)$, באשר $c \in L^\times$, $\alpha_1, \ldots, \alpha_n \in L$.*

(ב) אם L/K הרחבה אלגברית וכל פולינום $f \in K[X]$ ממעלה $n \geq 1$ מתפצל מעל L, אז L סגור אלגברי של K.

6. ריבוי של שורש

יהי K שדה ויהי $\tilde{K}$ סגור אלגברי שלו.

הגדרה 6.1: יהי $f = \sum_{i=0}^{\infty} a_i X^i \in K[X]$. **הנגזרת** של f היא $f' = \sum_{i=0}^{\infty} i a_i X^{i-1} \in K[X]$. (כאן $i = \overbrace{1 + \cdots + 1}^{i} \in K$). ∎

למה 6.2 (תכונות של נגזרת): *יהיו* $f, g \in K[X]$, $c \in K$.

(א) $(f+g)' = f' + g'$;

(ב) $(cf)' = cf'$;

(ג) $c' = 0$;

(ד) $(fg)' = f'g + fg'$;

(ה) $(f \circ g)' = (f' \circ g)g'$ *(כאן* $(f \circ g)(X) = f(g(X))$*).*

הוכחה: (א), (ב), (ג) קלים, מושארים כתרגיל.

(ד) נניח כי $f = f_1 + f_2$ באשר $(f_i g)' = f_i' g + f_i g'$ עבור $i = 1, 2$. אז

$$(fg)' = (f_1 g + f_2 g)' = (f_1 g)' + (f_2 g)' = f_1' g + f_1 g' + f_2' g + f_2 g' =$$
$$(f_1' + f_2')g + (f_1 + f_2)g' = f'g + fg'$$

לכן בלי הגבלת הכלליות $f = cX^i$ מונום. באופן דומה בלי הגבלת הכלליות $g = dX^j$ מונום. אז $(fg)'$ הוא

$$(cX^i dX^j)' = (cdX^{i+j})' = (i+j)cdX^{i+j-1} = icX^{i-1}dX^j + cX^i jdX^{j-1} = f'g + fg'$$

(ה) נניח כי $f = f_1 + f_2$ באשר $(f_i \circ g)' = (f_i' \circ g)g'$ עבור $i = 1, 2$. אז

$$(f \circ g)' = (f_1 \circ g + f_2 \circ g)' = (f_1 \circ g)' + (f_2 \circ g)' = (f_1' \circ g)g' + (f_2' \circ g)g' =$$
$$(f_1' \circ g + f_2' \circ g)g' = (f_1 + f_2)' \circ g)g' = (f' \circ g)g'$$

לכן בלי הגבלת הכלליות $f = cX^i$ מונום ואז צריך להוכיח כי $(cg^i)' = icg^{i-1}g'$, כלומר, $(g^i)' = ig^{i-1}g'$.
נוכיח את הטענה באינדוקציה על i. אם $i = 0$ או $i = 1$, הטענה ברורה. נניח נכונות עבור $i - 1$. אז

$$(g^i)' = (gg^{i-1})' = g'(g^{i-1}) + g(g^{i-1})' = g'(g^{i-1}) + g(i-1)g^{i-2}g' = ig^{i-1}g'. \quad ∎$$

הערה 6.3: יהי $f = \sum_{i=0}^{\infty} a_i X^i \in K[X]$. אז $f' = 0 \Leftrightarrow ia_i = 0$ לכל i $\Leftrightarrow a_i = 0$ או $i = 0$ ב-K, לכל i. לכן

(א) אם $\mathrm{char}(K) = 0$ אז $f' = 0 \Leftrightarrow a_i = 0$ לכל $i \geq 1$ $\Leftrightarrow f$ קבוע, כלומר, $f \in K$.

(ב) אם $\mathrm{char}(K) = p > 0$ אז $f' = 0 \Leftrightarrow a_i = 0$ לכל $p \nmid i \Leftrightarrow f = \sum_{i=0}^{\infty} a_{pi} X^{pi} \Leftrightarrow f = g(X^p)$ עבור איזה $g \in K[X]$. ∎

יהי $0 \neq f \in K[X]$ ו־$\alpha \in K$. אז קיים $r \geq 0$ יחיד עבורו $f \mid (X-\alpha)^r$ ב־$K[X]$ אבל $f \nmid (X-\alpha)^{r+1}$ ב־$K[X]$. אז α שורש של f אם ורק אם $r \geq 1$.

הגדרה 6.4: r הוא **הריבוי של** α **ב־**f; α **שורש פשוט** של f אם $r = 1$; α **שורש כפול** של f אם $r = 2$; α **שורש מרובה** של f אם $r \geq 2$. ∎

משפט 6.5: *יהי $f \in K[X]$ ויהי $\alpha \in K$ שורשו. אז α שורש פשוט אם ורק אם $f'(\alpha) \neq 0$.*

הוכחה: לפי ההנחה $f = (X-\alpha)g$ באשר $g \in K[X]$ ו־α פשוט אם ורק אם $g(\alpha) \neq 0$. אבל $f' = g + (X-\alpha)g'$, לכן $f'(\alpha) = g(\alpha)$. ∎

משפט 6.6: *ל־ $0 \neq f \in K[X]$ אין שורשים מרובים ב־ $\tilde{K}$ אם ורק אם $1 \in \gcd(f, f')$.*

הוכחה: יהי $d \in \gcd(f, f')$ ויהי $\alpha \in \tilde{K}$. אז

$$\alpha \text{ שורש מרובה של } f \Leftrightarrow f(\alpha) = f'(\alpha) = 0 \Leftrightarrow (X-\alpha) \mid f, f' \Leftrightarrow (X-\alpha) \mid d \Leftrightarrow d(\alpha) = 0,$$

לכן: ל־f אין שורש מרובה ב־$\tilde{K} \Leftrightarrow$ ל־d אין שורש ב־$\tilde{K} \Leftrightarrow d \in \tilde{K}^\times$. ∎

דוגמה 6.7: נניח כי $\mathrm{char}(K) = p > 0$. יהי $f(X) = X^n - 1$ באשר $p \nmid n$. אז $f' = nX^{n-1} \neq 0$ וקל לראות ש־$1 \in \gcd(f, f')$. לכן ל־f יש בדיוק n שורשים שונים ב־$\tilde{K}$.

יהי $h(X) = X^p - 1$. אז $h' = 0$, לכן $h \ni \gcd(h) = \gcd(h, h')$ ובפרט $1 \notin \gcd(h, h')$. לכן ל־$h(X)$ יש שורשים מרובים ב־$\tilde{K}$. ואכן, $h(X) = (X-1)^p$, לכן יש לו שורש יחיד 1, בעל ריבוי p. ∎

משפט 6.8: *יהי $f \in K[X]$ אי פריק. אז ל־ f שורשים מרובים ב־ $\tilde{K}$ אם ורק אם $f' = 0$.*

הוכחה: לפי המשפט הקודם. אם $f' = 0$ אז $1 \notin \gcd(f) = \gcd(f, f')$. אם $f' \neq 0$, יהי $d \in \gcd(f, f')$. אז $d \mid f'$ לכן $\deg d \leq \deg f' < \deg f$. אך $d \mid f$ ו־f אי פריק, לכן $d \in K^\times$. ∎

מסקנה 6.9: *יהי $f \in K[X]$ אי פריק.*

(א) אם $\mathrm{char}(K) = 0$ *אז ל־ f אין שורשים מרובים ב־ $\tilde{K}$.*

(ב) אם $\mathrm{char}(K) = p > 0$ *אז ל־ f יש שורשים מרובים ב־ $\tilde{K}$ אם ורק אם $f(X) = g(X^p)$ עבור איזה $g \in K[X]$.*

הוכחה: לפי המשפט הקודם והערה 6.3. ∎

דוגמה 6.10: יהי $K = \mathbb{F}_p(t)$, שדה הפונקציות הרציונליות מעל $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. אז $f(X) = X^p - t$ אי פריק מעל K (אכן, K הוא שדה המנות של תחום ראשי $R = \mathbb{F}_p[t]$ ו־$t \in R$ ראשוני; לפי בוחן איזנשטיין f אי פריק.)
יהי $\alpha \in \tilde{K}$ שורשו. אז $f(X) = (X-\alpha)^p$. ∎

7. הרחבות פרידות

יהי K שדה. יהי $\tilde{K}$ סגור אלגברי של K.

משפט 7.1: *תת־חבורה סופית של החבורה $K^\times$ היא מעגלית (ציקלית).*

הוכחה: תהי $A \leq K^\times$ תת־חבורה סופית. אז A חילופית, ולכן $A = \prod_p A_p$ המכפלה הישרה של של חבורת סילוב־p שלה. כיוון שמכפלה ישרה של חבורות מעגליות מסדרים זרים היא מעגלית, די להוכיח שכל A_p מעגלית. לכן בלי הגבלת הכלליות A חבורת־p.

יהי $p^r = \max(\mathrm{ord}\,(\alpha) |\ \alpha \in A)$. אז $p^r \leq |A|$ וצריך להוכיח $p^r \geq |A|$. כל $\alpha \in A$ הינו מסדר p^i, באשר $r \geq i$, לכן $\alpha^{p^r} = \left((\alpha)^{p^i}\right)^{p^{r-i}} = 1$, כלומר, α שורש של $X^{p^r} - 1$. אבל לפולינום זה לכל היותר p^r שורשים שונים ב־K, לכן $|A| \leq p^r$. ∎

הגדרה 7.2: (א) פולינום $f \in K[X]$ הוא **פריד** (**ספרבילי**) אם כל שורשיו ב־$\tilde{K}$ פשוטים.

(ב) איבר α **פריד** (**ספרבילי**) מעל K אם α אלגברי מעל K ו־$\mathrm{irr}(\alpha, K)$ פריד.

(ג) הרחבה L/K **פרידה** (**ספרבילית**) אם L/K אלגברית וכל $\alpha \in L$ פריד מעל K.

(ד) K הינו **מושלם** (perfect) אם כל הרחבה אלגברית של K פרידה, כלומר, לכל פולינום אי פריק מעל K יש שורשים פשוטים ב־$\tilde{K}$. ∎

מסקנה 6.9(א) נותנת:

משפט 7.3: *אם $\mathrm{char}(K) = 0$ אז K מושלם.*

דוגמה 7.4: $\mathbb{F}_p(t)$ אינו מושלם: $f(X) = X^p - t$ אי פריק, יש לו שורש אחד (מרובה). ∎

משפט 7.5 (משפט האיבר הפרימיטיבי): *תהי L/K הרחבה סופית פרידה. אז יש $\alpha \in L$ כך ש־$L = K(\alpha)$.*

הוכחה: אם K שדה סופי אז L מרחב וקטורי ממימד סופי מעל שדה סופי ולכן גם הוא סופי. לכן $L^\times$ חבורה סופית. לפי משפט 7.1 יש $\alpha \in L^\times$ כך ש־$L^\times = \{\alpha^i |\ i \in \mathbb{N}\}$. אז $L = K(\alpha)$.

נניח כי K שדה אינסופי. לפי מסקנה 4.15(ב) יש $\alpha_1, \ldots, \alpha_k \in L$ כך ש־$L = K(\alpha_1, \ldots, \alpha_k)$. נמשיך באינדוקציה על k. עבור $k = 1$ אין מה להוכיח. עבור $k = 2$ נוכיח:

טענה: *יהיו $a, b \in L$. אז יש $c \in K$ כך ש־$K(a, b) = K(a - cb)$.*

יהיו

$$f = \mathrm{irr}(a, K) = (X - a)(X - a_1) \cdots (X - a_m) \qquad a_i \in \tilde{K},$$

$$g = \mathrm{irr}(b, K) = (X - b)(X - b_1) \cdots (X - b_n), \qquad b_j \in \tilde{K}$$

באשר $a, a_1, \ldots, a_m$ שונים זה מזה ו־$b, b_1, \ldots, b_n$ שונים זה מזה.

הקבוצה $S=\{\frac{a_i-a}{b_j-b}|\ 1\le i\le m,\ 1\le j\le n\}\cup\{0\}$ היא סופית. לכן קיים $c\in K\smallsetminus S$. נגדיר $\gamma=a-cb$. אז $K(\gamma)\subseteq K(a,b)$. כיוון ש־$c\notin S$, מתקיים $c(b_j-b)\ne a_i-a, 0$ לכל i,j, כלומר

$$\gamma+cb_j\ne a_i,a \qquad \text{לכל } i,j. \tag{1}$$

יהי $h(X)=f(\gamma+cX)\in K(\gamma)[X]$. אז $h(b)=f(\gamma+cb)=f(a)=0$, ו־$h(b_j)=f(\gamma+cb_j)\ne 0$, לפי (1). לכן $X-b\in\gcd(h,g)\in K(\gamma)[X]$, ומכאן $b\in K(\gamma)$. לכן גם $a=\gamma+cb\in K(\gamma)$. בכך הוכחה הטענה.

יהי $k\ge 2$. לפי הטענה יש β כך ש־$K(\alpha_1,\alpha_2)=K(\beta)$. לפי הנחת האינדוקציה יש α כך ש־

$$K(\alpha_1,\dots,\alpha_k)=K(\alpha_1,\alpha_2)(\alpha_3,\dots,\alpha_k)=K(\beta)(\alpha_3,\dots,\alpha_k)=$$
$$=K(\beta,\alpha_3\dots,\alpha_k)=K(\alpha). \qquad \blacksquare$$

דוגמה 7.6: יהי $L=\mathbb{F}_p(t,u)$, שדה הפונקציות הרציונליות בשני משתנים t,u מעל $\mathbb{F}_p$. יהי

$$K=\mathbb{F}_p(t^p,u^p)=\Big\{\sum_{ij}a_{ij}t^{pi}u^{pj}\big/\sum_{ij}b_{ij}t^{pi}u^{pj}\Big|a_{ij},b_{ij}\in\mathbb{F}_p\Big\}\subseteq L.$$

אז $L=K(t,u)$ ו־$[K(t):K],[K(u):K]\le p$, לכן $[L:K]\le p^2$. אפשר לראות כי $[L:K]=p^2$, כי $(t^iu^j|\ 0\le i,j<p)$ בלתי תלויים לינארית מעל K. (בדוק!) אבל $L\ne K(\alpha)$ לכל $\alpha\in L$. אכן, אם $\alpha=\sum_{ij}a_{ij}t^iu^j/\sum_{ij}b_{ij}t^iu^j$, באשר $a_{ij},b_{ij}\in\mathbb{F}_p$, אז $\alpha^p=\sum_{ij}a_{ij}^pt^{pi}u^{pj}/\sum_{ij}b_{ij}^pt^{pi}u^{pj}\in K$, לכן $[K(\alpha):K]\le p$. $\blacksquare$

הגדרה 7.7: אם $L_1/K,L_2/K$ שתי הרחבות, יהי

$$\mathrm{Ism}_K(L_1,L_2)=\{\sigma\colon L_1\to L_2|\ \sigma \text{ הוא שיכון־} K\}.$$

אם L/K אלגברית, יהי $[L:K]_s=|\mathrm{Ism}_K(L,\tilde K)|\in\mathbb{N}\cup\{\infty\}$ **מעלת הפרידות של** L/K. גודל זה זה אינו תלוי בבחירה של סגור אלגברי $\tilde K$. לכן בלי הגבלת הכלליות $L\subseteq\tilde K$.

דוגמה 7.8: יהי $L=K(\alpha)$, באשר $\alpha\in\tilde K$. יהי $p=\mathrm{irr}(\alpha,K)$, נאמר, $p=(X-\alpha_1)\cdots(X-\alpha_n)$ מעל $\tilde K$, באשר $\alpha_1=\alpha$. אם $\sigma\in\mathrm{Ism}_K(L,\tilde K)$, אז $\sigma(\alpha)$ שורש של p, לכן $\sigma(\alpha)=\alpha_i$ עבור איזה i. אבל לכל $1\le i\le n$ יש איזומורפיזם יחיד $\sigma_i\colon L\to K(\alpha_i)\subseteq\tilde K$ כך ש־$\sigma_i(\alpha)=\alpha_i$. לכן $\mathrm{Ism}_K(L,\tilde K)=\{\sigma_1,\dots,\sigma_n\}$. מכאן ש־$[L:K]_s$ הוא מספר השורשים *השונים* מבין $\alpha_1,\dots,\alpha_n$. בפרט

(א) $[L:K]_s\le[L:K]$;

(ב) $[L:K]_s=[L:K]$ אם ורק אם α פריד מעל K. $\blacksquare$

משפט 7.9: *תהיינה* $K \subseteq L \subseteq M$ *הרחבות אלגבריות. אז* $[M:K]_s = [M:L]_s \cdot [L:K]_s$.

הוכחה: בלי הגבלת הכלליות $M \subseteq \tilde{K}$, לכן $\tilde{K}$ סגור אלגברי של K, L, M. צריך להוכיח: $|\mathrm{Ism}_K(M,\tilde{K})| = |\mathrm{Ism}_L(M,\tilde{K})| \cdot |\mathrm{Ism}_K(L,\tilde{K})|$. תהי $\rho\colon \mathrm{Ism}_K(M,\tilde{K}) \to \mathrm{Ism}_K(L,\tilde{K})$ העתקת הצמצום. לפי משפט 5.6(ג), היא על. לכן די להראות כי

- לכל $\lambda \in \mathrm{Ism}_K(L,\tilde{K})$ מתקיים $|\rho^{-1}(\lambda)| = |\mathrm{Ism}_L(M,\tilde{K})|$,

ואכן, לפי מסקנה 5.7 אפשר להרחיב את λ לאוטומורפיזם $\tilde{\lambda}$ של $\tilde{K}$. יש העתקה

$$\mathrm{Ism}_L(M,\tilde{K}) = \{\sigma\colon M \to \tilde{K} \mid \sigma|_L = 1_L\} \longrightarrow \{\sigma'\colon M \to \tilde{K} \mid \sigma'|_L = \lambda\} = \rho^{-1}(\lambda)$$

הנתונה על ידי $\sigma \mapsto \tilde{\lambda} \circ \sigma$ ואילו $\sigma' \mapsto \tilde{\lambda}^{-1} \circ \sigma'$ היא ההופכי שלה. לכן שתי הקבוצות שוות עוצמה. ∎

משפט 7.10: *תהי* L/K *הרחבה סופית. אז*

(א) $[L:K]_s \le [L:K]$;

(ב) $[L:K]_s = [L:K]$ *אם ורק אם* L/K *פרידה.*

הוכחה: (א) לפי מסקנה 4.15(ב), $L = K(\alpha_1,\dots,\alpha_n)$. נגדיר $L_i = K(\alpha_1,\dots,\alpha_i)$ לכל $0 \le i \le n$. אז $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = L$ ומתקיים $L_i = L_{i-1}(\alpha_i)$. לפי דוגמה 7.8, $[L_i : L_{i-1}]_s \le [L_i : L_{i-1}]$ לכל i. לכן לפי נוסחות המכפלה

$$[L:K]_s = \prod_{i=1}^{n} [L_i : L_{i-1}]_s \le \prod_{i=1}^{n} [L_i : L_{i-1}] = [L:K].$$

(ב) אם L/K פרידה, אז $L = K(\alpha)$ עבור איזה $\alpha \in L$, לכן, לפי דוגמה 7.8, $[L:K]_s = [L:K]$. אם L/K אינה פרידה, אז יש $\alpha \in L$ שאינו פריד מעל K, לכן לפי דוגמה 7.8, $[K(\alpha):K]_s < [K(\alpha):K]$. לפי (א), $[L:K(\alpha)]_s \le [L:K(\alpha)]$, לכן לפי נוסחות המכפלה $[L:K]_s < [L:K]$. ∎

מסקנה 7.11: *איבר* α *פריד מעל* K *אם ורק אם* $K(\alpha)/K$ *פרידה.*

הוכחה: α פריד מעל K אם ורק אם $[K(\alpha):K]_s = [K(\alpha):K]$ אם ורק אם $K(\alpha)/K$ פרידה. ∎

תרגיל 7.12: *יהיו* $K \subseteq L \subseteq M$ *שדות. יהי* $\alpha \in M$. *אם* α *פריד מעל* K *אז הוא פריד מעל* L.

הוכחה: בלי הגבלת הכלליות $\tilde{K} \subseteq \tilde{L} \subseteq \tilde{M}$. יהיו $f = \mathrm{irr}(\alpha,K) \in K[X]$, $p = \mathrm{irr}(\alpha,L) \in L[X]$. אז ל־$f$ אין שורשים מרובים ב־$\tilde{K}$ ולכן גם לא ב־$\tilde{L}$. אבל $p \mid f$ ב־$L[X]$ ולכן ב־$\tilde{L}[X]$, לכן גם ל־p אין שורשים מרובים ב־$\tilde{L}$. לכן α פריד מעל L. ∎

משפט 7.13: *יהיו* $K \subseteq L, F \subseteq M$ *שדות.*

(א) M/K *פרידה אם ורק אם* L/K, M/L *פרידות.*

(ב) *אם L/K פרידה, אז LF/F פרידה.*

(ג) *אם L/K, F/K פרידות אז LF/K פרידה*

הוכחה: (ג) נובע באופן פורמלי מתוך (א), (ב).

(א) אם M/K סופית, זה נובע מנוסחות המכפלה. במקרה הכללי: נניח כי M/K פרידה. אז L/K פרידה, כי $L \subseteq M$, ו־M/L פרידה לפי תרגיל 7.12.

להיפך, נניח כי L/K, M/L פרידות. יהי $\alpha \in M$ ויהי $p = \operatorname{irr}(\alpha, L) = \sum_i a_i X^i \in L[X]$. יהי $E = K(a_0, a_1, \dots) \subseteq L$. אז $[E : K] < \infty$ ו־$p = \operatorname{irr}(\alpha, E) \in E[X]$. לפי ההנחה p פריד, לכן α פריד מעל E, ולכן $[E(\alpha) : E]_s = [E(\alpha) : E]$. לפי הפסקה הקודמת E/K פרידה, כי $K \subseteq E \subseteq L$. לכן $[E : K]_s = [E : K]$. לפי נוסחת המכפלה $[E(\alpha) : K]_s = [E(\alpha) : K]$. לכן α פריד מעל K.

(ב) כמו בהוכחת (ב) של משפט 4.18, $LF = \bigcup_{S \subseteq L \text{ סופית}} F(S)$. לכן די להוכיח כי $F(S)/F$ הרחבה פרידה לכל $S \subseteq L$ סופית. לפי משפט 7.5 יש $\alpha \in L$ כך ש־$K(S) = K(\alpha)$, לכן $F(S) = F(\alpha)$. כעת α פריד מעל K, לכן לפי תרגיל 7.12 הוא פריד מעל F. לכן $F(S) = F(\alpha)$ פרידה מעל F ∎

טענה 7.14: *נניח $L = K(S) \subseteq \tilde{K}$. אז L/K פרידה אם ורק אם כל $\alpha \in S$ פריד מעל K.*

הוכחה: אם L/K פרידה אז כל $\alpha \in L$ פריד מעל K (הגדרה 7.2(ג)).

להיפך, נניח כי כל $\alpha \in S$ פריד מעל K. אז $K(\alpha)/K$ פרידה לכל $\alpha \in S$, לפי מסקנה 7.11. לכן אם S סופית אז L/K פרידה לפי משפט 7.13(ג), באינדוקציה על מספר אברי S.

במקרה הכללי $\bigcup_{S' \subseteq S \text{ סופית}} K(S')$ הוא שדה (כי $K(S') \cup K(S'') \subseteq K(S' \cup S'')$ לכל $S', S'' \subseteq S$ סופיות) שמוכל ב־$K(S)$ ומכיל את S, לכן שדה זה הוא L. לפי הפסקה הקודמת כל אבריו הם פרידים, לכן L/K פרידה. ∎

8. הרחבות נורמליות

יהי K שדה. יהי $\tilde{K}$ סגור אלגברי של K.

הגדרה 8.1: (א) $0 \neq f \in K[X]$ **מתפצל מעל** K אם $f = c(X-\alpha_1)\cdots(X-\alpha_n)$, באשר $c \in K^\times$ ו־$\alpha_1, \dots, \alpha_n \in K$.

(ב) תהי $\mathcal{F} \subseteq K[X]$ קבוצה של פולינומים ממעלה ≤ 1. הרחבה L/K היא **שדה פיצול של** $\mathcal{F}$ **מעל** K אם כל $f \in \mathcal{F}$ מתפצל מעל L ו־L נוצר על ידי השורשים של אברי $\mathcal{F}$ ב־L.

הערה 8.2: קיום ויחידות. התת־שדה L של $\tilde{K}$ שנוצר מעל K על ידי כל השורשים ב־$\tilde{K}$ של כל אברי $\mathcal{F}$ הוא שדה הפיצול היחיד של $\mathcal{F}$ מעל K בתוך $\tilde{K}$. זהו השדה הקטן ביותר ב־$\tilde{K}$ שמכיל את K וכל $f \in \mathcal{F}$ מתפצל מעליו.

הגדרה 8.3: הרחבה אלגברית L/K היא **נורמלית** אם כל $p \in K[X]$ אי פריק, שיש לו שורש ב־L, מתפצל מעל L.

משפט 8.4: *יהי L שדה, $K \subseteq L \subseteq \tilde{K}$. התנאים הבאים שקולים:*

(א) *L/K נורמלית.*

(ב) *יש משפחה $\mathcal{F} \subseteq K[X]$ כך ש־L הוא שדה הפיצול שלה ב־$\tilde{K}$.*

(ג) *כל הומומורפיזם־K $\sigma\colon L \to \tilde{K}$ הוא אוטומורפיזם של L.*

(ד) *כל אוטומורפיזם־K של $\tilde{K}$ מעתיק את L על L.*

הוכחה: (א) $\Leftarrow$(ב): תהי $\mathcal{F} = \{\mathrm{irr}(\alpha, K) \mid \alpha \in L\}$ ויהי L' שדה הפיצול של $\mathcal{F}$ בתוך $\tilde{K}$. נראה $L = L'$. לפי (א) כל $f \in \mathcal{F}$ מתפצל מעל L, לכן $L' \subseteq L$. להיפך, כל $\alpha \in L$ הוא שורש של איזה $f \in \mathcal{F}$, לכן $\alpha \in L'$; מכאן $L \subseteq L'$.

(ב) $\Leftarrow$(ג): כיוון ש־σ חח"ע, הוא איזומורפיזם־K $L \to \sigma(L)$. לכן גם $\sigma(L)$ הוא שדה הפיצול של $\mathcal{F}$ מעל K בתוך $\tilde{K}$. מהיחידות, $L = \sigma(L)$.

(ג) $\Leftarrow$(ד): ברור.

(ד) $\Leftarrow$(א): יהי $p \in K[X]$ אי פריק, יהי $\alpha \in L$ שורשו, והי $\alpha' \in \tilde{K}$ שורש אחר שלו. צריך להראות כי $\alpha' \in L$. לפי משפט 4.11(ז) קיים איזומורפיזם־K $\sigma_0\colon K(\alpha) \to K(\alpha') \subseteq \tilde{K}$. לפי מסקנה 5.7 אפשר להרחיב את σ_0 לאוטומורפיזם־K σ של $\tilde{K}$. לכן $\alpha' \in \sigma(L) = L$. ∎

דוגמאות 8.5: (א) כל הרחבה **ריבועית** L/K (דהיינו, $[L:K] = 2$) היא נורמלית.

אכן, יהי $p \in K[X]$ אי פריק שיש לו שורש $\alpha \in L$. אז $p = (X-\alpha)q$, באשר $q \in L[X]$. אך $K \subseteq K(\alpha) \subseteq L$, לכן $\deg p = [K(\alpha):K] \leq [L:K] = 2$. מכאן $q = c \in L^\times$ או $q = c(X-\beta)$, באשר $\beta \in L$, $c \in L^\times$. בשני המקרים p מתפצל מעל L.

(ב) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ הרחבות ריבועיות ולכן נורמליות. אבל $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ אינה נורמלית. אכן, $\sqrt[4]{2}$ שורש של $X^4 - 2 \in \mathbb{Q}[X]$ שהינו אי פריק מעל $\mathbb{Q}$ (איזנשטיין), לכן $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}) = X^4 - 2$. שורשיו

ב־$\mathbb{C}$ הם $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. אך $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$, כי $\pm i\sqrt[4]{2} \notin \mathbb{R}$, ו־$\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.

(ג) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ אינה נורמלית. אך $\mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ שדה הפיצול של $X^4 - 2$ מעל $\mathbb{Q}$, לכן $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ נורמלית. ∎

משפט 8.6: *יהיו $K \subseteq L, F \subseteq M$ שדות.*

(א) *אם M/K נורמלית אז M/L נורמלית.*

(ב) *אם L/K נורמלית, אז LF/F נורמלית.*

(ג) *אם L/K, F/K נורמליות אז LF/K, $L \cap F/K$ נורמליות.*

הוכחה: (א) יש $\mathcal{F} \subseteq K[X]$ כך ש־M שדה הפיצול של $\mathcal{F}$ מעל K. אז M שדה הפיצול של $\mathcal{F} \subseteq L[X]$ מעל L.

(ב) יש $\mathcal{F} \subseteq K[X]$ כך ש־L שדה הפיצול של $\mathcal{F}$ מעל K. אז LF שדה הפיצול של $\mathcal{F} \subseteq F[X]$ מעל F.

(ג) לפי משפט 4.18, LF/K אלגברית. לכן סגור אלגברי של LF הוא סגור אלגברי של K. נסמנו $\tilde{K}$. יהי σ אוטומ' K־ של $\tilde{K}$. אז $\sigma(F) = F$, $\sigma(L) = L$. לכן $\sigma(L \cap F) = L \cap F$ ו־$\sigma(LF) = \sigma(L)\sigma(F) = LF$.

∎

משפט 8.7: *תהי L/K הרחבה אלגברית, $L \subseteq \tilde{K}$. אז קיימת הרחבת נורמלית קטנה ביותר M/K כך ש־ $L \subseteq M \subseteq \tilde{K}$.*
אם L/K סופית, גם M/K סופית. אם $L = K(S)$ אז M שדה הפיצול של $\{\mathrm{irr}(\alpha, K) |\ \alpha \in S\}$ ב־ $\tilde{K}$.

הוכחה: תהי $S \subseteq L$ כך ש־$L = K(S)$ (למשל, $S = L$). תהי $\mathcal{F} = \{\mathrm{irr}(\alpha, K) |\ \alpha \in S\}$. יהי M שדה הפיצול של $\mathcal{F}$ ב־$\tilde{K}$. אז M/K נורמלית, $S \subseteq M$, לכן $L = K(S) \subseteq M$. אם $L \subseteq M' \subseteq \tilde{K}$ ו־M'/K נורמלית, אז לכל $f \in \mathcal{F}$ יש שורש ב־M'־$L \subseteq$, ולכן f מתפצל מעל M'. לכן $M \subseteq M'$.

נניח כי L/K סופית. אז יש S סופית כך ש־$L = K(S)$. אז $\mathcal{F}$ סופית, ולכן M נוצר מעל K על ידי קבוצה סופית (כל שורשי $\mathcal{F}$). לפי מסקנה 4.15(ב), M/K סופית. ∎

הגדרה 8.8: הרחבה M כזאת תקרא **הסגור הנורמלי** של L/K.

טענה 8.9: *יהי $M \subseteq \tilde{K}$ הסגור הנורמלי של L/K פרידה. אז M/K פרידה.*

הוכחה: לפי משפט 8.7, M הוא שדה הפיצול של $\mathcal{F} = \{\mathrm{irr}(\alpha, K) |\ \alpha \in L\}$. כלומר, $M = K(S)$, באשר S קבוצת כל השורשים של אברי $\mathcal{F}$ ב־$\tilde{K}$. כל אברי $\mathcal{F}$ הם פרידים, לכן כל אברי S הם פרידים. לפי טענה 7.14, $M = K(S)$ פרידה מעל K. ∎

תרגיל 8.10: *יהי $f \in K[X]$ ממעלה $n \geq 1$. יהי L שדה הפיצול שלו מעל K. אז $[L : K] \leq n!$.*

דוגמה: יהי $f(X) = X^3 - 3X - 1$. יהי L שדה הפיצול שלו מעל $\mathbb{Q}$. אז $[L : \mathbb{Q}] = 3$.

ההוכחה מבוססת על סדרת טענות:

(א) ל־f אין שורש ב־$\mathbb{Z}$:

בדיקה ישירה מראה ש־± 1 אינם שורשים של f. כל מספר אחר $k \in \mathbb{Z}$ יש ראשוני p שמחלק את k, ואז הוא מחלק את $k^3 - 3k$. מאידך, p אינו מחלק את 1, לכן $k^3 - 3k \neq 1$, כלומר, k אינו שורש של f.

(ב) f אי פריק מעל $\mathbb{Z}$:

אחרת ל־f יש גורם ממעלה ראשונה מעל $\mathbb{Z}$. גורם זה הינו מתוקן, כי מכפלת המקדמים העליונים של הגורמים של f הוא המקדם העליון של f, שהינו 1. לכן גורם זה הוא מהצורה $X-k$, באשר $k \in \mathbb{Z}$. אבל אז k שורש של f, בסתירה ל(א).

(ג) לפי הלמה של גאוס, f אי פריק מעל $\mathbb{Q}$.

יהי α שורש של f בסגור האלגברי של $\mathbb{Q}$ ויהי $L=\mathbb{Q}(\alpha)$. לפי (ג)

(ד) $[L:\mathbb{Q}]=3$

לבסוף לא קשה (אם כי קצת מייגע - ראה בהמשך) לבדוק כי

$$\begin{aligned}\beta =&\alpha^2-\alpha-2\\ \gamma =&-\alpha^2+2\end{aligned}$$

הם שורשים של f. אז, כיוון ש־α,β,γ הם שונים זה מזה, הם שלושת השורשים של f בסגור האלגברי של $\mathbb{Q}$. כיוון שהם ב־L, השדה הזה הוא שדה הפיצול של f מעל $\mathbb{Q}$.

