תורת רמזי

משה ירדן, אוניברסיטת תל אביב

כד באב, תשע"ב

תמצית: ברשימה זו מופיעים שני משפטים מרכזיים של תורת הצרופים, משפט Ramsey ומשפט Hales-Jewett יחד עם כמה מִשְׁמושיהם, בין הַיֶתר גם לארתמטיקת השדות. הקורא המְעֻנין להרחיב מֻפנה בזה לרשימתו של בֹעז צבן [Tsa11]. המחבר מודה לאהרֹן רזון על קריאה בִּקָרְתית של הרשימה ועל נִסוח והוכחת למה 2.3 .

1. משפט Ramsey

YESMAR 4 ,tupni

בסעיף זה נביא את המשפט המְפֻרסם של רַמְזִי עבור קבוצות אינסופיות, שִׁמוש שלו לארתמטיקת השדות ולבסוף את משפט רמזי לקבוצות סופיות.

עבור קבוצה X ומספר טבעי n נסמן ב $X^{[n]}$ את אֹסף תת הקבוצות של X בעלות n אֵברים (סימון אחר הנהוג לאֹסף הנ״ל הוא $\binom{A}{n}$). אם A הִנה תת קבוצה של X, אזי $A^{[n]} \subseteq X^{[n]}$.

aMAR 81 ,tupni

משפט 1.1 (משפט רַמְזִי האינסופי): *יהיו Q קבוצה סופית לא ריקה, X קבוצה אינסופית, n מספר טבעי ו $f\colon X^{[n]} \to Q$ פונקציה. אזי קַיֶמת ל X תת קבוצה אינסופית A כך ש f קבועה על $A^{[n]}$.*

הערה: בדרך כלל מתיַחסים ל Q כאל קבוצה של ״צבעים״ ואל f כאל פונקצית ״צביעה״, כלומר כפונקציה ה״צובעת״ כל תת קבוצה של X בעלת n אברים ב״צבע״ מתוך Q. במונחים אלו אומרת המסקנה של המשפט שלכל תת הקבוצות של A בעלות n אברים יש אותו ה״גַּוֶן״. ∎

הוכחה בהשראה על n (עִבּוד של הוכחה המופיעה בויקיפדיה): עבור $n = 1$ נובע מההגדרה ש $X^{[1]} = X$ ו f היא אפוא פונקציה מ X לקבוצה Q. הואיל ו Q סופית, X אינסופית ו $X = \bigcup_{q\in Q} f^{-1}(q)$, קַיָם $q \in Q$ כך ש $A = f^{-1}(q)$ אינסופית. בפרט, f קבועה על A.

נחלק את שארית ההוכחה לשני חלקים.

חלק א: *השראה.* נניח עתה ש $n \geq 2$ ושהמשפט נכון עבור $n-1$. נוכיחוֹ עבור n. לצֹרך זה נבנה בהשראה סִדרה יורדת

$$X = X_0 \supset X_1 \supset X_2 \supset \cdots$$

של תת קבוצות אינסופית של X וסִדרה של אברים $a_0, a_1, a_2, \ldots$ של אֵברים של X המקיְמים לכל $j \geq 1$ את הטענות הבאות:

(א1) $a_j \in X_j \smallsetminus X_{j+1}$.

(א2) לכל $B, B' \in X_{j+1}^{[n-1]}$ מתקיֵם $f(\{a_j\} \cup B) = f(\{a_j\} \cup B')$ (שים לב ש $a_j \notin B \cup B'$ ולכן כל אחת מן הקבוצות $\{a_j\} \cup B$ ו $\{a_j\} \cup B'$ היא בת n אברים).

ואכן, נניח שמצאנו כבר אברים $a_0, a_1, \ldots, a_{m-1} \in X$ וקבוצות $X = X_0 \supset X_1 \supset \cdots \supset X_m$ המקיְמים את התנאי (א) עבור $j = 0, \ldots, m-1$. נבחר $a_m \in X_m$, נתבונן בקבוצה $Y = X_m \smallsetminus \{a_m\}$ ונגדיר פונקציה $g\colon Y^{[n-1]} \to Q$ על ידי

$$g(B) = f(\{a_m\} \cup B).$$

שוב, $B \ni a_m$ לכל $B \in Y^{[n-1]}$ ולכן $\{a_m\} \cup B \in X^{[n]}$, כך ש $g(B)$ מֻגדר היטב. הנחת השראה על $(Y, n-1, g)$ נותנת תת קבוצה אינסופית X_{m+1} של Y כך ש g קבועה על $X_{m+1}^{[n-1]}$. במִלים אחרות,

$$f(\{a_m\} \cup B) = f(\{a_m\} \cup B')$$

לכל $B, B' \in X_{m+1}^{[n-1]}$. בזאת מתמלאת הדרישה (א) עבור $j = m$ וההשראה הֻשלמה.

חלק ב: *סִיום ההוכחה.* מ (א) נובע שאם $0 \le i_1 < i_2 < \cdots < i_n$ הם מספרים שלמים, אזי $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ הם אֵברים שונים של X ו $\{a_{i_2}, \ldots, a_{i_n}\} \in X_{i_1+1}^{[n-1]}$. לכן, $f(\{a_{i_1}, a_{i_2}, \ldots, a_{i_n}\})$ תלוי רק ב a_{i_1}. הואיל ו Q סופית, קיֶמת קבוצה אינסופית I של מספרים שלמים לא שליליִים וקיָם $q \in Q$ כך ש $f(\{a_{i_1}, a_{i_2}, \ldots, a_{i_n}\}) = q$ בכל מקרה ש $i_1, i_2, \cdots, i_n \in I$ ו $i_1 < i_2 < \cdots < i_n$.

הקבוצה $A = \{a_i \mid i \in I\}$ הִנה אפוא אינסופית והיא מקיֶמת $f(B) = q$ לכל $B \in A^{[n]}$, כמבֻקש. ∎

השִמוש הבא של הגרסה האינסופית של משפט רמזי מופיע במאמרם של ליאור ברי־סורוקר וארנו פֵּם [BSF12].

