אוניברסיטת תל אביב
הפקולטה למדעים מדויקים על שם ריימונד ובברלי סקלר
בית הספר למתמטיקה

הרחבות מעין סגורות אלגברית

חיבור לקבלת תואר "דוקטור לפילוסופיה"

מאת
ליאור ברי־סורוקר

בהנחיית
פרופסור דן הרן

מוגש לסנאט של אוניברסיטת תל אביב
אלול תשס"ח

הנה העצים במלמול עליהם
הנה האויר הסחרחר מגובה
אינני רוצה
לכתוב עליהם
רוצה בליבם לנגוע

תודות:

ראשית אני רוצה להודות למנחי פרופסור דן הרן. תודה על שהצגת בפני את התחום הנפלא של תורת גלואה, על היחס החם, העזרה והתמיכה שכה הזדקקתי לה במתמטיקה ובכל שאר הנושאים שמסביב.

אני שמח להודות לפרופסור משה ירדן על תמיכתו הרבה שגרמה לי להרגיש כאילו אני תלמידו.

תודה לפרופסור מרצל הרצוג על שיחות מתמטיות.

לחברים שלי מהמחלקה אני מודה רבות על שיחות מעניינות ועל כך שתמיד היה עם מי לשתות קפה. במיוחד אני מודה לאלי להר, שחף ניצן־חכמוב, סשה סודין, אלעד פארן, ארנו פס, דובי קלמר, ליאור רוזנצויג וכל מי ששכחתי.

לבסוף, זה עונג להודות למשפחתי: להורי שלומית ויורם, לאחיי גגי, רן ושי, להורים של חמוטל נחום ודגנית, ולבסוף לחמוטל שלי.

תוכן עניינים

פרק 1

מבוא

1.1 רקע ומוטיבציה

1.1.1 הבעיה העשירית של הילברט

בבעיתו העשירית שואל הילברט האם קיים אלגוריתם כללי שמכריע האם למשוואה אלגברית עם מקדמים שלמים יש פתרון בשלמים. בשנת 1972 הראה Matijasevich שאין אלגוריתם כזה ובכך ענה בשלילה על הבעיה. עבודתו התבססה על עבודות קודמות החל משנות ה 30 של Davis, Putnam ו J. Robinson.

בעקבות התפתחויות אלו, רובינסון שאלה האם הבעיה העשירית של הילברט נכונה עבור חוג השלמים האלגברים $\tilde{\mathbb{Z}}$. ואכן בשנת 1987 Rumely מצא אלגוריתם לפתרון משוואות פולינומיאליות מעל $\tilde{\mathbb{Z}}$ בעזרת העקרון המקומי־גלובלי הבא. יהי $\tilde{\mathbb{Q}}$ שדה המספרים האלגברים. אזי לוריעה V מעל $\tilde{\mathbb{Q}}$ יש נקודה שלמה, כלומר $V(\tilde{\mathbb{Z}}) \neq \emptyset$, אם ורק אם ל V יש נקודה שלמה בכל השלמה של $\tilde{\mathbb{Q}}$.

ירדן ורזון הכלילו העקרון המקומי־גלובלי של רומלי לשפע של חוגים אלגברים [17, 18] ובכך ענו בחיוב על הבעיה העשירית של הילברט לחוגים אלו. החידוש המרכזי בעבודתם הינו ההגדרה של הרחבות מעין סגורות אלגברית [16]:

הגדרה 1.1.1 *יהי M שדה ותהי K תת קבוצה. נאמר ש M/K הינו* **הרחבה מעין סגורה אלגברית** *(או לחילופין M מעין סגור אלגברית מעל K) אם לכל פולינום אי פריק לחלוטין $f(T,X) \in M[T,X]$ ופריד ב X קיימים אינסוף $(a,b) \in K \times M$ עבורם $f(a,b) = 0$.*

כאשר לוקחים $K = M$ מכלילה הגדרה זו את ההגדרה הקלאסית של שדות מעין סגורים אלגברית המהווים נושא מרכזי בתחום *אריתמטיקת השדות* (כמה ספרים בנושא הם [8, 21, 34]).

נרצה לתאר יותר בפרוט את התוצאה של ירדן־רזון. יהי K שדה ויהי $e \geq 1$ מספר שלם. עבור e־איה של אוטומורפיזמי גלואה $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ נסמן ב $K_s(\boldsymbol{\sigma}) = \{x \in K_s \mid \sigma_i(x) = x, \ \forall\ i\}$ את שדה השבת של $\boldsymbol{\sigma}$ בסגור פריד K_s

של K ונסמן ב $\langle\boldsymbol{\sigma}\rangle$ את תת החבורה הסגורה של חבורת גלואה המוחלטת $\mathrm{Gal}(K)$ של K הנוצרת על ידי $\sigma_1,\dots,\sigma_e$.

משפט א' *יהי R תחום הילברטי בן מניה, K שדה המנות של R ויהי $e \geq 1$ שלם. אזי $K_s(\boldsymbol{\sigma})/R$ הוא מעין סגור אלגברית והחבורה $\langle\boldsymbol{\sigma}\rangle$ היא חופשית מדרגה e עבור כמעט כל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ (ביחס למידת האר על $\mathrm{Gal}(K)^e$).*

כאן תחום הילברטי הוא תחום שלמות עם התכונה הבאה. לכל $f \in K(X)[Y]$ שהוא אי פריק ופריד ב Y קיים $a \in R$ עבורו $f(a,Y)$ נשאר אי פריק. לדוגמא, חוג השלמים של שדה גלובלי K הוא תחום הילברטי.

תוצאה קלאסית של ירדן [8, משפטים 18.5.6 ו 18.6.1] נותנת ש $K_s(\boldsymbol{\sigma})$ הוא שדה מעין סגור אלגברית וש $\langle\boldsymbol{\sigma}\rangle$ היא חופשית מדרגה e. שאר המשפט, כלומר מעין הסגירות האלגברית של $K_s(\boldsymbol{\sigma})/R$, הוא התוצאה המרכזית במאמר [16].

עתה הכל מוכן לקראת הצגת הרחבת העקרון המקומי־גלובלי של רומלי.

משפט ב' *יהי K שדה גלובלי. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)$ לשדה $M = K_s(\boldsymbol{\sigma})$ יש התכונה הבאה. ליריעה V המוגדרת מעל M יש נקודה שלמה ב M אם ורק אם יש ליריעה נקודה שלמה בכל השלמה (ביחס לאידאלים ראשוניים של חוג השלמים).*

משפט זה הוא מקרה פרטי של [18, משפט 2.5].

1.1.2 קשרים עם תחומים אחרים

עד עתה תארנו את המניע המקורי של ירדן־רזון להגדרת הרחבות מעין סגורות אלגברית. נציין שירדן ורזון שיפרו (וממשיכים לשפר) את משפט ב' בסדרת מאמרים (הגרסה האחרונה נכון לכתיבת שורות אלו מופיעה ב [18]). אולם יישומים נוספים להרחבות מעין סגורות אלגברית אשר אינם קשורים לבעיה העשירית של הילברט ולעקרון המקומי־גלובלי של רומלי החלו להופיע.

שפע שדות הילברטיים

הרחבת גלואה N/K נקראת חסומה אם קבוצת הסדרים $\{\mathrm{ord}(\sigma) \mid \sigma \in \mathrm{Gal}(N/K)\}$ היא חסומה. במאמר [25] רזון משתמש במשפט א', כלומר ריבוי ההרחבות המס"א של שדה הילברטי, כדי למצוא שפע של הרחבות הילברטיות:

משפט ג' *יהי K שדה הילברטי בן מניה ו N/K הרחבה אבלית שאינה חסומה. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ כל תת הרחבה M של $K_s(\boldsymbol{\sigma})N/N$ היא הלברטית.*

שתי התוצאות הבאות מראות שלשדה K עם הרחבה מעין סגורה אלגברית "לא מנוונת" יש כמה תכונות נחמדות. הרעיון המרכזי העומד מאחורי שתי תוצאות אלו הוא ששדה כזה מקיים גרסה חלשה של משפט אי הפריקות של הילברט, כפי שמתואר בהמשך ההקדמה. נתאר בקיצור את התוצאות הללו.

משפט דיריכלה לחוגי פולינומים

האנלוג של Artin-Kornblum למשפט דיריכלה על ראשוניים בסדרות חשבוניות נותן את התוצאה הבאה עבור שדה סופי $\mathbb{F}$.

משפט ד' *לכל $a,b \in \mathbb{F}[X]$ זרים ולכל שלם n גדול מספיק קיים $c \in \mathbb{F}[X]$ כך שהפולינום $a+bc$ הוא אי פריק ממעלה n.*

טבעי לשאול האם משפט דיריכלה תקף עבור חוג פולינומים מעל שדה אינסופי. כמובן שמשפט זה אינו מתקיים עבור $\mathbb{C}$ או $\mathbb{R}$. הבחנה יותר עדינה (אבל עדיין קלה) היא שמשפט דיריכלה תקף עבור שדה הילברטי K (ראה פרק 7). בעבודה זו אנו מוכיחים שמשפט דיריכלה נכון עבור שדה K בתנאי שיש ל K הרחבה מעין סגורה אלגברית מתאימה.

משפט I *יהי K שדה, $a,b \in K[X]$ זרים ו n שלם מספיק גדול. נניח שקיימות הרחבה מעין סגורה אלגברית M/K והרחבה פרידה N/M ממעלה n. אזי קיימים אינסוף $c \in K[X]$ כך ש $a+bc$ הוא אי פריק ממעלה n.*

תוצאה זו הופיעה ב [1].

תבניות עקבה משוקללות

תהי L/K הרחבה פרידה ממעלה n. אזי L מצוידת *בתבנית עקבה* שהינה התבנית הריבועית הלא מנוונת המוגדרת על ידי $x \mapsto \mathrm{Tr}_{L/K}(x^2)$ לכל $x \in L$. *תבנית העקבה המשוקללת* הינה ההכללה הבאה. נקבע $\lambda \in L^\times$. אזי תבנית העקבה המשוקללת (ב λ) היא התבנית הריבועית הלא מנוונת המוגדרת על ידי

$$x \mapsto \operatorname*{Tr}_{L/K}(\lambda x^2),$$

לכל $x \in L$.

Scharlau [30] ו Waterhouse [35] הוכיחו (באופן בלתי תלוי) שמעל שדה הילברטי K כל תבנית ריבועית לא מנוונת איזומורפית לתבנית עקבה משוקללת. ב [3] קלמר והכותב מרחיבים את העבודה של ווטרהאוס־שרלאו לשדות שיש להם הרחבות מעין סגורות אלגברית.

משפט ה' *יהי K שדה. נניח שקיימות הרחבה מעין סגורה אלגברית M/K והרחבה פרידה N/M ממעלה n. אזי כל תבנית ריבועית לא מנוונת ממימד n מעל K איזומורפית לתבנית עקבה משוקללת.*

הערה 1.1.2 *בעקבות שני המשפטים האחרונים התכונה של שדה K שיש לו הרחבה מעין סגורה אלגברית M/K עם הרחבה פרידה N/M ממעלה n מקבלת עניין. בהמשך נתאר כמה משפחות של שדות בעלות תכונה זו עבור הרבה n־ים. לדוגמא הרחבות פרו־פתירות של $\mathbb{Q}$.*

1.2 מבנה גלואה של הרחבות מעין סגורות אלגברית

בעבודה זו אנו מפתחים כלים אלמנטרים לחקירת הרחבות של שדות. למשל אנו מכלילים בעיות שיכון להרחבות של שדות. את הכלים הללו אנו מיישמים לחקירת הרחבות מעין סגורות אלגברית. בפרט אנו מקבלים תכונה מרכזית של הרחבות מעין סגורות אלגברית – *תכונת ההרמה* (טענה 3.4.6). הבה נתאר את התוצאות הנובעות מתורה זו.

1.2.1 הגבלות על הרחבות מעין סגורות אלגברית

במאמר [16] שבו הופיעו הרחבות מעין סגורות אלגברית לראשונה מצאו ירדן ורזון כמה הרחבות גלואה M של $\mathbb{Q}$ כך ש M מעין סגור אלגברית כשדה, אבל M אינו הרחבה מעין סגורה אלגברית של אף שדה מספרים. כדי להוכיח זאת הם השתמשו במשפט הכבד של Faltings. בעקבות תוצאה זו הם שאלו האם זה צרוף מקרים או תופעה כללית.

במאמר [15] ירדן עונה על שאלה זאת על ידי כך שהוא מראה שההרחבה היחידה של שדה מספרים שרירותי שהיא גם גלואה וגם מעין סגורה אלגברית היא הסגור האלגברי $\tilde{\mathbb{Q}}$. כדי להוכיח זאת ירדן אינו משתמש במשפט פלטינגס, אלא בתוצאות אחרות. דהיינו במשפט הצפיפות של פרובניוס, באיפיון של Neukirch של שדות סגורים p־אדית בין כל ההרחבות האלגבריות של $\mathbb{Q}$ ובתכונה המיוחדת של $\mathbb{Q}$ שאין לו תת שדות נאותים (!). מסיבה זו התוצאה של ירדן מוגבלת לשדות מספרים.

ההתקדמות הבאה היא להכליל את התוצאה של ירדן לשדה נוצר סופית ואינסופי K כלשהו. ואכן על ידי שיכלול שיטת ירדן־רזון, כלומר שימוש במשפט פלטינגס (ובמשפט Grauert-Manin באיפיון חיובי) ירדן והמחבר [2] הכלילו את התוצאה של ירדן עבור K.

משפט I *יהי K שדה נוצר סופית ואינסופי. ההרחבה היחידה של K שהיא גם גלואה וגם מעין סגורה אלגברית הינה הסגור הפריד K_s של K.*

בעזרת תכונת ההרמה המוזכרת לעיל ומכפלות זר של חבורות סופיות, אנחנו מוכיחים מחדש בצורה אלמנטרית ופשוטה את המשפט הנ״ל. יתר על כן, ההוכחה שלנו אינה משתמשת בשום תכונה של שדות נוצרים סופית, לכן המשפט נכון לשדה שרירותי K.

משפט II *תהי M/K הרחבה פרידה, נאותה ומעין סגורה אלגברית. אזי הסגור גלואה של M/K הוא הסגור הפריד K_s של K.*

בפרט אם M/K הרחבת גלואה מעין סגורה אלגברית, אז $M = K$ או $M = K_s$.

למבנה גלואה של הרחבה מעין סגורה אלגברית M/K יש הגבלות נוספות. התוצאה הבאה מאפיינת את כל ההרחבות המעין סגורות אלגברית הסופיות:

משפט III *תהי M/K הרחבה מעין סגורה אלגברית סופית. אז או ש M/K אי פרידה בטוהרה ו K מעין סגור אלגברית או ש K סגור ממשית ו M הסגור האלגברי של K.*

(שימו לב שקיימים הרחבות מעין סגורות אלגברית סופיות שהן אי פרידות בטוהרה, לפרטים נוספים ראו דיון המופיע לפני מסקנה 4.2.4.)

למשפט האחרון יש שימוש מפתיע: בעזרתו ניתן לענות בחיוב על בעיה 18.7.8 של [8] במקרה של שדות נוצרים סופית: עבור שדה הילברטי K, הבעיה שואלת האם "משפט התחתית" הבא מתקיים עבור K. כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ לשדה $M = K_s(\boldsymbol{\sigma})$ אין תת שדות L כך ש $1 < [M : L] < \infty$.

במאמר [10] הרן מוכיח גרסה קודמת של משפט התחתית, דהיינו תחת ההנחה הנוספת ש $K \subseteq L$. יש לציין שאם, למשל, $K = \mathbb{F}_p(x)$, אז $[M : M^p] = p$ לכל הרחבה פרידה M/K (ראה דיון לפני משפט 8.2.2 לפרטים נוספים). לכן משפט התחתית לא מתקיים מסיבה טריוויאלית. כדי להפטר ממכשלה זו נוסיף את הדרישה ש M/L פריד.

עתה משפט התחתית נכון עבור שדה נוצר סופית אינסופי, וכפי שצוין, המרכיב המרכזי בהוכחה הוא משפט III.

משפט IV *משפט התחתית תקף לשדה נוצר סופית אינסופי.*

1.2.2 הורדת חבורות גלואה

במאמר [26] רזון מראה, עבור הרחבה מעין סגורה אלגברית M/K, שכל הרחבה פרידה N/M בעצם מגיעה מהרחבה פרידה של K.

משפט ז' *תהי M/K הרחבה מעין סגורה אלגברית ותהי N/M הרחבה פרידה. אזי קיימת הרחבה פרידה L/K המופרדת לינארית מ M מעל K כך ש $N = ML$.*

אנו מכלילים את התוצאה של רזון, ומביאים תוצאת ירידה חזקה יותר:

משפט V *תהיינה M/K הרחבה מעין סגורה אלגברית ו N/M הרחבת גלואה סופית. נניח ש $\mathrm{Gal}(N/M) \leq H$, באשר H ניתנת למימוש רגולרי מעל K. אזי קיימת הרחבת גלואה L/K כך ש $\mathrm{Gal}(L/K) \leq H$ ו $N = LM$.*

ואכן שימוש משפט V עם חבורת הסימטריה $H = S_n$ מוכיח את משפט ז' (ראה הוכחת מסקנה 4.1.4). מעניין לציין שההוכחה המקורית של רזון של משפט ז' דומה להוכחה שאנו מביאים כאן רק מאוד ספציפית: מתייחסים רק למימוש הרגולרי של $H = S_n$ על ידי הפולינום הכללי $f(T_1, \dots, T_n, X) = X^n + T_1 X^{n-1} + \cdots + T_n$.

הסיבה שקראנו למשפט V תוצאת ירידה באה מהמקרה בו G ניתנת למימוש רגולרי מעל K: אם $G=\mathrm{Gal}(N/M)$ היא ניתנת למימוש רגולרי מעל K, נקח $H=G$ במשפט ונקבל ש G ניתנת למימוש כחבורת גלואה מעל K (כיוון ש $G=\mathrm{Gal}(L/K)$ במקרה זה). לכן G *יורדת* מ M ל K.

מכיוון שחבורות אבליות ניתנות למימוש רגולרי מעל כל שדה נקבל כמסקנה את השויון

$$M^{\mathrm{ab}}=MK^{\mathrm{ab}}.$$

1.3 זוגות פרויקטיבים

יש קשר עמוק בין שדות מעין סגורים אלגברית לבין חבורות פרוסופיות פרויקטיביות כפי שהמשפט הבא מדגים.

משפט ח' *חבורת הגלואה המוחלטת של שדה מעין סגור אלגברית היא פרויקטיבית, ולהפך, כל חבורה פרויקטיבית ניתנת למימוש כחבורת הגלואה המוחלטת של שדה מעין סגור אלגברית.*

Ax הוכיח את החלק הראשון [8, משפט 11.6.2] ולובצקי וון דר דריס (v.d.Dries) הוכיחו את החלק השני [8, מסקנה 23.1.2].

קשר דומה מתקיים בין הרחבות מעין סגורות אלגברית של שדות מעין סגורים אלגברית לבין *זוגות פרויקטיבים*. זוג פרויקטיבי (Γ,Λ) מורכב מחבורה פרוסופית Λ ותת חבורה סגורה Γ עבורם כל *בעית שיכון כפולה וסופית* פתירה בחולשה (ראה הגדרה 5.1.1).

משפט VI *(א) תהי M הרחבה מעין סגורה אלגברית של שדה מעין סגור אלגברית K. אזי $(\mathrm{Gal}(M),\mathrm{Gal}(K))$ זוג פרויקטיבי.*

(ב) תהי M הרחבה אלגברית של שדה מעין סגור אלגברית K. אזי M/K מעין סגור אלגברית אם ורק אם $(\mathrm{Gal}(M),\mathrm{Gal}(K))$ פרויקטיבי.

(ג) יהי (Γ,Λ) זוג פרויקטיבי. אזי קיימת הרחבה מעין סגורה אלגברית M של שדה מעין סגור אלגברית K כך ש $\Gamma\cong\mathrm{Gal}(M)$, $\Lambda\cong\mathrm{Gal}(K)$.

ממשפט זה נובע שכל תכונה של זוגות פרויקטיבים ניתנת לתרגום לתוצאה על הרחבות מעין סגורות אלגברית של שדות מעין סגורים אלגברית. קשר זה מהווה מניע לחקר הזוגות הפרויקטיבים.

מעניין לציין שלמרות שכאשר K שדה שאינו מעין סגור אלגברית, לא ניתן להעביר תוצאות על זוגות פרויקטיבים באופן ישיר להרחבות מעין סגורות אלגברית

של K. עדיין ניתן ליישם את הרעיונות והכלים. ואכן השיטות האלמנטריות שהוצגו בסעיף 1.2 מגיעות בצורה כזו.

המחקר של זוגות פרויקטיבים מתפצל לשני כיוונים. ראשית אנו מבססים את תוצאות מקבילות לתוצאות של הרחבות מעין סגורות אלגברית. למשל המשפט המתאים למשפט II אומר שהזוגות הפרויקטיבים הנורמלים (כלומר $\Gamma \triangleleft \Lambda$) הם $\Gamma = 1$ או $\Gamma = \Lambda$. לפעמים האנאלוגים התורת חבורתיים חזקים יותר, למשל, האנאלוג של משפט V הוא:

משפט VII *יהי* (Γ, Λ) *זוג פרויקטיבי. אזי* $\Lambda = N \rtimes \Gamma$*, עבור איזשהו* $N \triangleleft \Lambda$.

שנית, אנו מוצאים משפחות של זוגות פרויקטיבים. מהטרנזיטיביות של הרחבות מעין סגורות אלגברית (טענה 3.4.8) אנו מקבלים דוגמאות חדשות של הרחבות מעין סגורות אלגברית. למשל

משפט VIII *כל חבורה פרויקטיבית* P *ניתנת למימוש כחבורת גלואה המוחלטת של הרחבה מעין סגורה אלגברית של איזשהו שדה הילברטי* K*. יתר על כן, אם הדרגה של* P *לכל היותר בת מניה, ניתן לקחת* $K = \mathbb{Q}_{ab}$.

לצערנו, לא הצלחנו ליישם שיטות אלו כדי למצוא הרחבות מעין סגורות אלגברית חדשות של $\mathbb{Q}$.

1.4 משפט אי הפריקות של הילברט – הגרסה החלשה

ישנו קשר מעניין ועמוק בין בעיות שיכון, הצבות אי פריקות בפולינומים ונקודות רציונליות על יריעות. המשפט הבא מהווה ראיה מצוינת לקשר הזה.

משפט ט' *יהי* K *שדה מעין סגור אלגברית. אזי* K *הוא הילברטי אם ורק אם* K *הוא חופשי־*ω

(נזכר כי מעין הסגירות האלגברית אומרת שלכל יריעה יש נקודות רציונליות, תכונת ההילברטיות גוררת שלכל פולינום אי פריק יש ייחודים אי פריקים ותכונת החופשיות־ω אומרת שכל בעית שיכון סופית פתירה.) בעבודתם על שדות פרובניוס [7], הרן, ירדן ופריד מעדנים את הקשר הנ״ל.

אנו מבודדים מהמשפט הזה את התנאי המדויק שמקשר את שלושת המושגים (למה 6.1.2). אחרי זה אנו מיישמים את התנאי הכללי שקיבלנו לשדה K שיש לו הרחבות מעין סגורות אלגברית ומקבלים גרסה חלשה של משפט אי הפריקות של הילברט (טענה 6.2.1). מקרה פרטי נחמד הוא במקרה שהפולינום הוא ״הכי אי פריק״.

משפט IX *יהיו K שדה ו $f(T,X) \in K[T,X]$ פולינום אי פריק, פריד וממעלה n ב X שחבורת הגלואה שלו מעל $\tilde{K}(T)$ היא S_n. ($\tilde{K}$ הוא סגור אלגברי של K.) נניח שקיימות הרחבה מעין סגורה אלגברית M/K והרחבה פרידה N/M ממעלה n. אזי קיימים אינסוף $a \in K$ עבורם $f(a,X)$ הוא אי פריק מעל K.*

תוצאה זו מהווה חלק מרכזי בהוכחת המשפטים I ו ה'.

1.5 שדות עם הרחבות מעין סגורות אלגברית

לאור התוצאות שתוארו עד עכשיו, תכונה משמעותית עבור שדה K היא שיש לו הרחבות מעין סגורות אלגבריות "לא טריוויאליות."

אנו מתמקדים בשני פנים של מציאת הרחבות מעין סגורות אלגברית. ראשית אנו מכלילים את משפט א' במקרה ש K שדה נוצר סופית אינסופי. (שימו לב ששדה כזה הוא תמיד הילברטי.)

משפט X *יהי K שדה נוצר סופית אינסופי ויהי $e \geq 1$ שלם. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ ולכל שדה $F \subseteq K_s(\boldsymbol{\sigma})$ שאינו אלגברי מעל שדה סופי ההרחבה $K_s(\boldsymbol{\sigma})/F$ היא מעין סגורה אלגברית.*

איננו יודעים האם הטענה נכונה במקרה היותר כללי שבו K הוא שדה הילברטי בן מניה שרירותי, למשל $K = \mathbb{Q}_{ab}$. תשובה חיובית תגרור את משפט התחתית עבור כל שדה הילברטי בן מניה.

הכוון השני דן בשדה קבוע F והמטרה היא למצוא הרחבות מעין סגורות אלגברית של F. למעשה אנו מתעניינים בשאלה הבאה.

שאלה 1.5.1 *עבור אילו מספרים טבעיים n קיימות הרחבה מעין סגורה אלגברית M/F והרחבה פרידה N/M ממעלה n?*

עבור כמה משפחות של הרחבות של שדות הילברטיים בני מניה אנו נותנים תשובה מספקת לשאלה.

משפט XI *יהי K שדה הילברטי בן מניה ותהי F/K הרחבה אלגברית ופרידה. אזי קיימות הרחבה מעין סגורה אלגברית M/F והרחבה פרידה N/M ממעלה n במקרים הבאים.*

(א) F/K היא פרו־פתירה ו $n \geq 5$.

(ב) קיים מספר ראשוני p כך ש $p \nmid [\hat{F}:K]$ (כמספרי־על), באשר $\hat{F}$ הוא הסגור גלואה של F/K.

למשפט זה יש כמה מסקנות, למשל מרחיבים את משפט ה' לתוצאה הבאה.

משפט י' *יהי K הילברטי (מעוצמה שרירותית) ותהי F/K הרחבה פרו־פתירה (בהתאמה הרחבה שסגור הגלואה שלה זר ל p). אזי לכל $n \geq 5$ (בהתאמה $n \geq 1$) כל תבנית ריבועית ממימד n מעל F איזומורפית לתבנית עקבה משוכללת.*

תוצאה זו הופיעה ב [3].

פרק 2

הקדמות בתורת גלואה

בפרק זה מונחים היסודות בתורת גלואה ובתורת החבורות הסופיות הדרושים בעבודה זו. אנו קובעים את הסימונים ונותנים תכונות בסיסיות אשר ישמשו אותנו בהמשך. בנוסף חלק מהפרטים הטכניים של הפרקים הבאים נמצאים בפרק זה. הקורא המומחה יכול לדלג על פרק זה ולחזור אליו כאשר ידרש.

2.1 פעולות של חבורת גלואה

תהי F/K הרחבת גלואה. חבורת הגלואה $G = \mathrm{Gal}(F/K)$ באה מצוידת עם כמה פעולות טבעיות, הבאות מפולינומים ומתתי חבורות. נתאר שתיים מהפעולות להלן.

ראשית יהי $f(X) \in K[X]$ פולינום פריד (ומתוקן) שמתפצל מעל F. אזי f מתפרק למכפלת גורמים לינארים, $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$, באשר כל $\alpha_i \in F$ והם שונים. מכיוון ש G משבית את מקדמי f, הוא מתמיר את שורשיו. תכונות של הפולינום f מקודדות בפעולה הזו (ולמעשה רעיון זה מקורו בגלואה עצמו). הלמה הבאה ממחישה את הקשר הזה.

למה 2.1.1 *תהי R קבוצת כל שורשי f.*

(א) R יוצרת את F מעל K אם ורק אם G פועלת נאמנה על R.

(ב) ישנה התאמה בין הפרוק $f(X) = \prod_{i=1}^{m} f_i(X)$ של f לגורמים אי פריקים מעל K לבין הפרוק $R = \dot\bigcup_{i=1}^{m} R_i$ של R למסלולי-G. ההתאמה נתנת על ידי $f_i(X) = \prod_{\alpha\in R_i}(X - \alpha)$ (תחת סידור מחדש של הגורמים f_i).

(ג) f אי פריק אם ורק אם (G, R) טרנזיטיבית.

הוכחה. יהי $E \subseteq F$ השדה הנוצר על ידי R. לפי התאמת גלואה $E = F$ אם ורק אם אף $1 \neq \sigma \in G$ לא משבית את E. מכך נובע (א).

כדי להוכיח את (ב) נבחין כי מקדמי $f_i(X) = \prod_{\alpha\in R_i}(X - \alpha)$ מושבתים על ידי G, ולכן $f_i \in K[X]$. בנוסף אם f_i היה פריק, אז לפי התאמת גלואה, היתה תת קבוצה

נאותה ולא ריקה של R_i שהיתה שמורת־G, בסתירה לכך ש R_i מסלול. לבסוף (ג) הוא מקרה פרטי של (ב). ■

הפעולה השניה של G באה מתתי חבורות. תהי $H \leq G$ תת חבורה. אזי G פועלת על הקוסטים G/H של H ב G על ידי כפל משמאל. פעולה זו איזומורפית[1] (באופן לא טבעי) לפעולה הקודמת.

אכן, יהי $E = F^H$ שדה השבת של H ב F ויהיו $\alpha_1, \ldots, \alpha_n \in E$ קבוצה יוצרת של E מעל K, כלומר $E = K(\alpha_1, \ldots, \alpha_n)$. יהי $f(X) \in K[X]$ הפולינום המינימלי שכל $\alpha_1, \ldots, \alpha_n$ הם שורשיו. אזי G מתמיר את שורשי $f(X)$ ומהתאמת גלואה נובע כי $H = \mathrm{Gal}(F/E)$. לכן המייצב של $\alpha_1, \ldots, \alpha_n$ הוא H.

2.2 בעיות שיכון

חבורה פרוסופית מוגדרת כגבול הפוך של חבורות סופיות או באופן שקול כחבורה טופולוגית קומפקטית האוסדורף אי־קשירה לחלוטין [8, למה 1.1.7]. מהתאור הראשון זה נראה סביר שחבורה פרוסופית Γ תהיה נתנת לאפיון על ידי עצמים סופיים. ואכן אם Γ נוצרת סופית (כחבורה טופולוגית), אז היא נקבעת (עד כדי איזומורפיזם) על ידי הקבוצה

$$\{\Gamma/N \mid \Gamma \text{ פתוחה ונורמלית ב } N\}/\sim$$

של כל המנות הסופיות (עד כדי איזומורפיזם) [8, טענה 16.10.7].

אולם באופן כללי זה לא המצב. לדוגמא, גם למכפלה הישרה $\Gamma_1 = \prod_G G$ של כל החבורות הסופיות G וגם לחבורה הפרוסופית החופשית על מספר בן מניה של יוצרים $\Gamma_2 = \hat{F}_\omega$ יש את התכונה שכל חבורה סופית היא מנה שלהם. אבל $\Gamma_1 \ncong \Gamma_2$ (כי, למשל, Γ_2 חסרת פיתול). מסיבה זו צריך אוביקט סופי יותר עדין – *בעיות שיכון סופיות*.

נציג שתי תוצאות קלאסיות לפני שנכנס לחלק היותר טכני.

- חבורה פרוסופית Γ היא פרויקטיבית אם ורק אם כל בעית שיכון סופית פתירה בחולשה [27, למה 7.6.1].
- תהי Γ חבורה פרוסופית מדרגה אינסופית κ. אזי Γ חופשית אם ורק אם לכל בעית שיכון סופית לא טריוויאלית יש κ פתרונות [8, משפט 25.1.7].

[1] אם G אינסופית, נדרוש ש H פתוחה.

2.2.1 בעיות שיכון עבור חבורות פרוסופיות

תהי Γ חבורה פרוסופית. **בעית שיכון** עבור Γ היא תרשים

$$\begin{tikzcd} & \Gamma \arrow[d, "\mu"] \arrow[dl, dotted, "\exists\theta?"'] \\ G \arrow[r, "\alpha"] & A \end{tikzcd}$$

באשר G ו A חבורות פרוסופיות ו μ ו α אפימורפיזמים (רציפים). כשנרצה לקצר נרשום את בעית השיכון כזוג (μ, α).

פתרון של בעית שיכון (μ, α) הוא אפימורפיזם $\theta\colon \Gamma \to G$ כך ש $\alpha\theta = \mu$. אם θ מקיים $\alpha\theta = \mu$ אבל הוא לא בהכרח על נאמר ש θ **פתרון חלש**. בפרט חבורה פרוסופית G היא מנה של Γ אם ורק אם בעית השיכון $(\Gamma \to 1, G \to 1)$ פתירה.

אם G סופית (בהתאמה, α מתפצל) נאמר שבעית השיכון היא **סופית** (בהתאמה, **מתפצלת**).

שתי בעיות שיכון $(\mu\colon \Gamma \to A, \alpha\colon G \to A)$ ו $(\nu\colon \Gamma \to B, \beta\colon H \to B)$ נקראות **שקולות** אם קיימים איזומורפיזמים $i\colon G \to H$ ו $j\colon A \to B$ עבורם התרשים הבא חילופי.

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "i"] & A \arrow[d, "j"] & \Gamma \arrow[l, "\mu"'] \arrow[d, equal] \\ H \arrow[r, "\beta"] & B & \Gamma \arrow[l, "\nu"'] \end{tikzcd}$$

זה ברור שכל פתרון (חלש) של (μ, α) מתאים לפתרון (חלש) של (ν, β) ולהפך.

הלמה הבאה נותנת קרטריון פשוט, אבל שימושי, לכך שפתרון חלש יהיה פתרון, כלומר על.

למה 2.2.1 *פתרון חלש $\theta\colon \Gamma \to G$ של בעית שיכון $(\mu\colon \Gamma \to A, \alpha\colon G \to A)$ הוא על אם ורק אם $\ker(\alpha) \le \theta(\Gamma)$.*

הוכחה. נניח ש $\ker(\alpha) \le \theta(\Gamma)$. יהי $g \in G$, נסמן $a = \alpha(g)$, ויהי $f \in \mu^{-1}(a)$. אזי $\theta(f)^{-1}g \in \ker(\alpha) \le \theta(\Gamma)$, ולכן $g \in \theta(\Gamma)$.

הכוון ההפוך מיידי. ■

2.2.2 בעיות שיכון עבור שדות

יהי K שדה ונסמן ב K_s את הסגור הפריד שלו. חבורת הגלואה המוחלטת $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ היא פרוסופית. לכן בעית שיכון עבור K היא בעצם בעית שיכון עבור $\mathrm{Gal}(K)$.

באופן מפורש, בעית שיכון עבור K היא זוג $(\mu\colon \mathrm{Gal}(K) \to A, \alpha\colon G \to A)$ של אפימורפיזמים. אם נסמן ב L את שדה השבת של $\ker(\mu)$, אז $\mu = \bar{\mu}\mu_0$,

באשר $\mu_0\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K)$ היא העתקת השיכון ו $\bar{\mu}\colon \mathrm{Gal}(L/K) \to A$ הוא איזומורפיזם. נקבל כי בעיות השיכון (μ, α) ו $(\mu_0, \bar{\mu}^{-1}\alpha)$ שקולות.

מעתה ואילך אנחנו נניח (כשנצטרך) ש $A = \mathrm{Gal}(L/K)$ וש μ היא העתקת הצמצום.

$$\begin{tikzcd} & \mathrm{Gal}(K) \arrow[dl, dotted, "\exists\theta?"'] \arrow[d, "\mu"] \\ G \arrow[r, "\alpha"] & \mathrm{Gal}(L/K) \end{tikzcd} \tag{2.1}$$

בהנתן פתרון חלש $\theta\colon \mathrm{Gal}(K) \to G$ שדה השבת F של $\ker(\theta)$ נקרא **שדה הפתרון**.

במונחי שדות, פתרון של בעית שיכון מתאים לשיכון־K של L בתוך שדה הפתרון F כך שהעתקת הצמצום $\mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K)$ מתלכדת עם α. בפרט נקבל שבעיות השיכון $(\mu, \mathrm{res}\colon \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K))$ ו (μ, α) שקולות.

