עֲקֳמִים אֵלִפְטִיִים

מאת

משה ירדן

תל אביב, תשס"ה

הקדמה

לאחר משפט אי הפריקות של הלברט (Hilbert) משנת 1892 אפשר לראות את משפט מורדל־וייל כנקֻדת היסוד של הגאומטריה הארתמטית.

משפט מורדל־וייל: *יהי K שדה הנוצר סופית מעל השדה הראשוני שלו ותהי A יריעה אבלית מעל K. אזי $A(K)$ היא חבורה אבלית נוצרת סופית.*

המשפט הוכח לראשונה על ידי מורדל (Mordell) ב 1922 עבור $K = \mathbb{Q}$ ובמקרה ש A הנו עקם אלפטי. וייל (Weil) הכליל את המשפט לשדות מספרים וליריעות אבליות. את המקרה הכללי ביותר הוכיחו לבסוף לנג (Lang) ונרון (Néron) ב 1959.

עקרון הוכחת המשפט כללי ביותר. בהנתן חבורה אבלית B מוצאים מספר טבעי $m \geq 2$ ומוכיחים תחילה ש B/mB הנה חבורה סופית (משפט מורדל־וייל החלש). אחר כך בונים פונקצית גבה $h\colon B \to \mathbb{R}$ המקימת שלשה תנאים שבהם מופע המצד (=פרמטר) m. מכאן מסיקים ש B חבורה סופית. להסקה זו קראתי "משפט מורדל־וייל המֻפשט.

כדי לישם את משפט מורדל־וייל המפשט הגדרתי מהו "שדה ארתמטי". זהו שדה K יחד עם קבוצה של הערכות בדידות לכל הרחבה סופית L של K המקימת את תנאי הסופיות הרגילים של שדות גלובליים, כלומר מספר מחלקות האידאלים הנו סופי וחבורת אחדות־S (באשר S תת קבוצה סופית של הערכות) נוצרת סופית (משפט האחדות של דיריכלה (Dirichlet)). אחר כך אני מתבונן ב"פנקטור אבלי" A. זהו פנקטור מקטגורית ההרחבות האלגבריות של K לקטגורית החבורות האבליות המקים את כל התכונות שיש ליריעה אבלית מעל K. בפרט פועלת חבורת גלואה המֻחלטת על A וקים מספר טבעי $m \geq 2$ כך ש $A_m(\tilde{K})$ סופי ($\tilde{K}$ הנו הסגור האלגברי של K), וכפל ב m מעתיק את $A(\tilde{K})$ על עצמו. כמו כן צריך להניח שמחוץ לקבוצה סופית של הערכות "רעות" יש ל A העמדה (טובה ביחס ל m. בפרט נדרש שהנקדות מסדר המחלק את m עוברות באפן חד חד ערכי בהעמדה זו. מהנחות אלו נובע משפט מורדל־וייל החלש.

את פונקצית הגבה מגדיר אני רק עבור $K = \mathbb{Q}$ במקרה שבו A הנו עקם אלפטי E הנתן על ידי משואת ויירשטרש (Weierstrass) $Y^2 = X^3 + aX + b$. ללא הוכחה מציֵן אני שמשפט רימן־רוך (Riemann-Roch) מאפשר להגדיר פעֻלת חבור על $E(\tilde{\mathbb{Q}})$ ההופך קבוצה זו לחבורה אבלית באפן שסכום שלש נקדות הנו אפס אם ורק אם הן מונחות על ישר אחד. מכאן אפשר לחשב את נסחאות החבור באפן מפרש. בפרט אפשר לקבע ש $E_2(\tilde{K})$ הנו חבורה מפרשת של ארבעה אברים. בעזר ההצגה המפרשת של כפל ב 2 והנקדות מסדר 2 אפשר לאשר את כל התכונות הנדרשות עבור $m = 2$ ולסים את הוכחת משפט מורדל־וייל למקרה זה (זהו למעשה משפט מורדל המקורי).

כדי לסים את כל הפרטים של ההוכחה יש עדין לבסס את יסודות תורת המספרים האלגבריים עד למשפט סופיות מספר מחלקות האידאלים ומשפט האחדות של דיריכלה. בנוסף לכך יש לבסס את תורת הפונקציות האלגבריות

של משתנה אחד ובעקר משפט רימן־רוך ולהגדיר בעזרתם את מבנה החבורה האבלית של עקם אלפטי. קצר הזמן והמקום לא אפשר לעשות דברים אלו בקורס וברשימות הנוכחיות. הקורא המעֻנין נקרא להשלים אותם באפן עצמאי.

משה ירדן

תל אביב, תשסא

א. משפט Mordell-Weil המופשט

בסעיף זה נתבונן בשדה K ו**בפנקטור אבלי** A מעל K. פנקטור זה מתאים לכל שדה הרחבה L של K חבורה אבלית $A(L)$. לשכון של שדות $L \to L'$ מתאים הפנקטור שכון $A(L) \to A(L')$ של חבורות אבליות ומתקים $A(L_1) \cap A(L_2) = A(L_1 \cap L_2)$. אברי $A(L)$ יקראו **נקודות רציונליות־**L של A. ל A נצרף כמה פנקטורים נוספים. ראשית, לכל n טבעי, יהי $A_n(L) = \{\mathbf{a} \in A(L) \mid n\mathbf{a} = 0\}$ תת החבורה של $A(L)$ המורכבת מכל הנקודות המתאפסות על ידי n. **חבורת הפתול** תהיה

$$A_{\mathrm{tor}}(L) = \bigcup_{n=1}^{\infty} A_n(L).$$

לבסוף, נתבונן גם ב**דרגה** $\mathrm{rank}(A(L))$ של $A(L)$. זוהי העצמה של תת קבוצה מרבית של $A(L)$ שאינה תלויה לינארית מעל $\mathbb{Z}$.

ברצוננו לנסח תנאים על K ועל A שיגררו אחריהם שהחבורה $A(L)$ נוצרת סופית לכל הרחבה סופית L של K. גרירה זו תקרא **משפט Mordell-Weil** עבור A. נכונותו תגרר אחריה את התוצאות הבאות:

(1a) $A_{\mathrm{tor}}(L)$ הוא חבורה סופית.

(1b) $\mathrm{rank}(A(L)) < \infty$.

(1c) לכל m טבעי, חבורת המנה $A(L)/mA(L)$ סופית.

ואכן, מהמשפט היסודי של החבורות החלופיות הנוצרות סופית נובע ש $A(L) = A_{\mathrm{tor}}(L) \oplus \mathbb{Z}^r$ באשר $r = \mathrm{rank}(A(L))$ הוא מספר שלם אי שלילי ו $A_{\mathrm{tor}}(L) = \bigoplus_p \bigoplus_{i=1}^{m_p} \mathbb{Z}/p^{k_i(p)}\mathbb{Z}$, באשר p עובר של כל המספרים הראשוניים, m_p הוא מספר שלם אי שלילי השווה לאפס עבור כמעט כל p ו $k_i(p)$ הם מספרים טבעיים.

תוצאה $(1c)$ ידועה בשם **המשפט החלש** של Mordell-Weil. מסתבר שהמשפט החלש של Mordell-Weil אינו רק תוצאה של משפט Mordell-Weil אלא גם אחד מיסודות הוכחתו. היסוד השני הנו קיום "פונקצית גבה" על $A(L)$ המקימת תנאים מסוימים המפרטים במשפטון א.ב:

הגדרה א.א: **פונקצית גבה** על חבורה אבלית B הנה פונקציה $h\colon B \to \mathbb{R}$ המקימת את התנאים הבאים:

(2a) לכל $\mathbf{q} \in B$ קים קבוע ממשי $c_1(\mathbf{q})$ כך שלכל $\mathbf{p} \in B$ מתקים $h(\mathbf{p}+\mathbf{q}) \le 2h(\mathbf{p}) + c_1(\mathbf{q})$.

(2b) קים מספר טבעי $m \ge 2$, הנקרא ה**מֵצַד** של h, וקים קבוע ממשי c_2 כך שלכל $\mathbf{p} \in B$ מתקים $h(m\mathbf{p}) \ge m^2 h(\mathbf{p}) - c_2$.

(2c) לכל קבוע ממשי c_3 הקבוצה $\{\mathbf{p} \in B \mid h(\mathbf{p}) \le c_3\}$ סופית. ∎

משפטון א.ב: *תהי B חבורה חלופית עם פונקצית גבה h בעלת מצד m. אם B/mB הנה חבורה סופית, אזי B נוצרת סופית.*

הוכחה: נבחר אברים $\mathbf{q}_1,\dots,\mathbf{q}_r$ ב B המיצגים את B מודולו mB. הם מקימים $B=\bigcup_{i=1}^r(mB+\mathbf{q}_i)$. יהי $\mathbf{p}\in B$. נראה שאם נפחית מ $\mathbf{p}$ צרוף מתאים של $\mathbf{q}_1,\dots,\mathbf{q}_r$, נקבל כפולה שלמה של אבר של B בעל גבה החסום על ידי קבוע שאינו תלוי ב $\mathbf{p}$. האברים $\mathbf{q}_1,\dots,\mathbf{q}_r$ והאברים בעלי גבה החסום על ידי הקבוע הנ״ל יצרו את B. לצרך זה נחקה את המתכון של אוקלידס וניצור באנדוקציה סדרה של אברים $\mathbf{p}_0,\mathbf{p}_1,\mathbf{p}_2,\dots$ של B וסדרה של מספרים $i_1,i_2,i_3,\dots$ בין 1 ל r כך ש $\mathbf{p}_0=\mathbf{p}$ ולכל n

$$\mathbf{p}_{n-1}=m\mathbf{p}_n+\mathbf{q}_{i_n}. \tag{3}$$

יהי $c_1=\max(0,c_1(-\mathbf{q}_1),\dots,c_1(-\mathbf{q}_r))$. אזי לפי $(2b)$ $h(m\mathbf{p}_n)\ge m^2h(\mathbf{p}_n)-c_2$. לכן, לפי $(2a)$

$$\begin{aligned}h(\mathbf{p}_n)&\le\frac{1}{m^2}[h(m\mathbf{p}_n)+c_2]\\&=\frac{1}{m^2}[h(\mathbf{p}_{n-1}-\mathbf{q}_{i_n})+c_2]\\&\le\frac{1}{m^2}[2h(\mathbf{p}_{n-1})+c_1+c_2]\end{aligned}$$

לכן $c=c_1+c_2$ מקים

$$h(\mathbf{p}_n)\le\frac{1}{m^2}[2h(\mathbf{p}_{n-1})+c] \tag{4}$$

נשתמש ב (4) n פעמים עד שנגיע ל $\mathbf{p}_0$:

$$\begin{aligned}h(\mathbf{p}_n)&\le\frac{2}{m^2}h(\mathbf{p}_{n-1})+\frac{1}{m^2}c\\&\le\frac{2}{m^2}\Big[\frac{2}{m^2}h(\mathbf{p}_{n-2})+\frac{1}{m^2}c\Big]+\frac{1}{m^2}c\\&=\Big(\frac{2}{m^2}\Big)^2h(\mathbf{p}_{n-2})+\Big[\frac{1}{m^2}+\frac{2}{m^4}\Big]c\\&\le\Big(\frac{2}{m^2}\Big)^2\Big[\frac{2}{m^2}h(\mathbf{p}_{n-3})+\frac{1}{m^2}c\Big]+\Big[\frac{1}{m^2}+\frac{2}{m^4}\Big]c\\&=\Big(\frac{2}{m^2}\Big)^3h(\mathbf{p}_{n-3})+\Big[\frac{1}{m^2}+\frac{2}{m^4}+\frac{2^2}{m^6}\Big]c\\&\ \vdots\\&\le\Big(\frac{2}{m^2}\Big)^nh(\mathbf{p})+\Big[\frac{1}{m^2}+\frac{2}{m^4}+\cdots+\frac{2^{n-1}}{m^{2n}}\Big]c\\&<\Big(\frac{2}{m^2}\Big)^nh(\mathbf{p})+\frac{1}{m^2}\Big[1+\frac{2}{m^2}+\Big(\frac{2}{m^2}\Big)^2+\Big(\frac{2}{m^2}\Big)^3+\cdots\Big]c\\&=\Big(\frac{2}{m^2}\Big)^nh(\mathbf{p})+\frac{c}{m^2-2}\le\frac{h(\mathbf{p})}{2^n}+\frac{c}{2}\end{aligned}$$

אם נקח n מספיק גדול נקבל מכאן ש $h(\mathbf{p}_n) \leq \frac{h(\mathbf{p})}{2^n} + \frac{c}{2} < \frac{c}{2} + \frac{c}{2} = c$. מצד שני, שמוש חוזר ב (3) נותן

$$\begin{aligned}
\mathbf{p} &= m\mathbf{p}_1 + \mathbf{q}_{i_1} \\
&= m(m\mathbf{p}_2 + \mathbf{q}_{i_2}) + \mathbf{q}_{i_1} = m^2\mathbf{p}_2 + m\mathbf{q}_{i_2} + \mathbf{q}_{i_1} \\
&= m^2(m\mathbf{p}_3 + \mathbf{q}_{i_3}) + m\mathbf{q}_{i_2} + \mathbf{q}_{i_1} = m^3\mathbf{p}_3 + m^2\mathbf{q}_{i_3} + m\mathbf{q}_{i_2} + \mathbf{q}_{i_1}
\end{aligned}$$

לכן, $\mathbf{p} = m^n\mathbf{p}_n + \sum_{j=1}^{n} m^{j-1}\mathbf{q}_{i_j}$. במלים אחרות, $\mathbf{p}$ הנו צרוף לינארי של אברי הקבוצה הסופית $\{\mathbf{q} \in A \mid h(\mathbf{q}) < c\} \cup \{\mathbf{q}_1, \ldots, \mathbf{q}_r\}$, כמבוקש. ∎

ב. הערכות בדידות

אבני היסוד של הארתמטיקה של קבוצת המספרים הטבעיים ושל שדה המספרים הרציונליים הם המספרים הראשוניים. נתבונן במספר ראשוני p. כל מספר רציונלי u שונה מאפס נתן להצגה בצורה $u=\frac{a}{b}p^k$ באשר a ו b מספרים שלמים הזרים ל p ו k הוא מספר שלם הנקבע באפן יחיד על ידי u. נסמן אותו ב $v_p(u)$. הפונקציה $v_p\colon \mathbb{Q}^\times \to \mathbb{Z}$ מקימת כמה כללים, כגון $v_p(uu') = v_p(u) + v_p(u')$ ו $v_p(u+u') \ge \min\left(v_p(u), v_p(u')\right)$. את הכללים האלו אנו מבקשים להפשיט ולהניח בזה את אבני היסוד לארתמטיקה של שדות כלליים יותר.

ב.א הערכות בדידות וחוגי הערכה. הערכה בדידה (**מנורמלת**) של שדה K הנה העתקה $v\colon K \to \mathbb{Z}\cup\{\infty\}$ המקימת את התנאים הבאים:

(1a) $v(ab) = v(a) + v(b)$;

(1b) $v(a+b) \ge \min(v(a), v(b))$;

(1c) $v(a) = \infty$ אם ורק אם $a = 0$;

(1d) קים $a \in K^\times$ כך ש $v(a) = 1$.

לפי ההגדרה מקים הסימן ∞ המצֹרף ל $\mathbb{Z}$ את הכללים הבאים:

(2a) $\infty + \infty = m + \infty = \infty + m = \infty$

(2b) $m < \infty$ לכל $m \in \mathbb{Z}$.

מהכללים (1) ו (2) נובעים כללים נוספים:

(3a) $v(1) = 0$, $v(-a) = v(a)$ לכל $a \in K$

(3b) $v(u^{-1}) = -v(u)$ אם $u \ne 0$.

(3c) אם $v(a) < v(b)$, אזי $v(a+b) = v(a)$ (השתמש בזהות $a = (a+b) - b$).

(3d) אם $\sum_{i=1}^n a_i = 0$ ו $a_i \ne 0$ לכל i, אזי קימים $i < j$ כך ש $v(a_i) = v(a_j)$.

הקבוצה $O_v = \{a \in K \mid v(a) \ge 0\}$ הנה **תת חוג** של K הנקרא **חוג ההערכה** של v. לחוג זה יש אידאל מֵרַבִּי יחיד $M_v = \{a \in K \mid v(a) > 0\}$. אידאל זה נוצר על ידי כל אבר π המקים $v(\pi) = 1$. אבר כזה נקרא **אבר ראשוני** של ההערכה v. כל אידאל אחר של O_v הוא חזקה של M_v, דהיינו יש לו הצורה $\pi^n O_v$ באשר n מספר שלם אי שלילי. חבורת האברים ההפיכים של O_v תהיה $O_v^\times = \{u \in K^\times \mid v(u) = 0\}$. ל $\bar{K}_v = O_v/M_v$ קוראים **שדה השאריות** של K ב v. לכל $a \in O_v$ נסמן ב $\bar{a}$, אם לא יהיה מקום לבלבול, את האבר $a + M_v$ של $\bar{K}_v$.

משפטון ב.ב (משפט הקֵרוב החלש): *תהיינה $v_1, \dots, v_n$ הערכות בדידות שונות של שדה K, יהיו $a_1, \dots, a_n$ אברים של K ויהיו $m_1, \dots, m_n$ מספרים שלמים. אזי קים $x \in K$ כך ש $v_i(x - a_i) = m_i$ עבור $i = 1, \dots, n$.*

הוכחה: להוכחה כמה שלבים.

שלב א: *$O_{v_i} \neq O_{v_j}$ עבור $i \neq j$.* ואכן, נניח בשלילה ש $O_{v_i} = O_{v_j}$. אזי, לאידאל המרבי המשותף של שני החוגים יש הצורה $O_{v_i}\pi_i$ באשר $v_i(\pi_i) = 1$ וגם $O_{v_j}\pi_j$ באשר $v_j(\pi_j) = 1$. לכן, $\pi_i = u\pi_j$ באשר u הנו אבר הפיך של החוג. הערך של u תחת כל אחת מההערכות הנו 0. לכן, $v_i(\pi_j) = 1$ ו $v_j(\pi_i) = 1$. מכאן נובע ש $v_i = v_j$, בנגוד להנחה.

שלב ב: *$O_{v_i} \not\subseteq O_{v_j}$ עבור $i \neq j$.* ואכן, נניח בשלילה ש $O_{v_i} \subseteq O_{v_j}$. אזי, לפי שלב א, $O_{v_i} \subset O_{v_j}$. נבחר $a \in O_{v_j} \setminus O_{v_i}$. אזי $v_j(a) \geq 0$ ו $v_i(a) < 0$.

עתה נבחר $b \in K$ כך ש $v_j(b) < 0$ ונבחר n מספיק גדול כך ש $v_i(a^{-n}b) = -nv_i(a) + v_i(b) > 0$. עבור j יתקים $v_j(a^{-n}b) < 0$. לכן $a^{-n}b \notin O_{v_j}$ ולכן $a^{-n}b \notin O_{v_i}$. מכאן נובע ש $v_i(a^{-n}b) < 0$, בנגוד לנאמר לעיל.

שלב ג: *לכל i קים y_i ב K כך ש $v_i(y_i) \geq 0$ ו $v_j(y_i) < 0$ לכל $j \neq i$.* נוכיח טענה זו באנדוקציה על n. עבור $n = 2$ נובעת הטענה משלב ב. נניח אפוא ש $n \geq 3$ ושהטענה הוכחה כבר עבור $n - 1$. נבחר k בין 1 ל n השונה מ i. אפשר להניח ש $k \neq i$.

הנחת האנדוקציה נותנת $y \in K$ כך ש $v_i(y) \geq 0$ ו $v_j(y) < 0$ לכל $j \neq i, k$. המקרה $n = 2$ נותן $z \in K$ כך ש $v_i(z) \geq 0$ ו $v_k(z) < 0$. נבחר m טבעי מספיק גדול כך ש $v_k(z^m) < v_k(y)$ ואם $v_j(z) < 0$ אזי $v_j(z^m) < v_j(y)$. האבר $y_i = y + z^m$ יקים את הטענה.

שלב ד: *לכל i קים $x_i \in K$ כך ש $v_i(x_i) > 0$ ו $v_j(x_i) < 0$ לכל $j \neq i$.* יהי y_i כמו בשלב ג. נבחר $z \in K$ כך ש $v_i(z) > 0$. יהי m מספר טבעי מספיק גדול. אזי $x_i = y_i^m z$ יקים את הטענה.

שלב ה: *לכל i בין 1 ו n ולכל k טבעי קים $z_i \in K$ כך ש $v_i(z_i - 1) > k$ ו $v_j(z_i) > k$ לכל $j \neq i$.* יהי x_i כבשלב ד. נבחר m מספיק גדול. אזי $z_i = \frac{1}{1-x_i^m}$ יקים את הטענה.

שלב ו: *לכל l טבעי קים $z \in K$ כך ש $v_i(z - a_i) > l$ לכל i.* נבחר k מספיק גדול ולכל i נבחר z_i כמו בשלב ה. אזי $z = \sum_{i=1}^{r} a_i z_i$ יקים את הטענה.

שלב ז: *קים $x \in K$ כך ש $v_i(x - a_i) = m_i$ לכל i.* יהי z כמו בשלב ו עם $l > m_i$. לכל i נבחר $b_i \in K$ כך ש $v_i(b_i) = m_i$. לפי שלב ו קים $z' \in K$ כך ש $v_i(z' - b_i) > m_i$ לכל i. האבר $x = z + z'$ יקים את הטענה.

בזאת מסתימת הוכחת המשפט. ∎

ב.ג דֻגמאות להערכות בדידות: א. שדה המספרים הרציונליים. יהי p מספר ראשוני. כל מספר רציונלי u שונה מאפס נתן להצגה בצורה $u = p^m \frac{a}{b}$, באשר m מספר שלם ו a, b הם מספרים שלמים שונים מאפס שאינם מתחלקים ב p. בהצגה זו נקבע m באפן יחיד. נגדיר אפוא $v_p(u) = m$ ונקבל באפן כזה הערכה בדידה של $\mathbb{Q}$ הנקראת **ההערכה ה־p־אדית**. לדגמה $v(p) = 1$ אולם $v(l) = 0$ לכל מספר ראשוני השונה מ p. חוג ההערכה של v_p הנו

$O_{v_p} = \{\frac{a}{b} \mid a,b \in \mathbb{Z},\ p \nmid b\}$ ושדה השאריות הנו $\mathbb{F}_p$, השדה היחיד בעל p אברים. נתן להראות שכל הערכה בדידה של $\mathbb{Q}$ מתלכדת עם v_p עבור איזה שהוא p ראשוני.

ב. שדה פונקציות רציונליות. נצא משדה כלשהוא K_0, נבחר אבר נעלה (= טרנסצנדנטי) t מעל K_0 ונתבונן בשדה הפונקציות הרציונליות $K = K_0(t)$. יהי $p \in K_0[t]$ פולינום אי פריק. כל אבר שונה מאפס u של K נתן להצגה כמנה $u = p^m \frac{f}{g}$, באשר $m \in \mathbb{Z}$ ו $f, g \in K_0[t]$ פולינומים שונים מאפס. שוב, m נקבע באפן יחיד על ידי p. ההגדרה $v_p(u) = m$ נותנת לנו הערכה בדידה של K המסומנת ב v_p אשר p הוא אבר ראשוני שלה. הערכה זו **טריביאלית** על K_0, כלומר $v_p(c) = 0$ לכל $c \in K_0^\times$. חוג ההערכה של v_p הנו $O_{v_p} = \{\frac{f}{g} \mid f,g \in K_0[t],\ p \nmid g\}$. ואלו שדה השאריות הנו $\bar{K}_v = K_0(c)$, באשר c הנו שרש של p. שדה זה נקבע באפן יחיד עד כדי איזומורפיזם־K_0.

ואכן, שני פולינומים אי פריקים הנבדלים זה מזה על ידי כפל בקבוע נותנים אותה הערכה בדידה של K. לעומת זאת פולינומים זרים נותנים הערכות בדידות שונות של K. בנוסף להערכות v_p הנ"ל יש ל K רק הערכה אחת נוספת שהיא טריביאלית על K_0. הערכה זו מסומנת ב v_∞ ומוגדרת על ידי הנוסחה $v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f)$ עבור פולינומים $f, g \in K_0[t]$ כך ש $g \neq 0$.

ג. שדה סופי. נראה כאן שלשדה סופי K אין הערכות בדידות. ואכן יהי $\mathbb{F}_p$ השדה הראשוני של K. נניח בשלילה ש v הוא הערכה בדידה של K. אזי כל אבר $a \in \mathbb{F}_p^\times$ הוא סכום של מספר סופי של 1־ים ולכן שיך ל O_v. באפן דומה גם $a^{-1} \in O_v$. מהזהות $aa^{-1} = 1$ נובע ש $v(a) + v(a^{-1}) = 0$. שני המחוברים באגף שמאל אי שליליים ולכן שוים לאפס.

מהנחת השלילה נובע שקיים $x \in K^\times$ כך ש $v(x) < 0$. אבר זה מקים משואה עם מקדמים ב $\mathbb{F}_p$: $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. למחובר x^n באגף שמאל יש ערך הקטן מהערכים של כל שאר המחוברים. לכן, לפי $(3b)$, $nv(x) = v(0) = \infty$, סתירה. ∎

למה ב.ד: *תהי v הערכה בדידה של שדה K. אם R תת חוג נאות של K המקיף את O_v, אזי $R = O_v$.*

הוכחה: נבחר אבר ראשוני π של ההערכה v. נניח בשלילה שקים $x \in R \smallsetminus O_v$. אזי $v(x) < 0$ ולכן קים $m > 0$ וקים $u \in O_v^\times$ כך ש $x = u\pi^{-m}$. לכן $\pi^{-1} = u^{-1}\pi^{m-1}x \in R$. לכן $\pi^k \in R$ לכל k שלם.

עתה, כל אבר שונה מאפס של K נתן להצגה בצורה $u'\pi^k$ עבור $k \in \mathbb{Z}$ ו $u' \in O_v^\times$. לכן $K = R$, בסתירה להנחת המשפט. ∎

ב.ה הערכות בדידות תחת הרחבות סופיות. תהי L/K הרחבת שדות סופית. תהי w הערכה בדידה של L ותהי v הערכה בדידה של K. נאמר ש w **שוכנת מעל** v אם $O_w \cap K = O_v$. מכאן נובע ש $M_w \cap O_v = M_v$. יהיו π_w ו π_v אברים ראשוניים של w ו v בהתאמה. אזי קים מספר טבעי $e = e(w/v)$ כך ש $w(\pi_v) = e$ (ולכן $M_v O_w = M_w^e$). מספר זה נקרא **ציון ההסתעפות (ramification index)** של w מעל v. בעזרת $(3d)$

אפשר להוכיח ש $e \leq [L:K]$. ביתר דיוק, האברים $1, \pi_w, \ldots, \pi_w^{e-1}$ אינם תלויים לינארית מעל K.

כמו כן, $\bar{K}_v = O_v/M_v$ משוכן באפן טבעי ב $\bar{L}_w = O_w/M_w$. אם $x_1, \ldots, x_n$ הם אברי O_w אשר מודולו M_w אינם תלויים לינארית מעל $\bar{K}_v$, אזי הם אינם תלויים לינארית גם מעל K. ואכן, נניח ש $a_1, \ldots, a_n$ הם אברים של K שלא כלם אפס כך ש $0 = \sum_{i=1}^n a_i x_i$. יהי $m = \min(v(a_1), \ldots, v(a_n))$. אזי כל אחד מהאברים $b_i = \pi_v^{-m} a_i$ שיך ל O_v ולפחות אחד מהם הפיך. מעבר לשדה השאריות $\bar{L}_w$ יתן סתירה. בפרט נקבל ש $f = f(w/v) = [\bar{L}_w : \bar{K}_v] \leq [L:K]$. מספר זה נקרא **מעלת שדות השאריות**.

אנו נאמר ש w **אינו מסעף מעל** v (**או מעל** K) אם ההרחבה $\bar{L}_w/\bar{K}_v$ פרידה ואם $e(w/v) = 1$.

נניח עתה ש L' הנה הרחבה סופית של L וש w' שוכנת מעל w ל L'. מההגדרות נובע ש

$$e(w'/v) = e(w'/w)e(w/v) \quad \text{ו} \quad f(w'/v) = f(w'/w)f(w/v).$$

בפרט, w'/v אינו מסעף אם ורק אם w'/w ו w/v אינם מסעפים.

נשים לב לכך שלחוג O_v יש התכונה הבאה: אם $x \in K$, אזי $x \in O_v$ או $x^{-1} \in O_v$. באפן כללי נכנה תת חוג O של K **חוג הערכה** אם לכל $x \in K$ מתקיים $x \in O$ או $x^{-1} \in O$.

משפטון ב.ו (משפט ההרחבה של Chevalley): *יהי φ הומומורפיזם של תחום שלמות R בעל שדה מנות K לתוך שדה $\bar{K}$ ויהי L שדה המקיף את R. אזי קים ל L חוג הערכה O עם אידאל מרבי M כך ש $O \cap K = R$ ו $M \cap R = \mathrm{Ker}(\varphi)$. יתר על כן, אפשר לבחר את O כך שהשדה O/M הנו הרחבה אלגברית של $\bar{K}$.*

הוכחה: ראה למשל משפט 1 בעמוד 8 של [Lan]. ∎

משפטון ב.ז: *תהי v הערכה בדידה של שדה K ותהי L הרחבה פרידה סופית של K. אזי כל הערכה של L מעל v בדידה. יתר על כן, יהיו w_i, $i \in I$ כל ההערכות הבדידות של L השוכנות מעל v. אזי*

$$\sum_{i \in I} e(w_i/v) f(w_i/v) = [L:K] \tag{4}$$

בפרט, מספר ה w_i־ים סופי וגדול מאפס.

הוכחה: ראה עמוד 425 של [Bou]. ∎

תהי L/K הרחבת שדות סופית. אנו נאמר שההערכה בדידה v של K **אינה מסעפת** ב L אם כל הערכה w של L השוכנת מעל v אינה מסעפת מעל v.

למה ב.ח: *יהי v הערכה בדידה של K, יהי L הרחבה סופית פרידה של K ויהי x אבר קדום של L/K כך ש $f(X) = \mathrm{irr}(x, K) \in O_v[X]$ וכך ש $\bar{f}(X) = \prod_{i=1}^{r} h_i(X)$, באשר $h_i \in \bar{K}_v[X]$ הם פולינומים אי פריקים, פרידים וזרים זה לזה. אזי v אינו מסעף ב L.*

הוכחה: לכל i בין 1 לבין r נבחר שרש c_i של h_i בסגור האלגברי של $\bar{K}_v$. אזי נתן להרחיב את העתקת המנה $\varphi_v\colon O_v \to \bar{K}_v$ להומומורפיזם $\psi_i\colon O_v[x] \to \bar{K}_v(c_i)$ כך ש $\psi_i(x) = c_i$. משפט ההרחבה של שבליה נותן חוג הערכה O_i של L עם אידאל מרבי M_i כך ש $M_i \cap O_v[x] = \mathrm{Ker}(\psi_i)$. לכן $M_i \cap O_v = M_v$. מתוספת ב.ז נובע ש O_i הנו חוג ההערכה של הערכה בדידה w_i. הערכה זו שוכנת אפוא מעל v ומקימת $\bar{K}_v(c_i) \subseteq \bar{L}_{w_i}$.

אלו היה $w_i = w_j$ עבור איזה j שהוא השונה מ i, היינו מקבלים ש $O_i = O_j$ ולכן $\mathrm{Ker}(\psi_i) = \mathrm{Ker}(\psi_j)$. מכאן היינו מקבלים איזומורפיזם־$\bar{K}$, $\sigma\colon \bar{K}_v(c_i) \to \bar{K}_v(c_j)$ כך ש $\sigma(c_i) = c_j$, בסתירה לזרות של h_i ו h_j.

נניח שמלבד $w_1, \dots, w_r$ יש ל v עוד הרחבות $w_{r+1}, \dots, w_s$ ל L. לפי (4),

$$
\begin{aligned}
[L:K] = \deg(f) = \deg(\bar{f}) = \sum_{i=1}^{r} \deg(h_i) &= \sum_{i=1}^{r} [\bar{K}_v(c_i) : \bar{K}_v] \\
&\le \sum_{i=1}^{r} [\bar{L}_{w_i} : \bar{K}_v] \le \sum_{i=1}^{s} e(w_i/v)[\bar{L}_{w_i} : \bar{K}_v] = [L:K]
\end{aligned}
$$

לכן $\sum_{i=1}^{r} [\bar{L}_{w_i} : \bar{K}_v] = [L:K]$, $r = s$, $e(w_i/v) = 1$ ו $\bar{K}_v(c_i) = \bar{L}_{w_i}$, בפרט $\bar{L}_{w_i}/\bar{K}_v$ הנה הרחבה פרידה עבור $i = 1, \dots, r$. מכל זה עולה ש v אינו מסעף ב L. ∎

ב.ט הרחבות שלמות. יהי R תחום שלמות בעל שדה מנות K. יהי L הרחבה סופית של K ויהי $x \in L$. נאמר ש x **שלם** מעל R אם x מקיֵם משואה מתוקנת $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ עם מקדמים $a_i \in R$. נסמן את אסף כל אברי L השלמים מעל R ב S. נתן להראות ש S הוא תת חוג של L המקיף את R. יתר על כן, S הוא החתוך של כל חוגי ההערכה של L המקיפים את R (ראה משפטון 4 בעמוד 12 של [La1]). בנוסף לזה $\mathrm{Quot}(S) = L$ וכל אבר של L השלם מעל S שיך ל S. החוג S **סגור** אפוא **בשלמות**. הוא נקרא **הסגור השלם** של R ב L.

לדגמה, $\mathbb{Z}$ סגור בשלמות. אם K הוא **שדה מספרים**, דהיינו הרחבה סופית של $\mathbb{Q}$, אזי הסגור השלם של $\mathbb{Z}$ ב K מסומן ב O_K ונקרא **חוג המספרים השלמים** של K.

אם R הוא חוג הערכה בדידה, אזי כל חוג הערכה של L המקיף את R הנו חוג הערכה בדידה. במקרה זה, S הוא אפוא החתוך של כל חוגי ההערכה הבדידה של L המקיפים את R. כל חוג הערכה בדידה סגור בשלמות.

ב.י הערכות בדידות תחת הרחבות גלואה. תהי v הערכה בדידה של שדה K ותהי L הרחבת גלואה סופית של K. תהי w הערכה בדידה של L המונחת מעל v. אזי לכל $\sigma \in \mathrm{Gal}(L/K)$ הפונקציה $w \circ \sigma\colon L \to \mathbb{Z} \cup \{\infty\}$ הנה הערכה בדידה של L המונחת מעל v. להפך,לכל הערכה בדידה נוספת w' של L המונחת מעל v

קים $\sigma \in \mathrm{Gal}(L/K)$ כך ש $w' = w \circ \sigma$. (ראה למשל תוצאה 1 בעמוד 16 של [La2]). החבורה $D(w/v) = \{\sigma \in \mathrm{Gal}(L/K) \mid w \circ \sigma = w\}$ נקראת חבורת הפרוק של w (מעל K). ההרחבה $\bar{L}_w/\bar{K}_v$ הנה נורמלית. לכל $\sigma \in D(w/v)$ מתאים אבר $\bar{\sigma} \in \mathrm{Aut}(\bar{L}_w/\bar{K}_v)$ המקיים $\bar{\sigma}\bar{x} = \overline{\sigma x}$ לכל $x \in O_w$ (באשר הגג מסמן כרגיל צמצום מודולו M_w). ההעתקה $\sigma \mapsto \bar{\sigma}$ נותנת סדרה מדויקת קצרה

$$1 \to I(w/v) \to D(w/v) \to \mathrm{Aut}(\bar{L}_w/\bar{K}_v) \to 1$$

(ראה משפטון 14 בעמוד 15 של [La2]). $D(w/v)$ היא **חבורת הפרוק** של w מעל L ואלו $I(w/v)$ נקראת **חבורת ההתמדה** של w מעל L. בנוסף על כך מתקיים, $[\bar{L}_w : \bar{K}_v]_i e(w/v) = |I(w/v)|$, באשר הגורם הראשון באגף שמאל הנו מעלת אי הפרידות של ההרחבה $\bar{L}_w/\bar{K}_v$. בפרט w/v אינו מסעף אם ורק אם חבורת ההתמדה טריביאלית. לכל $\tau \in \mathrm{Gal}(L/K)$ מתקיים $D(w \circ \tau/v) = \tau^{-1}D(w/v)\tau$ ו $I(w \circ \tau/v) = \tau^{-1}I(w/v)\tau$. לכן, v אינו מסעף ב L אם ורק אם $I(w/v) = 1$. מספר ההרחבות השונות של v ל L שוה ל $(\mathrm{Gal}(L/K) : D(w/v))$. ביתר דיוק, אם $\sigma_1, \ldots, \sigma_m$ הנם מיצגים של המחלקות הימניות של $\mathrm{Gal}(L/K)$, אזי $w \circ \sigma_1, \ldots, w \circ \sigma_m$ הם בדיוק ההרחבות השונות של v ל L.

