אלגברה ב2

משה ירדן, אוניברסיטת תל אביב, תשס"ח

תכן העניָנים

הקדמה

הקורס ב"אלגברה ב2" ממשיך את הקורסים "אלגברה לינארית 1", "אלגברה לינארית 2" ו"אלגברה ב1" הנתנים בדרך כלל בשנת הלמודים הראשונה ובמחצית הראשונה של שנת הלִמודים השניה. המושג היסודי של ממד של מרחב וקטורי מ"אלגברה לינארית 1" מופיע ב "אלגברה ב2" כמעלה של הרחבת שדות. כדי לחקׂר עֲרכים עצמיים של העתקות לינאריות, לומדים ב "אלגברה לינארית 2" את התכונות הבסיסיות של פולינומים במשתנה אחד. בחלק הראשון "תורת השדות" של "אלגברה ב2" מעמיקים בנושא זה ומנצלים אותו לחֵקר הרחבות של שדות וּביחוד לחקר הרחבות אלגבריות. אנו מוכיחים שלכל שדה K יש סגוׂר אלגברי $\tilde{K}$ וסגוׂר זה יחיד עד כדי אוטומורפיזם-K. החלק השני של הקורס נקרא "תורת גלואה". הוא משלֵב את תורת השדות ותורת החבורות הנִלמדת ב"אלגברה ב1". על השגיהָ של תורת גלואה נמנים פתרונות של בעיות שכבר המתמטקאים הקדמונים התחבטו בהן. אנו נראה שאי אפשר ל"רבּעַ את העִגול" ואי אפשר לחלק זוית כללית לשלשה חלקים שוים בעזרת סרגל ומחֻגה. כמו כן נוכיח שאי אפשר לפתׂר משואה כללית ממעלה 5 ומעלה בעזרת ארבעת כללי החשבון והוצאות שׂרש. בנוסף לזה נציג את הבעיה ההפוכה של תורת גלואה על האפשרות לממוש כל החבורות הסופיות מעל $\mathbb{Q}$ ונפתׂר אותה עבור החבורות האבליות הסופיות ועבור החבורות הסימטריות.

משה ירדן

מבשרת ציון, חשון, תשס"ח

1. תורת השדות

אם K הוא שדה המוכל בשדה L, אפשר לראות את L כמרחב וקטורי מעל K. הממד של L כמרחב וקטורי נקרא "המעלה של ההרחבה L/K" ומסֻמן ב $[L:K]$. אנו נתעניֵן בעִקר במקרה שבו $[L:K]<\infty$. במקרה זה לכל $x\in L$ קיָם מספר טבעי n כך שהחֲזקות $1,x,\ldots,x^n$ תלויות לינארית מעל K. במלים אחרות, קיָמים $a_0,a_1,\ldots,a_n\in K$ שלא כֻּלם אפס כך ש $a_0+a_1x+\cdots+a_nx^n=0$, הוֶה אומֵר, x הִנו שֹרש של הפולינום $f(X)=a_nX^n+\cdots+a_1X+a_0$. אם n מזערי בעל תכונה זו, אזי $f(X)$ אי פריק בחוג $K[X]$. אם בנוסף לזה, $n=[L:K]$, אזי החזקות $1,x,\ldots,x^{n-1}$ מהוות בסיס ל L/K ולכן כל אבר של L נִתן להצגה כצרוף לינארי של חזקות אלו עם מקדמים ב K. במלים אחרות, L מתלכד עם החוג $K[x]$.

להפך, לכל פולינום אי פריק $f\in K[X]$ ממעלה n קיָם שדה L המקיף את K ממעלה n כך ש $L=K[x]$ ו x הוא שרש של f. יתר על כן, L יחיד עד כדי איזומורפיזם־K. אחד המשפטים המרכזיים שנוכיח בפרק זה אומר שאפשר להרחיב בניה זו ולבנות שדה $\tilde{K}$ שכל אבר שלו אלגברי מעל K ולכל פולינומם ממעלה חיובית מעל $\tilde{K}$ יש שרש ב $\tilde{K}$. שדה זה נקרא "הסגוֹר האלגברי של K".

מעל $\tilde{K}$, כל פולינום $f\in K[X]$ מתפרק למכפלה של גורמים לינאריים. בפרט, אם המקדם העליון של f שוה ל 1, מתפרק f בצורה $f(X)=\prod_{i=1}^n(X-x_i)$, באשר $x_1,\ldots,x_n$ הם השרשים של f. אם $x_1,\ldots,x_n$ שונים זה מזה, אומרים ש f פריד וכל אחד מהאברים $x_1,\ldots,x_n$ הִנו "פריד מעל K". משפט האבר הקדום אומר שאם כל אחד מהאברים של הרחבה ממעלה סופית L של K פריד, אזי קיָם $x\in L$ כך ש $L=K[x]$.

סוג אחר של הרחבות בעל חשיבות מרכזית בתורת השדות הוא "הרחבות נורמליות". אלו הן הרחבות L בעלות התכונה הבאה: אם לפולינום $f\in K[X]$ יש שרש ב L, אזי f מתפרק למכפלה של גורמים לינאריים מעל L. הרחבות L של K שהן גם פרידות וגם נורמליות נקראות "הרחבות גלואה". אלו יהוו את נשוא הדיון של הפרק השני.

1.1 תזכֹרות ותוספות על חוגים

בסעיף זה נזכיר מושגים ותוצאות בסיסיות מתורת החוגים החִלופיים המופיעים בְּרֻבּם בחוברת ההרצאות "אלגברה א" של פרופסור שמשון עמיצור בעריכת אורי לירון ובהוצאת אקדמון, ירושלים תשל"ב. הנחתנו היא שחֹמר זה נלמד כבר בקורס "אלגברה לינארית ו" ולכן נביא את התוצאות ללא הוכחות. תוצאה שאינה נלמדת בדרך כלל באותו הקורס והנסמכת על הלמה של צורן תובא כאן עם הוכחה.

חוגים ואידאלים.

חוג (חִלופי עם יחידה) הנו קבוצה R יחד עם שתי פְּעֻלות בינריות, חִבּור $(+)$ וכפל $(\cdot)$ ואברים מצֻיָּנים 0 ו 1 המקיְמים את התנאים הבאים:

(א1) $(R,+)$ מהוה חבורה חִלופית עם 0 כאבר האפס.

(א2) הכפל מקיֵם את תנאי החִלוף והצֵרוף ומתקיֵם $1\cdot x=x$ לכל $x\in R$.

(א3) מתקיֵם תנאי הפִלוג: $x(y+z)=xy+xz$.

לדֻגמה, קבוצת המספרים השלמים $\mathbb{Z}$ יחד עם החבור והכפל והאברים 0 ו 1 הרגילים מהוָה חוג.

אם לכל אבר שונה מאפס x של R קיָם הָפכי, כלומר אבר x' שעבורו $xx'=1$, אזי R הנו **שדה**.

העְתקה $\varphi\colon R\to S$ בין שני חוגים נקראת **הומומורפיזם** אם היא שומרת על החִבור והכפל וכן $\varphi(1)=1$. אם φ על, היא נקראת **אפימורפיזם** . אם φ חד חד ערכית, היא נקראת **מונומורפיזם** או גם **שִׁכּון** . לבסוף, אם φ חד חד ערכית ועל, היא נקראת **איזומורפיזם** .

תת קבוצה לא ריקה I של R מכֻנה **אידאל** אם היא סגורה תחת חִבור ותחת כפל באבר כלשהוא של R. המלים אחרות, אם $a\in I$ ו $x\in R$, אזי $xa\in I$. אומרים על האידאל I שהוא **נאות** אם אינו מתלכד עם R, לחִלופין $1\notin I$. כל קבוצה מהצורה $a+I=\{a+x\mid x\in I\}$ נקראת **מחלקה ימנית** לפי I. אֹסף המחלקות הימניות מסֻמן ב R/I. אפשר להפֹך אֹסף זה לחוג בעזרת ההגדרות הבאות:

$$(x+I)+(y+I)=(x+y)+I \qquad (x+I)(y+I)=xy+I$$

האפס של R/I מֻגדר כ I ואלו אבר היחידה הנו $1+I$. ההעתקה $\pi\colon R\to R/I$ המֻדרת **על ידי** $\pi(x)=x+I$ הנה אפימורפיזם של חוגים הנקרא **העְתקת המנה.** מההגדרה נובע ש $\pi(x)=0$ אם ורק אם $x\in I$.

לכל $x\in R$ הקבוצה $Rx=\{ax\mid a\in R\}$ היא אידאל של R הנקרא **האידאל הראשי הנוצר על ידי** x .

לדֻגמה, ממשפט החִלוק עם שארית נובע שכל אידאל של $\mathbb{Z}$ הוא ראשי.

להפך, אם $\varphi\colon R\to S$ הוא הומומרפיזם של חוגים, אזי $\mathrm{Ker}(\varphi)=\{x\in R\mid \varphi(x)=0\}$ הנו אידאל של R הנקרא **הגרעין של** φ. אם φ על, אזי φ משרה באֹפן טבעי איזומורפיזם $\bar\varphi\colon R/\mathrm{Ker}(\varphi)\to S$ כך ש $\varphi=\bar\varphi\circ\pi$, באשר $\pi\colon R\to R/\mathrm{Ker}(\varphi)$ הוא העתקת המנה. טענה זו נקראת **משפט האיזומורפיזם לחוגים.**

אידאל M של R מכֻנה **מרבי** אם M נאות ואם אין ל R שום אידאל נאות המקיף ממש את M. במקרה זה R/M הנו שדה. להפך, אם R/M שדה, אזי M מרבי.

תהי X תת קבוצה של R. האידאל **הנוצר על ידי** X הוא אסף כל הסכומים $\sum_{x\in X} a_x x$ שבהם a_x הם אברים של R שכמעט כֻלם אפס. הוא מסֻמן ב $\sum_{x\in X} Rx$. לדֻגמה, אם $p \in \mathbb{Z}$, אזי $p\mathbb{Z}$ מרבי אם ורק אם p ראשוני, ובמקרה זה $\mathbb{Z}/p\mathbb{Z}$ הנו שדה בין p אברים.

חוג (חלופי עם יחידה) R נקרא **תחם שלמות** אם מהשויון $xy = 0$ עבור אברים $x, y \in R$ נובע תמיד ש $x = 0$ או $y = 0$. במקרה זה קיָם שדה מזערי K המַקיף את R. שדה זה נקרא **שדה המנות** של R. כל אבר של K נִתן להצגה כמנה $\frac{x}{y}$ עם $x, y \in R$ ו $y \neq 0$. שויון מנות $\frac{x}{y} = \frac{x'}{y'}$ שקול לשויון $xy' = x'y$ של אברים של R. סכום ומכפלה של מנות מֻגדרים לפי הנֻסחאות הרגילות. לבסוף מזהים אבר x של R עם המנה $\frac{x}{1}$ ומשכנים בכך את R ב K. לדֻגמה, **שדה המספרים הרציונליים** $\mathbb{Q}$ הוא שדה המנות של $\mathbb{Z}$.

הלמה של צורן.

אחד מהכלים החזקים העומדים לרשותנו בתורת החוגים (והשדות) הוא הלמה של צורן. יחס בינרי $\leq$ על קבוצה X מכֻנה **יחס סֵדר חלקי** אם הוא מקיֵם את שלש הדרישות הבאות לכל $x, y, z \in X$.

(1ב) $x \leq x$.

(2ב) $x \leq y$ ו $y \leq x$ גורר ש $x = y$.

(3ב) $x \leq y$ ו $y \leq x$ גורר ש $x \leq z$.

במקרה זה נאמר שהזוג $(X, \leq)$ מהוה **קבוצה סדורה חלקית**. נאמר שאברים x, y של X **נִתנים להשואה** אם $x \leq y$ או $x \leq y$. תת קבוצה C של X תקרא **שרשרת** אם כל שני אברים של C נִתנים להשואה. אם $A \subseteq X$ ו $m \in X$ מקיֵם $a \leq m$ לכל $a \in A$, אזי m נקרא **חסם מלעיל של** A. אבר $\bar{x}$ של X נקרא **אבר מרבי** אם אין שום אבר של X הגדול ממש מ $\bar{x}$.

למה 1.1.1 (הלמה של צורן): *תהי $\langle X, \leq \rangle$ קבוצה סדורה חלקית לא ריקה. נניח שלכל שרשרת לא ריקה ב X יש חסם מלעיל. אזי יש ב X אבר מרבי.*

הוכחה: ראה סעיף 9 ברשימות הקורס "תורת הקבוצות". ∎

הרֵי השִמוש הראשון של הלמה.

למה 1.1.2: *לכל אידאל נאות I של חוג R קיָם אידאל מרבי M של R המַקיף את I.*

הוכחה: נסמן ב $\mathcal{J}$ את קבוצה כל האידאלים הנאותים של R המַקיפים את I. קבוצה זו אינה ריקה כי I שיָך אליה. יחס ההכלה הנו יחס סדר חלקי על $\mathcal{J}$. תהי $\mathcal{C}$ שרשרת ב $\mathcal{J}$ ויְהי J אחוד כל האידאלים השיָכים ל $\mathcal{C}$. אם $x, y \in J$ אזי x שיָך לאידאל J_1 השיָך ל $\mathcal{J}$ ו y שיָך לאידאל J_2 השיָך ל $\mathcal{J}$. לפי הגדרת השרשרת מוכל אחד משני האידאלים

J_1 ו J_2 באחר. נניח למשל ש $J_1 \subseteq J_2$. אזי $x, y \in J_2$ ולכן $x + y \in J_2$. מכאן ש $x + y \in J$. באֹפן דומה נובע ש $ax \in J$ לכל $a \in R$. לכן J הוא אידאל. הואיל ו 1 אינו שיָך לאף אחד מאברי $\mathcal{J}$, הוא גם אינו שיָך ל J. לבסוף $I \subseteq J$. לכן, J הנו חסם מלעיל של $\mathcal{J}$.

הלמה של צורן נותנת אבר מרבי M ב $\mathcal{J}$. אבר זה הנו אידאל מרבי של I המקיף את I. ∎

בסיסים של מרחבים וקטוריים.

בקורס באלגברה לינארית מוכיחים שלכל מרחב וקטורי נוצר סופית יש בסיס ומספר אברי הבסיס תלוי אך ורק במרחב. נכליל כאן עֻבדות אלו למרחבים וקטוריים כלליים.

משפט הבסיס: *יהי V מרחב וקטורי מעל שדה F.*

(א) *קים ל V בסיס B.*

(ב) *אם B_0 היא תת קבוצה של V שאינה תלויה לינארית, אזי נִתן לבחר את B כך שיקיף את B_0.*

(ג) *אם B' הוא בסיס נוסף של V, אזי $|B| = |B'|$.*

העצמה המשֻתפת של כל הבסיסים של V תקרא **הממד** *של V.*

הוכחת (א) ו (ב): מהלמה של צורן נובע שקיֶמת קבוצה לא תלויה לינארית מרבית B המקיפה את B_0. היא תהיה בסיס של V.

הוכחת (ג): האלגברה הלינארית הבסיסית מטפלת במקרה ש B סופית. לכן, נוכל להניח ש B ו B' אינסופיות. נרשם $B = \{v_i \mid i \in I\}$ ו $B' = \{u_j \mid j \in J\}$ כך ש $v_i \neq v_{i'}$ אם $i \neq i'$ ו $u_j \neq u_{j'}$ אם $j \neq j'$. בפרט, $|B| = |I|$ ו $|B'| = |J|$.

לכל $i \in I$ קיָמים $\alpha_{ij} \in F$ אשר כמעט כֻּלם אפס כך ש $v_i = \sum_{j \in J} \alpha_{ij} u_j$. הקבוצה $J_i = \{j \in J \mid \alpha_{ij} \neq 0\}$ סופית.

טענה: $J = \bigcup_{i \in I} J_i$. ואכן, יהי $j \in J$. אזי קיָמים $\beta_{ji} \in F$ שלא כֻּלם אפס כך ש $u_j = \sum_{i \in I} \beta_{ji} v_i$. לכן,

$$u_j = \sum_{i \in I} \beta_{ji} \sum_{k \in J} \alpha_{ik} u_k = \sum_{k \in J} \Big(\sum_{i \in I} \beta_{ji} \alpha_{ik} \Big) u_k$$

השואת המקדמים של u_j בשני האגפים נותנת $\sum_{i \in I} \beta_{ji} \alpha_{ij} = 1$. מכאן שקים $i \in I$ כך ש $\alpha_{ij} \neq 0$. לכן, $j \in J_i$.

מהטענה נובע ש $|B'| = |J| = |\bigcup_{i \in I} J_i| \le \aleph_0 \cdot |I| = |I| = |B|$. באפן סימטרי, $|B| \le |B'|$. לפי משפט קנטור־ברנשטיין, $|B| = |B'|$. ∎

פולינומים במשתנה אחד.

יהי R חוג ו X משתנה. נסמן ב $R[X]$ את **חוג הפולינומים ב X מעל R**. כל אבר שלו הוא סכום פורמלי $\sum_{i=0}^{\infty} a_i X^i$ שבו ה a_i־ים הם אברים של R שכמעט כֻּלם אפס והנקראים **מקדמֵי הפולינום**. פולינום נוסף $\sum_{i=0}^{\infty} b_i X^i$ **שוה לקודם** אם $a_i = b_i$ לכל i. הסכום והמכפלה של שני פולינומים מֻגדרים על ידי הנֻסחאות הבאות:

$$(\sum_{i=0}^{\infty} a_i X^i) + (\sum_{i=0}^{\infty} b_i X^i) = \sum_{i=0}^{\infty} (a_i + b_i) X^i \qquad (\sum_{i=0}^{\infty} a_i X^i)(\sum_{j=0}^{\infty} b_j X^j) = \sum_{k=0}^{\infty} \sum_{i+j=k} a_i b_j X^k$$

נשכן את R לתוך $R[X]$ על ידי שנתאים לכל אבר $a \in R$ את הפולינום $a + 0 \cdot X + 0 \cdot X^2 + \cdots$ (שיִקרא **פולינום קבוע**).

לכל אבר x של חוג S המקיף את R קיָם הומומורפיזם יחיד $\varphi\colon R \to S$ כך ש $\varphi(X) = x$ ו $\varphi(a) = a$ לכל $a \in R$. במקרה זה נאמר ש φ הנו **הומומורפיזם־**R.

המַעֲלה של פולינום $f(X) = \sum_{i=0}^{\infty} a_i X^i$ השונה מאפס הנה ה n המֵרבי שעבורו $a_n \neq 0$. במקרה זה נרשֹם $n = \deg(f)$ ו $f(X) = \sum_{i=0}^{n} a_i X^i$.

אם R הוא תחום שלמות (ובפרט, אם R הוא שדה), אזי $\deg(fg) = \deg(f) + \deg(g)$ לכל $f, g \in R[X]$.

משפט החִלוק עם שארית: *יהי K שדה ויהיו $f, g \in K[X]$ שני פולינומים כך ש $g \neq 0$. אזי קיָמים $g, r \in K[X]$ יחידים כך ש $f = qg + r$ ו $r = 0$ או $\deg(r) < \deg(g)$.*

הוכחה: נוכיח רק את הקִיום של g, r. יהיו

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \qquad a_n \neq 0$$
$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0 \qquad b_m \neq 0$$

אם $m < n$, נבחר $q = 0$ ו $r = f$. אחרת נסמן $f_1(X) = f(X) - \frac{a_n}{b_m} X^{n-m} g(X)$. אזי $\deg(f_1) < \deg(f)$. השראה (=אנדוקציה) על $\deg(f)$ נותנת $q_1, r \in K[X]$ כך ש

$$f_1(X) = q_1(X) g(X) + r(X)$$

ו $\deg(r) < \deg(g)$. לכן, $f(X) = \big(\frac{a_n}{b_m} X^{n-m} + q_1(X)\big) g(X) + r(X)$, כמבֻקש. ∎

המחלק המֵרבי המשֻׁתף של שני פולינומים שונים מאפס $f, g \in K[X]$ הנו פולינום d המחלק גם את f וגם את g כך שכל מחלק משֻׁתף של f ו g מחלק גם את d. פולינום זה נקבע באפן יחיד עד כדי כפל בקבוע שונה מאפס ומסֻמן ב $\gcd(f, g)$. בפרט, אם $\gcd(f, g) = 1$ אומרים ש f ו g **זרים זה לזה**.

המתכון של אוקלידס: *לכל שני פולינומים $f, g \in K[X]$ שונים מאפס יש ב $K[X]$ מחלק מְשֻׁתָּף מרבי. יתר על כן, קַיָּמִים $p, q \in K[X]$ כך ש $pf + qg = d$.*

הוכחה: בלי הגבלת הכלליות נניח ש $\deg(f) \geq \deg(g)$. נחלק את f ב g עם שארית כדי לקבל פולינומים $q, r \in K[X]$ כך ש $f = qg + r$ ו $\deg(r) < \deg(g)$. לכן, $\min(\deg(g), \deg(r)) < \min(\deg(f), \deg(g))$. הנחת השראה על המעלה הקטנה בין המעלות של שני הפולינומים נותנת מחלק מְשֻׁתָּף גדול ביותר d של g, r ופולינומים $p_1, q_1 \in K[X]$ כך ש $p_1 g + q_1 r = d$. לכן $q_1 f = q_1 qg + q_1 r = q_1 qg - p_1 g + d$. עתה נשים לב לכך ש $\gcd(f, g) = \gcd(g, r)$. בנוסף, $q_1 f + (p_1 - q_1 q)g = d$, כמבֻקש. ∎

פולינום $p \in K[X]$ מכֻנה **אי פריק** אם בכל פרוק $p = fg$ שלו, אחד משני הפולינומים f או g קבוע. לדֻגמה, כל פולינום ממעלה 1 הנו אי פריק. הפולינום p מכֻנה **ראשוני** אם מתוך $p|fg$ נובע ש $p|f$ או $p|g$. נאמר ששני פולינומים $f, g \in K[X]$ הם **חֲבֵרִים** אם קַיָּם $c \in K^\times$ כך ש $g = cf$.

משפט הפריקות החד ערכית: *יהי K שדה. אזי*

(א) *כל אידאל של $K[X]$ הוא **ראשי**, כלומר נוצר על ידי אבר אחד.*

(ב) *כל אבר אי פריק ב $K[X]$ הנו ראשוני.*

(ג) *$K[X]$ הוא **בעל פריקות חד ערכית**, כלומר כל אבר של החוג נִתן להצגה כמכפלה של פולינומים אי פריקים וההצגה היא יחידה עד כדי סדר הגורמים ועד כדי חברות.*

הוכחת א: יהי $\mathfrak{a}$ אידאל שונה מאפס ב $K[X]$. נבחר ב $\mathfrak{a}$ אבר g שונה מאפס בעל מעלה מזערית. משפט החִלוק עם שארית נותן לכל $f \in \mathfrak{a}$ פולינומים $q, r \in K[X]$ כך ש $f = qg + r$ ו $\deg(r) < 0$. אזי $r \in \mathfrak{a}$. מהמזעריות של מעֻלת g נובע ש $r = 0$. לכן, $f = qg$. מכאן נובע ש $\mathfrak{a} = K[X]g$, כפי שנטען.

הוכחת ב: יהי $p \in K[X]$ פולינום אי פריק ונניח ש f, g הם פולינומים כך ש $p|fg$. נניח בְשלילה ש $p \nmid f$ ו $p \nmid g$. הואיל ו p אי פריק, נובע מכאן ש $\gcd(p, f) = 1$ ו $\gcd(p, g) = 1$. המתכון של אוקלידס נותן אפוא $h_1, h_2, j_1, j_2 \in K[X]$ כך ש $h_1 p + j_1 f = 1$ ו $h_2 p + j_2 g = 1$. אם נכפיל את שני השויונות האלו, נקבל $h_1 h_2 p^2 + h_1 j_2 fp + h_2 j_1 fp + j_1 j_2 fg = 1$ ואגף שמאל מתחלק ב p בעוד שאגף ימין שוה ל 1. מסתירה זו אנו למֵדים ש $p|f$ או $p|g$.

הוכחת ג: כל פולינום ממעלה 1 הנו אי פריק. יהי $n > 1$ ונניח בהשראה שכל פולינום ממעלה קטנה מ n הנו מכפלה של פולינומים אי פריקים. יהי $f \in K[X]$ פולינום ממעלה n. אם f אי פריק, סִיַּמנו. אחרת, $f = gh$ באשר $\deg(g), \deg(h) < n$. לפי ההנחה, גם g וגם h הנם מכפלה של פולינומים אי פריקים. לכן גם f הנו מכפלה של פולינומים אי פריקים.

לבסוף, נניח ש $f = p_1 \cdots p_m$ ו $f = q_1 \cdots q_n$ הן הצגות של פולינום f כמכפלה של פולינומים אי פריקים. אזי, $p_1 \cdots p_m = q_1 \cdots q_n$. השראה על m מוכיחה לפי (א) ש p_1 מחלק את אחד מהגורמים באגף ימין. אם נפעיל עליהם תמורה מתאימה, נוכל להניח בלי הגבלת הכלליות ש $p_1|q_1$. הואיל ו q_1 אי פריק, נובע שקיָם $c \in K^\times$ כך ש $q_1 = cp_1$. צמצום ב p_1 והכפלת q_2 ב c נותנת את השויון $p_2 \cdots p_m = q_2 \cdots q_n$. השראה על m מוכיחה ש $m = n$ ושלאחר תמורה מתאימה של הגורמים באגף ימין, p_i הנו חבר של q_i עבור $i = 2, \ldots, n$.

הוכחנו אפוא שהפרוק של פולינום למכפלה של גורמים אי פריקים הנו חד ערכי. ∎

הבֿחן הבא שִמושי לְבדיקת אי פריקות של פולינומים מעל $\mathbb{Z}$ ומעל $K[X]$. בצרוף עם הלמה של גאוס, נִתן לבדֹק בעזרתו במקרים רבים פריקות של פולינומים מעל $\mathbb{Q}$ ומעל $K(X)$.

משפטון 1.1.3 (הבֿחן של Eisenstein): *יהיו R חוג בעל פריקות חד ערכית, $f(X) = \sum_{i=0}^n a_i X^i$ פולינום מעל R ו p אבר אי פריק של R. נניח ש $p \nmid a_n$, $p|a_i$ לכל $0 \le i \le n-1$ ו $p^2 \nmid a_0$. אזי $f(X)$ אי פריק ב $R[X]$.*

הוכחה: נניח בשלילה שקיָם פרוק

$$\sum_{k=0}^n a_k X^k = \sum_{i=0}^d b_i X^i \sum_{j=0}^e c_j X^j$$

עם $1 \le d, e \le n-1$ ו $b_i, c_j \in R$. אזי $a_k = \sum_{i+j=k} b_i c_j$ לכל k. בפרט, $a_0 = b_0 c_0$ ו $a_n = b_d c_e$. מהשויון האחרון נובע ש $p \nmid b_d$ ו $p \nmid c_e$. יהי l המספר הקטן ביותר כך ש $p \nmid b_l$ ויהי m המספר הקטן ביותר כך ש $p \nmid c_m$. לא יתכן ש $l + m = n$, אחרת $p|b_i$ לכל $i < l$ ו $p|c_j$ לכל $j < m$. בפרט, $p|b_0$ ו $p|c_0$ (כאן אנו משתמשים בכך ש $0 < d, e$) ולכן $p^2 | b_0 c_0 = a_0$, בסתירה להנחה.

נרשֹם את a_{l+m} בצורה הבאה:

$$a_{l+m} = b_l c_m + \sum_{\substack{i+j=l+m \\ (i,j) \ne (l,m)}} b_i c_j$$

אזי $p|a_{l+m}$ ו $p \nmid |b_l c_m$. אולם אם $i + j = l + m$ ו $(i,j) \ne (l,m)$ אזי $i < l$ או $j < m$ ולכן $p|b_i$ או $p|c_j$. בכל אחד משני המקרים $p|b_i c_j$. סתירה זו מוכיחה ש f אינו פריק. ∎

תרגיל 1.1.4: יהי p מספר ראשוני. הוכח שהפולינום $X^{p-1} + X^{p-2} + \cdots + 1$ אי פריק מעל $\mathbb{Q}$. ∎

תרגיל 1.1.5: לכל מספר טבעי n תן דֻגמה לפולינום אי פריק $f \in \mathbb{Q}[X]$ ממעלה n. ∎

תרגיל 1.1.6: הוכח שאם a הוא מספר שלם ו n מספר טבעי כך ש $a \ne b^n$ לכל $b \in \mathbb{Z}$, אזי $\sqrt[n]{a}$ הוא מספר אי רציונלי. ∎

תרגיל 1.1.7: יהי K שדה. תן דֻגמה לפולינום אי פריק ממעלה n מעל $K(X)$. ∎

יהי $f(X) = \sum_{i=0}^{n} a_i X^i$ פולינום עם מקדמים בחוג R בעל פריקות חד ערכית. למחלק המשֻתף המרבי של $a_0, \ldots, a_n$ קוראים **התכן של** f ומסמנים אותו ב $\mathrm{cont}(f)$. אם $\mathrm{cont}(f) = 1$, אומרים ש f **קדום**.

משפטון 1.1.8 (הלמה של גאוס [עמיצור, עמוד 223]): *יהי R חוג בעל פריקות חד ערכית ויהיו $f, g \in R[X]$. אזי $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$. בפרט, אם f ו g קדומים, גם fg קדום.*

הוכחה: *נחלק את f ו g בתכנים שלהם כדי להניח ש f ו g קדומים. יהיו אפוא $f(X) = \sum_{i=0}^{m} a_i X^i$, $g(X) = \sum_{j=0}^{n} b_j X^j$ ו $f(X)g(X) = \sum_{k=0}^{mn} c_k X^k$. אזי $c_k = \sum_{i+j=k} a_i b_j$ לכל k.*

יהי p אבר אי פריק של R. הואיל ו f קדום, קיָם $0 \le r \le m-1$ כך ש $p | a_{r+1}, \ldots, a_m$ ו $p \nmid a_r$. הואיל ו g קדום, קיָם $0 \le s \le n-1$ כך ש $p | b_{s+1}, \ldots, b_n$ ו $p \nmid b_s$. נתבונן ב

$$c_{r+s} = a_r b_s + \sum_{\substack{i+j=r+s \\ (i,j)\neq(r,s)}} a_i b_j$$

לפי ההנחה $p \nmid a_r b_s$. אם $i+j = r+s$ ו $(i,j) \neq (r,s)$, אזי $i \ge r+1$ או $j \ge s+1$. לכן, $p|a_i$ או $p|b_j$. בכל מקרה, $p|a_i b_j$. מכאן נובע ש $p \nmid c_{r+s}$. לכן, fg קדום. ∎

תוצאה 1.1.9: *יהי R חוג בעל פריקות חד ערכית ויהי $f \in R[X]$ פולינום אייזנשטיין. אזי f אי פריק בחוג $K[X]$.*

הוכחה: נניח בשלילה ש $f = gh$ באשר $g, h \in K[X]$ ו $1 \le \deg(g), \deg(h) < \deg(f)$. אם נוציא את המכנה המשֻתף המרבי של מקדמי g ו h החוצה ואת המחלק המשֻתף של שני הפולינומים שיתקבלו באפן כזה, נקבל פולינומים קדומים $g_1, h_1 \in R[X]$ ואברים $a, b \in R$ שונים מאפס כך ש $bf = ag_1h_1$. מהלמה של גאוס נובע ש $a = ub$ באשר u אבר הפיך של R. לכן, $f = ug_1h_1$, בסתירה לבֹחן אייזנשטיין. ∎

תוצאה 1.1.10: *אם R הוא חוג בעל פריקות חד ערכית, גם $R[X]$ הוא בעל פריקות חד ערכית. בפרט, אם $f \in R[X]$ הוא פולינום קדום ו $f = f_1 \cdots f_m$ הוא פרוק למכפלה של גורמים אי פריקים ב $R[X]$, אזי זהו גם פרוק למכפלה של גורמים אי פריקים ב $K[X]$.*

פולינומים בכמה משתנים.

יהי R חוג. פולינום במשתנים $X_1, \ldots, X_n$ עם מקדמים ב R הנו בִטוי פורמלי $\sum_{\mathbf{i}} a_{\mathbf{i}} X_1^{i_1} \cdots X_n^{i_n}$ שבו $\mathbf{i} = (i_1, \ldots, i_n)$ עובר על כל ה n־יות של מספרים שלמים אי שליליים והמקדמים $a_{\mathbf{i}}$ הם אברים של R שכמעט כֻלם אפס. סכום וכפל של פולינומים כאלו מֻגדר על ידי הנֻסחאות הבאות:

$$\sum_{\mathbf{i}} a_{\mathbf{i}} X_1^{i_1} \cdots X_n^{i_n} + \sum_{\mathbf{i}} b_{\mathbf{i}} X_1^{i_1} \cdots X_n^{i_n} = \sum_{\mathbf{i}} (a_{\mathbf{i}} + b_{\mathbf{i}}) X_1^{i_1} \cdots X_n^{i_n}$$

$$\sum_{\mathbf{i}} a_{\mathbf{i}} X_1^{i_1} \cdots X_n^{i_n} + \sum_{\mathbf{j}} b_{\mathbf{j}} X_1^{j_1} \cdots X_n^{j_n} = \sum_{\mathbf{k}} \Big(\sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} a_{\mathbf{i}} b_{\mathbf{j}} \Big) X_1^{k_1} \cdots X_n^{k_n}$$

נְסחאות אלו הופכות את אסף כל הפולינומים האלו לחוג המסֻמן ב $R[X_1,\dots,X_n]$.

נזהה את הפולינום $\sum_{\mathbf{i}} a_{\mathbf{i}} X_1^{i_1}\cdots X_n^{i_n}$ עם הפולינום $\sum_{\mathbf{i}} a_{\mathbf{i}} X_1^{i_1}\cdots X_n^{i_n} X_{n+1}^{i_{n+1}}$ שבו $\mathbf{i}=(i_1,\dots,i_n,i_{n+1})$ הוא $(n+1)$־יה של מספרים שלמים אי שליליים המקיֶמת $i_{n+1}=0$. זִהוי זה מאפשר לנו להתבונן גם בחוגי פולינומים $S=R[X_i \mid i\in I]$ בקבוצה $\{X_i \mid i\in I\}$ כלשהיא של משתנים. כל אבר של S הוא פולינום במספר סופי של משתנים מתוך הקבוצה עם מקדמים ב R. אם A הוא חוג המקיף את R ו $\{x_i \mid i\in I\}$ היא תת קבוצה של A, אזי קיָם הומומורפיזם־R יחיד $\varphi\colon S\to A$ המקיֵם $\varphi(X_i)=x_i$ לכל $i\in I$.