2.2.3 בעיות שיכון גאומטריות ורציונליות

נגדיר עתה בעיות שיכון עבור שדה K הבאות מאוביקטים גאומטרים.

הגדרה 2.2.2 *תהי E הרחבה רגולרית נוצרת סופית של K, תהי F/E הרחבת גלואה ויהי $L = F \cap K_s$. אזי העתקת הצמצום $\alpha\colon \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)$ היא על, כיוון ש $E \cap L = K$. נקרא לבעית השיכון*

$$\begin{tikzcd} & \mathrm{Gal}(K) \arrow[d, "\mu"] \\ \mathrm{Gal}(F/E) \arrow[r, "\alpha"] & \mathrm{Gal}(L/K) \end{tikzcd} \tag{2.2}$$

בעית שיכון **גאומטרית**.

אם $E = K(t_1, \ldots, t_e) = K(\boldsymbol{t})$ הוא שדה פונקציות רציונליות, אזי בעית השיכון (2.2) שמקבלת את הצורה

$$\begin{tikzcd} & \mathrm{Gal}(K) \arrow[d, "\mu"] \\ \mathrm{Gal}(F/K(\boldsymbol{t})) \arrow[r, "\alpha"] & \mathrm{Gal}(L/K) \end{tikzcd} \tag{2.3}$$

נקראת **רציונלית**.

נשים לב, שכביכול, הרציונליות של בעית השיכון תלויה ב $e \geq 1$. אולם בלמה 2.4.5 מוכח שאם התנאי מתקיים עבור איזשהו e, אז הוא מתקיים גם עבור $e = 1$.

טענה 2.2.3 *כל בעית שיכון סופית שקולה לבעית שיכון גאומטרית.*

הוכחה של טענה זו ניתן למצוא ב [8, למה 11.6.1]. לכן מעתה ואילך נוכל להצטמצם לדיון בבעיות שיכון גאומטריות.

נאמר שחבורה סופית G **ניתנת למימוש רגולרי**, אם קיימת בעית שיכון רציונלית (2.3) כך ש $\mathrm{Gal}(F/K(\boldsymbol{t})) \cong G$ ו $L = K$. התוצאה הקלאסית הבאה נותנת כמה משפחות של חבורות הניתנות למימוש רגולרי מעל כל שדה.

משפט 2.2.4 *כל החבורות האבליות, כל חבורות הסימטריה וכל חבורות החילופין ניתנות למימוש רגולרי מעל כל שדה.*

הוכחה מופיעה, למשל, ב [8]. תוצאה זו איננה מייצגת בשום אופן את מצב העיניינים העדכני בנוגע לחבורות הניתנות למימוש רגולרי.

2.3 מכפלות סיב

יהיו $\alpha_1\colon G_1 \to A$ ו $\alpha_2\colon G_2 \to A$ אפימורפיזמים של חבורות (פרוסופיות). אזי מכפלת הסיב מוגדרת על ידי

$$.G_1 \times_A G_2 = \{(g_1, g_2) \in G_1 \times G_2 \mid \alpha_1(g_1) = \alpha_2(g_2)\} \leq G_1 \times G_2$$

חבורה זו מצויידת בשתי הטלות טבעיות $\pi_i\colon G_1 \times_A G_2 \to G_i$ המוגדרות על ידי $\pi_i(g_1, g_2) = g_i$, $i = 1, 2$.

מכפלות סיב מופיעות הרבה ב"טבע". אנחנו נשתמש בהן בעיקר כדי לעבור מבעית שיכון נתונה לבעית שיכון יותר גדולה ויותר נוחה.

הגדרה 2.3.1 *בעית שיכון* $(\mu'\colon \Gamma \to A', \alpha'\colon G' \to A')$ *עבור חבורה פרוסופית* Γ **חולשת** *על בעית שיכון* $(\mu\colon \Gamma \to A, \alpha\colon G \to A)$ *אם כל פתרון (חלש)* θ' *של* (μ', α') *משרה פתרון (חלש)* θ *של* (μ, α) *בעזרת תרשים חילופי כנ"ל.*

(2.4)

$$\begin{tikzcd}
& \Gamma \arrow[dl, dotted, "\theta'"'] \arrow[d, "\mu'"] \arrow[dd, bend left, "\mu"] \\
G' \arrow[r, "\alpha'"] \arrow[d, "\pi"] & A' \arrow[d, "\nu"] \\
G \arrow[r, "\alpha"] & A
\end{tikzcd}$$

כאן $\pi\colon G' \to G$ *הוא על.*

הלמה הבאה נותנת בעית שיכון חולשת בעזרת מכפלת סיב.

למה 2.3.2 *תהי* $(\mu\colon \Gamma \to A, \alpha\colon G \to A)$ *בעית שיכון עבור חבורה פרוסופית* Γ. *יהי* $\mu'\colon \Gamma \to A'$ *אפימורפיזם כך ש* $\ker(\mu') \leq \ker(\mu)$. *יהי* $G' = G \times_A A'$ *ויהי* $\alpha'\colon G' \to A'$ *ההטלה המתאימה. אזי בעית השיכון* (μ', α') **חולשת** *על* (μ, α). *יתר על כן*

(א) נניח כי $\theta\colon \Gamma \to G$ הוא פתרון חלש ויש $\ker(\mu') \le \ker(\theta)$. אזי (μ', α') מתפצלת. (בפרט אם (μ, α) מתפצלת, אז גם (μ', α').)

(ב) פתרון חלש θ של (μ, α) משרה פתרון חלש θ' של (μ', α') המוגדר על ידי $\theta'(x) = (\theta(x), \mu'(x))$.

הוכחה. התרשים החילופי (2.4), באשר π היא ההטלה של מכפלת הסיב ו ν מושרה מ μ' ו μ גורר ש (μ', α') חולשת על (μ, α), כדרוש.

(ב) הוא מיידי.

לבסוף נוכיח את (א). ההעתקה $\theta \times \mu'\colon \Gamma \to G'$ שולחת את $x \in \Gamma$ לזוג $(\theta(x), \mu'(x))$. יהי $K = \ker(\theta \times \mu')$. ברור ש $K = \ker(\theta) \cap \ker(\mu')$, ולכן על פי ההנחה $K = \ker(\mu')$. נסיק כי $\theta \times \mu'$ משרה העתקה $\beta'\colon A' \to G'$. אזי $\alpha'\beta'\mu' = \alpha'(\theta \times \mu') = \mu'$, ומכך $\alpha'\beta' = \mathrm{id}$. ■

מכפלות סיב גם מתארות את חבורת הגלואה של צרוף של שתי הרחבות גלואה. במקרה זה ההעתקות הצמצום מתממשות כהטלות של מכפלת הסיב.

למה 2.3.3 *תהיינה M_1 ו M_2 הרחבות גלואה של שדה K ויהי $L = M_1 \cap M_2$. אזי $\mathrm{Gal}(M_1M_2/K)$ איזומורפי בצורה קאנונית ל $\mathrm{Gal}(M_1/K) \times_{\mathrm{Gal}(L/K)} \mathrm{Gal}(M_2/K)$. תחת האיזומורפיזם הזה ההעתקות הצמצום מתממשות כהטלות.*

הוכחה. האיזומורפיזם הטבעי

$$\mathrm{Gal}(M_1M_2/K) \to \mathrm{Gal}(M_1/K) \times_{\mathrm{Gal}(L/K)} \mathrm{Gal}(M_2/K)$$

ניתן על ידי $\sigma \mapsto (\sigma|_{M_1}, \sigma|_{M_2})$. (ראה [20, IV §1 משפט 1.14].) ■

יש קשר בין מכפלות סיב ופתרונות בלתי תלוים של בעיות שיכון. בהנתן קבוצת פתרונות $\{\theta_i \mid i \in I\}$ של בעית שיכון סופית $(\mu\colon \Gamma \to A, \alpha\colon G \to A)$ עבור חבורה פרוסופית Γ נאמר שהם **בלתי תלוים** אם הקבוצה $\{\ker(\theta_i) \mid i \in I\}$ היא בלתי תלויה ביחס למידת האר של $\ker(\mu)$. באופן מפורש הפתרונות הם בלתי תלוים אם ורק אם

$$(\ker(\mu) : \bigcap_{i\in I_0} \ker(\theta_i)) = \prod_{i\in I_0} (\ker(\mu) : \ker(\theta_i))$$

לכל תת קבוצה סופית $I_0 \subseteq I$.

נסמן ב

$$G_A^I = \{(g_i) \in G^I \mid \alpha(g_i) = \alpha(g_j),\ \ \forall i, j \in I\}$$

את מכפלת הסיב של I עותקים של G. לכל $i \in I$ תהי $\pi_i\colon G_A^I \to G$ העתקת המנה על הרכיב ה i-י. בנוסף מוגדרת $\alpha_I\colon G_A^I \to A$ על ידי $\alpha_I = \alpha\pi_i$, עבור איזשהו $i \in I$. הגדרה זו כמובן שאינה תלויה ב i.

למה 2.3.4 *אם* $\theta\colon \Gamma \to G_A^I$ *פתרון של* (μ, α_I)*, אז* $\{\theta_i = \pi_i\theta \mid i \in I\}$ *הם פתרונות בלתי תלויים של* (μ, α).

הוכחה. לכל $I_0 \subseteq I$ סופית נתאים את ההטלה $\pi_{I_0}\colon G_A^I \to G_A^{I_0}$ ונסמן $\theta_{I_0} = \pi_{I_0}\theta$.

$$\begin{tikzcd}
& \Gamma \arrow[dl, "\theta"'] \arrow[d, "\mu"] \arrow[ddl, bend left, "\theta_{I_0}"] \\
G_A^I \arrow[r, "\alpha_I"] \arrow[d, "\pi_{I_0}"'] & A \arrow[d, equal] \\
G_A^{I_0} \arrow[r, "\alpha_{I_0}"] & A
\end{tikzcd}$$

מהתרשים לעיל עם $I_0 = \{i\}$ נובע כי θ_i פתרון, $i \in I$.
כיוון ש

$$1 = \theta_{I_0}(x) = \pi_{I_0}(\theta(x)) \iff \forall i \in I_0,\ 1 = \pi_i(\theta(x)) = \theta_i(x)$$

נקבל כי $\bigcap_{i \in I_0} \ker(\theta_i) = \ker(\theta_{I_0})$. לכן

$$\begin{aligned}
(\ker(\mu) : \bigcap_{i \in I_0} \ker(\theta_i)) &= (\ker(\mu) : \ker(\theta_{I_0})) = \frac{|G_A^{I_0}|}{|A|} = \left(\frac{|G|}{|A|}\right)^{|I_0|} \\
&= \prod_{i \in I_0} (\ker(\mu) : \ker(\theta_i))
\end{aligned}$$

זה מוכיח שהפתרונות בלתי תלוים כדרוש. ■

2.4 אתרים

בסעיף זה נזכיר את ההגדרות והתכונות הבסיסיות של אתרים, להרחבות ופרטים נוספים ראה [8].

אתר φ של שדה F זה ההעתקה $\varphi\colon F \to M \cup \{\infty\}$ כך ש M הוא שדה ומתקיימות התכונות הבאות.

(א) $x + \infty = \infty + x = \infty$, $\forall x \in M$.

(ב) $x \cdot \infty = \infty \cdot x = \infty$, $\forall x \in M^\times (:= M \setminus \{0\})$.

(ג) $\varphi(x + y) = \varphi(x) + \varphi(y)$ (מתי שאגף ימין מוגדר).

(ד) $\varphi(xy) = \varphi(x)\varphi(y)$ (מתי שאגף ימין מוגדר).

(ה) $\exists x, y \in F$ כך ש $\varphi(x) = \infty$ ו $\varphi(y) \neq 0, \infty$.

אם F ו M מכילים שדה משותף K, ו $\varphi(x) = x$ לכל $x \in K$, נאמר ש φ הוא **אתר־**K.

אתר φ של שדה F בא עם חוג מקומי $\mathcal{O}_\varphi = \{x \in F \mid \varphi(x) \neq \infty\}$ שהאידאל המקסימלי הוא $\mathfrak{m}_\varphi = \{x \in \mathcal{O}_\varphi \mid \varphi(x) = 0\}$. שדה המנה $\mathcal{O}_\varphi/\mathfrak{m}_\varphi$ איזומורפי בצורה קאנונית **לשדה השאריות** $\bar{F} = \{\varphi(x) \mid x \in \mathcal{O}_\varphi\}$. אתר φ נקרא **רציונלי־**K אם שדה השאריות הוא K, כלומר $\bar{F} = K$. אתרים הם **שקולים** אם יש להם אותו חוג מקומי. בפרט לאתרים שקולים יש שדות שאריות איזומורפים קאנונית.

תהי E/K הרחבה רגולרית ותהי F/E הרחבת גלואה סופית. נניח ש φ אתר־K של E. אזי, לפי למת Chevalley, ניתן להרחיב את φ לאתר $\Phi\colon F \to M \cup \{\infty\}$, באשר M מציין את הסגור האלגברי של $\bar{E}$ [8, טענה 2.3.1]. מעתה ואילך תמיד נניח כי $\bar{F}/\bar{E}$ פריד. מהנחה זו נובע כי $\bar{F}/\bar{E}$ גלואה. נקרא לחבורה $\mathrm{Gal}(\bar{F}/\bar{E})$ **חבורת השאריות**.

יהי $L = F \cap K_s$, אז $L \subseteq \bar{F}$. (אכן, הואיל ו $K \subseteq \mathcal{O}_\Phi$, L שלם מעל K ו $\mathcal{O}_\Phi$ סגור בשלמות, נובע כי $L \subseteq \mathcal{O}_\Phi$.) אם נרכיב את Φ עם אוטומורפיזם גלואה של $\bar{F}/\bar{E}$, נוכל להניח ש Φ הוא אתר־L. לתת החבורה

$$D_{\Phi/\varphi} = \{\sigma \in \mathrm{Gal}(F/E) \mid \sigma\mathcal{O}_\Phi = \mathcal{O}_\Phi\} = \{\sigma \in \mathrm{Gal}(F/E) \mid \sigma\mathfrak{m}_\Phi = \mathfrak{m}_\Phi\}$$

של $\mathrm{Gal}(F/E)$ קוראים **חבורת הפרוק** של Φ/φ. שדה השבת של חבורת הפרוק ב F נקרא (כצפוי) **שדה הפרוק** של Φ/φ. שדה הפרוק מאופיין על ידי התכונה שהוא תת ההרחבה המרבית של F/E עם אותו שדה שאריות כמו של E.

יש אפימורפיזם טבעי מחבורת הפרוק לחבורת השארית הניתן על ידי $\sigma \in D_{\Phi/\varphi} \mapsto \bar{\sigma} \in \mathrm{Gal}(\bar{F}/\bar{E})$, באשר $\bar{\sigma}$ מוגדר על ידי $\bar{\sigma}(x + \mathfrak{m}_\Phi) = \sigma x + \mathfrak{m}_\Phi$. הגרעין של האפימורפיזם הזה נקרא **חבורת ההתמדה**, ומסומן על ידי $I_{\Phi/\varphi}$. לכן

$$.I_{\Phi/\varphi} = \{\sigma \in \mathrm{Gal}(F/E) \mid x - \sigma(x) \in \mathfrak{m}_\Phi, \forall x \in \mathcal{O}_\Phi\}$$

כאשר חבורת ההתמדה היא טריוויאלית אומרים שהאתר Φ הוא **לא מסועף** מעל φ (או לחילופין φ לא מסועף ב F). במילים אחרות , Φ לא מסועף מעל φ אם ורק אם חבורת השאריות איזומורפית לחבורת הפרוק.

מעתה ואילך נניח ש F ו E הם שדות פונקציות. כלומר נניח ש F ו E הן הרחבות פרידות סופיות של $K(\boldsymbol{t})$, באשר $\boldsymbol{t} = (t_1, \ldots, t_e)$ היא e־איה של משתנים ו $e > 0$ שלם.

למה 2.4.1 *יהי $x \in F$ כך ש $F = E(x)$. אזי קיים $g(\boldsymbol{t}) \in K(\boldsymbol{t})$ שונה מאפס כך שלכל אתר־K φ של F המקיים $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי וגם $g(\boldsymbol{a}) \neq 0$ מתקיים $\bar{x} = \varphi(x)$ סופי, φ לא מסועף מעל E ו $\bar{F} = \bar{E}(\bar{x})$.*

הוכחה. יהי $f(\boldsymbol{t}, X) \in K[\boldsymbol{t}, X]$ הפולינום האי פריק של x מעל $K(\boldsymbol{t})$. תהי

$g(\boldsymbol{t}) \in K[\boldsymbol{t}]$ מכפלת המקדם העליון של f (כפולינום ב X) והדיסקרימיננטה שלו. כיוון ש f פריד, $g \neq 0$.

יהי $R = K[\boldsymbol{t}, g^{-1}]$ ויהיו U, S הסגורים השלמים של R ב F, E, בהתאמה. אזי $S = R[x]$ ([8, הגדרה 6.1.3]), ובפרט $S = U[x]$. נסיק כי S/U הוא כיסוי של חוגים, ולכן הטענה נובעת מ [8, למה 6.1.3]. ■

יהי $x \in F$ איבר פרימיטיבי של F/E, כלומר $F = E(x)$ ותהי $g(\boldsymbol{t}) \in K[\boldsymbol{t}]$ מהלמה לעיל. נניח ש $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי וש $g(\boldsymbol{a}) \neq 0$. יהי f הפולינום האי פריק של x מעל E.

אזי $\bar{f} = \varphi(f)$ פריד (כיוון ש Φ לא מסועף מעל E). לכן Φ משרה העתקה חחעל בין $\mathcal{X}$, קבוצת כל שורשי f, לבין $\bar{\mathcal{X}}$, קבוצת כל שורשי $\bar{f}$. נסמן ב $\rho\colon S_{\mathcal{X}} \to S_{\bar{\mathcal{X}}}$ את האיזומורפיזם המתאים של חבורות התמורות.

עתה $D_{\Phi/\varphi}$ משוכן ב $S_{\mathcal{X}}$ (כי $\mathrm{Gal}(F/E)$ משוכן) ו $\mathrm{Gal}(\bar{F}/\bar{E})$ משוכן $S_{\bar{\mathcal{X}}}$. ואנחנו מקבלים את התוצאה הבאה.

למה 2.4.2 *הצמצום של* $\rho\colon S_{\mathcal{X}} \to S_{\bar{\mathcal{X}}}$ *לחבורת הפרוק* $D_{\Phi/\varphi}$ *מתלכד עם ההעתקה הטבעית* $D_{\Phi/\varphi} \to \mathrm{Gal}(\bar{F}/\bar{E})$.

ההעתקה הטבעית הנ״ל מתחברת לבעיות שיכון באופן הבא. אתר Φ/φ לא מסועף המקיים $\bar{E} = K$ משרה הומומורפיזם טבעי $\Phi^*\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ שמתפרק דרך חבורת השאריות ותמונתו $\Phi^*(\mathrm{Gal}(K)) = D_{\Phi/\varphi}$ היא חבורת הפרוק. מתקיים

$$\Phi(\Phi^*(\sigma)x) = \sigma\Phi(x)$$

לכל $\sigma \in \mathrm{Gal}(K)$ ולכל $x \in \mathcal{O}_\Phi$. לכן, אם Φ אתר־L נקבל כי $\mathrm{res}_{F,L} \circ \Phi^* = \mathrm{res}_{K_s,L}$, כלומר Φ^* הוא פתרון חלש של בעית השיכון

$$(\mathrm{res}\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K), \mathrm{res}\colon \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K)).$$

פתרונות כאלו נקראים *גאומטרים* וידונו בהרחבה בהמשך.

יהי Ψ אתר־L נוסף של F הנמצא מעל φ. אזי $\Phi = \Psi\sigma$ עבור איזשהו אוטומורפיזם גלואה $\sigma \in \mathrm{Gal}(F/E)$, חבורות הפרוק המתאימות הן צמודות (על ידי σ) והפתרונות Ψ^* ו Φ^* נבדלים על ידי הצמדה זו. לכן, כדי לפשט סימונים, וכאשר אין סכנה לבלבול, אנו משמיטים את Φ מהסימון. למשל D_φ מסמל את $D_{\Phi/\varphi}$ עבור איזושהי הרחבה קבועה Φ של φ ו φ^* בעצם מייצג את Φ^*; נאמר ש φ לא מסועף ב F אם Φ/φ לא מסועף, וכו.

תהי $\boldsymbol{t} = (t_1, \dots, t_e)$ e־איה של משתנים מעל K. איברים $a_1, \dots, a_e \in K_s$ מגדירים ייחוד $K[\boldsymbol{t}] \to K[\boldsymbol{a}]$. ניתן להרחיב ייחוד זה לאתר־K של $K(\boldsymbol{t})$ לתוך $K_s \cup \{\infty\}$, נסמנו φ. אם $e = 1$, האתר φ נקבע ביחידות על ידי $a = a_1 \in K_s$, ובפרט שדה השאריות הוא $K(a)$.

אולם כאשר $e>1$ האתר φ לא יחיד ושדה השאריות יכול להיות שונה מ $K(\boldsymbol{a})$. (הסיבה לכך היא שאיבר מהצורה $\varphi(\frac{t_i-a_i}{t_j-a_j})$, $i\neq j$, יכול להיות ∞ או כל איבר של K_s.) למרות האמור לעיל, ניתן להרחיב את הייחוד $\boldsymbol{a}\to\boldsymbol{t}$ לאתר־K φ של $K(\boldsymbol{t})$ באופן כזה ששדה השאריות יהיה $K(\boldsymbol{a})$ ולכל הרחבה סופית L/K שדה השאריות של $L(\boldsymbol{t})$ יהיה $L(\boldsymbol{a})$ (תחת הרחבה של φ לאתר־L של $L(\boldsymbol{t})$) [8, למה 2.2.7].

2.4.1 נקודות על יריעות ואתרים

תהי V יריעה אלגברית המוגדרת מעל K. בעבודה זו יריעות הן אי פריקות מעל הסגור האלגברי. יהי E שדה הפונקציות של V. יהי $\boldsymbol{a}\in V(K)$ ותהי $U=\mathrm{Spec}R$ סביבה אפינית של $\boldsymbol{a}$. אזי $\boldsymbol{a}$ מגדיר הומומורפיזם־K $s_{\boldsymbol{a}}\colon R\to K$.

ההומורפיזם $s_{\boldsymbol{a}}$ ניתן להרחבה לאתר־K של E. כמו במקרה של הרחבת ייחודים לאתרים, יש כמה דרכים בהם ניתן להרחיב את $s_{\boldsymbol{a}}$ ל E כאשר V אינו עקומה וניתן להרחיב לאתר־K כך ששדה השאריות יהיה $K(\boldsymbol{a})$.

יהי $\nu\colon V\to\mathbb{A}^{\dim(V)}$ מורפיזם סופי ופריד מעל K. אזי הרחבת השדות המתאימה $E/K(\boldsymbol{t})$ היא סופית ופרידה. יהי $\boldsymbol{a}\in K_s^{\dim(V)}(=\mathbb{A}^{\dim(V)}(K_s))$ ויהי $\boldsymbol{b}\in\nu^{-1}(\boldsymbol{a})\subseteq V(K_s)$. לפי למה 2.4.1 יש $g\in K[\boldsymbol{t}]$ שונה מאפס, כך שאם $g(\boldsymbol{a})\neq 0$, אז ניתן להרחיב את הייחוד $\boldsymbol{t}\mapsto\boldsymbol{a}$ לאתר־K של E כך ש $\overline{K(\boldsymbol{t})}=K(\boldsymbol{a})$ ו $\bar{E}=K(\boldsymbol{b})$.

2.4.2 פתרונות גאומטרים לבעיות שיכון

נתחיל עם בעית שיכון גאומטרית

$$(\mu\colon \mathrm{Gal}(K)\to\mathrm{Gal}(L/K),\alpha\colon\mathrm{Gal}(F/E)\to\mathrm{Gal}(L/K))$$

עבור שדה K. כפי שראינו קודם אתר φ של E שאינו מסועף ב F ועם שדה שאריות $\bar{E}=K$ משרה פתרון חלש φ^* שתמונתו חבורת הפרוק.

הגדרה 2.4.3 *פתרון חלש $\theta\colon\mathrm{Gal}(K)\to\mathrm{Gal}(F/E)$ של בעית שיכון גאומטרית (μ,α) נקרא* ***גאומטרי*** *אם קיים אתר־K φ שאינו מסועף ב F כך ש $\theta=\varphi^*$.*

פתרונות גאומטרים מתנהגים היטב תחת הרחבת סקלרים.

למה 2.4.4 *תהי (μ,α) בעית שיכון גאומטרית. תהי M/K הרחבת גלואה עם $L\subseteq M$. אזי בעית השיכון הגאומטרית*

$$(\mu'\colon\mathrm{Gal}(K)\to\mathrm{Gal}(M/K),\alpha'\colon\mathrm{Gal}(FM/E)\to\mathrm{Gal}(M/K)),$$

באשר α' ו μ' הן ההעתקות הצמצום המתאימות חולשת על בעית השיכון (μ,α) ביחס להעתקות הצמצום. יתר על כן, אם ψ^* הוא פתרון גאומטרי (חלש) של (μ',α'), אז $(\psi|_F)^*$ הוא פתרון גאומטרי (חלש) של (μ,α).

הוכחה. ההרחבה E/K הינה רגולרית, ולכן לפי למה 2.3.3 מתקיים

$$\mathrm{Gal}(FM/E)=\mathrm{Gal}(F/E)\times_{\mathrm{Gal}(LE/E)}\mathrm{Gal}(ME/E)\cong\mathrm{Gal}(F/E)\times_{\mathrm{Gal}(L/K)}\mathrm{Gal}(M/K),$$

באשר ההטלות מתלכדות עם ההעתקות הצמצום המתאימות. זה מוכיח ש (μ',α') חולשת על (μ,α) לפי למה 2.3.2.

עתה יהי ψ^* פתרון גאומטרי (חלש) של (μ',α'). נסמן $\varphi=\psi|_F$. אזי φ לא מסועף ב F ו $\mathrm{res}_{FM,F}\circ\psi^*=\varphi^*$. ■

שימוש במשפט Matsusaka-Zariski ולמת Bertini-Noether מאפשר לצמצם את מספר המשתנים ב (2.3) למשתנה אחד.

למה 2.4.5 *יהיו K שדה אינסופי, L/K הרחבת גלואה סופית ו $(u,\boldsymbol{t})$ $e+1$־איה של משתנים. בהנתן בעית שיכון רציונלית (2.3) יש פתרון לבעיה*

$$(\mu_u\colon \mathrm{Gal}(K(u))\to\mathrm{Gal}(L/K),\alpha\colon\mathrm{Gal}(F/K(\boldsymbol{t}))\to\mathrm{Gal}(L/K))$$

כך ששדה הפתרון רגולרי מעל L.

הוכחה. יהי $x\in F$ שלם מעל $L[\boldsymbol{t}]$ כך ש $F=K(\boldsymbol{t},x)$. יהי $f(\boldsymbol{T},X)\in L[\boldsymbol{T},X]$ הפולינום האי פריק הפריד והמתוקן ב X עבורו $f(\boldsymbol{t},x)=0$.

נקח שני משתנים U,V ונסמן ב E את הסגור האלגברי של $L(U,V)$. יהי

$$0\neq h(T_1,\dots,T_r)\in K[\boldsymbol{T}]$$

הפולינום הניתן בלמה 2.4.1 עבור $F/K(\boldsymbol{t})$ ו x. ממשפט מצוסקה־זריצקי [8, טענה 10.5.4] אנו מקבלים ש $f(T_1,\dots,T_{e-1},U+VT_1,X)$ אי פריק בחוג $E[T_1,\dots,T_{e-1},X]$.

עתה מלמת ברטיני־נתר [8, טענה 10.4.2] קיים $c(U,V)\in L[U,V]$ שונה מאפס כך שהפולינום $f(T_1,\dots,T_{e-1},\alpha_e+\beta_eT_1,X)$ נשאר אי פריק לחלוטין מעל L עבור כל $\alpha_e,\beta_e\in L$ המקיימים $c(\alpha_e,\beta_e)\neq 0$. היות ו K אינסופי קיימים $\alpha_e,\beta_e\in K$, $\beta_e\neq 0$ כך ש $c(\alpha_e,\beta_e)\neq 0$ ו $h(T_1,\dots,T_{r-1},\alpha_e+\beta_eT_1)\neq 0$. באינדוקציה על e נקבל $\alpha_i,\beta_i\in K$, $\beta_i\neq 0$, $i=2,\dots,e$ כך ש $g(T,X)=f(T,\alpha_2+\beta_2T,\dots,\alpha_e+\beta_eT,X)$ אי פריק לחלוטין מעל K ו $h(T,\alpha_2+\beta_2T,\dots,\alpha_e+\beta_eT)\neq 0$.

נרחיב את הייחוד $\boldsymbol{t}\mapsto(u,\alpha_2+\beta_2u,\dots,\alpha_e+\beta_eu)$ לאתר־L φ של F ונסמן ב $F_0/K(u)$ את הרחבת שדות השאריות המתאימה ל $F/K(\boldsymbol{t})$. לפי למה 2.4.1 מתקיים $F_0=L(u,x_0)$, באשר $x_0=\varphi(x)$ הוא שורש $g(u,X)$. בפרט F_0 רגולרי מעל L. האתר φ משרה פתרון גאומטרי חלש $\varphi^*\colon\mathrm{Gal}(K(u))\to\mathrm{Gal}(F/K(\boldsymbol{t}))$ של (μ_u,α) עם שדה שאריות F_0. אבל

$$\begin{aligned}[F_0:K(u)] &= [F_0:L(u)][L:K]=\deg_X g(u,X)[L:K]=\deg_X f(\boldsymbol{t},X)[L:K]\\ &= [F:L(\boldsymbol{t})][L:K]=[F:K(\boldsymbol{t})]\end{aligned}$$

ולכן φ^* על. ■

2.5 מכפלות זר

בפרק זה אנו עומדים להציג את מכפלות הזר, ובאופן יותר כללי את מכפלות הזר השזורות.

2.5.1 הגדרה

יהיו A, $G_0 \leq G$ חבורות סופיות. נניח ש G_0 פועלת על A (מימין). יהי

$$\mathrm{Ind}_{G_0}^G(A) = \{f\colon G \to A \mid f(\sigma\tau) = f(\sigma)^\tau,\ \ \forall \sigma \in G, \tau \in G_0\} \cong A^{(G:G_0)}.$$

כאן הכפל מוגדר לפי רכיבים. אזי G פועלת על ידי הזזה על $\mathrm{Ind}_{G_0}^G(A)$, כלומר $f^\sigma(\tau) = f(\sigma\tau)$. **מכפלת הזר השזורה** היא המכפלה החצי ישרה

$$A \operatorname{wr}_{G_0} G = \mathrm{Ind}_{G_0}^G(A) \rtimes G,$$

כלומר, ניתן להציג איבר של $A \operatorname{wr}_{G_0} G$ באופן יחיד כמכפלה $f\sigma$, באשר $f \in \mathrm{Ind}_{G_0}^G(A)$ ו $\sigma \in G$. הכפל ניתן, תחת הצגה זו, על ידי $(f\sigma)(g\tau) = fg^{\sigma^{-1}}\sigma\tau$.
מכפלת הזר השזורה מצוידת בההעתקת המנה $\alpha\colon A \operatorname{wr}_{G_0} G \to G$ המוגדרת על ידי $\alpha(f\sigma) = \sigma$.

כאשר $G_0 = 1$, מכפלת הזר השזורה נקראת **מכפלת זר**. נקצר את הסימון $A \operatorname{wr}_1 G$ ונרשום $A \operatorname{wr} G$.

ניתן לשכן את $A \rtimes G_0$ ב $A \operatorname{wr}_{G_0} G$.

למה 2.5.1 *לכל $a \in A$ נגדיר $f_a \in \mathrm{Ind}_{G_0}^G(A)$ על ידי*

$$f_a(\sigma) = \begin{cases} a^\sigma & \sigma \in G_0 \\ 1 & \text{אחרת} \end{cases}$$

אזי $\rho\colon A \rtimes G_0 \to A \operatorname{wr}_{G_0} G$ המוגדר על ידי $\rho(a\sigma) = f_a\sigma$ הוא מונומורפיזם.

הוכחה. ברור ש ρ חח"ע ומכיוון ש $(f_a)^\tau = f_{a^\tau}$ לכל $a \in A$ ו $\tau \in G_0$ נקבל ש ρ גם הומומורפיזם. ■

2.5.2 מכפלות זר שזורות ובעיות שיכון

התוצאה הבאה מחזקת את למה 2.2.1 במקרה של בעיות שיכון עם מכפלות זר שזורות.

למה 2.5.2 *תהי $(\varphi\colon \Gamma \to G, \alpha\colon A \operatorname{wr}_{G_0} G \to G)$ בעית שיכון סופית עבור חבורה פרוסופית Γ ויהי $\theta\colon \Gamma \to A \operatorname{wr}_{G_0} G$ פתרון חלש. נניח ש $A = \{f_a \mid a \in A\} \leq \theta(\Gamma)$. אז θ פתרון.*

הוכחה. התמונה של θ היא שמורת־G ולכן $A^\sigma \le \theta(\Gamma)$ לכל $\sigma \in G$. נסיק כי

$$\operatorname{Ind}_{G_0}^G(A) = \prod_{\sigma\in G} A^\sigma \le \theta(\Gamma).$$

אבל $\operatorname{Ind}_{G_0}^G(A) = \ker(\alpha)$; לכן מלמה 2.2.1 נובע ש θ פתרון. ■

יש קשר עמוק בין בעיות שיכון למכפלות זר שזורות. אחת התוצאות מקשר זה היא משפט היהלום של הרן [11]. אנחנו נביא תוצאה פשוטה ברוח הקשר הזה, אך ראשית הכנה.

ההעתקה $\pi\colon \operatorname{Ind}_{G_0}^G(A) \rtimes G_0 \to A \rtimes G_0$ המוגדרת על ידי $\pi(f\sigma) = f(1)\sigma$ היא אפימורפיזם. אכן, זה ברור ש π על. עתה לכל $f \in \operatorname{Ind}_{G_0}^G(A)$ ו $\sigma \in G_0$ מתקיים

$$\pi(f^\sigma) = f(\sigma) = f(1)^\sigma = \pi(f)^\sigma,$$

ולכן π הוא הומומורפיזם. נקרא להעתקה π **העתקת שפירו**. נשים לב שההעתקה ρ שהוגדרה בלמה 2.5.1 היא חתך של π, כלומר $\pi\rho$ היא העתקת הזהות על $A \rtimes G_0$.

למה 2.5.3 *יהיו $\Gamma \le \Lambda$ חבורות פרוסופיות. יהי $\nu\colon \Lambda \to G$ אפימורפיזם על חבורה סופית, יהי $G_0 = \nu(\Gamma)$ ונקבע $\mu = \nu|_\Gamma$. נניח כי G_0 פועל על חבורה סופית A ויהי θ פתרון חלש של $(\nu\colon \Lambda \to G, \alpha\colon A \operatorname{wr}_{G_0} G \to G)$. אזי $\eta = \pi\theta|_\Gamma$ מוגדר היטב ומהווה פתרון חלש של $(\mu\colon \Gamma \to G_0, \beta\colon A \rtimes G_0 \to G_0)$.*

הוכחה. ראשית, כיוון ש $\alpha\theta(\Gamma) = \nu(\Gamma) = G_0$ מתקיים $\theta(\Gamma) \le \operatorname{Ind}_{G_0}^G(A) \rtimes G_0$. לכן $\eta = \pi\theta|_\Gamma$ מוגדר היטב. ברור עתה ש η פתרון חלש של (μ,β). ■

נצטרך את הטענה הטכנית הבאה.

