מבוא לתורת השדות

עוזי וישנה

מבוא לתורת השדות
מהדורה 1.38

הקדמה. שדות הם החוגים המוצלחים ביותר: הם קומוטטיביים, וכל האברים שלהם הפיכים. המרכז של כל חוג פשוט הוא שדה, ולכן אין זה פלא ששדות תופסים מקום מרכזי בתורת החוגים. יתרה מזו, מכיוון ששדות מיוחדים מופיעים באופן טבעי בשטחים אחרים של המתמטיקה, יש לתורת השדות חשיבות עצמאית. במבוא נתמקד באברים אלגבריים, ונראה שכל שדה מוכל בשדה סגור אלגברית. החלק העיקרי של הקורס מוקדש לתורת גלואה, החוקרת שדות באמצעות הרחבות סופיות. תורת גלואה, שפיתח (בעיקר) אווריסט גלואה בסביבות 1830, הולידה את תורת החבורות, ופתרה שתיים מקבוצות הבעיות המרכזיות במתמטיקה של אותה עת: הבעיות הגאומטריות של ימי קדם מחד, וההוכחה שלא ניתן לפתור את המשוואה הפולינומית ממעלה $n \geq 5$, מאידך. חוברת זו מציגה, לצד מבוא כללי לתורת השדות ויסודות התאוריה של גלואה, גם פתרון לשאלות אלו.

עוזי וישנה, 9.2013

תוכן עניינים

1 מבוא **7**

1.1 רקע מתורת החוגים . . . 7

1.1.1 חוגים ואידאלים . . . 7

1.1.2 שדות . . . 8

1.1.3 מושגי יסוד בתחומי שלמות . . . 8

1.1.4 חוג הפולינומים מעל שדה . . . 9

1.1.5 בניות של שדות . . . 9

1.1.6 אי־פריקות של פולינומים . . . 10

שורשים . . . 10

קריטריון אייזנשטיין . . . 11

הלמה של גאוס . . . 11

1.2 הרחבות של שדות . . . 12

1.2.1 שדה הוא חוג פשוט . . . 12

1.2.2 יוצרים של הרחבה . . . 13

1.2.3 פולינומים בשדה הרחבה . . . 13

1.2.4 הצבה והפולינום המינימלי . . . 14

1.2.5 ממד של הרחבות . . . 15

כפליות הממד . . . 15

הממד של הרחבה פשוטה . . . 16

1.2.6 שדה מפצל . . . 17

2 תורת גלואה **19**

2.1 שדות פיצול . . . 19

2.1.1 שיכונים . . . 19

2.2 ספרביליות . . . 21

2.2.1 מאפיין של שדה . . . 21

2.2.2 פולינומים ספרביליים . . . 22

2.2.3 שיכונים במקרה הספרבילי . . . 23

2.2.4 הרחבות ספרביליות . . . 24

תוכן עניינים

2.2.5 הרחבות אי־ספרביליות טהורות 25
2.3 חבורות גלואה 27
2.3.1 אוטומורפיזמים 27
2.3.2 חבורת גלואה 27
2.3.3 הסדר של חבורת גלואה 28
2.3.4 שדה השבת 28
2.3.5 התאמת גלואה 28
2.3.6 ממד וסדר 29
2.4 הרחבות גלואה 30
2.4.1 סדר וממד 31
2.5 המשפט היסודי 31
2.5.1 הלמה של ארטין 32
2.5.2 המשפט היסודי של תורת גלואה 33
2.5.3 בעיית ההיפוך 35
2.5.4 סגור גלואה 35
2.5.5 מספר שדות הביניים 36
2.5.6 הרכבה של שדות 36

3 שימושים 37
3.1 שורשי יחידה 37
3.1.1 החבורה הכפלית של שדה 37
3.1.2 הפולינומים הציקלוטומיים 38
3.1.3 השדה $\mathbb{Q}[\rho_n]$ 39
3.2 משוואות ממעלה שלישית ורביעית 40
3.2.1 משוואה ממעלה שלישית 41
פתרון בעזרת פונקציות סימטריות 41
3.2.2 הדיסקרימיננטה 43
3.2.3 משוואה ממעלה רביעית 44
הפתרון של פרארי 44
ניתוח הפתרון של פרארי 44
פתרון בעזרת סדרת ההרכב 46
3.3 פתירות על־ידי רדיקלים 48
3.3.1 הנורמה והעקבה 48
3.3.2 הרחבות רדיקליות 48
3.3.3 הרחבות ציקליות 49
3.3.4 חבורות פתירות 50
3.3.5 משפט גלואה על פתירות לפי רדיקלים 51
3.4 בניות במחוגה וסרגל והבעיות של ימי קדם 53
3.4.1 בניות במחוגה וסרגל 53
3.4.2 שדה המספרים הניתנים לבניה 54

3.4.3 שרשראות של הרחבות ריבועיות 55
3.4.4 בניית מצולעים משוכללים 56
3.4.5 הבעיות הגאומטריות של ימי קדם 57
3.4.6 אוריגמי 57
3.5 שדות סופיים 57

4 נושאים נוספים בתורת השדות 59
4.1 הרחבות אלגבריות 59
4.1.1 הרחבה נוצרת סופית 59
4.1.2 אלגבריות ויוצרים 60
4.1.3 סגור אלגברי יחסי 60
4.1.4 שדה סגור אלגברית 60
4.1.5 הסגור האלגברי של שדה 61
4.1.6 יחידות הסגור האלגברי 61
4.2 הרחבות טרנסצנדנטיות 62
4.2.1 פונקציות סימטריות 63
4.2.2 הרחבות מדרגה 1 63
4.3 נושאים נוספים 63

תוכן עניינים

פרק 1

מבוא

נכתבו ספרים רבים על תורת השדות בכלל ועל תורת גלואה בפרט. כמה אפשרויות מומלצות:

1. Lectures in Abstract Algebra III / Jacobson
2. Groups, Rings, Fields / Rowen
3. Algebra / Lang
4. Galois Theory / Tignol - דוגמאות מפורטות על משוואות ממעלה נמוכה.
5. Introduction to Galois Theory / Humphrys - נקודת מבט הסטורית.
6. Galois Theory / Cox

1.1 רקע מתורת החוגים

1.1.1 חוגים ואידאלים

מבנה אלגברי עם שתי פעולות (הנקראות חיבור וכפל) ושני קבועים (אפס ואחד) הוא **חוג**, אם הוא מהווה חבורה אבלית ביחס לחיבור, מונויד ביחס לכפל, ומתקיימת תכונת הדיסטריבוטיביות: $(x+y)z = xy+xy$, $x(y+z) = xy+xz$. בין הדוגמאות המוכרות: חוג השלמים, חוגי מטריצות וחוגי פולינומים. חוג הוא **קומוטטיבי** אם $xy = yx$ לכל x, y.

אידיאל של חוג R הוא קבוצת אברים $I \subseteq R$ הסגורה לחיבור וחיסור וסגורה לפעולת כפל 'מבחוץ', כלומר $xa, ax \in I$ לכל $a \in I$ ו־$x \in R$. במקרה כזה מסמנים $I \lhd R$. אידיאל הוא האנלוג לתת־חבורה נורמלית בתורת החבורות, בכך שאם $I \lhd R$ אז חבורת המנה R/I היא חוג ביחס לפעולת הכפל המושרית מ־R. לדוגמא, לכל n, $n\mathbb{Z} \lhd \mathbb{Z}$, וחוג המנה $\mathbb{Z}/n\mathbb{Z}$ הוא חוג המספרים מודולו n, עם פעולות החיבור והכפל

המודולריות. אידיאל שאינו שווה לחוג כולו נקרא אידיאל אמיתי. כל אידיאל אמיתי מוכל באידיאל אמיתי מקסימלי (טענה זו נובעת מן הלמה של צורן).

1.1.2 שדות

שדה הוא חוג קומוטטיבי שבו כל איבר $x \neq 0$ הוא הפיך. לדוגמא, $\mathbb{Q}$, $\mathbb{R}$ ו־$\mathbb{C}$ הם שדות. לעומת זאת $\mathbb{Z}$ אינו שדה. יש גם שדות סופיים, למשל $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, כאשר p מספר טבעי ראשוני.

גם תורת המודולים מעל שדות פשוטה בתכלית: כל מודול מעל שדה הוא חופשי, בעל דרגה מוגדרת היטב (הקרויה ממד); יש מרחב וקטורי יחיד, עד כדי איזומורפיזם, מכל ממד.

יהי K שדה. תת־קבוצה $F \subseteq K$ שהיא שדה בעצמה (ביחס לאותן פעולות) נקראת **תת־שדה**.

תרגיל 1.1.1 (*) תת־קבוצה $\emptyset \neq F \subseteq K$ היא תת־שדה אם היא סגורה לחיבור ונגדי, לכפל ולהפכי. תת־חוג $F \subseteq K$ הוא תת־שדה אם הוא סגור להפכי.

1.1.3 מושגי יסוד בתחומי שלמות

חוג קומוטטיבי שאין לו מחלקי אפס נקרא **תחום שלמות**. תחום שלמות שבו כל אידיאל הוא ראשי (כלומר נוצר על־ידי איבר אחד) נקרא **תחום ראשי**. אם מוגדרת על תחום שלמות R פונקציה $d\colon R \to \mathbb{N} \cup \{-\infty\}$ כך שלכל a ולכל $b \neq 0$ יש איבר $x \in a - Rb$ כך ש־$d(x) < d(b)$, אז R הוא **תחום אוקלידי**. כל תחום אוקלידי הוא תחום שלמות.

איבר p בתחום שלמות R הוא **אי־פריק** אם כל פירוק $p = ab$ הוא טריוויאלי (היינו אחד הגורמים הפיך). איבר p הוא **ראשוני** אם מ־$p \,|\, ab$ נובע ש־$p \,|\, a$ או $p \,|\, b$. כל איבר ראשוני הוא אי־פריק. בתחום ראשי, כל איבר אי־פריק הוא ראשוני, כך שהמושגים מתלכדים. בתחום ראשי, כל איבר אפשר לפרק למכפלה של ראשוניים באופן יחיד (היחידות היא עד־כדי החלפת סדר הגורמים, וכפל בהפיכים).

יהי R תחום ראשי. **המחלק המשותף המקסימלי** של $a, b \in R$ הוא אותו d (יחיד עד כדי כפל בהפיך) כך ש־$Ra + Rb = Rd$. הגדרה זו שקולה לכך ש־$d \,|\, a, b$ ו־$x \,|\, d$ לכל $x \,|\, a, b$. האברים a, b הם **זרים** אם $Ra + Rb = R$, אם ורק אם 1 הוא צירוף לינארי שלהם (מעל R), אם ורק אם כל מחלק משותף $x \,|\, a, b$ הוא הפיך. **משפט השאריות הסיני** קובע שאם a, b זרים, אז $R/Rab \cong R/Ra \times R/Rb$ (ובאופן כללי יותר, אם $a_1, \ldots, a_t$ זרים בזוגות, אז $R/Ra_1 \cdots a_t \cong R/Ra_1 \times \cdots \times R/Ra_t$).

אם R חוג קומוטטיבי ו־$M \lhd R$ אידיאל מקסימלי (כלומר, אין אידיאל $M' \lhd R$ כך ש־$M \subset M'$), אז חוג המנה R/M הוא שדה. בתחום ראשי, לכל איבר אי־פריק p, האידיאל Rp הוא מקסימלי, ולכן המנה R/Rp היא שדה.

1.1.4 חוג הפולינומים מעל שדה

יהי R חוג. החוג $R[\lambda] = \left\{\sum_{n=0}^{N} a_n\lambda^n :\ a_0,\dots,a_N \in R\right\}$, כאשר N אינו מוגבל, נקרא **חוג הפולינומים** במשתנה אחד מעל R. על הבניה הזו אפשר לחזור: במקום $(R[\lambda_1])[\lambda_2]$ כותבים $R[\lambda_1,\lambda_2]$, משום שסדר הוספת המשתנים אינו חשוב:

$$(R[\lambda_1])[\lambda_2] \cong (R[\lambda_2])[\lambda_1].$$

באופן כללי יותר מגדירים באינדוקציה $R[a_1,\dots,a_n] = (R[a_1,\dots,a_{n-1}])[a_n]$.

כאשר $R=F$ הוא שדה, החוג $F[\lambda]$ הוא חוג אוקלידי באמצעות פונקציית המעלה $d(\sum a_n\lambda^n) = \max_{a_n\neq 0} n$, ולכן הוא ראשי וחלות עליו כל התכונות הטובות שהוזכרו בתת־הסעיף הקודם.

בפרט, לכל פולינום $f\in F[\lambda]$ יש פירוק יחיד לגורמים אי־פריקים.

טענה 1.1.2 יהי $f\in F[\lambda]$, פולינום ממעלה n. חוג המנה $F[\lambda]/\langle f\rangle$ הוא מרחב וקטורי, עם הבסיס $\left\{x^i+\langle f\rangle :\ i=0,\dots,n-1\right\}$.

חוג המנה $F[\lambda]/\langle f\rangle$ הוא שדה אם ורק אם $\langle f\rangle = R[\lambda]f$ אידיאל מקסימלי, אם ורק אם f אי־פריק. אם $f=gh$ כאשר g,h זרים, אז לפי משפט השאריות הסיני $F[\lambda]/\langle f\rangle \cong F[\lambda]/\langle g\rangle \times F[\lambda]/\langle h\rangle$. לכן, אם נפרק $f = g_1^{n_1}\cdots g_t^{n_t}$, אז $F[\lambda]/\langle f\rangle \cong \prod F[\lambda]/\langle g_i^{n_i}\rangle$. חוג מהצורה $F[\lambda]/\langle g^n\rangle$ הוא חוג מקומי (שדה אם ורק אם $n=1$), ו(אם g אי־פריק), אינו ניתן לפירוק כמכפלה של חוגים.

1.1.5 בניות של שדות

להלן כמה בניות של שדות (נציג אחרות בהמשך).

1. חוגי מנה:

(א) לכל חוג קומוטטיבי R ולכל אידיאל מקסימלי M, R/M הוא שדה.

(ב) בפרט, יהי R תחום שלמות, ויהי $p\in R$ איבר אי־פריק. אז R/pR הוא שדה. למשל, $\mathbb{Z}/p\mathbb{Z}$ הוא שדה סופי בן p אברים.

(ג) בפרט, אם $f\in F[\lambda]$ הוא אי־פריק, אז $F[\lambda]/\langle f\rangle$ הוא שדה. נחזור לעסוק בבניה זו בהמשך (טענה 1.2.23).

2. שדה שברים:

(א) יהי R תחום שלמות. **שדה השברים** $\left\{\frac{a}{b} :\ a,b\in R, b\neq 0\right\}$, שבו השוויון מוגדר כך ש־$\frac{a}{b} = \frac{a'}{b'}$ אם $ab' = a'b$, הוא שדה ביחס לפעולות הטבעיות $\frac{a}{b}+\frac{a'}{b'} = \frac{ab'+a'b}{bb'}$ ו־$\frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}$. את שדה השברים של R מסמנים ב־$\mathrm{q}(R)$. למשל, שדה השברים של $\mathbb{Z}$ הוא $\mathbb{Q}$. שדה השברים של שדה F שווה (ליתר

דיוק, איזומורפי) לשדה עצמו. אם R תחום ראשי, כל שבר אפשר להציג בצורה $\frac{a}{b}$ כאשר a,b זרים.

כל תת־חוג של שדה הוא תחום שלמות, ובזכות הבניה של שדה שברים גם ההיפך נכון: כל תחום שלמות מוכל בשדה.

(ב) בפרט, אם F שדה, אז שדה השברים של $F[\lambda]$ נקרא **שדה הפונקציות הרציונליות** (במשתנה אחד) מעל F, ומסמנים אותו ב־$F(\lambda)$ (שימו לב לסוגריים העגולים במקרה זה, לעומת הסוגריים המרובעים במקרה של חוג הפולינומים.) אברי השדה $F(\lambda)$ הם השברים מהצורה $\frac{f(\lambda)}{g(\lambda)}$ כאשר f,g פולינומים ו־$g\neq 0$, עם הפעולות הטבעיות של שברים.

(ג) באופן כללי יותר, לכל מספר משתנים $\lambda_1,\dots,\lambda_n$, שדה השברים של חוג הפולינומים $F[\lambda_1,\dots,\lambda_n]$ נקרא **שדה הפונקציות הרציונליות ב־n משתנים**, ומסמנים אותו ב־$F(\lambda_1,\dots,\lambda_n)$.

3. יהי F שדה. אוסף הטורים הפורמליים $\sum_{n=-N}^{\infty}a_n\lambda^n$, שבו $a_n\in F$, הטורים מתחילים בנקודה כלשהי (ועשויים להיות אינסופיים), נקרא **השדה של טורי לורן** מעל F, ומסמנים אותו ב־$F((\lambda))$. זהו אכן שדה, המכיל את שדה הפונקציות $F(\lambda)$.

תרגיל 1.1.3 (*) לכל הומומורפיזם של חוגים $F\hookrightarrow K$, יש **המשכה** להומומורפיזם $F(\lambda)\hookrightarrow K(\lambda)$ (המשכה היא הומומורפיזם מ־$F(\lambda)$ המתלכד עם ההומומורפיזם הנתון על F).

1.1.6 אי־פריקות של פולינומים

יהי F שדה. כפי שראינו, המנה $F[\lambda]/\langle p\rangle$ היא שדה אם ורק אם p פולינום אי־פריק (מעל F). נדון באי־פריקות של פולינומים משלוש זוויות (שיטה רביעית, של הפולינום המינימלי, מוצגת במסקנה 1.2.13).

שורשים

פולינום ממעלה ראשונה הוא לעולם אי־פריק, ולכן נדון כאן רק בפולינומים ממעלה גבוהה יותר. איבר $a\in F$ הוא **שורש** של הפולינום $f\in F[\lambda]$ אם $f(a)=0$ (וראה תת־סעיף 1.2.4).

תרגיל 1.1.4 (*) a הוא שורש של $f\in F[\lambda]$ אם ורק אם $\lambda-a$ מחלק את $f(\lambda)$.
הדרכה. חילוק עם שארית: כתוב $f(\lambda)=q(\lambda)(\lambda-a))+r(\lambda)$ כאשר $\deg(r)<\deg(\lambda-a)=1$.

לכן, פולינום (ממעלה >1) עם שורש הוא פריק. מאידך,

תרגיל 1.1.5 (*) אם פולינום ממעלה 2 או 3 פריק, אז יש לו שורש.

אם כך, פולינום ממעלה נמוכה הוא פריק אם ורק אם יש לו שורש. טענה זו אינה נכונה במעלות מ־4 ומעלה:

תרגיל 1.1.6 (*) תן דוגמא לפולינום פריק מעל $\mathbb{Q}$, ממעלה 4, שאין לו שם שורשים.

איך מראים שלפולינום אין שורשים? נניח ש־R תחום ראשי, $F = \mathrm{q}(R)$ ו־$f = a_n\lambda^n + \cdots + a_0 \in R[\lambda]$ (כל פולינום מעל F אפשר להביא לצורה כזו על־ידי כפל בסקלר).

תרגיל 1.1.7 (*) אם **שבר מצומצם** $\frac{c}{d} \in F$ (כלומר c, d זרים) הוא שורש של f, אז $d \,|\, a_n$ ו־$c \,|\, a_0$. בפרט, אם הפולינום **מתוקן** (כלומר המקדם המוביל שלו הוא 1), אז כל שורש שלו ב־F נמצא למעשה ב־R.

לתרגיל 1.1.4 יש מסקנה חשובה אחרת.

תרגיל 1.1.8 (*) לכל $a \neq a'$, הפולינומים $\lambda - a$, $\lambda - a'$ זרים זה לזה.

מסקנה 1.1.9 מספר השורשים של פולינום $f \neq 0$ מעל שדה כלשהו, אינו עולה על המעלה שלו.

קריטריון אייזנשטיין

יהי R תחום שלמות. נניח ש־$p \in R$ ראשוני. פולינום $a_n\lambda^n + \cdot + a_0 \in R[\lambda]$ נקרא **פולינום אייזנשטיין** אם מתקיימים התנאים הבאים: $p \nmid a_n$, $p \,|\, a_{n-1}, \dots, a_0$, $p^2 \nmid a_0$.

טענה 1.1.10 פולינום אייזנשטיין הוא אי־פריק מעל R.

התרגיל הבא מאפשר לעבור מפולינום שאינו מקיים את הקריטריון, לכזה שכן מקיים אותו:

תרגיל 1.1.11 (*) אם $f(x)$ פריק מעל R אז לכל $a, b \in R$, $a \neq 0$, גם $f(ax+b)$ פריק.

תרגיל 1.1.12 (**) הראה ש־$x^6 + x^3 + 1$ אי־פריק מעל $\mathbb{Z}$. **הדרכה.** מצא הצבה שאחריה הפולינום יקיים את התנאי עבור $p = 3$.

הלמה של גאוס

טענה 1.1.10 מציגה מקרה שבו פולינום הוא אי־פריק מעל חוג R. אלא שאנחנו מעוניינים באי־פריקות מעל שדה (למשל שדה השברים של R), ואי־פריקות מעל R אינה מועילה:

תרגיל 1.1.13 (**) נניח ש־$R \subseteq R_1$ הם תחומי שלמות, $f \in R[\lambda]$. אם f אי־פריק מעל R_1 אז הוא גם אי־פריק מעל R, אבל ההיפך אינו בהכרח נכון.

בפרט,

תרגיל 1.1.14 (**) נניח ש־R תחום שלמות, $F = \mathrm{q}(R)$, $f \in R[\lambda]$. אם f אי־פריק מעל F אז הוא גם אי־פריק מעל R, אבל ההיפך אינו בהכרח נכון.

הלמה הבאה מספקת פתרון לבעיה הזו.

טענה 1.1.15 (הלמה של גאוס) יהי R תחום ראשי. אם $f \in R[\lambda]$ אי־פריק מעל R, אז f אי־פריק גם מעל F.