התוצאה הבאה נובעת מתוצאה 1.1.10 בהשראה על n.

משפטון 1.1.11: *לכל שדה K ולכל n יש לחוג $K[X_1,\dots,X_n]$ פריקות חד ערכית.*

1.2 שדה רִאשוני

אנו מתחילים בהגדרות השדה, איזומורפיזם של שדות, שדות ראשוניים ואפיון של שדות. כמו כן מוצאים אנו שהשדות הראשוניים הִנם $\mathbb{Q}$ או $\mathbb{F}_p$.

הגדרה 1.2.1: **שדה** הנו קבוצה K יחד עם פעֻלות חִבור וכפל ושני אברים מצֻינים שונים זה מזה 0 ו 1 המקיְמים את התנאים הבאים:

(וא) K הנו חבורה חִלופית ביחס לחִבור ואבר האפס 0.

(וב) הקבוצה $K^\times = K \smallsetminus \{0\}$ הנו חבורה חִלופית ביחס לכפל והאבר היחידה 1.

(וג) חֹק הפִלוג $x(y+z) = xy + xz$ מתקיֵם לכל $x, y, z \in F$.

דֻגמאות לשדות הן שדה המספרים הרציונליים $\mathbb{Q}$, שדה המספרים הממשיים $\mathbb{R}$, שדה המספרים המרֻכבים $\mathbb{C}$ והשדה בעל p אברים $\mathbb{F}_p$.

השדה האחרון שוה לחוג המנה $\mathbb{Z}/p\mathbb{Z}$ שאבריו הם המחלקות הימניות $a + p\mathbb{Z}$ עם $a \in \mathbb{Z}$. משפט החלוק עם שארית מאפשר להציג כל מספר שלם n באפן יחיד בצורה $n = ap + b$ באשר $a \in \mathbb{Z}$ ו $0 \le b \le p-1$. לכן מֻרכב $\mathbb{Z}/p\mathbb{Z}$ בדיוק מ p האברים $0 + p\mathbb{Z}, 1 + p\mathbb{Z}, \ldots, (p-1) + p\mathbb{Z}$. אם $(a + p\mathbb{Z})(b + p\mathbb{Z}) = 0 + p\mathbb{Z}$, אזי $p|ab$ ולכן אחד משני הגורמים שוה לאפס. מכאן ש $\mathbb{Z}/p\mathbb{Z}$ הוא תחום שלמות. אם x הוא אבר שונה מאפס של $\mathbb{Z}/p\mathbb{Z}$, אזי כפל ב x נותן העתקה חד חד ערכית של $\mathbb{Z}/p\mathbb{Z}$ לתוך עצמו. הואיל והחוג $\mathbb{Z}/p\mathbb{Z}$ סופי, העתקה זו הנה על. בפרט קיָם $y \in \mathbb{Z}/p\mathbb{Z}$ כך ש $xy = 1 + p\mathbb{Z}$. מכאן ש $\mathbb{Z}/p\mathbb{Z}$ הנו שדה המסֻמן גם ב $\mathbb{F}_p$. ∎

הגדרה 1.2.2: **איזומורפיזם** $\alpha\colon K \to K'$ של שדות הנו העתקה חד חד ערכית ועל המקיֶמת $\alpha(x + y) = \alpha(x) + \alpha(y)$ ו $\alpha(xy) = \alpha(x)\alpha(y)$.

אם קיָם איזומורפיזם בין שני שדות K ו K' נאמר שהם **איזומורפיים** זה לזה ונסמן $K \cong K'$. ∎

תרגיל 1.2.3:

(א) הוכח שכל תחום שלמות סופי הנו שדה.

(ב) הוכח שאם F הוא שדה בן p אברים ו p ראשוני, אזי קיָם איזומורפיזם יחיד $\alpha\colon F \to \mathbb{F}_p$. ∎

הגדרה 1.2.4: תת קבוצה K_1 של שדה K_2 תִקרֵא **תת שדה** אם היא מהוָה שדה תחת פעֻלות החִבור והכפל של K_2, כלומר K_1 סגור תחת פעֻלות החִבור, החִסור, הכפל והחִלוק. במקרה זה אומרים ש K_2 הנה **הרחבה** של K_1.

לדֻגמה, $\mathbb{R}$ הנו הרחבה של $\mathbb{Q}$ ו $\mathbb{C}$ הנה הרחבה של $\mathbb{R}$.

אנו מסמנים ב $K[X]$ את חוג הפולינומים במשתנה X עם מקדמים ב K וב $K(X)$ את שדה המנות שלו הנקרא גם **שדה הפונקציות הרציונליות מעל** K:

$$K(X) = \left\{ \frac{f(X)}{g(X)} \mid \ f, g \in K[X],\ g \neq 0 \right\}$$

אם L, L' הן שתי הרחבות של שדה K ו $\alpha\colon L \to L'$ הוא איזומורפיזם המקיֵם $\alpha(a) = a$ לכל $a \in K$, אומרים ש α הנו **איזומורפיזם־**K ומסמנים $L \cong_K L'$.

איזומורפיזם־K של L על עצמו נקרא גם **אוטומורפיזם־**K ∎

הערה 1.2.5: שדה ראשוני. אם $\{K_i \mid i \in I\}$ הנו אֹסף של תת שדות של שדה K אזי גם חתוכם $\bigcap_{i\in I} K_i$ הנו תת שדה של K. בפרט החתוך של כל תת השדות של K הנו שדה F. נקרא לו **השדה הראשוני** של K.

כדי לקבֹע את F נחזֹר ונסמן ב $\bar{0}$ וב $\bar{1}$ את אברי האפס והאחד של K. לכל n טבעי נסמן ב $\bar{n}$ את הסכום של n פעמים $\bar{1}$. אזי ההעתקה $\alpha\colon \mathbb{Z} \to K$ המֻגדרת על ידי $\alpha(n) = \bar{n}$ ו $\alpha(-n) = -\bar{n}$ לכל $n \geq 0$ הנה הומומורפיזם של חוגים (כלומר שומרת על החבור, החסור והכפל) ו $\alpha(\mathbb{Z}) = \{\bar{n} \mid n \in \mathbb{Z}\}$ הנו תחום שלמות המוכל ב F. נבדיל בין שני מקרים.

מקרה א: *$\bar{n} \neq 0$ לכל n טבעי.* במקרה זה $\alpha(\mathbb{Z})$ איזומורפי ל $\mathbb{Z}$. לכן, האֹסף $\bar{\mathbb{Q}} = \{\frac{\bar{m}}{\bar{n}} \mid m, n \in \mathbb{Z},\ n \neq 0\}$ מהוה תת שדה של F האיזומורפי ל $\mathbb{Q}$. מהגדרת F כתת השדה המזערי של K נובע ש $F = \bar{\mathbb{Q}}$. נוכל אפוא לזהות במקרה זה כל מספר שלם n אם תמונתו $\bar{n}$ ב $\bar{\mathbb{Q}}$ ולזהות את $\mathbb{Q}$ עם $\bar{\mathbb{Q}}$. תחת זִהוי זה מהוֶה $\mathbb{Q}$ את השדה הראשוני של K. במקרה זה נאמר **שהאִפיון** של K הנו 0 ונסמן $\mathrm{char}(K) = 0$.

מקרה ב: *קיָם n טבעי כך ש $\bar{n} = 0$.* נסמן ב p את המספר הטבעי הקטן ביותר המקיֵם $\bar{p} = 0$. מספר זה הנו ראשוני. אחרת היו קיָמים מספרים טבעיים $1 < a, b < p$ כך ש $\bar{a}\bar{b} = 0$. הואיל ו F הנו שדה מתקיֵם $\bar{a} = 0$ או $\bar{b} = 0$, בסתירה להגדרת p.

משפט החִלוק עם שארית מאפשר לנו להציג כל מספר שלם n באפן יחיד בצורה $n = ap + b$, באשר $a, b \in \mathbb{Z}$ ו $0 \leq b \leq p-1$. לכן, $\alpha(\mathbb{Z}) = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ הוא תחום שלמות סופי המוכל ב F ו $\mathrm{Ker}(\alpha) = p\mathbb{Z}$. מכאן ש $\alpha(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. מהמזעריות של F נובע ש $F = \mathbb{F}_p$.

במקרה זה נאמר שהאִפיון של K הנו p ונסמן $\mathrm{char}(K) = p$. כמו כן נרשֹם את $\bar{n}$ בתור n לכל n טבעי ונזכֹר שבאפיון p אבר זה הנו הסכום של n פעמים אבר היחידה של $\mathbb{F}_p$. ∎

תרגיל 1.2.6: הוכח שאם $p = \mathrm{char}(K) > 0$, אזי ההעתקה $x \mapsto x^p$ מהוָה איזומורפיזם של K לתוך עצמו.
רמז: השתמש בנֻסחת הבינום של ניוטון. ∎

1.3 הרחבות של שדות

הרחבות של שדות ממֻיָּנות לשני סוגים, אלגבריות ונעלות. אנו מראים פה שהרחבה אלגברית של שדה K הנוצרת על ידי אבר אחד היא למעשה חוג הפולינומים $K[x]$ באבר x שהוא שֹׁרש של פולינום אי פריק $f \in K[X]$. הרחבה זו נקבעת עד כדי איזומורפיזם־K על ידי הפולינום. להפך, נראה פה שלכל פולינום אי פריק $f \in K[X]$ קיָם שרש בהרחבה של K.

הערה 1.3.1: תהי L/K הרחבה של שדות ו S תת קבוצה של L. נסמן את החִתוך של כל תת השדות של L המַקיפים את $K \cup S$ ב $K(S)$ ונקרא לו **השדה הנוצר על ידי** S **מעל** K. שדה זה אינו אלא קבוצת כל הבִטויים מהצורה

$$\frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)}$$

שבהם f, g הם פולינומים עם מקדמים ב K ב n נעלמים, $s_1, \ldots, s_n \in S$ והמכנה שונה מאפס. אם $S = \{x_1, \ldots, x_n\}$ היא קבוצה בת n אברים, נסמן גם $K(x_1, \ldots, x_n)$ במקום $K(S)$ ונאמר ש $K(S)$ **נוצר סופית מעל** K. במקרה זה

$$K(x_1, \ldots, x_n) = \Big\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \mid\ f, g \in K[X_1, \ldots, X_n],\ g(x_1, \ldots, x_n) \neq 0 \Big\}$$

במקרה ש ו $S = \{x\}$ בעלת אבר אחד נקבל את השדה

$$K(x) = \Big\{ \frac{f(x)}{g(x)} \mid\ f, g \in K[X],\ g \neq 0 \Big\}$$

דֻגמאות להרחבות הנוצרות על ידי מספר סופי של אברים הם $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\pi)$ ו $\mathbb{C} = \mathbb{R}(\sqrt{-1})$.

יהי $x \in L$. נאמר ש x **אלגברי מעל** K אם קיָם פולינום $f \in K[X]$ שונה מאפס כך ש $f(x) = 0$, אחרת נאמר ש x **נַעֲלה מעל** K.

אם כל אברי הרחבה L של שדה K אלגבריים מעל K, נאמר ש L **אלגברית** מעל K, אחרת נאמר ש L **נעלָה** מעל K. ∎

המשפטון הבא אומר שכל ההרחבות של שדה K הנוצרות על ידי אבר נעלה אחד איזומורפיות־K לשדה $K(X)$.

משפטון 1.3.2: *יהי K שדה ו X משתנה.*

(א) *שדה הפונקציות הרציונליות $K(X)$ הנו הרחבה של K ו X נעלה מעל K.*

(ב) *אם אברים x,y של שדות הרחבה של K נעֲלים מעל K, אזי ההעתקה*

$$\frac{f(x)}{g(x)} \mapsto \frac{f(y)}{g(y)}$$

עבור $f,g \in K[X]$ ו $g \neq 0$ הִנה איזומורפיזם־K של $K(x)$ על $K(y)$.

לעומת זאת יתכנו לשדה K הרחבות אלגבריות הנוצרות על ידי אבר אחד שאינן איזומורפיות־K זו לזו.

משפטון 1.3.3: *יהי $x \neq 0$ אבר אלגברי מעל שדה K ויהי $f \in K[X]$ פולינום שונה מאפס בעל מעלה מזערית המקיֵם $f(x) = 0$. אזי:*

(א) *f אי פריק ב $K[X]$.*

(ב) *אם $0 \neq g \in K[X]$ ו $g(x) = 0$, אזי $f|g$.*

(ג) *קיָם ב $K[X]$ פולינום אי פריק* **מתֻקן** *(כלומר המקדם העליון שלו שוה ל 1) יחיד בעל שֹרש x. נקרא לו* **הפולינום האי פריק** *של x ונסמן אותו ב $\mathrm{irr}(x,K)$.*

(ד) *ההעתקה $g(X) \to g(x)$ משרה איזומורפיזם־K של חוג המנה $K[X]/f(X)K[X]$ על $K(x)$.*

(ה) *כל אבר של $K(x)$ נִתן להצגה יחידה בצורה $g(x)$, באשר $g \in K[X]$ הוא פולינום ממעלה קטנה מ $\deg(f)$. בפרט נקבל שהחוג $K[x]$ מתלכד עם השדה $K(x)$.*

הוכחה א: לפי ההנחה קיָם פולינום שונה מאפס ב $K[X]$ בעל שֹרש x. לכן קיָם גם פולינום f כזה בעל מעלה מזערית. מההנחה ש $x \neq 0$ נובע ש f אינו קבוע, כלומר $\deg(f) \geq 1$.

נניח בשלילה ש $f = gh$ הנו פרוק לא טריביאלי של f, כלומר $g,h \in K[X]$ ו

$$1 \leq \deg(g), \deg(h) < \deg(f).$$

הצבה של x בשִויון האחרון נותנת $0 = f(x) = g(x)h(x)$ ולכן, $g(x) = 0$ או $h(x) = 0$. בכל אחד מהמקרים מקבלים סתירה למִזעריות של $\deg(f)$.

הוכחת ב: נחלק את g ב f עם שארית כדי לקבל $q,r \in K[X]$ כך ש $g = qf + r$ ו $\deg(r) < \deg(f)$. הצבה של x בשויון האחרון נותנת $g(x) = q(x)f(x) + r(x)$ ולכן $r(x) = 0$. מהמזעריות של $\deg(f)$ נובע ש $r = 0$ ולכן $g = qf$, כלומר $f|g$, כנדרש.

הוכחת ג: נחלק את f במקדם העליון שלו כדי להניח בלי הגבלת הכלליות ש f מתֻקן. אם g הנו פולינום מתֻקן נוסף בעל מעלה מזערית המקיֵם $g(x) = 0$, אזי לפי (ב) f ו g מחלקים זה את זה ולכן שוים זה לזה.

הוכחת ד: ההצבה של x במקום X נותנת הומומורפיזם $\alpha\colon K[X] \to K(x)$ שתמונתו היא החוג $K[x]$. מ (ב) נובע ש $\mathrm{Ker}(\alpha) = f(X)K[X]$. לכן, $K[X]/f(X)K[X] \cong_K K[x]$. אם $0 \neq u \in K[x]$, אזי קיָם

$g \in K[X]$ כך ש $g(x) = u$. בפרט, g אינו מתחלק ב f. הואיל ו f אי פריק, f זר ל g. המתכון של אוקלידס נותן אפוא $f', g' \in K[X]$ כך ש $ff' + gg' = 1$ הַצבה של x בשויון זה נותנת $g(x)g'(x) = 1$, כלומר u הפיך ב $K[x]$. מכאן נובע ש $K[x]$ הוא שדה. הואיל ו $K(x)$ הנו שדה המנות של $K[x]$ נקבל מכאן ש $K[x] = K(x)$ הוא שדה.

הוכחת ה: אם $h \in K[X]$, אזי קַיָמים $q, g \in K[X]$ כך ש $h = qf + g$ ו $\deg(g) < \deg(f)$. הצבה של x בשויון האחרון נותנת ש $h(x) = g(x)$, כמבֻקש. טענתנו נובעת עתה מהשויון $K(x) = K[x]$. ∎

המשפטון הבא מוכיח שהשדה $K(x)$ המופיע במשפטון 1.3.2 נקבע עד כדי איזומורפיזם־K על ידי $\mathrm{irr}(x, K)$.

משפטון 1.3.4: *יהי $\alpha\colon K \to K'$ איזומורפיזם של שדות. נרחיב את α לאיזומורפיזם $': K[X] \to K'[X]$ של חוגי הפולינומים בעזרת ההגדרה $(\sum a_i X^i)' = \sum \alpha(a_i) X^i$. יהי $f \in K[X]$ פולינום אי פריק. אזי $f' \in K'[X]$ הוא פולינום אי פריק ו $\deg(f) = \deg(f')$. יתר על כן, אם x ו x' הם שָרשים של f ו f', אזי ההעתקה $g(x) \mapsto g'(x')$ הנה איזומורפיזם של $K(x)$ על $K'(x')$ המרחיב את α. יתר על כן, זוהי ההרחבה היחידה של α לאיזומורפיזם $K(x) \cong K'(x')$ המעתיקה את x על x'.*

הוכחה: האיזומורפיזם $': K[X] \to K'[X]$ מעתיק את $f(X)$ על $f'(X)$ ולכן את האידאל המרבי $f(X)K[X]$ של $K[X]$ על האידאל המרבי $f'(X)K'[X]$ של $K'[X]$. משפט האיזומורפיזם הראשון של חוגים נותן איזומורפיזם־K של חוגי המנה $K[X]/f(X)K[X] \cong K'[X]/f'(X)K'[X]$. משפטון 1.3.2 מתרגם איזומורפיזם זה לאיזומורפיזם $K(x) \to K'(x')$ המרחיב את α ומעתיק את x על x'.

$$
\begin{tikzcd}
0 \arrow[r] & f(X)K[X] \arrow[r] \arrow[d] & K[X] \arrow[r] \arrow[d] & K(x) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & f'(X)K[X] \arrow[r] & K'[X] \arrow[r] & K'(x) \arrow[r] & 0
\end{tikzcd}
$$

לחִלופין נשים לב לכך שההעתקה $\beta\colon K[x] \to K'[x']$ המֻגדרת על ידי $\beta(g(x)) = g'(x')$ הנה הומומרפיזם המֻגדר היטב. ואכן, אם $g_1(x) = g_2(x)$, אזי לפי משפטון 1.3.2(ב), $f|(g_1 - g_2)$. לכן, $f'|(g_1' - g_2')$ ולכן $g_1'(x') = g_2'(x')$. הגרעין של β שוה לאפס, כי אם $g'(x') = 0$ אזי $f'|g'$ ולכן $f|g$ ולכן $g(x) = 0$. מכאן ש β הוא איזומורפיזם. טענתנו נובעת עתה מהזהוי $K(x) = K[x]$ ו $K'(x') = K'[x']$ (משפטון 1.3.2(ה)). ∎

המקרה הפרטי של משפטון 1.3.4 שבו $K = K'$ ו $\alpha = \mathrm{id}_K$ נותן לנו משפט יחידות להרחבה האלגברית $K(x)$:

תוצאה 1.3.5: *יהיו K שדה, $f \in K[X]$ פולינום אי פריק, ו x, x' שָׁרשים של f בשדות הרחבה של K. אזי קַיָם איזומורפיזם־K יחיד של $K(x)$ על $K(x')$ המעתיק את x על x'.*

לאחר משפטי היחידות להרחבות אלגבריות נוכיח משפט קִיום.

משפטון 1.3.6: *יהי K שדה ו $f \in K[X]$ פולינום אי פריק. אזי קֶיֶמֶת ל K הרחבה L שבה יש ל f שֹׁרֶש.*

הוכחה: כפי שהזכרנו לעיל, האידאל $f(X)K[X]$ של החוג הראשי $K[X]$ הוא מרבי ולכן חוג המנה $L = K[X]/f(X)K[X]$ הוא שדה. נשכן את K לתוך L על ידי שנזהה אבר a של K עם המחלקה $a + f(X)K[X]$. האבר $x = X + f(X)K[X]$ מקיֵם

$$f(x) = f(X + f(X)K[X]) = f(X) + f(X)K[X] = 0,$$

כנדרש. ∎

לשדה $K(x)$ שבנינו במשפטון 1.3.6 נקרא **שְׂדֵה שֹׁרֶש** של f מעל K.

1.4 מעלת הרחבה

אם L/K הנה הרחבה של שדות, אפשר לראות את L כמרחב וקטורי מעל K. לממד של מרחב זה נקרא **המעלה של L מעל K** ונסמנו ב $[L:K]$. מספר זה הנו מספר טבעי, או מספר מונה אינסופי. במקרה השני נסמן גם $[L:K]=\infty$.

משפטון 1.4.1: *יהיו K שדה ו x אבר בשדה הרחבה של K.*

(א) *אם x נעלה מעל K, אזי $[K(x):K]=\infty$.*

(ב) *אם x אלגברי מעל K ו $n=\deg(\mathrm{irr}(x,K))$, אזי $[K(x):K]=n$. יתר על כן, $1,x,\ldots,x^{n-1}$ הוא בסיס של L מעל K.*

הוכחת א: במקרה זה החזקות $1,x,x^2,x^3,\ldots$ של x אינן תלויות אלגברית מעל K. לכן, $[K(x):K]=\infty$.

הוכחת ב: חלק (ה) של משפטון 1.3.3 אומר שכל אבר של $K(x)$ נתן להצגה יחידה בצורה

$$a_0+a_1x+\cdots+a_{n-1}x^{n-1}$$

עם מקדמים $a_i\in K$. מכאן ש $1,x,\ldots,x^{n-1}$ הוא בסיס ל L מעל K ולכן $[L:K]=n$. ∎

מסקנה 1.4.2: *אבר x בהרחבה של שדה K הנו אלגברי מעל K אם ורק אם $[K(x):K]<\infty$.*

דֻגמה 1.4.3: יהיו K שדה ו a אבר שאינו רִבוע ב K. אזי הפולינום X^2-a אי פריק מעל K. לפי משפטון 1.4.1, יש לפולינום זה שרש x בשדה הרחבה של K. אבר זה מקַיֵם $x^2=a$, $[K(x):K]=2$ ו $1,x$ מהוים בסיס של $K(x)$ מעל K. נאמר ש x הוא **שרש רבועי** של a ונסמן $x=\sqrt{a}$. אם $\mathrm{char}(K)\neq 2$, אזי $-x$ הוא שרש רבועי נוסף של a ו X^2-a מתפרק מעל $K(\sqrt{a})$ למכפלה של גורמים לינאריים שונים זה מזה

$$X^2-a=(X-\sqrt{a})(X+\sqrt{a})$$

אם y הוא שרש של X^2-a בשדה L המַקיף את $K(\sqrt{a})$, אזי $(y-\sqrt{a})(y+\sqrt{a})=y^2-a=0$ ולכן, $y=\sqrt{a}$ או $y=-\sqrt{a}$. במִלים אחרות, ל X^2-a יש ב L בדיוק שני שרשים. השרש $\sqrt{a}$ נקבע באפן חד ערכי רק עד כדי הסימן.

אם לעומת זאת $\mathrm{char}(K)=2$, אזי לפי תרגיל 1.3.1, X^2-a מתפרק מעל $K(\sqrt{a})$ בצורה

$$X^2-a=X^2-(\sqrt{a})^2=(X-\sqrt{a})^2$$

ולכן יש ל X^2-a רק שרש אחד בכל הרחבה של $K(\sqrt{a})$.

נחזור עתה למקרה שבו $\mathrm{char}(K) \neq 2$ ונתבונן בפולינום הרבועי $f(X) = aX^2 + bX + c$ שבו $a, b, c \in K$, $a \neq 0$ **והדִסקרימיננטה** $d = b^2 - 4ac$ אינה רבוע ב K. אזי $f(X)$ אי פריק מעל K, אולם מתפרק מעל הרחבה רבועית L של K למכפלה של שני גורמים לינאריים שונים זה מזה

$$aX^2 + bX + c = a(X - x_1)(X - x_2)$$

x_1, x_2 הם כל השרשים של $f(X)$ בכל שדה הרחבה של L והם מקיְמים

$$x_1 + x_2 = -\frac{b}{c} \qquad x_1 x_2 = \frac{c}{a}$$

נִתן לחשב אותם מתוך המקדמים בעזרת הנֻסחה הידועה:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \qquad \blacksquare$$

נֻסחת המגדל 1.4.4: *יהי $M \supseteq L \supseteq K$ מגדל של שדות. אזי* $[M : K] = [M : L][L : K]$.

הוכחה: מהלמה של צורן נובע שלכל מרחב וקטורי יש בסיס. יהיו אפוא $V = \{v_i \mid i \in I\}$ ו $W = \{w_j \mid j \in J\}$ בסיסים ל M/L ו L/K בהתאמה, אזי $|I| = [L : K]$ ו $|J| = [M : L]$. כדי להוכיח את המשפטון מספיק להראות שהקבוצה $VW = \{v_i w_j \mid i \in I,\ j \in J\}$ מהוָה בסיס ל M/K. זה נעשה על ידי הוכחת שתי טענות.

טענה א: *הקבוצה VW פורשת את M מעל K.* כל $y \in M$ נִתן להצגה כצרוף לינארי $y = \sum_{i \in I} x_j w_j$, באשר $x_j \in L$ וכמעט כֻלם אפס. נרשֹם כל אחד מה x_j־ים כצרוף לינארי $x_j = \sum_{i \in I} a_{ij} v_i$ באשר $a_{ij} \in K$ וכמעט כֻלם אפס. נציב בשויון הראשון ונקבל $y = \sum_{(i,j) \in I \times J} a_{ij} v_i w_j$, כנדרש.

טענה ב: *הקבוצה VW אינה תלויה לינארית מעל K.* יהיו a_{ij} אברים של K שכמעט כֻלם אפס כך ש $\sum_{i,j} a_{ij} v_i w_j = 0$. אזי $\sum_{j \in J} \big(\sum_{i \in I} a_{ij} v_i \big) w_j = 0$. לכן, $\sum_{i \in I} a_{ij} v_i = 0$ לכל j ולכן $a_{ij} = 0$ לכל i ו j, נדרש. $\blacksquare$

למה 1.4.5:

(א) *יהי $M \supseteq L \supseteq K$ מגדל של שדות כך ש* $\infty > [M : K] = [L : K]$*. אזי* $M = L$.

(ב) *יהיו $K \subseteq L, E$ שדות כך ש* $\infty > [L : K]$ *ו L ו E מוכלים בשדה משֻתף. אזי* $[LE : E] \leq [L : K]$.

(ג) *יהיו $K \subseteq L_1, L_2 \subseteq L$ שדות כך ש* $L_1 L_2 = L$, $\infty > [L : K]$ *ו* $[L : K] = [L_1 : K][L_2 : K]$*. אזי,* $L_1 \cap L_2 = K$.

הוכחת א: השדה L הוא תת מרחב של M ובעל אותו הממד. לכן $M = L$.

הוכחת ב: אם $L = K$, שני האגפים שוים ל 1. אחרת, נבחר $x \in L \smallsetminus K$ ויהיו $f = \mathrm{irr}(x, K)$ ו $g = \mathrm{irr}(x, E)$. אזי $g|f$ ולכן, לפי משפטון 1.4.1, $[E(x) : E] = \deg(g) \le \deg(f) = [K(x) : K]$. הנחת השראה על $[L : K]$ נותנת $[LE : E(x)] \le [L : K(x)]$. לכן, לפי נֻסחת המגדל,

$$[LE : E] = [LE : E(x)][E(x) : E] \le [L : K(x)][K(x) : K] = [L : K],$$

כנִטען.

הוכחת ג: נסמן $L_0 = L_1 \cap L_2$. מההנחה ומִנֻסחת המגדל נובע ש

$$[L_1 : K][L : L_1] = [L : K] = [L_1 : K][L_2 : K]$$

לכן, לפי (ב),

$$[L : L_1] = [L_2 : K] = [L_2 : L_0][L_0 : K] \ge [L : L_1][L_0 : K]$$

מכאן נובע ש $[L_0 : K] \le 1$, לכן $[L_0 : K] = 1$ ולכן $L_0 = K$, כפי שנטען. ∎

משפטון 1.4.6: *תהי L/K הרחבת שדות.*

(א) *אם $[L : K] < \infty$, אזי כל אבר של L אלגברי מעל K.*

(ב) *$[L : K] < \infty$, אם ורק אם קַיָּמים ב L אברים אלגבריים $x_1, \ldots, x_n$ כך ש $L = K(x_1, \ldots, x_n)$.*

הוכחת א: נניח ש $[L : K] < \infty$ ויהי $x \in L$. אזי $K(x)$ הוא תת מרחב של L מעל K ולכן $[K(x) : K] < \infty$. לפי מסקנה 1.4.2, x אלגברי מעל K.

הוכחת ב: נניח קודם ש $[L : K] < \infty$. אזי קַיָּם ל L/K בסיס סופי, $x_1, \ldots, x_n$. בפרט $L = K(x_1, \ldots, x_n)$. לפי (א), כל אחד מהאברים x_i אלגברי.

להפך, נניח ש $L = K(x_1, \ldots, x_n)$ וכל אחד מה x_i־ים אלגברי מעל K. נסמן $K' = K(x_1, \ldots, x_{n-1})$. הנחת השראה נותנת ש $[K' : K] < \infty$. בנוסף לזה, $\mathrm{irr}(x, K)$ הנו פולינום שונה מאפס עם מקדמים ב K' (אם כי אינו בהכרח אי פריק מעל K') ש x שרש שלו. לכן, לפי מסקנה 1.4.2, $[K'(x_n) : K'] < \infty$. מִנֻסחת המגדל נובע אפוא ש $[L : K] = [L : K'][K' : K] < \infty$. ∎

הערה 1.4.7: בהמשך נַראה דֻגמאות להרחבות אלגבריות שאינן סופיות. ∎

תרגיל 1.4.8: הוכח שאם $x_1, \ldots, x_n$ הם אברים אלגבריים מעל שדה K, אזי החוג $K[x_1, \ldots, x_n]$ מתלכד עם השדה $K(x_1, \ldots, x_n)$. ∎

הערה 1.4.9: גם ההפוך של הטענה של תרגיל 1.4.7 נכון: אם $x_1,\dots,x_n$ הם אברים של שדה הרחבה של שדה K כך ש $K[x_1,\dots,x_n]$ הנו שדה, אזי $x_1,\dots,x_n$ אלגבריים מעל K. טענה זו הנה אחת מהגרסאות השקולות של "משפט האפסים של הִלברט" ולא תוכח בקורס זה. ∎

משפטון 1.4.10: *אם L/K ו M/L הן הרחבות אלגבריות, אזי גם ההרחבה M/K אלגברית.*

הוכחה: לכל אבר x של M קיָמים לפי ההנחה אברים $b_0,\dots,b_n\in L$ שלא כֻּלם אפס כך ש

$$.b_0+b_1x+\cdots+b_nx^n=0$$

בפרט x אלגברי מעל השדה $K'=K(b_0,\dots,b_n)$. לכן, לפי מסקנה 1.4.2, $[K'(x):K']<\infty$. לפי משפטון 1.4.6(ב), כל אחד מהאברים b_i אלגברי מעל K. לכן, לפי משפטון 1.4.6(א), $[K':K]<\infty$. לכן, לפי נֻסחת המגדל, $[K'(x):K']<\infty$. הפעלה של משפטון 1.4.6(ב) על x מוכיחה לבסוף ש x אלגברי מעל K. מכאן נובע ש M אלגברי מעל K. ∎

מסקנה 1.4.11: *יהיו $x_1,\dots,x_n$ אברים אלגבריים של שדה M המקיף שדה K. אזי לכל פולינום $f\in K[X_1,\dots,X_n]$ האבר $f(x_1,\dots,x_n)$ של M אלגברי מעל K. בפרט, אם $x,y\in M$ אלגבריים מעל K, אזי גם $x+y$, xy ו $\frac{x}{y}$ (אם $y\neq 0$) אלגבריים מעל K.*

הערה 1.4.12: ההוכחה שנתנו לכך ש $x+y$, xy ו $\frac{x}{y}$ אלגבריים מעל K אם x,y אלגבריים אומרת שקיָמים פולינומים עם מקדמים ב K שבין שרשיהם מצויים שלשת האברים הראשונים. אולם אין ההוכחה נותנת מתכון לחשוב המקדמים של הפולינומים האלו מתוך המקדמים של $\mathrm{irr}(x,K)$ ו $\mathrm{irr}(y,K)$. אפשר לתת הוכחה בונה כזו בעזרת מושגים מתורת גלואה שנִלמד מאוחר יותר. ∎

תרגיל 1.4.13: *הוכח שהשדה $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ מקיֵם $[K:\mathbb{Q}]=4$ ו $1,\sqrt{2},\sqrt{3},\sqrt{6}$ מהוים בסיס ל $K/\mathbb{Q}$.*

תרגיל 1.4.14: *יהיו K שדה, x אבר אלגברי מעל K ממעלה אי זוגית ו $L=K(x)$. הוכח ש $L=K(x^2)$.*

תרגיל 1.4.15: *יהי $L=\mathbb{Q}(x)$, באשר x הוא שרש של המשואה*

$$.X^3+X^2+X+2=0$$

הוכח ש $[E:\mathbb{Q}]=3$ (רמז: הוכח שאין לפולינום שרשים שלמים) ובטא כל אחד מהבטויים $(x^2+x+1)(x^2+x)$ ו $(x-1)^{-1}$ בצורה ax^2+bx+c עם $a,b,c\in\mathbb{Q}$

תרגיל 1.4.16: *יהיו x,y אברים אלגבריים מעל שדה K. נסמן $f=\mathrm{irr}(x,K)$ ו $g=\mathrm{irr}(y,K)$. נניח ש $\gcd(\deg(f),\deg(g))=1$. הוכח ש $[K(x,y):K]=[K(x):K][K(y):K]$ וש g אי פריק מעל $K(x)$.*

תרגיל 1.4.17: *תהיינה E ו F שתי הרחבות סופיות של שדה K המוכלות בשדה משֻתף.*

(א) *הוכח ש* $[EF : K] \leq [E : K][F : K]$.

(ב) *הוכח שאם* $[E : K]$ *ו* $[F : K]$ *זרים זה לזה, אזי* $[EF : K] = [E : K][F : K]$.