החישובים: כיוון ש־α מקיים $\alpha^3-3\alpha-1=f(\alpha)=0$, מתקיים

$$\begin{aligned}\alpha^3 =&3\alpha+1\\ \alpha^4 =&3\alpha^2+\alpha\\ \alpha^5 =&3\alpha^3+\alpha^2=3(3\alpha+1)+\alpha^2=\alpha^2+9\alpha+3\\ \alpha^6 =&\alpha^3+9\alpha^2+3\alpha=3\alpha+1+9\alpha^2+3\alpha=9\alpha^2+6\alpha+1\end{aligned}$$

מכאן:

$$\begin{aligned}\beta =&\alpha^2-\alpha-2\\ \beta^2 =&(\alpha^2-\alpha-2)^2=\alpha^4+\alpha^2+4-2\alpha^3-4\alpha^2+4\alpha=\\ =&3\alpha^2+\alpha+\alpha^2+4-6\alpha-2-4\alpha^2+4\alpha=-\alpha+2\\ \beta^3 =&(\alpha^2-\alpha-2)(-\alpha+2)=-\alpha^3+\alpha^2+2\alpha+2\alpha^2-2\alpha-4=-3\alpha-1+3\alpha^2-4=\\ =&3(\alpha^2-\alpha-2)+1=3\beta+1\end{aligned}$$

ולכן $f(\beta)=0$.

סכום השורשים של f הוא הנגדי של המקדם של X^2 ב־f, כלומר 0, ולכן השורש השלישי של f הוא $\gamma=0-\alpha-\beta=-\alpha-(\alpha^2-\alpha-2)=\alpha^2+2$. ∎

9. הרחבות של שדות סופיים

יהי K שדה סופי, $|K| = q < \infty$. יהי $\tilde{K}$ סגור אלגברי של K.

משפט 9.1: *(א)* $\mathrm{char}(K) > 0$.

(ב) $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

(ג) $\alpha^q = \alpha$ *לכל* $\alpha \in K$.

(ד) *אם* L/K *הרחבה ממעלה* $n < \infty$ *אז* $|L| = q^n$.

(ה) $q = p^k$, *באשר* $p = \mathrm{char}(K)$ *ו־*$k = [K : \mathbb{F}_p]$.

הוכחה: (א) השדה הראשוני של K מוכל ב־K, לכן גם הוא סופי.

(ב) $|K^\times| = |K| - 1 = q - 1$ ולפי משפט 7.1, $K^\times$ חבורה מעגלית.

(ג) אם $\alpha = 0$, ברור. יהי $\alpha \in K^\times$. הסדר של איבר בחבורה מחלק את הסדר של החבורה, לכן $\alpha^{q-1} = 1$. נכפיל זאת ב־α.

(ד) $L \cong K^n$ (איזומורפיזם של מרחבים וקטוריים מעל K).

(ה) לפי (ד), עבור ההרחבה $K/\mathbb{F}_p$ במקום L/K. ∎

משפט 9.2: *יהי* $n \in \mathbb{N}$. *אז* $K_n = \{\alpha \in \tilde{K} | \ \alpha^{q^n} = \alpha\}$ *הוא שדה, והוא הרחבה ממעלה* n *של* K.

הוכחה: נסמן $p = \mathrm{char}(K)$.

יהיו $\alpha, \beta \in K_n$. אז $(\alpha\beta)^{q^n} = \alpha^{q^n}\beta^{q^n} = \alpha\beta$, לכן $\alpha\beta \in K_n$. באופן דומה $\alpha/\beta \in K_n$, אם $\beta \neq 0$. באינדוקציה, $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ לכל $m \geq 0$. לפי המשפט הקודם q חזקה של p, לכן גם q^n. מכאן $(\alpha+\beta)^{q^n} = \alpha^{q^n} + \beta^{q^n}$. מכאן $\alpha + \beta \in K_n$. באופן דומה $\alpha - \beta \in K_n$. (אם $p = 2$, אז $-1 = 1$ ב־K.) לכן K_n שדה. לפי משפט 9.1(ג), $K \subseteq K_n$.

אברי K_n הם השורשים של $f = X^{q^n} - X$ ב־$\tilde{K}$. ל־f אין שורשים מרובים, כי $f' = q^n X^{q^n - 1} - 1 = -1$ זר ל־f. לכן $|K_n| = \deg f = q^n$. לפי משפט 9.1(ד), $[K_n : K] = n$. ∎

משפט 9.3: *יהי* $n \in \mathbb{N}$. *אז*

(א) K_n *ההרחבה היחידה של* K *ממעלה* n *בתוך* $\tilde{K}$. *בפרט,* $K = (\mathbb{F}_p)_k$, *באשר* $\mathbb{F}_p$ *השדה הראשוני של* K *ו־*$k = [K : \mathbb{F}_p]$.

(ב) K_n/K *נורמלית:* K_n *הוא שדה הפיצול של* $X^{q^n} - X = f$ *מעל* K *בתוך* $\tilde{K}$.

(ג) K_n/K *פרידה.*

הוכחה: (א) תהי $L \subseteq \tilde{K}$ הרחבה ממעלה n של K. אז $|L| = q^n = |K_n|$, לכן די להוכיח $L \subseteq K_n$.

ואכן, יהי $\alpha \in L$. אם $\alpha = 0$ אז $\alpha \in K_n$. אם $\alpha \in L^\times$, אז הסדר שלו מחלק את סדר החבורה $L^\times$, לכן $\alpha^{q^n - 1} = 1$ לכל $\alpha \in L^\times$. לכן $\alpha^{q^n} = \alpha$.

(ב) ברור.

(ג) יהי $\alpha \in K_n$. אז $f(\alpha) = 0$, לכן $f \mid \operatorname{irr}(\alpha, K)$. אבל ל־$f$ אין שורשים מרובים (כי $f' = -1$) לכן גם ל־$\operatorname{irr}(\alpha, K)$ אין שורשים מרובים. ∎

תרגיל 9.4: *יהי p ראשוני ויהי $\widetilde{\mathbb{F}_p}$ סגור אלגברי שלו. לכל $n \in \mathbb{N}$ תהי $\mathbb{F}_{p^n} = (\mathbb{F}_p)_n$ ההרחבה היחידה של $\mathbb{F}_p$ ממעלה n בתוך $\widetilde{\mathbb{F}_p}$. הוכח: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ אם ורק אם $m \mid n$.*

10. המשפטים היסודיים של תורת גלואה

יהי K שדה. יהי $\tilde{K}$ סגור אלגברי של K.

אם L/K הרחבת שדות, $\mathrm{Aut}(L/K)$ יסמן את קבוצת אוטומורפיזמי־K של L. זוהי חבורה (ביחס להרכבה).

הגדרה 10.1: הרחבה L/K נקראת **הרחבת גלואה** (Galois) אם היא אלגברית, נורמלית ופרידה. ∎

דוגמה 10.2: כל הרחבה ריבועית של שדה בעל אפיון 0; שדה פיצול L של פולינום $f \in K[X]$ שאין לו שורשים מרובים; הרחבת הסגור האלגברי $\tilde{K}/K$, אם K מושלם. ∎

הגדרה 10.4: תהי L/K הרחבת גלואה. קבוצת כל אוטומורפיזמי־K של L היא חבורה $\mathrm{Gal}(L/K)$ (ביחס להרכבה), שנקראת **חבורת גלואה של** L/K.

יהי $\tilde{K}$ סגור אלגברי של K כך ש־$L \subseteq \tilde{K}$. אז $\mathrm{Gal}(L/K) = \mathrm{Ism}_K(L, \tilde{K})$. לכן:

משפט 10.5: *תהי L/K הרחבת גלואה סופית. אז* $|\mathrm{Gal}(L/K)| = [L : K]$.

דוגמה 10.6: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1 = 1_L, \varepsilon\}$, באשר $\varepsilon(\sqrt{2}) = -\sqrt{2}$, כלומר $\varepsilon(a + b\sqrt{2}) = a - b\sqrt{2}$, אכן, $f = X^2 - 2$ אי פריק מעל $\mathbb{Q}$. כל $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}/\mathbb{Q})$ בהכרח מעתיק שורש של f לשורש אחר שלו, לכן $\sigma(\sqrt{2}) = \pm\sqrt{2}$. אך יש הומומורפיזם־$\mathbb{Q}$ יחיד $\sigma\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ עבורו $\sigma(\sqrt{2}) = \sqrt{2}$ (או $\sigma(\sqrt{2}) = -\sqrt{2}$). ∎

תרגיל 10.7: *תהי L/K פרידה ויהי $n \in \mathbb{N}$ כך ש־ $[K(\alpha) : K] \le n$ לכל $\alpha \in L$. אז $[L : K] \le n$. (בפרט L/K סופית.)*

הוכחה: נניח בשלילה כי $[L : K] > n$. אז יש $\alpha_1, \ldots, \alpha_{n+1} \in L$ בלתי תלויים לינארית מעל K. לפי משפט האיבר הפרימיטיבי יש $\alpha \in L$ כך ש־$K(\alpha) = K(\alpha_1, \ldots, \alpha_{n+1})$. אז $[K(\alpha) : K] = \dim_K K(\alpha_1, \ldots, \alpha_{n+1}) > n$, סתירה. ∎

הגדרה 10.8: יהי L שדה ותהי H חבורה של אוטומורפיזמים שלו (לא בהכרח כולם), כלומר $H \le \mathrm{Aut}(L)$. נסמן $L^H = \{\alpha \in L |\ \sigma(\alpha) = \alpha$ לכל $\sigma \in H\}$. אז L^H הוא תת־שדה של L שנקרא **שדה השֶבֶת** של H ב־L. נשים לב ש־$H \subseteq \mathrm{Aut}(L/L^H)$. ∎

משפט 10.9 (הלמה של ארטין): *יהי L שדה ותהי H חבורה של אוטומורפיזמים של L כך שלכל $\alpha \in L$ הקבוצה $\{\sigma(\alpha) |\ \sigma \in H\}$ סופית. יהי $E = L^H$. אז L/E הרחבת גלואה. אם H סופית אז L/E סופית ו־$H = \mathrm{Gal}(L/E)$.*

הוכחה: יהי $\alpha \in L$. נבחר $\sigma_1, \ldots, \sigma_r \in H$ כך ש־$\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ הם כל האיברים השונים של $\{\sigma(\alpha) |\ \sigma \in H\}$. בלי הגבלת הכלליות $\sigma_1 = 1_L$. אם $\tau \in H$ אז

$$\tau\sigma_1(\alpha), \ldots, \tau\sigma_r(\alpha) \in \{\tau\sigma(\alpha) |\ \sigma \in H\} = \{\sigma(\alpha) |\ \sigma \in H\}$$

שונים זה מזה, לכן

$$.\{\tau\sigma_1(\alpha),\dots,\tau\sigma_r(\alpha)\} = \{\sigma_1(\alpha),\dots,\sigma_r(\alpha)\}$$

יהי $f = \prod_{i=1}^{r}\big(X-\sigma_i(\alpha)\big) \in L[X]$. לכל אוטומורפיזם τ של L נסמן ב־τf את הפולינום ב־$L[X]$ המתקבל מ־f על ידי הפעלת τ על מקדמים של f. אם $\tau \in H$, אז

$$\tau f = \prod_{i=1}^{r}\big(X-\tau\sigma_i(\alpha)\big) = \prod_{i=1}^{r}\big(X-\sigma_i(\alpha)\big) = f$$

לכן $f \in E[X]$. כעת, $f(\alpha)=0$ ומתקיים:

(א) ל־f (ולכן גם ל־$\mathrm{irr}(\alpha,E)$) אין שורשים מרובים, לכן α פריד מעל E.

(ב) f (ולכן גם $\mathrm{irr}(\alpha,E)$) מתפצל מעל L.

(ג) $[E(\alpha):E] = \deg\mathrm{irr}(\alpha,E) \le \deg f = r \le |H|$.

לפי (א), L/E פרידה. לפי (ב) היא נורמלית. לכן היא גלואה. נניח ש־H סופית. לפי (ג) ותרגיל 10.7, $[L:E] \le |H|$. לכן L/E סופית. מתקיים $|\mathrm{Gal}(L/E)| = [L:E]$ ו־$H \subseteq \mathrm{Gal}(L/E)$, לכן $H = \mathrm{Gal}(L/E)$. ∎

$\{\sigma(\alpha)|\ \sigma\in H\}$ סופית. יהי $E = L^H$. אז L/E הרחבת גלואה. אם H סופית אז L/E סופית ו־$H = \mathrm{Gal}(L/E)$.

תרגיל 10.10: *יהי L שדה ותהי H חבורה של אוטומורפיזמים של L כך שלכל $\alpha\in L$ הקבוצה $\{\sigma(\alpha)|\ \sigma\in H\}$ סופית (כמו בלמה של ארטין). יהי $E = L^H$. אם $\sigma\in\mathrm{Gal}(L/E)$ ו־$\alpha\in L$, אז יש $\tau\in H$ כך ש־$\sigma(\alpha)=\tau(\alpha)$.*

הוכחה: יהי f כמו בהוכחה של הלמה. אז $f\in E[X]$ ולכן $\sigma f = f$. כעת, α שורש של f, לכן $\sigma(\alpha)$ שורש של $\sigma f = f$. לכן יש $1\le i\le r$ כך ש־$\sigma(\alpha)=\sigma_i(\alpha)$. ניקח $\tau = \sigma_i \in H$. ∎

הגדרה 10.11: יהי L שדה ותהי H תת חבורה של $\mathrm{Aut}(L)$.

(א) **הסגור** של H הוא $\bar{H} = \{\sigma\in\mathrm{Aut}(L)|\ \sigma(\alpha)=\tau_\alpha(\alpha)$ כך ש־ $\tau_\alpha\in H$ קיים $\alpha\in L$ לכל $\}$.

(ב) H נקראת **סגורה** אם $\bar{H}=H$. ∎

תרגיל:

(א) *$\bar{H}$ תת חבורה של $\mathrm{Aut}(L)$.*

(ב) $H \subseteq \bar{H}$.

(ג) *אם $H \le G \le \mathrm{Aut}(L)$ אז $\bar{H}\subseteq\bar{G}$.*

למה 10.12: *יהי L שדה.*

(א) *יהי E תת שדה של L. אז $\mathrm{Aut}(L/E)$ סגורה.*

(ב) *תת חבורה סופית H של $\mathrm{Aut}(L)$ הינה סגורה.*

(ג) *אם L הרחבה אלגברית של K ו־ $E = L^H$ שדה השבת של $H \leq \mathrm{Aut}(L/K)$, אז L/E גלואה ו־ $\mathrm{Gal}(L/E) = \bar{H}$.*

הוכחה: (א) יהי σ בסגור של $\mathrm{Aut}(L/E)$. אז לכל $\alpha \in L$ יש $\tau_\alpha \in \mathrm{Aut}(L/E)$ כך ש־$\sigma(\alpha) = \tau_\alpha(\alpha)$. בפרט לכל $\alpha \in E$ מתקיים $\sigma(\alpha) = \tau_\alpha(\alpha) = \alpha$, לכן $\sigma \in \mathrm{Aut}(L/E)$.

(ב) לפי הלמה של ארטין, $H = \mathrm{Gal}(L/E) = \mathrm{Aut}(L/E)$, עבור איזה $E \subseteq L$. לכן לפי (א), H סגורה.

(ג) תחילה נשים שאם $\alpha \in L$ אז $\{\sigma(\alpha) |\ \sigma \in H\}$ מוכלת בקבוצת השורשים של $\mathrm{irr}(\alpha, K)$, ולכן היא סופית. לפי הלמה של ארטין, L/E גלואה.

$\mathrm{Gal}(L/E) \subseteq \bar{H}$: לפי תרגיל 10.10.

$\bar{H} \subseteq \mathrm{Gal}(L/E)$: מתקיים $H \subseteq \mathrm{Gal}(L/E)$, לכן $\bar{H} \subseteq \overline{\mathrm{Gal}(L/E)}$; לפי (א), $\mathrm{Gal}(L/E) = \overline{\mathrm{Gal}(L/E)}$. ∎

משפט 10.13 (המשפט היסודי של תורת גלואה): *תהי L/K הרחבת גלואה. נסמן $G = \mathrm{Gal}(L/K)$. אז $E \mapsto \mathrm{Gal}(L/E)$ היא התאמה חד חד ערכית בין שתי הקבוצות הבאות*

$$\{E|\ E \text{ שדה}, \ K \subseteq E \subseteq L\} \longrightarrow \{H|\ H \text{ תת־חבורה סגורה של } G\}.$$

ההעתקה ההפוכה נתונה על ידי $H \mapsto L^H$.

במלים אחרות, $E = L^{\mathrm{Gal}(L/E)}$ לכל $K \subseteq E \subseteq L$, ו־ $\mathrm{Gal}(L/L^H) = H$ לכל $H \leq G$ (תת־חבורה סגורה).

הוכחה: שתי ההעתקות מוגדרות היטב: אם $K \subseteq E \subseteq L$, אז L/E גלואה, ו־$\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/K) = G$ סגורה. אם $H \leq G$, אז $K \subseteq L^H \subseteq L$. אם H סגורה, לפי הלמה 10.12(ג), $\mathrm{Gal}(L/L^H) = H$. נותר להוכיח:

טענה: *תהי L/E גלואה. אז $E = L^{\mathrm{Gal}(L/E)}$.*

אכן, $E \subseteq \{\alpha \in L|\ \sigma(\alpha) = \alpha$ לכל $\sigma \in \mathrm{Gal}(L/E)\} = L^{\mathrm{Gal}(L/E)}$. להיפך, יהי $\alpha \in L^{\mathrm{Gal}(L/E)}$. יהי $\tilde{E}$ סגור אלגברי של E כך ש־$E \subseteq L \subseteq \tilde{E}$. כל הומומורפיזם־$E$ $\sigma_0 \in \mathrm{Ism}_E(E(\alpha), \tilde{E})$ ניתן להרחבה ל־$\sigma \in \mathrm{Ism}_E(L, \tilde{E}) = \mathrm{Gal}(L/E)$. לפי ההנחה, $\sigma(\alpha) = \alpha$, לכן $\sigma_0(\alpha) = \alpha$, לכן σ_0 הזהות. לכן $[E(\alpha) : E]_s = 1$. אבל $E(\alpha)/E$ פרידה, לכן $[E(\alpha) : E] = 1$, כלומר, $\alpha \in E$. ∎

מסקנה 10.14: *להרחבה פרידה סופית L/K יש רק מספר סופי של שדות ביניים (כלומר, שדות E כך ש־ $K \subseteq E \subseteq L$).*

הוכחה: יהי M הסגור הנורמלי של L/K. אז M/K גלואה סופית. לכן $\mathrm{Gal}(M/K)$ סופית ולכן יש לה מספר סופי של תת־חבורות. לפי המשפט, הן עומדות בהתאמה חח"ע עם קבוצת שדות הביניים של M/K. לכן יש מספר סופי של שדות ביניים של M/K, ובפרט מספר סופי של שדות ביניים של L/K. ∎

משפט 10.15: *תהי L/K הרחבת גלואה ויהיו $K \subseteq E_1, E_2 \subseteq L$. אז*

(א) $\mathrm{Gal}(L/E_1) \leq \mathrm{Gal}(L/E_2) \ \Leftrightarrow\ E_2 \subseteq E_1$.

(ב) $\mathrm{Gal}(L/E_1 \cap E_2) = \overline{\langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle}$.

(ב') $\mathrm{Gal}(L/E_1 \cap E_2) = \langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle$, *אם* L/K *סופית.*

(ג) $\mathrm{Gal}(L/E_1E_2) = \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$.

הוכחה: נסמן $G = \mathrm{Gal}(L/K)$, $G_i = \mathrm{Gal}(L/E_i)$ עבור $i = 1, 2$. לפי משפט 10.13, $E_i = L^{G_i}$ עבור $i = 1, 2$.

(א) $\Rightarrow$: לפי ההגדרות.

$\Leftarrow$: צריך להוכיח: $G_1 \le G_2 \Leftarrow L^{G_2} \subseteq L^{G_1}$. זה נובע מההגדרות.

(ב) "$\supseteq$": לפי (א) $\mathrm{Gal}(L/E_1 \cap E_2) \supseteq \mathrm{Gal}(L/E_i)$, עבור $i = 1, 2$, לכן $\mathrm{Gal}(L/E_1 \cap E_2) \supseteq \langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle$. אבל $\mathrm{Gal}(L/E_1 \cap E_2)$ סגורה, לכן היא מכילה את הסגור של $\langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle$.

"$\subseteq$": נסמן $H = \overline{\langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle}$. אז $G_1, G_2 \le H$, לכן $L^H \subseteq E_1, E_2$, כלומר, $L^H \subseteq E_1 \cap E_2$, ומכאן $\mathrm{Gal}(L/E_1 \cap E_2) \le \mathrm{Gal}(L/L^H) = H$.

(ב') אם L/K סופית, אז $\overline{\langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle} = \langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle$.

(ג) "$\subseteq$": $E_1E_2 \supseteq E_1, E_2$, לכן לפי (א), $\mathrm{Gal}(L/E_1E_2) \subseteq \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2)$. לכן $\mathrm{Gal}(L/E_1E_2) \subseteq \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$.

להיפך, יהי $\sigma \in \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$. אז $\sigma(\alpha) = \alpha$ לכל $\alpha \in E_1 \cup E_2$. כיוון ש־$E_1E_2 = K(\alpha |\ \alpha \in E_1 \cup E_2)$, ברור ש־$\sigma$ משבית כל אברי E_1E_2. לכן $\sigma \in \mathrm{Gal}(L/E_1E_2)$. ∎

למה 10.16: *תהי* L/K *הרחבת גלואה,* $K \subseteq E \subseteq L$ *שדה, ו־*$\sigma \in \mathrm{Gal}(L/K)$. *אז* $K \subseteq \sigma(E) \subseteq L$ *ו־*$\mathrm{Gal}(L/\sigma(E)) = \sigma \mathrm{Gal}(L/E) \sigma^{-1}$.

הוכחה: $K = \sigma(K) \subseteq \sigma(E) \subseteq \sigma(L) = L$. כמו כן

$$\begin{aligned}\mathrm{Gal}(L/\sigma(E)) =&\{\tau \in \mathrm{Aut}(L) |\ \tau\big(\sigma(\alpha)\big) = \sigma(\alpha) \text{ לכל } \alpha \in E\} = \\ &\{\tau \in \mathrm{Aut}(L) |\ \sigma^{-1}\tau\sigma(\alpha) = \alpha \text{ לכל } \alpha \in E\} = \\ &\{\sigma\tau'\sigma^{-1} \in \mathrm{Aut}(L) |\ \tau'(\alpha) = \alpha \text{ לכל } \alpha \in E\} = \sigma \mathrm{Gal}(L/E) \sigma^{-1}\end{aligned}$$

(בחישוב לעיל עשינו שינוי משתנה: $\tau' = \sigma^{-1}\tau\sigma$). ∎

משפט 10.17: *תהי* L/K *הרחבת גלואה,* $K \subseteq E \subseteq L$ *שדה. אז*

(א) E/K *נורמלית (כלומר, גלואה) אם ורק אם* $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$.

(ב) *אם* E/K *גלואה, אז הצמצום* $\sigma \mapsto \sigma|_E$ *הוא אפימורפיזם* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ *וגרעינו* $\mathrm{Gal}(L/E)$. *לכן* $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$.

הוכחה: בלי הגבלת הכלליות $K \subseteq E \subseteq L \subseteq \tilde{K}$.

(א) E/K נורמלית $\Leftrightarrow$

$\Leftrightarrow$ $\sigma_0(E) = E$ לכל $\sigma_0 \in \mathrm{Ism}_K(E, \tilde{K})$ (הגדרת הנורמליות)

$\Leftrightarrow$ $\sigma(E) = E$ לכל $\sigma \in \mathrm{Gal}(L/K)$ (σ_0 ניתן להרחבה ל־$\sigma \in \mathrm{Ism}_K(L, \tilde{K}) = \mathrm{Gal}(L/K)$)

$\Leftrightarrow$ $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/\sigma(E))$ לכל $\sigma \in \mathrm{Gal}(L/K)$ (המשפט היסודי או משפט 10.15)

$\Leftrightarrow$ $\mathrm{Gal}(L/E) = \sigma\mathrm{Gal}(L/E)\sigma^{-1}$ לכל $\sigma \in \mathrm{Gal}(L/K)$ (המשפט הקודם)

$\Leftrightarrow$ $\mathrm{Gal}(L/E) \triangleleft \mathrm{Gal}(L/K)$.

(ב) לפי מסקנה 5.7, כל $\sigma_0 \in \mathrm{Gal}(E/K) = \mathrm{Ism}_K(E, \tilde{K})$ ניתן להרחבה לאוטומורפיזם של $\tilde{K}$; צמצומו ל־L הוא איבר $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Ism}_K(L, \tilde{K})$ כך ש־$\sigma|_E = \sigma_0$. לכן הצמצום על. ברור שהוא הומומורפיזם של חבורות. לבסוף $\mathrm{Gal}(L/E) = \{\sigma \in \mathrm{Gal}(L/K) |\ \sigma|_E = 1_E\} = \mathrm{Ker}(\sigma \mapsto \sigma|_E)$.

∎

דוגמה 10.18: יהי L שדה הפיצול של $f = X^3 - 2$ (אי פריק לפי קריטריון איזנשטיין) מעל $\mathbb{Q}$. אז $L/\mathbb{Q}$ הרחבת גלואה. מתקיים $f = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\omega)(X - \sqrt[3]{2}\omega^2)$, באשר $\omega = e^{\frac{2\pi i}{3}}$ שורש יחידה שלישי של 1, כלומר, ω שורש של $X^3 - 1 = (X-1)(X^2 + X + 1)$, ולכן $\mathrm{irr}(\omega, \mathbb{Q}) = X^2 + X + 1$. לכן

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

כעת, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, לכן $[L : \mathbb{Q}] = 6$. לכן $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ או $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

אבל $L \supseteq \mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$, ו־$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ אינה נורמלית (אחרת $\mathbb{Q}(\sqrt[3]{2})$ היה שדה הפיצול של f מעל $\mathbb{Q}$), לכן $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) \not\triangleleft \mathrm{Gal}(L/\mathbb{Q})$, בפרט $\mathrm{Gal}(L/\mathbb{Q})$ אינה חילופית, ולכן $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

בנוסף לכך, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, לכן $\mathbb{Q}(\omega)/\mathbb{Q}$ נורמלית, ולכן $\mathrm{Gal}(L/\mathbb{Q}(\omega)) \triangleleft \mathrm{Gal}(L/\mathbb{Q})$ תת־חבורה מסדר 3. לכן $\mathrm{Gal}(L/\mathbb{Q}(\omega))$ מתאימה ל־A_3 תחת האיזומורפיזם $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. ∎

משפט 10.19: *תהי L/K הרחבת גלואה, ותהי F/K הרחבה כלשהי, כך ש־L, F מוכלים בשדה משותף. אז*

(א) *LF/F הרחבת גלואה;*

(ב) *$\sigma \mapsto \sigma|_L$ הוא איזומורפיזם $\mathrm{Gal}(LF/F) \to \mathrm{Gal}(L/F \cap L)$.*

הוכחה: (א) משפט 8.6(ב) ומשפט 7.13(ב).

(ב) יהי C סגור אלגברי של LF; אז $F, L \subseteq C$. בלי הגבלת הכלליות $\tilde{K} = \{\alpha \in C |\ K \text{ אלגברי מעל } \alpha\}$ הסגור האלגברי של K בתוך C. אז $L \subseteq \tilde{K}$.

יהי $\sigma \in \mathrm{Gal}(LF/F)$. אז $\sigma|_F = 1$, לכן $\sigma|_{L\cap F} = 1$. כמו כן $\sigma(L) \subseteq \sigma(LF) = LF \subseteq C$ ו־$\sigma(L)$ אלגברי מעל K, לכן $\sigma(L) \subseteq \tilde{K}$. כיוון ש־$L/K$ נורמלית, $\sigma(L) = L$. לכן $\sigma|_L \in \mathrm{Gal}(L/L \cap F)$.

בלי הגבלת הכלליות $L \cap F = K$ (אחרת נחליף K ב־$F \cap L$).

קל לראות שהצמצום $\mathrm{Gal}(LF/F) \to \mathrm{Gal}(L/K)$ הוא הומומורפיזם. הוא חד חד ערכי, כי אם $\sigma \in \mathrm{Gal}(LF/F)$ מקיים $\sigma|_L = 1$ אז $\sigma|_{LF} = 1$, כלומר, $\sigma = 1$. תהי H תמונתו. נראה ש־$H = \mathrm{Gal}(L/K)$.

נניח קודם ש־L/K סופית. יהי $\alpha \in L^H$. אז $\sigma(\alpha) = \alpha$ לכל $\sigma \in H$, ולכן לכל $\sigma \in \mathrm{Gal}(LF/F)$. לכן $\alpha \in L \cap F = K$. מכאן $L^H = K$. לכן לפי הלמה של ארטין או לפי המשפט היסודי של תורת גלואה $H = \mathrm{Gal}(L/K)$. לכן, במקרה זה, העתקת הצמצום הינה על ובפרט איזומורפיזם.

במקרה הכללי יהי $\tau \in \mathrm{Gal}(L/K)$. לכל שדה ביניים $K \subseteq E \subseteq L$ כך ש־E/K הרחבת גלואה סופית מתקיים $F \subseteq EF \subseteq LF$ ו־$\tau|_E \in \mathrm{Gal}(E/K)$. לפי הפסקה הקודמת קיים יחיד $\sigma_{EF} \in \mathrm{Gal}(EF/F)$ כך ש־$(\sigma_{EF})|_E = \tau|_E$. לכל $\alpha \in L$ יש E/K הרחבת גלואה סופית (למשל, סגור גלואה של $K(\alpha)/K$) כך ש־$K(\alpha) \subseteq E \subseteq L$. לכן $L = \bigcup_E E$, ומכאן $LF = \bigcup_E EF$. נשים לב שאם E_1, E_2 שתי הרחבות גלואה סופיות של K מוכלות ב־L, אז יש הרחבת גלואה סופית E של K מוכלת ב־L כך ש־$E_1, E_2 \subseteq E$.

נגדיר $\sigma\colon LF \to LF$ על ידי $\sigma|_{EF} = \sigma_{EF}$, לכל E. ההגדרה טובה:

אם $E' \subseteq E$ שתי הרחבות גלואה סופיות של K מוכלות ב־L, אז מתוך $(\sigma_{EF})|_E = \tau|_E$ נסיק על ידי צמצום כי $((\sigma_{EF})|_{E'F})|_{E'} = \tau|_{E'}$, ולפי היחידות $(\sigma_{EF})|_{E'F} = \sigma_{E'F}$.

ברור ש־σ הוא אוטומורפיזם של LF ששומר על F וצמצומו ל־L הוא τ. ∎

תרגיל 10.20: *יהיו $\pi_1\colon G_1 \to G_0,\ \pi_2\colon G_2 \to G_0$ הומומורפיזמים של חבורות. אז*

$$G_1 \times_{G_0} G_2 := \{(\sigma_1, \sigma_2) \in G_1 \times G_2 |\ \pi_1(\sigma_1) = \pi_2(\sigma_2)\}$$

תת־חבורה של $G_1 \times G_2$. אם $G_0 = 1$ אז $G_1 \times_{G_0} G_2 = G_1 \times G_2$.

משפט 10.21: *תהיינה $L_1, L_2 \subseteq \tilde{K}$ הרחבות גלואה של K. אז*

(א) *L_1L_2/K הרחבת גלואה.*

(ב) *$L_1 \cap L_2/K$ הרחבת גלואה.*

(ג) *$\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times_{\mathrm{Gal}(L_1\cap L_2/K)} \mathrm{Gal}(L_2/K)$ על ידי $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$.*

(ד) *בפרט, אם $L_1 \cap L_2 = K$ אז $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.*

הוכחה: (א) L_1L_2/K פרידה לפי משפט 7.13(ג) ונורמלית לפי משפט 8.6(ג).

(ב) $L_1 \cap L_2/K$ פרידה לפי משפט 7.13(א) ונורמלית לפי משפט 8.6(ג).

(ג) נסמן $L = L_1L_2$. ברור ש־$\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ הוא הומומורפיזם מ־$\mathrm{Gal}(L/K)$ לתוך $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$. גרעינו

$$\mathrm{Gal}(L/L_1) \cap \mathrm{Gal}(L/L_2) = \mathrm{Gal}(L/L_1L_2) = \mathrm{Gal}(L/L) = 1.$$

ותמונתו בתוך $\mathrm{Gal}(L_1/K) \times_{\mathrm{Gal}(L_1\cap L_2/K)} \mathrm{Gal}(L_2/K)$. נראה שהוא על חבורה זו.