למה 2.5.4 *תהי $A \operatorname{wr}_{G_0} G$ מכפלת זר שזורה של חבורות סופיות. את העתקת שפירו המתאימה נסמן ב $\pi\colon \operatorname{Ind}_{G_0}^G(A) \rtimes G_0 \to A \rtimes G_0$. יהי $i\colon G_0 \to A \rtimes G_0$ חתך כלשהו של העתקת המנה $\alpha_0\colon A \rtimes G_0 \to G_0$. אזי קיים חתך $j\colon G \to A \operatorname{wr}_{G_0} G$ של העתקת המנה $\alpha\colon A \operatorname{wr}_{G_0} G \to G$ כך ש $j(\sigma) \in \operatorname{Ind}_{G_0}^G(A) \rtimes G_0$ וגם $\pi(j(\sigma)) = i(\sigma)$ לכל $\sigma \in G_0$.*

הוכחה. לכל $\sigma \in G_0$ נגדיר $a_\sigma = i(\sigma)\sigma^{-1}$, כלומר $i(\sigma) = a_\sigma\sigma$. כיוון ש i הומומורפיזם, עבור כל $\sigma,\tau \in G_0$ מתקיים

$$a_{\sigma\tau} = a_\sigma a_\tau^{\sigma^{-1}}. \tag{2.5}$$

(נשים לב שכשמציבים $\sigma = \tau = 1$ מקבלים $a_1 = 1$.) נבחר קבוצת מייצגים R של המחלקות השמאליות של G_0 ב G, כלומר כל $\sigma \in G$ ניתן לכתיבה באופן יחיד כ $\sigma = \sigma'\rho$, $\sigma' \in G_0$ ו $\rho \in R$. נניח גם ש $1 \in R$. עתה נגדיר $a_\sigma = a_{\sigma'}$.

השוויון (2.5) ממשיך להתקיים תחת הרחבת ההגדרה לכל $\sigma \in G_0$ ו $\tau \in G$. אכן, נניח ש $\tau = \tau'\rho$, $\tau' \in G_0$ ו $\rho \in R$. אזי $a_\tau = a_{\tau'}$ ו $a_{\sigma\tau} = a_{\sigma\tau'}$. משויון (2.5) עם $\sigma, \tau' \in G_0$ נקבל כי

$$a_{\sigma\tau} = a_{\sigma\tau'} = a_\sigma a_{\tau'}^{\sigma^{-1}} = a_\sigma a_\tau^{\sigma^{-1}},$$

כדרוש. כדי להגדיר את j מספיק עתה לבנות $f_\sigma \in \mathrm{Ind}_{G_0}^G(A)$ לכל $\sigma \in G$ כך ש

$$f_\sigma(1) = a_\sigma, \tag{2.6}$$

$$f_{\sigma\tau}(\rho) = f_\sigma(\rho) f_\tau(\sigma^{-1}\rho) \tag{2.7}$$

לכל $\sigma, \tau \in G$. אכן, אם עשינו זאת, אז היינו מגדירים $j(\sigma) = f_\sigma\sigma$ והיה מתקיים $j(\sigma) \in \mathrm{Ind}_{G_0}^G(A) \rtimes G_0$. השוויון (2.7) גורר ש j הוא הומומורפיזם והשויון (2.6) גורר ש $\pi(j(\sigma)) = i(\sigma)$ לכל $\sigma \in G_0$. (נשים לב שההצבה $\tau = \rho = 1$ ב (2.7) נותנת $f_1(\sigma^{-1}) = f_\sigma(1)^{-1} f_\sigma(1) = 1$, כלומר $f_1 = 1$.)

נגדיר $f_\tau(\sigma) = a_{\sigma^{-1}}^{-1} a_{\sigma^{-1}\tau}$ (הגדרה זו באה מ (2.7) עם $\rho = 1$ ו (2.6)). אזי, בברור, (2.6) מתקיים. עבור $\sigma, \tau, \rho \in G$ מתקיים

$$f_\sigma(\rho) f_\tau(\sigma^{-1}\rho) = a_{\rho^{-1}}^{-1} a_{\rho^{-1}\sigma} a_{\rho^{-1}\sigma}^{-1} a_{\rho^{-1}\sigma\tau} = a_{\rho^{-1}}^{-1} a_{\rho^{-1}\sigma\tau} = f_{\sigma\tau}(\rho),$$

ולכן (2.7) מתקיים. יהי $\sigma, \tau \in G$ ו $\rho \in G_0$. לפי (2.5), נקבל ש

$$f_\sigma(\tau\rho) = a_{\rho^{-1}\tau^{-1}}^{-1} a_{\rho^{-1}\tau^{-1}\sigma} = (a_{\rho^{-1}} a_{\tau^{-1}}^{\rho})^{-1} a_{\rho^{-1}} a_{\tau^{-1}\sigma}^{\rho} = (a_{\tau^{-1}}^{-1} a_{\tau^{-1}\sigma})^{\rho} = (f_\sigma(\tau))^{\rho},$$

לכן, $f_\sigma \in \mathrm{Ind}_{G_0}^G(A)$, כדרוש. ■

טענה 2.5.5 *תהיינה A ו H חבורות סופיות, תהיינה H_0, G תת חבורות של H ותהי $G_0 = G \cap H_0$. נניח ש H_0, ולכן גם G_0, פועלת על A ושקיים חתך*

$$i\colon G_0 \to A \rtimes G_0 \le A \rtimes H_0$$

של העתקת המנה $A \rtimes G_0 \to G_0$. אזי קיים שיכון $j\colon G \to A \,\mathrm{wr}_{H_0} H$ כך שהתרשים

$$\begin{tikzcd}
G_0 \arrow[d, "j|_{G_0}"'] \arrow[dr, "i"] & \\
\mathrm{Ind}_{H_0}^H(A) \rtimes H_0 \arrow[r, "\pi"] & A \rtimes H_0
\end{tikzcd}$$

חילופי. (כאן π היא העתקת שפירו.)

הוכחה. יהי $f \in \mathrm{Ind}_{G_0}^G(A)$. נשים לב ש G/G_0 משוכן באופן טבעי ב H/H_0 על ידי ההעתקת σG_0 ל σH_0 תמונת השיכון היא $(G \cdot H_0)/H_0$. נרחיב את f ל $\tilde{f}\colon H \to A$ על ידי $\tilde{f}(\sigma h) = f(\sigma)^h$ אם $\sigma \in G$, $h \in H_0$ ו $f(\sigma) = 1$ אם $\sigma \in H \smallsetminus (G \cdot H_0)$.

אזי $\tilde{f} \in \mathrm{Ind}_{H_0}^H(A)$. יתר על כן, ההעתקה $\varphi\colon A \,\mathrm{wr}_{G_0} G \to A \,\mathrm{wr}_{H_0} H$ המוגדרת על ידי $\varphi(f\sigma) = \tilde{f}\sigma$, $f \in \mathrm{Ind}_{G_0}^G(A)$, $\sigma \in G$ היא שיכון.

$$\begin{tikzcd}
G \arrow[r, "j'"'] \arrow[rr, bend left, "j"] & A \operatorname{wr}_{G_0} G \arrow[r, "\varphi"'] & A \operatorname{wr}_{H_0} H \\
G_0 \arrow[u] \arrow[r, "j'"'] \arrow[d, equal] & \mathrm{Ind}_{G_0}^{G}(A) \rtimes G_0 \arrow[u] \arrow[r] \arrow[d, "\pi_0"] & \mathrm{Ind}_{H_0}^{H}(A) \rtimes H_0 \arrow[u] \arrow[d, "\pi"] \\
G_0 \arrow[r, "i"] & A \rtimes G_0 \arrow[r] & A \rtimes H_0
\end{tikzcd}$$

כעת, על פי הלמה הקודמת, עבור $i\colon G_0 \to A \rtimes G_0$ קיים $j'\colon G \to A \operatorname{wr}_{G_0} G$ כך ש $i(\sigma) = \pi_0(j'(\sigma))$ לכל $\sigma \in G_0$. (כאן π_0 זו העתקת שפירו המתאימה ל $A \operatorname{wr}_{G_0} G$.)
יהי $j = \varphi j'$. נוכיח כי $i(\sigma) = \pi(j(\sigma))$ לכל $\sigma \in G_0$.

אכן, יהי $\sigma \in G_0$. נסמן $j'(\sigma) = f\sigma$, $f \in \mathrm{Ind}_{G_0}^{G}(A)$ ואז $j(\sigma) = \varphi(f\sigma) = \tilde{f}\sigma$. לכן

$$\pi(j(\sigma)) = \tilde{f}(1)\sigma = f(1)\sigma = \pi_0(f\sigma) = \pi_0(j'(\sigma)) = i(\sigma),$$

כדרוש. ■

2.5.3 מכפלות זר שזורות בשדות

הגדרה 2.5.6 *תהי $\hat{F}/K$ הרחבת גלואה עם חבורת גלואה $A \operatorname{wr}_{G_0} G$. נסמן בקיצור $I = \mathrm{Ind}_{G_0}^{G}(A)$. לשרשרת התת חבורות*

$$1 \le \{f \in I \mid f(1) = 1\} \le I \le I \rtimes G_0 \le A \operatorname{wr}_{G_0} G$$

מתאים מגדל השדות (בסדר ההפוך)

$$K \subseteq L_0 \subseteq L \subseteq F \subseteq \hat{F}. \tag{2.8}$$

בפרט $G_0 = \mathrm{Gal}(L/L_0)$ ו $G = \mathrm{Gal}(L/K)$. במקרה כזה, אנו נאמר שהמגדל (2.8) **מממש** *את $A \operatorname{wr}_{G_0} G$.*

הערה 2.5.7 *נסתכל בבעיית השיכון $(\mu\colon \mathrm{Gal}(K) \to G, \alpha\colon A \operatorname{wr}_{G_0} G \to G)$, באשר $G = \mathrm{Gal}(L/K)$ ו μ היא העתקת הצמצום. אזי אם המגדל (2.8) מממש את $A \operatorname{wr}_{G_0} G$, אז ההעתקת הצמצום $\theta\colon \mathrm{Gal}(K) \to \mathrm{Gal}(\hat{F}/K)$ היא פתרון של הבעיה.*

הלמה הבאה, של הרן [12], נותנת להוריד בעיות שיכון מתפצלות בעזרת מכפלות זר שזורות.

אך ראשית כמה עובדות. יהיו M שדה ו N/M ו $F/M(t)$ הרחבות גלואה כך ש $N \subseteq F$, F/N רגולרי ו t משתנה. נניח שהעתקת הצמצום

$$\beta\colon \mathrm{Gal}(F/M(t)) \to \mathrm{Gal}(N/M)$$

מתפצלת. אז $F = EN$, באשר E הוא שדה השבת ב F של התמונה של $\mathrm{Gal}(N/M)$ תחת חתך של β. בנוסף E/M רגולרי ו $M(t) \subseteq E$.

יהי $x \in E$ איבר עבורו $E = M(t,x)$ ויהי $f(t,X) = \mathrm{irr}(x, M(t)) \in M[t,X]$ הפולינום האי פריק המתוקן של x. אזי f אי פריק לחלוטין (כיוון ש E/M רגולרי) ו f גלואה מעל $N(t)$ (כיוון ש $F = EN = N(t,x)$).

למה 2.5.8 *תהי M/K הרחבה אלגברית פרידה, יהי u משתנה ונתבונן בבעית השיכון הרציונלית הסופית הבאה*

$$(\mu\colon \mathrm{Gal}(M) \to \mathrm{Gal}(N_1/M), \beta\colon \mathrm{Gal}(F/M(u)) \to \mathrm{Gal}(N_1/M)).$$

בפרט, F/N_1 רגולרי. יהי $f(u,X) \in M[u,X]$ כנ״ל, כלומר f אי פריק לחלוטין, גלואה מעל $N_1(u)$ ושורש של f יוצר את $F/N_1(u)$. נניח שקיימת הרחבת גלואה סופית L/K עבורה מתקיים

(א) $f(u,X) \in L_0(u,X)$, *באשר* $L_0 = L \cap M$,

(ב) $f(u,X)$ *גלואה מעל* $L(u)$ *ו*

(ג) $N_1 \subseteq N$, *באשר* $N = ML$.

נסמן $G = \mathrm{Gal}(L/K)$, $G_0 = \mathrm{Gal}(L/L_0) \cong \mathrm{Gal}(N/M)$, *תהי* $\varphi\colon \mathrm{Gal}(K) \to G$ *העתקת הצמצום ויהי* $A = \ker(\beta) = \mathrm{Gal}(F/N_1(u)) \cong \mathrm{Gal}(FL/N(u))$. *אזי*

$$(\varphi\colon \mathrm{Gal}(K) \to G, \alpha\colon A \,\mathrm{wr}_{G_0}\, G \to G) \tag{2.9}$$

רציונלית. (כאן $\mathrm{Gal}(N_1/M)$ *פועלת על* A *דרך החתך של* β *ו* G_0 *פועלת על* A *דרך ההעתקת המנה* $G_0 \to \mathrm{Gal}(N_1/M)$*.)*

$$\begin{tikzcd}
 & & F \arrow[d, dash, "A"] \\
 & M(t) \arrow[r, dash, "G_0"] \arrow[d, dash] & N(t) \arrow[d, dash] \\
 & M \arrow[r, dash, "N_1"] \arrow[d, dash] & N \arrow[d, dash] \\
K \arrow[r, dash] \arrow[rr, dotted, dash, bend right, "G"'] & L_0 \arrow[r, dash, "G_0"] & L
\end{tikzcd}$$

הוכחה. נבחר $c_1, \dots, c_n$ בסיס של L_0/K ויהי $\boldsymbol{t} = (t_1, \dots, t_n)$ n־יה של משתנים. לפי [12, למה 3.1], קיימים שדות $F_0, \hat{F}_0$ כך ש

(א) $K(\boldsymbol{t}) \subseteq L_0(\boldsymbol{t}) \subseteq L(\boldsymbol{t}) \subseteq F_0 \subseteq \hat{F}_0$ מממש את $A \operatorname{wr}_{G_0} G$,

(ב) $\hat{F}_0/L$ רגולרי ו

(ג) $F_0 = L(\boldsymbol{t})(z)$, באשר $\operatorname{irr}(z, L(\boldsymbol{t})) = f(\sum_1^n c_i t_i, Z) \in L_0[\boldsymbol{t}, X]$.

בפרט, $\theta\colon \operatorname{Gal}(K(\boldsymbol{t})) \to \operatorname{Gal}(\hat{F}_0/K(\boldsymbol{t}))$ פתרון של (2.9) עם שדה שאריות רגולרי מעל L. לכן בעית השיכון היא רציונלית. ■

הערה 2.5.9 *הקשר בין שתי בעיות השיכון לעיל יותר עמוק ממה שהלמה מראה. במאמר [12] הרן מבסס את הקשר הזה ובעזרתו מוכיח את משפט היהלום לשדות הילברטיים. המשפט מכיל תנאי מספיק כללי לכך שהרחבה פרידה של שדה הילברטי תהייה הילברטית.*

מסקנה 2.5.10 *יהי $K \subseteq L \subseteq M$ מגדל של הרחבות אלגבריות פרידות כך ש L/K הרחבת גלואה סופית עם חבורת גלואה $G = \operatorname{Gal}(L/K)$ ותהי A חבורה סופית הניתנת למימוש רגולרי מעל K. אזי בעית השיכון*

$$(\operatorname{res}\colon \operatorname{Gal}(K) \to G, \alpha\colon A \operatorname{wr} G \to G)$$

היא רציונלית.

הוכחה. לפי ההנחה ש A ניתן למימוש רגולרי מעל K קיים F_0 רגולרי מעל K ו $t \in F_0$ כך ש $F_0/K(t)$ הרחבת גלואה סופית עם חבורת גלואה $A = \operatorname{Gal}(F_0/K(t))$. יהי $x \in F_0$ איבר פרימיטיבי ו $f(t,X) = \operatorname{irr}(x, K(t))$. נשתמש בלמה 2.5.8 כאשר $F_1 = F_0M$, $N_1 = M$ ו L כדי לקבל את המסקנה. ■

2.5.4 מכפלות זר כתמורות

לעיתים קרובות מכפלות זר מופיעות בטבע כחבורות של תמורות. להלן נציג את הנושא כפי שנצטרך ולא בכלליות המרבית, ראה למשל [22] בשביל המקרה הכללי.

יהיו A, G חבורות סופיות. ונניח ש A פועלת על קבוצה X. אזי $A \operatorname{wr} G$ פועלת על $X \times G$ לפי הכלל הבא.

$$(f\sigma)(x,\tau) = (f(\sigma\tau)x, \sigma\tau), \quad \forall f\sigma \in A \operatorname{wr} G,\ x \in X, \tau \in G.$$

פעולה זו אכן מוגדרת היטב כי

$$\begin{aligned} f\sigma f'\sigma'(x,\tau) &= f\sigma(f'(\sigma'\tau)x, \sigma'\tau) = (f(\sigma\sigma'\tau)(f'(\sigma'\tau)x), \sigma\sigma'\tau) \\ &= (ff'^{\sigma^{-1}}(\sigma\sigma'\tau)x, \sigma\sigma'\tau) = ff'^{\sigma^{-1}}\sigma\sigma'(x,\tau) \end{aligned}$$

טענה 2.5.11 *אם פעולת A על X נאמנה (בהתאמה, טרנזיטיבית), אז כך היא גם פעולת $A \operatorname{wr} G$ על $X \times G$.*

הוכחה. ברור. ■

חבורה A היא **ממעלה** n, אם A פועלת בנאמנות על קבוצה X בעלת n אברים. חבורת הסימטריה S_n היא מרבית ביחס לתכונה שכל חבורה ממעלה n ניתנת לשיכון ב S_n כחבורת תמורות. עתה נראה ש $S_n \operatorname{wr} G$ היא חבורת התמורות ה״מקסימלית״ כאשר מסתכלים על חבורות תמורות עם אפימורפיזם על G שגרעינו ממעלה n.

ביתר דיוק, יהי $\alpha\colon H \to G$ אפימורפיזם של חבורות סופיות. תהי X קבוצה בעלת n אברים. נאמר ש H **פועלת היטב** על $X \times G$ אם H פועלת על $X \times G$, הפעולה טרנזיטיבית, נאמנה וכל $h \in H$ מעתיק באופן חחעל את $X \times \{\tau\}$ על $X \times \{\alpha(h)\tau\}$ לכל $\tau \in G$. בפרט, כל $h \in H$ ו $\tau \in G$ מגדירים תמורה $h_\tau \in S_X$ על פי הנוסחא

$$h(x,\tau) = (h_\tau(x), \alpha(h)\tau).$$

עבור $h_1, h_2 \in H$, $g_1 = \alpha(h_1), g_2 = \alpha(h_2) \in G$ ו $(x,\tau) \in X \times G$, מתקיים

$$\begin{aligned}((h_1h_2)_\tau(x), g_1g_2\tau) &= (h_1h_2)(x,\tau) = h_1((h_2)_\tau(x), g_2\tau) \\ &= ((h_1)_{g_2\tau}(h_2)_\tau(x), g_1g_2\tau)\end{aligned}$$

ולכן

$$(h_1h_2)_\tau = (h_1)_{g_2\tau}(h_2)_\tau. \tag{2.10}$$

תהי A חבורה טרנזיטיבית ממעלה n. אזי מכפלת הזר $A \operatorname{wr} G$ פועלת היטב על $X \times G$. התוצאה הבאה מראה שמכפלת הזר $S_n \operatorname{wr} G$ היא מרבית ביחס לחבורות שפועלות היטב.

למה 2.5.12 *תהי $X = \{1,\dots,n\}$, תהי $\alpha\colon S_n \operatorname{wr} G \to G$ העתקת המנה ויהי $\beta\colon H \to G$ אפימורפיזם של חבורות סופיות. נניח ש H פועלת היטב על $X \times G$. אזי קיים שיכון $\nu\colon H \to S_n \operatorname{wr} G$ המכבד את הפעולות על $X \times G$ כך ש $\alpha\nu = \beta$.*

הוכחה. נגדיר

$$\nu\colon H \to S_n \operatorname{wr} G, \qquad \nu(h) = f_h g,$$

באשר $g = \beta(h)$ ו $f_h(\sigma)(x) = h_{g^{-1}\sigma}(x)$, לכל $x \in X$. ברור ש $\alpha\nu = \beta$. יתר על כן ν מכבד את הפעולות על $X \times G$. אכן,

$$\nu(h)(x,\tau) = (f_h(\beta(h)\tau)x, \beta(h)\tau) = (h_\tau(x), \beta(h)\tau) = h(x,\tau).$$

כיוון שהפעולות של H ושל $S_n \operatorname{wr} G$ הן נאמנות, נובע כי ν חח״ע. נותר להראות ש ν הומומורפיזם.

כיוון ש $\nu(h_1h_2) = f_{h_1h_2}g_1g_2$ ו $\nu(h_1)\nu(h_2) = f_{h_1}f_{h_2}^{g_1^{-1}}g_1g_2$, מספיק לוודא ש $f_{h_1h_2} = f_{h_1}f_{h_2}^{g_1^{-1}}$. ואכן, לפי (2.10)

$$\begin{aligned} f_{h_1h_2}(\sigma)(x) &= (h_1h_2)_{g_2^{-1}g_1^{-1}\sigma}(x) = (h_1)_{g_1^{-1}\sigma}(h_2)_{g_2^{-1}g_1^{-1}\sigma}(x) = \\ &= f_{h_1}(\sigma)f_{h_2}(g_1^{-1}\sigma)(x) = (f_{h_1}f_{h_2}^{g^{-1}})(\sigma)(x) \end{aligned}$$

כדרוש. ∎

2.5.5 משפט השיכון

למכפלת הזר התכונה המעניינת שכל ההרחבות של A ו G משוכנות במכפלת הזר $A \operatorname{wr} G$. אנו לא נשתמש בתוצאה זו.

משפט 2.5.13 *תהי*

$$1 \longrightarrow A \longrightarrow H \xrightarrow{\pi} G \longrightarrow 1$$

סדרה מדויקת קצרה של חבורות סופיות. אזי קיים שיכון $i\colon H \to A \operatorname{wr} G$ כך ש $\alpha i = \pi$, באשר $\alpha\colon A \operatorname{wr} G \to G$ היא העתקת ההטלה.

ניתן למצוא הוכחה ב [22, מסקנה 2.10].

פרק 3

בעיות שיכון כפולות והרחבות מעין סגורות אלגברית

פרק זה מהווה את עמוד השדרה של עבודת המחקר. חקר תורת גלואה של שדה K מתבצע בעזרת בעיות שיכון סופיות. אנו מציגים בפרק זה הכללה של מושג בעיות שיכון להרחבות של שדות – *בעיות שיכון כפולות* עבור הרחבת שדות K/K_0. בעית שיכון כפולה מורכבת משתי בעיות שיכון תואמות – אחת עבור K והשנייה עבור K_0.

תוצאה ידועה (למרות שמנוסחת במינוח שונה) היא שכל פתרון לבעית שיכון גאומטרית עבור שדה מעין סגור אלגברית הוא גאומטרי (ראה סעיף 2.4.2 להגדרות). באופן מקביל אנו מאפיינים את תכונת המעין סגירות אלגברית של הרחבה בעזרת קיום של פתרונות גאומטריים של בעיות שיכון כפולות מסוימות.

באופן מפתיע הרחבות מעין סגורות אלגברית מקיימות תכונה חזקה יותר מקיום פתרון גאומטרי – כל פתרון חלש של בעית שיכון עבור K (תחת הנחת רגולריות מסוימת) ניתן להרמה לפתרון גאומטרי של בעית השיכון הכפולה. תכונה מרכזית זו נקראת *תכונת ההרמה* והיא התוצאה המרכזית של הפרק. בנוסף אנו מראים שכאשר K_0 שדה נוצר סופית יש תכונת הרמה חזקה עוד יותר, למרות שהיא יותר טכנית.

הגישה התורת חבורתי הזו יעילה מאוד. בפרקים הבאים נשתמש בה כדי לחקור את מבנה גלואה של הרחבות מעין סגורות אלגברית ולשימושים נוספים.

3.1 תכונות בסיסיות של הרחבות מעין סגורות אלגברית

נתחיל בהגדרת שדה מעין סגור אלגברית.

הגדרה 3.1.1 *שדה K הוא* **מעין סגור אלגברית** *אם לכל יריעה אי פריקה לחלוטין המוגדרת מעל K יש נקודה רציונלית־K.*

במאמר [16] ירדן ורזון הכלילו את ההגדרה עבור שדה ותת קבוצה.

הגדרה 3.1.2 שדה K נקרא **הרחבה מעין סגורה אלגברית** של תת קבוצה K_0 אם לכל יריעה אי פריקה לחלוטין ממימד $e \geq 1$ המוגדרת מעל K ולכל ההעתקה פרידה רציונלית ושולטת $\nu\colon V \to \mathbb{A}^e$ קיים $\boldsymbol{b} \in V(K)$ כך ש $\boldsymbol{a} = \nu(\boldsymbol{b}) \in K_0^e$.

הערה 3.1.3 בעבודה זו נתמקד במקרה בו K_0 תת שדה ולכן אנו משתמשים במינוח הרחבה.

הערה 3.1.4 אם K/K_0 מעין סגור אלגברית, אז K_0 חייב להיות אינסופי. אכן, אם K_0 היה סופי, אז גם $\nu^{-1}(K_0^e)$ היה סופי. לכן היינו מקבלים של $\tilde{V} = V \smallsetminus \nu^{-1}(K_0^e)$ אין אף נקודה $\boldsymbol{b} \in \tilde{V}(K)$ עבורה $\nu(\boldsymbol{a}) \in K_0^e$.

הערה 3.1.5 אם הרחבה K/K_0 היא מעין סגורה אלגברית, אז ברור שהשדה K הוא מעין סגור אלגברית. בפרט, K הוא מעין סגור אלגברית אם ורק אם ההרחבה K/K מעין סגורה אלגברית.

למשל אם K הוא הרחבת $\mathbb{Z}_l$ של שדה סופי ראשוני $\mathbb{F}_p$, אזי K הוא מעין סגור אלגברית. כל תת שדה נאות של K הוא סופי, ולכן K אינו הרחבה מעין סגורה אלגברית של אף תת שדה נאות.

גם באיפיון 0 יש שדה מעין סגור אלגברית K שאינו הרחבה מעין סגורה אלגברית של אף תת שדה נאות (מסקנה 4.2.2).

הטענה הבאה מביאה הגדרות שקולות של הרחבות מעין סגורות אלגברית במונחים של פולינומים ואתרים, וכוללת רדוקציה לעקומות מישוריות. ההוכחה של הטענה מופיעה ברובה ב [16]. למען השלמות, נביא כאן הוכחה פורמלית.

טענה 3.1.6 התנאים הבאים שקולים עבור הרחבת שדות K/K_0.

(3.1.6א) K/K_0 מעין סגור אלגברית.

(3.1.6ב) עבור כל פולינום $f(\boldsymbol{T}, X) \in K[T_1, \ldots, T_e, X]$ אי פריק לחלוטין ופריד ב X וכל $r(\boldsymbol{T}) \in K[\boldsymbol{T}]$ שונה מאפס קיים $(\boldsymbol{a}, b) \in K_0^e \times K$ עבורו $r(\boldsymbol{a}) \neq 0$ ו $f(\boldsymbol{a}, b) = 0$.

(3.1.6ג) עבור כל פולינום $f(T, X) \in K[T, X]$ אי פריק לחלוטין ופריד ב X וכל $r(T) \in K[T]$ שונה מאפס קיים $(a, b) \in K_0 \times K$ עבורו $r(a) \neq 0$ ו $f(a, b) = 0$.

(3.1.6ד) עבור כל הרחבה רגולרית נוצרת סופית E/K עם בסיס נעלות מפריד $\boldsymbol{t} = (t_1, \ldots, t_e)$ וכל $r(\boldsymbol{t}) \in K(\boldsymbol{t})$ שונה מאפס, קיים אתר־K φ של E שאינו מסועף מעל $K(\boldsymbol{t})$ כך ש $\bar{E} = K$, $\overline{K_0(\boldsymbol{t})} = K_0$, $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי ו $r(\boldsymbol{a}) \neq 0, \infty$.

(3.1.6ה) עבור כל הרחבה רגולרית נוצרת סופית E/K ממעלת נעלות 1 עם בסיס נעלות מפריד t וכל $r(t) \in K[t]$ שונה מאפס קיים אתר־K φ של E שאינו מסועף מעל $K(t)$ כך ש $\bar{E} = K$, $\overline{K_0(t)} = K_0$, $a = \varphi(t) \neq \infty$ ו $r(a) \neq 0, \infty$.

הוכחה. ב [16, למה 1.3] מוכחים השקילויות בין (3.1.6א), (3.1.6ב) ו (3.1.6ג). ברור שמ (3.1.6ד) נובע (3.1.6ה). לכן מספיק להראות ש (3.1.6ב) גורר את (3.1.6ד) וש (3.1.6ה) גורר את (3.1.6ג).

(3.1.6ב) $\Leftarrow$ (3.1.6ד): יהי $x \in E/K(\boldsymbol{t})$ שלם מעל $K[\boldsymbol{t}]$ כך ש $E = K(\boldsymbol{t}, x)$. יהי $f(\boldsymbol{T}, X) \in K[\boldsymbol{T}, X]$ הפולינום האי פריק לחלוטין שהוא פריד ומתוקן ב X המקיים $f(\boldsymbol{t}, x) = 0$. יהי $g(\boldsymbol{t}) \in K[\boldsymbol{t}]$ הפולינום השונה מאפס הניתן בלמה 2.4.1 עבור $E/K(\boldsymbol{t})$ ו x. על פי ההנחה קיים $(\boldsymbol{a}, b) \in K_0^e \times K$ כך ש $f(\boldsymbol{a}, b) = 0$ ו $g(\boldsymbol{a})r(\boldsymbol{a}) \neq 0, \infty$. נרחיב את הייחוד $\boldsymbol{t} \mapsto \boldsymbol{a}$ לאתר־K φ של E המקיים את התכונות הבאות ונסיים את ההוכחה: (1) $\varphi(x) = b \neq \infty$ (זה מתקיים כיוון ש x שלם מעל $K[\boldsymbol{t}]$); (2) $\overline{K_0(\boldsymbol{t})} = K_0$ ו $\bar{E} = K(b) = K$ (למה 2.4.1); (3) φ לא מסועף מעל $K(\boldsymbol{t})$ (למה 2.4.1).

(3.1.6ה) $\Leftarrow$ (3.1.6ג): יהיו $f(T, X) = \underbrace{\sum_{k=0}^{n}} a_k(T)X^k$ ו $r(T)$ כמו ב (3.1.6ג). יהי $r'(T) = r(T)a_n(T)$. יהיו t משתנה ו $x \in K(t)$ כך ש $f(t, x) = 0$. נסמן $E = K(t, x)$. אזי E רגולרי מעל K ופריד מעל $K(t)$. התנאי (3.1.6ה) עבור E ו $r'(t)$ נותן אתר φ של E המקיים את התכונות הבאות. (1) $a = \varphi(t) \in K_0$ מה שגורר ש $b = \varphi(x)$ סופי (כיוון ש $\varphi(f(t, x)) = 0$ ול $f(a, X)$ מקדם מוביל שונה מאפס); (2) $\bar{E} = K$ מה שמסיים את ההוכחה כיוון ש $b \in \bar{E} = K$. ■

3.2 פתרונות גאומטריים והרחבות מעין סגורות אלגברית

התוצאה הבאה מאפיינת מתי פתרון חלש לבעית שיכון הוא גאומטרי בעזרת אתר רציונלי של הרחבה רגולרית מסוימת. התוצאה משפרת עבודות קודמות של Roquette על שדות הילברטיים מעין סגורים אלגברית [8, מסקנה 27.3.3] ושל הרן־ירדן־פריד על שדות פרובניוס [8, טענה 24.1.4].

טענה 3.2.1 *יהי K שדה ותהי*

$$(\mu\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K), \alpha\colon \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K))$$

בעית שיכון עבור K כמו ב (2.2), כלומר E/K רגולרי ו $L = F \cap K_s$. יהי $\theta\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ פתרון חלש. אזי קיימת הרחבה פרידה סופית $\hat{E}/E$ כך ש $\hat{E}$ רגולרי מעל K ולכל אתר רציונלי־K φ של E/K שאינו מסועף ב F

$\varphi^* = \theta$ אם ורק אם φ ניתן להרחבה לאתר רציונלי־K של $\hat{E}$.

הוכחה. נתחיל במקרה הפשוט, כאשר $\mathrm{Gal}(F/E) \cong \mathrm{Gal}(L/K)$. אזי לבעית השיכון (2.2) יש פתרון יחיד (והוא $\alpha^{-1}\mu$). לפיכך, מכיוון ש φ^* הוא פתרון חלש, חייב להתקיים ש $\varphi^* = \theta$, והטענה מוכחת כאשר $\hat{E} = E$.

נעבור עתה למקרה הכללי. תהי M/K הרחבת גלואה סופית כך שמתקיים $\mathrm{Gal}(M) = \ker(\theta)$ (ובפרט $L \subseteq M$) ויהי $\hat{F} = FM$.

$$\begin{tikzcd}
& F \arrow[r, dash] \arrow[d, dash] & \hat{F} \arrow[d, dash] \\
E \arrow[r, dash] \arrow[d, dash] \arrow[urr, dotted, dash, "\hat{E}"] & EL \arrow[r, dash] \arrow[d, dash] & EM \arrow[d, dash] \\
K \arrow[r, dash] & L \arrow[r, dash] & M
\end{tikzcd}$$

מכיוון ש F ו M מופרדים לינארית מעל L, השדות F ו EM מופרדים לינארית מעל EL. לפי למה 2.3.3 מתקיים

$$\mathrm{Gal}(\hat{F}/E) = \mathrm{Gal}(F/E) \times_{\mathrm{Gal}(L/K)} \mathrm{Gal}(M/K).$$

נגדיר $\hat{\theta}\colon \mathrm{Gal}(K) \to \mathrm{Gal}(\hat{F}/E)$ על ידי $\hat{\theta}(\sigma) = (\theta(\sigma), \sigma|_M)$. יהי $\hat{E}$ שדה השבת של $\hat{\theta}(\mathrm{Gal}(K))$ ב $\hat{F}$. אזי התרשים הבא חילופי:

$$\begin{tikzcd}
& \mathrm{Gal}(K) \arrow[dl, "\hat{\theta}"'] \arrow[d, "\mu"] \arrow[ddl, dotted, "\theta"] \\
\mathrm{Gal}(\hat{F}/\hat{E}) \arrow[r, "\hat{\alpha}"] \arrow[d] & \mathrm{Gal}(M/K) \arrow[d] \\
\mathrm{Gal}(F/E) \arrow[r, "\alpha"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

כאן $\hat{\alpha}$ היא העתקת הצמצום. בפרט $\hat{E}/K$ רגולרי. בנוסף

$$\ker(\hat{\theta}) = \ker(\theta) \cap \mathrm{Gal}(M) = \mathrm{Gal}(M),$$

הווה אומר $\mathrm{Gal}(\hat{F}/\hat{E}) \cong \mathrm{Gal}(M/K)$.

אם φ ניתן להרחבה לאתר רציונלי-K $\hat{\varphi}$ של $\hat{E}$, אז לפי החלק הפשוט $\hat{\varphi}^* = \hat{\theta}$. עתה מלמה 2.4.4 נובע כי $\varphi^* = \theta$.

מצד שני, נניח ש $\varphi^* = \theta$. נרחיב את φ לאתר-M $\hat{\varphi}$ של $\hat{F}$. אזי מ $\mathrm{res}_{\hat{F},F}\hat{\varphi}^* = \varphi^*$ ו $\mathrm{res}_{\hat{F},M}\hat{\varphi}^* = \mathrm{res}_{K_s,M}$ נובע שמתקיים

$$\hat{\varphi}^*(\sigma) = (\varphi^*(\sigma), \sigma|_M) = \hat{\theta}(\sigma),$$

ולכן שדה השאריות של $\hat{E}$ תחת $\hat{\varphi}$ הוא K. (ואכן אם $\bar{x} = \varphi(x)$ עבור $x \in \hat{E}$, אזי $\sigma(\bar{x}) = \varphi(\varphi^*(\sigma)x) = \varphi(x) = \bar{x}$, לכל $\sigma \in \mathrm{Gal}(K)$, ולכן $\bar{x} \in K$.) ■

הערה 3.2.2 *במהלך ההוכחה ראינו שמתקיים $\hat{E} \subseteq FM$, באשר M הוא שדה הפתרון של θ.*

הערה 3.2.3 *בהוכחה הראינו כי* $\ker\hat{\theta} = \mathrm{Gal}(M)$*, כלומר* $\hat{\alpha}$ *הוא איזומורפיזם. לכן מתקיים* $\hat{E}M = \hat{F}$*. לכן ההוכחה היא בעצם ניסוח תורת חבורתי של שיכול שדות.*

טענה 3.2.1 שימושית מאוד. למשל התוצאה הבאה שהיא למעשה ניסוח מחדש של [8, למה 24.1.1] (ללא החלק של איברים בלתי תלוים־p) היא מסקנה ישירה של הטענה.