למה 1.2: *לכל סִדרה $L_0, L_1, L_2, \ldots$ של הרחבות פרידות סופיות של שדה K כך ש $L_i \cap L_j = K$ לכל $1 \le i < j$ קיֶמת תת סדרה $M_0, M_1 M_2, \ldots$ מֻפרדת לינארית מעל K כך ש $M_0 = L_0$.* bMAR 801 ,tupni

הוכחה: נגדיר קודם כל $M_0 = L_0$. עתה נניח בהשראה ש $M_1, \ldots, M_n$ היא תת סדרה סופית של $L_1, L_2, L_3, \ldots$ כך ש $M_0, M_1, \ldots, M_n$ מֻפרדים לינארית מעל K. יהי $\hat{M}$ סגוֹר גלואה של $M_0 M_1 \cdots M_n/K$. נניח בשלילה ש $\hat{M} \cap L_i$ מַקיף ממש את K לכל $i \ge n+1$. הואיל ויש ל $\hat{M}$ רק מספר סופי של תת שדות המקיפים את K, נותן עקרון שׁבך היונים $j > i \ge n+1$ כך ש $\hat{M} \cap L_i = \hat{M} \cap L_j$. אולם אז, $L_i \cap L_j$ מקיף ממש את K. מסתירה זו להנחת הלמה נובע שקיָם $i \ge n+1$ כך ש $\hat{M} \cap L_i = K$. נסמן אפוא $M_{n+1} = L_i$ ונקבל ש $M_0, M_1, \ldots, M_{n+1}$ מֻפרדים לינארית מאל K. בזה הֻשלמה ההשראה. ∎

משפטון 1.3: *תהי N הרחבת גלואה של שדה K. נניח שקיָם מספר טבעי m וקיָמות אינסוף הרחבות פרידות של K ב N ממעלה m. אזי קיֶמת ל K הרחבת גלואה סופית K', קיָם מספר טבעי d וקיֶמת סדרה אינסופית $L_1, L_2, L_3, \ldots$ של הרחבות גלואה של K' ב N ממעלה d שהיא מֻפרדת לינארית.* FSB 431 ,tupni

הוכחה: לפי ההנחה קיֶמת קבוצה אינסופית $\mathcal{M}$ של הרחבות של K בתוך N ממעלה m. יהי $M \in \mathcal{M}$ ויהי $\hat{M}$ סגוֹר גלואה של M/K. אזי $\hat{M} \subseteq N$ (כי N/K גלואה) ו $[\hat{M} : K] \le m!$. הואיל ולהרחבה $\hat{M}/K$ יש רק מספר סופי של תת הרחבות, קיָם מספר טבעי d (שאינו עולה על $m!$) וקיֶמת תת קבוצה אינסופית $\mathcal{L}$ של

$\{\hat{M} \mid M \in \mathcal{M}\}$ כך ש $[L:K]=d$ לכל $L \in \mathcal{L}$. בלי הגבלת הכלליות נניח ש d הנו המספר הטבעי הקטן ביותר בעל תכונה זו.

לכל $1 \le i \le d-1$ נסמן $\mathcal{L}_i = \{\{L,L'\} \in \mathcal{L}^{[2]} \mid [L \cap L' : K] = i\}$ הואיל ולכל $\{L,L'\} \in \mathcal{L}^{[2]}$ החִתוך $L \cap L'$ מוכל ממש ב L, מתקיֵם $\mathcal{L}^{[2]} = \dot{\bigcup}_{i=1}^{d-1} \mathcal{L}_i$. לפי משפט 1.1, קיָם $1 \le i \le d-1$ וקיֶמת תת קבוצה אינסופית $\mathcal{L}'$ של $\mathcal{L}$ כך ש $\mathcal{L}'^{[2]} \subseteq \mathcal{L}_i$. מהמזעריות של d נובע שהקבוצה $\{L \cap L' \mid \{L,L'\} \in (\mathcal{L}')^{[2]}\}$ סופית. לכן, לפי עקרון שׁבך היונים, יש ל K הרחבת גלואה סופית K' וקיֶמת תת קבוצה אינסופית $\mathcal{L}''$ של $\mathcal{L}'$ כך ש $L \cap L' = K'$ לכל $\{L,L'\} \in \mathcal{L}''^{[2]}$. למה 1.2, נותנת עתה תת קבוצה אינסופית $\mathcal{L}'''$ של $\mathcal{L}''$ שהיא מְפרדת לינארית מעל K', כנדרש. ∎

הרי הגרסה הסופית של משפט רמזִי:

dMAR 971 ,tupni

משפט 1.4 (משפט רמזי הסופי): *לכל שני מספרים טבעיים k,l וקבוצה סופית לא ריקה Q קיָם מספר טבעי n כך שלכל קבוצה X בת n אברים, ולכל העתקה $f\colon X^{[k]} \to Q$ קיָם $q \in Q$ וקיֶמת $A \subseteq X$ בת l אברים כך ש $f(A^{[k]}) = \{q\}$.*

הוכחה: יהיו k,l מספרים טבעיים ו Q קבוצה סופית. נניח בִּשלילה שלכל n טבעי קיֶמת קבוצה X_n בת n אברים וקיֶמת העתקה $f_n\colon X_n^{[k]} \to Q$ כך שלכל תת קבוצה A של X_n בת l אברים ולכל $q \in Q$ מתקיֵם $f(A^{[k]}) \ne \{q\}$. נבחר מסנן על לא ראשי $\mathcal{D}$ של $\mathbb{N}$ ונסמן $X = \prod_{n \in \mathbb{N}} X_n/\mathcal{D}$ ו $f = \prod_{n \in \mathbb{N}} f_n/\mathcal{D}$. אזי X היא קבוצה אינסופית ו f הנה העתקה מ $X^{[k]}$ ל Q. לפי משפט 1.1, קיָם $q \in Q$ וקיֶמת ל X תת קבוצה אינסופית Y כך ש $f(Y^{[k]}) = \{q\}$.

לפי המשפט היסודי של מכפלות העל קיָם מספר טבעי n, קיֶמת ל X_n תת קבוצה B בת לפחות l אברים וקיָם $q \in Q$ כך ש $f_n(B^{[k]}) = \{q\}$. נבחר ל B תת קבוצה A בת l אברים. אזי $A^{[k]} \subseteq B^{[k]}$. לכן, גם $f(A^{[k]}) = \{q\}$. סתירה זו להנחה בפסקה הקודמת מסיֶמת את הוכחת המשפט. ∎

2. **משפט** Hales-Jewett SELAH
5 ,tupni

המשפט העִקרי המופיע בסעיף זה הוכח על ידי Hales ו Jewett ב [HaJ63] בתור הכללה של משפט של van der Waerden והֻרחב מאז בכִוונים שונים. ההוכחה המובֵאת כאן הִנה עִבוד של ההוכחה המקורית.