תרגיל 1.4.18: יהיו $K \subseteq L$ שדות, נסמן $m = [L : K]$ ויהי V מרחב וקטורי ממעלה n מעל L. הוכח ש V הוא מרחב וקטורי ממעלה mn מעל K. ∎

תרגיל 1.4.19: יהי K שדה, יהי $f \in K[X]$ פולינום ממעלה n ויהי L שדה הפִצול של f מעל K. הוכח ש $[L : K] \leq n!$. ∎

תרגיל 1.4.20: הוכח שאם K הנו שדה ו $x_1, \ldots, x_n$ הם אברים של $\tilde{K}$, אזי $K(x_1, \ldots, x_n)$ הוא אֹסף כל הב־טויים מהצורה $f(x_1, \ldots, x_n)$ שבהם $f \in K[X_1, \ldots, X_n]$ הוא פולינום המקיֵם $\deg_{X_i} f < [K(x_i) : K]$. ∎

1.5 שָׁרשים של פולינומים

נראה בסעיף זה שלפולינום שונה מאפס יש רק מספר סופי של שָׁרשים, נגדיר את הרִבוי של שרש ונפתח מתכון להבדיל בין שרש פשוט לשרש מְרֻבֶּה.

משפטון 1.5.1: *יהי K שדה, $f \in K[X]$ פולינום ו $a \in K$ שֹרש שלו. אזי $X - a | f(X)$.*

הוכחה: אם נחלק את $f(X)$ ב $X - a$ עם שארית נקבל פולינומים $q, r \in K[X]$ כך ש $f(X) = q(X)(X - a) + r(X)$ ו $\deg(r) < 1$. לכן, r הוא פולינום קבוע. אם נציב בשויון האחרון a במקום X נקבל ש $r = 0$. לכן $f(X) = q(X)(X - a)$, כלומר $X - a | f(X)$. ∎

תוצאה 1.5.2: *לכל פולינום $f \in K[X]$ ממעלה n יש ב K לכל היותר n שָׁרשים שונים.*

הוכחה: טענתנו בודאי נכונה אם אין ל f שרשים ב K. נניח אם כן שיש ל f שרש $a \in K$. משפטון 1.5.1 נותן $g \in K[X]$ כך ש $f(X) = g(X)(X - a)$. הואיל ו $\deg(g) = \deg(f) - 1$, אומרת הנחת השראה שיש ל g לכל היותר $n - 1$ שרשים שונים ב K. כל שרש של f הנו שרש של g או שהוא שוה ל a. לכן יש ל f לכל היותר n שרשים שונים ב K. ∎

הערה 1.5.3: הדֻגמה של הפולינום $f(X) = (X - 1)^n$ מראה שיִתכן שלפולינום ממעלה n יהיה רק שרש אחד בשדה. ∎

תוצאה 1.5.4: *אם K הוא שדה אינסופי ואם $0 \neq f \in K[X]$, אזי $f(a) \neq 0$ עבור כמעט כל $a \in K$. בפרט קיָם $a \in K$ כך ש $f(a) \neq 0$.*

הערה 1.5.5: לעומת זאת, אם K הוא שדה סופי, אזי הפולינום $f(X) = \prod_{a \in K}(X - a)$, מתאפס בכל $a \in K$. ∎

תוצאה 1.5.6: *יהיו A תת קבוצה אינסופית של שדה K ו $f \in K[X_1, \ldots, X_n]$ פולינום שונה מאפס. אזי קיָמים $a_1, \ldots, a_n \in K$ כך ש $f(a_1, \ldots, a_n) \neq 0$.*

הוכחה: אם נרשֹם $f(X_1, \ldots, X_n) = \sum_{i=0}^{d} f_i(X_1, \ldots, X_{n-1})X_n^i$ עם $f_i \in K[X_1, \ldots, X_{n-1}]$, נקבל שקיָם i כך ש $f_i \neq 0$. הנחת השראה על n נותנת אפוא $a_1, \ldots, a_{n-1} \in A$ כך ש $f_i(a_1, \ldots, a_{n-1}) \neq 0$. הפולינום $g(X_n) = \sum_{i=0}^{d} f_i(a_1, \ldots, a_{n-1})X_n^i$ שיָם ל $K[X_n]$ ושונה מאפס. לפי תוצאה 1.5.4, קיָם $a_n \in A$ כך ש $g(a_n) \neq 0$, במלים אחרות, $f(a_1, \ldots, a_n) \neq 0$, כנדרש. ∎

הגדרה 1.5.7: *רִבוי של שרש.* יהיו K שדה, $f \in K[X]$ פולינום שונה מאפס, ו $a \in K$ שֹרש של f. לפי משפטון 1.5.1, $X - a | f(X)$. לכן קיָמים $r \geq 1$ טבעי ופולינום $g \in K[X]$ כך ש $f(X) = g(X)(X - a)^r$ ו $g(a) \neq 0$, כלומר $(X - a)^r$ היא החזקה הגבוהה ביותר של $X - a$ המחלקת את $f(X)$. נקרא ל r **הרִבוי** של a

כשרש של f. אם $r=1$ נאמר ש a הוא **שרש פשוט** של f, אם $r=2$ נאמר ש a הוא **שרש כפול** ואם $r \geq 2$ נאמר ש a הוא **שרש מֻרְבה**. ∎

הגדרה 1.5.8: נגזרת של פולינום. בתורת הפונקציות הממשיות או המֻרכבות מגדירים את הנגזרת של פולינום על ידי מעבר לְגבול ומוצאים נֻסחה פשוטה עבורה במונחים של הפולינום המקורי. מעל שדה כלשהוא לוקחים נֻסחה זו כהגדרת הנְגזרת.

באֹפן מפֹרש, יהי $f(X)=\sum_{i=0}^n a_iX^i$ פולינום עם מקדמים בשדה K. נגדיר את **הנגזרת** של $f(X)$ כפולינום $f'(X)=\sum_{i=1}^n ia_iX^{i-1}$. בנֻסחה זו יש לסימן i שלשה תפקידים. האחד **כצִיון** (=אִנדקס), השני כסכום של i פעמים 1 בשדה K (בפרט $i=0$ אם i כציון מתחלק ב p) והשלישי כמספר שלם במעריך של X.

פעֻלת הנגזרת מקיֶמת את הכללים הבאים:

(וא) $\deg(f)=n$ גורר ש $\deg(f') \leq n-1$. אם בנוסף לכך $\mathrm{char}(K)=0$, אזי $\deg(f')=n-1$.

(וב) $(f+g)'=f'+g'$.

(וג) $(fg)'=f'g+fg'$.

(וד) אם $c \in K$, אזי $(cf)'=cf'$. בפרט $c'=0$.

(וה) יהי $f(X)=\sum_{i=0}^n a_iX^i$ ונניח ש $f'=0$. אם $\mathrm{char}(K)=0$, אזי $f \in K$ קבוע. אם $\mathrm{char}(K)=p>0$, אזי $a_i=0$ לכל i שאינו מתחלק ב p. לכן, $f(X)=\sum_{j=0}^m a_{pj}X^{pj}$.

(וו) כלל השרשרת: אם $g,h \in K[X]$ הם פולינומים ו $f(X)=g(h(X))$, אזי $f'(X)=g'(h(X))h'(X)$. (הוכח תחילה את המקרה שבו $h(X)=X^i$ ואחר כך עבור $g(X)=\sum_{i=0}^n a_i(h(X))^i$). ∎

מושג הנגזרת מאפשר לנו לתת בֹחן פשוט לפשטות של שרש של פולינום.

משפטון 1.5.9: *יהיו K שדה, $f \in K[X]$ פולינום ו $a \in K$ שרש של f. אזי a הנו שרש פשוט אם ורק אם $f'(a) \neq 0$.*

הוכחה: נניח קודם ש a הנו שרש פשוט. אזי $f(X)=(X-a)g(X)$ באשר $g \in K[X]$ ו $g(a) \neq 0$. לכן, $f'(X)=g(X)+(X-a)g(X)$ ומכאן $f'(a)=g(a) \neq 0$.

עתה נניח ש a הוא שרש מֻרבה. אזי $f(X)=(X-a)^rg(X)$, באשר $r \geq 2$ ו $g \in K[X]$. לכן, $f'(X)=r(X-a)^{r-1}g(X)+(X-a)^rg'(X)$ ולכן, $f'(a)=0$. ∎

הבֹחן הבא מאפשר לנו לקבֹע אם לפולינום יש שרשים מֻרבים בשדה הרחבה של K בעזרת פעֻלות ב K.

משפטון 1.5.10: *יהי f פולינום ב X עם מקדמים בשדה K ותהי L הרחבה של K שמעליה מתפרק f למכפלה של גורמים לינאריים.*

(א) *אם $f'=0$, אזי כל השָרשים של f ב L מֻרבים.*

(ב) *נניח ש $f' \neq 0$. אזי כל השרשים של f ב L פשוטים אם ורק אם* $\gcd(f, f') = 1$.

הוכחה: אם $f' = 0$, אזי $f'(a) = 0$ לכל שרש של f ולכן, לפי משפטון 1.5.9 כל השרשים של f מְרֻבים.

נניח אפוא ש $f' \neq 0$ ויהי $d = \gcd(f, f')$. קְפי למה 1.5.9, כל השרשים של f ב L פשוטים אם ורק אם אין ל f ול f' שרשים משֻתפים, כלומר אם אין ל d שרשים ב L. הואיל ו d מחלק את f, מתפרק d לגורמים לינאריים ב L. לכן, אין ל d שרשים ב L אם ורק אם $\deg(d) = 0$, כלומר אם $d = 1$. ∎

משפטון 1.5.11: *יהי $f \in K[X]$ פולינום אי פריק ותהי L הרחבה של K שמעליה מתפרק f למכפלה של גורמים לינאריים. אזי יש ל f שרשים מְרֻבים ב L אם ורק אם* $f' = 0$.

הוכחה: נניח קודם ש $f' = 0$ ויהי a שֹרש של f ב L. אזי $f'(a) = 0$ ולכן, לפי משפטון 1.5.9, a הנו שרש מרבה.

להפך, נניח ש $f' \neq 0$. אזי $d = \gcd(f, f') \neq 0$. הואיל ו $d|f'$ מתקיֵם

$$\deg(d) \leq \deg(f') \leq \deg(f) - 1\,.$$

הואיל ו f אי פריק, נובע מכאן ש d קבוע ולכן $d = 1$ (מניחים ש d מתֻקן). לכן, לפי משפטון 1.5.10, אין ל f שרשים מרבים ב L. ∎

משפטון 1.5.12: *יהי $f \in K[X]$ פולינום אי פריק.*

(א) *אם $\mathrm{char}(K) = 0$, אזי יש ל f רק שרשים פשוטים.*

(ב) *נניח ש $p = \mathrm{char}(K) > 0$. אזי יש ל f שרשים מְרֻבים אם ורק אם קיָם $g \in K[X]$ כך ש* $f(X) = g(X^p)$.

הוכחת א: במקרה זה $\deg(f') = \deg(f) - 1$, בפרט $f' \neq 0$. לכן, לפי משפטון 1.5.11, כל שרשי f פשוטים.

הוכחת ב: נניח שיש ל f שרשים מְרֻבים. אזי, לפי משפטון 1.5.11, $f' = 0$. לכן, לפי כלל (וה), $f(X) = \sum_{j=0}^m a_{pj} X^{pj}$. אם נסמן $g(X) = \sum_{i=0}^m a_{pi} X^p$, נקבל ש $f(X) = g(X^p)$.

להפך, אם יש ל f הצורה האחרונה, אזי $f'(X) = 0$ ולכן כל שרשי f מְרֻבים. ∎

דֻגמה 1.5.13: יהי $K = \mathbb{F}_p(t)$ ו t נעֱלה מעל K. לפי בֹחן אייזנשטיין הפולינום $f(X) = X^p - t$ אי פריק מעל K. אם $x \in \tilde{K}$ הוא שרש של f אזי $x^p = t$ ו $f(X) = X^p - x^p = (X - x)^p$. ל $f(X)$ יש אפוא שרש אחד ורִבויו p. ∎

תרגיל 1.5.14: יהי K שדה בעל אפיון חיובי p ויהי $a \in K$. נניח שאין ל a שרש p־י ב K. הוכח ש $X^{p^n} - a$ אי פריק ב $K[X]$ לכל n טבעי. ∎

1.6 שדה פצול

אחרי שהראינו בסעיף 1.3 כיצד לצרף שֹרש אחד של פולינום לשדה המקדמים שלו, נראה כאן כיצד לצרף את כל השרשים.

הגדרה $1.6.1$: יהי f פולינום שונה מאפס עם מקדמים בשדה K. **שדה פְצול של** f **מעל** K הנו הרחבה N של K המקיֶמת את הדרישות הבאות:

(וא) $f(X)$ מתפרק לגורמים לינאריים מעל N, כלומר $f(X) = c(X - x_1) \cdots (X - x_n)$.

(וב) $N = K(x_1, \dots, x_n)$.

שדה הפצול של פולינום האפס מעל K יֻגדר כ K. ∎

המשפטון הבא נותן את הקיום והיחידות של שדה הפְצול.

משפטון $1.6.2$: *יהי* f *פולינום ממעלה חיובית עם מקדמים בשדה* K.

(א) *קיֶם ל* f *שדה פְצול* N *מעל* K.

(ב) $[N : K] < \infty$.

(ג) *לכל איזומורפיזם* $\alpha\colon K \to K'$ *של שדות ולכל שדה פצול* N' *של* $f' = \alpha(f)$ *מעל* K' *קיֶמת הרחבה של* α *לאיזומורפיזם* $\beta\colon N \to N'$.

הוכחה בהשראה על מעלת f: אם $\deg(f) = 1$ שדה הפצול הוא K עצמו. יהי עתה $n = \deg(f) \geq 2$ ונניח שהמשפטון הוכח לכל השדות ולכל הפולינומים ממעלה $n - 1$. בלי הגבלת הכלליות נניח ש f מְתֻקן. נבחר ל f גורם אי פריק g ב $K[X]$. לפי משפטון $1.3.6$ קיֶמת ל K הרחבה L ובה שרש a של g. הואיל ו $g|f$, מתקיֵם $f(a) = 0$ ולכן, לפי משפטון $1.5.1$, מחלק $X - a$ את $f(X)$ ב $K(a)[X]$. כלומר, $h(X) = \frac{f(X)}{X-a}$ הנו פולינום ממעלה $n - 1$ עם מקדמים ב $K(a)$. לפי הנחת ההשראה, קיֶם ל h שדה פצול N מעל $K(a)$ כלומר $h(X) = (X - a_2) \cdots (X - a_n)$ ו $N = K(a, a_2, \dots, a_n)$. יתר על כן, $[N : K(a)] < \infty$. הואיל ו $f(X) = (X - a)(X - a_2) \cdots (X - a_n)$, אנו מקבלים מכאן ש N הוא גם שדה פְצול של f מעל K. לפי נֻסחת המגדל, $[N : K] = [N : K(a)][K(a) : K] < \infty$.

כדי להוכיח את (ג), נעיר ש f' מתפרק מעל N' לגורמים לינאריים. הואיל ו $g' = \alpha(g)$ הוא גורם אי פריק של f' גם g' מתפרק מעל N' לגורמים לינאריים. נבחר שֹרש a' של $g' = \alpha(g)$ ב N'. לפי משפטון $1.3.4$, נִתן להרחיב את α לאיזומורפיזם $\beta_0\colon K(a) \to K(a')$ המעתיק את a על a'. בפרט β_0 מעתיק את $h(X) = \frac{f(X)}{X-a}$ על $h'(X) = \frac{f'(X)}{X-a'}$. כמו לעיל נובע ש N' הוא שדה פְצול של h' מעל $K(a')$. לכן, לפי הנחת ההשראה, נִתן להרחיב את β_0 לאיזומורפיזם $\beta\colon N \to N'$. ∎

תרגיל $1.6.3$: *יהי* $f \in K[X]$ *פולינום ממעלה* n *ויהי* L *שדה הפְצול של* f *מעל* K. *הוכח ש* $[L : K] \leq n!$.

תרגיל 1.6.4: *מצא את שדה הפִצול של* $X^{p^8}-1$ *מעל* $\mathbb{F}_p$.

תרגיל 1.6.5: *חשב את המעלה של שדה הפִצול של* X^3-2 *מעל* $\mathbb{F}_7$.

תרגיל 1.6.6: *תאר את שדה הפִצול של כל אחד מהפולינומים הבאים מעל* $\mathbb{Q}$ *ומצא את מעלתו:*

(א) X^2-2.

(ב) X^2-1.

(ג) X^3-2.

(ד) $(X^3-2)(X^2-2)$.

(ה) X^2+X+1.

(ו) X^6+X^3+1.

(ז) X^5-7.

תרגיל 1.6.7: *תהיינה* L *ו* M *שתי הרחבות של שדה* K *המוכלות בשדה משֻתף. נאמר ש* L ***מֻפרד לינארית*** *מ* M *מעל* K *אם כל* $x_1,\dots,x_n$ *ב* L *שאינם תלויים לינארית מעל* K *אינם תלויים לינארית גם מעל* M. *הוכח שיַחס המֻפרדות הלינארית סימטרי.*

תרגיל 1.6.8: *תהיינה* L *ו* M *הרחבות סופיות של שדה* K. *הוכח ש* L *ו* M *מֻפרדים לינארית מעל* K *אם ורק אם* $[ML:K]=[M:K][L:K]$.

תרגיל 1.6.9: *יהי* K *שדה, יהי* $f\in K[X]$ *פולינום אי פריק, יהי* x *שרש של* f *ותהי* L *הרחבה של* K. *הוכח ש* $K(x)$ *מֻפרד לינארית מ* L *מעל* K *אם ורק אם* f *אי פריק מעל* L.

תרגיל 1.6.10: *יהי* t *אבר נעלה מעל שדה* K. *נסמן* $E=K\left(\frac{t^3}{t+1}\right)$ *ו* $F=K(t)$. *חשב את* $[F:E]$.

תרגיל 1.6.11: *יהי* $K\subseteq L\subseteq M$ *מגדל של שדות ותהי* E *הרחבה של* K. *נניח שכל השדות הללו מוכלים בשדה משֻתף. הוכח ש* E *מֻפרד לינארית מ* M *מעל* K *אם ורק אם* E *מֻפרד לינארית מ* L *מעל* K *ו* LE *מֻפרד לינארית מ* M *מעל* L.

1.7 הסגור האלגברי של שדה

אנו אומרים על שדה M שהוא **סגור אלגברית** אם כל פולינום $f \in M[X]$ ממעלה חיובית מתפרק מעל M לגורמים לינאריים. אנו נראה פה שלכל שדה K יש הרחבה סגורה אלגברית $\tilde{K}$ שהיא אלגברית מעל K. הרחבה זו הנה יחידה עד כדי איזומורפיזם־K והיא תקרא "הסְגור האלגברי של K".

למה 1.7.1: *תנאי מספיק (וגם הכרחי) לכך ששדה M יהיה סגור אלגברית הוא שלכל פולינום ממעלה חיובית עם מקדמים ב M יהיה שׂרש ב M.*

הוכחה: יהי $f \in M[X]$ פולינום ממעלה חיובית. לפי ההנחה קיָם ל f שרש $a \in M$. לפי משפטון 1.5.1 קיָם פולינום $g \in M[X]$ כך ש $f(X) = (X-a)g(X)$. הואיל ו $\deg(g) = \deg(f) - 1$, מבטיחה הנחת השראה ש g מתפרק למכפלה של גורמים לינאריים מעל M. לכן מתפרק גם f למכפלה של גורמים לינאריים מעל M. ∎

הגדרה 1.7.2: הרחבה L של שדה K תקְנה **סגור אלגברי של** K אם L סגור אלגברית ואם L אלגברי מעל K. ∎

למה 1.7.3: *תהי M הרחבה סגורה אלגברית של שדה K. נסמן ב L את אֹסף כל אברי M שהם אלגבריים מעל K. אזי L הוא שדה סגור אלגברית.*

הוכחה: לפי מסקנה 1.4.11, סכום, מכפלה ומנה של אברים אלגבריים מעל K הנו שוב אלגברי מעל K. לכן, L הנו שדה. כדי להוכיח ש L סגור אלגברית, מספיק להוכיח, לפי למה 1.7.1 שלכל פולינום אי פריק $f \in L[X]$ יש שרש ב L.

ואכן, f מתפרק למכפלה של גורמים לינאריים מעל M. נבחר שרש x של f ב M. אזי $L(x)/L$ הנה הרחבה אלגברית. הואיל וגם L/K הרחבה אלגברית, נובע ממשפטון 1.4.10 ש $K(x)$ אלגברי מעל K. בפרט x אלגברי מעל K. לפי הגדרת L, שיָך x ל L. ∎

דֻגמה 1.7.4: שדה המספרים המרֻכבים $\mathbb{C}$ סגור אלגברית. משפט זה מוכח בתורת הפונקציות המרֻכבות על יסוד משפט ליוביל האומר שפוקציה אנליטית שלמה וחסומה בכל המישור הנה קבועה. אנו נוכיח משפט זה בהמשך בעזרת תורת גלואה ומשפטי סילו.

לפי למה 1.7.3, אסף המספרים המרֻכבים שהם אלגבריים מעל $\mathbb{Q}$ מהוה שדה סגור אלגברית. מאידך, שדה זה, שנסמנו ב $\tilde{\mathbb{Q}}$, אלגברי מעל $\mathbb{Q}$. לכן $\tilde{\mathbb{Q}}$ הנו סגור אלגברי של $\mathbb{Q}$. להלן נראה שלכל שדה יש סגוֹר אלגברי. ∎

למה 1.7.5: *לכל שדה K קיֶמת הרחבה סגורה אלגברית M.*

הוכחה (Emil Artin): נסמן ב $\mathcal{F}$ את אֹסף כל הפולינומים $f \in K[X]$ ממעלה חיובית. לכל $f \in \mathcal{F}$ נתאים משתנה חדש X_f ונתבונן בחוג הפולינומים $R = K[X_f \mid f \in \mathcal{F}]$. עתה נבנה את האידאל $I = \sum_{f\in\mathcal{F}} Rf(X_f)$ של R הנוצר על ידי כל האברים $f(X_f)$ שעבורם $f \in \mathcal{F}$.

טענה א: $R\neq I$.   אחרת היה קַיָמים $e_f\in R$ שכמעט כֻּלם אפס כך ש $\sum_{f\in\mathcal{F}} e_f f(X_f)=1$. קַיָמים אפוא $f_1,\dots,f_n\in\mathcal{F}$ ופולינומים g_i ב n משתנים עם מקדמים ב K כך ש

$$1=\sum_{i=1}^{n} g_i(X_{f_1},\dots,X_{f_n})f_i(X_{f_i}). \tag{1}$$

נסמן $h=f_1\cdots f_n$ ויהי L שדה הפִּצול של h מעל K. לכל i נבחר שֹרש x_i של f_i ב L ונגדיר הומומורפיזם־K $\varphi\colon K[X_{f_1},\dots,X_{f_n}]\to L$ על ידי $\varphi(X_{f_i})=x_i$ עבור $i=1,\dots,n$. אם נפעיל הומומורפיזם זה על (1), נקבל ש $1=\sum_{i=1}^{n} g_i(x_1,\dots,x_n)f_i(x_i)=0$. סתירה זו מוכיחה ש $1\notin I$, כנדרש.

מטענה א נובע, לפי למה 1.1.2, שקַיָם ל R אידאל מרבי J המַקיף את I. יהי $K_1=R/J$ שדה המנה המתאים. נשכן את K לתוך K_1 על ידי ההעתקה $a\mapsto a+J$. לכל $f\in\mathcal{F}$ מתקַיֵם $f(X_f)\in I\subseteq J$ ולכן, $f(X_f+J)=f(X_f)+J=0$.

באפן דומה נוכל לבנות הרחבה K_2 של K_1 שבה יש שרש לכל פולינום ממעלה חיובית ב $K_1[X]$. בהשראה נבנה סדרה עולה של שדות $K=K_0\subseteq K_1\subseteq K_2\subseteq\cdots$ כך שלכל פולינום ממעלה חיובית עם מקדמים ב K_m יש שרש ב K_{m+1}. האחוד $M=\bigcup_{m=0}^{\infty}K_m$ הנו הרחבה סגורה אלגברית של K. ואכן, כל פולינום $f\in M[X]$ ממעלה חיובית שיָך ל $K_m[X]$ עבור איזה שהוא m ולכן יש לו שרש ב K_{m+1}, בפרט יש לו שרש ב M. לפי למה 1.7.1, M סגור אלגברית. ∎

משפטון 1.7.6: *לכל שדה K יש סגוֹר אלגברי.*

הוכחה: לפי למה 1.7.5 יש ל K הרחבה סגורה אלגברית M. קבוצת כל אברי M שהם אלגבריים מעל K תהיה, לפי למה 1.7.3, סגוֹר אלגברי של K. ∎

לאחר שהוכחנו את קיום הסגוֹר האלגברי של שדה, נרצה עתה להוכיח את יחידותו, עד כדי איזומורפיזם־K.

משפטון 1.7.7: *יהי $\alpha\colon K\to K'$ איזומורפיזם של שדות ויהיו L ו L' סגוֹרים אלגבריים של K ו K' בהתאמה. אזי קַיָם איזומורפיזם $\gamma\colon L\to L'$ של שדות המרחיב את α.*

הוכחה: נסמן ב $\mathcal{E}$ את אֹסף כל הזוגות (E,β) שבהם E הוא שדה בינַיִם בין K ל L ו β הוא שִכון של E לתוך L' המרחיב את α. אסף זה אינו ריק שכן הוא מכיל את הזוג (K,α). נסדר את $\mathcal{E}$ באפן חלקי בעזרת ההגדרה הבאה: $(E_1,\beta_1)\le(E_2,\beta_2)$ אם $E_1\subseteq E_2$ ו $\beta_2|_{E_1}=\beta_1$. אם $\mathcal{E}_0=\{(E_i,\beta_i)\mid i\in I\}$ היא שרשרת ב $\mathcal{E}$, אזי $E=\bigcup_{i\in I}E_i$ הוא שדה המַקיף את K ומוכל ב L וההעתקה $\beta\colon E\to L'$ המֻגדרת על ידי $\beta(x)=\beta_i(x)$ עבור $x\in E_i$ הנָה שִכון של E לתוך L' המֻגדר היטב ומרחיב את α. לכן, (E,β) הוא חסם מלעיל של השרשרת $\mathcal{E}_0$.

הלמה של צורן נותנת לנו אבר מרבי (F,γ) של $\mathcal{E}$. יהי $F'=\gamma(F)$. עלינו להוכיח ש $F=L$ ו $F'=L'$.

ואכן, כל אבר $x\in L$ הנו אלגברי מעל K ולכן גם מעל F. יהי $f=\mathrm{irr}(x,F)$. אזי $f'=\gamma(f)$ הוא פולינום אי

פריק ו $\deg(f') = \deg(f) \geq 1$. הואיל ו L' סגור אלגברית, קיָם ל f' שרש $x' \in L'$. לפי משפטון 1.3.4, נִתן להרחיב את γ לאיזומורפיזם $\delta\colon F(x) \to F'(x')$. לכן, $(F,\gamma) \leq (F(x),\delta)$. מהמרביות של (F,γ) נובע ש $F = F(x)$, כלומר $x \in F$. מזה אנו מסיקים ש $F = L$.

בכּוון הֶהפוך נֵצא מאבר $x' \in L'$ ונסמן $f' = \mathrm{irr}(x', F')$ ו $f = \gamma^{-1}(f)$. אזי f אי פריק ממעלה חיובית וקיָם לו אפוא שֹרש x ב L. כמו בסעיף הקודם, קיָם איזומורפיזם $\delta\colon F(x) \to F'(x')$ המרחיב את γ. מהמרביות של (F,γ) נובע ש $x \in F$. לכן, $\deg(f') = \deg(f) = 1$ ומכאן ש $x' \in F'$, כנדרש. ∎

המִקרה שבו $K = K'$ נותן לנו את היחידות של הסגוֹר האלגברי.

משפט 1.7.8: *לכל שדה K יש סגוֹר אלגברי יחיד עד כדי איזומורפיזם־K. נסמן אותו ב $\tilde{K}$.*

דֻגמה 1.7.9: לפי בֹחן אייזנשטיין (תוצאה 1.1.9), הפולינום $X^n - 2$ אי פריק מעל $\mathbb{Q}$ לכל n טבעי. לכן המעלה של כל שדה שרש שלו תהיה n. הואיל ו n אינו חסום נקבל מכאן ש $[\tilde{\mathbb{Q}} : \mathbb{Q}] = \infty$.

באפן דומה, לכל שדה K ואבר נעלה t מעל K הפולינום $X^n - t$ אי פריק מעל $F = K(t)$. לכן, כמו מקודם $[\tilde{F} : F] = \infty$. ∎

הערה 1.7.10: *האברים הצמודים ל x.* מתוצאה 1.3.5 נובע שאם x הנו אבר אלגברי מעל K, אזי קבוצת השרשים של $\mathrm{irr}(x,K)$ שוָה לקבוצת כל האברים σx שבהם σ הנו שכון־K של $K(x)$ לתוך $\tilde{K}$. כל אחד מהאברים הללו נקרא **צמוד של** x **מעל** K. ∎

1.8 **הרחבות נורמליות**

נתבונן בשדה K ונקבע לו סגור אלגברי $\tilde{K}$. בהנתן קבוצת פולינומים $\mathcal{F}$ עם מקדמים ב K נקרא לשדה הנוצר על ידי כל שרשי הפולינומים ב $\tilde{K}$ השיָכים ל $\mathcal{F}$ **שדה הפִצול של** $\mathcal{F}$. אם $\mathcal{F}$ מֻרכבת מפולינום אחד בלבד f, אזי שדה הפִצול של $\mathcal{F}$ מתלכד עם שדה הפִצול של f (הגדרה 1.6.1).

מההגדרה נובע ששדה הפִצול של $\mathcal{F}$ מעל K נקבע באפן חד ערכי בתוך $\tilde{K}$. כמו כן נובע מההגדרה שאם L הוא שדה הפִצול של $\mathcal{F}$ מעל K, אזי $\mathcal{F}$ הוא שדה הפצול של $\mathcal{F}$ מעל כל הרחבה של K המוכלת ב L. המשפטון הבא מבטיח את אי התלות של שדה הפִצול בסגור האלגברי המיֻחד $\tilde{K}$ שבחרנו ל K.

משפטון 1.8.1: *יהיו $\alpha\colon K \to K'$ איזומורפיזם של שדות, $\mathcal{F}$ קבוצה של פולינומים ב $K[X]$, $\mathcal{F}' = \alpha(\mathcal{F})$, L שדה פִצול של $\mathcal{F}$ ו L' שדה פִצול של $\mathcal{F}'$. אזי נִתן להרחיב את α לאיזומורפיזם* $\beta\colon L \to L'$.

הוכחה: יהיו $\tilde{K}$ ו $\widetilde{K'}$ סגורים אלגבריים של K ו K' בהתאמה. משפטון 1.7.7 נותן הרחבה $\tilde{\alpha}$ לאיזומרפיזם $\tilde{\alpha}\colon \tilde{K} \to \widetilde{K'}$. איזומורפיזם זה יעתיק את קבוצת כל השרשים של הפולינומים $f \in \mathcal{F}$ השיָכים ל $\tilde{K}$ על קבוצת כל השרשים של הפולינומים $f' \in \mathcal{F}'$ השיָכים ל $\tilde{K}'$. לכן $\tilde{\alpha}(L) = L'$. ∎

הגדרה 1.8.2: הרחבה אלגברית תִקרא **נורמלית** אם כל פולינום אי פריק $f \in K[X]$ שיש לו שֹרש ב L מתפרק לגורמים לינאריים ב L. ∎

משפטון 1.8.3: *הרחבה אלגברית L/K הנה נורמלית אם ורק אם L הוא שדה הפִצול מעל K של קבוצת פולינומים מעל* K.

הוכחה: נניח קודם ש L נורמלי מעל K. אזי L הוא שדה הפִצול מעל K של הקבוצה $\{\mathrm{irr}(x,K) \mid x \in L\}$.

להפך, נניח ש L הוא שדֵה הפִצול מעל K של תת קבוצה $\mathcal{F}$ של $K[X]$. יהי $x \in L$ ונסמן $f = \mathrm{irr}(x,K)$. מספיק שנוכיח שכל שרש x' של f ב $\tilde{K}$ שיָך ל L. ואכן, לפי משפטון 1.3.4, קיָם איזומורפיזם־K $\alpha\colon K(x) \to K(x')$ המקיֵם $\alpha(x) = x'$. מההגדרה נובע ש L הנו גם שדה הפִצול של $\mathcal{F}$ מעל $K(x)$. כמו כן, $\alpha(\mathcal{F}) = \mathcal{F}$. לכן, לפי משפטון 1.8.1, נִתן להרחיב את α לאיזומורפיזם של L על שדה הפִצול של $\mathcal{F}$ מעל $K(x')$. שוב, מההגדרה נובע ששדה אחרון זה הנו גם שדה הפִצול של $\mathcal{F}$ מעל K. במלים אחרות, $L' = L$. לכן, $x' \in L$, כמבֻקש. ∎

תוצאה 1.8.4: *יהי $M \subseteq L \subseteq K$ מגדל של שדות כך שההרחבה M/K נורמלית. אזי גם ההרחבה M/L נורמלית.*

הוכחה: לפי משפטון 1.8.3, M הוא שדה הפִצול מעל K של תת קבוצה $\mathcal{F}$ של $K[X]$. לכן M הוא גם שדה הפִצול של $\mathcal{F}$ מעל L. לכן, לפי משפטון 1.8.3, M נורמלי גם מעל L. ∎

משפטון 1.8.5: *תהי L/K הרחבה נורמלית של שדות.*

(א) *כל שִׁכּוּן־K של L לתוך $\tilde{K}$ מעתיק את L על עצמו.*

(ב) *כל איזומורפיזם־K $\sigma\colon E \to E'$ של שדות בינַיִם של L/K נִתן להרחבה לאוטומורפיזם־K של L.*

הוכחת א: לפי ההנחה, L מתקבלת מ K על ידי צֵרוף כל השרשים השַיָכים ל $\tilde{K}$ של קבוצת פולינומים $\mathcal{F}$ עם מקדמים ב K. אם σ הוא שִכּוּן־K של L לתוך $\tilde{K}$, אזי σ מתמיר את קבוצת השרשים הנ"ל. לכן, σ שומר על L.