מסקנה 3.2.4 *כל פתרון חלש של בעית שיכון סופית (2.2) עבור שדה מעין סגור אלגברית* K *הוא גאומטרי.*

הוכחה. לפי טענה 3.2.1 לכל פתרון חלש קיימת הרחבה רגולרית נוצרת סופית $\hat{E}$ של K כך שהפתרון הוא גאומטרי אם ורק אם יש אתר רציונלי K של $\hat{E}$. אולם כיוון ש K מעין סגור אלגברית, תמיד יש אתר כזה. ■

הוכחת למה 24.1.1 של ירדן־פריד מטענה 3.2.1. יהיו K מעין סגור אלגברית, S/R כיסוי גלואה רגולרי ונוצר סופית של חוגים מעל K ו F/E הרחבת שדות המנות. נסמן ב L את הסגור האלגברי של K ב F. יהי E' תת הרחבה של F/E כך שהעתקת הצמצום $\alpha'\colon \mathrm{Gal}(F/E') \to \mathrm{Gal}(L/K)$ על. נניח ויש אפימורפיזם $\gamma\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E')$ כך ש $\alpha\gamma = \nu$, באשר $\nu\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K)$ היא העתקת הצמצום. יהי M שדה השבת של $\ker\gamma$ ב K_s.

צריך להוכיח שיש אפימורפיזם $\varphi\colon S \to M$ כך ש $\varphi(R) = K$ ו $D_\varphi = \mathrm{Gal}(F/E')$.

בסימונים שלנו, γ הוא פתרון של (ν, α'). לפי המסקנה הקודמת $\gamma = \varphi^*$, באשר φ אתר של E שאינו מסועף ב F וכך ששדה השאריות $\bar{E} = K$. לכן

$$.D_\varphi = \varphi^*(\mathrm{Gal}(K)) = \gamma(\mathrm{Gal}(K)) = D_\varphi$$

למעשה ניתן לבחור את φ כך ש $S \subseteq O_\varphi$, כיוון שהדרישה היחידה היא ששדה השאריות של $\hat{E}$ הוא K. ואז $\varphi(S) = \bar{F} = M$ ו $\varphi(R) = \bar{E} = K$. ■

3.3 בעיות שיכון כפולות

בסעיף זה מופיעה ההכללה של בעיות שיכון להרחבות של שדות. מומלץ לקורא להזכר בהגדרות ובסימונים של בעיות שיכון המופיעים, בפרק ההקדמות, אם הוא מרגיש צורך.

3.3.1 הגדרת בעיות שיכון כפולות

תהי K/K_0 הרחבת שדות. **בעית שיכון כפולה** עבור K/K_0 מורכבת משתי בעיות שיכון, אחת $(\mu\colon \mathrm{Gal}(K) \to G, \alpha\colon H \to G)$ עבור K והשנייה

$$(\mu_0\colon \mathrm{Gal}(K_0) \to G_0, \alpha\colon H_0 \to G_0)$$

עבור K_0, שהן *תואמות* במובן הבא: $H \le H_0$, $G \le G_0$ ואם נרשום $i\colon H \to H_0$ ו $j\colon G \to G_0$ עבור ההעתקות השיכון ו $r\colon \mathrm{Gal}(K) \to \mathrm{Gal}(K_0)$ עבור ההעתקת הצמצום, אז התרשים שלהלן הוא חילופי.

$$\begin{tikzcd}
& \mathrm{Gal}(K_0) \arrow[dl, dotted, "\exists\theta_0?"'] \arrow[dr, "\mu_0"] & \\
H_0 \arrow[rr, "\alpha_0"] & & G_0 \\
& \mathrm{Gal}(K) \arrow[uu, "r"] \arrow[dl, dotted, "\exists\theta?"'] \arrow[dr, "\mu"] & \\
H \arrow[uu, hook, "i"] \arrow[rr, "\alpha"] & & G \arrow[uu, hook', "j"']
\end{tikzcd} \tag{3.1}$$

בהנתן בעית שיכון כפולה עבור K/K_0, אנו קוראים לבעית השיכון המתאימה עבור K (בהתאמה K_0) בעית השיכון **התחתונה** (בהתאמה **העליונה**). בעית שיכון כפולה נקראת **סופית** אם הבעיה העליונה סופית (ולכן גם התחתונה). אנו קוראים לה **מתפצלת** אם בעית השיכון העליונה מתפצלת (אבל לאו דוקא התחתונה).

פתרון חלש של בעית שיכון כפולה (3.1) הוא פתרון חלש θ_0 של הבעיה העליונה שמצטמצם לפתרון חלש θ של הבעיה התחתונה (דרך העתקת הצמצום r). במקרה שהרחבת השדות K/K_0 אלגברית ופרידה, אז ההעתקת הצמצום היא בעצם העתקת השיכון ולכן התנאי על θ_0 הוא ש $\theta_0(\mathrm{Gal}(K)) \le H$. כדי להדגיש את קיום θ, בד״כ נתייחס לפתרון חלש של בעית שיכון כפולה כזוג (θ, θ_0) (באשר θ הוא הצמצום של θ_0 ל $\mathrm{Gal}(K)$).

3.3.2 בעיות שיכון כפולות רציונליות

תהי (3.1) בעית שיכון כפולה עבור K/K_0 ונסמן ב L_0 ו L את שדות השבת של $\ker(\mu_0)$ ושל $\ker(\mu)$, בהתאמה. אזי קיימים איזומורפיזמים $\bar{\mu}_0\colon \mathrm{Gal}(L_0/K_0) \to G_0$ ו $\bar{\mu}\colon \mathrm{Gal}(L/K) \to G$. נקבל (כמו במקרה של בעיות שיכון) שהחלפת G_0 ו G עם $\mathrm{Gal}(L_0/K_0)$ ו $\mathrm{Gal}(L/K)$ (והחלפת כל ההעתקות המתאימות) נותן בעית שיכון כפולה שקולה. התאימות של בעית השיכון מתממשת על ידי התנאי $L = L_0K$.

למה 3.3.1 *כל בעית שיכון כפולה שבה הבעיה העליונה רציונלית שקולה לבעית*

שיכון כפולה מהצורה הבאה.

$$\begin{tikzcd}
& \mathrm{Gal}(K_0) \arrow[dr, "\mu_0"] & \\
\mathrm{Gal}(F_0/K(\boldsymbol{t})) \arrow[rr, "\alpha_0"] & & \mathrm{Gal}(L_0/K_0) \\
& \mathrm{Gal}(K) \arrow[uu, "r"] \arrow[dr, "\mu"] & \\
\mathrm{Gal}(F/E) \arrow[uu, hook, "i"] \arrow[rr, "\alpha"] & & \mathrm{Gal}(L/K) \arrow[uu, hook', "j"']
\end{tikzcd} \tag{3.2}$$

יתר על כן, התוצאה נשארת נכונה אפילו כאשר לוקחים $\boldsymbol{t} = t$ משתנה יחיד.

$$\begin{tikzcd}
& & K(\boldsymbol{t}) \arrow[rr, dash] \arrow[dl, dash] \arrow[dd, dash] & & L(\boldsymbol{t}) \arrow[r, dash] \arrow[dl, dash] \arrow[dd, dash] & F \arrow[dd, dash] \\
& K \arrow[rr, dash] \arrow[dd, dash] & & L \arrow[dd, dash] & & \\
& & (L_0 \cap K)(\boldsymbol{t}) \arrow[rr, dash] \arrow[dl, dash] & & L_0(\boldsymbol{t}) \arrow[r, dash] \arrow[dl, dash] & F_0 \\
K_0 \arrow[r, dash] & L_0 \cap K \arrow[rr, dash] & & L_0 & &
\end{tikzcd}$$

הוכחה. תהי (3.1) בעית שיכון כפולה פתירה רגולרית. לפי ההגדרה בעית השיכון העליונה פתירה רגולרית, ולכן ניתן להחליף את בעית השיכון העליונה של (3.1) בבעית שיכון שקולה כמו ב (3.2). בנוסף, מלמה 2.4.5 נובע שניתן לקחת $\boldsymbol{t} = t$.

יהי $F = F_0K$ ו $L = L_0K$. תנאי התאימות נותן ש H ניתנת לשיכון לתוך $\mathrm{Gal}(F_0/K_0(\boldsymbol{t}))$ (בעזרת i) כתת חבורה של $\mathrm{Gal}(F/K(\boldsymbol{t})) \cong \mathrm{Gal}(F_0/(L_0 \cap K)(\boldsymbol{t}))$. יהי $E \subseteq F$ שדה השבת של H, כלומר $H = \mathrm{Gal}(F/E)$. תחת זיהויים אלו ההעתקה $\alpha\colon \mathrm{Gal}(F/K(\boldsymbol{t})) \to \mathrm{Gal}(L/K)$ היא העתקת הצמצום. לכן מ $\alpha(H) = \mathrm{Gal}(L/K)$ נובע ש $E \cap L = K$, ולכן E רגולרי מעל K. ■

הגדרה 3.3.2 *בעית שיכון כפולה (3.2) כמו בלמה לעיל נקראית* **רציונלית**.

הערה 3.3.3 *הכוון ההפוך של הלמה הנ״ל גם תקף. כלומר נניח שנתונים הרחבה רגולרית נוצרת סופית E/K, בסיס נעלות מפריד $\boldsymbol{t}$ של E/K והרחבת גלואה סופית $F_0/K_0(\boldsymbol{t})$ כך ש $E \subseteq F$, באשר $F = F_0K$. אז כל ההעתקות הצמצום ב (3.2) הן על, ועל כן (3.2) מגדיר בעית שיכון כפולה רציונלית עבור K/K_0.*

3.3.3 פתרונות גאומטריים של בעיות שיכון כפולות

ראשית נזכר שפתרון חלש θ של בעית שיכון

$$(\mu\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K), \alpha\colon \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K))$$

הוא גאומטרי אם $\theta = \varphi^*$, עבור איזשהו אתר רציונלי־K φ של E שאינו מסועף ב F. עתה נקרא לפתרון חלש (θ, θ_0) של בעית שיכון כפולה (3.2) **גאומטרי** אם $(\theta, \theta_0) = (\varphi^*, \varphi_0^*)$, באשר φ^* פתרון גאומטרי חלש של בעית השיכון התחתונה ו $\varphi_0 = \varphi|_{K_0}$.

נשים לב שמכיוון ש φ_0^* הוא פתרון חלש של בעית השיכון העליונה, שדה השאריות של $K_0(\boldsymbol{t})$ הוא K_0. בפרט, אם $\varphi(\boldsymbol{t})$ סופי, אז $\varphi(\boldsymbol{t}) \in K_0^e$. בנוסף נבחין שעבור אתר־$K$ של E שאינו מסועף ב F המקיים $\bar{E} = K$ ו $\overline{K_0(\boldsymbol{t})} = K_0$, הזוג (φ^*, φ_0^*) הוא אכן פתרון חלש של (3.2), כיוון ש $\varphi_0^* = \mathrm{res}_{K_s, K_{0s}} \varphi^*$.

3.4 תכונת ההרמה

בסעיף זה ננסח ונוכיח את תכונת ההרמה. תחילה נצמצם את הדיון להרחבות פרידות ואלגבריות על ידי כך שנראה שאם K/K_0 מעין סגור אלגברית, אז מתקיים $K \cap K_{0s}/K_0$ מעין סגור אלגברית ו $\mathrm{Gal}(K) \cong \mathrm{Gal}(K \cap K_{0s})$ תחת העתקת הצמצום. לאחר מכן נאפיין הרחבות מעין סגורות אלגברית שהן פרידות ואלגבריות במונחי פתרונות גאומטריים לבעיות שיכון כפולות. מאיפיון זה תנבע תכונת ההרמה. לבסוף נוכיח תכונת הרמה חזקה (אבל מסובכת) שמקיימים הרחבות מעין סגורות אלגברית של שדות נוצרים סופית.

3.4.1 הרחבות מעין סגורות אלגברית שאינן אלגבריות פרידות

ב [16, מסקנה 1.5], ירדן ורזון מוכיחים את התוצאה הבאה.

למה 3.4.1 (ירדן־רזון) *אם K/K_0 מעין סגור אלגברית, אז גם $K \cap K_{0s}/K_0$ מעין סגור אלגברית.*

יתר על כן, מתקיים:

משפט 3.4.2 *יהי K/K_0 מעין סגור אלגברית. אזי $K \cap K_{0s}/K_0$ מעין סגור אלגברית וגם ההעתקת הצמצום $\mathrm{res}\colon \mathrm{Gal}(K) \to \mathrm{Gal}(K \cap K_{0s})$ היא איזומורפיזם.*

הוכחה. מספיק להראות ש $K_s = K_{0s}K$. תהי L/K הרחבת גלואה סופית עם חבורת גלואה G מסדר n. נשכן את G בתוך חבורת הסימטריה S_n. יהי $F_0/K_0(\boldsymbol{t})$ מימוש רגולרי של S_n (משפט 2.2.4) ונניח ש F_0 בלתי תלוי אלגברית ב K מעל K_0. אזי $F = F_0K$ רגולרי מעל K ו $\mathrm{Gal}(F/K(\boldsymbol{t})) \cong S_n$. מתקיים

$$\begin{aligned}\mathrm{Gal}(FL/K(\boldsymbol{t})) &= \mathrm{Gal}(FL/L(\boldsymbol{t})) \times \mathrm{Gal}(FL/F)\\ &\cong \mathrm{Gal}(F/K(\boldsymbol{t})) \times \mathrm{Gal}(L/K) \cong S_n \times G\end{aligned}$$

יהי E שדה השבת של תת החבורה $\Delta = \{(g,g) \mid g \in G\}$ ב FL. לכן מתקיים $\mathrm{Gal}(FL/E) \cong \Delta$. לפי התאמת גלואה, $S_n\Delta = S_n \times G$ גורר ש $E \cap L = K$ ו $G \cap \Delta = \Delta \cap S_n = 1$ גורר ש $FL = EL = FE$. בפרט, E/K רגולרי.

$$\begin{tikzcd}[arrows=dash]
F \arrow[r] \arrow[d] & FL \arrow[d] \\
K(\boldsymbol{t}) \arrow[r] \arrow[ur, "E" description] \arrow[d] & L(\boldsymbol{t}) \arrow[d] \\
K \arrow[r] & L
\end{tikzcd}$$

יהיו x_F, x_E, x_{FL} איברים פרימיטיבים של $F/K(t)$, $E/K(\boldsymbol{t})$ ו $FL/K(\boldsymbol{t})$, בהתאמה.
תהי $h(\boldsymbol{t}) \in K[\boldsymbol{t}]$ מכפלת הפולנומים המתאימים הניתנים בלמה 2.4.1.
כיוון ש K/K_0 הוא מעין סגור אלגברית, קיים אתר־K φ של E כך ש $\bar{E} = K$, $\overline{K_0(\boldsymbol{t})} = K_0$, $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי ו $h(\boldsymbol{a}) \neq 0$. נרחיב את φ לאתר־L Φ של FL.
אזי, $FL = EL$ גורר ש $\overline{FL} = \overline{EL} = L(\Phi(x_E)) = L$. אולם כיוון ש $F = F_0K$, נקבל ש $\bar{F} = \bar{F}_0K$, לכן $L = \overline{FL} = \overline{FE} = K(\Phi(x_E), \Phi(x_F)) = \bar{F} = \bar{F}_0K \subseteq K_{0s}K$, כנדרש. ■

הערה 3.4.3 *המשפט נובע גם מהתוצאה המרכזית של [26].*

התורה האלמנטרית של שדות מעין סגורים אלגברית מתנהגת יפה. לכן מכיוון שחבורות הגלואה המוחלטות של השדות המעין סגורים אלגברית K ו $K \cap K_{0s}$ איזומורפיות, השדות שקולים אלמנטרית תחת התנאים הסבירים הבאים:

מסקנה 3.4.4 *תהי K/K_0 הרחבה פרידה (לאו דוקא אלגברית) מעין סגורה אלגברית. נניח של K ו $K \cap K_{0s}$ אותה דרגת אי־שכלול[1]. אזי K הוא הרחבה אלמנטרית של $K \cap K_{0s}$.*

הוכחה. התוצאה נובעת מ [8, מסקנה 20.3.4] וממשפט 3.4.2. ■

3.4.2 אפיון הרחבות מעין סגורות אלגברית פרידות ואלגבריות

טענה 3.4.5 *תהי K/K_0 הרחבה פרידה ואלגברית. אזי התנאים הבאים שקולים:*

(3.4.5א) *K/K_0 מעין סגור אלגברית.*

(3.4.5ב) *לכל בעית שיכון כפולה סופית ורציונלית (3.2) עבור K/K_0 ולכל פונקציה רציונלית שונה מאפס $r(\boldsymbol{t}) \in K(\boldsymbol{t})$, קיים פתרון גאומטרי חלש (φ^*, φ_0^*) כך ש $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי ו $r(\boldsymbol{a}) \neq 0, \infty$.*

[1] imperfect degree

(3.4.5ג) *לכל בעית שיכון כפולה סופית ורציונלית (3.2) עבור K/K_0 עם $\boldsymbol{t}=t$ משתנה קיימים אינסוף פתרונות גאומטרים חלשים.*

הוכחה. הגרירה (3.4.5א)$\Leftarrow$(3.4.5ב) נובעת מטענה 3.1.6 (חלק 3.1.6ד) והגדרת פתרון גאומטרי חלש.

הגרירה (3.4.5ב)$\Leftarrow$(3.4.5ג) היא מיידית.

(3.4.5ג)$\Leftarrow$(3.4.5א): נשתמש בטענה 3.1.6 ונראה ש (3.1.6ה) מתקיים. תהי E/K הרחבה רגולרית עם בסיס נעלות מפריד t ויהי $r(t) \in K[t]$ שונה מאפס. נבחר הרחבת גלואה סופית F_0 של $K_0(t)$ כך ש $E \subseteq F_0K$ (קיום F_0 נובע מכך ש K/K_0 פרידה ואלגברית) ויהיו $F = F_0K$, $L = F \cap K_s$ ו $L_0 = F_0 \cap K_{0s}$. לפי ההנחה קיימים אינסוף פתרונות גאומטרים חלשים (φ^*, φ_0^*) של בעית השיכון הכפולה

$$\begin{tikzcd}
 & \mathrm{Gal}(K_0) \arrow[dl, dotted, "\varphi_0^*"'] \arrow[dr] & \\
\mathrm{Gal}(F_0/K_0(t)) \arrow[rr] & & \mathrm{Gal}(L_0/K_0) \\
 & \mathrm{Gal}(K) \arrow[uu] \arrow[dl, dotted, "\varphi^*"'] \arrow[dr] & \\
.\mathrm{Gal}(F/E) \arrow[uu] \arrow[rr] & & \mathrm{Gal}(L/K) \arrow[uu]
\end{tikzcd}$$

כאן כל ההעתקות הן ההעתקות הצמצום. כיוון שרק עבור מספר סופי של פתרונות $\varphi(t)$ אינסופי או $r(\varphi(t)) = 0, \infty$, קיים פתרון המקיים $\varphi(t) \neq \infty$ ו $r(\varphi(t)) \neq 0, \infty$. בפרט, $\bar{E} = K$ ו $\overline{K_0(t)} = K_0$, כדרוש ב (3.1.6ה). ■

תהי K/K_0 הרחבה מעין סגורה אלגברית ונתבונן בבעית שיכון כפולה רציונלית עבור K/K_0. התכונה המרכזית הבאה – תכונת ההרמה – מאפשרת להרים כל פתרון חלש של בעית השיכון התחתונה לפתרון גאומטרי חלש של בעית השיכון הכפולה.

טענה 3.4.6 (תכונת ההרמה) *תהי K/K_0 הרחבה מעין סגורה אלגברית, תהי (3.2) בעית שיכון כפולה סופית ורציונלית עבור K/K_0 ויהי $\theta\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ פתרון חלש של בעית השיכון התחתונה של (3.2). אזי קיים פתרון גאומטרי חלש (φ^*, φ_0^*) של (3.2) כך ש $\theta = \varphi^*$.*

יתר על כן, אם $r(\boldsymbol{t}) \in K(\boldsymbol{t})$ שונה מאפס, ניתן לבחור את φ כך ש $\boldsymbol{a} = \varphi(\boldsymbol{t}) \in K_0^e$ ו $r(\boldsymbol{a}) \neq 0, \infty$.

הוכחה. לפי טענה 3.2.1 קיימת הרחבה פרידה ואלגברית $\hat{E}/E$ שהיא רגולרית מעל K בעלת התכונה הבאה. אם Φ אתר רציונלי-K של $\hat{E}$ ואם $\varphi = \Phi|_E$ לא מסועף ב F, אז $\varphi^* = \theta$.

עתה מכיוון שההרחבה K/K_0 מעין סגורה אלגברית נובע שקיים אתר רציונלי־ K Φ של $\hat{E}$ כך ש $\varphi = \Phi|_E$ לא מסועף ב F, שדה השאריות של $K_0(\boldsymbol{t})$ הוא K_0, $\boldsymbol{a} = \Phi(\boldsymbol{t})$ סופי ו $r(\boldsymbol{a}) \neq 0, \infty$. נסמן $\varphi_0 = \varphi|_{K_0(\boldsymbol{t})}$. אזי (φ^*, φ_0^*) הוא פתרון גאומטרי חלש ו $\varphi^* = \theta$. ■

מסקנה פשוטה ראשונה מתכונת ההרמה היא הטרנזיטיביות של הרחבות מעין סגורות אלגברית. למיטב ידיעתנו אין בספרות דרך אחרת להוכיח תכונה זו.

למה 3.4.7 *יהי $K_0 \subseteq K_1 \subseteq K_2$ מגדל של הרחבות אלגבריות פרידות. נניח ש K_2/K_1 ו K_1/K_0 הן מעין סגורים אלגברית. אזי K_2/K_0 מעין סגור אלגברית.*

הוכחה. תהי

$$\begin{aligned}((\mu_0 &\colon \mathrm{Gal}(K_0) \to \mathrm{Gal}(L_0/K_0), \alpha_0 \colon \mathrm{Gal}(F_0/K_0(t)) \to \mathrm{Gal}(L_0/K_0),\\ (\mu_2 &\colon \mathrm{Gal}(K_2) \to \mathrm{Gal}(L_2/K_2), \alpha_2 \colon \mathrm{Gal}(F_2/E) \to \mathrm{Gal}(L_2/K_2))\end{aligned}$$

בעית שיכון כפולה, סופית ורציונלית עבור K_2/K_0 (ראה תרשים המופיע למטה). לפי למה 3.4.5 מספיק למצוא פתרון גאומטרי חלש לבעיה זו. יהיו $F_1 = F_0K_1$, $L_1 = L_0K_1$. כיוון ש K_2/K_1 מעין סגור אלגברית קיים גאומטרי חלש $(\varphi_2^*, \varphi_1^*)$ לבעית השיכון הכפולה המוגדרת על ידי החלק התחתון של הדיאגרמה הבאה.

$$\begin{tikzcd}
& \mathrm{Gal}(K_0) \arrow[dl, dotted, "\varphi_0^*"'] \arrow[dr, "\mu_0"] & \\
\mathrm{Gal}(F_0/K_0(t)) \arrow[rr, "\alpha_0"] & & \mathrm{Gal}(L_0/K_0) \\
& \mathrm{Gal}(K_1) \arrow[uu] \arrow[dl, dotted, "\varphi_1^*"'] \arrow[dr, "\mu_1"] & \\
\mathrm{Gal}(F_1/K_1(t)) \arrow[uu] \arrow[rr, "\alpha_1"] & & \mathrm{Gal}(L_1/K_1) \arrow[uu] \\
& \mathrm{Gal}(K_2) \arrow[uu] \arrow[dl, dotted, "\varphi_2^*"'] \arrow[dr, "\mu_2"] & \\
.\mathrm{Gal}(F_2/E) \arrow[uu] \arrow[rr, "\alpha_2"] & & \mathrm{Gal}(L_2/K_2) \arrow[uu]
\end{tikzcd} \tag{3.3}$$

עתה נרים את φ_1^* לפתרון גאומטרי חלש $(\varphi_1^*, \varphi_0^*)$ של הבעיה המוגדרת מהחלק העליון של התרשים. זה אפשרי לפי תכונת ההרמה ביחס להרחבה המעין סגורה אלגברית K_1/K_0. כיוון ש $\varphi_0^*|_{\mathrm{Gal}(K_2)} = \varphi_1^*|_{\mathrm{Gal}(K_2)} = \varphi_2^*$ נקבל ש $(\varphi_2^*, \varphi_0^*)$ פתרון גאומטרי חלש של הבעיה המקורית. ■

טענה 3.4.8 *יהי κ סודר ויהי*

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_\kappa$$

מגדל של הרחבות פרידות אלגבריות. נניח כי $K_{\alpha+1}/K_\alpha$ מעין סגור אלגברית לכל $\alpha < \kappa$ וגם $K_\alpha = \bigcup_{\beta<\alpha} K_\beta$ לכל סודר גבולי $\alpha \leq \kappa$. אזי K_κ/K_0 מעין סגור אלגברית.

הוכחה. נוכיח את הטענה באינדוקציה טרנספיניטית. יהי $\alpha \leq \kappa$. את הצעד העוקב הוכחנו בלמה הקודמת.

יה α סודר גבולי. תהי

$$\begin{tikzcd}
 & \mathrm{Gal}(K_0) \arrow[dr] & \\
\mathrm{Gal}(F_0/K_0(\boldsymbol{t})) \arrow[rr] & & \mathrm{Gal}(L_0/K_0) \\
 & \mathrm{Gal}(K_\alpha) \arrow[uu] \arrow[dr] & \\
\mathrm{Gal}(F_\alpha/E_\alpha) \arrow[uu] \arrow[rr] & & \mathrm{Gal}(L_\alpha/K_\alpha) \arrow[uu]
\end{tikzcd} \tag{3.4}$$

בעית שיכון כפולה ורציונלית עבור K_α/K_0. כאן $F_\alpha = F_0K_\alpha$ ו $L_\alpha = L_0K_\alpha$. עתה מכיוון שההרחבות L_0/K_0 ו $F_0/K_0(\boldsymbol{t})$ סופיות, קיים $\beta < \alpha$ עבורו מתקים $\mathrm{Gal}(F_\alpha/K_\alpha) \cong \mathrm{Gal}(F_\beta/K_\beta)$ ו $\mathrm{Gal}(L_\alpha/K_\alpha) \cong \mathrm{Gal}(L_\beta/K_\beta)$ (תחת העתקת הצמצום המתאימה), באשר $F_\beta = F_0K_\beta$ ו $L_\beta = L_0K_\beta$.

הנחת האינדוקציה נותנת פתרון גאומטרי חלש לבעית השיכון הכפולה (3.4) עם β במקום α. פתרון חלש זה משרה פתרון גאומטרי חלש של (3.4) תחת האיזומורפיזמים לעיל. ■

3.5 תכונת ההרמה החזקה עבור הרחבות מעין סגורות אלגברית של שדות נוצרים סופית

בסעיף זה K_0 מסמן שדה נוצר סופית (מעל השדה הראשוני שלו). נוכיח תכונת הרמה חזקה עבור הרחבות מעין סגורות אלגברית של K_0. הרכיב הנוסף הדרוש הוא השערת מורדל (שהוכחה על ידי פלטינגס באפיון 0 ועל ידי Grauert-Manin באפיון חיובי). הלמה הבאה מבוססת על השערת מורדל:

למה 3.5.1 (**[16, טענה 5.4]**) *יהיו K_0 שדה נוצר סופית אינסופי, $f \in K_0[T,X]$ פולינום אי פריק לחלוטין ופריד ב X, $g \in K_0[T,X]$ פולינום אי פריק ופריד X, ו $0 \neq r \in K_0[T]$. אזי קיימים הרחבה אי פרידה בטהרה K_0' של K_0, פונקציה*

רציונלית לא קבועה $q \in K_0'(T)$ ותת קבוצה סופית B של K_0' כך ש $f(q(T),X)$ אי פריק לחלוטין ולכל $a \in K_0' \smallsetminus B$ $g(q(a),X)$ אי פריק ב $K_0'[X]$ ו $r(q(a)) \neq 0$.

תהי K/K_0 הרחבת שדות תהי (3.2) בעיית שיכון כפולה רציונלית עבור K/K_0 (עם $\boldsymbol{t} = t$). עבור כל תת הרחבה K_1 של K/K_0 מתאימה בעיית שיכון כפולה רציונלית והיא

$$\begin{tikzcd}
 & \mathrm{Gal}(K_1) \arrow[dr, "\mu_1"] & \\
\mathrm{Gal}(F_1/K_1(t)) \arrow[rr, "\alpha_1"] & & \mathrm{Gal}(L_1/K_1) \\
 & \mathrm{Gal}(K) \arrow[uu] \arrow[dr, "\mu"] & \\
,\mathrm{Gal}(F/E) \arrow[uu] \arrow[rr, "\alpha"] & & \mathrm{Gal}(L/K) \arrow[uu]
\end{tikzcd} \tag{3.5}$$

באשר $F_1 = F_0K_1$, $L_1 = L_0K_1$ ו μ_1 ו α_1 הן העתקות הצמצום.

נניח כי K_1'/K_1 הרחבה אי פרידה בטהרה. אזי בעיית השיכון הכפולה (3.5) נשמרת עם נחליף את כל השדות המופיעים בצרוף שלהם עם K_1'.

טענה 3.5.2 (תכונת ההרמה החזקה) *תהי K הרחבה מעין סגורה אלגברית של שדה נוצר סופית K_0. תהי*

$$\mathcal{E}(K) = (\mu\colon \mathrm{Gal}(K) \to \mathrm{Gal}(L/K), \alpha\colon \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K))$$

בעיית שיכון עבור K כמו ב (2.2)[2] ויהי $\theta\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ פתרון חלש של $\mathcal{E}(K)$. אזי קיימות תת הרחבה סופית K_1/K_0 של K/K_0 והרחבה סופית אי פרידה בטהרה K_1'/K_1 עם התכונות הבאות.

(א) לכל בעיית שיכון כפולה רציונלית (3.2) (שבה בעיית השיכון התחתונה היא $\mathcal{E}(K)$), ניתן להרים את θ לפתרון חלש (θ, θ_1) של בעיית השיכון הכפולה (3.5) כך ש θ_1 **על**.

(ב) הפתרון (θ, θ_1) הוא פתרון גאומטרי של בעיית השיכון הכפולה שמקבלים מ (3.5) על ידי החלפת כל השדות בצרוף שלהם עם K_1'.

הוכחה. מטענה 3.2.1 קיימת הרחבה פרידה $\hat{E}/E$ שהיא רגולרית מעל K כך שאתר־K φ של E שאינו מסועף ב F מקיים $\varphi^* = \theta$ אם ורק אם φ ניתן להרחבה לאתר רציונלי־K של $\hat{E}$. יהי $f(t,X) \in K[t,X]$ פולינום אי פריק לחלוטין ששורשו x יוצר את $\hat{E}/K(t)$, כלומר $\hat{E} = K(t,x)$. יהי M שדה השבת של $\ker(\theta)$ בסגור הפריד

[2] כלומר E רגולרי (ומעלת הנעלות היא 1) מעל K, F/E סופית וגלואה, $L = F \cap K_s$ וכל ההעתקות הן העתקות הצמצום.

K_s. אזי M/K הרחבת גלואה סופית. יהי $h(X) \in K[X]$ פולינום גלואה ששורשו יוצר את M/K.

נבחר תת הרחבה סופית K_1 של K/K_0 המכילה את מקדמי f ו h וכך ש h גלואה מעל K_1. יהי M_1 שדה הפיצול של h מעל K_1 ויהיו L_1, F_1 השדות של בעית השיכון הכפולה המתאימה (3.5). אזי $\mathrm{Gal}(M_1/K_1) \cong \mathrm{Gal}(M/K)$, ולפיכך גם $\mathrm{Gal}(L_1/K_1) \cong \mathrm{Gal}(L/K)$.

$$\begin{tikzcd}
 & & & F \arrow[dll, dash] \arrow[ddd, dash] & \\
 & E \arrow[r, dash] \arrow[d, dash] & EL \arrow[rr, dash] \arrow[d, dash] & & EM \arrow[d, dash] \\
 & K(t) \arrow[r, dash] \arrow[dd, dash] & L(t) \arrow[rr, dash] \arrow[dd, dash] & & M(t) \arrow[dd, dash] \\
 & & & F_1 \arrow[dl, dash] & \\
K_0(t) \arrow[r, dash] & K_1(t) \arrow[r, dash] & L_1(t) \arrow[rr, dash] & & M_1(t)
\end{tikzcd}$$

יהי $g(t,X) \in K_1[T,X]$ פולינום אי פריק ששורשו יוצר את $F_1/K_1(t)$. נבחר $r(t) \in K_1(t)$ כך ש $r(a) \neq 0$ גורר שהראשוני $(t-a)$ לא מסועף ב F_1 ושהמקדמים המובילים של $f(t,X)$ ו $g(t,X)$ לא מתאפסים ב a. יהיו K_1'/K_1 ההרחבה האי פרידה בטהרה, $B \subseteq K_1'$ תת הקבוצה הסופית של K_1' ו $q \in K_1'(T)$ הפונקציה הרציונלית שאינה קבועה המתקבלים מלמה 3.5.1 עבור K_1, g, f, ו r. יהי $K' = KK_1'$.

כיוון ש K'/K_1' היא מעין סגורה אלגברית ([16, מסקנה 2.5]), קיימים $a \in K_1' \smallsetminus B$ ו $b \in K'$ עבורם $f(q(a),b) = 0$ (טענה 3.1.6). נרחיב את הייחוד $t \mapsto q(a)$ לאתר רציונלי-K Φ של $\hat{E}K_1'$. אזי $\varphi = \Phi|_{EK_1'}$ לא מסועף ב FK_1' (כיוון ש $r(q(a)) \neq 0$). נסיק כי (φ^*, φ_1^*) פתרון גאומטרי חלש של בעית השיכון הכפולה $((\mu,\alpha),(\mu_1,\alpha_1))$ שמקבלים מ (3.5) על ידי החלפת כל השדות בצרופם עם K_1'.

יתר על כן, כיוון ש $F_1K_1'/K_1'(t)$ נוצר על ידי שורש של $g(t,X)$ ו$g(q(a),X)$ אי פריק, הפתרון φ_1^* הוא על. וסיימנו להוכיח את (ב). סעיף (א) נובע מיידית מסעיף (ב) כיוון ש (φ^*, φ_1^*) הוא פתרון (לאו דוקא גאומטרי) של $((\mu,\alpha),(\mu_1,\alpha_1))$. ■

פרק 4

על מבנה גלואה של הרחבות מעין סגורות אלגברית

במאמר [16] משתמשים ירדן ורזון במשפט פלטינגס כדי להוכיח שכמה הרחבות גלואה של המספרים הרציונלים $\mathbb{Q}$ אינן מעין סגורות אלגברית מעל אף שדה מספרים. אז הם שואלים האם זה צרוף מקרים או תופעה כללית.

במאמר [15] מיישב ירדן את השאלה על ידי כך שהוא מוכיח שההרחבה המעין סגורה אלגברית היחידה של שדה מספרים היא הסגור האלגברי שלו. תוצאה זו מתבססת על משפט הצפיפות של פרובניוס, האיפיון של Neukirch של שדות סגורים p־אדית מבין כל ההרחבות האלגבריות של $\mathbb{Q}$ ועל התכונה המיוחדת של $\mathbb{Q}$ שאין לו תתי שדות נאותים(!).

בהמשך, במאמר משותף עם ירדן [2], אנו משכללים את השיטה של ירדן ורזון ומרחיבים את התשובה של ירדן למשפחה היותר גדולה של שדות נוצרים סופית בעזרת השערת מורדל (שכזכור הוכחה על ידי פלטינגס באיפיון 0 ועל ידי Grauert-Manin באיפיון חיובי).

עתה, בעזרת תכונת ההרמה, ניתן להוכיח מחדש את כל התוצאות הנ״ל בצורה אלמנטרית. ההוכחה החדשה אינה משתמשת בשום תכונה של שדות נוצרים סופית ולכן היא בעצם תקפה לשדה שרירותי K (משפט 4.2.3). תוצאה זו ואחרות (כגון תוצאות ירידה של חבורות גלואה) המופיעות בפרק זה מוכיחות שהדרך ה״נכונה״ להבנת הרחבות מעין סגורות אלגברית עוברת דרך בעיות שיכון כפולות.