חֲלֻקָּה של קבוצה X הנה אֹסף $\{X_q \mid q \in Q\}$ של תת קבוצות זרות של X שאִחודן שוה ל X. אנו נתיַחס גם להצגה $X = \dot\bigcup_{q\in Q} X_q$ כַּחֲלֻקָה של X. נעיר שחלק מהקבוצות X_q יכולות להיות ריקות*. בהתאם לכך מתאימה לחלֻקה הנ"ל העתקה $f\colon X \to Q$ כך ש $f^{-1}(q) = X_q$ לכל $q \in Q$. להפך, כל העתקה f כנ"ל מגדירה חלֻקה של X.

נעיר שאם הקבוצה X אינה ריקה ו $X = \dot\bigcup_{q\in Q} X_q$ היא חלֻקה, גם Q אינה ריקה.

נסמן ב $\mathcal{P}(X)$ את אֹסף תת הקבוצות של קבוצה X.

תהי X קבוצה, $\mathcal{S}$ אֹסף של קבוצות ו Q קבוצה סופית. נאמר ש $\mathcal{S}$ **סָדִיר־Q ב** X אם לכל חלֻקה $X = \dot\bigcup_{q\in Q} X_q$ קיָם $q \in Q$ וקיֶמת ל X_q תת קבוצה S השיֶכת ל $\mathcal{S}$. לחִלופין, $\mathcal{S}$ סדיר־Q ב X אם ורק אם לכל העְתקה $f\colon X \to Q$ קיָם $q \in Q$ וקיֶמת $S \in \mathcal{S}$ כך ש $S \subseteq f^{-1}(q)$.

נעיר שאם הקבוצה הריקה שיֶכת ל $\mathcal{S}$, אזי $\mathcal{S}$ סדיר־Q ב X לכל Q ו X.

למה 2.1: *אם אֹסף של קבוצות $\mathcal{S}$ סדיר־ Q בקבוצה X, אזי* GHC
74 ,tupni

(א) *$\mathcal{S}$ סדיר־ Q' ב X לכל קבוצה Q' בעֲלת אותו מספר האברים כמו Q.*

(ב) *$\mathcal{S}$ סדיר־ Q' ב X לכל תת קבוצה Q' של Q.*

(ג) *$\mathcal{S}$ סדיר־ Q ב X' לכל קבוצה X' המַקיפה את X.*

הוכחת ב: בלי הגבלת הכלליות נניח ש $\mathcal{S} \notin \emptyset$. תהי $X = \dot\bigcup_{q\in Q'} X_q$ חלֻקה. אזי גם $X = \dot\bigcup_{q\in Q'} X_q \,\dot\cup\, \dot\bigcup_{q\in Q\setminus Q'} \emptyset$ הִנה חלֻקה. לפי ההנחה, מקיפה אחת מהקבוצות של החלֻקה האחרונה קבוצה S השיֶכת ל $\mathcal{S}$. לפי ההנחה, $S \neq \emptyset$. לכן, קיָם $q \in Q'$ כך ש $S \subseteq X_q$, כנִדרש.

הוכחת ג: אם $X' = \dot\bigcup_{q\in Q} X'_q$ הִנה חלֻקה, אזי גם $X = \dot\bigcup_{q\in Q}(X \cap X'_q)$ הִנה חלֻקה. לפי ההנחה קיָם $S \in \mathcal{S}$ כך ש $S \subseteq X \cap X'_q$. לכן, קיָם $S \subseteq X'_q$, כנִדרש. ∎

אם $\mathcal{S}$ סדיר־Q ב X לכל קבוצה סופית Q אומרים ש $\mathcal{S}$ **סדיר ב** X.

---

* נעיר שברֹב הספרים דורשים שהקבוצות המשתתפות בחלֻקה תהיינה זרות. יוצא מן הכלל הוא הספר בתורת המִדה של הַלמוֹס. במקרה שלנו נֹח לשתֵף בחלֻקה גם קבוצות ריקות.

עבור שני אֳספים $\mathcal{S}$ ו $\mathcal{T}$ של קבוצות מסמנים

$$\mathcal{S} \otimes \mathcal{T} = \{S \times T \mid \ S \in \mathcal{S} \text{ and } T \in \mathcal{T}\}$$

למה 2.2: *תהיינה X ו Q קבוצות סופיות ו Y קבוצה כלשהיא. יהי $\mathcal{S}$ אֹסף סדיר־Q ב X. יהי $\mathcal{T}$ אֹסף סדיר־Q^X ב Y. אזי האֹסף $\mathcal{T} \otimes \mathcal{S}$ סדיר־Q ב $X \times Y$.* aLAH 68 ,tupni

הוכחה: בלי הגבלת הכלליות נניח שלא $\mathcal{S}$ ולא $\mathcal{T}$ מכילות את הקבוצה הריקה.

תהי $f\colon X \times Y \to Q$ העתקה. לכל $y \in Y$ נגדיר העתקה $f_y\colon X \to Q$ על ידי הנֻסחה $f_y(x) = f(x, y)$ לכל $x \in X$. נתבונן בהעתקה $g\colon Y \to Q^X$ המֻגדרת על ידי $g(y) = f_y$. הואיל ו $\mathcal{T}$ סדיר־Q^X ב Y, קיֶמת העתקה $\varphi\colon X \to Q$ וקיֶמת $T \in \mathcal{T}$ כך ש $T \subseteq g^{-1}(\varphi)$. לכן,

(א) לכל $y, y' \in T$ מתקיֵם $f_y = f_{y'}$,

במִלים אחרות,

(ב) לכל $y, y' \in T$ ו $x \in X$ מתקיֵם $f(x, y) = f(x, y')$.