הוכחת ב: השדה L הוא גם שדה הפִצול של $\mathcal{F}$ מעל E. לפי משפטון 1.8.1 נִתן להרחיב את σ לאיזומורפיזם של L על שדה הפצול של $\mathcal{F}$ ב $\tilde{K}$. איזומורפיזם זה יעתיק את L, לפי (א), על L, כמבֻקש. ∎

דֻגמה 1.8.6: אם $K \subseteq L \subseteq M$ ו M נורמלי מעל K, אזי L אינו בהכרח נורמלי מעל K.

ואכן, לפי בֹחן אייזנשטיין (משפטון 1.1.9), הפולינום $X^4 - 2$ אי פריק מעל $\mathbb{Q}$. יהי $\sqrt[4]{2}$ השרש הממשי החיובי שלו ונסמן $L = \mathbb{Q}(\sqrt[4]{2})$. השָרשים של $X^4 - 2$ הם $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, באשר $i^2 = -1$. הואיל ו i אינו שַיָך ל $\mathbb{R}$, הוא אינו שַיָך גם ל $\mathbb{Q}(\sqrt[4]{2})$, לכן $i\sqrt[4]{2} \notin L$. מכאן ש L אינו נורמלי מעל $\mathbb{Q}$.

מאידך $M = \mathbb{Q}(\sqrt[4]{2}, i)$ הוא שדה הפִצול מעל $\mathbb{Q}$ של הפולינום $X^4 - 2$ ולכן M נורמלי מעל $\mathbb{Q}$. ∎

הרחבה L/K תקרא **רִבּועית** L/K אם היא ממעלה 2.

למה 1.8.7: *כל הרחבה רבועית L/K היא נורמלית.*

הוכחה: L הוא שדה שרש מעל K של פולינום אי פריק f ממעלה 2. ל f יש לכל היותר שני שרשים שסכומם שַיָך ל K. לכן שניהם שַיָכים ל L. לפי משפטון 1.8.3 ש L נורמלי מעל K.

דֻגמה 1.8.8: אם L/K ו M/L הן הרחבות נורמליות אין M/K בהכרח נורמלית.

ואכן, לפי למה 1.8.7 כל אחת מהרחבות הבֵינַיִם במגדל $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ נורמלית אולם, לפי דֻגמה 1.8.6, ההרחבה $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ אינה נורמלית. ∎

תרגיל 1.8.9: יהי K שדה, יהי $f \in K[x]$ פולינום אי פריק, תהי L הרחבה נורמלית סופית של K ויהיו $g, h \in L[X]$ גורמים אי פריקים של $f(X)$. הוכח שקַיָם אוטומורפיזם σ של L מעל Kכך ש $\sigma(g) = h$. ∎

1.9 משפט האבר הקדום

מקום מרכזי בתורת גלואה של שדות באִפיון 0 תופשות ההרחבות הנורמליות. באִפיון חיובי צריכים להוסיף לנורמליות תכונה נוספת המכֻנה "פרידות". אנו נוכיח בסעיף זה שכל הרחבה פרידה סופית נוצרת על ידי אבר אחד.

פולינום $f \in K[X]$ עם מקדמים בשדה K נקרא **פריד** אם כל שרשיו פשוטים. אומרים על אבר $x \in \tilde{K}$ שהוא **פריד מעל** K אם $\mathrm{irr}(x,K)$ פריד. לבסוף, הרחבה אלגברית E/K מכֻנה **פרידה** אם כל אבר של E פריד מעל K.

משפטון 1.9.1: *כל הרחבה אלגברית E/K באִפיון אפס פרידה.*

הוכחה: לפי משפטון 1.5.12, כל פולינום אי פריק באפיון 0 פריד. לכן, כל הרחבה אלגברית באפיון אפס פרידה. ∎

הגדרה 1.9.2: אומרים ששדה K הנו **משֻׁכלל** אם כל הרחבה אלגברית שלו פרידה. ∎

משפטון 1.9.3:

(א) *כל שדה בעל אפיון 0 הוא משֻׁכלל.*

(ב) *כל שדה סגור אלגברית הנו משֻׁכלל.*

(ג) *שדה K בעל אפיון חיובי p הנו משֻׁכלל אם ורק אם $K^p = K$ (באשר K^p מסמן כאן את אסף כל חזקות־p של אברי K).*

(ד) *אם שדה K הנו משֻׁכלל, כל הרחבה אלגברית שלו הנה משֻׁכללת.*

(ה) *כל שדה סופי הנו משֻׁכלל.*

(ו) *השדה $\mathbb{F}_p(t)$ (עם t נעֲלה) אינו משֻׁכלל.*

הוכחת ג: נניח קודם ש $K^p = K$ ויהי $f \in K[X]$ פולינום אי פריק. נניח בשלילה ש f אינו פריד. אזי, לפי משפטון 1.5.12(ב), קיָם $g \in K[X]$ כך ש $f(X) = g(X^p)$. אם נרשֹם את g בפרוט, $g(X) = \sum_{i=0}^{n} a_i X^i$, נקבל מההנחה שקיָמים $b_i \in K$ כך ש $b_i^p = a_i$. לכן, $f(X) = \sum_{i=0}^{n} a_i X^{ip} = \sum_{i=0}^{n} b_i^p X^{ip} = (\sum_{i=0}^{n} b_i X^i)^p$, בסתירה להנחה ש f אי פריק.

להפך, נניח ש K משֻׁכלל. יהי $a \in K$ ונבחר $b \in \tilde{K}$ כך ש $b^p = a$. אזי $X^p - a = (X-b)^p$ ולכן, יש ל $g(X) = \mathrm{irr}(b,K)$, בתור מחלק של $X^p - a$, שרש אחד בלבד והוא b. הואיל ו K משֻׁכלל, b הוא שרש פשוט של g. לכן, $\deg(g) = 1$ ומכאן ש $b \in K$, כמבֻקש.

הוכחת ד: כל אבר אלגברי x מעל L הוא גם אלגברי מעל K. לכן כל שרשי $\mathrm{irr}(x,K)$ פשוטים. הואיל ו $\mathrm{irr}(x,L) | \mathrm{irr}(x,K)$ גם כל שרשי L פשוטים. לכן, L משֻׁכלל.

הוכחת ה: יהי K שדה סופי בעל אִפיון חיובי p. אזי, ההעתקה $x \mapsto x^p$ של K לתוך עצמו הנָה חד חד ערכית. לכן, היא גם על. במלים אחרות, לכל $y \in K$ קיָם $x \in K$ כך ש $y = x^p$. לפי (ג), K משֻכלל.

הוכחת ו: לפי דֻגמה 1.5.13, הפולינום האי פריק $X^p - t$ אינו פריד. לכן, $\mathbb{F}_p(t)$ אינו משֻכלל. ∎

אחת מהתכונות החשובות של הרחבות פרידות סופיות היא שהן נוצרות על ידי אבר אחד. בהוכחה אנו מבדילים בין המקרה שהשדות אינסופיים למקרה שהשדות סופיים. כדי לטפל במקרה האחרון זקוקים אנו לתוצאה העומדת בין תורת החבורות ותורת השדות.

משפטון 1.9.4: *יהי K שדה. אזי כל תת חבורה סופית G של החבורה הכפלית $K^\times$ של K הנה מעגלית.*

הוכחה: לפי המשפט היסודי של החבורות האבליות הסופיות, G היא מכפלה ישרה של חבורות סילו שלה. לכן, מספיק להוכיח את המשפטון במקרה ש G היא מסדר p^n באשר p מספר ראשוני. יהי g אבר בעל סדר מרבי ב G. בחבורה סופית הסדר של כל אבר מחלק את הסדר של החבורה. לכן, $\mathrm{ord}(g) = p^m$, באשר $m \le n$. אם $x \in G$ הוא אבר כלשהוא של G, אזי $\mathrm{ord}(x) = p^k$ באשר $k \le m$. לכן, $x^{p^m} = (x^{p^k})^{p^{m-k}} = 1$. אנו מקבלים אפוא שלפולינום $X^{p^m} - 1$ יש ב K לפחות p^n שרשים. מצד שני יש למשואה הזו לכל היותר p^m שרשים (תוצאה 1.5.2). לכן, $m = n$ ומכאן ש G מעגלית ונוצרת על ידי g. ∎

משפט 1.9.5 (משפט האבר הקדום של Abel): *תהי $L = K(x_1, \cdots, x_n)$ הרחבה סופית של שדה K. נניח ש $x_2, \ldots, x_n$ פרידים מעל K. אזי קיָם $z \in L$ כך ש $L = K(z)$. האבר z יקרא* **אבר קדום של ההרחבה** L/K.

הוכחה: אם K סופי, אזי גם L סופי, בתור מרחב וקטורי מממד סופי מעל K. בפרט $L^\times$ היא חבורה סופית. יהי z יוצר שלה (משפטון 1.9.4). אזי $L = K(z)$.

נניח אפוא ש K אינסופי. השראה על n מראה שמספיק להוכיח שאם x אלגברי מעל K ו y אלגברי פריד מעל K, אזי קיָם z כך ש $K(x, y) = K(z)$.

נסמן אפוא $f = \mathrm{irr}(x, K)$ ויהיו $x_1, \ldots, x_m$ השרשים השונים של f ב $\tilde{K}$. לפי ההנחה $g = \mathrm{irr}(y, K)$ הנו פולינום אי פריק ממעלה d ו $g(Y) = \prod_{j=1}^d (Y - y_j)$ הוא פרוק לגורמים לינאריים שונים זה מזה מעל $\tilde{K}$. הפולינום

$$q(T) = \prod_{(i,j) \ne (i',j')} \big((x_i + Ty_j) - (x_{i'} + Ty_{j'})\big)$$

שיָך ל $\tilde{K}[T]$ ושונה מאפס. הואיל ו K אינסופי, קיָם לפי תוצאה 1.5.4 אבר $b \in K$ כך ש $q(b) \ne 0$. במִלים אחרות,

$$x_i + by_j \ne x_{i'} + Ty_{j'} \tag{1}$$

לכל $(i,j) \neq (i',j')$.

בלי הגבלת הכלליות, $x = x_1$ ו $y = y_1$. נסמן $z = x + by$. אזי $K(z) \subseteq K(x,y)$. כדי להוכיח את ההכלה בכִוון הֶהפוך נתבונן בפולינום $h(Y) = f(z - bY)$ שמקדמיו ב $K(z)$. הוא מקיֵם $h(y) = f(z - by) = f(x) = 0$. בנוסף לזה נובע מ (1) ש $z - by_j \neq x_i$ לכל i ולכל $j \neq 1$ ולכן $h(y_j) = f(z - by_j) \neq 0$. קִבלנו אפוא ש y הנו השרש היחיד המשֻתף ל g ו h. לכן $\gcd(g,h) = (Y - y)^k$ עבור איזה שהוא $k \geq 1$. הואיל ולפי ההנחה $(Y - y)^2 \nmid g(Y)$, נובע ש $k = 1$, כלומר $\gcd(g,h) = Y - y$. הואיל ומקדמי הפולינומים g, h שיָכים ל $K(z)$ גם מקדמי המחלק המשֻתף המרבי שלהם שיָכים ל $K(z)$. לכן $y \in K(z)$. מכאן ש $x = z - by \in K(z)$. בסִכומו של דבר הוכחנו ש $K(x,y) = K(z)$, כמבֻקש. ∎

תוצאה 1.9.6: *אם L/K הנה הרחבה פרידה סופית, אזי קיָם $z \in L$ כך ש $L = K(z)$.*

תרגיל 1.9.7: תהי L/K הרחבה סופית שיש לה רק מספר סופי של שדות בינַים. הוכח שקיָם $x \in L$ כך ש $L = K(x)$. ∎

1.10 הרחבות פרידות

בסעיף זה נאפיֵן הרחבה פרידה סופית L של שדה K ככזו שמספר האיזומורפיזמים־K שלה לתוך $\tilde{K}$ שוה למעלתה. כמו כן נראה שקבוצת ההרחבות הפרידות של K סגורה תחת לקיחת תת שדות וצרופים של שדות.

תהי L הרחבה אלגברית של שדה K. נסמן ב $[L:K]_s$ את מספר האיזומורפיזמים־K של L לתוך $\tilde{K}$ ונקרא לו **מעלת הפרידות של L מעל K**. אם L היא הרחבה סופית של K, אזי $L = K(x_1,\ldots,x_n)$. כל איזומורפיזם־K σ של L לתוך $\tilde{K}$ נקבע באפן יחיד על ידי פעֻלתו של $x_1,\ldots,x_n$. הואיל ו σx_i הוא שרש של $\mathrm{irr}(x_i,K)$ ולפולינום זה יש רק מספר סופי של ערכים, יש ל σ רק מספר סופי של אפשריות. במִלים אחרות, $[L:K]_s < \infty$.

למה 1.10.1: *תהי L הרחבה אלגברית של שדה K ויהיו $\sigma\colon K \to K_1$ ו $\tau\colon K \to K_2$ איזומורפיזמים של שדות. נסמן ב $S(\sigma)$ את קבוצת כל ההרחבות של σ לשכון של L לתוך $\tilde{K}_1$ וב $S(\tau)$ את קבוצת כל ההרחבות של τ לשִכול של L לתוך $\tilde{K}_2$. אזי $|S(\sigma)| = |S(\tau)|$. יתר על כן, $|S(\sigma)| = [L:K]_s$.*

הוכחה: נבחר הרחבה $\tilde{\sigma}$ של σ לאיזומורפיזם $\tilde{K} \to \tilde{K}_1$ ונבחר הרחבה $\tilde{\tau}$ של τ לאיזומורפיזם $\tilde{K} \to \tilde{K}_2$. אם $\sigma' \in S(\sigma)$, אזי $(\tilde{\tau}\circ\tilde{\sigma}^{-1})|_{\sigma'(L)} \circ \sigma' \in S(\tau)$. ההעתקה ההפוכה נִתנת על ידי הִפוך התפקידים של σ ו τ, כלומר $\tau' \mapsto (\tilde{\sigma}\circ\tilde{\tau}^{-1})|_{\tau'(L)} \circ \tau'$. לכן, $S(\sigma)$ ו $S(\tau)$ שוות עצמה.

בפרט, אם נקח $K_2 = K$ ו $\tau = \mathrm{id}_K$ נקבל ש $|S(\sigma)|$ הוא מספר האיזומורפיזמים־K של L לתוך $\tilde{K}$, כלומר $|S(\sigma)| = [L:K]_s$. ∎

משפטון 1.10.2: *יהי $K \subseteq L \subseteq M$ מגדל של הרחבות סופיות. אזי* $[M:K]_s = [M:L]_s[L:K]_s$.

הוכחה: נסמן $l = [L:K]_s$ ויהיו $\sigma_1,\ldots,\sigma_l$ כל השִכונים־K של L לתוך $\tilde{K}$. לכל i תהי $S(\sigma_i)$ קבוצת כל ההרחבות של σ_i לשִכון של M לתוך $\tilde{K}$. אזי $S = \dot{\bigcup}_{i=1}^{l} S(\sigma_i)$ היא קבוצת כל השִכונים־K של M לתוך $\tilde{K}$. לפי למה 1.10.1, $|S(\sigma_i)| = [M:L]_s$. לכן,

$$[M:K]_s = |S| = |\dot{\bigcup_{i=1}^{l}} S(\sigma_i)| = \sum_{i=1}^{l} |S(\sigma_i)| = l[M:L]_s\,,$$

כפי שהיה להוכיח. ∎

משפטון 1.10.3: *תהי L הרחבה סופית של שדה K. אזי:*

(א) $[L:K]_s \le [L:K]$.

(ב) *אם $x \in \tilde{K}$, אזי מספר הצמודים של x מעל K שוה ל $[K(x):K]_s$. יתר על כן, x פריד מעל K אם ורק אם* $[K(x):K]_s = [K(x):K]$.

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

(ד) *תהי L/K הרחבה ממעלה סופית n ויהי $x \in L$. אם מספר הצמודים של x מעל K הוא n, אזי $L = K(x)$.*

הוכחת א: נטפל קודם במקרה שבו $L = K(x)$. יהיו $x_1, \ldots, x_m$ השרשים השונים של $\mathrm{irr}(x, K)$ ב $\tilde{K}$. אזי $m \le \deg(\mathrm{irr}(x, K)) = [K(x) : K]$. מאידך m הוא מספר שכוני־K של $K(x)$ לתוך $\tilde{K}$ (משפטון 1.3.4), כלומר $m = [L : K]_s$. לכן, $[L : K]_s \le [L : K]$.

במקרה הכללי $L = K(y_1, \ldots, y_n)$. השראה על n נותנת ש

$$[K(y_1, \ldots, y_{n-1}) : K]_s \le [K(y_1, \ldots, y_{n-1}) : K]. \tag{2}$$

ל המקרה $n = 1$ שהוכח בפסקה הקודמת מבטיח ש

$$[L : K(y_1, \ldots, y_{n-1})]_s \le [L : K(y_1, \ldots, y_{n-1})] \tag{3}$$

מִנֻסחאות המגדל 1.4.4 ו 1.10.2, מ (2) ו (3) נובע ש $[L : K]_s \le [L : K]$.

הוכחת ב: מספר הצמודים ל x מעל K שוה למספר השרשים השונים של $\mathrm{irr}(x, K)$ ומספר זה שוה, לפי הערה 1.7.10, למספר שכונֵי־K של $K(x)$ לתוך $\tilde{K}$ כלומר ל $[K(x) : K]_s$.

השויון $[K(x) : K]_s = [K(x) : K]$ מתקיֵם אם ורק אם מספר השרשים השונים של $\mathrm{irr}(x, K)$ שוה למעלה של $\mathrm{irr}(x, K)$. זה קורה אם ורק אם $\mathrm{irr}(x, K)$ פריד, כלומר אם x פריד מעל K.

הוכחת ג: נניח קודם ש $[L : K]_s = [L : K]$. יהי $x \in L$. אזי, לפי נֻסחאות המגדל,

$$[L : K(x)]_s [K(x) : K]_s = [L : K(x)][K(x) : K].$$

לפי חלק א, $[L : K(x)]_s \le [L : K(x)]$ ו $[K(x) : K]_s \le [K(x) : K]$. לכן,

$$[K(x) : K]_s = [K(x) : K].$$

לפי (ב), x אלגברי פריד מעל K. מכאן נובע ש L/K הנה הרחבה פרידה.

להפך, נניח ש L/K הנה הרחבה פרידה. אם $L = K$, אזי בודאי $[L : K]_s = [L : K]$. אחרת, נבחר $x \in L \smallsetminus K$. אזי x פריד מעל K ולכן, לפי (ב), $[K(x) : K]_s = [K(x) : K]$. יִשום של נֻסחאות המגדל והשראה על המעלה נותנים ש $[L : K]_s = [L : K]$.

הוכחת ד: לפי (ב),

$$n = [K(x) : K]_s \le [K(x) : K] \le [L : K] = n.$$

לכן, $L = K(x)$. ∎

משפטון 1.10.4: *יהי $K \subseteq L \subseteq M$ מגדל של הרחבות אלגבריות.*

(א) *אם ההרחבה M/K פרידה, גם L/K ו M/L פרידות.*

(ב) *אם x אלגברי פריד מעל K, ההרחבה $K(x)/K$ פרידה.*

(ג) *אם ההרחבות L/K ו M/L פרידות, גם M/K פרידה.*

(ד) *אם E ו L הנן הרחבות אלגבריות פרידות של K, גם EL/K פרידה.*

הוכחת א: כל אבר של L הוא גם אבר של M ולכן פריד מעל K. מכאן שההרחבה L/K פרידה.

אם $x \in M$, אזי כל השרשים של $\mathrm{irr}(x, K)$ ב $\tilde{K}$ פשוטים. הואיל ו $\mathrm{irr}(x, L)$ מחלק את $\mathrm{irr}(x, K)$, גם כל השרשים של $\mathrm{irr}(x, L)$ ב $\tilde{K}$ פשוטים. לכן גם ההרחבה M/L פרידה.

הוכחת ב: מההנחה על x נובע שמספר השרשים של $\mathrm{irr}(x, K)$ ב $\tilde{K}$ שוה למעלתו. לכן, $[K(x) : K]_s = [K(x) : K]$. לפי משפטון 1.10.3, $K(x)$ פריד מעל K.

הוכחת ג: יהי $x \in M$. אזי $\mathrm{irr}(x, L)$ הוא פולינום פריד. מקדמיו יוצרים הרחבה סופית L_0 של K המוכלת ב L. לפי (א), L_0 פרידה מעל K. בנוסף $M_0 = L_0(x)$ פריד מעל L_0, (לפי (ב)). לכן, מספיק להוכיח את טענה (ב), במקרה ש $[M : K] < \infty$. במקרה זה נוכל להשתמש בנֻסחאות המגדל ובמשפטון 1.10.3, כדי לרשֹם את השויונות

$$[M : K]_s = [M : L]_s[L : K]_s = [M : L][L : K] = [M : K]$$

ולהסיק ש M/L פרידה.

הוכחת ד: שוב נוכח להניח, בלי הגבלת הכלליות, ש L/K הנה הרחבה סופית. יהי x אבר קדום שלה (משפט 1.9.5). אזי, $EL = E(x)$. מכך ש L/K פרידה נובע שכל שרשי $\mathrm{irr}(x, K)$ ב $\tilde{K}$ פשוטים. הואיל ו $\mathrm{irr}(x, E)$ מחלק את $\mathrm{irr}(x, K)$ גם כל שרשי $\mathrm{irr}(x, E)$ פשוטים. לכן, ההרחבה EL/E פרידה. הואיל וגם E/K פרידה, נובע מ (א) שגם EL/K פרידה. ∎

מסקנה 1.10.5: *יהי K שדה ו $x, y \in \tilde{K}$. אם x, y פרידים מעל K, אזי גם $x + y$, xy ו $\frac{x}{y}$ (אם $y \neq 0$) פרידים מעל K. לכן אסף האברים הפרידים מעל K של $\tilde{K}$ מהוה שדה הנקרא* **הסגוֹר הפריד של** K *והמסֻמן ב K_s. שדה זה הוא אחוד כל ההרחבות הפרידות הסופיות של K.*

תרגיל 1.10.6: תהי $L = K(x_1, \ldots, x_m)$ הרחבה פרידה של שדה אינסופי K. הוכח שקיָמים $a_1, \ldots, a_n \in K$ כך ש $x = a_1x_1 + \cdots + a_nx_n$ הוא אבר קדום של ההרחבה L/K. ∎

אנו מראים בסעיף זה שכל הרחבה אלגברית נתנת להשגה בשני שלבים, קודם כל הרחבה פרידה ואחר כך הרחבה אי פרידה בטָהֳרה.

משפטון 1.11.1: *אם L/K הנה הרחבה אלגברית, אזי האֹסף L_0 כל האברים הפרידים של L מעל K הנה ההרחבה הפרידה המרבית של K בתוך L. לכל $x \in L \smallsetminus L_0$ ההרחבה $L_0(x)/L_0$ אינה פרידה. יתר על כן, במקרה זה $p = \mathrm{char}(K) \neq 0$ ו x הוא שרש של פולינום אי פריק מהצורה $X^{p^n} - a$, באשר $a \in L_0$.*

הוכחה: החלק הראשון של המשפטון הוא מסקנה ישירה של מסקנה 1.10.5. ליֶתר דיוק, $L_0 = L \cap K_s$.

נתבונן עתה באבר $x \in L \smallsetminus L_0$. אזי x אינו פריד מעל L_0 (אחרת היה x, לפי משפטון 1.10.4, פריד מעל K ולכן שיָך ל L_0). לכן, יש ל $f(X) = \mathrm{irr}(x, L_0)$ שרשים מרֻבים ו $p = \mathrm{char}(K) \neq 0$ (משפטון 1.9.3). יתר על כן, לפי משפטון 1.5.12(ב), קיָם $g \in L_0[X]$ כך ש $f(X) = g(X^p)$. יהי n המספר הטבעי הגדול ביותר שעבורו קיָם $h \in L[X_0]$ כך ש $f(X) = h(X^{p^n})$. נסמן $a = x^{p^n}$. אזי, $h(a) = h(x^{p^n}) = f(x) = 0$. אלו היה ל h פרוק לא טריביאלי $h = h_1h_2$ מעל L_0, היינו מקבלים פרוק לא טריביאלי $f(X) = h(X^{p^n}) = h_1(X^{p^n})h_2(X^{p^n})$ מעל L_0, בסתירה להגדרת f. לכן, h אי פריק מעל L_0. אִלו לא היה a שיָך ל L_0, היה a שרש מרֻבה של h. לכן, שוב לפי משפטון 1.5.12(ב), היה קיָם פולינום $h_0 \in L_0[X]$ כך ש $h(X) = h_0(X^p)$. לכן היה $f(X) = h_0(X^{p^{n+1}})$, בסתירה למרביות של n. מִסתירה זו נובע ש $a \in L_0$, כמבֻקש. ∎

משפטון 1.11.2: *יהי K שדה בעל אִפיון חיובי p ותהי L הרחבה אלגברית של K. הטַעֲנות הבאות שקולות זו לזו:*

(א) $[L : K]_s = 1$.

(ב) *כל אבר של L הִנו* **אי פריד בטהֳרה מעל** *K כלומר, קיָם n שלם אי שלילי כך ש $x^{p^n} \in K$.*

(ג) *כל אבר $x \in L$ הנו שרש של פולינום אי פריק מעל K מהצורה $X^{p^n} - a$.*

(ד) *L נוצר מעל K על ידי אברים אי פרידים בטהֳרה.*

הוכחה: בלי הגבלת הכלליות נוכל להניח ש $[L : K] < \infty$.

הוכחת (א) $\Longrightarrow$(ב) ו (ג): תהי L_0 ההרחבה הפרידה המרבית של K בתוך L. לפי נֻסחת המגדל לדרגת הפרידות, $[L_0 : K]_s = 1$. מאידך, $[L : K] = [L_0 : K]_s$ (משפטון 1.10.3). לכן, $L_0 = K$. לפי משפטון 1.11.1 מקיֵם כל אבר של L משואה אי פריקה מהצורה $X^{p^n} - a = 0$ עם $a \in K$.

הוכחת (ב) $\Longrightarrow$(א): יהי σ שִכון־K של L לתוך $\tilde{K}$. לפי ההנחה, כל אבר $x \in L$ הוא שרש של פולינום אי פריק $f(X) = X^{p^n} - a$ אם $a \in K$. מהזהות $f(X) = (X - x)^{p^n}$ נובע השרש היחיד של $f(X)$ זה הנו x. הואיל ו $f(\sigma x) = \sigma(f(x)) = 0$, אנו מקבלים ש $\sigma x = x$. במִלים אחרות, $\sigma = \mathrm{id}_L$. לכן $[L : K]_s = 1$, כמבֻקש.

(ג) $\Longleftarrow$*(ד)* ו *(ד)* $\Longleftarrow$*(ב)*: ברור. ∎

אין זה קשה לראות שסכום, מכפלה ומנה של אברים ב $\tilde{K}$ אי פרידים בטהֲרה מעל K מהוֶה שוב אבר אי פריד בטהֲרה. לכן, אסף כל אברי $\tilde{K}$ שהם אי פרידים בטהֲרה מעל K מהוה שדה המכֻנה **הסגוֹר האי פריד בטהֲרה המרבית של** K והמסֻמן ב K_{ins}.

תרגיל 1.11.3: יהי p מספר ראשוני, יהי K שדה ויהי a אבר של K. הוכח שאם למשואה $X^p - a$ אין שרשים ב K, אזי הפולינום $X^p - a$ אי פריק. הבדל בהוכחתך בין המקרה $\text{char}(K) = p$ לבין המקרה שבו $\text{char}(K) \neq p$. ∎

תרגיל 1.11.4: יהי K שדה בעל אפיון חיובי p ויהי x אבר אלגברי מעל K. הוכח ש x פריד מעל K אם ורק אם $K(x) = K(x^{p^n})$ לכל n טבעי. ∎

תרגיל 1.11.5: יהיו K שדה בעל אפיון חיובי p ויהיו t, u משתנים לא תלויים אלגברית מעל K.

(א) הוכח ש $[K(t,u) : K(t^p, u^p)] = p^2$.

(ב) הוכח שאם K אינסופי, אזי יש אינסוף שדות השוכנים בין $K(t^p, u^p)$ לבין $K(t,u)$ ∎

1.12 הרחבות נַעֲלות

בסעיף זה נפתֵח את המושגים "בסיס נעֲלות" ו"דרגת נעלות" של הרחבת שדות. אלו הם מושגים בסיסיים בגאומטריה אלגברית אולם אנו לא נזקק להם בפתוח של תורת גלואה.

תהי F/K הרחבה של שדות. אומרים על אברים $t_1, \ldots, t_n$ של F **שאינם תלויים אלגברית** אם $f(t_1, \ldots, t_n) \neq 0$ לכל $f \in K[X_1, \ldots, X_n]$ שונה מאפס. אומרים על תת קבוצה T של F שהיא **אינה תלויה אלגברית** מעל K אם כל תת קבוצה סופית שלה אינה תלויה אלגברית מעל K. לבסוף, תת קבוצה B של F הנה **בסיס נעֲלות** של F/K, אם B אינה תלויה אלגברית מעל K ואם $F/K(B)$ היא הרחבה אלגברית.

משפטון 1.12.1 (קיום בסיס נעלות): *יהיו F/K הרחבת שדות, T תת קבוצה של F ו A תת קבוצה של T. נניח ש A אינה תלויה אלגברית מעל K ו $F/K(T)$ הנה הרחבה אלגברית. אזי קיָם ל F/K בסיס נעלות B כך ש $A \subseteq B \subseteq T$.*

הוכחה: נסדר את אֹסף תת הקבוצות של T לפי הכלה. אחוד שרשרת של תת קבוצות ש T המַקיפות את A ואינן תלויות אלגברית מעל K הוא שוב קבוצה שאינה תלויה אלגברית מעל K. לכן, לפי הלמה של צורן קיֶמת ל T תת קבוצה מרבית B המקיפה את A ואינה תלויה אלגברית מעל K.

טענה: *כל $t \in T$ אלגברי מעל $K(B)$.* הטענה ברורה אם $t \in B$. נניח אפוא בשלילה ש $t \notin B$ ו t נעלה מעל $K(B)$. אזי $B \cup \{t\}$ אינה תלויה אלגברית מעל K. אחרת קימים $b_1, \ldots, b_m \in B$ שונים זה מזה וקיָם פולינום $f \in K[X_1, \ldots, X_{m+1}]$ שונה מאפס כך ש $f(b_1, \ldots, b_m, t) = 0$. אם נרשם $f(X_1, \ldots, X_{m+1}) = \sum_{i=0}^{d} f_i(X_1, \ldots, X_m)t^i$ נקבל ש $\sum_{i=0}^{d} f_i(b_1, \ldots, b_m)t^i = 0$ ולכן $f_i(b_1, \ldots, b_m) = 0$. הואיל ו $b_1, \ldots, b_m$ אינם תלויים אלגברית, $f_i = 0$ עבור כל i. לכן, $f = 0$, בסתירה להנחה. מסתירה זו נובע שאכן t אלגברי מעל $K(t)$.

מהטענה נובע ש $K(T)$ אלגברי מעל $K(B)$. הואיל ולפי ההנחה F אלגברי מעל $K(T)$, אנו מקבלים ש F אלגברי מעל $K(B)$. בסִכומו של דבר אנו מקבלים ש B הנו בסיס של F/K. ∎

עתה נרצה להוכיח את יחידות העָצמה של בסיסי הנעלות. תכונה זו דומה ליחידות העצמה של הבסיסים של מרחב וקטורי והוכחתה מתבססת בראש וראשונה על למת החלפה.

למת החלפה 1.12.2: *יהיו F/K הרחבת שדות, $u_1, \ldots, u_n$ אברים של F כך ש $F/K(u_1, \ldots, u_n)$ הנה הרחבה אלגברית, ו $t_1, \ldots, t_m$ אברים של F שאינם תלויים אלגברית מעל K. אזי $m \leq n$ וקיֶמת תמורה σ של הקבוצה $\{1, \ldots, n\}$ כך ש $F/K(t_1, \ldots, t_m, u_{\sigma(m+1)}, \ldots, u_{\sigma(n)})$ הנה הרחבה אלגברית.*

הוכחה: השראה על m אומרת ש $m - 1 \leq n$ ונותנת תמורה κ של $\{1, \ldots, n\}$ כך ש F אלגברי מעל השדה

$$.E = K(t_1, \ldots, t_{m-1}, u_{\kappa(m)}, \ldots, u_{\kappa(n)})$$

בפרט t_m אלגברי מעל E. קיָם אפוא פולינום שונה מאפס $f \in K[X_1, \dots, X_{n+1}]$ כך ש

$$.f(t_1, \dots, t_m, u_{\kappa(m)}, \dots, u_{\kappa(n)}) = 0 \tag{1}$$

אחד מהאברים $u_{\kappa(m)}, \dots, u_{\kappa(n)}$ חיָב להופיע באגף שמאל של (1), אחרת היינו מקבלים סתירה לאי התלות האלגברית של $t_1, \dots, t_m$. קיֶמת אפוא תמורה λ של הקבוצה $\{\kappa(m), \dots, \kappa(n)\}$ כך ש $\lambda(\kappa(m))$ מופיע באגף שמאל של (1). נרחיב את λ לתמורה של הקבוצה $\{1, \dots, n\}$ ונסמן $\sigma = \lambda \circ \kappa$. אזי $u_{\sigma(m)}$ אלגברי מעל השדה $E' = K(t_1, \dots, t_m, u_{\sigma(m+1)}, \dots, u_{\sigma(n)})$. הואיל ו F אלגברי מעל $K(t_1, \dots, t_m, u_{\sigma(m)}, \dots, u_{\sigma(n)})$ נקבל ש F אלגברי גם מעל $K(t_1, \dots, t_m, u_{\sigma(m+1)}, \dots, u_{\sigma(n)})$, כמבֻקש. ■

משפטון 1.12.3: *יהיו* B, B' *שני בסיסֵי נעלות של הרחבת שדות* F/K. *אזי* $|B| = |B'|$.

הוכחה: נניח קודם שאחד משני הבסיסים סופי. למשל B' סופי בעל n אברים. הואיל ו $F/K(B')$ אלגברי, אומרת למת ההחלפה 1.12.2 שמספר אברי B אינו עולה על n. בפרט B סופית. מאותה סבה, $|B| \leq |B'|$. לכן, $|B| = |B'|$.