1.2 הרחבות של שדות

זוג שדות $F \subseteq K$ נקרא **הרחבה** של שדות; במקרה זה K נקרא הרחבה של F. הדגש הוא על כך שהשדה K מרחיב את השדה F, וכולל כביכול פתרונות למשוואות שאי־אפשר לפתור ב־F. הרחבה כזו מסמנים גם ב־K/F (אין לזה שום קשר עם הסימון הזהה של חוג מנה). שדות המקיימים $F \subseteq L \subseteq K$ נקראים **שדות ביניים** של ההרחבה K/F.

1.2.1 שדה הוא חוג פשוט

חוג פשוט הוא חוג שאין לו אידיאלים פרט ל־0.

תרגיל 1.2.1 (*) חוג קומוטטיבי הוא פשוט אם ורק אם הוא שדה.

לעובדה זו יש מסקנה חשובה:

תרגיל 1.2.2 (*) כל הומומורפיזם (של חוגים עם יחידה) $F \to A$, כאשר F שדה, הוא **שיכון** (כלומר הומומורפיזם חד־חד־ערכי).

בפרט, כל הומומורפיזם בין שדות הוא שיכון, כלומר הוא מגדיר הרחבה של השדה הקטן לתוך השדה הגדול. כל הכלה $F \subseteq K$ מגדירה שיכון באופן טבעי. במקרים רבים אפשר לשכן את אותו השדה בשדה גדול בכמה דרכים.

תרגיל 1.2.3 (**) 1. אם $\mathbb{Q} \subseteq K$, אז יש שיכון יחיד $\mathbb{Q} \hookrightarrow K$ (והוא השיכון הטבעי).

2. מצא שני שיכונים שונים של $\mathbb{Q}[\sqrt{2}]$ ב־$\mathbb{R}$.

3. הראה שאין אף שיכון של $\mathbb{Q}[\sqrt{-2}]$ לתוך $\mathbb{R}$.

1.2.2 יוצרים של הרחבה

הערה 1.2.4 יהיו $F \subseteq E$ שדות, ויהי Λ אוסף של שדותביניים. אז החיתוך $\bigcap_{L\in\Lambda} L$ הוא שדה.

יהיו $F \subseteq K$ שדות עם קבוצת איברים $S \subseteq K$. חיתוך תת־השדות של K הכוללים את S הוא תת־השדה הנוצר על־ידי S, ומסמנים אותו ב־$F(S)$. זהו השדה הקטן ביותר הכולל את F ואת S. אוסף המנות של פולינומים באיברים של S הוא שדה, השווה לפיכך ל־$F(S)$.

בפרט, אפשר לבחור $S = \{a\}$ ולקבל את השדה $F(a)$. הרחבה כזו, באיבר אחד, נקראת **הרחבה פשוטה**.

הערה 1.2.5 אם Λ קבוצת שדות סדורה ליניארית, אז $\bigcup_{F\in\Lambda} F$ שדה.

1.2.3 פולינומים בשדה הרחבה

תהי $F \subseteq K$ הרחבה של שדות. חוג הפולינומים $F[\lambda]$ מוכל ב־$K[\lambda]$, ולכן כל פולינום מעל F הוא גם פולינום מעל K. יש אברים ב־$F[\lambda]$ שהתכונות שלהם עשויות להשתנות כשעוברים לחוג הגדול יותר.

לדוגמא, פולינום $f \in F[\lambda]$ עשוי להיות אי־פריק מעל F ולהתפרק מעל שדה הרחבה K של F. למשל, x^4+1 אי־פריק מעל $\mathbb{Q}$, אבל מתפרק מעל $\mathbb{Q}[\sqrt{2}]$ למכפלה

$$(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1).$$

מכיוון שהפירוק מעל K הוא יחיד, הפירוק של f לגורמים איפריקים מעל F מעודן ב־K: כל גורם אי־פריק מעל K מחלק (מעל K) גורם אי־פריק מעל F.

טענה 1.2.6 נניח ש־ $F \subseteq K$ שדות, ו־ $f,g \in F[\lambda]$.

1. המחלק המשותף המקסימלי של f,g כפולינומים מעל F שווה למחלק המשותף המקסימלי שלהם כפולינומים מעל K.
2. בפרט:
   (א) אם פולינומים $f,g \in F[\lambda]$ הם זרים מעל F, אז הם זרים גם מעל K.
   (ב) אם $f,g \in F[\lambda]$ ו־$f \,|\, g$ מעל K, אז $f \,|\, g$ גם מעל F.

הוכחה. יהי d_F המחלק המשותף המקסימלי מעל F, ויהי d_K המחלק המשותף המקסימלי מעל K. מחד, $d_F \,|\, d_K$ לפי ההגדרה של d_K, משום ש־d_F מחלק את f,g בחוג $K[\lambda]$. מאידך, $d_F = af+bg$ עבור $a,b \in F[\lambda]$, ולכן $d_K \,|\, d_F$ מעל K. מכאן שעד כדי כפל בסקלר, $d_K = d_F$.

הטענה השניה נובעת מהראשונה משום ש־f,g זרים אם ורק אם המחלקה משותף המקסימלי שלהם הוא 1, ו־$f \,|\, g$ אם ורק אם המחלק המשותף המקסימלי הוא f. □

לסיכום, המושג 'פולינום אי־פריק' תלוי בשדה שמעליו בוחנים את הפולינום; שדה יכול להיות אי־פריק מעל שדה אחד, ופריק מעל שדה גדול יותר. אבל המושגים 'פולינומים זרים' ו־'מחלק' אינם תלויים בשדה הבסיס.

תרגיל 1.2.7 (**) לכל הרחבה K/F, $F(\lambda)\cap K[\lambda] = F[\lambda]$; ראה טענה 1.2.6. **הערה.** פורמלית כדי שלחיתוך תהיה משמעות יש לחשוב על $F(\lambda)$ ועל $K[\lambda]$ כעל תת־קבוצות של $K(\lambda)$.

1.2.4 הצבה והפולינום המינימלי

תהי A **אלגברה** מעל F (היינו, חוג A שהמרכז שלו מכיל את F). אז לכל $a \in A$, **הומומורפיזם ההצבה** $F[\lambda]\to A$ הוא ההומומורפיזם המוגדר לפי

$$\Phi_a : f(\lambda) \mapsto f(a).$$

אם הגרעין של Φ_a הוא אפס, אומרים ש־a **טרנסצנדנטי.** פירושו של דבר הוא שלא קיים פולינום המאפס את a (פרט כמובן לפולינום האפס).

תרגיל 1.2.8 (*) אם a טרנסצנדנטי, $F[a]$ איזומורפי לחוג הפולינומים.

אם הגרעין $\mathrm{Ker}(\Phi_a)\lhd F[\lambda]$ אינו אפס, אז a **אלגברי.** במקרה זה יש יוצר f_a של $\mathrm{Ker}(\Phi_a)$ (יחיד עד כדי כפל בסקלר), שהוא **הפולינום המינימלי של** a. לפי משפט האיזומורפיזם הראשון,

$$F[\lambda]/\langle f_a\rangle \cong \mathrm{Im}(\Phi_a) = F[a]. \qquad (1.1)$$

למינימליות יש משמעות כפולה, ולמרבה הנוחות שתיהן מתלכדות:

טענה 1.2.9 הפולינום המתוקן הוא בעל מעלה מינימלית בקבוצת הפולינומים המאפסים את a, והוא מחלק כל פולינום אחר המאפס את a (ולכן הוא גם המינימום לגבי יחס החלוקה).

מסקנה 1.2.10 יהי $a \in A$ איבר אלגברי מעל F, עם פולינום מינימלי f_a. אז

$$\dim(F[a]) = \deg(f_a).$$

הוכחה. $F[\lambda]/\langle f_a\rangle \cong \mathrm{Im}\Phi_a = F[a]$ היא תת־אלגברה של A, והממד מתקבל מטענה 1.1.2. □

טענה 1.2.11 אם A תחום שלמות, אז הפולינום המינימלי f_a אי־פריק, ואז $F[a]$ שדה.

הוכחה. אם $f_a = f_1 f_2$ אז מ־$0 = (f_1 f_2)(a) = f_1(a) f_2(a)$ נובע $f_1(a) = 0$ או $f_2(a) = 0$, בסתירה למינימליות של המעלה. ומכיוון ש־$F[\lambda]$ תחום ראשי, האידיאל שאיבר אי־פריק יוצר הוא מקסימלי. $\square$

החידוש בטענה זו הוא שכאשר a אלגברי, לכל פולינום ב־a (אם אינו מתחלק בפולינום המינימלי) יש פולינום אחר ב־a כך שמכפלתם היא 1. להלן הוכחה חישובית לעובדה שימושית זו:

תרגיל 1.2.12 **(**)** נניח ש־f_a, פולינום אי־פריק מעל F, הוא הפולינום המינימלי של a. אם $g(a) \neq 0$ אז $g(\lambda)$ זר ל־$f_a(\lambda)$, ולכן קיימים $\alpha(\lambda), \beta(\lambda) \in F[\lambda]$ כך ש־$\alpha(\lambda) f_a(\lambda) + \beta(\lambda) g(\lambda) = 1$. הראה ש־$g(a)^{-1} = \beta(a)$.

הטענה האחרונה היא הקריטריון הנוסף לאי־פריקות שהבטחנו בתת־סעיף 1.1.6:

מסקנה 1.2.13 תהי K/F הרחבה של שדות, ויהי $a \in K$. אז הפולינום המינימלי של a מעל F הוא אי־פריק (מעל F).

(מיידי מטענה 1.2.11 משום ש־K הוא תחום שלמות.)

כעת נניח ש־A שדה. נסמן ב־$F(a)$ את תת־השדה הנוצר על־ידי a.

הערה 1.2.14 כאשר a אלגברי, $F[a] = \mathrm{Im}\Phi_a$ הוא שדה כפי שראינו (הערה 1.2.11), ולכן $F(a) = F[a]$.

תרגיל 1.2.15 **(*)** אם a טרנסצנדנטי, אז $F(a)$ איזומורפי לשדה פונקציות רציונליות $F(\lambda)$.

1.2.5 ממד של הרחבות

נסמן את הממד של מרחב וקטורי V מעל שדה K ב־$\dim_K V$.

את K/F הרחבה של שדות, אז K הוא מרחב וקטורי מעל F (עם הכפל בסקלר המושרה מכפל ב־K), ולכן יש ממד, שאותו נסמן ב־$[K:F] = \dim_F K$. הממד הוא אינווריאנט חשוב ביותר בתורת השדות.

כפליות הממד

טענה 1.2.16 יהי V מרחב וקטורי מעל שדה K, כאשר $F \subseteq K$ תת־שדה. אז

$$\dim_F V = [K:F] \dim_K V.$$

מסקנה 1.2.17 בפרט בשרשרת הרחבות $F \subseteq K \subseteq E$,

$$[E:F] = [E:K] \cdot [K:F].$$

הממד של הרחבה פשוטה

כפי שראינו, הממד $[F[a]:F]$ שווה לדרגת הפולינום המינימלי של a מעל F.

טענה 1.2.18 תהי $F \subseteq L$ הרחבה של שדות, ויהי $a \in E$ איבר בשדה $L \subseteq E$. אז

$$[L[a]:L] \leq [F[a]:F].$$

הוכחה. הפולינום המינימלי של a מעל L מחלק (מעל L) את הפולינום המינימלי של אותו איבר מעל F. □

דוגמא 1.2.19 בטענה 1.2.18 יכול להיות אי־שוויון אמיתי: קח $F = \mathbb{Q}$, $L = F[\rho\alpha]$, $a = \alpha$ כאשר $\alpha^3 = 2$ ו־ $\rho = \frac{-1+\sqrt{-3}}{2}$. אז $[F[a]:F] = 3$ > $2 = [L[a]:L]$.

תרגיל 1.2.20 (**) אם $F \subseteq L \subseteq E$ ו־$a \in E$, ומתקיים $[L[a]:L] = [F[a]:F] - 1$, אז יש שיכון $L \hookrightarrow F[a]$ **הדרכה**. הפולינום המינימלי של a מעל F מתפצל מעל L לגורמים $(\lambda - a')g(\lambda)$.

מסקנה 1.2.21 בטענה 1.2.18 קח $L = F[b]$, אז $[F[a,b]:F] \leq [F[a]:F][F[b]:F]$. באינדוקציה נובע מזה כי

$$[F[a_1,\dots,a_n]:F] \leq \prod [F[a_i]:F]. \tag{1.2}$$

הערה 1.2.22 אי־השוויון במסקנה 1.2.18 הפוך מן הטענה האנלוגית לחבורות, שם לכל $H_1, H_2 \leq G$ מתקיים

$$[G:H_1 \cap H_2] \geq [H_1:H_1 \cap H_2] \cdot [H_2:H_1 \cap H_2],$$

ובפרט לכל חבורה G, תת־חבורה H ואברים $a,b \in G$,

$$[\langle H,a,b\rangle:H] \geq [\langle H,a\rangle:H] \cdot [\langle H,b\rangle:H].$$

1.2.6 שדה מפצל

טענה 1.2.23 נניח ש־$f \in F[\lambda]$ פולינום אי־פריק. אז בשדה $F[\lambda]/\langle f\rangle$ יש ל־f שורש.

הוכחה. הראה באמצעות חישוב ישיר ש־$\lambda + \langle f\rangle$ הוא שורש של f. □

טענה 1.2.24 עבור כל פולינום f מעל שדה F, יש הרחבה K של F שבה יש שורש של f.

הוכחה. יהי g גורם אי־פריק של f, אז $F[\lambda]/\langle g\rangle$ הוא שדה שיש בו שורש ל־g, ולכן ל־f. □

הגדרה 1.2.25 יהי $f \in F[\lambda]$ פולינום מתוקן. הפולינום f **מתפצל** ב־F אם קיימים $\alpha_1, \dots, \alpha_n \in F$ כך ש־ $f(\lambda) = \prod(\lambda - \alpha_i)$. במקרה זה אומרים ש־$F$ **מפצל** את f.

הרחבה E/F שבה הפולינום מתפצל נקראת **שדה מפצל** של f. עלינו להכליל מושג זה עבור שיכונים: כל שיכון $\phi\colon F \to E$ משרה שיכון של חוגי הפולינומים $\phi\colon F[\lambda] \to E[\lambda]$, לפי הנוסחה $\phi(a_n\lambda^n + \dots + a_0) = \phi(a_n)\lambda^n + \dots + \phi(a_0)$. נאמר שהשיכון מפצל את $f \in F[\lambda]$ אם $\phi(f)$ מתפצל ב־E.

מטענה 1.2.24 נובע באינדוקציה:

מסקנה 1.2.26 לכל פולינום f מעל שדה יש שדה מפצל, שממדו אינו עולה על $(\deg f)!$.

הוכחה. נסמן $n = \deg(f)$. יהי a שורש של גורם אי־פריק g של f; ניקח $F_1 = F[\lambda]/\langle g\rangle$. מעל F_1 אפשר לכתוב $f(\lambda) = (\lambda - a)f_1(\lambda)$. לפי הנחת האינדוקציה יש שדה מפצל E של f_1 מעל F_1, כך ש־$[E\colon F_1] \leq (n-1)!$. כמובן, E מפצל את f, ומתקיים $[E\colon F] = [E\colon F_1][F_1\colon F] \leq (n-1)!\deg(g) \leq n!$. □

פרק 2

תורת גלואה

2.1 שדות פיצול

יהי $f \in F[\lambda]$. הרחבה K/F היא **שדה פיצול** של f, אם K שדה מפצל מינימלי של f. כלומר, K מפצל את f, אז אף שדה ביניים $F \subseteq K' \subset K$ אינו מפצל. מה מסביר תופעה כזו? מעל השדה K אפשר לפצל את הפולינום לגורמים לינאריים $f(\lambda) = \prod(\lambda - \alpha_i)$, ואז הפולינום מתפצל מעל תת־שדה $F \subseteq K' \subset K$ אם ורק אם $\alpha_1, \dots, \alpha_n \in K'$. מכאן שאם E שדה המפצל את f, כלומר $f(\lambda) = \prod(\lambda - \alpha_i)$ עם $\alpha_i \in E$, אז E מכיל תת־שדה שהוא שדה פיצול, $K = F[\alpha_1, \dots, \alpha_n]$. לפי ההוכחה של מסקנה 1.2.26, זוהי הרחבה שהממד שלה $[K:F] \le n!$.

הערה 2.1.1 אם $F \subseteq L \subseteq K$ ו־ K שדה פיצול של $f \in F[\lambda]$ מעל F, אז K שדה פיצול גם מעל L, עם אותם יוצרים.

2.1.1 שיכונים

כפי שכבר ציינו, מנקודת המבט של תורת החוגים, שדה הוא חוג קומוטטיבי פשוט. אחת התוצאות היא:

מסקנה 2.1.2 כל הומומורפיזם של שדות הוא שיכון.

יהיו F, L, E שדות כך ש־ $F \subseteq L$, ויהי $\phi : F \hookrightarrow E$ שיכון. שיכון $\overline{\phi} : L \hookrightarrow E$ נקרא **המשכה** של ϕ, אם הצמצום של $\overline{\phi}$ ל־F שווה ל־ϕ. אפשר לשרטט מצב זה בדיאגרמה (ראו להלן). אומרים שהדיאגרמה **קומוטטיבית** אם לכל איבר בנקודת המוצא F, התמונה ביעד E שווה בשתי הדרכים; כלומר, אם $\overline{\phi}(a) = \phi(a)$ לכל $a \in F$. הדיאגרמה

קומוטטיבית אם ורק אם $\overline{\phi}$ הוא המשכה של ϕ:

$$\begin{array}{ccc} L & \xrightarrow{\overline{\phi}} & E \\ \uparrow & & \| \\ F & \xrightarrow{\phi} & E \end{array}$$

הגדרה 2.1.3 *אם L/F הרחבה של שדות ו־ $F \hookrightarrow E$ שיכון, נסמן ב־ $n^L_{F\hookrightarrow E}$ את מספר ההמשכות של השיכון לשיכון $L \hookrightarrow E$.*

תרגיל 2.1.4 (**) יהי F_0 תת־השדה הראשוני של F (כלומר F הוא השדה $\mathbb{Q}$ או אחד השדות $\mathbb{Z}/p\mathbb{Z}$). הראה שיש שיכון יחיד $F_0 \hookrightarrow F$.

תרגיל 2.1.5 (*) אם F, K חולקים אותו שדה ראשוני F_0, הראה ש־ $n^F_{F_0\subseteq K}$ הוא מספר השיכונים של F ב־K.

דוגמא 2.1.6 $\mathbb{Q}[i]$ משוכן ב־ $\mathbb{C}$ בשתי דרכים, כלומר $n^{\mathbb{Q}[i]}_{\mathbb{Q}\subseteq\mathbb{C}} = 2$.

למה 2.1.7 יהי $\varphi\colon F \hookrightarrow E$ שיכון. תהי $F_1 = F[a]$ הרחבה פשוטה, ויהי $f \in F[\lambda]$ הפולינום המינימלי של a. אז $n^{F_1}_{F\hookrightarrow E}$ שווה למספר השורשים של $\varphi(f)$ ב־E. בפרט:

1. מתקיים $n^{F_1}_{F\hookrightarrow E} \le [F_1\colon F]$.
2. יש המשכה של φ ל־ $F_1 \to E$ אם ורק אם ל־$\varphi(f)$ יש לפחות שורש אחד ב־E.

נאמר שפולינום g המתפצל בשדה E הוא **ספרבילי** שם, אם בפירוק שלו לגורמים אין אף גורם כפול (מהצורה $(\lambda-\alpha)^2$). בצורה פחות מדוייקת מקובל לומר ש'כל השורשים של f ב־E שונים זה מזה' (בהמשך נראה שתכונה זו אינה תלויה ב־E כלל).

משפט 2.1.8 *יהי $\varphi\colon F \hookrightarrow E$ שיכון.*

1. *לכל הרחבה סופית K/F,*
$$n^K_{F\hookrightarrow E} \le [K\colon F].$$

2. *אם K נוצר מעל F על־ידי שורשים של פולינום f שתמונתו $\varphi(f)$ מתפצלת ב־E, אז*
   - *(א) יש הרחבה $K \hookrightarrow E$ של φ.*
   - *(ב) אם $\varphi(f)$ ספרבילי ב־E אז $n^K_{F\hookrightarrow E} = [K\colon F]$.*

הוכחה. עבור 1, כתוב $K = F[a_1, \dots, a_n]$. נוכיח את הטענה באינדוקציה על n. נסמן $F_1 = F[a_1]$. לפי למה 2.1.7 יש $n^{F_1}_{F \hookrightarrow E} \leq [F_1 : F]$ המשכות של השיכון אל $\varphi_1 : F_1 \to E$. לפי הנחת האינדוקציה, לכל אחת מאלה יש $n^K_{F_1 \hookrightarrow E} \leq [K : F_1]$ המשכות ל־$K \to E$, ואם נסכם על כל ההמשכות הראשונות נקבל בסך־הכל

$$n^K_{F \hookrightarrow E} = \sum_{\varphi_1} n^K_{\varphi_1 : F_1 \to E} \leq \sum_{\varphi_1} [K : F_1] \leq [F_1 : F][K : F_1] = [K : F] \tag{2.1}$$

המשכות אל K.

את 2 נוכיח באותו אופן, אלא שהפעם נניח ש־$a_1, \dots, a_n$ כולם שורשים של f ב־K. שוב ניקח $F_1 = F[a_1]$. לפי למה 2.1.7 $1 \leq n^{F_1}_{F \hookrightarrow E}$ כי יש ב־E שורשים ל־$\varphi(f)$, והשוויון $n^{F_1}_{F \hookrightarrow E} = [F_1 : F]$ מתקיים אם $\varphi(f_1)$ ספרבילי ב־E, כאשר $f_1 \mid f$ הוא הפולינום המינימלי של a_1. אם $n = 1$, זה נובע מהספרביליות של $\varphi(f)$.