יהיו $\sigma_1 \in \mathrm{Gal}(L_1/K), \sigma_2 \in \mathrm{Gal}(L_2/K)$ כך ש־$\sigma_1|_{L_1 \cap L_2} = \sigma_2|_{L_1 \cap L_2}$. נרחיב את σ_1 ל־$\tilde{\sigma} \in \mathrm{Gal}(L/K)$. לפי משפט 10.19(ב) אפשר להרחיב את $(\tilde{\sigma}|_{L_2})^{-1}\sigma_2 \in \mathrm{Gal}(L_2/L_1 \cap L_2)$ לאיבר $\tau \in \mathrm{Gal}(L/L_1) \leq \mathrm{Gal}(L/K)$. יהי $\sigma = \tilde{\sigma}\tau \in \mathrm{Gal}(L/K)$. אז

$$\sigma|_{L_2} = \tilde{\sigma}|_{L_2}\tau|_{L_2} = \tilde{\sigma}|_{L_2}(\tilde{\sigma}|_{L_2})^{-1}\sigma_2 = \sigma_2 \qquad \text{וגם} \qquad \sigma|_{L_1} = \tilde{\sigma}|_{L_1}\tau|_{L_1} = \sigma_1 1 = \sigma_1 \quad \blacksquare$$

11. דוגמאות

משפט 11.1: *השדה $\mathbb{C}$ סגור אלגברית.*

כדי להוכיח משפט זה, צריך קודם להגדיר $\mathbb{C}$. עבורנו, $\mathbb{C} = \mathbb{R}(i)$, באשר $i^2 = -1$ שורש של $X^2+1 \in \mathbb{R}[X]$, ונשתמש בתכונות הבאות של $\mathbb{R}$:

(א) $\mathbb{R}$ שדה סדור: יש בו קבוצה חלקית P (איברים חיוביים), סגורה תחת חיבור וכפל ב־$\mathbb{R}$, ו־$\mathbb{R}$ הוא איחוד זר של $P, -P, \{0\}$. (בפרט סכום של ריבועים שונים מ־0 הוא איבר חיובי. מכאן: $i \notin \mathbb{R}$ ו־$\mathrm{char}(\mathbb{R}) = 0$.)

(ב) כל איבר חיובי הוא ריבוע ב־$\mathbb{R}$.

(ג) לכל $f \in \mathbb{R}[X]$ ממעלה אי זוגית יש שורש ב־$\mathbb{R}$.

טענה 1: *כל $z \in \mathbb{C}$ הוא ריבוע ב־$\mathbb{C}$.* אכן, יהי $z = a + bi$, באשר $a, b \in \mathbb{R}$. צריך למצוא $c, d \in \mathbb{R}$ כך ש־$(c+di)^2 = a + bi$, כלומר, $c^2 - d^2 = a, 2cd = b$. נגדיר $C = \frac{a+\sqrt{a^2+b^2}}{2}, D = \frac{-a+\sqrt{a^2+b^2}}{2}$. אז $C - D = a$ ו־$4CD = b^2 \in P \cup \{0\}$, לכן $C, D \in P \cup \{0\}$ או $-C, -D \in P \cup \{0\}$. במקרה הראשון נגדיר $d = \pm\sqrt{D}$, $c = \sqrt{C}$, כאשר הסימן של d ייבחר כך ש־$2cd = b$. במקרה השני נחליף את $\sqrt{a^2+b^2}$ בנגדי שלו; אז C, D "החדשים" הם $-D, -C$ "הישנים", ולכן הם ב־$P \cup \{0\}$.

טענה 2: *ל־$\mathbb{C}$ אין הרחבה ריבועית.* אכן, אם $[F : \mathbb{C}] = 2$, אז $F = \mathbb{C}(\alpha)$, באשר α שורש של $f = X^2 + bX + c \in \mathbb{C}[X]$. אבל אז $0 = \alpha^2 + b\alpha + c = (\alpha + \frac{b}{2})^2 - (\frac{b}{2})^2 + c$, לכן

$$\Big(\alpha + \frac{b}{2}\Big)^2 = \Big(\frac{b}{2}\Big)^2 - c.$$

לפי טענה 1, $(\frac{b}{2})^2 - c$ ריבוע ב־$\mathbb{C}$, לכן $\alpha + \frac{b}{2} \in \mathbb{C}$. מכאן $\alpha \in \mathbb{C}$, סתירה.

הוכחת המשפט: צריך להראות שאם $L/\mathbb{C}$ סופית, אז $L = \mathbb{C}$. בלי הגבלת הכלליות, $L/\mathbb{R}$ גלואה. אכן, $L/\mathbb{R}$ סופית, פרידה (כי $\mathrm{char}(\mathbb{R}) = 0$), לכן סגור גלואה שלה M הוא הרחבה סופית של $\mathbb{R}$. נחליף L ב־M כדי להניח ש־$L/\mathbb{R}$ גלואה.

תהי $G = \mathrm{Gal}(L/\mathbb{R})$ ותהי $H \leq G$ חבורת סילוב־2 שלה. אז $[L : \mathbb{R}] = |G|$ ו־$[L : L^H] = |H|$, לכן $[L^H : \mathbb{R}] = [G : H]$ מספר אי זוגי. לפי משפט האיבר הפרימיטיבי יש $\alpha \in L^H$ כך ש־$L^H = \mathbb{R}(\alpha)$. יהי $f = \mathrm{irr}(\alpha, \mathbb{R})] \in \mathbb{R}[X]$. אז f ממעלה אי זוגית, לכן יש לו שורש ב־$\mathbb{R}$, אבל הוא אי פריק, לכן ממעלה 1. מכאן $\alpha \in \mathbb{R}$, ולכן $L^H = \mathbb{R}$. לכן G חבורת־2.

אז גם $G_1 = \mathrm{Gal}(L/\mathbb{C}) \leq G$ חבורת־2. אם היא אינה טריוויאלית, יש לה תת־חבורה G_2 בעלת אינדקס 2. שדה השבת של G_2 ב־L הוא הרחבה ריבועית של $\mathbb{C}$, בסתירה לטענה 2. ∎

דוגמה 11.2: יהי K שדה ויהיו $t_1, \ldots, t_n$ משתנים מעליו. אז החבורה הסימטרית S_n פועלת על חוג הפולינומים $K[t_1, \ldots, t_n]$ באופן הבא:

$$\sigma\Big(\sum_{m=(m_1,\ldots,m_n)} a_m t_1^{m_1} \cdots t_n^{m_n}\Big) = \sum_{m=(m_1,\ldots,m_n)} a_m\, t_{\sigma(1)}^{m_1} \cdots t_{\sigma(n)}^{m_n}.$$

פעולה זו ניתנת להרחבה לשדה המנות $L = K(t_1, \ldots, t_n)$. לכן $S_n \leq \mathrm{Aut}(L)$. יהי $E = L^{S_n}$. לפי הלמה של ארטין, L/E הרחבת גלואה ו־$\mathrm{Gal}(L/E) = S_n$. מהו E?

הפולינומים הסימטריים היסודיים $s_1, \ldots, s_n$ במשתנים $t_1, \ldots, t_n$ ודאי נמצאים בשדה השבת E. לכן $L \supseteq E \supseteq E_0 := K(s_1, \ldots, s_n)$. אבל $L = E_0(t_1, \ldots, t_n)$ הוא שדה הפיצול של

$$f(X) := (X + t_1) \cdots (X + t_n) = X^n + s_1 X^{n-1} + s_2 X^{n-2} + \ldots + s_n \in E_0[X]$$

מעל E_0, לכן לפי תרגיל 8.10, $[L : E_0] \leq n!$. מצד שני, $[L : E] = |S_n| = n!$. לכן $E = E_0$, כלומר, $L^{S_n} = K(s_1, \ldots, s_n)$.

יתר על כן, קיים הומומורפיזם של חוגים $K[s_1, \ldots, s_n] \to K[t_1, \ldots, t_n]$ על ידי $s_i \mapsto t_i$. הוא על, וגרעינו $\{g \in K[t_1, \ldots, t_n] \big| g(s_1, \ldots, s_n) = 0\} = \{0\}$, לפי משפט 3.9. לכן $K[t_1, \ldots, t_n] \cong_K K[s_1, \ldots, s_n]$. איזומורפיזם זה ניתן להרחבה לאיזומורפיזם שדות $K(t_1, \ldots, t_n) \cong_K K(s_1, \ldots, s_n)$. לכן

מסקנה 11.3: *יהי K שדה ויהיו $t_1, \ldots, t_n$ משתנים מעליו. יהי L שדה הפיצול של $f = X^n + t_1 X^{n-1} + \ldots + t_n$ מעל $E = K(t_1, \ldots, t_n)$. אז $\mathrm{Gal}(L/E) = S_n$.*

מסקנה 11.4: *כל חבורה סופית G איזומורפית לחבורת גלואה.*

הוכחה: יהי $n = |G|$. אז G איזומורפית לתת־חבורה של S_n. לפי המסקנה הקודמת G איזומורפית לתת־חבורה של $\mathrm{Gal}(L/E)$, נאמר, H. אז L/L^H גלואה ו־$\mathrm{Gal}(L/L^H) = H \cong G$. ∎

משפט 11.5: *יהי K שדה סופי, $|K| = q$, ויהי $\tilde{K}$ סגור אלגברי שלו.*

(א) *ההעתקה $\varphi_q \colon \tilde{K} \to \tilde{K}$ הנתונה על ידי $x \mapsto x^q$ היא אוטומורפיזם־K של $\tilde{K}$; נקרא האוטומורפיזם של* Frobenius.

(ב) *תהי K_n ההרחבה היחידה של K ממעלה n בתוך $\tilde{K}$. אז K_n/K גלואה ו־$\mathrm{Gal}(K_n/K) = \langle \varphi_q|_{K_n} \rangle$ מעגלית.*

הוכחה: (א) כיוון ש־q הוא חזקה של $p = \mathrm{char}(K)$ (משפט 9.1(ה)), $(x + y)^q = x^q + y^q$; כמובן, $(xy)^q = x^q y^q$. לכן φ_q הומומורפיזם. כיוון שאברי K מקיימים $x^q = x$ (משפט 9.2), $\varphi_q|_K = 1$. לפי תרגיל 4.19, φ_q אוטומורפיזם.

(ב) לפי משפט 9.3, K_n/K גלואה. לכן $\varphi_q|_{K_n}$ אוטומורפיזם של K_n, כלומר $\varphi_q|_{K_n} \in \mathrm{Gal}(K_n/K)$.
כיוון ש־$n = [K_n : K] = |\mathrm{Gal}(K_n/K)|$, די להוכיח ש־$m := \mathrm{ord}\, \varphi_q|_{K_n} \geq n$. ואכן, $(\varphi_q|_{K_n})^m = 1$, לכן $\varphi_q^m(x) = x$, כלומר, לכן $x^{q^m} = x$, לכל $x \in K_n$. מכאן $K_n \subseteq K_m$ ולכן $m \geq n$. ∎

הערה 11.6: $\varphi_{p^n} = (\varphi_p)^n$. ∎

הערה 11.7: *מהי* $Gal(\tilde{K}/K)$, אם $K = K_q$. יהי $\varphi = \varphi_q \in \mathrm{Gal}(\tilde{K}/K)$ האוטומורפיזם של פרובניוס של K.

יהי $\sigma \in \mathrm{Gal}(\tilde{K}/K)$. אז לכל $n \in \mathbb{N}$ יש $a_n \in \mathbb{Z}/n\mathbb{Z}$ יחיד כך ש־$\sigma|_{K_n} = (\varphi|_{K_n})^{a_n} = (\varphi^{a_n})|_{K_n}$.
אם $m|n$, אז $K_m \subseteq K_n$ ו־$(\sigma_{K_n})|_{K_m} = \sigma|_{K_m}$, כלומר, $(\varphi|_{K_m})^{a_m} = (\varphi|_{K_m})^{a_n}$ ובגלל היחידות של a_m, מתקיים $a_m \equiv a_n \pmod m$. לכן $(a_k)_{k=1}^{\infty}$ בתוך הקבוצה

$$\left\{(a_k)_{k=1}^{\infty} \in \hat{\mathbb{Z}} = \{(a_k)_{k=1}^{\infty} \in \prod_{k=1}^{\infty} \mathbb{Z}/k\mathbb{Z} \middle| \, m|n \Rightarrow a_m \equiv a_n \pmod m\right\}$$

להיפך, לכל $(a_k)_{k=1}^{\infty} \in \hat{\mathbb{Z}}$ נגדיר העתקה $\sigma\colon \tilde{K} \to \tilde{K}$ על ידי $\sigma|_{K_n} = (\varphi|_{K_n})^{a_n} = (\varphi^{a_n})|_{K_n}$ לכל n.

טענה: *ההגדרה טובה.* אם $m|n$ אז $K_m \subseteq K_n$ ו־$(\sigma_{K_n})|_{K_m} = \sigma|_{K_m}$.
אם $m_1, m_2 \in \mathbb{N}$ ו־$\alpha \in K_{m_1} \cap K_{m_2}$,
$n = m_1 m_2$ מתחלק ב־m_1, m_2 ולפי הפסקה הקודמת $\sigma|_{K_{m_1}}(\alpha) = \sigma|_{K_n}(\alpha) = \sigma|_{K_{m_2}}(\alpha)$.

∎

ברור ששתי ההעתקות הפוכות זו לזו.

יתר על כן, $\hat{\mathbb{Z}}$ היא תת חבורה של $\prod_{k=1}^{\infty} \mathbb{Z}/k\mathbb{Z}$ וההתאמה $\mathrm{Gal}(\tilde{K}/K) \to \hat{\mathbb{Z}}$ היא איזומורפיזם חבורות.

∎

מכאן נובע, לפי הטענה הבאה, ש־$\mathrm{Gal}(\tilde{K}/K)$ איננה בת מניה.

טענה 11.8: $|\hat{\mathbb{Z}}| = \aleph$.

הוכחה: אכן, $\hat{\mathbb{Z}} \leq \prod_{k=1}^{\infty} \mathbb{Z}/k\mathbb{Z}$, לכן

$$|\hat{\mathbb{Z}}| \leq |\prod_{k=1}^{\infty} \mathbb{Z}/k\mathbb{Z}| \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \aleph$$

להיפך, אם $m|n$, אז ההומומורפיזם $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ על, לכן לכל $a_m \in \mathbb{Z}/m\mathbb{Z}$ יש $\frac{n}{m}$ איברים $a_n \in \mathbb{Z}/n\mathbb{Z}$ כך ש־$a_m \equiv a_n \pmod m$.

לכן לכל $a_{1!} \in \mathbb{Z}/1!\mathbb{Z}$ (יש רק אחד!) יש 2 איברים $a_{2!} \in \mathbb{Z}/2!\mathbb{Z}$ כך ש־$a_{1!} \equiv a_{2!} \pmod{1!}$;
לכל $a_{2!} \in \mathbb{Z}/2!\mathbb{Z}$ כזה יש 3 איברים $a_{3!} \in \mathbb{Z}/3!\mathbb{Z}$ כך ש־$a_{2!} \equiv a_{3!} \pmod{2!}$;
לכל $a_{3!} \in \mathbb{Z}/3!\mathbb{Z}$ כזה יש 4 איברים $a_{4!} \in \mathbb{Z}/4!\mathbb{Z}$ כך ש־$a_{3!} \equiv a_{4!} \pmod{3!}$; וכן הלאה.

לכן יש לפחות $\aleph = 2^{\aleph_0}$ סדרות שונות $(a_{n!})_{n=1}^{\infty}$ כאלה.

כל סדרה כזאת נשלים לסדרה $(a_k)_{k=1}^{\infty} \in \hat{\mathbb{Z}}$ כך: אם $k|n!$, נגדיר $a_k \equiv a_{n!} \pmod k$. ההגדרה טובה, כי אם $k|n!$ וגם $k|m!$, ולמשל $m \leq n$, אז $a_{m!} \equiv a_{n!} \pmod{m!}$ ולכן $a_{m!} \pmod k \equiv a_{n!} \pmod k$.

לכן $\aleph \geq |\hat{\mathbb{Z}}|$. ∎

12. חבורת גלואה של פולינום

יהי K שדה ויהי $f \in K[X]$ פולינום מתוקן בעל שורשים פשוטים בסגור אלגברי של K. יהי L שדה פיצול של f. אז $f = (X-\alpha_1)\cdots(X-\alpha_n)$, באשר $\alpha_1,\dots,\alpha_n \in L$ שונים זה מזה, ו־$L = K(\alpha_1,\dots,\alpha_n)$. נסמן $A = \{\alpha_1,\dots,\alpha_n\}$.

כפי שכבר אמרנו, L/K הרחבת גלואה סופית. אם α שורש של f ו־$\sigma \in \mathrm{Gal}(L/K)$, אז גם $\sigma(\alpha)$ שורש של f. לכן $\sigma|_A$ היא תמורה של A. ההעתקה $\sigma \mapsto \sigma|_A$ הוא הומומורפיזם $\mathrm{Gal}(L/K) \to S(A)$. הוא חד חד ערכי: אם $\sigma|_A = 1$ אז $\sigma(\alpha_i) = \alpha_i$ לכל $1 \le i \le n$, ולכן $\sigma = 1$. תמונתו של הומומורפיזם זה ב־$S(A)$ נקראת **חבורת גלואה של** f ותסומן $\mathrm{Gal}(f,K)$. אז $\mathrm{Gal}(L/K) \to \mathrm{Gal}(f,K)$ איזומורפיזם.

החבורה $\mathrm{Gal}(f,K)$ היא חבורת תמורות על A. בדרך כלל נזהה את $S(A)$ עם S_n, אך זיהוי זה תלוי בזיהוי של A עם $\{1,\dots,n\}$. זיהוי זה קובע את $\mathrm{Gal}(f,K)$ עד כדי ההצמדה ב־S_n:

תרגיל 12.1: *תהיינה A, B שתי קבוצות ותהי $\lambda\colon A \to B$ חח"ע ועל.*

(א) *יש איזומורפיזם $\lambda^*\colon S(B) \to S(A)$ הנתון על ידי $\lambda^*(\sigma) = \lambda^{-1} \circ \sigma \circ \lambda$.*

(ב) *אם $\rho \in S(A)$ אז $\mu := \lambda \circ \rho\colon A \to B$ חח"ע ועל ו־$\mu^* = [\rho] \circ \lambda^*$ (כאן $[\rho]$ היא העתקת ההצמדה על $S(A)$ הנתונה על ידי $[\rho](\sigma) = \rho^{-1}\sigma\rho$).*

(ג) *אם גם $\mu\colon A \to B$ חח"ע ועל, אז $\rho := \lambda^{-1} \circ \mu \in S(A)$ ומתקיים $\mu^* = [\rho] \circ \lambda^*$.*

מסקנה 12.2: *$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(f,K) \le S(A) \cong S_n$, לכן $|\mathrm{Gal}(f,K)|$ מחלק את $n!$.*

הערה 12.3: חבורת תמורות G של קבוצה A (כלומר, $G \le S(A)$) מגדירה יחס שקילות על A: $\alpha \sim_G \alpha'$ אם יש $\tau \in G$ כך ש־$\alpha' = \tau(\alpha)$. מחלקת שקילות נקראת **מסלול־**G. לכן $A = \bigcup_k A_k$, באשר A_k היא מסלול־G לכל k. G נקראת **טרנזיטיבית** אם A היא מסלול־G יחיד, כלומר, לכל $\alpha, \alpha' \in A$ יש $\tau \in G$ כך ש־$\alpha' = \tau(\alpha)$.

תהי $G = \mathrm{Gal}(f,K)$ ותהי A קבוצת השורשים שלה. לכל A_k נתאים פולינום $f_k = \prod_{\alpha \in A_k}(X-\alpha)$. אז $f = \prod_k f_k$. ∎

למה 12.4: *$f_k \in K[X]$ והוא אי פריק, לכל k. בפרט, f אי פריק אם ורק אם $\mathrm{Gal}(f,K)$ טרנזיטיבית.*

הוכחה: החבורה $G = \mathrm{Gal}(L/K)$ פועלת על $L[X]$ על ידי פעולה על מקדמי הפולינומים. לכל $\sigma \in G$ מתקיים $\sigma(A_k) = A_k$, לכן $\sigma(f_k) = f_k$ ומכאן $f_k \in L^G[X] = K[X]$.

יהי $g \in K[X]$ גורם אי פריק מתוקן של f_k. יהי α שורש של g. אז $\alpha \in A_k$. לכל $\alpha' \in A_k$ יש $\sigma \in G$ כך ש־$\alpha' = \sigma(\alpha)$, לכן α' גם שורש של g. מכאן $f_k = g$ ובפרט f_k אי פריק. ∎

דוגמה 12.5: הפולינום הכללי ממעלה n. יהי K_0 שדה ויהיו $t_1,\dots,t_n$ משתנים מעליו. יהי $K = K_0(t_1,\dots,t_n)$. אז $f(X) = X^n + t_1X^{n-1} + t_2X^{n-2} + \cdots + t_n \in K[X]$ נקרא **הפולינום הכללי ממעלה** n. ראינו בדוגמה 11.2 כי $\mathrm{Gal}(f,K) = S_n$. ∎

נציין ללא הוכחה:

משפט 12.6 (משפט האי פריקות של הילברט): *יהי* $g(t_1,\dots,t_n,X)\in\mathbb{Q}[t_1,\dots,t_n][X]$ *מתוקן. אז יש* $a_1,\dots,a_n\in\mathbb{Q}$ *כך ש־* $\mathrm{Gal}\big(g(a_1,\dots,a_n,X),\mathbb{Q}\big)\cong\mathrm{Gal}\big(g,\mathbb{Q}(t_1,\dots,t_n)\big)$.

מסקנה 12.7: *לכל* n *יש* $L/\mathbb{Q}$ *גלואה כך ש־* $S_n\cong\mathrm{Gal}(L/\mathbb{Q})$.

הילברט גם הוכיח מסקנה דומה עבור A_n במקום S_n.

אך באופן כללי הבעיה הבאה פתוחה:

בעיה 12.8 (בעית גלואה ההפוכה): *תהי* G *חבורה סופית. האם יש* $L/\mathbb{Q}$ *גלואה כך ש־*$G\cong\mathrm{Gal}(L/\mathbb{Q})$*?*

תוצאה חשובה בכיוון זה היא:

משפט 12.9 (שפרביץ', 1954): *כן, אם* G *חבורה פתירה.*

חבורת גלואה של פולינום ממעלה 3.

יהי $f=X^3+aX^2+bX+c\in K[X]$ פריד. יהי $f=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ הפירוק מעל סגור אלגברי; $\alpha_1,\alpha_2,\alpha_3$ שונים זה מזה. אז $\mathrm{Gal}(f,K)\le S_3$. אם L שדה פיצול שלו, אז $K\subseteq K(\alpha_1)\subseteq L$, לכן, אם f אי פריק, אז

$$3=[K(\alpha_1):K]\,\big|\,[L:K]=|\mathrm{Gal}(f,K)|\,\big|\,|S_3|=6.$$

מכאן שיש שתי אפשרויות:

(א) $K(\alpha_1)=L$ ואז $\mathrm{Gal}(f,K)=A_3$; או

(ב) $K(\alpha_1)\subsetneqq L$ ואז $\mathrm{Gal}(f,K)=S_3$.

כיצד ניתן להבחין בין שני המקרים? או, אם לא נניח ש־f אי פריק, מתי $\mathrm{Gal}(f,K)\le A_3$?

תרגיל 12.10: *יהי* $D=(X_1-X_2)^2(X_2-X_3)^2(X_3-X_1)^2$. *יהיו* s_1,s_2,s_3 *הפולינומים הסימטריים היסודיים ב־* X_1,X_2,X_3. *מצא* $g\in\mathbb{Z}[S_1,S_2,S_3]$ *ממשקל* ≤ 6 *כך ש־* $D=g(s_1,s_2,s_3)$.

פתרון: נשים לב ש־D הוא פולינום סימטרי ב־X_1,X_2,X_3 ממעלה 6. יתר על כן, הוא הומוגני, כלומר, כל המונומים שלו ממעלה 6. לפי משפט 3.10, יש $g\in\mathbb{Z}[S_1,S_2,S_3]$ יחיד כך ש־$D=g(s_1,s_2,s_3)$ והוא ממשקל ≤ 6. נשים לב שכל מונום ממשקל d ב־s_1,s_2,s_3 הוא פולינום הומוגני ממעלה d ב־X_1,X_2,X_3. לכן מונומים ממשקל 6 ב־g נותנים (אחרי ההצבה של s_1,s_2,s_3) את כל המונומים של D אילו מונומים ממשקל <6 ב־g נותנים 0. מהיחידות של g נובע שיש לו רק מונומים ממשקל 6. לכן

$$(X_1-X_2)^2(X_2-X_3)^2(X_3-X_1)^2=ks_1^6+\ell s_1^4s_2+ms_1^3s_3+ns_1^2s_2^2+ps_1s_2s_3+qs_2^3+rs_3^2 \quad (1)$$

באשר $k,\ell,m,n,p,q,r\in\mathbb{Z}$. עלינו למצוא אותם. השיטה היא להציב ב־(1) במקום X_1,X_2,X_3 איברי $\mathbb{C}$ שונים במשוואה לעיל ובכך לקבל מערכת של משוואות לינאריות ב־7 נעלמים ואז לפתור אותה.

(א) נקח $s_1=0,s_2=0,s_3=1$, כלומר, נציב במקום X_1,X_2,X_3 את השורשים של X^3-1, דהיינו, $1,\omega,\omega^2$, באשר $\omega=e^{\frac{2\pi i}{3}}$. נזכור ש־$\omega^2+\omega+1=0$. אז אגף שמאל של (1) הוא

$$(1-\omega)^2(\omega-\omega^2)^2(\omega^2-1)^2=\big((1-\omega)(1-\omega)(1-\omega)\big)^2=\big((1-\omega)^2\big)^3=$$
$$(1-2\omega+\omega^2)^3=(-3\omega)^3=-27$$

ואילו אגף ימין הוא r, לכן $r=-27$.

(ב) נקח $s_1=0,s_2=1,s_3=0$, כלומר, נציב במקום X_1,X_2,X_3 את השורשים של X^3+X, דהיינו, $0,i,-i$. אז אגף שמאל של (1) הוא $(0-i)^2(i+i)^2(-i-0)^2=i^2(2i)^2i^2=4i^6=-4$, לכן $q=-4$.

(ג) נקח $s_1=1,s_2=0,s_3=0$, כלומר, נציב במקום X_1,X_2,X_3 את השורשים של X^3-X^2, דהיינו, $0,0,1$. אז אגף שמאל של (1) הוא 0, כי שני שורשים שווים, לכן $k=0$.

(ד) נציב במקום X_1,X_2,X_3 את $0,1,1$. אז $s_1=2,s_2=1,s_3=0$. שוב אגף שמאל של (1) הוא 0, ואילו אגף ימין הוא $k2^6+\ell 2^4+n2^2+q$, כלומר (אחרי ההצבה של k,q) $16\ell+4n-4=0$. לכן $4\ell+n=1$.

(ה) נציב במקום X_1,X_2,X_3 את $0,1,-2$. אז $s_1=-1,s_2=-2,s_3=0$. אז אגף שמאל של (1) הוא $(1\cdot 3\cdot 2)^2=36$, ואילו אגף ימין הוא $k+\ell(-2)+n4+q(-8)$, לכן $36=-2\ell+4n+32$ ומכאן $-\ell+2n=2$.

(ו) לפי (ד), (ה), $\ell=0,n=1$.

(ז) נציב במקום X_1,X_2,X_3 את $2,2,-1$. אז $s_1=3,s_2=0,s_3=-4$. אז אגף שמאל של (1) הוא שוב 0 ואילו אגף ימין הוא $m\cdot 3^3(-4)-27(-4)^2$. לכן $m=-4$.

(ח) לבסוף נקח $s_1=-1,s_2=1,s_3=-1$, כלומר, נציב במקום X_1,X_2,X_3 את השורשים של $X^3+X^2+X+1=(X+1)(X^2+1)$, דהיינו, $-1,i,-i$. אז אגף שמאל של (1) הוא $(-1-i)^2(-1+i)^2(2i)^2=\big((-1)^2-i^2\big)^2(2i)^2=2^2(-4)=-16$ ואילו אגף ימין הוא $(-4)(-1)^3(-1)+n\cdot 1\cdot 1+p\cdot 1+q+r(-1)^2$ לכן $-16=-34+p$ ומכאן $p=18$.

אם כך, הפתרון הוא $D=-4s_1^3s_3+s_1^2s_2^2+18s_1s_2s_3-4s_2^3-27s_3^2$, ולכן

$$g(S_1,S_2,S_3)=-4S_1^3S_3+S_1^2S_2^2+18S_1S_2S_3-4S_2^3-27S_3^2. \quad \blacksquare$$

נחזור לדיוננו. (איננו מניחים ש־f אי פריק.) נסמן

$$\delta=(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)=\prod_{i<j}(\alpha_i-\alpha_j).$$

אז $\Delta = \delta^2$ נקרא **הדיסקרימיננטה של** f. לפי התרגיל

$$\Delta = g(-a,b,-c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

זהו פולינום במקדמים a,b,c של f מעל השדה הראשוני של K. לכל $\sigma \in \mathrm{Gal}(L/K)$:

(1) $\sigma(\delta) = \pm\delta$; לכן $\sigma(\Delta) = \Delta$. מכאן $\Delta \in K$ (כמובן, זה גם נובע מתרגיל 12.10).

(2) אם $\sigma|_A \in A_3$ אז $\sigma(\delta) = \delta$; אם $\sigma|_A \notin A_3$ אז $\sigma(\delta) = -\delta$. לכן

(3) אם $\mathrm{char}(K) \neq 2$, אז $\sigma(\delta) = \delta \Leftrightarrow \sigma|_A \in A_3$.

לכן אם $\mathrm{char}(K) \neq 2$,

$$\mathrm{Gal}(f,K) \le A_3 \Leftrightarrow \sigma(\delta) = \delta \text{ לכל } \sigma \in \mathrm{Gal}(L,K) \Leftrightarrow \delta \in K \Leftrightarrow \Delta \text{ ריבוע ב־} K.$$

דוגמה 12.11: יהי $f(X) = X^3 - 3X + 1 \in K[X]$. אז $f' = 3X^2 - 3 = 3(X-1)(X+1)$. יהי L שדה פיצול של f מעל K.

(א) אם $\mathrm{char}(K) = 3$, אז $f = X^3 + 1 = (X+1)^3$ בעל שורש משולש. אז $L = K$.

אם $\mathrm{char}(K) \neq 3$, אז ל־f אין שורשים מרובים (כי ± 1 אינו שורש של f, ולכן f, f' זרים). במקרה זה $\Delta = -4(-3)^3 - 27 = 3^3(4-1) = 3^4 \in K^2$. לכן:

(ב) אם $\mathrm{char}(K) \neq 2,3$, אז $\mathrm{Gal}(f,K) \le A_3$. כלומר, $\mathrm{Gal}(f,K) = A_3$ (ואז $[L:K] = 3$) או $\mathrm{Gal}(f,K) = 1$ (ואז $[L:K] = 1$). לכן:

(ב1) אם f אי פריק אז $\mathrm{Gal}(f,K) = A_3$.

(ב2) אם f פריק אז $\mathrm{Gal}(f,K) = 1$. אכן, $f = (X-\alpha)g$ באשר $\alpha \in K$ ו־$g \in K[X]$ ממעלה 2. לכן L הוא שדה הפיצול של g ולכן $[L:K] \le 2! = 2$. מכאן $[L:K] = 1$.

(ג) למען השלמות נציין שחלק (ב) נכון גם אם $\mathrm{char}(K) = 2$, מסיבות אחרות. אכן, $f \in \mathbb{F}_2[X]$, והוא אי פריק מעל $\mathbb{F}_2$, כי $f(0), f(1) \neq 0$. לכן שורש שלו יוצר הרחבה ממעלה 3 של $\mathbb{F}_2$. הרחבה זו היא בהכרח $\mathbb{F}_{2^3}$ והיא נורמלית, לפי משפט 9.3. לכן $\mathbb{F}_{2^3}$ הוא שדה הפיצול של f מעל $\mathbb{F}_2$. יוצא ש־$L = \mathbb{F}_{2^3}K$ ולכן $\mathrm{Gal}(L/K)$ איזומורפית לתת־חבורה של $\mathrm{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2)$. לכן היא מסדר 1 או 3. ∎

חישוב של חבורת גלואה של פולינום.

האלגוריתם הבא מבוסס על פירוק של פולינומים מעל שדות.

הגדרה 12.12: יהיו $t_1,\dots,t_n,u_1,\dots,u_n,X,Y_1,\dots,Y_n$ משתנים בלתי תלויים מעל $\mathbb{Z}$. נקצר:

$$\mathbf{Y} = (Y_1,\dots,Y_n), \qquad \mathbf{u} = (u_1,\dots,u_n), \qquad \mathbf{t} = (t_1,\dots,t_n).$$

לכל $n \in \mathbb{N}$ נגדיר פולינום

$$G_n = \prod_{\pi \in S_n} \left(X - t_{\pi(1)}u_1 - \cdots - t_{\pi(n)}u_n\right) \in \mathbb{Z}[\mathbf{u},X][\mathbf{t}]. \tag{1}$$

נזכור ש־S_n פועלת על $\mathbb{Z}[\mathbf{u},X][\mathbf{t}]$ כחבורת התמורות על $t_1,\dots,t_n$. יהי $\sigma\in S_n$. אז

$$\sigma(G_n)=G_n\big(t_{\sigma(1)},\dots,t_{\sigma(n)}\big)=\prod_{\pi\in S_n}\big(X-t_{\sigma\pi(1)}u_1-\cdots-t_{\sigma\pi(n)}u_n\big)=G_n$$

כלומר, G_n סימטרי. לכן יש $P_n(Y_1,\dots,Y_n)\in\mathbb{Z}[\mathbf{u},X][\mathbf{Y}]$ יחיד כך ש־

$$G_n=P_n\big(s_1(\mathbf{t}),\dots,s_n(\mathbf{t})\big). \tag{2}$$

נקרא ל־P_n **פולינום קרוֹנֶקֶר ה־n־י**. לדוגמה,

$$\begin{aligned}G_2&=(X-t_1u_1-t_2u_2)(X-t_2u_1-t_1u_2)=\\&=X^2-(t_1+t_2)(u_1+u_2)X+t_1t_2(u_1^2+u_2^2)+(t_1^2+t_2^2)u_1u_2\\&=X^2-s_1(\mathbf{t})(u_1+u_2)X+s_2(\mathbf{t})(u_1^2+u_2^2)+\big(s_1^2(\mathbf{t})-2s_2(\mathbf{t})\big)u_1u_2\end{aligned}$$

לכן $P_2=X^2-Y_1(u_1+u_2)X+Y_2(u_1^2+u_2^2)+(Y_1^2-2Y_2)u_1u_2$.

