אוניברסיטת תל אביב
הפקולטה למדעים מדויקים על שם
ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

הילברטיות תחת הרחבות אלגבריות ומידת האר

עבודת גמר שהוגשה כחלק מהדרישות לקבלת תואר מוסמך במדעים
(M.Sc.) באוניברסיטת תל אביב

ע"י

ברי ליאור

העבודה הוכנה בהנחייתו של פרופ' דן הרן

תמוז, תשס"ד

תודות:

ברצוני להודות למנחי פרופ' דן הרן. על השקעתו הבלתי פוסקת. על סובלנותו הרבה. על שיחות מועילות, מרתקות וארוכות. על ההצעות המעולות שתרמו רבות לעבודה זו. על העניין הרב שנתן לי בנושא. ולבסוף על העידוד שנתן, שכה הזדקקתי לו. תודה.

אנצל הזדמנות זו להודות לאמי ואבי, שתמיד תמכו בי בכל דרך שבחרתי. ולבסוף תודה לחמוטל, אשתי, על הכל.

תוכן עניינים

1 מבוא 3

2 מכפלת הזר המפותלת 7

2.1 הגדרות וסימונים 7

2.2 תת חבורות מדרגה 2 של מכפלת הזר המפותלת . . . 8

2.3 פרוש בשדות 12

3 מידת האר של חבורות פרו־סופיות 20

3.1 הגדרות וסימונים 20

3.2 אי תלות הסתברותית במכפלות חצי ישרות 20

3.3 חבורות פרו־סופיות לא חסומות 23

4 שימושים 25

4.1 סימונים 25

4.2 פולינום אחד 25

4.3 המשפט המרכזי 29

I מבוא באנגלית i

תקציר

אנו נותנים הוכחה חדשה למשפט הבא של א. רזון:
משפט: יהי K שדה הילברטי בן מנייה ויהי $e \geq 2$ מספר שלם. תהי M הרחבה אבלית של K כך שהקבוצה $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}(M/K)\}$ לא חסומה. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ כל שדה בין $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ לבין M הוא הילברטי.

1 מבוא

הרחבה אלגברית פרידה M של שדה הילברטי K היא הילברטית, אם היא מקיימת את התנאי התורת חבורתי (במהותו) הבא: עבור בעיות שיכון מסוימות, עם מכפלות זר מפותלות, **לא** יהיו פתרונות המוכלים בהרחבות גלואה מסוימות המקיפות את M [Ha, משפט 3.2]. במאמר [Ha] משנת 1999 טוען ד. הרן כי כל התוצאות שהיו ידועות כבר לפני כן המסוכמות ב־ [JL] משנת 1992 ־ למשל, כל הרחבה אבלית של שדה הילברטי היא הילברטית, משפט Weissauer [FrJ1, טענה 15.5] וכדומה ־ נובעות מתנאי זה. הרן מוכיח תוצאה חדשה המוצאת הרחבות אלגבריות פרידות הילברטיות חדשות:

משפט היהלום של הרן [Ha, משפט 4.1]: *אם M_1, M_2 הרחבות גלואה של שדה הילברטי K, אז כל הרחבה M של K המקיימת $M \subseteq M_1M_2$ ו־ $M \not\subseteq M_i$, $i = 1, 2$, היא הילברטית.*

אולם, בשנת 1997, זמן קצר לפני הגשת המאמר של הרן, במאמר [Ra] בונה א. רזון הרחבות פרידות של שדה הילברטי שהן הילברטיות, ואותן, לכאורה, לא ניתן להסיק מהתנאי של הרן.

משפט 1 (רזון [Ra]) *יהי K שדה הילברטי בן מנייה ויהי $e \geq 2$ מספר שלם. תהי M הרחבה אבלית של K כך שהקבוצה $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}(M/K)\}$ לא חסומה. אזי כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ כל שדה בין $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ לבין M הוא הילברטי.*

למעשה, רזון מוכיח שלכל הרחבה אבלית M' של K המקיפה את M, השדה $M'K_s(\sigma)$ הינו הילברטי מעל M', ומראה שניתן להחליף את השדות ההילברטיים בחוגים הילברטיים. בעבודה זו נתעניין רק בשאלת ההילברטיות של שדות, ולכן אנו מתמקדים במשפט 1 (הנובע מהתוצאה היותר כללית הנ"ל).

כדי להוכיח את משפט 1, משתמש רזון במושג *שדה מעין סגור אלגברית מעל שדה (חוג)* ראה [JR, הגדרה 1.1] המכליל את המושג שדה מעין סגור אלגברית. להלן כמה תכונות של שדות מעין סגורים אלגברית ([FrJ1]). בסוגריים אנו מביאים את הכללתן לשדות מעין סגורים אלגברית מעל שדה ([JR], [Ra]).

(א) אם E הינו שדה מעין סגור אלגברית (מעל K) ו־E' הרחבה אלגברית של E ($E' = EM$, באשר M/K הרחבה אלגברית), אז E' הינו שדה מעין סגור אלגברית (מעל M).

(ב) אם K הוא שדה הילברטי בן מנייה, אז כמעט לכל $\sigma \in \mathrm{Gal}(K)^e$ השדה $K_s(\sigma)$ מעין סגור אלגברית (מעל K).

(ג) אם E הינו שדה מעין סגור אלגברית (מעל K) וחופשי־ω, אז E הוא שדה הילברטי (מעל K).

מ־(א), (ב) נובע כי כמעט לכל $\sigma \in \mathrm{Gal}(K)^e$ ולכל הרחבה אבלית M' של K המקיפה את M, השדה $M'K_s(\sigma)$ הוא מעין סגור אלגברית מעל M'. תוצאה ידועה של מ. ירדן היא שהשדה $K_s(\sigma)$ הוא חופשי־e, כמעט לכל $\sigma \in \mathrm{Gal}(K)^e$ [FrJ1, משפט 16.13], לפיה ניתן לראות ש־ $M'K_s(\sigma)$ היא חופשית־ω. לכן, על פי (ג), השדה $M'K_s(\sigma)$ הילברטי מעל M'. אי לכך כל שדה ביניים בין $M'K_s(\sigma)$ ל־M' הוא הילברטי [Ra, למה 2.3], וקיבלנו הוכחה למשפט 1.

נראה כי בהוכחתו של רזון אין שימוש בשום דבר הדומה לתנאי של הרן. יתר על כן, לא ברור איך ניתן להפעיל את השיטות של הרן במקרה זה.

בעבודה זו נתאים את הכלים שהופיעו ב־ [Ha] למקרה הנ"ל, כלומר "שיסכימו" עם תורת המידה. לצורך כך כבר לא ניתן לעבוד עם מכפלת הזר המפותלת, אלא עם תת חבורות שלה המופיעות "בהסתברות גבוהה".

בפרק 2 נדון במכפלות זר מפותלות $A \operatorname{wr}_{G'} G$. בעיקר נתעניין בתת חבורות בעלות דרגה 2 של מכפלת הזר המפותלת שהן *מלאות* (הגדרה 2.2.3). לתת חבורות אלו ישנן שתי תכונות חשובות. בלשון לא מדויקת, התמונה של תת חבורה כזו תהיה לא חילופית תחת העתקות מנה מסוימות (אלא אם היא טריוויאלית). התכונה השנייה היא היכולת "לשחזר" את מבנה החבורה A מתת החבורה. אנו מראים כי ישנן הרבה תת חבורות כאלו. בפרק זה נתרגם גם את התוצאות בתורת החבורות לתוצאות בתורת השדות באמצעות תורת גלואה.

בפרק 3 נדון בתורת המידה של חבורות פרו־סופיות בכלל, ושל חבורות פרו־סופיות *לא חסומות* (הגדרה 3.3.1) בפרט.

בפרק 4 אנו נשלב בין תורת החבורות לתורת המידה. נראה (באמצעות הכלים שפותחו בפרק 3) כי ניתן לבחור את תת החבורות בעלות דרגה 2 (הנידונות בפרק 2) בהסתברות "גבוהה".

נתחיל בפולינום $f(T,X) \in K_s[T,X]$ אי פריק לחלוטין וגלואה מעל $K_s(T)$. נממש את חבורת הזר המפותלת $A \operatorname{wr}_{G'} G$ מעל השדה ההילברטי K, באשר A היא חבורת הגלואה של f מעל $K_s(T)$. לאחר מכן, נצרף "שדה אקראי" (כלומר את $K_s(\boldsymbol{\sigma})$ כאשר $\boldsymbol{\sigma}$ נבחר בהסתברות 1) למימוש של מכפלת הזר, ובכך נקבל מימוש של תת חבורה מלאה מעל $K_s(\boldsymbol{\sigma})$.

האפשרות "לשחזר" את המבנה של A מבטיחה כי הפולינום f נשאר אי פריק מעל $K_s(\boldsymbol{\sigma})$.

לבסוף, אנו מצרפים את הסגור האבלי לשדה המדובר. המנה של תת החבורה המלאה נמצאת תחת הרחבה אבלית זו ($K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma})$) ולכן היא חילופית. לפי התכונה הראשונה של תת חבורה מלאה המנה חייבת להיות טריוויאלית. לכן הפולינום ישאר אי פריק גם אחרי צרוף הסגור האבלי של K.

2 מכפלת הזר המפותלת

בחלק זה נראה שאם לחבורת זר מפותלת $A \operatorname{wr}_{G'} G$ יש איבר ב־ G בעל "סדר" גדול ב־ G/G', אז יש לחבורה זו תת חבורה בעלת דרגה 2 שהיא "כמעט" חבורת זר מפותלת. כמובן, צריך להסביר בדיוק למה הכוונה ב"סדר" של איבר בקבוצה G/G' שאינה חבורה, ומה הכוונה במילה "כמעט".

2.1 הגדרות וסימונים

תהיינה A ו־ G חבורות סופיות ותהי G' תת חבורה של G. נניח כי G' פועלת על A (מימין). נסמן ב־ $A \operatorname{wr}_{G'} G = G \ltimes \operatorname{Ind}_{G'}^{G}(A)$ את מכפלת הזר המפותלת [Ha, הגדרה 1.1] או [FrJ2, הגדרה 13.7.2]. ביתר פרוט,

$$\operatorname{Ind}_{G'}^{G}(A) = \{\xi \colon G \to A \mid \xi(\sigma\rho) = \xi(\sigma)^{\rho}, \quad \forall \sigma \in G,\ \ \rho \in G'\}$$

עם פעולת הכפל הרגילה, $(\xi\zeta)(\sigma) = \xi(\sigma)\zeta(\sigma)$. החבורה G פועלת על $\operatorname{Ind}_{G'}^{G}(A)$ באופן הבא: $(\xi^{\tau})(\sigma) = \xi(\tau\sigma)$, באשר $\xi \in \operatorname{Ind}_{G'}^{G}(A)$ ו־ $\sigma, \tau \in G$. החבורה $A \operatorname{wr}_{G'} G$ וגם ההטלה על G, $\operatorname{pr} \colon A \operatorname{wr}_{G'} G \to G$, נקראות *מכפלת זר מפותלת*. החבורה A משוכנת ב־ $\operatorname{Ind}_{G'}^{G}(A)$ על ידי $a \mapsto \xi_a$ כאשר $\xi_a(\rho) = \begin{cases} a^{\rho} & \rho \in G' \\ 1 & \rho \notin G' \end{cases}$. נבחר מערכת מייצגים Σ של מחלקות ימניות $G'\sigma$ ב־ G, המכילה את איבר היחידה. לכל $\sigma \in \Sigma$ מתקיים

$$A^{\sigma} = \{\xi \in \operatorname{Ind}_{G'}^{G}(A) \mid \xi(G \smallsetminus \sigma^{-1}G') = 1\}.$$

אזי $\operatorname{Ind}_{G'}^{G}(A) = \prod_{\sigma \in \Sigma} A^{\sigma}$. נסמן ב־ $N_G = \prod_{\sigma \neq 1} A^{\sigma}$ את הגרעין של ההטלה על הרכיב הראשון, דהיינו ההטלה $\xi \mapsto \xi(1)$.