כעת, f הוא פולינום מעל F_1, K שדה נוצר על־ידי אותם שורשים מעל F_1, ולכל שיכון $\varphi' : F_1 \to E$, E מפצל את $\varphi'(f) = \varphi(f)$. לפי הנחת האינדוקציה, ראשית, כל שיכון $F_1 \hookrightarrow E$ אפשר להמשיך לשיכון $K \hookrightarrow E$, ושנית, אם $\varphi(f)$ ספרבילי ב־E אז מתקיים שוויון $n^K_{F_1 \hookrightarrow E} = [K : F_1]$. לכן, אם גם $\varphi(f)$ וגם $\varphi(f_1)$ ספרביליים ב־E יש שוויון $n^K_{F \hookrightarrow F} = [K : F]$; אבל כאשר $\varphi(f)$ ספרבילי גם $\varphi(f_1)$ ספרבילי. □

משפט 2.1.9 *לכל פולינום מעל שדה F יש שדה פיצול יחיד עד־כדי איזומורפיזם.*

הוכחה. יהיו K, K' שדות פיצול. לפי משפט 2.1.8.2(א) יש שיכון $K \hookrightarrow K'$, שהוא על כי K' מפצל מינימלי. □

מעתה אפשר לדבר על **שדה הפיצול** של פולינום (מעל שדה נתון), בהא הידיעה. שדה הפיצול אכן תלוי בשדה הבסיס: למשל, שדה הפיצול של $\lambda^2 + 1 \in \mathbb{Q}[\lambda]$ מעל $\mathbb{Q}$ הוא $\mathbb{Q}[i]$, אבל שדה הפיצול של אותו פולינום מעל $\mathbb{R}$ הוא $\mathbb{C}$.

מסקנה 2.1.10 יהיו $F \subseteq F_1 \subseteq K$ שדות, ו־$F \hookrightarrow E$ שיכון.
אם $n^K_{F \to E} = [K : F]$, אז $n^{F_1}_{F \to E} = [F_1 : F]$, ולכל שיכון $\phi : F_1 \to E$ הממשיך את השיכון הנתון $F \hookrightarrow E$, $n^K_{\phi : F_1 \to E} = [K : F_1] \geq 1$.

הוכחה. באי־השוויון (2.1) שווים זה לזה אגף שמאל ואגף ימין, ומכאן שיש שוויון בכל שלב בדרך.□

2.2 ספרביליות

2.2.1 מאפיין של שדה

המאפיין של השדה F הוא הסדר של 1 בחבורה החיבורית של השדה, או 0 אם הסדר הוא אינסופי. את המאפיין של F מסמנים ב־$\text{char}F$. מאפיין חיובי של שדה הוא תמיד מספר ראשוני. תת־השדה הנוצר על־ידי 1 נקרא **תת־השדה הראשוני** של F. תת־השדה הראשוני תלוי רק במאפיין, והוא שווה ל־$\mathbb{Q}$ במאפיין אפס, או לשדה $\mathbb{Z}/p\mathbb{Z}$ במאפיין p. מכאן שכל שדה מכיל עותק של $\mathbb{Q}$ או של איזשהו $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

תרגיל 2.2.1 (*) בכל הרחבה K/F, לשני השדות אותו מאפיין.

הערה 2.2.2 אם F שדה ממאפיין p, אז $(a+b)^p = a^p + b^p$ לכל $a,b \in F$. לכן הפונקציה $x \mapsto x^p$ היא שיכון (!) של שדות $F \to F$. את התמונה של השיכון הזה מסמנים $F^p = \{a^p : a \in F\}$; זהו תת־שדה של F, שהוא איזומורפי ל־F.

תרגיל 2.2.3 (*) תן דוגמא לשדה F ממאפיין p כך ש־$F^p \neq F$.

הגדרה 2.2.4 ***שדה הוא מושלם אם המאפיין שלו אפס, או שהמאפיין $p > 0$ ומתקיים $F^p = F$.***

2.2.2 פולינומים ספרביליים

הגדרה 2.2.5 פולינום $f \in F[\lambda]$ הוא **ספרבילי** (מעל F) אם כל שורשיו בשדה הפיצול שלו מעל F שונים זה מזה.

הערה 2.2.6 נניח ש־ $f = f_1 \cdots f_t$ פירוק לגורמים אי־פריקים (מתוקנים) מעל F. אז f ספרבילי אם ורק אם כל ה־f_i שונים וספרביליים. (משום שבשדה הפיצול של f, לגורמים אי־פריקים שונים אין שורשים משותפים).

לדוגמא, $(x^2+1)^2$ אינו ספרבילי.

הערה 2.2.7 $Jacobson$ קורא לפולינום ספרבילי, אם כל גורם אי־פריק שלו הוא ספרבילי. לפי הגדרה זו, $(x^2+1)^2$ דווקא כן ספרבילי מעל $\mathbb{Q}$. ההגדרה שלנו נמצאת למשל בספרו של $Lang$, והיא מקובלת יותר.

מסקנה 2.2.8 אם $f \in F[\lambda]$ ספרבילי ו־$g \mid f$ מעל F, אז גם g ספרבילי.

על חוג הפולינומים $F[\lambda]$ מגדירים נגזרת פורמלית לפי החוק $(\sum a_i \lambda^i)' = \sum a_i i \lambda^{i-1}$.

תרגיל 2.2.9 (*) הוכח את **כלל לייבניץ** $(fg)' = fg' + f'g$.

טענה 2.2.10 הפולינום $f \in F[\lambda]$ ספרבילי אם ורק אם $(f, f') = 1$.

הוכחה. לפי טענה 1.2.6 אפשר לחשב את המחלק המשותף המקסימלי בשדה הפיצול K. אם f אינו ספרבילי אז אפשר לכתוב $f(\lambda) = (\lambda - a)^2 g(\lambda)$ לאיזשהו $a \in K$, ואז $f'(\lambda) = 2(\lambda - a) g(\lambda) + (\lambda - a)^2 g'(\lambda)$ אינו זר ל־$f(\lambda)$ משום ששניהם מתחלקים ב־$(\lambda - a)$. מאידך, נניח שהפולינום ספרבילי. נכתוב $f(\lambda) = \prod (\lambda - a_i)$ עבור $a_i \in K$ השונים זה מזה, אז לפי כלל לייבניץ

$$f'(\lambda) = \sum_{i=1}^{n} (\lambda - a_1) \cdots (\lambda - a_{i-1})(\lambda - a_{i+1}) \cdots (\lambda - a_n),$$

ולכן לכל j, $f'(a_j) = \prod_{i \neq j} (a_j - a_i) \neq 0$, כלומר אף a_j אינו שורש של $f'(\lambda)$; אבל $a_1, \dots, a_n$ הם השורשים היחידים של $f(\lambda)$, ומכאן שהפולינומים זרים. □

תרגיל 2.2.11 **(**)** הפולינום $\lambda^5+\lambda^2+1 \in F[\lambda]$ ספרבילי אם ורק אם $\mathrm{char}F \neq 53, 61$.

טענה 2.2.12 יהי $g \in F[\lambda]$ פולינום אי־פריק. אז התנאים הבאים שקולים:

1. g אינו ספרבילי.
2. $g' = 0$.
3. $p = \mathrm{char}F > 0$ ויש פולינום g_1 כך ש־$g(\lambda) = g_1(\lambda^p)$.

הוכחה. (2) $\Leftrightarrow$ (1): מכיוון ש־g אי־פריק, $g = (g, g')$ אם ורק אם $(g, g') \neq 1$ אם ורק אם g אינו ספרבילי. אבל $g = (g, g') \,|\, g'$ אינו אפשרי ל־$g' \neq 0$ בגלל המעלה, ומתקיים אם $g = 0$.

(3) $\Leftrightarrow$ (2): נכתוב $g(\lambda) = \sum a_i \lambda^i$. אם $0 = g' = \sum i a_i \lambda^{i-1}$, אז $n a_n = 0$ כאשר $n = \deg(g)$, כך ש־$n = 0$ בשדה. לכן המאפיין הוא ראשוני כלשהו, p, ולא אפס. בנוסף לזה, $i a_i = 0$ בשדה לכל i, ולכן $a_i = 0$ לכל i זר ל־p. כלומר, $g(\lambda) = g_1(\lambda^p) = \sum a_i (\lambda^p)^{i/p}$ כאשר $g_1(\lambda) = \sum a_i \lambda^{i/p}$. מאידך אם $g(\lambda) = g_1(\lambda^p)$ אז $g'(\lambda) = (\lambda^p)' g_1'(\lambda^p) = p\lambda^{p-1} g_1'(\lambda^p) = 0$ לפי הכלל לנגזרת פנימית (או לפי בדיקה ישירה). □

ספרביליות אינה תלויה בשדה:

מסקנה 2.2.13 יהיו $F \subseteq K$ שדות, ויהי $f \in F[\lambda]$. אז f ספרבילי כפולינום מעל F אם ורק אם הוא ספרבילי כפולינום מעל K.

הוכחה. לפי טענה 2.2.12 הספרביליות תלויה רק בנגזרת, שאינה תלויה בשדה. □

הערה 2.2.14 בהמשך לטענה 2.2.12, אם $g \in F[\lambda]$ אי־פריק ולא ספרבילי, ו־$g(\lambda) = g_1(\lambda^p)$, אז g_1 אי־פריק ו־$\deg(g) = p\deg(g_1)$.

2.2.3 שיכונים במקרה הספרבילי

בהמשך ללמה 2.1.7:

למה 2.2.15 יהי $F \hookrightarrow E$ שיכון ותהי $F_1 = F[a]$ הרחבה פשוטה של F; אז $n_{F\hookrightarrow E}^{F_1} = [F_1 : F]$ אם ורק אם f ספרבילי ומתפצל ב־E.

באותו אופן, לפי משפט 2.1.8.2:

משפט 2.2.16 *יהיו f פולינום מעל F, K שדה פיצול של f מעל F, ו־ E שדה מפצל. אז $n_{F\subseteq E}^{K} = [K : F]$ אם ורק אם f ספרבילי.*

2.2.4 הרחבות ספרביליות

הגדרה 2.2.17 *איבר של הרחבה K/F הוא **איבר ספרבילי** אם הפולינום המינימלי שלו ספרבילי. ההרחבה נקראת **הרחבה ספרבילית** אם כל האיברים שלה ספרביליים.*

תרגיל 2.2.18 (*) בכל הרחבה K/F, כל $a \in F$ הוא ספרבילי. **הדרכה**. הפולינום המינימלי שלו הוא $\lambda - a$, שהוא פולינום ספרבילי.

תרגיל 2.2.19 (*) כל הרחבה של שדות במאפיין אפס היא ספרבילית. **הדרכה**. לפי טענה 2.2.12 כל פולינום אי־פריק במאפיין אפס הוא ספרבילי.

טענה 2.2.20 יהיו $F \subseteq K \subseteq E$ שדות, ויהי $a \in E$. אם a ספרבילי מעל F, אז הוא ספרבילי מעל K.

הוכחה. הפולינום המינימלי g של a מעל K מחלק (מעל K) את הפולינום המינימלי של a מעל F, שאותו נסמן ב־f. לפי מסקנה 2.2.13 f ספרבילי מעל K, ולפי מסקנה 2.2.8 גם g ספרבילי. □

להלן דוגמא טיפוסית להרחבה לא ספרבילית.

טענה 2.2.21 יהיו $F \subseteq E$ שדות ממאפיין p, ויהי $a \in E$. נניח ש־$a^p \in F$ ו־$a \notin F$. אז

1. הפולינום המינימלי של a מעל F הוא $\lambda^p - a^p$.
2. a אינו ספרבילי מעל F.

הוכחה. ברור ש־a הוא שורש של $f(\lambda) = \lambda^p - a^p$. יהי $g(\lambda)$ הפולינום המינימלי של a מעל F. אז $g \,|\, f$ מעל F, ולכן גם מעל E, אלא ששם $f(\lambda) = (\lambda - a)^p$, ולכן $g(\lambda) = (\lambda - a)^k$ לאיזשהו $k \leq p$. מאידך $g(\lambda) \in F[\lambda]$, ולכן המקדם החופשי שלו $a^k \in F$; אם $k < p$ נובע מכאן $a \in F$, בסתירה להנחה. אבל $f' = 0$, ומכאן ש־f לא ספרבילי. □

טענה 2.2.22 תהי K/F הרחבה של שדות ממאפיין p, ויהי $a \in K$. אז a ספרבילי אם ורק אם $F[a^p] = F[a]$.

הוכחה. יהי g הפולינום המינימלי של a מעל F. אם האיבר a אינו ספרבילי אז g אינו ספרבילי, וקיים g_1 כך ש־$g(\lambda) = g_1(\lambda^p)$; במקרה זה $\dim(F[a^p]) = \deg(g_1) < \deg(g) = \dim(F[a])$ לפי מסקנה 1.2.10, ולכן $F[a^p] \subset F[a]$. מצד שני, אם $F[a^p] \subset F[a]$, אז a אינו ספרבילי מעל $F[a^p]$ לפי טענה 2.2.12, ולכן אינו ספרבילי גם מעל F לפי טענה 2.2.20. □

משפט 2.2.23 *תהי K/F הרחבת שדות סופית ממאפיין p. אז K/F ספרבילית אם ורק אם $FK^p = K$ (כאשר FK^p הוא תת־השדה הקטן ביותר של K המכיל את K^p).*

הוכחה. אם K/F ספרבילית, אז לכל $a \in K$ מתקיים $a \in F[a] = F[a^p] \subseteq FK^p$ לפי טענה 2.2.22 ולכן $K = FK^p$.

מצד שני, נניח ש־$K = FK^p$, ויהי $a \in K$ איבר לא ספרבילי מעל F; עלינו להגיע לסתירה. לפי טענה 2.2.22, $F[a^p] \subset F[a]$, ולכן a אינו ספרבילי מעל $F[a^p]$, ובנוסף $K = F[a^p]K^p \subseteq FK^p$. נחליף, אם כך, את F ב־$F[a^p]$, וכך נוכל להניח ש־$a^p \in F$. נשלים את $\{a\}$ לבסיס $a_1, \dots, a_n$ של ההרחבה, עם $a_1 = a$, כך ש־$K = \sum Fa_i$. נגדיר העתקה לינארית $P\colon K \to K$, כמרחבים לינאריים מעל F, לפי $P(a_i) = a_i^p$. מכיוון ש־$\sum Fa_i^p = F\sum F^p a_i^p = F(\sum Fa_i)^p = FK^p = K$ לפי ההנחה, P על, ולכן גם חד־חד־ערכי. אבל $P(a - a^p) = P(a) - P(a^p) = a^p - a^p = 0$ לפי ההגדרה, ולכן $a = a^p \in F$, בסתירה להנחה. □

מסקנה 2.2.24 יהיו $F \subseteq K \subseteq E$ שדות. אם ההרחבות E/K ו־K/F ספרביליות, אז גם E/F ספרבילית.

הוכחה. לפי משפט 2.2.23, $E = KE^p$ ו־$K = FK^p$, ומספיק לחשב $FE^p = F(KE^p)^p = FK^pE^{p^2} = KK^pE^{p^2} = K(KE^p)^p = KE^p = E$. □

משפט 2.2.25 *הרחבה K/F הנוצרת על־ידי איברים ספרביליים היא ספרבילית.*

הוכחה. ראשית, נניח ש־K נוצר על־ידי איבר אחד, כלומר $K = F[a]$ כאשר $a \in K$ ספרבילי מעל F. אז $FK^p = F[a^p] = F[a] = K$ לפי טענה 2.2.22, ו־K/F ספרבילית לפי משפט 2.2.23.

שנית, נניח ש־K נוצר סופית, כלומר $K = F[a_1, \dots, a_n]$ כאשר a_i ספרביליים מעל F. נסמן $K_i = F[a_1, \dots, a_i]$. לפי טענה 2.2.20, כל a_i ספרבילי מעל K_{i-1}, ולפי החלק הראשון K_i ספרבילי מעל K_{i-1}. אינדוקציה על־פי מסקנה 2.2.24 מראה ש־K/F ספרבילית.

וכעת תהי K/F הרחבה הנוצרת על־ידי הקבוצה כלשהי S שכל אבריה (אלגבריים ו)ספרביליים מעל F. יהי $a \in K$, אז קיימת תת־קבוצה סופית $S_0 \subseteq S$ כך ש־$a \in F(S_0) = F[S_0]$, ו־$F[S_0]$ ספרבילי לפי החלק הקודם של המשפט; לכן גם a ספרבילי. □

2.2.5 הרחבות אי־ספרביליות טהורות

הרחבה K/F היא **אי־ספרבילית טהורה** אם כל איבר $a \in K$ שאינו ב־F הוא לא ספרבילי.

הערה 2.2.26 אם K/F אי־ספרבילית טהורה ו־$F \subseteq L \subseteq K$, אז גם K/L וגם L/F אי־ספרביליות טהורות.

דוגמא 2.2.27 יהי F שדה, ויהי $a \in F$ כך ש־$a \notin F^p$. אז $F[\sqrt[p]{a}]$ הוא הרחבה אי־ספרבילית טהורה של F.

טענה 2.2.28 הממד של הרחבה אי־ספרבילית טהורה (ממד סופי) הוא חזקה של p.

הוכחה. **באינדוקציה על הממד. יהי $a \in K$ איבר שאינו ב־F. לפי טענה 2.2.22, $F[a^p] \subset F[a]$, ולפי טענה 2.2.21, $p = [F[a]:F[a^p]]$. לפי הנחת האינדוקציה $[F[a^p]:F]$ ו־$[K:F[a]]$ הם חזקות־p, וסיימנו כי $[K:F] = [K:F[a]] \cdot [F[a]:F[a^p]] \cdot [F[a^p]:F]$.** □

מסקנה 2.2.29 תהי K/F הרחבה כלשהי של שדות.

1. האוסף K_{sep} של אברי K שהם ספרביליים מעל F, הוא שדה.
2. $F \subseteq K_{sep} \subseteq K$.
3. ההרחבה K_{sep}/F ספרבילית מקסימלית;
4. ההרחבה K/K_{sep} אי־ספרבילית טהורה.

הוכחה. **1. יהיו $a, b \in K_{sep}$, $a \neq 0$; לפי משפט 2.2.25, כל איבר של $F[a,b]$ הוא ספרבילי, ובפרט $-a, a+b, a^{-1}, ab$ ספרביליים.**

2. כל איבר של F הוא ספרבילי (תרגיל 2.2.18).

3. כל איבר ספרבילי ב־K שייך ל־K_{sep}.

4. אם $a \in K$ ספרבילי מעל K_{sep} אז ההרחבה $K_{sep}[a]/K_{sep}$ ספרבילית לפי משפט 2.2.25, ואז $K_{sep}[a]/F$ ספרבילית לפי הטרנזיטיביות ו־a ספרבילי מעל F כאיבר בהרחבה ספרבילית; אבל אז $a \in K_{sep}$.

□

אם כך, בכל הרחבה K/F יש תת־הרחבה ספרבילית מקסימלית K_{sep} (הנקראת גם **הסגור הספרבילי היחסי של F בתוך K**); K אי־ספרבילי טהור מעל תת־השדה הזה. כך אפשר לפרק כל הרחבה לצעד ספרבילי ואחריו צעד איספרבילי.

האם אפשר להפוך את הסדר, ולבצע ראשית הרחבה אי־ספרבילית ואחר־כך הרחבה ספרבילית? הדוגמא הבאה מראה שזה בלתי אפשרי.

דוגמא 2.2.30 יהי k שדה מושלם ממאפיין 2, וניקח $F = k(\lambda, \mu)$ ו־

$$K = F[x \mid x^4 = \lambda x^2 + \mu].$$

הסגור הספרבילי של F בתוך K הוא $F[x^2]$, ו־$K/F[x^2]$ אי־ספרבילי. מאידך, אין ב־K אף איבר אי־ספרבילי מעל F (לפי חישוב ישיר: אין אף איבר מחוץ ל־F שריבועו ב־F).

2.3 חבורות גלואה

2.3.1 אוטומורפיזמים

אוטומורפיזם של הרחבת שדות K/F הוא אוטומורפיזם $K \to K$ המקבע את כל אברי F. כל אנדומורפיזם $K \to K$ הוא אוטומורפיזם מעל תת־השדה הראשוני של K, אבל אוטומורפיזמים של הרחבה מאפשרים ללמוד את המבנה של K מעל F, ולא כשדה בעלמא.

הערה 2.3.1 נניח ש־$K = F(S)$; אז כל אוטומורפיזם של ההרחבה K/F נקבע לפי התמונות של אברי S.

בפרט, אם $K = F[a]$, אז אוטומורפיזם $\sigma : K \to K$ נקבע לפי הערך $\sigma(a)$.

לטענה הקלה הבאה תפקיד מרכזי בקשר בין פולינומים לאוטומורפיזמים:

טענה 2.3.2 יהי $\sigma : K \to K$ אוטומורפיזם מעל F. לכל שורש $a \in K$ של פולינום $f \in F[\lambda]$, גם $\sigma(a)$ הוא שורש (משום ש־$f(\sigma(a)) = \sigma(f(a)) = 0$).

יש להבחין שלא כל פונקציה המעבירה כל יוצר של K/F לשורש אחר של אותו פולינום מינימלי אפשר להמשיך לאוטומורפיזם.

2.3.2 חבורת גלואה

הגדרה 2.3.3 *תהי K/F הרחבה של שדות. **חבורת גלואה** של ההרחבה היא החבורה $\mathrm{Gal}(K/F)$ של כל האוטומורפיזמים $K \to K$ השומרים את אברי F.*

תרגיל 2.3.4 (**) חשב את חבורות גלואה של ההרחבות $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}[\rho_3]/\mathbb{Q}$. תאר את האוטומורפיזמים של $\mathbb{Q}[2^{1/3}, \rho_3]/\mathbb{Q}$ ושל $\mathbb{Q}[2^{1/3}, \rho_3]/\mathbb{Q}[\rho_3]$.

דוגמא 2.3.5 חבורת גלואה $\mathrm{Gal}(\mathbb{Q}[2^{1/3}]/\mathbb{Q})$ היא טריוויאלית.

הערה 2.3.6 נניח ש־$K = F[\alpha_1, \ldots, \alpha_n]$ כאשר α_i הם שורשי פולינום מעל f. אז כל אוטומורפיזם משרה תמורה על השורשים, ומוגדר לפיה. כלומר, יש שיכון

$$\mathrm{Gal}(K/F) \hookrightarrow S_n.$$

בהערה 2.3.6 אין צורך להניח ש־f אי־פריק. אם $f = f_1 \cdots f_t$, כמו במקרה $f = (x^2 - 2)(x^2 - 3)$, מתקבלת הצגה לתוך המכפלה $\prod S_{\deg f_i}$.