4.1 ירידת חבורות גלואה

התוצאה הבאה מאפשרת להוריד חבורות גלואה בהרחבה מעין סגורה אלגברית.

משפט 4.1.1 *תהי K/K_0 הרחבה מעין סגורה אלגברית, תהי $\varphi\colon \mathrm{Gal}(K) \to \mathrm{Gal}(K_0)$ ההעתקת הצמצום ויהי $\theta\colon \mathrm{Gal}(K) \to G$ אפימורפיזם על חבורה סופית G. נניח שקיים שיכון $i\colon G \hookrightarrow G_0$ של G לתוך חבורה סופית G_0 הניתנת למימוש רגולרי*

מעל K_0. אזי קיים הומומורפיזם $\theta_0\colon \mathrm{Gal}(K_0) \to G_0$ כך ש $\theta_0\varphi = i\theta$:

$$\begin{tikzcd} \mathrm{Gal}(K) \arrow[r, "\varphi"] \arrow[d, "\theta"'] \arrow[dr, phantom, "©"] & \mathrm{Gal}(K_0) \arrow[d, "\theta_0"] \\ .G \arrow[r, "i"'] & G_0 \end{tikzcd}$$

הוכחה. ההעתקה $\theta\colon \mathrm{Gal}(K) \to G$ היא פתרון לבעית השיכון התחתונה של בעית השיכון הכפולה

$$\begin{tikzcd} & \mathrm{Gal}(K_0) \arrow[dl, dotted, "\theta_0"'] \arrow[dr] & \\ G_0 \arrow[rr] & & 1 \\ & \mathrm{Gal}(K) \arrow[uu] \arrow[dl, "\theta"'] \arrow[dr] & \\ .G \arrow[uu] \arrow[rr] & & 1 \arrow[uu] \end{tikzcd} \tag{4.1}$$

כיוון ש G_0 ניתנת למימוש רגולרי מעל K הבעיה (4.1) היא רציונלית.

מתכונת ההרמה (טענה 3.4.6), ניתן להרים את θ לפתרון (גאומטרי) חלש (θ, θ_0) של (4.1). ■

במקרה בו $G = G_0$, ממשפט 4.1.1 נובע מיד:

מסקנה 4.1.2 *תהי K/K_0 הרחבה מעין סגורה אלגברית. תהי G חבורה גלואה סופית מעל K הניתנת למימוש רגולרי מעל K_0. אזי G גם חבורת גלואה מעל K_0.*

כיוון שכל חבורה אבלית ניתנת למימוש רגולרי (משפט 2.2.4) אנו מקבלים:

מסקנה 4.1.3 *תהי K/K_0 הרחבה מעין סגורה אלגברית. אזי $K^{\mathrm{ab}} = K_0^{\mathrm{ab}}K$.*

הדבר הבא שנעשה זה להוכיח מחדש את [26, משפט 5] בעזרת משפט 4.1.1 והעובדה שחבורת הסימטריה ניתנת למימוש רגולרי מעל כל שדה. ההוכחה החדשה נותנת תובנה להוכחה המקורית והטכנית של רזון.

מסקנה 4.1.4 (רזון) *תהי K/K_0 הרחבה מעין סגורה אלגברית ותהי L/K הרחבה פרידה ואלגברית. אזי קיימת הרחבה אלגברית פרידה L_0/K_0 המופרדת לינארית מ K מעל K_0 כך ש $L = L_0K$.*

הוכחה. בעזרת הלמה של צורן ניתן להראות שמספיק להוכיח את הטענה כאשר $[L : K] < \infty$. (לא נעשה זאת פה כי זה נעשה בצורה טובה ב [26].)

נניח אם כן ש $[L:K]<\infty$. יהיו M סגור הגלואה של L/K, $G=\mathrm{Gal}(M/K)$, $G'=\mathrm{Gal}(M/L)$ ו $\theta\colon \mathrm{Gal}(K)\to G$ העתקת הצמצום. הפעולה של G על קבוצת המחלקות הימניות $\Sigma=G/G'$ משרה שיכון $i\colon G\to S_\Sigma$.

כיוון ש S_Σ ניתנת למימוש רגולרי (משפט 2.2.4), נובע ממשפט 4.1.1 שקיים הומומורפיזם $\theta_0\colon \mathrm{Gal}(K_0)\to S_\Sigma$ כך ש $\theta_0|_{\mathrm{Gal}(K)}=i\theta$ בפרט, התמונה H של θ_0 מכילה את $i(G)$, ולכן H טרנזיטיבית. אזי $(H:H')=|\Sigma|=[L:K]$, באשר H' הוא המייצב בתוך H של המחלקה הימנית $G'\in\Sigma$. בנוסף, התת חבורה $G'\leq G$ היא המייצב ב G של המחלקה הימנית $G'\in\Sigma$. לכן נקבל כי $H'\cap i(G)=i(G')$. לכן $i^{-1}(H)=G'$.

יהיו M_0 שדה השבת של $\ker(\theta_0)$ (כלומר $\mathrm{Gal}(M_0)=\ker(\theta_0)$) ו $L_0\subseteq M_0$ השדה המתאים ל H' (כלומר $\mathrm{Gal}(L_0)=\theta_0^{-1}(H')$). כיוון ש i חח״ע ו $\theta_0|_{\mathrm{Gal}(K)}=i\theta$ נקבל

$$\mathrm{Gal}(L) \;=\; \theta^{-1}(G')=\theta^{-1}i^{-1}(H')=\varphi^{-1}\theta_0^{-1}(H')=\varphi^{-1}(\mathrm{Gal}(L_0))=\mathrm{Gal}(L_0K).$$

לכן $L=L_0K$.

לסיום, L_0 מופרד לינארית מ K כיוון ש $[L_0:K_0]=(H:H')=[L:K]$. ■

הערה 4.1.5 *בהוכחה האחרונה H' היה המייצב של נקודה בתת חבורה של S_n. באופן כללי מייצב זה אינו תת חבורה נורמלית, גם אם L/K גלואה. לכן L_0/K_0 איננה בהכרח גלואה, גם אם L/K גלואה.*

דוגמא. בדוגמא זו נבנה מגדל של שדות $K_0\subseteq K_1\subseteq K$ כך ש K/K_1 מעין סגור אלגברית, K/K_0 לא מעין סגור אלגברית, ו K_1/K_0 הרחבה סופית.

תהי $K_0=\mathbb{Q}_{\mathrm{sol}}$ ההרחבה הפרו־פתירה המירבית של $\mathbb{Q}$. ל K_0 אין הרחבות ממעלה 2. אם להרחבה K של K_0 יש הרחבה ממעלה 2, נאמר L/K, אז K/K_0 לא מעין סגור אלגברית. אכן, לפי מסקנה 4.1.4 אילו K/K_0 היה מעין סגור אלגברית, אז היה קיים L_0/K_0 כך ש $2=[L:K]=[L_0:K_0]$, סתירה.

תהי K_1/K_0 הרחבה סופית ונאותה ו $e\geq 1$. לפי משפט Weissauer [8, משפט 13.9.1] K_1 הילברטי. לכן לכמעט כל $\boldsymbol{\sigma}\in\mathrm{Gal}(K_1)^e$ ההרחבה K/K_1 היא מעין סגורה אלגברית ו $\mathrm{Gal}(K)$ היא חופשית על e יוצרים, באשר $K=\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. בפרט ל K יש הרחבה ממעלה 2 ולכן K אינו מעין סגור אלגברית מעל K_0 לפי הפסקה הקודמת.

4.2 הגבלות על מבנה גלואה של הרחבה מעין סגורה אלגברית

לא כל הרחבה יכולה להיות מעין סגורה אלגברית. סעיף זה חושף כמה מההגבלות.

בפרק זה נשתמש במכפלות זר ועל כן מומלץ לקורא להזכר בהגדרות ובתכונות הבסיסיות שלהן המופיעות בסעיף 2.5.

למה 4.2.1 *תהי K/K_0 הרחבת גלואה נאותה מעין סגורה אלגברית. אזי K סגור בפרידות.*

הוכחה. תהי A חבורת גלואה מעל K ויהי $\theta\colon \mathrm{Gal}(K) \to A$ האפימורפיזם המתאים. תהי G מנה סופית לא טריוויאלית של $\mathrm{Gal}(K/K_0)$ ותהי $\varphi\colon \mathrm{Gal}(K_0) \to G$ ההעתקת הצמצום. ניתן להניח ש $A \le S_n$ עבור איזשהו טבעי גדול n. נגדיר שיכון $i\colon A \to S_n \operatorname{wr} G$ על ידי $i(a) = (f_a, 1)$, באשר $f_a(1) = a$ ו $f_a(\sigma) = 1$ לכל $\sigma \in G$ לא טריוויאלי. כיוון ש S_n ניתנת למימוש רגולרי מעל כל שדה, בעית השיכון $(\varphi, S_n \operatorname{wr} G \to G)$ היא רציונלית מעל K_0 (מסקנה 2.5.10).

מתכונת ההרמה ניתן להרים את הפתרון θ של בעית השיכון התחתונה לפתרון חלש (θ, θ_0) של בעית השיכון הכפולה

$$\begin{tikzcd}
 & \mathrm{Gal}(K_0) \arrow[dl, "\theta_0"'] \arrow[dr] & \\
S_n \operatorname{wr} G \arrow[rr] & & G \\
 & \mathrm{Gal}(K) \arrow[uu] \arrow[dl, "\theta"'] \arrow[dr] & \\
.A \arrow[uu] \arrow[rr] & & 1 \arrow[uu]
\end{tikzcd}$$

עתה $\mathrm{Gal}(K) \triangleleft \mathrm{Gal}(K_0)$, לכן $i(A)$ אינוורינטי תחת תמונת $\mathrm{Gal}(K_0)$. כיוון שפעולת G מזדהה עם פעולת ההצמדה ב $A \operatorname{wr} G$ נובע כי $i(A)$ אינוורינטי תחת פעולת G. זה בברור לא יתכן , אלא אם כן $A = 1$. (אכן, לכל $1 \ne a \in A$ ולכל $1 \ne \sigma \in G$ מתקיים $f_a^\sigma \notin A$.)

לכן K סגור בפרידות וההוכחה נסתיימה. ■

יש כמה דוגמאות להרחבות גלואה של $\mathbb{Q}$ שהן מעין סגורות אלגברית *כשדות*. כך נקבל דוגמאות לשדות מעין סגורים אלגברית שאינם הרחבה מעין סגורה אלגברית של אף תת שדה נאות.

מסקנה 4.2.2 *תהי K הרחבת גלואה של $\mathbb{Q}$ שונה מ $\tilde{\mathbb{Q}}$. אזי K אינה הרחבה מעין סגורה אלגברית של אף תת שדה נאות. מסקנה זו תקפה גם אם K מעין סגור אלגברית. בפרט היא תקפה במקרים הבאים.*

(א) $\tilde{\mathbb{Q}}[\boldsymbol{\sigma}]$ שהיא הרחבת גלואה המקסימלית של $\mathbb{Q}$ המוכלת ב $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ [8, משפט 18.10.2].

(ב) $\mathbb{Q}_{\mathrm{tot},\mathbb{R}}(i)$, באשר $\mathbb{Q}_{\mathrm{tot},\mathbb{R}}$ היא הרחבת הגלואה הממשית המקסימלית של $\mathbb{Q}$ ו $i^2 = -1$ [24].

(ג) הצרוף $\mathbb{Q}_{\rm sym}$ של כל הרחבות הגלואה של $\mathbb{Q}$ עם חבורת גלואה סימטרית [8, משפט 18.10.3].

הוכחה. אם $K/\mathbb{Q}$ גלואה, אז K/K_0 גלואה מעל כל תת שדה. לכן הטענה נובעת מלמה 4.2.1. ■

תוצאה קצת יותר חזקה היא הבאה.

משפט 4.2.3 *סגור גלואה של הרחבה פרידה נאותה מעין סגורה אלגברית הוא הסגור הפריד.*

הוכחה. יהי K/K_0 הרחבה מעין סגורה אלגברית נאותה ויהי N סגור הגלואה. ממסקנה 4.1.4 נובע שקיימת הרחבה פרידה N_0/K_0 המופרדת לינארית מ K מעל K_0 כך ש $N = N_0K$. בפרט N/N_0 היא הרחבת גלואה מעין סגורה אלגברית נאותה. מלמה 4.2.1 נובע ש N סגור בפרידות, כדרוש. ■

התוצאה לעיל היא הכללה של תוצאה של Chatzidakis מ 1986 שהוכיחה שאם K הילברטי בן מניה ו $e \geq 1$, אז כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ השדה $K_s(\boldsymbol{\sigma})$ אינו הרחבת גלואה של K', לכל $K \subseteq K' \subsetneq K_s(\boldsymbol{\sigma})$. (כזכור, כמעט לכל $\boldsymbol{\sigma}$ ההרחבה $K_s(\boldsymbol{\sigma})/K$ היא מעין סגורה אלגברית.)

נעבור עתה להרחבות מעין סגורות אלגברית סופיות. ברור שכל שדה מעין סגור אלגברית הינו הרחבה מעין סגורה אלגברית של עצמו. דוגמא טריוויאלית נוספת היא הרחבה C/R, באשר C הוא הסגור האלגברי של שדה סגור ממשית R. במקרה זה $[C:R]=2$ [20, VI §9 מסקנה 9.3].

משפחה נוספת של דוגמאות באה מהרחבות אי פרידות בטהרה: תהי K הרחבה אי פרידה בטהרה של שדה מעין סגור אלגברית K_0. אזי K/K_0 מעין סגור אלגברית [16, מסקנה 2.3]. לכן אם K/K_0 הרחבה אי פרידה בטהרה סופית, קיבלנו עוד דוגמא להרחבה מעין סגורה אלגברית סופית.

התוצאה הבאה מראה שאלה למעשה כל ההרחבות המעין סגורות אלגברית הסופיות שיש.

מסקנה 4.2.4 *תהי K/K_0 הרחבה סופית. אז K/K_0 מעין סגורה אלגברית אם ורק אם*

(א) K_0 סגור ממשית ו K הסגור האלגברי של K_0, או

(ב) K_0 מעין סגור אלגברית ו K/K_0 אי פריד בטהרה.

הוכחה. תהי K_1 ההרחבה הפרידה המקסימלית של K_0 המוכלת ב K. אזי K/K_1 אי פריד בטהרה [20, V §6 טענה 6.6]. לפי [16, מסקנה 2.3] K_1/K_0 מעין סגור אלגברית, ובפרט K_1 הוא שדה מעין סגור אלגברית. אם $K_1 = K_0$ סיימנו.

נניח כי $K_1 \neq K_0$. ממשפט 4.2.3 נובע כי סגור הגלואה N של K_1/K_0 הוא הסגור הפריד. לכן, ממשפט Artin-Schreier ‏[20, §9 VI מסקנה 9.3] נובע ש $N = K_1$ והוא סגור אלגברית וש K_0 סגור ממשית. בפרט האיפיון של K הוא 0 ולכן $K_1 = K$. ■

פרק 5

זוגות פרויקטיבים

בפרק זה אנו מגדירים את המקבילה התורת חבורתית של הרחבות מעין סגורות אלגברית והיא הזוגות הפרויקטיבים. הקשר הזה מניע אותנו לחקור זוגות אלו.

מחקר זה משפיע על הבנת הרחבות מעין סגורות אלגברית בשני אופנים. הראשון, יש לנו איפיון של הרחבות מעין סגורות אלגברית של שדות מעין סגורים אלגברית בעזרת זוגות פרויקטיבים.

טענה 5.0.5 *(א) תהי M הרחבה מעין סגורה אלגברית של שדה מעין סגור אלגברית K. אזי $(\mathrm{Gal}(M), \mathrm{Gal}(K))$ הוא זוג פרויקטיבי.*

(ב) תהי M הרחבה אלגברית של שדה מעין סגור אלגברית K. אזי M/K מעין סגורה אלגברית אם ורק אם $(\mathrm{Gal}(M), \mathrm{Gal}(K))$ זוג פרויקטיבי.

(ג) יהי (Γ, Λ) זוג פרויקטיבי. אזי קיימת הרחבה מעין סגורה אלגברית M של שדה מעין סגור אלגברית K כך ש $\Gamma \cong \mathrm{Gal}(M)$, $\Lambda \cong \mathrm{Gal}(K)$.

(ההגדרה של זוג פרויקטיבי והוכחת הטענה מופיעים בגוף הפרק.)

למרות שאיננו יכולים להשתמש בתוצאות על זוגות פרויקטיבים להרחבות מעין סגורות אלגברית של שדות לא מעין סגורים אלגברית באופן ישיר, אנחנו כן יכולים להשתמש ברעיונות ובשיטות. זה מסביר את השימוש החוזר ונשנה של שיטות תורת חבורתיות שהופיע בפרקים הקודמים. בפרט הכלי המרכזי, תכונת ההרמה, בא משיקולים תורת חבורתיים.

בעזרת טענה 5.0.5 אנו יכולים להעביר תוצאות על הרחבות מעין סגורות אלגברית לתוצאות על זוגות פרויקטיבים. בפרק זה ניתן הוכחות ישירות ולא דרך שיטה זו משתי סיבות. ראשית, בדרך כלל ההוכחות התורת חבורתיות פשוטות יותר מההוכחות של תורת השדות. הסיבה השניה היא שאנחנו עובדים בקטגוריה כללית יותר של חבורות, דהיינו חבורות פרו-$\mathcal{C}$, כאשר $\mathcal{C}$ הינה תצורת מלניקוב של חבורות סופיות (ראה בהמשך).

5.1 התכונות הבסיסיות של זוגות פרויקטיבים

5.1.1 הגדרות

לאורך כל הפרק הזה נקבע את $\mathcal{C}$ להיות תצורת מלניקוב של חבורות סופיות. זה אומר ש $\mathcal{C}$ סגורה תחת מכפלות סיב ובהנתן סדרה קצרה מדויקת

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

מתקיים $A, C \in \mathcal{C}$ אם ורק אם $B \in \mathcal{C}$. בפרט $\mathcal{C}$ סגורה תחת מכפלות ישרות. מהסדרה המדויקת

$$1 \longrightarrow A^{(G:G_0)} \longrightarrow A \operatorname{wr}_{G_0} G \longrightarrow G \longrightarrow 1$$

נובע ש $A, G \in \mathcal{C}$ אם ורק אם $A \operatorname{wr}_{G_0} G \in \mathcal{C}$.

שלושת המשפחות הבאות הן תצורות מלניקוב. משפחת כל החבורות הסופיות; משפחת כל חבורות־p עבור ראשוני p; משפחת כל החבורות הפתירות.

יהיו $\Gamma \leq \Lambda$ חבורות פרו־$\mathcal{C}$. בעית שיכון־$\mathcal{C}$ כפולה עבור הזוג (Γ, Λ) היא תרשים חילופי

$$\begin{tikzcd}
& \Lambda \arrow[dl, dotted, "\theta"'] \arrow[dr, "\nu"] & \\
H \arrow[rr, "\beta"] & & B \\
& \Gamma \arrow[uu, "\varphi"] \arrow[dl, "\eta"'] \arrow[dr, "\mu"] & \\
G, \arrow[uu, "j"] \arrow[rr, "\alpha"] & & A \arrow[uu, "i"']
\end{tikzcd} \tag{5.1}$$

באשר $G, H, A, B \in \mathcal{C}$, $A \leq B$, $G \leq H$, i, j, φ הן העתקות השיכון וכל העתקות האנכיות α, μ, β, ν הן על. לכן בעית שיכון־$\mathcal{C}$ כפולה מורכבת שתי בעיות שיכון־$\mathcal{C}$ תואמות: בעית השיכון **התחתונה** עבור Γ ו**העליונה** עבור Λ.

כאשר $\mathcal{C}$ היא משפחת החבורות הסופיות, נשמיט את סימון ה $\mathcal{C}$ ונאמר ש (5.1) היא בעית שיכון כפולה סופית (כמו ב (3.1)). לעיתים נרשום את (5.1) בכתיב מקוצר – $((\mu, \alpha), (\nu, \beta))$.

בעית שיכון־$\mathcal{C}$ כפולה היא **מתפצלת** אם בעית השיכון העליונה מתפצלת, כלומר עבור (5.1) קיים $\beta' \colon B \to H$ כך ש $\beta\beta' = \mathrm{id}_B$. אם בנוסף גם בעית השיכון התחתונה מתפצלת נאמר שבעית השיכון־$\mathcal{C}$ הכפולה **מתפצלת ממש**.

אם נרשה לחבורות G, H, A, B להיות פרו־$\mathcal{C}$, אזי (5.1) היא **בעית שיכון־פרו־$\mathcal{C}$ כפולה**.

בהנתן פתרון חלש $\eta\colon \Gamma \to G$ של בעית השיכון התחתונה ופתרון חלש $\theta\colon \Lambda \to H$ של בעית השיכון העליונה, נאמר ש (η,θ) הוא **פתרון חלש** של (5.1) אם η ו θ תואמות, כלומר $j\eta = \theta\varphi$.

נשים לב שפתרון חלש η של (5.1) נקבע לחלוטין על ידי θ. אכן, θ משרה פתרון לבעית השיכון־$\mathcal{C}$ הכפולה אם ורק אם $\theta(\Gamma) \le G$, ואז $\eta = \theta|_\Gamma$.

הגדרה 5.1.1 *זוג (Γ,Λ) של חבורות פרו־$\mathcal{C}$ נקרא **פרויקטיבי־$\mathcal{C}$** אם כל בעית שיכון־$\mathcal{C}$ כפולה היא פתירה בחולשה.*

נתחיל בכמה תכונות בסיסיות של זוגות פרויקטיבים. הראשונה היא טריוויאלית.

טענה 5.1.2 *התנאים הבאים שקולים עבור חבורה פרו־$\mathcal{C}$ Λ.*

(א) Λ היא פרויקטיבית־$\mathcal{C}$.

(ב) הזוג $(1,\Lambda)$ הוא פרויקטיבי־$\mathcal{C}$.

(ג) הזוג (Λ,Λ) הוא פרויקטיבי־$\mathcal{C}$.

למה 5.1.3 *תהי (5.1) בעית שיכון־$\mathcal{C}$ כפולה עבור הזוג (Γ,Λ) של חבורות פרו־$\mathcal{C}$. נניח שבעיות השיכון התחתונה והעליונה פתירות בחולשה. אזי קיימת בעית שיכון־$\mathcal{C}$ כפולה מתפצלת ממש החולשת על (5.1).*

הוכחה. יהי $\theta\colon \Lambda \to H$ פתרון חלש של בעית השיכון העליונה ו $\eta\colon \Gamma \to G$ של התחתונה. נבחר תת חבורה נורמלית פתוחה N של Λ כך ש $N \le \ker(\theta)$ ו $\Gamma \cap N \le \ker(\eta)$.

יהיו $\hat{B} = \Lambda/N$, $\hat{A} = \Gamma/\Gamma\cap N$ ויהיו $\hat{H} = H \times_B \hat{B}$, $\hat{G} = G \times_A \hat{A}$. אזי התרשים החילופי הבא מגדיר בעית שיכון־$\mathcal{C}$ כפולה החולשת על (5.1).

$$\begin{tikzcd}
 & \Gamma \arrow[d] & & \Lambda \arrow[d] \\
\hat{G} \arrow[r] \arrow[d] & \hat{A} \arrow[d] & \hat{H} \arrow[r] \arrow[d] & \hat{B} \arrow[d] \\
G \arrow[r, "\alpha"] & A & H \arrow[r, "\beta"] & B
\end{tikzcd}$$

(כאן כל ההעתקות מוגדרות קאנונית.) עתה מלמה 2.3.2 נובע שבעיה זו מתפצלת ממש. ■

מסקנה 5.1.4 *יהי (Γ,Λ) זוג של חבורות פרו־$\mathcal{C}$ ונניח ש Λ היא פרויקטיבית־$\mathcal{C}$. אזי (Γ,Λ) פרויקטיבי־$\mathcal{C}$ אם ורק אם כל בעית שיכון־$\mathcal{C}$ מתפצלת ממש פתירה בחולשה.*

הוכחה. כיוון ש Λ פרויקטיבית־$\mathcal{C}$, גם Γ היא גם פרויקטיבית־$\mathcal{C}$ [8, טענה 22.4.7]. לכן כל בעית שיכון־$\mathcal{C}$ עבור Λ (בהתאמה Γ) פתירה חלש. מלמה 5.1.3 נובע שלכל בעית שיכון־$\mathcal{C}$ כפולה עבור (Γ, Λ) קיימת בעית שיכון־$\mathcal{C}$ מתפצלת ממש החולשת עליה.

הכוון השני מיידי. ■

טענה 5.1.5 *יהי* (Γ, Λ) *זוג פרויקטיבי־*$\mathcal{C}$. *אזי כל בעית שיכון־פרו־*$\mathcal{C}$ *עבור* (Γ, Λ) *פתירה בחולשה.*

הוכחה. ההוכחה הולכת במקביל להוכחת [8, למה 22.3.2]. ראשית כדי לפתור בעיות שיכון־פרו־$\mathcal{C}$ עבור (Γ, Λ) נצטרך לפתור בעיות שיכון־פרו־$\mathcal{C}$ כלליות יותר, בהן ההעתקות בבעית השיכון העליונה לא בהכרח על.

כאשר מדובר בבעיות שיכון־$\mathcal{C}$ כפולות כאלה, אנו אכן יכולים לפתור אותן: נניח שב (5.1) ν, μ הם לא על. ראשית $\ker(\alpha), \ker(\beta) \in \mathcal{C}$ כיוון ש $\mathcal{C}$ תצורת מלניקוב. כיוון ש Γ, Λ פרו־$\mathcal{C}$ נובע כי $\nu(\Gamma), \mu(\Lambda) \in \mathcal{C}$. לבסוף $\alpha^{-1}(\nu(\Gamma)), \beta^{-1}(\mu(\Lambda)) \in \mathcal{C}$, שוב כיוון ש $\mathcal{C}$ תצורת מלניקוב.

$$1 \longrightarrow \ker(\alpha) \longrightarrow \alpha^{-1}(\nu(\Gamma)) \xrightarrow{\alpha} \nu(\Gamma) \longrightarrow 1$$

$$1 \longrightarrow \ker(\beta) \longrightarrow \beta^{-1}(\mu(\Lambda)) \xrightarrow{\beta} \mu(\Lambda) \longrightarrow 1$$

נחליף A, B עם $\nu(\Gamma), \mu(\Lambda)$ ואת G, H עם $\alpha^{-1}(\nu(\Gamma)), \beta^{-1}(\mu(\Lambda))$. אז בבעית השיכון־$\mathcal{C}$ החדשה כל ההעתקות הן על ועל פי ההנחה היא פתירה חלש.

נעבור עתה לבעיות שיכון־פרו־$\mathcal{C}$ כפולות. תהי (5.1) בעית שיכון־פרו־$\mathcal{C}$ כפולה ונרשום $K = \ker(\beta)$. נוכיח את הטענה בשני צעדים.

צעד א, *כאשר הגרעין* K *סופי.* אזי G פתוחה ב KG כי $(KG : G) \leq |K|$. נבחר תת חבורה פתוחה נורמלית $U \leq H$ כך ש $U \cap KG \leq G$ ו $K \cap U = 1$ (זיכרו ש K סופית ו H האוסדורף). אזי $U \cap KG = U \cap G$. ממשפט האיזומורפיזם השני בחבורה UG נובע ש $(KG \cap UG : G) = (U \cap (KG \cap UG) : U \cap G) = (U \cap KG : U \cap G) = 1$, כלומר

$$.(KG) \cap (UG) = G \qquad (5.2)$$

נסמן $\bar{H} = H/U$, ויהיו $\pi \colon H \to \bar{H}$ ההעתקת המנה, $\bar{G} = \pi(G)$, $\bar{B} = B/\beta(U)$, $\bar{A} = A/A \cap \beta(U)$ ו $\bar{\beta} \colon \bar{H} \to \bar{B}$, $\bar{\alpha} \colon \bar{G} \to \bar{A}$ האפימורפיזמים המושרים בהתאמה מ β, α.

כיוון ש $\bar{H} \in \mathcal{C}$, קיים הומומורפיזם $\bar{\theta} \colon \Lambda \to \bar{H}$ כך ש $\bar{\theta}(\Gamma) \leq \bar{G}$ (יהי $\bar{\eta} = \bar{\theta}|_\Gamma$)

עבורו

$$\begin{tikzcd} & \Gamma \arrow[d, "\nu"] \arrow[dl, dotted, "\bar\eta"'] \arrow[dl, phantom] \\ G \arrow[r, "\alpha"] \arrow[d] & A \arrow[d] \\ \bar G \arrow[r, "\bar\alpha"] & \bar A \end{tikzcd} \qquad \begin{tikzcd} & & & \Lambda \arrow[d, "\mu"] \arrow[dl, dotted, "\beta"'] \arrow[ddl, dotted, "\bar\theta"] & \\ 1 \arrow[r] & K \arrow[r] \arrow[d, equal] & H \arrow[r, "\beta"] \arrow[d, "\pi"'] & B \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & K \arrow[r] & \bar H \arrow[r, "\bar\beta"] & \bar B \arrow[r] & 1 \end{tikzcd}$$

הם תרשימים חילופיים. הריבוע הימני בבעית השיכון הימנית הוא קרטזי כיוון ש $K \cap U = 1$ ([8], דוגמא 22.2.7(c)). לכן ניתן להרים את $\bar\theta$ ל $\theta\colon \Lambda \to H$ כך ש $\beta\theta = \mu$ (ראה [8], למה 22.2.1). נטען כי $\theta(\Gamma) \le G$. אכן,

$$A \ge \mu(\Gamma) = \beta(\theta(\Gamma)),$$

ולכן $\theta(\Gamma) \le K\beta^{-1}(A) = K\alpha^{-1}(A) = KG$. בנוסף,

$$\bar G \ge \bar\theta(\Gamma) = \pi(\theta(\Gamma)),$$

ולכן $\theta(\Gamma) \le UG$. נסיק עתה מ (5.2) שמתקיים $\theta(\Gamma) \le (KG) \cap (UG) = G$, כדרוש.

צעד ב, *המקרה הכללי.* נשתמש בלמה של צורן. נסתכל במשפחת הזוגות (L,θ), באשר $L \subseteq K$ נורמלי ב H, θ פתרון חלש של בעית השיכון הבאה ו $\theta(\Gamma) \subseteq GL/L$.

$$\begin{tikzcd} & & & \Lambda \arrow[d] \arrow[dl, dotted, "\theta"'] & \\ 1 \arrow[r] & K/L \arrow[r] & H/L \arrow[r, "\bar\beta"] & B \arrow[r] & 1 \end{tikzcd}.$$

נגדיר $(L,\theta) \le (L',\theta')$ אם $L \subseteq L'$ והתרשים

$$\begin{tikzcd} & \Lambda \arrow[d] \arrow[dl, dotted, "\theta"'] \arrow[ddl, dotted, "\theta'"] \\ H/L \arrow[r] \arrow[d] & B \arrow[d, equal] \\ H/L' \arrow[r] & B \end{tikzcd}$$

חילופי. עבור שרשרת $\{(L_i,\theta_i)\}$ החסם התחתון הוא (L,θ), באשר $L = \bigcap_i L_i$ ו $\theta = \varprojlim \theta_i$ (נשים לב כי $\theta(\Gamma) \subseteq GL/L$ לפי [8], למה 1.2.2(b)). יהי (L,θ) איבר מינימלי במשפחה.

נטען כי $L = 1$. אחרת, קיימת תת חבורה נורמלית פתוחה U של H כך ש $L \not\le U$. כיוון ש $L/U \cap L$ סופי נובע מהצעד הראשון שקיים פתרון חלש θ' של בעית

השיכון הבאה המקיים $\theta'(\Gamma) \subseteq G(U\cap L)/(U\cap L)$.

$$\begin{tikzcd} & & & \Lambda \arrow[d, "\theta"] \arrow[dl, dotted, "\theta'"'] \\ 1 \arrow[r] & L/U\cap L \arrow[r] & H/U\cap L \arrow[r] & H/L \end{tikzcd}.$$

זו סתירה למינימליות של (L,θ) ולכן $L=1$. ■

חבורה פרויקטיבית־$\mathcal{C}$ Λ מאופיינת על ידי התכונה שכל סדרה קצרה מדויקת של חבורות פרו־$\mathcal{C}$

$$1 \longrightarrow K \longrightarrow \Delta \longrightarrow \Lambda \longrightarrow 1$$

מתפצלת. אפיון דומה נכון גם עבור זוגות פרויקטיבים־$\mathcal{C}$.

מסקנה 5.1.6 *יהי (Γ,Λ) זוג של חבורות פרו־$\mathcal{C}$. אזי (Γ,Λ) פרויקטיבי־$\mathcal{C}$ אם ורק אם השורות של כל תרשים חילופי של חבורות פרו־$\mathcal{C}$*

$$\begin{tikzcd} \Delta \arrow[r, shift left, "\beta"] & \Lambda \arrow[l, shift left, dotted, "\beta'"] \arrow[r] & 1 \\ E \arrow[u] \arrow[r, shift left, "\alpha"] & \Gamma \arrow[u] \arrow[l, shift left, dotted, "\alpha'"] \arrow[r] & 1 \\ 1 \arrow[u] & 1 \arrow[u] & \end{tikzcd}$$

מתפצלות באופן תואם. כלומר קיים פיצול $\beta'\colon \Lambda \to \Delta$ של β (כלומר $\beta\beta' = \mathrm{id}$) כך ש $\beta'(\Gamma) \le E$ ו $\alpha' = \beta'|_\Gamma$ הוא פיצול של α.

הוכחה. מאחר ופיצולים של אפימורפיזמים $\gamma\colon M \to N$ מתאימים באופן חחעל לפתרונות של בעית השיכון $(\mathrm{id}\colon N \to N, \gamma\colon M \to N)$, התוצאה נובעת מיידית מטענה 5.1.5. ■

5.1.2 תכונות בסיסיות ואיפיונים

טענה 5.1.7 (תכונת ההרמה) *יהי (Γ,Λ) זוג פרויקטיבי־$\mathcal{C}$ ונסתכל בבעית שיכון־פרו־$\mathcal{C}$ עבור (Γ,Λ). אזי כל פתרון חלש η של בעית השיכון התחתונה ניתן להרמה לפתרון חלש (η,θ) של בעית השיכון הכפולה.*

הוכחה. תהי (5.1) בעית שיכון־פרו־$\mathcal{C}$ כפולה עבור (Γ,Λ) ויהי $\eta\colon \Gamma \to G$ פתרון חלש של בעית השיכון התחתונה. נגדיר $\hat{H} = H \times_B \Lambda$ ותהי

$$\hat{G} = \{(\eta(\gamma),\gamma) \mid \gamma \in \Gamma\} \le G \times_A \Gamma.$$

כיוון ש $\Gamma \cong \hat{G}$, קיים פתרון יחיד לבעית השיכון התחתונה ב

$$\begin{tikzcd}
 & \Lambda \arrow[dl, dotted, "\hat{\theta}"'] \arrow[dr, "\mathrm{id}"] & \\
\hat{H} \arrow[rr, "\hat{\beta}"] & & \Lambda \\
 & \Gamma \arrow[uu] \arrow[dl, dotted, "\hat{\eta}"'] \arrow[dr, "\mathrm{id}"] & \\
\hat{G} \arrow[uu] \arrow[rr, "\hat{\alpha}"] & & \Gamma \arrow[uu]
\end{tikzcd}$$

.

עתה טענה 5.1.5 נותנת פתרון חלש $(\hat{\eta}, \hat{\theta})$ של הבעיה הכפולה. בפרט מתקיים $\hat{\eta}(\gamma) = \hat{\alpha}^{-1}(\gamma) = (\eta(\gamma), \gamma)$. מזה נובע ש (η, θ) פתרון חלש של (5.1), באשר $\theta = \pi\hat{\theta}$ ו $\pi\colon \hat{H} \to H$ ההעתקת המנה. ■

התוצאה הבאה נובעת מתכונת ההרמה בעזרת אותו טיעון שמשתמשים כדי להוכיח את מסקנה 5.1.6 מטענה 5.1.5.