ב.יא השלמות. הערכה בדידה v של שדה K מגדירה טופולוגיה על K הנקראת טופולוגית־v. בסיס לסביבות הפתוחות של אבר $a \in K$ הוא אסף כל הקבוצות בעלות הצורה $\{x \in K \mid v(x-a) \geq m\}$ שבהן $a \in K$ ו $m \in \mathbb{Z}$. אומרים ש K **מְשלם** (complete) (ביחס ל v) אם כל סדרת קושי של K בטופולוגית־v מתכנסת. אם K עדין אינו מְשלם־v אפשר להשלים אותו. כלומר, אפשר לבנות שדה $\hat{K}_v$ מְשלם תחת הרחבה בדידה $\hat{v}$ המרחיבה את v (במובן זה ש $\hat{v}(a) = v(a)$ לכל $a \in K$) כך ש K צפוף־v ב $\hat{K}_v$. שדה זה יחיד עד כדי איזומורפיזם־K.

$\hat{K}$ מתקבל למשל כחוג כל סדרות קושי־v של K מודולו האידאל של הסדרות המתכנסות־v לאפס.

לדגמה, ההשלמה של $\mathbb{Q}$ ביחס להערכה ה p־אדית מסומנת ב $\mathbb{Q}_p$ ונקראת **שדה המספרים ה p־אדיים**. את אבריה אפשר להציג באפן יחיד כטורים אינסופיים $a = \sum_{i=m}^{\infty} a_i p^i$, באשר $m \in \mathbb{Z}$ ו a_i הוא מספר שלם בין 0 ל $p-1$. אם $a_m \neq 0$, אזי $\hat{v}_p(a) = m$. חוג ההערכה של $\mathbb{Q}_p$ מסומן ב $\mathbb{Z}_p$. הוא כולל בדיוק את כל הטורים הנ"ל שעבורם $m \geq 0$.

ההשלמה של השדה $K = K_0(t)$ ביחס להערכה של K/K_0 שעבורה t אבר ראשוני היא שדה טורי החזקות הפורמליים $K_0((t))$. אבר בשדה זה הנו טור חזקות פורמלי $\sum_{i=m}^{\infty} a_i t^i$ שבו $m \in \mathbb{Z}$ ו $a_i \in K_0$. שוב, הערך של טור כזה הנו m אם $a_m \neq 0$.

מהגדרת ההשלמה עולה ששדה השאריות של $\hat{K}_v$ שוה ל $\bar{K}_v$ ושאבר ראשוני של v הנו גם אבר ראשוני של $\hat{v}$.

משפטון ב.יב (הלמה של Hensel): *יהי K שדה מְשלם תחת הערכה בדידה v.*

(א) *יהי $f \in O_v[X]$ ויהי $a \in O_v$ כך ש $v(f(a)) > 0$ ו $v(f'(a)) = 0$ (f' מסמן את הנגזרת של f). אזי קים x יחיד ב O_v כך ש $f(x) = 0$ ו $v(x-a) > 0$.*

(ב) *תהי (L,w) הרחבה סופית של (K,v) ויהיו $w_1,\dots,w_n$ אברים של L שאינם תלויים לינארית מעל K. נתבונן באברים $x_i=\sum_{j=1}^n a_{ij}w_j$, $i=1,2,3,\dots$, של L עם מקדמים $a_{ij}\in K$. נניח ש $\{x_i\}_{i=1}^\infty$ היא סדרת קושי־w. אזי כל אחת מסדרות המקדמים $\{a_{ij}\}_{i=1}^\infty$ הנה סדרת קושי. בפרט (L,w) מֻשלם.*

(ג) *בסימונים של (ב), $x_i\to 0$ אם ורק אם $a_{ij}\to 0$ לכל j.*

(ד) *יהי L הרחבה פרידה סופית של K. אזי נתן להרחיב את v באפן יחיד להערכה בדידה של L אשר L מֻשלם תחתיה.*

הוכחת א: נגדיר באנדוקציה סדרת אברים x_n של O_v כך ש $x_0=a$, ו $x_{n+1}=x_n-\frac{f(x_n)}{f'(x_n)}$. אזי $v(f(x_n))\ge n+1$ ו $v(x_{n+1}-x_n)\ge n+1$. לכן x_n מתכנס לאבר x של O_v בעל התכונות המבוקשות.

הוכחת ב: המקרה שבו $n=1$ ברור. נניח אפוא ש $n>1$ ושהלמה הוכחה עבור $n-1$.

נניח בשלילה למשל ש $\{a_{in}\}_{i=1}^\infty$ אינה סדרת קושי. אזי קים $m\in\mathbb{Z}$ כך שלכל i טבעי קים $k(i)\ge i$ כך ש $v(a_{k(i),n}-a_{i,n})\le m$. הסדרה $\{x_{k(i)}-x_i\}_{i=1}^\infty$ שואפת־w לאפס. לכן, האגף השמאלי של

$$\frac{x_{k(i)}-x_i}{a_{k(i),n}-a_{i,n}}-w_n=\sum_{j=1}^{n-1}\frac{a_{k(i),j}-a_{ij}}{a_{k(i),n}-a_{in}}w_j \tag{5}$$

שואף־w ל $-w_n$ ומהוה אפוא סדרת קושי־w. מהנחת האנדוקציה נובע שכל אחת מסדרות המקדמים של אגף ימין הנה סדרת קושי־v. הואיל ו (K,v) מֻשלם, סדרת המקדמים של w_j באגף ימין שואפת לאבר b_j של K. אם נתן אפוא ל i לשאף לאינסוף ב (5), נקבל בגבול $-w_n=\sum_{j=1}^{n-1}b_jw_j$. זאת תהיה סתירה לאי התלות של $w_1,\dots,w_n$.

הוכחת ג: לפי (ב) קיָם $b_j\in K$ כך ש $a_{ij}\to b_j$. לכן, $\sum_{j=1}^n b_jw_j=0$. מאי התלות של $w_1,\dots,w_n$ נובע ש $b_j=0$ לכל j.

הוכחת ד: יהיו w ו w' הרחבות של v ל L. יהי x אבר של L כך ש $w(x)<0$. אזי $w(x^{-n})$ הם מספרים שלמים השואפים לאינסוף יחד עם n. במלים אחרות, האברים x^{-n} שואפים־w לאפס. מ (ג) נובע שסדרות המקדמים שלהם (ביחס לבסיס קבוע של L/K) שואפות־v לאפס. לכן x^{-n} שואפים־w' לאפס. בפרט קים n כך ש $w'(x^{-n})>0$. מכאן ש $w'(x)<0$.

באפן סימטרי נובע שאם $w'(x)<0$, אזי $w(x)<0$. לכן $O_w=O_{w'}$, כפי שהיה להוכיח. ∎

דֻגמה: אם p ראשוני ו $n|p-1$, אזי $\mathbb{Q}_p$ מכיל שרש יחידה מסדר n. ∎

אם L היא הרחבה סופית פרידה של K ו w הערכה השוכנת מעל v ל L, אזי נתן לשכן את $\hat{K}_v$ באפן טבעי ב $\hat{L}_w$. מתקים, $e(w/v)=e(\hat{w}/\hat{v})$ ו $f(w/v)=f(\hat{w}/\hat{v})$. בפרט, w מסעף מעל v אם ורק אם $\hat{w}$ מסעף מעל $\hat{v}$. יתר על כן, השדה $L\hat{K}_v$ הנו הרחבה סופית של $\hat{K}_v$ ולכן מֻשלם. הואיל והוא שוכן בין L לבין $\hat{L}_w$, L צפוף בו. לכן, $L\hat{K}_v=\hat{L}_w$.

בעקבות למת הנזל נסמן גם את ההרחבה היחידה של v ל L ב v. חוג ההערכה של v ב K (או ב L) יסומן ב O_K (או ב O_L) שדות השאריות המתאימים יסומנו ב $\bar{K}$ ו $\bar{L}$ וציון ההסתעפות יסומן ב $e(L/K)$. הנסחה (4) מקבלת במקרה זה את הצורה

$$e(L/K)[\bar{L} : \bar{K}] = [L : K]. \tag{6}$$

בהתאם לכך נאמר ש L **אינו מסעף מעל** K אם $\bar{L}/\bar{K}$ פריד ו $e(L/K) = 1$. לחלופין, $\bar{L}/\bar{K}$ פריד ו $[\bar{L} : \bar{K}] = [L : K]$.

נתן להוכיח שאם $\bar{K}_v$ בלמה ב.ח הוא שדה אינסופי, אזי ההפוך של למה ב.ח נכון. אם K מֻשלם ביחס ל v, ההפוך נכון גם ללא הגבלה זו:

למה ב.יג: *יהי K שדה מֻשלם תחת הערכה בדידה v ויהי L הרחבה פרידה סופית של K. אם L/K אינה מסעפת, אזי קים פולינום מתֻקן אי פריק $f \in O_K[X]$ וקים $x \in O_L$ כך ש $f(x) = 0$, $L = K(x)$ ו $\bar{f}(X)$ אי פריק מעל $\bar{K}$ ופריד.*

הוכחה: נבחר אבר קדום c עבור ההרחבה $\bar{L}/\bar{K}$ ויהי $h = \mathrm{irr}(c, \bar{K})$. אזי h הוא פולינום אי פריק ופריד ממעלה $[L : K]$. נרים את c לאבר x של O_L. יהי $f = \mathrm{irr}(x, K)$. מלמת הנזל ומסעיף משנה ב.ט נובע ש O_L הנו הסגור השלם של O_K ב L. בפרט נקבל ש f הנו פולינום מתֻקן עם מקדמים ב O_K. יתר על כן, $\deg(f) = [K(x) : K] \le [L : K]$. מצד שני, $\bar{f}(c) = \overline{f(x)} = 0$. לכן $h|\bar{f}$. לכן $[L : K] = [\bar{L} : \bar{K}] = \deg(h) \le \deg(\bar{f}) = \deg(f) \le [L : K]$. לכן $\bar{f} = h$ ו $\deg(f) = [L : K]$. בפרט, $L = K(x)$. ∎

הרי שמוש „גלובלי" להשלמות.

משפטון ב.יד: *תהי v הערכה בדידה של שדה K.*

(א) *תהי L הרחבה פרידה סופית של K שבה v אינה מסעפת. תהי K' הרחבה סופית של K ותהי v' הערכה של K' המונחת מעל ל v. אזי v' אינה מסעפת ב LK'.*

(ב) *אם v אינה מסעפת בכמה הרחבות סופיות פרידות של K, אזי v אינה מסעפת גם בצרוף שלהן.*

הוכחה: טענה (ב) נובעת מ (א) ומהכפליות של ציון ההסתעפות. נוכיח אפוא את (א).

תהי w' הערכה של $L' = LK'$ המונחת מעל v'. נסמן ב w את הצמצום של w' ל L. אזי w הנה הערכה בדידה של L המונחת מעל v. נסמן $\hat{K} = \hat{K}_v$. אזי $\hat{L} = \hat{L}_w = L\hat{K}$, $\hat{K}' = \hat{K}'_{v'} = K'\hat{K}$ ו $\hat{L}' = \hat{L}'_{w'} = L'\hat{K}$. לפי ההנחה, w אינה מסעפת מעל v. לכן, $\hat{L}/\hat{K}$ הנה הרחבה לא מסעפת של שדות שלמים. לפי למה ב.יג, קים ל $\hat{L}/\hat{K}$ אבר קדום x ב $O_{\hat{L}}$ וקים פולינום מתֻקן $f \in O_K[X]$ כך ש $f(x) = 0$ ו $\bar{f}(X)$ אי פריק ופריד מעל $\bar{K}$. לכן $\hat{L}' = \hat{K}'(x)$ ו $\bar{f}(X)$ מתפרק למכפלה של פולינומים אי פריקים ואי פרידים מעל $\bar{K}'$. לפי למה ב.ח, $\hat{L}'/\hat{K}'$ אינה מסעפת. לכן גם w'/v' אינה מסעפת. מכאן נובע שההערכה v' אינה מסעפת ב L'. ∎

המשפט היסודי של הארתמטיקה אומר שכל מספר שלם נתן לפרוק באפן יחיד (עד כדי סדר הגורמים ועד כפל ב -1) למכפלה של מספרים ראשוניים. בדרך כלל אין משפט זה נכון בחוג המספרים השלמים O_K של שדה מספרים K. אולם צורה מוחלשת של המשפט נשארת נכונה: כל אידאל שונה מאפס של O_K נתן לפרוק באפן יחיד (עד כדי סדר הגורמים) למכפלה של אידאלים ראשוניים של O_K. תכונה זו אופינית ל„חוגי דדקינד" שאותם נתאר בסעיף זה.

יהי R תחום שלמות בעל שדה מנות K. אנו נאמר ש R הוא חוג **Noether** אם כל אידאל של R נוצר סופית. לדגמה, כל חוג ראשי הוא חוג נטר סגור בשלמות. בפרט, כל חוג הערכה בדידה הוא חוג נטר סגור בשלמות. אם K_0 הוא שדה, אזי כל חוג $K_0[t_1, \ldots, t_n]$ הנו נטרי.

לכל אידאל ראשוני P של R נתאים חוג

$$R_P = \left\{ \frac{a}{b} \mid \ a \in R \text{ and } b \in R \smallsetminus P \right\}$$

זהו **החוג המקומי** של R ב P. יש לו אידאל מרבי יחיד PR_P. והוא מקיֵם, $PR_P \cap R = P$. אם R הוא חוג נטר, גם R_P הוא חוג נטר.

למה ג.א: *אם R הוא תחום שלמות אזי $R = \bigcap R_M$, באשר M עובר על כל האידאלים המרביים של R. אם I ו J הם אידאלים של R כך ש $IR_M = JR_M$ לכל אידאל מרבי M של R, אזי $I = J$.*

הוכחה: נניח שאבר $x \in \mathrm{Quot}(R)$ שיך לכל R_M. אזי לכל M קימים $a_M \in R$ ו $b_M \in R \smallsetminus M$ כך ש $b_M x = a_M$. נסמן ב B את האידאל של R הנוצר על ידי כל האברים b_M. אם $B \neq R$, אזי B מוכל באידאל מרבי M. לכן, $b_M \in M$, בסתירה לבחירה. לכן $B = R$. בפרט קימת קבוצה סופית $\mathcal{M}$ של אידאלים מרביים ולכל $M \in \mathcal{M}$ קים $c_M \in R$ כך ש $\sum_{M \in \mathcal{M}} c_M b_M = 1$. לכן

$$.x = \sum_{M \in \mathcal{M}} x b_M c_M = \sum_{M \in \mathcal{M}} a_M c_M \in R$$

באפן דומה מוכיחים גם את החלק השני של הלמה. ∎

יהי שוב R תחום שלמות בעל שדה מנות K. **אידאל שבור** של R הנו תת מודול־R A שונה מאפס של K שעבורו קים אבר $x \in R$ שונה מאפס כך ש $xA \subseteq R$. בפרט כל אידאל של R הנו אידאל שבור. כמו כן, לכל $x \in K^\times$, xR הוא אידאל שבור הנקרא **אידאל שבור ראשי.**

נגדיר את **המכפלה** של שני אידאלים שבורים A ו B כמודול־R הנוצר על ידי כל המכפלות ab שבהן $a \in A$ ו $b \in B$. **ההפוך** של A יהיה $A^{-1} = \{x \in K \mid \ xA \subseteq R\}$. גם AB וגם A^{-1} הנם אידאלים שבורים של R.

משפטון ג.ב: *יהי R חוג נטר סגור בשלמות שבו כל אידאל ראשוני שונה מאפס של R הוא מרבי. אזי אסף כל האידאלים השבורים של R מהוה חבורה ביחס לכפל שבה R הוא אבר היחידה. יתר על כן, כל אידאל שונה מאפס של R נתן להצגה באפן יחיד (עד כדי סדר) כמכפלה של אידאלים ראשוניים שונים מאפס.*

הוכחה: ראה משפט 2 בעמוד 18 של [La2]. ∎

תחום שלמות R המקים את התנאים של משפטון ג.ב נקרא חוג **Dedekind**. ממשפטון ג.ב נובע שכל אידאל שבור I של R נתן להצגה באפן יחיד (עד כדי סדר) כמכפלה $I = \prod P^{e_P}$ שבה P עובר על כל האידאלים הראשוניים השונים מאפס של R וe_P הם מספרים שלמים שכמעט כלם אפס. האידאל השבור I מוכל ב R (במקרה זה אומרים ש I **שלם**) אם ורק אם $e_P \geq 0$ לכל P. יתר על כן, נתן להוכיח שלכל אידאל ראשוני שונה מאפס P של R, החוג המקומי R_P הנו חוג הערכה בדידה אשר שדה השאריות שלה שוה ל R/P. נסמן ב v_P את ההערכה המתאימה לו. אזי, כל אבר $\pi \in P \smallsetminus P^2$ הנו אבר ראשוני של v_P. באפן יותר כללי, אם $x \in K^\times$, ו $Rx = \prod P^{e_P}$ היא הצגה של האידאל השבור Rx שבה e_P מספרים שלמים שכמעט כלם אפס, אזי $v_P(x) = e_P$ לכל P. להפך, יהי O חוג הערכה של $\mathrm{Quot}(R)$ המקיף את R ויהי M האידאל המרבי של O. אזי $P = M \cap R$ הוא אידאל ראשוני של R. נבחר $m \in M$, $m \neq 0$ ונציג אותו כמנה $m = \frac{a}{b}$ של אברי R. אזי $a = mb$ שיך גם ל R וגם ל M ולכן ל P. מכאן ש $P \neq 0$. לכן P מרבי. מההנחה ש R חוג דדקינד נובע ש R_P הוא חוג הערכה בדידה. יתר על כן, $R_P \subseteq O$. לכן, לפי למה ב.ד, $O = R_P$. בסופו של דבר נצין שֶׁלְאידאלים ראשוניים שונים מתאימות הערכות בדידות שונות.

למה ג.ג: *חוג דדקינד R בעל מספר סופי של אידאלים ראשוניים הוא ראשי.*

הוכחה: יהיו $P_1, \ldots, P_r$ האידאלים הראשוניים השונים של R. יהי A אידאל של R. נציג אותו כמכפלה $A = \prod_{i=1}^r P^{e_i}$. לכל i נבחר אבר ראשוני π_i עבור v_{P_i}. משפט הקרוב החלש נותן $a \in K$ כך ש $v_{P_i}(a - \pi_i^{e_i}) \geq e_i + 1$. בפרט, לפי למה ג.א, $a \in \bigcap_{i=1}^r R_{P_i} = R$. יתר על כן, $v_{P_i}(a) = e_i$. לכן, $Ra = \prod_{i=1}^r P_i^{e_i} = A$. ∎

משפטון ג.ד: *יהי R חוג דדקינד בעל שדה מנות K ויהי L הרחבה סופית פרידה של K. אזי הסגור השלם S של R ב L הנו חוג דדקינד.*

הוכחה: ראה משפטון 1 בעמוד 13 של [CaF]. ∎

נעיר שאם Q הוא אידאל ראשוני שונה מאפס של S ו x הוא אבר שונה מאפס של Q, אזי x מקים משואה אי פריקה ומתוקנת עם מקדמים ב R. כלומר, $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, באשר $a_0, \ldots, a_{n-1} \in R$ ו $a_0 \neq 0$. מתקים $a_0 \in Q \cap R$ ולכן $P = Q \cap R$ הוא אידאל שונה מאפס של R. אנו אומרים ש Q **שוכן מעל** P. ההערכה v_Q של L שוכנת אז מעל v_P להפך, אם אנו יוצאים מאידאל

ראשוני שונה מאפס P של R, אזי PS הוא אידאל של S ולכן נתן להצגה בצורה $PS = \prod_{i=1}^r Q_i^{e_i}$. האידאלים $Q_1, \ldots, Q_r$ הם האידאלים הראשוניים של S המונחים מעל P ו $e_i = e(v_{Q_i}/v_P)$, ו $[S/Q_i : R/P] = [\bar{L}_{v_{Q_i}} : \bar{K}_{v_P}]$. מ (4) בסעיף ב. נובע ש $[L : K] = \sum_{i=1}^r e_i[S/Q_i : R/P]$.

ג.ה: דגמאות לחוגי דדקינד. כל חוג ראשי הנו חוג דדקינד. בפרט, כל חוג הערכה בדידה הוא חוג דדקינד. כמו כן, $\mathbb{Z}$ הנו חוג דדקינד. בנוסף לזה חוג הפולינומים $K_0[t]$ במשתנה t מעל שדה כלשהוא K_0 הוא חוג דדקינד. ממשפטון ג.ד נובע שחוג המספרים השלמים של שדה מספרים הוא חוג דדקינד. ∎

הגדרה ג.ו: מְקוּם ביחס לקבוצה כפלית. יהי R תחום שלמות עם שדה מנות K. תת קבוצה לא ריקה S של R תכונה **כפלית** אם $0 \notin S$ ואם S סגורה תחת כפל. במקרה זה נגדיר את **חוג המנות** של R ביחס ל S כ

$$S^{-1}R = \left\{\frac{a}{b} \mid\ a \in R,\ b \in S\right\}$$

זהו חוג המקיף את R ומוכל ב K. אם I הוא אידאל של R, אזי האידאל של $S^{-1}R$ הנוצר על ידו הנו

$$S^{-1}I = \left\{\frac{a}{b} \mid\ a \in I,\ b \in S\right\}.$$

דֻגמה לקבוצה כפלית ב R הנה קבוצה כל החזקות של אבר a שונה מאפס של R. דגמה אחרת היא $S = R \smallsetminus P$, באשר P הוא אידאל ראשוני של R. במקרה זה $S^{-1}R = R_P$. באפן כללי, אם P_i, $i \in I$, היא קבוצה של אידאלים ראשוניים, אזי $S = \bigcap_{i\in I} R \smallsetminus P_i$ היא קבוצה כפלית. ∎

למה ג.ז: *יהיו R, K ו S כבהגדרה ג.ו.*

(א) *אם אידאל ראשוני P של R מקים $P \cap S \neq \emptyset$, אזי $S^{-1}P = S^{-1}R$.*

(ב) *אם אידאל ראשוני P של R מקים $P \cap S = \emptyset$, אזי $S^{-1}P$ הוא אידאל ראשוני נאות של $S^{-1}R$. יתר על כן, $S^{-1}P \cap R = P$ ו $R_P = (S^{-1}R)_{S^{-1}P}$.*

(ג) *כל אידאל I' של $S^{-1}R$ מקים $S^{-1}(I' \cap R) = I'$.*

(ד) *אם P' הוא אידאל ראשוני של $S^{-1}R$, אזי $P = P' \cap R$ הוא אידאל ראשוני של R המקים $P \cap S = \emptyset$.*

(ה) *ההעתקה $P \mapsto S^{-1}P$ מעתיקה את קבוצה האידאלים הראשוניים של R המקימים $P \cap S = \emptyset$ באפן חד חד ערכי על קבוצת האידאלים הראשוניים של $S^{-1}R$. ההעתקה ההפוכה היא $P' \mapsto P' \cap R$.*

(ו) *ההעתקה המוגדרת ב (ה) שומרת על הכלה. בפרט, M הוא אידאל מרבי של R אם ורק אם $S^{-1}M$ הוא אידאל מרבי של $S^{-1}R$. במקרה זה, $R/M = S^{-1}R/S^{-1}M$.*

(ז) *$S^{-1}R = \bigcap R_M$, באשר M עובר על כל האידאלים המרביים של R הזרים ל S.*

(ח) *אם R הוא חוג דדקינד, גם $S^{-1}R$ הוא חוג דדקינד.*

הוכחה: נסמן $R' = S^{-1}R$ ולכל אידאל I של R נסמן $I' = S^{-1}I$.

(א) כל אבר של S הפיך ב R'.

(ב) אם $P' = R'$, אזי קיימים $P \in P$ ו $s \in S$ כך ש $\frac{p}{s} = 1$. לכן $p = s$ ולכן $P \cap S \neq \emptyset$, בנגוד להנחה.

אם $x \in S^{-1}P \cap R$, אזי $x = \frac{p}{s}$ עבור $p \in P$ ו $s \in S$. לכן, $xs = p \in P$ ולכן $x \in P$.

מכאן נובע ש $R_P \subseteq R'_{P'}$. להפך, כל אבר של החוג באגף ימין נתן להצגה בצורה $\frac{a/s}{b/s'}$ באשר $a, b \in R$, $b \notin P$ ו $s, s' \in S$. אבר זה שוה ל $\frac{as'}{bs}$ ו $bs \notin P$. לכן מתקים שויון בין החוגים המקומיים הנ"ל.

(ג) אם $i' \in I'$, אזי $i' = \frac{i}{s}$ באשר $i \in R$ ו $s \in S$. מהשוויון $i = i's$ נובע ש $i \in I' \cap R$, בנדרש.

(ד) אלו היה קים $s \in P \cap S$ היה s שיך ל P' ולכן $P' = R'$, בנגוד להנחה.

(ה) הטענה נובעת מ (ג) ו (ד).

(ו) הואיל ו $M' \cap R = M$, עלינו להראות רק ש $R' = M' + R$. ואכן כל $r' \in R'$ נתן להצגה בצורה $r' = \frac{r}{s}$ באשר $r' \in R$ ו $s \in S$. לפי ההנחה, s אינו שיך לאידאל המרבי M של R. לכן קים $b \in R$ ו $m \in M$ כך ש $bs = 1 - m$. לכן $r' = mr' + br \in M' + R$ כמבוקש.

(ז) הטענה היא מקרה פרטי של למה ג.א.

(ח) הואיל ו R סגור בשלמות גם R' סגור בשלמות הואיל ו R הוא חוג נטר, נובע מ (ג) שגם R' הוא חוג נטר. לבסוף, הואיל וכל אידאל ראשוני שונה מאפס של R הוא מרבי, נובע מ (ו) שגם כל אידאל ראשוני של R' הוא מרבי. $\blacksquare$

ד. משפטי סופיות בחוגי דדקינד

בסעיף זה נצַיֵד כל אחת מההרחבות הסופיות של השדה K בעצמים ארתמטיים. משפטי הסופיות שנוכיח עבורם יהיו אחד המרכיבים להוכחת המשפט החלש של מורדל־וויל.

ד.א מחלקים ראשוניים. יהי O חוג דדקינד עם שדה מנות K. תהי L הרחבה סופית של K. נסמן ב O_L את הסגור השלם של O ב L. לפי משפטון ג.ד, O_L הנו חוג דדקינד. נבחר קבוצה $\mathcal{P}_L$ העומדת בהתאמה חד חד ערכית עם האידאלים המרביים של O_L. אברי $\mathcal{P}_L$ יכֻנו **מחלקים ראשוניים** של L. לכל $\mathfrak{p} \in \mathcal{P}_L$ נסמן ב $P_\mathfrak{p}$ את האידאל הראשוני של O_L המתאים לו, ב $O_\mathfrak{p}$ את החוג המקומי של O_L ב $P_\mathfrak{p}$, ב $M_\mathfrak{p}$ את האידאל המרבי של $O_\mathfrak{p}$ וב $v_\mathfrak{p}$ את ההערכה הבדידה המתֻקנת של K המתאימה ל $O_\mathfrak{p}$. אם נרצה להתיחס ל L, נוסיף את L מצד שמאל ל $\mathfrak{p}$. לדוגמה, נרשם $O_{L,\mathfrak{p}}$ במקום $O_\mathfrak{p}$.

נסמן את חבורת האידאלים השבורים של O_L ב $\mathcal{I}_L$. חבורת המנה $\mathcal{C}_L = \mathcal{I}_L/\{xO_L \mid x \in L^\times\}$ מכֻנָה **חבורת מחלקות האידאלים** (**class group**) של L (ביחס ל $\mathcal{P}_L$). הואיל וכל אידאל שבור של O_L הופך לאידאל רגיל אחרי כפל באבר של O_L, נתן תמיד לבחור מערכת מיצגים ל $\mathcal{C}_L$ המורכבת מאידאלים של O_L. נניח ש

(1) $\mathcal{C}_L$ הנה חבורה סופית.

ד.ב שלמי־S. תהי S תת קבוצה של $\mathcal{P}_L$. נתבונן בחוג

$$O_{L,S} = \{x \in L \mid v_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \in \mathcal{P}_L \smallsetminus S\} = \bigcap_{\mathfrak{p} \in \mathcal{P}_L \smallsetminus S} O_\mathfrak{p} \ .$$

זהו חוג המקיף את O_L ומוכל ב L. הוא נקרא **חוג שלמי־S**. חוג זה הנו מְקוּם של O בקבוצה הכפלית $T = \bigcap_{\mathfrak{p} \in \mathcal{P}_L \smallsetminus S}(O_L \smallsetminus P_\mathfrak{p})$. ואכן, אם $\mathfrak{q} \in \mathcal{P}_L \smallsetminus S$, אזי $\mathcal{P}_\mathfrak{q} \cap (O_L \smallsetminus P_\mathfrak{q}) = \emptyset$ ולכן $P_\mathfrak{q} \cap T = \emptyset$. לפי למה ג.ז(ב), $T^{-1}P_\mathfrak{q}$ הוא אידאל נאות של $T^{-1}O_L$. יתר על כן, $(T^{-1}O_L)_{T^{-1}O_\mathfrak{q}} = O_\mathfrak{q}$. אם $\mathfrak{q} \in S$, נבחר לפי (1) מספר טבעי n ואבר $x \in O$ כך ש $P_\mathfrak{q}^n = xO_L$. אבר זה מקַיֵם $x \in P_\mathfrak{q} \smallsetminus \bigcup_{\mathfrak{p} \in \mathcal{P}_L \smallsetminus S} P_\mathfrak{p}$ ולכן שַיָךְ ל $P_\mathfrak{q} \cap T$. מלמה ג.ז(א) נובע ש $T^{-1}P_\mathfrak{q} = T^{-1}O_L$. מכל זה עולה שהאידאלים הראשוניים השונים מאפס של $T^{-1}O_L$ הנם מהצורה $T^{-1}P_\mathfrak{p}$ באשר $\mathfrak{p} \in \mathcal{P}_L \smallsetminus S$. לכן, לפי למה ג.א, $T^{-1}O_L = \bigcap_{\mathfrak{p} \in \mathcal{P}_L \smallsetminus S} O_\mathfrak{p} = O_{L,S}$.

ממה שהשגנו בסעיף הקודם, בצרוף למה ג.ז נובע:

למה ד.ג: *יהי* $\mathfrak{p} \in \mathcal{P}_L$. *נסמן* $P_\mathfrak{p} = M_\mathfrak{p} \cap O_L$.

(א) *אם* $\mathfrak{p} \in S$, *אזי* $P_\mathfrak{p}O_{L,S} = O_{L,S}$.

(ב) *לאידאלים הראשוניים השונים מאפס של* $O_{L,S}$ *יש הצורה* $M_\mathfrak{p} \cap O_{L,S} = P_\mathfrak{p}O_{L,S}$ *באשר* $\mathfrak{p}$ *עובר על אברי* $\mathcal{P}_L \smallsetminus S$.

(ג) *לכל אידאל* I *של* $O_{L,S}$ *מתקים* $I = (I \cap O_L)O_{L,S}$.

(ד) $O_{L,S}$ *הוא חוג דדקינד.*

למה ד.ד: *לכל תת קבוצה סופית S של $\mathcal{P}_L$ קימת תת קבוצה סופית S' המקיפה אותה כך ש $O_{L,S'}$ הנו חוג ראשי.*

הוכחה: ואכן, נבחר לפי (1) אידאלים $I_1,\dots,I_r$ של O_L המיצגים את $\mathcal{I}_L$ מודולו חבורת האידאלים השבורים הראשיים. יהיו $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ כל אברי $\mathcal{P}_L$ המעֹרבים ב $I_1,\dots,I_r$. לכל i נסמן $P_i = P_{\mathfrak{p}_i}$. תהי $S' = S \cup \{\mathfrak{p}_1,\dots,\mathfrak{p}_s\}$.

מלמה ד.ג(ג) נובע שמספיק להוכיח שלכל אידאל I של O_L האידאל $IO_{L,S'}$ של $O_{L,S'}$ הוא ראשי.

ואכן, קים j וקים $x \in L^\times$ כך ש $I = xI_j$. מהבניה נובע ש $I_j = \prod_{i=1}^s P_i^{k_i}$, באשר k_i מספרים שלמים אי שליליים. מלמה ד.ד(א) (עבור S' במקום S) נובע אפוא ש $IO_{L,S'} = xO_{L,S'}$. ∎

נסמן ב $U_{K,S}$ את חבורת האברים ההפיכים של $O_{L,S}$ ונניח:

(2) לכל תת קבוצה סופית S של $\mathcal{P}_L$ החבורה $U_{K,S}$ נוצרת סופית.

לשדה K יחד עם חוג דדקינד O המקים $K = \mathrm{Quot}(O)$ ואת תנאי הסופיות (1) ו (2) נקרא **שדה ארתמטי.** מההגדרות עולה שבמקרה זה כל הרחבה סופית פרידה L של K יחד עם O_L הנה שדה ארתמטי.

ד.ה תורת קומר. יהי m מספר טבעי שאינו כפולה של $\mathrm{char}(K)$. נניח ש K מקיף את חבורת שרשי היחידה μ_m מסדר m. זוהי חבורה מעגלית מסדר m. נבחר לה יוצר ζ_m. הרחבה L של K תכונה **הרחבה אבלית בעלת מעריך** m אם היא הרחבת גלואה ו $\mathrm{Gal}(L/K)$ היא חבורה אבלית בעלת מעריך m. כלומר $\sigma^m = 1$ לכל $\sigma \in \mathrm{Gal}(L/K)$ (ביתר דיוק צריך לומר „הרחבה אבלית בעלת מעריך המחלק את m"). אם B היא תת חבורה של $K^\times$ המקיפה את $(K^\times)^m$, אזי $B/(K^\times)^m$ היא חבורה אבלית בעלת מעריך m. לחבורה זו נתאים את ההרחבה האבלית $L = K(B^{1/m}) = K(\sqrt[m]{b} \mid b \in B)$. נסמן $G = \mathrm{Gal}(L/K)$ ו $\bar{B} = B/(K^\times)^m$. הפונקציה $\kappa\colon G \times \bar{B} \to \mu_m$ המוגדרת על ידי הנוסחה

$$\kappa(\sigma, \bar{b}) = \frac{\sigma\sqrt[m]{b}}{\sqrt[m]{b}}$$

שבה $\bar{b} = b(K^\times)^m$ הנה בילינארית ולא מנוונת. כלומר, κ הנה קודם כל כפלית בכל אחד משני המשתנים. שנית, אם $\sigma \in G$ מקים $\kappa(\sigma,\bar{b}) = 1$ לכל $b \in B$, אזי $\sigma = 1$. באפן דומה, אם $b \in B$ מקים $\kappa(\sigma,\bar{b}) = 1$ לכל $\sigma \in G$, אזי $\bar{b} = 1$. מכאן נובע ש G איזומורפי באפן קנוני ל $\mathrm{Hom}(\bar{B},\mu_m)$. לכן G איזומורפי (באפן לא קנוני) ל $\bar{B}$. בנוסף לזה, נשמרת κ תחת ההצמדה של המשתנה הראשון עם אברי G. כלומר, אם $\tau \in G$, אזי $\kappa(\tau^{-1}\sigma\tau,\bar{b}) = \kappa(\sigma,\bar{b})$.

אם C היא תת חבורה של $K^\times$ המקיפה את B כחבורה בעלת אנדקס סופי, אזי $L(B^{1/m}) \subseteq L(C^{1/m})$.

תורת קומר אומרת עוד שההתאמה $B \mapsto K(B^{1/m})$ היא חד חד ערכית על אסף כל ההרחבות האבליות של K בעלות מעריך m. הוכחות אפשר למצא ב [Lang, Chap. VII, §8].

למה ד.ו: *תהי v הערכה בדידה של שדה K, יהי $a \in K$ ויהי m מספר טבעי כך ש $v(m) = 0$. אזי v אינה מסעפת ב $K(\sqrt[m]{a})$ אם ורק אם $m|v(a)$.*

הוכחה: נסמן $x = \sqrt[m]{a}$ ו $L = K(x)$. אזי $x^m = a$.

נניח קודם ש $m \nmid v(a)$. יהי w הרחבה של v ל L ויהי $e = e(w/v)$. אזי $mw(x) = ev(a)$. לכן קים ל m גורם ראשוני p המחלק את e. בפרט $e \neq 1$ ולכן v מסעף ב L.

להפך, נניח שקים k שלם כך ש $v(a) = km$. נבחר אבר $c \in K$ כך ש $v(c) = 1$. אזי $u = ac^{-km}$ מקים $v(u) = 0$. עוד נסמן $y = xc^{-k}$. אזי $y^m = u$ ו $L = K(y)$. מההנחה ש $v(m) = 0$ נובע ש $m \nmid \mathrm{char}(\bar{K}_v)$. לכן לפולינום $Y^m - \bar{u}$ אין שרשים כפולים. מלמה ב.ח נובע ש v אינו מסעף ב L. ∎

משפטון ד.ז: *יהי K שדה ארתמטי. תהי S תת קבוצה סופית של $\mathcal{P}_K$ ויהי $m \geq 2$ מספר טבעי שאינו כפולה של $\mathrm{char}(K)$. אזי ההרחבה האבלית המרבית של K בעלת מעריך m המסעפת לכל היותר מעל S הנה סופית.*

הוכחה: נסמן את ההרחבה האבלית המרבית של K בעלת מעריך m המסעפת לכל היותר מעל S ב $K_S^{(m)}$. יהי L הרחבה סופית של K. נסמן ב S' את אסף כל המחלקים הראשוניים של L השוכנים מעל לאברי S. אזי $K_S^{(m)}L$ היא הרחבה אבלית בעלת מעריך m המסעפת לכל היותר מעל S' (משפטון ב.יד) ולכן היא מוכלת ב $L_{S'}^{(m)}$. אלו היינו יודעים ש $[L_{S'}^{(m)} : L] < \infty$, היינו יכולים להסיק ש $[K_S^{(m)} : K] < \infty$.