תהי $\bar{A}$ חבורת מנה לא טריוויאלית של A ונסמן $M = \ker(A \to \bar{A})$. נסמן את האפימורפיזם $A \to \bar{A}$ ב־ $a \mapsto \bar{a}$. אם $M^{G'} = M$, אז G' פועלת על $\bar{A}$ ויש

אפימורפיזם טבעי המעתיק איבר (σ,ξ) של $A\operatorname{wr}_{G'} G$ לאיבר $\overline{(\sigma,\xi)} = (\sigma,\bar{\xi})$ של $\bar{A}\operatorname{wr}_{G'} G$. כאן $\bar{\xi}(\sigma) = \overline{\xi(\sigma)}$.

הגדרה 2.1.1 תהיינה $G' \leq G$ חבורות סופיות ויהי $\beta \in G$. נגדיר $\operatorname{ord}_{G'}(\beta)$ להיות הסדר של β בחבורה $\langle\beta\rangle / (\langle\beta\rangle \cap G')$.

טענה 2.1.2 *תהיינה $G' \leq G$ חבורות סופיות ו־$\beta \in G$.*

(א) $\operatorname{ord}_{G'}(\beta) = (\langle\beta\rangle : \langle\beta\rangle \cap G') = \min(k \geq 1 \mid \beta^k \in G')$,

(ב) $\operatorname{ord}_{G'}(\beta) \mid k \iff \beta^k \in G'$,

(ג) *יהי* $d = \operatorname{ord}_{G'}(\beta)$. *אזי* $\operatorname{ord}_{G'}(\beta^{n_0}) = \frac{d}{\gcd(n_0,d)}$ *ובפרט* $\operatorname{ord}_{G'}(\beta^{n_0}) \geq \frac{d}{n_0}$,

(ד) *אם* $G' \lhd G$, *אז* $\operatorname{ord}_{G'}(\beta)$ *הוא הסדר של התמונה של* β *במנה* G/G',

(ה) $\operatorname{ord}_1(\beta) = \operatorname{ord}(\beta)$,

(ו) *אם* $G \geq G' \geq G''$, *אז* $\operatorname{ord}_{G'}(\beta) \mid \operatorname{ord}_{G''}(\beta)$ *ובפרט* $\operatorname{ord}_{G'}(\beta) \leq \operatorname{ord}_{G''}(\beta)$.

הוכחה. סעיפים א'־ה' ברורים. כדי לראות שסעיף ו' נכון, נסתכל בסדרה המדויקת הבאה $1 \longrightarrow \langle\beta\rangle / (\langle\beta\rangle \cap G') \longrightarrow \langle\beta\rangle / (\langle\beta\rangle \cap G'')$. נוכל להסיק כי $(\langle\beta\rangle : (\langle\beta\rangle \cap G')) \mid (\langle\beta\rangle : (\langle\beta\rangle \cap G''))$. **על פי סעיף א'** $\operatorname{ord}_{G'}(\beta) \mid \operatorname{ord}_{G''}(\beta)$.

■

2.2 תת חבורות מדרגה 2 של מכפלת הזר המפותלת

למה 2.2.1 *תהיינה G, H, N, M חבורות כך ש־G פועלת על N ו־ H פועלת על M. נניח כי יש שיכונים $j\colon M \to N,\ i\colon H \to G$. נאמר כי השיכונים תואמים אם $j(m^h) = j(m)^{i(h)}$ לכל $h \in H$, $m \in M$. אזי:*

קיים שיכון $\psi\colon H \ltimes M \to G \ltimes N$ כך שהתרשים הבא חילופי אם ורק אם השיכונים תואמים.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G \ltimes N & \longrightarrow & G & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle j} & & \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle i} & & \\ 1 & \longrightarrow & M & \longrightarrow & H \ltimes M & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

יתר על כן, ניתן לבחור את ψ כך ש־

(א) $\psi(H \ltimes M) \cap G = \psi(H)$,

(ב) $\psi(H \ltimes M) \cap N = \psi(M)$.

הוכחה. נסמן את האיברים של מכפלה חצי ישרה ב־$(g,n) = gn$. חוק הכפל הינו $ng = gn^g$ וההופכי נתון על ידי $(gn)^{-1} = g^{-1}n^{-(g^{-1})}$.

אם השיכונים תואמים, נגדיר $\psi\colon H \ltimes M \to G \ltimes N$ על ידי הכלל

$$\psi(h,m) = (i(h), j(m)) = i(h)j(m).$$

בדיקה פשוטה (להלן) מראה כי ψ הומומורפיזם.

$$\begin{aligned} &\psi((h_1m_1)(h_2m_2)) = \\ &= \psi(h_1h_2m_1^{h_2}m_2) = i(h_1h_2)j(m_1^{h_2}m_2) = \\ &= i(h_1)i(h_2)j(m_1)^{i(h_2)}j(m_2) = i(h_1)j(m_1)i(h_2)j(m_2) = \\ &= \psi(h_1m_1)\psi(h_2m_2) \end{aligned}$$

כמו כן, ψ הינו שיכון. אכן, אם מתקיים $i(h_1)j(m_1) = i(h_2)j(m_2)$, נובע כי $i(h_1) = i(h_2)$ ו־$j(m_1) = j(m_2)$. מאחר ו־i,j שיכונים, נובע כי $h_1 = h_2$ ו־$m_1 = m_2$.

ולהפך, אם קיים שיכון $\psi\colon H \ltimes M \to G \ltimes N$ כך שהתרשים חילופי, אז מתקיים

$$\begin{aligned}\psi(mh) &= \psi(m)\psi(h) = j(m)i(h) = i(h)j(m)^{i(h)} \\ \psi(mh) &= \psi(hm^h) = i(h)j(m^h)\end{aligned}$$

ולכן $j(m^h) = j(m)^{i(h)}$, כלומר, השיכונים תואמים.

יהי $gn = \psi(hm)$, אזי $\psi(H \ltimes M) \cap G$. אזי, מאחר ו־ ψ חח"ע, נובע כי $g = \psi(h) = i(h)$, $n = \psi(m) = j(m)$. אם $n = 1$, נקבל כי $m = 1$ ולכן קיבלנו את (א). אם $g = 1$, אז $h = 1$ ולכן קיבלנו את (ב). ■

כזכור, עבור חבורת הזר המפותלת $A \operatorname{wr}_{G'} G$ אנו מסמנים ב־N_G את הגרעין של ההטלה $\operatorname{Ind}_{G'}^G(A) \to A$ הנתונה על ידי $\xi \mapsto \xi(1)$.

טענה 2.2.2 *תהי H תת חבורה של G ותהי $H' = H \cap G'$. אזי H' פועלת על A ו־ $A \operatorname{wr}_{H'} H$ ניתנת לשיכון בחבורה $A \operatorname{wr}_{G'} G$. יתר על כן, שיכון זה מקיים*

(א) $A \operatorname{wr}_{H'} H \cap G = H$,

(ב) $A \operatorname{wr}_{H'} H \cap \operatorname{Ind}_{G'}^G(A) = \operatorname{Ind}_{H'}^H(A)$,

(ג) $A \operatorname{wr}_{H'} H \cap N_G = \operatorname{Ind}_{H'}^H(A) \cap N_G = N_H$.

הוכחה. לכל $\xi \in \operatorname{Ind}_{H'}^H(A)$ נגדיר $\hat{\xi} \in \operatorname{Ind}_{G'}^G(A)$ באופן הבא. לכל $\sigma \in H$ נגדיר $\hat{\xi}(\sigma) = \xi(\sigma)$. נרחיב את ההגדרה של $\hat{\xi}$ למחלקות שמאליות hG' על פי הכלל $\hat{\xi}(\sigma\rho) = \xi(\sigma)^\rho$ כאשר $\sigma \in H, \rho \in G'$. בשאר המחלקות של G' נגדיר $\hat{\xi}(\sigma) = 1$ לכל $\sigma \in G \setminus \bigcup_{\tau \in H} \tau G'$. הפונקציה $\hat{\xi}$ מוגדרת היטב מאחר ואם $\sigma_1\rho_1 = \sigma_2\rho_2$ עבור $\sigma_1, \sigma_2 \in H$ ועבור $\rho_1, \rho_2 \in G'$, אז $\rho_1\rho_2^{-1} = \sigma_1^{-1}\sigma_2 \in H$ ולכן $\rho_1\rho_2^{-1} \in H'$. לכן

$$\hat{\xi}(\sigma_1\rho_1) = \xi(\sigma_1)^{\rho_1} = \xi(\sigma_1)^{\rho_1\rho_2^{-1}\rho_2} = \xi(\sigma_1\rho_1\rho_2^{-1})^{\rho_2} = \xi(\sigma_2)^{\rho_2} = \hat{\xi}(\sigma_2\rho_2).$$

נסמן ב־ $i\colon H \to G$ את שיכון ההכלה, ונסמן ב־ $j\colon \mathrm{Ind}_{H'}^{H}(A) \to \mathrm{Ind}_{G'}^{G}(A)$ את ההעתקה המעתיקה $\xi \in \mathrm{Ind}_{H'}^{H}(A)$ ל־ $\hat{\xi} \in \mathrm{Ind}_{G'}^{G}(A)$. ברור כי j הינה מונומורפיזם. נראה כי i, j הינם שיכונים תואמים, דהיינו, נראה כי לכל $\xi \in \mathrm{Ind}_{H'}^{H}(A)$ ולכל $\sigma \in H$ מתקיים $j(\xi^{\sigma}) = j(\xi)^{i(\sigma)}$. אם $\upsilon \notin \bigcup_{\tau \in H} \tau G'$ אז $j(\xi^{\sigma})(\upsilon) = j(\xi)^{i(\sigma)}(\upsilon) = 1$. עבור $\tau \in H, \rho \in G'$ מתקיים

$$j(\xi^{\sigma})(\tau\rho) = \xi^{\sigma}(\tau)^{\rho} = \xi(\sigma\tau)^{\rho} = j(\xi)^{i(\sigma)}(\tau\rho).$$

נשתמש בלמה 2.2.1 כדי להסיק מכאן כי מכפלת הזר המפותלת $A \operatorname{wr}_{H'} H$ ניתנת לשיכון במכפלת הזר המפותלת $A \operatorname{wr}_{G'} G$. טענות (א), (ב) ו־(ג) נובעות מההגדרה של השיכון שבנינו. ■

הגדרה 2.2.3 תהי $A \operatorname{wr}_{G'} G$ מכפלת זר מפותלת ותהי $\boldsymbol{S}$ תת חבורה שלה. נסמן $H = \mathrm{pr}(\boldsymbol{S})$, $H' = H \cap G'$ ונסתכל על $A \operatorname{wr}_{H'} H$ כתת חבורה של $A \operatorname{wr}_{G'} G$. אזי $\boldsymbol{S}$ נקראת *מלאה*, אם $\boldsymbol{S} \leq A \operatorname{wr}_{H'} H$ וגם מתקיימות שתי התכונות הבאות:

(א) לכל חבורת מנה לא טריוויאלית $\bar{A} \cong A/M$ של A כך ש־ $M^{H'} = M$, החבורה $\bar{\boldsymbol{S}}$ איננה חילופית. (החבורה $\bar{\boldsymbol{S}}$ הינה התמונה של $\boldsymbol{S}$ תחת האפימורפיזם $A \operatorname{wr}_{H'} H \to \bar{A} \operatorname{wr}_{H'} H$).