אפשר לראות את P_n,G_n כפולינומים מעל $\mathbb{Z}$ (הראשון במשתנים $\mathbf{u},X,\mathbf{t}$, השני במשתנים $\mathbf{u},X,\mathbf{Y}$) ולכן אפשר לראות אותם כפולינומים מעל כל שדה K, כאשר את המקדמים רואים כאיברים בשדה הראשוני של K. ∎

משפט 12.13: *יהי R תחום פריקות בעל שדה מנות K ויהי $f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in R[X]$ פולינום פריד.*

(א) *נגדיר* $g(\mathbf{u},X)=P_n(-a_1,\dots,(-1)^na_n)\in R[\mathbf{u},X]$.

(ב) *נפרק* $g(\mathbf{u},X)$ *לגורמים אי פריקים מתוקנים* $g_1(\mathbf{u},X),\dots,g_r(\mathbf{u},X)\in K(\mathbf{u})[X]$. *לפי הלמה של גאוס* $g_j(\mathbf{u},X)\in R[\mathbf{u},X]=R[\mathbf{u}][X]$, *כי* $R[\mathbf{u}]$ *תחום פריקות ו־*$K(\mathbf{u})$ *שדה המנות שלו.*

אז $g_1(\mathbf{u},X),\dots,g_r(\mathbf{u},X)$ *שונים זה מזה, ולכל* $1\le j\le r$

(ג) *לכל* $\omega\in S_n$ *יש* $1\le i\le r$ *כך ש־* $g_j(u_{\omega(1)},\dots,u_{\omega(n)},X)=g_i(\mathbf{u},X)$.

(ד) *החבורה* $\mathrm{Gal}(f,K)$ *צמודה ב־* S_n *לחבורה*

$$\{\omega\in S_n|\ g_j(u_{\omega(1)},\dots,u_{\omega(n)},X)=g_j(\mathbf{u},X)\}.$$

הוכחה: יהיו $\alpha_1,\dots,\alpha_n\in\tilde{K}$ השורשים של f (הם שונים זה מזה). יהי $L=K(\alpha_1,\dots,\alpha_n)$ שדה הפיצול של f מעל K. אז L/K הרחבת גלואה סופית. לפי הערה 3.4, $a_i=(-1)^is_i(\alpha_1,\dots,\alpha_n)$ לכל $1\le i\le n$.

לפי משפט 10.19, $L(\mathbf{u})/K(\mathbf{u})$ הרחבת גלואה סופית והעתקת הצמצום $\mathrm{res}\colon \mathrm{Gal}\big(L(\mathbf{u})/K(\mathbf{u})\big)\to\mathrm{Gal}(L/K)$ הוא איזומורפיזם על תת חבורה של $\mathrm{Gal}(L/K)$, כי $L(\mathbf{u})=K(\mathbf{u})L$. אבל כל $\sigma\in\mathrm{Gal}(L/K)$ ניתן להרחבה לאוטומורפיזם של $L[\mathbf{u}]$ (היא פועלת על המקדמים של הפולינומים ושומרת $u_1,\dots,u_n$ במקום) ומכאן לאוטומורפיזם של שדה המנות שלו $L(\mathbf{u})$ ששומר על איברי $K(\mathbf{u})$, כלומר, σ ניתן להרחבה לאיבר של $\mathrm{Gal}\big(L(\mathbf{u})/K(\mathbf{u})\big)$, ולכן res על $\mathrm{Gal}(L/K)$.

לכל $\pi \in S_n$ נסמן

$$\pi(\theta) = \alpha_{\pi(1)}u_1 + \cdots + \alpha_{\pi(n)}u_n \in L[\mathbf{u}]$$

ונשים לב ש־$\pi(\theta) = \pi'(\theta)$ אם ורק אם $\pi = \pi'$. אז

$$g(\mathbf{u}, X) = P_n\big(-a_1, \ldots, (-1)^n a_n\big) = P_n\big(s_1(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n)\big) =$$
$$= G_n(\alpha_1, \ldots, \alpha_n) = \prod_{\pi \in S_n} \big(X - \pi(\theta)\big)$$

ואגף ימין הוא פירוק לגורמים בחוג $L[\mathbf{u}][X]$, לכן

$$g_j(\mathbf{u}, X) = \prod_{\pi \in V_j} \big(X - \pi(\theta)\big)$$

עבור איזה קבוצה $\emptyset \neq V_j \subseteq S_n$, כך ש־$S_n = \dot\bigcup_{j=1}^r V_j$ (איחוד זר). מכאן נובע של־$g_1, \ldots, g_r$ (כפולינומים ב־X) יש שורשים שונים ולכן הם שונים זה מזה. לכל j נבחר ונקבע $\rho_j \in V_j$. אז $g_j = \mathrm{irr}\big(\rho_j(\theta), K(\mathbf{u})\big)$.

טענה: $V_j = \mathrm{Gal}(f, K)\rho_j$ *(שוויון תת־קבוצות של S_n).*

אכן, יהי $\pi \in S_n$. אז $\pi \in V_j \quad \Leftrightarrow$

$\Leftrightarrow$ $\pi(\theta)$ שורש של $g_j = \mathrm{irr}\big(\rho_j(\theta), K(\mathbf{u})\big)$

$\Leftrightarrow$ יש $\sigma \in \mathrm{Gal}\big(L(\mathbf{u})/K(\mathbf{u})\big)$ כך ש־ $\sigma\big(\rho_j(\theta)\big) = \pi(\theta)$, כלומר

$$\sigma(\alpha_{\rho_j(1)})u_1 + \cdots + \sigma(\alpha_{\rho_j(n)})u_n = \alpha_{\pi(1)}u_1 + \cdots + \alpha_{\pi(n)}u_n$$

$\Leftrightarrow$ יש $\sigma \in \mathrm{Gal}\big(L(\mathbf{u})/K(\mathbf{u})\big)$ כך ש־ $\sigma(\alpha_{\rho_j(i)}) = \alpha_{\pi(i)}$ לכל i

$\Leftrightarrow$ יש $\sigma \in \mathrm{Gal}\big(L(\mathbf{u})/K(\mathbf{u})\big)$ כך ש־ $\sigma(\alpha_i) = \alpha_{\pi\rho_j^{-1}(i)}$ לכל i

$\Leftrightarrow$ יש $\sigma \in \mathrm{Gal}(L/K)$ כך ש־ $\sigma(\alpha_i) = \alpha_{\pi\rho_j^{-1}(i)}$ לכל i

$\Leftrightarrow$ $\pi\rho_j^{-1} \in \mathrm{Gal}(f, K)$

$\Leftrightarrow$ $\pi \in \mathrm{Gal}(f, K)\rho_j$.

בכך הוכחה הטענה.

נסמן $G = \mathrm{Gal}(f, K) \leq S_n$. אז

$$g_j(\mathbf{u}, X) = \prod_{\pi \in V_j} \big(X - \pi(\theta)\big) = \prod_{\pi \in G\rho_j} \big(X - \alpha_{\pi(1)}u_1 - \cdots - \alpha_{\pi(n)}u_n\big)$$

כעת יהי $\omega \in S_n$. אז

$$g_j(u_{\omega(1)}, \ldots, u_{\omega(n)}, X) = \prod_{\pi \in G\rho_j} (X - \alpha_{\pi(1)}u_{\omega(1)} - \cdots - \alpha_{\pi(n)}u_{\omega(n)}) =$$
$$= \prod_{\pi \in G\rho_j} (X - \alpha_{\pi\omega^{-1}(1)}u_1 - \cdots - \alpha_{\pi\omega^{-1}(n)}u_n) = \prod_{\pi \in G\rho_j} \big(X - \pi\omega^{-1}(\theta)\big) =$$
$$= \prod_{\pi \in G\rho_j\omega^{-1}} \big(X - \pi(\theta)\big)$$

ואגף ימין הוא $g_i(\mathbf{u},X)$ עבור איזה i, כי $G\rho_j\omega^{-1}$ הוא קוסט של G ב־S_n. זה מוכיח את (ג).

כמו כן,

$$\Leftrightarrow\ \rho_j\omega\rho_j^{-1}\in G\ \Leftrightarrow\ G\rho_j=G\rho_j\omega^{-1}\ \Leftrightarrow\ g_j(u_1,\dots,u_n,X)=g_j(u_{\omega(1)},\dots,u_{\omega(n)},X)$$

$\omega\in\rho_j^{-1}G\rho_j$. זה מוכיח את (ד). ∎

כעת יהיו $R=\mathbb{Z}$ ו־$K=\mathbb{Q}$. נקבע ראשוני p ועבור פולינום h עם מקדמים ב־$\mathbb{Z}$ נסמן ב־$\bar{h}$ את תמונתו של h מודולו p (פולינום עם מקדמים ב־$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$).

יהי $f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in\mathbb{Z}[X]$ כך ש־$\bar{f}\in\mathbb{F}_p[X]$ פריד. יהי

$$P_n\big(\mathbf{u},X,-a_1,\dots,(-1)^na_n\big)=g(\mathbf{u},X)=g_1(\mathbf{u},X)\cdots g_r(\mathbf{u},X)$$

כמו לעיל. אז הפולינום המתאים ל־$\bar{f}\in\mathbb{F}_p[X]$ הוא

$$P_n\big(\mathbf{u},X,-\bar{a}_1,\dots,(-1)^n\bar{a}_n\big)=\bar{g}(\mathbf{u},X)=\bar{g}_1(\mathbf{u},X)\cdots\bar{g}_r(\mathbf{u},X)$$

אך הגורמים $\bar{g}_1(\mathbf{u},X),\dots,\bar{g}_r(\mathbf{u},X)$ אינם בהכרח אי פריקים מעל $\mathbb{F}_p(\mathbf{u})$. נפרק אותם לגורמים אי פריקים, נאמר, $\bar{g}_1(\mathbf{u},X)=\bar{g}_{11}(\mathbf{u},X)\cdots\bar{g}_{1s}(\mathbf{u},X)$.

יהי $\omega\in S_n$ כך ש־ $\bar{g}_{11}(u_{\omega(1)},\dots,u_{\omega(n)},X)=\bar{g}_{11}(\mathbf{u},X)$. לפי משפט 12.13(ג) יש $1\le i\le r$ כך ש־ $g_1(u_{\omega(1)},\dots,u_{\omega(n)},X)=g_i(\mathbf{u},X)$, ומכאן $\bar{g}_1(u_{\omega(1)},\dots,u_{\omega(n)},X)=\bar{g}_i(\mathbf{u},X)$. לכן

$$.\bar{g}_{11}(\mathbf{u},X)\mid\bar{g}_1(\mathbf{u},X),\bar{g}_i(\mathbf{u},X)$$

ומכאן $i=1$ (אחרת $\bar{g}_{11}$ היה מופיע פעמיים בפירוק של $\bar{g}$). לכן

$$g_1(u_{\omega(1)},\dots,u_{\omega(n)},X)=g_1(\mathbf{u},X)\Leftarrow\bar{g}_{11}(u_{\omega(1)},\dots,u_{\omega(n)},X)=\bar{g}_{11}(\mathbf{u},X)$$

ולכן (אם נסדר את השורשים של f ושל $\bar{f}$ באופן מתאים) $\mathrm{Gal}(\bar{f},\mathbb{F}_p)\le\mathrm{Gal}(f,\mathbb{Q})$. קיבלנו, אם כך:

משפט 12.14: *יהי $f\in\mathbb{Z}[X]$ פריד ומתוקן כך ש־$\bar{f}\in\mathbb{F}_p[X]$ פריד. אז קיים שיכון (מונומורפיזם) של חבורות תמורות $\mathrm{Gal}(\bar{f},\mathbb{F}_p)\to\mathrm{Gal}(f,\mathbb{Q})$. כלומר, אם $\alpha_1,\dots,\alpha_n\in\tilde{\mathbb{Q}}$ שורשים של f, אפשר לסדר את השורשים $\bar{\alpha}_1,\dots,\bar{\alpha}_n\in\widetilde{\mathbb{F}_p}$ של $\bar{f}$ כך ש־$\mathrm{Gal}(\bar{f},\mathbb{F}_p)\le\mathrm{Gal}(f,\mathbb{Q})$ כתת־חבורות של S_n.*

הערה 12.15: חישוב של $\mathrm{Gal}(\bar{f},\mathbb{F}_p)$. יהי $\bar{f}\in\mathbb{F}_p[X]$ פריד ומתוקן. תהי A קבוצת השורשים של $\bar{f}$. לפי משפט 11.5, $\mathrm{Gal}(\bar{f},\mathbb{F}_p)=\langle\sigma\rangle$ מעגלית באשר $\sigma=\varphi|_A$ צמצום של הפרובניוס ל־A. צריך למצוא את σ (כאיבר של S_n).

יהי $\bar{f}=\bar{f}_1\cdots\bar{f}_k$ הפירוק של $\bar{f}$ לגורמים אי פריקים מתוקנים מעל $\mathbb{F}_p$. לפי הערה 12.3, $A=\dot{\bigcup}_{i=1}^k A_i$ באשר A_i קבוצת השורשים של $\bar{f}_i$ וכל A_i הוא מסלול־$\mathrm{Gal}(\bar{f},\mathbb{F}_p)$. לכן $A_i=\{\alpha_i,\varphi(\alpha_i),\dots,\varphi^{\deg\bar{f}_i-1}(\alpha_i)\}$ עבור איזה $\alpha_i\in A_i$. מכאן ש־σ הוא מכפלה של k חישוקים (ציקלו־סים) זרים בעלי אורך $\deg\bar{f}_1,\dots,\deg\bar{f}_k$.

דוגמה 12.16: יהי $f = X^5 - X - 1$. נסמן ב־f_p (במקום $\bar{f}$) את תמונתו ב־$\mathbb{F}_p[X]$.

(א) $f_2 = (X^2 + X + 1)(X^3 + X^2 + 1)$ פירוק לגורמים אי פריקים מעל $\mathbb{F}_2$, לכן, בלי הגבלת הכלליות, $\pi = (1\ 2)(3\ 4\ 5) \in \mathrm{Gal}(f_2, \mathbb{F}_2)$.

(ב) f_5 אי פריק מעל $\mathbb{F}_5$ לכן $\mathrm{Gal}(f_5, \mathbb{F}_5)$ נוצרת על ידי חישוק מאורך 5.

לכן $\mathrm{Gal}(f, \mathbb{Q})$ מכילה את $\pi^3 = (1\ \ 2)$ וחישוק ρ מאורך 5. נחליף את ρ בחזקה מתאימה ואז $\rho = (1\ \ 2\ \ \ldots)$, לכן בלי הגבלת הכלליות $\rho = (1\ \ 2\ \ 3\ \ 4\ \ 5)$. כידוע, $S_5 = \langle (1\ 2), (1\ \ 2\ \ 3\ \ 4\ \ 5) \rangle$. לכן $\mathrm{Gal}(f, \mathbb{Q}) = S_5$. ∎

13. שורשי היחידה

יהי K שדה ויהי $\tilde{K}$ סגור אלגברי שלו. אז $K^\times$ חבורה (ביחס לכפל).

הגדרה 13.1: איבר $\zeta \in K^\times$ הוא

(א) **שורש יחידה n־י**, אם $\zeta^n = 1$, כלומר, $\mathrm{ord}\ \zeta \mid n$. קבוצת שורשי יחידה n־יים ב־K תסומן $\mu_n(K)$.

(ב) **שורש יחידה n־י פרימיטיבי**, אם $\zeta^n = 1$ ו־$\zeta^k \neq 1$ לכל $1 \leq k < n$, כלומר, $\mathrm{ord}\ \zeta = n$.

(ג) **שורש יחידה**, אם $\zeta^n = 1$ עבור איזה $n \in \mathbb{N}$, כלומר, $\mathrm{ord}\ \zeta < \infty$. קבוצת שורשי יחידה ב־$K$ תסומן $\mu(K)$.

הערה 13.2: (א) $\mu_n(K)$ היא קבוצת השורשים של $X^n - 1$ ב־K. לכן $|\mu_n(K)| \leq n$.

(ב) $|\mu_n(\tilde{K})| = n$ אם ורק אם $X^n - 1$ פריד, כלומר, $n \neq 0$ ב־K, כלומר, $\mathrm{char}(K) \nmid n$.

(ג) $\mu_n(K)$ היא תת־חבורה סופית של $K^\times$. לפי משפט 7.1 היא מעגלית.

(ד) אם $\zeta \in K$ שורש יחידה n־י פרימיטיבי אז $\langle\zeta\rangle = \mu_n(K)$ ו־$|\mu_n(K)| = n$.

(ה) יש ב־$\tilde{K}$ שורש יחידה n־י פרימיטיבי אם ורק אם $\mathrm{char}(K) \nmid n$.

(ו) אם $\mathrm{ord}\,\zeta = n$ אז $\mathrm{ord}\,\zeta^i = \frac{n}{\gcd(n,i)}$, לכן: אם ζ n־י פרימ׳, אז ζ^i n־י פרימ׳ אם ורק אם i זר ל־n. ∎

למה 13.3: *נסמן $W = \mu_n(\tilde{K})$. יהי $\zeta \in W$ שורש יחידה n־י פרימיטיבי. אז $K(\zeta) = K(W)$ הרחבת גלואה סופית של K ויש שיכון $i\colon \mathrm{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ הנתון על ידי $\sigma(\zeta) = \zeta^{i(\sigma)}$.*

הוכחה: כיוון ש־$\zeta \in W$, מתקיים $K(\zeta) \subseteq K(W)$. כיוון שאברי W הם חזקות של ζ, מתקיים $K(W) \subseteq K(\zeta)$. לכן $K(\zeta) = K(W)$. לפי הערה 13.2(א), $K(W)$ הוא שדה פיצול של $X^n - 1$. לפי הערה 13.2(ד),(ב), $X^n - 1$ פריד. לכן $K(W)/K$ גלואה סופית.

יהי $\sigma \in \mathrm{Gal}(K(W)/K)$. אז $\bigl(\sigma(\zeta)\bigr)^n = \sigma(\zeta^n) = 1$ לכן $\sigma(\zeta) \in W$. לכן יש $i \in \mathbb{Z}$ כך ש־$\sigma(\zeta) = \zeta^i$. הוא אינו יחיד, אבל $\zeta^i = \zeta^j \Leftrightarrow \zeta^{i-j} = 1 \Leftrightarrow n \mid i - j$. לכן התמונה של i ב־$\mathbb{Z}/n\mathbb{Z}$ מוגדרת היטב; נסמן אותה $i(\sigma)$. בכך הגדרנו העתקה $i\colon \mathrm{Gal}(K(\zeta)/K) \to \mathbb{Z}/n\mathbb{Z}$ שמקיימת $\sigma(\zeta) = \zeta^{i(\sigma)}$.

ברור ש־$i(1) = 1$. אם $\sigma, \tau \in \mathrm{Gal}(K(W)/K)$ אז

$$\zeta^{i(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\tau(\zeta)) = \sigma\bigl(\zeta^{i(\tau)}\bigr) = \bigl(\sigma(\zeta)\bigr)^{i(\tau)} = \zeta^{i(\sigma)i(\tau)},$$

לכן $i(\sigma\tau) = i(\sigma)i(\tau)$. בפרט $i(\sigma)i(\sigma^{-1}) = i(1) = 1$, לכן $i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$, ו־$i$ הוא הומומורפיזם. אם $\sigma \in \mathrm{Ker}\, i$, אז $\sigma(\zeta) = \zeta^1 = \zeta$, לכן $\sigma = 1$. לכן i חד חד ערכית. ∎

הערה 13.4: (א) $(\mathbb{Z}/n\mathbb{Z})^\times = \{k + n\mathbb{Z} |\ 0 \leq k < n,\ \text{זרים } k, n\}$.

(אכן, $k \in \mathbb{Z}$ הפיך ב־$\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ יש $m \in \mathbb{Z}$ כך ש־$km \equiv 1 \mod n$ $\Leftrightarrow$ יש $\ell, m \in \mathbb{Z}$ כך ש־$km + \ell n = 1$ $\Leftrightarrow$ k, n זרים). לכן $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) := |\{k |\ 0 \leq k < n,\ \text{זרים } k, n\}|$.

(ב) משפט השאריות הסיני: אם m, n זרים אז

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ על ידי $a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$; לכן

$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$; מכאן

$\varphi(mn) = \varphi(m)\varphi(n)$.

בפרט, אם $p_1, \ldots, p_r$ ראשוניים שונים, אז

$(\mathbb{Z}/{p_1}^{m_1} \cdots {p_r}^{m_r}\mathbb{Z})^\times \cong (\mathbb{Z}/{p_1}^{m_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/{p_r}^{m_r}\mathbb{Z})^\times$.

(ג) יהי p ראשוני. אז $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$, ביתר דיוק,

אם $p \neq 2$ ו־$m \geq 1$, אז $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \cong \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$, ואם

$p = 2$ ו־$m > 1$ אז $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

מסקנה 13.5: *יהי $\zeta \in \tilde{K}$ שורש יחידה n־י פרימיטיבי. אז $[K(\zeta) : K] \leq \varphi(n)$ ו־$\mathrm{Gal}\big(K(\zeta)/K\big)$ אבלית. מתקיים $[K(\zeta) : K] = \varphi(n)$ אם ורק אם כל ζ^k, באשר k זר ל־n, הוא שורש של $\mathrm{irr}(\zeta, K)$.*

משפט 13.6: *יהי $\zeta \in \tilde{\mathbb{Q}}$ שורש יחידה n־י פרימיטיבי. אז*

(א) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$;

(ב) $\mathrm{Gal}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

הוכחה: לפי למה 13.3, (ב) נובע מ־(א).

(א) יהי $f = \mathrm{irr}(\zeta, \mathbb{Q})$. לפי מסקנה 13.5, $\deg f \leq \varphi(n)$ וכדי להוכיח $\deg f \geq \varphi(n)$, די להראות:

אם $f(\xi) = 0$ אז $f(\xi^k) = 0$ לכל k זר ל־n.

אבל $k = p_1 p_2 \cdots p_r$, באשר $p_1, p_2, \ldots, p_r$ ראשוניים. לכן באינדוקציה על r די להראות:

טענה: אם $f(\xi) = 0$ אז $f(\xi^p) = 0$ *לכל $p \nmid n$ ראשוני.*

אכן, $f \mid X^n - 1$, לכן $X^n - 1 = fh$ עבור איזה $h \in \mathbb{Q}[X]$ מתוקן. לפי הלמה של גאוס, $f, h \in \mathbb{Z}[X]$. כעת, $(\xi^p)^n = (\xi^n)^p = 1$, כלומר, ξ^p שורש של fh. נניח בשלילה כי $f(\xi^p) \neq 0$. אז $h(\xi^p) = 0$. לכן ξ שורש של $h(X^p)$, ולכן $f \mid h(X^p)$. אז יש $g \in \mathbb{Q}[X]$ מתוקן כך ש־$h(X^p) = fg$. לפי הלמה של גאוס, $g \in \mathbb{Z}[X]$.

עבור $a \in \mathbb{Z}$ נסמן ב־$\overline{a}$ את תמונה של a ב־$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; עבור $q = \sum_i b_i X^i \in \mathbb{Z}[X]$ נסמן $\overline{q} = \sum_i \overline{b_i} X^i \in \mathbb{F}_p[X]$. אם $h = \sum_i a_i X^i \in \mathbb{Z}[X]$ אז

$$\overline{f}\,\overline{g} = \overline{fg} = \overline{h(X^p)} = \sum_i \overline{a_i}(X^p)^i = \sum_i \overline{a_i}^p X^{ip} = \big(\sum_i \overline{a_i} X^i\big)^p = \overline{h}^p,$$

לכן כל שורש של $\overline{f}$ הוא גם שורש של $\overline{h}$. אבל $X^n - 1 = \overline{f}\,\overline{h}$, לכן לפולינום $X^n - 1$ יש שורשים מרובים (ב־$\tilde{\mathbb{F}}_p$) סתירה (כי $p \nmid n$). ∎

הגדרה 13.7: יהי K שדה, $n \nmid \operatorname{char} K$. **הפולינום הציקלוטומי ה־n־י** (מעל K) הוא הפולינום

$$\Phi_{n,K}(X) = \prod_{\substack{\zeta\in\tilde{K} \\ \text{שורש יחידה} \\ n\text{־י פרימיטיבי}}} (X-\zeta) = \prod_{\zeta\in\tilde{K}^\times,\ \operatorname{ord}\zeta=n} (X-\zeta) = \prod_{\substack{0\le k<n \\ k,n\ \text{זרים}}} (X-\zeta_n^k),$$

באשר ζ_n שורש יחידה n־י פרימיטיבי. נסמן $\Phi_n = \Phi_{n,\mathbb{Q}}$. ∎

טענה 13.8: *(א)* $\Phi_n = \operatorname{irr}(\zeta_n, \mathbb{Q})$.

(ב) $\Phi_n \in \mathbb{Z}[X]$.

(ג) $\Phi_{1,K}(X) = X-1$; $\Phi_{n,K}(X) = \frac{X^n-1}{\prod_{d|n,\ d<n}\Phi_{d,K}(X)}$.

(ד) *הפולינום הציקלוטומי אינו תלוי בשדה: $\Phi_{n,K}$ הוא התמונה של Φ_n תחת ההומומורפיזם* $\mathbb{Z}[X]\to K[X]$.

הוכחה: (א) לפי מסקנה 13.5 ומשפט 13.6.

(ב) לפי (א), $\Phi_n \in \mathbb{Q}[X]$ מתוקן. מתקיים $\Phi_n | X^n-1$ ב־$\tilde{\mathbb{Q}}[X]$, לכן גם ב־$\mathbb{Q}[X]$. לפי הלמה של גאוס, $\Phi_n \in \mathbb{Z}[X]$.

(ג) $\prod_{d|n}\Phi_{d,K} = \prod_{d|n}\prod_{\substack{\zeta\in\tilde{K}^\times \\ \operatorname{ord}\zeta=d}}(X-\zeta) = \prod_{\substack{\zeta\in\tilde{K}^\times \\ \operatorname{ord}\zeta|n}}(X-\zeta) = X^n-1$, ומכאן המסקנה.

(ד) באינדוקציה על n, לפי (ג). ∎

לפי טענה 13.8(ד) אפשר לחשב את Φ_n, באינדוקציה על n. למשל,

$$\Phi_p(X) = \frac{(X^p-1)}{(X-1)} = X^{p-1}+\dots+X+1 \qquad (p \text{ ראשוני}),$$

$$\Phi_6(X) = \frac{X^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{X^6-1}{(X-1)(X+1)(X^2+X+1)} = \frac{X^6-1}{X^4+X^3-X-1} = \\ = X^2-X+1.$$

מסקנה 13.9: אם m,n *זרים אז:*

(א) $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$.

(ב) $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) = \mathbb{Q}$.

הוכחה: (א) "$\subseteq$": $\operatorname{ord}(\zeta_n)=n$, $\operatorname{ord}(\zeta_m)=m$, לכן $\operatorname{ord}(\zeta_m\zeta_n)=mn$. לכן $\zeta_m\zeta_n$ הוא שורש יחידה mn־י פרימיטיבי, ולכן ζ_{mn} הוא חזקה שלו. מכאן $\zeta_{mn}\in\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$.

"$\supseteq$": $\operatorname{ord}(\zeta_{mn})=mn$, לכן $\operatorname{ord}(\zeta_{mn}^m)=n$, כלומר, ζ_{mn}^m הוא שורש יחידה n־י פרימיטיבי. לכן ζ_n הוא חזקה שלו. מכאן $\zeta_n\in\mathbb{Q}(\zeta_{mn})$, ולכן $\mathbb{Q}(\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})$. באופן דומה $\mathbb{Q}(\zeta_m)\subseteq\mathbb{Q}(\zeta_{mn})$.

(ב) קיים תרשים של שדות, עם ציון מעלות (שוויון המעלות בצלעות הנגדיות של המעוין נובע ממשפט 10.19)

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn}) \arrow[dl, dash, "b"'] \arrow[dr, dash, "a"] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash, "a"'] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash, "b"] \\
 & \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \arrow[d, dash, "c"'] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

לפי משפט 13.6, $ac = \varphi(m), bc = \varphi(n), abc = \varphi(mn)$. כיוון ש־$\varphi(mn) = \varphi(m)\varphi(n)$, כלומר, $abc = (ac)(bc)$, יוצא $c = 1$. ∎

נשתמש במשפט הבא מתורת המספרים:

משפט 13.10 (Dirichlet): *יהיו* $a, n \in \mathbb{N}$ *זרים. אז יש אינסוף ראשוניים* p *כך ש־*$p \equiv a \pmod{n}$.

משפט 13.11: *תהי* A *חבורה אבלית סופית. אז יש* $L/\mathbb{Q}$ *גלואה סופית כך ש־*$A \cong \mathrm{Gal}(L/\mathbb{Q})$.

הוכחה: כידוע, $A \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ עבור איזה $n_1, \ldots, n_r$. לפי משפט דיריכלה יש ראשוניים שונים*(!)* $p_1, \ldots, p_r$ כך ש־$p_i \equiv 1 \pmod{n_i}$ לכל i. נסמן $G_i = \mathrm{Gal}\big(\mathbb{Q}(\zeta_{p_i}/\mathbb{Q})\big)$ לכל i. אז $G_i \cong (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \mathbb{Z}/(p_i - 1)\mathbb{Z}$, לכן יש $H_i \le G_i$ בעלת אינדקס n_i. יהי $L_i \subseteq \mathbb{Q}(\zeta_{p_i})$ שדה השבת שלה; אז $\mathrm{Gal}(L_i/\mathbb{Q}) \cong G_i/H_i \cong \mathbb{Z}/n_i\mathbb{Z}$. לכן די להוכיח:

טענה: *יהיו* $p_1, \ldots, p_r$ *ראשוניים שונים. לכל* $1 \le i \le r$ *יהי* $L_i \subseteq \mathbb{Q}(\zeta_{p_i})$. *אז*
$\mathrm{Gal}(L_1 \cdots L_r/\mathbb{Q}) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(L_r/\mathbb{Q})$.

אכן, זה נובע באינדוקציה על r: עבור $r = 1$ הטענה ברורה.
נניח $\mathrm{Gal}(L_1 \cdots L_{r-1}/\mathbb{Q}) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(L_{r-1}/\mathbb{Q})$. אז

$$(L_1 \cdots L_{r-1} \cap L_r) \subseteq \big(\mathbb{Q}(\zeta_{p_1}) \cdots \mathbb{Q}(\zeta_{p_{r-1}})\big) \cap \mathbb{Q}(\zeta_{p_r}) \subseteq \mathbb{Q}(\zeta_{p_1 \cdots p_{r-1}}) \cap \mathbb{Q}(\zeta_{p_r}) \subseteq \mathbb{Q},$$

לכן $(L_1 \cdots L_{r-1}) \cap L_r = \mathbb{Q}$. מכאן לפי משפט 10.21(ד),

$$\mathrm{Gal}(L_1 \cdots L_{r-1}L_r/\mathbb{Q}) \cong \mathrm{Gal}(L_1 \cdots L_{r-1}/\mathbb{Q}) \times \mathrm{Gal}(L_r/\mathbb{Q}) \cong$$

$$\big(\mathrm{Gal}(L_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(L_{r-1}/\mathbb{Q})\big) \times \mathrm{Gal}(L_r/\mathbb{Q}) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(L_r/\mathbb{Q})$$

∎

הערה 13.12: (א) המשפט הקודם הוא מקרה פרטי של משפט שפרביץ' (אותו לא הוכחנו).

(ב) הבניה שלנו היא כזאת ש־$L \subseteq \mathbb{Q}(\zeta_n)$ עבור איזה n. משפט Kronecker-Weber אומר שזה בהכרח חייב להיות כך.

(ג) הוכחה של משפט דיריכלה אינה קלה. אך השתמשנו במשפט זה רק עבור $a = 1$, ובמקרה זה יש הוכחה קלה, שמשתמשת בחומר שלמדנו בפרק זה: ∎

למה 13.13: *יהי* $f \in \mathbb{Z}[X]$ *ממעלה* $n \geq 1$*. אז הקבוצה* $P_f = \{p \text{ ראשוני} | \ (\exists x \in \mathbb{Z})\, p | f(x) \neq 0\}$ *אינסופית.*

הוכחה: כיוון ש־$\deg f \geq 1$, יש $a \in \mathbb{Z}$ כך ש־$b := f(a) \neq 0$. אז יש $h \in \mathbb{Z}[X]$ ממעלה n כך ש־$f(a+bX) = bh(X)$ ו־$h(0) = 1$. (אכן, פיתוח טיילור סביב a נותן $f(a+bX) = \sum_{i=0}^n c_i b^i X^i$, באשר $c_0 = f(a) = b$ ו־$c_i \in \mathbb{Z}$ לכל i; נגדיר $h(X) = (\sum_{i=0}^n c_i b^i X^i)/b$.) נשים לב ש־$P_h \subseteq P_f$.

נניח בשלילה ש־P_f סופית, $P_f = \{p_1, \ldots, p_k\}$. יש $x \in \mathbb{Z}$ כך ש־$c := h(p_1 \cdots p_k x) \neq 0, \pm 1$. אז $c \equiv h(0) = 1 \mod p_i$ לכל i ובפרט $p_i \nmid c$. לכן יש p ראשוני כך ש־$p|c$ אך $p \neq p_i$ לכל i. אבל אם $p|c$ אז $p \in P_h \subseteq P_f$, סתירה. ∎

הוכחה של משפט דיריכלה עבור $a = 1$: יהי $f = \Phi_n \in \mathbb{Z}[X]$. לפי למה 13.13 יש אינסוף ראשוניים $p > n$ (ובפרט $p \nmid n$) עבורם יש $x \in \mathbb{Z}$ כך ש־$p|f(x)$. נראה שעבור כל p כזה $n|p-1$, כלומר, $p \equiv 1 \pmod n$.