2.3.3 הסדר של חבורת גלואה

הערה 2.3.7 כאשר $[K:F]$ סופי, כל שיכון $K \to K$ השומר על F שומר על הממד, ולכן הוא אוטומורפיזם. (בממד אינסופי הטענה אינה נכונה, כפי שמראה דוגמא 3.5.1).

טענה 2.3.8 תהי K/F הרחבה סופית. הסדר של חבורת גלואה $\mathrm{Gal}(K/F)$ הוא, לפי הערה 2.3.7, מספר השיכונים $|\mathrm{Gal}(K/F)| = n_{F\subseteq K}^{K}$.

לפי למה 2.1.7, אם $F_1 = F[a]$, אז $|\mathrm{Gal}(F_1/F)|$ שווה למספר השורשים של הפולינום המינימלי f ב־F_1.
לפי משפט 2.1.8.1:

משפט 2.3.9 *לכל הרחבה סופית K/F,* $|\mathrm{Gal}(K/F)| \leq [K:F]$.

במשפט 2.2.16, ניקח $E = K$:

משפט 2.3.10 *יהי K שדה פיצול של פולינום ספרבילי מעל F. אז* $[K:F] = |\mathrm{Gal}(K/F)|$.

2.3.4 שדה השבת

יהי K שדה. לכל תת־שדה $F \subseteq K$ מתאימה חבורת אוטומורפיזמים $\mathrm{Gal}(K/F)$.
בכיוון ההפוך, לכל חבורת אוטומורפיזמים G מתאים תת־שדה

$$K^G = \{a \in K:\ (\forall \sigma \in G)\sigma(a) = a\},$$

הנקרא **שדה השבת** של G.

הערה 2.3.11 אם $K \subseteq L \subseteq F$ אז $\mathrm{Gal}(K/L) \leq \mathrm{Gal}(K/F)$. ואם $G \subseteq H$ אז $K^G \subseteq K^H$.

הערה 2.3.12 לכל $F \subseteq K$ מתקיים $F \subseteq K^{\mathrm{Gal}(K/F)}$ (כי אברי F קבועים תחת כל אוטומורפיזם של K/F), ולכל חבורת אוטומורפיזמים G של K, $G \subseteq \mathrm{Gal}(K/K^G)$ (כי כל אוטומורפיזם ב־G שומר על כל אברי K^G).

2.3.5 התאמת גלואה

נטפל בהתאמה של חבורה לשדה ושדה לחבורה באופן פורמלי.
נסמן ב־$\mathcal{F}$ את סריג תת־השדות של K, וב־ $\mathcal{G}$ את סריג תת־החבורות של $\mathrm{Aut}(K)$, ונגדיר העתקות

$$\circ : \mathcal{F} \longrightarrow \mathcal{G}$$
$$\mathcal{F} \longleftarrow \mathcal{G} : *$$

לפי $L^\circ = \mathrm{Gal}(K/L)$ ו־ $H^* = K^H$.

הערה 2.3.13 תכונות מיידיות של ההעתקות הללו:

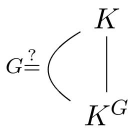
1. שתי ההעתקות הופכות סדר הכלה (זו הערה 2.3.11).
2. תמיד $L \subseteq L^{\circ *}$ ו־$H \subseteq H^{*\circ}$ (זו הערה 2.3.12).

ומזה נובע:

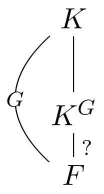
3. $L^{\circ * \circ} = L^{\circ}$ ו־ $H^{*\circ *} = H^{*}$.
4. $H^{*\circ} = H$ אם ורק אם $H = L^{\circ}$ לשדה כלשהו L; בדומה, $L^{\circ *} = L$ אם ורק אם $L = H^{*}$ לחבורה כלשהי H.

אם לנסח את 2 ו־4 על־פי הסימונים הקאנוניים:

הערה 2.3.14 1. תהי G חבורת אוטומורפיזמים של K. אז $G \subseteq \mathrm{Gal}(K/K^G)$, עם שוויון אם ורק אם G חבורה גלואה של הרחבה כלשהי. (לפי מסקנה 2.5.4, תמיד $\mathrm{Gal}(K/K^G) = G$).



2. תהי K/F הרחבה. אז $F \subseteq K^{\mathrm{Gal}(K/F)}$, עם שוויון אם ורק אם F הוא שדה שבת של חבורה כלשהי. (ראה מסקנה 2.3.16: F שדה שבת אם ורק אם K/F 'הרחבת גלואה').



2.3.6 ממד וסדר

להתאמת גלואה שהוצגה בסעיף הקודם נוסיף את מרכיב הגודל: לחבורות אוטומורפיזמים סופיות יש סדר, $|H|$; לתת־שדות יש ממד, $[K:F]$. מכיוון שלא יהיה חשש לבלבול, נסמן $|F| = [K:F]$. לגדלים אלה יש תכונה שימושית: אם $H \subseteq G$ (חבורות סופיות) אז $|H| \leq |G|$, ומ־$|H| = |G|$ נובע $H = G$. באופן דואלי, בשדות: אם $F \subseteq L \subseteq K$ (הרחבות מקו־ממד סופי) אז $|L| \leq |F|$ ומ־ $|L| = |F|$ נובע $F = L$.

כעת אפשר לקרוא את משפט 2.3.9: לכל $F \subseteq K$ (סופי),

$$|F^{\circ}| \leq |F|. \tag{2.2}$$

בכך נוצר חוסר סימטריה מסויים, משום שאיננו יודעים טענה דואלית על חבורות אוטומורפיזמים.

משפט 2.3.10 מצביע על תכונה המיוחדת למקרה ש־K/F שדה פיצול של פולינום ספרבילי. נבחין שאם K/F כזה ו־ $F \subseteq L$, אז K הוא שדה פיצול של אותו פולינום ספרבילי גם מעל L. לכן נקרא לתת־שדה כזה 'תת־שדה גדול', ונבחין שתת־שדה המכיל תת־שדה גדול הוא גדול בעצמו. משפט 2.3.10 קובע שלכל F גדול, $|F| = |F^\circ|$.

טענה 2.3.15 אם F גדול, אז $F^{\circ *} = F$.

הוכחה. לפי ההנחה $|F| = |F^\circ|$; אבל $F \subseteq F^{\circ *}$, כלומר גם $F^{\circ *}$ גדול, ולכן $|F^{\circ * \circ}| = |F^{\circ *}|$. כעת $|F^{\circ *}| = |F^{\circ * \circ}| = |F^\circ| = |F|$ לפי הערה 2.3.13.3, מש"ל. □

בלשון קונוונציונלית,

מסקנה 2.3.16 אם K/F שדה פיצול של פולינום ספרבילי, אז $F = K^{\mathrm{Gal}(K/F)}$.

2.4 הרחבות גלואה

הגדרה 2.4.1 הרחבה E/F היא נורמלית אם הפולינום המינימלי מעל F של כל $a \in E$, מתפצל ב־E.

הרחבה נורמלית וספרבילית נקראת **הרחבת גלואה**.

הערה 2.4.2 אם K/F גלואה ו־ $F \subseteq L \subseteq K$, אז גם K/L גלואה.

משפט 2.4.3 *תהי K/F הרחבה סופית. התנאים הבאים שקולים:*

1. *K/F הרחבת גלואה.*
2. *K הוא שדה פיצול של פולינום ספרבילי מעל F (כלומר: F גדול).*
3. *$F = K^G$ עבור חבורת אוטומורפיזמים מתאימה של K.*

הוכחה. (1) ⇐ (2): תהי S קבוצת יוצרים (סופית) של K/F. לכל $a \in S$ יהי f_a הפולינום המינימלי מעל F. לפי ההנחות $f = \prod f_a$ ספרבילי ומתפצל מעל K. אבל K שדה הפיצול של f.
(2) ⇐ (3): מסקנה 2.3.16.
(3) ⇐ (1): יהי $a \in K$. צריך להוכיח שהפולינום המינימלי f של a מעל F הוא ספרבילי ומתפצל ב־K. יהיו $a = a_1, \dots, a_n$ השורשים השונים של f ב־K, ויהי $g(\lambda) = \prod(\lambda - a_i)$. ברור ש־ $g \,|\, f$ מעל K. אבל G פועלת על קבוצת השורשים ומתקיים $\sigma(g) = g$ לכל $\sigma \in G$. לכן $g \in F[\lambda]$, וכיוון ש־f אי־פריק, $f = g$. לכן f ספרבילי ומתפצל ב־K. □

נוסיף עוד שתי תכונות שקולות:

טענה 2.4.4 התכונות (1), (2), (3) שקולות גם לבאות:

4. $F = K^{\mathrm{Gal}(K/F)}$ (היינו $F = F^{\circ *}$).

5. $|\mathrm{Gal}(K/F)| = [K:F]$ (או $|F^{\circ}| = |F|$).

הוכחה. את (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) הוכחנו במשפט 2.4.3. השקילות (3) $\Leftrightarrow$ (4) היא הערה 2.3.14.2. הגרירה (2) $\Leftarrow$ (5) היא משפט 2.3.10.

נוכיח (5) $\Leftarrow$ (4). נניח $|F| = |F^{\circ}|$. מכיוון ש־ $F^{\circ *}$ הוא שדה שבת, זהו שדה גדול, ולכן הוא מקיים את תכונה (5): $|F^{\circ *}| = |F^{\circ * \circ}|$. אבל $F^{\circ} = F^{\circ * \circ}$ ולכן $|F^{\circ *}| = |F^{\circ * \circ}| = |F^{\circ}| = |F|$, ו־ $F = F^{\circ *} = K^{\mathrm{Gal}(K/F)}$ הוא שדה שבת. □

2.4.1 סדר וממד

נסכם את התכונות הידועות עד כאן על הסדר והממד.

טענה 2.4.5 לכל תת־שדה F ולכל חבורת אוטומורפיזמים G מתקיים

$$|G| \leq |G^{*}| = |G^{* \circ}|;$$
$$|F^{\circ}| = |F^{\circ *}| \leq |F|.$$

הוכחה. לפי טענה 2.4.4, $F = F^{\circ *}$ אם ורק אם $|F^{\circ}| = |F|$. עבור $F = G^{*}$ הטענה הראשונה מתקיימת, ולכן תמיד $|G^{* \circ}| = |G^{*}|$, אבל $G \subseteq G^{* \circ}$, וזה מוכיח את השורה הראשונה. אם נציב $G = F^{\circ}$ נקבל בשוויון הימני $|F^{\circ *}| = |F^{\circ}|$ כי $F^{\circ} = F^{\circ * \circ}$, והרי $|F^{\circ *}| \geq |F|$ כי $F \subseteq F^{\circ *}$. □

קיבלנו את (2.2) כמסקנה.

את אי־השוויון $|F| \leq |F^{\circ}|$ אי־אפשר להחליף בשוויון. ראינו בדוגמא 2.3.5 שיתכן $|F| = 3 < 1 = |F^{\circ}|$. זה גם מראה שיתכן $F^{\circ} = L^{\circ}$ בלי $F = L$; בדוגמא לעיל $F^{\circ} = K^{\circ} = 1$.

את אי־השוויון על חבורות נחליף בשוויון בפרק הבא.

2.5 המשפט היסודי

לפי הידוע לנו עד כה, אם G חבורת אוטומורפיזמים של K, אז יתכן ש־$G \subset G_1 =$ $\mathrm{Gal}(K/K^{G})$, כלומר יש ל־K/K^{G} יותר אוטומורפיזמים משהגדירו את שדה השבת. כאן $G_1 = G^{* \circ}$, והרי לשתי החבורות יש אותו שדה שבת $G^{*} = G_1^{*}$. לכן ה'תקלה' בהכלה $G \subset G_1$ משמעה גם ששדה השבת אינו מגדיר היטב את החבורה שהגדירה אותו. הלמה של ארטין מראה שכל הבעיות האלה אינן מתרחשות.

2.5.1 הלמה של ארטין

את התוצאה $|G| \le [K:K^G]$ (טענה 2.4.5) אפשר להוכיח ישירות באמצעות למה שיש לה גם שימושים אחרים. תהי G חבורה של אוטומורפיזמים של K, ונסמן $F = K^G$. כל אוטומורפיזם הוא איבר של $\mathrm{End}_F(K) \cong \mathrm{M}_n(F)$ כאשר $n = [K:F]$. זהו מרחב וקטורי מעל K, על־ידי הפעולה $(k\varphi)(x) = k\varphi(x)$. ככזה, הממד שלו הוא כמובן n.

למה 2.5.1 האיברים של $G \subset \mathrm{End}_F(K)$ בלתי־תלויים ליניארית מעל K. בפרט $|G| \le [K:F]$.

הוכחה. נניח שיש צירוף ליניארי $\sum k_i\sigma_i = 0$ שבו לא כל המקדמים אפס. נבחר צירוף כזה עם מספר קטן ביותר של מונומים. על־ידי הרכבה מימין אפשר להניח ש־ $\sigma_1 = 1$. לפי ההנחה $\sum k_i\sigma_i(x) = 0$ לכל $x \in K$. קח $t \in K$ שאינו נשמר תחת σ_2. על־ידי הצבת tx במקום x מקבלים $\sum k_i\sigma_i(t)\sigma_i(x) = 0$, אבל גם $\sum k_i\sigma_1(t)\sigma_i(x) = 0$. אם נחסר נקבל יחס קצר יותר, בסתירה. □

נימוק דומה למדי, מעט יותר מורכב, מוכיח גם את הכיוון ההפוך. נפתח בהערה כללית.

הערה 2.5.2 תהי $G \subseteq \mathrm{Gal}(K/F)$ חבורה של אוטומורפיזמים. תהי $\forall j : \sum_i a_{ij}x_i = 0$ מערכת משוואות מעל K בנעלמים x_i, שהיא אינווריאנטית להפעלת G: לכל משוואה $\sigma \in G$ ולכל j, המשוואה $\sum \sigma(a_{ij})x_i = 0$ נובעת מן המערכת. אז גם מרחב הפתרונות אינווריאנטי להפעלת G, כלומר אם $(x_1,\dots,x_m)$ פתרון, אז לכל $\sigma \in G$ גם $(\sigma(x_1),\dots,\sigma(x_m))$ פתרון. אכן, נניח ש־$\sum a_{ij}x_i = 0$ לכל j, אז לכל $\sigma \in G$ ולכל j, $\sum a_{ij}\sigma(x_i) = \sigma(\sum \sigma^{-1}(a_{ij})x_i) = 0$.

למה 2.5.3 (הלמה של ארטין) תהי G חבורת אוטומורפיזמים של שדה כלשהו K. אז $[K:K^G] \le |G|$.

הוכחה. נכתוב $G = \{\sigma_1 = 1,\dots,\sigma_n\}$. צריך להוכיח שאם $m > n$ אז כל m איברים $a_1,\dots,a_m \in K$ הם תלויים ליניארית מעל $F_1 = K^G$.

במערכת המשוואות $\sum_j \sigma_i(a_j)x_j = 0$ יש m נעלמים ו־n משוואות, ולכן יש לה פתרון שונה מאפס $x_1,\dots,x_m \in K$. נתבונן בפתרון כזה שבו מספר ה־$x_j \neq 0$ מינימלי. על־ידי סידור מחדש של ה־a_j, אפשר להניח $x_1 \neq 0$. נחלק את הפתרון ב־x_1, ונקבל פתרון שבו $x_1 = 1$. לפי הערה 2.5.2, גם הווקטור $(\sigma(x_1),\dots,\sigma(x_m))$ פתרון. אבל $\sigma(x_1) = x_1$, ולכן חיסור שני הפתרונות יתן פתרון עם מספר קטן יותר של גורמים שונים מאפס, בסתירה, אלא אם $\sigma(x_j) = x_j$ לכל j. מכיוון שזה נכון לכל σ, $x_1,\dots,x_m \in K^G$, ועבור $i = 1$ מתקבלת התלות הליניארית $\sum x_ja_j = 0$. □

הוכחנו $|G| \le |G^*|$. מטענה 2.4.5 מקבלים כעת $|G^{*\circ}| = |G^*| = |G|$; אבל $G \subseteq G^{*\circ}$, ולכן $G^{*\circ} = G$.

מסקנה 2.5.4 לכל חבורת אוטומורפיזמים G של שדה K,

$$\mathrm{Gal}(K/K^G) = G$$

ו־

$$[K:K^G] = |G|.$$

2.5.2 המשפט היסודי של תורת גלואה

תהי K/F הרחבת גלואה עם $G = \mathrm{Gal}(K/F)$. ההעתקות $L^\circ = \mathrm{Gal}(K/L)$ ו־ $H^* = K^H$ מעבירות תת־חבורות של G (הסריג $\mathcal{G}$) להרחבות ביניים של F (הסריג $\mathcal{F}$), ולהיפך.

משפט 2.5.5 *ההעתקות* $\circ : L \mapsto \mathrm{Gal}(K/L)$ ו־ $* : H \mapsto K^H$ *הן אנטי־איזומורפיזמים הפוכים זה לזה של הסריגים $\mathcal{G}$ ו־$\mathcal{F}$. בנוסף לזה:* $|H| = [K:K^H]$ ו־$[K:L] = |\mathrm{Gal}(K/L)|$.

הוכחה. אלו אנטי־הומומורפיזמים של הסריגים לפי הערה 2.3.13.(1).
לפי הערה 2.4.2, K גלואה מעל כל הרחבת ביניים $F \subseteq L \subseteq K$, ולפי מסקנה 2.4.4 נובע מכאן $L = L^{\circ *}$. לפי מסקנה 2.5.4, $H = H^{*\circ}$. לכן ההעתקות הופכות זו את זו, ומכאן שהן אנטי־איזומורפיזמים. השוויון $|H| = |H^*|$ נובע ממסקנה 2.5.4, אבל כל שדה ביניים הוא מהצורה H^* ולכן גם $|L| = |L^\circ|$. □

בפרט:

מסקנה 2.5.6

$$\langle H_1, H_2\rangle^* = H_1^* \cap H_2^*, \qquad (H_1 \cap H_2)^* = H_1^* H_2^*;$$

$$(L_1 \cap L_2)^\circ = \langle L_1^\circ, L_2^\circ\rangle, \qquad (L_1 L_2)^\circ = L_1^\circ \cap L_2^\circ.$$

$$K^{\langle H_1, H_2\rangle} = K^{H_1} \cap K^{H_2}, \qquad K^{(H_1 \cap H_2)} = K^{H_1} K^{H_2};$$

$$\mathrm{Gal}(K/L_1 \cap L_2) = \langle \mathrm{Gal}(K/L_1), \mathrm{Gal}(K/L_2)\rangle,$$

$$\mathrm{Gal}(K/L_1 L_2) = \mathrm{Gal}(K/L_1) \cap \mathrm{Gal}(K/L_2).$$

נשאלת השאלה אלו הרחבות ביניים של K/F הן גלואה מעל F (הרי K הרחבת גלואה של כל שדה ביניים לפי הערה 2.4.2).

משפט 2.5.7 *תהי K/F הרחבת גלואה עם $\mathrm{Gal}(K/F) = G$. אז E^H/F הרחבה נורמלית אם ורק אם $H \trianglelefteq G$, ובמקרה זה $\mathrm{Gal}(E^H/F) \cong G/H$.*

הוכחה. מחישוב,

$$\begin{aligned} K^{\tau H \tau^{-1}} &= \{a \in K:\ (\forall \sigma \in H)\tau\sigma\tau^{-1}(a) = a\} \\ &= \{\tau(b):\ b \in K,\ (\forall \sigma \in H)\tau\sigma(b) = \tau(b)\} \\ &= \tau(\{b \in K:\ (\forall \sigma \in H)\sigma(b) = b\} \\ &= \tau(K^H). \end{aligned}$$

נסמן $L = K^H$. נניח ש־L הרחבה נורמלית של F. יהי $a \in L$, אז לכל $\tau \in G$ $\tau(a)$ שורש של הפולינום המינימלי של a מעל F, ולכן $\tau(a) \in L$. מכאן ש־$K^{\tau H \tau^{-1}} = \tau(L) = L = K^H$. מכאן ש־ $\tau H \tau^{-1} = H$ לכל $\tau \in G$, ולכן $H \trianglelefteq G$.

כעת נניח ש־$H \trianglelefteq G$. לפי החישוב, $\tau(L) = L$ לכל $\tau \in G$, ולכן הצמצום של איברי G ל־L מגדיר הומומורפיזם $\theta\colon \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$. קל לבדוק ש־$L^{\theta(G)} \subseteq K^G = F$, ולכן θ על. אבל $\mathrm{Ker}(\theta) = \{\tau \in G:\ \tau|_L = 1\} = \mathrm{Gal}(L/F)$, ולכן $\mathrm{Gal}(L/F) \cong G/\mathrm{Ker}(\theta) = \mathrm{Gal}(K/F)/\mathrm{Gal}(L/F)$. מכאן ש־ $|\mathrm{Gal}(L/F)| = [L\colon F] = \frac{[K:F]}{[K:L]} = [G\colon \mathrm{Gal}(K/L)]$, ולפי טענה 2.4.4 פירושו של דבר הוא ש־L/F גלואה. □

המשפט היסודי קובע ש־$[K\colon F] = \mathrm{Gal}(K/F) = n^K_{F\subseteq K}$. אם נציב עובדה זו במסקנה 2.1.10, נקבל שתי תוצאות מעניינות:

מסקנה 2.5.8 תהי K/F הרחבת גלואה. לכל שדה ביניים $F \subseteq L \subseteq K$ יש $[L\colon F]$ שיכונים $L \hookrightarrow K$.

לכן מספר תת־השדות של K האיזומורפיים ל־L שווה ל־$\frac{[L:F]}{|\mathrm{Gal}(L/F)|}$.

בפרט, אם L/F הרחבת גלואה, אז אף תת־שדה אחר של L אינו איזומורפי לו.

מסקנה 2.5.9 תהי K/F הרחבת גלואה. כל איזומורפיזם של שדות ביניים מושרה על־ידי אוטומורפיזם של K.