מסקנה 5.1.8 *יהי (Γ, Λ) זוג פרויקטיבי־$\mathcal{C}$ ונתבונן בתרשים כמו במסקנה 5.1.6. אזי כל פיצול α' של α ניתן להרמה לפיצול β' של β.*

טענה 5.1.9 (טרנזיטיביות) *יהיו $\Lambda_3 \le \Lambda_2 \le \Lambda_1$ חבורות פרו־$\mathcal{C}$. אזי*

(א) אם (Λ_3, Λ_1) פרויקטיבי־$\mathcal{C}$, אז גם (Λ_3, Λ_2) פרויקטיבי־$\mathcal{C}$.

(ב) אם (Λ_2, Λ_1) ו (Λ_3, Λ_2) הם פרויקטיבים־$\mathcal{C}$, אז גם (Λ_3, Λ_1) פרויקטיבי־$\mathcal{C}$.

הוכחה. כדי להראות את (א) מספיק לפתור בעית שיכון־$\mathcal{C}$ מתפצלת ממש

$$\begin{tikzcd}
 & \Lambda_3 \arrow[d, "\varphi_3"] & & & \Lambda_2 \arrow[d, "\varphi_2"] & \\
G_3 \arrow[r, "\alpha_3"] & A_3 & 1 \arrow[r] & K_2 \arrow[r] & G_2 \arrow[r, "\alpha_2"] & A_2 \arrow[r] & 1
\end{tikzcd} \tag{5.3}$$

עבור (Λ_3, Λ_2). נקבע פיצול של α_2 כדי לזהות את G_2 עם $K_2 \rtimes A_2$. ניתן להניח כי $\ker(\varphi_2) = \Lambda_2 \cap L$, באשר L היא תת חבורה פתוחה ונורמלית של Λ_1. (אחרת, ניתן לבחור תת חבורה נורמלית פתוחה L של Λ_1 כך ש $\ker(\varphi_2) \ge \Lambda_2 \cap L$ ולהחליף את A_i עם $\Lambda_i/(\Lambda_i \cap L)$ ואת G_i עם מכפלת הסיב המתאימה, $i = 2, 3$.)

תהי $A_1 = \Lambda_1/L$ ותהי $\varphi_1\colon \Lambda_1 \to A_1$ העתקת המנה. נשכן את G_3 ב $K_2 \operatorname{wr}_{A_2} A_1$ לפי התכונות של טענה 2.5.5. בפרט תחת העתקת שפירו

$$\pi\colon \operatorname{Ind}_{A_2}^{A_1}(K_2) \rtimes A_2 \to K_2 \rtimes A_2$$

מתקיים $\pi(G_3) = G_3$. לבעית השיכון־$\mathcal{C}$ הכפולה

$$\begin{tikzcd}
 & \Lambda_3 \arrow[d, "\varphi_3"] & & \Lambda_1 \arrow[d, "\varphi_1"] \\
G_3 \arrow[r, "\alpha_3"] & A_3 & K_2 \operatorname{wr}_{A_2} A_1 \arrow[r, "\alpha_2"] & A_1
\end{tikzcd}$$

יש פתרון חלש (η_3',η_1') כיוון שהזוג (Λ_3,Λ_1) פרויקטיבי. נסמן $\eta_i = \pi\eta_1'|_{\Lambda_i}$, עבור $i=2,3$. אזי $\eta_2(\Lambda_2)\le K_2\rtimes A_2$ וכפי שצוין לעיל $\eta_3(\Lambda_3)\le G_3$.

לכן (η_3,η_2) הוא פתרון חלש של (5.3) וזה מסיים את הוכחת (א).

הוכחת (ב) אנאלוגית להוכחה של למה 3.4.7. כדי לראות זאת פשוט צריך להתעלם מהמונח "גאומטרי" בכל מקום שהוא מופיע בהוכחה.

למען השלמות ניתן הוכחה המסתמכת על סדרות מדויקות. נתבונן בסדרה המדויקת הבאה שעמודותיה חח"ע.

$$\begin{tikzcd}
\Delta_1 \arrow[r, "\alpha_1"] & \Lambda_1 \arrow[r] & 1 \\
\Delta_2 \arrow[u] \arrow[r, "\alpha_2"] & \Lambda_2 \arrow[u] \arrow[r] & 1 \\
\Delta_3 \arrow[u] \arrow[r, "\alpha_3"] & \Lambda_3 \arrow[u] \arrow[r] & 1
\end{tikzcd}$$

לפי מסקנה 5.1.6 מספיק להראות שהשורה העליונה והתחתונה מתפצלות באופן תואם. כיוון ש (Λ_3,Λ_2) פרויקטיבי, שתי השורות התחתונות מתפצלות באופן תואם, יהיו α_3',α_2' החתכים המתאימים. לפי מסקנה 5.1.8 ניתן להרים את α_2' לחתך α_1' של α_1. לכן α_3',α_1' הם חתכים תואמים. ■

הערה 5.1.10 *בטענה לעיל יכול לקרות ש (Λ_3,Λ_1) הוא פרויקטיבי־$\mathcal{C}$ אבל (Λ_2,Λ_1) הוא לא. לדוגמא, יהיו Λ_1 חבורה פרויקטיבית $\mathcal{C}$ $1\ne\Lambda_2\triangleleft\Lambda_1$ ו $\Lambda_3=1$. אזי $(1,\Lambda_1)$ הוא פרויקטיבי־$\mathcal{C}$ (טענה 5.1.2) בעוד שאם $\Lambda_1\ne\Lambda_2$, אז הזוג (Λ_2,Λ_1) הוא לא (טענה 5.3.2).*

זוגות פרויקטיבים מתנהגים היטב תחת לקיחת תת חבורות.

טענה 5.1.11 *יהי (Γ,Λ) זוג פרויקטיבי־$\mathcal{C}$, תהי $\Lambda_0\le\Lambda$ תת חבורה של Λ ונרשום $\Gamma_0=\Gamma\cap\Lambda_0$. אזי (Γ_0,Λ_0) הוא פרויקטיבי־$\mathcal{C}$.*

הוכחה. לפי למה 5.1.3 מספיק להראות שכל בעית שיכון־$\mathcal{C}$ מתפצלת ממש עבור (Γ_0,Λ_0) פתירה בחולשה. תהי

$$((\mu_1\colon\Gamma_0\to A_1,\alpha_1\colon G_1\to A_1),(\nu_1\colon\Lambda_0\to B_1,\beta_1\colon H_1\to B_1))$$

בעית שיכון־$\mathcal{C}$ מתפצלת ממש עבור (Γ_0,Λ_0).

המקרה בו Λ_0 פתוחה ב Λ. תהי N תת חבורה נורמלית ופתוחה של Λ כך ש $N\le\ker\nu_1$. אזי $N\cap\Gamma_0\le\ker(\mu_1)$. תהי $\nu\colon\Lambda\to B=\Lambda/N$ ההעתקת המנה. יהיו B_0, A ו A_0 התמונות של Λ_0, Γ ו Γ_0 תחת ν (בהתאמה) ויהיו ν_0, μ ו μ_0 הצמצומים של ν לתת החבורות המתאימות. יהיו $G_0=G_1\times_{A_1}A_0$, $H_0=H_1\times_{B_1}B_0$ ויהיו $\alpha_0\colon G_0\to A_0$ ו $\beta_0\colon H_0\to B_0$ ההטלות. בעית השיכון־$\mathcal{C}$ הכפולה המתפצלת ממש

$((\mu_0,\alpha_0),(\nu_0,\beta_0))$ חולשת על $((\mu_1,\alpha_1),(\nu_1,\beta_1))$ (למה 2.3.2). לכן מספיק לפתור באופן חלש את $((\mu_0,\alpha_0),(\nu_0,\beta_0))$.

כמובן ש $A_0 \le B_0\cap A$. להפך, יהי $\bar{x}\in B_0\cap A$. אזי $\bar{x}=\nu(x)$, באשר $x=yn$, $x\in\Lambda_0$, $y\in\Gamma$ ו $n\in N$. כיוון ש $N\le\Lambda_0$, נקבל כי $y=xn^{-1}\in\Lambda_0$, ולכן $y\in\Gamma_0$. כיוון ש $\nu(y)=\nu(x)=\bar{x}$, מתקיים $\nu(\Gamma_0)\ge\nu(\Lambda_0)\cap\nu(\Gamma)$. לסיכום $A_0=B_0\cap A$.

אם $\alpha_0'\colon A_0\to G_0$ הוא פיצול של α_0, אזי מספיק למצוא פתרון חלש (η_0,θ_0) כך ש $\eta_0(\Gamma_0)=\alpha_0'(A_0)$. נסיק כי ניתן להחליף את G_0 ב $\alpha_0'(A_0)$ כדי להניח ש $G_0\cong A_0$.

יהי $\beta_0'\colon B_0\to H_0$ פיצול של β_0. נזהה את H_0 עם $K\rtimes B_0$ בעזרת β_0', באשר $K=\ker(\beta_0)$. זיהוי זה משרה שיכון $i\colon A_0\to K_0\rtimes B_0$ המקיים $\beta_0 i=\alpha_0$.

$$\begin{tikzcd}
K_0\rtimes B_0 \arrow[r, two heads, "\beta_0"] & B_0 \arrow[r, hook] & B \\
A_0 \arrow[u, hook, "i"] \arrow[r, "\alpha_0"] & A_0 \arrow[u, hook] \arrow[r, hook] & A \arrow[u, hook]
\end{tikzcd}$$

תהי $\beta\colon K\operatorname{wr}_{B_0}B\to B$ ההעתקת המנה ותהי $\pi\colon \operatorname{Ind}_{B_0}^{B}(K)\rtimes B_0\to K\rtimes B_0$ העתקת שפירו המתאימה. מטענה 2.5.5 נקבל שיכון $j\colon A\to K\operatorname{wr}_{B_0}B$ כך ש $\pi j|_{A_0}=i$ ובפרט $\beta j(a)=a$ לכל $a\in A$. יהי $\alpha=\beta|_{j(A)}\colon j(A)\to A$.

$$\begin{tikzcd}
 & \Lambda \arrow[dl, "\theta"'] \arrow[dr, "\nu"] & \\
K\operatorname{wr}_{B_0}B \arrow[rr, "\beta"] & & B \\
 & \Gamma \arrow[uu] \arrow[dl, "\eta"'] \arrow[dr, "\mu"] & \\
j(A) \arrow[uu] \arrow[rr, "\alpha"] & & A \arrow[uu]
\end{tikzcd}$$

כיוון שהזוג (Γ,Λ) הוא פרויקטיבי-$\mathcal{C}$, קיים פתרון חלש (η,θ) של $((\mu,\alpha),(\nu,\beta))$. נגדיר $\eta_0=\pi\eta|_{\Gamma_0}$ ו $\theta_0=\pi\theta|_{\Lambda_0}$. אזי (η_0,θ_0) הוא פתרון חלש של $((\mu_0,\alpha_0),(\nu_0,\beta_0))$.

$$\begin{tikzcd}
 & \Gamma_0 \arrow[dl, "\eta"'] \arrow[d, "\mu_0"] \arrow[ddl, bend left, "\eta_0"] \\
j(A_0) \arrow[r, "\alpha"] \arrow[d, "\pi"] & A_0 \arrow[d, equal] \\
A_0 \arrow[r, "\alpha_0"] & A_0
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \Lambda_0 \arrow[dl, "\theta"'] \arrow[d, "\nu_0"] \arrow[ddl, bend left, "\theta_0"] \\
\operatorname{Ind}_{B_0}^{B}(K)\rtimes B_0 \arrow[r, "\beta"] \arrow[d, "\pi"] & B_0 \arrow[d, equal] \\
K\rtimes B_0 \arrow[r, "\beta_0"] & B_0
\end{tikzcd}$$

המקרה הכללי. נקבע תת חבורה פתוחה ונורמלית N של Λ כך ש $N\cap\Lambda_0 \le \ker\nu_1$. אזי $N\cap\Gamma_0 \le \ker(\mu_1)$. ניתן להרחיב את ν_1 לחבורה $\Lambda_0 N$ על ידי $\nu_1(\lambda n) = \nu_1(\lambda)$ לכל $\lambda\in\Lambda_0$ ו $n\in N$. באופן דומה, $\Gamma_0(N\cap\Gamma)$ היא תת חבורה פתוחה של Γ ו μ_1 ניתן להרחבה לחבורה זו. נשים לב שהצמצום של ν_1 ל $\Gamma_0(N\cap\Gamma)$ שווה ל μ_1.

לפי [8, למה 1.2.2(b)] קיימת תת חבורה פתוחה Λ' של Λ המכילה את $\Lambda_0 N$ וכך ש $\Lambda'\cap\Gamma \le \Gamma_0(N\cap\Gamma)$. תהי $\Gamma' = \Lambda'\cap\Gamma$. אזי מוגדרת בעית השיכון־$\mathcal{C}$ הכפולה

$$((\mu_1\colon \Gamma'\to A_1, \alpha_1\colon G_1\to A_1), (\nu_1\colon \Lambda'\to B_1, \beta_1\colon H_1\to B_1))$$

עבור (Γ',Λ').

לפי החלק הראשון (Γ',Λ') הוא זוג פרויקטיבי־$\mathcal{C}$, ולכן קיים פתרון חלש (η,θ) של בעיה זו. כעת, אם נגדיר $\eta_0 = \eta|_{\Gamma_0}$ ו $\theta_0 = \theta|_{\Lambda_0}$, נקבל את הפתרון החלש (η_0,θ_0) של בעית השיכון המקורית. ■

הערה 5.1.12 *התוצאה המקבילה עבור הרחבות מעין סגורות אלגברית – אם M/K מעין סגורה אלגברית ו L/K אלגברית, אז ML/L מעין סגורה אלגברית – מוכח באמצעות עקרון הירידה של וייל [16, למה 2.1] (הנקרא גם צמצום הסקלרים). זה רמז לנו שצריך להשתמש במכפלות זר במקרה התורת חבורתי.*

מסקנה 5.1.13 *יהי (Γ,Λ) זוג פרויקטיבי־$\mathcal{C}$ ותהי $\Gamma \le N$ תת חבורה. אזי קיים $M\le\Lambda$ כך ש $N=\Gamma\cap M$ ו $\Gamma\cdot M=\Lambda$. יתר על כן, אם $N\lhd\Gamma$, אז $M\lhd\Lambda$.*

הוכחה. יהי $\hat{N} = \bigcap_\sigma N^\sigma$ ותהי $\eta\colon \Gamma\to\Gamma/\hat{N}$ העתקת המנה. נרים את η לפתרון (η,θ) של בעית השיכון־פרו־$\mathcal{C}$

$$((\Gamma\to 1, \Gamma/\hat{N}\to 1), (\Lambda\to 1, \Gamma/\hat{N}\to 1)).$$

נסמן $\hat{M} = \ker(\theta)$ ו $M = \theta^{-1}(N/\hat{N})$. אזי (כיוון ש $\eta = \theta|_\Gamma$)

$$N = \eta^{-1}(N/\hat{N}) = \Gamma\cap\theta^{-1}(N/\hat{N}) = \Gamma\cap M.$$

מכך ש $\theta(\Gamma) = \Gamma/\hat{N}$ נובע ש $\Gamma\hat{M} = \Lambda$, ובפרט $\Gamma\cdot M = \Lambda$.

כדי לסיים את ההוכחה, נשים לב ש $N\lhd\Gamma$ גורר ש $N=\hat{N}$, ולכן $M=\hat{M}$. כלומר $M\lhd\Lambda$, כדרוש. ■

במקרה הפרטי ש $N=1$ בתוצאה לעיל נקבל את המסקנה הבאה.

מסקנה 5.1.14 *אם (Γ,Λ) זוג פרויקטיבי־$\mathcal{C}$ אז $\Lambda = M\rtimes\Gamma$ עבור איזשהו $M\lhd\Lambda$.*

5.2 משפחות של זוגות פרויקטיבים

בסעיף זה (לצורך פשטות הסימונים) נקח את $\mathcal{C}$ להיות משפחת כל החבורות הסופיות.

5.2.1 מכפלות חופשיות

יהיו Γ_1, Γ_2 חבורות פרוסופיות. המכפלה (הפרוסופית) החופשית $\Gamma = \Gamma_1 * \Gamma_2$ מוגדרת על פי התכונה האוניברסלית הבאה. תהי $(\mu\colon \Gamma \to A, \alpha\colon H \to A)$ בעית שיכון (שרירותית) עבור Λ. יהיו $A_1 = \mu(\Gamma_1)$, $A_2 = \mu(\Gamma_2)$, $H_1 = \alpha^{-1}(A_1)$ ו $H_2 = \alpha^{-1}(A_2)$. בנוסף יהיו μ_1, μ_2 הצמצומים המתאימים של μ ל Γ_1, Γ_2 ו α_1, α_2 הצמצומים המתאימים של α ל H_1, H_2. אזי כל שני פתרונות חלשים θ_1, θ_2 של (μ_1, α_1) ושל (μ_2, α_2) ניתנים להרמה יחידה לפתרון חלש θ של (μ, α).

טענה 5.2.1 *יהי Γ גורם חופשי של חבורה פרויקטיבית Λ. אזי (Γ, Λ) פרויקטיבי.*

הוכחה. לפי ההנחה $\Lambda = \Gamma * N$. תתי החבורות Γ, N הן פרויקטיביות כתתי חבורת של חבורה פרויקטיבית. נתבונן בבעית השיכון הכפולה (5.1). יהיו $A_1 = \nu(N)$ ו $G_1 = \beta^{-1}(A_1)$. יהיו η_1, η פתרונות חלשים של (μ_1, α_1) ו (μ, α), באשר $\mu_1 = \nu|_N$ ו $\alpha_1 = \beta|_{G_1}$.

לפי הגדרת המכפלה החופשית ניתן להרים את η_1, η לפתרון חלש θ של (ν, β).
לכן (η, θ) הוא פתרון חלש של (5.1). ■

התוצאה הבאה מופיעה ב [14].

למה 5.2.2 (הרן־לובוצקי) *יהי κ מונה ותהי P חבורה פרויקטיבית מדרגה $\leq \kappa$. אזי $\hat{F}_\kappa \cong P * \hat{F}_\kappa$.*

כמסקנה נקבל שכל חבורה פרויקטיבית משוכנת בחבורה חופשית כזוג פרויקטיבי.

מסקנה 5.2.3 *תהי Λ חבורה פרוסופית חופשית מדרגה אינסופית κ. אזי לכל חבורה פרויקטיבית Γ מדרגה $\leq \kappa$ קיים שיכון כך ש (Γ, Λ) פרויקטיבי.*

5.2.2 תתי חבורות אקראיות

נתחיל בכמה סימונים שיקלו עלינו בהמשך. נכתוב e־איה בעזרת אותיות מודגשות, למשל $\boldsymbol{b} = (b_1, \ldots, b_e)$. עבור הומומורפיזם $\beta\colon H \to B$, נרשום $\beta(\boldsymbol{h}) = \boldsymbol{b}$ אם $\beta(h_i) = b_i$ לכל $i = 1, \ldots, e$. תהי C מחלקה של N^e ב H^e, באשר $N \leq \ker(\beta)$. נשתמש בסימון $\beta(C)$ עבור האיבר היחיד $\boldsymbol{b} \in B^e$ עבורו מתקיים $\beta(\boldsymbol{c}) = \boldsymbol{b}$ לכל $\boldsymbol{c} \in C$.

טענה 5.2.4 *יהיו $\Lambda = \hat{F}_\omega$ ו $e \geq 1$. אזי כמעט לכל $\boldsymbol{\sigma} \in \Lambda^e$, הזוג $(\langle \boldsymbol{\sigma} \rangle, \Lambda)$ הוא פרויקטיבי.*

הוכחה. כחבורה פרוסופית, מצוידת Λ במידת האר m. תהי

$$\begin{tikzcd} & \Lambda \arrow[d, "\mu"] \\ H \arrow[r, "\beta"] & B \end{tikzcd} \tag{5.4}$$

בעיית שיכון סופית עבור Λ, יהי $\boldsymbol{b} \in B^e$, תהי $A = \langle \boldsymbol{b} \rangle$ התת חבורה של B הנוצרת על ידי רכיבי $\boldsymbol{b}$ ויהי $\boldsymbol{h} \in H^e$ כך ש $\beta(\boldsymbol{h}) = \boldsymbol{b}$. נגדיר $\Sigma = \Sigma(\boldsymbol{b}, \boldsymbol{h}, \mu, \beta) \subseteq \Lambda^e$ להיות הקבוצה הבאה.

$$\Sigma = \{\boldsymbol{\sigma} \in \Lambda^e \mid (\mu(\boldsymbol{\sigma}) = \boldsymbol{b}) \Rightarrow [\exists \theta \colon \Lambda \to H, (\theta(\boldsymbol{\sigma}) = \boldsymbol{h}) \wedge (\beta\theta = \mu)]\},$$

כלומר קבוצת כל ה e־יות $\boldsymbol{\sigma} \in \Lambda^e$ כך שקיים פתרון חלש θ של (5.4) המקיים $\theta(\boldsymbol{\sigma}) = \boldsymbol{h}$ וכל זה בתנאי ש $\mu(\boldsymbol{\sigma}) = \boldsymbol{b}$. נשים לב ש $\Sigma = (\Sigma \cap C) \cup (\Lambda^e \smallsetminus C)$, באשר C היא מחלקה של $\ker(\mu)^e$ ב Λ^e המקיימת $\mu(C) = \boldsymbol{b}$.

נפרק את ההוכחה לשלושה חלקים. בשני השלבים הראשונים נחשב ונראה כי $m(\Sigma \cap C) = m(C)$, ולכן $m(\Sigma) = 1$.

חלק א, בניית פתרונות. תהי

$$\Delta = \{(b_i) \in H^{\mathbb{N}} \mid \beta(b_i) = \beta(b_j) \ \forall i, j \in \mathbb{N}\}.$$

לכל $i \in \mathbb{N}$ מוגדרת ההטלה $\pi_i \colon \Delta \to H$ על הרכיב ה i־י. נקבע $\hat{\beta} \colon \Delta \to B$ על ידי $\hat{\beta}(x) = \beta\pi_i(x)$, $x \in \Delta$. הגדרה זו אינה תלויה ב i ו $\hat{\beta}$ הוא אפימורפיזם.

יהי $\theta \colon \Lambda \to \Delta$ פתרון של $(\mu \colon \Lambda \to B, \hat{\beta} \colon \Delta \to B)$ ([27], משפט 3.5.9]). אזי לכל $i \in \mathbb{N}$ ההעתקה $\theta_i = \pi_i\theta$ היא פתרון של (5.4). יתר על כן, לפי למה 2.3.4 הקבוצה $\{\ker(\theta_i)\}$ היא קבוצה בלתי תלויה של תת חבורות של $\ker(\mu)$.

חלק ב, בו מחשבים את $m(\Sigma)$. עבור כל $i \in \mathbb{N}$ נקח את המחלקה X_i של $\ker(\theta_i)^e$ עבורה מתקיים $\theta_i(X_i) = \boldsymbol{h}$. אזי כיוון ש

$$\mu(X_i) = \beta\theta_i(X_i) = \beta(\boldsymbol{h}) = \boldsymbol{b},$$

נקבל כי $X_i \subseteq C$. מהחלק הראשון נקבל ש $\{X_i \mid i \in \mathbb{N}\}$ קבוצה בלתי תלויה של C.

מלמת בורל־קנטלי [8, למה 18.3.5] נובע ש $\sum_i m_C(X_i) = \sum_i \frac{|B|^e}{|H|^e} = \infty$ גורר ש $m_C(X) = 1$, באשר m_C היא מידת האר המנורמלת על C ו $X = \cap_{j=1}^{\infty} \cup_{i=j}^{\infty} X_i$. כדי לסיים את החישוב מספיק להראות ש $X \subseteq \Sigma$.

ואכן, יהי $\boldsymbol{\sigma} \in X$. אזי $\boldsymbol{\sigma} \in X_i$ עבור איזשהו i. כלומר θ_i פתרון של (5.4) ו $\theta_i(\boldsymbol{\sigma}) = \boldsymbol{h}$. לכן $\boldsymbol{\sigma} \in \Sigma$ ו $X \subseteq \Sigma$, כדרוש.

חלק ג, בו מסתיימת ההוכחה. יהי Υ החיתוך של כל $\Sigma(\boldsymbol{b}, \boldsymbol{h}, \mu, \beta)$. $m(\Upsilon) = 1$ כיוון שזהו חיתוך בן מניה של קבוצות ממידה 1. יהי $\boldsymbol{\sigma} \in \Upsilon$ ויהי $\Gamma = \langle \boldsymbol{\sigma} \rangle$.

עלינו להראות שהזוג (Γ, Λ) פרויקטיבי. לצורך כך נסתכל בבעיית שיכון (5.1). נבחר $\boldsymbol{h} \in G$ כך ש $\beta(\boldsymbol{h}) = \mu(\boldsymbol{\sigma})$. כיוון ש $\boldsymbol{\sigma} \in \Sigma(\mu(\boldsymbol{\sigma}), \boldsymbol{h}, \mu, \beta)$, קיים פתרון $\theta \colon \Lambda \to H$ כך ש $\theta(\Gamma) = \langle \theta(\boldsymbol{\sigma}) \rangle = \langle \boldsymbol{h} \rangle \leq G$. ■

הערה 5.2.5 *תוך כדי ההוכחה של הטענה הוכחנו תוצאה מעט יותר חזקה שמקיים הזוג $\langle\boldsymbol{\sigma}\rangle \le \Lambda$ כמעט לכל $\boldsymbol{\sigma} \in \Lambda^e$: לכל בעית שיכון כפולה (5.1) ולכל $\boldsymbol{h} \in G^e$ המקיים $\alpha(\boldsymbol{h}) = \mu(\boldsymbol{\sigma})$ קיים פתרון חלש $\theta\colon \Lambda \to B$ המקיים $\theta(\boldsymbol{\sigma}) = \boldsymbol{h}$.*

5.3 הגבלות על זוגות פרויקטיבים

בסעיף זה נמשיך להוכיח תוצאות על זוגות פרויקטיבים-$\mathcal{C}$ המקבילות לתוצאות על הרחבות מעין סגורות אלגברית.

למה 5.3.1 *יהי $\Gamma \lhd \Lambda$ זוג פרויקטיבי-$\mathcal{C}$. אזי $\Gamma = 1$ או $\Gamma = \Lambda$.*

הוכחה. תהי $N \lhd \Gamma$ תת חבורה נורמלית ופתוחה של Γ ותהי $D \lhd \Lambda$ תת חבורה נורמלית ופתוחה של Λ כך ש $\Gamma \le D$. יהיו $A = \Gamma/N$, $G = \Lambda/D$ ותהיינה $\eta\colon \Gamma \to A$, $\mu\colon \Lambda \to G$ העתקות המנה המתאימות. נזהה את A עם תת החבורה $\{f_a \mid a \in A\}$ של $A \operatorname{wr} G$. (כאן $f_a(1) = a$ ו $f_a(\sigma) = 1$ לכל $\sigma \neq 1$.)
נרים את η לפתרון חלש θ של

$$\begin{tikzcd} & \Gamma \arrow[dl, "\eta"'] \arrow[d] \\ .A \arrow[r] & 1 \end{tikzcd} \qquad \begin{tikzcd} & \Lambda \arrow[dl, "\theta"'] \arrow[d, "\mu"] \\ A \operatorname{wr} G \arrow[r, "\pi"] & G \end{tikzcd}$$

למה 2.5.2 גוררת ש θ על. אזי מכך ש $\Gamma \lhd \Lambda$ נקבל $A = \lhd A \operatorname{wr} G$. זה גורר ש $A = 1$ או $G = 1$, והתוצאה נובעת. ■

טענה 5.3.2 *יהי $\Gamma \lneqq \Lambda$ זוג פרויקטיבי-$\mathcal{C}$. אזי $\bigcap_{x\in\Lambda} \Gamma^x = 1$.*

הוכחה. תהי $\Gamma_0 = \bigcap_{x\in\Lambda} \Gamma^x$. ממסקנה 5.1.13 אנו מקבלים Λ_0 כך ש $\Gamma_0 = \Lambda_0 \cap \Gamma$ ו $\Gamma\Lambda_0 = \Lambda$. בפרט $\Gamma_0 \neq \Lambda_0$. יתר על כן, מטענה 5.1.11 אנו מקבלים ש (Γ_0, Λ_0) הוא זוג פרויקטיבי-$\mathcal{C}$. אבל $\Gamma_0 \lhd \Lambda_0$ ו $\Gamma_0 \neq \Lambda_0$ ולכן $\Gamma_0 = 1$ (למה 5.3.1). ■

מסקנה 5.3.3 *יהי (Γ, Λ) זוג פרויקטיבי-$\mathcal{C}$. נניח ש Γ פתוחה ב Λ. אזי $\Gamma = \Lambda$.*

הוכחה. נניח ש $\Gamma \neq \Lambda$ (ובפרט $\Lambda \neq 1$). כיוון ש Γ פתוחה גם $\bigcap_{x\in\Lambda} \Gamma^x$ פתוחה. לפי טענה 5.3.2 נקבל כי $\bigcap_{x\in\Lambda} \Gamma^x = 1$. נסיק כי $\Lambda = \Lambda/\bigcap_{x\in\Lambda} \Gamma^x$ סופית ולא טריוויאלית, בסתירה לכך ש Λ פרויקטיבית-$\mathcal{C}$. ■

טענה 5.3.4 *תהי Λ חבורה פרו-$\mathcal{C}$ ו Γ תת חבורת סילוב-p. נניח של Λ יש מנה פשוטה לא אבלית שסדרה מתחלק ב p. אזי (Γ, Λ) אינה פרויקטיבית-$\mathcal{C}$.*

הוכחה. נניח את ההפך, דהיינו ש (Γ, Λ) פרויקטיבי-$\mathcal{C}$. אזי מסקנה 5.1.14 נותנת ש $\Lambda = M \rtimes \Gamma$. נשים לב ש $|M| = (\Lambda : \Gamma) \nmid p$ כיוון ש Γ סילוב-p.

יהי $\psi\colon \Lambda \to S$ אפימורפיזם על חבורה פשוטה לא אבלית שסדרה מתחלק ב p. אזי $\psi(M) \neq S$.

מחד, $\psi(M) = 1$, כיוון ש $\psi(M) \triangleleft S$. מאידך, $\psi(\Gamma)$ תת חבורה נאותה של S. (אחרת S היתה חבורת־p.) התוצאה עתה נובעת מהסתירה

$$S = \psi(\Lambda) = \psi(M)\psi(\Gamma) = \psi(\Gamma) < S.$$

■

5.4 שימושים להרחבות מעין סגורות אלגברית

5.4.1 הוכחת טענה 5.0.5

תהי M הרחבה מעין סגורה אלגברית של שדה מעין סגור אלגברית K. כיוון ש $M \cap K_s/K$ מעין סגור אלגברית ו $\mathrm{Gal}(M) \cong \mathrm{Gal}(M \cap K_s)$ (משפט 3.4.2), ניתן להניח ש M/K היא פרידה ואלגברית. יהיו $\Gamma = \mathrm{Gal}(M)$ ו $\Lambda = \mathrm{Gal}(K)$.

K מעין סגור אלגברית ולכן Λ פרויקטיבית [8, משפט 11.6.2]. לפי מסקנה 5.1.4 כדי להוכיח ש (Γ, Λ) פרויקטיבית מספיק להראות שכל בעית שיכון סופית כפולה מתפצלת ממש (5.1) פתירה בחולשה. מעל שדה מעין סגור אלגברית K כל בעית שיכון סופית מתפצלת היא רציונלית [24, 13] ולכן (5.1) רציונלית. לכן קיים פתרון חלש לפי טענה 3.4.5.

עתה נניח ש M היא הרחבה אלגברית פרידה של שדה מעין סגור אלגברית K וש (Γ, Λ) פרויקטיבית. מטענה 3.4.5 כדי להראות ש M/K מעין סגור אלגברית צריך לפתור גאומטרית ובאופן חלש כל בעית שיכון סופית כפולה ורציונלית. עתה, כיוון ש (Γ, Λ) פרויקטיבי יש פתרון חלש, ומכיוון ש K מעין סגור אלגברית זהו פתרון גאומטרי (מסקנה 3.2.4).

לבסוף יהי (Γ, Λ) זוג פרויקטיבי. אנו צריכים למצוא הרחבה מעין סגורה אלגברית M/K כך ש $\Gamma = \mathrm{Gal}(M)$, $\Lambda = \mathrm{Gal}(K)$.

לפי [8, מסקנה 23.1.2], קיים שדה מעין סגור אלגברית K כך ש $\Lambda \cong \mathrm{Gal}(K)$. יהי M שדה השבת של Γ, ולכן $\Gamma \cong \mathrm{Gal}(M)$. כיוון ש (Γ, Λ) פרויקטיבי, לפי הפסקה השלישית, M/K מעין סגור אלגברית. ■

5.4.2 דוגמאות חדשות של הרחבות מעין סגורות אלגברית

טענה 5.4.1 *יהי K_0 שדה ותהי K/K_0 הרחבה מעין סגורה אלגברית. נניח כי $\mathrm{Gal}(K)$ חופשית מדרגה κ. אזי לכל חבורה פרויקטיבית P מדרגה $\leq \kappa$ קיימת הרחבה מעין סגורה אלגברית M/K_0 כך ש $P \cong \mathrm{Gal}(M)$.*

הוכחה. לפי משפט 3.4.2 ניתן להניח כי K/K_0 הרחבה פרידה ואלגברית. כעת, מסקנה 5.2.3 וטענה 5.0.5 נותנים הרחבה מעין סגורה אלגברית M/K כך שמתקיים

$\mathrm{Gal}(M) \cong P$. עתה מתכונת הטרנזיטיביות (טענה 3.4.8) נובע ש M/K_0 מעין סגורה אלגברית. ■

הרחבת גלואה N/K נקראת **לא חסומה** אם הקבוצה $\{\mathrm{ord}(\sigma) \mid \sigma \in \mathrm{Gal}(N/K)\}$ לא חסומה.

מסקנה 5.4.2 *יהיו P חבורה פרויקטיבית מדרגה לכל היותר בת מניה, E שדה הילברטי בן מניה ו K_0/E הרחבה אבלית לא חסומה. אזי ל K_0 יש הרחבה מעין סגורה אלגברית M כך ש $\mathrm{Gal}(M) \cong P$.*

הוכחה. בהוכחת [25, טענה 3.8] מראים שקיימת הרחבה מעין סגורה אלגברית K/K_0 כך ש $\mathrm{Gal}(K) \cong \hat{F}_\omega$. לכן הטענה הקודמת מסיימת את ההוכחה. ■

מסקנה 5.4.3 *תהי P חבורה פרויקטיבית. אזי קיים שדה הילברטי K והרחבה מעין סגורה אלגברית M/K כך ש $\mathrm{Gal}(M) \cong P$.*

פרק 6

משפט אי הפריקות של הילברט — הגרסה החלשה

נזכר ששדה הילברטי K הוא שדה המקיים את התנאי הבא.

▲ לכל פולינום $f(T,X) \in K[T,X]$ אי פריק ופריד ב X קיים ייחוד $T \mapsto a \in K$ תחתיו $f(a,X)$ נשאר אי פריק.

למרות שבמבט ראשון הילברטיות ומעין סגירות אלגברית נראות תכונות מנוגדות, יש קשר מפתיע בינהן.

משפט 6.0.4 *שדה מעין סגור אלגברית K הוא הילברטי אם ורק אם הוא חופשי־ω*

כאן שדה K הוא **חופשי־**ω אם

△ כל בעית שיכון סופית עבור K היא פתירה.

Roquette הוכיח את הגרירה $\Rightarrow$ (ראה [8, מסקנה 27.3.3]). Fried-Völklein [9] הוכיחו את הטענה באפיון 0 ו Pop סיים עם הוכחה של המקרה הכללי [24] על ידי פתוח הדבקה קשיחה. כאן ראוי לציין שהרן וירדן הוכיחו תוצאה זו בעזרת הדבקה אלגברית [13].

בפרק זה אנו משפרים את משפט 6.0.4 על ידי יצירת גרסה כמותית – "משפט אי הפריקות החלש של הילברט". שימו לב כי משפט 6.0.4 מניח **שלכל עקומה יש נקודה רציונלית** (כלומר K מעין סגור אלגברית), ותחת הנחה זו מקשרים את התכונה △ של **כל** בעיות השיכון הסופיות עבור K עם התכונה ▲ של **כל** הפולינומים האי פריקים. בהוכחות המקובלות של משפט זה, כדי להראות שייחוד שומר על פולינום אי פריק, אובייקט חזק יותר נשמר והוא חבורת הגלואה של הפולינום.