עתה נניח שגם B וגם B' אינסופיים. כל $b' \in B'$ אלגברי מעל $K(B)$ ולכן קיֶמת ל B תת קבוצה סופית $B_{b'}$ כך ש b' אלגברי מעל $K(B_{b'})$. נסמן $A = \bigcup_{b' \in B'} B_{b'}$ ונניח בשלילה שקיָם $b \in B \smallsetminus A$. האבר b אלגברי מעל $K(B')$ ולפי הבניה $K(A, B')$ אלגברי מעל $K(A)$. לכן, b אלגברי מעל $K(A)$, בסתירה לאי התלות האלגברית של $A \cup \{b\}$..

קבלנו אפוא ש $B = \bigcup_{b' \in B'} B_{b'}$. לכן $|B| \leq |B'|\aleph_0 = |B'|$. באֹפן סימטרי נובע ש $|B'| \leq |B|$. לכן, $|B| = |B'|$. ■

לערך המשֻתף של כל העָצמות של בסיסי הנעלות של הרחבת שדות F/K קוראים **מַעֲלת הנעלות** של F/K ומסמנים אותו ב $\mathrm{trans.deg}(F/K)$.

משפטון 1.12.4: *יהיו* E/K *ו* F/E *הרחבות של שדות. אזי*

$$.\mathrm{trans.deg}(F/K) = \mathrm{trans.deg}(F/E) + \mathrm{trans.deg}(E/K)$$

הוכחה: יהי A בסיס נעלות של E/K ויהִי B בסיס נעלות של F/E. אזי A זר ל B, יתר על כן האחוד $A \cup B$ אינו תלוי אלגברית מעל K. בנוסף ההרחבה $E/K(A)$ אלגברית, לכן $E(B)/K(A, B)$ אלגברית. כמו כן, $F/E(B)$ אלגברית. לכן, $F/K(A, B)$ אלגברית. מכל זה נובע ש $A \cup B$ מהוה בסיס נעלות ל F/K. לכן, $\mathrm{trans.deg}(F/K) = |A| + |B| = \mathrm{trans.deg}(E/K) + \mathrm{trans.deg}(F/E)$, כפי שהיה להוכיח. ■

1.13 המשפט היסודי של האלגברה

המשפט היסודי של האלגברה אומר ששדה המספרים המרְכבים $\mathbb{C}$ סגור אלגברית. בסעיף זה נִתן הוכחה למשפט זה המְשתת על תכונות פונקציה רציפה במשתנה מרְכב, מה ששקול לתכונות של פונקציה רציפה בשני משתנים ממשיים. בקורס תורת הפונקציות המרְכבות מוכיחים את המשפט כתוצאה של משפט ויירשטרס האומר שפוקציה אנליטית חסומה בכל המישור המרְכב הנה קבועה. בסעיף 2.10 נביא הוכחה נוספת למשפט זה הנסמכת על תורת גלואה.

משפט: *לכל פולינום ממעלה חיובית עם מקדמים מרְכבים יש שֹרש מרְכב.*

הוכחה: יהי $f \in \mathbb{C}[Z]$ פולינום ממעלה חיובית n. נניח בשלילה ש $f(z) \neq 0$ לכל $z \in \mathbb{C}$. נסמן $c_1 = \inf_{|z|\le 1} |f(z)|$. הואיל ו f הוא פולינום, $|f(z)|$ שואף לאינסוף כאשר $|z|$ שואף לאינסוף. לכן, קיָם $r_2 \geq 1$ כך ש $|f(z)| > c_1$ אם $|z| > r_2$. נסמן $c_2 = \inf_{|z|\le r_2} |f(z)|$. אזי

$$c_2 \leq \inf_{|z|\le 1} |f(z)| = c_1 \leq \inf_{|z|> r_2} |f(z)|.$$

מכאן ש $c_2 \leq |f(z)|$ לכל $z \in \mathbb{C}$.

הואיל ו f כפולינום הוא פונקציה רציפה ופונקציה רציפה מקבלת את הערך המזערי בכל עִגול סגור, קיָם z_2 כך ש $|z_2| \leq r_2$ ו $f(z_2) = c_2$. מהנחתנו נובע ש $c_2 > 0$. כמו כן, $|f(z_2)| \leq |f(z)|$ לכל $z \in \mathbb{C}$.

נסמן $g(z) = \frac{f(z+z_2)}{c_2}$. אזי g הוא פולינום ממעלה n המקיֵם $|g(z)| \geq 1 = g(0)$ לכל $z \in \mathbb{C}$. נִתן לרשֹם את g בצורה $g(Z) = 1 + a_k Z^k + \cdots + a_n Z^n$, באשר $a_k, \ldots, a_n \in \mathbb{C}$, $1 \leq k \leq n$ ו $a_k \neq 0$. כמו כן $a_k = re^{\theta\pi i}$, באשר $r > 0$, θ ממשי ו $i = \sqrt{-1}$. נבחר עתה $z = \rho e^{\kappa\pi i}$ עם $\rho > 0$ קטן דַיו ו κ ממשי המקיְמים:

(א) $\theta + k\kappa = -1$,

(ב) $|a_{k+1}z + \cdots + a_n z^{n-k}| < r$.

מהזהות $e^{-\pi i} = -1$, ומ (א) נובע ש $1 + a_k z^k = 1 + r\rho^k e^{(\theta+k\kappa)\pi i} = 1 - r\rho^k$. לכן נובע מ (ב) שֶ

$$\begin{aligned} |g(z)| &= |1 + a_k z^k + a_{k+1} z^{k+1} + \cdots + a_n z^n| \\ &\leq |1 + a_k z^k| + |a_{k+1} z^{k+1} + \cdots + a_n z^n| \\ &= 1 - r\rho^k + |a_{k+1} z + \cdots + a_n z^{n-k}|\rho^k < 1 \end{aligned}$$

בסתירה לכך שהערך המזערי ש g מקבל על $\mathbb{C}$ הוא 1. ∎

2. תורת גלואה

כפי שצִיַנו בהקדמה לפרק הראשון, הרחבת שדות L/K נקראת "הרחבת גלואה" אם היא פרידה ונורמלית. להרחבה כזו אנו מתאימים את "חבורת גלואה", כלומר את החבורה $\mathrm{Gal}(L/K)$ של כל האוטומורפיזמים של L המשביתים כל אחד מאברי K. המשפט היסודי של תורת גלואה בונה התאמה חד חד ערכית הופכת סדר בין שְׂריג שדות הבינַיִם של הרחבת גלואה סופית L/K לבין תת החבורות של $\mathrm{Gal}(L/K)$. לשדה בינַיִם E התאמה זו מתאימה את תת החבורה $\mathrm{Gal}(L/E)$.

בעִקבות משפט זה מבקשת תורת גלואה לתאר את כל חבורות גלואה של הרחבות גלואה של שדה נתון K. בפרט, אם K הוא שדה סופי, אזי סדרו הוא חזקה q של מספר ראשוני. במקרה זה, אם L הוא הרחבה ממעלה n של K, אזי $\mathrm{Gal}(L/K)$ היא חבורה מעגלית הנוצרת על ידי "אוטמורפיזם פרובניוס" המֻגדר על ידי $x \mapsto x^q$. להפך, כל חבורה מעגלית סופית מופיעה כחבורת גלואה כזו.

המצב פחות ברור מעל $\mathbb{Q}$. במקרה זה אין יודעים מהן החבורות הסופיות המופיעות כחבורות גלואה. אנו נראה פה שכל חבורה אבלית סופית וכל חבורה סימטרית נתנות לממוש מעל $\mathbb{Q}$. כמו כן נראה שנִתן לפתר משואה אלגברית עם מקדמים ב $\mathbb{Q}$ בעזרת ארבעת פעֻלות החשבון הרגילות והוצאות שרש אם חבורת גלואה שלה מעל $\mathbb{Q}$ פתירה. בפרט, נקבל שהמשואה הכללית ממעלה שאינה קטנה מ 5 אינה נתנת לפתרון בעזרת הוצאות שרש.

נושא קרוב הוא בנִיות בעזרת סרגל ומחֻגה. בניות אלו קשורות להרחבות־2 של $\mathbb{Q}$. בעזרת מושג זה נוכיח שאי אפשר לרבע את העִגול ואי אפשר לחלק זוית כללית לשלשה חלקים שוים בעזרת סרגל ומחֻגה.

2.1 המשפטים היסודיים של תורת גלואה

המשפט היְסודי של תורת גלואה מתאר התאמה חד חד ערכית על הופכת סדר בין שריג שדות הבינַיִם של הרחבת גלואה סופית L/K לשריג תת החבורות של חבורת גלואה $\mathrm{Gal}(L/K)$. משפט זה מתקבל מצרוף כל הלמות והמשפטונים המופיעים בסעיף זה.

הרחבה L של שדה K נקראת **הרחבת גלואה** אם היא אלגברית, נורמלית ופרידה. אֹסף כל האוטומורפיזמים־K של L מהוֶה חבורה תחת פעֻלת ההרכבה הנקראת **חֲבורת גלואה של L מעל K** והמסֻמנת ב $\mathrm{Gal}(L/K)$.

בהנתן שדה L וַחֲבורת אוטומורפיזמים G שלו, נסמן ב L^G את אסף אברי L **המֻשבתים** תחת G, כלומר

$$L^G = \{x \in L \mid \ \sigma x = x \text{ for all } \sigma \in G\}$$

אסף זה מהוה תת שדה של L הנקרא **שדה השֶבֶת של G**.

למה 2.1.1: *תהי L/K הרחבת גלואה ותהי $G = \mathrm{Gal}(L/K)$. אזי:*

(א) $K = L^G$.

(ב) *אם E הוא שדה בינַיִם של L/K, אזי L/E היא הרחבת גלואה.*

(ג) *ההעתקה $E \mapsto \mathrm{Gal}(L/E)$ מעְתיקה את קבוצת שדות הבֵינים של L/K באפן חד חד ערכי לתוך קבוצה תת החבורות של G.*

הוכחת א: מההגדרה נובע ש $K \subseteq L^G$. להפך, נניח בשלילה שקַיָם $x \in L^G \setminus K$. אזי $f = \mathrm{irr}(x, K)$ הוא פולינום אי פריק פריד ממעלה גדולה מ 1, כי L/K הנה הרחבה פרידה. לכן קיָם ל f שרש x' ב $\tilde{K}$ השונה מ x. הואיל ו L/K נורמלי, $x' \in L$. לפי משפטון 1.3.4, קיָם איזומורפיזם־K σ_0 המעתיק את x על x'. לפי משפטון 1.8.5, נִתן להרחיב את σ_0 לאוטומורפיזם־K σ של L. האוטומורפיזם σ ישתיֵך ל G ויקיֵם $\sigma x = x'$. מצד שני, $\sigma x = x$, לפי ההנחה על x. מסתירה זו אנו לומדים ש $x \in K$.

הוכחת ב: לפי תוצאה 1.8.4, L/E הנה הרחבה נורמלית. לפי משפטון 1.10.4, L/E פרידה. לכן, L/E היא הרחבת גלואה.

הוכחת ג: יהיו E ו E' שדות בינַיִם כך ש $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/E')$. נסמן, $H = \mathrm{Gal}(L/E)$ ו $H' = \mathrm{Gal}(L/E')$. לפי (א) ו (ב), $E = L^H$ ו $E' = L^{H'}$. לכן, $E = E'$, כנדרש. ∎

למה 2.1.2 (Emil Artin): *תהי L/K הרחבה אלגברית פרידה ויהי n מספר טבעי. נניח ש $[K(x) : K] \leq n$ לכל $x \in L$. אזי, $[L : K] \leq n$.*

הוכחה: נניח בשלילה ש $[L : K] > n$. אזי קיָמים $x_1, \ldots, x_{n+1} \in L$ שאינם תלויים לינארית מעל K. בפרט, $[K(x_1, \ldots, x_{n+1}) : K] \geq n + 1$. מאידך, לפי משפט האבר הקדום קיָם $x \in L$ כך ש $K(x) = K(x_1, \ldots, x_n)$ ולפי ההנחה $[K(x) : K] \leq n$. מסתירה זו נובע ש $[L : K] \leq n$. ∎

למה 2.1.3: *תהי L/K הרחבה גלואה סופית. אזי,* $|\mathrm{Gal}(L/K)| = [L:K]$.

הוכחה: הלמה הזו היא מקרה פרטי של למה 1.10.1. למרות זאת, בגלל חשיבותה, נביא כאן הוכחה ישירה שלה.

יהי x אבר קדום של ההרחגה הפרידה L/K ויהי $f = \mathrm{irr}(x, K)$. אזי f מתפרק לגורמים לינאריים שונים זה מזה מעל L $f(X) = \prod_{i=1}^{n}(X - x_i)$, באשר $n = [L:K]$ (כי L/K נורמלית). ההתאמה $\mathrm{Gal}(L/K) \mapsto \{x_1, \ldots, x_n\}$ המתאימה לכל σ את השרש x_i של f שעבורו $\sigma x = x_i$ היא חד חד ערכית ועל (משפטון 1.3.4). לכן, $|\mathrm{Gal}(L/K)| = n$, כנִטען. ∎

הערה 2.1.4: *הרחבה של אוטומורפיזמים לשדה הפונקציות הרציונליות.* תהי G חבורת אוטומורפיזמים של שדה L. לכל $\sigma \in G$ נתאים אוטומורפיזם σ' של $L[X]$ בעזרת ההגדרה

$$\sigma'(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \sigma(a_i) X^i$$

עתה נרחיב את σ' לאוטומורפיזם של $L(X)$ שיסֻמן אף הוא ב σ' על ידי שנגדיר $\sigma'\left(\frac{f}{g}\right) = \frac{\sigma' f}{\sigma' g}$. מהכִפליות של σ' על פולינומים נובע שזוהי הגדרה טובה.

ההעתקה $\sigma \mapsto \sigma'$ הנה חד חד ערכית ושומרת על החבור ועל הכפל. במִלים אחרות, היא שִכון של G לתוך חבורת כל האוטומטרופיזמים של $L(X)$. אנו נזהה את σ עם σ' ונִראה את G גם כחבורת אוטומורפיזמים של $L(X)$. ∎

משפטון 2.1.5 (Emil Artin): *יהי L שדה ותהי G חבורת אוטומורפיזם מסדר n של L. נסמן $K = L^G$. אזי L/K היא הרחבת גלואה מסדר n ו* $\mathrm{Gal}(L/K) = G$.

הוכחה: ראשית נוכיח שלכל $x \in L$ ההרחבה $K(x)$ הנה פרידה ממעלה $\geq n$. לצרך זה יהיו $\sigma_1 x, \ldots, \sigma_m x$ האברים השונים של הקבוצה $A = \{\sigma x \mid \sigma \in G\}$. לכל $\tau \in G$ ההעתקה $\sigma x \mapsto \tau\sigma x$, מעתיקה את A באֹפן חד חד ערכי לתוך עצמה. הואיל ו A סופית, העתקה זו היא על. לכן $(\tau\sigma_1 x, \ldots, \tau\sigma_m x)$ היא תמורה של ה m־יה $(\sigma_1 x, \ldots, \sigma_m x)$. אם נפעיל את τ על הפולינום $f(X) = \prod_{i=1}^{n}(X - \sigma_i x)$ שמקדמיו ב L, נקבל

$$\tau(f(X)) = \prod_{i=1}^{m}(X - \tau\sigma_i x) = \prod_{i=1}^{m}(X - \sigma_i x) = f(X)$$

לכן, שומר τ את מקדמי f. מכאן ש $f \in K[X]$. הואיל ו $x \in A$, נובע מהגדרת f ש $f(x) = 0$. הואיל ו $\sigma_1 x, \ldots, \sigma_m x$ שונים זה מזה, אנו מקבלים ש x פריד מעל K ו $[K(x):K] \leq m \leq n$. יתר, על כן, $\mathrm{irr}(x, K)$ מחלק את הפולינום $f(X)$ המתפרק לגורמים לינאריים מעל K. לכן, גם $\mathrm{irr}(X, K)$ מתפרק לגורמים לינאריים מעל K (למעשה $f(X) = \mathrm{irr}(x, K)$). מכאן נובע ש L/K גם נורמלי.

אנו מקבלים ש $[L:K]$ היא הרחבת גלואה סופית ו $[K(x):K] \leq n$ לכל $x \in L$. לכן, לפי למה 2.1.2, $[L:K] \leq n$. מצד שני, $G \leq \mathrm{Gal}(L/K)$, ולכן, לפי למה 2.1.3,

$$n = |G| \leq |\mathrm{Gal}(L/K)| = [L:K] \leq n.$$

לכן, $[L:K] = n$ ו $G = \mathrm{Gal}(L/K)$, כפי שהיה להוכיח. ∎

משפטון 2.1.6: *תהי L/K הרחבת גלואה סופית וִיהְיוּ E_1, E_2 שדות בינַיִם. אזי:*

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

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

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

הוכחת א: הגרירה $\Longrightarrow$ נובעת מההגדרות. כדי להוכיח את הגרירה ההפוכה נסמן $H_1 = \mathrm{Gal}(L/E_1)$ ו $H_2 = \mathrm{Gal}(L/E_2)$ ונניח ש $H_2 \leq H_1$. אזי, לפי ההגדרות, $L^{H_1} \subseteq L^{H_2}$. לפי למה 2.1.1(א), $E_1 = L^{H_1} \subseteq L^{H_2} \subseteq E_2$, כנדרש.

הוכחת ב: הואיל ו $E_1 \subseteq E_1E_2$ ו $E_2 \subseteq E_1E_2$, נובעת ההכלה

$$\mathrm{Gal}(L/E_1E_2) \leq \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$$

מההגדרות. להפך, אם $\sigma \in \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$, אזי $\sigma x = x$ לכל $x \in E_1$ וגם לכל $x \in E_2$. לכן, $\sigma x = x$ לכל $x \in E_1E_2$. מכאן ש $\sigma \in \mathrm{Gal}(L/E_1E_2)$.

הוכחת ג: נסמן $H_1 = \mathrm{Gal}(L/E_1)$, $H_2 = \mathrm{Gal}(L/E_2)$ ו $H = \langle H_1, H_2 \rangle$. לפי ההגדרות

$$H_1, H_2 \leq \mathrm{Gal}(L/E_1 \cap E_2)$$

ולכן $H \leq \mathrm{Gal}(L/E_1 \cap E_2)$.

להפך, לפי למה 2.1.1(א), $L^H \subseteq L^{H_1} \cap L^{H_2} = E_1 \cap E_2$. לכן, לפי משפטון 2.1.5, $H = \mathrm{Gal}(L/L^H) \geq \mathrm{Gal}(L/E_1 \cap E_2)$.

אם נצרף את המסקנות של שני הסעיפים הקודמים, נקבל את השויון המבֻקש. ∎

משפטון 2.1.7: *תהי L/K הרחבת גלואה סופית, תהי $G = \mathrm{Gal}(L/K)$ ותהיינה H_1 ו H_2 תת חבורות של G. אזי:*

(א) $H_1 \leq H_2 \iff L^{H_2} \subseteq L^{H_1}$.

(ב) $L^{H_1 \cap H_2} = L^{H_1} L^{H_2}$.

(ג) $L^{\langle H_1,H_2\rangle} = L^{H_1}\cap L^{H_2}$.

הוכחה: נסמן $E_1 = L^{H_1}$ ו $E_2 = L^{H_2}$. אזי $\mathrm{Gal}(L/E_1) = H_1$ ו $\mathrm{Gal}(L/E_2) = H_2$ (משפטון 2.1.5). תנאים (א), (ב) ו (ג) נובעים עתה מהתנאים המתאימים במשפטון 2.1.6. לדֻגמה,

$$L^{H_1\cap H_2} = L^{\mathrm{Gal}(L/E_1E_2)} = E_1E_2 = L^{H_1}L^{H_2}. \quad \blacksquare$$

משפטון 2.1.8: *תהי L/K הרחבת גלואה. יהי E שדה בינַיִם ותהי H תת חבורה של $\mathrm{Gal}(L/K)$.*

(א) $\mathrm{Gal}(L/\sigma E) = \sigma\mathrm{Gal}(L/E)\sigma^{-1}$.

(ב) $L^{\sigma H\sigma^{-1}} = \sigma L^H$.

הוכחה: נובעת מההגדרות. $\blacksquare$

משפטון 2.1.9: *תהי L/K הרחבת גלואה ויהי E שדה בינַיִם. אזי E/K הנה הרחבת גלואה אם ורק אם $\mathrm{Gal}(L/E)\triangleleft\mathrm{Gal}(L/K)$. במקרה זה ההעתקה $\sigma\mapsto\sigma|_E$ היא אפימורפיזם של $\mathrm{Gal}(L/K)$ על $\mathrm{Gal}(E/K)$ שגרעינה הוא $\mathrm{Gal}(L/E)$. מכאן ש $\mathrm{Gal}(E/K)\cong\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$.*

הוכחה: נניח קודם ש $\mathrm{Gal}(L/E)$ היא תת חבורה נורמלית של $\mathrm{Gal}(L/K)$. בתור תת שדה של L השדה E פריד מעל K. כדי להוכיח ש E נורמלי מעל K נרחיב כל שכון־K σ_0 של E לתוך $\tilde{K}$ לאוטומורפיזם σ של L (משפטון 1.8.5). מהנורמליות של $\mathrm{Gal}(L/E)$ נובע ש $\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/E)$. לכן, לפי משפטון 2.1.8, $\mathrm{Gal}(L/\sigma E) = \mathrm{Gal}(L/E)$. לפי למה 2.1.1, $\sigma E = E$. לכן, E/K נורמלית ומכאן שהיא גם גלואה.

להפך, אם E/K היא הרחבת גלואה, אזי $\sigma E = E$ לכל $\sigma\in\mathrm{Gal}(L/K)$ ולכן, לפי משפטון 2.1.8, $\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma E) = \mathrm{Gal}(L/E)$. מכאן, ש $\mathrm{Gal}(L/E)\triangleleft\mathrm{Gal}(L/K)$.

נניח עתה את המסקנה האחרונה. אזי, לכל $\sigma\in\mathrm{Gal}(L/K)$ מתקיֵם, לפי ההגדרה, $\sigma|_E = 1$ אם ורק אם $\sigma\in\mathrm{Gal}(L/E)$.

המסקנה האחרונה של המשפטון נובעת ממשפט האיזומורפיזם הראשון של תורת החבורות. $\blacksquare$

משפטון 2.1.10: *תהי L/K הרחבת גלואה סופית ו E הרחבה כלשהיא של K. נניח ש L ו E מוכלים בשדה משֻתף ו $L\cap E = K$. אזי LE/E היא הרחבת גלואה והעתקת הצמצום $\sigma\mapsto\sigma|_L$ מהוָה איזומורפיזם של $\mathrm{Gal}(LE/E)$ על $\mathrm{Gal}(L/K)$.*

הוכחה: נבחר אבר קדום x עבור ההרחבה L/K ויהי $f = \mathrm{irr}(x,K)$. אזי f מתפרק מעל L למכפלה של גורמים לינאריים שונים זה מזה. נסמן $F = LE$. אזי, $F = E(x)$. לכן, F הוא שדה הפִצול של f מעל E. הואיל ו f פריד, F/E היא הרחבת גלואה.

אם $\sigma \in \mathrm{Gal}(F/E)$, אזי $\sigma x = x$ לכל $x \in E$ ולכן גם לכל $x \in L$. מכאן שהעתקת הצמצום הנה הומומורפיזם של $\mathrm{Gal}(F/E)$ לתוך $\mathrm{Gal}(L/K)$. נסמן את תמונתו ב H. מהשויון $F = LE$ נובע שהעתקת הצמצום הנה חד חד ערכית. לפי למה 2.1.1,

$$L^H = L \cap F^{\mathrm{Gal}(F/E)} = L \cap E = K.$$

לכן, לפי משפטון 2.1.5, $H = \mathrm{Gal}(L/K)$. בזאת הוכחנו שהעתקת הצמצום הנה איזומורפיזם. ∎

משפטון 2.1.11: *תהיינה L_1 ו L_2 הרחבות גלואה סופיות של K. אזי גם $L = L_1 L_2$ וגם $L_0 = L_1 \cap L_2$ הן הרחבות גלואה סופיות של K. יתר על כן, ההעתקה $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ היא איזומורפיזם*

$$\mathrm{Gal}(L/K) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \mid \sigma_1|_{L_0} = \sigma_2|_{L_0}\} \qquad (1)$$

הוכחה: L_1 הוא שדה הפצול של פולינום פריד $f_1 \in K[X]$ ואלו L_2 הוא שדה הפצול של פולינום פריד $f_2 \in K[X]$. לכן, L הוא שדה הפצול של הקבוצה $\{f_1, f_2\}$. מכאן ש L/K היא הרחבת גלואה.

כל אחת משתי החבורות $\mathrm{Gal}(L/L_1)$ ו $\mathrm{Gal}(L/L_2)$ נורמלית ב $\mathrm{Gal}(L/K)$ (משפטון 2.1.9). לפי משפטון 2.1.6, $\mathrm{Gal}(L/L_0) = \langle \mathrm{Gal}(L/L_1), \mathrm{Gal}(L/L_2) \rangle$. לכן, $\mathrm{Gal}(L/L_0) \triangleleft \mathrm{Gal}(L/K)$. שוב, לפי משפטון 2.1.9, L_0 היא הרחבת גלואה של K.

נסמן את אגף ימין של (1) ב H ואת ההעתקה $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ של $\mathrm{Gal}(L/K)$ לתוך H ב Φ. אם $\Phi(\sigma) = 1$, אזי $\sigma x = x$ עבור כל $x \in L_1$ ועבור כל $x \in L_2$, לכן עבור כל $x \in L$. לכן, $\sigma = 1$, כלומר Φ חד חד ערכית.

כדי להוכיח ש Φ על נתבונן בזוג $(\sigma_1, \sigma_2) \in H$. נרחיב את σ_1 לאבר $\tau_1 \in \mathrm{Gal}(L/K)$ ונרחיב את σ_2 לאבר $\tau_2 \in \mathrm{Gal}(L/K)$. מהגדרת H נובע ש $\tau_2^{-1}\tau_1 \in \mathrm{Gal}(L/L_0)$. משפטון 2.1.10 נותן $\tau \in \mathrm{Gal}(L/L_2)$ כך ש $\tau|_{L_1} = \tau_2^{-1}\tau_1|_{L_1}$. לכן, $\tau_2\tau|_{L_1} = \sigma_1$ ואלו $\tau_2\tau|_{L_2} = \sigma_2$, כמבֻקש. ∎

מקרה פרטי חשוב של המשפטון האחרון מתקבל כאשר $L_1 \cap L_2 = K$.

תוצאה 2.1.12: *תהיינה L_1 ו L_2 הרחבות גלואה סופיות של K. נניח ש $L_1 \cap L_2 = K$ ונסמן $L = L_1 L_2$. אזי ההעתקה $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ הנה איזומורפיזם $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.*

השראה מאפשרת להרחיב את התוצאה האחרונה ל n הרחבות גלואה:

תוצאה 2.1.13: *תהיינה $L_1, \ldots, L_n$ הרחבות גלואה סופיות של K. נניח ש $L_1 \cdots L_m \cap L_{m+1} = K$ לכל $1 \le m \le n-1$ ונסמן $L = L_1 \cdots L_n$. אזי ההעתקה $\sigma \mapsto (\sigma|_{L_1}, \cdots \sigma|_{L_n})$ הנה איזומורפיזם*

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_1/K) \times \cdots \times \mathrm{Gal}(L_n/K).$$

תרגיל 2.1.14: יהי K שדה בעל אפיון השונה מ 2 ומ 3, יהי $f(X)=X^3+bX+c$ פולינום אי פריק מעל K ויהיו x_1,x_2,x_3 שרשי f ב $\tilde{K}$ (עם רִבוּיָם). נסמן $\delta=(x_1-x_2)(x_2-x_3)(x_1-x_3)$ ו $\Delta=\delta^2$.

(א) הוכח ש $\Delta=-4b^3-27c^2$.

(ב) נסמן את שדה הפִצוּל של f מעל K ב L. הוכח שאם Δ הוא רבוע ב K, אזי $\mathrm{Gal}(L/K)\cong A_3$, אחרת $\mathrm{Gal}(L/K)\cong S_3$. ∎

תרגיל 2.1.15: תהי L/K הרחבת גלואה ותהי K' הרחבה נוספת של K. נניח ש K' ו L מוכלים בשדה משֻתף. הוכח ש $K'\cap L=K$ אם ורק אם K' ו L מֻפרדים לינארית מעל K. ∎

תרגיל 2.1.16: הוכח שחבורת גלואה של הפולינום X^4-2 מעל $\mathbb{Q}$ היא חבורת השִניון D_8 הנוצרת על ידי שני אברים σ,τ עם היחסים $\tau^2=\sigma^4=1$ ו $\tau\sigma\tau=\sigma^{-1}$. ∎

תרגיל 2.1.17: נסמן $x=\sqrt{(2+2\sqrt{2})(3+\sqrt{3})}$. הוכח ש $\mathbb{Q}(x)/\mathbb{Q}$ היא הרחבת גלואה וחבורת גלואה שלה הנה חבורת הרִבעונים Q_8. רמז: הוכח בין היֶתר ש $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$ הנה חבורה לא חִלופית. ∎

.26

2.2 תוצאות ראשונות

בסעיף זה נביא שתי מסקנות מִיָדיות של המשפט היסודי של גלואה.

הגדרה 2.2.1: תהי L/K הרחבה פרידה. אזי L מוכלת בסגוֹר הפריד K_s של K. סגור זה הנו הרחבת גלואה של K המַקיפה את L. לחִתוך $\hat{L}$ של כל הרחבות גלואה של K המקיפות את L נקרא **סגוֹר גלואה של** L/K. שדה זה הנו שדה הפִּצול מעל K של קבוצת כל הפולינומים שמקדמיהם ב K ובעלי שרש ב L. אם $[L:K]<\infty$, אזי $\hat{L}$ יהיה גם שדה הפצול של כל קבוצה סופית של פולינומים $f_1,\ldots,f_m$ ששרשיהם יוצרים את L מעל K. בפרט $[\hat{L}:K]<\infty$. ∎

משפטון 2.2.2: *להרחבה פרידה סופית* L/K *יש רק מספר סופי של הרחבות בֵינַיִם.*

הוכחה: יהי $\hat{L}$ סגוֹר גלואה של L/K. אזי $\hat{L}/K$ היא הרחבת גלואה סופית ולכן, $G=\mathrm{Gal}(\hat{L}/K)$ הנה חבורת סופית. לפי המשפט היסודי של תורת גלואה, יש ל $\hat{L}/K$ הרחבות בינַיִם כמספר תת החבורות של G. הואיל וכל הרחבת בינַיִם של L/K היא גם הרחבת בינַיִם של $\hat{L}/K$, מספר הרחבות הבינַיִם של L/K סופי. ∎

הגדרה 2.2.3: הרחבת שדות L/K תכֻנה **אַבֵלית** אם L/K היא הרחבת גלואה ו $\mathrm{Gal}(L/K)$ הנה חבורה אבלית. ∎

משפטון 2.2.4:

(א) *אם* L/K *היא הרחבה אבלית סופית של שדות ואם* E *הוא שדה בינַיִם, אזי גם* E/K *הוא הרחבה אבלית.*

(ב) *תהיינה* $L_1,\ldots,L_n$ *הרחבות אבליות סופיות של שדה* K *בתוך סגור אלגברי* $\tilde{K}$. *אזי גם צֵרופן* L *הוא הרחבה אבלית של* K.

הוכחת א: לפי ההנחה $\mathrm{Gal}(L/K)$ אבלית. לכן, $\mathrm{Gal}(L/E)\lhd\mathrm{Gal}(L/K)$ ו

$$\mathrm{Gal}(E/K)\cong\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$$

אבלית.

הוכחת ב: ההעתקה $\sigma\mapsto(\sigma|_{L_1},\ldots,\sigma|_{L_n})$ הנה שִכון של $\mathrm{Gal}(L/K)$ לתוך

$$\mathrm{Gal}(L_1/K)\times\cdots\times\mathrm{Gal}(L_n/K).$$

הואיל והחבורה האחרונה אבלית, גם $\mathrm{Gal}(L/K)$ אבלית. ∎

תרגיל 2.2.5: *הוכח ש* $\sqrt{2}+\sqrt{3}$ *הנו מספר אלגברי ממעלה* 4 *מעל* $\mathbb{Q}$.

2.3 שדות סופיים

תורת גלואה של שדות סופיים הנה פשוטה במיֻחד. הסדר של כל שדה סופי הנו חזקה של האפיון שלו. להפך, לכל חזקה של שדה ראשוני קיָם שדה יחיד עד כדי איזומורפיזם שסדרו חזקה זו. אם L היא הרחבת גלואה סופית של שדה סופי K מסדר n, אזי $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. להפך, לכל n טבעי קיֶמת הרחבה יחידה L ב $\tilde{K}$ מהצורה הזו.

משפטון 2.3.1: *יהי K שדה סופי בעל אפיון p.*

(א) *קיָם n טבעי כך ש K הוא הרחבה ממעלה n של $\mathbb{F}_p$ ו $|K| = p^n$.*

(ב) *$K^\times$ היא חבורה מעגלית ממעלה $p^n - 1$.*

(ג) *כל $x \in K$ מתקיֵם $x^{p^n} = x$.*

הוכחה: השדה K הנו הרחבה סופית של $\mathbb{F}_p$. אם נסמן $n = [K : \mathbb{F}_p]$, נקבל ש K הוא מרחב וקטורי ממֵמד n מעל $\mathbb{F}_p$. בתור שכזה מספר אבריו הוא p^n.

מספר אברי החבורה הכפלית $K^\times$ הוא $p^n - 1$. לפי משפטון 1.9.4, $K^\times$ מעְגלית. בפרט $x^{p^n-1} = 1$ ולכן $x^{p^n} = x$ לכל $x \in K^\times$. השויון האחרון נכון גם עבור $x = 0$. ∎

משפטון 2.3.2: *לכל p ראשוני ולכל n טבעי קיָם שדה יחיד עד כדי איזומורפיזם מסדר p^n. נסמנו ב $\mathbb{F}_{p^n}$.*

הוכחה: עבור $n = 1$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. באפן כללי, יהי $\mathbb{F}_{p^n}$ שדה הפצול של הפולינום $f(X) = X^{p^n} - X$ מעל $\mathbb{F}_p$. הואיל ו $f'(X) = -1$, $\gcd(f(X), f'(X)) = 1$ ולכן יש ל $f(X)$ p^n שרשים שונים ב $\mathbb{F}_{p^n}$ (משפטון 1.5.10) . אסף השרשים האלו סגור תחת חבור, כפל וחִלוק (באברים שונים מאפס) ולכן מהוה תת שדה F של $\mathbb{F}_{p^n}$ המקיף את $\mathbb{F}_p$. לכן $F = \mathbb{F}_{p^n}$ ו $|\mathbb{F}_{p^n}| = p^n$.