יֶתר על כן, T אינה ריקה. נבחר אֵפוא $y \in T$ ונתבונן בהעתקה $f_y\colon X \to Q$. הואיל ו $\mathcal{S}$ סדיר־Q ב X, קיָמים $q \in Q$ ו $S \in \mathcal{S}$ כך ש $S \subseteq f_y^{-1}(q)$. במִלים אחרות, $f(x, y) = q$ לכל $x \in S$. מ (ב) נקבל אפוא עבור כל $y' \in T$ וכל $x \in S$ ש $f(x, y') = q$, כלומר $S \times T \subseteq f^{-1}(q)$. לכן, $\mathcal{T} \otimes \mathcal{S}$ סדיר־Q ב $X \times Y$. ∎

נזכיר ש**אֲגֻדָה** הנה קבוצה לא ריקה יחד עם פעֻלה (בדרך כלל כפל) צֵרופית. לדֻגמה, קבוצת המספרים הטבעיים הנה אגֻדה חִבורית.

אם Σ הִנה אגֻדה ו A, B הן תת קבוצות של Σ, נִרשֹם $AB = \{ab \mid \ a \in A, \ b \in B\}$.

תהי A קבוצה סופית לא ריקה של אותיות. נסמן ב Σ את האגֻדה החָפשית הנוצרת על ידי A. כל אבר של Σ הנו מִלה ב A, לדֻגמה $a_1 a_2 \cdots a_m$, שאותיותיה $a_1, a_2, \ldots, a_m$ נקבעות באֹפן חד ערכי. נזהֶה אותה אפוא עם הסִדרה $\mathbf{a} = (a_1, a_2, \cdots, a_m)$. המספר m נקרא **האֹרך** של המִלה $\mathbf{a}$. בהתאם לכך נִתן להציג את Σ כאִחוד זר:

$$\Sigma = \dot{\bigcup_{n=1}^{\infty}} A^n$$

אם $\mathbf{b} = b_1 b_2 \cdots b_n$ הנה מִלה נוספת אזי **המכפלה** $\mathbf{ab}$ של האותיות מֻגדרת כַּמִלה $a_1 \cdots a_m b_1 \cdots b_n$.

תהי עתה x אות שאינה שַׁיֶּכֶת ל A. נסמן ב Σ_x את האֲגֻדָּה החָפְשִׁית הנוצרת על ידי $A \cup \{x\}$. כל מִלָּה w ב Σ_x נִתָּן לראות גם כהַעְתָּקָה $w\colon A \to \Sigma$. הערך $w(a)$ של w באֵבר a של A הנה המִלָּה המתקבלת מ w על ידי החלפת כל המופעים של x ב w ב a. לדֻגמה, אם $\Sigma = \{1, 2, 3, 4, 5\}$ ו

$$w = 103x545xx43$$

אזי

$$w(1) = 10315451143$$

$$w(2) = 10325452243$$

$$w(3) = 10335453343$$

נשים לב לכך שכל אחת מהעַמודות של המטריצה מסֵדר 3×11 המופיעה באגף ימין הנה קבועה או שהיא

$$\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$$

עמודה כזו מתקבלת בדיוק מתחת למופעים של x במִלה w.

בעִקבות הסימון Σ_x נסמן גם $A_x^n = (A \cup \{x\})^n$ ונקבל ש $\Sigma_x = \dot{\bigcup}_{n=1}^{\infty} A_x^n$. אם $w \in A_x^n$, אזי $w(a) \in A^n$ לכל $a \in A$.

למה 2.3: *תהי A קבוצה סופית לא ריקה ויהי x אבר שאינו שַׁיָּךְ ל A. נניח שלכל קבוצה סופית K קַיָּם מספר טבעי p כך שהאסף $\{w(A) \mid w \in A_x^p \setminus A^p\}$ סדיר־K ב A^p. אזי, לכל מספר טבעי n ולכל קבוצה סופית Q קַיָּם מספר טבעי r כך שהאסף $\mathcal{W} = \{w_1(A) \cdots w_n(A) \mid w_1, \ldots, w_n \in A_x^r \setminus A^r\}$ סדיר־Q ב A^{nr}.* cLAH 002 ,tupni

הוכחה: המקרה $n = 1$ נובע מהנחת הלמה. ואכן, בהנתן קבוצה סופית Q קַיָּם מספר טבעי m כך שהאסף $\mathcal{S} = \{w(A) \mid w \in A_x^m \setminus A^m\}$ סדיר־Q ב A^m.

נניח אפוא ש $n \geq 2$ ונניח בהשראה שקַיָּם מספר טבעי s כך שהאסף

$$\mathcal{T} = \{w_1(A) \cdots w_{n-1}(A) \mid w_1, \ldots, w_{n-1} \in A_x^s \setminus A^s\}$$

סדיר־Q^{A^m} ב $A^{(n-1)s}$.

לפי למה 2.2, האסף $\mathcal{S} \otimes \mathcal{T}$ סדיר־Q ב $A^m \times A^{(n-1)s}$.

יהי $r=\max(m,s)$. נבחר $a\in A$ ונגדיר העתקה $\mu\colon A^m\times A^{(n-1)s}\to A^{nr}$ באֹפן הבא:

$$\begin{aligned}&\mu(a_1,\ldots,a_m,b_{11},\ldots,b_{1s},\ldots,b_{n-1,1},\ldots,b_{n-1,s})\\ &=(a_1,\ldots,a_m,\overbrace{a,\ldots,a}^{r-m\text{ times}},b_{11},\ldots,b_{1s},\overbrace{a,\ldots,a}^{r-s\text{ times}},\ldots,b_{n-1,1},\ldots,b_{n-1,s},\overbrace{a,\ldots,a}^{r-s\text{ times}})\end{aligned}$$

עתה נתבונן בַּחלֻקה $A^{nr}=\biguplus_{q\in Q}A_{nr,q}$. אזי גם $A^m\times A^{(n-1)s}=\biguplus_{q\in Q}\mu^{-1}(A_{nr,q})$ היא חלֻקה. לפי הפִסקה הקודמת, קיָמים $q\in Q$, $S\in\mathcal{S}$ ו $T\in\mathcal{T}$ כך ש $S\times T\subseteq\mu^{-1}(A_{nr,q})$ ולכן $\mu(S\times T)\subseteq A_{nr,q}$. כדי לסיֵם את הוכחת הלמה מספיק אפוא להוכיח שהאֹסף $\mathcal{W}$ המֻגדר בלמה מקיֵם את הטענה הבאה:

טענה: $\mu(S\times T)\in\mathcal{W}$. ואכן, בסימונים דלעיל, קיֶמת מלה $w_0\in A_x^m\smallsetminus A^m$ כך ש $S=w_0(A)$ וקיָמות מִלים $w_1,\ldots,w_{n-1}\in A_x^s\smallsetminus A^s$ כך ש $T=w_1(A)\cdots w_{n-1}(A)$. נסמן ב w_0' את המִלה w_0 ולאחריה $r-m$ פעמים האות a. לכל $1\le i\le n-1$ נסמן ב w_i' את המִלה w_i ולאחריה $r-s$ פעמים האות a. אזי $w_0'\in A_x^r\smallsetminus A^r$, $w_i'\in A_x^r\smallsetminus A^r$ ו $\mu(S\times T)=w_0'(A)w_1'(A)\cdots w_{n-1}'(A)\subseteq\mathcal{W}$, כנטען. ∎

LJH
672 ,tupni

משפט 2.4: *לכל שתי קבוצות סופיות לא ריקות A ו Q ואבר x שאינו שיָך ל A קיָם מספר טבעי p כך ש*

(א) *הקבוצה* $\{w(A)\mid w\in A_x^p\smallsetminus A^p\}$ סדירת־Q ב A^p.

במִלים אחרות,

(א') *לכל חלֻקה* $A^p=\biguplus_{q\in Q}A_{p,q}$ *קיָם* $q\in Q$ *וקיָם* $w\in A_x^p\smallsetminus A^p$ כך ש $w(A)\subseteq A_{p,q}$.

הוכחה: תהיינה A ו Q קבוצות סופיות לא ריקות וִיהי x אבר שאינו שיָך ל A. נבחר $a_0\in A$ ונסמן $A'=A\smallsetminus\{a_0\}$. אם A או Q מכילות רק אבר אחד, התנאי (א') מתקיֵם עבור $p=1$. נניח אפוא שגם ב A וגם ב Q יש לפחות שני אֲברים.

הנחת השראה: *התנאים (א) ו (א') נכונים עבור A' ו Q וכן עבור A ועבור כל תת קבוצה חלקית של Q בעלת $|Q|-1$ אברים.* לפי למה 2.1, קיָם מספר טבעי r כך ש

(1) לכל תת קבוצה נאותה K של Q, האֹסף $\{w(A)\mid w\in A_x^r\smallsetminus A^r\}$ סדיר־K ב A^r.

נסמן ב Σ' את תת האֲגֻדה החפשית של Σ הנוצרת על ידי A'. הנחת ההשראה נותנת לכל קבוצה סופית K מספר טבעי r'' כך שהאֹסף $\{w(A')\mid w\in(A')_x^{r''}\smallsetminus(A')^{r''}\}$ סדיר־K בתת הקבוצה הסופית $(A')^{r''}$ של Σ'. לכן, לפי למה 2.3, קיָם מספר טבעי r' כך שעבור $\mathcal{S}=\{w(A')\mid w\in(A')^{r'}\smallsetminus(A')^{r'}\}$

(2) האֹסף $\mathcal{S}_{r+1}=\{w_0(A')w_1(A')\cdots w_r(A')\mid w_0,w_1,\ldots,w_r\in(A')_x^{r'}\smallsetminus(A')^{r'}\}$ סדיר־Q ב $(A')^{r'(r+1)}$.

האֹרך של כל אחד מה w_i־ים ב (2) הנו r'. לכן

(3) האֹרך של כל אחת מהמִלים $w_0w_1\cdots w_r$ המופיעים ב (2) הנו $p = r'(r+1)$. בפרט, $S \subseteq (A')^p$ לכל $S \in \mathcal{S}_{r+1}$.

חלֻקה של A^p: נתבונן עתה בַּחֲלֻקה $A^p = \dot\bigcup_{q\in Q} A_{p,q}$. חלֻקה זו מגדירה חלֻקה

$$(A')^p = \dot\bigcup_{q\in Q}((A')^p \cap A_{p,q}).$$

לפי (2), קיָמים $q_0 \in Q$ ו $w_0, w_1, \ldots, w_r \in (A'_x)^{r'} \smallsetminus (A')^{r'}$ כך ש

(4) $w_0(A')w_1(A')\cdots w_r(A') \subseteq (A')^p \cap A_{p,q_0}$.

נסמן $Q' = Q \smallsetminus \{q_0\}$.

מ (3) נובע ש $w_0(A)w_1(A)\cdots w_r(A) \subseteq A^p$. בכך אנו מקבלים העתקה

$$\varphi\colon A^r \to w_0(a_0)w_1(A)\cdots w_r(A)$$

המֻגדרת על ידי

$$\varphi(a_1\cdots a_r) = w_0(a_0)w_1(a_1)\cdots w_r(a_r).$$

לכל מִלה $w \in \Sigma_x \smallsetminus \Sigma$ המקיֶמת $w(A) \subseteq A^r$ ולכל $a \in A$ קיָמים $a_1, \ldots, a_r \in A$ יחידים כך ש $w(a) = a_1\cdots a_r$. לפי ההגדרה, $\varphi(w(a)) = w_0(a_0)w_1(a_1)\cdots w_r(a_r)$. נסמן

$$\mathcal{W} = \{w(A) \subseteq A^r \mid w \in \Sigma_x \smallsetminus \Sigma\}, \qquad \mathcal{W}' = \{\varphi(w(A)) \mid w \in \Sigma_x \smallsetminus \Sigma,\ w(A) \subseteq A^r\}.$$

טענה א: *האֹסף $\mathcal{W}'$ סדיר־Q' ב $w_0(a_0)w_1(A)\cdots w_r(A)$.* ואכן, אם

$$w_0(a_0)w_1(A)\cdots w_r(A) = \dot\bigcup_{q\in Q'} W_q,$$

היא חלֻקה, אזי גם $A^r = \sum_{q\in Q'}\varphi^{-1}(W_q)$ היא חלֻקה. לפי (1), קיָמים $q \in Q'$ ו $W \in \mathcal{W}$ כך ש $W \subseteq \varphi^{-1}(W_q)$. לכן, $\varphi(W) \subseteq W_q$, כנדרש.