נפעיל אפוא עקרון זה במדת הצרך לגבי השדה $K(\mu_m)$, כדי להניח ש $\mu_m \subseteq K$.

שנית נעיר שאם T היא תת קבוצה סופית של $\mathcal{P}_K$ המקיפה את S, אזי $K_S^{(m)} \subseteq K_T^{(m)}$. לכן, לפי למה ד.ד, נוכל להגדיל את S במדת הצרך כדי להניח ש $O_{K,S}$ הוא חוג ראשי וכן ש $v_\mathfrak{p}(m) = 0$ לכל $\mathfrak{p} \notin S$ (O_K הנו חוג דדקינד).

לפי תורת קומר, $K_S^{(m)}$ היא צרוף כל ההרחבות $K(\sqrt[m]{b})$ המסעפות לכל היותר מעל S. לפי למה ד.ו, מחלק ראשוני $\mathfrak{p}$ של K אינו מסעף ב $K(\sqrt[m]{b})$ אם ורק אם $m|v_\mathfrak{p}(b)$. לכן, $K_S^{(m)} = K(B^{1/m})$, באשר $B = \{b \in K^\times \mid m|v_\mathfrak{p}(b) \text{ for all } \mathfrak{p} \notin S\}$. מתורת קומר נובע אפוא שמספיק להוכיח שהחבורה $B/(K^\times)^m$ סופית.

טענה: *ההומומורפיזם $u \mapsto u(K^\times)^m$ מעתיק את $U_{K,S}$ על $B/(K^\times)^m$.* ואכן, יהי $b \in B$. אזי קים אידאל שבור I של $O_{K,S}$ כך ש $bO_{K,S} = \prod P_\mathfrak{p}^{v_\mathfrak{p}(b)}O_{K,S} = I^m$. מבחירת S נובע שקים $a \in K^\times$ כך ש $aO_{K,S} = I$. לכן $bO_{K,S} = a^mO_{K,S}$ ולכן קים $u \in U_{K,S}$ כך ש $b = ua^m$.

לפי (5), $U_{K,S}$ נוצרת סופית. לכן, לפי הטענה, גם $B/(K^\times)^m$ נוצרת סופית. הואיל והמעריך של $B/(K^\times)^m$ סופי, חבורה זו סופית. ∎

ה. המשפט הַחַלָּש של מורדל־וייל

יהי K שדה ארתמטי. נסמן ב $\mathcal{L}$ את הקטגוריה של ההרחבות האלגבריות של K יחד עם איזומורפיזמים־K. יהי A פנקטור מ $\mathcal{L}$ לקטגוריות החבורות האבליות. לכל $L \in \mathcal{L}$ $A(L)$ הוא אפוא חבורה אבלית. לשכון־K $\sigma\colon L \to L'$ בין שני שדות ב $\mathcal{L}$ יתאים שכון $\sigma\colon A(L) \to A(L')$ (בעל אותו שם) של חבורות אבליות. בפרט יתקיים

$(1a)$ אם $L \xrightarrow{\sigma} L' \xrightarrow{\tau} L''$, אזי $\tau(\sigma(\mathbf{p})) = (\tau\sigma)(\mathbf{p})$ לכל $\mathbf{p} \in A(L)$.

$(1b)$ להעתקת הזהות $L \to L$ תתאים העתקת הזהות $A(L) \to A(L)$.

$(1c)$ אם L/K הרחבת גלואה, $\sigma \in \mathrm{Gal}(L/K)$ ו $\mathbf{p}, \mathbf{q} \in A(L)$, אזי $\sigma(\mathbf{p}+\mathbf{q}) = \sigma\mathbf{p} + \sigma\mathbf{q}$.

בנוסף לזה נדרש:

$(1d)$ אם $L \subseteq L'$, אזי $A(L) \subseteq A(L')$. בפרט אם $L \subseteq K_s$, אזי $A(L) \subseteq A(K_s)$ (K_s הנו הסגור הפריד של K).

$(1e)$ $A\bigl(\bigcap_{i\in I} L_i\bigr) = \bigcap_{i\in I} A(L_i)$.

$(1f)$ לכל $N \in \mathcal{L}$ החבורה $A(N)$ הנה האחוד של כל החבורות $A(L)$ באשר L עובר על כל ההרחבות הסופיות של K המוכלות ב N.

$(1g)$ יהי N הרחבת גלואה של K, יהי $K \subseteq L \subseteq N$ שדה ויהי $\mathbf{p} \in A(N)$. אזי $\sigma\mathbf{p} = \mathbf{p}$ לכל $\sigma \in \mathrm{Gal}(N/L)$ אם ורק אם $\mathbf{p} \in A(L)$.

לכל נְקֻדה $\mathbf{p} \in A(K_s)$ ולכל $K' \in \mathcal{L}$ נסמן ב $K'(\mathbf{p})$ את החתוך של כל השדות $L \in \mathcal{L}$ שעבורם $K' \subseteq L$ ו $\mathbf{p} \in A(L)$. מ $(1e)$ ו $(1f)$ נובע ש $K'(\mathbf{p})$ הוא השדה הקטן ביותר בעל תכונה זו. יתר על כן, $K'(\mathbf{p})$ הוא הרחבה פרידה סופית של K'. כמן כן נקבל ש $\sigma K'(\mathbf{p}) = K'(\sigma\mathbf{p})$ לכל $\sigma \in \mathrm{Gal}(K')$.

לכל תת קבוצה $P \subseteq A(K_s)$ נסמן ב $K'(P)$ את הצרוף של כל השדות $K'(\mathbf{p})$ שבהם $\mathbf{p} \in P$. אם P קבוצה סופית, אזי $K'(P)$ הנו הרחבה סופית של K'. אם בנוסף לזה $\mathrm{Gal}(K')$ שומרת את P, אזי $K'(P)/K'$ היא הרחבת גלואה.

יהי עתה m מספר טבעי הגדול או שוה ל 2 ומקיים $\mathrm{char}(K) \nmid m$. כפל ב m מגדיר עבור כל $L \in \mathcal{L}$ הומומורפיזם $\mathrm{mult}_m\colon A(L) \to A(L)$. נסמן את גרעינו ב $A_m(L)$. נניח:

$(2a)$ $A_m(K_s)$ היא חבורה סופית.

$(2b)$ mult_m מעתיק את $A(K_s)$ על $A(K_s)$.

בפרט השדה $K(A_m)$ המוגדר כ $K(A_m(K_s))$ הוא הרחבת גלואה סופית של K.

למה ה.א: *תהי L הרחבת גלואה סופית של K. אם $A(L)/mA(L)$ הנה חבורה סופית, אזי גם $A(K)/mA(K)$ סופית.*

הוכחה: ההכלה $A(K) \subseteq A(L)$ משרה סדרה מדויקת:

$$0 \to (A(K) \cap mA(L))/mA(K) \to A(K)/mA(K) \to A(L)/mA(L).$$

כדי להוכיח את הלמה, מספיק אפוא שנוכיח שהחבורה $(A(K) \cap mA(L))/mA(K)$ סופית.

לצרך זה נבחר לכל $\bar{\mathbf{p}} \in (A(K) \cap mA(L))/mA(K)$ נקֻדה $\mathbf{p} \in A(K) \cap mA(L)$ המיצגת אותה. עתה נבחר נקֻדה $\mathbf{q_p} \in A(L)$ המקימת $m\mathbf{q_p} = \mathbf{p}$. ולכל $\sigma \in \mathrm{Gal}(L/K)$ נסמן $\lambda_{\mathbf{p}}(\sigma) = \sigma\mathbf{q_p} - \mathbf{q_p}$. אזי $m\lambda_{\mathbf{p}}(\sigma) = \sigma(m\mathbf{q_p}) - mq_{\mathbf{p}} = \sigma\mathbf{p} - \mathbf{p} = 0$. אנו מקבלים באפן כזה העתקה $\lambda_{\mathbf{p}} \colon \mathrm{Gal}(L/K) \to A_m(L)$ (התלויה בבחירת $\mathbf{q_p}$).

אם $\mathbf{p}'$ היא נקֻדה נוספת של $A(K) \cap mA(L)$ ו $\lambda_{\mathbf{p}} = \lambda_{\mathbf{p}'}$, אזי $\sigma\mathbf{q_p} - \mathbf{q_p} = \sigma\mathbf{q_{p'}} - \mathbf{q_{p'}}$ ולכן $\sigma(\mathbf{q_p} - \mathbf{q_{p'}}) = \mathbf{q_p} - \mathbf{q_{p'}}$ לכל $\sigma \in \mathrm{Gal}(L/K)$. לכן, $\mathbf{q_p} - \mathbf{q_{p'}} \in A(K)$ ולכן, $\mathbf{p} - \mathbf{p}' \in mA(K)$.

ההתאמה $\bar{\mathbf{p}} \mapsto \lambda_{\mathbf{p}}$ מעתיקה אפוא את $A(K) \cap mA(L)/mA(K)$ באפן חד חד ערכי לתוך הקבוצה $\mathrm{Map}\big(\mathrm{Gal}(L/K) \to A_m(L)\big)$ הואיל וגם $\mathrm{Gal}(L/K)$ וגם $A_m(L)$ הן קבוצות סופיות, נובע מכאן ש $A(K) \cap mA(L)$ היא חבורה סופית, כמבוקש. ∎

מלמה ה.א ומ $(2a)$ נובע שכדי להוכיח ש $A(K)/mA(K)$ הוא חבורה סופית, אפשר להניח ש

$(3a)$ $A_m(K_s) = A_m(K)$.

מהנחה זו נובע:

$(3b)$ אם $\mathbf{q} \in A(K_s)$ ו $m\mathbf{q} \in A(K)$, אזי $K(\mathbf{q})/K$ היא הרחבה אבלית בעלת מעריך m.

ואכן, אם $\sigma \in \mathrm{Gal}(K)$, אזי $m\sigma\mathbf{q} = \sigma(m\mathbf{q}) = m\mathbf{q}$. לכן, $m(\sigma\mathbf{q} - \mathbf{q}) = 0$. לכן, לפי $(3a)$, $\sigma\mathbf{q} - \mathbf{q} \in A(K)$. בפרט $\sigma\mathbf{q} \in A(K(\mathbf{q}))$ ולכן $K(\mathbf{q})/K$ הנה הרחבת גלואה.

אם $\sigma \in \mathrm{Gal}(K(\mathbf{q})/K)$, אזי $\sigma\mathbf{q} - \mathbf{q} = \mathbf{a}(\sigma) \in A_m(K)$. אם $\tau \in \mathrm{Gal}(K(\mathbf{q})/K)$, אזי

$$\mathbf{a}(\sigma\tau) = \sigma\tau\mathbf{q} - \mathbf{q} = \sigma(\mathbf{q} + \mathbf{a}(\tau)) - \mathbf{q} = \sigma\mathbf{q} - \mathbf{q} + \mathbf{a}(\tau) = \mathbf{a}(\sigma) + \mathbf{a}(\tau)$$

לכן ההעתקה $\sigma \mapsto \mathbf{a}(\sigma)$ הנה הומומורפיזם של $\mathrm{Gal}(K(\mathbf{q})/K)$ לתוך $A_m(K)$.

אם $\mathbf{a}(\sigma) = 0$, אזי $\sigma\mathbf{q} = \mathbf{q}$. נסמן ב L_0 את שדה השבת של σ ב $K(\mathbf{q})$. הוא יקים $\tau\mathbf{q} = \mathbf{q}$ לכל $\tau \in \mathrm{Gal}(L_0)$. לכן, לפי $(1g)$, $\mathbf{q} \in A(L_0)$. מהגדרת $K(\mathbf{q})$ נובע ש $L_0 = K(\mathbf{q})$. לכן $\sigma = 1$.

מכאן ש $\mathrm{Gal}(K(\mathbf{q})/K)$ חבורה אבלית בעלת מעריך m.

בהנחות אלו נגדיר פונקציה

$$\kappa \colon A(K) \times \mathrm{Gal}(K) \to A_m(K)$$

בשיטה דומה לזו שהשתמשנו בה בהוכחת למה ה.א. עבור $\mathbf{p} \in A(K)$ נבחר על סמך $(2b)$ נקֻדה $\mathbf{q} \in A(K_s)$ כך ש $m\mathbf{q} = \mathbf{p}$, ונגדיר עבור כל $\sigma \in \mathrm{Gal}(K)$

$$.\kappa(\mathbf{p}, \sigma) = \sigma\mathbf{q} - \mathbf{q}$$

נקרא ל κ **זווג Kummer**.

למה ה.ב:

(א) *זווג קומר מוגדר היטב.*

(ב) *זווג קומר הנו בי־לינארי.*

(ג) *הגרעין של זווג קומר במשתנה השמאלי הנו* $mA(K)$.

(ד) *הגרעין של זווג קומר במשתנה הימני הנו* $\mathrm{Gal}(N)$ *באשר* $N = K(\frac{1}{m}A(K))$ *הוא צרוף כל השדות* $K(\mathbf{q})$ *שעבורם* $\mathbf{q} \in A(K_s)$ *ו* $m\mathbf{q} \in A(K)$.

הוכחת (א): עלינו להוכיח קודם כל שבסימונים של הגדרת זווג קומר, $\kappa(\mathbf{p}, \sigma) \in A_m(K)$. ואכן,

$$.m\kappa(\mathbf{p}, \sigma) = \sigma(m\mathbf{q}) - m\mathbf{q} = \sigma\mathbf{p} - \mathbf{p} = 0$$

שנית, עלינו להוכיח שההגדרה אינה תלויה בנקֻדה $\mathbf{q}$. ואכן, אם $\mathbf{q}'$ היא נקֻדה אחרת ב $A(K_s)$ כך ש $m\mathbf{q}' = \mathbf{p}$, אזי $m(\mathbf{q}' - \mathbf{q}) = 0$ ולכן, לפי $(3a)$, $\mathbf{q}' - \mathbf{q} \in A_m(K_s) \subseteq A(K)$. לכן, $\sigma(\mathbf{q}' - \mathbf{q}) = \mathbf{q}' - \mathbf{q}$ ולכן, $\sigma\mathbf{q}' - \mathbf{q}' = \sigma\mathbf{q} - \mathbf{q}$.

הוכחת (ב): נצא מ $\mathbf{p}_1, \mathbf{p}_2 \in A(K)$ ונבחר $\mathbf{q}_1, \mathbf{q}_2 \in A(K_s)$ כך ש $m\mathbf{q}_1 = \mathbf{p}_1$ ו $m\mathbf{q}_2 = \mathbf{p}_2$. אזי $m(\mathbf{q}_1 + \mathbf{q}_2) = \mathbf{p}_1 + \mathbf{p}_2$ ולכן,

$$\begin{aligned}\kappa(\mathbf{p}_1 + \mathbf{p}_2, \sigma) &= \sigma(\mathbf{q}_1 + \mathbf{q}_2) - (\mathbf{q}_1 + \mathbf{q}_2)\\ &= (\sigma\mathbf{q}_1 - \mathbf{q}_1) + (\sigma\mathbf{q}_2 - \mathbf{q}_2) = \kappa(\mathbf{p}_1, \sigma) + \kappa(\mathbf{p}_2, \sigma)\end{aligned}$$

כדי להוכיח את הלינאריות במשתנה הימני של κ, נתבונן ב $\tau \in \mathrm{Gal}(K)$. אזי

$$.\kappa(\mathbf{p}, \tau\sigma) = \tau\sigma\mathbf{q} - \mathbf{q} = \tau(\sigma\mathbf{q} - \mathbf{q}) + (\tau\mathbf{q} - \mathbf{q}) = \tau\kappa(\mathbf{p}, \sigma) + \kappa(\mathbf{p}, \tau) = \kappa(\mathbf{p}, \sigma) + \kappa(\mathbf{p}, \tau)$$

הוכחת (ג): נניח ש $\mathbf{p} \in A(K)$ מקים, $\kappa(\mathbf{p}, \sigma) = 0$ עבור כל $\sigma \in \mathrm{Gal}(K)$. יהי $\mathbf{q} \in A(K_s)$ כך ש $m\mathbf{q} = \mathbf{p}$. אזי $\sigma\mathbf{q} = \mathbf{q}$ לכל $\sigma \in \mathrm{Gal}(K)$. לכן, $\mathbf{q} \in A(K)$ ולכן $\mathbf{p} \in mA(K)$. להפך, כל $\mathbf{p} \in mA(K)$ נמצא בגרעין השמאלי של κ.

הוכחת (ד): יהי $\sigma \in \mathrm{Gal}(K)$ אבר בגרעין הימני של κ. אזי לכל $\mathbf{q} \in A(K_s)$ המקים $m\mathbf{q} \in A(K)$ מתקים $\sigma\mathbf{q} = \mathbf{q}$ ולהפך. ∎

השדה $N = K(\frac{1}{m}A(K))$ הנו הרחבת גלואה של K. מהלמה עולה שזווג קומר משרה זווג לא מנוון

$$\bar{\kappa}\colon A(K)/mA(K) \times \mathrm{Gal}(N/K) \to A_m(K)$$

דהיינו, $\bar{\kappa}$ הנו תבנית בי־לינארית לא מנוונת. בעזרתה אפשר להגדיר שכון

$$\Lambda\colon A(K)/mA(K) \to \mathrm{Hom}(\mathrm{Gal}(N/K), A_m(K)) \tag{4}$$

לכל $\mathbf{p} \in A(K)$ ולכל $\sigma \in \mathrm{Gal}(N/K)$ מגדירים $\Lambda(\mathbf{p} + mA(K))(\sigma) = \bar{\kappa}(\mathbf{p}, \sigma)$. אם נראה שההרחבה N/K סופית, נקבל שאגף ימין של (4) סופי. מכאן ינבע שגם אגף שמאל של (4) סופי. בזאת תסתים הוכחת המשפט החלש של מורדל־וייל עבור m.

עתה נרצה להפעיל את משפטון ד.ז על תת קבוצה סופית מתאימה S של $\mathcal{P}_K$. לצרך זה נצטרך להרחיב את הפנקטור A.

(5) **העמדה טובה של** A. קימת תת קבוצה סופית $\mathrm{Bad}_K(A,m)$ של $\mathcal{P}_K$, כך ש לכל הרחבה פרידה סופית L של K ולכל מחלק ראשוני $\mathfrak{q}$ של L שאינו מונח מעל $\mathrm{Bad}_K(A,m)$ קימת קימת חבורה $A(\bar{L}_\mathfrak{q})$ והומומורפיזם $\mathrm{red}_\mathfrak{q}\colon A(L) \to A(\bar{L}_\mathfrak{q})$ באפן ש

$(5a)$ אם $v_\mathfrak{q}(m) = 0$ אזי $\mathrm{red}_\mathfrak{q}$ מעתיק את $A_m(L)$ באפן חד חד ערכי לתוך $A_m(\bar{L}_\mathfrak{q})$. נסמן $\mathrm{red}_\mathfrak{q}(\mathbf{q}) = \bar{\mathbf{q}}$.

$(5b)$ אם L' היא הרחבה פרידה סופית של L ו $\mathfrak{q}'$ הוא מחלק ראשוני של L' השוכן מעל $\mathfrak{q}$, אזי $A(\bar{L}_\mathfrak{q}) \subseteq A(\bar{L}'_{\mathfrak{q}'})$ והצמצום של $\mathrm{red}_{\mathfrak{q}'}$ ל $A(L)$ שוה ל $\mathrm{red}_\mathfrak{q}$.

$(5c)$ אם בנוסף לזה L היא הרחבת גלואה של K, אזי $\mathrm{Aut}(\bar{L}_\mathfrak{q}/\bar{K}_\mathfrak{p})$ פועלת על $A(\bar{L}_\mathfrak{q})$. יתר על כן אם $\sigma \in D(\mathfrak{q}/\mathfrak{p})$ ו $\bar{\sigma}$ הוא התמונה של σ תחת ההעתקה $D(\mathfrak{q}/\mathfrak{p}) \to \mathrm{Aut}(\bar{L}_\mathfrak{q}/\bar{K}_\mathfrak{p})$ המוזכרת בסעיף ב.י, אזי $\overline{\sigma\mathbf{q}} = \bar{\sigma}\bar{\mathbf{q}}$ לכל $\mathbf{q} \in A(L)$ (בהמשך נאמר שיש ל A **העמדה טובה ב** $\mathfrak{p}$).

למה ה.ג: *יהי* $S = \mathrm{Bad}_K(A,m) \cup \{\mathfrak{p} \in \mathcal{P}_K \mid v_\mathfrak{p}(m) \neq 0\}$. *נניח ש* $A_m(K) = A_m(K_s)$. *אזי השדה* $N = K(\frac{1}{m}A(K))$ *מסעף לכל היותר מעל* S.

הוכחה: יהי $\mathfrak{p} \in \mathcal{P}_K \smallsetminus S$. תהי $\mathbf{p}$ נקֻדה ב $A(K)$. נבחר $\mathbf{q} \in A(K_s)$ כך ש $m\mathbf{q} = \mathbf{p}$. נסמן $L = K(\mathbf{q})$. מ $(3a)$ נובע ש L הרחבת גלואה סופית של K. ממשפטון ב.יד(ב) נובע שמספיק להוכיח ש $\mathfrak{p}$ אינו מסעף ב L.

ואכן, יהי $\mathfrak{q}$ מחלק ראשוני של L המונח מעל $\mathfrak{p}$. תת סעיף ב.י אומר שמספיק להוכיח ש $I(\mathfrak{q}/\mathfrak{p}) = 1$.

יהי $\sigma \in I(\mathfrak{q}/\mathfrak{p})$. אזי $\bar{\sigma} = 1$. לפי $(5c)$, $\overline{\sigma\mathbf{q}} = \bar{\sigma}\bar{\mathbf{q}} = \bar{\mathbf{q}}$. הואיל וגם $m\sigma\mathbf{q} = \mathbf{p}$, נקבל מ $(3a)$ ש

$A_m(K) \ni \sigma\mathbf{q}-\mathbf{q}$ ו $\overline{\sigma\mathbf{q}-\mathbf{q}}=0$. לכן, לפי $(5a)$, $\sigma\mathbf{q}=\mathbf{q}$. הואיל ושויון זה נכון לכל $\mathbf{q}$ כנ"ל, $\sigma=1$. לכן $I(\mathfrak{q}/\mathfrak{p})=1$ וכך $\mathfrak{q}/\mathfrak{p}$, אינו מסעף. ∎

משפטון ה.ד (המשפט הַחַלש של מורדל־וויל): *יהי K שדה ארתמטי ו A פנקטור אבלי המקים את הדרישות (1), (2) ו (5) של סעיף זה. יהי $m \geq 2$ מספר טבעי שאינו מתחלק ב $\mathrm{char}(K)$. אזי $A(K)/mA(K)$ היא חבורה סופית.*

הוכחה: מלמה ה.א נובע שנתן להניח, בלי הגבלת הכלליות, ש $A(K) \subseteq A_m(K_s)$. יהי $N=K(\frac{1}{m}A(K))$. לפי טענה $(3b)$, N הוא הרחבה אבלית של K בעלת מעריך m. לפי למה ה.ג, N מסעף לכל היותר מעל הקבוצה הסופית S הנזכרת באותה למה. לכן, לפי משפטון ד.ז, N/K היא הרחבה סופית. מהשכון (4) נובע ש $A(K)/mA(K)$ הוא חבורה סופית. ∎

ו. חשובים בפולינום ממעלה שלישית

החשובים שנבצע בסעיף זה יהוו בסיס לודוי תכונותיהם של העקומים האלפטיים שנחקר בסעיף הבא.

יהי אפוא K שדה ויהיו a, b אברים ב K. נתבונן בפולינום

$$f(X) = X^3 + aX + b \tag{1}$$

ונפרק אותו לגורמים לינאריים מעל $\tilde{K}$:

$$f(X) = (X - \xi_1)(X - \xi_2)(X - \xi_3) \tag{2}$$

נסמן $\delta = (\xi_2 - \xi_1)(\xi_3 - \xi_1)(\xi_3 - \xi_2)$. אזי $\Delta = -\delta^2$ הוא **הדיסקרימיננטה** של $f(X)$. בפרט $\Delta \neq 0$ אם ורק אם ξ_1, ξ_2, ξ_3 שונים זה מזה. הואיל ו Δ הוא פולינום סימטרי ב ξ_1, ξ_2, ξ_3 אפשר להביע אותו כפולינום במקדמי $f(X)$, כלומר ב a, b.

למה ו.א: $\delta^2 = -4a^3 - 27b^2$.

הוכחה: נתבונן במטריצת ונ־דר־מונדה:

$$M = \begin{pmatrix} 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 \\ \xi_1^2 & \xi_2^2 & \xi_3^2 \end{pmatrix}$$

כידוע $\det(M) = \delta$. לכל $k \geq 0$ נסמן $p_k = \sum_{i=0}^{3} \xi_i^k$. כידוע הדטרימננטה של המטריצה המוחלפת M^t שוה לדטרמיננטה של M. לכן

$$\delta^2 = \det(MM^t) = \begin{vmatrix} 3 & p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{vmatrix} \tag{3}$$

מ (1) ו (2) נובע ש

$$\xi_1\xi_2\xi_3 = -b, \quad \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = a, \quad \xi_1 + \xi_2 + \xi_3 = 0 \tag{4}$$

לכן $p_1 = 0$ ו $p_2 = p_1^2 - 2a = -2a$. כדי לחשב את p_3 נשתמש בכך ש ξ_i הוא שרש של $f(X)$ ולכן

$$\xi_i^3 = -a\xi_i - b, \qquad i = 1, 2, 3 \tag{5}$$

לכן $p_3 = -3b$. עתה נכפיל את (5) ב ξ_i

$$\xi_i^4 = -a\xi_i^2 - b\xi_i \qquad i = 1, 2, 3$$

ונסכם כדי לקבל $p_4 = -ap_2 - bp_1 = 2a^2$. אם נציב את כל הערכים האלו ב (3) ונחשב את הדטרימיננטה המתקבלת נקבל

$$\delta^2 = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = -4a^3 - 27b^2$$

כנדרש. ∎

למה ו.ב: *עבור* $\Delta = 4a^3 + 27b^2$ *מקימים הפולינומים*

$$F(X,Z) = X^4 - 2aX^2Z^2 - 8bXZ^3 + a^2Z^4$$

$$G(X,Z) = 4X^3Z + 4aXZ^3 + 4bZ^4$$

$$f_1(X,Z) = 12X^2Z + 16aZ^3$$

$$g_1(X,Z) = 3X^3 - 5aXZ^2 - 27bZ^3$$

$$f_2(X,Z) = 4(4a^3 + 27b^2)X^3 - 4a^2bX^2Z + 4a(3a^3 + 22b^2)XZ^2 + 12b(a^3 + 8b^2)Z^3$$

$$g_2(X,Z) = a^2bX^3 + a(5a^3 + 32b^2)X^2Z + 2b(13a^3 + 96b^2)XZ^2 - 3a^2(a^3 + 8b^2)Z^3$$

את הזהויות הבאות ב $\mathbb{Q}[a,b,X,Z]$:

$$f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7 \tag{6a}$$

$$f_2(X,Z)F(X,Z) + g_2(X,Z)G(X,Z) = 4\Delta X^7 \tag{6b}$$

הוכחה: אם נראה את הפולינומים הנ"ל כפולינומים ב X, Z עם מקדמים בחוג $\mathbb{Q}[a,b]$ נמצא שכלם הומוגניים. לכן הזהויות (6) שקולות לזהויות המתקבלות על ידי הצבת 1 במקום Z בכל מקום. את הזהויות במשתנה X נתן לבדק על ידי חשוב ידני או על ידי שמוש בתכנה מתמטית מתאימה, למשל Maple. ∎

מסקנה ו.ג: *אם* a, b *הם אברים של שדה* K *כך ש* $\mathrm{char}(K) \neq 2$ *ו* $\Delta = 4a^3 + 27b^2 \neq 0$*, אזי הפולינומים* $X^4 - 2aX^2 - 8bX + a^2$ *ו* $X^3 + aX + b$ *של* $K[X]$ *זרים זה לזה.*

ז. חק החבור של עקומים אלפטיים

הדגמה המענינת היחידה שנביא ברשימות אלו לפנקטור אבלי המקים את כל הדרישות תהיה זו של עקם אלפטי.

יהי אפוא K שדה בעל אפיון שונה מ 2 ומ 3. לכל שני אברים a, b של K המשואה

$$Y^2 = X^3 + aX + b \tag{1}$$

מגדירה עקם מישורי E. עקם זה יהיה, לפי ההגדרה, הפנקטור המתאים לכל שדה הרחבה L של K את הקבוצה $E(L) = \{\infty\} \cup \{(x, y) \in L^2 \mid\ y^2 = x^3 + ax + b\}$. כל אבר של $E(L)$ יקרא **נקודה רציונלית־**L של E. הנקודה ∞, תקרא **נקֻדת האינסוף** של $E(L)$. שאר הנקודות תכֻנינה **סופיות**. אם L' הוא שדה המקיף את L אזי $E(L')$ מקיף את $E(L)$.

באפן דומה נוכל להגדיר את **המישור האפיני** $\mathbb{A}^2$ כפנקטור המתאים לכל L כנ"ל את קבוצת הנקודות $\mathbb{A}^2(L) = L^2$. את המשתנים x ו y נראה גם כפונקציות מ $\mathbb{A}^2$ ל $\mathbb{A}^1$. בהנתן נקודה $\mathbf{p}$ של $\mathbb{A}^2(L)$ תהיה $x(\mathbf{p})$ הקאורדינטה הראשונה של $\mathbf{p}$ ו $y(\mathbf{p})$ תהיה הקואורדינטה השניה שלה.

את המישור האפיני נשכֵן במישור הפרויקטיבי $\mathbb{P}^2(L)$. הוא יהיה קבוצת מחלקות השקילות של השלישיות (x_0, x_1, x_2) של אברי L שלא כלן אפס. שתי שלישיות (x_0, x_1, x_2) ו (x'_0, x'_1, x'_2) **שקולות זו לזו** אם קים $a \in L^\times$ כך ש $x'_i = ax_i$ עבור $i = 0, 1, 2$. נסמן את מחלקת השקילות של (x_0, x_1, x_2) ב $(x_0{:}x_1{:}x_2)$. אסף כל מחלקות השקילות האלו יסומן ב $\mathbb{P}^2(L)$. הפנקטור $\mathbb{P}^2$ המוגדר באפן כזה נקרא **המישור הפרויקטיבי.** כל נקודה של $\mathbb{P}^2(L)$ מהצורה $(0{:}x_1{:}x_2)$ תקרא **נקודה אינסופית,** שאר הנקודות תכונינה **סופיות.** ההעתקה $(x_0{:}x_1{:}x_2) \to (\frac{x_1}{x_0}, \frac{x_2}{x_0})$ מעתיקה את קבוצת הנקודות הסופיות של $\mathbb{P}^2(L)$ באפן חד חד ערכי על הקבוצה $\mathbb{A}^2(L)$. ההעתקה ההפוכה הנה $(x, y) \mapsto (1{:}x{:}y)$.

בפרט, מעתיק השכון של $\mathbb{A}^2(L)$ לתוך $\mathbb{P}^2(L)$ את קבוצת הנקודות הסופיות של $E(L)$ על קבוצת הנקודות הסופיות של העקם הפרויקטיבי המוגדר על ידי המשואה

$$X_0X_2^2 = X_1^3 + aX_0^2X_1 + bX_0^3 \tag{2}$$

יתר על כן, הנקודה האינסופית היחידה של $\mathbb{P}^2(L)$ המקימת את המשואה (2) הנה $(0{:}0{:}1)$. זוהי נקֻדת האינסוף של כל הישרים המקבילים לציר ה Y־ים. לכן, נזהה את $E(L)$ במדת הצרך גם עם קבוצת כל נקודות $\mathbb{P}^2(L)$ המקימות את (2) ובזהוי זה יתאים ∞ ל $(0{:}0{:}1)$.

יהי

$$f(X) = X^3 + aX + b, \qquad \Delta = \Delta_E = 4a^3 + 27b^2 \tag{3}$$

$$\Delta = -(\zeta_2-\zeta_1)^2(\zeta_3-\zeta_2)^2(\zeta_3-\zeta_1)^2 \quad \text{ו} \quad f(X)=(X-\zeta_1)(X-\zeta_2)(X-\zeta_3) \qquad (4)$$

Δ תקרא ה**דסקרימיננטה** של E. אנו נניח מכאן ואילך ש $\Delta \neq 0$, כלומר ש ζ_1,ζ_2,ζ_3 שונים זה מזה. בהנחה זו יקרא הפנקטור E **עקם אלפטי**.

נסמן $h(X_0,X_1,X_2) = X_1^3 + aX_0^2X_1 + bX_0^3 - X_0X_2^2$. נחשב את הנגזרות החלקיות של h:

$$\frac{\partial h}{\partial X_0} = 2aX_0X_1 + 3bX_0^2 - X_2^2 \qquad \frac{\partial h}{\partial X_1} = 3X_1^2 + aX_0^2 \qquad \frac{\partial h}{\partial X_2} = -2X_0X_2$$

נקודה $(x_0{:}x_1{:}x_2)$ של $E(L)$ תכונה **חריגה** (**סנגולרית**) אם שלש הנגזרות החלקיות של h מתאפסות בה:

$$2ax_0x_1 + 3bx_0^2 - x_2^2 = 0 \qquad 3x_1^2 + ax_0^2 = 0 \qquad -2x_0x_2 = 0$$

כל נקודה אחרת של $E(L)$ תקרא **פשוטה**. מההנחה $\Delta \neq 0$ נובע שכל נקודות $E(L)$ פשוטות. במלים אחרות, E הנו עקם **חלק**.

ואכן, תהי $(x_0{:}x_1{:}x_2)$ נקודה חריגה של $E(L)$. אם $x_0 = 0$, אזי גם $x_1 = 0$ ו $x_2 = 0$, סתירה. במקרה $x_0 \neq 0$ נוכל להניח (על ידי חלוקה ב x_0) ש $x_0 = 1$. אזי $x_2 = 0$, $x_1^3 + ax_1 + b = 0$ ו $2ax_1 + 3b = 0$. אם $a = 0$, אזי גם $b = 0$ (כי $3 \neq 0$) ולכן $\Delta = 0$, סתירה. לכן $a \neq 0$. אם $b = 0$, אזי $a = 0$ או $x_1 = 0$. לכן $a = 0$, סתירה. לכן $b \neq 0$. נציב אפוא $x_1 = -\frac{3b}{2a}$ במשואה הראשונה ונקבל $-\Delta = -27b^2 - 4a^3 = 0$, בסתירה להנחה.

יהי Λ ישר ב $\mathbb{P}^2$ המוגדר מעל $\tilde{K}$. הואיל ו E מֻגדר על ידי עקֹם ממעלה 3, חולק $\Lambda(\tilde{K})$ את $E(\tilde{K})$ לכל היותר בשלש נקודות שונות: $\Lambda(\tilde{K}) \cap E(\tilde{K}) = \{\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3\}$. יש כמה אפשרויות:

$(5a)$ $\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3$ שונות זו מזו. אם $\mathbf{p}_1$ ו $\mathbf{p}_2$ רציונליות־L, אזי Λ מוגדר מעל L ו $\mathbf{p}_3$ רציונלי־L.

$(5b)$ אם $\mathbf{p}_1 = \mathbf{p}_2$, אזי Λ משיק ל E ב $\mathbf{p}_1$. אם בנוסף לזה $\mathbf{p}_1$ רציונלי־L, אזי Λ מוגדר מעל L ו $\mathbf{p}_3$ רציונלי־L.

$(5c)$ אם $\mathbf{p}_1 = \mathbf{p}_2 = \mathbf{p}_3$, אזי $\mathbf{p}_1$ הוא **נְקדת פתול** של E. כלומר, המשיק ל E ב $\mathbf{p}_1$ חותך את E ברבוי 3.

ההנחה $\Delta \neq 0$ מאפשרת גם להפך את E לפנקטור אבלי. ביתר דיוק, אפשר להפך את $E(L)$ לחבורה חבורית חלופית באפן שפעולת חבור תקים את הכללים הבאים:

$(6a)$ נְקדת האינסוף הנה אבר האפס של $E(L)$.

$(6b)$ שלש נקודות שונות $\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3$ של $E(L)$ מונחות על ישר אחד אם ורק אם $\mathbf{p}_1 + \mathbf{p}_2 + \mathbf{p}_3 = 0$.

$(6c)$ אם ישר Λ משיק ל E בנקודה $\mathbf{p}$ של $E(L)$ וחותך את $E(L)$ בנקודה נוספת $\mathbf{q}$, אזי $2\mathbf{p} + \mathbf{q} = 0$.