(ב) נסמן ב־ φ את ההטלה $\mathrm{Ind}_{G'}^{G}(A) \to A$ המוגדרת ע"י $\xi \mapsto \xi(1)$. אז מתקיים $\varphi\left(\boldsymbol{S} \cap \mathrm{Ind}_{H'}^{H}(A)\right) = A$.

למה 2.2.4 *תהיינה $G' \leq G$ ו־ A חבורות סופיות. נסמן $n = \mathrm{rank} A$. נניח כי G' פועלת על A ותהי $A \operatorname{wr}_{G'} G$ חבורת הזר המפותלת. יהי $\beta \in \mathrm{Z}(G)$ כך ש־ $\mathrm{ord}_{G'}(\beta) \geq 2n$. אז קיים $\xi \in \mathrm{Ind}_{G'}^{G}(A)$ כך שלכל $\alpha \in G$ תת החבורה $\langle \beta, \alpha\xi \rangle$ היא מלאה.*

הוכחה. יהיו $a_1, \ldots, a_n$ יוצרים של A. נסמן $m = \mathrm{ord}_{G'}(\beta)$. אזי $\beta, \ldots, \beta^m$ הם נציגים למחלקות השמאליות של $\langle\beta\rangle \cap G'$ ב־ $\langle\beta\rangle$. כיוון ש־ $m \geq 2n$ ניתן להגדיר ξ כפונקציה מ־$\langle\beta\rangle$ ל־A באופן הבא.

$$\xi(\beta^k) = \begin{cases} a_i & 1 \leq i \leq n \text{ וגם } k = 2i \\ 1 & \text{אחרת} \end{cases},$$

עבור $\sigma = \beta^k\rho$, באשר $\rho \in \langle\beta\rangle \cap G'$ ו־$1 \leq k \leq m$, נגדיר $\xi(\sigma) = \xi(\beta^k)^\rho$.

יהי $\alpha \in G$, $\boldsymbol{S} = \langle\beta, \alpha\xi\rangle$. מהבנייה ברור כי $\xi \in \mathrm{Ind}_{\langle\beta\rangle\cap G'}^{\langle\beta\rangle}(A)$. בפרט, $H = \langle\beta, \alpha\rangle = \mathrm{pr}(\boldsymbol{S})$ ו־ $\xi \in \mathrm{Ind}_{\langle\beta,\alpha\rangle\cap G'}^{\langle\beta,\alpha\rangle}(A)$. נסיק כי $\boldsymbol{S} \leq A \operatorname{wr}_{H'} H$ באשר $H' = H \cap G'$. תהי $\bar{A} \neq 1$ חבורת מנה של A כך שפעולת G' שומרת על הגרעין של $A \to \bar{A}$. יש i כך ש־ $\bar{a}_i \neq \bar{1}$. מאחר ו־ $\beta \in \mathrm{Z}(G)$, מתקיים $(\alpha\xi)^\beta = \alpha^\beta\xi^\beta = \alpha\xi^\beta$. אבל

$$\bar{\xi}(\beta^{2i-1}) = \bar{1} \neq \bar{a}_i = \bar{\xi}(\beta^{2i}) = \bar{\xi}^\beta(\beta^{2i-1})$$

ולכן $\overline{(\alpha\xi)^\beta} \neq \overline{(\alpha\xi)}$, כלומר, $\bar{\boldsymbol{S}}$ איננה חילופית. בכך הוכחנו את 2.2.3(א).

לכל $1 \leq i \leq n$, נגדיר $h_i = (\alpha\xi)^{-\beta}(\alpha\xi)^{\beta^{2i}} = \xi^{-\beta}\xi^{\beta^{2i}}$. כאן השתמשנו בכך ש־ $\beta \in \mathrm{Z}(G)$. אזי מתקיים $h_i(1) = \xi^{-\beta}(1)\xi(\beta^{2i}) = \xi^{-1}(\beta)a_i = a_i$. נשים לב כי $h_i \in \boldsymbol{S} \cap \mathrm{Ind}_{H'}^H(A)$. לכן נסיק כי התמונה של $\boldsymbol{S} \cap \mathrm{Ind}_{H'}^H(A)$ ע"י φ היא על. לכן תנאי (ב) של הגדרה 2.2.3 מתקיים. ■

2.3 פרוש בשדות

הגדרה 2.3.1 יהי $K \subseteq K' \subseteq L$ מגדל של שדות. נניח כי L/K הרחבת גלואה סופית, נסמן $G = \mathrm{Gal}(L/K)$, $G' = \mathrm{Gal}(L/K')$. יהי $\beta \in G$. נגדיר $\mathrm{ord}_{K'}(\beta) = \mathrm{ord}_{G'}(\beta)$ (ראה הגדרה 2.1.1).

ננסח כעת טענה הנובעת ישירות מטענה 2.1.2

טענה 2.3.2 *יהי $K \subseteq K' \subseteq K'' \subseteq L$ מגדל של שדות, L/K הרחבת גלואה סופית יהי $\beta \in \mathrm{Gal}(L/K)$. אז*

(א) $\mathrm{ord}_{K'}(\beta) = (\langle\beta\rangle : \langle\beta\rangle \cap \mathrm{Gal}(L/K')) = \min(k \geq 1 \mid \beta^k|_{K'} = \mathrm{id})$,

(ב) יהי $d = \mathrm{ord}_{K'}(\beta)$. *אזי* $\mathrm{ord}_{K'}(\beta^{n_0}) = \frac{d}{\gcd(n_0,d)}$ *ובפרט* $\mathrm{ord}_{K'}(\beta^{n_0}) \geq \frac{d}{n_0}$,

(ג) אם K'/K *הרחבת גלואה, אז* $\mathrm{ord}_{K'}(\beta)$ *הוא הסדר של* $\beta|_{K'}$ *בחבורה* $\mathrm{Gal}(K'/K)$,

(ד) $\mathrm{ord}_{K'}(\beta) \mid \mathrm{ord}_{K''}(\beta)$ *ובפרט* $\mathrm{ord}_{K'}(\beta) \leq \mathrm{ord}_{K''}(\beta)$.

נניח כי K'/K הרחבה אלגברית פרידה, ונניח כי F/K' גלואה. עבור שיכון־K, $\sigma\colon K' \to K_s$, נסמן ב־ F^σ את השדה $F^{\hat{\sigma}}$ כאשר $\hat{\sigma}$ הינה הרמה של σ ל־ $\mathrm{Gal}(K)$. שדה זה מוגדר היטב. נסמן ב־ $\mathcal{E}(K'/K)$ את אוסף כל שיכוני־K, $K' \to K_s$.

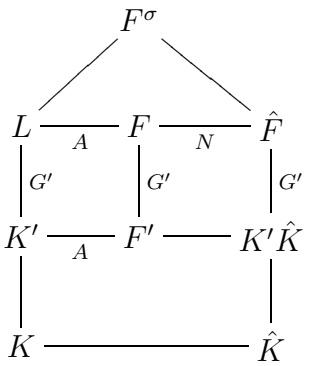
הערה 2.3.3 **נאמר כי מגדל של שדות $K \subseteq K' \subseteq L \subseteq F \subseteq \hat{F}$ ממשש את החבורה $A \operatorname{wr}_{G'} G$ אם [Ha, הערה 1.2] או [FrJ2, הערה 13.7.6]:**

(א) L/K, F/K' ו־ $\hat{F}/K$ הן הרחבות גלואה.

(ב) השדות $\{F^\sigma\}_{\sigma\in\mathcal{E}(K'/K)}$ מופרדים לינארית מעל L ו־ $\hat{F} = \prod_{\sigma\in\mathcal{E}(K'/K)} F^\sigma$.

(ג) קיים שדה $\hat{K}$ כך ש־ $L \cap \hat{K} = K$ ו־ $L\hat{K} = \hat{F}$.

(ד) $G \cong \mathrm{Gal}(\hat{F}/\hat{K}) \cong \mathrm{Gal}(L/K)$. נסמן $A = \mathrm{Gal}(F/L)$, $F' = F \cap (K'\hat{K})$, אז מתקיים $G' \cong \mathrm{Gal}(L/K') \cong \mathrm{Gal}(F/F') \cong \mathrm{Gal}(\hat{F}/K'\hat{K})$.



החבורה $G' = \mathrm{Gal}(F/F')$ פועלת על החבורה $A \triangleleft \mathrm{Gal}(F/K')$ ע"י הצמדה ב־ $\mathrm{Gal}(F/K')$ ו־ $G = \mathrm{Gal}(\hat{F}/\hat{K})$ פועל על $\mathrm{Ind}_{G'}^{G}(A) = \mathrm{Gal}(\hat{F}/L)$ ע"י הצמדה ב־ $\mathrm{Gal}(\hat{F}/K)$. לפי תורת גלואה נסיק כי $\mathrm{Gal}(\hat{F}/K) \cong G \ltimes \mathrm{Ind}_{G'}^{G}(A) = A \operatorname{wr}_{G'} G$.

ולהפך, נניח כי $\mathrm{Gal}(\hat{F}/K) \cong A \operatorname{wr}_{G'} G$. נסמן ב־$F$ את שדה השבת של N_G, ב־L את שדה השבת של $\mathrm{Ind}_{G'}^{G}(A)$, וב־$\hat{K}$ את שדה השבת של G. נסמן ב־K' את שדה השבת של התמונה של G' תחת האיזומורפיזם $\mathrm{res}_L : G \to \mathrm{Gal}(L/K)$. אז התנאים לעיל מתקיימים.