טענה ב: $\mathcal{W}' \subseteq \{w'(A) \subseteq A^p \mid w' \in \Sigma_x \smallsetminus \Sigma\}$. תהי אפוא $w \in \Sigma_x \smallsetminus \Sigma$ מִלה לא קבועה כך ש $w(A) \subseteq A^r$. אזי הארֹך של w הנו r. קַיָמים אפוא $u_1, \ldots, u_r \in A_x$ כך ש $w = u_1 \cdots u_r$ ו $u_i = x$ לפחות עבור i אחד בין 1 ל r. נסמן $u_0 = a_0$ וִיהי $w' = (w_0 \circ u_0)(w_1 \circ u_1) \cdots (w_r \circ u_r)$. נוכיח ש $w'(A) = \varphi(w(A))$.

ואכן, יהי $a \in A$, יהי $w(a) = a_1 \cdots a_r$ ויהי $0 \leq i \leq r$. אם $u_i \in A$, אזי $u_i(a) = u_i = a_i$ ולכן,

$$w_i(u_i(a)) = w_i(a_i). \quad (5)$$

אם $u_i = x$, אזי $u_i(a) = a = a_i$ ולכן (5) נכון גם במקרה זה. מכאן ש

$$w'(a) = w_0(u_0(a))w_1(u_1(a)) \cdots w_r(u_r(a)) = w_0(a_0)w_1(a_1) \cdots w_r(a_r) = \varphi(w(a))$$

כנדרש.

נבדיל עתה בין שני מקרים:

מקרה א: $w_0(a_0)w_1(A) \cdots w_r(A) \subseteq \bigcup_{q \in Q'} A_{p,q}$. אזי, לפי טענה א, קים $q \in Q'$ וקַיָם $W \in \mathcal{W}'$ כך ש $W \subseteq A_{p,q}$. לפי טענה ב, קיָם $w' \in \Sigma_x \smallsetminus \Sigma$ כך ש $w'(A) \subseteq A_{p,q}$, כנדרש ב (א').

מקרה ב: *מקרה א אינו מתקיֵם, כלומר קיָמים* $a_1, \ldots, a_r \in A$ כך $b = w_0(a_0)w_1(a_1) \cdots w_r(a_r) \in A_{p,q_0}$. נזכֹר עתה ש $w_0, w_1, \ldots, w_r \in (A'_x)^{r'} \smallsetminus (A')^{r'}$. לכל $0 \leq i \leq r$ נגדיר

$$w'_i = \begin{cases} w_i(a_i) & \text{אם } a_i \in A' \\ w_i & \text{אם } a_i = a_0 \end{cases}$$

ונסמן $w' = w'_0 w'_1 \cdots w'_r$. הואיל ו $w_0 \in (A'_x)^{r'} \smallsetminus (A')^{r'}$, מתקיֵם $w' \in (A'_x)^p \smallsetminus (A')^p$. כמו כן, $w'_i(a_0) = w_i(a_i)$ לכל $0 \leq i \leq r$ ולכן

$$w'(a_0) = w'_0(a_0)w'_1(a_0) \cdots w'_r(a_0) = w_0(a_0)w_1(a_1) \cdots w_r(a_r) \in A_{p,q_0}. \quad (6)$$

עתה נתבונן ב $a' \in A'$. אם $a_i \in A'$, אזי $w'_i(a') = w_i(a_i)$. אם $a_i = a_0$, אזי $w'_i(a') = w_i(a')$. בכל אחד משני המקרים $w'_i(a') \in w_i(A')$. לכן, לפי (4),

$$w'(a') \in w_0(A')w_1(A') \cdots w_r(A') \subseteq A_{p,q_0}. \quad (7)$$

מ (6) ו (7) נובע ש $w'(A) \subseteq A_{p,q_0}$, כנדרש ב (א'). ∎

dLAH 564 ,tupni

משפט 2.5 (Hales-Jewett): *תהיינה A ו Q קבוצות סופית ו x אבר שאינו שיָך ל A. נסמן ב Σ (בהתאמה ב Σ_x) את האגֻדה החָפשית הנוצרת על ידי A (בהתאמה $A \cup \{x\}$). אזי לכל חלֻקה $\Sigma = \bigcup_{q \in Q} \Sigma_q$ קיָמים $q \in Q$ ו $w \in \Sigma_x \setminus \Sigma$ כך ש $w(A) \subseteq \Sigma_q$.*

הוכחה: לכל p טבעי, נתבונן בחלֻקה $A^p = \bigcup_{q \in Q} (A^p \cap \Sigma_q)$. לפי משפט 2.4, קיָם p טבעי, קיָם $q \in Q$ וקיָם $w \in A^p_x \setminus A^p$ כך ש $w(A) \subseteq A^p \cap \Sigma_q$. לכן, $w \in \Sigma_x \setminus \Sigma$ ו $w(A) \subseteq \Sigma_q$, כנדרש. ∎

אפשר לראות את Q גם כִּקבוצת צבעים ואת החלֻקה גם כִּצְביעה של Q. במונחים האלו אפשר לנסח את משפט 2.5 גם באֹפן הבא:

משפט 2.5' (Hales-Jewett): *לכל צביעה של האגֻדה החפשית הנוצרת על ידי קבוצה סופית A במספר סופי של צבעים קיֶמת מִלה לא קבועה w באברי A כך שהקבוצה $\{w(a) \mid a \in A\}$* ***חד־גונית*** *(כלומר בעלת צבע אחד).*

fLAH 894 ,tupni

משפט 2.6 (van der Waerden): *לכל צביעה של $\mathbb{N}$ במספר סופי של צבעים ולכל m טבעי קיֶמת סִדרה חשבונית חד־גונית מאֹרך m.*

הוכחה: תהי Q קבוצה סופית ונתבונן בַּחֲלֻקה $\mathbb{N} = \bigcup_{q \in Q} N_q$. נסמן $A = \{1, \ldots, m\}$ ונתבונן באגֻדה החפשית Σ הנוצרת על ידי A. נגדיר העתקה $\varphi\colon \Sigma \to \mathbb{N}$ על ידי $\varphi(a_1 a_2 \cdots a_k) = a_1 + a_2 + \cdots + a_k$. אזי $\Sigma = \bigcup_{q \in Q} \varphi^{-1}(N_q)$ היא חלֻקה של Σ. יהי x אבר שאינו שיָך ל A. משפט 2.5 נותן $q \in Q$ ו $w \in \Sigma_x \setminus \Sigma$ כך ש $w(A) \subseteq \varphi^{-1}(N_q)$ ולכן $\varphi(w(A)) \subseteq N_q$.