הואיל ו $\mathbb{F}_p$ נקבע על ידי מספר אבריו עד כדי איזומורפיזם והואיל ושדה הפִצול נקבע עד כדי איזומורפיזם (משפטון 1.6.2), גם $\mathbb{F}_{p^n}$ נקבע על ידי סִדרו עד כדי איזומורפיזם. ∎

היְחידות של $\mathbb{F}_{p^n}$ הנה הרבה יותר חזקה ממה שנאמר במשפטון 2.3.2.

משפט 2.3.3: *יהי p מספר ראשוני.*

(א) *לכל חזקה q של p קיָם תת שדה יחיד $\mathbb{F}_q = \{x \in \tilde{\mathbb{F}}_p \mid x^q = x\}$ ב $\tilde{\mathbb{F}}_p$ מסדר q.*

(ב) *אם q ו q' הן שתי חֲזקות של p, אזי $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ אם ורק אם $q' = q^r$ עבור איזה שהוא מספר טבעי r. יתר על כן, כל הרחבה סופית של $\mathbb{F}_q$ ב $\tilde{\mathbb{F}}_q$ הנה מהצורה $\mathbb{F}_{q'}$ עבור איזו שהיא חזקה q' של q.*

(ג) *לכל חזקה q של p ולכל מספר טבעי r ההרחבה $\mathbb{F}_{q^r}/\mathbb{F}_q$ מעְגלית ונוצרת על ידי האוטומורפיזם φ_q המֻגדר על ידי $\varphi_q(x) = x^q$. אוטומורפיזם זה נקרא* **האוטומורפיזם של פרובניוס** *(המצֹרף ל q).*

הוכחת א: כפי שצינו לעיל, הקבוצה $\{x \in \tilde{\mathbb{F}} \mid x^q = x\}$ מהוָה שדה וכל אבר של שדה בֶּן q אברים שיָך לקבוצה זו. לכן, היא מהוה את תת השדה היחיד של $\tilde{\mathbb{F}}_p$ מסדר q.

הוכחת ב: אם $q' = q^r$ ואם $x \in \mathbb{F}_q$, אזי $x^q = x$ ולכן $x^{q^r} = x$. מכאן ש $x \in \mathbb{F}_{q'}$.

להפך, אם $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$, נסמן $r = [\mathbb{F}_{q'} : \mathbb{F}_q]$. אזי $\mathbb{F}_{q'}$ הוא מרחב וקטורי מעל $\mathbb{F}_q$ שממדו r. לכן, $|\mathbb{F}_{q'}| = |\mathbb{F}_q|^r = q^r$. מכאן ש $q' = q^r$.

הוכחת ג: $\mathbb{F}_{q^r}$ הוא שדה הפִצול של הפולינום הפריד $X^{q^r} - X$ מעל $\mathbb{F}_q$. לכן, $\mathbb{F}_{q^r}/\mathbb{F}_q$ הנה הרחבת גלואה ממעלה r. כדי להוכיח שהיא מעגלית, מספיק אפוא להוכיח שכל החֲזקות $1, \varphi_q, \ldots, \varphi_q^{r-1}$ של φ_q שונות זו מזו. ואכן, אם $0 \le i \le j \le r-1$ מקיִמים $\varphi_q^i = \varphi_q^j$, אזי $x^{q^i} = x^{q^j}$ לכל $x \in \mathbb{F}_{q^r}$. בפרט נכון שויון זה ליוצר x של החבורה המעְגלית $\mathbb{F}_{q^r}^\times$ (משפטון 2.3.1). הואיל וסדרו הוא $q^r - 1$, נקבל ש $q^r - 1 | q^{j-i}$. לכן, $i = j$. ∎

תרגיל 2.3.4: יהי K שדה ו $f \in K[X]$ פולינום. הוכח שאם אֹסף השרשים של f ב $\tilde{K}$ מהוה שדה, אזי $\mathrm{char}(K) = p > 0$ וקים n טבעי כך ש $X^{p^n} - X$ מחלק את $f(X)$. ∎

תרגיל 2.3.5: יהי K שדה סופי. הוכח שלכל $a \in K$ קיָמים $x, y \in K$ כך ש $x^2 + y^2 = a$. רמז: נסמן $q = |K|$ ונשים לב לכך שמספר הרִבועים ב K הוא $\frac{q+1}{2}$ ואלו מספר האברים מהצורה $a - y^2$ גם הוא $\frac{q+1}{2}$. ∎

תרגיל 2.3.6: יהי n מספר טבעי, יהי p מספר ראשוני שאינו מחלק את n ויהי ζ שרש יחידה ב $\tilde{\mathbb{F}}_p$ מסדר n. הוכח ש $[\mathbb{F}_p(\zeta) : \mathbb{F}_p]$ שוה לסדר של p מודולו n. ∎

תרגיל 2.3.7: יהי K שדה סופי בעל q אברים ויהי k מספר טבעי. הוכח ש $\sum_{x \in K^\times} x^k = -1$ אם $q - 1 | k$ ו $\sum_{x \in K^\times} x^k = 0$ אם $q - 1 \nmid k$. רמז: כדי להוכיח את הטענה השניה שים לב לכך שיוצר a של $K^\times$ מקיֵם $a^k \ne 1$. ∎

תרגיל 2.3.8: יהי K שדה סופי ו $\alpha \colon K \to K$ העתקה. הוכח שקיָם פולינום $f \in K[X]$ המקיֵם $f(x) = \alpha(x)$ לכל $x \in K$. ∎

תרגיל 2.3.9: יהי K שדה סופי ו F תת קבוצה המכילה את האברים $0, 1$ והסגורה תחת החבור והכפל. הוכח ש F הנו תת שדה של K. ∎

תרגיל 2.3.10: יהי p מספר ראשוני אי זוגי. הוכח את משפט וילסון: $(p-1)! \equiv -1 \mod p$. רמז: השתמש במשפט הקטן של פרמה. ∎

2.4 שָׁרָשֵׁי יְחִידָה

שרשי היחידה הם האברים האלגבריים הנוחים ביותר לנִתוח. יתר על כן, הם ממלאים תפקיד מרכזי בתורת השדות ותורת גלואה. אם מצרפים אותם לשדה מקַבלים הרחבות אבליות. בסעיף זה נתרכז במיֻחד בהרחבות של $\mathbb{Q}$ המתקבלות על ידי צרוף שרשי יחידה ונתאר את הרחבות גלואה המתאימות.

הגדרה 2.4.1: אבר ζ בסגור האלגברי של שדה K נקרא **שֹרש יחידה** אם קיָם n טבעי כך ש $\zeta^n = 1$. במקרה זה נאמר גם ש ζ הוא **שרש יחידה** n**־י**. אם בנוסף לכך $\zeta^k \neq 1$ לכל $1 \leq k \leq n-1$, אומרים ש ζ הוא **שרש יחידה מסדר** n ומסמנים אותו ב ζ_n.

אֹסף כל שרשי היחידה ה n־יים ב $\tilde{K}$ מהוה חֲבורה כפלית המסֻמנת ב $\mu_n(\tilde{K})$. אבריה הם בדיוק שרשי הפולינום $X^n - 1$ ולכן סדרה אינו עולה על n. לפי משפטון 1.9.4, $\mu_n(\tilde{K}))$ מעגלית. אם $n = p$ הוא מספר ראשוני ו $p = \mathrm{char}(K)$, אזי $X^p - 1 = (X-1)^p$ ולכן, $\mu_p(\tilde{K})$ היא חבורה טריביאלית ואין ב $\tilde{K}$ שום שרש יחידה מסדר p.

אם $n \nmid \mathrm{char}(K)$, אזי הפולינום $X^n - 1$ פריד, ולכן $|\mu_n(\tilde{K})| = n$. כל יוצר של $\mu_n(\tilde{K})$ הנו שֹרש יחידה מסדר n. שרש זה אינו יחיד. למעשה ζ_n^i הוא שרש יחידה מסדר n אם ורק אם $\gcd(i,n) = 1$. מספר שָׁרשי היחידה מסדר n מסֻמן ב $\varphi(n)$, בתורת המספרים נהוג לכנות את φ בשם **פונקצית אוילר.**

אם $K = \mathbb{C}$, אזי שרשי היחידה ה n־יים הם $e^{\frac{2pi}{n}k}$, באשר e הוא בסיס הלוגרימים הטבעיים, $i = \sqrt{-1}$ ו $k = 0, 1, \ldots, n-1$. שרשי היחידה מסדר n הם אותם שרשי היחידה ה n־יים שבהם $\gcd(k,n) = 1$. ∎

משפט יסודי בתורת המספרים אומר ש φ היא פונקציה כפלית:

משפטון 2.4.2: *אם* $\gcd(m,n) = 1$*, אזי* $\varphi(mn) = \varphi(m)\varphi(n)$.

הוכחה: מהגדרת פונקצית אוילר נובע ש $\varphi(n)$ אינו אלא הסדר של חבורת האברים ההפיכים $(\mathbb{Z}/n\mathbb{Z})^\times$ של החוג הסופי $\mathbb{Z}/n\mathbb{Z}$. ההעתקה $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ המֻגדרת היטב על ידי $x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$ היא חד חד ערכית (כאן משתמשים בכך ש m ו n זרים זה לזה). הואיל ולשני האגפים אותו הסדר (דהיינו mn), נובע שההעתקה הנ"ל הנה איזומורפיזם: $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. לכן גם חבורות האברים ההפיכים של שני האגפים איזומורפיות זו לזו: $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. חִשוב הסדרים של שני האגפים מוכיח את השויון המבֻקש $\varphi(mn) = \varphi(m)\varphi(n)$. ∎

למה 2.4.3: *יהי* K *שדה ו* n *מספר טבעי. נניח ש* $n \nmid \mathrm{char}(K)$*. אזי* $K(\zeta_n)/K$ *היא הרחבה אבלית ממעלה* $\leq \varphi(n)$*. יתר על כן, קיָם שִכון* $i\colon \mathrm{Gal}(K(\zeta_n)/K)) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *המֻגדר על ידי הנֻסחה* $\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$.
∎

הוכחה: הנגזרת של הפולינום $X^n - 1$ *הנה* nX^{n-1}*. הואיל ו* $n \nmid \mathrm{char}(K)$ *שונה* n *ב* K *מאפס. לכן, המחלק המשֻתף*

של שני הפולינומים הוא 1. *מכאן ש* X^n-1 *הוא פולינום פריד (משפטון* $1.5.10$*). הואיל ו* $K(\zeta_n)$ *הנו שדה הפִצול של* X^n-1*, נובע ש* $K(\zeta_n)$ *הוא הרחבת גלואה של* K.

כל אבר σ *של* $\mathrm{Gal}(K(\zeta_n)/K)$ *שומר על הסדר הכפלי של כל אבר. בפרט, לפי הגדרה* $2.4.1$, $\sigma(\zeta_n)=\zeta_n^k$ *באשר* k *הוא מספר שלם זר ל* n *הנקבע באפן יחיד מודולו* n. *אם נסמן,* $i(\sigma)=k+n\mathbb{Z}$*, נקבל ש* $i(\sigma)\in(\mathbb{Z}/n\mathbb{Z})^\times$. *הואיל ו* σ *נקבע על ידי* $\sigma(\zeta_n)$*, מעתיקה* i *את* $\mathrm{Gal}(K(\zeta_n)/K)$ *באֹפן חד חד ערכי לתוך* $(\mathbb{Z}/n\mathbb{Z})^\times$.

יהי τ *אבר נוסף של* $\mathrm{Gal}(K(\zeta_n)/K)$. *אזי* $\sigma(\tau(\zeta_n))=\sigma(\zeta_n^{i(\tau)})=\sigma(\zeta_n)^{i(\tau)}=\zeta_n^{i(\sigma)i(\tau)}$. *לכן,* $i(\sigma\tau)=i(\sigma)i(\tau)$. *מכאן ש* i *הוא שִכון של* $\mathrm{Gal}(K(\zeta_n)/K)$ *לתוך* $(\mathbb{Z}/n\mathbb{Z})^\times$. *הואיל והחבורה השניה היא אבלית, גם הראשונה היא כזו.* ∎

השִכון שלמה $2.4.3$ *נותנת לנו הופך לאיזומורפיזם במקרה ש* $K=\mathbb{Q}$.

משפט $2.4.4$: *לכל* n *טבעי מתקַימים:*

(א) $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$.

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

הוכחה: טענה (ב) היא מסקנה של טענה (א) ולמה $2.4.3$. לכן, מספיק להוכיח את (א).

הואיל ו $\mathbb{Z}$ הוא חוג בעל פריקות חד ערכית, גם $\mathbb{Z}[X]$ הוא חוג בעל פריקות חד ערכית (תוצאה $1.1.10$). בפרט X^n-1 מתפרק ב $\mathbb{Z}[X]$ למכפלה של גורמים אי פריקים. אחד מהגורמים שנסמנו ב f מאפס את ζ_n. נסמן את מכפלת האחרים ב h כדי לקבל

$$X^n-1=f(X)h(X). \tag{1}$$

מכפלת המקדמים העליונים של f ו h היא 1, לכן בלי הגבלת הכלליות נוכל להניח שגם f וגם h מתֻקנים. לפי תוצאה $1.1.9$, f אי פריק גם בחוג $\mathbb{Q}[X]$, ולכן $f=\mathrm{irr}(\zeta_n,\mathbb{Q})$. מכאן נובע ש $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\deg(f)$. הואיל ו $[\mathbb{Q}(\zeta_n):\mathbb{Q}]\le\varphi(n)$ (למה $2.4.3$), מספיק להוכיח ש $f(\zeta_n^k)=0$ לכל k שלם הזר ל n.

טענה א: *אם* p *הוא מספר ראשוני שאינו מחלק את* n*, אזי* $f(\zeta_n^p)=0$. נניח בְשלילה ש $f(\zeta_n^p)\ne0$. אזי, לפי (1), $h(\zeta_n^p)=0$. לכן $f(X)$ מחלק את $h(X^p)$ ב $\mathbb{Q}[X]$. שוב, לפי הלמה של גאוס, $f(X)$ מחלק את $h(X^p)$ ב $\mathbb{Z}[X]$. בְמלים אחרות, קיָם $g\in\mathbb{Z}[X]$ כך ש $f(X)g(X)=h(X^p)$. נסמן עתה את ההעמדה של $\mathbb{Z}$ ושל $\mathbb{Z}[X]$ מודולו p בגג. הואיל ו $x^p=x$ לכל $x\in\mathbb{F}_p$, נובע מהשויון האחרון ש $\bar{f}(X)\bar{g}(X)=\bar{h}(X)^p$. לכן, $\gcd(\bar{f},\bar{h})\ne1$. מצד שני, $X^n-1=\bar{f}(X)\bar{h}(X)$ ו $\mathrm{char}(\mathbb{F}_p)\nmid n$. לכן, כמו מקודם, $\gcd(\bar{f},\bar{h})=1$. מְסתירה זו נובע ש $f(\zeta_n^p)=0$, כנִטען.

טענה ב: $f(\zeta_n^k)=0$ *לכל k שלם הזר ל n.* כדי להוכיח את הטַענה נרשֹם את k כמכפלה $k=p_1\cdots p_r$ של מספרים ראשוניים שאינם מחלקים את n. השראה על r נותנת ש $f(\zeta_n^{p_1\cdots p_{r-1}})=0$. לפי הגדרה 2.4.1, $\xi=\zeta_n^{p_1\cdots p_{r-1}}$ הנו מחלק יחידה מסדר n. לכן, אם נַיִשׂם את טַענה א ל ξ במקום ל ζ, נקבל ש $f(\zeta_n^k)=f(\xi^{p_r})=0$, כפי שהיה להוכיח. ∎

משפט 2.4.5: *יהיו m ו n מספרים טבעיים זרים זה לזה. אזי:*

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

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

(ג) $\mathrm{Gal}(\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)/\mathbb{Q})\cong\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

הוכחת א: מהיחס $\mathrm{ord}(\zeta_{mn}^m)=n$ נובע ש $\mathbb{Q}(\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})$. באֹפן דומה נובע ש $\mathbb{Q}(\zeta_m)\subseteq\mathbb{Q}(\zeta_{mn})$. לכן, $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})$.

מההנחה ש $\gcd(m,n)=1$ נובע ש $\mathrm{ord}(\zeta_m\zeta_n)=mn$. לכן, נִתן לקחת את $\zeta_m\zeta_n$ כ ζ_{mn} ולקבל ש $\mathbb{Q}(\zeta_m,\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})=\mathbb{Q}(\zeta_m\zeta_n)$. מצד שני $\mathbb{Q}(\zeta_m\zeta_n)\subseteq\mathbb{Q}(\zeta_m,\zeta_n)$. לכן כל השויונות ב (א) נכונים.

הוכחת ב: מ (א) וממשפטון 2.4.2 נובע ש

$$[\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n):\mathbb{Q}]=[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}]=\varphi(mn)=\varphi(m)\varphi(n)=[\mathbb{Q}(\zeta_m):\mathbb{Q}][\mathbb{Q}(\zeta_n):\mathbb{Q}]$$

לכן, לפי למה 1.4.5, $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$.

הוכחת ג: הטענה נובעת מ (ב) לפי תוצאה 2.1.12. ∎

תרגיל 2.4.6: הכלל את משפט 2.4.5 והוכח עבור מספרים טבעיים m,n ש $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)})$ ו $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{\gcd(m,n)})$. ∎

משפט 2.4.7 (Dirichlet): *לכל מספר טבעי n ולכל מספר שלם a הזר ל n קיָמים אינסוף מספרים ראשוניים* $p\equiv a \mod n$.

ההוכחה הרגילה של משפט דיריכלה משתמשת בתורת הפונקציות המרֻכבות. כדי לממש חבורות אבליות סופיות מעל $\mathbb{Q}$ מספיק מקרה פרטי של המשפט שאותו נוכיח כאן בעזרת התורה של שרשי היחידה שפִתחנו בסעיף זה.

הערה 2.4.8: הפולינום החשרורי. נסמן $\Phi_n=\mathrm{irr}(\zeta_n,\mathbb{Q})$. זהו פולינום אי פריק עם מקדמים ב $\mathbb{Q}$ ממעלה $\varphi(n)$ (משפט 2.4.4). הואיל ו ζ_n הוא גם שרש של X^n-1, מחלק $\Phi_n(X)$ את X^n-1 ב $\mathbb{Q}[X]$. יתר על כן, לפי הלמה של גאוס, מחלק $\Phi_n(X)$ את X^n-1 ב $\mathbb{Z}[X]$. במִלים אחרות, קיָם $h\in\mathbb{Z}[X]$ כך ש $X^n-1=\Phi_n(X)h(X)$. בפרט, אם נציב 0 בשני האגפים, נקבל $-1=\Phi_n(0)g(0)$. לכן, $\Phi_n(0)=\pm1$.

∎

למה 2.4.9: *יהי q מספר ראשוני שאינו מחלק את n. אם יש ל $\Phi_q(X)$ שׁרש מודולו q, אזי* $q \equiv 1 \mod n$.

הוכחה: נתבונן בהעמדה $\rho_0\colon \mathbb{Z} \to \mathbb{F}_q$ מודולו q שגרעינה $q\mathbb{Z}$. הואיל ולפי משפט 2.4.4 האברים $1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}$ יוצרים את $\mathbb{Z}[\zeta_n]$ מעל $\mathbb{Z}$ וגם אינם תלויים לינארית מעל $\mathbb{Q}$, המספר q אינו הפיך בחוג $\mathbb{Z}[\zeta_n]$. לכן, $q\mathbb{Z}[\zeta_n]$ הוא אידאל נאות של החוג. לפי למה 1.1.2, $q\mathbb{Z}[\zeta_n]$ מוכל באידאל מרבי q של $\mathbb{Z}[\zeta_n]$. החִתוך $\mathbb{Z} \cap$ q הנו אידאל נאות של $\mathbb{Z}$ המקיף את $q\mathbb{Z}$. לכן, נתן להרחיב את ρ_0 להומומורפיזם ρ של $\mathbb{Z}[\zeta_n]$ על שדה המנות $\mathbb{Z}[\zeta_n]/$q שאינו אלה הרחבה סופית של $\mathbb{F}_q$. במלים אחרות, ρ מעתיק את $\mathbb{Z}[\zeta_n]$ לתוך $\tilde{\mathbb{F}}_q$. נשתמש בגג כדי לסמן את התמונות של אברי $\mathbb{Z}[\zeta_n]$ תחת ρ.

מהפרוק $X^n - 1 = \prod_{i=1}^n (X - \zeta_n^i)$ נובע ש

$$X^n - 1 = \prod_{i=1}^n (X - \bar{\zeta}_n^i)$$

הואיל ו $q \nmid n$, האברים $1, \bar{\zeta}_n, \dots, \bar{\zeta}_n^{n-1}$ שונים זה מזה. לכן, ρ מעתיק את החבורה $\mu_n(\tilde{\mathbb{Q}})$ באֹפן איזומורפי על החבורה $\mu_n(\tilde{\mathbb{F}}_q)$. בפרט, $\mathrm{ord}(\bar{\zeta}_n) = n$.

הפולינום $\Phi_n(X)$ מתפרק מעל $\tilde{\mathbb{Q}}$ לגורמים לינאריים $\Phi_n(X) = \prod (X - \zeta_n^i)$ באשר i עובר על כל המספרים הטבעיים בין 1 ל n הזרים ל n. לכן, $\bar{\Phi}_n(X) = \prod (X - \bar{\zeta}_n^i)$, באשר i עובר על כל המספרים הטבעיים בין 1 ל n הזרים ל n. אם קיָם מספר טבעי z כך ש $\Phi_n(z) \equiv 0 \mod q$, אזי $\bar{z} \in \mathbb{F}_q^\times$ ו $\bar{\Phi}_n(\bar{z}) = 0$. לכן קיָם i זר ל n כך ש $\bar{z} = \bar{\zeta}_n^i$, מכאן ש $\mathrm{ord}(\bar{z}) = n$. הואיל וסדר של אבר בחבורה סופית מחלק את הסדר של החבורה, נקבל מכאן ש $n | q - 1$, כלומר ש $q \equiv 1 \mod n$. ∎

משפט 2.4.10: *לכל n טבעי יש אינסוף מספרים ראשוניים q המקיְמים* $q \equiv 1 \mod n$.

הוכחה: נניח בשלילה שקיָמים רק מספר סופי של מספרים ראשוניים כאלו והם $q_1, \dots, q_m$. נבחר מספר טבעי y כך ש $\Phi_n(q_1 \cdots q_m n y)$ גדול מ 1 ויהי q גורם ראשוני של מספר זה. אזי, $\Phi_n(q_1 \cdots q_m y) \equiv 0 \mod q$. לפי הערה 2.4.8, $\Phi_n(q_1 \cdots q_m n y) \equiv \Phi_n(0) \equiv \pm 1 \mod n$ ולכן $q \nmid n$. לפי למה 2.4.9, $q \equiv 1 \mod n$ ולכן קיָם $1 \le i \le m$ כך ש $q = q_i$. בפרט, $q_1 \cdots q_m n y \equiv 0 \mod q$. לכן,

$$\Phi_n(q_1 \cdots q_m n y) \equiv \Phi_n(0) \equiv \pm 1 \mod q.$$

מכאן ש $\pm 1 \equiv 0 \mod q$, סתירה. ∎

משפט 2.4.11: *כל חבורה אבלית סופית נִתנת למִמוש מעל* $\mathbb{Q}$.

הוכחה: תהי A חבורה אבלית סופית. לפי המשפט היסודי של תורת החבורות האבליות הסופיות נִתן להציג את A כמכפלה ישרה $A = \prod_{i=1}^n A_i$, באשר A_i הִנה חבורה מעְגלית מסדר $q_i = p_i^{k_i}$ עבור איזה שהוא מספר ראשוני p_i.

נבחר בעזרת משפט דיריכלֶה מספרים ראשוניים שונים זה מזה $l_1,\dots,l_n$ כך ש $l_i \equiv 1 \mod q_i$ עבור $i=1,\dots,n$. נסמן $L_i=\mathbb{Q}(\zeta_{l_i})$. לפי משפט 2.4.4 ולפי משפטון 2.3.1,

$$\operatorname{Gal}(L_i/L) \cong (\mathbb{Z}/l_i\mathbb{Z})^\times \cong \mathbb{Z}/(l_i-1)\mathbb{Z}.$$

הואיל ו $q_i|l_i-1$, החבורה המעגלית מסדר q_i הנה מנה של $\mathbb{Z}/(l_i-1)\mathbb{Z}$. לכן, קַיָם ל L_i תת שדה (יחיד) K_i כך ש $\operatorname{Gal}(K_i/\mathbb{Q}_i) \cong \mathbb{Z}/q_i\mathbb{Z}$.

נסמן $K=K_1\cdots K_n$. יהי $1 \le m \le n-1$. אזי, לפי **תוצאה** 2.4.5,

$$K_1\cdots K_m \cap K_{m+1} \subseteq L_1\cdots L_m \cap L_{m+1} = \mathbb{Q}(\zeta_{q_1\cdots q_m}) \cap \mathbb{Q}(\zeta_{q_{m+1}}) = \mathbb{Q}$$

לכן $K_1\cdots K_m \cap K_{m+1}=\mathbb{Q}$. לכן, לפי **תוצאה** 2.1.13,

$$\operatorname{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^n \operatorname{Gal}(K_i/K) \cong \prod_{i=1}^n \mathbb{Z}/q_i\mathbb{Z} \cong A$$

כפי שהיה להוכיח. ∎

הואיל וכל חבורה שסדרה אינו עולה על 5 אבלית, אנו מקבלים את התוצאה הבאה:

תוצאה 2.4.12: *כל חבורה מסדר ≤ 5 נִתנת לממוש מעל $\mathbb{Q}$.*

הוכחת משפט 2.4.11 מממֶשת כל חבורה חִלופית בתוך שדה מהצורה $\mathbb{Q}(\zeta_n)$, עבור איזה n שהוא טבעי. מסתבר שהדבר אינו מקרי. המשפט הבא מראה שתופעה זו הִנה מחֻיֶבת המציאות. כדי להוכיח משפט זה, זקוקים אנו לִידיעות בתורת המספרים האלגבריים שאין בְיָדינו.

משפט 2.4.13 (Kronecker-Weber): *כל הרחבה אבלית סופית K של $\mathbb{Q}$ מוכלת בשדה מהצורה $\mathbb{Q}(\zeta_n)$.*

הערה 2.4.14: *הבעיה ההפוכה של תורת גלואה.* בעיה זו שואלת על החבורות הסופיות שנִתָן **לממֵש** מעל $\mathbb{Q}$. במִלים אחרות, מהן החבורות הסופיות G שעבורן קיֶמת ל $\mathbb{Q}$ הרחבת גלואה L כך ש $\operatorname{Gal}(L/K) \cong G$.

שפרביץ הוכיח שכל חבורה פתירה סופית נִתנת לממוש מעל $\mathbb{Q}$. הִלברט הוכיח (בעזרת המשפט הידוע בשם "משפט אי הפריקות של הִלברט") שכל חבורה סימטרית S_n וכל חבורת חילופין A_n נִתנות לממוש מעל $\mathbb{Q}$. גם חבורות פשוטות סופיות רבות אחרות מֻמשו מעל $\mathbb{Q}$ וביניהן כמעט כל החבורות **הלא סדירות** (=ספורדיות). ∎

תרגיל 2.4.15: *יהי ζ שֹרש מרֻכב של הפולינום X^6+X^3+1. מצא את כל השִכונים של $\mathbb{Q}(\zeta)$ לתוך $\mathbb{C}$.*

תרגיל 2.4.16: *תהי K הרחבה סופית של $\mathbb{Q}$. הוכח ש K מכיל רק מספר סופי של שרשי יחידה.*

2.5 תלות לינארית של אָפינים

בסעיף זה נוכיח משפט עזר שיעזור לנו לנתח הרחבות מעגליות.

אפין (קרי: אוֹפין) הנו הומומורופיזם $\chi\colon G \to K^\times$, באשר G חבורה ו K שדה.

משפטון 2.5.1 (Emil Artin): *יהיו $\chi_1, \dots, \chi_n\colon G \to K^\times$ אפינים שונים. אזי, $\chi_1, \dots, \chi_n$ אינם תלויים לינרית מעל K. במִלים אחרות, אם $a_1, \dots, a_n \in K$ מקיְמים $\sum_{i=1}^n a_i\chi_i = 0$ (כהעתקה מ G לתוך K), אזי* $a_1, \dots, a_n = 0$.

הוכחה: המקרה $n = 1$ ברור. נניח אפוא ש $n \geq 2$ ונניח בשלילה שלא כל ה a_i־ים שוים לאפס ולמשל $a_1 \neq 0$. מההנחה נובע שקיָם $\tau \in G$ כך ש $\chi_1(\tau) \neq \chi_n(\tau)$. עוד נובע מההנחה ש $\sum_{i=1}^n a_i\chi_i(\sigma) = 0$, לכל $\sigma \in G$. לכן,

$$\sum_{i=1}^n a_i\chi_i(\sigma)\chi_n(\tau) = 0 \quad . \tag{1}$$

בנוסף לכך $\sum_{i=1}^n a_i\chi_i(\sigma\tau) = 0$ ולכן

$$\sum_{i=1}^n a_i\chi_i(\sigma)\chi_i(\tau) = 0 \tag{2}$$

אם נחסר את (2) מ (1) נקבל $\sum_{i=1}^{n-1} a_i\chi_i(\sigma)\big(\chi_n(\tau) - \chi_i(\tau)\big) = 0$ לכל $\sigma \in G$. לכן,

$$\sum_{i=1}^{n-1} a_i\big(\chi_n(\tau) - \chi_i(\tau)\big)\chi_i = 0 \, . \tag{3}$$

הנחת השראה על n גוררת שכל מקדמי (3) שוים לאפס. בפרט, $a_1(\chi_n(\tau) - \chi_1(\tau)) = 0$, בסתירה להנחות.
∎

תוצאה 2.5.2: *תהי L/K הרחבה פרידה ממעלה סופית n, יהיו $\sigma_1, \dots, \sigma_n$ שִכּוני־K השונים של L לתוך $\tilde{K}$ ויהי $w_1, \dots, w_n$ בסיס של L/K. אזי $\sigma_1, \dots, \sigma_n$ אינם תלויים לינארית מעל $\tilde{K}$, שורות (וגם עמודות) המטריצה $A = (\sigma_i w_j)_{1\leq i,j\leq n}$ אינן תלויות לינארית ו* $\det(\sigma_i w_j)_{1\leq i,j\leq n} \neq 0$.

הוכחה: הצמצומים של $\sigma_1, \dots, \sigma_n$ ל $L^\times$ הם אפינָים לתוך $\tilde{K}^\times$. לפי 2.5.1, אפינים אֵלו אינם תלויים לינארית. אִלו שורות המטריצה A היו תלויות לינארית, היו קיָמים $c_1, \dots, c_n \in \tilde{K}$ כך ש

$$\sum_{i=1}^n c_i(\sigma_i w_1 \ \sigma_i w_2 \ \cdots \ \sigma_n w_n) = 0 \quad .$$

לכן, $\sum_{i=1}^n c_i\sigma_i w_j = 0$ לכל j. הואיל ו $w_1, \dots, w_n$ יוצרים את L מעל K, נובע מכאן ש $\sum_{i=1}^n c_i\sigma x = 0$ לכל $x \in L$. במִלים אחרות, $\sum_{i=1}^n c_i\sigma_i = 0$, בסתירה לאי התלות הלינארית של $\sigma_1, \dots, \sigma_n$. ∎

2.6 הרחבות מעגליות

הרחבה L/K של שדות מכֻנה **מעגלית** אם היא גלואה ו $\mathrm{Gal}(L/K)$ היא חבורה מעגלית סופית. אם יש ב K שֹרש יחידה מסדר n, אזי ההרחבות המעגליות של K ממעלה n מתקבלות על ידי צרוף שָרשים מסדר n של אברים של K. כדי להוכיח את הטענה נכניס שני מושגים המסיְעים לחקירת הרחבות של שדות.

תהי L/K הרחבה פרידה ממעלה n ויִהיו $\sigma_1, \ldots, \sigma_n$ כל שִכוּנֵי־K של L לתוך $\tilde{K}$. נגדיר בעזרתם העתקה $\mathrm{norm}_{L/K}\colon L \to K$ שתקרֵא **נורמה** והעתקה $\mathrm{trace}_{L/K}\colon L \to K$ שתִקרא **עִקבה** באֹפן הבא:

$$\mathrm{norm}_{L/K}(x) = \prod_{i=1}^{n} \sigma_i x \qquad \mathrm{trace}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i x$$

להעתקות אלו התכונות הבאות:

(וא) $\mathrm{trace}_{L/K}(ax+by) = a \cdot \mathrm{trace}_{L/K}(x) + b \cdot \mathrm{trace}_{L/K}(y)$ עבור $x, y \in L$ ו $a, b \in K$.

(וב) $\mathrm{norm}_{L/K}(xy) = \mathrm{norm}_{L/K}(x)\mathrm{norm}_{L/K}(y)$. עבור $x, y \in L$.

(וג) $\mathrm{norm}_{L/K}(a) = a^n$ אם $a \in K$.

(וד) אם M/L היא הרחבה פרידה סופית של L ו $x \in M$, אזי $\mathrm{trace}_{M/K}(x) = \mathrm{trace}_{L/K}(\mathrm{trace}_{M/L}(x))$ ו $\mathrm{norm}_{M/K}(x) = \mathrm{norm}_{L/K}(\mathrm{norm}_{M/L}(x))$.