נניח כי $K, K', L, F, \hat{F}$ מממשים את $A \operatorname{wr}_{G'} G$, כאשר A, G חבורות סופיות ו־ G' תת־חבורה של G הפועלת על A. לכל $L \subsetneq P \subseteq F$ הרחבת גלואה של K' עם חבורת גלואה $\bar{A} = \mathrm{Gal}(P/L)$, נתאים $\hat{P} = \prod_{\sigma \in \mathcal{E}(K'/K)} P^\sigma$. לכן $K, K', L, P, \hat{P}$ מממשים את $\bar{A} \operatorname{wr}_{G'} G$ ובפרט $\hat{P}$ הוא סגור גלואה של P מעל K. מטענה 2.2.2 נוכל להסיק את הטענה:

טענה 2.3.4 *יהיו $K, K', L, F, \hat{F}$ שדות המממשים את $A \operatorname{wr}_{G'} G$ עבור איזשהם $G' \leq G$, A ופעולה של G' על A. תהי $H \leq G$ ו־ $H' = H \cap G'$. לפי טענה 2.2.2 $A \operatorname{wr}_{H'} H$ משוכנת ב־$A \operatorname{wr}_{G'} G$. יהי D שדה השבת של $A \operatorname{wr}_{H'} H$ ב־ $\hat{F}$. אזי $D, K'D, LD, FD, \hat{F}$ ממשים את $A \operatorname{wr}_{H'} H$.*

הוכחה. ע"פ טענה 2.2.2 ועל פי תורת גלואה נובע כי

$$\begin{aligned}
\mathrm{Gal}(\hat{F}/D) &\cong A\,\mathrm{wr}_{H'}\,H, \\
\mathrm{Gal}(\hat{F}/LD) &= \mathrm{Ind}_{G'}^{G}(A)\cap A\,\mathrm{wr}_{H'}\,H=\mathrm{Ind}_{H'}^{H}(A), \\
\mathrm{Gal}(\hat{F}/FD) &= N_G\cap A\,\mathrm{wr}_{H'}\,H=N_H, \\
\mathrm{Gal}(\hat{F}/\hat{K}D) &= G\cap A\,\mathrm{wr}_{H'}\,H=H, \\
\mathrm{Gal}(LD/K'D) &= \mathrm{Gal}(\hat{F}/K'\hat{K}D)=G'\cap A\,\mathrm{wr}_{H'}\,H=G'\cap H=H'.
\end{aligned}$$

נסיק מהערה 2.3.3 כי $D, K'D, LD, FD, \hat{F}$ ממשים את $A\,\mathrm{wr}_{H'}\,H$. ■

טענה 2.3.5 *תהי E/K הרחבה של שדות, נזהה את החבורה $\mathrm{Gal}(\hat{F}E/E)$ עם החבורה $A\,\mathrm{wr}_{G'}\,G$ ונסמנה $\boldsymbol{S}$. תהי $A\,\mathrm{wr}_{H'}\,H\le \mathrm{Gal}(\hat{F}/\hat{F}\cap E)\le \mathrm{Gal}(\hat{F}/K)\cong A\,\mathrm{wr}_{G'}\,G$, באשר $H=\mathrm{pr}(\boldsymbol{S})$ ו־ $H'=H\cap G'$. נסמן ב־ D את שדה השבת של $A\,\mathrm{wr}_{H'}\,H$ ב־ $\hat{F}$. אזי $\boldsymbol{S}$ תת חבורה מלאה של $A\,\mathrm{wr}_{G'}\,G$ אם ורק אם מתקיימים שלושת התנאים הבאים:*

(1) לכל P כמוגדר לעיל החבורה $\mathrm{res}_{\hat{P}}\boldsymbol{S}\cong \mathrm{Gal}(\hat{P}E/E)$ איננה חילופית.

(2) $\mathrm{Gal}(FE/LE)\cong \mathrm{Gal}(F/L)=A$ ובפרט $[FE:LE]=[F:L]$.

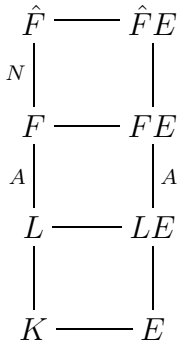
(3) $D\subseteq E$.

הוכחה. ע"פ תורת גלואה, $\boldsymbol{S}\le A\,\mathrm{wr}_{H'}\,H$ אם ורק אם $D\subseteq \hat{F}\cap E$. הואיל ו־ $D\subseteq \hat{F}$, מתקיים $D\subseteq \hat{F}\cap E$ אם ורק אם $D\subseteq E$. כלומר, התנאי $\boldsymbol{S}\le A\,\mathrm{wr}_{H'}\,H$ שקול ל (3).

על פי תורת גלואה ישנה התאמה חח"ע בין הרחבות גלואה P של L המוכלות ב־ F לבין תת חבורות נורמליות $M\triangleleft A$. מתקיים (א) $L\neq P$ אם ורק אם $M\neq A$; (ב) P גלואה מעל K' אם ורק אם $M^{G'}=M$. לכן ישנה

התאמה חח"ע ועל בין הרחבות $L \subsetneq P \subseteq F$ שהן גלואה מעל K' לבין תת חבורות נורמליות $M \neq A$ של A המקיימות $M^{G'} = M$. אם P מתאים ל־M ונסמן $\bar{A} = A/M \neq 1$, אז מתקיים $\mathrm{Gal}(\hat{P}/K) \cong \bar{A} \operatorname{wr}_{G'} G$. לכן $\mathrm{res}_{\hat{P}} \boldsymbol{S} = \bar{\boldsymbol{S}}$ ולכן 2.2.3(א) שקול לתנאי 1.

נסתכל בחבורה $N = N_G$ $\mathrm{Gal}(\hat{F}/K)$. השדה F מתאים לתת החבורה הגרעין של ההטלה $f \mapsto f(1)$ מ־$\mathrm{Ind}_{G'}^{G}(A)$ על A. השדה L מתאים לחבורה $\mathrm{Ind}_{G'}^{G}(A)$, ולכן $[F : L] = (\mathrm{Ind}_{G'}^{G}(A) : N) = |A|$. נסתכל על $\boldsymbol{S} \cap N$ ו־$\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A)$ כתת חבורות של $\boldsymbol{S} \cong \mathrm{Gal}(\hat{F}E/E)$. לפי תורת גלואה מתאים השדה FE לתת החבורה $\boldsymbol{S} \cap N$ והשדה LE מתאים לתת החבורה $\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A)$. לכן מתקיים $[FE : LE] = (\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A) : \boldsymbol{S} \cap N)$.



הואיל ו־$\mathrm{Gal}(FE/LE) \leq \mathrm{Gal}(F/L)$, נסיק כי $\mathrm{Gal}(FE/LE) = \mathrm{Gal}(F/L)$ אם ורק אם $[FE : LE] = [F : L]$. לכן

$$\mathrm{Gal}(FE/LE) = \mathrm{Gal}(F/L) \iff (\boldsymbol{S} \cap \mathrm{Ind}_{G'}^{G}(A) : \boldsymbol{S} \cap N) = |A|.$$

ולכן תנאי 2 שקול לתנאי 2.2.3(ב). ■

לצורך המשפט המרכזי נצטרך ליישם את למה 2.2.4 בשדות.

למה 2.3.6 *תהי $\boldsymbol{S} \leq A \operatorname{wr}_{G'} G$ תת חבורה מלאה כך שההטלה על G, $\mathrm{pr}(\boldsymbol{S})$, אבלית. יהיו $K, K', L, F, \hat{F}$ שדות המממשים את $A \operatorname{wr}_{G'} G$. תהי E/K הרחבה*

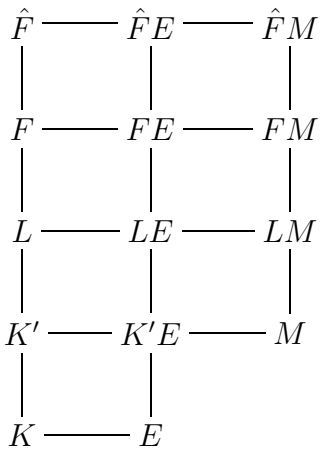
כך ש־$\hat{F} \cap E$ מוכל בשדה השבת של $\boldsymbol{S}$ ב־$\hat{F}$ ותהי M/E הרחבה אבלית כך ש־$K'E \subseteq M$. אז $[FM : LM] = [F : L]$.

הוכחה. *שלב ראשון:* **ניתן להניח כי** $\boldsymbol{S} \cong \mathrm{Gal}(\hat{F}E/E)$.

אכן, נסמן ב־E' את שדה השבת של $\boldsymbol{S}$ ב־$\hat{F}E$. אם $E \subsetneq E'$, אז נחליף את E ב־E' ואת M ב־ME'. אם נראה כי $[FME' : LME'] = [F : L]$, אז בפרט ינבע כי $[FM : LM] = [F : L]$.

שלב שני: **ניתן להניח כי** $\mathrm{pr}(\boldsymbol{S}) = G$.

אכן, נסמן $H = \mathrm{pr}(\boldsymbol{S})$, $H' = H \cap G'$. יהי D שדה השבת של $A \operatorname{wr}_{H'} H$ ב־$\hat{F}$. השדות $D, DK', DL, DF, \hat{F}$ ממשים את $A \operatorname{wr}_{H'} H$ (טענה 2.3.4). נחליף את השדות $K \subseteq K' \subseteq L \subseteq F \subseteq \hat{F}$ בשדות $D \subseteq DK' \subseteq DL \subseteq DF \subseteq \hat{F}$. מאחר ו־$D \subseteq E$ (טענה 2.3.5), נובע כי $K'D \subseteq K'E \subseteq M$. מאחר ו־$[DF : DL] = |A| = [F : L]$, מספיק להראות כי מתקיים $[DFM : DLM] = [DF : DL]$.



שלב שלישי: **סיום הוכחת הלמה.**

מטענה 2.3.5 (2) נובע כי $[F : L] = [FE : LE]$. על פי השלב הראשון, $\boldsymbol{S} = \mathrm{Gal}(\hat{F}E/E)$ ולכן $\mathrm{pr}(\boldsymbol{S}) = \mathrm{Gal}(LE/E)$. מצד שני, על פי השלב השני,

$\mathrm{pr}(\boldsymbol{S}) = G = \mathrm{Gal}(L/K)$. לכן נקבל כי $[L:K] = [LE:E]$. נסיק כי

$$[F:K'] = [F:L][L:K'] = [FE:LE][LE:K'E] = [FE:K'E].$$

השתמשנו בעובדה כי אם $[L:K] = [LE:E]$, אזי לכל שדה ביניים K' מתקיים $[L:K'] = [LE:K'E]$. הואיל ו־$\mathrm{Gal}(FE/K'E) \leq \mathrm{Gal}(F/K')$, נובע כי $\mathrm{Gal}(F/K') = \mathrm{Gal}(FE/K'E)$.

נניח כי $FE \cap LM \neq LE$. החיתוך הוא שדה ביניים של $FE/K'E$ המכיל את LE ולכן מתאים לו שדה P כך ש $L \subseteq P \subseteq F$, $PE = FE \cap LM$ ו־P/K' גלואה. כיוון ש־ $PE \neq LE$ גם $P \neq L$. לשדה P נתאים את השדה $\hat{P} = \prod_{\sigma\in G} P^\sigma = \prod_{\sigma\in\mathcal{E}(K'/K)} P^\sigma$ מעל K. שדה זה הינו סגור גלואה של P מעל K. יתר על כן, $\hat{P}E$ הינו סגור גלואה של PE מעל E. אכן, סגור גלואה של PE מעל E הינו צרוף כל השדות הצמודים, דהיינו,

$$\prod_{\sigma\in\boldsymbol{S}} (PE)^\sigma = \prod_{\sigma\in\mathrm{pr}(\boldsymbol{S})} (PE)^\sigma = \prod_{\sigma\in G} P^\sigma E = \hat{P}E .$$

בשוויונות הללו השתמשנו בכך ש־$\mathrm{pr}(\boldsymbol{S}) = G$ ובעובדה כי PE/LE גלואה ולכן $(PE)^\sigma$ תלוי רק בצמצום של $\sigma \in \boldsymbol{S}$ ל־ LE.