נִרשֹם $w = w_1 w_2 \cdots w_k$ באשר $w_i \in A \cup \{x\}$ ולפחות אחד ה w_i־ים הִנו x. נסמן ב d את מספר הפעמים ש x מופיע בין ה w_i־ים ונסמן ב b את הסכום של ה w_i־ים השיָכים ל A. אזי לכל $j \in A$ מתקיֵם $w(j) = w_1(j) w_2(j) \cdots w_k(j)$ ו

$$\varphi(w(j)) = \sum_{i=1}^{k} w_i(j) = \sum_{w_i \neq x} w_i + \sum_{w_i = x} j = b + jd.$$

מהפסקה הקודמת נובע אפוא שהסדרה החשבונית $b+d, b+2d, \ldots, b+md$ שיֶכת כֻלה ל N_q. ∎

נזכֹר ש**תת מרחב אפיני** של מרחב וקטורי V הנו תת קבוצה מהצורה $v_0 + W$, באשר v_0 הנו אֵבר ו W הנו תת מרחב של V.

RLG 345 ,tupni

משפט 2.7 (Graham-Leeb-Rothchild): *לכל מרחב וקטורי V בעל ממד אינסופי מעל שדה סופי F ולכל צביעה של V על ידי מספר סופי של צבעים יש תת מרחב אפיני חד־גוני מממד גדול כרצוננו.*

הוכחה: נתבונן בחלֻקה סופית $V=\dot\bigcup_{q\in Q} V_q$. עתה יהי n מספר טבעי ונבחר קבוצה

$$\{v_{ij} \mid i=1,\dots,n;\ j=1,2,3,\dots\}$$

של אברים של V שאינם תלויים לינארית מעל F. נסמן ב Σ את האגֻדה החפשית הנוצרת על ידי F^n. כל אֵבר $\mathbf{a}\in\Sigma$ הנו מִלה $\mathbf{a}=\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_k$ באשר $\mathbf{a}_j=(a_{1j},\dots,a_{nj})\in F^n$ עבור $j=1,\dots,k$. נגדיר העתקה $\varphi\colon\Sigma\to V$ על ידי

$$.\varphi(\mathbf{a})=\sum_{i=1}^{n}\sum_{j=1}^{k}a_{ij}v_{ij}$$

העתקה זו מגדירה חלֻקה $\Sigma=\dot\bigcup_{q\in Q}\varphi^{-1}(V_q)$. יהי x אבר שאינו שיָך ל F^n. משפט 2.5 נותן $q\in Q$ ומִלה $w\in\Sigma_x\setminus\Sigma$ כך ש $w(F^n)\subseteq\varphi^{-1}(V_q)$ ולכן

$$.\varphi(w(F^n))\subseteq V_q \tag{8}$$

נראה אבר $\mathbf{b}\in F^n$ כעֲמודה בעלת גֹבה n שהפבר ה i־י שלה הוא אבר b_i של F. נרשֹם $w=w_1w_2\cdots w_k$, באשר $w_j=\mathbf{a}_j\in F^n$ או $w_j=x$ ולפחות אחד מה w_j־ים הנו x. אזי $w(\mathbf{b})$ אינו אלא המטריצה המתקבלת מהמטריצה $(a_{ij})_{1\le i\le n,\ 1\le j\le k}$ על ידי החלפת כל עֲמודה j־ית שעבורה $w_j=x$ בעמודה $\mathbf{b}$. לכן,

$$.\varphi(w(\mathbf{b}))=\sum_{i=1}^{n}\sum_{\substack{j=1\\ w_j\ne x}}^{k}a_{ij}v_{ij}+\sum_{i=1}^{n}\sum_{\substack{j=1\\ w_j=x}}^{k}b_iv_{ij} \tag{9}$$

נסמן

$$v_0=\sum_{i=1}^{n}\sum_{\substack{j=1\\ w_j\ne x}}^{k}a_{ij}v_{ij}$$

ולכל $1\le i\le n$ נסמן

$$.v_i=\sum_{\substack{j=1\\ w_j=x}}^{k}v_{ij}$$

מבחירת ה v_{ij}־ים ומכך שקיָם $1\le j\le k$ כך ש $w_j=x$ נובע ש $v_1,\dots,v_n$ אינם תלויים לינארית. לפי (9),

$$.\varphi(w(\mathbf{b}))=v_0+\sum_{i=1}^{n}b_iv_i$$

מ (8) נובע אפוא שתת המרחב האפיני $W=v_0+\sum_{i=1}^{n}Fv_i$ שממדו n מוכל כֻּלו ב V_q, כפי שהיה להוכיח.

∎

3. משפט Im-Larsen NESRAL 4 ,tupni

התוצאה הבאה מופיעה במאמרם [ImL12] של Bo-Hae Im ו Michael Larsen ומשמשת שם בסיס עִקרי להוכחה של משפט בארתמטיקת השדות.

למה 3.1 (Im-Larsen): *לכל שתי קבוצות סופיות I ו Q קיָם מספר טבעי n כך שלכל חלֻקה $I^n = \dot{\bigcup}_{q\in Q} I_{n,q}$ קיָמות העְתקות $g_1,\dots,g_n\colon I\to I$ המקיָמות:* eLAH 21 ,tupni

(א) *לכל $1\le j\le n$ ההעתקה g_j קבועה או שהיא העתקת הזהות.*

(ב) *לפחות אחת מההעתקות g_j הנה העתקת הזהות.*

(ג) *קיָם $q\in Q$ כך ש $\{(g_1(i),g_2(i),\dots,g_n(i)) \mid i\in I\}\subseteq I_{n,q}$.*

הוכחה: יהי x אבר שאינו שיָך ל I. לפי משפט 2.4, קיָם מספר טבעי n כך שהקבוצה $\{w(I)\mid w\in I_x^n\setminus I^n\}$ סדירת־Q ב I^n. תהי אפוא $I^n=\dot{\bigcup}_{q\in Q} I_{n,q}$ חלֻקה. אזי קיָם $q\in Q$ וקיֶמת מִלה לא קבועה $w\in I_x^n\setminus I^n$ כך ש $w(I)\subseteq I_{n,q}$. נרשֹם $w=g_1g_2\dots g_n$, באשר $g_1,\dots,g_n\in I\cup\{x\}$. אזי כל g_j היא העתקה מ I ל I. הואיל ו x מופיע ב w מתקימות הטענות (א) ו (ב). כמו כן, התנאי $w(I)\subseteq I_{n,q}$ שקול ל (ג). ∎