משפטון 2.6.1 (המשפט ה 90 של הִלברט): *תהי L/K הרחבה מעגלית, יהי σ יוצר של $\mathrm{Gal}(L/K)$ ויהי $y \in L$. אזי $\mathrm{norm}_{L/K}(y) = 1$ אם ורק אם קיָם $x \in L^\times$ כך ש $y = \frac{x}{\sigma x}$.*

הוכחה: נסמן $n = [L : K]$ ונניח קודם שקיָם $x \in L$ כך ש $y = \frac{x}{\sigma x}$. אזי

$$\mathrm{norm}_{L/K}(y) = \prod_{i=0}^{n-1} \sigma^i \left(\frac{x}{\sigma x}\right) = \frac{x(\sigma x)\cdots(\sigma^{n-1}x)}{(\sigma x)(\sigma^2 x)\cdots(\sigma^n x)} = 1 \quad .$$

להפך, נניח ש $\mathrm{norm}_{L/K}(y) = 1$. נתבונן ב n האברים

$$1, y, y\sigma y, \cdots, y(\sigma y)\cdots(\sigma^{n-2}y)$$

הואיל והם שונים מאפס, נובע מאי התלות הלינארית של $1, \sigma, \ldots, \sigma^{n-1}$ שההעתקה

$$\sigma^0 + y\sigma^1 + y(\sigma y)\sigma^2 + \cdots + y(\sigma y)\cdots(\sigma^{n-2}y)\sigma^{n-1}$$

מ $L^\times$ לתוך L שונה מאפס. קיָם אפוא $z \in L^\times$ כך ש

$$x = z + y(\sigma z) + y(\sigma y)(\sigma^2 z) + \cdots + y(\sigma y)\cdots(\sigma^{n-2}y)(\sigma^{n-1}z) \neq 0$$

נפעיל את σ על שני אֲגפי השויון:

$$\sigma x = \sigma z + (\sigma y)(\sigma^2 z) + (\sigma y)(\sigma^2 y)(\sigma^3 z) + \cdots + (\sigma y)(\sigma^2 y)\cdots(\sigma^{n-1} y)(\sigma^n z)$$

ונכפיל את שני האגפים ב y:

$$y\sigma x = y\sigma z + y(\sigma y)(\sigma^2 z) + y(\sigma y)(\sigma^2 y)(\sigma^3 z) + \cdots + y(\sigma y)(\sigma^2 y)\cdots(\sigma^{n-1} y)(\sigma^n z)$$

האבר האחרון באגף ימין אינו אלא $\mathrm{norm}_{L/K}(y)z$, השוה לפי ההנחה ל z. לכן, $x = y\sigma x$, כמבֻקש. ∎

משפט 2.6.2 (Kummer): *יהי K שדה, יהי n מספר טבעי שאינו מתחלק ב $\mathrm{char}(K)$. נניח שקיָם ב K שרש יחידה ζ_n מסדר n.*

(א) *תהי L הרחבה מעגלית של K ממעלה n. אזי קיָם $x \in L$ כך ש $L = K(x)$ ו $x^n \in K$.*

(ב) *יהיו $a \in K$ ו $x \in K_s$ אברים המקיְמים $x^n = a$. אזי $K(x)/K$ הִנה הרחבה מעגלית ממעלה d, באשר d הנו המחלק הקטן ביותר של n שעבורו $x^d \in K$.*

הוכחת א: יהי σ יוצר של $\mathrm{Gal}(L/K)$. אזי

$$\mathrm{norm}_{L/K}(\zeta_n^{-1}) = \prod_{i=0}^{n-1} \sigma^i(\zeta_n^{-1}) = (\zeta_n^{-1})^n = 1 \ .$$

המשפט ה 90 של הִלברט נותן $x \in L^\times$ כך ש $\zeta_n^{-1} = \frac{x}{\sigma x}$ ולכן $\sigma x = \zeta_n x$. הואיל ו $\zeta_n \in K$, נובע משִׁויון זה בהשראה על i ש $\sigma^i x = \zeta_n^i x$ עבור $i = 0, \ldots, n-1$. האברים האלו שונים זה מזה וכֻלם צמודים ל x מעל K. לכן $L = K(x)$ (משפטון 1.10.3). נוסף על כך מתקיֵם $\sigma(x^n) = (\sigma x)^n = (\zeta_n x)^n = x^n$. לכן, $x^n \in K$, כנִטען.

הוכחת ב: למשואה $X^n - a = 0$ יש n שָׁרשים שונים ב $K(x)$ והם $x, \zeta_n x, \zeta_n^2 x, \ldots, \zeta_n^{n-1} x$. בפרט $K(x)$ הנו שדה הפִּצול של $X^n - a$ ולכן $K(x)/K$ היא הרחבת גלואה. הואיל וכל צמוד של x הוא אחד השרשים הללו, קיֶמת לכל $\sigma \in \mathrm{Gal}(K(x)/K)$ חזקה w_σ של ζ_n כך ש $\sigma x = w_\sigma x$. אם τ הנו אבר נוסף של $\mathrm{Gal}(K(x)/K)$, אזי

$$w_{\tau\sigma} x = \tau\sigma x = \tau(w_\sigma x) = w_\sigma \tau x = w_\sigma w_\tau x$$

ולכן $w_{\tau\sigma} = w_\tau w_\sigma$. במלים אחרות, ההעתקה $w_\sigma \mapsto \sigma$ של $\mathrm{Gal}(K(x)/K)$ לתוך החבורה המעגלית $\mu_n(K)$ מסדר n הִנה הומומורפיזם. הגרעין של העתקה זו טריביאלי. לכן, $\mathrm{Gal}(K(x)/K)$ היא חבורה מעגלית מסדר d המחלק את n. אם σ יוצר את $\mathrm{Gal}(K(x)/K)$, אזי $d = \mathrm{ord}(\sigma) = \mathrm{ord}(w_\sigma)$. לכן,

$\sigma(x^d) = (\sigma x)^d = (w_\sigma x)^d = x^d$ ולכן $x^d \in K$, כפי שהיה להוכיח. אם k הוא מספר טבעי כך ש $x^k \in K$, אזי $x^k = \sigma(x^k) = w_\sigma^k x^k$ ולכן, $w_\sigma^k = 1$. לכן, $k \geq \mathrm{ord}(w_\sigma) = d$. ∎

למשפט קומר יש מקבילה באפיון חיובי שנביאֶנה ללא הוכחה.

משפט 2.6.3 (Artin-Schreier): *יהי K שדה בעל אפיון חיובי p.*

(א) *תהי L הרחבה מעגלית של K ממעלה p. אזי $L = K(x)$ ו x הוא שרש של משואה אי פריקה מהצורה $X^p - X - a = 0$ מעל K.*

(ב) *נתבונן בפולינום $f(X) = X^p - X - a$ עם $a \in K$. אזי או ש $f(X)$ מתפרק לגורמים לינאריים מעל K או ש $f(X)$ אי פריק מעל K. אם במקרה האחרון, $x \in \tilde{K}$ הוא שרש של $f(X)$, אזי $K(x)/K$ היא הרחבה מעגלית ממעלה p ו $f(X) = \prod_{i=0}^{p-1}(X - x - i)$.*

הוכחה: ראה [Lan93, p. 290]. ∎

נִתן להכליל את משפט ארטין־שרייר להרחבות מעגליות ממעלה p^n בעזרת וקטורי Witt .

תרגיל 2.6.4: יהי $f \in K[X]$ פולינום אי פריק ופריד ממעלה ראשונית p ויהיו x_1, x_2 שני שרשים שונים של f ב K_s כך ש $K(x_1) = K(x_2)$. הוכח ש $K(x_1)/K$ הנה הרחבה מעגלית (ממעלה p). רמז: יהיו $x_1, \ldots, x_d$ כל השרשים של f השיָכים ל $L = K(x_1)$. אם L' הוא שדה הצמוד ל L מעל K ושונה מ L, אזי $L' = K(x'_1, \ldots, x'_d)$ באשר $x'_1, \ldots, x'_d$ הם שרשים של f ו $x_i \neq x'_j$ לכל i, j. ∎

תרגיל 2.6.5: יהי n מספר טבעי שאינו מתחלק באפיון של שדה K. נניח ש $\zeta_n \in K$ ויהיו a, b אברים של K כך ש $[K(\sqrt[n]{a}) : K] = [K(\sqrt[n]{b}) : K]$. הוכח ש $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ אם ורק אם קיָם אבר $c \in K$ וקיָם r שלם הזר ל n כך ש $a = b^r c^n$. ∎

תרגיל 2.6.6: תהי q חזקה של מספר ראשוני אי זוגי. הוכח ש $(\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^2) = 2$ והסק מכאן שמספר הרבועים ב $\mathbb{F}_q^\times$ שוה למספר האי רבועים בחבורה זו. ∎

2.7 הרחבות פתירות

אנו נצביע בסעיף זה על הקשר בין האפשרות לפתֹר משואה אלגברית בנעלם אחד מעל שדה K בעזרת ארבעת פעֻלות החשבון הבסיסיות והוצאות שרש לבין פתירות של חבורת גלואה של שדה הפִּצול של המשואה.

הגדרה 2.7.1: פתירות על ידי שרשים. תהי L/K הרחבה פרידה סופית. נאמר ש ההרחבה L/K **שָׁרשונית** אם קָיָם מגדל של שדות $K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r$ כך ש $L \subseteq M_r$ ולכל $0 \le i \le r-1$ מתקבל M_{i+1} מ M_i באחד משְׁני האֳפנים הבאים:

(א) $M_{i+1} = M_i(\sqrt[n]{a})$, באשר $a \in M_i$ ו $n \nmid \mathrm{char}(K)$,

(ב) $M_{i+1} = M_i(x)$, באשר $x^p - x - a = 0$, $p = \mathrm{char}(K)$ ו $a \in K$.

יהי $f \in K[X]$ פולינום אי פריק ופריד ויהי $x \in K_s$ שרש של f. אנו נאמר שהמשואה $f(X) = 0$ **פתירה על ידי שרשים** אם ההרחבה $K(x)/K$ שרשונית. במקרה זה נִתן להציג את x בעזרת אברי K על ידי הפעֻלות חבור, חִסור, כפל, חִלוק והוצאות שרש.

לבסוף נאמר שהרחבה של שדות N/K הנה **פתירה** אם N/K הנה הרחבת גלואה סופית ו $\mathrm{Gal}(N/K)$ הנה חבורה פתירה. ∎

משפט 2.7.2: *תהי L/K הרחבה פרידה סופית עם סגור גלואה $\hat{L}$. אזי L/K שָׁרשונית אם ורק אם ההרחבה $\hat{L}/K$ פתירה.*

הוכחה: נניח קודם שההרחבה $\hat{L}/K$ פתירה. אזי $\hat{L}/K$ היא הרחבת גלואה סופית והחבורה $G = \mathrm{Gal}(\hat{L}/K)$ פתירה. במִלים אחרות, קיֶמת ל G סִדרה נורמלית $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1$ כך שהמנה G_i/G_{i+1} אבלית עבור $i = 0, 1, \ldots, r-1$. יתר על כן, אפשר לעדֵן את הסדרה כך שכל אחת מהמנות G_i/G_{i+1} תהיה מעגלית מסדר ראשוני. נסמן ב L_i את שדה השֶׁבֶת של G_i ב $\hat{L}$. אזי

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r = \hat{L}$$

הוא מגדל שדות ו L_i/L_{i-1} היא הרחבה מעגלית ממעלה ראשונית p_i עבור $i = 1, \ldots, r$. נסמן ב n את המכפלה של כל אותם ה p_i־ים השונים מ $\mathrm{char}(K)$ ויהי $M_i = L_i(\zeta_n)$, $i = 0, \ldots, r$. אזי

$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r$ היא סדרה של הרחבות גלואה ו $L \subseteq \hat{L} \subseteq M_r$.

$$\begin{tikzcd}
 & \hat{L} = L_r \arrow[r, dash] \arrow[d, dash, "p_r"] \arrow[dl, dash] & M_r \arrow[d, dash] \\
 & L_{r-1} \arrow[r, dash] \arrow[d, dotted, dash] & M_{r-1} \arrow[d, dotted, dash] \\
L \arrow[d, dash] & L_1 \arrow[r, dash] \arrow[d, dash, "p_1"] & M_1 \arrow[d, dash] \\
K \arrow[r, equal] & L_0 \arrow[r, dash] & M_0 = L_0(\zeta_n)
\end{tikzcd}$$

לכל $1 \leq i \leq r$ מתקיֵם $M_{i+1} = L_{i+1}(\zeta_n) = L_{i+1}M_i$ ולכן

$$\mathrm{Gal}(M_{i+1}/M_i) \cong \mathrm{Gal}(L_{i+1}/L_{i+1} \cap M_i)$$

היא חבורה חלקית של החבורה המעגלית $\mathrm{Gal}(L_{i+1}/L_i)$ מסדר p_i. מכאן ש $\mathrm{Gal}(M_{i+1}/M_i)$ היא חבורה טריביאלית או חבורה מעגלית מסדר p_i. אם $p_i = \mathrm{char}(K)$, אזי M_{i+1}/M_i היא הרחבת ארטין־שרייר. אחרת, M_{i+1}/M_i היא הרחבת קומר (כי במקרה זה $\zeta_{p_i} \in M_i$). בנוסף לזה, $M_0 = K(\zeta_n)$ ולכן ההרחבה L/K שָרשונית.

להפך, נניח שההרחבה L/K שָרשונית. אזי קיָם מגדל של שדות $K = E_0 \subseteq \cdots \subseteq E_{r-1} \subseteq E_r$, כך $L \subseteq E_r$ ולכל $0 \leq i \leq r-1$ מתקבל E_{i+1} מ E_i על ידי צרוף שרש n־י של אבר של E_i, באשר n אינו מתחלק ב $\mathrm{char}(K)$ או ש E_{i+1}/E_i היא הרחבת ארטין־שרייר.

נניח בהשראה על r ש E_{r-1} מוכלת בהרחבת גלואה פתירה F_{r-1} של K. אם E_r היא הרחבת ארטין־שרייר של E_{r-1} או ש E_r מתקבלת מ E_{r-1} על ידי צרוף שרש יחידה, נסמן $M = F_{r-1}$ ו $F_r = E_rM$. אחרת, $E_r = E_{r-1}(\sqrt[n]{a})$ באשר $a \in E_{r-1}$ ו $n \nmid \mathrm{char}(K)$. במקרה זה נסמן $M = F_{r-1}(\zeta_n)$ ו $F_r = E_rM$.

בכל מקרה M/K היא הרחבה פתירה ו F_r/M היא הרחבה אבלית סופית.

$$\begin{tikzcd}
 & & & N= (\sigma_1 F_r)\cdots(\sigma_s F_r) \arrow[d, dash] \\
\hat{L} \arrow[urrr, dash] \arrow[dd, dash] & E_r \arrow[rr, dash] \arrow[d, dash] & & F_r \arrow[d, dash] \\
 & E_{r-1} \arrow[r, dash] \arrow[d, dotted, dash] & F_{r-1} \arrow[r, dash] & M \\
L \arrow[d, dash] & E_1 \arrow[d, dash] & & \\
K \arrow[r, equal] & E_0 & &
\end{tikzcd}$$

יהיו $\sigma_1, \ldots, \sigma_s$ כל שכוני־K של M לתוך K_s. הואיל ו M/K היא הרחבת גלואה, $\sigma_i M = M$ ולכן, $\sigma_i F_r/M$ היא הרחבה מעגלית, עבור $i = 1, \ldots, s$. בתור צרוף של הרחבות מעגליות, הצרוף

$$N = (\sigma_1 F_r)\cdots(\sigma_s F_s)$$

הנו הרחבה אבלית של M. (משפטון 2.2.4). בנוסף, N הוא הרחבת גלואה של K ולכן הרחבה פתירה של K. הואיל ו F מקיף את L, הוא מקיף גם את $\hat{L}$, לכן $\mathrm{Gal}(\hat{L}/K)$ הנה מנה של החבורה הפתירה $\mathrm{Gal}(N/K)$. מכאן ש $\mathrm{Gal}(\hat{L}/K)$ פתירה, כפי שהיה להוכיח. ∎

לאחר שהראינו שכל חבורה אבלית סופית נִתנת למִמוש מעל $\mathbb{Q}$ נוכיח בסעיף זה אותו הדבר לגבי החבורות הסימטריות. אחת התוצאות תהיה שאי אפשר לפתֹר משואה כללית ממעלה $5 \leq$ בעזרת ארבעת פעֻלות החשבון הרגילות והוצאות שֹרש.

הערה 2.8.1: *חבורת גלואה של פולינום.* יהי K שדה ויהי $f \in K[X]$ פולינום ממעלה n בעל n שֹרשים שונים $x_1, \ldots, x_n$ ב $\tilde{K}$. אזי, שדה הפִצול של f מעל K הוא $L = K(x_1, \ldots, x_n)$ ומהוֶה הרחבת גלואה של K ממעלה שאינה עולה על $n!$. נסמן $G = \mathrm{Gal}(L/K)$.

לכל $\sigma \in G$, מהוָה $(\sigma x_1, \ldots, \sigma x_n)$ תמורה של ה n־יה $\mathbf{x} = (x_1, \ldots, x_n)$ שתסֻמן ב $\pi(\sigma)$. ביֶתר פרוט, $\pi(\sigma)(x_i) = \sigma x_i$. ההעתקה π מהוָה שִכון של G לתוך חבורת התמורות $S(\mathbf{x})$ של $\mathbf{x}$. התמונה של G בתוך $S(\mathbf{x})$ תסֻמן ב $\mathrm{Gal}(f, K)$ ותִקרא **חבורת גלואה של** f **מעל** K. ∎

נזכיר שחֲבורת תמורות G של קבוצה X הנה **יוצאת** (transitive) אם לכל $x, y \in G$ קיָם $\sigma \in G$ כך ש $\sigma x = y$.

למה 2.8.2: *פולינום פריד* $f \in K[X]$ *הנו אי פריק ב* $K[X]$ *אם ורק אם החבורה* $\mathrm{Gal}(f, K)$ *יוצאת.*

הוכחה: נסמן ב L את שדה הפִצול של f מעל K. נניח ש f אי פריק ויהיו $i \neq j$. אזי קיָם איזומורפיזם־K $K(x_i) \to K(x_j)$ המעתיק את x_i ל x_j (משפטון 1.3.4) והנִתן מִצדו להרחבה לאוטומורפיזם של L, כלומר לאבר $\sigma \in \mathrm{Gal}(L/K)$. בפרט, $\sigma x_i = x_j$. לכן, $\mathrm{Gal}(f, K)$ יוצאת.

להפך, נניח שחבורת התמורות $\mathrm{Gal}(f, K)$ יוצאת. יהי g גורם אי פריק של f ב $K[X]$. נבחר שרש x של g בשדה הפצול של f מעל K. אזי, לכל שרש x' של f קיָם $\sigma \in \mathrm{Gal}(f, K)$ כך ש $\sigma x = x'$. לכן x' הוא גם שרש של g. הואיל ו f פריד, אנו מקבלים מכאן ש $g = f$. לכן, f אי פריק. ∎

הגדרה 2.8.3: אנו אומרים שאברים $t_1, \ldots, t_n$ בשדה הרחבה של K **אינם תלויים אלגברית** אם $h(t_1, \ldots, t_n) \neq 0$ לכל פולינום שונה מאפס $h \in K[X_1, \ldots, X_n]$. במקרה זה נקרא לפולינום

$$f(\mathbf{t}, X) = X^n + t_1 X^{n-1} + \cdots + t_n$$

במשתנה X שמקדמיו שיָכים לחוג $K[\mathbf{t}]$ (באשר $\mathbf{t} = (t_1, \ldots, t_n)$) **הפולינום הכללי ממעלה** n. כל פולינום מתֻקן ב $K[X]$ מתקבל על ידי הצבת אברים במקום המשתנים $t_1, \ldots, t_n$. ∎

הגדרה 2.8.4: *הפולינומים הסימטריים היסודיים.* לכל $1 \leq k \leq n$ הפולינום

$$p_k(X_1, \ldots, X_n) = \sum_{\mathbf{j}} X_{j_1} X_{j_2} \cdots X_{j_k} \tag{1}$$

באשר $\mathbf{j} = (j_1, \ldots, j_k)$ עובר על כל ה k־יות של מספרים שלמים המקַיְמות

$$.1 \le j_1 < j_2 < \cdots < \cdots < j_k \le n$$

נקרא **הפולינום הסימטרי היסודי ממעלה** k במשתנים $X_1, \ldots, X_n$. הוא מְשבת תחת כל תמורה של $X_1, \ldots, X_n$.

∎

משפט 2.8.5: *חבורת גלואה של הפולינום הכללי ממעלה n מעל $K(\mathbf{t})$ איזומורפית לחבורה הסימטרית S_n ממעלה n.*

הוכחה: יהי $f(\mathbf{t}, X) = \prod_{i=1}^{n}(X - x_i)$ הפרוק של f מעל $\widetilde{K(\mathbf{t})}$. נסמן $\mathbf{x} = (x_1, \ldots, x_n)$. אזי $K(\mathbf{x})$ הוא שדה הפִצול של $f(\mathbf{t}, X)$ מעל $K(\mathbf{t})$ ו

$$X^n + t_1 X^{n-1} + \cdots + t_n = \prod_{i=1}^{n}(X - x_i) \tag{2}$$

מצד שני, יהיו $y_1, \ldots, y_n$ אברים שאינם תלויים אלגברית ונסמן $\mathbf{y} = (y_1, \ldots, y_n)$. אזי כל תמורה של הקבוצה $y_1, \ldots, y_n$ נִתנת להרחבה לאוטומורפיזם של השדה $K(\mathbf{y})$. נוכל אפוא לראות את חבורת כל התמורות $S(\mathbf{y})$ של $\{y_1, \ldots, y_n\}$ כחבורת אוטומורפיזמים של $K(\mathbf{y})$. נסמן את שדה השֶבֶת של $S(\mathbf{y})$ ב E. לפי משפטון 2.1.5, $K(\mathbf{y})/E$ היא הרחבת גלואה ו $\mathrm{Gal}(K(\mathbf{y})/E) \cong S(\mathbf{y})$. בפרט, $[K(\mathbf{y}) : E] = |S(\mathbf{y})| = n!$.

לכל $1 \le k \le n$ נסמן $u_k = (-1)^k p_k(\mathbf{y})$. אזי u_k מְשבת על ידי כל אחד מאברי $S(\mathbf{y})$ ולכן שיָך ל E. מכאן ש $K(\mathbf{u}) \subseteq E$. לכן, לפי הפסקה הקודמת, $[K(\mathbf{y}) : K(\mathbf{u})] \ge n!$, באשר $\mathbf{u} = (u_1, \ldots, u_n)$.

מהגדרת הפולינומים הסימטריים היסודיים עולה ש

$$.X^n + u_1 X^{n-1} + \cdots + u_n = \prod_{i=1}^{n}(X - y_i)$$

לכן $K(\mathbf{y})$ הוא שדה הפִצול ש $f(\mathbf{u}, X)$ מעל $K(\mathbf{u})$. בפרט $[K(\mathbf{y}) : K(\mathbf{u})] \le n!$. אם נצרף אי שויון זה למסקנות של הפסקה הקודמת, נקבל ש $K(\mathbf{u}) = E$ ולכן $K(\mathbf{y})/K(\mathbf{u})$ הנו הרחבת גלואה ו $\mathrm{Gal}(K(\mathbf{y})/K(\mathbf{u})) \cong S(\mathbf{y}) \cong S_n$.

הואיל ו $y_1, \ldots, y_n$ אינם תלויי אלגברית מעל K, נִתן להרחיב את ההעתקה $y_i \mapsto x_i$, $i = 1, \ldots, n$ לאפימורפיזם־K $\varphi\colon K[\mathbf{y}] \to K[\mathbf{x}]$. הוא מקיֵם

$$,\varphi(u_k) = (-1)^k \varphi(p_k(\mathbf{y})) = (-1)^k p_k(\varphi(\mathbf{y})) = (-1)^k p_k(\mathbf{x}) = t_k$$

עבור $k = 1, \ldots, n$ ולכן $\varphi[K(\mathbf{u})] = K[\mathbf{t}]$. לכן, $\varphi_0 = \varphi|_{K[\mathbf{u}]}$ הנו אפימורפיזם־K של $K[\mathbf{u}]$ על $K[\mathbf{t}]$.

כל אבר $v \in K[\mathbf{u}]$ נִתן להצגה בצורה $v = g(\mathbf{u})$, באשר $g \in K[X_1, \ldots, X_n]$. לכן, $\varphi(v) = g(\varphi(\mathbf{u})) = g(\mathbf{t})$. אם $\varphi(v) = 0$, נקבל מאי התלות של $t_1, \ldots, t_n$ ש $g = 0$ ולכן גם $v = 0$. במלים אחרות, φ_0 הנו איזומורפיזם. לכן, נתן להרחיב את φ_0 לאיזומורפיזם $\varphi_0'\colon K(\mathbf{u}) \to K(\mathbf{t})$. איזומורפיזם זה מעתיק את $f(\mathbf{u}, X)$ על $f(\mathbf{t}, X)$. ולכן גם את שדה הפצול $K(\mathbf{y})$ של $f(\mathbf{u}, X)$ מעל $K(\mathbf{u})$ על שדה הפצול $K(\mathbf{x})$ של $f(\mathbf{t}, X)$ מעל $K(\mathbf{t})$. הואיל ו $K(\mathbf{y})/K(\mathbf{u})$ היא הרחבת גלואה עם חבורת גלואה איזומורפית ל S_n, גם $K(\mathbf{x})/K(\mathbf{t})$ היא כזו. במלים אחרות, $\mathrm{Gal}(f(\mathbf{t}, X), K(\mathbf{t})) = S_n$. ∎

תוצאה 2.8.6: *הפולינום הכללי ממעלה n מעל $K(\mathbf{t})$ פריד ואי פריק.*

הוכחה: נסמן את הפולינום הכללי ממעלה n ב f ואת שרשיו ב $x_1, \ldots, x_n$. לפי משפט 2.8.5, $\mathrm{Gal}(f, K(\mathbf{t})) = S(\mathbf{x})$ היא חבורה יוצאת. לכן, לפי למה 2.8.2, f אי פריק מעל $K(\mathbf{t})$. ∎

אומרים שפונקציה רציונלית $f \in K(X_1, \ldots, X_n)$ הנה **סימטרית** אם היא נשמרת תחת כל תמורה של המשתנים.

תוצאה 2.8.7:

(א) *יהי K שדה ו $x_1, \ldots, x_n$ משתנים. אזי כל פונקציה רציונלית סימטרית ב $x_1, \ldots, x_n$ עם מקדמים ב K נִתנת להצגה כפונקציה רציונלית סימטרית בפולינום הסימטריים היסודיים עם מקדמים ב K.*

(ב) *יהי R תחום שלמות בעל פריקות חד ערכית. אזי כל פולינום סימטרי $g \in R[x_1, \ldots, x_n]$ נִתן להצגה כפולינום בפולינומים הסימטריים היסודיים עם מקדמים ב R.*

(ג) *הפולינומים הסימטריים היְסודיים אינם תלויים אלגברית. כלומר, אם פולינום $h \in K[X_1, \ldots, X_n]$ שונה מאפס, אזי $h(p_1(\mathbf{X}), \ldots, p_n(\mathbf{X})) \neq 0$.*

(ד) *ההצגה של פונקציה או פולינום סימטרי ב (א) או ב (ב) על ידי הפולינומים הסימטריים היסודיים הִנה חד ערכית.*

הוכחת א: תהי $g(\mathbf{x}) \in K(\mathbf{x})$ פונקציה סימטרית. אזי $g(\mathbf{x})$ נשמרת תחת כל אבר של $S(\mathbf{x})$. לפי משפט 2.8.5 והוכחתו, $g(\mathbf{x}) \in K(\mathbf{t})$ באשר $t_1, \ldots, t_n$ הם הפולינומים הסימטריים היסודיים ב $x_1, \ldots, x_n$.

הוכחת ב: נסמן ב K את שדה המנות של R. יהי $g(\mathbf{x}) \in R[\mathbf{x}]$ פולינום סימטרי. אזי, $g(\mathbf{x}) \in K(\mathbf{t})$. מצד שני כל אחד מהאברים $x_1, \ldots, x_n$ הנו שרש של פולינום מתֻקן מעל $R[\mathbf{t}]$ ולכן שלם מעליו (כאן אנו משתמשים במושגים ותוצאות שלא נלמדו בקורס זה). מכאן שגם $g(\mathbf{x})$ שלם מעל $R[\mathbf{t}]$. הואיל ו $t_1, \ldots, t_n$ אינם תלויים אלגברית מעל K, $R[\mathbf{t}]$ הוא חוג בעל פריקות חד ערכית ולכן סגור בשלמות. מכאן ש $g(\mathbf{x}) \in R[\mathbf{t}]$, מה שגורר את טענתנו.

הוכחת ג: בהוכחת משפט 2.8.5 ראינו שאם יוצאים מאברים $y_1, \ldots, y_n$ שאינם תלויים אלגברית מעל השדה K ומגדירים $u_i = p_i(\mathbf{y})$, אזי ההעתקה $\mathbf{u} \mapsto \mathbf{t}$ נִתנת להרחבה לאיזומורפיזם־K $K(\mathbf{u}) \cong K(\mathbf{t})$. האברים

$t_1,\dots,t_n$ נִבחרו בהוכחה כך שלא יהיו תלויים אלגברית מעל K. לכן, גם $u_1,\dots,u_n$ אינם תלויים אלגברית מעל K.

הוכחת ד: הטענה נובעת מטענה (ג). ∎

תוצאה 2.8.8: *אם* $n \le 4$*, אזי המשואה הכללית מסדר* n *פתירה על ידי שרשים. אם* $n \ge 5$*, המשואה הכללית מסדר* n *אינה פתירה על ידי שרשים.*

הוכחה: בתורת החבורות מוכיחים ש S_n פתירה אם ורק אם $n \le 4$. הואיל וחבורת גלואה של המשואה הכללית מסדר n איזומורפית ל S_n (משפט 2.8.5), נובעת התוצאה ממשפט 2.7.2. ∎

כדי להוכיח את התוצאה הבאה, זקוקים אנו למשפט יסודי בתורת השדות שהוכח על ידי הִלברט ב 1892. למשפט כמה הוכחות. אף אחת מהן אינה קצרה במִדה מספקת כדי להביאה במסגרת זו.

משפטון 2.8.9 (משפט אי הפריקות של הלברט): *יהיו* $t_1,\dots,t_n$ *משתנים ויהי* $f \in \mathbb{Q}[t_1,\dots,t_n,X]$ *פולינום פריד. אזי קיָמים* $a_1,\dots,a_n \in \mathbb{Q}$ *כך ש* $\mathrm{Gal}(f(\mathbf{a},X),\mathbb{Q}) \cong \mathrm{Gal}(f(\mathbf{t},X),\mathbb{Q}(\mathbf{t}))$.

משפט 2.8.10: *לכל* n *טבעי נִתנת החבורה* S_n *לממוש מעל* $\mathbb{Q}$.

הוכחה: נְיַשֵּׁם את משפט אי הפריקות של הלברט על הפולינום הכללי ממעלה n. ∎

תרגיל 2.8.11: הוכח על סמך משפט אי הפריקות של הִלברט שאם $t_1,\dots,t_n$ משתנים ו $f \in \mathbb{Q}[\mathbf{t},X]$ הוא פולינום אי פריק, אזי קיָמים $a_1,\dots,a_n \in \mathbb{Q}$ כך ש $f(\mathbf{a},\mathbb{Q})$ הוא פולינום אי פריק. ∎

תרגיל 2.8.12: יהי K שדה, ויהי $f \in K[X]$ פולינום פריד ממעלה n עם שרשים $x_1,\dots,x_n$. נסמן ב $L = K(x_1,\dots,x_n)$ את שדה הפִצול של f מעל K ונניח ש $\mathrm{Gal}(L/K) \cong S_n$.

(א) הוכח ש f אי פריק מעל K.

(ב) הוכח ש $[K(x_1,\dots,x_{m+1}) : K(x_1,\dots,x_m)] = m$ עבור $m = 1,\dots,n-1$.

(ג) הסֵק שאין ל $K(x_1)$ שום אוטומורפיזם־K לא טריביאלי. ∎

נתונות במישור האוקלידי $\mathbb{R}^2$ נקודות, ישרים ומעגלים. הישרים נתונים כזוג של נקודות והמעגלים נתונים כמרכז (שהוא נקודה) וכמחוג (שהוא קטע). קטע נתן כזוג של נקודות. עלינו לבנות מנתונים אלו עצם גאומטרי בעזרת סרגל ומחוגה המקימים דרישות מסימות. נראה בסעיף זה שפתרון הבעיה ההנדסית הזו תלוי בכך שחבורות גלואה מסימות הנגזרות מהנתונים תקימנה תנאים מסימים שיפרטו להלן.

לדגמה, נתונים לנו ישר L ונקדה z_1 מחוץ ל L ואנו מתבקשים להוריד נצב לישר דרך הנקדה. לצרך זה נחוג מעגל סביב z_1 עם מחוג גדול דיו שיחתך את הישר בשתי נקדות שונות y_2, y_1. סביב y_1 ו y_2 נחוג מעגלים בעלי אותו מחוג שיהיה גדול דיו כך שהמעגלים יחתכו. נסמן את אחת מנקדות החתוך ב y_3. הישר העובר דרך z_1 ו y_3 יהיה נצב לישר הנתון L.

כדי להעביר את בעית הבניה הכללית למונחים אלגבריים, נעבר קודם כל מ $\mathbb{R}^2$ ל $\mathbb{C}$ על ידי שנחליף כל זוג (x, y) של מספרים ממשיים במספר המרכב $x + yi$, באשר כרגיל $i = \sqrt{-1}$. נראה אפוא את הנתונים כ m־יה $(z_1, \ldots, z_m)$ של מספרים מרכבים ואת הפתרון כוקטור $\mathbf{x}$ של מספרים מרכבים שיגדיר את העצם העומד לבניה. את הדרישות נציג כמערכת משואות $f_i(z_1, \ldots, z_m, \mathbf{x}) = 0$, $i = 1, \ldots, k$, עם מקדמים שלמים ש $z_1, \ldots, z_m, \mathbf{x}$ צריכים לקים.

למה 2.9.1: *תנאי הכרחי ומספיק לכך שנתן לבנות פתרון $\mathbf{x}$ של בעית בניה מנתונים $z_1, \ldots, z_m$ בעזרת סרגל ומחוגה הוא שנתן לבטא את $\mathbf{x}$ על בעזרת $z_1, \ldots, z_m$ ידי שמוש בפעלות חבור, חסור, כפל, חלוק והוצאת שרש רבועי.*

הוכחה שהתנאי הכרחי: נניח שנתן לבנות את $\mathbf{x}$ מ $z_1, \ldots, z_m$ בעזרת סרגל ומחוגה. הבניה נעשית שלב אחר שלב, כך שבכל שלב משתמשים בכל הנקדות שנבנו כבר בשלבים הקודמים. בשלב ה i־י בונים נקדה y_i בעזרת הנקדות $z_1, \ldots, z_m, y_1, \ldots, y_{i-1}$. בסופו של דבר, הנקדות $x_1, \ldots, x_n$ ימצאות בין הנקדות y_i. הפעלות המותרות בבניה הם:

(א) בחירת נקדה z במישור השונה המקימת כמה שויונות או אי שויונות לינאריים או רבועיים ביחס לנקדות שנבנו קודם לכן כך ש z שיך לשדה הנוצר על ידי כל הנקדות שנבנו קודם לכן מעל $\mathbb{Q}$.