בגרסה הכמותית שלנו, מצד שני, אנו קובעים פולינום אי פריק אחד (שרירותי). עבורו אנו מוצאים בעיית שיכון מסוימת עם התכונה שפתרון *טרנזיטיבי* נותן ייחוד אי פריק בתנאי שלעקומה מסוימת יש נקודה רציונלית. הטיעון המרכזי מופיע בטענה 3.2.1.

כאשר K מעין סגור אלגברית, התנאי הזה, כלומר קיום פתרון טרזיטיבי, הוא מספיק והכרחי לקיום ייחוד אי פריק. זה אולי מפתיע שבניגוד לנ״ל יכול להיות לפולינום ייחוד אי פריק אפילו אם חבורת גלואה שלו אינה ניתנת למימוש כחבורת גלואה מעל K (ואז בפרט אין ייחוד השומר את החבורה).

אחרי ביסוס משפט אי הפריקות החלש של הילברט, אנו מיישמים אותו על שדה K שיש לו הרחבה מעין סגורה אלגברית. יישום זה נותן תנאי מספיק לקיום ייחוד אי פריק במונחי בעיות שיכון כפולות. תוצאה זו מעניינת לשימושים שיופיעו בפרקים הבאים ובעתיד.

6.1 בעיות שיכון ופולינומים

תהי E הרחבה רגולרית נוצרת סופית של שדה K. עבור פולינום אי פריק ופריד $f(X) \in E[X]$, יהיו F/E שדה הפיצול ו $L = F \cap K_s$. כזכור $\mathrm{Gal}(F/E)$ פועלת נאמנה על שורשי $f(X)$. נרשום $A = \mathrm{Gal}(L/K)$ ו $G = \mathrm{Gal}(F/E)$. יהי $G_0 \leq G$ המייצב של שורש (קבוע) $x \in F$ של f.

בעית השיכון המושרית מ f היא

$$\mathcal{E}_f = (\nu \colon \mathrm{Gal}(K) \to A, \alpha \colon G \to A) \tag{6.1}$$

עם תת החבורה **המצוינת** G_0. כאן ν ו α הן העתקות הצמצום.

יהי $\theta \colon \mathrm{Gal}(K) \to G$ פתרון חלש של בעית השיכון המושרית ונסמן את תמונתו ב $D = \theta(\mathrm{Gal}(K))$. אם D פועל טרנזיטיבית על שורשי f, נאמר ש θ הוא **טרנזיטיבי**. כיוון ש G_0 הוא המייצב של הפעולה, D פועל טרזיטיבית על שורשי f אם ורק אם D פועל טרנזיטיבית על G/G_0 אם ורק אם $(G : G_0) = (D : D \cap G_0)$. לכן טרנזיטיביות הפתרון נקבעת על ידי תת החבורה המצוינת. בפרט נקבל את התוצאה הבאה.

למה 6.1.1 *אם θ פתרון (כלומר על), אז θ טרנזיטיבית.*

הלמה הבאה מאפיינת מתי פולינום $f(X) \in E[X]$ נשאר אי פריק תחת אתר של E.

למה 6.1.2 *יהיו E, F ו f כמו שתואר לעיל ויהי φ אתר רציונלי־K של E/K. נניח כי $\varphi(f)$ מוגדר היטב, פריד ומאותה מעלה כמו של f. אזי $\varphi(f)$ אי פריק מעל K אם ורק אם הפתרון הגאומטרי φ^* של בעית השיכון המושרית הוא טרנזיטיבי.*

הוכחה. יהי $\mathcal{X} \subseteq F$ קבוצת כל שורשי f ותהי $\bar{\mathcal{X}} \subseteq K_s$ קבוצת השורשים המתאימה של $\varphi(f)$. אזי $\varphi(\mathcal{X}) = \bar{\mathcal{X}}$. לפי ההנחות $|\bar{X}| = \deg_X f = \deg_X \varphi(f) = \bar{\mathcal{X}}$, ולכן φ מעתיקה את $\mathcal{X}$ באופן חחעל.

כעת, $\varphi(f)$ אי פריק אם ורק אם $\mathrm{Gal}(K)$ פועלת טרנזיטיבית על $\bar{\mathcal{X}}$. נזכר כי $\varphi(\varphi^*(\sigma)(x)) = \sigma(\varphi(x))$ לכל $\sigma \in \mathrm{Gal}(K)$ ו $x \in \mathcal{X}$ (ראה למה 2.4.2). יהיו $x_1, x_2 \in \mathcal{X}$ ו $\varphi(x_1), \varphi(x_2) \in \bar{\mathcal{X}}$. אזי

$$\begin{aligned}\exists \sigma \in \mathrm{Gal}(K), \sigma(\varphi(x_1)) = \varphi(x_2) &\iff \exists \sigma \in \mathrm{Gal}(K), \varphi(\varphi^*(\sigma)(x_1)) = \varphi(x_2)\\ &\iff \exists \sigma \in \mathrm{Gal}(K), \varphi^*(\sigma)(x_1) = x_2\end{aligned}$$

לכן $\mathrm{Gal}(K)$ פועלת טרנזיטיבית על $\bar{\mathcal{X}}$ אם ורק אם תמונת φ^* פועלת טרנזיטיבית על $\mathcal{X}$, כלומר φ^* טרנזיטיבי. ■

התוצאה הנ״ל טוענת בפרט שתנאי הכרחי לכך שלפולינום יהיה אתר תחתיו הוא נשאר אי פריק הוא שלבעית השיכון המושרית יש פתרון טרנזיטיבי. תנאי זה הוא גם מספיק, בתנאי שלהרחבה רגולרית מסוימת של K יש אתר רציונלי-K:

למה 6.1.3 *תהי E/K הרחבה רגולרית נוצרת סופית. יהי $f \in E[X]$ פולינום אי פריק ופריד. נניח שלבעית השיכון המושרית יש פתרון טרנזיטיבי. אזי קיימת הרחבה פרידה סופית $\hat{E}/E$ שהינה רגולרית מעל K כך שהתנאי הבא מתקיים. לכל אתר רציונלי-K φ של $\hat{E}$, $\varphi(f)$ הוא אי פריק, בתנאי ש $\varphi(f)$ מוגדר היטב, פריד ומאותה מעלה של f.*

הוכחה. יהי θ הפתרון הטרנזיטיבי של בעית השיכון המושרית. יהי $\hat{E}$ ההרחבה המתקבלת מטענה 3.2.1. אזי אם שדה השאריות של $\hat{E}$ הוא K נקבל ש $\varphi^* = \theta$. לכן מלמה 6.1.2 נובע כי $\varphi(f)$ אי פריק. ■

כיוון שלכל הרחבה רגולרית נוצרת סופית של שדה מעין סגור אלגברית K יש אינסוף אתרים רציונלים-K נקבל את הטענה הבאה.

טענה 6.1.4 *יהיו K שדה מעין סגור אלגברית, E/K הרחבה רגולרית נוצרת סופית ו $f(X) \in E[X]$ פולינום אי פריק ופריד. אזי קיים אתר φ של E כך ש $\varphi(f)$ מוגדר היטב, אי פריק ומאותה מעלה כמו f אם ורק אם בעית השיכון המושרית פתירה טרנזיטיבית.*

הערה 6.1.5 *למיטב ידיעתי, בעבודות קודמות בנושא,כדי למצוא ייחוד אי פריק של פולינום משמרים את חבורת הגלואה של הפולינום.*

החידוש העיקרי בסעיף זה הוא שאיננו שומרים על חבורת הגלואה כדי ש f ישאר אי פריק. גישה זו שימושית מאוד ליישומים. למשל בפרק 7 דרוש ייחוד אי פריק של פולינום שחבורת גלואה שלו היא S_n. התוצאות של פרקים אלו תקפות למשל גם עבור הרחבות פרו-פתירות K של $\mathbb{Q}$. ההבחנה הנ״ל אכן חשובה כיוון שמעל שדה כזה יכול לקרות ש S_n אינה ניתנת למימוש.

אכן, נניח כי $K = \mathbb{Q}_{\mathrm{sol}}$ ונניח ש S_n ניתנת למימוש מעליו. אולם אם $n \geq 2$, אז $\mathbb{Z}/2\mathbb{Z}$ הינה מנה של S_n, ולכן גם $\mathbb{Z}/2\mathbb{Z}$ ניתנת למימוש מעל $\mathbb{Q}_{\mathrm{sol}}$. מסתירה זו נקבל כי $n = 1$.

6.2 משפט אי הפריקות החלש של הילברט עבור הרחבות מעין סגור־ות אלגברית

בסעיף זה נתייחס למקרה יותר קלאסי. במקום הרחבה רגולרי נוצרת סופית שרירותית E/K, נקח $E = K(\boldsymbol{t})$ שדה פונקציות רציונליות, באשר $\boldsymbol{t}$ הוא e־איה של משתנים. במילים אחרות, אנו נתבונן בפולינום $f(\boldsymbol{T}, X)$ המוגדר מעל K שהוא אי פריק בחוג $K[\boldsymbol{T}, X]$[1] ופריד ב X ונשאל האם קיים ייחוד שמשאיר את f אי פריק ופריד. בצורה יותר מפורשת, האם קיימת ההעתקה $\boldsymbol{T} \mapsto \boldsymbol{a} \in K^e$ כך ש $f(\boldsymbol{a}, X) \in K[X]$ אי פריק, פריד ו $\deg(f(\boldsymbol{a}, X)) = \deg_X(f(\boldsymbol{T}, X))$.

יהיו F שדה הפיצול של $f(\boldsymbol{t}, X)$ מעל $E = K(\boldsymbol{t})$, $L = F \cap K_s$ ו

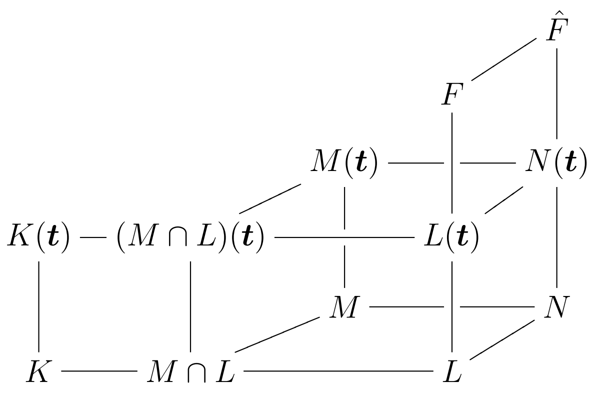
$$\mathcal{E}_f = (\mu\colon \mathrm{Gal}(K) \to A, \alpha\colon G \to A) \tag{6.1}$$

בעית השיכון המושרית. כאן $G = \mathrm{Gal}(F/K(\boldsymbol{t}))$ ו $A = \mathrm{Gal}(L/K)$.

בהנתן הרחבת שדות M/K שהיא מופרדת אלגברית מ $K(\boldsymbol{t})$ נגדיר את בעית השיכון המתאימה

$$\mathcal{E}_f(M) = (\mu\colon \mathrm{Gal}(M) \to B, \beta\colon H \to B). \tag{6.2}$$

כאן $N = LM$, $\hat{F} = FM$, $B = \mathrm{Gal}(N/M) \cong \mathrm{Gal}(L/M \cap L)$ ו $H = \mathrm{Gal}(\hat{F}/M(\boldsymbol{t})) \cong \mathrm{Gal}(F/M \cap L(\boldsymbol{t}))$. אזי $B \le A$ ו $H \le G$, ולכן $\beta = \alpha|_H$.



נשים לב כי הזוג $(\mathcal{E}_f(M), \mathcal{E}_f)$ מהווה בעית שיכון כפולה עבור M/K.

טענה 6.2.1 *יהיו K שדה, $f \in K[\boldsymbol{T}, X]$ פולינום אי פריק ופריד ב X ותהי*

$$\mathcal{E}_f = (\mu\colon \mathrm{Gal}(K) \to A, \alpha\colon G \to A)$$

בעית השיכון המושרית עם תת חבורה מצוינת G_0. נניח שקיימת הרחבה מעין סגורה אלגברית M/K (המופרדת אלגברית מ $K(\boldsymbol{t})$) ויהי $\mathcal{E}_f(M)$ בעית השיכון המתאימה (6.2).

[1] אם $f(\boldsymbol{T}, X)$ אי פריק בחוג $K[\boldsymbol{T}, X]$, אז $f(\boldsymbol{t}, X)$ אי פריק מעל $K(\boldsymbol{t})$ (לפי הלמה של גאוס). מצד שני, נניח ש $f(\boldsymbol{t}, X) \in K(\boldsymbol{t})[X]$ אי פריק מעל $K(\boldsymbol{t})$. אזי קיים $c(\boldsymbol{t}) \in K(\boldsymbol{t})$ כך ש $f^*(\boldsymbol{T}, X) = c(\boldsymbol{T}) f(\boldsymbol{T}, X) \in K[\boldsymbol{T}, X]$ וגם הוא פולינום פרימיטיבי. לכן f^* אי פריק בחוג $K[\boldsymbol{T}, X]$.

כל אחד מהתנאים הבאים מספיק לקיום ייחוד אי פריק $K^e \ni \boldsymbol{a} \mapsfrom \boldsymbol{T}$ עבור f.

(א) $\mathcal{E}_f(M)$ פתירה.

(ב) $(G:G_0)=(H:H_0)$, באשר $H_0 = H \cap G_0$ ו $\mathcal{E}_f(M)$ פתירה טרנזיטיבית ביחס לתת החבורה המצוינת H_0.

הוכחה. יהי $r(\boldsymbol{t})$ המכפלה של המקדם המוביל והדיסקרימיננטה של f. נניח וקיים פתרון חלש $\eta\colon \mathrm{Gal}(M) \to H$ של $\mathcal{E}_f(M)$.

בעזרת תכונת ההרמה (טענה 3.4.6) ניתן להרים את η לפתרון גאומטרי חלש φ^* של $\mathcal{E}_f$ כך ש $\boldsymbol{a} = \varphi(\boldsymbol{t})$ סופי (ולכן שייך ל K^e) ו $r(\boldsymbol{a}) \neq 0$. בפרט, φ לא מסועף ב F.

בסעיף (א) נתון η על. אזי $\ker(\beta) \leq \eta(\mathrm{Gal}(M))$. אבל $\ker(\beta) = \ker(\alpha)$, ולכן $\ker(\alpha) \leq \eta(\mathrm{Gal}(M)) \leq \varphi^*(\mathrm{Gal}(K))$. מכאן נובע ש φ^* הוא על (למה 2.2.1), והתוצאה נובעת מלמה 6.1.2.

בסעיף (ב) נתון η טרנזיטיבי ומתקיים $(G:G_0)=(H:H_0)$. נסמן את תמונת η ב $C = \eta(\mathrm{Gal}(M))$. כיוון ש η טרנזיטיבי מתקיים $(C : C \cap H_0) = (H : H_0)$ (ראה דיון המופיע לאחר הגדרת פתרון טרנזיטיבי). יהי $D = \varphi^*(\mathrm{Gal}(K))$. אזי $C \leq H \cap D$, לכן $C \cap H_0 = C \cap H \cap G_0 = C \cap G_0$. מתקיים

$$(G:G_0) \quad \geq \quad (D : D\cap G_0) \geq (C : C \cap H_0) = (H:H_0) = (G:G_0).$$

נסיק כי $(G:G_0) = (D : D\cap G_0)$, כלומר φ^* טרנזיטיבית. עתה התוצאה נובעת מלמה 6.1.2. ■

הערה 6.2.2 *בהוכחה בעצם הוכחנו ש $f(\boldsymbol{a}, X)$ הוא אי פריק מעל M.*

הערה 6.2.3 (על תנאי (ב)) *נשתמש בסימוני הטענה הקודמת. מאחר ו G_0 הוא המייצב של שורש $x \in F$ של $f(\boldsymbol{t}, X)$ מתקיים $(G:G_0) = \deg_X(f)$. עתה יהי $g(\boldsymbol{t}, X)$ הפולינום האי פריק של x מעל $M(\boldsymbol{t})$. אזי g מחלק את f בחוג $M(\boldsymbol{t})[X]$ ו $(H:H_0) = \deg_X g$. נסיק כי $(H:H_0) = (G:G_0)$ אם ורק אם f אי פריק מעל $M(\boldsymbol{t})$.*

בפרט, אם f אי פריק לחלוטין, התנאי $(H:H_0) = (G:G_0)$ תמיד מתקיים.

עוד דוגמא בה התנאי מתקיים היא כאשר $A \cong B$. אכן, כיוון ש $\ker(\alpha) \cong \ker(\beta)$ נקבל כי

$$|G| = |A||\ker(\alpha)| = |B||\ker(\beta)| = |H|,$$

לכן $G \cong H$, ובפרט $(G:G_0) = (H:H_0)$.

בהמשך נשתמש בטענה 6.2.1 על פולינומים שהם "הכי אי פריקים" במובן מסוים. מקרים אלו חשובים, כיוון שבבניות נעלות קל יחסית לקבל אי פריקות קיצונית.

פולינום $f(\boldsymbol{T},X) \in K[\boldsymbol{T},X]$ ממעלה n ב X נקרא **פולינום סימטרי יציב** אם חבורת הגלואה של $f(\boldsymbol{t},X)$ מעל $\tilde{K}(\boldsymbol{t})$ היא החבורה הסימטרית S_n. סביר להתייחס לפולינום סימטרי יציב כפולינום הכי אי פריק ממעלה n. ברור שפולינום סימטרי יציב הוא אי פריק לחלוטין, פריד ב X ושדה הפיצול שלו F מעל $K(\boldsymbol{t})$ הוא רגולרי מעל K. לכן בעית השיכון המושרה היא בעצם בעית המימוש הבאה:

$$.\mathcal{E}_f = (\mathrm{Gal}(K) \to 1, S_n \to 1)$$

כאן תת החבורה המצוינת היא S_{n-1}.

הערה 6.2.4 *יהי E/K רגולרית נוצרת סופית. ניתן לשאול האם קיים בסיס נעלות מפריד $\boldsymbol{t}$ עבור E/K כך שפולינום $f(\boldsymbol{t},X) \in K(\boldsymbol{t})[X]$ ששורשו יוצר את $E/K(\boldsymbol{t})$ הוא סימטרי יציב ממעלה n.*

משפט היציבות ([8, משפט 18.9.3]) טוען שאכן קיימים אינסוף n־ים עבורם יש כזה בסיס נעלות מפריד.

לפולינום סימטרי יציב יש תנאי מספיק נחמד לקיום ייחוד אי פריק.

מסקנה 6.2.5 *יהיו K שדה, $r(\boldsymbol{T}) \in K[\boldsymbol{T}]$ לא קבוע ו $f(\boldsymbol{T},X) \in K[\boldsymbol{T},X]$ פולינום סימטרי יציב ממעלה n. נניח שקיימות הרחבה מעין סגורה אלגברית M/K והרחבה פרידה N/M ממעלה n. אזי קיים $\boldsymbol{a} \in K^e$ כך ש $r(\boldsymbol{a}) \neq 0$ ו $f(\boldsymbol{a},X)$ פולינום אי פריק ופריד ממעלה n.*

הוכחה. כיוון ש F (שדה הפיצול של $f(\boldsymbol{t},X)$ מעל $K(\boldsymbol{t})$) רגולרי מעל K, מתקיים $\mathrm{Gal}(FM/M(\boldsymbol{t})) \cong \mathrm{Gal}(F/K(\boldsymbol{t}))$. לכן

$$\mathcal{E}_f(M) = (\mathrm{Gal}(M) \to 1, S_n \to 1)$$

היא בעית השיכון המתאימה.

יהי $\hat{N}$ סגור גלואה של N/M ותהי $\eta\colon \mathrm{Gal}(M) \to \mathrm{Gal}(\hat{N}/M)$ העתקת הצמצום. פעולת $\mathrm{Gal}(\hat{N}/M)$ על המחלקות הימניות של $\mathrm{Gal}(\hat{N}/N)$ משרה שיכון $\mathrm{Gal}(\hat{N}/M) \to S_n$ עם תמונה טרנזיטיבית. לכן η פתרון טרנזיטיבי של $\mathcal{E}_f(M)$. עתה טענה 6.2.1 מסיימת את ההוכחה. ■

6.3 כמה מסקנות

משפט א' מהמבוא מציין שלכל שדה הילברטי בן מניה יש הרחבה מעין סגורה אלגברית עם חבורת גלואה מוחלטת חופשית מדרגה e, באשר $e \geq 1$ מספר טבעי שרירותי. התוצאה הבאה מביאה את הכיוון ההפוך.

מסקנה 6.3.1 *יהי K שדה. נניח שעבור אינסוף מספרים טבעיים $e > 1$, קיימת הרחבה מעין סגורה אלגברית M/K כך שחבורת גלואה המוחלטת $\mathrm{Gal}(M)$ חופשית מדרגה e. אזי K הילברטי.*

הוכחה. יהי $f \in K[\boldsymbol{T}, X]$ פולינום אי פריק ופריד ב X ותהי $\mathcal{E}_f$ בעית השיכון המושרה כמו ב (6.1). נקח הרחבה מעין סגורה אלגברית M/K עם חבורת גלואה מוחלטת חופשית $\mathrm{Gal}(M)$ מדרגה לפחות $|G|$.

תהי $\mathcal{E}_f(M)$ בעית השיכון המתאימה ל M כמו ב (6.2). מתקיים

$$\mathrm{rank}\mathrm{Gal}(M) \geq |G| \geq |H| \geq \mathrm{rank}H.$$

לכן $\mathcal{E}_f(M)$ פתירה ([8, טענה 17.7.3], ול f יש ייחוד אי פריק (טענה 6.2.1). ■

ניתן הוכחה חדשה לתוצאה הבאה של רזון [25, למה 2.2].

מסקנה 6.3.2 (רזון) *יהי K שדה ו M/K הרחבה מעין סגורה אלגברית חופשית־ω אזי M הילברטי מעל K. בפרט, K הילברטי.*

הוכחה. יהי $f(\boldsymbol{T}, X) \in K[\boldsymbol{T}, X]$ פולינום אי פריק ופריד ב X. כיוון שמעל M כל בעית שיכון סופית פתירה, לפי טענה 6.2.1 יש ייחוד אי פריק $\boldsymbol{T} \mapsto \boldsymbol{a} \in K^e$ ל f. יתר על כן, $f(\boldsymbol{a}, X)$ נשאר אי פריק מעל M (הערה 6.2.2). ■

בשלב זה ננסח שאלות העולות באופן טבעי.

שאלה 6.3.3 *יהי K שדה אינסופי נוצר סופית. האם קיימת הרחבה מעין סגורה אלגברית M/K שהיא חופשית־ω?*

לצערנו איננו יודעים אפילו את התשובה לשאלה כאשר $K = \mathbb{Q}$. למעשה איננו יודעים אפילו את התשובה לשאלה הבאה שהיא הרבה יותר פשוטה.

שאלה 6.3.4 *יהי K שדה נוצר סופית ותהי M/K הרחבה מעין סגורה אלגברית. האם $\mathrm{Gal}(M)$ נוצרת סופית?*

פרק 7

משפט דיריכלה לחוגי פולינומים

7.1 מבוא והתוצאה המרכזית

משפט דיריכלה הקלאסי על ראשוניים בסדרות חשבוניות טוען שאם a, b שלמים זרים, אז יש אינסוף $c \in \mathbb{N}$ כך ש $a + bc$ ראשוני. Kornblum [19] הוכיח אנאלוג של משפט דיריכלה לחוג הפולינומים $F[X]$ מעל שדה סופי F. ארטין עידן את התוצאה של קורנבלום והוכיח שאם $a(X), b(X) \in F[X]$ הם פולינומים זרים, אז לכל שלם מספיק גדול n קיים $c(X) \in F[X]$ כך ש $a(X) + b(X)c(X)$ אי פריק ממעלה n מעל F [28, משפט 4.8].

כדי למנוע חזרות, נאמר שמשפט דיריכלה תקף עבור חוג פולינומים $F[X]$ וקבוצה של טבעיים $\mathcal{N}$, אם לכל שני פולינומים זרים $a, b \in F[X]$ קיימים אינסוף $c \in F[X]$ כך ש $a + bc$ אי פריק ממעלה n בתנאי ש $n \in \mathcal{N}$ מספיק גדול.

ירדן העלה את השאלה האם תוצאת ארטין־קורנבלום ניתנת להכללה לשדות אחרים. כמובן שאם F סגור אלגברית, אזי $a(X) + b(X)c(X)$ תמיד פריק (אלא אם כן מעלתו 1). מצד שני, אם F הילברטי, אז משפט דיריכלה תקף באופן טריוויאלי. אכן, $a(X) + b(X)Y$ הוא פולינום אי פריק, ולכן יש אינסוף $c \in F$ כך ש $a(X) + b(X)c$ אי פריק ב $F[X]$. כדי לקבל פולינומים אי פריקים ממעלה גדולה יותר רק צריך לבחור $c_0(X) \in F[X]$ שזר ל $a(X)$ וממעלה גדולה, ואז לחזור על הטיעון לעיל עבור $a(X) + b(X)c_0(X)Y$.

בעזרת משפט אי הפריקות החלש של הילברט, הטיעון הפשוט לעיל ניתן להרחבה לשדות שיש להם הרחבות מעין סגורות אלגברית כמוסבר להלן. נתחיל בסימון: עבור שדה F נסמן ב $\mathcal{N}(F)$ את קבוצת כל המספרים הטבעיים n כך שקיימים הרחבה מעין סגורה אלגברית M/F והרחבה פרידה N/M ממעלה $n = [N : M]$.

משפט 7.1.1 *יהי F שדה ו $\mathcal{N} = \mathcal{N}(F)$ אזי משפט דיריכלה תקף עבור F ו $\mathcal{N}$*

יהי $n \in \mathcal{N}$ גדול מספיק. מהטיעון שהוסבר לעיל וממסקנה 6.2.5 נובע שמספיק למצוא $c \in F[X]$ ממעלה n כך ש $f(Y, X) = a(X) + b(X)c(X)Y$ ממעלה n וחבורת

הגלואה של $f(Y,X)$ מעל $\tilde{F}(Y)$ היא S_n. לכן הוכחת משפט 7.1.1 מצטמצמת להוכחת הטענה הבאה.

טענה 7.1.2 *יהי F שדה אינסופי עם סגור אלגברי $\tilde{F}$ ויהיו $a,b \in F[X]$ פולינומים זרים. אזי לכל $n \geq 2\max(\deg a, \deg b) + \log n(1+o(1))$ קיים $c(X) \in F[X]$ כך ש $f(X,Y) = a(X) + b(X)c(X)Y$ אי פריק מעל $F(Y)$ ממעלה n ב X ו $\mathrm{Gal}(f(X,Y), \tilde{F}(Y)) \cong S_n$.*

נשים לב שהרחבה אלגברית אינסופית F של שדה סופי היא מעין סגורה אלגברית [8, מסקנה 11.2.4]. לפי משפט 7.1.1, $F[X]$ מקיים את משפט דיריכלה עם $\mathcal{N} = \{n \mid \exists N/M,\ n = [N:M]\}$. תוצאה זו כבר נובעת מגירסה כמותית של משפט ארטין־קורנבלום. אף על פי כן, להוכחה שלנו יש את היתרון שהבניות הן במהותן מפורשות: הפולינום $c(X)$ שמופיע במשפט 7.1.1 שווה לפולינום $c(X)$ מטענה 7.1.2 כפול גורם, נאמר α, המגיע מתכונת המעין סגירות אלגברית. הבניה בטענה 7.1.2 מפורשת לחלוטין כיוון שאינה משתמשת בכלום פרט לאלגוריתם של אוקלידס.

7.2 פולינומים מעל שדות אינסופיים

7.2.1 חישובים עם פולינומים

התוצאה הראשונה היא מקרה פרטי של הלמה של גאוס.

למה 7.2.1 *פולינום $f(X,Y) = a(X) + b(X)Y \in F[X,Y]$ הוא אי פריק אם ורק אם $a(X)$ ו $b(X)$ זרים.*

למה 7.2.2 *יהיו $a,b,c \in F[X]$ כך ש $\gcd(a,b) = 1$ ו $c \neq 0$. אזי קיימת תת קבוצה סופית $S \subseteq F$ כך שלכל $\alpha \in F \smallsetminus S$ הפולינומים $a + \alpha b$ ו c הם זרים. יתר על כן, אם $b' \neq 0$, ניתן לבחור את S כך ש $a + \alpha b$ פריד.*

הוכחה. יהי $S = \{-\frac{a(\gamma)}{b(\gamma)} \mid b(\gamma) \neq 0 \text{ ו } c(\gamma) = 0, \gamma \in \tilde{F}\} \cap F$. אזי ל $a + \alpha b$ אין שורשים משותפים ב $\tilde{F}$ עם c לכל $\alpha \notin S$, ולכן הם זרים.

יהי $d(Y) \in F[Y]$ הדיסקרימיננטה של $a(X) + Yb(X)$ מעל $F(Y)$, אזי $b'(X) \neq 0$ גורר ש $\frac{\partial}{\partial X}(a(X) + Yb(X)) \neq 0$, ולכן $d(Y) \neq 0$. במקרה הזה, נוסיף את כל שורשי $d(Y)$ ל S. ■

למה 7.2.3 *יהיו $a,b,p_1,p_2 \in F[X]$ פולינומים זרים בזוגות ויהיו $\alpha_1, \alpha_2 \in F$ אברים שונים השונים מאפס. אזי לכל $n > \deg p_1 + \deg p_2$ קיים $c \in F[X]$ ממעלה n ופולינומים פרידים $h_1, h_2 \in F[X]$ כך ש $a = p_i h_i + bc\alpha_i$ ו $\gcd(h_i, ap_i) = 1$ לכל $i = 1,2$.*

הוכחה. נרשום $b_i = b\alpha_i$. כיוון ש $\gcd(b_i p_{3-i}, p_i) = 1$ עבור $i = 1, 2$ קיימים c_1, c_2, $h_{1,0}$, $h_{2,0}$ ב $F[X]$ כך ש

$$i = 1, 2 \qquad a = p_i h_{i,0} + b_i c_i p_{3-i}, \tag{7.1}$$

עם $\deg c_i < \deg p_i$. עבור $\bar{c} = c_1 p_2 + c_2 p_1$ ו $h_{i,1} = h_{i,0} - c_{3-i} b_i$, נקבל ש

$$i = 1, 2 \qquad a = p_i h_{i,1} + b_i \bar{c}. \tag{7.2}$$

כאן $h_{i,1}$ זר ל b_i, כיוון ש a ו p_i זרים ל b_i. ממשוואה (7.1) עם $i = 2$ וממשוואה (7.2) עם $i = 1$ נקבל את השוויון

$$p_1 h_{1,1} \equiv a - b_1 \bar{c} \equiv a - b_1 c_2 p_1 \equiv b_2 c_2 p_1 - b_1 c_2 p_1 \equiv p_1 b c_2 (\alpha_2 - \alpha_1) \pmod{p_2}.$$

לכן $h_{1,1}$ זר ל p_2, כיוון ש $b c_2 p_1$ זר ל p_2 (נובע ממשוואה (7.1) עם $i = 2$). באופן דומה, $h_{2,1}$ זר ל p_1.

נסמן $c = \bar{c} + p_1 p_2 s$ עבור איזשהו $s \in F[X]$. אזי עבור $h_i = h_{i,1} - b_i p_{3-i} s$, נקבל

$$i = 1, 2 \qquad a = p_i h_i + b_i c.$$

כדי לסיים את ההוכחה מספיק למצוא $s \in F[X]$ כך ש h_1 ו h_2 פרידים, $\deg c = n$ ו $\gcd(h_i, a p_i) = 1$. נבחר $s \in F[X]$ כך ש $\deg s = n - (\deg p_1 + \deg p_2) \geq 1$, $(b p_i s)' \neq 0$ ו $\gcd(s, h_{i,1}) = 1$ עבור $i = 1, 2$ (למשל $s(X) = (X - \beta)^{k-1}(X - \gamma)$, באשר $\beta, \gamma \in F$ הם לא שורשים של $h_{1,1} h_{2,1} b p_1 p_2$).

מלמה 7.2.2 עם $h_{i,1}$, $b p_{3-i} s$, $a p_i$ (עבור $i = 1, 2$) נקבל תת קבוצה סופית $S \subseteq F$ כך שלכל $\alpha \in F \smallsetminus S$ הפולינום $h_{i,1} - \alpha b p_{3-i} s$ הוא פריד וזר ל $a p_i$. נחליף את s עם αs, עבור $\alpha \neq 0$ מסוים כך שיתקיים $\alpha_i \alpha \in F \smallsetminus S$, כדי להניח ש $\alpha_1, \alpha_2 \in F \smallsetminus S$. לפולינום s הזה יש את התכונות הרצויות. ■

7.2.2 למות נוספות

הלמה הבאה נותנת תנאי מספיק על חבורה טרנזיטיבית להיות פרימיטיבית ואפילו להיות S_n (השווה עם [33, למה 4.4.3]).

למה 7.2.4 *תהי $A \leq S_n$ תת חבורה טרנזיטיבית ויהי e מספר טבעי בקטע $\frac{n}{2} < e < n$ כך ש $\gcd(e, n) = 1$. אזי, אם A מכילה חישוק־e, אז A פרימיטבית. יתר על כן, אם A מכילה בנוסף חילוף, אז $A = S_n$.*

הוכחה. יהי $\Delta \neq \{1, \ldots, n\}$ בלוק עבור A. מתקיים $|\Delta| \leq \frac{n}{2}$, כיוון ש $|\Delta|$ מחלק את n. בשביל להוכיח את הטענה הראשונה, מספיק להראות ש $|\Delta| = 1$, ומכיוון ש $\gcd(e, n) = 1$, מספיק אפילו להראות ש $e \mid |\Delta|$.

בלי הגבלת הכלליות נניח ש $\sigma = (1\ 2\ \cdots\ e) \in A$ וש $1 \in \Delta$. אזי $\Delta \not\subseteq \{1,\ldots,e\}$, כיוון ש $|\Delta| \geq \frac{n}{2} > e$. לכן $\Delta \neq \sigma\Delta$ מה שגורר ש $\Delta \cap \sigma\Delta = \emptyset$.

עתה כיוון ש $\sigma(x) = x$ לכל $n \geq x > e$, נקבל ש $\Delta \subseteq \{1,\ldots,e\}$. נסיק כי Δ הוא בלוק של $\langle\sigma\rangle$, לכן $e \mid |\Delta|$, כדרוש.

הטענה השניה נובעת כיוון שחבורה פרימיטיבית המכילה חילוף היא S_n [5, משפט 3.3A]. ■

התוצאה התורת־מספרית הבאה תהיה חשובה בהמשך.

למה 7.2.5 *לכל שני מספרים טבעיים n, m וראשוני p המקיימים $n \geq 2m + \log n(1 + o(1))$, קיים שלם e בקטע $n - m > e > n/2$ כך ש $\gcd(e, np) = 1$.*

הוכחה. יהי e

$$e = \begin{cases} \frac{n}{2} + 2, & \text{אם } n \text{ זוגי אבל לא מתחלק ב } 4, \\ \frac{n}{2} + 1, & \text{אם } n \text{ מתחלק ב } 4, \text{ או} \\ \frac{n+1}{2}, & \text{אם } n \text{ אי זוגי.} \end{cases}$$

אזי e השלם הראשון הגדול מ $\frac{n}{2}$ עבורו $\gcd(e,n) = 1$. אם $p \nmid e$, סיימנו (ורק צריך $n > 2m + 4$).

נניח עתה כי $p \mid e$ (ולכן $p \nmid n$). ראשית, אם n זוגי אבל לא מתחלק ב 4, אז המועמד הבא $e' = e + 2$ עובד, כיוון ש $\gcd(e', n) = 1$ ו $p \nmid e'$ (אחרת p מחלק את $e' - e = 2$, לכן e זוגי, סתירה.)

עתה אם n מתחלק ב 4, אז המספר הראשון שזר ל n שגדול מ e הוא $e' = \frac{n}{2} + q$, באשר q הראשוני הכי קטן שאינו מחלק n. אילו $p \mid e'$, היינו מקבלים ש $p \mid (e' - e) = q - 1$. בפרט, $p < q$, ולכן $p \mid n$ ממינימליות של q, סתירה.

לבסוף, אם n אי זוגי טיעון דומה יראה ש $e' = \frac{n+q}{2}$ זר ל np, באשר כעת q הוא הראשוני האי זוגי המינימלי שאינו מחלק את n.