$(6d)$ אם ישר Λ משיק ל E בנקודה $\mathbf{p}$ ואינו חותך יותר את $E(L)$, אזי $3\mathbf{p} = 0$.

הגדרת החבור על $E(L)$ באפן שהכללים (6) יתקיְמו נִתנת לבצוע באפן גאומטרי או גם בעזרת תורת שדות הפונקציות האלגבריות של משתנה אחד כפי שנראה להלן.

מכללים אלו נחשב את נסחאות החבור:

$(7a)$ אם ב $(6b)$ $\mathbf{p}_1 = (x, y)$, $\mathbf{p}_2 = (x', y')$ ו $\mathbf{p}_3 = 0$, אזי הישר העובר דרך $\mathbf{p}_1$ ו $\mathbf{p}_2$ מקביל לציר ה Y-ים. לכן $x = x'$ ולכן נובע מ (1) ש $y' = -y$. במלים אחרות, $-(x, y) = (x, -y)$.

$(7b)$ יהיו $\alpha, \beta \in L$ ויהי Λ הישר המוגדר על ידי $Y = \alpha X + \beta$. נניח שישר זה חותך את $E(L)$ בשלש נקודות $\mathbf{p}_i = (x_i, y_i)$, $i = 1, 2, 3$. אזי x_1, x_2, x_3 הם השרשים של הפולינום ממעלה שלישית המתקבל על ידי הצבה של $Y = \alpha X + \beta$ ב $g(X, Y) = X^3 + aX + b - Y^2$, כלומר הם השרשים של המשואה

$$X^3 - \alpha^2 X^2 + (a - 2\alpha\beta)X + b - \beta^2 = 0$$

לכן, $x_1 + x_2 + x_3 = \alpha^2$. אם $2(\mathbf{p}_1 + \mathbf{p}_2) \neq 0$ נובע מ $(7a)$ ש

$$x(\mathbf{p}_1 + \mathbf{p}_2) = \alpha^2 - (x_1 + x_2) \quad \text{ו} \quad y(\mathbf{p}_1 + \mathbf{p}_2) = -\alpha x(\mathbf{p}_1 + \mathbf{p}_2) - \beta . \qquad (7b1)$$

אם $2(\mathbf{p}_1 + \mathbf{p}_2) = 0$, אזי $\mathbf{p}_1 + \mathbf{p}_2 = -(\mathbf{p}_1 + \mathbf{p}_2)$. מהדיון אחרי $(7d2)$ נובע שבמקרה זה $y(\mathbf{p}_1 + \mathbf{p}_2) = 0$ ולכן $(7b1)$ תקף גם במקרה זה.

$(7c)$ נסחת החבור: נניח קודם ש $\mathbf{p}_1 \neq \pm\mathbf{p}_2$. אזי, לפי $(7a)$, $x_1 \neq x_2$ ו Λ מקבל את הצורה

$$\frac{Y - y_2}{X - x_2} = \frac{y_1 - y_2}{x_1 - x_2}$$

במונחים של $(7b)$ מקבלים ש

$$\alpha = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{ו} \quad \beta = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} \qquad (7c1)$$

לכן,

$$x(\mathbf{p}_1 + \mathbf{p}_2) = \frac{a(x_1 + x_2) + 2b + x_1 x_2^2 + x_2 x_1^2 - 2y_1 y_2}{(x_1 - x_2)^2} \qquad (7c2)$$

$(7d)$ נֻסחת השכפול: תהי $\mathbf{p} = (x, y)$ נקֻדה של $E(L)$ ויהי Λ היָשר דרך $\mathbf{p}$ המֻגדר על ידי המשואה

$$\frac{\partial g}{\partial X}(x, y)(X - x) + \frac{\partial g}{\partial Y}(x, y)(Y - y) = 0 . \qquad (7d1)$$

נחשב את הנגזרות החלקיות של $g(X, Y)$ עד סדר 3:

$$\frac{\partial g}{\partial X}(x, y) = 3x^2 + a \quad \frac{\partial^2 g}{\partial X^2}(x, y) = 6x \quad \frac{\partial^3 g}{\partial X^3} = 6$$
$$\frac{\partial g}{\partial Y}(x, y) = -2Y^2 \quad \frac{\partial^2 g}{\partial Y^2}(x, y) = -x$$

כל שאר הנגזרות שוות ל 0. הצבה של ערכים אלו ב $(7d1)$ נותנת למשואה המתארת את Λ את הצורה

$$(3x^2+a)(X-x)-2y(Y-y)=0\ . \qquad (7d2)$$

כדי לחשב את נקֻדות החתוך של Λ ו E נניח תחילה ש $y\neq 0$. אזי אפשר לכתב מחדש את $(7d2)$ בצורה $Y=\alpha X+\beta$ באשר

$$\alpha=\frac{3x^2+a}{2y} \quad \text{ו} \quad \beta=y-\frac{3x^3+ax}{2y}. \qquad (7d3)$$

בפרט Λ אינו מקביל לציר ה Y־ים ולכן נקֻדת החתוך שלו עם ישר האינסוף שונה מ $(0{:}0{:}1)$. הואיל וזוהי נקֻדת האינסוף היחידה של E, כל נקֻדות $\Lambda\cap E$ סופיות. כדי לחשב אותן נפתח את $g(X,Y)$ לטור טֵילור (סופי) סביב הנקֻדה (x,y):

$$g(X,Y)=\sum_{k=0}^{3}\sum_{i=0}^{k}\frac{1}{k!}\frac{\partial^k g}{\partial X^i\partial X^{k-i}}(x,y)(X-x)^i(Y-y)^{k-i}\ . \qquad (7d4)$$

האבר באגף ימין המתאים ל $k=0$ הנו $g(x,y)=0$. אם נַציב את $Y-y=\alpha(X-x)$ ב $g(X,Y)$ מ $(7d2)$ נקבל שגם האבר המתאים ל $k=1$ מתאפס וחשובי הנגזרות דלעיל נותנים

$$g(X,\alpha X+\beta)=(3x-\alpha^2)(X-x)^2+(X-x)^3\ .$$

השרש x של המשואה $g(X,\alpha X+\beta)=0$ כפול אפוא והשרש האחר הנו $x_3=\alpha^2-2x$. מ $(7d3)$ נקבל ש $y_3=\alpha x_3+\beta$. במלים אחרות, קבלנו ש Λ מַשיק ל E בנקֻדה $\mathbf{p}=\mathbf{p}_1=\mathbf{p}_2=(x,y)$ ונקֻדת החתוך השלישית $\mathbf{p}_3=(x_3,y_3)$ נִתנת לעיל. מ $(6c)$ עולה ש $\mathbf{p}+\mathbf{p}_3=0$ ולפי $(7a)$, $2\mathbf{p}=(x_3,-y_3)=(\alpha^2-2x,-\alpha x_3-\beta)$. אם נפתח את אגף ימין של $x(2\mathbf{p})=\alpha^2-2x$ נקבל ש

$$x(2\mathbf{p})=\frac{x^4-2ax^2-8bx+a^2}{4x^3+4ax+4b}. \qquad (7d5)$$

הואיל והמכנה שוה ל $4y^2$ אין הוא מתאפס. במלים אחרות, $2\mathbf{p}\neq 0$. לפי $(7a)$,

$$y(2\mathbf{p})=-\alpha x(2\mathbf{p})-\beta=-\frac{3x^2+a}{y}x(2\mathbf{p})-y+\frac{3x^3+ax}{2y}$$

לכן

$$y(2\mathbf{p})y=-(3x^2+a)x(2\mathbf{p})-(x^3+ax+b)+\frac{1}{2}(3x^3+ax)\ . \qquad (7d8)$$

אם $y=0$ אזי x הנו אחד משלשת השרשים השונים של הפולינום $f(X)$. יתר על כן, $\frac{\partial g}{\partial Y}(x,y)=2y=0$ ולכן, $\frac{\partial g}{\partial X}(x,y)\neq 0$ (כי $\mathbf{p}$ פשוטה). לכן, לפי $(7d1)$, מקבלת נסחת Λ את הצורה $X=x$. כלומר Λ מקביל לציר ה Y־ים. נקֻדת החתוך השלישית של Λ עם E תהיה 0. לכן, $2(x,0)=0$. בפרט $-(x,0)=(x,0)$. כמובן שגם $2\cdot 0=0$. יחד עם הפסקה הקודמת נקבל את המסקנה $E_2(\tilde{K})=\{\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3,0\}$, באשר $\mathbf{p}_i=(\xi_i,0)$, באשר ξ_1,ξ_2,ξ_3 הם שלשת השרשים השונים של המשואה $f(X)=0$. לכן $E_2(\tilde{K})\cong(\mathbb{Z}/2\mathbb{Z})^2$.

ממסקנה ו.ג עולה שהמונה והמכנה של $(7d2)$ זרים זה לזה. בפרט, אם המכנה מתאפס, המונה אינו מתאפס. במקרה זה $x(2\mathbf{p})=\infty$ ולכן $2\mathbf{p}=0$. אפשר אפוא לראות את $(7d2)$ כנסחת השכפול גם במקרה ש $y=0$.

משפטון ז.א: *נניח ש K הוא שדה בעל אפיון שונה מ 2 ומ 3. אזי העקם האלפטי E המוגדר מעל K על ידי המשואה (1) והמקֻים $\Delta_E\neq 0$ הנו פנקטור אבלי מעל K. יתר על כן, E מקֻים את התנאים (1) ו (2) של סעיף ה עבור $m=2$. בנוסף לזה, אם O הוא חוג דדקינד ו $\mathcal{P}_K$ היא קבוצת המחלקים הראשוניים של K המתאימים לאידאלים המרביים של O, נגדיר*

$$\mathrm{Bad}_K(E)=\{\mathfrak{p}\in\mathcal{P}_K\mid\ v_{\mathfrak{p}}(a)<0\text{ or }v_{\mathfrak{p}}(b)<0\text{ or }v_{\mathfrak{p}}(\Delta)\neq 0\text{ or }v_{\mathfrak{p}}(2)\neq 0\text{ or }v_{\mathfrak{p}}(3)\neq 0\}\ .$$

אזי ל E יש העמדה טובה בכל מחלק ראשוני שאינו שיך ל $\mathrm{Bad}_K(E)$. ביתר דיוק, (5) של סעיף ה מתקֻים עבור $m=2$.

הוכחה: נסחאות החבור של E מוגדרות על ידי פונקציות רציונליות בפרמטרים a ו b השיכים ל K. קל להראות שהן מקימות את חק החלוף. יותר קשה להוכיח את חק הצרוף. זאת נעשה באפן עקיף, בעזרת משפט רימן־רוך בסעיף יג. אז ינבע ש $E(L)$ הוא אכן חבורה אבלית לכל L אלגברי המקיף את K.

יהי $\sigma\colon L\to L'$ איזומורפיזם־K. נגדיר $\sigma(x,y)=(\sigma x,\sigma y)$ ו $\sigma(0)=0$. התנאי (1) של סעיף ה נובע עתה מהגדרת אברי $E(L)$ כזוגות (x,y) ונקֻדת האפס והגדרת החבור על ידי פונקציות רציונליות עם מקדמים ב K. שאר התנאים על E תלויים ב m. נניח אפוא מכאן ואילך ש $m=2$.

ב $(7d)$ הראינו ש $E_2(L)$ מכילה בדיוק ארבעה אברים. בפרט מתקֻים $(2a)$ של סעיף ה. כדי להראות שכפל ב 2 מעתיק את $E(K_s)$ על עצמו (תנאי $(2b)$ של סעיף ה), נתבונן בנקודה $\mathbf{p}'=(x',y')\in E(K_s)$. עבורה קיָם $x\in K_s$ כך ש

$$.x^4-2ax^2-8bx+a^2=x'(4x^3+4ax+4b) \qquad (7d7)$$

אלו היה הבטוי בסגרים של אגף ימין של $(7d7)$ שוה לאפס היה גם אגף שמאל שוה לאפס בנגוד לזרות של שני הפולינומים (מסקנה ו.ג). לכן קיָם $x\in K_s$ המקיָם את $(7d7)$. כדי לחשב את y נניח עתה ש $y'\neq 0$ ונגדיר את y על ידי המשואה

$$.\ y'y=-(3x^2+a)x'-(x^3+ax+b)+\frac{1}{2}(3x^3+ax) \qquad (7d6)$$

הואיל וכל אחד משני הפתרונות השונים של המשואה $Y^2 = x^3 + ax + b$ מקיְמים את המשואה $(7d6)$ (עבור y), הנקֻדה $\mathbf{p} = (x, y)$ שיָכת ל $E(K_s)$ ומקיֶמת (לפי $(7d5)$ ו $(7d6)$) את התנאי $2\mathbf{p} = \mathbf{p}'$. אם $y' = 0$, אזי $\mathbf{p}'$ הוא אחת מארבעת הנקֻדות מסדר 2 של $E(K_s)$. נבחר נקֻדה $\mathbf{q}' \in E(K_s)$ שסדרה שונה מ 2. אזי $2(\mathbf{p}' + \mathbf{q}') = 2\mathbf{q}' \neq 0$. לפי המקרה הקודם, קיָמות נקֻדות $\mathbf{q}, \mathbf{r} \in E(K_s)$ כך ש $2\mathbf{q} = \mathbf{q}'$ ו $2\mathbf{r} = \mathbf{p}' + \mathbf{q}'$. הנקֻדה $\mathbf{p} = \mathbf{r} - \mathbf{q}$ תקיֵם $2\mathbf{p} = \mathbf{p}'$. בכך השלמנו את ההוכחה שכפל ב 2 מעתיק את $E(K_s)$ על עצמו.

לבסוף נתבונן במחלק ראשוני $\mathfrak{p} \in \mathcal{P}_K \smallsetminus \mathrm{Bad}_K$. הואיל ו $\bar{\Delta} \neq 0$ ההעמדה מודולו $\mathfrak{p}$ מעבירה את E לעקם $\bar{E}$ המוגדר מעל $\bar{K}_\mathfrak{p}$ על ידי $Y^2 = \bar{f}(X)$.

כדי להגדיר את $\mathrm{red}_\mathfrak{p}$ נעבר לקואורדינטות הומוגניות. תהי L הרחבה פרידה סופית של K. נתבונן במחלק ראשוני $\mathfrak{q}$ של L המונח מעל $\mathfrak{p}$. נסמן את ההעמדה מודול $\mathfrak{q}$ בגג. עבור $\mathbf{p} = (x_0{:}x_1{:}x_2)$ ב $\mathbb{P}^2(L)$ נבחר i כך ש $v_\mathfrak{q}(x_i) \leq v_\mathfrak{q}(x_j)$ עבור $j = 0, 1, 2$ ונסמן $x_j' = \frac{x_j}{x_i}$. אזי $\mathbf{p} = (x_0'{:}x_1'{:}x_2')$, $v_\mathfrak{q}(x_j') \geq 0$ עבור $j = 0, 1, 2$ ו $x_i' = 1$. לכן $\bar{\mathbf{p}} = (\bar{x}_0'{:}\bar{x}_1'{:}\bar{x}_2') \in \mathbb{P}^2(\bar{L})$. בכך אנו מקבלים העתקה $\mathrm{red}\colon \mathbb{P}^2(L) \to \mathbb{P}^2(\bar{L})$. עתה נראה את $E(L)$ כאסף כל הנקודות $\mathbf{p} = (x_0{:}x_1{:}x_2)$ של $\mathbb{P}^2(L)$ המקימות את המשואה ההומוגנית ממעלה 3

$$X_0X_2^2 = X_1^3 + aX_0^2X_1 + bX_0^3. \tag{9}$$

$\bar{E}(\bar{L})$ יהיה אסף הנקודות של $\mathbb{P}^2(\bar{L})$ המקימות את המשואה

$$X_0X_2^2 = X_1^3 + \bar{a}X_0^2X_1 + \bar{b}X_0^3. \tag{10}$$

לכן $\mathrm{red}_\mathfrak{p}$ מעתיק את $E(L)$ לתוך $\bar{E}(\bar{L})$.

אם $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in \mathbb{P}^2(L)$ מקימות $\mathbf{p}_1 + \mathbf{p}_2 + \mathbf{p}_3 = 0$, אזי לפי $(6b)$ הן מונחות על ישר אחד

$$\Lambda\colon \quad \alpha_0X_0 + \alpha_1X_1 + \alpha_2X_2 = 0$$

באשר $(\alpha_0{:}\alpha_1{:}\alpha_2) \in \mathbb{P}^2(L)$. כמו מקודם נוכל להכפיל את המקדמים באבר מתאים של $L^\times$ כך שהמשואה

$$\bar{\Lambda}\colon \quad \bar{\alpha}_0X_0 + \bar{\alpha}_1X_1 + \bar{\alpha}_2X_2 = 0$$

תתאר ישר מעל $\bar{L}$. לפי ההנחה $\mathbf{p}_i \in E(L) \cap \Lambda(L)$. לכן $\bar{\mathbf{p}}_i \in \bar{E}(\bar{\Lambda}) \cap \bar{\Lambda}(\bar{L})$, $i = 1, 2, 3$.

כדי להסיק מכאן ש $\bar{\mathbf{p}}_1 + \bar{\mathbf{p}}_2 + \bar{\mathbf{p}}_3 = 0$ עלינו עוד להראות שכל נקֻדה המונחת על $\bar{E}(\bar{L}) \cap \bar{\Lambda}(\bar{L})$ הנה אחת מהנקדות $\bar{\mathbf{p}}_1, \bar{\mathbf{p}}_2, \bar{\mathbf{p}}_3$. לשם כך נתבונן שוב בפולינום $h(X_0, X_1, X_2) = X_1^3 + aX_0^2X_1 + bX_0^3 - 2X_0X_2$. נניח למשל ש $\bar{\alpha}_2 \neq 0$. על ידי הכפלה ב α_2^{-1} נוכל אפוא להניח ש $\alpha_2 = 1$. נקדות החתוך של $E(L)$ ו $\Lambda(L)$ יהיו הנקודות

$(x_0:x_1:-\alpha_0x_0-\alpha_1x_1)$ שעבורן $(x_0:x_1)$ פותרים את המשואה $h(X_0,X_1,-\alpha_0X_0-\alpha_1X_1)=0$.

באפן דומה, נקֻדות החתוך של $\bar{E}(\bar{L})$ ו $\bar{\Lambda}(\bar{L})$ יהיו הנקדות $(\bar{x}_0:\bar{x}_1:-\bar{\alpha}_0\bar{x}_0-\bar{\alpha}_1\bar{x}_1)$ שעבורן $(\bar{x}_0:\bar{x}_1)$ פותרים את המשואה $\bar{h}(X_0,X_1,-\bar{\alpha}_0X_0-\bar{\alpha}_1X_1)=0$. אולם

$$h(X_0,X_1,-\alpha_0X_0-\alpha_1,X_1)=\prod_{i=1}^{3}(x_{0i}X_1-x_{1i}X_0)$$
$$\bar{h}(X_0,X_1,-\bar{\alpha}_0X_0-\bar{\alpha}_1X_1)=\prod_{i=1}^{3}(\bar{x}_{0i}X_1-\bar{x}_{1i}X_0).$$

לכן, $\bar{p}_1,\bar{p}_2,\bar{p}_3$ הן כל הנקדות על $E(\bar{L})\cap\Lambda(\bar{L})$, כנדרש.

כמו כן, $\overline{-\mathbf{p}}=-\bar{\mathbf{p}}$ (לפי $(7a)$). לכן $\mathrm{red}_{\mathfrak{p}}\colon E(L)\to\bar{E}(\bar{L})$ הוא הומומורפיזם.

עתה נחזר לקואורדינטות אפיניות ונזכר ש $E_2(K_s)=\{\infty\}\cup\{(\xi_i,0)\mid i=1,2,3\}$. נבחר הרחבה פרדיה סופית L של K המכילה את ξ_1,ξ_2,ξ_3 ונבחר מחלק ראשוני $\mathfrak{q}$ מעל $\mathfrak{p}$. נעמיד את (4) מודולו $\mathfrak{p}$:

$$\bar{f}(X)=(X-\bar{\zeta}_1)(X-\bar{\zeta}_2)(X-\bar{\zeta}_3)\quad\text{ו}\quad\bar{\Delta}=-(\bar{\zeta}_1-\bar{\zeta}_1)^2(\bar{\zeta}_3-\bar{\zeta}_2)^2(\bar{\zeta}_3-\bar{\zeta}_1)^2 \tag{11}$$

הואיל ו $\xi_i^3+a\xi_i+b=0$ ו $v_p(a),v_p(b)\ge 0$, מתקיֵם $\bar{\xi}_i\in\bar{L}$. כמו כן,

$$\bar{E}_2(\bar{K}_s)=\{\infty\}\cup\{(\bar{\xi}_i,0)\mid i=1,2,3\}.$$

לכן ההעמדה מודולו $\mathfrak{q}$ מעתיקה את $E_2(L)$ באפן חד חד ערכי על $\bar{E}_2(\bar{L})$, כנדרש ב $(5a)$ של סעיף ה.

לבסוף נניח ש L הנו הרחבת גלואה סופית של K, σ אבר של חבורת הפרוק $D(\mathfrak{q}/\mathfrak{p})$ ו $\mathbf{p}\in E(L)$. נבחר $x_0,x_1,x_2\in L^\times$ כך ש $\mathbf{p}=(x_0,x_1,x_2)$ ולמשל $v_{\mathfrak{q}}(x_0)=0$ ו $v_{\mathfrak{q}}(x_1),v_{\mathfrak{q}}(x_2)\ge 0$. לפי ההנחה, σ שומר על $O_{\mathfrak{q}}$ ולכן גם על חבורת האברים ההפיכים $O_{\mathfrak{q}}^\times$. לכן, $v_{\mathfrak{q}}(\sigma x)=0$ ו $v_{\mathfrak{q}}(\sigma x_1),v_{\mathfrak{q}}(\sigma x_2)\ge 0$. מכאן נובע $\bar{\sigma}\bar{\mathbf{p}}=(\bar{\sigma}\bar{x}_0:\bar{\sigma}\bar{x}_1:\bar{\sigma}\bar{x}_2)=(\overline{\sigma x_0}:\overline{\sigma x_1}:\overline{\sigma x_2})=\overline{\sigma\mathbf{p}}$. ∎

תוצאה ז.ב: *נניח ש K הוא שדה בעל אפיון שונה מ 2 ומ 3. תהי $\mathcal{P}_K$ קבוצה של מחלקים ראשוניים המקימת את הדרישות (1)־(5) של סעיף ד. יהי E העקם האלפטי המוגדר מעל K על ידי המשואה (1). אזי $E(K)/2E(K)$ היא חבורה סופית.*

הוכחה: משפטון ז.א אומר ש E הוא פנקטור אבלי המקים את התנאים (1), (2) ו (5) של סעיף ה עבור $m=2$. לכן, לפי משפטון ה.ה, $E(K)/2E(K)$ היא חבורה סופית. ∎

ח. פונקצית גבה על עקם אלפטי מעל $\mathbb{Q}$

המקרה הפשוט ביותר שבו נתן להגדיר פונקצית גבה על עקם אלפטי כך שתקים את הדרישות בהגדרה א.א הנו מעל שדה המספרים הרציונליים $\mathbb{Q}$. נניח אפוא שהעקם נתן כרגיל על ידי המשואה $Y^2 = X^3 + AX + B$ ו $\Delta = 4A^3 + 27B^2 \neq 0$.

למה ח.א: *יהי K שדה בעל אפיון שונה מ 2 ו 3. יהי E עקם אלפטי מעל K הנתן על ידי המשואה $Y^2 = X^3 + AX + B$. יהי $u \in K^\times$ ויהיו $A' = u^4 A$, $B' = u^6 B$. אזי המשואה $Y^2 = X^3 + A'X + B'$ מגדירה עקם אלפטי E' מעל K. יתר על כן, לכל הרחבה L של K ההעתקה $\alpha\colon (x,y) \mapsto (u^2x, u^3y)$ מגדירה איזומורפיזם של $E(L)$ על $E'(L)$.*

הוכחה: לפי ההנחה $\Delta = 4A^3 + 27B^2 \neq 0$. מכאן נובע ש $\Delta' = 4u^{12}A^3 + 27u^{12}B^2 = u^{12}\Delta \neq 0$. לכן E' הוא אכן עקם אלפטי.

בדיקה מראה ש α מעתיקה את $E(L)$ באפן חד חד ערכי של $E'(L)$. כמו כן מראה בדיקה ש α שומרת גם על נסחת החבור ב $(7c)$ ועל נסחת השכפול $(7d2)$ שבסעיף ז. ∎

הגדרה ח.ב: כל אבר שונה מאפס של $\mathbb{Q}$ נתן לרשם כשבר מְצֻמצם, $x = \frac{a}{b}$. בשבר זה a ו b הם מספרים שלמים הזרים זה לזה. נגדיר $H(x) = \max(|a|,|b|)$. אם $x = \frac{a'}{b'}$ הוא הצגה לא מְצֻמצמת של x, אזי $|a| \leq |a'|$ ו $|b| \leq |b'|$ ולכן $H(x) \leq \max(|a'|,|b'|)$. נגדיר גם $H(0) = 1$.

עתה נגדיר פונצית גבה $h\colon E(\mathbb{Q}) \to \mathbb{R}$ בעזרת הנסחה:

$$h(\mathbf{p}) = \begin{cases} \log H(x(\mathbf{p})) & \text{if } \mathbf{p} \neq 0 \\ 0 & \text{if } \mathbf{p} = 0 \end{cases}$$

ונשים לב לכך ש $h(\mathbf{p}) \geq 0$. ∎

הלמה הבאה תספק את כל הדרישות של פונקציות הגבה.

למה ח.ג:

(א) *תהי $\mathbf{p}_0 \in E(\mathbb{Q})$. אזי קים קבוע c_1, התלוי ב $\mathbf{p}_0, A, B$, כך שלכל $\mathbf{p} \in E(\mathbb{Q})$ מתקים $h(\mathbf{p} + \mathbf{p}_0) \leq 2h(\mathbf{p}) + c_1$.*

(ב) *קים קבוע c_2, התלוי ב A, B, כך שלכל $\mathbf{p} \in E(\mathbb{Q})$ מתקים $h(2\mathbf{p}) \geq 4h(\mathbf{p}) - c_2$.*

(ג) *לכל קבוע c_3 הקבוצה $\{\mathbf{p} \in E(\mathbb{Q}) \mid h(\mathbf{p}) \leq c_3\}$ סופית.*

הוכחה: נשתמש בלמה ח.א כדי לעבר במקרה הצרך לעקם איזומורפי שבו המקדמים A ו B המופיעים בהגדרת E שלמים.

הוכחת א: אם נדרש ש $c_1 > \max(h(\mathbf{p}_0), h(2\mathbf{p}_0))$, נוכל להניח ש $\mathbf{p}_0 \neq 0$ ו $\mathbf{p} \neq 0, \pm\mathbf{p}_0$. יהי אפוא $\mathbf{p}_0 = (x_0, y_0)$ ונתבונן בנקודה $\mathbf{p} = (x,y)$. יהיו $x = \frac{a}{e}$ ו $y = \frac{b}{e'}$ הצגות מְצֻמצמות שבהן $e, e' > 0$. מהנסחה

$y^2 = x^3 + Ax + B$ נובע שלכל מספר ראשוני p מתקיים $v_p(x) < 0$ אם ורק אם $v_p(y) < 0$. במקרה זה $2v_p(y) = 3v_p(x)$, $v_p(x) = -v_p(e)$ ו $v_p(y) = -v_p(e')$. לכן, $2v_p(e') = 3v_p(e)$. מכאן נובע שקים מספר טבעי d כך ש $e = d^2$ ו $e' = d^3$. שקול דומה חל לגבי $\mathbf{p}_0$. הוכחנו אפוא ש

$$\mathbf{p} = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad \mathbf{p}_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

וכל השברים המופיעים כאן מצֻמצמים. מנסחת החבור $(7c2)$ של סעיף ז מקבלים

$$\begin{aligned} x(\mathbf{p} + \mathbf{p}_0) &= \frac{Ax + Ax_0 + 2B + xx_0^2 + x^2x_0 - 2yy_0}{x^2 - 2xx_0 + x_0^2} \\ &= \frac{Aad^2d_0^4 + Ad^4a_0d_0^2 + 2Bd^4d_0^4 + ad^2a_0^2 + a^2a_0d_0^2 - 2bdb_0d_0}{a^2d_0^4 - 2ad^2a_0d_0^2 + d^4a_0^2} \end{aligned}$$

מכאן נובע שקים קבוע חיובי c_1' התלוי רק ב $A, B, \mathbf{p}_0$ כך ש

$$H(x(\mathbf{p} + \mathbf{p}_0)) \leq c_1' \max(|a|^2, |d|^4, |bd|, |ad^2|) \tag{1}$$

אם $|d^2| \leq |a|$ אזי $|ad^2| \leq |d|^4$. אם $|a| \leq |d^2|$, אזי $|ad^2| \leq |a|^2$. לכן, בכל מקרה נובע מ (1) ש

$$H(x(\mathbf{p} + \mathbf{p}_0)) \leq c_1' \max(|a|^2, |d|^4, |bd|) \tag{2}$$

מהנסחה $b^2 = a^3 + Aad^4 + Bd^6$, נובע שקים קבוע חיובי c_1'', התלוי רק ב $A, B, \mathbf{p}_0$ כך ש $|b| \leq c_1'' \max(|a|^{3/2}, |d|^3, |ad^4|^{1/2})$. שוב, אם $|a| \leq |d|^2$, אזי $|ad^4|^{1/2} \leq |d|^3$. אם $|d|^2 \leq |a|$, אזי $|ad^4|^{1/2} \leq |a|^{3/2}$. לכן, $|b| \leq c_1'' \max(|a|^{3/2}, |d|^3)$. אם נציב אי שויון זה ב (2) נקבל ש

$$H(x(\mathbf{p} + \mathbf{p}_0)) \leq c_1'c_1'' \max(|a|^2, |d|^4, |a|^{3/2}|d|) \tag{3}$$

שוב, אם $|a| \leq |d|^2$, אזי $|a|^{3/2}|d| \leq |d|^4$. אם $|d|^2 \leq |a|$, אזי $|a|^{3/2}|d| \leq |a|^2$. לכן, (3) נותן ש $H(x(\mathbf{p} + \mathbf{p}_0)) \leq c_1'c_1'' \max(|a|^2, |d|^4)$. מההגדרה נובע ש $H(x) = \max(|a|, |d|^2)$. לכן

$$H(x(\mathbf{p} + \mathbf{p}_0)) \leq c_1'c_1'' H(x(\mathbf{p}))^2$$

אם נקח את הלוגריתמוס של שני האגפים ונציב $c_1 = \log c_1' + \log c_1''$, נקבל ש $h(\mathbf{p} + \mathbf{p}_0) \leq 2h(\mathbf{p}) + c_1$, כנדרש.

הוכחת ב: אם נדרש ש $c_2 \geq 4h(\mathbf{q})$ לכל אחת מהנקודות $\mathbf{q}$ של $E_2(\mathbb{Q})$ נוכל להניח בהוכחת ב ש $2\mathbf{p} \neq 0$. נסחת שכפול $(7d2)$ של סעיף ז הנה

$$x(2\mathbf{p}) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

נתבונן בשני הפולינומים ההומוגניים $F(X,Z)$ ו $G(X,Z)$ שהוגדרו בלמה ו.ב:

$$\begin{aligned} F(X,Z) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4 \\ G(X,Z) &= 4X^3Z + 4AXZ^3 + 4BZ^4 \end{aligned} \tag{4}$$

אם נרשם $x = x(\mathbf{p}) = \frac{a}{b}$ עם $\gcd(a,b) = 1$ נקבל על ידי הצבה ב (4) ש

$$.x(2\mathbf{p}) = \frac{F(a,b)}{G(a,b)} \tag{5}$$

כדי להעריך את $H(x(2\mathbf{p}))$ מלרע עלינו לצמצם את אגף ימין של (5). לצרך זה נגדיר

$$.\delta = \gcd(F(a,b), G(a,b))$$

מלמה ו.ב נובע ש

$$\begin{aligned} f_1(a,b)F(a,b) - g_1(a,b)G(a,b) &= 4\Delta b^7 \\ .f_2(a,b)F(a,b) + g_2(a,b)G(a,b) &= 4\Delta a^7 \end{aligned} \tag{6}$$

לפי הגדרתו, מחלק δ את אגפי שמאל של (6). לכן מחלק δ את $4\Delta a^7$ ואת $4\Delta b^7$. מהזרות של a^7 ו b^7 נובע ש $\delta | 4\Delta$ ולכן $|\delta| \le |4\Delta|$. מכאן נובע ש

$$.H(x(2\mathbf{p})) = \max\left(\left|\frac{F(a,b)}{\delta}\right|, \left|\frac{G(a,b)}{\delta}\right|\right) \ge \frac{1}{|4\Delta|}\max\left(|F(a,b)|, |G(a,b)|\right) \tag{7}$$

באפן כללי, אם $|u_1|, |u_2| \le \bar{u}$ ו $|v_1|, |v_2| \le \bar{v}$, אזי

$$.|u_1v_1 + u_2v_2| \le |u_1||v_1| + |u_2||v_2| \le 2\bar{u}\bar{v}$$

אם נישם עקרון זה לשויונות (6), נקבל ש

$$\begin{aligned} |4\Delta b^7| &\le 2\max\left(|f_1(a,b)|, |g_1(a,b)|\right)\max\left(|F(a,b)|, |G(a,b)|\right) \\ .|4\Delta a^7| &\le 2\max\left(|f_2(a,b)|, |g_2(a,b)|\right)\max\left(|F(a,b)|, |G(a,b)|\right) \end{aligned} \tag{8}$$

כל אחד מהבטויים $f_1(a,b)$, $f_2(a,b)$, $g_1(a,b)$ ו $g_2(a,b)$ הנו פולינום הומוגני ב a ו b ממעלה 3 במקדמים התלויים רק ב A ו B. לכן קים קבוע חיובי c' התלוי רק ב A, B כך ש

$$.\max\left(|f_1(a,b)|, |g_1(a,b)|, |f_2(a,b)|, |g_2(a,b)|\right) \le c'\max\left(|a|^3, |b|^3\right) \tag{9}$$

צרוף של (8 ו (9) נותן:

$$. \max\left(|4\Delta a^7|, |4\Delta b^7|\right) \le 2c' \max\left(|a|^3, |b|^3\right) \max\left(|F(a,b)|, |G(a,b)|\right)$$

אם נצמצם $\max\left(|a|^3, |b|^3\right)$ משני האגפים נקבל

$$.\frac{1}{|4\Delta|} \max\left(|F(a,b)|, |G(a,b)|\right) \ge (2c')^{-1} \max\left(|a|, |b|\right)^4 \qquad (10)$$

הואיל ו $H(x(\mathbf{p})) = \max(|a|, |b|)$, נקבל מ (7) ו (10) ש $H(x(2\mathbf{p})) \ge (2c')^{-1} H(x(\mathbf{p}))^4$. עתה נקח את הלוגריתמוס של שני האגפים ונקבל קבוע c_2 התלוי רק ב A ו B כך ש $h(2\mathbf{p}) \ge 4h(\mathbf{p}) - c_2$, כנדרש.

הוכחת ג: מספר הזוגות (a,b) של מספרים שלמים המקימים $\max(|a|, |b|) \le c$ עבור קבוע חיובי c נתון אינו עולה על $(2c+1)^2$. לכן, מספר המספרים הרציונליים x המקימים $H(x) \le c$ אינו עולה על $(2c+1)^2$. לכל מספר רציונלי של x יש לכל היותר שני ערכים y כך ש $(x,y) \in E(\mathbb{Q})$. לכן, לכל קבוע c_3, הקבוצה $\{\mathbf{p} \in E(\mathbb{Q}) \mid h(\mathbf{p}) \le c_3\}$ סופית. ∎

ח.ד קבוצת מחלקים ראשוניים. יהי $\mathcal{P}_{\mathbb{Q}}$ אסף המספרים הראשונים. לכל מספר ראשוני p מתאימה, לפי דגמה ב.ג הערכה בדידה v_p, ומתקים תנאי (1) של סעיף ד. בפרט, O_p מורכב מכל השברים המצֻמצים שהמכנה שלהם אינו מתחלק ב p. לכן, חתוך כל החוגים O_p הנו חוג המספרים השלמים $\mathbb{Z}$. זהו חוג ראשי ובפרט חוג דדקינד (תנאי (2) של סעיף ד).

יהי L הרחבה סופית של $\mathbb{Q}$. תורת המספרים האלגבריים מלמדת אותנו שמספר מחלקות האידאלים של O_L סופי ומתקים משפט האחדות של דיריכלה. במלים אחרות, גם התנאים (1) ו (2) של סעיף ד מתמלאים.