מאחר ו־$\hat{P}E$ הינו סגור גלואה של PE מעל E ומאחר ש־$PE \subseteq LM$, נובע כי $\hat{P}E \subseteq LM$. בשלב השני הראינו כי $\mathrm{Gal}(LE/E) = \mathrm{pr}(\boldsymbol{S})$ ולכן LE/E אבלית. לפי ההנחה M/E אבלית ולכן LM/E אבלית. בפרט $\mathrm{Gal}(\hat{P}E/E)$ אבלית. מאידך על פי טענה 2.3.5 (1) $\mathrm{Gal}(\hat{P}E/E)$ איננה אבלית. סתירה.

מסתירה זו נסיק כי $FE \cap LM = LE$ ולכן נסיק כי FE, LM מופרדים לינארית מעל LE ובפרט $[FM:LM] = [FE:LE] = [F:L]$. ■

מסקנה 2.3.7 *יהי $n_0 \in \mathbb{N}$ ותהי $A \operatorname{wr}_{G'} G$ מכפלת זר של חבורות סופיות. נסמן ב־n את הדרגה של A. נניח כי $K, K', L, F, \hat{F}$ מממשים את $A \operatorname{wr}_{G'} G$. תהי*

כך ש־ $\beta \in G$ *וכך שלכל* $\xi \in \mathrm{Ind}_{G'}^{G}(A)$ *אזי קיים* $\beta^{n_0} \in \mathrm{Z}(G)$ *ו־* $\mathrm{ord}_{K'}(\beta) \geq 2nn_0$. *המקיימים* $\sigma_1, \sigma_2 \in \mathrm{Gal}(K)$ *ולכל הרחבה אבלית* $M/K_s(\boldsymbol{\sigma})$ *המקיימת* $K'K_s(\boldsymbol{\sigma}) \subseteq M$ *מתקיים* $[FM : LM] = [F : L]$.

הוכחה. נסמן $\beta_0 = \beta^{n_0}$. **על פי טענה 2.3.2 (ב) מתקיים** $\mathrm{ord}_{K'}(\beta_0) \geq 2n$. **נקח** $\xi \in \mathrm{Ind}_{G'}^{G}(A)$ **מלמה 2.2.4 עבור** β_0 **במקום** β. **יהיו** σ_1, σ_2 **המקיימים את הנחות המסקנה, כלומר, הם מקיימים** $\sigma_1|_{\hat{F}} = \beta, \sigma_2|_{\hat{F}} = \alpha\xi$ **עבור איזשהו** $\alpha \in G$. **תת החבורה** $\boldsymbol{S} = \langle \beta_0, \alpha\xi \rangle$ **של** $A \operatorname{wr}_{G'} G$ **היא מלאה (למה 2.2.4).** $\mathrm{pr}(\boldsymbol{S})$ **הינה אבלית כי** $\beta_0 \in \mathrm{Z}(G)$.

נסמן $E = K_s(\boldsymbol{\sigma})$. **מאחר ו־**$\langle \sigma_1^{n_0}, \sigma_2 \rangle \leq \langle \sigma_1, \sigma_2 \rangle$ **נובע כי** $E \subseteq K_s(\sigma_1^{n_0}, \sigma_2)$ **ולכן** $\hat{F} \cap E$ **מוכל בשדה השבת של** $\boldsymbol{S}$ **ב־**$\hat{F}$. **נשתמש בלמה הקודמת כדי לקבל** $[FM : LM] = [F : L]$ **לכל הרחבה אבלית** $M/K_s(\boldsymbol{\sigma})$ **המקיימת** $K'K_s(\boldsymbol{\sigma}) \subseteq M$. ■

3 מידת האר של חבורות פרו־סופיות

3.1 הגדרות וסימונים

נגדיר מידת האר, Haar Measure, μ של חבורה פרו־סופית A לפי [FrJ1, פרק 16], כלומר מידת האר מתוקנת (כלומר, $\mu(A)=1$) על חבורה קומפקטית.

שתי תת קבוצות X,Y של חבורה פרו־סופית A נקראות *בלתי תלויות* אם $\mu(X\cap Y)=\mu(X)\mu(Y)$. משפחה של תת קבוצות $\{X_i\}_{i\in I}$ של A נקראת *בלתי תלויה* אם $\mu(\cap_{j\in J}X_j)=\prod_{j\in J}\mu(X_j)$ לכל $J\subseteq I$ תת קבוצה סופית.

לשדה K נתאים את המידה של חבורת גלואה המוחלטת שלו, דהיינו, מידת האר של החבורה $\mathrm{Gal}(K)=\mathrm{Gal}(K_s/K)$. נסמן מידה זו ב־$\mu$.

שני שדות L_1,L_2 מעל שדה K נקראים *מופרדים לינארית מעל* K אם כל קבוצה בלתי תלויה לינארית $\{x_1,\ldots,x_n\}$ של איברים של L_1 מעל K נשארת בלתי תלויה לינארית מעל L_2 [La, VIII,§3]. הגדרה זו למעשה אינה תלויה בסדר השדות [FrJ2, למה 2.5.1]. אוסף סופי של שדות $\{L_1,\ldots,L_n\}$, $n>2$, נקרא *מופרד לינארית מעל* K אם $\{L_1,\ldots,L_{n-1}\}$ מופרדים לינארית מעל K וגם L_n מופרד לינארית מ־ $L_1\cdots L_{n-1}$ מעל K. גם במקרה זה אין חשיבות לסדר השדות. משפחה של שדות $\{L_1,L_2,L_3,\ldots\}$ נקראת *מופרדת לינארית מעל* K אם כל תת קבוצה סופית שלה מופרדת לינארית מעל K.

יש קשר הדוק בין שדות מופרדים לינארית מעל שדה K לבין תת קבוצות של $\mathrm{Gal}(K)$ בלתי תלויות. דוגמאות לקשר זה ניתן לראות ב [FrJ1, למה 16.9] או בלמה 3.2.1 להלן.

3.2 אי תלות הסתברותית במכפלות חצי ישרות

למה 3.2.1 *לכל $i\in\mathbb{N}$ יהי $K\subseteq N\subseteq M_i$ מגדל של הרחבות גלואה סופיות נניח כי $\{M_i\}$ מופרדים לינארית מעל N, ותהי $S_i\subseteq\mathrm{Gal}(M_i/K)$ קבוצה כך ש־*

$\mathrm{res}\colon \mathrm{Gal}(M_i/K) \to \mathrm{Gal}(N/K)$ *מעתיקה את* S_i *באופן חח"ע על* $\mathrm{Gal}(N/K)$. *אז* $X_i = \{\sigma \in \mathrm{Gal}(K) \mid \mathrm{res}_{M_i}(\sigma) \in S_i\}$ *בלתי תלויים.*

הוכחה. צריך להראות כי לכל $n \in \mathbb{N}$ ולכל $i_1, \ldots, i_n$ מספרים טבעיים שונים, $\mu(\bigcap_{j=1}^{n} X_{i_j}) = \prod_{j=1}^{n} \mu(X_{i_j})$. לשם פשטות הסימונים נניח כי $i_j = j$.

היות ו־ $X_i = \mathrm{res}_{M_i}^{-1}(S_i)$, ומאחר ומידת האר של חבורה סופית הינה מידת הספירה הרגילה, נובע כי $\mu(X_i) = \frac{\#S_i}{[M_i:K]} = \frac{[N:K]}{[M_i:K]} = \frac{1}{[M_i:N]}$.

נסמן $\hat{M} = M_1 \cdots M_n$. היות והשדות $\{M_i\}$ מופרדים לינארית מעל N, נובע ע"פ תורת גלואה כי

$$\begin{aligned} \mathrm{Gal}(\hat{M}/K) &\cong \{(\sigma_1, \ldots, \sigma_n) \in \prod_{i=1}^{n} \mathrm{Gal}(M_i/K) \mid \mathrm{res}_N \sigma_1 = \cdots = \mathrm{res}_N \sigma_n\}, \\ \mathrm{Gal}(\hat{M}/N) &\cong \mathrm{Gal}(M_1/N) \times \cdots \times \mathrm{Gal}(M_n/N), \end{aligned}$$

כאשר האיזומורפיזם לעיל מוגדר על ידי $\sigma \mapsto (\sigma_1, \ldots, \sigma_n)$, באשר $\sigma_i = \mathrm{res}_{M_i}\sigma$ לכל $1 \le i \le n$.

תהי $S = \{\sigma \in \mathrm{Gal}(\hat{M}/K) \mid \sigma_i \in S_i \text{ לכל } i\}$. נספור כמה איברים יש ב־$S$. יהי $\alpha \in \mathrm{Gal}(N/K)$ ויהי $1 \le i \le n$. מאחר ו־ S_i מועתקת באופן חח"ע על $\mathrm{Gal}(N/K)$ יש $\sigma_i \in S_i$ יחיד המועתק על α. לכן יש איבר יחיד של S שצמצומו ל־N הוא α. מכאן שב־S יש $[N:K]$ איברים. נסמן ב־μ' את המידה של $\mathrm{Gal}(\hat{M}/K)$ ונקבל כי

$$\mu(\bigcap_{i=1}^{n} X_i) = \mu'(S) = \frac{[N:K]}{[\hat{M}:K]} = \frac{1}{[\hat{M}:N]} = \prod_{i=1}^{n} \frac{1}{[M_i:N]} = \prod_{i=1}^{n} \mu(X_i).$$

■

למה 3.2.2 *[FrJ1, עמוד 209] תהיינה* H, G *חבורות פרו־סופיות. נסמן ב־* $G \times H$ *את חבורת המכפלה. תהיינה* $X_i \subseteq G$, $i \in \mathbb{N}$, *אוסף קבוצות בלתי תלויות ביחס למידת האר של* G *ו־*$Y_j \subseteq H$, $j \in \mathbb{N}$, *אוסף קבוצות בלתי תלויה ביחס למידת האר של* H. *אז האוסף* $\{X_i \times Y_i\}$ *בלתי תלוי ביחס למידת המכפלה.*

הוכחה. מספיק להראות כי המידה של חיתוך של מספר סופי של $X_i \times Y_i$ שווה למכפלת המידות, ואכן

$$\begin{aligned}\mu\left(\bigcap_{i=1}^{N}(X_i \times Y_i)\right) &= \mu\left(\left(\bigcap_{i=1}^{N} X_i\right) \times \left(\bigcap_{i=1}^{N} Y_i\right)\right) = \\ &= \mu_G\left(\bigcap_{i=1}^{N} X_i\right) \cdot \mu_H\left(\bigcap_{i=1}^{N} Y_i\right) = \prod_{i=1}^{N} \mu_G\left(X_i\right) \cdot \prod_{i=1}^{N} \mu_H\left(Y_i\right) = \\ &= \prod_{i=1}^{N} \mu_G(X_i) \cdot \mu_H(Y_i) = \prod_{i=1}^{N} \mu(X_i \times Y_i)\end{aligned}$$

ולכן הסדרה $\{X_i \times Y_i\}$ בלתי תלויה. ■

מסקנה 3.2.3 *לכל $i \in \mathbb{N}$ יהי $K \subseteq N \subseteq M_i$ מגדל של הרחבות גלואה סופיות מעל K עם חבורות גלואה איזומורפיות ל־ $G, G \ltimes I$ בהתאמה. יהיו $c_1, c_2 \in I$. לכל $i \in \mathbb{N}$ יהיו G_i, c_{i1}, c_{i2} התמונות של G, c_1, c_2 תחת האיזומורפיזם $G \ltimes I \to \mathrm{Gal}(M_i/K)$. אם $\{M_i\}$ מופרדים לינארית מעל N, אז כמעט לכל $\boldsymbol{\sigma} = (\sigma_1, \sigma_2) \in \mathrm{Gal}(K)^2$, קיימים אינסוף i־ים עבורם $\mathrm{res}_{M_i}(\sigma_1, \sigma_2) \in (G_i c_{i1}, G_i c_{i2})$.*

הוכחה. נפעיל את למה 3.2.1 על הקבוצות

$$X_i = \{\sigma \in \mathrm{Gal}(K) \mid \sigma|_{M_i} \in G_i c_{i1}\}, \quad Y_i = \{\sigma \in \mathrm{Gal}(K) \mid \sigma|_{M_i} \in G_i c_{i2}\}.$$

תנאי הלמה מתקיימים ולכן $\{X_i\}, \{Y_j\}$ הן שתי סדרות בלתי תלויות ביחס למידת האר של $\mathrm{Gal}(K)$. נסיק מלמה 3.2.2 כי $\{X_i \times Y_i\}$ היא סדרה בלתי תלויה ביחס למידת המכפלה.