הוכחה. **כל איזומורפיזם של שדות ביניים $\phi\colon L \to L'$ הוא שיכון $L \to L' \subseteq K$, ולפי מסקנה 2.1.10 שיכון כזה ניתן להמשכה לשיכון $\sigma\colon K \to K$, שהוא אוטומוזפיזם לפי הממד. במלים אחרות, ϕ הוא הצמצום של σ ל־L.** □

מסקנה 2.5.10 (בהמשך להערה 2.3.6) נניח ש־K/F היא הרחבת הפיצול של $f \in F[\lambda]$. אז חבורת גלואה $\mathrm{Gal}(K/F)$ פועלת טרנזיטיבית על השורשים של f, אם ורק אם f אי־פריק.

הוכחה. אם הפולינום פריק, אוטומורפיזם אינו יכול להעביר שורש של גורם אחד לשורש של גורם אחר.

מצד שני, נניח ש־f פריק. אם α, α' שורשים של f, אז $F[\alpha] \cong F[\lambda]/\langle f\rangle \cong F[\alpha']$ לפי (1.1), כאשר האיזומורפיזמים מעבירים $\alpha \mapsto \lambda + \langle f\rangle \mapsto \alpha'$. לפי מסקנה 2.5.9 יש אוטומורפיזם $\sigma \in \mathrm{Gal}(K/F)$ כך ש־$\sigma(\alpha) = \alpha'$. □

2.5.3 בעיית ההיפוך

אחת הבעיות המרכזיות בתורת גלואה היא **בעיית ההיפוך**: האם כל חבורה סופית G מהווה חבורת גלואה של איזושהי הרחבה $K/\mathbb{Q}$? נענה כאן על שאלה קלה בהרבה, ונראה שכל חבורה סופית מהווה חבורת גלואה של הרחבה כלשהי. לאור הערה 2.3.6, עלינו לטפל בתת־חבורות של S_n.

טענה 2.5.11 תהי $G \subseteq S_n$ תת־חבורה כלשהי. אז קיימת הרחבת גלואה K/F כך ש־$\mathrm{Gal}(K/F) \cong G$.

הוכחה. נבחר שדה כלשהו k, ונתבונן בשדה הפונקציות הרציונליות $K = k(\alpha_1, \dots, \alpha_n)$. החבורה S_n פועלת כחבורת תמורות על היוצרים $\alpha_1, \dots, \alpha_n$, ובעזרת פעולה זו היא מהווה חבורה של אוטומורפיזמים של K. כתת־חבורה, גם G פועלת על K. שדה השבת $F = K^G$ כולל את הפונקציות שהן סימטריות ביחס לפעולת G. לפי משפט 2.4.3, K/F היא הרחבת גלואה, ו־$G = \mathrm{Gal}(K/F)$. □

נתבונן בפולינום $f(\lambda) = \prod(\lambda - \alpha_i) \in K^{S_n}[\lambda] \subseteq K^G[\lambda]$.

תרגיל 2.5.12 (*) הפולינום f אי־פריק מעל $F = K^G$, אם ורק אם פעולת G על $\{1, \dots, n\}$ היא טרנזיטיבית.

2.5.4 סגור גלואה

טענה 2.5.13 לכל הרחבה ספרבילית סופית L/F יש הרחבת גלואה K/F כך ש־ $L \subseteq K$.

הרחבה מינימלית כזו נקראת 'סגור גלואה' של L/F. אם $L = F[\alpha_1, \dots, \alpha_t]$ ו־f_i הפולינום המינימלי של α_i מעל F, אז שדה הפיצול של $f_1 \cdots f_t$ הוא סגור גלואה של L/F.

נתבונן בסגור גלואה מנקודת המבט של התאמת גלואה: נסמן $G = \mathrm{Gal}(K/F)$, אז $L = K^H$ עבור תת־חבורה $H \leq G$. אם $N \lhd G$ תת־חבורה המוכלת ב־H, אז K^N/F הרחבת גלואה המכילה את L, ולפי המינימליות $N = 1$. במלים אחרות, תת־החבורה הנורמלית המקסימלית ש־N מכיל, $\mathrm{Core}_G(H) = \cap_{g \in G} gHg^{-1}$, היא טריוויאלית.

מסקנה 2.5.14 אם K/F סגור גלואה של הרחבה L/F, אז יש שיכון $\mathrm{Gal}(K/F) \hookrightarrow S_n$ כאשר $n = [L\,{:}\,F]$. בפרט $\mathrm{Gal}(K/F) \hookrightarrow S_{[K:F]}$ לכל הרחבת גלואה K/F.

הוכחה. לפי הלמה של שטייניץ (למה 2.5.18) $L = F[\alpha]$, ואז אוטומורפיזמים של K מוגדרים על־ידי פעולת התמורה שלהם על השורשים השונים של הפולינום המינימלי f של α בתוך K. □

הערה 2.5.15 אם K/F גלואה ו־ $L = K^H$ עבור $H \leq G = \mathrm{Gal}(K/F)$, אז:

1. תת־השדה המקסימלי של L שהוא גלואה מעל F הוא $K^{\langle gHg^{-1}:g\in G\rangle}$;
2. תת־השדה המינימלי של K המכיל את L שהוא גלואה מעל F הוא $K^{\mathrm{Core}_G(H)}$;
3. תת־השדה המינימלי של L ש־L גלואה מעליו הוא $K^{N_G(H)}$; לכן $\mathrm{Gal}(L/F) = \mathrm{N}_G(H)/H$.

2.5.5 מספר שדות הביניים

מסקנה 2.5.16 בכל הרחבת גלואה סופית יש מספר סופי של שדות ביניים.

מסקנה 2.5.17 לכל הרחבה ספרבילית סופית L/F יש מספר סופי של שדות ביניים. (קח $L \supseteq K$ כך ש־ K/F גלואה, והפעל את מסקנה 2.5.16).

(טענה זו אינה נכונה אם L/F אינה ספרבילית.)

למה 2.5.18 (הלמה של שטייניץ) כל הרחבה ספרבילית סופית L/F היא הרחבה פשוטה.

הוכחה. ההוכחה למקרה ש־F אינסופי. בהמשך (הערה 3.1.2) נראה שהטענה נכונה גם במקרה הסופי. יהיו $x, y \in L$. יש אינסוף איברים מהצורה $x + \alpha y$, $\alpha \in F$, אבל (מסקנה 2.5.17) רק מספר סופי של שדות ביניים של F/L. לכן יש שני ערכים שונים $\alpha, \alpha' \in F$ כך ש־ $L_0 = F[x + \alpha y] = F[x + \alpha' y]$. אבל אז $x + \alpha y, x + \alpha' y \in L_0$, ולכן $(\alpha - \alpha')y \in L_0$ ומכאן $y \in L_0$ ו־ $x \in L_0$. כלומר, $F[x + \alpha y] = F[x, y]$. כעת הטענה נובעת מאינדוקציה על מספר היוצרים. □

2.5.6 הרכבה של שדות

אפשר לדלג

- הגדרת ההרכבה K_1K_2, כאשר $K_1, K_2 \subseteq E$.
- חבורת גלואה של ההרכבה מעל $F = K_1 \cap K_2$.

טענה 2.5.19 אם $F \subseteq F', K \subseteq E$, אז $[F'K : K] \leq [F' : F]$. (באינדוקציה על מספר היוצרים של F'/F, לפי טענה 1.2.18).

פרק 3

שימושים

3.1 שורשי יחידה

איבר $\rho \in F$ נקרא **שורש יחידה** אם יש $n > 0$ כך ש־$\rho^n = 1$. במלים אחרות שורשי יחידה הם האברים מסדר סופי בחבורה הכפלית של השדה. שורש יחידה הוא **מסדר** n אם $\rho^n = 1$; הוא נקרא **פרימיטיבי** אם הסדר שלו, כאיבר בחבורה, שווה ל־n.

מעל שדות ממאפיין אפס, מסמנים ב־$\rho_n = e^{\frac{2\pi i}{n}}$ את האיבר המסויים של שדה המספרים המרוכבים $\mathbb{C}$ המוגדר לפי הנוסחה הטריגונומטרית. בחירה זו אינה מהותית, משום שאם ρ_n שורש יחידה פרימיטיבי מסדר n, אז שורשי היחידה אחרים מאותו סדר הם החזקות ρ_n^k עבור $k \in U_n$, כאשר U_n היא חבורת אוילר (שסדרה $\phi(n)$ הוא פונקציית אוילר בנקודה n).

3.1.1 החבורה הכפלית של שדה

משפט 3.1.1 *כל תת־חבורה כפלית סופית של שדה היא ציקלית.*

הוכחה. נסמן $e = \exp(G)$. אז כל אברי G הם שורשים של הפולינום $x^e - 1$, ולפי מסקנה 1.1.9, $|G| \leq e$. לכן $e = |G|$, ומכיוון שבחבורה אבלית תמיד יש איבר שסדרו שווה לאקספוננט, G ציקלית. □

הערה 3.1.2 כעת אפשר להשלים את ההוכחה של הלמה של שטייניץ, למה 2.5.18. תהי K/F הרחבה ספרבילית של שדות סופיים (את המקרה האינסופי כבר הוכחנו). אז $K^\times$ חבורה סופית ולכן ציקלית. נסמן ב־$a \in K^\times$ יוצר של החבורה, אז בהכרח $K = F[a]$.

לעומת זאת, חבורות כפליות אינסופיות של שדה יכולות להיות בעלות מבנה מורכב. לדוגמא, החבורה הכפלית $\mathbb{Q}^\times$ היא מכפלה ישרה $\langle -1 \rangle \times \langle 2 \rangle \times \langle 3 \rangle \times \langle 5 \rangle \times \cdots$, כלומר $\mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}}$.

3.1.2 הפולינומים הציקלוטומיים

כל שורש יחידה מסדר n מאפס את הפולינום $\lambda^n - 1$, אבל זהו אינו הפולינום המינימלי, משום שהוא פריק בעליל.

נגדיר את **הפולינום הציקלוטומי מסדר** n, $\Phi_n(\lambda) \in \mathbb{C}[\lambda]$, באופן הבא:

$$\Phi_n(\lambda) = \prod_{(k,n)=1} (\lambda - \rho_n^k)$$

כאשר $\rho_n = \exp(\frac{2\pi}{n})$ הוא שורש יחידה פרימיטיבי מסדר n (אבל להגדרת הפולינום אין זה משנה מהו השורש שנבחר).

מן ההגדרה נובע ש־

$$\deg(\Phi_n(\lambda)) = \phi(n).$$

מסקנה 3.1.3 השורשים של $\Phi_n(\lambda)$ הם שורשי היחידה הפרימיטיביים מסדר n.

ברור ש־

$$\prod_{d\,|\,n} \Phi_d(\lambda) = \prod_{d\,|\,n} \prod_{(k,n)=d} (\lambda - \rho_n^{nk/d}) = \prod_{i=0}^{n-1} (\lambda - \rho_n^i) = \lambda^n - 1.$$

משפט 3.1.4 $\Phi_n(\lambda) \in \mathbb{Z}[\lambda]$.

הוכחה. באינדוקציה על n. עבור $n = 1$, $\Phi_n(\lambda) = \lambda - 1$. נניח שהטענה נכונה לכל מחלק של n, אז $\Phi_n(\lambda) \,|\, \lambda^n - 1$ מעל המרוכבים, עם מנה $\prod_{d\,|\,n,\, d<n} \Phi_d(\lambda) = \Phi'_n(\lambda)$, ולכן $\Phi_n(\lambda) \in \mathbb{Q}[\lambda]$. לפי הלמה של גאוס, $\Phi_n(\lambda) \in \mathbb{Z}[\lambda]$ כי המנה היא פולינום מתוקן ולכן פרימיטיבי. □

בזכות המשפט הזה, הפולינום הציקלוטומי מוגדר מעל כל שדה.

דוגמא 3.1.5

$$\begin{aligned}
\Phi_2(\lambda) &= \frac{\lambda^2-1}{\lambda-1} = \lambda+1;\\
\Phi_3(\lambda) &= \frac{\lambda^3-1}{\lambda-1} = \lambda^2+\lambda+1;\\
\Phi_4(\lambda) &= \frac{\lambda^4-1}{(\lambda-1)(\lambda+1)} = \lambda^2+1;\\
\Phi_5(\lambda) &= \frac{\lambda^5-1}{\lambda-1} = \lambda^4+\lambda^3+\lambda^2+\lambda+1;\\
\Phi_6(\lambda) &= \frac{\lambda^6-1}{(\lambda-1)(\lambda+1)(\lambda^2+\lambda+1)} = \lambda^2-\lambda+1;\\
\Phi_{105}(\lambda) &= \lambda^{48}+\lambda^{47}+\lambda^{46}-\lambda^{43}-\lambda^{42}-2\lambda^{41}-\cdots+\lambda^2+\lambda+1
\end{aligned}$$

(Φ_{105} הוא הפולינום הציקלוטומי הראשון עם מקדם שאינו $0, \pm 1$.)

משפט 3.1.6 *הפולינומים* $\Phi_n(\lambda)$ *אי־פריקים מעל* $\mathbb{Q}$.

הוכחה. אחרת, לפי הלמה של גאוס, אפשר להניח שיש פירוק לא טריוויאלי $\Phi_n(\lambda) = g(\lambda)h(\lambda)$ כאשר $g, h \in \mathbb{Z}[\lambda]$, ו־$g$ אי־פריק. אז קיימים שורש ρ של g וראשוני p זר ל־n, כך ש־ ρ^p שורש של h. מכאן ש־$g(\lambda) \,|\, h(\lambda^p)$ מעל $\mathbb{Z}$.

מעתה נעבוד מעל $\mathbb{Z}/p\mathbb{Z}$. נבחין ש־ $\lambda^n - 1$ ספרבילי כי $(\lambda^n - 1)' = n\lambda^{n-1}$ ו־ $n \not\equiv 0 \pmod p$, ומכאן נובע בפרט ש־g ספרבילי. מודולו p מתקיים $g(\lambda) \,|\, h(\lambda^p) = h(\lambda)^p$ ולכן $g \,|\, h$, ומכאן שגם $g^2 \,|\, \Phi_n \,|\, (\lambda^n - 1)$ מודולו p, סתירה לספרביליות. □

3.1.3 השדה $\mathbb{Q}[\rho_n]$

לפי משפט 3.1.6, $\Phi_n(\lambda)$ הוא הפולינום המינימלי של ρ_n מעל $\mathbb{Q}$. לכן

$$[\mathbb{Q}[\rho_n] \colon \mathbb{Q}] = \deg(\Phi_n(\lambda)) = \phi(n).$$

יתרה מזו, $\mathbb{Q}[\rho_n]$ הוא שדה הפיצול של $\Phi_n(\lambda)$ (וגם של $\lambda^n - 1$), שהוא ספרבילי, ולכן $\mathbb{Q}[\rho_n]/\mathbb{Q}$ היא הרחבת גלואה. אם כך, מהי חבורת גלואה שלה?

טענה 3.1.7 $\mathrm{Gal}(\mathbb{Q}[\rho_n]/\mathbb{Q}) \cong U_n$.

הוכחה. נגדיר התאמה $f : \mathrm{Gal}(\mathbb{Q}[\rho_n]/\mathbb{Q}) \to U_n$ לפי $\sigma \mapsto k$ אם $\sigma(\rho_n) = \rho_n^k$; תמיד קיים $k \in U_n$ יחיד כזה, משום ש־$\sigma(\rho_n)$ הוא שורש של $\Phi_n(\lambda)$. מאידך, לכל $k \in U_n$, ρ_n^k הוא שורש של הפולינום המינימלי Φ_n. מכאן ש־ $\rho_n \mapsto \rho_n^k$ מגדיר איזומורפיזם

$$\mathbb{Q}[\rho_n] \cong \mathbb{Q}[\lambda]/\langle \Phi_n(\lambda) \rangle \cong \mathbb{Q}[\rho_n^k],$$

ולכן ההתאמה היא על. לבסוף, קל לבדוק ש־$f(\sigma\sigma') = f(\sigma)f(\sigma')$. □

דוגמא 3.1.8 נתבונן בשדה $\mathbb{Q}[\rho_{12}]$. חבורת גלואה היא $\mathrm{Gal}(\mathbb{Q}[\rho_{12}]/\mathbb{Q}) \cong U_{12} = \langle -1, 5\rangle$. יש בה שני יוצרים: $\sigma : \rho \mapsto \rho^5$ ו־$\tau : \rho \mapsto \rho^{-1}$. מכיוון שהחבורה $\mathrm{Gal}(\mathbb{Q}[\rho]/\mathbb{Q}) = \langle \sigma, \tau\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, יש בדיוק שלושה תת־שדות, שכולם הרחבות ריבועיות של $\mathbb{Q}$: $\mathbb{Q}[\rho]^{\sigma} = \mathbb{Q}[\rho+\rho^5]$, $\mathbb{Q}[\rho]^{\tau} = \mathbb{Q}[\rho+\rho^{-1}]$, ו־$\mathbb{Q}[\rho]^{\sigma\tau} = \mathbb{Q}[\rho+\rho^7]$. תרגיל: הראה ששדות אלו הם, לפי הסדר, $\mathbb{Q}[\rho^3] = \mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{3}]$ ו־$\mathbb{Q}[\rho^2] = \mathbb{Q}[\sqrt{-3}]$, בהתאמה.

תרגיל 3.1.9 (**) הראה ש־$\mathbb{Q}[\rho_{24}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{-1}]$.

הערה 3.1.10 ***משפט קרונקר־וובר***, שהוא אחד המשפטים המרכזיים בתורת המספרים האלגברית, קובע שכל הרחבה אבלית של $\mathbb{Q}$ (כלומר הרחבת גלואה שחבורת גלואה שלה אבלית) מוכלת באיזשהו $\mathbb{Q}[n]$.

תרגיל 3.1.11 (־*)** הראה שלכל ראשוני p, $\sqrt{\pm p} \in \mathbb{Q}[\rho_p]$.

תרגיל 3.1.12 (***) בהנתן $d \in \mathbb{Z}$, מצא n כך ש־$\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q}[\rho_n]$.

3.2 משוואות ממעלה שלישית ורביעית

בעוד שאת המשוואה ממעלה שנייה ידעו לפתור היוונים (וכנראה גם הבבלים), פתרונה של המשוואה ממעלה שלישית לא היה ידוע עד תחילת המאה ה־16. המתמטיקאים באותו זמן עדיין לא 'הכירו' במספרים שליליים, וכך הם התייחסו למשוואות $x^3+px+q=0$ או $x^3+px=q$ (כאשר p,q שלמים חיוביים) כאל בעיות נבדלות.

ב־1515 גילה המתמטיקאי האיטלקי שפיונה דל פרו איך לפתור חלק מן המשוואות ממעלה שלישית. באותה תקופה היו מתמטיקאים מתחרים זה בזה בפתרון משוואות, ולכן הסתיר דל פרו את הפתרון שלו. ב־1535 גילה האיטלקי ניקולו טרטליה מחדש את אותם פתרונות וסיפר עליהם לג'ירולמו קרדאנו, שהשלים את המקרים החסרים ופרסם אותם בספר. את המשוואה ממעלה רביעית הצליחו לפתור זמן קצר אחר־כך, ב־1545.

פתרונה של המשוואה ממעלה שלישית היה ההישג האמיתי הראשון של המתמטיקאים בראשית תקופת הרנסאנס, ובכך הוא סייע לשבור את השיתוק שאחז בהם מאז תחילת ימי הביניים. בנוסף, פתרונו של קרדנו אילץ את המתמטיקאים להתייחס ברצינות למספרים המרוכבים, משום שפתרונות אמיתיים (דהיינו, ממשיים) מתקבלים לפעמים תוך מניפולציות של מספרים מרוכבים.

את הפתרון של משוואות ממעלה רביעית מצא לודוביקו פרארי האיטלקי, בשנת 1545, כשלושים שנה אחרי שנמצא הפתרון למשוואה ממעלה שלישית. בעקבות פתרונות אלו, האמינו המתמטיקאים של סוף תקופת הרנסאנס שאפשר יהיה לפתור גם משוואות ממעלה גבוהה יותר באותו אופן, ומאמצים ניכרים הושקעו בבעיה זו. יותר ממאתיים שנה חלפו עד שנילס הנריק אבל הראה (בשנות השלושים של המאה ה־19) שפתרון כזה אינו אפשרי, ואווריסט גלואה הניח את היסודות לתורת גלואה, שמסבירה את ההבדל היסודי בין משוואות ממעלה חמישית ומעלה (שאינן ניתנות לפתרון על ידי פעולות של חיבור, חיסור, כפל וחילוק והוצאת שורש) ובין משוואות ממעלה נמוכה יותר.

3.2.1 משוואה ממעלה שלישית

תרגיל 3.2.1 (+*) מעל שדה ממאפיין זר ל־n, כל משוואה פולינומית ממעלה n אפשר להביא על־ידי הצבה לינארית למצב שבו המקדם של x^{n-1} הוא אפס.

הערה 3.2.2 כך פותרים משוואה כללית ממעלה שלישית. נתבונן במשוואה

$$x^3 + ax - b = 0 :$$

נציב $x = \alpha + \beta$, אז

$$\alpha^3 + \beta^3 + (3\alpha\beta + a)x - b = 0;$$

נבחר

$$\alpha\beta = -a/3, \tag{3.1}$$

אז $\alpha^3\beta^3 = -a^3/27$, ואילו

$$\alpha^3 + \beta^3 = b,$$

כך ש־α^3, β^3 הם הפתרונות למשוואה הריבועית $z^2 - bz - a^3/27 = 0$. הוצאת שורש ריבועי נותנת את α^3, β^3, והוצאת שורש שלישי מאחד מאלה נותנת את α או את β (שלושה ערכים אפשריים); היחס (3.1) מחשב את הפרמטר הנותר, ומכיוון שהפתרון הוא הסכום $\alpha + \beta$, ממילא מתקבלים אותם פתרונות בשתי האפשרויות.

ננתח את הפתרון. נניח ש־$a, b \in F$, ויהי K שדה הפיצול של הפולינום $f(x) = x^3 + ax - b$, עם השורשים $x_1, x_2, x_3 \in K$. המשוואה הריבועית נותנת $z = \frac{1}{2}(b \pm \sqrt{b^2 + 4a^3/27})$. כלומר, במקרה הכללי, $L = F[\alpha^3] = F[\beta^3] = F[\sqrt{b^2 + 4a^3/27}]$ הוא הרחבה ריבועית של F.