משפט ח.ה (משפט מורדל־וייל עבור עקמים אלפטיים מעל $\mathbb{Q}$): *יהי E עקם אלפטי מעל $\mathbb{Q}$. אזי $E(\mathbb{Q})$ היא חבורה נוצרת סופית.*

הוכחה: מ ח.ד ומתוצאה ז.ב נובע ש $E(\mathbb{Q})/2E(\mathbb{Q})$ הנה חבורה סופית. למה ח.ג אומרת שפונקצית הגבה h על $E(\mathbb{Q})$ מקימת את התנאים של הגדרה א.א. לכן, לפי משפטון א.ב, החבורה $E(\mathbb{Q})$ נוצרת סופית. ∎

ט. שדות פונקציות של משתנה אחד

הרחבת שדות F/K תכונה **שדה פונקציות של משתנה אחד** אם מתקיימים התנאים הבאים:

$(1a)$ מעלת הנעלות (=טרנסצנדנטיות) של F/K היא 1.

$(1b)$ F נוצר סופית מעל K.

$(1c)$ K סגור אלגברית בתוך F.

במקרה זה קים t ב F, נעלה מעל K, כך ש $[F : K(t)] < \infty$. הואיל וכל ההערכות של $K(t)$ שהן טריביאליות על K הנן בדידות, גם הרחבותיהן ל F בדידות (משפטון ב.ז). הואיל ושדות השאריות של ההערכות של $K(t)/K$ הם הרחבות סופיות של K, גם שדות השאריות של הרחבותיהן ל F הם הרחבות סופיות של K.

נגדיר **מחלק ראשוני** של F/K כמחלקת שקילות של הערכות של F/K. נסמן ב $\mathcal{P}$ את אסף המחלקים הראשוניים של F/K. בכל פעם ש F/K לא יהיה ברור מתוך הענין, נשתמש גם בסמון $\mathcal{P}_{F/K}$. לכל $\mathfrak{p} \in \mathcal{P}$ נבחר הערכה $v_\mathfrak{p}$ כך ש $v_\mathfrak{p}(F^\times) = \mathbb{Z}$ ונסמן ב $\bar{F}_\mathfrak{p}$ את שדה השאריות המתאים. המספר $\deg(\mathfrak{p}) = [\bar{F}_\mathfrak{p} : K]$ יקרא **המעלה** של $\mathfrak{p}$.

נסמן ב $\mathcal{D}$ את החבורה האבלית החבורית החפשית הנוצרת על ידי אברי $\mathcal{P}$. אברי $\mathcal{D}$ יקראו **מחלקים** של F/K. כל מחלק $\mathfrak{a}$ של F/K נתן לרשם באפן יחיד בצורה $\mathfrak{a} = \sum_{\mathfrak{p}\in\mathcal{P}} \alpha_\mathfrak{p}\mathfrak{p}$, באשר $\alpha_\mathfrak{p}$ הם מספרים שלמים אשר כמעט כלם שוים לאפס. **התומך** של $\mathfrak{a}$ יהיה הקבוצה $\mathrm{Supp}(\mathfrak{a}) = \{\mathfrak{p} \in \mathcal{P} \mid \alpha_\mathfrak{p} \neq 0\}$. נגדיר הומומורפיזם $v_\mathfrak{p}\colon \mathcal{D} \to \mathbb{Z}$ על ידי $v_\mathfrak{p}(\mathfrak{a}) = \alpha_\mathfrak{p}$. לכאורה משתמשים אנו ב $v_\mathfrak{p}$ בשני מובנים שונים. אולם למעשה השמושים תואמים זה לזה. ואכן נגדיר את **המחלק** של אבר x של $F^\times$ כ $\mathrm{div}(x) = \sum v_\mathfrak{p}(x)\mathfrak{p}$. זוהי הגדרה טובה כיון ש $v_\mathfrak{p}(x) = 0$ עבור כמעט כל $\mathfrak{p} \in \mathcal{P}$. אם x **קבוע**, כלומר אם $x \in K$, אזי $v_\mathfrak{p}(x) = 0$ לכל $\mathfrak{p} \in \mathcal{P}$ ולכן $\mathrm{div}(x) = 0$. אם x אינו קבוע, נתבונן בהערכה v_0 (לחלופין v_∞) של $K(x)/K$ המֻגדרת על ידי $v_0(x) = 1$ (לחלופין $v_\infty(x) = -1$). כל $\mathfrak{p} \in \mathcal{P}$ שעבורו $v_\mathfrak{p}$ שוכן מעל v_0 (לחלופין v_∞), נקרא **אפס** (לחלופין **קטב**) של x. מספר האפסים (לחלופין, קטבים) של x סופי וגדול מאפס. לכן, $\mathrm{div}(x) \neq 0$. נגדיר את **מחלק האפסים** ו**מחלק הקטבים** של x בעזרת הנסחאות הבאות:

$$\mathrm{div}_0(x) = \sum_{v_\mathfrak{p}(x)>0} v_\mathfrak{p}(x)x, \qquad \mathrm{div}_\infty(x) = -\sum_{v_\mathfrak{p}(x)<0} v_\mathfrak{p}(x)x.$$

אזי $\mathrm{div}(x) = \mathrm{div}_0(x) - \mathrm{div}_\infty(x)$. בפרט, $v_\mathfrak{p}(\mathrm{div}(x)) = v_\mathfrak{p}(x)$.

נגדיר את **המעלה** של מחלק $\mathfrak{a}$ על ידי $\deg(\mathfrak{a}) = \sum v_\mathfrak{p}(\mathfrak{a})\deg(\mathfrak{p})$. הפונקציה $\deg : \mathcal{D} \to \mathbb{Z}$ המתקבלת באפן כזה הנה הומומורפיזם. אם $F/K(x)$ הרחבה פרידה, נובע מנסחה (4) של סעיף ב ש

$$\deg(\mathrm{div}_0(x)) = [F : K(x)] = \deg(\mathrm{div}_\infty(x)) \,. \tag{2}$$

ואכן, אם $v_1,\dots,v_r$ הן ההערכות של F המונחות מעל v_0 ו $\mathfrak{p}_i$ הוא המחלק הראשוני של F/K המתאים ל v_i, אזי $e(v_i/v_0)=v_i(x)$ ובסימון $\bar{F}_i=\bar{F}_{\mathfrak{p}_i}$ מקבלים

$$.f(v_i/v_0)=[\bar{F}_i:\overline{K(t)}_{v_0}]=[\bar{F}_i:K]=\deg(\mathfrak{p}_i)$$

לכן,

$$\begin{aligned}\deg(\mathrm{div}_0(x))=\sum_{i=1}^{r}v_i(\mathrm{div}_0(x))\deg(\mathfrak{p}_i)&=\sum_{i=1}^{r}v_i(x)[\bar{F}_i:K]\\&=\sum_{i=1}^{r}e(v_i/v_0)f(v_i/v_0)=[F:K(x)]\end{aligned}$$

בדרך כלל מוכיחים את הנסחה (2) באפן ישיר, גם במקרה ש $F/K(x)$ אינה הרחבה פרידה. אחר כך מסיקים מ (2) את הנסחה (4) של סעיף ב. מ (2) נובע $\deg(\mathrm{div}(x))=0$.

נגדיר יחס סדר חלקי על $\mathcal{D}$ על ידי שנקבע $\mathfrak{a}\le\mathfrak{b}$ אם ורק אם $v_\mathfrak{p}(\mathfrak{a})\le v_\mathfrak{p}(\mathfrak{b})$ לכל $\mathfrak{p}\in\mathcal{P}$. לכל מחלק $\mathfrak{a}$ נתאים מרחב וקטורי $\mathcal{L}(\mathfrak{a})$ מעל K:

$$.\mathcal{L}(\mathfrak{a})=\{x\in F\mid\ \mathrm{div}(x)+\mathfrak{a}\ge 0\}$$

אפשר להראות ש $\dim(\mathfrak{a}):=\dim(\mathcal{L}(\mathfrak{a}))<\infty$.

מחלק מהצורה $\mathrm{div}(x)$ שבו $x\in F^\times$ יְכֻנה **מחלק ראשי.** הואיל ו $\mathrm{div}(xy)=\mathrm{div}(x)+\mathrm{div}(y)$, נקבל ש $xy\in\mathcal{L}(\mathfrak{a}+\mathfrak{b})$ אם $x\in\mathcal{L}(\mathfrak{a})$ ו $y\in\mathcal{L}(\mathfrak{b})$. לכן, קבוצת כל המחלקים הראשיים מהוָה תת חבורה של $\mathcal{D}$. חבורת המנה $\mathcal{C}:=\mathcal{D}/\mathrm{div}(F^\times)$ מכונה **חבורת מחלקות המחלקים** של F/K. כל אבר של $\mathcal{C}$ הנו **מחלקת מחלקים.** אם שני מחלקים נמצאים באותה המחלקה, אזי יש להם אותו הממד ואותה המעלה. לכן נוכל לדבר על **הממד** ו**המעלה** של מחלקת מחלקים.

בין המחלקות קימת מחלקה מיוחדת המכונה **תקנית** (**קנונית**). כל מחלק $\mathfrak{w}$ במחלקה זו נקרא **מחלק תקני.** בנוסף לזה קים מספר שלם אי שלילי g, המכונה **הגזע** (genus) של F/K, בעל התכונה הבאה: לכל מחלק $\mathfrak{a}$

$$.\dim(\mathfrak{a})=\deg(\mathfrak{a})+1-g+\dim(\mathfrak{w}-\mathfrak{a}) \tag{3}$$

נסחה זו הנה אחת מהצורות השקולות של **משפט רימן־רוך.** הטענות הבאות הופכות נסחה זו ליותר שמושית:

(4a) $\dim(0)=1$. אם $x\in F^\times$, אזי $\deg(\mathrm{div}(x))=0$ ו $\dim(\mathrm{div}(x))=1$.

(4b) $\dim(\mathfrak{w})=g$ ו $\deg(\mathfrak{w})=2g-2$.

(4c) אם $\deg(\mathfrak{a})<0$, אזי $\dim(\mathfrak{a})=0$.

(4d) אם $\deg(\mathfrak{a}) > 2g-2$, אזי $\dim(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g$.

הוכחת (4a): לפי ההגדרה $\mathcal{L}(0) = \{y \in F \mid \operatorname{div}(y) \geq 0\}$. בפרט, אם $y \in \mathcal{L}(0)$, אזי אין ל y קטבים ולכן y קבוע. לכן $\mathcal{L}(0) = K$ וממדו הוא אפוא 1.

באפן דומה, אם $x \in F^\times$ ו $y \in \mathcal{L}(\operatorname{div}(x))$, אזי $\operatorname{div}(xy) \geq 0$ ולכן, $y \in x^{-1}K$. מכאן נובע שוב ש $\dim(\operatorname{div}(x)) = 1$.

הוכחת (4b): נציב $\mathfrak{a} = 0$ ב (3) ונקבל לפי (4a) ש $1 = \dim(0) = 1 - g + \dim(\mathfrak{w})$. לכן, $\dim(\mathfrak{w}) = g$.
עתה נציב $\mathfrak{a} = \mathfrak{w}$ ב (3): $g = \dim(\mathfrak{w}) = \deg(\mathfrak{w}) + 1 - g + \dim(0)$. לכן, $\deg(\mathfrak{w}) = 2g-2$.

הוכחת (4c): אם $\deg(\mathfrak{a}) < 0$ ואם $y \in \mathcal{L}(\mathfrak{a})$ ו $y \neq 0$, אזי $\operatorname{div}(y) + \mathfrak{a} \geq 0$. לכן,

$$0 = \deg(\operatorname{div}(y)) \geq -\deg(\mathfrak{a}) > 0,$$

סתירה. לכן, $\dim(\mathcal{L}(\mathfrak{a})) = 0$.

הוכחת (4d): אם $\deg(\mathfrak{a}) > 2g-2$, אזי, לפי (4b), $\deg(\mathfrak{w} - \mathfrak{a}) < 0$. לכן, לפי (4c), $\dim(\mathfrak{w} - \mathfrak{a}) = 0$. לכן, לפי (3), $\dim(\mathfrak{a}) = \deg(\mathfrak{a}) + 1 - g$, כפי שהיה להוכיח.

י. שדות פונקציות רציונליות

יהי K שדה ו t אבר נעלה מעל K. נתבונן בשדה הפונקציות הרציונליות $F = K(t)$ מעל K ונוכיח שגזעו שווה ל 0.

ראשית נעיר ש K סגור אלגברית ב F. ואכן, יהי $u \in F$ אבר אלגברי מעל K. נרשם $u = \frac{f(t)}{g(t)}$, באשר $f, g \in K[t]$ הם פולינומים. נניח בשלילה ש $u \notin K$. אזי אגף שמאל של השויון $f(t) - ug(t) = 0$ אינו שוה לאפס באפן זהותי כפולינום ב t. לכן t אלגברי מעל K, בסתירה להנחה.

בסעיף ב.ג ראינו שיש ל F שני סוגים של מחלקים ראשוניים. ראשית, המחלקים $\mathfrak{p}$ המתאימים לפולינומים האי פריקים $p(t)$. במקרה זה $\bar{F}_{\mathfrak{p}} \cong K[t]/p(t)K[t]$ ולכן $\deg(\mathfrak{p}) = \deg(p(t))$. שנית יש ל F/K המחלק $\mathfrak{p}_\infty$ המתאים לפולינום האי פריק t^{-1} ב $K[t^{-1}]$. לכן $\deg(\mathfrak{p}_\infty) = 1$.

פונקציה רציונלית $f(t)$ כלשהיא נתנת לפרוק לגורמים אי פריקים בצורה

$$e_i \in \mathbb{Z} \qquad f(t) = p_1(t)^{e_1} \cdots p_r(t)^{e_r}.$$

המחלק הראשי המתאים לה הנו

$$\operatorname{div}(f(t)) = \sum_{i=1}^{r} e_i \mathfrak{p}_i - \deg(f(t))\mathfrak{p}_\infty.$$

באשר $\mathfrak{p}_i$ הוא המחלק הראשוני המתאים ל $p_i(t)$ ו $\deg(f(t))$ הנו ההבדל של המעלות של המונה והמכנה של $f(t)$. מנסחה זו אנו מקבלים שהמרחב $\mathcal{L}(n\mathfrak{p}_\infty)$ מורכב בדיוק מכל הפולינומים שמעלתם $\le n$. בסיס למרחב זה הנו $1, t, t^2, \ldots, t^n$. לכן $\dim(n\mathfrak{p}_\infty) = n + 1$. אם $n > 2g - 2$ נקבל ממשפט רימן־רוך ש $\dim(n\mathfrak{p}_\infty) = n\deg(\mathfrak{p}_\infty) + 1 - g$, כלומר, $n + 1 = n + 1 - g$ ולכן $g = 0$. הוכחנו אפוא:

משפטון י.א: *אם $F = K(t)$ הוא שדה פונקציות רציונליות מעל שדה K, אזי $g = 0$.*

המשפט ההפוך מתאר את כל האפשרויות לשדה פונקציות בעל גזע 0.

משפטון י.ב: *יהי F/K שדה פונקציות בעל גזע 0. אזי $F = K(t)$ הוא שדה פונקציות רציונליות מעל K או ש F הוא הרחבה רבועית של $K(t)$.*

אם בנוסף לזה יש ל F/K מחלק ראשוני $\mathfrak{p}$ ממעלה 1, אזי $F = K(t)$.

הוכחה: נבחר ל F/K מחלק תקני $\mathfrak{w}$. אזי $\deg(\mathfrak{w}) = -2$. לכן $\deg(-\mathfrak{w}) = 2 > 2g - 2$. לכן, לפי משפט רימן־רוך, $\dim(-\mathfrak{w}) = 3$. קימים אפוא ב $\mathcal{L}(-\mathfrak{w})$ שלשה אברים x, y, z שאינם תלויים לינארית מעל K. בפרט נקבל ש $t = yx^{-1}$ נעלה מעל K. מתקים

$$\operatorname{div}(t) = (\operatorname{div}(y) - \mathfrak{w}) - (\operatorname{div}(x) - \mathfrak{w}),$$

$0 \geq \mathrm{div}(y) - \mathfrak{w}$ ו $0 \geq \mathrm{div}(x) - \mathfrak{w}$. לכן $\mathfrak{w}$ $\mathrm{div}_\infty(t) \leq \mathrm{div}(x) -$. לכן,

$$[F : K(t)] = \deg(\mathrm{div}_\infty(t)) \leq \deg(\mathrm{div}(x) - \mathfrak{w}) = 2.$$

מכאן נובע החלק הראשון של המשפטון.

נניח עתה שקיים ל F/K מחלק ראשוני $\mathfrak{p}$ ממעלה 1. ממשפט רימן־רוך נובע ש $\dim(\mathfrak{p}) = 2$. לכן קיימים ב $\mathcal{L}(\mathfrak{p})$ שני אברים t, u שאינם תלויים לינארית מעל K. אחד מהם, נאמר t, אינו קבוע. הוא מקיים $\mathrm{div}(t) + \mathfrak{p} \geq 0$ ולכן $\mathfrak{p} = \mathrm{div}_\infty(t)$. לכן, $[F : K(t)] = \deg(\mathrm{div}_\infty(t)) = 1$. כך ש $F = K(t)$. ∎

הערה י.ג: אפשר להראות שאם F/K הוא שדה פונקציות בעל גזע אפס שאינו רציונלי ו $\mathrm{char}(K) \neq 2$, אזי $F = K(t, u)$ באשר $u^2 = at^2 + c$ ו $a, c \in K$, $a \neq 0$. ∎

∎

יא. שדות אלפטיים

שדות הפונקציות הפשוטים ביותר לאחר שדות פונקציות רציונליות הם ההרחבות הרבועיות של שדות פונקציות רציונליות. מבין השדות האלו נתעכב בסעיף זה על אלו בעלי גזע 1 ומתוכם במיוחד על אלו בעלי מחלק ראשוני ממעלה אחד. נקרא להם **שדות אלפטיים**.

יהי K שדה בעל אפיון שונה מ 2, יהי x אבר נעלה מעל K ויהי F הרחבה רבועית של $K(x)$. עוד נניח שאין קימת הרחבה אלגברית L של K כך ש $F = L(x)$. אזי K סגור אלגברית ב F.

נתן לרשם את F בצורה $F = K(x, y)$ באשר y מקים משואה רבועית אי פריקה

$$b(x), c(x) \in K(x) \qquad y^2 + b(x)y + c(x) = 0.$$

על ידי השלמה לרבוע נעבר למשואה

$$\left(y + \frac{b(x)}{2}\right)^2 + c(x) - \frac{b(x)^2}{4} = 0$$

ולכן נוכל להניח ש y מקים משואה מהצורה $y^2 = f(x)$. את $f(x)$ אפשר לפרק לגורמים אי פריקים ועל ידי השמטת כל החזקות הזוגיות של פולינומים אי פריקים נתן להניח ש $f(x)$ הוא פולינום ממעלה m שאינו מתחלק ברבוע של פולינום אי פריק.

הערה יא.א: אוטומורפיזמים של שדות פונקציות. יהי F/K שדה פונקציות אלגבריות של משתנה אחד ויהי σ אוטומורפיזם של F מעל K. לכל $\mathfrak{p} \in \mathcal{P}$ מגדיר התנאי

$$v_{\sigma\mathfrak{p}}(z) = v_{\mathfrak{p}}(\sigma^{-1}z)$$

מחלק ראשוני $\sigma\mathfrak{p}$ של F/K. אם τ הוא אוטומורפיזם נוסף של F/K, אזי $(\tau\sigma)\mathfrak{p} = \tau(\sigma\mathfrak{p})$. כמו כן, משאיר אוטומורפיזם הזהות את $\mathfrak{p}$ במקומו. לכן, σ משרה תמורה של $\mathcal{P}$. נתן להרחיב תמורה זו באפן לינארי לאוטומורפיזם של $\mathcal{D}$. באפן מפרש, אם $\mathfrak{a} = \sum \alpha_{\mathfrak{p}}\mathfrak{p}$, אזי $\sigma\mathfrak{a} = \sum \alpha_{\mathfrak{p}}\sigma\mathfrak{p}$. בפרט $\mathfrak{a} \leq \mathfrak{b}$ אם ורק אם $\sigma\mathfrak{a} \leq \sigma\mathfrak{b}$. כמו כן עבור $z \in F^\times$ נקבל מההצגה $\operatorname{div}(z) = \sum v_{\mathfrak{p}}(z)\mathfrak{p}$ ש

$$\sigma(\operatorname{div}(z)) = \sum v_{\mathfrak{p}}(z)\sigma\mathfrak{p} = \sum v_{\sigma^{-1}\mathfrak{p}}(z)\mathfrak{p} = \sum v(\sigma z)\mathfrak{p} = \operatorname{div}(\sigma z).$$

אם $\mathfrak{a}$ הוא מחלק, אזי התנאי $\operatorname{div}(z) + \mathfrak{a} \geq 0$ שקול אפוא לתנאי $\operatorname{div}(\sigma z) + \sigma\mathfrak{a} \geq 0$. לכן, $\sigma\mathcal{L}(\mathfrak{a}) = \mathcal{L}(\sigma\mathfrak{a})$. ∎

משפטון יא.ב: *יהי K שדה בעל אפיון שונה מ 2, יהי x אבר נעלה מעל K, יהי $f(x)$ פולינום ב $K[x]$ ממעלה חיובית m שאינו מתחלק ברבוע, יהי y אבר המקיים $y^2 = f(x)$ ויהי $F = K(x,y)$. אזי F הוא שדה פונקציות מעל K, $[F : K(x)] = 2$ והגזע שלו נתן על ידי הנסחה*

$$g = \begin{cases} \frac{m-2}{2} & \text{if } 2|m \\ \frac{m-1}{2} & \text{if } 2 \nmid m \end{cases}$$

בפרט, $g = 0$ עבור $m = 1,2$, $g = 1$ עבור $m = 3,4$, $g = 2$ עבור $m = 5,6$ וכו'.

הוכחה: כדי להוכיח ש F/K הנו שדה פונקציות עלינו להוכיח ש K סגור אלגברית בתוך F. לצרך זה נעיר קודם כל ש $y \notin K(x)$. אחרת קימים פולינומים g,h ב $K[x]$ זרים זה לזה כך ש $y = \frac{g(x)}{h(x)}$. מ $g(x)^2 = f(x)h(x)^2$ היינו מקבלים ש $g(x)^2|f(x)$, בסתירה להנחה.

נניח עתה בשלילה ש F מקיף שדה L אלגברי מעל K ממעלה גדולה מ 1. אזי $[L(x) : K(x)] = [L : K]$ ו $F \supseteq L(x) \supseteq K(x)$. לכן, $F = L(x)$. לכן, $[L : K] = 2$. מתקים אפוא $L = K(c)$, באשר $c^2 = b \in K$. לכן, $F = K(x,c)$ ו $c \notin K(x)$. קימים אפוא $u(x), v(x) \in K(x)$ כך ש $y = u(x) + v(x)c$. העלאה ברבוע תתן, $f(x) = u(x)^2 + v(x)^2b + 2u(x)v(x)c$. השואת מקדמי c בשני האגפים תתן $u(x)v(x) = 0$. אם $u(x) = 0$, אזי $f(x) = v(x)^2b$. אם $v(x) = 0$, אזי $f(x) = u(x)^2$. בשני המקרים נקבל סתירה להנחה ש $f(x)$ אינו מתחלק ברבוע או ש $f(x)$ אינו קבוע. מסקנה: F/K הנו שדה פונקציות.

את נסחת הגזע נוכיח רק במקרה החשוב לנו ביותר שבו $m = 3$. עלינו להוכיח שבמקרה זה $g = 1$.

כל אבר z של F נתן להצגה בצורה יחידה על ידי $z = r_1(x) + yr_2(x)$, באשר $r_i(x) \in K(x)$. נסמן את האבר הלא טריביאלי של $\mathrm{Gal}(F/K(x))$ ב σ. הוא יקֵים $\sigma z = r_1(x) - yr_2(x)$.

יהי עתה n מספר טבעי כך ש $z \in \mathcal{L}(n \cdot \mathrm{div}_\infty(x))$. לפי הערה יא.א, גם $\sigma z \in \mathcal{L}(n \cdot \mathrm{div}_\infty(x))$. לכן $2r_1(x) = z + \sigma z \in \mathcal{L}(n \cdot \mathrm{div}_\infty(x))$. במלים אחרות, $\mathrm{div}(r_1(x)) + n \cdot \mathrm{div}_\infty(x) \geq 0$. בפרט, לכל מחלק ראשוני $\mathfrak{p}$ של $F/K(x)$ שאינו קטב של x מתקים $v_\mathfrak{p}(r_1(x)) \geq 0$. לכן $r_1(x)$ הנו פולינום ב x. אם $\mathfrak{p}$ הנו קטב של x, כלומר $v_\mathfrak{p}(x) < 0$, אזי $v_\mathfrak{p}(r_1(x)) = \deg(r_1)v_\mathfrak{p}(x)$. לכן, $\deg(r_1)v_\mathfrak{p}(x) - nv_\mathfrak{p}(x) \geq 0$. מכאן, $\deg(r_1) \leq n$.

כמו כן

$$r_1(x)^2 - f(x)r_2(x)^2 = r_1(x)^2 - y^2r_2(x)^2 = z \cdot \sigma z \in \mathcal{L}(2n \cdot \mathrm{div}_\infty(x))$$

הואיל וגם $r_1(x)^2 \in \mathcal{L}(2n \cdot \mathrm{div}_\infty(x))$ נקבל מכאן ש $f(x)r_2(x)^2 \in \mathcal{L}(2n \cdot \mathrm{div}_\infty(x))$. כמו מקודם נובע מכאן ש $f(x)r_2(x)^2$ הוא פולינום ממעלה $\leq 2n$. הואיל ו $f(x)$ הוא פולינום ממעלה 3 שאינו מתחלק ברבוע, נובע מכאן ש $r_2(x)$ הוא פולינום ממעלה שאינה עולה על $n - \frac{3}{2}$. אולם $\deg(r_2(x))$ הוא מספר שלם ולכן, $\deg(r_2(x)) \leq n - 2$.

מצד שני אם $v_{\mathfrak{p}}(x) < 0$, אזי $2v_{\mathfrak{p}}(y) = 3v_{\mathfrak{p}}(x)$. לכן, עבור $i = 0,1$ ו $j \leq n-2$, נקבל $v_{\mathfrak{p}}(y^i x^j) = iv_{\mathfrak{p}}(y) + jv_{\mathfrak{p}}(x) \geq \left(\frac{3}{2} + (n-2)\right)v_{\mathfrak{p}}(x) \geq nv_{\mathfrak{p}}(x)$. לכן

$$1, x, \ldots, x^n, y, yx, \ldots, yx^{n-2}$$

מהוה בסיס ל $\mathcal{L}(n \cdot \mathrm{div}_\infty(x))$. מכאן נובע ש $\dim(n \cdot \mathrm{div}_\infty(x)) = 2n$. בנוסף לזה

$$\deg(\mathrm{div}_\infty(x)) = [F : K(x)] = 2\ .$$

לכן, אם $n > g-1$, נקבל ממשפט רימן־רוך ש

$$2n = \dim(n \cdot \mathrm{div}_\infty(x)) = 2n + 1 - g.$$

לכן $g = 1$, כפי שנטען.

לבסוף נעיר שאם $m = 2$, אזי בסימונים דלעיל נקבל ש $r_2(x)$ הנו פולינום ממעלה שאינה עולה על $n-1$ ו $\dim(n \cdot \mathrm{div}_\infty(x)) = 2n+1$. משפט רימן־רוך יתן (עבור n גדול) $2n+1 = 2n+1-g$ ולכן $g = 0$.

∎

הערה יא.ג: מחלקי האינסוף של x ושל y. במהלך הוכחת משפטון יא.ג עמדנו על כך ש $\deg(\mathrm{div}_\infty(x)) = [F : K(x)] = 2$. לכן יש ל $\mathrm{div}_\infty(x)$ שלש אפשרויות:

(א) $\mathrm{div}_\infty(x) = 2\mathfrak{p}$, באשר $\mathfrak{p}$ מחלק ראשוני ו $\deg(\mathfrak{p}) = 1$.

(ב) $\mathrm{div}_\infty(x) = \mathfrak{p}$, באשר $\mathfrak{p}$ מחלק ראשוני ו $\deg(\mathfrak{p}) = 2$.

(ג) $\mathrm{div}_\infty(x) = \mathfrak{p} + \mathfrak{q}$, באשר $\mathfrak{p}$ ו $\mathfrak{q}$ מחלקים ראשוניים שונים ממעלה 1.

כמו כן עמדנו על כך ש $v_{\mathfrak{p}}(x) < 0$ אם ורק אם $v_{\mathfrak{p}}(y) < 0$ ובמקרה זה $2v_{\mathfrak{p}}(y) = 3v_{\mathfrak{p}}(x)$. לכן $2\mathrm{div}_\infty(y) = 3\mathrm{div}_\infty(x)$. אם מתקימות אחת מהאפשרויות (ב) או (ג), אזי $v_{\mathfrak{p}}(x) = -1$. לכן, $2v_{\mathfrak{p}}(y) = -3$, סתירה. לכן, $\mathrm{div}_\infty(x) = 2\mathfrak{p}$ ו $\mathrm{div}_\infty(y) = 3\mathfrak{p}$, באשר $\mathfrak{p}$ הוא מחלק ראשוני ממעלה 1. ∎

כדי להוכיח את ההפוך של משפטון יא.ב נביא קודם את התוצאה הבאה:

למה יא.ד: *יהי K שדה בעל אפיון שונה מ 2 ומ 3. יהי $f \in K[X]$ פולינום ממעלה 3. אם יש ל f שרש כפול ב $\tilde{K}$, אזי שרש זה שיך ל K.*

הוכחה: נסמן ב L את שדה הפצול של f מעל K. הוא הרחבת גלואה של K. לפי ההנחה $f(X) = (X-c)^2(X-c')$. בין אם $c = c'$ ובין אם $c \neq c'$, מתקים $\sigma c = c$ לכל $\sigma \in \mathrm{Gal}(L/K)$. לכן $c \in K$. ∎

משפטון יא.ה: *יהי F/K שדה פונקציות אלגבריות של משתנה אחד בעל גזע 1. נניח ש $\mathrm{char}(K) \neq 2,3$ ושקים ל F/K מחלק ראשוני $\mathfrak{o}$ ממעלה 1. אזי $F = K(x,y)$ באשר $y^2 = x^3 + ax + b$ ו $f(X) = X^3 + aX + b$ הוא פולינום עם מקדמים ב K בלי שרשים כפולים.*

הוכחה: ממשפט רימן־רוך נובע ש $\dim(n\mathfrak{o}) = n$ לכל n טבעי. בפרט, $\dim(2\mathfrak{o}) = 2$. לכן קים ל $\mathcal{L}(2\mathfrak{o})$ בסיס מהצורה $1, x$ ו x אינו קבוע ולכן $x \notin \mathcal{L}(\mathfrak{p}) = K$. בפרט $\mathrm{div}(x) + 2\mathfrak{o} \geq 0$ ולכן $\mathrm{div}_\infty(x) = 2\mathfrak{o}$. לכן, $[F : K(x)] = \deg(\mathrm{div}_\infty(x)) = 2$.

המרחב $\mathcal{L}(3\mathfrak{o})$ מקיף את $\mathcal{L}(2\mathfrak{o})$ וממדו 3. לכן אפשר לבחר y ב F כך ש $\{1, x, y\}$ הנו בסיס של $\mathcal{L}(3\mathfrak{o})$ מעל K. בפרט $y \notin \mathcal{L}(2\mathfrak{o})$ ולכן $\mathrm{div}_\infty(y) = 3\mathfrak{o}$. מכאן נובע ש $v_\mathfrak{o}(x) = -2$ ו $v_\mathfrak{o}(y) = -3$. לכן יש לששת האברים $1, x, y, x^2, xy, x^3$ ערכי־$v_\mathfrak{o}$ שונים זה מזה. זה גורר שאברים אלו אינם תלויים לינארית מעל K.

מאידך שיכים שבעת האברים $1, x, y, x^2, xy, y^2, x^3$ למרחב $\mathcal{L}(6\mathfrak{o})$ שממדו 6. לכן הם תלויים לינארית מעל K. קימים אפוא קבועים $a_1, \ldots, a_6 \in K$ כך ש

$$y^2 + a_1xy + a_2y = a_3x^3 + a_4x^2 + a_5x + a_6. \tag{1}$$

האבר y אינו שיך ל $K(x)$, אחרת $y = \frac{p(x)}{q(x)}$, באשר p ו q הם פולינומים זרים זה לזה. אם היינו מציבים בטוי זה ב (1), היינו מקבלים ש $q(x)$ קבוע ו $p(x)$ הוא פולינום ממעלה שאינה עולה על 1. כלומר $y = b_1x + b_2$ באשר $b_1, b_2 \in K$. זה היה סותר את אי התלות של $1, x, y$ מעל K. מהפסקה הראשונה של ההוכחה נובע ש $F = K(x,y)$.

אם נשתמש בהנחה ש $\mathrm{char}(K) \neq 2$, נוכל על ידי החלפות משתנים מתאימות להגיע לקשר המבוקש במשפט. ביתר דיוק, אם נחליף את y ב $y + \frac{1}{2}a_1x$, נוכל להניח קודם כל ש $a_1 = 0$. אחר כך נחליף את y ב $y + \frac{a_2}{2}$ כדי להניח ש $a_2 = 0$. אם במצב זה $a_3 = 0$, אזי $g = 0$ (לפי משפטון יא.א), בסתירה להנחה. לכן $a_3 \neq 0$ ונוכל להחליף את x ב a_3x ואת y ב a_3y כדי להניח ש $a_3 = 1$. לבסוף נחליף את x ב $x + \frac{a_4}{3}$ כדי להניח ש $a_4 = 0$. המשואה (1) מקבלת אפוא את הצורה $y^2 = x^3 + ax + b$.

לבסוף, נניח בשלילה שלפולינום $f(x) = x^3 + ax + b$ יש שרש כפול ב $\tilde{K}$, כלומר $f(x) = (x - c_1)(x - c_2)^2$, באשר $c_1, c_2 \in \tilde{K}$. לפי למה יא.ד, $c_1, c_2 \in K$. לכן, $K(x,y) = K(y')$, באשר $y' = \frac{y}{x - c_1}$. בפרט F/K הוא שדה פונקציות רציונליות ולכן בעל גזע 0 (משפטון י.א), בסתירה להנחה. ∎

יב. נקֻדות פשוטות על עקמים מישוריים

המטרה בסעיף זה היא לתאר את ההתאמה בין נקֻדות פשוטות על עקמים מישוריים לבין מחלקים ראשוניים של שדות הפונקציות של העקמים האלו. לצרך זה נזקק לכמה מושגים ותוצאות מאלגברה קומוטטיבית שאותן לא נוכיח. בתאור מושגים אלו נשתמש במונח "חוג" כקיצור ל"חוג חלופי עם יחידה", לרב אפילו ל"תחום שלמות".

חוג R נקרא **חוג נטר** אם מתקיימים אחד משני התנאים השקולים הבאים:

$(1a)$ כל אידאל של R נוצר סופית.

$(1b)$ כל שרשרת עולה של אידאלים של R הנה סופית.

לדגמה, כל שדה K הוא חוג נטר. חוג ראשי הוא חוג נטר. בפרט, $\mathbb{Z}$ ו $K[X]$ הם חוגי נטר. אם $\varphi\colon R \to R'$ הוא אפימורפיזם של חוגים ו R הוא חוג נטר, גם R' הוא חוג נטר. אם R הוא תחום שלמות נטרי ו $\mathfrak{p}$ הוא אידאל ראשוני של R, אזי ה**מקום** של R ב $\mathfrak{p}$, כלומר

$$R_\mathfrak{p} = \left\{ \frac{a}{b} \mid a, b \in R,\ b \notin \mathfrak{p} \right\}$$

הוא חוג נטר. בחוג זה

$$\mathfrak{p}R_\mathfrak{p} = \left\{ \frac{a}{b} \mid a \in \mathfrak{p},\ b \in R \smallsetminus \mathfrak{p} \right\}$$

הוא האידאל המרבי היחיד. בפרט, $R_\mathfrak{p}$ הוא "חוג מקומי".

באפן כללי, **חוג מקומי** הוא חוג R בעל אידאל מרבי יחיד $\mathfrak{m}$. הואיל וכל אבר שאינו הפיך בחוג מוכל באידאל נאות של R, נקבל מההגדרה ש $R \smallsetminus \mathfrak{m}$ הוא חבורת האברים ההפיכים $R^\times$ של R.