נסמן ב־$\bar{x} \in \mathbb{F}_p, \bar{f} \in \mathbb{F}_p[X]$ את הרדוקציות של x, f מודולו p. כיוון ש־$p|f(x)$, מתקיים $\bar{f}(\bar{x}) = 0$. לפי טענה 13.8(ד), $\bar{f} = \Phi_{n,\mathbb{F}_p}$. לכן $\bar{x} \in \mathbb{F}_p^\times$ ו־$\operatorname{ord} \bar{x} = n$. כיוון ש־$\bar{x} \in \mathbb{F}_p^\times$, מתקיים $\bar{x}^{p-1} = 1$. לכן $n = \operatorname{ord} \bar{x} | p-1$. ∎

14. אי תלות לינארית של קרקטרים

הגדרה 14.1: **קרקטר** של חבורה G הוא הומומורפיזם חבורות $\chi\colon G \to K^\times$, באשר K שדה.

משפט 14.2 (Artin): *קרקטרים שונים $\chi_1, \dots, \chi_n\colon G \to K^\times$ הם (כאיברים במרחב הוקטורי של הפונקציות מ־G לתוך K) בלתי תלויים לינארית מעל K, כלומר, אם $a_1, \dots, a_n \in K$ ו־*

$$a_1\chi_1 + \cdots + a_n\chi_n = 0 \quad \text{(= פונקציית האפס)} \tag{1}$$

אז $a_1 = \cdots = a_n = 0$.

הוכחה: באינדוקציה על n. עבור $n = 1$ זה ברור, כי $\chi_i \neq 0$ לכל i. נניח שהטענה נכונה עבור $n - 1$ קרקטרים ושמתקיים (1). כיוון ש־$\chi_1 \neq \chi_n$, יש $g_0 \in G$ כך ש־$\chi_1(g_0) \neq \chi_n(g_0)$. נכפיל את (1) ב־$\chi_n(g_0)$:

$$a_1\chi_n(g_0)\chi_1 + \cdots + a_{n-1}\chi_n(g_0)\chi_{n-1} + a_n\chi_n(g_0)\chi_n = 0. \tag{2}$$

מצד שני, לכל $g \in G$, מתקיים $a_1\chi_1(g_0g) + \cdots + a_n\chi_n(g_0g) = 0$, לכן $a_1\chi_1(g_0)\chi_1(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0$. מכאן

$$a_1\chi_1(g_0)\chi_1 + \cdots + a_{n-1}\chi_{n-1}(g_0)\chi_{n-1} + a_n\chi_n(g_0)\chi_n = 0 \tag{3}$$

נחסיר את (2) מ־(3):

$$a_1\big(\chi_1(g_0) - \chi_n(g_0)\big)\chi_1 + \cdots + a_{n-1}\big(\chi_{n-1}(g_0) - \chi_n(g_0)\big)\chi_{n-1} = 0$$

לפי הנחת האינדוקציה, $a_1\big(\chi_1(g_0) - \chi_n(g_0)\big) = 0$, ולכן $a_1 = 0$. נציב זאת ב־(1). לפי הנחת האינדוקציה, $a_2 = \cdots = a_n = 0$. ∎

מסקנה 14.3: *תהי L/K הרחבה פרידה ממעלה n. יהי $\alpha_1, \dots, \alpha_n \in L$ בסיס של L מעל K ויהיו $\sigma_1, \dots, \sigma_n$ כל האיברים השונים של $\mathrm{Ism}_K(L, \tilde{K})$. אז* $\det\big(\sigma_i(\alpha_j)\big) \neq 0$.

הוכחה: די להוכיח שהשורות של המטריצה $\big(\sigma_i(\alpha_j)\big) \in \mathrm{M}_n(\tilde{K})$ בלתי תלויות לינארית מעל $\tilde{K}$. השורה ה־i היא $\xi_i = \big(\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)\big)$. יהיו $a_1, \dots, a_n \in \tilde{K}$ כך ש־$\sum_i a_i\xi_i = 0$. אז $\sum_i a_i\sigma_i(\alpha_j) = 0$ לכל j. מכאן נובע ש־$\sum_i a_i\sigma_i$ היא פונקציה האפס על L. אכן, יהי $\alpha \in L$. אז $\alpha = \sum_{j=1}^n b_j\alpha_j$, באשר $b_1, \dots, b_n \in K$, ולכן

$$\sum_{i=1}^n a_i\sigma_i(\alpha) = \sum_{i=1}^n a_i\sigma_i\big(\sum_{j=1}^n b_j\alpha_j\big) = \sum_{i=1}^n a_i\sum_{j=1}^n b_j\sigma_i(\alpha_j) = \sum_{j=1}^n b_j\sum_{i=1}^n a_i\sigma_i(\alpha_j) = 0\,.$$

אבל $\sigma_1, \dots, \sigma_n\colon L^\times \to \tilde{K}^\times$ הם קרקטרים שונים, לכן לפי המשפט $a_1 = \cdots = a_n = 0$. ∎

15. הרחבות מעגליות

הגדרה 15.1: תהי L/K הרחבה גלואה סופית. נגדיר שתי העתקות:

(א) $T_{L/K}\colon L \to K$ הנתונה על ידי $T_{L/K}(\alpha) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(\alpha)$ נקראת **העקבה מ־L לתוך** K.

(ב) $N_{L/K}\colon L \to K$ הנתונה על ידי $N_{L/K}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(\alpha)$ נקראת **הנורמה מ־L לתוך** K.

הערה 15.2: זהו רק מקרה פרטי של הגדרה כללית יותר: העקבה והנורמה מוגדרות לכל הרחבה סופית L/K, באופן הבא: אם $\alpha \in L$ אז $x \mapsto \alpha x$ היא העתקה לינארית (מעל L ולכן) מעל K. $T_{L/K}(\alpha)$ ו־$N_{L/K}(\alpha)$ מוגדרת כעקבה והדטרמיננטה של העתקה זו, בהתאמה. ∎

למה 15.3: *תהי L/K הרחבת גלואה סופית. אז $T_{L/K}$ אינה העתקת האפס ויש $\beta \in L$ כך ש־* $T_{L/K}(\beta) = 1$.

הוכחה: נתבונן באברי $\mathrm{Gal}(L/K)$ כקרקטרים $L^\times \to L^\times$. לפי משפט 14.2, $T_{L/K} = \sum_{\sigma\in\mathrm{Gal}(L/K)} 1\sigma$ אינה העתקת האפס. נבחר $\alpha \in L$ כך ש־$c := T_{L/K}(\alpha) \neq 0$. אז $T_{L/K}(\alpha/c) = c/c = 1$. ∎

משפט 15.4 (משפט 90 של הילברט): *תהי L/K הרחבה מעגלית סופית בעלת חבורת גלואה G ויהי σ יוצר של G. יהי $\beta \in L^\times$. אז $N_{L/K}(\beta) = 1$ אם ורק אם יש $\alpha \in L^\times$ כך ש־* $\beta = \frac{\alpha}{\sigma(\alpha)}$.

הוכחה: נניח $\beta = \frac{\alpha}{\sigma(\alpha)}$. אז

$$N_{L/K}(\beta) = \prod_{\tau\in G} \tau\Big(\frac{\alpha}{\sigma(\alpha)}\Big) = \prod_{\tau\in G} \frac{\tau(\alpha)}{\tau\sigma(\alpha)} = \frac{\prod_{\tau\in G}\tau(\alpha)}{\prod_{\tau\in G}\tau\sigma(\alpha)} = 1.$$

להיפך, נניח $N_{L/K}(\beta) = 1$. יהי $n = |G|$. הקרקטרים $1, \sigma, \ldots, \sigma^{n-1}\colon L^\times \to L^\times$ הם שונים, לכן לפי משפט ארטין בת"ל מעל L, לכן $1 \cdot 1_L + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1} \neq 0$. לכן יש $z \in L$ כך ש־

$$\alpha := z + \beta\sigma(z) + \beta\sigma(\beta)\sigma^2(z) + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(z) \neq 0.$$

מתקיים

$$\begin{aligned}
\beta\sigma(\alpha) &= \\
&\beta\sigma(z) + \beta\sigma(\beta)\sigma^2(z) + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(z) + \beta\sigma(\beta)\cdots\sigma^{n-1}(\beta)\sigma^n(z) = \\
&\beta\sigma(z) + \beta\sigma(\beta)\sigma^2(z) + \ldots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(z) + z = \alpha
\end{aligned}$$

כי $\beta\sigma(\beta)\cdots\sigma^{n-1}(\beta) = N_{L/K}(\beta) = 1$ ו־$\sigma^n = 1_L$. לכן $\beta = \frac{\alpha}{\sigma(\alpha)}$. ∎

משפט 15.5 (Kummer): *יהי K שדה, $n \in \mathbb{N}$ כך ש־$n \nmid \mathrm{char}(K)$. נניח ש־$\zeta_n \in K$.*

(א) *תהי L/K הרחבה מעגלית ממעלה n. אז יש $\alpha \in L^\times$ כך ש־$L = K(\alpha)$ ו־$\alpha^n \in K$ (כלומר, α שורש של $X^n - a \in K[X]$).*

(ב) *יהי $a \in K^\times$ ויהי $\alpha \in \tilde{K}$ שורש של $X^n - a$. אז $K(\alpha)/K$ מעגלית ממעלה d, באשר $d \mid n$ ו־$\alpha^d \in K$.*

הוכחה: (א) יהי σ יוצר של $\mathrm{Gal}(L/K)$. מתקיים $N_{L/K}(\zeta_n^{-1}) = \prod_{i=0}^{n-1} \sigma^i(\zeta_n^{-1}) = (\zeta_n^{-1})^n = 1$, לכן לפי משפט 90 של הילברט יש $\alpha \in L^\times$ כך ש־$\zeta_n^{-1} = \alpha/\sigma(\alpha)$, כלומר, $\sigma(\alpha) = \zeta_n\alpha$. באינדוקציה $\sigma^i(\alpha) = \zeta_n^i\alpha$ לכל $i = 0, \dots, n-1$, לכן $\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha \in L$ שורשים של $\mathrm{irr}(\alpha, K)$. הם שונים זה מזה, לכן $[K(\alpha) : K] \geq n$, ולכן $L = K(\alpha)$. כמו כן, $\sigma^i(\alpha^n) = \big(\sigma^i(\alpha)\big)^n = (\zeta_n^i\alpha)^n = \zeta_n^{in}\alpha^n = \alpha^n$, לכן $\alpha^n \in L^{\mathrm{Gal}(L/K)} = K$.

(ב) האיברים $\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha \in K(\alpha)$ הם שורשים של $X^n - a$, שונים זה מזה, לכן הם כל השורשים של $X^n - a$. אז $L := K(\zeta_n, \alpha) = K(\alpha)$, שדה הפיצול של $X^n - a$ מעל K, הוא הרחבת גלואה של K.

אם $\sigma \in \mathrm{Gal}(L/K)$, אז גם $\sigma(\alpha)$ שורש של $X^n - a$, לכן $\big(\frac{\sigma(\alpha)}{\alpha}\big)^n = \frac{\sigma(\alpha)^n}{\alpha^n} = 1$, כלומר $\frac{\sigma(\alpha)}{\alpha}$ שורש יחידה n־י. לכן יש $\omega(\sigma) \in \langle\zeta_n\rangle = \mu_n(\tilde{K}) \cong \mathbb{Z}/n\mathbb{Z}$ כך ש־$\sigma(\alpha) = \omega(\sigma)\alpha$. אם $\sigma, \tau \in \mathrm{Gal}(L/K)$ אז

$$\omega(\sigma\tau)\alpha = (\sigma\tau)(\alpha) = \sigma\big(\tau(\alpha)\big) = \sigma\big(\omega(\tau)\alpha\big) = \omega(\tau)\sigma(\alpha) = \omega(\tau)\omega(\sigma)\alpha = \omega(\sigma)\omega(\tau)\alpha,$$

לכן $\omega(\sigma\tau) = \omega(\sigma)\omega(\tau)$. לפי כך ω הוא הומומורפיזם חבורות. גרעינו הוא $\{\sigma \mid \sigma(\alpha) = \alpha\} = \{1\}$, לכן ω שיכון. מכאן נובע ש־$\mathrm{Gal}(L/K)$ היא מעגלית מסדר d, באשר $d \mid n$.

אם $\sigma \in \mathrm{Gal}(L/K)$, אז $d \mid \mathrm{ord}\,\sigma = \mathrm{ord}\,\omega(\sigma)$, לכן

$$\sigma(\alpha^d) = \big(\sigma(\alpha)\big)^d = \big(\omega(\sigma)\alpha\big)^d = \big(\omega(\sigma)\big)^d\alpha^d = \alpha^d.$$

לכן $\alpha^d \in K$. ∎

כעת נדון בהרחבות מעגליות ממעלה ראשונית p מעל שדה בעל איפיון p.

משפט 15.6 (משפט 90 של הילברט, גרסה חיבורית): *תהי L/K הרחבה מעגלית סופית בעלת חבורת גלואה G ויהי σ יוצר של G. יהי $\beta \in L$. אז $T_{L/K}(\beta) = 0$ אם ורק אם יש $\alpha \in L$ כך ש־$\beta = \alpha - \sigma(\alpha)$.*

הוכחה: נניח $\beta = \alpha - \sigma(\alpha)$. אז

$$T_{L/K}(\beta) = \sum_{\tau \in G} \tau\big(\alpha - \sigma(\alpha)\big) = \sum_{\tau \in G} \tau(\alpha) - \tau\sigma(\alpha) = \sum_{\tau \in G} \tau(\alpha) - \sum_{\tau \in G} \tau\sigma(\alpha) = 0.$$

להיפך, נניח $T_{L/K}(\beta) = 0$. יהי $n = |G|$. לפי למה 15.3 יש $z \in L$ כך ש־ $T_{L/K}(z) = 1$. יהי

$$\alpha = \beta\sigma(z) + \big(\beta + \sigma(\beta)\big)\sigma^2(z) + \cdots + \big(\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta)\big)\sigma^{n-1}(z).$$

אז

$$\sigma(\alpha) =$$
$$\sigma(\beta)\sigma^2(z) + \big(\sigma(\beta)+\sigma^2(\beta)\big)\sigma^3(z) + \cdots + \big(\sigma(\beta)+\sigma^2(\beta)+\cdots+\sigma^{n-2}(\beta)\big)\sigma^{n-1}(z) +$$
$$\cdots + \big(\sigma(\beta)+\sigma^2(\beta)+\cdots+\sigma^{n-1}(\beta)\big)\sigma^n(z)$$

והמחובר האחרון (השורה האחרונה) הוא $\big(T_{L/K}(\beta)-\beta\big)z = -\beta z$. לכן

$$\alpha - \sigma(\alpha) = \beta\sigma(z) + \beta\sigma^2(z) + \cdots + \beta\sigma^{n-1}(z) + \beta z = \beta\, T_{L/K}(z) = \beta. \qquad \blacksquare$$

משפט 15.7 (Artin-Schreier): *יהי K שדה, $\mathrm{char}(K) = p > 0$.*

(א) *תהי L/K הרחבה מעגלית ממעלה p. אז יש $\alpha \in L$ כך ש־$L = K(\alpha)$ ו־α שורש של $X^p - X - a \in K[X]$ עבור איזה $a \in K$.*

(ב) *יהי $a \in K$ ויהי $\alpha \in \tilde{K}$ שורש של $f = X^p - X - a$. אז $K(\alpha)/K$ מעגלית ממעלה 1 או p. במקרה הראשון כל שורשי f ב־K, ובמקרה השני f אי פריק.*

הוכחה: (א) יהי σ יוצר של $\mathrm{Gal}(L/K)$. מתקיים $T_{L/K}(-1) = \sum_{i=0}^{p-1}\sigma^i(-1) = p(-1) = 0$, לכן לפי משפט 90 של הילברט יש $\alpha \in L$ כך ש־$\alpha - \sigma(\alpha) = -1$, כלומר, $\sigma(\alpha) = \alpha+1$. באינדוקציה $\sigma^i(\alpha) = \alpha+i$ לכל $i \ge 0$, לכן $\alpha, \alpha+1, \ldots, \alpha+(p-1) \in L$ שורשים של $\mathrm{irr}(\alpha, K)$. הם שונים זה מזה, לכן $[K(\alpha):K] \ge p$, ולכן $L = K(\alpha)$. כמו כן, $\sigma^i(\alpha^p - \alpha) = \sigma^i(\alpha^p) - \sigma^i(\alpha) = (\alpha+i)^p - (\alpha+i) = \alpha^p - \alpha$ לכן $a := \alpha^p - \alpha \in L^{\mathrm{Gal}(L/K)} = K$.

(ב) האיברים $\alpha, \alpha+1, \ldots, \alpha+(p-1) \in K(\alpha)$ הם שורשים של f. אכן,

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

לכל $i \in \mathbb{F}_p$. הם שונים זה מזה, לכן הם כל השורשים של f. אז $K(\alpha)$, שדה הפיצול של f, שהינו פריד מעל K, הוא הרחבת גלואה של K.

אם $\sigma \in \mathrm{Gal}\big(K(\alpha)/K\big)$, אז גם $\sigma(\alpha)$ שורש של f, לכן יש $\omega(\sigma) \in \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ כך ש־$\sigma(\alpha) = \alpha + \omega(\sigma)$.

אם $\sigma, \tau \in \mathrm{Gal}\big(K(\alpha)/K\big)$, אז

$$\alpha + \omega(\sigma\tau) = (\sigma\tau)(\alpha) = \sigma\big(\tau(\alpha)\big) = \sigma\big(\alpha + \omega(\tau)\big) = \sigma(\alpha) + \omega(\tau) = \alpha + \omega(\sigma) + \omega(\tau),$$

לכן $\omega(\sigma\tau) = \omega(\sigma) + \omega(\tau)$. לפי כך ω הוא הומומורפיזם חבורות. גרעינו הוא $\{\sigma \mid \sigma(\alpha) = \alpha\} = \{1\}$, לכן ω שיכון. מכאן נובע ש־$\mathrm{Gal}\big(K(\alpha)/K\big)$ היא מעגלית מסדר d, באשר $p \mid d$, כלומר, $d = 1$ או $d = p$. במקרה הראשון $\alpha \in K$; כיוון שכל שורש של f מהצורה $\alpha + i$, באשר $i \in K$, גם הוא ב־K. במקרה השני $[K(\alpha):K] = p = \deg f$, לכן f אי פריק. $\blacksquare$

המשפט הקודם מאפשר בניה של הרחבות מעגליות מסדר p^n עבור n כלשהו מעל שדות בעלי אפיון p:

משפט 15.8: *יהי K שדה, $\mathrm{char}(K) = p > 0$. תהי L/K הרחבה מעגלית ממעלה $p^n > 1$. אז יש הרחבה מעגלית L'/K ממעלה p^{n+1} כך ש־ $K \subseteq L \subseteq L'$.*

הוכחה: תהי $T = T_{L/K}$ העקבה. תהי $G = \mathrm{Gal}(L/K)$ ויהי σ יוצר של G. נגדיר $L' = L(\alpha)$, באשר α שורש של $f = X^p - X - a$, עבור $a \in L$ מתאים.

שלב א: *מציאת a.* לפי למה 15.3 יש $\beta \in L$ כך ש־$T(\beta) = 1$.

מתקיים $T(\beta^p) = \sum_{\tau \in G} \tau(\beta^p) = \sum_{\tau \in G} \big(\tau(\beta)\big)^p = \big(\sum_{\tau \in G} \tau(\beta)\big)^p = \big(T(\beta)\big)^p = 1$. לכן $T(\beta^p - \beta) = T(\beta^p) - T(\beta) = 1 - 1 = 0$. לפי משפט 15.6 יש $a \in L$ כך ש־

$$\sigma(a) - a = \beta^p - \beta. \tag{1}$$

שלב ב: *$f = X^p - X - a$ אי פריק מעל L.* נניח שלא. יהי $\alpha \in \tilde{L}$ שורש של f. לפי משפט 15.7(ב), $\alpha \in L$. יהי $g(X) = X^p - X - (\beta^p - \beta) \in L[X]$. לפי (1), $\sigma(\alpha) - \alpha$, שורש שלו, כי

$$\big(\sigma(\alpha) - \alpha\big)^p - \big(\sigma(\alpha) - \alpha\big) - (\beta^p - \beta) = \big(\sigma(\alpha^p) - \alpha^p\big) - \big(\sigma(\alpha) - \alpha\big) - \big(\sigma(a) - a\big) =$$

$$\sigma(\alpha^p - \alpha - a) - (\alpha^p - \alpha - a) = \sigma(0) - 0 = 0.$$

אבל גם β שורש שלו, ולכן גם $\beta + i$, לכל $0 \le i < p$. אלה p שורשים שונים של פולינום ממעלה p, לכן הם כל שורשיו. לכן יש i כך ש־$\sigma(\alpha) - \alpha = \beta + i$. מכאן $T\big(\sigma(\alpha) - \alpha\big) = T(\beta + i)$. אבל $T\big(\sigma(\alpha) - \alpha\big) = T\big(\sigma(\alpha)\big) - T(\alpha) = T(\alpha) - T(\alpha) = 0$ ואילו $T(\beta + i) = T(\beta) + p^n i = 1 + 0 = 1$, סתירה. לכן f אי פריק.

שלב ג: *L'/K מעגלית.* (יש לשים לב שבשלב זה עדיין איננו יודעים ש־L'/K נורמלית.) נגדיר $L' = L(\alpha)$. אז $[L' : L] = p$, לכן $[L' : K] = p^{n+1}$. כיוון ש־L'/L, L/K גלואה, L'/K פרידה. לפי (1)

$$(\alpha + \beta)^p - (\alpha + \beta) = \alpha^p - \alpha + \beta^p - \beta = a + \beta^p - \beta = \sigma(a),$$

לכן $\alpha + \beta$ שורש של $\sigma(f) = X^p - X - \sigma(a) \in L[X]$. לכן ניתן להרחיב את σ לאוטומורפיזם σ' של L' כך ש־$\sigma'(\alpha) = \alpha + \beta$.

(ביתר פירוט: קודם נרחיב את σ לאיזומורפיזם שדות $\sigma \colon L' \to L''$, עבור שדה כלשהו L''. אז $L'' = \sigma\big(L(\alpha)\big) = L\big(\sigma(\alpha)\big)$. כיוון ש־$\alpha$ שורש של f, $\sigma(\alpha)$ שורש של $\sigma(f)$. לפי משפט 4.9(ב) קיים איזומורפיזם $\sigma_2 \colon L'' \to L'$ כך ש־$\sigma_2\big(\sigma(\alpha)\big) = \alpha + \beta$. נגדיר $\sigma' = \sigma_2 \circ \sigma$.) באינדוקציה

$$(\sigma')^j(\alpha) = \alpha + \beta + \sigma(\beta) + \cdots + \sigma^{j-1}(\beta).$$

בפרט $(\sigma')^{p^n}(\alpha) = \alpha + T(\beta) = \alpha + 1 \neq \alpha$, ולכן $(\sigma')^{p^n} \neq 1$. אבל $(\sigma')^{p^n}|_L = \sigma^{p^n} = 1$, לכן $(\sigma')^{p^n} \in \mathrm{Gal}(L'/L)$. מכאן $(\sigma')^{p^{n+1}} = \big((\sigma')^{p^n}\big)^p = 1$. כלומר, $\mathrm{ord}\,\sigma' | p^{n+1}$, אך $\mathrm{ord}\,\sigma' \nmid p^n$; לכן $\mathrm{ord}\,\sigma' = p^{n+1}$.

יהי $K \subseteq E \subseteq L'$ שדה השבת של $\langle \sigma' \rangle$. לפי משפט 10.9, L'/E גלואה ו־$\mathrm{Gal}(L'/E) = \langle \sigma' \rangle$ מעגלית מסדר p^{n+1}. בפרט $[L' : E] = |\langle \sigma' \rangle| = p^{n+1} = [L' : K]$, לכן $E = K$. ∎

16. הרחבות פתירות

בפרק זה תהי $\mathcal{C}$ משפחה של חבורות סופיות. ביתר דיוק, $\mathcal{C}$ קבוצה של מחלקות איזומורפיזם של חבורות סופיות, אך נכתוב $G \in \mathcal{C}$ אם מחלקת האיזומורפיזם של G נמצאת ב־$\mathcal{C}$.

הגדרה 16.1: המשפחה $\mathcal{C}$ נקראת **מלאה** אם היא סגורה תחת תת־חבורות, חבורות מנה, מכפלות ישרות, והרחבות (כלומר, אם $N \lhd G$ ו־$N, G/N \in \mathcal{C}$ אז גם $G \in \mathcal{C}$).

דוגמה 16.2: (א) משפחות מלאות: כל החבורות הסופיות; חבורות־p, עבור p ראשוני מסוים; חבורות פתירות (=בעלות גורמי הרכב חילופיים).

(ב) משפחות לא מלאות: חבורות אבליות (אינה סגורה תחת הרחבות). ∎

מעתה תהי $\mathcal{C}$ משפחה מלאה.

הגדרה 16.3: הרחבה סופית L/K נקראת **הרחבת־$\mathcal{C}$** אם יש הרחבת גלואה L'/K כך ש־$\mathrm{Gal}(L'/K) \in \mathcal{C}$ ו־$L \subseteq L'$. באופן שקול, L/K פרידה ו־$\mathrm{Gal}(\hat{L}/K) \in \mathcal{C}$ (כאן $\hat{L}$ הוא סגור גלואה של L מעל K).

מקרים פרטיים: הרחבה פתירה והרחבת־p (עבור p ראשוני). ∎

משפט 16.4: *יהיו $K \subseteq L, F \subseteq M$ שדות. אז*

(א) *M/K הרחבת־$\mathcal{C}$ אם ורק אם L/K, M/L הרחבות־$\mathcal{C}$.*

(ב) *אם L/K הרחבת־$\mathcal{C}$ אז FL/F הרחבת־$\mathcal{C}$.*

(ג) *אם L/K, F/K הרחבות־$\mathcal{C}$ אז LF/K הרחבת־$\mathcal{C}$.*

הוכחה: כל השדות שלהלן מוכלים בסגור האלגברי $\tilde{M}$ של M, בלי הגבלת הכלליות.

(ב) תהי L'/K גלואה כך ש־$L \subseteq L'$ ו־$\mathrm{Gal}(L'/K) \in \mathcal{C}$. אז FL'/F גלואה, $FL \subseteq FL'$, ו־$\mathrm{Gal}(FL'/F) \cong \mathrm{Gal}(L'/F \cap L') \leq \mathrm{Gal}(L'/K)$, לכן FL/F הרחבת־$\mathcal{C}$.

(ג) יהיו L', F' סגורי גלואה של L, F מעל K, בהתאמה. אז $LF \subseteq L'F'$. לפי משפט 10.21, $L'F'/K$ הרחבת גלואה וחבורת גלואה שלה איזומורפית לתת־חבורה של $\mathrm{Gal}(L'/K) \times \mathrm{Gal}(F'/K)$, ולכן היא ב־$\mathcal{C}$.

(א) $\Leftarrow$: תהי M'/K גלואה כך ש־$M \subseteq M'$ ו־$\mathrm{Gal}(M'/K) \in \mathcal{C}$. אז $L \subseteq M'$, לכן L/K הרחבת־$\mathcal{C}$. כמו כן $\mathrm{Gal}(M'/L) \leq \mathrm{Gal}(M'/K) \in \mathcal{C}$, לכן $\mathrm{Gal}(M'/L) \in \mathcal{C}$, ולכן M/L הרחבת־$\mathcal{C}$.

$\Rightarrow$: בלי הגבלת הכלליות L/K גלואה, אחרת נחליף את L בסגור גלואה L' של L מעל K ואת M ב־$L'M$: לפי (ב), $L'M/L'$ הרחבת־$\mathcal{C}$, ואם נראה ש־$L'M/K$ הרחבת־$\mathcal{C}$ אז לפי "$\Leftarrow$" גם M/K הרחבת־$\mathcal{C}$.

יהיו $\sigma_1, \sigma_2, \ldots, \sigma_m = 1$ כל אברי $\mathrm{Ism}_K(M, \tilde{M})$ ונסמן $\hat{M} = \sigma_1(M) \cdots \sigma_m(M)$. כיוון ש־$M/L$ הרחבת־$\mathcal{C}$ ו־$\sigma_i(L) = L$, גם גם $\sigma_i(M)/L$ הרחבת־$\mathcal{C}$, לכל i. לפי (ג), באינדוקציה על m, $\hat{M}/L$ הרחבת־$\mathcal{C}$.

כיוון ש־L/K, M/L פרידות סופיות, גם M/K פרידה סופית. לכן יש $\alpha \in M$ כך ש־$M = K(\alpha)$. אז $\{\sigma_i(\alpha)\}_{i=1}^m$ הם כל השורשים של $\mathrm{irr}(\alpha, K)$ ב־$\tilde{M}$. לכן

$$\hat{M} = \sigma_1(M)\cdots\sigma_m(M) = K\big(\sigma_1(\alpha)\big)\cdots K\big(\sigma_m(\alpha)\big) = K\big(\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\big)$$

הוא שדה הפיצול של $\mathrm{irr}(\alpha, K)$ מעל K, לכן $\hat{M}/K$ גלואה.

כיוון ש־$\mathrm{Gal}(\hat{M}/L), \mathrm{Gal}(L/K) \in \mathcal{C}$ ו־$\mathcal{C}$ סגורה תחת הרחבות, גם $\mathrm{Gal}(\hat{M}/K) \in \mathcal{C}$. אבל $M = \sigma_1(M) \subseteq \hat{M}$, לכן M/K הרחבת־$\mathcal{C}$. ∎

מעתה עד סוף הפרק יהיו כל השדות בעלי אפיון 0.

הגדרה 16.5: הרחבה L/K נקראת **שורשית** אם יש $\alpha \in L$ ו־$n \in \mathbb{N}$ כך ש־$L = K(\alpha)$ ו־$\alpha^n \in K$.

למה 16.6: *תהי L/K הרחבה שורשית. אז L/K פתירה.*

הוכחה: $K \subseteq L \subseteq K(\zeta_n, \alpha)$, לכן די להוכיח ש־$K(\zeta_n, \alpha)/K$ פתירה. לפי המשפט הקודם די להוכיח כי $K(\zeta_n)/K$ ו־$K(\zeta_n, \alpha)/K(\zeta_n)$ פתירות. ואכן, $K(\zeta_n)/K$ אבלית ו־$K(\zeta_n, \alpha)/K(\zeta_n)$ מעגלית. ∎

יהי $f \in K[X]$ אי פריק. המשוואה $f(X) = 0$ **פתירה** אם אפשר "לבטא" שורש $\alpha \in \tilde{K}$ של f מתוך איברים של K בעזרת הפעולות $+, -, \cdot, ^{-1}$ ובעזרת הוצאת שורש $\sqrt[n]{\ }$ לכל $n \in \mathbb{N}$. למשל,

$$\alpha = \frac{\sqrt[n]{(\sqrt[m]{a} + \sqrt{b})}}{\sqrt[k]{c}},$$

באשר $a, b, c \in K$. ביתר דיוק:

הגדרה 16.7: יהי $f \in K[X]$ אי פריק. המשוואה $f(X) = 0$ **פתירה** אם מתקיימים שני התנאים הבאים:

(א) קיימת סדרה (**מגדל**) של שדות $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k = L$ כך ש־K_i/K_{i-1} שורשית לכל i;

(ב) ל־f יש שורש ב־L. ∎

משפט 16.8: *יהי $\alpha \in \tilde{K}$ שורש של f. אז $f(X) = 0$ פתירה אם ורק אם $K(\alpha)/K$ הרחבה פתירה.*

הוכחה: $\Leftarrow$: לפי למה 16.6, K_i/K_{i-1} פתירה לכל i. לכן L/K פתירה ומכאן ש־$K(\alpha)/K$ פתירה.

$\Rightarrow$: לפי ההנחה יש F/K גלואה סופית כך ש־$\alpha \in F$ ו־$G = \mathrm{Gal}(F/K)$ חבורה פתירה, כלומר, $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = 1$ ו־G_{i-1}/G_i מעגלית לכל i. יהי $n = [F : K]$ ויהי $F_i = F^{G_i}$ לכל i. אז $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = F$, באשר F_i/F_{i-1} הרחבת גלואה עם חבורה G_{i-1}/G_i מעגלית מסדר $\geq n$.

יהי $E = K(\zeta_1, \ldots, \zeta_n)$. אז

$$\begin{aligned} K = K(\zeta_1) \subseteq K(\zeta_1, \zeta_2) \subseteq \cdots \subseteq & K(\zeta_1, \zeta_2, \ldots, \zeta_n) = E = \\ & = EF_0 \subseteq EF_1 \subseteq \cdots \subseteq EF_k = EF \end{aligned} \tag{1}$$

לכל $1 \leq i \leq k$ ההרחבה EF_i/EF_{i-1} היא הרחבת גלואה והחבורה שלה איזומורפית לתת־חבורה של $\mathrm{Gal}(F_i/F_{i-1}) \cong G_{i-1}/G_i$ ולכן היא מעגלית, מסדר $n \geq n_i$. כיוון ש־$\zeta_{n_i} \in E \subseteq EF_{i-1}$, מתקיים $EF_i = EF_{i-1}(\alpha_i)$, באשר $\alpha_i^{n_i} \in EF_{i-1}$. כמובן, $K(\zeta_1,\dots,\zeta_{i-1})/K(\zeta_1,\dots,\zeta_i)$ שורשית לכל $1 \leq i \leq n$. בכך מקיים מגדל (1) תנאי (א) של הגדרה 16.7. כמו כן, ל־f יש שורש $\alpha \in F \subseteq EF$. לכן $f(X) = 0$ פתירה. ∎

מסקנה 16.9: *יהי $f \in K[X]$ אי פריק. המשוואה $f(X) = 0$ פתירה אם ורק אם $\mathrm{Gal}(f,K)$ חבורה פתירה.*

הוכחה: אכן, $\mathrm{Gal}(f,K) = \mathrm{Gal}(L/K)$, באשר L שדה הפיצול של f מעל K, שהינו סגור גלואה של $K(\alpha)/K$, באשר α שורש של f. ∎

מסקנה 16.10 (גלואה): *אם $\mathrm{Gal}(f,K) \cong S_n$ או $\mathrm{Gal}(f,K) \cong A_n$, עבור $n \geq 5$, אז $f(X) = 0$ אינה פתירה. בפרט, אם $t_1,\dots,t_n$ משתנים בלתי תלויים מעל שדה K_0, אז $X^n + t_1X^{n-1} + \cdots + t_{n-1}X + t_n = 0$ אינה פתירה מעל $K = K_0(t_1,\dots,t_n)$.*

17. בנייה בעזרת סרגל ומחוגה

בעיות בניה בעזרת סרגל ומחוגה הן בעיות בגיאומטריה. ניתן קודם דוגמה ואחר כך ננסח את מושג באופן מדויק.