מאחר ו־ $\mu(X_i) = \mu(Y_i) = \frac{1}{\#I} > 0$, נובע כי

$$(\mu \times \mu)(X_i \times Y_i) = \mu(X_i) \cdot \mu(Y_i) = \frac{1}{(\#I)^2},$$

ולכן $\sum_{i=1}^{\infty}(\mu \times \mu)(X_i \times Y_i) = \infty$. נשתמש בלמת Borel-Cantelli [FrJ1, למה 16.7] כדי להסיק כי $(\mu \times \mu)(\bigcap_{N=1}^{\infty} \bigcup_{i=N}^{\infty}(X_i \times Y_i)) = 1$. ■

3.3 חבורות פרו־סופיות לא חסומות

חבורה פרו־סופית אבלית A נקראת *חסומה* אם הקבוצה $\{\mathrm{ord}(a) \mid a \in A\} \subseteq \mathbb{N}$ חסומה [Ro, עמוד 104], אחרת נאמר כי A *איננה חסומה*.

ב־ [Ra, למה 3.2] הוכח כי אם חבורה פרו־סופית אבלית A איננה חסומה, אז $\mu\{a \in A \mid \mathrm{ord}(a) = \infty\} = 1$. לכן ניתן להכליל ולהגדיר:

הגדרה 3.3.1 תהי A חבורה פרו־סופית. נאמר כי A *איננה חסומה* אם כמעט כל איבריה מסדר אינסופי, כלומר, $\mu(\{a \in A \mid \mathrm{ord}(a) = \infty\}) = 1$.

טענה 3.3.2 *תהי A חבורה פרו־סופית. אז שלושת התנאים הבאים שקולים:*

(א) החבורה A איננה חסומה.

(ב) לכל $m \in \mathbb{N}$ מתקיים $\mu(\{a \in A \mid \mathrm{ord}(a) \geq m\}) = 1$.

(ג) לכל $\varepsilon > 0$ ולכל $m \in \mathbb{N}$, קיימת תת חבורה $N \lhd A$ פתוחה עבורה מתקיים $\mu(\{a \in A \mid \mathrm{ord}_N(a) \geq m\}) \geq 1 - \varepsilon$ ($\mathrm{ord}_N(a)$ הינו הסדר של aN בחבורה A/N).

הוכחה. נסמן $X_\infty = \{a \in A \mid \mathrm{ord}(a) = \infty\}$, $X_m = \{a \in A \mid \mathrm{ord}(a) \geq m\}$, $X_m(N) = \{a \in A \mid \mathrm{ord}_N(a) \geq m\}$. לכל $m \in \mathbb{N}$ הקבוצה X_m הינה קבוצה פתוחה, מאחר ואם $\mathrm{ord}(y) \geq m$, אז קיימת תת חבורה $N \lhd A$ פתוחה עבורה $\mathrm{ord}_N(y) \geq m$, ולכן $yN \subseteq X_m$.

$1 \Leftrightarrow 2$ חלק זה נובע מיידית מהעובדה כי $X_\infty = \bigcap_{m=1}^{\infty} X_m$.

$2 \Leftarrow 3$ מאחר ולכל $N \lhd A$ מתקיים $X_m(N) \subseteq X_m$, נובע כי לכל $\varepsilon > 0$ קיימת תת חבורה $N \lhd A$ עבורה $\mu(X_m) \geq \mu(X_m(N)) \geq 1 - \varepsilon$, ולכן $\mu(X_m) = 1$.

$2 \Leftarrow 3$ **יהיו** $\varepsilon > 0,\ m \in \mathbb{N}$. **מאחר ו־** $\mu(X_m) = 1$**, נובע ע"פ הרגולריות של המידה כי יש תת קבוצה סגורה (ולכן קומפקטית)** $K \subseteq X_m$**, כך ש** $\mu(K) \geq 1 - \varepsilon$**. הואיל והקבוצה** X_m **פתוחה, לכל** $y \in K$ **קיימת תת חבורה** $N_y \triangleleft A$ **פתוחה כך ש** $yN_y \subseteq X_m$**. מאחר ו** K **קומפקטית ניתן לבחור מהכיסוי הפתוח** $K \subseteq \bigcup_{y \in K} yN_y$ **תת כיסוי סופי, נאמר** $y_1N_1, \ldots, y_rN_r$**. נסמן**

$$N = N_1 \cap N_2 \cap \cdots \cap N_r.$$

מספיק להראות כי $K \subseteq X_m(N)$**. אכן, אם** $y \in K$**, אז קיים** $1 \leq i \leq r$ **כך ש־** $y \in y_iN_i$ **ולכן** $\mathrm{ord}_{N_i}(y) \geq m$ **ולכן** $\mathrm{ord}_N(y) \geq \mathrm{ord}_{N_i}(y) \geq m$ **(טענה 2.1.2 סעיף (ו)).**

■

4 שימושים

4.1 סימונים

הגדרה 4.1.1 יהי K שדה ותהי M הרחבת גלואה שלו. נאמר כי M/K *איננה חסומה* אם $\mathrm{Gal}(M/K)$ איננה חסומה.

יהי K שדה הילברטי בן מנייה ותהי M/K הרחבה אבלית לא חסומה של K. נסמן $\mathcal{G} = \mathrm{Gal}(K)$, ונסמן ב־ μ, μ_e את מידות Haar המתוקנות של $\mathcal{G}, \mathcal{G}^e$ בהתאמה.

בסעיף זה נרצה להוכיח את **משפט 1**, בעזרת מכפלות הזר המפותלות וקריטריון להילברטיות [Ha, למה 2.4].

4.2 פולינום אחד

יהי $f(T,X)$ פולינום אי פריק לחלוטין. נרצה להראות שכמעט לכל σ ניתן להציב אינסוף a־ים כך ש־$f(a,X)$ נשאר אי־פריק מעל $MK_s(\sigma)$ ואפילו מעל $K_{\mathrm{ab}}K_s(\sigma)$. נעיר כי בסעיף זה איננו מניחים כי K הוא בן מנייה.

לצורך החלק המרכזי נזדקק ללמה קטנה מתורת השדות.

למה 4.2.1 *תהי M/K הרחבה אבלית ותהי K_0/K הרחבת גלואה ממעלה n_0. נסמן $G = \mathrm{Gal}(MK_0/K)$. אז לכל $\beta \in G$, $\beta^{n_0} \in \mathrm{Z}(G)$.*

הוכחה. על פי תורת גלואה $G \leq \mathrm{Gal}(M/K) \times \mathrm{Gal}(K_0/K)$. נסמן, אם כן, $\beta = (x,y)$ כאשר $x \in \mathrm{Gal}(M/K), y \in \mathrm{Gal}(K_0/K)$. מכאן $\beta^{n_0} = (x^{n_0}, y^{n_0}) = (x^{n_0}, 1)$. מאחר ו־$\mathrm{Gal}(M/K)$ אבלית, נובע כי $\beta^{n_0} \in \mathrm{Z}(G)$. ■

למה 4.2.2 *יהי K שדה הילברטי ויהיו $v_1, v_2 \in K_s$ אברים פרידים מעל K. יהי $f(T,X) \in K(v_1)[T,X]$ פולינום אי פריק לחלוטין, מתוקן ב־ X וגלואה מעל*

$K(v_1,v_2)(T)$. יהי $\varepsilon>0$. אז קיימת $\Upsilon\subseteq\mathcal{G}^2$ בעלת מידה $1-\varepsilon\le$ כך שלכל $\boldsymbol{\sigma}\in\Upsilon$ מתקיים

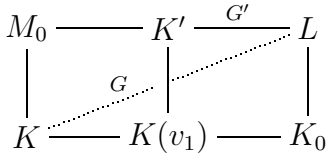
(*) אם $v_1\in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ אז קיימים אינסוף $a\in M(v_1)$ כך ש־ $f(a,X)$ אי פריק מעל $K_{\mathrm{ab}}(v_1,v_2)K_s(\boldsymbol{\sigma})$.

הוכחה. נגדיר $A=\mathrm{Gal}(f,K_s(T))$, ונסמן $n=\mathrm{rank}A$. תהי K_0 הרחבת גלואה סופית של K המקיפה את $K(v_1,v_2)$, ונסמן $n_0=[K_0:K]$. יהי $m\ge 2nn_0$ מספר שלם.

חלק א: הגדרת Υ בעלת מידה $1-\varepsilon\le$.

שלב ראשון: בניית G ו־G'.

ההרחבה M/K איננה חסומה (הגדרה 3.3.1) ולכן קיימת הרחבה M_0 סופית של K המוכלת ב־M כך ש־ $\mu(\{\sigma\in\mathcal{G}\mid \mathrm{ord}_{M_0}(\sigma)\ge m\})\ge 1-\varepsilon$ (טענה 3.3.2). נסמן $K'=M_0(v_1)$ ו־$L=M_0K_0$. ההרחבה L/K הינה הרחבת גלואה. נסמן $G=\mathrm{Gal}(L/K)$ ו־$G'=\mathrm{Gal}(L/K')$. אזי G' פועל על $A\cong\mathrm{Gal}(f,L(T))$.



נסמן $\Sigma_1'=\{\sigma\in\mathcal{G}\mid \mathrm{ord}_{K'}(\sigma)\ge m\}$ (ראה הגדרה 2.3.1). לכל $\sigma\in\mathcal{G}$ המקיימת $\mathrm{ord}_{M_0}(\sigma)\ge m$ מתקיים בפרט $\mathrm{ord}_{K'}(\sigma)\ge m$ (טענה 2.3.2), ולכן

$$\mu(\Sigma_1')\ge 1-\varepsilon. \tag{1}$$

שלב שני: מימוש $A\,\mathrm{wr}_{G'}\,G$ מעל K.