למה יב.א: *יהי R_0 תחום נטר ויהי $R = R_0[x_1, \ldots, x_n]$ הוא תחום שלמות נוצר סופית מעל R_0, אזי R הוא חוג נטר. לכן, גם כל מקום של R באידאל ראשוני הוא חוג נטר.*

הוכחה: המקרה שבו $n = 1$ ו x_1 נעלה מעל R_0 ידוע כ**משפט הבסיס של הלברט**. ממנו נובעת הלמה, באנדוקציה, עבור המקרה שבו $x_1, \ldots, x_n$ אינם תלויים אלגברית מעל R_0, כלומר R הוא חוג פולינומים ב n משתנים מעל R_0. באפן כללי, R הוא חוג מנה של חוג פולינומים ולכן הוא חוג נטר. ∎

למה יב.ב (הלמה של Nakayama): *יהי V מודול נוצר סופית מעל חוג מקומי R. יהי $\mathfrak{m}$ האידאל המרבי היחיד של R. אם $\mathfrak{m}V = V$, אזי $V = 0$.*

הוכחה: יהי n המספר המזערי של יוצרים של V מעל R. נניח בשלילה ש $n \geq 1$. אזי קיימים $v_1, \ldots, v_n$ כך ש $V = \sum_{i=1}^n Rv_i$. לפי ההנחה, קיימים $m_1, \ldots, m_n \in \mathfrak{m}$ כך ש $v_n = \sum_{i=1}^n m_i v_i$. לכן, $(1 - m_n)v_n = \sum_{i=1}^{n-1} m_i v_i$. הואיל ו $1 - m_n$ אינו שיך ל $\mathfrak{m}$, הוא הפיך ב R. לכן,

$$v_n = \sum_{i=1}^{n-1} (1 - m_n)^{-1} m_i v_i.$$

מכאן ש $V = \sum_{i=1}^{n-1} Rv_i$, בסתירה למזעריות של n. ∎

למה יב.ג: *יהי R תחום נטר מקומי בעל אידאל מרבי $\mathfrak{m}$. נסמן $F = \mathrm{Quot}(R)$. נניח ש $\mathfrak{m}$ נוצר על ידי אבר אחד t. אזי קימת הערכה בדידה v של F כך ש $R = O_v$ ו $v(t) = 1$.*

הוכחה: נתבונן באידאל $\mathfrak{a} = \bigcap_{n=1}^{\infty} \mathfrak{m}^n$ של R. בפרט, $\mathfrak{a}$ הוא מודול־R נוצר סופית. מהקשר $\mathfrak{m} \cdot \mathfrak{m}^m = \mathfrak{m}^{n+1}$ נובע ש $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$. לכן, לפי למה יב.ב, $\mathfrak{a} = 0$.

מההנחה נובע אפוא שכל אבר שונה מאפס a של R נתן להצגה בצורה $a = ut^n$ באשר $n \geq 0$ ו $u \in R^\times$. נגדיר אפוא $v(a) = n$ ונרחיב את v לכל F על ידי הנסחה $v\left(\frac{a}{b}\right) = v(a) - v(b)$, $v(0) = \infty$. הפונקציה $v\colon F \to \mathbb{Z} \cup \{\infty\}$ תהיה ההערכה הבדידה המבוקשת של R. ∎

יהי עתה K שדה ו $f \in K[X,Y]$ פולינום שונה מאפס. לכל הרחבה L של K נוכל להתבונן בקבוצה $\Gamma(L) = \{(a,b) \in L^2 \mid f(a,b) = 0\}$. אם $L \subseteq L'$ אזי $\Gamma(L) \subseteq \Gamma(L')$. לכן Γ הוא פנקטור מקטגורית השדות המקיפים את K לקטגורית הקבוצות. נקרא ל Γ **העקם האפיני המישורי** המוגדר על ידי f מעל K. אבר של $\Gamma(L)$ יקרא **נְקֻדה רציונלית־L** של Γ.

אם $f(X,Y)$ אי פריק ב $K[X,Y]$, נבחר אבר נעלה x מעל K ונבחר y בסגור האלגברי של $K(x)$ כך ש $f(x,y) = 0$. מהלמה של גאוס נובע ש $f(x,Y) = \mathrm{irr}(y, K(x))$. לכן, אם $g \in K[X,Y]$, אזי $g(x,y) = 0$ אם ורק אם f מחלק את g ב $K[X,Y]$. במלים אחרות, ההעתקה $(X,Y) \to (x,y)$ נתנת להרחבה להומומורפיזם של $K[X,Y]$ על $K[x,y]$ שגרעינו, $K[X,Y]f(X,Y)$. לכן, $K[x,y] \cong K[X,Y]/K[X,Y]f(X,Y)$. תחום השלמות, $K[x,y]$ נקרא **חוג הקואורדינטות** של Γ מעל K. מהנאמר לעיל, $K[x,y]$ הוא תחום נטר. שדה המנות שלו, $K(x,y)$, נקרא **שדה הפונקציות הרציונליות** של Γ מעל K. הזוג (x,y) נקרא **נְקֻדה יוצרת** של Γ מעל K.

מאי הפריקות של f נובע שאין קימים Γ_1 ו Γ_2 מעל K כך ש $\Gamma(\tilde{K}) = \Gamma_1(\tilde{K}) \cup \Gamma_2(\tilde{K})$ וכל אחד מהמאוחדים באגף ימין מוכל ממש באגף שמאל. במקרה זה נאמר ש Γ **אי פריק מעל** K. להפך, אם Γ עקם אי פריק מעל K, אזי קים $f \in K[X,Y]$ אי פריק כך ש $\Gamma(L) = \{(a,b) \in L^2 \mid f(a,b) = 0\}$ לכל הרחבה L של K.

אפשר להראות שאם $f(X,Y)$ אי פריק גם ב $L[X,Y]$, אזי $K(x,y)$ **מופרד לינארית** מ L מעל K. כלומר, בסיס של L $\{w_i \mid i \in I\}$ מעל K נשאר בסיס של $L(x,y)$ מעל $K(x,y)$. כל פולינום $g \in L[X,Y]$ נתן לרשם בצורה $g = \sum_{i \in I} g_i w_i$, באשר $g_i \in K[X,Y]$. אזי $g(x,y) = 0$, אם ורק אם $g_i(x,y) = 0$ לכל $i \in I$ ולכן, g הוא כפולה של f ב $L[X,Y]$. לכן, (x,y) הוא גם נְקֻדה יוצרת מעל L.

בפרט, אם $f(X,Y)$ אי פריק ב $\tilde{K}[X,Y]$ אומרים ש f **אי פריק לחלוטין**. לדגמה, הפולינום $Y^2 - X^3 - aX - b$ אי פריק לחלוטין.

נניח עתה ש $f(X,Y)$ הוא פולינום אי פריק ויהי $R = K[x,y]$ חוג הקואורדינטות של Γ מעל K. נתבונן

בנקֻדה $(a,b)\in\Gamma(K)$. הקבוצה $\mathfrak{p}=\{g(x,y)\in R\mid\ g(a,b)=0\}$ מוגדרת היטב ומהוה אידאל ראשוני של R. המקום של R ב $\mathfrak{p}$ הנו אפוא

$$K[x,y]_{(a,b)}=\Big\{\frac{g(x,y)}{h(x,y)}\mid\ g,h\in K[X,Y],\ h(a,b)\neq 0\Big\}$$

לפי, למה יב.א, זהו תחום נטר מקומי. נקרא לו **החוג המקומי של** Γ **ב** (a,b) **מעל** K ונסמנו ב $O_{\Gamma,(a,b)}$. האידאל המרבי שלו הנו

$$\Big\{\frac{g(x,y)}{h(x,y)}\mid\ g,h\in K[X,Y],\ g(a,b)=0,\ h(a,b)\neq 0\Big\}.$$

נאמר ש (a,b) היא **נקֻדה פשוטה** של Γ, אם $\frac{\partial f}{\partial a}\neq 0$ או $\frac{\partial f}{\partial b}\neq 0$. נסמן את אסף כל הנקֻדות הרציונליות־K והפשוטות של Γ ב $\Gamma_{\mathrm{simp}}(K)$.

למה יב.ד: *יהי Γ עקם מישורי מעל K ותהי (a,b) נקֻדה רציונלית־K פשוטה של Γ. אזי החוג המקומי של Γ ב (a,b) מעל K הנו חוג הערכה של שדה הפונקציות של Γ מעל K.*

הוכחה: תהי (x,y) נקֻדה יוצרת של Γ מעל K. נסמן $R=K[x,y]_{(a,b)}$, $F=\mathrm{Quot}(R)$ ויהי $\mathfrak{m}$ האידאל המרבי של R. נניח למשל ש $\frac{\partial f}{\partial a}\neq 0$. נוכיח ש $y-b$ יוצר את $\mathfrak{m}$. מלמה יב.ג ינבע ש R הנו חוג הערכה בדידה של F.

ואכן, יהי $g(x,y)\in\mathfrak{m}$. אזי $g(a,b)=0$ ולכן, אם נפתח את $g(X,Y)$ לטור טיילור מסביב לנקֻדה (a,b) ונציב $(X,Y)=(x,y)$, נקבל ש $g(x,y)$ הוא צרוף לינארי של $x-a$ ו $y-b$ עם מקדמים ב R. לכן, $\mathfrak{m}=R(x-a)+R(y-b)$.

את התהליך הזה נפעיל במיוחד לגבי f:

$$f(X,Y)=\frac{\partial f}{\partial b}(X-a)+\frac{\partial f}{\partial b}(Y-b)+\text{higher terms}$$

ו

$$0=f(x,y)=\frac{\partial f}{\partial a}(x-a)+\frac{\partial f}{\partial b}(y-b)+(x-a)u+(y-b)v$$

באשר $u,v\in\mathfrak{m}$. לכן,

$$0=\Big(\frac{\partial f}{\partial a}+u\Big)(x-a)+\Big(\frac{\partial f}{\partial b}+v\Big)(y-b).$$

הואיל ו $\frac{\partial f}{\partial a}\neq 0$ ו $u\in\mathfrak{m}$, המקדם של $x-a$ הפיך ב R. לכן, $x-a\in R(y-b)$. מכאן נובע ש $\mathfrak{m}=R(y-b)$, כפי שהבטחנו לעיל. ∎

כדי ללכת בכוון ההפוך נוכיח קודם כל שתי למות כלליות על הערכות:

למה יב.ה: *תהי $(L,w)/(K,v)$ הרחבה סופית של שדות מערכים. אם v טריביאלית (כלומר $v(a)=0$ לכל $a \in K$), אזי גם w טריביאלית.*

הוכחה: נתבונן באבר x של $L^\times$. נחליף את x ב x^{-1} במקרה הצרך כדי להניח ש $v(x) \geq 0$. אבר זה מקים משואה $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ עם מקדמים ב K כך ש $a_0 \neq 0$. נסמן את ההומומורפיזם הקנוני $O_w \to O_w/M_w$ בגג. אם נפעיל אותו על המשואה נקבל: $\bar{x}^n + \bar{a}_{n-1}\bar{x}^{n-1} + \cdots + \bar{a}_0 = 0$. הואיל ו $\bar{a}_0 \neq 0$, גם $\bar{x} \neq 0$. לכן $v(x) = 0$. ∎

למה יב.ו: *תהי w הערכה בדידה של שדה F ותהי v הערכה של F כך ש $O_v \subseteq O_w$. אזי $O_w = O_v$ ולכן v שקול ל w.*

הוכחה: נניח בשלילה שקיים $x \in O_v \smallsetminus O_w$. אזי $v(x) \geq 0$ ו $w(x) < 0$. מצד שני קים $y \in F$ כך ש $v(y) < 0$. נבחר n טבעי כך ש $w(x^{-n}y) \geq 0$. בפרט $x^{-n}y \in O_w \subseteq O_v$ ולכן $x^{-n}y \subseteq O_v$. מצד שני, $v(x^{-n}y) = -nv(x) + v(y) < 0$ ולכן $x^{-n}y \notin O_v$, סתירה. ∎

יב.ז הנקֻדה המתאימה להערכה. יהי Γ עקם אפיני מישורי אי פריק מעל K עם נקֻדה יוצרת (x,y) ועם שדה פונקציות רציונליות $F = K(x,y)$. תהי v הערכה של F/K כך ש $\bar{F}_v = K$. נניח ש $x, y \in O_v$. נסמן בגג את ההעתקה הקנונית $O_v \to O_v/M_v$. אזי $\bar{x} = a$ ו $\bar{y} = b$ הם אברים של K. מהתנאי $f(x,y) = 0$ נובע שגם $f(a,b) = 0$. במלים אחרות $(a,b) \in \Gamma(K)$.

החוג המקומי $K[x,y]_{(a,b)}$ מוכל בחוג ההערכה O_v. אם (a,b) נקֻדה פשוטה של $\Gamma(K)$ אזי, לפי למה יב.ד, $K[x,y]_{a,b}$ הוא חוג הערכה בדידה של F. מלמה יב.ה, נובע ש $K[x,y]_{(a,b)} = O_v$. יהי $\mathfrak{p}$ המחלק הראשוני של F/K הנקבע על ידי v. ההעתקה $\pi\colon \Gamma_{\mathrm{simp}}(K) \to \mathcal{P}_{F/K}$ המעתיקה את (a,b) ל $\mathfrak{p}$ היא אפוא חד חד ערכית. אם כל נקֻדה של $\Gamma(K)$ פשוטה על Γ, אזי $\mathrm{Im}(\pi)$ הנו אסף כל המחלקים הראשוניים $\mathfrak{p}$ של F/K ממעלה 1 כך ש $v_\mathfrak{p}(x), v_\mathfrak{p}(y) \geq 0$.

כדי להגיע גם למחלקים ראשוניים שאינם מקימים את התנאי האחרון, עלינו להחליף את Γ **בהשלמה הפרויקטיבית** שלו. ∎

יב.ח עקמים פרויקטיביים מישוריים. יהי $f(X,Y) = \sum_{i,j \leq d} a_{ij} X^i Y^j$ פולינום אי פריק ב $K[X,Y]$ ממעלה d. נסמן ב Γ את העקם האפיני ש $f(X,Y)$ מגדיר. נתאים ל f את הפולינום ההומוגני במשתנים X_0, X_1, X_2:

$$f^*(X_0, X_1, X_2) = \sum_{i+j \leq d} a_{ij} X_0^{d-i-j} X_1^i X_2^j$$

נסמן ב Γ^* את **העקם הפרויקטיבי המישורי** ש f^* מגדיר. גם הוא יהיה פנקטור המתאים לכל הרחבה L של K את תת הקבוצה הבאה של $\mathbb{P}^2(L)$:

$$\Gamma^*(L) = \{(a_0{:}a_1{:}a_2) \in \mathbb{P}^2(L) \mid f^*(a_0, a_1, a_2) = 0\}.$$

אם $f(X,Y)$ אי פריק מעל K גם $f^*(X_0,X_1,X_2)$ אי פריק מעל K. אם $(a,b) \in \Gamma(L)$, אזי $(1{:}a{:}b) \in \Gamma^*(L)$. להפך, אם $(a_0{:}a_1{:}a_2) \in \Gamma^*(L)$ ו $a_0 \neq 0$, אזי $f(a,b) = 0$, באשר $a = \frac{a_1}{a_0}$ ו $b = \frac{a_2}{a_0}$.
נְקֻדות $\Gamma(L)$ מתאימות אפוא באופן חד חד ערכי לנְקֻדות הסופיות של $\Gamma^*(L)$. בהתאמה זו עוברות נְקֻדות פשוטות לנְקֻדות פשוטות. ביתר דיוק מתקיים:

$$\frac{\partial f^*}{\partial X_1}(a_0{:}a_1{:}a_2) \neq 0 \quad \text{אם ורק אם} \quad \frac{\partial f}{\partial X}(a,b) \neq 0$$
$$\frac{\partial f^*}{\partial X_2}(a_0{:}a_1{:}a_2) \neq 0 \quad \text{אם ורק אם} \quad \frac{\partial f}{\partial Y}(a,b) \neq 0$$

באופן כללי מְכֻנה נְקֻדה $(a_0{:}a_1{:}a_2)$ של $\Gamma(L)$ **פשוטה** אם $\frac{\partial f^*}{\partial a_i} \neq 0$ עבור לפחות i אחד בין 0 לבין 2.

מלבד הנְקֻדות הסופיות יש ל $\Gamma^*(L)$ גם נְקֻדות אינסופיות, דהיינו כאלו שעבורן $a_0 = 0$. נְקֻדות אלו נמצאות על עקמים אפיניים מישוריים אחרים. ביתר דיוק, כל נְקֻדה $(a_0{:}a_1{:}a_2)$ של $\Gamma(L)$ שעבורה $a_1 \neq 0$ מתאימה באופן חד חד ערכי לנְקֻדה $\left(\frac{a_0}{a_1}, \frac{a_2}{a_1}\right)$ הנמצאת על העקם האפיני המישורי Γ_1 הנקבע על ידי המשואה $f^*(X_0,1,X_2) = 0$. הנְקֻדות שעבורן $a_2 \neq 0$ מתאימות באופן חד חד ערכי לנְקֻדות $\left(\frac{a_0}{a_2}, \frac{a_1}{a_2}\right)$ המונחות על העקם האפיני המישורי Γ_2 הנקבע על ידי המשואה $f^*(X_0,X_1,1) = 0$. לשם אחידות הכתיב נרשם גם Γ_0 במקום Γ. כמו במקרה $i = 0$, כן עבור $i = 1$ ועבור $i = 2$, נְקֻדות פשוטות מתאימות לנְקֻדות פשוטות. נעיר שגם x וגם y שונים מאפס, $\left(\frac{1}{x}, \frac{y}{x}\right)$ היא נְקֻדה יוצרת של Γ_1 ו $\left(\frac{1}{y}, \frac{x}{y}\right)$ היא נְקֻדה יוצרת של Γ_2. בפרט F הוא שדה הפונקציות גם של Γ_1 וגם של Γ_2. יתר על כן, אם למשל $a_0, a_1 \neq 0$, אזי החוג המקומי של Γ_0 ב $\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}\right)$ שוה לחוג המקומי של Γ_1 ב $\left(\frac{a_0}{a_1}, \frac{a_2}{a_1}\right)$. נוכל אפוא לזהות את $\Gamma_i(L)$ כתת קבוצה של $\Gamma^*(L)$ ולקבל ש

$$.\Gamma^*(L) = \Gamma_0(L) \cup \Gamma_1(L) \cup \Gamma_2(L)$$

העקם Γ^* יקרא **ההשלמה הפרויקטיבית** של Γ. אם כל נְקֻדות $\Gamma^*(\tilde{K})$ פשוטות נאמר ש Γ^* **חלק**. ∎

משפטון יב.ט: *יהי Γ עקם אפיני מישורי מעל שדה K. יהי F שדה הפונקציות של Γ מעל K ויהי Γ^* ההשלמה הפרויקטיבית של Γ. נניח שכל נְקֻדות $\Gamma^*(K)$ פשוטות. אזי קימת העתקה חד חד ערכית מ $\Gamma^*(K)$ על קבוצת המחלקים הראשוניים של F/K ממעלה 1. בהתאמה זו עוברת נְקֻדה $\mathbf{p}$ של $\Gamma^*(K)$ למחלק הראשוני המתאים לחוג המקומי של Γ^* ב $\mathbf{p}$.*

הוכחה: נוכיח קודם שלכל מחלק ראשוני $\mathfrak{p}$ של F/K בעל מעלה 1 מתאימה נְקֻדה על אחד מהעקמים Γ_i. ואכן, אם (x,y) הוא נְקֻדה יוצרת של Γ, נרשם $x_0 = 1$, $x_1 = x$ ו $x_2 = y$. יהי i בין 0 ל 2 כך ש $v_\mathfrak{p}(x_i)$ מזערי בין $v_\mathfrak{p}(x_0), v_\mathfrak{p}(x_1), v_\mathfrak{p}(x_2)$. אזי הזוג המתקבל מסלוק 1 מהשלישיה $\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \frac{x_2}{x_i}\right)$ הוא נְקֻדה יוצרת של Γ_i מעל K והקואורדינטות של נְקֻדה זו שיכות לחוג ההערכה של $v_\mathfrak{p}$. מ יב.ז נובע שנְקֻדה זו עוברת תחת ההערכה הקנונית של $O_\mathfrak{p}$ לנְקֻדה $\mathbf{p}$ של $\Gamma_i(K)$ וחוג ההערכה של Γ_i ב $\mathbf{p}$ שוה ל $O_\mathfrak{p}$.

עתה נראה שההעתקה חד חד ערכית. יהיו אפוא $\mathbf{p} = (a_0{:}a_1{:}a_2)$ ו $\mathbf{p}' = (a_0'{:}a_1'{:}a_2')$ נקֻדות של $\Gamma^*(K)$ המתאימות למחלק ראשוני משֻתף $\mathfrak{p}$ של F/K. אזי $O_{\Gamma^*,\mathbf{p}} = O_{\Gamma^*,\mathbf{p}'}$. נניח למשל ש $a_0 \neq 0$ ונסמן בגג את העתקת המנה של $O_{\Gamma^*,\mathbf{p}} \to K$. אזי $\overline{x_1/x_0} = \bar{x} = a_1/a_0$ ו $\overline{x_2/x_0} = \bar{y} = a_2/a_0$. לכן, $v_\mathfrak{p}(x_0) \leq v_\mathfrak{p}(x_1), v_\mathfrak{p}(x_2)$. אלו היה $a_0' = 0$ ולמשל $a_1' \neq 0$, היינו מקבלים באותו האפן ש $v_\mathfrak{p}(x_1) < v_\mathfrak{p}(x_0)$ת בסתירה לאי השויון האחרון. לכן $a_0' \neq 0$, $\overline{x_1/x_0} = a_1'/a_0'$ ו $\overline{x_1/x_0} = a_2'/a_0'$ כך ש $\mathbf{p} = \mathbf{p}'$. ∎

יג. חבורת המחלקים ממעלה 0 של שדות אלפטיים

יהי K שדה בַעל אפיון שונה מ 2 ומ 3. נתבונן בעקם אלפטי E הנתן על ידי משואה מהצורה

$$Y^2 = X^3 + AX + B$$

עם דיסקרימיננטה $\Delta = 4A^2 + 27B^3 \neq 0$. בסעיף ז עמדנו על כך שכל נקודות $E(K)$ פשוטות. עתה נראה כיצד מאפשר משפט רימן־רוך להפך את $E(K)$ לחבורה חלופית באפן שתתקים הדרישה (6) של סעיף ז.

נבחר נקודה יוצרת (x, y) ל E מעל K ויהי $F = K(x, y)$ שדה הפונקציות הרציונליות של F מעל K. ממשפטון יא.ב נובע שהגזע של F/K שוה ל 1.

יג.א התאמה בין נקודות רציונליות־K למחלקים ראשוניים ממעלה 1. נסמן ב $\mathcal{P}_1$ את אסף המחלקים הראשוניים של F/K ממעלה 1. משפט יב.ט נותן התאמה חד חד ערכית של $E(K)$ על $\mathcal{P}_1$. ביתר דיוק, לנקודה (a, b) סופית של $E(K)$ מתאים המחלק הראשוני $\mathfrak{p}$ המקים $O_\mathfrak{p} = K[x, y]_{(a,b)}$. את ההעתקה $(x, y) \mapsto (a, b)$ נתן להרחיב באפן יחיד להומומרפיזם $\varphi_\mathfrak{p}\colon O_\mathfrak{p} \to K$ שגרעינו הוא האידאל המרבי היחיד של $O_\mathfrak{p}$. נקודת האינסוף היחידה על $E(K)$ מסומנת ב ∞. המחלק הראשוני המתאים לנקודה זו מסומן ב $\mathfrak{o}$ והוא מקים

$$\mathrm{div}_\infty(x) = 2\mathfrak{o} \qquad \mathcal{L}(2\mathfrak{o}) = K + Kx \tag{1a}$$

$$\mathrm{div}_\infty(y) = 3\mathfrak{o} \qquad \mathcal{L}(3\mathfrak{o}) = K + Kx + Ky \tag{1b}$$

הקואורדינטות ההומוגניות של נקודת האינסוף הן $(0{:}0{:}1)$ והן מקימות את המשואה ההומגנית

$$.X_0X_2^2 = X_1^3 + AX_0^2X_1 + BX_0^3$$

אם נחלק משואה זו ב X_2^3 ונציב $U = \frac{X_0}{X_2}$, $V = \frac{X_1}{X_2}$ נקבל מרכיב אפיני של E העובר דרך נקודת האינסוף. המשואה האפינית המתאימה היא $U = V^3 + AU^2V + BU^3$ והקואורדינטות של נקודת האינסוף על מרכיב זה הן $(0, 0)$. ∎

יג.ב התאמה בין $\mathcal{P}_1$ לבין $\mathcal{D}_0$. נסמן עתה את חבורת מחלקות המחלקים של F/K ממעלה 0 ב $\mathcal{D}_0$. אם $\mathfrak{a}$ הוא מחלק של F/K ממעלה 0, נסמן ב $[\mathfrak{a}]$ את המחלקה שלו. ההעתקה $\mathfrak{p} \mapsto [\mathfrak{p} - \mathfrak{o}]$ מעתיקה את $\mathcal{P}_1$ לתוך $\mathcal{D}_0$. העתקה זו הנה חד חד ערכית. ואכן, אם $\mathfrak{p}, \mathfrak{p}' \in \mathcal{P}_1$, $\mathfrak{p} \neq \mathfrak{p}'$ ו $[\mathfrak{p}' - \mathfrak{o}] = [\mathfrak{p} - \mathfrak{o}]$ אזי קים $z \in F^\times$ כך ש $\mathfrak{p}' - \mathfrak{o} = \mathfrak{p} - \mathfrak{o} + \mathrm{div}(z)$. לכן, $\mathfrak{p}' = \mathfrak{p} + \mathrm{div}(z)$ ולכן, $\mathrm{div}_0(z) = \mathfrak{p}'$. מכאן נובע ש $\deg(\mathrm{div}_0(z)) = \deg(\mathfrak{p}') = 1$. לכן, לפי (2) של סעיף ט, $[F : K(z)] = 1$. במלים אחרות, $F = K(z)$, לכן, לפי משפטון י.א, שוה הגזע של F/K ל 0, בנגוד לנאמר לעיל.

להפך, יהי $\mathfrak{a}$ מחלק של F/K ממעלה 0. אזי, $\deg(\mathfrak{a}+\mathfrak{o}) = 1$ ולכן, לפי משפט רימן־רוך, $\dim(\mathfrak{a}+\mathfrak{o}) = 1$. קיים אפוא $z \in F^\times$ כך ש $\mathfrak{a} + \mathfrak{o} + \mathrm{div}(z) \geq 0$. הואיל והמעלה של אגף שמאל שוה ל 1 קיים $\mathfrak{p} \in \mathcal{P}_1$ כך ש $\mathfrak{p} = \mathfrak{a} + \mathfrak{o} + \mathrm{div}(z)$. בפרט, $[\mathfrak{a}] = [\mathfrak{p} - \mathfrak{o}]$. יחד עם הפסקה הקודמת נקבל שההעתקה $\mathcal{P}_1 \to \mathcal{D}_0$ חד חד ערכית ועל. ∎

יג.ג מתן מבנה של חבורה ל $E(K)$. נסכם את ההעתקות החד חד ערכיות שהגדרנו ב יג.א ו יג.ב בתרשים הבא:

$$\begin{array}{ccccc} E(K) & \longrightarrow & \mathcal{P}_1 & \longrightarrow & \mathcal{D}_0 \\ (a,b) & \mapsto & \mathfrak{p}_{(a,b)} & \mapsto & [\mathfrak{p}_{(a,b)} - \mathfrak{o}] \\ \infty & \mapsto & \mathfrak{o} & \mapsto & [\mathfrak{o}] \end{array}$$

הואיל ו $\mathcal{D}_0$ היא חבורה אבלית, משרות העתקות אלו מבנה של חבורה אבלית על $E(K)$ אשר נקודת האפס שלה היא נקודת האינסוף. ביתר פרוט, אם $\mathbf{p}_1, \ldots, \mathbf{p}_n$ הן נקודות של $E(K)$ ו $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ הם המחלקים הראשוניים המתאימים להם, אזי $\sum_{i=1}^n \mathbf{p}_i = 0$ אם ורק אם $\sum_{i=1}^n [\mathfrak{p}_i - \mathfrak{o}] = 0$, כלומר, קיים $z \in F^\times$ כך ש $\sum_{i=1}^n \mathfrak{p}_i - n\mathfrak{o} = \mathrm{div}(z)$. ∎

משפטון יג.ד:

(א) *שלש נקודות שונות* $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ *של* $E(K)$ *מונחות על ישר אחד אם ורק אם* $\mathbf{p}_1 + \mathbf{p}_2 + \mathbf{p}_3 = 0$

(ב) *יהי* $\mathbf{p} \in E(K)$ *ויהי* Λ *הישר המשיק ל* E *ב* $\mathbf{p}$. *תהי* $\mathbf{p}'$ *נקודת החתוך הנוספת של* Λ *עם* $E(K)$. *אזי* $2\mathbf{p} + \mathbf{p}' = 0$.

הוכחת א: יהי $\mathfrak{p}_i$ המחלק הראשוני המתאים ל $\mathbf{p}_i$, $i = 1,2,3$. נבדיל בין שני מקרים.

מקרה א.א: *הנקודות* $\mathbf{p}_i$ *סופיות.* בהנחה זו $\mathbf{p}_i = (a_i, b_i)$ ו $b_i^2 = a_i^3 + Aa_i + B$ עבור $i = 1,2,3$. אזי $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ שונים זה מזה.

נניח קודם שהנקודות נמצאות על ישר אחד, כלומר קיימים $\alpha, \beta, \gamma \in K$ שלא כלם אפס כך ש

$$\alpha a_i + \beta b_i + \gamma = 0 \qquad i = 1,2,3 \tag{2}$$

לכן, $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ הם אפסים של האבר $z = \alpha x + \beta y + \gamma$ של $F^\times$. מ (1) נובע ש $\mathrm{div}_\infty(z) = 3\mathfrak{o}$. לכן $\deg(\mathrm{div}_0(z)) = 3$ ולכן $\mathrm{div}_0(z) = \mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3$. מכאן נובע ש

$$\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{o} = \mathrm{div}_0(z) - \mathrm{div}_\infty(z) = \mathrm{div}(z) \tag{3}$$

ולכן, לפי הגדרת החבור ב יג.ג

$$\mathbf{p}_1 + \mathbf{p}_2 + \mathbf{p}_3 = 0. \tag{4}$$

להפך, נניח ש (4) מתקיים. אזי קיים $z \in F^\times$ כך ש (3) נכון. לכן $z \in \mathcal{L}(3\mathfrak{o})$. מ $(1a)$ נובע שקיימים $\alpha, \beta, \gamma \in K$ שלא כלם אפס כך ש $z = \alpha x + \beta y + \gamma$. מ (3) נובע ש $\alpha a_i + \beta b_i + \gamma = 0$ עבור $i = 1, 2, 3$. במלים אחרות $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ מונחות על הישר $\alpha X + \beta Y + \gamma = 0$.

מקרה א.ב: *אחת מהנקודות $\mathbf{p}_i$ היא נקודת האינסוף.* נניח למשל ש $\mathbf{p}_3 = \infty$. אזי לישר העובר דרך שלש הנקודות יש הצורה $X = a$. לכן קיים $b \in K$ כך ש $\mathbf{p}_1 = (a, b)$, $\mathbf{p}_2 = (a, -b)$ ו $b \neq 0$. נסמן $z = x - a$. אזי $\mathrm{div}_\infty(z) = \mathrm{div}_\infty(x) = 2\mathfrak{o}$ ו $\mathfrak{p}_1$ ו $\mathfrak{p}_2$ הם אפסים של z. לכן,

$$\mathrm{div}(z) = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{o}. \tag{6}$$

מחק החבור נובע ש $\mathbf{p}_1 + \mathbf{p}_2 = 0$, כמבוקש.

להפך, נניח ש $\mathbf{p}_1 + \mathbf{p}_2 = 0$. אזי קיָם $z \in \mathcal{L}(2\mathfrak{o})$ המקיֵם את (6). מ $(1a)$ נובע שקיימים $\alpha, \beta \in K$, $\alpha \neq 0$ כך ש $z = \alpha x + \beta$. לפי (6), $\alpha a_i + \beta = 0$ עבור $i = 1, 2$. לכן, שלש הנקֻדות $\mathbf{p}_1$, $\mathbf{p}_2$ ו ∞ מונחות על הישר $\alpha X + \beta = 0$.

הוכחת ב: יהיו $\mathfrak{p}$ ו $\mathfrak{p}'$ בהתאמה המחלקים הראשוניים המתאימים ל $\mathbf{p}$ ו $\mathbf{p}'$. נבדיל בין כמה מקרים.

מקרה ב.א: *הנקודה $\mathbf{p}$ סופית.* נסמן $\mathbf{p} = (a, b)$ ו $h(X, Y) = X^3 + AX + B - Y^2$. אזי Λ נתן על ידי המשואה

$$\frac{\partial h}{\partial a}(X - a) + \frac{\partial h}{\partial b}(Y - b) = 0.$$

נסמן $z = \frac{\partial h}{\partial a}(x - a) + \frac{\partial h}{\partial b}(y - b)$. אם נפתח את $h(X, Y)$ מסביב ל (a, b) נקבל

$$h(X, Y) = \frac{\partial h}{\partial a}(X - a) + \frac{\partial h}{\partial b}(Y - b) + c(X - a)^2 + d(Y - b)^2 + e(X - a)^3, \tag{7}$$

באשר $c, d, e \in K$. אם נציב $X = x$ ו $Y = y$, נקבל $0 = z + c(x - a)^2 + d(y - b)^2 + e(x - a)^3$. לכן, $v_\mathfrak{p}(z) \geq 2$.

נניח קודם ש $\frac{\partial h}{\partial b} \neq 0$. אזי, $\mathbf{p}'$ סופית (כי (0:1:0) היא נקֻדת האינסוף היחידה של E). לפי (1), $\mathrm{div}_\infty(z) = 3\mathfrak{o}$. בנוסף, $v_{\mathfrak{p}'}(z) \geq 1$. הואיל ו $\deg(\mathrm{div}_0(z)) = \deg(\mathrm{div}_\infty(z)) = 3$ מתקיֵם $\mathrm{div}_0(z) = 2\mathfrak{p} + \mathfrak{p}'$ ולכן $\mathrm{div}(z) = 2\mathfrak{p} + \mathfrak{p}' - 3\mathfrak{o}$. לכן, לפי חק החבור, $2\mathbf{p} + \mathbf{p}' = 0$, כפי שנטען.

עתה נניח ש $\frac{\partial h}{\partial b} = 0$. אזי, $\frac{\partial h}{\partial a} \neq 0$ ו $z = \frac{\partial h}{\partial a}$. לכן, לפי (1), $\mathrm{div}_\infty(z) = 2$ ומכאן $\mathrm{div}(z) = 2\mathfrak{p} - 2\mathfrak{o}$. לפי חֹק החבור, $2\mathbf{p} = 0$.

מקרה ב.ב: $\mathbf{p} = \infty$. כדי לחשב את משואת Λ נעבר לקואורדינטות הומוגניות:

$$h^*(X_0, X_1, X_2) = X_1^3 + AX_0^2 X_1 + BX_0^3 - X_0 X_2^2$$

המשואה של Λ תהיה

$$\frac{\partial h^*}{\partial X_0}(0,0,1)X_0 + \frac{\partial h^*}{\partial X_1}(0,0,1)X_1 + \frac{\partial h^*}{\partial X_2}(0,0,1)X_2 = 0.$$

חשוב מראה שמשואה זו אינה אלא $X_0 = 0$. כלומר, Δ הוא ישר האינסוף. ישר זה חותך את $E(K)$ רק בנקודת האינסוף שהיא אבר האפס של החבורה. סכום של שלש פעמים נקודה זו שוה כמובן לאפס. ∎

יד. הסגור השלם

יהי R תחום שלמות, L שדה המקיף את R ו x אבר של L. נאמר ש x **שלם** מעל R אם מתקים אחד משני התנאים הבאים:

$(1a)$ x הנו שרש של פולינום מתֻקן עם מקדמים ב R.

$(1b)$ קים מודול־R שונה מאפס V המוכל ב L והנוצר סופית מעל R כך ש $xV \subseteq V$.

טענה יד.א: *התנאים $(1a)$ ו $(1b)$ שקולים זה לזה.*

הוכחה: נניח קודם ש $(1a)$ נכון. כלומר, קימים $a_0, \ldots, a_{n-1} \in R$ כך ש $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. המודול $V = \sum_{i=0}^{n-1} Rx^i$ יקיֵם את התנאי $(1b)$.

להפך, נניח ש $V = \sum_{i=1}^{n} Rv_i$ הנו תת מודול־R של L השונה מאפס ושעבורו $xV \subseteq V$. קימים אפוא $a_{ij} \in R$ כך ש $xv_i = \sum_{j=1}^{n} a_{ij}v_j$. נסמן $A = (a_{ij})_{1 \le i,j \le n}$. לפי ההנחה לא כל ה v_i־ים שוים לאפס. לכן, x הנו ערך עצמי של המטריצה A. לכן, x הנו שרש של הפולינום האפיני $\det(xI - A)$ של A. זהו פולינום מתֻקן ממעלה n שמקדמיו הם פולינומים ב a_{ij} ולכן שיכים ל R. נובע אפוא ש x מקיֵם את התנאי $(1b)$. ∎

יהיו $S \subseteq R$ תחומי שלמות. נאמר ש S **שלם** מעל R אם כל אבר של S שלם מעל R. נאמר ש S **נוצר סופית כאלגברת־**R אם קימים $x_1, \ldots, x_n$ כך ש $S = R[x_1, \ldots, x_m]$.