(ב) העברת ישר דרך שתי נקדות נתונות.

(ג) שרטוט מעגל סביב נקדה נתונה ברדיוס נתון.

(ד) מציאת נקדות חתוך של ישרים ומעגלים שנבנו כבר. נקדות החתוך מתאימות לפתרות מערכות משואות לינאריות ומשואות רבועיות. לכן אפשר לתאר את הפתרונות בעזרת ארבעת פעלות החשבון הרגילות והוצאת שרש רבועי.

הוכחה שהתנאי מספיק: נניח שהפתרון $\mathbf{x}$ נתן לבטוי בעזרת הפעלות הנ"ל. כל אחת מהפעלות הללו נתנת לבניה בעזרת סרגל ומחוגה.

כדי לחבר שני מספרים מרֻכבים z_1, z_2 בונים את הקדקד הרביעי של המקבילית ששאר קדקדיה הם $0, z_1, z_2$.

כדי לחשב את המכפלה $x = x_1x_2$ של שני מספרים ממשיים, x_1, x_2 משתמשים בזהות $\frac{x_1}{x} = \frac{1}{x_2}$ ובמשפט ששני ישרים מקבילים החותכים את השוקיִם של זוית מקצים עליה קטעים פרופורציוניים.

כדי לחשב את המכפלה $z = z_1z_2$ של שני מספרים מרֻכבים רושמים אותם קודם כל בצורה $z = x + iy$, $z_1 = x_1 + iy_1$ ו $z_2 = x_2 + iy_2$ מוצאים את x_1, x_2, y_1, y_2 על ידי הורדת נִצבים על הצירים ואחר כך משתמשים בנֻסחה $z_1z_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$.

כדי לחשב את $y = \frac{1}{x}$ עבור מספר ממשי $x \neq 0$, משתמשים בזהות $\frac{1}{x} = \frac{y}{1}$ ובמשפט על יחסים מקבילים שהובא לעיל.

כדי לפתר משואה רבועית $X^2 + aX + c = 0$ עם מקדמים מרֻכבים, צריכים להשתמש בארבעת פעֻלות החשבון שתֹארו לעיל ובהוצאת שרש $w = \sqrt{z}$. מספיק להראות כיצד לבנות בעזרת סרגל ומחֻגה שרש של מספר ממשי חיובי r. תהי a הנקֻדה על הישר הממשי באמצע הדרך בין -1 ל r. נבנה מעגל סביב a שמחוגו $\frac{r+1}{2}$. מעגל זה יחתך את הקרן החיובית של ציר ה y־ים בנקֻדה b. הזוית $\angle(-1)br$ נשענת על קֹטר של מעגל ולכן היא ישרה. כמו כן הזוית $\angle(-1)ob$ ישרה. לכן כל אחת מהזויות $\angle(-1)b0$ ו $\angle(-1)rb$ משלימות את הזוית $\angle b(-1)r$ ל 90^0. מכאן שהן שוות ולכן הטנגנסים שלהם שוים זה לזה. אם נסמן את הארך של הקטע $0b$ ב s נקבל ש $\frac{1}{s} = \frac{s}{r}$, כלומר $s^2 = r$, כמבֻקש. ∎

הגדרה 2.9.2: יהי p מספר ראשוני. הרחבת שדות L/K נקראת **הרחבת־p** אם L/K היא הרחבת גלואה סופית ו $\mathrm{Gal}(L/K)$ היא חבורת־p, כלומר $[L : K]$ היא חזקה של p.

במקרה זה, אם E הוא שדה בֵּינַיִם ו E/K גלואה, אזי גם E/K היא הרחבת p. אם $L_1, \ldots, L_n$ הן הרחבות־p של K, אזי גם הצרוף שלהן L הוא הרחבת־p. ואכן, ההעתקה $\sigma \mapsto (\sigma|_{L_1}, \ldots, \sigma|_{L_n})$ משכֶּנת את $\mathrm{Gal}(L/K)$ לתוך $\mathrm{Gal}(L_1/K) \times \cdots \times \mathrm{Gal}(L_n/K)$. ∎

למה 2.9.3: *תנאי הכרחי ומספיק לכך שנִתן לבנות פתרון $\mathbf{x}$ של בעית בניה מנתונים $z_1, \ldots, z_n$ בעזרת סרגל ומחֻגה הוא שהשדה $\mathbb{Q}(\mathbf{z}, \mathbf{x})$ מוכל בהרחבת־ 2 של $\mathbb{Q}(\mathbf{z})$. (אנו משתמשים כאן בסימון הוקטורי $\mathbf{z} = (z_1, \ldots, z_n)$).*

הוכחה שהתנאי הכרחי: אם נִתן לבנות את $\mathbf{x}$ בעזרת סרגל ומחֻגה, אזי לפי למה 2.9.1, קיָם מגדל שדות $\mathbb{Q}(\mathbf{z}) = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = \mathbb{Q}(\mathbf{z}, \mathbf{x})$ כך ש $[F_{i+1} : F_i] = 2$ עבור $i = 0, 1, \ldots, r-1$. מהגדרה 2.9.2 נובע שסגור גלואה של $F_r/\mathbb{Q}(\mathbf{z})$ הנו הרחבת־2.

הוכחה שהתנאי מספיק: להפך, נניח שקיֶמת ל $\mathbb{Q}(\mathbf{z})$ הרחבת־2 F המקיפה את $\mathbb{Q}(\mathbf{z}, \mathbf{x})$. אזי $G = \mathrm{Gal}(F/\mathbb{Q}(\mathbf{z}, \mathbf{x}))$ היא חבורת־2. לחבורה כזו קיֶמת סדרה נורמלית $1 = G_r \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ שגורמיה מסדר 2. אם נסמן ב F_i את שדה השֶבת של G_i ב F, נקבל ש F_{i+1} היא הרחבה רבועית של F_i ולכן מתקבלת על ידי פתרון משואה רבועית עם מקדמים שבנינו אותם כבר בשלב ה i־י. ∎

בעזרת משפט זה אפשר לפתֹר כמה מהבעיות שהיְוָנים העמידו.

בעיה 2.9.4: בנֵה בעזרת סרגל ומחֻגה קֻביה שנפחה שוה לפעמַים נפח של קֻביה נתונה.

נצא מקֻביה שארך צלעה 1. כדי לבצע את הבניה המבֻקשת, עלינו לפתֹר את המשואה $x^3 = 2$. הפתרון הוא $x = \sqrt[3]{2}$. אולם $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ אינו מוכל בהרחבת־2 של $\mathbb{Q}$. לכן, לפי למה 2.9.3, הבנִיה אינה אפשרית.

∎

בעיה 2.9.5: חלֵק זוית נתונה בעזרת סרגל ומחֻגה לשלשה חלקים שוים.

תהי $\alpha = 3\beta$ זוית. נניח שהיא נתונה על ידי $a = \cos\alpha$. נסמן $x = \cos\beta$. כדי לקבל את הקשר בין a ל x נצא מהנֻסחה $\cos 3\beta = 4cos^3\beta - 3\cos\beta$ ונִרשם אותה בצוה $4x^3 - 3x = a$. אם נקח למשל $a = \frac{1}{3}$ נקבל את המשואה $4x^3 - 3x = \frac{1}{3}$ שאינה פתירה מעל $\mathbb{Q}$ (ההצבה $y = \frac{1}{x}$ מעבירה אותה למשואת אייזנשטיין $y^3 + 9y^2 - 12 = 0$). לכן $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. מכאן אנו שוב מקבלים לפי למה 2.9.3, שהבניה אינה אפשרית.

∎

בעיה 2.9.6: בנה רִבוע ששטחו שוה לשטח עִגול נתון.

אם מחוג העגול הנתון שוה ל 1 וצלע הרבוע המבֻקש הנה x, אזי שטח העגול שוה ל π ושטח הרִבוע שוה ל x^2. מהקשר $x^2 = \pi$ נקבל ש $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{\pi})$ הוא הרחבה נעלה של $\mathbb{Q}$, בפרט אינה מוכלת בשום הרחבת־2 של $\mathbb{Q}$. שוב, הבניה אינה אפשרית. ∎

2.10 המשפט היסודי של האלגברה

הדֻגמה המֻבהקת ביותר לשדה סגור אלגברית היא שדה המספרים המרֻכבים $\mathbb{C}$. את המשפט הזה הוכיח גאוס בדרכים שונות. אנו נביא הוכחה המסתמכת על הרציפות של פולינומים, על משפט סילו בתורת החבורות, ועל תורת גלואה.

כדי להוכיח את המשפט נצא משדה המספרים הממשיים $\mathbb{R}$, נסמן $i = \sqrt{-1}$ ו $\mathbb{C} = \mathbb{R}(i)$.

למה 2.10.1:

(א) *לכל פולינום $f \in \mathbb{R}[X]$ ממעלה אי זוגית יש שֹׁרש ממשי.*

(ב) *לכל משואה רִבועית מעל $\mathbb{C}$ יש שרש בשדה זה.*

הוכחת א: נחלק את f במקדם העליון שלו אם יש צֹרך בדבר כדי להניח ש f מתֻקן. בתנאי זה, אם $x_1 \in \mathbb{R}$ שלילי וקטן דיו, אזי $f(x_1) < 0$ ואלו אם $x_2 \in \mathbb{R}$ חיובי וגדול דיו, אזי $f(x_1) > 0$. הואיל ופולינום בעל מקדמים ממשיים הוא פונקציה רציפה, קיָם $x_1 < x < x_2$ כך ש $f(x) = 0$.

הוכחת ב: נשים לב לכך ש $\mathbb{C}$ היא הרחבה רִבועית של $\mathbb{R}$. שִׁמוש בנֻסחה לפתירת משואה רִבועית מראה שמספיק להוכיח שלכל מספר $c = a + bi$ ב $\mathbb{R}(i)$ יש שֹׁרש רבועי בו.

נתחיל במקרה שבו $b = 0$ ו $a > 0$. נבחר $0 < x_1$ קרוב דיו לאפס כך ש $x_1^2 < a$. עתה נבחר $x_2 > 0$ גדול דיו כך ש $a < x_2^2$. כמו בהוכחת (א), קיָם $x \in \mathbb{R}$ כך ש $x^2 = a$. אם $a < 0$, נבחר $x \in \mathbb{R}$ כך ש $x^2 = -a$ ונמצא ש $(ix)^2 = -a$.

עתה נניח ש $b \neq 0$ ונשאף לפתֹּר את המשואה $(x + iy)^2 = a + bi$ במשתנים ממשיים x, y. העלאה בחזקה והשואת מקדמים מראים שמשואה זו שקולה לזוג המשואות

$$x^2 - y^2 = a \qquad 2xy = b$$

חִלוץ y מהמשואה הימנית והצבתו בשמאלית מוביל למשואה $4x^4 - 4ax^2 - b^2 = 0$. אחד מארבעת הפתרונות של המשואה הזו מקיֵם $x^2 = \frac{1}{2}(a + \sqrt{a^2 + b^2})$. אגף ימין במשואה זו הנו ממשי, ולכן לפי הפִסקה הקודמת יש למשואה פתרון ממשי. ∎

משפט 2.10.2: *שדה המספרים המרֻכבים $\mathbb{C}$ סגור אלגברית.*

הוכחה: עלינו להראות שכל הרחבה סופית L_0 של $\mathbb{C}$ מתלכדת עם $\mathbb{C}$. השדה L_0 הנו גם הרחבה סופית של $\mathbb{R}$. לכן, סגוֹר גלואה L של $L_0/\mathbb{R}$ הוא הרחבת גלואה סופית המקיפה את $\mathbb{C}$. מספיק להוכיח ש $\mathbb{C} = L$. זאת נעשה בשני שלבים.

שלב א: *חבורת סילו־2.* נסמן $G = \mathrm{Gal}(L/\mathbb{R})$. תהי G_2 חבורת סילו־2 של G ויהי K שדה השֶׁבת של G_2 ב L. אזי $K/\mathbb{R}$ הוא הרחבה סופית של $\mathbb{R}$ ממעלה אי זוגית. יהי x אבר קדום של הרחבה זו. אזי $f = \mathrm{irr}(x, \mathbb{R})$ הוא פולינום אי פריק ממעלה אי זוגית. לפי למה 2.10.1, יש ל f שרש ממשי. לכן, $\deg(f) = 1$ ומכאן ש $K = \mathbb{R}$.

שלב ב: *חבורת־2.* משלב (א) נובע ש G היא חבורת־2. לכן, גם $\mathrm{Gal}(L/\mathbb{C})$ היא חבורת־2. אלו היה L הרחבה נאותה של $\mathbb{C}$ היתה קיֶמת לחבורה $\mathrm{Gal}(L/\mathbb{C})$ תת חבורה בעלת צִיון (=אנדקס) 2. שדה השבת שלה E יהיה הרחבה רִבועית של $\mathbb{C}$, בסתירה ללמה 2.10.1(ב). מִסתירה זו נובע ש $L = \mathbb{C}$, כפי שהיה להוכיח. ∎

הערה 2.10.3: שדה סגור ממשית. עיון מדֻקדק בהוכחת משפט 2.10.3 מראה שהיא נשארת שרירה גם אם מחליפים את $\mathbb{R}$ בשדה R המקיֵם את טַענות למה 2.10.1 כך ש $C = R(\sqrt{-1})$ הוא הרחבה רִבועית של R ואת $\mathbb{C}$ ב C. את השדה R נִתן לסַדר על ידי שמגדירים את x כאי שלילי אם ורק אם הוא רִבוע ב R. יתר על כן, נִתן להראות שאי אפשר להרחיב את הסדר של R לשום הרחבה אלגברית נאותה שלו. לכן הוא נקרא **שדה סגור ממשית**. בעזרת הלמה של צורן אפשר להראות שלכל שדה סדור K יש **סגוֹר ממשי**, כלומר הרחבה אלגברית $\bar{K}$ שאליה נִתן להרחיב את הסדר של K ושהיא מֵרבית בעלת תכונה זו. לדֻגמה, אם משכנים את $\tilde{\mathbb{Q}}$ ב $\mathbb{C}$, אזי $R = \tilde{\mathbb{Q}} \cap \mathbb{R}$ הוא סגוֹר ממשי של $\mathbb{Q}$. ∎

המשפט הבא משלים במובן מסֻים את המשפט היסודי של האלגברה ואת הערה 2.10.4. למרות שאפשר היה להביא את הוכחתו בקורס, איננו עושים זאת מטעמי חֹסר זמן.

משפט 2.10.4 ([Lan93, p. 299, Cor. 3.3]): *יהי K שדה כך ש* $1 < [\tilde{K} : K] < \infty$. *אזי* $\mathrm{char}(K) = 0$ *ו* $\tilde{K} = K(\sqrt{-1})$.

משפט אי הפריקות של הִלברט מוכיח שכל חבורה סימטרית נִתנת לממוש מעל $\mathbb{Q}$. בסעיף זה נביא דֻגמאות לפולינומים מעל $\mathbb{Q}$ בעלי חבורת גלואה S_5. כפי שהוכחנו, אי אפשר למצא את השרשים של פולינומים אלו על ידי ארבע פעֻלות החשבון הרגילות והוצאות שרש. חִשוב דֻגמאות אלו מבֻסס על הצגה של חבורת גלואה של פולינום בעזרת אברים נעֱלים.

למה 2.11.1: *תהי L/K הרחבת גלואה סופית, יהי $f \in K[X_1,\dots,X_n]$ פולינום אי פריק, ויהי $f = f_1 \cdots f_r$ הפרוק של f לגורמים אי פריקים ב $L[X_1,\dots,X_n]$. אזי לכל $\sigma \in \mathrm{Gal}(L/K)$, $(\sigma(f_1),\dots,\sigma(f_r))$ היא תמורה של $(f_1,\dots,f_r)$. יתר על כן, כל שנַים מהגורמים צמודים זה לזה מעל K, כלומר לכל i,j קיָם $\sigma \in \mathrm{Gal}(L/K)$ כך ש $\sigma f_i = f_j$.*

הוכחה: ראשית נשים לב לכך שבנִסוח המשפט הסתמכנו על אפשרות הפרוק של פולינומים ב $L[X_1,\dots,X_n]$ לגורמים אי פריקים (משפטון 1.1.11). נִתן לכל $\sigma \in \mathrm{Gal}(L/K)$ לפעֹל על $L[X_1,\dots,X_n]$ בעזרת הפעֻלה על מקדמי הפולינומים. בפרט נקבל ש $f = \sigma(f_1)\cdots\sigma(f_r)$. מהפריקות החד ערכית בחוג $L[X_1,\dots,X_n]$ נובע ש $(\sigma(f_1),\dots,\sigma(f_n))$ היא תמורה של $(f_1,\dots,f_n)$. בפרט, σf_1 הנו צמוד של f_1.

יהיו עתה $g_1,\dots,g_s$ כל הצמודים ל f_1 מבין הפולינומים $f_1,\dots,f_r$ ונסמן $g = g_1\cdots g_s$. אזי $g|f$ ב $L[X_1,\dots,X_n]$. יתר על כן, לכל $\sigma \in \mathrm{Gal}(L/K)$ ה s־יה $(\sigma(g_1),\dots,\sigma(g_s))$ היא תמורה של $(g_1,\dots,g_s)$. לכן, $\sigma(g) = \sigma(g_1)\cdots\sigma(g_s) = g$. מכאן נובע ש $g \in K[X_1,\dots,X_n]$. הואיל ו f אי פריק ב $K[X_1,\dots,X_n]$, נובע מכאן ש $f = g$ ו $r = s$. לכן, $(g_1,\dots,g_r)$ היא תמורה של $(f_1,\dots,f_s)$ ומכאן שכל שנים מגורמי f צמודים זה לזה, כפי שהיה להוכיח. ∎

משפטון 2.11.2: *יהי F שדה סופי, יהי $f \in F[X]$ פולינום פריד ויהי $f = f_1 \cdots f_m$ הפרוק שלו לגורמים אי פריקים. נסמן $d_i = \deg(f_i)$, $i = 1,\dots,m$. אזי קיָם $\sigma \in \mathrm{Gal}(f,F)$ המתפרק למכפלה של m חשוקים זרים מאֳרכים $d_1,\dots,d_m$.*

הוכחה: יהי N שדה הפִצול של f מעל F. לפי משפט 2.3.3, $\mathrm{Gal}(N/F)$ היא חבורה מעגלית. יהי σ יוצר שלה. לכל $1 \le i \le m$ נבחר שרש x_i של f_i ב N. הצמצום של σ לשדה הפצול של f_i יוצר את חבורת גלואה של שדה זה מעל F וחבורה זו הנה מסדר d_i. לפי למה 2.11.1, $x_1, \sigma(x_i),\dots,\sigma^{d_i-1}(x_i)$ הנם כל d_i השרשים של f_i. לכן, ההצגה של σ כתמורה של שרשי f_i הנה חשוק מארך d_i. אם נותנים ל i לעבֹר מ 1 עד m, מקבלים את ההצגה המבֻקשת של σ. ∎

בנִיה 2.11.3: *בנִיה של חבורת גלואה של פולינום.* יהי $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ פולינום פריד עם מקדמים בשדה K, יהי $f(X) = \prod_{i=1}^n (X - x_i)$ הפרוק של $f(X)$ לגורמים לינאריים מעל K_s ויהי

$L = K(x_1, \dots, x_n)$ שדה הפצול של f מעל K. נבחר $n+1$ אברים $u_1, \dots, u_n, Z$ שאינם תלויים אלגברית מעל K ונסמן ב $S(\mathbf{u})$ את חבורת התמורות של $\{u_1, \dots, u_n\}$. אזי אפשר לראות את $S(\mathbf{u})$ כתת חבורה של חבורת כל האומורפיזמים של $L(\mathbf{u}, Z)$ המשביתים את $L(Z)$.

נסמן

$$y = x_1 u_1 + \cdots + x_n u_n \tag{1}$$

אם $\pi \in S(\mathbf{u})$, אזי $\pi(y) = x_1\pi(u_1) + \cdots + x_n\pi(u_n)$. נסמן

$$g(\mathbf{u}, Z) = \prod_{\pi \in S(\mathbf{u})} (Z - \pi(y)) \tag{2}$$

אזי, g הוא פולינום ב $u_1, \dots, u_n, Z$

$$g(\mathbf{u}, Z) = \sum_{\mathbf{i}} g_{\mathbf{i}}(\mathbf{x}) u_1^{i_1} \cdots u_n^{i_n} Z^{i_{n+1}}$$

עם מקדמים $g_{\mathbf{i}}(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ שהם פולינומים סימטריים ב $x_1, \dots, x_n$ התלויים אך ורק ב n. משפט הפולינומים הסימטריים (תוצאה 2.8.7) נותן פולינומים $h_{\mathbf{i}} \in \mathbb{Z}[X_1, \dots, X_n]$ התלויים אך ורק ב n כך ש $g_{\mathbf{i}}(\mathbf{x}) = h_i(\mathbf{a})$. לכן,

$$g(\mathbf{u}, Z) = \sum_{\mathbf{i}} h_{\mathbf{i}}(\mathbf{a}) u_1^{i_1} \cdots u_n^{i_n} Z^{i_{n+1}} \tag{3}$$

בפרט, $g(\mathbf{u}, Z) \in K[\mathbf{u}, Z]$. יהי

$$g(\mathbf{u}, Z) = g_1(\mathbf{u}, Z) \cdots g_r(\mathbf{u}, Z) \tag{4}$$

פרוק של g לגורמים אי פריקים ב $K[\mathbf{u}, Z]$. מהגדרת g נובע שגורמים אלו זרים זה לזה. כל $\pi \in S(\mathbf{u})$ משבית את $g(\mathbf{u}, Z)$. ממשפט הפרוק החד ערכי בחוג הפולינומים $K[\mathbf{u}, Z]$ נובע ש $(\pi(g_1), \dots, \pi(g_r))$ היא תמורה ש $(g_1, \dots, g_r)$. נסמן $G = \{\pi \in S(\mathbf{u}) \mid \pi(g_1) = g_1\}$. אזי G היא חבורה חלקית של $S(\mathbf{u})$. יתר על כן, הגדרת g נותנת תת קבוצה A של $S(\mathbf{u})$ כך ש

$$g_1(\mathbf{u}, Z) = \prod_{\pi \in A} (Z - \pi(y))$$

אם יש צֹרך בכך נשנה את המספור של גורמי g כדי להניח ש $1 \in A$, כלומר ש $Z - y | g$. ∎

משפטון 2.11.4: *בסימונים של בניה* 2.11.3, $G \cong \mathrm{Gal}(f,K)$.

הוכחה: לכל $\pi \in S(\mathbf{u})$ נגדיר $\pi' \in S(\mathbf{x})$ על ידי הנֻסחה:

$$\pi'(x_i) = x_j \Longleftrightarrow \pi(u_i) = u_j$$

ההעתקה $' : S(\mathbf{u}) \to S(\mathbf{x})$ הִנה איזומורפיזם. נראה שהיא מעתיקה את G על $\mathrm{Gal}(f,K)$.

טענה: $A = G$. ואכן יהי $\pi \in G$. אזי $\pi(g_1) = g_1$ ולכן $Z - \pi(y) | g_1$. לכן, $\pi \in A$. להפך, נניח ש $\pi \in A$. אלו היה $\pi(g_1) = g_i$ עם $i \neq 1$. היה $Z - \pi(y)$ מחלק גם את g_1 וגם את g_i, בנגוד למה שנאמר בִּבְניה 2.11.3. לכן $\pi(g_1) = g_1$ ומכאן ש $\pi \in G$.

יהי עתה $\pi \in G$. אזי, לפי הטענה, $Z - y$ ו $Z - \pi(y)$ הם גורמים אי פריקים של $g_1(\mathbf{u},Z)$. הואיל וזִהנו את $\mathrm{Gal}(L(\mathbf{u},Z)/K(\mathbf{u},Z))$ עם $\mathrm{Gal}(f,K)$, נותנת למה 2.11.1 $\sigma \in \mathrm{Gal}(L/K)$ כך ש $Z - \sigma(y) = Z - \pi(y)$ ולכן, $\sigma(y) = \pi(y)$. אם נרשֹם את השִוְיון האחרון בצורה מפֹרטת יותר, $\sigma(x_1)u_1 + \cdots + \sigma(x_n)u_n = x_1\pi(u_1) + \cdots + x_n\pi(u_n)$, נקבל ש $\sigma(x_i) = x_j$ אם ורק אם $\pi(u_j) = u_i$. במִלים אחרות, $(\pi')^{-1} = \sigma \in \mathrm{Gal}(f,K)$.

להפך, יהי $\sigma \in \mathrm{Gal}(L/K)$. נגדיר $\pi \in S(\mathbf{u})$ על ידי $\pi(u_j) = u_i$ אם $\sigma(x_i) = x_j$. אזי $\sigma = (\pi')^{-1}$ ו $\sigma(\pi(y)) = y$, כלומר $\pi(y) = \sigma^{-1}(y)$. הואיל ו $\sigma^{-1}(g_1) = g_1$, אנו מקבלים מכאן ש $Z - \pi(y) = Z - \sigma^{-1}(y) | g_1$. לכן, לפי הטענה, $\pi \in G$. ∎

הערה 2.11.5: *הַעֲמדה מודולו p.* נתבונן עתה במקרה שבו $K = \mathbb{Q}$ ובפולינום פריד

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X].$$

יהי p מספר ראשוני. נסמן העמדה לפי p בגג. בפרט $\bar{f}(X) = X^n + \bar{a}_nX^{n-1} + \cdots + \bar{a}_n \in \mathbb{F}[X]$. נניח ש $\bar{f}$ פריד עם שרשים $x_1', \ldots, x_n'$. אם נבנה את הפולינום $g'(\mathbf{u},Z)$ לפי הנֻסחה (2) ביחס לשרשים $x_1', \ldots, x_n'$ נקבל מההצגה (3) ש $g'(\mathbf{u},Z)$ אינו אלא הפולינום $\bar{g}(\mathbf{u},Z) = \sum_{\mathbf{i}} \bar{h}(\bar{\mathbf{a}}) u_1^{i_1} \cdots u_n^{i_n} Z^{i_{n+1}}$ המתקבל מ (3) על ידי העמדה מודולו p. העמדה של (4) לפי p נותנת, $\bar{g} = \bar{g}_1 \cdots \bar{g}_r$. יהי $\bar{g}_1 = q_1 \cdots q_s$ פרוק של $\bar{g}$ לגורמים אי פריקים ב $\mathbb{F}_p[X_1, \ldots, X_n]$. אם $\sigma \in S(\mathbf{u})$ מקיֵם $\sigma(q_1) = q_1$, אזי q_1 הוא גורם אי פריק גם של $\bar{g}_1$ וגם של $\sigma(\bar{g}_1)$. הואיל וההעתקה $g_i \mapsto \bar{g}_i$, $i = 1, \ldots, n$ היא חד חד ערכית ו $\overline{\sigma(g_i)} = \sigma(\bar{g}_i)$, נקבל מכאן ש $\sigma(g_1) = g_1$. במלים אחרות החבורה $G_1' = \{\sigma \in S(\mathbf{u}) \mid \sigma(g_1') = g_1'\}$ של $S(\mathbf{u})$ חלקית ל G. לפי משפטון 2.11.4, $G' \cong \mathrm{Gal}(\bar{f}, \mathbb{F}_p)$. לכן, $\mathrm{Gal}(\bar{f}, \mathbb{F}_p)$ איזומורפית כחבורת תמורות לתת חבורה של $\mathrm{Gal}(f,\mathbb{Q})$.

לפי משפט 2.3.3, החבורה $\mathrm{Gal}(f,\mathbb{F}_p)$ מעגלית. יהי σ יוצר שלה וִיהי $\bar{f} = f_1 \cdots f_s$ פרוק לגורמים אי פריקים ב $\mathbb{F}_p[X]$. נסמן $d_i = \deg(f_i)$. אזי σ מתפרק למכפלה של s חִשוקונים מסדרים $d_1, \ldots, d_s$. לכן יש ב $\mathrm{Gal}(f,\mathbb{Q})$ אבר עם ההצגה הזו. ∎

דֻּגמה 2.11.6: הפולינום $f(X) = X^5 - X - 1$ מתפרק ב $\mathbb{F}_2[X]$ לגורמים אי פריקים באֹפן הבא:

$$X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$$

לכן, לפי הערה 2.11.5, יש ב $\mathrm{Gal}(f, \mathbb{Q})$ תמורה σ_1 המתפרקת למכפלה של **חִשּׁוּק** באֹרך 2 וחִשּׁוּק מארך 3. σ_1^3 תהיה אפוא **חִלּוּף** כלומר חִשּׁוּק מארך 2. בדיקה מראה ש $f(X)$ אי פריק ב $\mathbb{F}_5[X]$. לכן יש ב $\mathrm{Gal}(f, \mathbb{Q})$ חִשּׁוּק מאֹרך 5. מכאן ש G היא תת חבורה יוצאת של S_5. מאידך המכפלה של חזקה מתאימה של החִשּׁוּק מארך 5 והחִלּוּף הנה חִשּׁוּק מאר 4. מהלמה הבאה נובע ש $G = S_5$. ∎

למה 2.11.7: *תהי G תת חבורה יוצאת של S_n המכילה* **חִלּוּף**, *כלומר חִשּׁוּק מארך 2, וחִשּׁוּק מארך $n-1$. אזי $G = S_n$.*

הוכחה: בהוכחה זו נראה את התמורות כפועלות מימין על הקבוצה $\{1, \ldots, n\}$. בלי הגבלת הכלליות נניח שהחִשּׁוּק $\sigma = (1\,2 \cdots n-1)$ שַׁיָּךְ ל G. לפי ההנחה קַיָּם ב G חִלּוּף $(i\,j)$. נבחר $\pi \in G$ כך ש $j^\pi = n$ ויהי $k = i^\pi$. אזי $G \ni (i\,j)^\pi = (i^\pi\, j^\pi) = (k\,n)$. אם נצמיד את $(k\,n)$ בכל החֲזָקוֹת של σ נקבל ש $(m\,n) \in G$ לכל $1 \le m \le n-1$. לכל $1 \le l \le n-1$ נבחר $\lambda \in G$ כך ש $n^\lambda = l$. אזי $(m^\lambda\, l) \in G$. כאשר m עובר על כל המספרים בין 1 לבין $n-1$ עובר m^λ על כל המספרים בין 1 ל n השונים מ l. לכן $(i\,j) \in G$ לכל $1 \le i < j \le n$. לפי תורת החבורות, $G = S_n$. ∎

משפט 2.11.8: *כל חבורה סימטרית S_n נִתנת לְמִמּוּשׁ מעל $\mathbb{Q}$.*

הוכחה: הואיל ו S_2 הנה החבורה בעלת שני אברים, אפשר להניח בלי הגבלת הכלליות ש $n \ge 3$.

ראשית נעיר שעבור כל מספר ראשוני p יש לשדה $\mathbb{F}_p$ הרחבה ממעלה n (משפט 2.3.3). לכן, לפי משפט האבר הקדום, יש ב $\mathbb{F}_p[X]$ פולינום מתֻקן $\bar{g}$ אי פריק ממעלה n. את הפולינום הזה נוכל להרים לפולינום מתֻקן g ממעלה n, ו g יהיה אי פריק ב $\mathbb{Z}[X]$ ולכן גם ב $\mathbb{Q}[X]$ (לפי למת גאוס).

בעזרת הערה זו נבחר אפוא פולינום מתֻקן $f_2 \in \mathbb{Z}[X]$ ממעלה n שיהיה אי פריק ב $\mathbb{F}_2[X]$. עתה נבחר פולינום מתֻקן $g_3 \in \mathbb{Z}[X]$ ממעלה $n-1$ שיהיה אי פריק ב $\mathbb{F}_3[X]$. נסמן $f_3(X) = (X-1)g_3(X)$. לבסוף נבחר פולינום רבועי מתֻקן $g_5 \in \mathbb{Z}[X]$ שיהיה אי פריק ב $\mathbb{F}_5[X]$. אם n אי זוגי נבחר פולינום מתֻקן $h_5 \in \mathbb{Z}[X]$ ממעלה $n-2$ שיהיה אי פריק ב $\mathbb{F}_5[X]$ ונסמן $f_5(X) = g_5(X)h_5(X)$. אם n זוגי, נבחר פולינום מתֻקן $j_5 \in \mathbb{Z}[X]$ ממעלה $n-3$ שיהיה אי פריק ב $\mathbb{F}_5[X]$ ונסמן $f_5(X) = (X-1)g_5(X)j_5(X)$. בכל אחד משני המקרים f_5 פריד ב $\mathbb{F}_5[X]$.

עתה נסמן $f = -15f_2 + 10f_3 + 6f_5$. אזי $f \in \mathbb{Z}[X]$ הוא פולינום מתֻקן ממעלה n, $f \equiv f_2 \mod 2$, $f \equiv f_3 \mod 3$ ו $f \equiv f_5 \mod 5$.

מהחפיפה הראשונה נובע, לפי הערה 2.11.5, ש $\mathrm{Gal}(f, \mathbb{Q})$ מכיל חִשּׁוּק מארך n. לכן, $\mathrm{Gal}(f, \mathbb{Q})$ הנה חבורה יוצאת. מהחפיפה השניה נובע, שוב לפי הערה 2.11.5, שיש ב $\mathrm{Gal}(f, \mathbb{Q})$ חִשּׁוּק מארך $n-1$. לבסוף

מהחפיפה השלישית נובע, לפי הערה 2.11.5, שיש ב $\mathrm{Gal}(f,\mathbb{Q})$ מכפלה של חִלוף וחִשוק מארך אי זוגי. העלאה בחזקה אי זוגית, מראה שיש ב $\mathrm{Gal}(f,\mathbb{Q})$ גם חִלוף. לכן, לפי משפטון 2.11.7, $\mathrm{Gal}(f,\mathbb{Q}) \cong S_n$. ∎