מסקנה 3.2.3 נניח שהפולינום $f(x) = x^3 + ax - b$ אי־פריק. חבורת גלואה שלו היא A_3 אם $b^2 + 4a^3/27$ הוא ריבוע ב־F, ו־S_3 אחרת.

פתרון בעזרת פונקציות סימטריות

יהי F שדה עם שורש שלישי של היחידה. נניח ש־$f(x) = x^3 + ax - b$ אי־פריק מעל F, כאשר $a, b \in F$. יהי E שדה הפיצול של F, עם השורשים $x_1, x_2, x_3 \in E$. כך

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1x_2 + x_2x_3 + x_3x_1 &= a, \\ x_1x_2x_3 &= b. \end{aligned}$$

חבורת גלואה של ההרחבה היא תת־חבורה של S_3, ומכיוון שתמיד אפשר לעבור לסדרת ההרכב המושרה, נוח לטפל בסדרת ההרכב של S_3 עצמה:

$$1 \lhd A_3 \lhd S_3,$$

המתאימה לשרשרת ההרחבות

$$F = E^{S_3} \subseteq E^{A_3} \subseteq E.$$

ברור ש־$E = F(x_1, x_2, x_3)$. נסמן $\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. ברור ש־$\sigma(\delta) = \delta$ אם $\sigma \in A_3$, וש־$\sigma(\delta) = -\delta$ אחרת. לכן $E^{A_3} = F[\delta]$. אפשר לחשב ש־

$$\delta^2 = -4a^3 - 27b^2,$$

כך ש־$E^{A_3} = F[\sqrt{-4a^3 - 27b^2}]$. כדי להשלים את הפתרון, עלינו למצוא את x_i במונחי δ. כדי להשיג משוואה זו, נבחין שהאיברים

$$z = x_1 + \rho x_2 + \rho^2 x_3, \qquad z' = x_1 + \rho^2 x_2 + \rho x_3$$

מקיימים $(123) \cdot z = \rho z$ ו־$(123) \cdot z' = \rho^{-1} z'$, ולכן $z^3, z'^3 \in E^{A_3}$. חישוב ישיר מעלה ש־

$$z^3 = \frac{27}{2} b - (3\rho + \frac{3}{2})\delta,$$

$$z'^3 = \frac{27}{2} b + (3\rho + \frac{3}{2})\delta;$$

בעוד ש־

$$zz' = -3a.$$

אם נהפוך את הסדר ונגדיר $z = \sqrt[3]{\frac{27}{2} b - (3\rho + \frac{3}{2})\delta}$ ו־$z' = -3az^{-1}$, אז

$$x_1 = \frac{1}{3}(z + z'),$$

$$x_2 = \frac{1}{3\rho}(z + \rho^2 z'),$$

$$x_3 = \frac{1}{3\rho^2}(z + \rho z').$$

3.2.2 הדיסקרימיננטה

נניח ש־ K שדה הפיצול של פולינום אי־פריק f מעל F. נכתוב $f(\lambda) = \prod(\lambda - \alpha_i)$ כאשר $\alpha_i \in K$. בפרט,

$$K = F[\alpha_0, \dots, \alpha_{n-1}].$$

הדיסקרימיננטה של f (וגם של ההרחבה K/F) מוגדרת כמכפלה

$$\mathrm{disc}(K/F) = \pm \prod_{i<j} (\alpha_i - \alpha_j) \in K^\times / \langle -1 \rangle.$$

כפי שאפשר לראות, הדיסקרימיננטה אינה איבר של K, אלא איבר כזה עד־כדי סימן, משום שהסימן תלוי בסדר השורשים. אכן, חבורת גלואה $G = \mathrm{Gal}(K/F)$ פועלת באופן טבעי על השורשים $\alpha_0, \dots, \alpha_{n-1}$, וזה מגדיר שיכון $G \hookrightarrow S_n$.

תרגיל 3.2.4 (*) לכל $\sigma \in G$, $\sigma(\mathrm{disc}(f)) = \mathrm{sgn}(\sigma)\mathrm{disc}(f)$.

תרגיל 3.2.5 (**) השיכון של G ב־S_n נושא אותה לתוך A_n, אם ורק אם $\mathrm{disc}(f) \in F$.

נסמן ב־$A \in \mathrm{M}_n(K)$ את המטריצה $A_{ij} = \alpha_i^j$ (האינדקסים בטווח $0, \dots, n-1$).
נסמן $\pi_t = \sum_{i=0}^{n-1} \alpha_i^t$; מכיוון ש־$\sigma(\pi_t) = \pi_t$ לכל $\sigma \in G$, $\pi_t \in F$ לכל t. כעת,

$$A^{\mathrm{t}} A = (\alpha_i^j)_{ji} (\alpha_i^k)_{ik} = (\sum_i \alpha_i^{j+k})_{jk} = (\pi_{j+k})_{jk},$$

כלומר $A^{\mathrm{t}} A \in \mathrm{M}_n(F)$, ולכן $\det A^2 = \det(A^{\mathrm{t}} A) \in F^\times$, אלא ש־$\det(A)$ היא דטרמיננטת ואנדרמונדה, וידוע ש־$\det A = \prod_{i<j}(\alpha_i - \alpha_j) = \mathrm{disc}(f)$, כך שבטענה $\det(A)^2 \in F$ אין חידוש. היתרון בחישוב זה הוא שמתוך π_t, שאותם אפשר לבטא כפונקציות של מקדמי הפולינום f, אפשר לקבל נוסחה מפורשת ל־$\mathrm{disc}(f)^2$.

תרגיל 3.2.6 (**) פתח נוסחה ל־$\mathrm{disc}(f)$ עבור $f = \lambda^3 + a\lambda + b$.

נסכם עבור פולינום אי־פריק $f = \lambda^3 + a\lambda + b$ ממעלה 3, ששורשיו בשדה הפיצול הם $\alpha_0, \alpha_1, \alpha_2$. יהי K/F שדה הפיצול של הפולינום.
* $\mathrm{Gal}(K/F) = A_3$ אם ורק אם $[K:F] = 3$ אם ורק אם $F[\alpha_0]/F$ גלואה אם ורק אם $\mathrm{disc}(K/F) \in F$;
* $\mathrm{Gal}(K/F) = S_3$ אם ורק אם $[K:F] = 6$ אם ורק אם $F[\alpha_0]/F$ אינו גלואה, אם ורק אם $\mathrm{disc}(K/F) \notin F$.

תרגיל 3.2.7 (**) תת־החבורות הטרנזיטיביות של S_4 הן: S_4, A_4, D_4 (שלושה עותקים צמודים), K_4 ו־$\mathbb{Z}_4$ (שלושה עותקים צמודים). מאלו, רק $K_4 \subseteq A_4$ מוכלות ב־A_4.

3.2.3 משוואה ממעלה רביעית

הפתרון של פרארי

יהי

$$f(x) = x^4 + ax^2 + bx + c$$

פולינום ממעלה רביעית, לאחר התיקון של תרגיל 3.2.1.
ננסה לפרק $f(x) = (x^2 - Ax + B)(x^2 + A'x + C)$; השוואת מקדמים מראה ש־$A' = A$, וכן

$$B + C - A^2 = a;$$
$$A(B - C) = b;$$
$$BC = c;$$

ומשתי המשוואות הראשונות נובע $B = \frac{1}{2}(A^2 + a + b/A)$ ו־$C = \frac{1}{2}(A^2 + a - b/A)$.
לכן $c = BC = \frac{1}{4}(A^4 + 2aA^2 + a^2 - b^2/A^2)$, כלומר

$$A^6 + 2aA^4 + (a^2 - 4c)A^2 - b^2 = 0.$$

אם נציב $T = A^2$, נקבל

$$T^3 + 2aT^2 + (a^2 - 4c)T - b^2 = 0,$$

וזו משוואה ממעלה שלישית (הקרויה **הרזולבנטה** של $f(x)$). את הרזולבנטה אפשר לפתור לפי הסעיף הקודם (זה דורש הוצאת שורש שני ואז הוצאת שורש שלישי). מזה מקבלים את A (הוצאת שורש שני נוסף) ומיד את B, C. כעת נותרו שתי משוואות ריבועיות, שאפשר לפתור כל אחת מהן על־ידי הוצאת שורש ריבועי. אלא שאת השורש של מכפלת הדיסקרימיננטות שלהן, $\Delta\Delta'$, כבר חישבנו כפי שיתברר בהמשך, ולכן נותר להוציא שורש ריבועי מאחת הדיסקרימיננטות כדי למצוא את ארבעת שורשי המשוואה.

ניתוח הפתרון של פרארי

נניח ש־$a, b, c \in F$, ויהי E שדה הפיצול של הפולינום, שבו השורשים x_1, x_2, x_3, x_4.
נניח ש־$\mathrm{Gal}(E/F) = S_4$, שהוא המקרה הכללי. נניח שבפירוק המשוואה לגורמים ריבועיים, $x^2 - Ax + B = (x - x_1)(x - x_2)$ ו־$x^2 + Ax + C = (x - x_3)(x - x_4)$.
במלים אחרות,

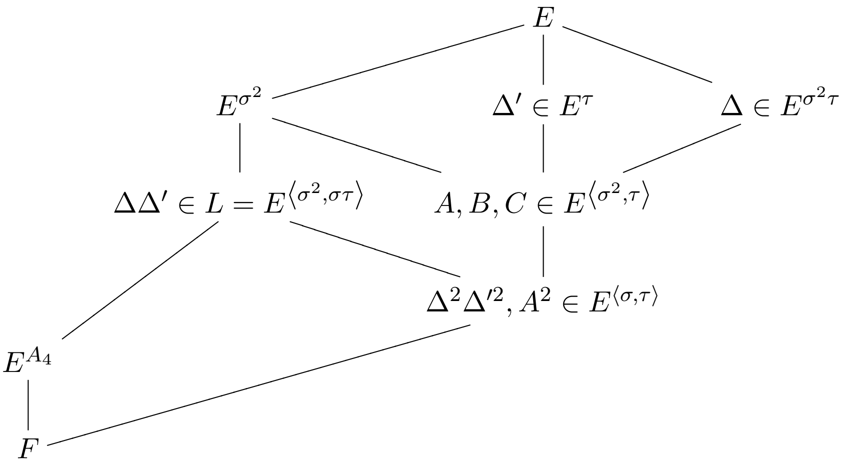
$$A = x_1 + x_2 = -(x_3 + x_4);$$

$$B = x_1x_2;$$

$$C = x_3x_4.$$

נסמן $\sigma = (1324)$ ו־$\tau = (12)$, כך ש־$\langle\sigma,\tau\rangle$ היא החבורה הדיהדרלית, מסדר 8. החבורה $\langle\sigma^2,\sigma\tau\rangle$ היא חבורת הארבעה של קליין, ולכן L/F היא הרחבת גלואה שחבורת גלואה שלה $S_4/K_4 = S_3$. קל לחשב ש־$\sigma(A) = -A$, $\sigma(B) = C$, $\sigma(C) = B$; $\tau(A) = A$, $\tau(B) = B$, $\tau(C) = C$. מכאן מיקומם של האברים בסריג תת־השדות.

להלן כמה תת־שדות של E/F:



נסמן $\Delta^2 = A^2 - 4B$ ו־$\Delta'^2 = A^2 - 4C$. אז

$$x_1 = \frac{1}{2}(A+\Delta),\ x_2 = \frac{1}{2}(A-\Delta),\ x_3 = \frac{1}{2}(-A+\Delta'),\ x_4 = \frac{1}{2}(-A-\Delta').$$

לכן $\Delta = 2x_1 - A = -2x_2 + A$ ו־$\Delta' = 2x_3 + A = -2x_4 + A$. מכאן ש־

$$\sigma(\Delta) = 2x_3 + A = \Delta'; \quad \sigma(\Delta') = 2x_2 - A = -\Delta;$$

$$\tau(\Delta) = 2x_2 - A = -\Delta; \quad \tau(\Delta') = \Delta'$$

בפרט, $\Delta\Delta' \in L$, ו־$\sigma(\Delta\Delta') = -\Delta\Delta'$.

נסמן ב־δ^2 את הדיסקרימיננטה של הרזולבנטה, אז $\sigma(\delta) = -\delta$, ולכן $\sigma(\delta\Delta\Delta') = \delta\Delta\Delta'$, כלומר $\Delta\Delta' \in F[A^2]\delta$.

פירושו של דבר הוא שלאחר חישוב A^2 ו־δ (מה שדרש הוצאת שורש שני ושלישי), כבר ידוע $\Delta\Delta'$. לכן נותר לחשב את A (הוצאת שורש שני), ואחר־כך למשל את Δ (הוצאת שורש מ־Δ^2).

פתרון בעזרת סדרת ההרכב

יהי F שדה עם שורש שלישי של היחידה, ρ. נתבונן בפולינום

$$f(x) = x^4 + \sigma_2 x^2 - \sigma_3 x + \sigma_4, \tag{3.2}$$

כאשר $\sigma_2, \sigma_3, \sigma_4 \in F$. נסמן את שורשי הפולינום בשדה הפיצול E ב־x_1, x_2, x_3, x_4. כך, לפי ההנחה,

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 + x_1x_3 + x_2x_4 &= \sigma_2, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= \sigma_3, \\ x_1x_2x_3x_4 &= \sigma_4. \end{aligned}$$

נניח להלן ש־$\mathrm{Gal}(E/F) = S_4$. סדרת ההרכב (היחידה, עקרונית) של S_4 היא

$$1 \lhd \langle(12)(34)\rangle \lhd K_4 \lhd A_4 \lhd S_4,$$

ובהתאמה יש שרשרת של תת־שדות

$$F \subset E^{A_4} \subset E^{K_4} \subset E^{\langle(12)(34)\rangle} \subset E.$$

לכל $i = 1, 2, 3$ נסמן

$$y_i = x_i x_4 + x_j x_k - \frac{1}{3}\sigma_2,$$

כאשר $\{i, j, k\} = \{1, 2, 3\}$. אלו אברים של E^{K_4}, וכל שניים מהם יוצרים אותו משום שאינם שייכים לאף תת־שדה. אפשר לחשב ש־

$$\begin{aligned} y_1 + y_2 + y_3 &= 0, \\ y_1y_2 + y_2y_3 + y_3y_1 &= -\frac{1}{3}\sigma_2^2 - 4\sigma_4, \\ y_1y_2y_3 &= \frac{2}{27}\sigma_2^3 + \sigma_3^2 - \frac{8}{3}\sigma_2\sigma_4; \end{aligned}$$

כלומר, הערכים y_1, y_2, y_3 הם הפתרונות למשוואה

$$y^3 + (-\frac{1}{3}\sigma_2^2 - 4\sigma_4)y - (\frac{2}{27}\sigma_2^3 + \sigma_3^2 - \frac{8}{3}\sigma_2\sigma_4) = 0. \tag{3.3}$$

הדיסקרימיננטה של הפולינום הזה,

$$\Delta = 256\sigma_4^3 - 128\sigma_2^2\sigma_4^2 + (16\sigma_2^4 + 144\sigma_2\sigma_3^2)\sigma_4 - 4\sigma_2^3\sigma_3^2 - 27\sigma_3^4,$$

היא גם הדיסקרימיננטה של $f(x)$. אם כך,

$$E^{A_4} = F[\sqrt{\Delta}].$$

נמשיך לטפס במעלה שרשרת תת־השדות. כדי לקבל מ־E^{A_4} את השדה E^{K_4} יש להוציא שורש שלישי, כפי שתואר בתת־הסעיף הקודם.

נסמן $s_i = x_i + x_4$; ברור ש־$E = F[s_1, s_2, s_3]$. קל לחשב ש־

$$s_i^2 = -(x_i + x_4)(x_j + x_k) = y_i - \frac{2}{3}\sigma_2 \in E^{K_4}$$

ו־

$$s_1 s_2 s_3 = \sigma_3 + (x_1 + x_2 + x_3 + x_4)x_4 = \sigma_3.$$

כלומר, האברים s_1, s_2, s_3 הם יוצרים סטנדרטיים להרחבות $E^{\langle (jk)(i4) \rangle}$, ומכפלתם שייכת ל־$F$. מכאן שדי לחשב שניים מהם: $s_1 = \sqrt{y_1 - \frac{2}{3}\sigma_2}$ ו־$s_2 = \sqrt{y_2 - \frac{2}{3}\sigma_2}$, ואז $s_3 = \sigma_3(s_1 s_2)^{-1}$.

לבסוף, $x_i = \frac{1}{2}(s_i - s_j - s_k)$, ו־$x_4 = \frac{1}{2}(s_1 + s_2 + s_3)$.

דוגמא 3.2.8 נתבונן בפולינום $f(x) = x^4 - 119x^2 + 594x - 728$, כלומר (3.2) עם $\sigma_2 = -119$, $\sigma_3 = -594$, $\sigma_4 = -728$. הפולינום ב־(3.3) הוא

$$g(y) = y^3 - \frac{5425}{3}y + \frac{81250}{27}.$$

נפתור את המשוואה הזו כמו בתת־הסעיף הקודם, עם $a = \frac{5425}{3}$ ו־$b = -\frac{81250}{27}$. החישוב מראה ש־$\delta^2 = 153000^2$. כעת יש לחשב את

$$z = \sqrt[3]{\frac{27}{2}b - (3\rho + \frac{3}{2})\delta} = \sqrt[3]{-270125 - 459000\rho} = 5\sqrt[3]{-2161 - 17 \cdot 216\rho} = 5(8-9\rho),$$

ואת $z' = -3az^{-1} = 5(17 + 9\rho)$. פתרונות המשוואה $g(y) = 0$ הם

$$y_1 = \frac{1}{3}(z + z') = \frac{125}{3},$$

$$y_2 = \frac{1}{3\rho}(z + \rho^2 z') = -\frac{130}{3},$$

$$y_3 = \frac{1}{3\rho^2}(z+\rho z') = \frac{5}{3}.$$

כעת נחשב $s_1 = \sqrt{y_1 - \frac{2}{3}\sigma_2} = \sqrt{121} = 11$ ו־$s_2 = \sqrt{y_2 - \frac{2}{3}\sigma_2} = \sqrt{36} = 6$,
ומכאן ש־$s_3 = \sigma_3(s_1 s_2)^{-1} = -\frac{594}{66} = 9$.
לבסוף, שורשי הפולינום הם

$$\begin{aligned} x_1 &= \frac{1}{2}(11-6-9) = -2, \\ x_2 &= \frac{1}{2}(-11+6-9) = -7, \\ x_3 &= \frac{1}{2}(-11-6+9) = -4, \\ x_4 &= \frac{1}{2}(11+6+9) = 13. \end{aligned}$$

3.3 פתירות על־ידי רדיקלים

3.3.1 הנורמה והעקבה

הגדרות בהרחבת גלואה. העקבה אדיטיבית והנורמה כפלית, ושתיהן לתוך השדה הקטן.

הגדרות בהרחבה כללית בעזרת ההצגה הרגולרית. הגדרות בהרחבה ספרבילית על־ידי סגור גלואה. טרנזיטיביות של הפונקציות.

העקבה היא על אם ורק אם ההרחבה ספרבילית.

גרסה אדיטיבית למשפט 90 של הילברט.

3.3.2 הרחבות רדיקליות

הגדרה 3.3.1 *הרחבה K/F נקראת הרחבה רדיקלית אם $K = F[\alpha]$ עם $\alpha^n \in F$, כאשר $n = [K:F]$.*

טענה 3.3.2 במאפיין שונה מ־2, כל הרחבה ריבועית (היינו ממימד 2) היא רדיקלית.

הוכחה. נניח ש־$K = F[\alpha]$. בגלל הממד, הפולינום המינימלי של α הוא $\alpha^2 - a\alpha + b = 0$ עם $a, b \in F$, ואז $K = F[\alpha - \frac{a}{2}]$ ו־$(\alpha - \frac{a}{2})^2 = \frac{a^2-4b}{4} \in F$. □

משפט 3.3.3 תהי K/F הרחבה רדיקלית ממימד n, כאשר $\rho_n \in F$ הוא שורש יחידה פרימיטיבי מסדר n. אז K/F היא הרחבת גלואה עם חבורת גלואה ציקלית.

הוכחה. לפי ההנחה $K = F[\alpha]$ כאשר $a = \alpha^n \in F$. הפולינום $\lambda^n - a$ מאפס את α, ומכיוון שמעלתו שווה לממד $[K:F]$, הוא אי־פריק. שורשי הפולינום הם $\rho^i\alpha$ עבור $i = 0, \dots, n-1$, וכולם שייכים ל־K, שהוא לכן שדה הפיצול של פולינום ספרבילי (מקיומם של שורשי יחידה מסדר n נובע ש־$\mathrm{char}F$ זר ל־n). כל אוטומורפיזם נקבע על־ידי התמונה של α שהיא אחד הערכים $\rho^i\alpha$, ומאידך כל העתקה $\alpha \mapsto \rho^i\alpha$ היא אכן אוטומורפיזם של $K[\alpha] \cong K[\lambda]/\langle\lambda^n - a\rangle$ כי המקור והתמונה הם שורשים של אותו פולינום אי־פריק. מכאן שחבורת גלואה נוצרת על־ידי ההעתקה $\rho\alpha \mapsto \alpha$, שהיא מסדר n. □

טענה 3.3.4 יהי p ראשוני, ויהי F שדה ממאפיין שאינו p, ו־$a \in F$. נניח ש־$\rho = \rho_p \in F$. אם הפולינום $\lambda^p - a$ פריק מעל F, אז הוא מתפצל שם.

הוכחה. יהי $\alpha = a^{1/p}$ בשדה הפיצול. שורשי הפולינום הם $\rho^i\alpha$, $i = 0, \dots, p-1$, ושדה הפיצול שלו הוא $F[\rho, \alpha]$. יהי $f \mid \lambda^p - a$ גורם אי־פריק מעל F, ממעלה d. מכיוון שמעל שדה הפיצול $\lambda^p - a = \prod_{i=0}^{p-1}(\lambda - \rho^i\alpha)$, בשדה הפיצול $f(\lambda)$ הוא מכפלה של גורמים מהצורה $\lambda - \rho^i\alpha$, ולכן המקדם החופשי שלו הוא $\rho^s\alpha^d$ עבור s מתאים. אם $d < p$ אז יש $n, m \in \mathbb{Z}$ כך ש־$nd + mp = 1$, ואז $F \ni (\rho^s\alpha^d)^n a^m = \rho^{sn}\alpha^{dn+pm} = \rho^{sn}\alpha$. לכן $\rho^i\alpha \in F$ לכל i, והפולינום מתפצל. □

הערה 3.3.5 טענה 3.3.4 אינה נכונה ללא ההנחה $\rho \in F$. אכן, לכל $p > 2$, הפולינום $\lambda^p - 2$ פריק מעל $\mathbb{Q}[2^{1/p}]$, אבל אינו מתפצל שם כי השדה הזה ממשי.