למה יד.ב: *יהיו $S \subseteq R$ תחומי שלמות. אם S שלם מעל R ונוצר סופית כאלגברת־R, אזי S נוצר סופית כמודול־R.*

הוכחה: יהיו $x_1, \ldots, x_m$ אברים של S שעבורם $S = R[x_1, \ldots, x_m]$. כל x_i מקים משואה מתֻקנת ממעלה d_i עם מקדמים ב R. אסף המכפלות $x_1^{j_1}x_2^{j_2}\cdots x_m^{j_m}$ שבהם $0 \le j_i < d_i$, $i = 1, \ldots, m$, יוצר את S כמודול־R. ∎

למה יד.ג: *יהיו $R \subseteq S \subseteq T$ תחומי שלמות. נניח ש T שלם מעל S ו S שלם מעל R. אזי, T שלם מעל R.*

הוכחה: יהי $x \in T$. אזי x מקיֵם משואה $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ שבה $b_0, \ldots, b_{n-1} \in S$. לפי למה יד.ב החוג $S_1 = R[b_0, \ldots, b_{n-1}]$ נוצר סופית כמודול־R. כמו כן, $T_1 = S_1[x]$ נוצר סופית כמודול־S_1. לכן, $T_1 = R[b_0, \ldots, b_{n-1}, x]$ נוצר סופית כמודול־R. בנוסף, $xT_1 \subseteq T_1$. לכן, x שלם מעל R. ∎

למה יד.ד: *יהי R תחום שלמות, K שדה המנות של R ו x אבר אלגברי מעל K. אזי קים $a \in R$ כך ש $a \ne 0$ ו ax שלם מעל R.*

הוכחה: x מקיֵם משואה $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ שבה $a_0, \ldots, a_{n-1}, a_n \in R$ ו $a_n \ne 0$. נסמן $y = a_nx$. הוא מקיֵם $y^n + a_na_{n-1}y^{n-1} + \cdots + a_n^na_0 = 0$ ולכן הנו שלם מעל R. ∎

יהי R תחום שלמות עם שדה מנות K. נאמר ש R **סגור בשלמות** אם כל אבר של K השלם מעל R שיך ל R.

למה יד.ה: *יהי R תחום שלמות ו L שדה המקיף את R. נסמן ב S את אסף כל אברי L שהם שלמים מעל R. אזי S הנו תחום שלמות סגור בשלמות המקיף את R. הוא נקרא* **הסגור השלם** *של R ב L. אם L אלגברי מעל שדה המנות של R, אזי L הנו שדה המנות של S.*

הוכחה: אבר a של R הוא שרש של המשואה $X - a = 0$ ולכן שיך ל S.

יהיו $x, y \in S$. אזי קַיָּמים ב L מודולי־R שונים מאפס ונוצרים סופית U ו V שעבורם $xU \subseteq U$ ו $yV \subseteq V$. אסף כל הסכומים הסופיים $\sum u_i v_i$ מהוה מודול־R שונה מאפס ונוצר סופית המסֻמן ב UV. עבורו $xyUV \subseteq UV$ ו $(x+y)UV \subseteq UV$. לכן $xy, x+y \in S$. הוכחנו אפוא ש S חוג.

אם $z \in L$ שלם מעל S, אזי, לפי למה יד.ג, z שלם מעל R ולכן שיך ל S.

לבסוף, נסמן את שדה המנות של R ב K. נניח ש L אלגברי מעל K. לפי למה יד.ד כל אבר של L הנו מנה של אבר של S באבר של R. לכן, L הנו שדה המנות של S. ∎

משפטון יד.ו: *כל תחום שלמות בעל פריקות חד ערכית סגור בשלמות.*

הוכחה: יהי R תחום שלמות בעל פריקות חד ערכית ויהי K שדה המנות שלו. נתבונן באבר x של K המקים משואה מתֻקנת $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ עם מקדמים $a_i \in R$. נרשם $x = \frac{u}{v}$ עם $u, v \in R$ זרים זה לזה. אזי $u^n + a_{n-1}u^{n-1}v + \cdots + a_0 v^n = 0$. כל מחלק ראשוני p של v יחלק את u. לכן, v הפיך ו $x \in R$.

∎

משפטון יד.ז: *יהי R תחום שלמות סגור בשלמות, K שדה המנות של R, L הרחבה פרידה ממעלה n של K ו S הסגור השלם של R ב L. אזי*

(א) *S מוכל במודול־R חפשי מדרגה n.*

(ב) *אם R בעל פריקות חד ערכית (בפרט אם $R = \mathbb{Z}$), אזי S הנו מודול־R חפשי מדרגה n.*

הוכחת א: נבחר בסיס $w_1, \ldots, w_n$ ל L מעל K. נכפיל בסיס זה לפי הצרך באבר שונה מאפס של R כדי להניח ש $w_1, \ldots, w_n \in S$ (למה יד.ד). יהי עתה $x \in S$. עבורו קימים $a_1, \ldots, a_n \in K$ כך ש $x = \sum_{j=1}^n a_j w_j$. יהיו $\sigma_1, \ldots, \sigma_n$ שכוני־K השונים של L לתוך $\tilde{K}$. הם יקימו $\sigma_i x = \sum_{j=1}^n a_j \sigma_i w_j$. מתורת גלואה נובע ש $d = \det(\sigma_i w_j) \neq 0$. נסחת קרמר נותנת $b_j \in \mathbb{Z}[\sigma_i x, \sigma_i w_j]_{1 \leq i,j \leq n}$ כך ש $a_j = \frac{b_j}{d}$, $j = 1, \ldots, n$. לכן, $x = \sum_{j=1}^n b_j d \cdot \frac{w_j}{d^2}$. כל אחד מהאברים $\sigma_i x$ ו $\sigma_i w_j$ שלם מעל R. לכן, לפי למה יד.ה, b_j ו d שלמים מעל R. כמו כן, $b_j d = a_j d^2 \in K$. לכן $b_j d \in R$.

נראה ש $d^2 \in K$. לצרך זה נתבונן ב $\sigma \in \mathrm{Gal}(K)$. אזי $\sigma d = \det(\sigma\sigma_i w_j)$. הואיל ו $(\sigma\sigma_1, \ldots, \sigma\sigma_n)$ הנה תמורה של $(\sigma_1, \ldots, \sigma_n)$, נקבל ש $\sigma d = \pm d$. לכן, $\sigma(d^2) = d^2$. מכאן נובע ש $d^2 \in K$. (למעשה, d^2 הנו שלם מעל R. לכן $d^2 \in R$.)

מהפסקה הקודמת נובע ש $b_j d = a_j d^2 \in K$, $j = 1, \ldots, n$. לכן, S מוכל במודול־R החפשי $\sum_{j=1}^{n} R\frac{w_j}{d^2}$.

הוכחת ב: מהמשפט היסודי של מודולים חפשיים מעל תחומי שלמות בעלי פריקות חד ערכית ומ (א) נובע ש S הנו מודול־R חפשי נוצר סופית. בסיס־R של S יהיה גם בסיס־K של L. לכן מספר אבריו חיב להיות n. ∎

טו. הנורמה המֻחלטת של אידאל

יהי R חוג דדקינד עם שדה מנות K. נניח שלכל אידאל מרבי P של R שדה השאריות $\bar{K}_P$ סופי. (הנחה זו מתקימת במקרה ש K שדה גלובלי.) נגדיר את הנורמה המֻחלטת של אידאל A של R בעזרת הנֻסחה

$$NA = (R : A)$$

מטרתנו בסעיף זה תהיה להוכיח ש NA הנו מספר טבעי ושהנורמה כפלית: $N(AB) = NA \cdot NB$.

למה טו.א: *יהיו A ו B אידאלים של R. אזי $B|A$ אם ורק אם $A \subseteq B$.*

הוכחה: נניח קודם ש $B|A$. אזי קים אידאל C כך ש $A = BC \subseteq B$.

להפך, נניח ש $A \subseteq B$. אזי $C = AB^{-1} \subseteq R$ לכן, C הנו אידאל של R המקים $A = BC$. במלים אחרות, $B|A$. ∎

למה טו.ב: $N(P^n) = (NP)^n$ *לכל אידאל מרבי P של R ולכל מספר טבעי n.*

הוכחה: לכל i טבעי חבורת המנה P^{i-1}/P^i מהוה מרחב וקטורי מעל השדה $\bar{K}_P = R/P$. הכפל של אבר $a+P$ של R/P באבר $b+P^i$ של P^{i-1}/P^i נתן על ידי $(a+P)(b+P^i) = ab+P^i$.

נוכיח ש $\dim(P^{i-1}/P^i) = 1$. ואכן, מיחידות הפרוק של האידאלים ב R נובע ש $P^i \subset P^{i-1}$. נבחר $b \in P^{i-1} \smallsetminus P^i$. אזי, $P^i \subset Rb + P^i \subseteq P^{i+1}$. מלמה טו.א נובע ש $P^i|Rb+P^i|P^{i-1}$. לכן, $Rb+P^i = P^{i-1}$. במלים אחרות, $b+P^i$ יוצר את המרחב P^{i-1}/P^i.

מהטענה נובע ש $R/P \cong P^{i-1}/P^i$. לכן, $(P^{i-1} : P^i) = NP$. מכאן,

$$NP^n = (R : P^n) = \prod_{i=1}^{n}(P^{i-1} : P^i) = (NP)^n. \quad ∎$$

משפטון טו.ג (משפט השאריות הסיני): *יהי O חוג חלופי ו $A_1, \ldots, A_n$ אידאלים המקימים $A_i + A_j = O$ עבור $i \neq j$.*

(א) *לכל $b_1, \ldots, b_n \in O$ קים $x \in O$ כך ש $x \equiv b_i \mod A_i$, עבור $i = 1, \ldots, n$.*

(ב) $O/\bigcap_{i=1}^n A_i \cong \prod_{i=1}^n O/A_i$.

הוכחת א: נניח תחִלה ש $n = 2$. לפי ההנחה קימים $a_1 \in A_1$ ו $a_2 \in A_2$ כך ש $a_1 + a_2 = 1$. לכן $b_1 - b_2 = a_1(b_1-b_2) + a_2(b_1-b_2)$ ולכן $b_1 - a_1(b_1-b_2) = b_2 + a_2(b_1-b_2)$. נסמן את הערך המשֻתף של שני האגפים ב x. הוא יקַים $x \equiv b_i \mod A_i$ עבור $i = 1, 2$.

נניח עתה ש $n \geq 3$ ושהמשפטון נכון עבור $n-1$. אזי קים $b \in O$ כך ש $b \equiv b_i \mod A_i$ עבור $i = 1, \ldots, n-1$. לכל i בין 1 ל $n-1$ קימים $a_i \in A_i$ ו $a_{n,i} \in A_n$ כך ש $a_i + a_{n,i} = 1$ ולכן $a_i = 1 - a_{i,n}$. לכן, $a_1 \cdots a_{n-1} = 1 - a_n$ עבור $a_n \in A_n$ ו $a_1 \cdots a_{n-1} \in A_1 \cdots A_{n-1}$.

המקרה $n=2$ נותן $x \in O$ כך ש $x \equiv b \mod A_1 \cdots A_{n-1}$ ו $x \equiv b_n \mod A_n$. הואיל ו $A_i \supseteq A_1 \cdots A_{n-1}$ עבור $i = 1, \ldots, i-1$ מקיֵם x את תנאי המשפטון.

הוכחת ב: ההעתקה $\alpha\colon O/\bigcap_{i=1}^n A_i \to \prod_{i=1}^n O/A_i$ המֻגדרת על ידי

$$\alpha(x + \bigcap_{i=1}^n A_i) = (x + A_1, \ldots, x + A_n)$$

מֻגדרת היטב ומהוה הומומורפיזם חד חד ערכי של חוגים. מ (א) נובע שהיא על. לכן, α הנו איזומורפיזם. ∎

משפטון טו.ד: *יהי R חוג דדקינד שבו R/P סופי לכל אידאל מרבי P. אזי NA הוא מספר טבעי ו $N(AB) = NA{\cdot}NB$ עבור כל שני אידאלים A ו B.*

הוכחה: יהיו $A_1, \ldots, A_n$ אידאלים של R זרים זה לזה. כלומר, עבור $i \neq j$ אין ל A_i ול A_j שום גורם ראשוני משֻתף. אלו היה $A_i + A_j \neq R$ היה קים אידאל מרבי P של R המקיף את $A_i + A_j$. מלמה טו.א היה נובע ש $P|A_i$ ו $P|A_j$ בסתירה להנחה. לכן, $A_i + A_j = R$.

בנוסף על זה $A_j \supseteq \bigcap_{i=1}^n A_i \supseteq \prod_{i=1}^n A_i$ לכל j. לכן, $A_j | \prod_{i=1}^n A_i$ לכל j. מהזרות של ה A_i־ים נובע ש $\bigcap_{i=1}^n A_i | \prod_{i=1}^n A_i$. לכן, $\bigcap_{i=1}^n A_i = \prod_{i=1}^n A_i$.

נפרק עתה את האידאל A למכפלה של חזקות של אידלים מרביים שונים זה מזה, $A = \prod_{i=1}^n P_i^{k_i}$. מתחִלת ההוכחה וממשפט השאריות הסיני נובע ש $R/A \cong \prod_{i=1}^n R/P_i^{k_i}$. לכן, לפי למה טו.ב,

$$NA = (R : A) = \prod_{i=1}^n (R : P_i^{k_i}) = \prod_{i=1}^n (NP_i)^{k_i}.$$

מכאן נובע גם ש $N(AB) = NA \cdot NB$. ∎

טז. הנורמה היחסית של אידאל

יהי R חוג דדקינד עם שדה מנות K. יהי L הרחבה פרידה סופית של K. נסמן ב S את הסגור השלם של R ב L. גם S הנו חוג דדקינד. נתבונן עתה באידאל ראשוני Q של S ויהי $P = Q \cap R$. נגדיר $\mathrm{Norm}_{L/K}Q = P^{f(Q/P)}$, באשר $f(Q/P) = [\bar{L}_Q : \bar{K}_P]$ הנו מעלת שדות השאריות המתאימים. נרחיב את $\mathrm{Norm}_{L/K}$ להומומורפיזם של $\mathcal{J}_L$ לתוך $\mathcal{J}_K$. במלים אחרות, יהי $B = \prod_{i=1}^r Q_i^{k_i}$ פרוק של אידאל שבור של L למכפלה של חזקות של אידאלים ראשוניים שונים. נגדיר $\mathrm{Norm}_{L/K}(B) = \prod_{i=1}^r \mathrm{Norm}_{L/K}(Q_i)^{k_i}$. בפרט הנורמה היחסית של אידאל של S תהיה אידאל של R. מטרת הסעיף הזה הִנָה להשוות את הנורמה היחסית של אידאלים לנורמה המֻחלטת שלהם במקרה ש $K = \mathbb{Q}$ ולנורמה היחסית של אברים.

למה טז.א: *יהי K שדה מספרים ו A אידאל של O_K. אזי* $\mathrm{Norm}_{K/\mathbb{Q}}A = NA \cdot \mathbb{Z}$.

הוכחה: שני האגפים של השויון כפליים ב A (משפטון טו.ד). לכן מספיק להוכיח את השויון במקרה ש A הנו אידאל ראשוני P. יהי p המספר הראשוני המונח מתחת ל P ויהי f מעלת שדה השאריות. אזי $\mathrm{Norm}_{K/\mathbb{Q}}P = p^f\mathbb{Z} = |\bar{K}_P| \cdot \mathbb{Z} = NP \cdot \mathbb{Z}$. ∎

למה טז.ב: *בסימונים דלעיל, יהיו L' הרחבה פרידה סופית של L ו S' הסגור השלם של S ב L'. אזי, לכל אידאל שבור B' של L' מתקים* $\mathrm{Norm}_{L'/K}B' = \mathrm{Norm}_{L/K}(\mathrm{Norm}_{L'/L}B')$.

הוכחה: שוב, שני אֲגפי השויון כפליים ב B'. לכן מספיק להוכיח אותו במקרה ש B' הנו אידאל ראשוני Q' של S'. לצרך זה נסמן $Q = Q' \cap S$ ו $P = Q \cap R$. אזי $f(Q'/P) = f(Q'/Q)f(Q/P)$. לכן

$$\begin{aligned}\mathrm{Norm}_{L'/K}Q' = P^{f(Q'/P)} &= P^{f(Q/P)f(Q'/Q)} = (\mathrm{Norm}_{L/K}Q)^{f(Q'/Q)} \\ &= \mathrm{Norm}_{L/K}(Q^{f(Q'/Q)}) = \mathrm{Norm}_{L/K}(\mathrm{Norm}_{L'/L}Q')\end{aligned}$$

כנדרש. ∎

למה טז.ג: *לכל אידאל שבור A של R מתקים* $\mathrm{Norm}_{L/K}(AS) = A^{[L:K]}$.

הוכחה: מספיק להוכיח את הלמה במקרה ש A הנו אידאל ראשוני P של R. יהיו $Q_1, \ldots, Q_r$ האידאלים הראשוניים של S המחלקים את P. יהיו $e_1, \ldots, e_r$ ציוני ההסתעפות ו $f_1, \ldots, f_r$ מעלות הרחבות שדות השאריות המתאימים. אזי $PS = \prod_{i=1}^r Q_i^{e_i}$ ו $\sum_{i=1}^r e_i f_i = [L : K]$. לכן,

$$\mathrm{Norm}_{L/K}(PS) = \prod_{i=1}^r (\mathrm{Norm}_{L/K}Q_i)^{e_i} = \prod_{i=1}^r P^{e_i f_i} = P^{\sum_{i=1}^r e_i f_i} = P^{[L:K]}$$

כמבֻקש. ∎

למה טז.ד: *נניח ש L/K הנה הרחבת גלואה. אזי σB $(\mathrm{Norm}_{L/K}B)S=\prod_{\sigma\in\mathrm{Gal}(L/K)}\sigma B$ לכל אידאל שבור B של L.*

הוכחה: נסמן $G=\mathrm{Gal}(L/K)$. מספיק להוכיח שכל אידאל ראשוני Q מקַיֵם $(\mathrm{Norm}_{L/K}Q)S=\prod_{\sigma\in G}\sigma Q$.

ואכן, יהי $P=Q\cap R$, $e=e(Q/P)$ ו $f=f(Q/P)$. אזי $e=e(\sigma Q/P)$ ו $f=f(\sigma Q/P)$ לכל $\sigma\in G$. יתר על כן, כל אידאל ראשוני של S המונח מעל P צמוד ל Q מעל K.

תהי $G_0=\{\tau\in G \mid \tau Q=Q\}$ חבורת הפרוק של Q. יהי $G=\bigcup_{i=1}^r\sigma_iG_0$. אזי $|G_0|=ef$ ו $\sigma_1Q,\dots,\sigma_rQ$ הם האידאלים הראשוניים השונים של S המחלקים את P. לכן, $PS=\prod_{i=1}^r\sigma_iQ^e$. מכאן נובע

$$(\mathrm{Norm}_{L/K}Q)S=(PS)^f=\prod_{i=1}^r\sigma_i(Q^{ef})=\prod_{i=1}^r\sigma_i\prod_{\tau\in G_0}\tau Q=\prod_{\sigma\in G}\sigma Q,$$

כמבֻקש. ∎

תוצאה טז.ה: *יהי K שדה מספרים ו $x\in K^\times$. אזי*

(א) $\mathrm{Norm}_{K/\mathbb{Q}}(xO_K)=(\mathrm{Norm}_{K/\mathbb{Q}}x)O_K$ ו

(ב) $N(xO_K)=|\mathrm{Norm}_{K/\mathbb{Q}}x|$.

הוכחה (א): נבחר הרחבת גלואה סופית L של $\mathbb{Q}$ המקיפה את K. ההעתקה $I\mapsto IO_L$ של $\mathcal{J}_Q$ (ושל $\mathcal{J}_K$) לתוך $\mathcal{J}_L$ הנה חד חד ערכית. לכן, מספיק להוכיח ש $\mathrm{Norm}_{K/\mathbb{Q}}(xO_K)O_L=\mathrm{Norm}_{K/\mathbb{Q}(x)}O_L$. הואיל והוצאת שרש ב $\mathcal{J}_L$ הנה חד ערכית, מספיק להוכיח ש

$$\mathrm{Norm}_{K/\mathbb{Q}}(xO_K)^{[L:K]}O_L=\mathrm{Norm}_{K/\mathbb{Q}}(x)^{[L:K]}O_L.$$

לפי למה טז.ג מספיק להוכיח

$$\mathrm{Norm}_{L/\mathbb{Q}}(xO_L)O_L=\mathrm{Norm}_{L/\mathbb{Q}}(x)O_L.$$

ואכן, לפי למה טז.ד

$$\begin{aligned}\mathrm{Norm}_{L/\mathbb{Q}}(xO_L)O_L&=\prod_{\sigma\in\mathrm{Gal}(L/\mathbb{Q})}\sigma(xO_L)\\&=\Big(\prod_{\sigma\in\mathrm{Gal}(L/\mathbb{Q})}\sigma x\Big)O_L=(\mathrm{Norm}_{L/\mathbb{Q}}x)O_L\end{aligned}$$

הוכחת (ב): לפי למה טז.א ו (א)

$$N(xO_K)\mathbb{Z}=\mathrm{Norm}_{K/\mathbb{Q}}(xO_K)=\mathrm{Norm}_{K/\mathbb{Q}}(x)\mathbb{Z}.$$

לכן $N(xO_K)=|\mathrm{Norm}_{K/\mathbb{Q}}(x)|$, כנדרש. ∎

∎

יז. מספר מחלקות האידאלים של שדה מספרים

יהי K שדה מספרים ו O חוג השלמים שלו. זהו חוג דדקינד. בפרט, אסף האידאלים השבורים $\mathcal{I}$ של K ביחס ל O מהוה חבורה תחת הכפל. המנה של חבורה $\mathcal{I}$ מודולו חבורת האידאלים השבורים הראשיים נקראת **חבורת מחלקות האידאלים של** K. מספר אבריה מסֻמן ב h ונקרא **מספר המחלקות** של K. מטרת הסעיף הנה להוכיח ש h הנו מספר טבעי.

אומרים שאידאלים שבורים A ו B **שקולים לינארית** אם קים $x \in K^\times$ כך ש $B = xA$. בהנתן אידאל שבור A של O קים, לפי ההגדרה, אבר $x \in O$, $x \neq 0$, כך ש $B = xA \subseteq O$. בפרט, B הנו אידאל שלם של O השקול לינארית ל A. לכן מספיק להוכיח שיש רק מספר סופי של מחלקות שקילות לינארית של אידאלים שלמים.

למה יז.א: *לכל $c > 0$ יש ב O רק מספר סופי של אידאלים A המקימים $NA \leq c$.*

הוכחה: יהי $A = P_1P_2\cdots P_r$ פרוק של A למכפלה של אידאלים מרביים (לאו דוקא שונים זה מזה). יהי p_i המספר הראשוני המונח מתחת ל P_i ו $f_i = [\bar{K}_{P_i} : \mathbb{F}_{p^i}]$. אזי $NP_i = |\bar{K}_{P_i}| = p_i^{f_i}$. לפי משפטון טו.ד, $c \geq NA = NP_1 \cdot NP_2 \cdots NP_r = p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r} \geq p_i$ לכן יש רק מספר סופי של אפשרויות ל p_i. מספר האידאלים המרביים של O המונחים מעל p_i סופי. לכן, יש רק מספר סופי של אפשרויות ל P_i. כמו כן, $p_i \geq 2$ ו $f_i \geq 1$. לכן, $2^r \leq c$ ולכן, $r \leq \frac{\log c}{\log 2}$ ו $f_i \leq \frac{log r}{\log 2}$. מכל זה עולה שיש ל O רק מספר סופי של אידאלים A עם $NA \leq c$. ∎

למה יז.ב: *קים $c > 0$ כך שכל אידאל A של O שקול לאידאל B המקים $NB \leq c$.*

הוכחה: נבחר בסיס $w_1, \ldots, w_n$ של O מעל $\mathbb{Z}$ (משפטון יד.ו). יהיו $\sigma_1, \ldots, \sigma_n$ שכוני־$\mathbb{Q}$ של K לתוך $\mathbb{C}$. נסמן $c_1 = \max_{1\leq i,j\leq n}|\sigma_i w_j|$ ו $c = (nc_1)^n$. נבחר עתה אידאל C של O השקול לינארית ל A^{-1}. נסמן

$$S = \Big\{ \sum_{j=1}^n a_j w_j \mid a_j \in \mathbb{Z},\ 0 \leq a_j \leq (NC)^{1/n} \Big\}.$$

אזי

$$|S| = \big([(NC)^{1/n}] + 1\big)^n > NC \tag{1}$$

לפי משפטון טו.ד, $NC = (O : C) < \infty$. לכן, לפי (1), קימים x, y שונים זה מזה ב S כך ש $x \equiv y \mod C$. יהי $z = x - y$. אזי, $z \neq 0$, $z \in C$ ו $z = \sum_{j=1}^n b_j w_j$ באשר $|b_j| \leq (NC)^{1/n}$. לכן,

$$|\mathrm{Norm}_{K/\mathbb{Q}} z| = \prod_{i=1}^n |\sum_{j=1}^n b_j\sigma_i w_j| \leq \prod_{i=n}^n \sum_{j=1}^n |b_j|\cdot|\sigma_i w_j| \leq \prod_{i=1}^n \Big((NC)^{1/n}\cdot nc_1\Big) = c\cdot NC \tag{2}$$

בנוסף לזה קים אידאל B של O כך ש $BC = zO$. בפרט $A \sim B = zC^{-1}$. מתוצאה טז.ה, ומשפטון טו.ד ומ (2) נקבל $NB \cdot NC = N(zO) = |\mathrm{Norm}_{K/\mathbb{Q}} z| \leq c \cdot NC$. לכן, $NB \leq c$. האידאל B מקים את דרישות הלמה. $\blacksquare$

הצרוף של למה יז.א ולמה יז.ב נותן:

משפט יז.ג: *חבורת מחלקות האידאלים של שדה מספרים הנה סופית.*

יח. ערכים מֻחלטים

ערך מֻחלט על שדה K הנו פונקציה $| \; | : K \to \mathbb{R}$ המקימת את הַתנאים הבאים.

(1a) $|x| \geq 0$ ו $|x| = 0$ אם ורק אם $x = 0$.

(1b) $|xy| = |x||y|$.

(1c) $|x + y| \leq |x| + |y|$.

אם מַחליפים את תנאי $(1c)$ בדרישה החזקה יותר,

(1c′) $|x + y| \leq \max(|x|, |y|)$,

אומרים שהערך המחלט הנו **אולטרה־מטרי** (או **לא ארכמדי**). אם תנאי $(1c')$ אינו מתקיֵם אומרים שהערך המחלט הנו **מטרי** (או **ארכמדי**).

אם $|x| = 1$ לכל $x \neq 0$ אומרים ש $| \; |$ **טריביאלי**. אם לא נאמר אחרת, נניח ש $| \; |$ אינו טריביאלי.

ערך מחלט $| \; |$ מַגדיר טופולוגיה על K. בסיס לסביבות a בטופולוגיה זו מהוה אסף הקבוצות $\{x \in K \mid |x - a| < \varepsilon\}$, באשר ε עובר על כל המספרים הממשיים החיוביים. כמו מעל שדה המספרים הממשיים גם ב K רציפות פעֻלות החבור, הכפל, והחלוק תחת טופולוגיה זו.

שני ערכים מֻחלטים, $| \; |$ ו $| \; |'$ **שקולים זה לזה** אם קים $\lambda > 0$ כך ש $|x|' = |x|^\lambda$ לכל $x \in K$. לחִלופין, $|x| < 1$ שקול ל $|x|' < 1$. לחלופי חלופין, $| \; |$ ו $| \; |'$ מגדירים אותה הטופולוגיה על K.

כמו הערכות לא שקולות מקַימים ערכים מחלטים לא שקולים את משפט הקרוב החלש:

משפטון יח.א (Artin-Whaples): *יהיו $| \; |_1, \ldots, | \; |_n$ ערכים מחלטים של שדה K ששום שנים מהם אינם שקולים זה לזה. יהיו $a_1, \ldots, a_n$ אברים של K ו $\varepsilon > 0$ מספר ממשי. אזי קים $x \in K$ כך ש $|x - a_i|_i < \varepsilon$ עבור $i = 1, \ldots, n$.*

אפשר להראות שתנאי הכרחי ומספיק לכך שערך מחלט $| \; |$ הנו אולטרה־מטרי הוא ש $|n| \leq 1$ לכל n טבעי.

נניח אפוא $| \; |$ אולטרה־מטרי ו $|x| < |y|$, אזי $|x + y| = |y|$. באפן כללי יותר, אם $|x_1|, \ldots, |x_n|$ שונים זה מזה, אזי $|x_1 + \cdots + x_n| = \max(|x_1|, \ldots, |x_n|)$.

הערך המחלט האולטרה מטרי $| \; |$ מגדיר הערכה $v\colon K \to \mathbb{R} \cup \{\infty\}$ על K. היא נתנת על ידי הנסחה $v(x) = -\log|x|$. להפך, בהנתן v כנ"ל, $|x| = c^{-v(x)}$ הנו ערך מחלט עבור כל קבוע $c > 1$. הערך המחלט $| \; |$ וההערכה v מגדירים אותה הטופולוגיה על K.

בפרט, להערכה בדידה v של K אשר שדה השאריות שלה בעל q אברים נתאים את הערך המחלט **המתֻקן** $\|x\|_v = q^{-v(x)}$. בפרט, **הערך המחלט ה p־אדי המתקן** של $\mathbb{Q}$ נתן על ידי הנֻסחה $\|x\|_p = p^{-v_p(x)}$, באשר v_p הנו ההערכה ה p־אדית. לדגמה, $\|p\|_p = p^{-1}$.

הערך המחלט המטרי היחיד של $\mathbb{Q}$ מֻשרה על ידי הערך המחלט הרגיל של $\mathbb{R}$. במלים אחרות, $\|x\|_\infty = \max(x, -x)$.

אסף הערכים המחלטים המְתֻקנים של $\mathbb{Q}$ מקים את **נסחת המכפלה:**

$$\prod_{v\in V(\mathbb{Q})} \|x\|_v = 1 \quad \text{לכל } x \neq 0 \tag{2}$$

באשר $V(\mathbb{Q})$ הנו קבוצת המספרים הראשוניים והסמל ∞.

ואכן, המשפט היסודי של תורת המספרים נותן את ההצגה $x = \prod_p p^{v_p(x)}$ עבור $x > 0$. לכן, $\prod_v \|x\|_v = \prod_p p^{-v_p(x)} \cdot x = 1$. את המקרה $x < 0$ מעמידים על המקרה $x > 0$ בעזרת הנסחה $\|x\|_v = \|-x\|_v$.

מטרת שארית הסעיף הנה לתקן את הערכים המחלטים של כל שדה מספרים כך שתתקים נסחת המכפלה.

לצרך זה נצא מערך מחלט כלשהוא $|\ |$ של שדה K. נסמן ב $\hat{K}$ את ההשלמה של K תחת $|\ |$. כמו במקרה של הערכות בדידות יֻגדר $\hat{K}$ כחוג סדרות קושי מודולו האידאל של הסדרות המתכנסות ל 0. גם כאן מֻרחב $|\ |$ באפן יחיד לערך מחלט של $\hat{K}$ באפן ש K צפוף ב $\hat{K}$. השדה $\hat{K}$ **מֻשלם** ביחס ל $|\ |$. כלומר, כל סדרת קושי ב $\hat{K}$ מתכנסת. הוא נקבע באפן יחיד עד כדי איזומורפיזם־K. אם $|x| = c^{-v(x)}$ עבור הערכה בדידה v ועבור כל $x \in K$ ו (K', v) הנו השלמה נוספת של (K, v), אזי קים איזומורפיזם־K $\sigma\colon K' \to \hat{K}$ כך ש $|\sigma x| = c^{-v(x)}$ לכל $x \in K'$.

בהנתן הרחבה סופית E של $\hat{K}$ נתן להרחיב את $|\ |$ לערך מחלט של E באפן יחיד. גם E יהיה מֻשלם תחת ההרחבה.

נתבונן עתה בהרחבה פרידה סופית L של K. מהנאמר בפסקה הקודמת נובע שכל שכון־K σ של L לתוך הסגור האלגברי של $\hat{K}$ מגדיר ערך מחלט $|\ |_\sigma$ על L המרחיב את $|\ |$:

$$|x|_\sigma = |\sigma x| \tag{3}$$

יתר על כן, σL צפוף־$|\ |$ ב $\hat{K} \cdot \sigma L$. לכן, $\hat{K} \cdot \sigma L$ הנו ההשלמה של L תחת $|\ |_\sigma$.

למה יח.ב: *יהי $|\ |$ ערך מחלט של שדה K. יהי L הרחבה פרידה סופית של K.*

(א) *יהיו σ ו τ שכוני־K של L לתוך הסגור האלגברי של $\hat{K}$. אזי $|\ |_\tau = |\ |_\sigma$ אם ורק אם קים איזומורפיזם־$\hat{K}$ $\lambda\colon \hat{K} \cdot \sigma L \to \hat{K} \cdot \tau L$ כך ש $\lambda \circ \sigma = \tau$.*

(ב) *כל הרחבה של $|\ |$ ל L מתקבלת לפי הנסחה (3) עבור איזה שהוא איזומורפיזם σ של L לתוך הסגור האלגברי של $\hat{K}$.*

(ג) *יהיו $|\ |_1, \ldots, |\ |_g$ ההרחבות של $|\ |$ לַעֲרכים מֻחלטים של L. לכל i יהי $\hat{L}_i$ ההשלמה של L תחת $|\ |_i$. אזי, $[L : K] = \sum_{i=1}^g [\hat{L}_i : \hat{K}]$. בפרט, מספר ההרחבות של $|\ |$ לערכים מֻחלטים של L אינו עולה על $[L : K]$.*

הוכחת א: נניח קודם שקים λ כנאמר בלמה. אזי $|y|' = |\lambda y|$ מגדיר ערך מחלט על $\hat{K} \cdot \sigma L$ המתלכד עם $|\ |$ על $\hat{K}$. מיחידות ההרחבה של $|\ |$ נובע ש $|y'| = |y|$ לכל $y \in \hat{K} \cdot \sigma L$. בפרט עבור $x \in L$ נקבל $|x|_\tau = |\tau x| = |\lambda \sigma x| = |\sigma x| = |x|_\sigma$.

להפך, נניח ש $|\tau x| = |\sigma x|$ לכל $x \in L$. לכל $y \in \hat{K} \cdot \sigma L$ קיימים $y_n \in L$ כך ש $y = \lim_{\to} \sigma y_n$ (הגבול נלקח ביחס להרחבה היחידה של $|\ |$ לסגור האלגברי של $\hat{K}$). בפרט $\{\sigma y_n\}_{n=1,2,3,\dots}$ סדרת קושי. מההנחה נובע שגם $\{\tau y_n\}_{n=1,2,3,\dots}$ מהוה סדרת קושי. הואיל ו $\hat{K} \cdot \tau L$ מֻשלם, מתכנסים τy_n לאבר y' של $\hat{K} \cdot \tau L$. אבר זה תלוי רק ב y. נגדיר אפוא $\lambda(y) = y'$ ונמצא ש $\lambda\colon \hat{K}\sigma L \to \hat{K}\tau L$ הנו איזומורפיזם־$\hat{K}$ המקים $\lambda \circ \sigma = \tau$, כמבֻקש.

הוכחת ב: תהי $|\ |'$ הרחבה של $|\ |$ לערך מחלט של L. תהי $(L', |\ |')$ השלמה של $(L, |\ |')$. נסמן ב K' את הסגור של K ב L'. אזי $(K', |\ |')$ הנו השלמה של $(K, |\ |)$. לכן, קים איזומורפיזם־K $\sigma\colon K' \to \hat{K}$ כך ש $|\sigma x'| = |x'|'$ לכל $x' \in K'$. נרחיב את σ לאיזומורפיזם $\sigma\colon L' \to \hat{L}$ עבור הרחבה סופית $\hat{L}$ של $\hat{K}$. מיחידות ההרחבה של הערך המחלט נובע ש $|\sigma x'| = |x'|'$ לכל $x' \in L'$. בפרט $|x|_\sigma = |\sigma x| = |x|'$ לכל $x \in L$, כנדרש.

הוכחת ג: נסמן ב $\mathrm{Embd}_K(L, \tilde{K})$ את קבוצת שכוני־K של L לתוך $\tilde{K}$. מספר אברי $\mathrm{Embd}_K(L, \tilde{K})$ שוה ל $[L : K]$. לפי (ב), הַהַעְתקה $\sigma \mapsto |\ |_\sigma$ מעתיקה את $\mathrm{Embd}_K(L, \tilde{K})$ על אסף ההרחבות של $|\ |$ לַעֲרכים מֻחלטים של L. נגדיר יחס שקילות על $\mathrm{Embd}_K(L, \tilde{K})$ על ידי "$\sigma \sim \tau$ אם $|\ |_\sigma = |\ |_\tau$". יהיו $\sigma_1, \dots, \sigma_g$ נציגים של מחלקות השקילות של $\mathrm{Embd}_K(L, \tilde{K})$. לכל i יהי $\hat{L}_i = \sigma_i L \cdot \hat{K}$ ההשלמה של K תחת $|\ |_{\sigma_i}$. לפי (א) עומדת מחלקת השקילות של σ_i בהתאמה חד חד ערכית עם הקבוצה $\mathrm{Embd}_{\hat{K}}(\hat{L}_i, \tilde{\hat{K}})$ שמספר אבריה $[\hat{L}_i : \hat{K}]$. לכן, $[L : K] = \sum_{i=1}^{g} [\hat{L}_i : \hat{K}]$. ∎

יהי עתה K שדה מספרים, ו p מספר ראשוני. תהי $|\ |'$ הרחבה של $|\ |_p$ לערך מחלט של K. נסמן ב w את ההערכה המתְקנת של K המתאימה ל $|\ |'$ ונחזר ונסמן את $|\ |'$ ב $|\ |_w$. יהי $(\hat{K}, |\ |_w)$ ההשלמה של $(K, |\ |_w)$. למה יח.ב(ב) מזהה את $\hat{K}$ עם הרחבה סופית של $\mathbb{Q}_p$ כך ש $|x|_w = |x|_p$ לכל $x \in \mathbb{Q}_p$. כמו כן שקול $|\ |_w$ שקול על $\hat{K}$ לערך המחלט המגדר על ידי $|x|_w^{[\hat{K}_w : \mathbb{Q}_p]}$.