נשאר להעריך את q – תרגיל סטנדרטי בתורת המספרים האנליטית: יהי $\omega(n)$ מספר המחלקים הראשוניים השונים של n.

אזי q קטן או שווה לראשוני ב $\omega(n) + 2$. כיוון שהראשוני ה k שווה ל $k \log k(1 + o(1))$ ו

$$\omega(n) \leq \frac{\log n}{\log\log n}(1 + o(1))$$

[23, משפט 2.10], נקבל

$$q \leq \omega(n)\log(\omega(n))(1 + o(1)) = \log n(1 + o(1)).$$

נשים לב שעבור $n = 4\prod_{2<l<q} l$ (כלומר 4 כפול מכפלת הראשוניים האי זוגיים הקטנים מ q) אי השויון הוא בעצם שויון. לכן ההערכה $n > 2m + \log(n)(1 + o(1))$ היא מדויקת. ■

התוצאה הבאה ידועה היטב, אולם לא מצאנו מראה מקום מתאים, לכן לשלמות העבודה נביא כאן הוכחה.

טענה 7.2.6 *יהי F שדה סגור אלגברית מאפיון $l \geq 0$. תהי E/K הרחבה פרידה ממעלה n של שדות פונקציות אלגבריות ממשתנה אחד מעל F. נניח כי מחלק ראשוני $\mathfrak{p}$ של K מתפרק למכפלה*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

ב E. נניח כי

(א) $l = 0$, או

(ב) $l > 0$ ו $\gcd(e_i, n) = 1$ עבור $i = 1, \ldots, r$, או

(ג) $l = e_r = 2$ ו $e_1, \ldots, e_{r-1}$ אי זוגיים.

אזי חבורת גלואה של סגור הגלואה של E/K (כתת חבורה של S_n) מכילה איבר מטיפוס ציקלי $(e_1, \ldots, e_r)$.

הוכחה. ההשלמה $\hat{K}$ של K ב $\mathfrak{p}$ היא שדה טורי לורנט פורמלים מעל F [31, II§4 משפט 2], נאמר $\hat{K} = F((Y))$. יהי x איבר פרימיטיבי של E/K שהוא שלם ב $\mathfrak{p}$ ויהי f הפולינום האי פריק של x מעל K.

אזי $E = K[X]/(f)$. יהי $f = f_1 \cdots f_r$ הפרוק של f מעל $\hat{K}$ למכפלת פולינומים פרידים, אי פריקים ומתוקנים. אזי לפי [31, II§3 משפט 1] ההשלמה של E ב $\mathfrak{P}_i$ היא $\hat{K}[X]/(f_i)$ ולכן $\deg(f_i) = e_i$, עבור $i = 1, \ldots, r$.

אם $l = 0$, או $l > 0$ ו $\gcd(e_i, l) = 1$, אז ל $F((Y))$ יש הרחבה יחידה ממעלה e_i, כלומר $F((Y^{1/e_i}))$ [4, III§6], והיא מעגלית. לכן ניתן להניח ששדה הפיצול של f מעל $F((Y))$ הוא $F((Y^{1/e}))$, באשר $e = \operatorname{lcm}(e_1, \ldots, e_r)$ אלא אם כן $l = e_r = 2$. במקרה כזה שדה הפיצול של f הוא הצרוף של $F((Y^{1/e'}))$ עם הרחבת ריבועית פרידה, באשר $e' = \operatorname{lcm}(e_1, \ldots, e_{r-1})$ הוא אי זוגי. בשני המקרים חבורת גלואה של f מעל $F((Y))$ היא ציקלית מסדר e. היוצר שלה σ פועל באופן ציקלי על שורשי כל אחד מהפולינומים f_i. נסיק כי הטיפוס הציקלי של σ הוא $(e_1, \ldots, e_r)$, כדרוש. ■

7.2.3 הוכחת טענה 7.1.2

יהי $f(X, Y) = a(X) + b(X)Y \in F[X, Y]$ פולינום אי פריק. עבור מספר שלם גדול n אנו צריכים למצוא $c(X) \in F[X]$ כך ש $f(X, c(X)Y) = a(X) + b(X)c(X)Y$ הוא אי פריק ממעלה n וחבורת הגלואה של $f(X, c(X)Y)$ מעל $\tilde{F}(Y)$ היא S_n.

למה 7.2.5 עם $m = \max\{\deg a(X), 2 + \deg b(X)\}$ ו $p = \mathrm{char}(F)$ נותנת (עבור $n \geq 2m + \log n(1+o(1))$) שלם $e > \frac{n}{2}$ כך ש

$$n > \max\{\deg a(X), e + 2 + \deg b(X)\}, \tag{7.3}$$

$$\gcd(e, np) = 1 \ (\text{או} \ \gcd(e,n) = 1 \Leftarrow p = 0). \tag{7.4}$$

יהיו $\alpha_1 \neq \alpha_2$ ו $\gamma_1 \neq \gamma_2$ איברים של F כך ש α_i שונה מאפס ו γ_i לא מאפס את $a(X)b(X)$, $i = 1, 2$. בלמה 7.2.3 בנינו (עבור a, b, $p_1 = (X-\gamma_1)^e$, $p_2 = (X-\gamma_2)^2$, α_1 ו α_2) פולינום $c(X) \in F[X]$ ממעלה $\deg c = n - \deg b(X)$ שזר לפולינום $a(X)$ כך ש

$$\begin{aligned} f(X, c(X)\alpha_1) &= a(X) + \alpha_1 b(X)c(X) = (X-\gamma_1)^e h_1(X), && (7.5) \\ f(X, c(X)\alpha_2) &= a(X) + \alpha_2 b(X)c(X) = (X-\gamma_2)^2 h_2(X). && (7.6) \end{aligned}$$

כאן $h_1(X), h_2(X) \in F[X]$ הם פולינומים פרידים הזרים ל $(X-\gamma_1)a(X)$ ול $(X-\gamma_2)a(X)$, בהתאמה. בפרט $\gcd(a,c) = 1$, ולכן $f(X, c(X)Y)$ הוא אי פריק (למה 7.2.1). לפי (7.3), $\deg_X f(X, c(X)Y) = \deg b(X) + \deg c(X) = n$. שימוש ב (7.4), (7.5) ו (7.6) בטענה 7.2.6 עם $\mathfrak{p} = (Y - \alpha_1)$ נותן חישוק־e ב $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y))$ ועם $\mathfrak{p} = (Y - \alpha_2)$ נותן חילוף. לכן $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y)) = S_n$ (למה 7.2.4), כפי שרצינו. ■

שאלה 7.2.7 *יהי $f(X,Y) \in F[X,Y]$ פולינום אי פריק לחלוטין. עבור n גדול, האם קיים $c(X) \in F[X]$ כך ש (א) $f(X, c(X)Y)$ פולינום יציב־X ממעלה m; (ב) $\mathrm{Gal}(f(X, c(X)Y), \tilde{F}(Y)) \cong S_n$?*

פרק 8

משפחות של הרחבות מעין סגורות אלגברית

מטרת הפרק היא לבנות כמה משפחות של הרחבות מעין סגורות אלגברית. ראשית אנו מוצאים שפע של שדות שהם מעין סגורים אלגברית מעל כל תת שדה שלהם שאינו אלגברי מעל שדה סופי. כמסקנה אנו פותרים את בעיה 18.7.8 ב [8] עבור שדות נוצרים סופית.

בחלק השני אנו קובעים שדה ומחפשים הרחבות מעין סגורות אלגברית שלו. בפרט נקבל שלכל הרחבה של שדה הילברטי בן מניה עם תכונות תורת חבורתיות מסוימות (למשל הרחבה פרו־פתירה) יש הרבה הרחבות מעין סגורות אלגברית. כך נקבל שהמשפטים I ו ה' תקפים עבור שדות אלו.

8.1 הרחבות מעין סגורות אלגברית מעל כל תת שדה

נזכר שירדן ורזון הוכיחו שאם K שדה היברטי בן מניה, אז $K_s(\boldsymbol{\sigma})/K$ מעין סגורה אלגברית כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. בסעיף זה נכליל את התוצאה במקרה ש K נוצר סופית ואינסופי.

יהיו

$$f_1(T_1, \ldots, T_e, X_1, \ldots, X_n), \ldots, f_m(T_1, \ldots, T_e, X_1, \ldots, X_n) \in K[\boldsymbol{T}, \boldsymbol{X}]$$

פולינומים אי פריקים ו $g(\boldsymbol{T}) \in K[\boldsymbol{T}]$ שונה מאפס. **קבוצת הילברט** המתאימה היא קבוצת כל הייחודים האי פריקים $\boldsymbol{T} \mapsto \boldsymbol{a}$ עבור $f_1, \ldots, f_m$ תחתם g לא מתאפסת, כלומר

$$H_K(f_1, \ldots, f_m; g) = \{\boldsymbol{a} \in K^e \mid g(\boldsymbol{a}) \neq 0 \text{ ו } f_i(\boldsymbol{a}, \boldsymbol{X}) \text{ אי פריק ב } K[\boldsymbol{X}] \ \forall i\}.$$

עתה K הוא **הילברטי** אם כל קבוצת הילברט לא ריקה כאשר $f_i = f_i(\boldsymbol{T}, X)$ גם פריד ב X לכל i. (לפעמים משתמשים במינוח "K הילברטי פריד".) תכונה

חזקה יותר היא שכל קבוצה הילברטית עבור K אינה ריקה. נקרא לשדות כאלו **הילברטיים־ח**.

במקרה שהאיפיון של K הוא אפס, שתי התכונות מתלכדות. כאשר איפיון K חיובי, יש איפיון פשוט עבור שדות הילברטיים כדי שיהיו היברטיים־ח.

יהי K שדה מאיפיון $p > 0$. קבוצת כל חזקות־p, K^p, היא תת שדה של K. אם $[K : K^p] = 1$, נאמר ש K **משוכלל**, אחרת K הוא **לא־משוכלל**.

משפט 8.1.1 (Uchida) *יהי K שדה הילברטי מאיפיון חיובי. אזי K הילברטי־ח אם ורק אם K לא־משוכלל.*

הגדרה 8.1.2 *שדה E נקרא* ***הילברטי מעל*** *תת קבוצה K אם*

$$H_E(f_1, \ldots, f_m; g) \cap K^r \neq \emptyset.$$

לכל $f_1, \ldots, f_m \in E[\boldsymbol{T}, X]$ שהם אי פריקים ופרידים ב X ולכל $g(\boldsymbol{T}) \in E[\boldsymbol{T}]$ שונה מאפס. אם בנוסף $H_E(f_1, \ldots, f_m; g) \cap K^r \neq \emptyset$ לכל $f_1, \ldots, f_m \in E[\boldsymbol{T}, \boldsymbol{X}]$ אי פריקים, אז נאמר ש E הוא ***הילברטי־ח מעל*** *K.*

נשים לב ש K הילברטי (בהתאמה הילברטי־ח) אם ורק אם הוא הילברטי (בהתאמה הילברטי־ח) מעל עצמו.

נתחיל עם ההבחנה שההוכחה של [16, טענה 3.1] בעצם נותנת את התוצאה החזקה יותר הבאה:

משפט 8.1.3 (ירדן־רזון) *יהי E שדה בן מניה הילברטי מעל תת קבוצה K. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(E)^e$ השדות $E_s(\boldsymbol{\sigma})$ ו $\tilde{E}(\boldsymbol{\sigma})$ מעין סגורים אלגברית מעל K.*

עכשיו כדי למצוא הרחבות מעין סגורות אלגברית חדשות, נתחיל במציאת שדות שהם הילברטיים מעל שדות אחרים.

למה 8.1.4 *יהיו K הילברטי־ח מעל תת קבוצה S ו E/K הרחבה נעלה טהורה. אזי E הילברטי־ח מעל S.*

הוכחה. יהיו $f_1(\boldsymbol{T}, \boldsymbol{X}), \ldots, f_r(\boldsymbol{T}, \boldsymbol{X}) \in E[\boldsymbol{T}, \boldsymbol{X}]$ פולינומים אי פריקים ויהי $0 \neq g(\boldsymbol{T}) \in E[\boldsymbol{T}]$. כיוון ש $E = K(u_\alpha \mid \alpha \in A)$, באשר $\{u_\alpha \mid \alpha \in A\}$ קבוצת משתנים, ניתן להניח ש $f_i(\boldsymbol{T}, \boldsymbol{X}) = g(\boldsymbol{u}, \boldsymbol{T}, \boldsymbol{X})$, באשר

$$g_1(\boldsymbol{u}, \boldsymbol{T}, \boldsymbol{X}), \ldots, g_r(\boldsymbol{u}, \boldsymbol{T}, \boldsymbol{X}) \in K[\boldsymbol{u}, \boldsymbol{T}, \boldsymbol{X}]$$

עבור וקטור סופי $\boldsymbol{u}$.

כיוון ש K הילברטי־ח S, קיים וקטור $\boldsymbol{a}$ של איברים ב S כך שכל $g_i(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{X})$ אי פריקים ב $K[\boldsymbol{u}, \boldsymbol{X}]$ ו $g(\boldsymbol{a}) \neq 0$. אבל האברים ב $\{u_\alpha \mid \alpha \in A\}$ בלתי תלויים אלגברית, לכן $f_i(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{X})$ אי פריקים גם בחוג היותר גדול $E[\boldsymbol{X}]$. ■

טענה 8.1.5 *יהי K שדה הילברטי־ח מעל S ותהי E/K הרחבה נוצרת סופית. אזי E הילברטי מעל S. יתר על כן, אם E/K גם פרידה, אז E אפילו הילברטי־ח מעל S.*

הוכחה. נבחר בסיס נעלות $\boldsymbol{t}$ עבור E/K, כלומר $K(\boldsymbol{t})/K$ הרחבה נעלה טהורה ו $E/K(\boldsymbol{t})$ סופית. יהי $H \subseteq E^r$ קבוצת הילברט פרידה עבור E. לפי [8, טענה 12.3.3], קיימת קבוצת הילברט $H_1 \subseteq K(\boldsymbol{t})^r$ כך ש $H_1 \subseteq H$. למה 8.1.4, נותנת ש $H_1 \cap S^r \neq \emptyset$, ולכן התוצאה נובעת.

אם E/K גם פריד, אז ניתן לבחור את $\boldsymbol{t}$ להיות בסיס נעלות מפריד, כלומר ניתן להניח ש $E/K(\boldsymbol{t})$ פרידה. עתה אותו טיעון כמו בפסקה הקודמת יעבוד עבור כל קבוצת הילברט $H \subseteq E^r$ (כאשר נשתמש ב [8, מסקנה 12.2.3] במקום ב [8, טענה 12.3.3]). ■

צרוף התוצאות שקבלנו עד עתה מרחיב את משפחת ההרחבות המעין סגורות אלגברית.

משפט 8.1.6 *יהיו $e \geq 1$ שלם, K שדה בן מניה ההילברטי־ח מעל תת קבוצה S, ו E/K הרחבה נוצרת סופית. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(E)^e$ השדות $E_s(\boldsymbol{\sigma})$ ו $\tilde{E}(\boldsymbol{\sigma})$ מעין סגורים אלגברית מעל S.*

בפרט התוצאה נכונה כאשר K שדה הילברטי־ח בן מניה ו $S = K$.

מסקנה 8.1.7 *יהיו $e \geq 1$ ו K שדה נוצר סופית אינסופי. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ $K_s(\boldsymbol{\sigma})$ היא הרחבה מעין סגורה אלגברית של כל תת שדה שאינו אלגברי מעל שדה סופי. יתר על כן, אם K מאפיון 0, אז $K_s(\boldsymbol{\sigma})$ מעין סגור אלגברית מעל כל תת חוג.*

הוכחה. נתחיל כאשר האיפיון של K הוא 0. אזי כל חוג מכיל את $\mathbb{Z}$, לכן מספיק להוכיח ש $K_s(\boldsymbol{\sigma})/\mathbb{Z}$ הרחבה מעין סגורה אלגברית כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$. ואכן, כיוון ש $\mathbb{Q}$ הילברטי מעל $\mathbb{Z}$, ממשפט 8.1.6 נובעת הטענה.

עתה נניח כי האיפיון של K הוא $p > 0$. כיוון שכל שדה F שאינו אלגברי מעל $\mathbb{F}_p$ מכיל שדה פונקציות רציונליות $\mathbb{F}_p(t)$ מספיק להוכיח ש $K_s(\boldsymbol{\sigma})/\mathbb{F}_p(t)$ מעין סגור אלגברית כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ ולכל $t \in K_s(\boldsymbol{\sigma}) \smallsetminus \tilde{\mathbb{F}}_p$.

יהי $G = \mathrm{Gal}(K)^e$ ותהי μ מידת האר המנורמלת המתאימה. לכל $t \in K_s \smallsetminus \tilde{\mathbb{F}}_p$ נגדיר תת קבוצה $\Sigma_t \subseteq G$ באופן הבא.

$$\Sigma_t = \{\boldsymbol{\sigma} \in G \mid \text{אם } t \in K_s(\boldsymbol{\sigma}) \text{, אז } K_s(\boldsymbol{\sigma})/\mathbb{F}_p(t) \text{ מעין סגורה אלגברית}\}. \tag{8.1}$$

נטען כי $\mu(\Sigma_t) = 1$. אכן, יהי $E = K(t)$. אזי E/K הרחבה סופית ופרידה. יהי $H = \mathrm{Gal}(E)^e$ תת החבורה המתאימה של G.

נבחין כי $t \in K_s(\boldsymbol{\sigma})$ אם ורק אם $\boldsymbol{\sigma} \in H$. לפי הגדרת Σ_t, מכך נובע ש

$$\Sigma_t = (H \cap \Sigma_t) \cup (G \smallsetminus H).$$

לכן מספיק להראות ש $\mu(H \cap \Sigma_t) = \mu(H)$, או באופן שקול, $\nu(H \cap \Sigma_t) = 1$, באשר ν מסמל את מידת האר המנורמלת על H.

השדה $\mathbb{F}_p(t)$ הוא הילברטי ([8, משפט 13.3.5]) ולא משוכלל ([8, למה 2.7.2]). לכן ממשפט אושידה (משפט 8.1.1) $\mathbb{F}_p(t)$ הילברטי־ת. בנוסף $E/\mathbb{F}_p(t)$ הרחבה נוצרת סופית כיוון ש K כזה.

כיוון ש $H \cap \Sigma_t$ היא קבוצת כל ה $\boldsymbol{\sigma} \in \mathrm{Gal}(E)^e$ עבורם $E_s(\boldsymbol{\sigma})/\mathbb{F}_p(t)$ מעין סגור אלגברית וכיוון ש $E_s = K_s$, ממשפט 8.1.6 נובע כי $\nu(H \cap \Sigma_t) = 1$, כדרוש.

כדי לסיים את ההוכחה נראה שהקבוצה $\Sigma = \bigcap_{K_s \smallsetminus \tilde{\mathbb{F}}_p} \Sigma_t$ שהיא ממידה 1 מקיימת את הדרוש, כלומר $\boldsymbol{\sigma} \in \Sigma$ גורר ש $E_s(\boldsymbol{\sigma})/\mathbb{F}_p(t)$ מעין סגור אלגברית. ■

8.2 משפט התחתית

בסעיף זה נדון בבעיה 18.7.8 של [8] ונפתור אותה עבור שדה נוצר סופית אינסופי. יהי K הילברטי ו $e \geq 1$ שלם. הבעיה שואלת האם *משפט התחתית* תקף, כלומר האם כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$, עבור כל תת שדה נאות N של $M = K_s(\boldsymbol{\sigma})$ מתקיים $[M : N] = \infty$.

דרגת אי המשוכללות של השדה ההילברטי $K = \mathbb{F}_p(t)$ היא p, כלומר $[K : K^p] = p$. יתר על כן, דרגת אי המשוכללות נשמרת תחת הרחבות פרידות ([8, למה 2.7.3]), לכן עבור כל הרחבה פרידה M/K מתקיים $[M : M^p] = p$. בפרט משפט התחתית, כפי שמנוסח לעיל, אינו תקף. לכן נדרוש ש M/N תהיה פרידה:

השערה 8.2.1 *יהי K שדה הילברטי ויהי $e \geq 1$ שלם. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ ולכל תת שדה נאות $N \subsetneqq K_s(\boldsymbol{\sigma})$, אם ההרחבה $K_s(\boldsymbol{\sigma})/N$ פרידה, אז היא אינסופית.*

במאמר [10] הרן מוכיח גרסה קודמת של ההשערה שבה יש את ההנחה הנוספת ש N מכיל את K. התוצאה להלן משתמשת באיפיון ההרחבות המעין סגורות אלגברית הסופיות כדי להוכיח את ההשערה עבור שדות נוצרים סופית אינסופיים.

משפט 8.2.2 *יהי K שדה נוצר סופית אינסופי ו $e > 1$. אזי השערה 8.2.1 תקפה עבור K.*

הוכחה. לפי מסקנה 8.1.7 כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ השדה $M = K_s(\boldsymbol{\sigma})$ הוא מעין סגור אלגברית מעל כל תת שדה נאות שאינו אלגברי מעל שדה סופי. לכן התוצאה נובעת ממסקנה 4.2.4. ■

8.3 הרחבות אלגבריות של שדות הילברטיים

בפרק זה נקבע את K להיות שדה הילברטי בן מניה. תהי F/K הרחבה של שדות. כיוון של K שפע הרחבות מעין סגורות אלגברית (משפט 8.1.6) נקבל משפחה של הרחבות מעין סגורות אלגברית של F:

$$\{MF \mid \text{הרחבה מעין סגורה אלגברית } M/K\}.$$

בסעיף זה נדון מתי משפחה זו מכילה שדות שאינם סגורים בפרידות. לצורך שימושים צריך יותר מידע, דהיינו צריך להבין את קבוצת הטבעיים הבאה.

$$\mathcal{N}_F = \{n \mid n = [N:M] \text{ קיימים } M/K \text{ מעין סגורה אלגברית ו } N/M \text{ פרידה כך ש}\}.$$

נשים לב כי תמיד $1 \in \mathcal{N}_F$. אם קיימת ל F הרחבה מעין סגורה אלגברית שאינה סגורה בפרידות (כלומר $|\mathcal{N}_F| > 1$), אז $\mathcal{N}_F$ אינסופי. אכן, M לא שדה ממשי פורמלי כיוון שלמשוואה $X^2+Y^2+1=0$ יש פתרון. לכן $[M_s:M]=\infty$ (לפי משפט ארטין־שרייר).

נתחיל בתוצאה על האינסופיות של $\mathcal{N}_F$ כאשר ל $\mathrm{Gal}(F/K)$ אין תת חבורות חופשיות מדרגה מסוימת.

משפט 8.3.1 *נניח ש F/K גלואה ושעבור טבעי $e \geq 1$ אין ל $\mathrm{Gal}(F/K)$ תת חבורות חופשיות מדרגה e. אזי $\mathcal{N}_F$ אינסופית.*

הוכחה. תהי $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ e־איה כך ש $M = K_s(\boldsymbol{\sigma})$ הרחבה מעין סגורה אלגברית של K ו $\langle\boldsymbol{\sigma}\rangle \cong \hat{F}_e$ חופשית מדרגה e (משפט אי).

עתה מספיק להראות ש $MF \neq K_s$. ואכן, אם היה מתקיים $MF = K_s$ היינו מקבלים ש

$$\mathrm{Gal}(F/F\cap M) \cong \mathrm{Gal}(K_s/M) = \langle\boldsymbol{\sigma}\rangle \cong \hat{F}_e,$$

סתירה. ∎

עתה נקח הרחבות מסוימות, למשל הרחבות פרו־פתירות, ונתאר את $\mathcal{N}_F$ במפורש. אולם תחילה למה תורת חבורתית פשוטה.

למה 8.3.2 *יהיו $N \leq N_0 \leq G$ חבורות פרוסופיות כך ש N נורמלית ב G. תהי H מנה של G כך של H ול G/N אין מנות משותפות פרט לחבורה הטריויאלית. אזי H מנה של N_0. בפרט, אם ל H יש תת חבורה פתוחה מאינדקס n, אז גם ל N_0 יש.*

הוכחה. יהי $U \lhd G$ כך ש $G/U = H$. כיוון ש G/NU היא מנה משותפת של G/U ו G/N, מתקיים $G/NU = 1$, ולכן $G = NU$. נסיק כי $N_0U = G$, ולכן $N_0/N_0\cap U \cong N_0U/U = G/U = H$. ∎

8.3.1 הרחבות פרו־פתירות

הרחבה סופית ופרידה נקראת **פתירה** אם חבורת גלואה של סגור הגלואה פתירה. הרחבה פרידה אינסופית נקראת **פרו־פתירה** אם היא צרוף של הרחבות פתירות.

משפט 8.3.3 *תהי F הרחבה פרו־פתירה של שדה הילברטי בן מניה K ויהי $e \geq 2$. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ השדה $M = FK_s(\boldsymbol{\sigma})$ הוא הרחבה מעין סגורה אלגברית של F שיש לה הרחבה פרידה מכל מעלה > 4. בפרט*

$$.\{5, 6, 7, \ldots\} \subseteq \mathcal{N}_F$$

הוכחה. יהי $\hat{F}$ הסגור גלואה של F/K, לכן החבורה $\mathrm{Gal}(\hat{F}/K)$ היא פרו־פתירה. כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ השדה $K_s(\sigma)$ הוא הרחבה מעין סגורה אלגברית של K וחבורת הגלואה המוחלטת $G = \langle \boldsymbol{\sigma} \rangle$ היא חופשית מדרגה e (משפט א'). נקבע $\boldsymbol{\sigma}$ כזה ונרשום $M = FK_s(\boldsymbol{\sigma})$. אזי M/F מעין סגור אלגברית.

תהי $N_0 = \mathrm{Gal}(M)$ חבורת גלואה המוחלטת של M ויהי $N = \mathrm{Gal}(\hat{F}K_s(\boldsymbol{\sigma}))$. אזי $G \leq N_0 \leq N$, N נורמלי ב G ו $G/N = \mathrm{Gal}(\hat{F}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma}))$. העתקת הצמצום $\mathrm{Gal}(\hat{F}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma})) \to \mathrm{Gal}(\hat{F}/K)$ היא שיכון, לכן G/N פרו־פתירה.

יהי $n > 4$, נראה של M יש הרחבה פרידה ממעלה n. לפי התאמת גלואה מספיק להראות של N_0 יש תת חבורה פתוחה מאינדקס n.

כיוון ש G חופשית מדרגה לפחות 2, A_n מנה שלה. כמובן של A_n ול G/N אין מנות משותפות לא טריוויאליות (כי A_n פשוטה ולא פתירה). מלמה 8.3.2 עם $H = A_n$ נקבל של N_0 יש תת חבורה פתוחה מאינדקס n (כיוון ש $(A_n : A_{n-1}) = n$). ■

8.3.2 הרחבות זרות ל p

יהיו p, m, k מספרים טבעיים כך ש p ראשוני שאינו מחלק את m אך מחלק את $\varphi(m)$. כאן φ מסמל את פונקצית אוילר. נקבע $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ מסדר (כפלי) p. אזי $\mathbb{Z}/p^k\mathbb{Z}$ פועל על $\mathbb{Z}/m\mathbb{Z}$ על ידי $xb := \alpha^x b$, $x \in \mathbb{Z}/p^k\mathbb{Z}$, $b \in \mathbb{Z}/m\mathbb{Z}$.

נסתכל במכפלה חצי ישרה $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ המורכבת מכל הזוגות (a, x), $a \in \mathbb{Z}/m\mathbb{Z}$ ו $x \in \mathbb{Z}/p^k\mathbb{Z}$ כשהמכפלה נתונה על ידי

$$.(a, x)(b, y) = (a + \alpha^x b, x + y)$$

בפרט

$$.(a, x)^n = (a(1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1}), nx) = \left(\frac{a(1 - \alpha^n)}{1 - \alpha}, nx\right)$$

החבורות $\mathbb{Z}/m\mathbb{Z}$ ו $\mathbb{Z}/p^k\mathbb{Z}$ משוכנות ב H בצורה הרגילה.

למה 8.3.4 *יהיו p, m, k ו $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ כנ"ל. אזי*

א. H נוצרת על ידי תתי החבורות סילוב־p.

ב. המנה הזרה ל p היחידה של H היא החבורה הטריוויאלית.

ג. לכל $n \mid |H| = p^k m$ קיימת תת חבורה H_0 מסדר n.

הוכחה. א. האיברים $(0,1)$ ו $(1,1) = (1,0)(0,1)$ יוצרים את H, ולכן מספיק להראות שהסדר שלהם מחלק את p^k (ולמעשה שווה, אך לא נראה זאת). ראשית מתקיים $(0,1)^{p^k} = (0, p^k) = (0,0)$. עתה כיוון ש $\alpha^{p^k} = (\alpha^p)^k = 1$ נקבל כי

$$(1,1)^{p^k} = \left(\frac{1-\alpha^{p^k}}{1-\alpha}, 0 \right) = (0,0).$$

ב. נובע מא.: אכן, תהי $\bar{H} = H/N$ מנה של H שסדרה זר ל p. אזי p^k מחלק את הסדר של N, ולכן N מכילה חבורת סילוב־p של H. אולם $N \lhd H$, לכן היא מכילה את כל תת החבורות סילוב־p. לפי א., $N = H$, כלומר $\bar{H} = 1$, כדרוש.

כדי להראות את ג., נניח כי $n \mid p^k m$. אזי $n = n_0 q$, באשר $n_0 \mid m$ ו $q \mid p^k$. יהיו A, B תת החבורות היחידות של $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/p^k\mathbb{Z}$ מסדרים n_0, q, בהתאמה. מהיחידות A היא שמורת־B. לכן $A \rtimes B \leq H$. ברור שהסדר של $H_0 = A \rtimes B$ הוא n. ■

הרחבה סופית F/K היא **זרה ל** p אם p לא מחלק את $[F : K]$. הרחבה אלגברית אינסופית היא **זרה ל** p אם כל תת הרחבה סופית שלה זרה ל p.

משפט 8.3.5 *יהיו p ראשוני ו F הרחבה פרידה של שדה הילברטי בן מניה K שסגור הגלואה של F/K זר ל p מעל K. יהי $e \geq 2$. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ השדה $M = FK_s(\boldsymbol{\sigma})$ הוא הרחבה מעין סגורה אלגברית של F שיש לה הרחבה פרידה מכל מעלה. בפרט $\mathcal{N}_F = \mathbb{N}$*

הוכחה. יהי $\hat{F}$ הסגור גלואה של F/K, לכן כל מנה סופית של $\mathrm{Gal}(\hat{F}/K)$ מסדר זר ל p. ממשפט א' נקבל שכמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ חבורת גלואה המוחלטת של $M_0 = K_s(\boldsymbol{\sigma})$ חופשית מדרגה e, כלומר $G = \langle \boldsymbol{\sigma} \rangle$, ובנוסף $M = M_0 F$ הרחבה מעין סגורה אלגברית של F. תהי $N_0 = \mathrm{Gal}(M)$ חבורת גלואה המוחלטת של M ותהי $N = \mathrm{Gal}(\hat{F}K_s(\boldsymbol{\sigma}))$. אזי $N \leq N_0 \leq G$, N נורמלי ב G ו $G/N = \mathrm{Gal}(\hat{F}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma}))$. העתקת הצמצום $G/N \to \mathrm{Gal}(\hat{F}/K)$ היא חח"ע, לכן כל מנה סופית של G/N היא מסדר זר ל p (כי היא תת חבורה של מנה סופית של $\mathrm{Gal}(\hat{F}/K)$).

לפי התאמת גלואה מספיק למצוא תת חבורה פתוחה של N_0 מאינדקס שרירותי. יהי $n = n_0 p^k$ מספר טבעי, באשר $\gcd(n_0, p) = 1$ ו $k \geq 0$. יהי l ראשוני המקיים $l \nmid n$ ו $p \mid l-1$ ונסמן $m = nl$. (ראשוני l כזה קיים כיוון שיש אינסוף ראשוניים

בסדרה החשבונית $(l \equiv 1 \pmod p$.) אזי $p \nmid m$ ו $p \mid \varphi(m)$. תהי $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ כמו בלמה 8.3.4. מסעיף ב. של הלמה נובע כי ל H ו G/N אין מנות משותפות לא טריוויאליות. עתה למה 8.3.2 ולמה 8.3.4ג. מוכיחות קיום תת חבורה פתוחה של N_0 מאינדקס n. ■

Bibliography

[1] L. Bary-Soroker, *Dirichlet's Theorem for Polynomial Rings*, Proc. of the AMS.

[2] L. Bary-Soroker and M. Jarden, *PAC Fields over Finitely Generated Fields*, Math. Z.

[3] L. Bary-Soroker and D. Kelmer, *On PAC extensions and scaled Trace forms*, Israel J. Math.

[4] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys, no. 6, American Mathematical Society, New York, 1951.

[5] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. Math. **73** (1983), no. 3, 349–366.

[7] M. D. Fried, D. Haran, and M. Jarden *Galois Stratification over Frobenius Fields*, Adv. in Math. **51** (1984), no. 1, 1–35.

[8] M. D. Fried and M. Jarden, *Field Arithmetic*, second ed., revised and enlarged by M. Jarden, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 11, Springer-Verlag, Berlin, 2005.

[9] M. D. Fried and H. Völklein, *The Embedding Problem over a Hilbertian PAC-field*, Ann. of Math. (2) **135** (1992), no. 3, 469–481.

[10] D. Haran, *The Bottom Theorem*, Arch. Math. (Basel) **45** (1985), no. 3, 229–231.

[11] D. Haran, *Free Subgroups of Free Profinite Groups*, J. Group Theory **2** (1999), no. 3, 307–317.

[12] D. Haran, *Hilbertian Fields under Separable Algebraic Extensions*, Inv. Math. **137** (1999), 85–112.

[13] D. Haran and M. Jarden, *Regular Split Embedding Problems over Complete Valued Fields*, Forum Mathematicum **10** (1998) 329—351.

[14] D. Haran and A. Lubotzky, *Maximal Abelian Subgroups of Free Profinite Groups*, Math. Proc. Cambridge Philos. Soc. **97** (1985), no. 1, 51–55.

[15] M. Jarden, *PAC Fields over Number Fields*, Journal de Theorie des Nombres de Bordeaux **18** (2006), no. 2, 371–377.

[16] M. Jarden and A. Razon, *Pseudo Algebraically Closed Fields over Rings*, Israel J. Math. **86** (1994), no. 1-3, 25–59.

[17] M. Jarden and A. Razon, *Rumely's local global principle for algebraic* P$\mathcal{S}$C *fields over rings*, Trans. Amer. Math. Soc. **350** (1998), no. 1, 55–85.

[18] M. Jarden and A. Razon, *Rumely Local Global Principle for Weakly P$\mathcal{S}$C Fields over Holomorphic Domains*, manuscript, 2006.

[19] H. Kornblum, *Über die Primfunktionen in einer Arithmetischen Progression*, Mathematische Zeitschrift **5** (1919), 100–111.

[20] S. Lang, *Algebra*, Revised third edition, Graduate Texts in Mathematics, **211**, Springer-Verlag, New York, 2002.

[21] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[22] J. D. P. Meldrum, *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 74, Longman, Harlow, 1995.

[23] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I*, Cambridge Studies in Advance Mathematics **97**, Cambridge University Press, Cambridge, 2007.

[24] F. Pop, *Embedding Problems over Large Fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34.

[25] A. Razon, *Abundance of Hilbertian Domains*, Manuscripta Mathematica **94** (1997), 531–542.

[26] A. Razon, *Splittings of* $\tilde{\mathbb{Q}}/\mathbb{Q}$, Arch. Math. (Basel) **74** (2000), no. 4, 263–265.

[27] L. Ribes and P. Zalesskii, *Profinite Groups*, Ergebn. der Mathematik, Vol. 40, Springer-Verlag, Berlin 2000.

[28] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[29] P. Samuel, *Lectures on Old and New Results on Algebraic Curves*, Tata Institute of Fundamental Research, Bombay, 1966.

[30] W. Scharlau, *On Trace Forms of Algebraic Number Fields*, Math. Z. **196** (1987), no. 1, 125–127.

[31] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, New York, 1979.

[32] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), no. 4, 651–676.

[33] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Damon, With a foreword by Darmon and the author.

[34] H. Völklein, *Groups as Galois groups, An introduction.* Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, Cambridge, 1996.

[35] W. C. Waterhouse, *Scaled Trace Forms over Number Fields*, Arch. Math. (Basel) **47** (1986), no. 3, 229–231.