3.3.3 הרחבות ציקליות

נתחיל בדוגמא קלה:

טענה 3.3.6 אם $\mathrm{char}F \neq 2$, אז כל הרחבה K/F ממימד 2 מעל F היא הרחבת גלואה (ולכן הרחבה ציקלית).

הוכחה. אם $\lambda^2 - a\lambda + b = 0$ הוא הפולינום המינימלי של $\alpha \in K$, עם $a, b \in F$, אז שורשי הפולינום הם $\alpha, a - \alpha$ ולכן הוא מתפצל ב־K. מכאן שזו הרחבת גלואה, עם חבורת גלואה $\mathbb{Z}_2$. □

תהי K/F הרחבה ציקלית, עם חבורת גלואה $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. אם $a = \sigma(b)b^{-1}$ אז בוודאי $\mathrm{N}(a) = \mathrm{N}(\sigma(b)b^{-1}) = \sigma(\mathrm{N}(b))\mathrm{N}(b)^{-1} = 1$.

משפט 3.3.7 (משפט 90 של הילברט) *בהרחבה ציקלית כנ"ל, גם ההיפך נכון: כל איבר a עם $\mathrm{N}(a) = 1$ הוא מהצורה $a = \sigma(b)b^{-1}$ לאיזשהו $b \in K$.*

הוכחה. קח $b = \sum_{i=0}^{n-1}(a \cdots \sigma^{i-1}(a))^{-1}\sigma^i(z)$ כלשהו שאינו אפס; קיים כזה לפי טענה 2.5.1. חישוב מראה ש־ $\sigma(b) = ab$. □

מסקנה 3.3.8 תהי K/F הרחבה ציקלית עם $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, ועם $\rho \in F$ שורש יחידה מסדר $n = [K:F]$. אז קיים $x \in K$ כך ש־ $\sigma(x) = \rho x$. כל איבר כזה הוא יוצר של ההרחבה, ומקיים $a = x^n \in F$. אפשר לכתוב $K = F[\sqrt[n]{a}]$.

הוכחה. מכיוון ש־ $\rho \in F$, $\mathrm{N}_{K/F}(\rho) = \rho^n = 1$, ולכן לפי משפט 3.3.7 קיים $x \in K$ כך ש־ $\sigma(x) = \rho x$. אם x כנ"ל אז $\sigma(x^n) = \sigma(x)^n = \rho^n x^n = x^n$, ואילו $\sigma^i(x) = \rho^i x \neq x$ לכל $0 < i < n$, כך ש־ x אינו שייך לאף תת־שדה של K. □

הערה 3.3.9 אם לא מניחים $\rho \in F$, התאור של הרחבות ציקליות הרבה יותר מסובך. ראה ספרו של *Edwards* לדיון בהרחבות ממימד 5.

3.3.4 חבורות פתירות

תהי G חבורה. **סדרה תת־נורמלית** היא סדרה של תת־חבורות

$$1 = G_t \subset G_{t-1} \subset \cdots \subset G_0 = G$$

כך ש־$G_i \lhd G_{i-1}$. הסדרה נקראת **סדרת הרכב** אם אי־אפשר לעדן אותה, כלומר אם כל המנות G_{i-1}/G_i הן חבורות פשוטות. לפי **משפט קרול־שמידט**, בכל סדרת הרכב של חבורה G יש אותן מנות. חבורה היא **פתירה** אם כל מנות ההרכב שלה הן חבורות ציקליות מסדר ראשוני. חבורה היא פתירה אם ורק אם יש לה סדרה תת־נורמלית שהמנות שלה אבליות.

כל חבורה אבלית היא פתירה. נניח ש־$N \lhd G$; החבורה G פתירה אם ורק אם N ו־G/N פתירות. החבורות הפשוטות הלא אבליות אינן פתירות. בפרט S_n עבור $n \geq 5$ אינה פתירה.

תת־חבורת הקומוטטורים של חבורה G מוגדרת כתת־החבורה G' הנוצרת על־ידי הקומוטטורים $[x, y] = xyx^{-1}y^{-1}$. המנה G/G' היא המנה האבלית המקסימלית של G. **הסדרה המרכזית היורדת** של חבורה G מוגדר באינדוקציה לפי $G^0 = G$ ו־ $G^{n+1} = (G^n)'$. חבורה היא פתירה אם ורק אם יש n כך ש־$G^n = 1$ (וכשהחבורה סופית, היא אינה פתירה אם ורק אם יש n כך ש־$G^n \neq 1$ ו־$G^n = (G^n)'$).

משפט 3.3.10 *תהי E/F הרחבת גלואה. אז חבורת גלואה $G = \mathrm{Gal}(E/F)$ פתירה אם ורק אם יש שרשרת של תת־שדות*

$$F = F_0 \subset F_1 \subset \cdots \subset F_t = K$$

כך שלכל i, F_{i+1}/F_i היא הרחבת גלואה ציקלית מסדר ראשוני.

הוכחה. החבורה פתירה אם ורק אם יש לה שרשרת תת־חבורות

$$1 = G_t \subset G_{t-1} \subset G_{t-2} \subset \cdots \subset G_0 = G$$

כך ש־$G_i \lhd G_{i+1}$ והמנות G_{i+1}/G_i ציקליות מסדר ראשוני. התאמת גלואה נושאת שרשרת כזו לשרשרת של תת־שדות עם הרחבות ציקליות מאותו סדר, ולהיפך. □

3.3.5 משפט גלואה על פתירות לפי רדיקלים

הגדרה 3.3.11 *יהי F שדה. נאמר שהרחבה $F\subset E$ היא **על־רדיקלית** אם יש שרשרת של הרחבות רדיקליות מסדרים ראשוניים*

$$F_0\subset F_1\subset\cdots\subset F_t=E.$$

*פולינום $f\in F[\lambda]$ הוא **פתיר על־ידי רדיקלים** אם הוא מתפצל בהרחבה על־רדיקלית (כלומר, שדה הפיצול שלו מוכל בהרחבה על־רדיקלית).*

משפט 3.3.12 *תהי E/F הרחבת גלואה, ונניח ש־ F מכיל שורשי יחידה מכל סדר המחלק את $[E:F]$. אז ההרחבה היא על־רדיקלית אם ורק אם $\mathrm{Gal}(E/F)$ פתירה.*

הוכחה. זהו משפט 3.3.10, משום שבנוכחות שורשי היחידה הרחבה היא ציקלית אם ורק אם היא רדיקלית. □

משפט 3.3.13 *יהי E/F שדה פיצול של פולינום אי־פריק מדרגה n, ונניח ש־ F מכיל שורשי יחידה מכל סדר עד n. אז f פתיר אם ורק אם $\mathrm{Gal}(E/F)$ פתירה.*

הוכחה. נניח שהחבורה $G=\mathrm{Gal}(E/F)$ פתירה. אז יש לה סדרת הרכב

$$1=G_t\subset G_{t-1}\subset G_{t-2}\subset\cdots\subset G_0=G$$

עם מנות ציקליות מסדר ראשוני. מכיוון ש־$|G|$ מחלק את $n!$, כל האינדקסים $[G_{i-1}:G_i]$ קטנים או שווים ל־n. ניקח $F_i=E^{G_i}$. לפי המשפט המרכזי, שרשרת תת־השדות

$$E=F_t\supset F_{t-1}\supset\cdots\supset F_0=F$$

מקיימת $\mathrm{Gal}(F_i/F_{i-1})\cong G_{i-1}/G_i$, כלומר ההרחבות F_i/F_{i-1} כולן ציקליות, מממד שאינו עולה על n. לפי ההנחה יש ב־F שורשי יחידה מכל ממד כזה, ולפי מסקנה 3.3.8 כל ההרחבות F_i/F_{i-1} רדיקליות.

מצד שני, אם יש שרשרת של שדות שכל ההרחבות שלה רדיקליות, וב־F יש שורשי יחידה .... ((...)) □

לכן אם K/F הרחבת גלואה, אז $\mathrm{Gal}(K/F)$ פתירה אם ורק אם יש שרשרת של הרחבות $F=F_0\subseteq F_1\subseteq\cdots\subseteq F_t=K$ כך שכל השלבים F_{i+1}/F_i ציקליים.

טענה 3.3.14 יהי $f\in\mathbb{Q}[\lambda]$ פולינום אי־פריק ממעלה ראשונית p, שיש לו בדיוק שני שורשים לא־ממשיים. אז חבורת גלואה של שדה הפיצול שלו היא S_p.

הוכחה. יהי K שדה הפיצול, ותהי $G=\mathrm{Gal}(K/F)$ חבורת גלואה. לפי מסקנה 2.5.10 החבורה פועלת טרנזיטיבית על השורשים, ולכן המייצב של שורש הוא תת־חבורה מאינדקס p. מכאן שהסדר של G מתחלק ב־p, ולפי משפט קושי יש בה איבר מסדר p; אבל האוטומורפיזם הוא איבר ב־S_p, ושם הוא מהווה מחזור באורך p. מאידך, G כוללת את פעולת ההצמדה המרוכבת, שהיא חילוף של שני שורשים לפי ההנחה. כל תת־חבורה של S_p הכוללת חמוזר באורך p וחילוף כוללת את כל החילופים, ולכן שווה ל־S_p. □

תרגיל 3.3.15 (**) חבורת גלואה של שדה הפיצול של $\lambda^5 - 10\lambda - 5$ היא S_5. מכאן שפולינום זה אינו פתיר על־ידי רדיקלים.

הערה 3.3.16 הילברט הוא שהוכיח שיש פולינומים מעל $\mathbb{Q}$ עם חבורת גלואה השווה ל־S_n לכל n. ההוכחה של הילברט מבוססת על ספציאליזציה של השורשים הגנריים, בקשר לנסיון שלו לתקוף את בעיית נתר.

מסקנה 3.3.17 אין נוסחה לפתרון משוואה ממעלה חמישית או יותר.

לכל ראשוני $p > 2$, נבנה פולינום אי־פריק ממעלה p מעל $\mathbb{Q}$, שיש לו בדיוק $p-2$ שורשים ממשיים (לפי הצעה של אוהד קליין, 2013).

טענה 3.3.18 יהי $f \in \mathbb{R}[x]$ פולינום שיש לו m מונומים; אז יש לו לכל היותר $2m-1$ שורשים ממשיים. יתרה מזו אם אחד המונומים של f הוא המקדם החופשי, אז יש ל־f לכל היותר $2m-2$ שורשים ממשיים.

הוכחה. באינדוקציה על m ועל מעלת הפולינום. הטענה נכונה ל־$m = 1$. יהי f פולינום עם m מונומים; בתחילה נניח שאחד מהם הוא המקדם החופשי. אז לנגזרת f' יש $m-1$ מונומים, ולפי הנחת האינדוקציה יש ל־f' לכל היותר $2m-3$ שורשים; לפי משפט רול, ל־f יש לכל היותר $2m-2$ שורשים. אם המקדם החופשי של f הוא אפס, אפשר לכתוב $f = x^i g$ כאשר המקדם החופשי של g אינו אפס, ואז ל־g יש עד $2m-2$ שורשים לפי הנחת האינדוקציה, ולכן ל־f לכל היותר $2m-1$ שורשים. □

טענה 3.3.19 יהי $n = 2m+3$ מספר אי־זוגי. נסמן $c = \frac{2m(m+1)(2m+1)}{3}$. אז לפולינום

$$f(x) = (x^2 + c)\prod_{k=-m}^{m}(x - 2k) + 2,$$

שמעלתו n, יש בדיוק $n-2$ שורשים ממשיים, והוא אי־פריק מעל $\mathbb{Q}$.

הוכחה. ראשית, $f(x)$ אי־פריק מעל $\mathbb{Q}$ לפי קריטריון אייזנשטיין, לפי בחינת המקדמים מודולו 2.
לפולינום המתוקן

$$h(x) = (x^2 + c)\prod_{k=-m}^{m}(x - 2k) = (x^2 + c)\prod_{k=1}^{m}(x^2 - (2k)^2)$$

יש מעלה $2m+2$, וכל המונומים שלו ממעלה זוגית; לכן יש לו לכל היותר $m+2$ מונומים; אבל בחירת $c = 4\sum_{k=1}^{m} k^2$ מבטיחה שהמקדם של x^{2m} הוא אפס, כך שיש רק $m+1$ מונומים.
מכאן של־$f(x) = xh(x) + 2$ יש לכל היותר $m+2$ מונומים, ולפי טענה 3.3.18 פירושו של דבר לכל היותר $2m+2 = n-1$ שורשים ממשיים. מכאן שיש שורש מרוכב α שאינו ממשי, אבל גם הצמוד $\bar{\alpha}$ הוא שורש, ומכאן שיש לכל היותר $n-2$ שורשים ממשיים.

מאידך, יהי $i = -m, \ldots, m$. לכל $k = -m, \ldots, m$, $2i + 1 - 2k < 0$ בדיוק כאשר $i < k \leq m$, כלומר $m - i$ פעמים. לכן ל־

$$f(2i+1) = (2i+1)((2i+1)^2 + c) \prod_{k=-m}^{m} (2i+1-2k) + 2$$

יש הסימן של $(-1)^{m-i}$. יחד עם העובדה ש־$\lim_{x\to-\infty} f(x) = -\infty$, יש כאן $2m+1 = n-2$ חילופי סימן, ולפי משפט ערך הביניים לפחות $n-2$ שורשים. □

3.4 בניות במחוגה וסרגל והבעיות של ימי קדם

בגאומטריה של יוון העתיקה היה מקובל להשתמש (ברוב המקרים) רק במחוגה ובסרגל. היוונים הקדמונים הציגו ארבע בעיות בניה שנותרו לא פתורות עד ראשית המאה ה־19: הכפל את הקוביה (הכפלת המזבח של אפולו באתונה); שילוש הזווית; ריבוע המעגל; בניית מצולע משוכלל בן שבע צלעות.

בעיה גאומרטית חשובה עוד יותר, הוכחת אקסיומת המקבילים, הוכחה כבלתי אפשרית בדרכים אחרות כאשר לובצ'בסקי, בוליי וגאוס בנו גאומטריות לא אוקלידיות.

בסעיף זה נראה שלא ניתן לפתור שלוש מארבע הבעיות. חוסר האפשרות לרבע את המעגל תלוי במשפט של לינדמן (1882), ש־π אינו אלגברי (שאותו לא נוכיח).

3.4.1 בניות במחוגה וסרגל

המחוגה מאפשרת לסרטט מעגל ברדיוס נתון שמרכזו נתון, והסרגל מאפשר להעביר את הישר העובר דרך שתי נקודות. לכל שני קוים נחתכים (ישרים או מעגלים) אפשר לסמן את נקודות החיתוך. נציג כמה בניות יסודיות במחוגה וסרגל.

טענה 3.4.1 את הבניות הבאות אפשר לבצע במחוגה וסרגל:

1. העברת אנך אמצעי לקטע נתון.
2. למצוא את נקודת האמצע של קטע.
3. הורדת אנך לישר דרך נקודה.
4. העלאת אנך לישר בנקודה נתונה.
5. העברת ישר מקביל לקטע נתון דרך נקודה נתונה. **הדרכה.** הורדת אנך והעלאת אנך.
6. לחצות זווית. **הדרכה.** חציית המרחק בין שתי נקודות החיתוך של צלעות הזווית עם מעגל שמרכזו בקודקודה.

תרגיל 3.4.2 (**) הראה כיצד לבנות במחוגה וסרגל:

1. ישר משיק למעגל דרך נקודה נתונה. **הדרכה**. העבר את המעגל שהקטע ממרכז המעגל הנתונה אל הנקודה הנתונה הוא קוטר שלו.

2. קטע השווה באורכו לקטע נתון ומונח על ישר נתון.

3. זווית השווה לזווית נתונה שקודקודה נתון וצלע אחת שלה נתונה.

יש גם בניות קשות בהרבה. למשל, העברת המשיקים המשותפים לשני מעגלים או מעגל משיק לשלושה מעגלים נתונים.

3.4.2 שדה המספרים הניתנים לבניה

נקבע במישור (המרוכב) זוג נקודות, 0 ו־1, ונשחק את המשחק האינדוקטיבי הבא: מותר לבנות ישר אם הוא עובר דרך שתי נקודות קיימות, מעגל אם מרכזו קיים והוא עובר דרך נקודה אחרת, ונקודה אם היא בחיתוך שני ישרים, שני מעגלים או ישר ומעגל. לאוסף הנקודות המתקבלות באופן הזה נקרא A, **שדה המספרים הניתנים לבניה**. לישר דרך 0 ו־1 נקרא $\mathbb{R}$.

טענה 3.4.3 במחוגה וסרגל אפשר

1. לחבר שני מספרים ממשיים.
2. להכפיל שני מספרים ממשיים.
3. לחשב את ההפכי של מספר ממשי.
4. להוציא שורש ממספר ממשי חיובי.

משפט 3.4.4 *החיתוך $A \cap \mathbb{R}$ הוא תת־שדה של $\mathbb{R}$, הסגור להוצאת שורש ממספרים חיוביים. זהו תת־השדה הקטן ביותר של $\mathbb{R}$ בעל תכונות אלו.*

טענה 3.4.5 במחוגה וסרגל אפשר

1. לחבר שני מספרים מרוכבים.
2. להכפיל שני מספרים מרוכבים.
3. לחשב את ההפכי של מספר מרוכב.
4. להוציא שורש ממספר מרוכב.

משפט 3.4.6 *אוסף הנקודות הניתנות לבניה, A, הוא תת־שדה של $\mathbb{C}$, הסגור להוצאת שורש. זהו תת־השדה הקטן ביותר של $\mathbb{C}$ בעל תכונות אלו.*

הוכחה. מיידי מטענה 3.4.5 וההגדרה. □

משפט 3.4.7 *התכונות הבאות של תת־שדה $E \subseteq \mathbb{C}$ שקולות:*

1. *E סגור להרחבות ריבועיות.*
2. *$E \cap \mathbb{R}$ סגור להוצאת שורש ריבועי של איבר חיובי, ו־ $E = (E \cap \mathbb{R})[i]$.*

(שדה נקרא **פיתגורי** אם כל סכום של שני ריבועים הוא ריבוע. שדה סדור נקרא **אוקלידי** אם כל איבר חיובי הוא ריבוע.)

3.4.3 שרשראות של הרחבות ריבועיות

אומרים ש־K הוא הרחבה ריבועית חוזרת של F אם קיימת שרשרת $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ של הרחבות ריבועיות.

למה 3.4.8 אם K/F הרחבה ריבועית חוזרת שהיא גלואה, אז כל שדה ביניים $F \subseteq L \subseteq K$ הוא הרחבה ריבועית חוזרת של K.

הוכחה. נכתוב $G = \mathrm{Gal}(K/F)$ ו־ $L = K^H$. כחבורת־2, G פתירה. תהי

$$1 \subseteq G_{n-1} \subseteq G_{n-2} \subseteq \cdots \subseteq G_1 \subseteq G_0 = G$$

סדרת הרכב, כלומר $G_i/G_{i-1} \cong \mathbb{Z}/2\mathbb{Z}$ לכל i.
קח $L_i = K^{HG_i}$. לכל i, $HG_{i-1}/HG_i \cong G_{i-1}/(G_{i-1} \cap HG_i)$ חבורת מנה של G_{i-1}/G_i, ולכן $[L_i\,{:}\,L_{i-1}] = [HG_{i-1}\,{:}\,HG_i] \,|\, [G_{i-1}\,{:}\,G_i] = 2$. □

למה 3.4.9 אם K, K' שדות ביניים של E ו־ K/F, K'/F הרחבות ריבועיות חוזרות, אז ההרכבה KK'/F היא הרחבה ריבועית חוזרת.

הוכחה. תהי $F \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ שרשרת של הרחבות ריבועיות. אז גם $K' = FK' \subseteq K_1K' \subseteq \cdots \subseteq K_nK' = KK'$ שרשרת כזו לפי טענה 2.5.19, ואיתה אפשר להמשיך שרשרת מ־F ל־K עד KK'. □

למה 3.4.10 אם K/F הרחבת ריבועית חוזרת, אז סגור־גלואה שלה, E/F, גם הוא הרחבה ריבועית חוזרת.

הוכחה. לפי הגדרת סגור גלואה, E נוצר על־ידי עותקים איזומורפיים של K, ולכן הטענה נובעת מלמה 3.4.9 באינדוקציה על מספר הצמודים. □

תרגיל 3.4.11 (**) בלמה 3.4.10, חסום את $[E\,{:}\,F]$ במונחי $[K\,{:}\,F]$.

משפט 3.4.12 *התכונות הבאות שקולות עבור $a \in \mathbb{C}$:*

1. *a שייך לשדה A של המספרים הניתנים לבניה.*

2. *a שייך להרחבה ריבועית חוזרת של $\mathbb{Q}$.*

3. *a שייך להרחבה ריבועית חוזרת שהיא גלואה מעל $\mathbb{Q}$.*

4. *$\mathbb{Q}[a]$ הוא הרחבה ריבועית חוזרת של $\mathbb{Q}$.*

5. *חבורת גלואה של הפולינום המינימלי של a היא חבורת־2.*

הוכחה. (1) $\Leftarrow$ (2) כי כל האברים ב־A נבנים. (2) $\Leftarrow$ (3) לפי למה 3.4.10. (3) $\Leftarrow$ (4) לפי למה 3.4.8. (4) $\Leftarrow$ (1) לפי הערה 3.3.2, כי אפשר להוציא ב־A שורשים.

(5) $\Leftarrow$ (2) בעזרת סדרת הרכב של חבורת גלואה. (3) $\Leftarrow$ (5) הסדר של חבורת גלואה שווה לממד ההרחבה שהוא חזקת 2. □

מסקנה 3.4.13 השדה A של המספרים הניתנים לבניה הוא איחוד של הרחבות גלואה סופיות.