סימון 17.1: אם A, B הן שתי נקודות שונות במישור, אז

- $\ell(A, B)$ יסמן את הישר דרך A, B.
- $c(A, B)$ יסמן את המעגל שמרכזו ב־A ושעובר דרך B.

דוגמה 17.2: בְּנֵה ריבוע בעל צלע נתונה. בבעיה זו נתון קטע AB במישור. עלינו להשלים אותו לריבוע $ABCD$.

פתרון: (לשם המחשה. ראה את התרשימים למטה. אין צורך להתעמק בפרטים.)

(1) בעזרת סרגל נצייר ישר $\ell_1 = \ell(A, B)$.

(2) בעזרת מחוגה נצייר מעגל $c_1 = c(A, B)$; הוא חותך את את ℓ_1 בנקודה B ובנקודה נוספת , אותה נסמן E.

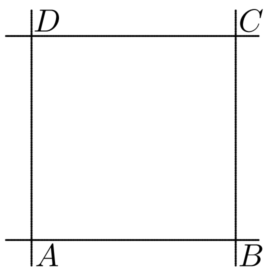
(3) נצייר מעגלים $c(E, B)$ ו־$c(B, E)$. הם נחתכים בשתי נקודות חיתוך. נבחר אחת מהן, F.

(4) נצייר ישר $\ell_2 = \ell(F, A)$ (אז $\ell_1 \perp \ell_2$; בדוק!).

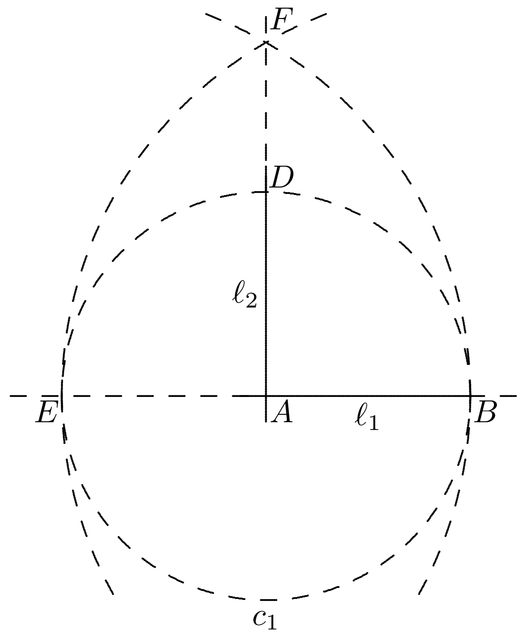
(5) נקודת החיתוך בין c_1 ו־ℓ_2 (שנמצאת בין A ל־F) תסומן D (אז $|AD| = |AB|$).

(6) באופן סימטרי (נחליף בין A ל־B) נבנה ישר ℓ_3 ניצב ל־ℓ_1 דרך B ונבנה עליו נקודה C כך ש־$|AB| = |BC|$.

(7) נצייר ישר $\ell(C, D)$. ∎



בניית ריבוע, חלק ב'



בניית ריבוע, חלק א'

וכעת מהמקרה הפרטי אל המקרה הכללי:

הגדרה 17.3: בניה בעזרת סרגל ומחוגה. זהו תהליך שמורכב ממספר סופי של צעדים. לפני כל צעד נתונים נתוני פתיחה גיאומטריים, עליהם מוסיפים בצעד עצמו נתונים נוספים. הנתונים החדשים משמשים נתוני פתיחה לצעד הבא.

ביתר דיוק, נתוני פתיחה הם קבוצה $\mathcal{P}$ של נקודות במישור. היא מגדירה קבוצה של מעגלים וישרים

$$\mathcal{C}(\mathcal{P}) = \{\ell(A,B)|\ A,B \in \mathcal{P}\} \cup \{c(A,B)|\ A,B \in \mathcal{P}\}.$$

בצעד עצמו נוסיף ל־$\mathcal{P}$ את כל נקודות החיתוך של אברי $\mathcal{C}(\mathcal{P})$. הקבוצה החדשה $\mathcal{P}'$ של נקודות תגדיר גם קבוצה חדשה $\mathcal{C}(\mathcal{P}')$ של ישרים ומעגלים.

דיון בהגדרה: (א) הסרגל הוא חָלָק; אי אפשר למדוד מרחקים בעזרתו.

(ב) יתכן ובבניה זו בונים בכל צעד נקודות, מעגלים או ישרים מיותרים ־ לא כולם נחוצים בהמשך הבניה או בתשובה הסופית. אך היעילות אינה חשובה לנו כאן. לכן אימצנו הגדרה זאת.

(ג) לפעמים נתוני פתיחה הם לא קבוצת נקודות אלא נקודות, ישרים ומעגלים או חלקים שלהם. אך אם נוסיף את נקודות החיתוך שלהם לנתוני הפתיחה, נקבל קבוצת נקודות, ממנה אפשר לשחזר את היסודות האחרים.

(ד) בפתרון בעית בניה צריך בסוף לבחור נקודות, ישרים ומעגלים (או חלקים שלהם ־ קטעים וקשתות), שהרי, כאמור, בנינו נקודות, ישרים ומעגלים מיותרים. נניח שאנו יודעים לעשות זאת.

(ה) לפי הכללים של הבניה לא ניתן לעשות את הדבר הבא: אחרי שציירנו מעגל $c(A,B)$, מרימים את המחוגה מבלי לשנות את זווית הפתיחה בין זרועותיה, תוקעים את החוד שלה בנקודה אחרת $D \in \mathcal{P}$ ומציירים סביבה מעגל. (המחוגה "מתקפלת" ברגע שמרימים את החוד מהנייר). אך לא קשה לראות (ראה תרגיל 17.4(ג) להלן) שבעזרת כללי הבניה שקבענו אפשר לבנות מקבילית $ABCD$ ולאחר מכן את המעגל המבוקש $c(D,C)$.

(ו) נניח שנתוני הפתיחה $\mathcal{P}$ סופיים. אז גם $\mathcal{C}(\mathcal{P})$ סופית, ולכן יש מספר סופי של נקודות חיתוך של אבריה. יוצא שבמקרה זה בכל צעד בבניה מוסיפים מספר סופי של נקודות. לכן הקבוצה $\hat{\mathcal{P}}$ של הנקודות החדשות שמתקבלות **בכל** הבניות האפשריות מתוך נתוני הפתיחה סופיים $\mathcal{P}$ היא בת מניה לכל היותר. אך המישור הממשי אינו בן מניה. מכאן ברור שבמקרה זה יש נקודות שלא נוכל לקבל בבניה. ∎

תרגיל 17.4 (בניות פשוטות):

(א) *נתונות נקודות A,B שונות. בְּנֵה אנך ל־$\ell(A,B)$ דרך A. (כלומר, בנה נקודה D כך ש־$\ell(A,D)\perp\ell(A,B)$.)*

(ב) *נתונות נקודות A,B,D לא על אותו ישר. בְּנֵה אנך ל־$\ell(A,B)$ דרך D. (כלומר, בנה נקודה A' על $\ell(A,B)$ כך ש־$\ell(D,A')\perp\ell(A,B)$.)*

(ג) *נתונות נקודות A,B,D לא על אותו ישר. בְּנֵה נקודה C כך ש־$ABCD$ מקבילית.*

(ד) *נניח ש־$\mathcal{C}(\mathcal{P})$ מכילה את ציר ה־xים ואת ציר ה־yים של המישור. תהי $A=(a_1,a_2)$ נקודה במישור. אז A ניתנת לבניה מתוך $\mathcal{P}$ אם ורק אם הקואורדינטות שלה (כלומר, הנקודות $a_1=(a_1,0)$ ו־$a_2=(a_2,0)$) ניתנות לבניה מ־$\mathcal{P}$.*

מתמטיקאים של יוון העתיקה התעסקו רבות בבניות בעזרת סרגל ומחוגה. נתאר עתה דוגמאות של בעיות גיאומטריות, להן חיפשו היוונים פתרון באמצעות בניה זו ־ אך לא הצליחו:

דוגמה 17.5: יהי $n \in \mathbb{N}$. בְּנֵה מצולע משוכלל בן n צלעות ובעל צלע נתונה AB. (הכללה של דוגמה 17.2.)

דוגמה 17.6: נתונה קוביה. בְּנֵה קוביה בעלת נפח גדול פי 2. זהו ניסוח קצת לא מדויק. הניסוח המדויק הוא: בהינתן קטע AB במישור, בנה נקודות C, D כך ש־$|CD|^3 = 2|AB|^3$.

דוגמה 17.7: רַבֵּעַ מעגל. שוב, זהו ניסוח מקוצר לבעיה. הניסוח המדויק הוא: בהינתן מעגל $c(E, F)$, בנה ריבוע $ABCD$ בעל אותו השטח כמו העיגול הנתון (=הפְּנִים של המעגל). במלים אחרות, אם המעגל הנתון בעל רדיוס 1, ולכן שטחו π, צריך לבנות קטע בעל אורך $\sqrt{\pi}$.

דוגמה 17.8: חַלֵּק זווית נתונה לשלוש זוויות שוות. כלומר, בהנתן שני ישרים $\ell(A, B), \ell(A, C)$ במישור, בחר אחת מבין הזיות ביניהם ובנה ישר $\ell(A, D)$ כך שאחת הזוויות בין $\ell(AD)$ ו־$\ell(A, B)$ היא שליש מהזווית ראשונה.

תורת גלואה נותנת מענה לבעיות אלה במובן הבא: היא אומרת באיזה מקרים ניתן לעשות את הבניה ובאיזה מקרים לא. (למעשה היא גם נותנת אלגוריתם לבניה, במקרה שאפשר לעשות אותה, אך לא נתעמק בזה.)

סימון 17.9: אלגבראיזציה של בעית בניה. נבחר שתי נקודות שונות $A, B \in \mathcal{P}$ ובעזרתן נזהה את המישור עם $\mathbb{C}$: נבחר את מערכת הצירים כך ש־$A = 0, B = 1$. אז כל (α, β) במישור מזוהה עם $z = \alpha + i\beta \in \mathbb{C}$. נסמן ב־$\hat{\mathcal{P}}$ את קבוצת המספרים $z \in \mathbb{C}$ שניתנים לבניה מתוך $\mathcal{P}$. ∎

תרגיל 17.10: *יהיו $x, y \in \hat{\mathcal{P}}$. אז*

(א) $x + y \in \hat{\mathcal{P}}$;

(ב) $x - y \in \hat{\mathcal{P}}$;

(ג) $xy \in \hat{\mathcal{P}}$;

(ד) $\frac{x}{y} \in \hat{\mathcal{P}}$, אם $y \neq 0$.

(ה) *הסק ש־$\hat{\mathcal{P}}$ הוא תת־שדה של $\mathbb{C}$ אשר מכיל את $\mathbb{Q}(\mathcal{P})$, השדה שנוצר מעל $\mathbb{Q}$ על ידי $\mathcal{P}$.*

תרגיל 17.11: *(א) נסמן $K = \mathbb{Q}(\mathcal{P})$. יהי $z \in \mathbb{C}$ כך ש־$[K(z) : K] \leq 2$. הוכח: $z \in \hat{\mathcal{P}}$.*

(ב) *נניח $\overline{\mathcal{P}} = \mathcal{P}$ (כלומר, $\mathcal{P}$ סגור תחת ההצמדה המרוכבת). יהי K שדה כך ש־$\mathbb{Q}(\mathcal{P})(i) \subseteq K \subseteq \mathbb{C}$. תהי $z \in \mathbb{C}$ נקודת חיתוך של שני אברי $\mathcal{C}(\mathcal{P})$ (ראה הגדרה 17.3). הוכח: $[K(z) : K] \leq 2$.*

משפט 17.12: *נניח $\overline{\mathcal{P}} = \mathcal{P}$ ונסמן $K = \mathbb{Q}(\mathcal{P})$. תהי $z \in \mathbb{C}$. אז:*

$z \in \mathbb{C}$ ניתנת לבניה מתוך $\mathcal{P}$ אם ורק אם $K(z)/K$ הרחבת־2.

הוכחה: $\Leftarrow$: נראה תחילה שיש מגדל של שדות

$$\mathbb{Q}(\mathcal{P}) = K_0 \subseteq K_1 = K_0(i) \subseteq K_2 \subseteq \cdots \subseteq K_k \quad \subseteq \quad \mathbb{C} \tag{1}$$

כך ש־$[K_j : K_{j-1}] \leq 2$ לכל j ו־$z \in K_k$. נעשה זאת באינדוקציה על מספר השלבים בבניה של z.

אם $z \in \mathcal{P}$, ניקח $k = 1$ ו־$K_1 = K_0(i)$. נניח $z \notin \mathcal{P}$.

בכל שלב הבנייה משתמשים רק במספר סופי של נקודות. לכן יש קבוצה סופית $\mathcal{R} = \{z_2, \ldots, z_n\}$ של חיתוכים של אברי $\mathcal{C}(\mathcal{P})$ כך שמשתמשים רק ב־$\mathcal{P}' := \mathcal{P} \cup \mathcal{R}$ בשלבים הבאים, אחרי השלב הראשון.

בלי הגבלת הכלליות $\overline{\mathcal{R}} = \mathcal{R}$ (אחרת נוסיף לאיברי $\mathcal{R}$ את צמודיהם), ולכן $\overline{\mathcal{P}'} = \mathcal{P}'$. לפי תרגיל 17.11(ב), $[K_1(z_j) : K_1] \le 2$ לכל $z_j \in \mathcal{R}$. נסמן $K_j = K_1(z_2, \ldots, z_j)$ לכל $2 \le j \le n$. אז $K_j = K_{j-1}(z_j)$, לכן גם $[K_j : K_{j-1}] \le 2$. כמו כן $K_n = K_1(\mathcal{R}) = \mathbb{Q}(\mathcal{P})(i)(\mathcal{R}) = \mathbb{Q}(\mathcal{P}')(i)$.

כעת אפשר לבנות את z מתוך $\mathcal{P}'$ עלי ידי שלב אחד פחות. לכן לפי הנחת האינדוקציה אפשר להמשיך את הסדרה $K_n \subseteq \cdots \subseteq K_1 \subseteq K_0$ לסדרה (1), בה $k \ge n$, כך ש־$[K_j : K_{j-1}] \le 2$ לכל j ו־$z \in K_k$.

אז K_j/K_{j-1} הרחבת־2 לכל j. לכן לפי משפט 16.4(א) (באינדוקציה על k), K_k/K הרחבת־2. כיוון ש־$K \subseteq K(z) \subseteq K_k$, גם $K(z)/K$ הרחבת־2.

$\Rightarrow$: יש הרחבת גלואה סופית L/K כך ש־$z \in L$ ו־$G = \mathrm{Gal}(L/K)$ חבורת־2. לכן יש סדרה $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = 1$ כך ש־$G_1 = \mathrm{Gal}(L/K(i))$ ו־$(G_{j-1} : G_j) \le 2$ לכל j. יהי $K_j = L^{G_j}$ לכל j. אז מתקיים (1), באשר K_j/K_{j-1} הרחבת גלואה עם חבורה G_{j-1}/G_j מסדר ≤ 2. לפי תרגיל 17.11(א), באינדוקציה על j, כל איבר ב־K_j ניתן לבניה מתוך $\mathcal{P}$. בפרט $z \in L = K_k$ ניתנת לבניה מתוך $\mathcal{P}$. ∎

מסקנה 17.13: *נניח $\overline{\mathcal{P}} = \mathcal{P}$ ויהי $K = \mathbb{Q}(\mathcal{P})$. אז תנאי הכרחי לכך שנקודה $z \in \mathbb{C}$ ניתנת לבניה מתוך נתוני פתיחה $\mathcal{P}$ הוא ש־$[K(z) : K]$ הוא חזקה של 2.*

הוכחה: אם z ניתנת לבניה מתוך $\mathcal{P}$ אז יש L/K גלואה כך ש־$[L : K]$ חזקה של 2 ו־$K \subseteq K(z) \subseteq L$. לפי הכפליות של מעלות ההרחבות (משפט 4.13), $[K(z) : K] \mid [L : K]$, לכן $[K(z) : K]$ חזקה של 2. ∎

הערה 17.14: היות ולכל $z \in \mathcal{P}$ מתקיים $\bar{z} \in \hat{\mathcal{P}}$, את התנאי $\overline{\mathcal{P}} = \mathcal{P}$ אפשר להשיג על ידי החלפת $\mathcal{P}$ ב־$\mathcal{P} \cup \overline{\mathcal{P}}$.

כבר מתוך מסקנה 17.13 אפשר להסיק שבניות מסוימות לא תיתכנה:

מסקנה 17.15: *לא ניתן בעזרת סרגל ומחוגה*

(א) *לבנות קוביה בעלת נפח כפול (ראה דוגמה 17.6);*

(ב) *לרבע מעגל (ראה דוגמה 17.7);*

(ג) *לחלק זווית $\pi/3$ לשלוש זוויות שוות (ראה דוגמה 17.8).*

הוכחה: נניח בשלילה שהבניה אפשרית.

(א) מתוך קטע AB אפשר לבנות קטע CD בעל אורך גדול פי $\sqrt[3]{2}$. מכאן קל לראות שאת הנקודה $\sqrt[3]{2}$ אפשר לבנות מתוך $\mathcal{P} = \{0, 1\}$. אז $\mathbb{Q}(\mathcal{P}) = \mathbb{Q}$ ולכן $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ חזקה של 2. אבל $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, סתירה.

(ב) בדומה ל־(א), $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ חזקה של 2. אבל $\mathbb{Q}(\pi)$ הוא הרחבה טרנסצנדנטית של $\mathbb{Q}$, סתירה. (הטרנסצנדנטיות של π הוא משפט לינדמן משנת 1882, כ־50 שנה אחרי גלואה.)

(ג) בלי הגבלת הכלליות הזווית היא AOB באשר O הראשית, $A = 1$ ו־$B = e^{i\frac{2\pi}{6}} = \zeta_6$. אז נוכל לבנות את הנקודה $\zeta_{18} = e^{i\frac{2\pi}{18}}$ מתוך $\mathcal{P} = \{O, A, B, \bar{B}\}$. נשים לב ש־$\bar{\zeta}_6 = \zeta_6^{-1}$, לכן $\mathbb{Q}(\mathcal{P}) = \mathbb{Q}(\zeta_6)$. לכן

$[\mathbb{Q}(\zeta_6,\zeta_{18}):\mathbb{Q}(\zeta_6)]$ חזקה של 2. אבל $\mathbb{Q}(\zeta_6,\zeta_{18})=\mathbb{Q}(\zeta_{18})$ ו־

$$[\mathbb{Q}(\zeta_{18}):\mathbb{Q}]=\varphi(18)=2\cdot 3\ ,\quad [\mathbb{Q}(\zeta_6):\mathbb{Q}]=\varphi(6)=\varphi(3)=2,$$

לכן $[\mathbb{Q}(\zeta_{18}):\mathbb{Q}(\zeta_6)]=3$, סתירה. ∎

בהמשך יהי $n\ge 3$.

מסקנה 17.16: *ניתן לבנות בעזרת סרגל ומחוגה מצולע משוכלל בן n צלעות (דוגמה 17.5) אם ורק אם $\varphi(n)$ חזקה של 2.*

הוכחה: אם AB צלע המצולע ו־O מרכזו, אז זווית AOB היא $\frac{2\pi}{n}$. קל לראות שאפשר לבנות את מצולע אם ורק אם אפשר לבנות את הנקודה $\zeta_n=e^{\frac{2\pi}{n}}$. לפי משפט 17.12 זה שקול לכך ש־$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ הרחבת־2. אבל לפי משפט 13.6 זוהי הרחבת גלואה ממעלה $\varphi(n)$, לכן היא הרחבת־2 אם ורק אם $\varphi(n)$ חזקה של 2. ∎

הערה 17.17: מתי $\varphi(n)$ הוא חזקה של 2?. יהי $n=p_1^{m_1}\cdots p_r^{m_r}$ הפירוק של n למכפלה של חזקות של ראשוניים שונים. אז $\varphi(n)=\varphi(p_1^{m_1})\cdots\varphi(p_r^{m_r})$. לכן $\varphi(n)$ חזקה של 2 אם ורק אם $\varphi(p_j^{m_j})$ חזקה של 2 לכל j.

לכן די לבחון את השאלה עבור $n=p^m$, באשר p ראשוני ו־$m\in\mathbb{N}$.

- אם $p=2$ אז $\varphi(2^m)=2^{m-1}$ חזקה של 2.
- אם p אי זוגי ו־$m>1$ אז $\varphi(p^m)=(p-1)p^{m-1}$ אינו חזקה של 2.
- אם p אי זוגי ו־$m=1$ אז $\varphi(p^m)=\varphi(p)=p-1$ הוא חזקה של 2 אם ורק אם $p=2^K+1$ עבור איזה K. אך אם K אינו חזקה של 2, אז $K=\ell q$, באשר $\ell,q>1$ ו־q אי זוגי; ואז $2^K+1=(2^\ell+1)\left(\sum_{j=0}^{q-1}(-1)^j(2^\ell)^j\right)$ אינו ראשוני. לכן אם p ראשוני אז $p=2^{2^k}+1$ עבור איזה k.

לכן ניתן לבנות מצולע משוכלל בן n צלעות אם ורק אם n הוא מכפלה של חזקה של 2 ושל מספרי פֶּרמָה (דהיינו, מהצורה $F_k=2^{2^k}+1$, באשר $k\ge 0$) ראשוניים שונים.

עד היום ידועים רק 5 מספרי פרמה ראשוניים:

$$F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537.$$

ידוע גם ש־F_k אינו ראשוני עבור $5\le k\le 32$. למשל, $F_5=4294967297=641\times 6700417$ (אויילר).

אי לכך בנית מצולע משוכלל בן n צלעות אפשרית אם $n=2^m\cdot 3^{m_0}\cdot 5^{m_1}\cdot 17^{m_2}\cdot 257^{m_3}\cdot 65537^{m_4}$, באשר $m\ge 0$ ו־$m_0,\dots,m_4\in\{0,1\}$, ואיננו יודעים האם היא אפשרית עבור n־ים נוספים.

אם $3\le n\le 100$ אז בנית מצולע משוכלל בן n צלעות אפשרית אם ורק אם

$$n\in\{3,4,5,6,8,10,12,15,16,17,20,24,30,32,34,40,48,51,60,64,68,80,85,96\}$$

∎

18. הרחבות אי פרידות טהורות

יהי K שדה. יהי $\tilde{K}$ סגור אלגברי של K.

הגדרה 18.1: תהי L/K הרחבה. אז $F = \{\alpha \in L |$ α פריד מעל $K\}$ נקרא **הסגור הפריד** של K בתוך L. ∎

משפט 18.2: *תהי L/K הרחבה. אז הסגור הפריד F של K בתוך L הוא שדה. זוהי ההרחבה הפרידה הגדולה ביותר של K שמוכלת ב־L. אם L/K נורמלית אז גם F/K נורמלית.*

הוכחה: אם $\alpha, \beta \in F$, אז $K(\alpha), K(\beta)$ פרידות, לכן $K(\alpha,\beta) \subseteq F$. לכן $\alpha+\beta, \alpha-\beta, \alpha\beta \in F$, וגם $\alpha/\beta \in F$, אם $\beta \neq 0$. לכן F שדה.

יהי σ אוטומורפיזם־K של $\tilde{K}$. כיוון ש־L/K נורמלית, $\sigma(L) = L$; אם $\alpha \in L$ אז: α פריד מעל K אם ורק אם $\sigma(\alpha)$ פריד מעל K. לכן $\sigma(F) = F$. לכן F/K נורמלית. ∎

משפט 18.3: *נניח $p = \mathrm{char}(K) > 0$. תהי L/K הרחבה אלגברית. התנאי הבאים שקולים זה לזה:*

(א) $[L:K]_s = 1$.

(ב) *לכל* $\alpha \in L$, $\mathrm{irr}(\alpha, K) = X^{p^n} - a$, *באשר* $n \geq 0$, $a \in K$.

(ג) *לכל* $\alpha \in L$ *יש* $n \geq 0$ *שלם כך ש־* $\alpha^{p^n} \in K$.

(ד) $L = K(\alpha_i |\ i \in I)$, *באשר לכל* $i \in I$ *יש* $n_i \geq 0$ *כך ש־* $\alpha_i^{p^{n_i}} \in K$.

(ה) *כל* $\alpha \in L$ *פריד מעל* K *הוא ב־*K.

הוכחה: בלי הגבלת הכלליות $L \subseteq \tilde{K}$.

(א)⇐(ב): יהי $f = \mathrm{irr}(\alpha, K)$. אם α' שורש של f, אז לפי משפט 4.11(ז) יש הומומורפיזם־K $\sigma\colon K(\alpha) \to K(\alpha') \subseteq \tilde{K}$ כך ש־$\sigma(\alpha) = \alpha'$. לפי משפט 5.6(ג) ניתן להרחיב אותו ל־$\sigma \in \mathrm{Ism}_K(L, \tilde{K})$, לכן $\sigma = 1_L$ לפי (א). לכן $\alpha' = \alpha$, כלומר, $f = (X-\alpha)^m$ עבור איזה $m \in \mathbb{N}$. נכתוב $m = p^n r$, באשר r זר ל־p ויהי $a = \alpha^{p^n} \in L$. אז

$$f = (X-\alpha)^{p^n r} = \left((X-\alpha)^{p^n}\right)^r = (X^{p^n} - a)^r = X^{p^n r} - raX^{p^n(r-1)} + \cdots \in K[X]$$

לכן $ra \in K$. אבל $r \neq 0$ ב־K, לכן $r \in K^\times$, ומכאן $a \in K$. כעת, α שורש של $X^{p^n} - a = (X-\alpha)^{p^n}$, אשר מחלק את f, לכן $f = X^{p^n} - a$.

(ב)⇐(ג)⇐(ד): ברור.

(ד)⇐(א): יהי $\sigma \in \mathrm{Ism}_K(L, \tilde{K})$. צריך להוכיח ש־$\sigma = 1_L$. כיוון שאברי L הם פונקציות רציונליות ב־α_i, די להראות ש־$\sigma(\alpha_i) = \alpha_i$ לכל $i \in I$. אך α_i שורש של $(X-\alpha_i)^{p^{n_i}} = X^{p^{n_i}} - \alpha_i^{p^{n_i}} \in K[X]$, שיש לו רק שורש אחד ב־$\tilde{K}$, לכן $\sigma(\alpha_i) = \alpha_i$.

(ב)⇐(ה): יהי $f = \mathrm{irr}(\alpha, K) = X^{p^n} - a$. אז $f' \neq 0$ אם ורק אם $n = 0$, ואז $\alpha = a \in K$.

(ה) ⇐(ג): אפשר לכתוב $\mathrm{irr}(\alpha, K) = g(X^{p^n})$, באשר $n \geq 0$ ו־$g \in K[X]$ פולינום עבורו אין $h \in K[X]$ שמקיים $g(X) = h(X^p)$. אז g אי פריק (פירוק שלו לשני גורמים נותן פירוק של $\mathrm{irr}(\alpha, K)$ לשני גורמים), אין לו שורשים מרובים ב־$\tilde{K}$ (מסקנה 6.9(ב)), α^{p^n} שורשו, לכן $\alpha^{p^n} \in K$. ∎

הגדרה 18.4: הרחבה אלגברית L/K היא **אי פרידה טהורה** אם היא מקיימת את התנאים השקולים של המשפט או אם $\mathrm{char}\, K = 0$ ו־$L = K$. אז כל $\alpha \in L$ **אי פריד טהור** מעל K. ∎

דוגמה 18.5: הרחבה אלגברית $\mathbb{F}_p(t, u)/\mathbb{F}_p(t^p, u^p)$ היא אי פרידה טהורה, כי $\mathbb{F}_p(t, u) = \mathbb{F}_p(t^p, u^p)(t, u)$ ו־t, u אי פרידים טהורים מעל $\mathbb{F}_p(t^p, u^p)$. ∎

משפט 18.6: *תהי L/K הרחבה אלגברית ויהי F הסגור הפריד של K בתוך L. אז L/F אי פרידה טהורה.*

הוכחה: לפי משפט 18.3(ה): יהי $\alpha \in L$ פריד מעל F. כיוון ש־F/K פרידה, α פריד מעל K ולכן $\alpha \in F$. ∎

למה 18.7: *תהי L/K הרחבה אלגברית, גם פרידה וגם אי פרידה טהורה. אז $L = K$.*

הוכחה: יהי $\alpha \in L$. אז α פריד מעל K. לפי משפט 18.3(ה), $\alpha \in K$. ∎

משפט 18.8: *יהיו $K \subseteq L, F \subseteq M$ שדות.*

(א) *M/K אי פרידה טהורה אם ורק אם L/K, M/L אי פרידות טהורות.*

(ב) *אם L/K אי פרידה טהורה, אז LF/F אי פרידה טהורה.*

(ג) *אם L/K, F/K פרידות אז LF/K אי פרידה טהורה*

הוכחה: (ג) נובע באופן פורמלי מתוך (א),(ב).

(א) לפי משפט 7.9, $[M : K]_s = [M : L]_s \cdot [L : K]_s$.

(ב) לפי משפט 18.3(ד): אם $L = K(\alpha_i |\ i \in I)$, באשר $\alpha_i^{p^{n_i}} \in K$ לכל i, אז $LF = F(\alpha_i |\ i \in I)$, באשר $\alpha_i^{p^{n_i}} \in F$ לכל i. ∎

למה 18.9: *נניח $p = \mathrm{char}(K) > 0$. תהי L/K הרחבה סופית.*

(א) *אם L/K אי פרידה טהורה אז $[L : K]$ הוא חזקה של p.*

(ב) *$[L : K]/[L : K]_s \in \mathbb{N}$ הוא חזקה של p.*

הוכחה: (א) לפי מסקנה 4.15(ב) יש מגדל $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = L$ כך ש־L_i/L_{i-1} פשוטה לכל i. לכן לפי משפט 18.8(א) אפשר להניח כי L/K פשוטה, $L = K(\alpha)$. אז $\mathrm{irr}(\alpha, K) = X^{p^n} - a$ עבור איזה $n \geq 0$. מכאן $[L : K] = p^n$.

(ב) יהי F הסגור הפריד של K בתוך L. לפי משפט 18.2, F/K פרידה; לפי משפט 18.6, L/F אי פרידה טהורה. לכן $[F : K] = [F : K]_s$, $[L : F]_s = 1$. לפי כפליות האינדקסים $[L : K]/[L : K]_s = [L : F]$, שהינו שלם וחזקה של p לפי (א). ∎

הגדרה 18.10: תהי L/K הרחבה סופית. אז $[L:K]_i = [L:K]/[L:K]_s$ נקרא **מעלת האי־פרידות** של L/K.

מסקנה 18.11: *הרחבה סופית L/K היא פרידה אם ורק אם $[L:K]_i = 1$.*

מסקנה 18.12: *אם $K \subseteq L \subseteq M$ הרחבות סופיות אז $[M:K]_i = [M:L]_i[L:K]_i$.*

משפט 18.6 נותן פירוק של הרחבה אלגברית להרחבה פרידה ואי פרידה טהורה מעליה. בד"כ אי אפשר להפוך את הסדר. אך זה אפשרי אם ההרחבה נורמלית:

משפט 18.13: *תהי L/K הרחבה נורמלית ויהי F הסגור הפריד של K בתוך L. תהי H חבורת האוטומורפיזמים של L מעל K ויהי $E = L^H$ שדה השבת שלה. אז E/K אי פרידה טהורה ו־L/E גלואה. יתר על כן, $L = FE$ ו־$E \cap F = K$.*

הוכחה: בלי הגבלת הכלליות $L \subseteq \tilde{K}$.

יהי $\sigma\colon E \to \tilde{K}$ הומומורפיזם־K. לפי מסקנה 5.7 ניתן להרחיב אותו ל־$\sigma'\colon L \to \tilde{K}$. כיוון ש־$L/K$ נורמלית, $\sigma' \in H$. לכן σ' הוא הזהות על $E = L^H$, כלומר, $\sigma = 1$. לפי משפט 18.3(א), E/K אי פרידה טהורה.

יהי $\alpha \in L$. אז α אלגברי מעל K. אם $\sigma \in H$ אז $\sigma(\alpha)$ גם שורש של $\mathrm{irr}(\alpha, K)$. לכן $\{\sigma(\alpha)|\ \sigma \in H\}$ סופית. לפי הלמה של ארטין (משפט 10.9) L/E היא הרחבת גלואה.

ההרחבה $E \cap F/K$ היא גם פרידה וגם אי פרידה טהורה. לכן $E \cap F = K$.