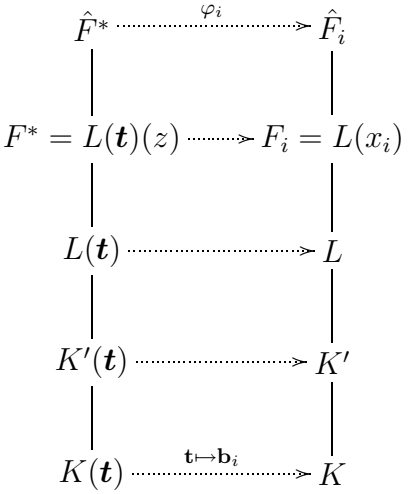
הפולינום $f(T,X)$ מוגדר מעל K' וגלואה מעל $L(T)$. יהי $d_1,\dots,d_r$ בסיס של K' מעל K ותהי $\boldsymbol{t}=(t_1,\dots,t_r)$ קבוצת משתנים בלתי תלויים אלגברית. על פי [Ha, למה 3.1] או [FrJ2, למה 13.8.1] קיימים $F^*,\hat{F}^*$ המקיימים

(א) $K(\boldsymbol{t}), K'(\boldsymbol{t}), L(\boldsymbol{t}), F^*, \hat{F}^*$ ממשים את $A\operatorname{wr}_{G'} G$ ו־ $\hat{F}^*$ רגולרי מעל L,

(ב) $F^* = L(\boldsymbol{t})(z)$ באשר $\operatorname{irr}(z, L(\boldsymbol{t})) = f\left(\sum_{i=1}^r d_i t_i, Z\right) \in K'[\boldsymbol{t}, Z]$.

ההרחבה $\hat{F}^*$ הינה רגולרית מעל L ו־K שדה הילברטי. באופן דומה לבנייה המופיעה ב־ [FrJ1, משפט 16.18], ניתן למצוא אינסוף ייחודי־L $\boldsymbol{t} \mapsto \boldsymbol{b}_i$, באשר $\boldsymbol{b}_i = (b_{1i}, \ldots, b_{ri}) \in K^r$, אותם ניתן להרחיב לאתרי־ L $\varphi_i \colon \hat{F}^* \to \hat{F}_i \cup \{\infty\}$ כך ש־ $\operatorname{Gal}(\hat{F}_i/K) \cong A\operatorname{wr}_{G'} G$ והשדות $\hat{F}_i$ מופרדים לינארית מעל L. יתר על כן, ניתן לבחור את $\boldsymbol{b}_i \in K^r$ כך ש־ φ_i ממפה את $K(\boldsymbol{t})$, $K'(\boldsymbol{t})$ ו־ $L(\boldsymbol{t})$ על $K(\boldsymbol{b}_i)\cup\{\infty\} = K\cup\{\infty\}$, $K'(\boldsymbol{b}_i)\cup\{\infty\} = K'\cup\{\infty\}$, $L(\boldsymbol{b}_i)\cup\{\infty\} = L\cup\{\infty\}$, בהתאמה, $i = 1, 2, \ldots$ (ראה [FrJ2, למה 2.2.7]).

אם נסמן $c_i = \sum_j d_j b_{ji} \in K'$ ו־ $x_i = \varphi_i(z)$, אז x_i הוא שורש של $f(c_i, X)$, והתמונה F_i של F^* תחת φ_i מקיימת $F_i = L(x_i)$. מכך ש־ $\{d_j\}$ בלתי תלויים לינארית מעל K ו־ $\boldsymbol{b}_i \in K^r$, נובע כי ייחודים שונים $\boldsymbol{t} \mapsto \boldsymbol{b}_i$ נותנים אברים c_i שונים.



שלב שלישי: בניית Υ.

כזכור, $G \le A\operatorname{wr}_{G'} G$. לכל $\tau \in A\operatorname{wr}_{G'} G$ נסמן ב־ G_i, τ_i את התמונות של G, τ תחת האיזומורפיזם המעתיק את $A\operatorname{wr}_{G'} G$ על $\operatorname{Gal}(\hat{F}_i/K)$.

יהי $\beta \in \mathrm{Gal}(L/K)$ **כך ש־**$\mathrm{ord}_{K'}(\beta) \geq m$. **לפי למה 4.2.1,** $\beta^{n_0} \in \mathrm{Z}(G)$.
על פי מסקנה 2.3.7 עם $M = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$, **קיים** $\xi \in \mathrm{Ind}_{G'}^{G}(A)$ **(**ξ **תלויה ב־**β**) כך שלכל** $\sigma_1, \sigma_2 \in \mathcal{G}$ **המקיימים** $\sigma_1|_{\hat{F}_i} = \beta_i,\ \sigma_2|_{\hat{F}_i} \in G_i\xi_i$ **מתקיים: אם** $v_1 \in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$**, אז**

$$[F_iK_{\mathrm{ab}}K_s(\boldsymbol{\sigma}) : LK_{\mathrm{ab}}K_s(\boldsymbol{\sigma})] = [F_i : L]. \qquad (2)$$

תהי

$$\Sigma_{12}(\beta) = \{(\sigma_1, \sigma_2) \in \mathcal{G}^2 \mid \mathrm{res}_{\hat{F}_i}(\sigma_1, \sigma_2) \in G_i \times G_i\xi_i \text{ עבור אינסוף } i\text{־ים}\}.$$

אז $\mu_2(\Sigma_{12}(\beta)) = 1$ **(מסקנה 3.2.3).**
נפרק את Σ_1' **למחלקות שמאליות של** $\mathrm{Gal}(L)$**, דהיינו,**

$$\Sigma_1' = \bigcup_{\substack{\beta \in \mathrm{Gal}(L/K) \\ \mathrm{ord}_{K'}(\beta) \geq m}} \Sigma_1(\beta),$$

באשר $\Sigma_1(\beta) = \{\sigma \in \mathcal{G} \mid \sigma|_L = \beta\}$. **עתה נגדיר**

$$\Upsilon = \bigcup_{\substack{\beta \in \mathrm{Gal}(L/K) \\ \mathrm{ord}_{K'}(\beta) \geq m}} (\Sigma_1(\beta) \times \mathcal{G}) \cap \Sigma_{12}(\beta).$$

כלומר $(\sigma_1, \sigma_2) \in \Upsilon \iff \mathrm{ord}_{K'}(\sigma_1) \geq m$ **וקיימים אינסוף** i**־ים כך ש־**$\sigma_1|_{\hat{F}_i} \in G_i$**,** $\sigma_2|_{\hat{F}_i} \in G_i\xi_i$ **וגם** ξ_i **מתאים ל־**β**. מאחר ו־** $\mu_2(\Sigma_{12}(\beta)) = 1$**,**

$$\begin{aligned} \mu_2(\Upsilon) &= \sum_{\beta} \mu_2\left((\Sigma_1(\beta) \times \mathcal{G}) \cap \Sigma_{12}(\beta)\right) \\ &= \sum_{\beta} \mu\left(\Sigma_1(\beta)\right) = \mu(\Sigma_1') \overset{(1)}{\geq} 1 - \varepsilon. \end{aligned}$$

חלק ב: כל $\boldsymbol{\sigma} \in \Upsilon$ **מקיים את תנאי (*).**
יהי $\boldsymbol{\sigma} \in \Upsilon$**. נסמן** $N = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ **ונניח כי** $v_1 \in N$**. יהי** $i \in \mathbb{N}$ **עבורו מתקיים** $\mathrm{res}_{\hat{F}_i}(\sigma_1, \sigma_2) \in G_i \times G_i\xi_i$**. ממשוואה (2) נוכל להסיק כי מתקיים**

$[F_iN : LN] = [F_i : L] = \deg f(c_i, X)$. **מאחר ו־** $F_i = L(x_i)$, **נובע כי** $F_iN = LN(x_i)$. **מאחר ו־** $f(c_i, x_i) = 0$, **נובע כי** $f(c_i, X) = \mathrm{irr}(x_i, LN)$. **לכן** $f(c_i, X)$ **אי פריק מעל** LN **ובפרט אי פריק מעל** $K_{\mathrm{ab}}(v_2)K_s(\boldsymbol{\sigma})$. **מאחר ויש אינסוף** i**־ים המקיימים זאת, יש אינסוף איברים** $c \in K' \subseteq M(v_1)$ **כך ש־**$f(c, X)$ **אי פריק מעל** $K_{\mathrm{ab}}(v_2)K_s(\boldsymbol{\sigma})$. ■

למה 4.2.3 *יהי* K *שדה הילברטי, יהי* $e \geq 2$ *מספר טבעי ויהיו* $v_1, v_2 \in K_s$. *יהי* $f(T, X) \in K(v_1)[T, X]$ *פולינום אי פריק לחלוטין, מתוקן ב־* X *וגלואה מעל* $K(v_1, v_2)(T)$. *אז כמעט לכל* $\boldsymbol{\sigma} \in \mathcal{G}^e$ *מתקיים תנאי (*).*

הוכחה. **ראשית נוכיח עבור** $e = 2$. **על פי הלמה הקודמת, לכל** $\varepsilon > 0$ **קיימת קבוצה** $\Upsilon_\varepsilon \subseteq \mathcal{G}^2$ **בעלת מידה** $\geq 1 - \varepsilon$, **כך שלכל** $\boldsymbol{\sigma} = (\sigma_1, \sigma_2) \in \Upsilon$ **מתקיים (*). נסמן** $\Sigma = \bigcup_{n\in\mathbb{N}} \Upsilon_{\varepsilon_n}$, **באשר** ε_n **סדרה שואפת לאפס. מתכונת השלמות של מידת האר נובע כי** Σ **קבוצה מדידה, וכמובן, בעלת מידה** 1.

עבור $e > 2$ **נגדיר** $\Sigma' = \Sigma \times \overbrace{\mathcal{G} \times \cdots \times \mathcal{G}}^{e-2 \text{ פעמים}}$ **באשר** Σ **היא הקבוצה המתאימה ל־**$e = 2$. Σ' **היא תת קבוצה של** $\mathcal{G}^e$ **בעלת מידה** 1. **לכל** $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \Sigma'$, **אם** $v_1 \in K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$, **אז בפרט** $v_1 \in K_{\mathrm{ab}}K_s(\sigma_1, \sigma_2)$, **ולכן יש אינסוף** $a \in M(v_1)$ **עבורם** $f(a, X)$ **אי פריק מעל** $K_{\mathrm{ab}}(v_2)K_s(\sigma_1, \sigma_2)$. **בפרט** $f(a, X)$ **אי פריק מעל השדה** $K_{\mathrm{ab}}(v_1, v_2)K_s(\boldsymbol{\sigma})$ **החלקי לשדה** $K_{\mathrm{ab}}(v_1, v_2)K_s(\sigma_1, \sigma_2)$.

■

4.3 המשפט המרכזי

ראשית ננסח קריטריון להילברטיות של שדות ביניים.