אם a ניתן לבניה, אז $[\mathbb{Q}[a]:\mathbb{Q}]$ הוא חזקה של 2. ההיפך אינו נכון. לפי משפט 3.4.12, אם $a \in \mathbb{C}$ יוצר שדה שאינו הרחבה ריבועית חוזרת של $\mathbb{Q}$, אז הוא אינו ניתן לבניה. לפי למה 3.4.10, אם a שורש של פולינום אי־פריק ממעלה 4, $f \in \mathbb{Q}[\lambda]$, ולשדה הפיצול של f חבורת גלואה S_4 או A_4, אז a אינו ניתן לבניה למרות ש־ $[\mathbb{Q}[a]:\mathbb{Q}] = 4$.

3.4.4 בניית מצולעים משוכללים

תרגיל: אפשר לבנות את $\cos(\alpha)$ אם ורק אם אפשר לבנות את $\sin(\alpha)$ אם ורק אם אפשר לבנות את $\cos(\alpha) + i\sin(\alpha)$.

מסקנה 3.4.14 אפשר לבנות את שורשי היחידה מסדר n אם ורק אם $\phi(n)$ הוא חזקת 2. כלומר, אם ורק אם $n = 2^t p_1 \cdots p_t$ כאשר כל p_i הוא ראשוני מהצורה $2^m + 1$.

תרגיל 3.4.15 (*) אם p הוא ראשוני מהצורה $2^m + 1$, אז הוא למעשה מהצורה $2^{2^m} + 1$. ראשוני כזה קרוי **ראשוני פרמה**. ראשוניי פרמה היחידים הידועים הם $3, 5, 17, 65537$.

תרגיל 3.4.16 (***) הראה ש־

$$\cos\left(\frac{2\pi}{17}\right) = \frac{\frac{\sqrt{17}-1}{2} + \sqrt{\frac{17-\sqrt{17}}{2}} + \sqrt{(3+\sqrt{17})\left(\sqrt{17} - \sqrt{\frac{17-\sqrt{17}}{2}}\right)}}{8}.$$

הסבר כיצד לבנות בעזרת מידע זה מצולע משוכלל בן 17 צלעות.

ב־Introduction to Geometry מספר Coxeter שמתמטיקאי בשם Hermes בילה כ־10 שנים (בסביבות 1900) בבניה של מצולע בן 65537 צלעות.

(ראו תרגילים על פולינומי צ'ביצב בחוברת התרגילים שלי.)

מסקנה 3.4.17 אי־אפשר לבנות משובע משוכלל.

3.4.5 הבעיות הגאומטריות של ימי קדם

הכפלת הקוביה בלתי אפשרית כי $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ מממד 3. אי־אפשר לבנות את $\cos(20°)$, כי זה שורש לפולינום האי־פריק $8x^3 - 6x - 1$. לכן אי אפשר לשלש את הזווית. (הראשון שהוכיח שאי־אפשר לשלש זווית היה Pierre Laurent Wantzel (1814–1869), ב־1837.)

ריבוע המעגל בלתי אפשרי כי π טרנסצנדנטי.

3.4.6 אוריגמי

יותר אקסיומות. ביון השאר אפשר למצוא משיק משותף לשתי פרבולות: "בהינתן שתי נקודות, P_1 ו־P_2, ושני קווים, L_1 ו־L_2, ניתן ליצור (בתנאים מסוימים) קפל שימקם בו־זמנית את נקודה P_1 על גבי L_1 ואת נקודה P_2 על גבי L_2" (הערה: המשיק לפרבולה שמדריכה L ומוקדה P הוא הקו המשקף את P אל L).

לדוגמה, כך אפשר למצוא את השורש השלישי של מספר באמצעות קיפולי נייר: ציירו מערכת צירים מאונכת על הדף; סמנו את הנקודות $(0,2)$ ו־ $(a,1)$. כעת הפעילו את האקסיומה כדי למצוא קפל המעתיק את הנקודה הראשונה על ציר ה־ x, ואת הנקודה השנייה על הישר $x=-a$. שיקוף כזה מעתיק את הנקודה $(0,2)$ לנקודה שמרחקה מראשית הצירים בדיוק $2a^{1/3}$.

3.5 שדות סופיים

לכל ראשוני p קיים שדה $\mathbb{F}_p$ מסדר p. השאלה היא מהם הסדרים האפשריים האחרים לשדה, וכמה שדות יש מכל סדר.

סדר. יהי F שדה סופי. אז המאפיין שלו סופי, ולכן F הרחבה של $\mathbb{F}_p$ עבור ראשוני p מתאים. מכיוון ש־ $n=[F:\mathbb{F}_p]$ סופי, $F \cong \mathbb{F}_p^n$ כמרחב וקטורי, ולכן $|F|=p^n$.

קיום. יהי $q=p^n$ חזקת ראשוני. יהי F שדה הפיצול של $\lambda^q - \lambda$ מעל $\mathbb{F}_p$. זהו פולינום ספרבילי, ולכן יש לו q שורשים. נסמן $F_0 = \{a \in F:\ a^q = a\}$ ־ קבוצת השורשים של הפולינום. אז $|F_0| = q$. לפי הערה 2.2.2, F_0 סגור לחיבור, והוא הרי סגור לכפל; לכן F_0 שדה מסדר q. (מכאן נובע גם ש־$F = F_0$).

יחידות. יהי F שדה מסדר $q = p^n$. כל האיברים של F מקיימים $a^q - a = 0$, כי החבורה הכפלית של F היא בגודל $q-1$. אבל לפולינום יש לכל היותר q שורשים, ולכן $\lambda^q - \lambda = \prod_{a\in F}(\lambda - a)$. מכאן ש־$F$ שדה הפיצול של $\lambda^q - \lambda$ מעל $\mathbb{F}_p$.

הכלה. נניח ש־$n \,|\, m$. אז $t^n - 1 \,|\, t^m - 1$, ובפרט $p^n - 1 \,|\, p^m - 1$. לכן גם $\lambda^{p^n-1} - 1 \,|\, \lambda^{p^m-1} - 1$ ומכאן $\lambda^{p^n} - \lambda \,|\, \lambda^{p^m} - \lambda$. לכן השדה מסדר n מוכל בשדה מסדר m, ויש לו עותק יחיד שם.

גלואה. כל הרחבה של שדות סופיים היא שדה פיצול של פולינום ספרבילי $\lambda^q - \lambda$, ולכן גלואה. בפרט, ההרחבה ספרבילית.

אוטומורפיזם פרובניוס. יהיו K/F שדות עם K סופי; נסמן $q = |F|$. הפעולה $\phi: x \mapsto x^q$ היא אוטומורפיזם של K. אם $|K| = q^d$, אז $\phi^d = 1$ על K, וזה אינו

נכון לאף חזקה קטנה יותר. לכן $\langle\phi\rangle$ היא חבורה של $d=[K:F]$ אוטומורפיזמים של K. לכן $\mathrm{Gal}(K/F)=\langle\phi\rangle$. כלומר: כל ההרחבות של שדות סופיים הן הרחבות גלואה ציקליות.

דוגמא 3.5.1 העלאה בחזקת p היא שיכון של $F \to F$ שאינו תמיד על. למשל, עבור $F=\mathbb{F}_p(\lambda)$, $F^p=F_p(\lambda^p)$ הוא תת־שדה מקו־ממד p.

פירוק לגורמים של פולינומים: אם $f(\lambda)\in\mathbb{F}_q[\lambda]$, $(f,\lambda^{q^m}-\lambda)$ הוא מכפלת הגורמים של f שמעלתם מחלקת את m. לאחר סילוק גורמים חוזרים בעזרת (f,f'), אפשר לכתוב $\mathbb{F}_q[\lambda]/\langle f\rangle\cong\prod L_i$ מכפלה של שדות, ואם f פריק יש לפחות נקודת שבת לא טריוויאלית אחת h של אנדומורפיזם פרובניוס. כעת $f=\prod(f,h-\alpha)$ פירוק לא טריוויאלי.

פרק 4

נושאים נוספים בתורת השדות

4.1 הרחבות אלגבריות

הרחבה E/F היא **הרחבה אלגברית** אם כל האיברים של E הם אלגבריים מעל F (הגדרה בתת־סעיף 1.2.4).

4.1.1 הרחבה נוצרת סופית

ההרחבה E/F נוצרת סופית אם יש קבוצה סופית $S \subset E$ כך ש־ $E = F(S)$.

משפט 4.1.1 *התכונות הבאות של הרחבה K/F שקולות:*

1. *ההרחבה ממַמד סופי.*
2. *ההרחבה אלגברית ונוצרת סופית.*
3. *ההרחבה נוצרת על־ידי מספר סופי של איברים אלגבריים.*

הוכחה. 1 $\Longleftarrow$ 2 $\Longleftarrow$ 3 קל, ו־ 3 $\Longleftarrow$ 1 לפי מסקנה 1.2.21. $\square$

מסקנה 4.1.2 הרחבה הנוצרת על־ידי מספר סופי של איברים אלגבריים היא אלגברית.

מסקנה 4.1.3 אם a, b אלגבריים, אז $a + b$, $a \cdot b$ ו־a^{-1} אלגבריים, משום שאלו אברים ב־ $F[a, b]$.

מסקנה 4.1.4 הרחבה אלגברית נוצרת סופית של הרחבה אלגברית נוצרת סופית היא אלגברית נוצרת סופית.

4.1.2 אלגבריות ויוצרים

המסקנות מתת־הסעיף הקודם נכונות גם בהרחבות שאינן נוצרות סופית.

הערה 4.1.5 אם $K = F(S)$ אז לכל $b \in K$ יש תת־קבוצה סופית $S_0 \subseteq S$ כך ש־ $b \in F(S_0)$.

לכן הרחבה הנוצרת על־ידי קבוצה כלשהי של איברים אלגבריים היא אלגברית.

טענה 4.1.6 הרחבה אלגברית של הרחבה אלגברית היא אלגברית. (קח K_0 להיות השדה הנוצר על־ידי מקדמי הפולינום המינימלי של b מעל K.)

4.1.3 סגור אלגברי יחסי

אוסף האיברים האלגבריים בהרחבה E/F הוא שדה לפי מסקנה 4.1.3. נקרא **הסגור האלגברי** של F בתוך E.

E/F אלגברית אם ורק אם הסגור האלגברי של F ב־E שווה ל־E.

אם הסגור האלגברי של F ב־E שווה ל־F, אומרים ש־F **סגור אלגברית** ב־E (שימו לב שזוהי סגירות אלגברית יחסית; המושג 'שדה סגור אלגברית' יוגדר בהמשך).

דוגמא 4.1.7 ההרחבה $F(\lambda)/F$ טרנסצנדנטית טהורה.

לפי טענה 4.1.6, הסגור האלגברי של F בתוך E סגור אלגברית ב־E.

מסקנה 4.1.8 כל הרחבה E/F אפשר לפרק ל־ $F \subseteq L \subseteq E$, כאשר L/F אלגברית ו־L סגור אלברית ב־E/L.

דוגמא 4.1.9 שדה המספרים האלגבריים הוא הסגור האלגברי של $\mathbb{Q}$ בתוך $\mathbb{C}$ (הוא אינו נוצר סופית).

4.1.4 שדה סגור אלגברית

משפט 4.1.10 *התנאים הבאים שקולים עבור שדה E:*

1. *לכל פולינום מעל E יש בו שורש.*
2. *כל פולינום מעל E מתפצל שם.*
3. *אין ל־E הרחבות אלגבריות אמיתיות.*
4. *אין ל־E הרחבות סופיות אמיתיות.*
5. *כל הפולינומים האי־פריקים הם ליניאריים.*

הוכחה. $(3) \Leftarrow (4) \Leftarrow (5) \Leftarrow (2) \Leftarrow (1) \Leftarrow (5) \Leftarrow (3)$. □

שדה המקיים תכונות אלה נקרא **סגור אלגברית**.

4.1.5 הסגור האלגברי של שדה

הגדרה 4.1.11 **סְגור אלגברי** של F הוא הרחבה אלגברית E/F כך ש־ E סגור אלגברית.

למה 4.1.12 אם E/F הרחבה אלגברית ו־E מפצל את כל הפולינומים מעל F, אז E סגור אלגברית.

הוכחה. תהי E_1/E הרחבה אלגברית, ויהי $\alpha \in E_1$. לפי טענה 4.1.6 $E[\alpha]$ אלגברי מעל F. הפולינומים המינימלי $f \in F[\lambda]$ של α מעל F מתפצל ב־E ולכן $\alpha \in E$. □

שאלה 4.1.13 אם $F \subseteq E$ הרחבה אלגברית ויש ב־E שורש לכל פולינום מעל F, האם E סגור אלגברית?

למה 4.1.14 לכל שדה F יש הרחבה אלגברית E/F עם שורש ב־E לכל פולינום מעל F.

הוכחה (ארטין). לכל פולינום מתוקן $f \in F[\lambda]$ נצמיד משתנה t_f, ונתבונן בחוג $R = F[t_f]$ הנוצר על־ידי כל המשתנים האלה. יהי I האידיאל הנוצר על־ידי כל האיברים $f(t_f)$.

נראה ש־ I אידיאל אמיתי, כלומר $1 \not\in I$. אחרת $\sum h_f f(t_f) = 1$ עבור איברים $h_f \in R$. בסכום הזה משתתף מספר סופי של פולינומים, ולכן (טענה 1.2.26) קיימת הרחבה K של F שבה יש לכולם שורש. נגדיר העתקה $R \to K$ השולחת כל t_f מאלה לשורש כזה, ושולחת את t_g לאפס אם g אינו משתתף בסכום. מתקבל $0 = 1$, סתירה להנחה. לכן I אידיאל אמיתי.

לפי הלמה של צורן, קיים אידיאל מקסימלי M המכיל את I. אז $\bar{F} = R/M$ שדה, ו־ $F = F/(F \cap M) \cong (F+M)/M \subseteq R/M$. לכל פולינום f יש שורש $t_f + M$ בשדה $\bar{F}$. □

משפט 4.1.15 *לכל שדה F יש סגור אלגברי.*

הוכחה. נסמן $F_0 = F$. לפי הלמה, לכל $n \geq 0$ קיימת הרחבה אלגברית F_{n+1}/F_n, שיש בה שורש לכל פולינום מעל F_n. האיחוד $E = \cup F_n$ הוא שדה (הערה 1.2.5) סגור אלגברית, ואלגברי מעל F (הערה 4.1.6). □

4.1.6 יחידות הסגור האלגברי

משפט 4.1.16 *יהי $F \hookrightarrow \hat{F}$ שיכון בתוך שדה סגור אלגברית. לכל הרחבה אלגברית K/F_0 ושיכון $F_0 \hookrightarrow F$, יש המשכה של $F_0 \hookrightarrow \hat{F}$ אל $K \hookrightarrow \hat{F}$.*

הוכחה. אם K/F_0 נוצרת סופית התוצאה נובעת ממשפט 2.1.8.2(א). למקרה הכללי נחוצה הלמה של צורן. נסמן ב־ Λ את אוסף הזוגות (K_0, ϕ) כאשר $F_0 \subseteq K_0 \subseteq K$ ו־ $\phi : K_0 \hookrightarrow \hat{F}$ שיכון, מסודר לפי $(K_0, \phi) \leq (K_0', \phi')$ אם $K_0 \subseteq K_0'$ ו־ $\phi'|_{K_0} = \phi$. הקבוצה אינה ריקה כי $(F_0, \hookrightarrow)$ שם. לפי הלמה של צורן יש ב־Λ איבר מקסימלי,

(K_1,ϕ_1). אם $K_1 \subset K$ אז יש הרחבה פשוטה $K_1 \subset K_2 = K_1[\alpha] \subseteq K$, אבל אז לפי מסקנה 2.1.7.2 יש ל־ϕ_1 הרחבה אל K_2, בסתירה למקסימליות. לכן $K = K_1$ משוכן ב־ $\hat{F}$. □

מסקנה 4.1.17 סגור אלגברי $\bar{F}/F$ משכן בתוכו עותק של כל הרחבה אלגברית של F.

משפט 4.1.18 *לכל שדה F יש סגור אלגברי יחיד עד כדי איזומורפיזם.*

הוכחה. אם $\bar{F}, \bar{F}'$ סגורים אלגבריים של F, אז לפי המשפט הקודם יש שיכון $\bar{F} \hookrightarrow \bar{F}'$, אבל $\bar{F}$ אלגברי מעל F ולכן גם מעל תמונת $\bar{F}'$, והרי תמונה זו סגורה אלגברית. □

מסקנה 4.1.19 יהי $F \hookrightarrow K$ שיכון של שדות, אז יש גם שיכון $\hat{F} \hookrightarrow \hat{K}$.

הוכחה. מכיוון ש־$\hat{F}/F$ אלגברית, זהו משפט 4.1.16 עם $F, \hat{F}, K$ בתפקידי F_0, K, F בהתאמה. □

תרגיל 4.1.20 (**) הוכח את מסקנה 4.1.19 ישירות, על־ידי הוכחת למה 4.1.14 במקביל עבור F ו־K.

4.2 הרחבות טרנסצנדנטיות

תהי E/F הרחבת שדות. קבוצת איברים $S \subseteq E$ היא 'בלתי תלויה אלגברית' מעל F אם לא קיימים פולינום $0 \neq f \in F[\lambda_1,\dots,\lambda_n]$ ואיברים שונים $s_1,\dots,s_n \in S$ כך ש־ $f(s_1,\dots,s_n) = 0$. במקרה כזה, ההרחבה $F(S)/F$ נקראת טרנסצנדנטית טהורה.

בסעיף 4.1.3 ראינו שלכל הרחבת שדות E/F יש הרחבת ביניים $F \subseteq K \subseteq E$ כך ש־ K/F אלגברית ו־K סגור אלגברית בתוך E. ההרחבה E/K עלולה להיות מסובכת (קחו למשל את $k(\lambda,\mu \,|\, \mu^2 = \lambda^3+1)$ מעל k), ובדרך כלל שימושי יותר להפוך את הסדר ולבצע קודם כל את ההרחבה הלא־אלגברית.

טענה 4.2.1 לכל הרחבה נוצרת סופית E/F יש הרחבת ביניים $F \subseteq E_0 \subseteq E$ כך ש־ E_0/F טרנסצנדנטי טהור ו־ E/E_0 אלגברית.

הוכחה. כך יהיה אם ניקח את S_0 להיות תת־קבוצה בלתי תלויה אלגברית מקסימלית. □

(להגדיר דרגת טרנסצנדנטיות, ולהוכיח שמוגדרת היטב)

4.2.1 פונקציות סימטריות

נתבונן בשדה $K = k(t_1,\dots,t_n)$, הרחבה טרנסצנדנטית טהורה של k. יש פעולה של S_n על K לפי החלפת משתנים; ברור ש־ $[K:K^{S_n}] = |S_n| = n!$.

נסמן $s_k = \sum_{i_1<\cdots<i_k} t_{i_1}\cdots t_{i_k}$, וניקח $L = k(s_1,\dots,s_n)$. כעת, $f(\lambda) = \prod(\lambda - t_i) \in L[\lambda]$, ולכן $[L[t_1]:L] \leq n$. באופן כללי יותר, הפולינום המינימלי של t_{i+1} מעל $L[t_1,\dots,t_i]$ מחלק את $\prod_{j\leq i}(\lambda - t_j)^{-1} f(\lambda)$, ולכן $[L[t_1,\dots,t_{i+1}]:L[t_1,\dots,t_i]] \leq n-i+1$. באינדוקציה, הממד של $K = L[t_1,\dots,t_n]$ מעל L אינו עולה על $n!$. אבל $L \subseteq K^{S_n}$, ולכן $L = K^{S_n}$.

מסקנה: כל פונקציה סימטרית היא פונקציה של ה־$s_1,\dots,s_n$. למעשה, מכיוון שדרגת הטרנסצנדנטיות של K היא n ו־ L/K אלגברי, $\operatorname{trdeg}(L) = n$ ולכן ה־ $s_1,\dots,s_n$ בלתי תלויים אלגברית. לכן ההצגה של איבר כפונקציה של הפונקציות הסימטריות האלמנטריות היא יחידה.

כעת תהי $G \leq S_n$. אז $L \subseteq K^G \subseteq K$ ולהרחבה K/K^G יש חבורת גלואה G. ברור ש־ K הוא שדה הפיצול של $f(\lambda)$ דלעיל מעל K^G, עם חבורת גלואה G. לכן, לכל תת־חבורה G של S_n, יש פולינום ממעלה n ש־ G חבורת גלואה של שדה הפיצול שלה. אם החבורה טרנזיטיבית, אז הפולינום אי־פריק כי יש אוטומורפיזם שמחליף כל שני שורשים.

בעיית נתר: האם K^G טרנסצנדנטי טהור. דוגמאות כמו S_n, A_n, C_n כאשר $\rho_n \in k$.

בעיית ההיפוך של תורת גלואה: האם אפשר לממש כל חבורה G מעל $\mathbb{Q}$ (התשובה חיובית למשל מעל $\mathbb{C}(t)$).

(מימוש כל חבורה סופית כחבורת גלואה.)

4.2.2 הרחבות מדרגה 1

הממד $[F(\lambda):F(f/g)] = \max\{\deg(f), \deg(g)\}$.

משפט לורות' (עמ' 157 ב־LAAIII): כל שדה ביניים של $F \subseteq F(\lambda)$ הוא מהצורה $F(f/g)$ עבור $f,g \in F[\lambda]$. להסיק שחבורת האוטומורפיזמים של $F(\lambda)/F$ היא $\mathrm{PGL}_2(F)$.

4.3 נושאים נוספים

להלן כמה נושאים שיכולנו לכסות במסגרת הקורס:

1. חבורות פרו־סופיות וחבורות גלואה האבסולוטית.
2. שדות מקומיים.
3. המשפט היסודי של האלגברה - שדה המספרים המרוכבים סגור אלגברית. תרגום ההוכחה לשפה של הרחבות שדות.

4. בעיית ההיפוך של תורת גלואה.
5. מבוא לפולינומים סימטריים (נוסחאות ניוטון).
6. שדות סדורים: פיתגוריות, אוקלידיות, שדה סגור ממשית. שדות שלמים (לפי סדרות ולפי חתכים).