ההרחבה L/EF היא גם פרידה וגם אי פרידה טהורה. לכן $L = EF$. ∎

תרגיל 18.14: *תהי K'/K הרחבה אלגברית ונניח שלכל $f \in K[X]$ ממעלה ≥ 1 יש שורש ב־K'. הוכח ש־K' הוא סגור אלגברי של K.*

הוכחה: די להוכיח ש־K' סגור אלגברית. (אילו ידענו שלכל $f \in K'[X]$ יש שורש ב־K', זה היה נובע מההגדרה; אך אנו יודעים זאת רק עבור פולינומים מעל K.) יהי $\tilde{K}$ סגור אלגברי של K'; הוא אלגברי מעל K, לכן גם סגור אלגברי של K. יהי $\gamma \in \tilde{K}$. יהי L הסגור הנורמלי של $K(\gamma)$ מעל K. כדי להראות ש־$\gamma \in K'$, די להראות כי $L \subseteq K'$. לפי משפט 8.7, L/K סופית.

יהי F הסגור הפריד של K ב־L. לפי המשפט הקודם יש $K \subseteq E \subseteq L$ כך ש־E/K אי פרידה טהורה ו־$L = EF$. כדי להוכיח כי $L \subseteq K'$, די להוכיח $E, F \subseteq K'$.

יהי $\alpha \in E$. אז ל־$\mathrm{irr}(\alpha, K)$ שורש יחיד ב־$\tilde{K}$, הוא α, לכן לפי ההנחה $\alpha \in K'$. מכאן $E \subseteq K'$.

כיוון ש־F/K פרידה וסופית, יש $\beta \in F$ כך ש־$F = K(\beta)$. יהי $f = \mathrm{irr}(\beta, K)$. לפי ההנחה, ל־$f$ יש שורש $\beta' \in K'$. יש אוטומורפיזם־K σ של $\tilde{K}$ כך ש־$\sigma(\beta) = \beta'$. כיוון ש־F/K נורמלית (משפט 18.2), $\sigma(F) = F$. לכן

$$F = \sigma(F) = \sigma\big(K(\beta)\big) = K(\beta') \subseteq K'. \quad ∎$$

19. הרחבות טרנסצנדנטיות

תהי L/K הרחבת שדות.

הגדרה 19.1: קבוצה $T \subseteq L$ נקראת **בלתי תלויה אלגברית מעל** K אם לכל $t_1, \ldots, t_n \in T$ שונים זה מזה ולכל $0 \neq f \in K[X_1, \ldots, X_n]$ מתקיים $f(t_1, \ldots, t_n) \neq 0$. ∎

הערה 19.2: תהי X קבוצה של משתנים ויהי $K[X]$ חוג הפולינומים במשתנים אלה.

(א) העתקה $\lambda\colon X \to L$ ניתן להרחיב באופן יחיד להומומורפיזם־K של חוגים (הצבה) $\lambda'\colon K[X] \to L$; הוא נתון על ידי $f\big(X_1, \ldots, X_n\big) \mapsto f\big(\lambda(X_1), \ldots, \lambda(X_n)\big)$, באשר $X_1, \ldots, X_n \in X$ שונים זה מזה ו־$f \in K[X_1, \ldots, X_n]$.

(ב) נניח ש־λ חד חד ערכית ותהי $T = \lambda(X)$. אז λ' חד חד ערכית אם ורק אם T בלתי תלויה אלגברית מעל K. במקרה זה $K[X] \cong K[T]$ ולכן אפשר לחשוב על T כקבוצה של משתנים. ∎

תרגיל 19.3: *תהי T בלתי תלויה אלגברית מעל K.*

(א) *אם $S \subseteq T$ אז S בלתי תלויה אלגברית מעל K.*

(ב) *אם $t \in T$ אז t טרנסצנדנטי מעל K.*

למה 19.4: *תהי T בלתי תלויה אלגברית מעל K ותהי $S \subseteq L$. אז S בלתי תלויה אלגברית מעל $K(T)$ אם ורק אם $T \cap S = \emptyset$ ו־$T \cup S$ בלתי תלויה אלגברית מעל K.*

הוכחה: "$\Leftarrow$": לפי (ב) אברי S אינם ב־$K(T)$ ולכן $T \cap S = \emptyset$. יהיו $t_1, \ldots, t_n \in T$ ו־$s_1, \ldots, s_m \in S$ שונים; נסמן $s = (s_1, \ldots, s_m)$, $t = (t_1, \ldots, t_n)$, $Y = (Y_1, \ldots, Y_m)$, $X = (X_1, \ldots, X_n)$, ויהי $f \in K[X, Y]$ כך ש־$f(t, s) = 0$. אז $f = \sum_i \sum_j a_{ij} X^i Y^j \in K[X, Y]$ (באשר $i = (i_1, \ldots, i_n)$ ו־$j = (j_1, \ldots, j_m)$ מולטי־אינדקסים) ו־$a_{ij} \in K$ כמעט כולם 0. כלומר, $f(t, s) = \sum_i \sum_j a_{ij} t^i s^j = 0$. מכאן $\sum_j (\sum_i a_{ij} t^i) s^j = 0$. כיוון ש־$S$ בלתי תלויה אלגברית מעל $K(T)$, $\sum_i a_{ij} t^i = 0$ לכל j. כיוון ש־T בלתי תלויה אלגברית מעל K, $a_{ij} = 0$ לכל i. לכן $f = 0$.

"$\Rightarrow$": יהיו $s_1, \ldots, s_m \in S$ שונים; נסמן $s = (s_1, \ldots, s_m)$, $Y = (Y_1, \ldots, Y_m)$. יהי $g \in K(T)[Y]$ כך ש־$g(s) = 0$. צריך להוכיח $g = 0$. בלי הגבלת הכלליות $g \in K[T][Y]$. כלומר, יש $f = \sum_i \sum_j a_{ij} X^i Y^j \in K[X, Y]$, באשר $X = (X_1, \ldots, X_n)$, ויש $t = (t_1, \ldots, t_n)$ איברים שונים ב־T, כך ש־$g = f(t, Y)$. אז $f(t, s) = g(s) = 0$, לכן $f = 0$. מכאן $g = 0$. ∎

תרגיל 19.5: *תהי T בלתי תלויה אלגברית מעל K. יהי $\alpha \in K(T)$ אלגברי מעל K. אז $\alpha \in K$.*

הוכחה: $\alpha = \frac{g(t)}{h(t)}$, באשר $n \in \mathbb{N}$, $g, h \in K[X_1, \ldots, X_n]$, ו־$t$ n־יה של אברים שונים ב־T כך ש־$h(t) \neq 0$. בלי הגבלת הכלליות גם $g(t) \neq 0$. כיוון ש־$K[X_1, \ldots, X_n]$ תחום פריקות (מסקנה 2.22), אפשר להניח ש־g, h זרים, אחרת נחלק את שניהם בגורמים אי פריקים משותפים.

לפי ההנחה יש $a_0, a_1, \dots, a_d \in K$, לא כולם אפס, כך ש־$\sum_{i=0}^d a_i\alpha^i = 0$. בלי הגבלת הכלליות $a_0, a_d \neq 0$. נכפיל ב־$h(t)^d$: $\sum_{i=0}^d a_i g(t)^i h(t)^{d-i} = 0$. כיוון ש־$T$ בלתי תלויה אלגברית מעל K, $\sum_{i=0}^d a_i g^i h^{d-i} = 0$. מכאן קל לראות שכל גורם אי פריק של אחד מבין g, h הוא גם גורם אי פריק של השני. אך g, h זרים, לכן אין להם גורמים אי פריקים. מכאן ש־$g, h \in K$ ולכן $\alpha \in K$. ∎

למה 19.6: *תהי $T \subseteq L$. שני התנאים הבאים שקולים:*

(א) *T בלתי תלויה אלגברית מרבית מעל K.*

(ב) *T בלתי תלויה אלגברית מעל K ו־$L/K(T)$ אלגברית*

הוכחה: תהי T בלתי תלויה אלגברית מעל K. אז

$L/K(T)$ אינה אלגברית

$\Leftrightarrow$ יש $\alpha \in L$ שאינו אלגברי מעל $K(T)$

$\Leftrightarrow$ יש $\alpha \in L$ כך ש־$\{\alpha\}$ בלתי תלויה אלגברית מעל $K(T)$

$\Leftrightarrow$ יש $\alpha \in L$ כך ש־$\alpha \notin T$ ו־$T \cup \{\alpha\}$ בלתי תלויה אלגברית מעל K (למה 19.4)

$\Leftrightarrow$ T אינה בלתי תלויה אלגברית מרבית מעל K. ∎

הגדרה 19.7: קבוצה $T \subseteq L$ נקראת **בסיס טרנסצנדנטיות של L מעל K** אם היא מקיימת את התנאים השקולים של למה 19.6. ∎

משפט 19.8: *כל שני בסיסי טרנסצנדנטיות של L/K הם שווי עוצמה.*

הוכחה: יהיו S, T שני בסיסי טרנסצנדנטיות של L/K. די להראות כי $|S| \leq |T|$. נבדיל בין שני מקרים:

מקרה א: *S סופי.* במקרה זה די להוכיח:

טענה: *יהיו $S, T \subseteq L$ כך ש־S בלתי תלויה אלגברית מעל K ו־L אלגברית מעל $K(T)$. יהיו $s_1, \dots, s_n \in S$ שונים זה מזה, $n \geq 0$. אז יש $t_1, \dots, t_n \in T$ שונים זה מזה כך ש־L אלגברית מעל $K(T_n)$,* באשר $T_n := \{s_1, \dots, s_n\} \cup (T \smallsetminus \{t_1, \dots, t_n\})$.

(אכן, עבור $n = |S|$ נובע מהטענה שיש ב־T לפחות n איברים שונים, לכן $|S| \leq |T|$.)

הוכחת הטענה: באינדוקציה על n. עבור $n = 0$ הטענה ברורה, כי $T_n = T$.

נניח נכונות עבור n ויהי $s_{n+1} \in S$ שונה מ־$s_1, \dots, s_n$. נסמן $s = (s_1, \dots, s_n)$. היות ו־s_{n+1} ב־L, הוא אלגברי מעל $K(T_n)$. לכן יש סדרה סופית $t = (t_{n+1}, \dots, t_{n+m})$ של אברי T_n, שונים מ־$s_1, \dots, s_n$, ויש $g_i, h_i \in K[X_1, \dots, X_m, Y_1, \dots, Y_n]$, עבור $0 \leq i \leq d$, כך ש־$h_i(t, s) \neq 0$ לכל i, $g_d(t, s) \neq 0$, ו־$\sum_{i=0}^d g_i(t, s)/h_i(t, s)s_{n+1}^i = 0$. בלי הגבלת הכלליות $h_i = 1$ לכל i, אחרת נכפיל משוואה זו ב־$\prod_i h_i(t, s)$. יהי $f = \sum_{i=0}^d g_i(X_1, \dots, X_m, Y_1, \dots, Y_n)Z^i$. אז $0 \neq f \in K[X_1, \dots, X_m, Y_1, \dots, Y_n, Z]$ ו־$f(t, s, s_{n+1}) = 0$. אחד המשתנים $X_1, \dots, X_m$ מופיע ב־f (אחרת $s_1, \dots, s_n, s_{n+1}$ תלויים אלגברית מעל

K, סתירה); בלי הגבלת הכלליות זהו X_1. לכן t_{n+1} אלגברי מעל $K(s_{n+1}, t_{n+2}, \ldots t_{n+m}, s)$, ובפרט מעל $K(T_{n+1})$, באשר $T_{n+1} := \{s_1, \ldots, s_n, s_{n+1}\} \cup (T \setminus \{t_1, \ldots, t_n, t_{n+1}\})$. בפרט $K(T_{n+1} \cup \{t_{n+1}\})$ אלגברית מעל $K(T_{n+1})$. אבל $T_n \subseteq T_{n+1} \cup \{t_{n+1}\}$, לכן L אלגברית מעל $K(T_{n+1} \cup \{t_{n+1}\})$. לכן L אלגברית מעל $K(T_{n+1})$. בכך הוכחה הטענה.

מקרה ב: S *אינסופי.* כל $t \in T$ אלגברי מעל $K(S)$, לכן אלגברי מעל $K(S_t)$ עבור איזה $S_t \subseteq S$ סופית. נראה תחילה ש־$S = \bigcup_{t \in T} S_t$.

נסמן את אגף שמאל ב־S'. אז $S' \subseteq S$. יהי $\alpha \in S \setminus S'$. אז α אלגברי מעל $K(T)$. כל $t \in T$ אלגברי מעל $K(S_t) \subseteq K(S')$, לכן $K(S')(T)$ אלגברית מעל $K(S')$. כיוון ש־α אלגברי מעל $K(S')(T)$, הוא אלגברי מעל $K(S')$. אבל לפי למה 19.4, $\{\alpha\}$ בלתי תלויה אלגברית מעל $K(S')$, סתירה. לכן $S' = S$.

מתוך $S = \bigcup_{t \in T} S_t$ נובע ש־T אינסופית, ולכן $|S| \leq |T| \cdot \aleph_0 = |T|$. ∎

משפט 19.9: *כל קבוצה בלתי תלויה אלגברית ב־L ניתנת להשלמה לבסיס טרנסצנדנטיות של L/K. בפרט, ל־L/K יש בסיס טרנסצנדנטיות.*

הוכחה: לפי הלמה של צורן אפשר להשלים את הקבוצה לקבוצה בלתי תלויה אלגברית מרבית ב־L. ∎

הגדרה 19.10: **מעלת הטרנסצנדנטיות** $\mathrm{tr.deg}(L/K)$ של הרחבה L/K היא עוצמת בסיס טרנסצנדנטיות שלה.

מסקנה 19.11: *יהיו $K \subseteq L \subseteq M$ שדות. אז* $\mathrm{tr.deg}(L/K) \leq \mathrm{tr.deg}(M/K)$.

הוכחה: השלם בסיס טרנסצנדנטיות של L/K לבסיס טרנסצנדנטיות של M/K. ∎

תרגיל 19.12: *יהיו L, L' שני שדות סגורים אלגברית כך ש־* $\mathrm{char}(L) = \mathrm{char}(L')$ *ו־* $|L| = |L'| > \aleph_0$. *אז* $L \cong L'$.

הוכחה: יהיו K, K' השדות הראשוניים של L, L'. לפי ההנחה יש איזומורפיזם $\lambda_1\colon K \to K'$. לכן $\mathrm{char}(L) = \mathrm{char}(L')$, יהיו T, T' בסיסי טרנסצנדנטיות של $L/K, L'/K'$, בהתאמה. אז L, L' הם סגורים אלגבריים של $K(T), K'(T')$, בהתאמה. נראה ש־$|T| = |T'|$.

אכן, $|K| \leq \aleph_0$. אם T סופית, אז $|K[T]| \leq \aleph_0$, לכן $|K(T)| \leq \aleph_0$, ולפי תרגיל 5.3, $|L| = \aleph_0$, סתירה. אם T אינסופית, אז עוצמת קבוצת המונומים ב־T היא $|T|$, לכן $|K[T]| = |T|$, לכן $|K(T)| = |T|$, ולפי תרגיל 5.3, $|L| = |T|$. מכאן $|T| = |T'|$.

יש העתקה חד חד ערכית ועל $\lambda_2\colon T \to T'$. ההעתקות λ_1, λ_2 ניתנות להרחבה להומומורפיזם יחיד $\lambda\colon K[T] \to K'[T']$. גם ההופכיים של λ_1, λ_2 ניתנים להרחבה להומומורפיזם יחיד $K'[T'] \to K[T]$. קל לראות שזהו ההופכי של λ. לכן λ איזומורפיזם. הוא ניתן להרחבה לאיזומורפיזם של שדות המנות $K'(T') \to K(T)$, וזה ניתן להרחבה לאיזומורפיזם של הסגורים האלגבריים שלהם $L \to L'$. ∎

20. אי פריקות של $X^n - a$

יהי K שדה. בפרק זה נבדוק מתי פולינום $X^n - a \in K[X]$ אי פריק.

תרגיל 20.1: *יהי* $a \in K$ *ויהי* $n \in \mathbb{N}$.

(א) *אם* $p|n$ *ראשוני ו־* $a \in K^p$ *אז* $X^n - a \in K[X]$ *פריק.*

(ב) *אם* $4|n$ *ו־* $a \in -4K^4$ *אז* $X^n - a \in K[X]$ *פריק.*

הוכחה: (א) נניח ש־$n = pm$ ויש $b \in K$ כך ש־$a = b^p$. אז

$$X^n - a = (X^m)^p - b^p = (X^m - b)(X^{m(p-1)} + bX^{m(p-2)} + \ldots + b^{p-2}X^m + b^{p-1}).$$

(ב) נניח ש־$n = 4m$ ויש $b \in K$ כך ש־$a = -4b^4$. אז

$$X^n - a = X^{4m} + 4b^4 = (X^{2m} + 2bX^m + 2b^2)(X^{2m} - 2bX^m + 2b^2). \qquad \blacksquare$$

משפט 20.2: *יהי* $n \in \mathbb{N}$ *ויהי* $a \in K$. *אם*

(א) $a \notin K^p$ *לכל* $p|n$ *ראשוני;*

(ב) *אם* $4|n$ *אז גם* $a \notin -4K^4$

אז $f = X^n - a \in K[X]$ *אי פריק.*

נקדים להוכחת המשפט דברי הכנה:

הגדרה 20.3: תהי L/K הרחבה סופית. נגדיר $T = T_{L/K}$ ו־$N = N_{L/K}$ כך: $N(\alpha) = \det S_\alpha$, $T(\alpha) = \operatorname{tr} S_\alpha$, באשר $S_\alpha \colon L \to L$ ההעתקה הלינארית־K הנתונה על ידי $S_\alpha(x) = \alpha x$.

למה 20.4: *נסמן* $d = [L : K]$.

(א) $N \colon L^\times \to K^\times$ *הוא הומומורפיזם של חבורות.*

(ב) *יהי* $\alpha \in L$ *ויהי* $f = \operatorname{irr}(\alpha, K) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. *אז* $N(\alpha) = (-1)^d a_0^{\frac{d}{n}}$.

(ג) *יהי* $a \in K$. *אז* $N(a) = a^d$.

(ד) *אם* L/K *היא גלואה אז* N *היא הנורמה (הגדרה 15.1).*

הוכחה: (א) אם $\alpha \neq 0$ אז S_α אוטומורפיזם של L ולכן $\det S_\alpha \neq 0$. יהיו $\alpha, \beta \in L$. אז $S_{\alpha\beta} = S_\alpha \circ S_\beta$, לכן $\det S_{\alpha\beta} = \det S_\alpha \ \det S_\beta$.

(ב) כידוע, $1, \alpha, \ldots, \alpha^{n-1}$ הוא בסיס של $K(\alpha)$ מעל K. יהי $x_1, \ldots, x_m$ בסיס של L מעל $K(\alpha)$, באשר $m = \frac{d}{n}$. לפי משפט 4.14

$$x_1, \alpha x_1, \ldots, \alpha^{n-1}x_1, x_2, \alpha x_2, \ldots, \alpha^{n-1}x_2, \ , \ \ldots, \ x_m, \alpha x_m, \ldots, \alpha^{n-1}x_m$$

הוא בסיס של L מעל K. המטריצה של S_α לפיו היא מטריצה של m גושים זהים $\begin{pmatrix} C & & 0 \\ & \ddots & \\ 0 & & C \end{pmatrix}$, באשר

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & & & \\ . & . & \ddots & \ddots & . & \vdots \\ & & & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{M}_n(K).$$

והדטרמיננטה שלה היא

$$(\det C)^m = \big((-1)^{n+1}(-a_0)\big)^m = \big((-1)^n a_0\big)^m = (-1)^d a_0^m.$$

(ג) $\mathrm{irr}(a, K) = X - a$, לכן לפי (ב) $N(\alpha) = (-1)^d(-a)^d = a^d$.

(ד) מושאר לקורא. לא נשתמש בחלק זה בהמשך. ∎

למה 20.5: *יהי p ראשוני ויהי $a \in K$ כך ש־$a \notin K^p$. אז $f = X^p - a \in K[X]$ אי פריק.*

הוכחה: יהי $\alpha \in \tilde{K}$ שורש של f ונסמן $d = [K(\alpha) : K] = \deg \mathrm{irr}(\alpha, K)$.

תהי $N = N_{K(\alpha)/K}$. מתקיים $\alpha^p = a$, לכן $\big(N(\alpha)\big)^p = N(\alpha^p) = N(a) = a^d$, לכן $a^d \in K^p$. אם f פריק אז $d < p$ ולכן $p \nmid d$. מכאן $a \in K^p$ (יש $k, \ell \in \mathbb{Z}$ כך ש־$kd + \ell p = 1$ ולכן $a = (a^d)^k (a^\ell)^p \in K^p$), סתירה. ∎

למה 20.6: *נניח $n = mq$, באשר*

(1) *q ראשוני אי זוגי; או*

(2) *$q = 2$ ו־$m \geq 2$ חזקה של 2.*

יהי $a \in K$ שמקיים את התנאים (א), (ב) של משפט 20.2. יהי $\alpha \in \tilde{K}$ שורש של $X^q - a$, ויהי $L = K(\alpha)$. נניח כי $[L : K] = q$. אז

(א') *$\alpha \notin L^p$ לכל $p|m$ ראשוני;*

(ב') *אם $4|m$ אז $-\alpha \notin 4L^4$.*

הוכחה: תהי N הנורמה $N_{L/K}$.

(א') יהי p ראשוני, $p|m$. בפרט $p|n$. נניח בשלילה כי $\alpha = \beta^p$, באשר $\beta \in L$. אז

$$(-1)^{q+1} a = (-1)^q(-a) = N(\alpha) = N(\beta)^p \in K^p.$$

אם q אי זוגי, זוהי סתירה לתנאי (א).

אם $q = 2$ ו־$m \geq 2$ חזקה של 2 אז $p = 2$ ו־$4|n$. אז $\beta = b + c\alpha$, באשר $b, c \in K$. לכן

$$\alpha = \beta^2 = (b + c\alpha)^2 = (b^2 + ac^2) + 2bc\alpha.$$

מכאן $b^2 + ac^2 = 0$, $2bc = 1$. (בפרט $c \neq 1$.) לכן $a = -\frac{b^2}{c^2} = -b^2(2b)^2 = -4b^4$, סתירה לתנאי (ב).

(ב') נניח $4|m$ (ולכן $4|n$) ונניח בשלילה כי $\alpha = -4\beta^4$, באשר $\beta \in L$. אז

$$(-1)^{q+1}a = (-1)^q(-a) = N(\alpha) = (-4)^q N(\beta)^4,$$

כלומר,

$$-a = 4^q N(\beta)^4.$$

אם q אי זוגי אז $-a = 4(2^{\frac{q-1}{2}})^4 N(\beta)^4 \in 4K^4$, וזוהי סתירה לתנאי (ב).

אם $q = 2$ ו־$m \geq 2$ חזקה של 2, יהי $i = \frac{\alpha}{4N(\beta)^2} \in L$. אז $i^2 = \frac{a}{4^2 N(\beta)^4} = -1$. לכן $\alpha = -4\beta^4 = (2i\beta^2)^2 \in L^2$, וזוהי סתירה לתנאי (א') שהוכחנו קודם (כי $2|m$). ∎

הוכחת משפט 20.2: באינדוקציה על n. עבור $n = 1$ הטענה ברורה. עבור n ראשוני היא נובעת מלמה 20.5. נניח ש־n אינו ראשוני והטענה נכונה לכל מחלק של n קטן מ־n.

אם n הוא חזקה של 2, יהי $q = 2$. אחרת יהי q מחלק ראשוני אי זוגי של n. יהי $m = n/q$. אז $m > 1$.

לפי הנחת האינדוקציה המשפט נכון עבור q, m. יהי $\alpha \in \tilde{K}$ שורש של $X^q - a$ ויהי $L = K(\alpha)$. אז $[L : K] = q$. לפי למה 20.6 והנחת האינדוקציה, $X^m - \alpha \in L[X]$ אי פריק. יהי $\gamma \in \tilde{K}$ שורש של $X^m - \alpha \in L[X]$, אז $[L(\gamma) : L] = m$. לכן $[L(\gamma) : K] = qm = n$. אבל $\alpha = \gamma^m \in K(\gamma)$, לכן $L(\gamma) = K(\alpha)(\gamma) = K(\gamma)$, ולכן $[K(\gamma) : K] = n$. כיוון ש־$\gamma^n = (\gamma^m)^q = \alpha^q = a$, הפולינום $X^n - a \in K[X]$ אי פריק. ∎

מסקנה 20.7: *יהי p ראשוני ויהי $a \in K$, $a \notin K^p$. אם $p \neq 2$ או $p = 2$ ו־$\sqrt{-1} \in K$, אז $X^{p^r} - a \in K[X]$ אי פריק לכל $r \geq 1$.*

הוכחה: נניח $p = 2$ ו־$i := \sqrt{-1} \in K$. אם $a \in -4K^4$ אז $a \in (2iK^2)^2 \subseteq K^2$, סתירה. ∎

מסקנה 20.8: *אם $[\tilde{K} : K] < \infty$ אז $\tilde{K} = K(i)$, באשר $i^2 = 1$. כמו כן $\tilde{K}/K$ גלואה.*

הוכחה: ההרחבה $\tilde{K}/K$ היא נורמלית. לפי משפט 18.13 יש $K \subseteq E \subseteq \tilde{K}$ כך ש־$\tilde{K}/E$ גלואה ו־E/K אי פרידה טהורה. אם $E \neq K$ אז $\mathrm{char}\, K = p > 0$ ויש $a \in K$ כך ש־$a \notin K^p$. לפי מסקנה 20.7, $[\tilde{K} : K] = \infty$, סתירה. לכן $E = K$ ו־$\tilde{K}/K$ היא גלואה. בלי הגבלת הכלליות $i \in K$, אחרת נחליף את K ב־$K(i)$.

תהי $G = \mathrm{Gal}(\tilde{K}/K)$. אם $G \neq 1$, יש ראשוני p שמחלק את $|G|$ ואז יש $H \leq G$ מסדר p. יהי $F = \tilde{K}^H$. אז $\tilde{K}/F$ מעגלית מסדר p. אם $p = \mathrm{char}\, K$ אז לפי משפט 15.8 יש ל־F הרחבה מסדר p^2, סתירה.

אם $p \neq \operatorname{char} K$, אז לפי משפט קומר $\tilde{K} = F(\alpha)$ באשר α שורש של $X^p - a$, עבור איזה $a \in F$. (התנאי $\zeta_p \in F$ במשפט קומר מתקיים, כי $[F(\zeta_p) : F]$ מחלק את $\varphi(p)$ וגם את $p = [\tilde{K} : F]$, ולכן הוא 1.) בפרט $a \notin F^p$. לכן לפי מסקנה 20.7, $X^{p^r} - a \in F[X]$ אי פריק לכל r, סתירה ל־$[\tilde{K} : F] = p$. ∎

21. דואליות בחבורות אבליות

בפרק זה נדון בחבורות אבליות. נשתמש בכתיב חיבורי לפעולה בחבורות אלה.

יהי $m \in \mathbb{N}$ ותהי $Z \cong \mathbb{Z}/m\mathbb{Z}$ חבורה מעגלית מסדר m.

הגדרה 21.1: חבורה אבלית A היא **בעלת מעריך** m אם $ma = 0$ לכל $a \in A$.

הגדרה 21.2: תהי A חבורה אבלית. נסמן

$$A^* = \mathrm{Hom}(A, Z) = \{\varphi\colon A \to Z \mid \text{הומומורפיזם } \varphi\}$$

זוהי חבורה אבלית, ביחס לפעולה החיבור $(\varphi_1 + \varphi_2)(a) = \varphi_1(a) + \varphi_2(a)$ בעלת מעריך m:
$(m\varphi)(a) = m\varphi(a) = 0, \qquad \varphi \in A^*,\ a \in A$.

הומומורפיזם של חבורות אבליות $f\colon A \to B$ משרה העתקה דואלית $f^*\colon B^* \to A^*$ על ידי $f^*(\psi) = \psi \circ f$. זהו הומומורפיזם:

$$f^*(\psi_1 + \psi_2) = (\psi_1 + \psi_2) \circ f = \psi_1 \circ f + \psi_2 \circ f = f^*(\psi) + f^*(\psi).$$

אם $A \xrightarrow{f} B \xrightarrow{g} C$ הומומורפיזמים של חבורות אבליות, ו־$C^* \xrightarrow{g^*} B^* \xrightarrow{f^*} A^*$ ההעתקות הדואליות, אז $(g \circ f)^* = f^* \circ g^*$. כמו כן $\mathrm{id}^* = \mathrm{id}$.

משפט 21.3: *תהיינה A, B חבורות אבליות. אז*

(א) $(A \oplus B)^* \cong A^* \oplus B^*$.

(ב) *אם A סופית ובעלת מעריך m, אז $A \cong A^*$.*

הוכחה: (א) תהיינה $p_A\colon A \oplus B \to A,\ p_B\colon A \oplus B \to B$ הטלות הקואורדינטות. הן מגדירות הומומורפיזמים $p_A^*\colon A^* \to (A \oplus B)^*,\ p_B^*\colon B^* \to (A \oplus B)^*$, ואלה מגדירים העתקה $H\colon A^* \oplus B^* \to (A \oplus B)^*$ על ידי

$$H(\varphi, \psi) = p_A^*(\varphi) + p_B^*(\psi) = \varphi \circ p_A + \psi \circ p_B$$

העתקה זו היא הומומורפיזם:

$$\begin{aligned} H\big((\varphi, \psi) + (\varphi', \psi')\big) &= H\big(\varphi + \varphi', \psi + \psi'\big) = (\varphi + \varphi') \circ p_A + (\psi + \psi') \circ p_B = \\ &= \varphi \circ p_A + \varphi' \circ p_A + \psi \circ p_B + \psi' \circ p_B = (\varphi \circ p_A + \psi \circ p_B) + (\varphi' \circ p_A + \psi' \circ p_B) = \\ &= H(\varphi, \psi) + H(\varphi', \psi') \end{aligned}$$

והיא חד חד ערכית: אם $H(\varphi, \psi) = 0$, כלומר, $(\varphi \circ p_A + \psi \circ p_B)(a, b) = 0$ לכל $(a, b) \in A \oplus B$, אז $\varphi(a) + \psi(b) = 0$ לכל $(a, b) \in A \oplus B$, ובפרט, אם ניקח $b = 0$ או $a = 0$, אז $\psi(b) = 0$ לכל $b \in B$, $\varphi(a) = 0,$ לכל $a \in A$. לכן $\varphi = 0, \psi = 0$, כלומר, $(\varphi, \psi) = 0$.

לבסוף, היא על: יהי $\Phi \in (A\oplus B)^*$, כלומר, $\Phi\colon A\oplus B\to Z$ הומומורפיזם. נגדיר $\psi\colon B\to Z$,$\varphi\colon A\to Z$ על ידי הצמצומים $\varphi(a)=\Phi(a,0),\ \psi(b)=\Phi(0,b)$. אז $\varphi\in A^*,\ \psi\in B^*$ ומתקיים

$$\Phi(a,b)=\Phi(a,0)+\Phi(0,b)=\varphi(a)+\psi(b)=\varphi\circ p_A(a,b)+\psi\circ p_B(a,b)=\big(H(\varphi,\psi)\big)(a,b)$$

לכל $a\in A,\ b\in B$ לכן $\Phi=H(\varphi,\psi)$.

(ב) כל חבורה אבלית סופית היא סכום ישר של חבורות מעגליות סופיות. אם היא בעלת מעריך m אז גם המחוברים הישרים שלה בעלי מעריך m. לכן, לפי (א), די להניח ש־A היא מעגלית סופית, $A=\langle x\rangle$.

יהי d הסדר של A. אז $\operatorname{ord}x=d|m$. ב־Z, שהינה מעגלית מסדר m יש תת חבורה יחידה Z' מסדר d, וכל איבר ב־Z שסדרו מחלק את d נמצא ב־Z'.

כל $c\in Z'$ מגדיר הומומורפיזם $\varphi_c\in A^*$ על ידי $\varphi_c(kx)=kc$. נראה שההעתקה $c\mapsto\varphi_c$ היא איזומורפיזם $Z'\to A^*$.

אכן, אם $c_1,c_2\in Z'$, אז $\varphi_{c_1+c_2}(x)=c_1+c_2=\varphi_{c_1}(x)+\varphi_{c_2}(x)=(\varphi_{c_1}+\varphi_{c_2})(x)$, לכן $\varphi_{c_1+c_2}=\varphi_{c_1}+\varphi_{c_2}$.

אם $\varphi_c=0$, אז $c=\varphi_c(x)=0$ ולכן $c\mapsto\varphi_c$ חד חד ערכית.

אם $\varphi\colon A\to Z$ הומומורפיזם, אז $c:=\varphi(x)$ מסדר שמחלק את d ולכן $c\in Z'$. ברור ש־$\varphi=\varphi_c$. לכן $c\mapsto\varphi_c$ על.

לכן $A^*\cong Z'=\mathbb{Z}/d\mathbb{Z}\cong A$. ∎

הגדרה 21.4: תהיינה A,B שתי חבורות אבליות. **בי־הומומורפיזם** או **זיווג** $A\times B\to Z$ היא העתקה, שתסומן $(a,b)\mapsto\langle a,b\rangle$, שמקיימת:

(א) לכל $b\in B$ ההעתקה $a\mapsto\langle a,b\rangle$, היא הומומורפיזם $\lambda_b\colon A\to Z$.

(ב) לכל $a\in A$ ההעתקה $b\mapsto\langle a,b\rangle$, היא הומומורפיזם $\rho_a\colon B\to Z$.

יהי $\langle,\rangle$ זיווג.