למה 4.3.1 *תהי* P/M *הרחבה אלגברית פרידה של שדות. אם לכל הרחבת ביניים* M' *של* P/M *ממעלה סופית, לכל הרחבת גלואה סופית* P'/P *ולכל פולינום אי פריק לחלוטין* $f \in M'[T, X]$, *מתוקן ב־* X *וגלואה מעל* $P'(T)$, *קיימים אינסוף*

$a \in M'$ עבורם $f(a,X)$ אי פריק מעל P', אז כל הרחבת ביניים של P/M הינה הילברטית

הוכחה. תהי Q הרחבת ביניים של P/M. כדי להוכיח ש־ Q הילברטית, על פי [Ha, למה 2.4] או [FrJ2, למה 13.1.4] מספיק לבדוק כי לכל פולינום $f \in Q[T,X]$ אי פריק לחלוטין, מתוקן ב־ X ולכל הרחבת גלואה סופית Q' של Q, קיימים אינסוף $a \in Q$ כך ש־ $f(a,X)$ אי פריק מעל Q'. יהיו f, Q ו־ Q' כאלו. תהי $M' \subseteq Q$ הרחבה ממעלה סופית של M כך ש־ f מוגדר מעל M'. נסמן $P' = PQ'$. אזי לפי הנחות הלמה קיימים אינסוף $a \in M' \subseteq P$ כך ש־ $f(a,X)$ אי פריק מעל P' ובפרט $f(a,X)$ אי פריק מעל Q'. ■

משפט 1 *יהי $e \geq 2$, יהי K שדה הילברטי בן מנייה ותהי M/K הרחבה אבלית לא חסומה. אז כמעט לכל $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ כל הרחבת ביניים של $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})/M$ היא הילברטית*

הוכחה. לכל $f \in K_s[T,X]$ אי פריק לחלוטין ומתוקן ב־ X, ולכל $v_1, v_2 \in K_s$ עבורם f מוגדר מעל $K(v_1)$ וגלואה מעל $K(v_1,v_2)(T)$, נגדיר את $\Sigma(f,v_1,v_2)$ כקבוצת ה $\boldsymbol{\sigma}$־ים מלמה 4.2.3. נגדיר

$$\Sigma = \bigcap_{f,v_1,v_2} \Sigma(f,v_1,v_2),$$

מאחר ו־ $\mu(\Sigma(f,v_1,v_2)) = 1$ ויש מספר בן מנייה של קבוצות כאלה, נובע כי $\mu(\Sigma) = 1$.

יהי $\boldsymbol{\sigma} \in \Sigma$. נסמן $P = K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ וניישם את למה 4.3.1. יהי $f \in P[T,X]$ פולינום אי פריק לחלוטין, מתוקן ופריד ב־X, ותהי P'/P הרחבת גלואה סופית עבורה f גלואה מעל $P'(T)$. יהי M' שדה ביניים של P/M כך ש f מוגדר מעליו. נבחר $v_1 \in M'$ כך ש $f \in K(v_1)[T,X]$.

יהי $v_2 \in K_s$ כך ש $P' \subseteq P(v_2)$ ו־ f גלואה מעל $K(v_1, v_2)(T)$. מאחר ו־ $\sigma \in \Sigma(f, v_1, v_2)$, נובע מלמה 4.2.3 כי קיימים אינסוף $a \in M(v_1)$, ולכן ב־ M', עבורם $f(a, X) \in P[X]$ הוא אי פריק מעל $P(v_2)$ ובפרט מעל P'. ■

הוכחת משפט רזון בדרך זו מביאה באופן טבעי לשאלה הבאה. האם ניתן להחליף את ההרחבה האבלית הלא חסומה בהרחבות אחרות?

ננסח השערות בסגנון משפט היהלום של הרן.

השערה 1 *יהיו M_1, M_2 שתי הרחבות גלואה של K ויהי $e \geq 2$ מספר טבעי. אם ההרחבה M_1M_2/M_i לא חסומה $(i = 1, 2)$, אז כמעט לכל $\sigma \in \mathrm{Gal}(K)^e$ כל שדה בין $M_1M_2K_s(\sigma)$ לבין M_1M_2 הילברטי.*

או ניסוח כללי יותר:

ניתן להכליל את הגדרה 4.1.1 באופן הבא: הרחבה M של K תקרא *לא חסומה* אם $\mu\{\sigma \in \mathrm{Gal}(K) | \mathrm{ord}_M \sigma = \infty\} = 1$.

השערה 2 *יהיו M_1, M_2 שתי הרחבות גלואה של K ויהי $e \geq 2$ מספר טבעי. תהי $M \subseteq M_1M_2$ כך שההרחבה $M/M \cap M_i$ לא חסומה $(i = 1, 2)$, אז כמעט לכל $\sigma \in \mathrm{Gal}(K)^e$ כל שדה בין $MK_s(\sigma)$ לבין M הילברטי.*

רשימת מקורות

[FrJ1] M. Fried, M. Jarden, Field Arithmetic. Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986

[FrJ2] M. Fried, M. Jarden, Field Arithmetic, Second edition. Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2004

[Ha] D. Haran, Hilbertian fields under seprable algebraic extensions. Inventiones mathematicae **137**, 85-112 (1999)

[JL] M. Jarden, A. Lubotzky, Hilbertian fields and free profinite groups. J. London Math. Soc. **46**, 205-227 (1992)

[JR] M. Jarden, A. Razon, Pseudo Algebriacally closed field over rings. Israel Journal of Mathematics **86**, 25-59 (1994)

[La] S. Lang, Algebra 3rd-edition. Addison-Wesley, Reading, 1993 Algebra, third edition, Addison-Wesley, Reading, (1994)

[Ra] A. Razon, Abundance of Hilbertian domains, manuscripta math. **94**, 531-542 (1997)

[Ro] Robinson, D. : A course in the theory of groups. Graduate texts in mathematics **80**, Springer, New York, (1982)

Tel-Aviv University

The Raymond and Beverly Sackler

Faculty of Exact Sciences

School of Mathematical Sciences

Hilbertianity under algebraic extensions and Haar measure

A thesis submitted in partial fulfillment of graduation requirements

of the degree of M.Sc. in Tel-Aviv University

By

Bary Lior

Prepared under the supervision of Prof. Dan Haran

July, 2004

Abstract

We give a new proof to the following theorem of A. Razon:

Theorem: *Let K be a countable Hilbertian field and let $e \geq 2$ be an integer. Let M be an abelian extension of K such that the set $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}(M/K)\}$ is unbounded. Then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ every field between $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and M is Hilbertian.*

I Introduction

An algebraic separable field extension M of a Hilbertian field K is Hilbertian, if it satisfies the following essentially group theoretic condition: For certain embedding problems with twisted wreath product there should be **no** solutions contained in a certain Galois extension of K containing M [Ha, Thm. 3.2]. In [Ha] from 1999, D. Haran claims that the hitherto known results in this subject summarized in [JL] in 1992 - e.g., every abelian extension of a Hilbertian field is Hilbertian, Weissauer's Theorem [FrJ1, Prop. 15.5], etc - follow from this condition. Haran also proves a new result which produce new Hilbertian algebraic separable field extensions:

Haran's Diamond Theorem *If M_1, M_2 are two Galois extensions of K such that $M_1 \not\subseteq M_2$ and $M_2 \not\subseteq M_1$, then every field extension M of K satisfying $M \subseteq M_1M_2$ and $M \not\subseteq M_i$, $i = 1, 2$, is Hilbertian.*

However, in 1997, shortly before Haran's paper was submitted, in [Ra] A. Razon builds algebraic separable extensions of Hilbertian field which, a-priori, do not follows from Haran's condition.

Theorem 1.(Razon) *Let K be a countable Hilbertian field and let $e \geq 2$ be an integer. Let M be an abelian extension of K such that the set $\{\mathrm{ord}(a) \mid a \in \mathrm{Gal}(M/K)\}$ is unbounded. Then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ every field between $K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})$ and M is Hilbertian.*

Actually, Razon proves that for every abelian extension M' of K that contains M, the field $M'K_s(\boldsymbol{\sigma})$ is Hilbertian *over* M'. Razon also shows that one can replace Hilbertian fields with Hilbertian rings ([Ra, Def 2.2]). In this paper we are only interested in Hilbertian fields, hence we focus on Theorem 1 (which follows from the above more general result).

In order to prove Theorem 1, Razon uses the notion of *Pseudo Algebraic Closed (PAC) Field over a field (ring)* [Ra, Def. 1.1] which generalizes the notion of a PAC field. Here are several known properties of PAC fields (see [FrJ1]). In the brackets we state the generalization of those properties to PAC fields over a field (see [Ra], [JR]).

(a) If E is PAC (over K) and E' is an algebraic extension of E ($E' = EM$, where M/K an algebraic extension), then E' is PAC (over M).

(b) If K is a Hilbertian countable field then for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the field $K_s(\boldsymbol{\sigma})$ is PAC (over K).

(c) If E is PAC (over K) and ω-free, then E is a Hilbertian field (over K).

It follows from (a),(b), that for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)$ and for every abelian extension M' of K containing M, the field $M'K_s(\boldsymbol{\sigma})$ is PAC over M. A known fact is that for almost every $\boldsymbol{\sigma} \in \mathrm{Gal}(G)^e$ the field $K_s(\boldsymbol{\sigma})$ is e- free [FrJ1, Thm. 16.13]. From this one can derive that $M'K_s(\boldsymbol{\sigma})$ is ω-free. Thus, by (c), the field $M'K_s(\boldsymbol{\sigma})$ is Hilbertian over M'. Hence, every intermediate field between $M'K_s(\boldsymbol{\sigma})$ to M' is Hilbertian [Ra, Lemma 2.3]. So we get a proof of Theorem 1.

It seems that Razon's proof does not use anything similar to Haran's

condition. Moreover, it is not obvious whether one can use Haran's methods in this case.

In this paper, we modify the methods that appeared in [Ha] to this case, i.e., to "agree" with measure theory. For this purpose we can no longer work with a twisted wreath product, but with its subgroups which occur with "high probability".

In Chapter 2 we discuss the twisted wreath product $A \operatorname{wr}_{G'} G$. We are mostly interested in subgroups of rank 2 which are *full* (Definition 2.2.3). Those subgroups satisfy two important properties. Roughly speaking, the image of such subgroups under certain quotient maps stays noncommutative (unless it is trivial) and the second property is the ability to "recover" the structure of A from the subgroup. We show that there are many such subgroups. In this chapter we also translate the results of group theory to results about fields via Galois theory.

In Chapter 3 we discuss measure theory of pro-finite groups in general, and measure theory of *unbounded groups* (Definition 3.3.1) in particular.

In Chapter 4 we combine group theory with measure theory. We show (using the result from Chapter 3) that one can choose the subgroups of rank 2 (discussed in Chapter 2) with "high probability".

We start from an irreducible polynomial $f(T,X) \in K_s[T,X]$. Then we realize the wreath product $A \operatorname{wr}_{G'} G$ over the Hilbertian field K, where A is the Galois group of f over $K_s(T)$.

After that, we adjoin a "random field" (i.e. the field $K_s(\boldsymbol{\sigma})$ where $\boldsymbol{\sigma}$ is chosen with probability 1) to the realization of the wreath product, and get a realization of full subgroup of $A \operatorname{wr}_{G'} G$ over $K_s(\boldsymbol{\sigma})$.

The ability to "recover" the structure of A ensures that the polynomial f remains irreducible over the $K_s(\boldsymbol{\sigma})$. Finally, we compose the field under consideration with the abelian closure of K. The quotient of the full subgroup contained in this abelian extension $(K_{\mathrm{ab}}K_s(\boldsymbol{\sigma})/K_s(\boldsymbol{\sigma}))$ is commutative. By the first property of full subgroups, this quotient must be trivial. This implies that the polynomial remains irreducible even if we compose it with the abelian closure of K.