למה 3.2 (Im-Larsen): *יהי K שדה אינסופי בעל אִפיון שונה מ 2 בעל מספר סופי של הרחבות רִבועיות ויהי H הֶעקֹם ההיפר־אלִפטי המֻגדר על ידי המשואה* bRAL 34 ,tupni

$$Y^2=(X-a_1)(X-a_2)\cdots(X-a_{2g+2})$$

באשר g הנו מספר טבעי ו $a_1,a_2,\dots,a_{2g+2}$ הִנם אברים שונים זה מזה של K. אזי קיֶמת ל K תת קבוצה סופית C וקיֶמת ל $K[X]$ תת קבוצה סופית Λ של פולינומים ממעלה 1 כך שלכל $k\in K\setminus C$ קיָמים $\lambda\in\Lambda$ ונקֻדה $(\lambda(k),y)\in H(K)$.

הוכחה: לפי תורת קוּמֶר, $Q=K^\times/(K^\times)^2$ הנה קבוצה סופית. נסמן $I=\{1,2,\dots,2g+2\}$. יהי n המספר הטבעי המקיֵם את למה 3.1 ביחס ל I ו Q ונסמן $N=\{1,2,\dots,n\}$. ננצל את האינסופיות של K כדי לבחֹר $b_1,b_2,\dots,b_n$ כך שהסכום של שום תת קבוצה לא ריקה של $\{b_1,b_2,\dots,b_n\}$ אינו אפס. נתבונן בתת הקבוצה הסופית

$$C=\{b_1a_{i_1}+b_2a_{i_2}+\cdots+b_na_{i_n}\mid i_1,\dots,i_n\in I\}$$

של K. אם $k\in K\setminus C$, אזי $k\ne b_1a_{i_1}+\cdots+b_na_{i_n}$ לכל $i_1,\dots,i_n\in I$. לכן נוכל לכל $q\in Q$ לסמן

$$I_{k,q}=\{(i_1,i_2,\dots,i_n)\in I^n\mid (k-b_1a_{i_1}-\cdots-b_na_{i_n})(K^\times)^2=q\}$$

ולקבל חלֻקה $I^n = \dot\bigcup_{q\in Q} I_{k,q}$. בחירת n נותנת העתקות $g_{k,1},\dots,g_{k,n}\colon I\to I$ המקַיְמות:

(וא) לכל $1\le j\le n$ ההעתקה $g_{k,j}$ קבועה או שהיא העתקת הזֶהות.

(וב) לפחות אחת מההעתקות $g_{k,j}$ הנה העתקת הזהות.

(וג) קיָם $q\in Q$ כך ש $\{(g_{k,1}(i),\dots,g_{k,n}(i)) \mid i\in I\}\subseteq I_{k,q}$.

עתה נסמן לכל $k\in K\smallsetminus C$

$$N_k=\{j\in N\mid g_{k,j}(i)=i \text{ for all } i\in I\},\quad N'_k=\{j\in N\mid g_{k,j}(i)=g_{k,j}(1) \text{ for all } i\in I\}.$$

לפי (וב), $N_k\neq\emptyset$ ו $N=N_k\,\dot\cup\, N'_k$. עוד נסמן

$$r_k=\sum_{j\in N_k} b_j,\qquad r'_k=\sum_{j\in N'_k} b_j a_{g_{k,j}(1)}.$$

מבחירת $b_1,\dots,b_n$ נובע ש $r_k\neq 0$. כמו כן, לכל $i\in I$,

$$k-b_1a_{g_{k,1}(i)}-\cdots-b_na_{g_{k,n}(i)}=k-\sum_{j\in N'_k} b_ja_{g_{k,j}(1)}-\sum_{j\in N_k} b_ja_i=k-r'_k-r_ka_i. \tag{2}$$

לכל $i\in I$ מתקיֵם, לפי (וג), $(g_{k,1}(i),\dots,g_{k,n}(i))\in I_{k,q}$. לכן, לפי (2) ולפי הגדרת $I_{k,q}$,

$$(k-r'_k-r_ka_i)(K^\times)^2=(k-b_1a_{g_{k,1}(i)}-\cdots-b_na_{g_{k,n}(i)})(K^\times)^2=q.$$

יהי $a\in K^\times$ ויהי $q=a(K^\times)^2$. אזי

$$\prod_{i=1}^{2g+2}\Big(\frac{k-r'_k}{r_k}-a_i\Big)=(r_k)^{-2g-2}\prod_{i=1}^{2g+2}(k-r'_k-r_ka_i)\in(r_k)^{-2g-2}a^{2g+2}(K^\times)^2\subseteq(K^\times)^2.$$

אם נסמן $x=\frac{k-r'_k}{r_k}$ נקבל אפוא $y\in K^\times$ כך ש $\prod_{i=1}^{2g+2}(x-a_i)=y^2$, כלומר $(x,y)\in H(K)$.

לבסוף נסמן

$$\Lambda=\Big\{\frac{X-\sum_{j\in N\smallsetminus M} b_ja_{g_{k,j}(1)}}{\sum_{j\in M} b_j}\ \Big|\ \emptyset\subset M\subseteq N\Big\}.$$

אזי Λ הִנה קבוצה סופית של פולינומים לינאריים ב $K[X]$ ולכל $k\in K$ קיָמים $\lambda\in\Lambda$ ו $y\in K$ כך ש $(\lambda(k),y)\in H(K)$, כפי שהיה להוכיח. ∎

References

[BSF12] L. Bary-Soroker and A. Fehm, *Random Galois extensions of Hilbertian fields*, manuscript, Tel Aviv, 2012.

[HaJ63] A. W. Hales and R. L. Jewett, *Regularity and positional games*, Transactions of the American Mathematical Society **106** (1963), 222-229.

[ImL12] B.-H. Im and M. Larsen, *Some applications of the Hales-Jewett theorem to field arithmetic*, Israel Journal of Mathematics

[Tsa11] B. Tsaban, *Ramsey Theory (Hebrew)*, http://u.cs.biu.ac.il/~tsaban/RT/RT12.html