(ג) גרעין משמאל שלו הוא $A'=\bigcap_{b\in B}\operatorname{Ker}(\lambda_b)=\{a\in A|\ (\forall b\in B)\langle a,b\rangle=0\}\le A$

(ד) גרעין מימין שלו הוא $B'=\bigcap_{a\in A}\operatorname{Ker}(\rho_a)=\{b\in B|\ (\forall a\in A)\langle a,b\rangle=0\}\le B$

הערה 21.5: יהי $A\times B\to Z$ זיווג $(a,b)\mapsto\langle a,b\rangle$. יהיו $A',\ B'$ הגרעינים מימין ומשמאל. אז הזיווג משרה זיווג $A/A'\times B/B'\to Z$ בעל גרעינים טריביאליים מימין ומשמאל. ∎

משפט 21.6: *יהי $A\times B\to Z$ זיווג של חבורות אבליות. יהיו $A'\le A,\ B'\le B$ הגרעינים מימין ומשמאל שלו. אז*

(א) *$a\mapsto\rho_a$ הוא הומומורפיזם $\eta\colon A\to B^*$ שגרעינו הוא הגרעין משמאל של הזיווג.*

(ב) *η משרה הומומורפיזם חד חד ערכי $\bar\eta\colon A/A'\to(B/B')^*$.*

(ג) *A/A' סופית בעלת מעריך m אם ורק אם B/B' סופית בעלת מעריך m; במקרה זה $\bar\eta$ הוא איזומורפיזם.*

הוכחה: (א) $\rho_{a_1+a_2}(b)=\langle a_1+a_2,b\rangle=\langle a_1,b\rangle+\langle a_2,b\rangle=\rho_{a_1}(b)+\rho_{a_2}(b)=(\rho_{a_1}+\rho_{a_2})(b)$.

כמו כן, $\rho_a = 0 \Leftrightarrow\ \rho_a(b) = 0$ לכל $b \in B \Leftrightarrow \langle a, b\rangle = 0$ לכל $b \in B \Leftrightarrow\ a \in A'$.

(ב) נפעיל את (א) על הזיווג המושרה $A/A' \times B/B' \to Z$, שגרעינו משמאל הוא טריביאלי. לפי (א), ההומומורפיזם $\bar{\eta}$ הוא חד חד ערכי.

(ג) אם B/B' סופית בעלת מעריך m, אז לפי משפט 21.3(ב), $B/B' \cong (B/B')^*$. לפי (ב), גם A/A' סופית בעלת מעריך m, ו־$|A/A'| \leq |B/B'|$. באופן סימטרי, אם A/A' סופית בעלת מעריך m, אז גם B/B' סופית בעלת מעריך m ו־$|B/B'| \leq |A/A'|$. לכן אם אחת שתי החבורות האלה סופית בעלת מעריך m, אז שתיהן בעלות אותו הסדר. לכן $\bar{\eta}$ הוא איזומורפיזם. ∎

22. תורת קומר ותורת ארטין־שרייר

מטרת הסעיף הזה היא לאפיין כל הרחבות (גלואה) אבליות של שדה (בתוך סגור אלגברי נתון) בעלות מעריך נתון. נדון רק במקרה בו המעריך זר לאפיון או שהוא ראשוני ושווה לאפיון.

יהי K שדה, יהי $\tilde{K}$ סגור אלגברי שלו, ויהי $m \in \mathbb{N}$.

הגדרה 22.1: הרחבה גלואה L/K היא **בעלת מעריך** m אם $\sigma^m = 1$ לכל $\sigma \in \operatorname{Gal}(L/K)$.

תורת קומר.

נניח כי m זר ל־$\operatorname{char}(K)$ ו־K מכיל שורש יחידה m־י פרימיטיבי ζ_m. אז $\mu := \{1, \zeta_m, \dots, \zeta_m^{m-1}\}$ קבוצת כל שורשי היחידה ה־m־יים. זוהי תת חבורה של $K^\times$.

נגדיר העתקה $\mathcal{M}\colon \tilde{K}^\times \to \tilde{K}^\times$ על ידי $\mathcal{M}(x) = x^m$. זהו הומומורפיזם, $\operatorname{Ker}\mathcal{M} = \mu$. אם $L \subseteq \tilde{K}$ תת שדה, אז $\mathcal{M}$ מעתיק את $L^\times$ לתוך $L^\times$.

סימון 22.2: (א) $K^{\times m} = \{a^m \mid a \in K^\times\} = \mathcal{M}(K^\times)$. זוהי תת חבורה של $K^\times$.

(ב) יהי $a \in K$. נסמן $a^{\frac{1}{m}} = \{\alpha \in \tilde{K} \mid \alpha^m = a\} = \mathcal{M}^{-1}(a)$. זהו קוסט של $\mu = \operatorname{Ker}\mathcal{M}$.

(ג) תהי $B \subseteq K$ קבוצה. נסמן $B^{\frac{1}{m}} = \{\beta \in \tilde{K} \mid \beta^m \in B\}$ ו־$K_B = K(B^{\frac{1}{m}}) = K(a^{\frac{1}{m}} \mid a \in B)$.

הערה 22.3: (א) אם $\alpha \in a^{\frac{1}{m}}$, אז $a^{\frac{1}{m}} = \{\alpha, \alpha\zeta_m, \dots, \alpha\zeta_m^{m-1}\}$. לכן $K(a^{\frac{1}{m}}) = K(\alpha)$.

(ב) K_B הוא צירוף השדות $K(a^{\frac{1}{m}})$, באשר a עובר על כל איברי B.

(ג) $K_B = K$ אם ורק אם $B \subseteq K^{\times m}$.

משפט 22.4: *יהי K שדה, יהי $m \in \mathbb{N}$ זר ל־$\operatorname{char}(K)$, ונניח ששורש יחידה m־י פרימיטיב שייך ל־K. תהי $B \subseteq K^\times$ קבוצה ויהי $K_B = K(B^{\frac{1}{m}})$. אז*

(א) *K_B/K הרחבת גלואה אבלית בעלת מעריך m.*

(ב) *לכל $\sigma \in \operatorname{Gal}(K_B/K)$ ולכל $a \in B$ קיים $\langle \sigma, a\rangle \in \mu$ יחיד כך ש־$\sigma(\alpha) = \alpha\langle\sigma, a\rangle$, באשר $\alpha \in \tilde{K}^\times$ כך ש־$\alpha^m = a$.*

נניח ש־B תת חבורה של $K^\times$ שמכילה את $K^{\times m}$. אז

(ג) *ההעתקה $\langle \sigma, a\rangle \mapsto (\sigma, a)$ היא זיווג של חבורות $\operatorname{Gal}(K_B/K) \times B \to \mu \cong \mathbb{Z}/m\mathbb{Z}$.*

(ד) *הגרעין משמאל $\{\sigma \in \operatorname{Gal}(K_B/K) \mid (\forall a \in B)\langle\sigma, a\rangle = 0\}$ הוא 0.*

(ה) *הגרעין מימין $\{a \in B \mid (\forall \sigma \in \operatorname{Gal}(K_B/K))\langle\sigma, a\rangle = 1\}$ הוא $K^{\times m}$.*

(ו) *K_B/K הרחבה סופית אם ורק אם $B/K^{\times m}$ חבורה סופית. במקרה זה $[K_B : K] = (B : K^{\times m})$.*

הוכחה: (א) נניח תחילה כי $B = \{a\}$, כלומר, $K_B = K(a^{\frac{1}{m}}) = K(\alpha)$, באשר $\alpha \in \tilde{K}^\times$ כך ש־$\alpha^m = a$.

לפי משפט קומר (משפט 15.5) K_B/K מעגלית ממעלה שמחלקת את m. בפרט היא בעלת מעריך m, ו־α פריד מעל K.

במקרה הכללי K_B נוצרת על ידי איברים פרידים (שורשים m־יים של איברי B) ולכן פרידה. היא צירוף של הרחבות נורמליות $K(a^{\frac{1}{m}})$, ולכן נורמלית: אם σ אוטומורפיזם־K של $\tilde{K}$, הוא מעתיק כל $K(a^{\frac{1}{m}})$ על עצמו, לכל $a \in B$, לכן את הצירוף שלהן K_B על עצמו.

לכן K_B/K הרחבת גלואה. היא אבלית בעלת מעריך m, כי לכל $\sigma, \tau \in \mathrm{Gal}(K_B/K)$ מתקיים: $\sigma^m|_{K(a^{\frac{1}{m}})} = 1$,$(\sigma\tau)|_{K(a^{\frac{1}{m}})} = (\tau\sigma)|_{K(a^{\frac{1}{m}})}$, לכל $a \in B$, לכן $\sigma\tau = \tau\sigma$, $\sigma^m = 1$.

(ב) יהי $a \in B$ ויהי $\alpha \in \tilde{K}^\times$ כך ש־$\alpha^m = a$. אז α שורש של $X^m - a = \prod_{\omega\in\mu}(X - \omega\alpha)$ שכל שורשיו שונים זה מזה, ולכן אם $\sigma \in \mathrm{Gal}(K_B/K)$ אז $\sigma(\alpha) = \alpha\omega$ עבור $\omega \in \mu$ יחיד.

הגדרה זו של ω איננ תלויה בבחירת שורש α של a: כל שורש של a הוא מהצורה $\alpha\zeta$, באשר $\zeta \in \mu$. לכן $\sigma(\alpha\zeta) = \sigma(\alpha)\zeta = \alpha\omega\zeta = (\alpha\zeta)\omega$.

נסמן $\langle\sigma, a\rangle = \omega$.

(ג) אם $\sigma, \tau \in \mathrm{Gal}(K_B/K)$ אז (כפי שהוכחנו במשפט Kummer)

$$\alpha\langle\sigma\tau, a\rangle = (\sigma\tau)(\alpha) = \sigma\big(\tau(\alpha)\big) = \sigma\big(\alpha\langle\tau, a\rangle\big) = \sigma(\alpha)\langle\tau, a\rangle = \alpha\langle\sigma, a\rangle\langle\tau, a\rangle,$$

לכן $\langle\sigma\tau, a\rangle = \langle\sigma, a\rangle\langle\tau, a\rangle$.

יהי $a, b \in B$ ויהיו $\alpha, \beta \in K_B$ כך ש־$\beta^m = b$,$\alpha^m = a$. אז $(\alpha\beta)^m = ab$. לכן

$$\alpha\beta\langle\sigma, ab\rangle = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \big(\alpha\langle\sigma, a\rangle\big)\big(\beta\langle\sigma b\rangle\big) = \alpha\beta\langle\sigma, a\rangle\langle\sigma, b\rangle$$

לכן $\langle\sigma, ab\rangle = \langle\sigma, a\rangle\langle\sigma, b\rangle$.

(ד) יהי $\sigma \in \mathrm{Gal}(K_B/K)$. נניח $\langle\sigma, a\rangle = 1$ לכל $a \in B$. אז $\sigma(\alpha) = \alpha$ לכל $\alpha \in K_B$ כך ש־$\alpha^m = a \in B$. כיוון ש־K_B נוצר על ידי איברים α כאלה, $\sigma = 1$.

(ה) יהי $a \in B$. נבחר $\alpha \in K_B$ כך ש־$\alpha^m = a \in B$. אז

$$1 = \langle\sigma, a\rangle \text{ לכל } \sigma \in \mathrm{Gal}(K_B/K) \Leftrightarrow \sigma(\alpha) = \alpha \text{ לכל } \sigma \in \mathrm{Gal}(K_B/K) \Leftrightarrow \alpha \in K \Leftrightarrow a \in K^{\times m}.$$

(ו) לפי (ד), (ה), הזיווג של (ג) משרה זיווג $\mathrm{Gal}(K_B/K) \times B/K^{\times m} \to \mu \cong \mathbb{Z}/m\mathbb{Z}$ שהגרעינים שלו מימין ומשמאל טריביאליים. לפי (א), $\mathrm{Gal}(K_B/K)$ בעלת מעריך m; ברור ש־$B/K^{\times m}$ בעלת מעריך m. לכן לפי משפט 21.6, אחת החבורות היא סופית אם ורק אם השנייה סופית, ואז הן איזומורפיות, ובפרט בעלות אותו סדר $|B/K^{\times m}| = |\mathrm{Gal}(K_B/K)| = [K_B : K]$. ∎

משפט 22.5 (תורת קומר): *ההעתקה $B \mapsto K_B$ היא התאמה חד חד ערכית ושומרת הכלה מקבוצת התת חבורות של $K^\times$ המכילות $K^{\times m}$ על קבוצת ההרחבות האבליות בעלות מעריך m של K בתוך $\tilde{K}$.*

הוכחה: אם $B_1 \subseteq B_2$ אז $B_1^{\frac{1}{m}} \subseteq B_2^{\frac{1}{m}}$, ולכן $K_{B_1} = K(B_1^{\frac{1}{m}}) \subseteq K(B_2^{\frac{1}{m}}) = K_{B_2}$.

להיפך, נניח ש־$K_{B_1} \subseteq K_{B_2}$ ונראה כי $B_1 \subseteq B_2$. יהי $b \in B_1$. אז $K(b^{\frac{1}{m}}) \subseteq K_{B_1} \subseteq K_{B_2}$. מכאן ש־$K(b^{\frac{1}{m}})$ מוכלת בהרחבה נוצרת סופית של K שמוכלת ב־K_{B_2}, כלומר, $K(b^{\frac{1}{m}}) \subseteq K(b_1^{\frac{1}{m}}, \dots, b_n^{\frac{1}{m}})$, באשר $b_1, \dots, b_n \in B_2$. לכן, כדי להוכיח ש־$b \in B_2$, די להניח ש־$B_2/K^{\times m}$ חבורה אבלית נוצרת סופית. כיוון שכל איבר בה מסדר סופי (מחלק את m), זוהי חבורה אבלית סופית. תהי $B = \langle B_2, b\rangle$, אז גם $B/K^{\times m}$ סופית, $K_B = K_{B_2}$, ולכן, לפי משפט 22.4(ו),

$$(B : K^{\times m}) = [K_B : K] = [K_{B_2} : K] = (B_2 : K^{\times m})$$

מכאן $B = B_2$, ולכן $b \in B_2$.

בכך הוכחנו שההעתקה $B \mapsto K_B$ היא חד חד ערכית. נראה שהיא על.

תהי L/K הרחבה אבלית בעלת מעריך m. תהי $B = L^{\times m} \cap K^\times = \{\beta^m \in K \mid \beta \in L^\times\}$. זוהי תת חבורה של $K^\times$ שמכילה את $K^{\times m}$. אם $b = \beta^m \in B$, אז $\beta \in L$, לכן $K_B \subseteq L$. להיפך, יהי $\alpha \in L^\times$. יהי L_0 סגור גלואה של $K(\alpha)$ מעל K, אז $L_0 \subseteq L$ ו־L_0/K הרחבת גלואה סופית. די להראות ש־$L_0 \subseteq K_B$.

כיוון ש־$\mathrm{Gal}(L/K)$ חבורה אבלית בעלת מעריך m, גם המנה הסופית שלה $\mathrm{Gal}(L_0/K)$ היא חבורה אבלית בעלת מעריך m. כידוע, חבורה אבלית סופית היא מכפלה ישרה של חבורות מעגליות. לכן

$$\mathrm{Gal}(L_0/K) = \mathrm{Gal}(L_1/K) \times \cdots \times \mathrm{Gal}(L_n/K),$$

באשר $K \subseteq L_1, \dots, L_n \subseteq L_0 \subseteq L$ הרחבות מעגליות סופיות של K, (בלי הגבלת הכלליות לא טריביאליות) ו־$L_1 \cdots L_n = L_0$. לכן די להראות ש־$L_i \subseteq K_B$ לכל $1 \le i \le n$. כל $\mathrm{Gal}(L_i/K)$ היא מנה של $\mathrm{Gal}(L_0/K)$, ולכן בעלת מעריך m. בפרט הסדר של החבורה d ($d \neq 1$) מחלק את m.

לפי משפט קומר $L_i = K(\beta)$, באשר $\beta^d \in K$, ולכן $\beta^m \in K$. כיוון ש־$L_i \neq K$, מתקיים $\beta \neq 0$, לכן $\beta \in L^\times$ ו־$\beta^m \in K^\times$. מכאן $b = \beta^m \in B$ ולכן $\beta \in K_B$. בפרט $L_i \subseteq K_B$. ∎

תורת ארטין־שרייר.

נניח כי $m = p = \mathrm{char}(K)$ נגדיר העתקה $\mathcal{P}\colon \tilde{K} \to \tilde{K}$ על ידי $\mathcal{P}(x) = x^p - x$. זהו הומומורפיזם של החבורה החיבורית של $\tilde{K}$ שמעתיק כל תת שדה של $\tilde{K}$ (ובפרט את K) לתוך עצמו; $\mathrm{Ker}\,\mathcal{P}$ הוא השדה הראשוני $\mathbb{F}_p$ של K.

סימון 22.6: (א) $\mathcal{P}(K) = \{\mathcal{P}(a) |\ a \in K\}$. זוהי תת חבורה של K (החבורה החיבורית של K).

(ב) יהי $a \in K$. נסמן $\mathcal{P}^{-1}(a) = \{\alpha \in \tilde{K} |\ \mathcal{P}(\alpha) = a\}$. זהו קוסט של $\mathbb{F}_p$.

(ג) תהי $B \subseteq K$ קבוצה. נסמן $\mathcal{P}^{-1}(B) = \{\beta \in \tilde{K} |\ \mathcal{P}(\beta) \in B\}$ ו־$K_B = K(\mathcal{P}^{-1}(B)) = K(\mathcal{P}^{-1}(a) |\ a \in B)$.

הערה 22.7: (א) אם $\alpha \in \mathcal{P}^{-1}(a)$, אז $\mathcal{P}^{-1}(a) = \{\alpha, \alpha+1, \ldots, \alpha+p-1\}$. לכן $K(\mathcal{P}^{-1}(a)) = K(\alpha)$.

(ב) K_B הוא צירוף השדות $K(\mathcal{P}^{-1}(a))$, באשר a עובר על כל איברי B.

(ג) $K_B = K$ אם ורק אם $B \subseteq \mathcal{P}(K)$.

משפט 22.8: *יהי K שדה, $p = \mathrm{char}(K) > 0$, תהי $B \subseteq K$ קבוצה, ויהי $K_B = K(\mathcal{P}^{-1}(B))$. אז*

(א) *K_B/K הרחבת גלואה אבלית בעלת מעריך p.*

(ב) *לכל $\sigma \in \mathrm{Gal}(K_B/K)$ ולכל $a \in B$ קיים $\langle \sigma, a\rangle \in \mathbb{F}_p$ יחיד כך ש־$\sigma(\alpha) = \alpha + \langle \sigma, a\rangle$, באשר $\alpha \in \mathcal{P}^{-1}(a)$.*

נניח ש־B תת חבורה של K שמכילה את $\mathcal{P}(K)$. אז

(ג) *ההעתקה $(\sigma, a) \mapsto \langle \sigma, a\rangle$ היא זיווג של חבורות $\mathrm{Gal}(K_B/K) \times B \to \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ באשר $\alpha \in K_B$ כך ש־$\mathcal{P}(\alpha) = a$.*

(ד) *הגרעין משמאל $\{\sigma \in \mathrm{Gal}(K_B/K) |\ (\forall a \in B)\langle \sigma, a\rangle = 0\}$ הוא 1.*

(ה) *הגרעין מימין $\{a \in B |\ (\forall \sigma \in \mathrm{Gal}(K_B/K))\langle \sigma, a\rangle = 0\}$ הוא $\mathcal{P}(K)$.*

(ו) *K_B/K הרחבה סופית אם ורק אם $B/\mathcal{P}(K)$ חבורה סופית. במקרה זה $[K_B : K] = (B : \mathcal{P}(K))$.*

הוכחה: (א) נניח תחילה כי $B = \{a\}$, כלומר, $K_B = K(\mathcal{P}^{-1}(a)) = K(\alpha)$, באשר $\alpha \in \tilde{K}$ כך ש־$\mathcal{P}(\alpha) = a$. לפי משפט ארטין־שרייר (משפט 15.7) K_B/K מעגלית ממעלה 1 או p ו־α פריד מעל K.

במקרה הכללי K_B נוצרת על ידי איברים פרידים ($\alpha \in \tilde{K}$ כך ש־$\mathcal{P}(\alpha) \in B$) ולכן פרידה. היא צירוף של הרחבות נורמליות $K(\mathcal{P}^{-1}(a))$, ולכן נורמלית: אם σ אוטומורפיזם־K של $\tilde{K}$, הוא מעתיק כל $K(\mathcal{P}^{-1}(a))$ על עצמו, לכל $a \in B$, לכן את הצירוף שלהן K_B על עצמו.

לכן K_B/K הרחבת גלואה. היא אבלית בעלת מעריך p, כי לכל $\sigma, \tau \in \mathrm{Gal}(K_B/K)$ מתקיים: $(\sigma\tau)|_{K(\mathcal{P}^{-1}(a))} = (\tau\sigma)|_{K(\mathcal{P}^{-1}(a))}$, $\sigma^p|_{K(\mathcal{P}^{-1}(a))} = 1$, לכל $a \in B$, לכן $\sigma\tau = \tau\sigma$, $\sigma^p = 1$.

(ב) יהי $a \in B$ ויהי $\alpha \in \tilde{K}$ כך ש־$\mathcal{P}(\alpha) = a$. אז α שורש של $X^p - X - a = \prod_{i=1}^{p-1}(X - \alpha - i)$ שכל שורשיו שונים זה מזה, ולכן אם $\sigma \in \mathrm{Gal}(K_B/K)$ אז $\sigma(\alpha) = \alpha + i$ עבור $0 \le i < p$ יחיד.

הגדרה זו של i איננ תלויה בבחירת שורש α של a: כל שורש של a הוא מהצורה $\alpha' = \alpha + j$, באשר $0 \le j \le n-1$. לכן $\sigma(\alpha') = \sigma(\alpha + j) = \sigma(\alpha) + j = \alpha + i + j = (\alpha + j) + i = \alpha' + i$.
נסמן $\langle \sigma, a \rangle = i$.

(ג) אם $\sigma, \tau \in \mathrm{Gal}(K_B/K)$ אז (כפי שהוכחנו במשפט Artin-Schreier)

$$\alpha + \langle \sigma\tau, a \rangle = (\sigma\tau)(\alpha) = \sigma\big(\tau(\alpha)\big) = \sigma\big(\alpha + \langle \tau, a \rangle\big) = \sigma(\alpha) + \langle \tau, a \rangle =$$
$$= \alpha + \langle \sigma, a \rangle + \langle \tau, a \rangle$$

לכן $\langle \sigma\tau, a \rangle = \langle \sigma, a \rangle + \langle \tau, a \rangle$.

יהי $a, b \in B$ ויהיו $\alpha, \beta \in K_B$ כך ש־$\mathcal{P}(\beta) = b$, $\mathcal{P}(\alpha) = a$. אז $\mathcal{P}(\alpha + \beta) = a + b$. לכן

$$(\alpha + \beta) + \langle \sigma, a + b \rangle = \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \big(\alpha + \langle \sigma, a \rangle\big) + \big(\beta + \langle \sigma b \rangle\big) =$$
$$= (\alpha + \beta) + \langle \sigma, a \rangle + \langle \sigma, b \rangle$$

לכן $\langle \sigma, a + b \rangle = \langle \sigma, a \rangle + \langle \sigma, b \rangle$.

(ד) יהי $\sigma \in \mathrm{Gal}(K_B/K)$. נניח $\langle \sigma, a \rangle = 0$ לכל $a \in B$. אז $\sigma(\alpha) = \alpha$ לכל $\alpha \in K_B$ כך ש־$\mathcal{P}(\alpha) = a \in B$. כיוון ש־$K_B$ נוצר על ידי איברים α כאלה, $\sigma = 1$.

(ה) יהי $a \in B$. נבחר $\alpha \in K_B$ כך ש־$\mathcal{P}(\alpha) = a \in B$. אז

$\langle \sigma, a \rangle = 0$ לכל $\sigma \in \mathrm{Gal}(K_B/K) \Leftrightarrow \sigma(\alpha) = \alpha$ לכל $\sigma \in \mathrm{Gal}(K_B/K) \Leftrightarrow \alpha \in K \Leftrightarrow a \in \mathcal{P}(K)$.

(ו) לפי (ד), (ה), הזיווג של (ג) משרה זיווג $\mathrm{Gal}(K_B/K) \times B/\mathcal{P}(K) \to \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ שהגרעינים שלו מימין ומשמאל טריביאליים. לכן הזיווג משרה איזומורפיזם $B/\mathcal{P}(K) \to \mathrm{Hom}(\mathrm{Gal}(K_B/K), \mathbb{Z})$ של חבורות אבליות. שתי החבורות הן בעלות מעריך p. לכן, בפרט, $B/\mathcal{P}(K)$ סופית אם ורק אם $\mathrm{Gal}(K_B/K)$ סופית ואם זה קורה, הן חבורות איזומורפיות. לכן אז $[K_B : K] = |\mathrm{Gal}(K_B/K)| = |B/\mathcal{P}(K)|$. ∎

משפט 22.9 (תורת ארטין־שרייר): *ההעתקה $B \mapsto K_B$ היא התאמה חד חד ערכית ושומרת הכלה מקבוצת התת חבורות של החבורה החיבורית של K המכילות את $\mathcal{P}(K)$ על קבוצת ההרחבות האבליות בעלות מעריך p של K בתוך $\tilde{K}$.*

הוכחה: אם $B_1 \subseteq B_2$ אז $\mathcal{P}^{-1}(B_1) \subseteq \mathcal{P}^{-1}(B_2)$, ולכן
$K_{B_1} = K(\mathcal{P}^{-1}(B_1)) \subseteq K(\mathcal{P}^{-1}(B_2)) = K_{B_2}$.

להיפך, נניח ש־$K_{B_1} \subseteq K_{B_2}$ ונראה כי $B_1 \subseteq B_2$. יהי $b \in B_1$. אז $K(\mathcal{P}^{-1}(b)) \subseteq K_{B_1} \subseteq K_{B_2}$. מכאן ש־$K(\mathcal{P}^{-1}(b))$ מוכלת בהרחבה נוצרת סופית של K שמוכלת ב־K_{B_2}, כלומר, $K(\mathcal{P}^{-1}(b)) \subseteq K(\mathcal{P}^{-1}(b_1), \dots, \mathcal{P}^{-1}(b_n))$, באשר $b_1, \dots, b_n \in B_2$. לכן, כדי להוכיח ש־$b \in B_2$, די להניח ש־$B/\mathcal{P}(K)$ חבורה אבלית נוצרת סופית. כיוון שכל איבר בה מסדר סופי (מחלק את p), זוהי חבורה אבלית סופית. תהי $B = \langle B_2, b \rangle$, אז גם $B/\mathcal{P}(K)$ סופית, $K_B = K_{B_2}$, ולכן, לפי משפט 21.6,

$$(B : \mathcal{P}(K)) = [K_B : K] = [K_{B_2} : K] = (B_2 : \mathcal{P}(K))$$

מכאן $B = B_2$, ולכן $b \in B_2$.

בכך הוכחנו שההעתקה $K_B \mapsto B$ היא חד חד ערכית. נראה שהיא על.

תהי L/K הרחבה אבלית בעלת מעריך p. תהי $B = \mathcal{P}(L) \cap K = \{\mathcal{P}(\beta) \in K \mid \beta \in L\}$. זוהי תת חבורה של K שמכילה את $\mathcal{P}(K)$. אם $b = \mathcal{P}(\beta) \in B$, אז $\beta \in L$, לכן $K_B \subseteq L$. להיפך, יהי $\alpha \in L$. יהי L_0 סגור גלואה של $K(\alpha)$ מעל K, אז $L_0 \subseteq L$ ו־L_0/K הרחבת גלואה סופית. די להראות ש־$L_0 \subseteq K_B$.

כיוון ש־$\mathrm{Gal}(L/K)$ חבורה אבלית בעלת מעריך p, גם המנה הסופית שלה $\mathrm{Gal}(L_0/K)$ היא חבורה אבלית בעלת מעריך p. כידוע, חבורה אבלית סופית היא מכפלה ישרה של חבורות מעגליות. לכן $\mathrm{Gal}(L_0/K) = \mathrm{Gal}(L_1/K) \times \cdots \times \mathrm{Gal}(L_n/K)$, באשר $K \subseteq L_1, \ldots, L_n \subseteq L_0 \subseteq L$ הרחבות מעגליות סופיות של K, (בלי הגבלת הכלליות לא טריביאליות) ו־$L_1 \cdots L_n = L_0$. לכן די להראות ש־$L_i \subseteq K_B$ לכל $1 \leq i \leq n$.

כל $\mathrm{Gal}(L_i/K)$ היא מנה של $\mathrm{Gal}(L_0/K)$, ולכן בעלת מעריך p. לכן היא מסדר p. לפי משפט ארטין־שרייר $L_i = K(\beta)$, באשר $b := \mathcal{P}(\beta) \in K$. מכאן $b \in B$ ולכן $\beta \in K_B$. בפרט $L_i \subseteq K_B$. ∎

תרגיל 22.10: *יהי K שדה ויהי $m \in \mathbb{N}$ זר ל־$\mathrm{char}\, K$. נניח ש־K מכיל שורש יחידה m־י פרימיטיבי. יהיו $a, b \in K^\times$. אז $K(a^{\frac{1}{m}}) \subseteq K(b^{\frac{1}{m}})$ אם ורק אם קיים $c \in K^\times$ ו־$0 \leq j < m$ כך ש־$a = b^j c^m$.*

הוכחה: ההרחבות $K(a^{\frac{1}{m}}), K(b^{\frac{1}{m}})$ מתאימות לתת חבורות $K^{\times m}\langle a\rangle, K^{\times m}\langle b\rangle$, בהתאמה. ההכלה מתרחשת אם ורק אם $K^{\times m}\langle a\rangle \leq K^{\times m}\langle b\rangle$. זה שקול ל־$a \in K^{\times m}\langle b\rangle$, כלומר, קיים $c \in K^\times$ ו־$b' \in \langle b\rangle$ כך ש־$a = b'c^m$. זה שקול לתנאי בתרגיל. ∎

23. נספח: מושגים אחדים מתורת הקבוצות.

תהי X קבוצה עי יחס סדר חלקי $\leq$ עליה. אם $x \leq y$, אומרים כי y *גדול או שווה ל־*x (או x *קטן או שווה ל־*y). נאמר כי y גדול מ־x (או x קטן מ־y) אם $x \leq y$, $x \neq y$.

הגדרה 23.1: איבר $x \in X$ נקרא

(א) **מרבי** (**מקסימלי**) אם אין איבר ב־X גדול ממנו, כלומר, אם כל $y \in X$ מקיים: אם $x \leq y$ אז $x = y$.

(ב) **מזערי** (**מינימימלי**) אם אין איבר ב־X קטן ממנו, כלומר, אם כל $y \in X$ מקיים: אם $y \leq x$ אז $y = x$.

(ג) **הגדול ביותר** אם הוא גדול או שווה מכל אברי X, כלומר, אם כל $y \in X$ מקיים $y \leq x$.

(ד) **הקטן ביותר** אם הוא קטן או שווה מכל אברי X, כלומר, אם כל $y \in X$ מקיים $x \leq y$. ∎

קיומם של איברים כאלה אינו מובטח.

יש לכל היותר איבר גדול ביותר אחד ב־X. אכן, אם $x, x' \in X$ גדולים ביותר, אז, בפרט $x \leq x'$ וגם $x' \leq x$, לכן $x = x'$. (לכן ה' הידיעה ב"הגדול".) באופן דומה יש לכל היותר איבר קטן ביותר אחד ב־X.

איבר גדול ביותר הוא בפרט מרבי (ואיבר קטן ביותר הוא בפרט מזערי) אך, באופן כללי, לא להיפך.

לעתים קרובות X היא משפחה של תת־קבוצות של קבוצה מסויימת. אז $\leq$ הוא יחס ההכלה $\subseteq$.

TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר

SCHOOL OF MATHEMATICAL SCIENCES בית הספר למדעי המתמטיקה

מבחן באלגברה ב' 2

0366.2133.01

לתלמידי דן הרן

ג' בתמוז, תשע"א

5 ביולי 2011

משך המבחן: 3 שעות.

אין להשתמש בחומר עזר כלשהו.

ענה על ארבע (בלבד) מתוך שש השאלות הבאות.

שאלה 1: יהי A חוג חילופי עם יחידה. יהי $f \in A[X_1,\dots,X_n]$ פולינום סימטרי. הוכח שקיים $g \in A[Y_1,\dots,Y_n]$ כך ש־$f = g(s_1,\dots,s_n)$, באשר $s_1,\dots,s_n$ הם הפולינומים הסימטריים היסודיים במשתנים $X_1,\dots,X_n$.

שאלה 2: יהי L שדה ותהי H חבורה סופית של אוטומורפיזמים של L. יהי $E = L^H$ שדה השבת של H ב־L. הוכח: L/E הרחבת גלואה סופית ו־$H = \mathrm{Gal}(L/E)$.

שאלה 3: בשאלה זו $\cong$ מסמן איזומורפיזם של שדות. הוכח או הפרך:

(א) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})$

(ב) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$

(ג) $\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[X]/(X^2-1)$

(ד) שדה הפיצול של X^2-2 מעל $\mathbb{Q}$ הינו ממעלה 2 מעל $\mathbb{Q}$.

(ה) שדה הפיצול של X^3-2 מעל $\mathbb{Q}$ הינו ממעלה 3 מעל $\mathbb{Q}$.

שאלה 4: תהי L/K הרחבה סופית ויהי $\alpha \in L$ כך ש־$[K(\alpha):K] = 2011$. הראה ש־$K(\alpha) = K(\alpha^6)$.

שאלה 5: יהי x איבר טרנסצנדנטי מעל שדה K ויהי $\alpha \in K(x) \setminus K$. הראה ש־$K(x)/K(\alpha)$ הרחבה אלגברית ו־α טרנסצנדנטי מעל K.

שאלה 6: יהי L שדה הפיצול של X^3-5 מעל $\mathbb{Q}$. הוכח או הפרך: $\sqrt{-1} \in L$.

בהצלחה!