מצד שני נגדיר ערך מחלט על $\hat{K}_w$ על ידי $\|x\|_w = q_w^{-w(x)}$, באשר $q_\omega = |\bar{K}_w|$. נסמן ב e את ציון ההסתעפות של w מעל $\mathbb{Q}$. עבור $x \in \mathbb{Q}_p$ מקבלים,

$$\|x\|_w = q_w^{-w(x)} = p^{-efv_p(x)} = p^{-v_p(x)[\hat{K}_w : \mathbb{Q}_p]} = |x|_p^{[\hat{K}_w : \mathbb{Q}_p]} = |x|_w^{[\hat{K}_w : \mathbb{Q}_p]}.$$

מיחידות ההרחבה של הערך המחלט מקבלים ש

$$\|x\|_w = |x|_w^{[\hat{K}_w : \mathbb{Q}_p]} \tag{4}$$

לכל $x \in \hat{K}_w$. אם נסמן ב P_w את האידאל הראשוני של O_K המתאים ל w, אזי $q_w = NP_w$ ו

$$\|x\|_w = NP_w^{-w(x)} \tag{5}$$

נסמן ב $V_0(K)$ את אסף ההערכות של K (עד כדי שקילות) . נבחר קבוצה $V_\infty(K)$ העומדת בהתאמה חד חד ערכית עם מחלקות השקילות של הערכים המחלטים המטריים של K. יהי $V(K) = V_0(K) \cup V_\infty(K)$. כל $w \in V_\infty(K)$ מתאים לשכון של K לתוך $\mathbb{C}$ המרחיב את השכון של $\mathbb{Q}$ לתוך $\mathbb{R}$. כמו לעיל $\hat{K}_w = \mathbb{R}K$ הנו ההשלמה של K ביחס ל w. נסמן ב $|\ |_w$ את ההרחבה היחידה של $|\ |_\infty$ ל $\hat{K}_w$. עתה נתקן ערך מחלט זה לפי הנסחה (4).

יש שתי אפשרויות: א. $\hat{K}_w = \mathbb{R}$ ואומרים ש w הנו ערך מחלט **ממשי**. ב. $\hat{K}_w = \mathbb{C}$ ואומרים ש w הנו ערך מחלט **מֻרכב**. במקרה השני $|\bar{z}|_w = |z|_w$ לכל $z \in \mathbb{C}$ (למה יח.ב(א)).

משפטון יח.ג (נסחת המכפלה): *יהי K שדה מספרים אלגברי ו $x \in K^\times$. אזי* $\prod_{w \in V(K)} \|x\|_w = 1$.

הוכחה: יהי $v \in V(\mathbb{Q})$. נסמן ב $E = \mathrm{Embed}(K/\mathbb{Q})$ את אסף כל השכונים של K לתוך הסגור האלגברי של $\hat{\mathbb{Q}}_v$. נגדיר שני אברים של $\mathrm{Embed}(K/\mathbb{Q})$ כשקולים אם הם נבדלים זה מזה באיזומורפיזם־$\mathbb{Q}_p$ כמפֹרט בלמה יח.ב. יהיו $\sigma_1, \ldots, \sigma_g$ נציגים של מחלקות השקילות. לכל i יהי w_i האבר של $V(L)$ המגדר על ידי הנסחה $|x|_{w_i} = |\sigma_i x|_v$, עבור $x \in L$. יהי $E_i = \mathrm{Embed}(\hat{K}_{w_i}/\hat{\mathbb{Q}}_v)$. לפי משפטון יח.ב

$$|\mathrm{Norm}_{K/\mathbb{Q}}(x)|_v = |\prod_{\sigma \in E} \sigma x|_v = \prod_{i=1}^{g} \prod_{\lambda \in E_i} |\lambda \sigma_i x|_v = \prod_{i=1}^{g} |x|_{w_i}^{[\hat{K}_{w_i}:\hat{\mathbb{Q}}_v]} = \prod_{i=1}^{g} \|x\|_{w_i}$$

עתה נפעיל את (2) על $\mathrm{Norm}_{K/\mathbb{Q}} x$:

$$\prod_{w \in V(K)} \|x\|_w = \prod_{v \in V(\mathbb{Q})} \prod_{w|v} \|x\|_w = \prod_{v \in V(\mathbb{Q})} |\mathrm{Norm}_{K/\mathbb{Q}}(x)|_v = 1 \quad \blacksquare$$

למה יח.ד: *יהיו L/K הרחבה סופית של שדות מספרים אלגבריים, $v \in V(K)$ ו $x \in K^\times$. אזי,*

$$\prod_{w|v} \|x\|_w = \|x\|_v^{[L:K]}.$$

הוכחה: יהי p המספר הראשוני המונח מתחת ל v. לפי למה יח.ב(ג),

$$\prod_{w|v} \|x\|_w = \prod_{w|v} |x|_w^{[\hat{L}_w:\mathbb{Q}_p]} = \prod_{w|v} |x|_v^{[\hat{L}_w:\mathbb{Q}_p]} = |x|_v^{\sum_{w|v}[\hat{L}_w:\mathbb{Q}_p]} = |x|_v^{[\hat{K}_v:\mathbb{Q}_p][L:K]} = \|x\|_v^{[L:K]},$$

כפי שהיה להוכיח. $\blacksquare$

יט. מחלקים

יהי K שדה מספרים. **מחלק** של K הנו פונקציה $\mathfrak{c}\colon V(K) \to \mathbb{R}$ המקימת את התנאים הבאים:

(1a) $\mathfrak{c}(v) > 0$ לכל $v \in V(K)$.

(1b) $\mathfrak{c}(v) = 1$ עבור כמעט כל v.

(1c) לכל $v \in V_0(K)$ קים $x \in K$ כך ש $\mathfrak{c}(v) = |x|_v$.

יהי $v \in V(K)$ ו $v_0 = v|_{\mathbb{Q}}$. נסמן $\nu(v) = [\hat{K}_v : \hat{\mathbb{Q}}_{v_0}]$ ו $\|\mathfrak{c}\|_v = \mathfrak{c}(v)^{\nu(v)}$. **הגֹדל** של $\mathfrak{c}$ יהיה המספר הממשי

$$\|\mathfrak{c}\| = \prod_{v \in V(K)} \mathfrak{c}(v)^{\nu(v)}$$

כל אבר $x \in K^\times$ מגדיר מחלק שערכו ב v שוה ל $|x|_v$. מחלק כזה נקרא **מחלק ראשי.** מכפלה של שני מחלקים $\mathfrak{c}, \mathfrak{c}'$ הנה המחלק $\mathfrak{c}\mathfrak{c}'$ המֻגדר על ידי הנסחה $(\mathfrak{c}\mathfrak{c}')(v) = \mathfrak{c}(v)\mathfrak{c}'(v)$. בפרט אם $x \in K^\times$ ו $\mathfrak{c}$ הנו מחלק אזי $x\mathfrak{c}$ הנו המחלק המֻגדר על ידי הנסחה $(x\mathfrak{c})(v) = |x|_v\mathfrak{c}(v)$. מנסחת המכפלה (משפטון יח.ג) נובע ש $\|x\mathfrak{c}\| = \|\mathfrak{c}\|$. בפרט הגדל של מחלק ראשי הנו 1.

יהי $\mathfrak{c}$ מחלק. נסמן

$$L(\mathfrak{c}) = \{x \in K \mid \ |x|_v \le \mathfrak{c}(v)\ \forall v \in V(K)\}$$

אפשר לראות את $L(\mathfrak{c})$ כקֻפסה רב ממדית שהארך של כמעט כל מקצועותיה שוה ל 1. את הגדל של $\mathfrak{c}$ אפשר לפרש כנפח של הקֻפסא. מספר האברים ב $L(\mathfrak{c})$ יסֻמן ב $\lambda(\mathfrak{c})$. התוצאה הבאה תאמר ש $\lambda(\mathfrak{c})$ הנו מספר סופי. בכל אפן, אם $a \in K^\times$, אזי ההעתקה $x \mapsto ax$ מעתיקה את $\mathcal{L}(\mathfrak{c})$ באפן חד חד ערכי על $\mathcal{L}(a\mathfrak{c})$. בפרט נקבל ש $\lambda(a\mathfrak{c}) = \lambda(\mathfrak{c})$.

דֻגמה יט.א: $K = \mathbb{Q}$. במקרה זה אפשר לראות כל מחלק כסדרה עם נקֻדת קצה באינסוף,

$$\mathfrak{c} = (2^{-\gamma(2)}, 3^{-\gamma(3)}, 5^{-\gamma(5)}, \ldots, e^{\gamma(\infty)})$$

שבה $\gamma(p)$ שלם לכל p ראשוני, $\gamma(p) = 0$ עבור כמעט כל p, e הנו בסיס הלוגריתמים הטבעיים, ו $\gamma(\infty)$ מספר ממשי כלשהוא. במקרה זה $\nu(p) = \nu(\infty) = 1$ לכל p. הגדל של $\mathfrak{c}$ הנו $\|\mathfrak{c}\| = \prod_p p^{-\gamma(p)} \cdot e^{\gamma(\infty)}$. כמו כן $L(\mathfrak{c})$ הנו קבוצת כל האברים $x \in \mathbb{Q}$ המקימים $v_p(x) \ge \gamma(p)$ עבור כל p ו $|x| \le e^{\gamma(\infty)}$. הואיל ו $\gamma(p) = 0$ עבור כמעט כל p המכנה של x חסום. מהתנאי באינסוף נובע שגם המונה של x חסום. לכן יש ל x רק מספר סופי של אפשרויות. במלים אחרות, $\lambda(\mathfrak{c}) < \infty$. ∎

למה יט.ב: *יהי K שדה מספרים.*

(א) *לכל $c > 0$ הקבוצה $L = \{x \in K \mid \ |x|_v \le c \text{ for all } v \in V(K)\}$ סופית.*

(ב) *לכל מחלק $\mathfrak{c}$ של K קים $a \in \mathbb{N}$ כך ש $\mathfrak{c}(av) \le 1$ לכל* $v \in V(K)$.

(ג) $\lambda(\mathfrak{c})$ *סופי לכל מחלק $\mathfrak{c}$ של* K.

הוכחה א: נניח תחִלה ש $K = \mathbb{Q}$. יהי $a \in L \smallsetminus \{0\}$. אם מספר ראשוני p מחלק את המכנה של a, אזי $c \ge |a|_p = p^{-v_p(a)}$ ו $v_p(a) < 0$. מ $-v_p(a)\log p \le \log c$ נובע ש p ו $v_p(a)$ חסומים. לכן המכנה של a חסום. הואיל ו $|a|_\infty \le c$, גם המונה של a חסום. לכן, יש רק מספר סופי של אפשרויות ל a.

נחזור עתה למקרה ש K שדה מספרים כלשהוא. יהי $x \in L$. אזי x הנו שרש של הפולינום

$$\prod_\sigma (X - \sigma x) = X^n + a_1 X^{n-1} + \cdots + a_n$$

במקדמים רציונליים $a_1, \ldots, a_n$, באשר σ עובר על כל שכוני K לתוך $\mathbb{C}$ ו $n = [K : \mathbb{Q}]$. לכל σ כנ"ל מתקים $|\sigma x|_v \le c$ לכל $v \in V(K)$. לכן קים $c_1 > 0$ התלוי רק ב c וב n כך ש $|a_i|_v \le c_1$ לכל $v \in V(\mathbb{Q})$ ועבור $i = 1, \ldots, n$. מהפסקה הקודמת עולה שיש רק מספר סופי של פולינומים המקימים תנאי זה. לכן, מספר ה x־ים ב L סופי.

הוכחת ב: תהי W תת קבוצה סופית של $V_0(K)$ המכילה את כל אותן ההערכות v המקימות $\mathfrak{c}(v) > 1$. נגדיל את W כך שיחד עם כל v תכיל W גם את כל ההערכות המונחות מעל הראשוני p המונח מתחת ל v. לכל p כזה נבחר $\alpha(p)$ טבעי כך ש $p^{-\alpha(p)}\mathfrak{c}(v) \le 1$ לכל v המונח מעל p. נסמן $a = \prod p^{\alpha(p)}$. אזי $|a|_v \mathfrak{c}(v) = p^{-\alpha(p)e(v/p)}\mathfrak{c}(v) \le 1$ עבור כל $v \in W$ ו $|a|_v \mathfrak{c}(v) = \mathfrak{c}(v) \le 1$ עבור כל $v \in V_0(K) \smallsetminus W$.

הוכחת (ג): יהי $a \in \mathbb{Z}$ כמו ב (ב). הואיל ו $\lambda(\mathfrak{c}) = \lambda(a\mathfrak{c})$ נוכל להחליף את $\mathfrak{c}$ במדת הצרך ב $a\mathfrak{c}$ כדי להניח ש $\mathfrak{c}(v) \le 1$ לכל $v \in V_0(K)$.

יהי $c > 0$ מספר הגדול מ 1 ומ $\mathfrak{c}(v)$ לכל $v \in V_\infty(K)$. אזי $L(\mathfrak{c})$ מוכלת בקבוצה הסופית L המופיעה ב (א). לכן, גם $L(\mathfrak{c})$ סופית. ∎

התוצאה הבאה אומרת שלמספר אברי $L(\mathfrak{c})$ יש אותו סדר גדל כמו לנפח של $\mathfrak{c}$.

משפטון יט.ג: *יהי K שדה מספרים. אזי קימים $c_1, c_2 > 0$ כך שלכל מחלק $\mathfrak{c}$ של K מתקים*

$$c_1\|\mathfrak{c}\| < \lambda(\mathfrak{c}) \le \max(1, c_2\|\mathfrak{c}\|)$$

הוכחה: נחלק את ההוכחה לשני חלקים.

הוכחת אי השויון הימני:

מקרה א: *יש ל K ערך מֻחלט מרֻכב w.* יהי m מספר שלם המקים

$$m < \sqrt{\lambda(\mathfrak{c})} \leq m+1 \tag{2}$$

אם $m \leq 0$ אי השויון הימני תקף. נניח אפוא ש $m \geq 1$. לפי ההגדרה מקים כל $z \in L(\mathfrak{c})$ את אי השויון $|z|_w \leq \mathfrak{c}(w)$. לכן $L(\mathfrak{c})$ מוכל ברבוע M במישור המרֻכב סביב הראשית שארך כל אחת מצלעותיו שוה ל $2\mathfrak{c}(w)$. נחלק כל אחת מצלעות M ל m חלקים שוים. באפן כזה נחלק את M ל m^2 רבועים שארך צלעותיהם $\frac{2\mathfrak{c}(w)}{m}$. הואיל וב $L(\mathfrak{c})$ יש, לפי (2), יותר מ m^2 אברים, קים רבוע קטן ובו שני אברים x, y של $L(\mathfrak{c})$ השונים זה מזה. המרחק ה w־י ביניהם אינו עולה על ארך האלכסון של הרבוע הקטן, כלומר

$$|x-y|_w \leq \frac{2\sqrt{2}\mathfrak{c}(w)}{m} \tag{3}$$

אם w' הנו ערך מֻחלט מטרי אחר של K אזי

$$|x-y|_{w'} \leq 2\mathfrak{c}(w') \tag{4}$$

אם v הנו ערך אולטרה־מטרי של K, אזי

$$|x-y|_v \leq \mathfrak{c}(v) \tag{5}$$

מנסחת המכפלה ומאי השויונות (3), (4) ו (5) נובע:

$$1 = \prod_{v \in V(K)} |x-y|_v^{\nu(v)} \leq \frac{c_3\|\mathfrak{c}\|}{m^2}$$

באשר $c_3 > 0$ הנו קבוע התלוי רק ב K. לכן, לפי (2), $\lambda(\mathfrak{c}) \leq (m+1)^2 \leq 4m^2 \leq 4c_3\|\mathfrak{c}\|$ כנדרש.

מקרה ב: *כל הערכים המֻחלטים המטריים של K ממשיים.* יהי m מספר שלם המקים $m < \lambda(\mathfrak{c}) \leq m+1$. שוב, נוכל להניח ש $m \geq 1$. נבחר ערך מֻחלט ממשי w ונחלק את הקטע $[-\mathfrak{c}(w), \mathfrak{c}(w)]$ ל m חלקים שוים. הואיל וב $L(\mathfrak{c})$ יש יותר מ m אברים, קימים x, y ב $L(\mathfrak{c})$ שונים זה מזה כך ש $|x-y|_w \leq \frac{2\mathfrak{c}(w)}{m}$. ממשיכים עתה כמו במקרה א.

הוכחת אי השויון השמאלי: נבחר בסיס־$\mathbb{Z}$ $w_1, \ldots, w_n$ של O_K (משפטון יד.ז) ונסמן

$$c_0 = n \cdot \max\left(|w_i|_v \mid i = 1, \ldots, n;\ v \in V_\infty(K)\right)$$

לכל v מטרי קים מספר רציונלי z_v המקים $c_0\mathfrak{c}(v)^{-1} \le z_v \le 2c_0\mathfrak{c}(v)^{-1}$. משפט Artin-Whaples (משפטון יח.א) נותן $z \in K^\times$ הקרוב־v לכל אחד מהמספרים z_v, $v \in V_\infty(K)$. הוא יקים

$$c_0 \le (z\mathfrak{c})(v) \le 2c_0 \qquad (6)$$

לכל v מטרי. לפי למה יט.ב(ב) נבחר מספר טבעי a כך ש $(az\mathfrak{c})(v) \le 1$ לכל v אולטרה־מטרי. מ (6) עולה ש $c_0|a|_v \le (az\mathfrak{c})(v) \le 2c_0|a|_v$ לכל v מטרי. הואיל וגם $\|\mathfrak{c}\|$ וגם $\lambda(\mathfrak{c})$ אינם משתנים כאשר מכפילים את $\mathfrak{c}$ בקבוע מ $K^\times$, נוכל להחליף את $\mathfrak{c}$ במדת הצרך ב $az\mathfrak{c}$ כדי להניח ש

$$\begin{aligned} c_0|a|_v \le \mathfrak{c}(v) \le 2c_0|a|_v \qquad & v \in V_\infty(K) \\ c(\mathfrak{v}) \le 1 \qquad & v \in V_0(K) \end{aligned} \qquad (7)$$

נבנה עתה אברים של $L(\mathfrak{c})$. לצרך זה נסמן

$$L = \{\sum_{i=1}^n a_i w_i \mid\ a_i \in \mathbb{Z} \text{ and } 0 \le a_i \le a\}$$

אזי יש ב L יותר מ a^n אברים. נרשֹם את $\mathfrak{c}$ בצורה

$$\mathfrak{c} = \mathfrak{c}_\infty \prod_{v \in V_0(K)} |\pi_v|_v^{b_v}$$

באשר $\mathfrak{c}_\infty$ הנו החלק האינסופי של $\mathfrak{c}$ המֻגדר על ידי $\mathfrak{c}_\infty(v) = \mathfrak{c}(v)$ עבור v מטרי ו $\mathfrak{c}_\infty(v) = 1$ עבור v אולטרה־מטרי ו π_v הנו אבר ראשוני ביחס ל v אם v אולטרה־מטרי. כמו כן b_v הם מספרים שלמים אי שליליים שכמעט כלם אפס.

לכל v אולטרה־מטרי מתאים אידאל ראשוני P_v של O_K. נסמן $A = \prod_{v \in V_0(K)} P_v^{b_v}$ ונתבונן בחבורת המנה O_K/A. מספר אבריה הנו NA. הואיל ו $|L| > a^n$ קימת ל L תת קבוצה L_0 בת יותר מ $\frac{a^n}{NA}$ אברים המוכלת במחלקה אחת של O_K מודול A.

נבחר אבר קבוע x ב L_0. לכל $y \in L_0 \smallsetminus \{x\}$ מתקים $x - y \in A$. לכן, $|x-y|_v \le |\pi_v|_v^{b_v} = \mathfrak{c}(v)$ לכל v אולטרה־מטרי. נתבונן ב v מטרי. קימים $b_1, \dots, b_n$ שלמים בין $-a$ ל a כך ש $x - y = \sum_{i=1}^n a_i w_i$. מהגדרת c_0 ומ (7) נובע ש $|x-y|_v \le c_0|a|_v \le \mathfrak{c}(v)$. מכל זה נובע ש $x - y \in L(\mathfrak{c})$. בנוסף לזה $0 \in L(\mathfrak{c})$. בזאת הוכחנו ש

$$\lambda(\mathfrak{c}) \ge |L_0| > \frac{a^n}{NA}. \qquad (8)$$

לפי למה יח.ד ולפי (7),

$$a^n = \prod_{v\in V_\infty(K)} |a|_v^{\nu(v)} \geq \prod_{v\in V_\infty(K)} \frac{\mathfrak{c}(v)^{\nu(v)}}{(2c_0)^{\nu(v)}} = c_1 \prod_{v\in V_\infty(K)} \|\mathfrak{c}\|_v \tag{9}$$

באשר $c_1 = \prod_{v\in V_\infty(K)}(2c_0)^{-\nu(v)}$. מאידך, אם v אולטרה־מטרי, p המספר הראשוני מתחת ל P_v, $e = e(P_v/p)$ ו $f = f(P_v/p)$, אזי

$$\frac{1}{NP_v} = \frac{1}{p^f} = |\pi_v|_v^{ef} = |\pi_v|_v^{\nu_v}$$

לכן, לפי משפטון טו.ד,

$$\frac{1}{NA} = \prod_{v\in V_0(K)} \frac{1}{NP_v^{b_v}} = \prod_{v\in V_0(K)} |\pi_v|_v^{b_v}. \tag{10}$$

מ (8), (9) ו (10) עולה ש $\lambda(\mathfrak{c}) \geq c_1\|\mathfrak{c}\|$, כנדרש. ∎

ממשפטון יט.ג נסיק את הלמה הבאה:

למה יט.ד: *לכל $v_0 \in V(K)$ קים קבוע $c(v_0) > 0$ בעל התכונה הבאה: לכל מחלק $\mathfrak{c}$ קים $y \in K^\times$ המקים*

$$1 \leq \|y\mathfrak{c}\|_v \leq c(v_0)$$

לכל $v \neq v_0$.

הוכחה: יהי c_1 הקבוע המופיע במשפטון יט.ג. נגדיר $c_0 = 1$ אם v_0 מטרי. אם v_0 אולטרה־מטרי נבחר אבר ראשוני π_0 ביחס ל v_0. בפרט $|\pi_0|_{v_0} < 1$. נגדיר $c_0 = |\pi_0|_{v_0}^{-\nu(v_0)}$. לבסוף נגדיר $c(v_0) = \frac{c_0}{c_1}$.

נתבונן עתה במחלק $\mathfrak{c}$. נגדיר מחלק $\mathfrak{c}'$ באפן הבא: $\mathfrak{c}'(v) = \mathfrak{c}(v)$ לכל $v \neq v_0$. נסמן

$$c_3 = \prod_{v\neq v_0} \|\mathfrak{c}\|_v = \prod_{v\neq v_0} \|\mathfrak{c}'\|_v.$$

אם v_0 מטרי, נגדיר את $\mathfrak{c}'(v_0)$ כך שֶׁיְּקַיֵּם $c_3 \cdot c'(v_0)^{\nu(v_0)} = \frac{1}{c_1}$. אזי $\|\mathfrak{c}'\| = \frac{1}{c_1}$. אם v_0 אולטרה־מטרי, נסמן $\alpha_k = c_1^{-1}|\pi_v|_v^{-\nu(v)k}$ לכל k שלם. כאשר k שואף לאינסוף, שואף α_k לאינסוף וכאשר k שואף למינוס אינסוף שואף α_k לאפס. לכן, קים k שלם כך ש $\alpha_k \leq c_3 < \alpha_{k+1}$ ולכן

$$\frac{1}{c_1} \leq |\pi_0|_{v_0}^{k\nu(v_0)} c_3 \leq \frac{|\pi_0|_{v_0}^{-\nu(v_0)}}{c_1}.$$

נגדיר $\mathfrak{c}'(v_0) = |\pi_0|_{v_0}^k$.

בשני המקרים $\mathfrak{c}'$ יקים

$$\frac{1}{c_1} \leq \|\mathfrak{c}'\| \leq \frac{c_0}{c_1} \tag{11}$$

לפי משפטון יט.ג, $\lambda(\mathfrak{c}') > c_1\|\mathfrak{c}'\| \geq 1$. לכן קים $x \in L(\mathfrak{c}')$ כך ש $x \neq 0$. במלים אחרות, $|x|_v \leq \|\mathfrak{c}'\|_v$ לכל $v \in V(K)$.

האבר $y = x^{-1}$ יקים $\|y\mathfrak{c}'\|_v \geq 1$ לכל $v \in V(K)$. לכן, $\|y\mathfrak{c}\|_v \geq 1$ לכל $v \neq v_0$.

אי השויון הימני נובע עבור $v \neq v_0$ מאי השויון השמאלי ומ (11):

$$\|y\mathfrak{c}\|_v = \|y\mathfrak{c}'\|_v = \frac{\|y\mathfrak{c}'\|}{\prod_{w\neq v}\|y\mathfrak{c}'\|_w} \leq \|y\mathfrak{c}'\| = \|\mathfrak{c}'\| \leq \frac{c_0}{c_1} = c(v_0)$$

כנדרש. ∎

יהי V מרחב וקטורי מעל $\mathbb{R}$ ממֵמד סופי. תת קבוצה A של V מכֻנה **בדידה** אם לכל $a \in A$ קימת סביבה פתוחה U של V כך ש $U \cap A = \{a\}$. במלים אחרות, הטופולוגיה המֻשרית על A מ V בדידה.

טענה כ.א: *תת קבוצה A של V הנה סגורה ובדידה אם ורק אם $B \cap A$ סופית לכל תת קבוצה חסומה B של V.*

הוכחה: נניח קודם ש A סגורה ובדידה ותהי B תת קבוצה חסומה של A. אלו היתה $B \cap A$ אינסופית היתה קימת לה נקֻדת הצטברות, בסתירה לבדידות של A.

להפך, נניח ש A אינ סגורה. נבחר $\bar{a}$ בסגור של A שאינו ב A. אזי בכל כדור פתוח סביב $\bar{a}$ נמצאים אינסוף אברים של A.

להפך, נניח ש A אינה בדידה. אזי יש ל A נקֻדת הצטברות a. בכל כדור פתוח סביב a יהיו אינסוף נקֻדות של A. ∎

דגמה כ.ב: הקבוצה $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$ אינסופית, בדידה וחסומה אולם אינה סגורה. ∎

תהי Γ תת חבורה של V. לממד של תת המרחב של V הנוצר על ידי Γ נקרא **הממד** של Γ. יהי אפוא $m = \dim(\Gamma)$. אזי יש ב Γ אברים $v_1, \dots, v_m$ שאינם תלויים לינארית מעל $\mathbb{R}$. בפרט, $v_1, \dots, v_m$ אינם תלויים לינארית מעל $\mathbb{Z}$. לכן, $\dim(\Gamma) \le \operatorname{rank}(\Gamma)$.

דגמה כ.ג:

(א) יהי $\Gamma = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. אזי $\dim(\Gamma) = 1$ ו $\operatorname{rank}(\Gamma) = 2$. יתר על כן, משפט של מנקובסקי אומר ש Γ צפופה ב $\mathbb{R}$ בפרט Γ אינה סגורה ב $\mathbb{R}$.

(ב) תת החבורה $\mathbb{Q}$ של $\mathbb{R}$ מקימת $\dim(\mathbb{Q}) = \operatorname{rank}(\mathbb{Q}) = 1$ אולם $\mathbb{Q}$ אינה נוצרת סופית. ∎

שריג ב V הנו תת חבורה Γ נוצרת סופית המקַימֶת $\dim(\Gamma) = \operatorname{rank}(\Gamma)$. בפרט

$$m = \operatorname{rank}(\Gamma) \le \dim(V) < \infty.$$

בנוסף לזה Γ חסרת פתול. לכן, לפי המשפט היסודי של החבורות האבליות הנוצרות סופית, Γ הנה חבורה אבלית חפשית מדרגה m. במלים אחרות, $\Gamma = \sum_{i=1}^m \mathbb{Z}v_i$ ו $v_1, \dots, v_m$ אינם תלויים לינארית מעל $\mathbb{Z}$. כמו כן $\mathbb{R}\Gamma = \sum_{i=1}^m \mathbb{R}v_i$. הואיל ו $\dim(\mathbb{R}\Gamma) = m$ האברים אינם תלויים לינארית מעל $\mathbb{R}$. הם מהוים אפוא בסיס של המרחב הוקטורי $\mathbb{R}\Gamma$. נכנה אותם גם בשם **בסיס** של השריג Γ.

משפטון כ.ד: *יהי V מרחב וקטורי ממֵמד סופי מעל $\mathbb{R}$ ו Γ תת חבורה של V. אזי Γ הנָה שריג אם ורק אם Γ סגורה ובדידה.*

הוכחה: נניח קודם ש Γ הנה שריג. יהי $(v_1, \dots, v_m)$ בסיס של Γ. נרחיב את $(v_1, \dots, v_m)$ לבסיס $(v_1, \dots, v_n)$ של V. תהי $v = \sum_{i=1}^m \alpha_i v_i$ נקֻדה ב V. אזי $U = \{\sum_{i=1}^m \alpha_i v_i \mid |\alpha_i - a_i| < 1,\ i = 1, \dots, m\}$ הנה סביבה פתוחה של v ב V המכילה לכל היותר נקֻדה אחת של Γ. לכן, Γ סגורה ובדידה.

להפך, נניח ש Γ חבורה סגורה ובדידה. נוכיח באנדוקציה על $\dim(\Gamma)$ ש Γ הנה שריג. אם $\dim(\Gamma)=0$, אזי $\Gamma=0$ הנו שריג טריביאלי. נניח אפוא ש $\dim(\Gamma)=m$ ושהטענה הוכחה כבר עבור $m-1$.

יהי W תת המרחב של V הנפרש על ידי Γ. יהי $(v_1,\dots,v_m)$ בסיס של W שאבריו שיכים ל Γ. נסמן $W_0=\sum_{i=1}^{m-1}\mathbb{R}v_i$. אזי $\Gamma_0=\Gamma\cap W_0$ הנה תת חבורה סגורה ובדידה של W_0 מממד $m-1$. הנחת האנדוקציה נותנת $w_1,\dots,w_{m-1}$ ב W שאינם תלויים לינארית כך ש $\Gamma_0=\sum_{i=1}^{m}\mathbb{Z}w_i$. בפרט $(w_1,\dots,w_{m-1})$ מהוה בסיס של W_0. יתר על כן, $v_m\notin W_0$. לכן, $(w_1,\dots,w_{m-1},v_m)$ מהוה בסיס של W.

כל אבר v של Γ נתן לרשם כסכום

$$v=\sum_{i=1}^{m-1}\alpha_i w_i+\alpha_m v_m \tag{1}$$

שבו $\alpha_i\in\mathbb{R}$ עבור $i=1,\dots,m$. נסמן ב T את אסף כל ה v־ים ב Γ שבהם $0\le\alpha_i<1$ עבור $i=1,\dots,m-1$ ו $0<\alpha_m\le 1$. בפרט T תת קבוצה חסומה של Γ ולכן סופית (טענה כ.א). כמו כן, T אינה ריקה כי היא מכילה את v_m. יהי

$$w_m=\sum_{i=1}^{m-1}\beta_i w_i+\beta_m v_m \tag{2}$$

אבר של T כך שבהצגות הנ"ל $\beta_m\le\alpha_m$ לכל $v\in\Gamma$. נוכיח ש $\Gamma=\sum_{i=1}^{m}\mathbb{Z}w_i$.

ואכן, הואיל ו $\beta_m\ne 0$, שיך w_m ל $\Gamma\smallsetminus W_0$. לכן, $(w_1,\dots,w_{m-1},w_m)$ מהוה בסיס של W. יהי אפוא $v\in\Gamma$. אזי $v=\sum_{i=1}^{m}\alpha_i w_i$ באשר $\alpha_i\in\mathbb{R}$. נרשם $\alpha_m=[\alpha_m]+\alpha'_m$ באשר $[\alpha_m]$ הנו החלק השלם של α_m ו $0\le\alpha'_m<1$ הנו החלק השבור. אזי, לפי (2)

$$\begin{aligned} v-[\alpha_m]w_m &= \sum_{i=1}^{m-1}\alpha_i w_i+\alpha'_m w_m \\ &= \sum_{i=1}^{m-1}\alpha_i w_i+\sum_{i=1}^{m-1}\alpha'_m\beta_i w_i+\alpha'_m\beta_m w_m \\ &= \sum_{i=1}^{m-1}\gamma_i w_i+\alpha'_m\beta_m w_m \end{aligned}$$

באשר $\gamma_i=\alpha_i+\alpha'_m\beta_i$. נרשם $\gamma_i=[\gamma_i]+\gamma'_i$ באשר $0\le\gamma'_i<1$. אזי

$$v-\sum_{i=1}^{m-1}[\gamma_i]w_i-[\alpha_m]w_m=\sum_{i=1}^{m-1}\gamma'_i w_i+\alpha'_m\beta_m w_m. \tag{3}$$

אגף שמאל של (3) שיך ל Γ. אלו היה $\alpha'_m > 0$, היה $0 < \alpha'\beta_m < \beta_m \leq 1$ ולכן היה אגף שמאל שיך ל T. זה היה סותר את המזעריות של β_m. לכן $\alpha'_m = 0$. מכאן נובע ש

$$v - [\alpha_m]w_m = \sum_{i=1}^{m-1} \alpha_i w_i. \tag{4}$$

אגף שמאל של (4) שיך ל Γ ואלו אגף ימין שיך ל W_0. לכן שיך אגף שמאל ל Γ_0. קיימים אפוא $a_1, \ldots, a_{m-1} \in \mathbb{Z}$ כך ש $v = \sum_{i=1}^{m} a_i w_i + [\alpha_m]w_m$, כנדרש. ∎

יהי K שדה מספרים ו S קבוצה סופית של ערכים מֻחלטים של K המכילה את כל הערכים המטריים. נסמן

$$K_S = \{x \in K^\times \mid |x|_v = 1 \quad \forall v \in V(K) \smallsetminus S\}$$

כל אבר K_S נקרא **אחֻדת־**S. אחדות־$V_\infty(K)$ הנן האברים ההפיכים של O_K. הקבוצה K_S מהוה תת חבורה של $K^\times$. מטרת הסעיף הזה הנה להוכיח ש K_S נוצרת סופית ולקבע את המבנה שלה. הצעד הראשון בכוון זה יהיה להוכיח שחבורת שרשי היחידה W_K של K סופית.

משפטון כא.א: *W_K הנה אסף כל האברים $x \in K^\times$ המקימים $|x|_v = 1$ לכל $v \in V(K)$. זוהי תת חבורה סופית של O_K.*

הוכחה: קודם כל נעיר שאם מספר ממשי חיובי u מקים $u^k = 1$ עבור k טבעי, אזי $u = 1$. לכן, אם $x \in K$ מקים $x^k = 1$, אזי $|x|_v^k = 1$ ולכן $|x|_v = 1$ לכל v.

הוכחנו אפוא ש W_K מוכלת בתת החבורה $W' = \{x \in K^\times \mid |x|_v = 1 \ \forall v \in V(K)\}$ של $K^\times$. לפי למה יט.ב, W' סופית. לכן, כל אבר ב W' הוא בעל סדר סופי, כלומר הוא שרש יחידה. מכאן ש $W = W'$, כנדרש.

∎

יהיו עתה $v_1, \ldots, v_s$ כל אברי S. נראה את $\mathbb{R}^s$ כחבורה חבורית ונגדיר הומומורפיזם $\lambda\colon K_S \to \mathbb{R}^s$ על ידי

$$\lambda(x) = \big(\log \|x\|_{v_1}, \log \|x\|_{v_2}, \ldots, \log \|x\|_{v_s}\big)$$

נראה את $\mathbb{R}^s$ גם כמרחב וקטורי מעל $\mathbb{R}$. מנֻסחת המכפלה (משפטון יח.ג) נובע ש

$$\log \|x\|_{v_1} + \log \|x\|_{v_2} + \cdots + \log \|x\|_{v_s} = 0$$

לכן $\Lambda = \lambda(K_S)$ מוכל במרחב העל ה $(s-1)$־ממדי L של $\mathbb{R}^s$ המֻגדר על ידי המשואה:

$$X_1 + X_2 + \cdots + X_s = 0 \qquad (1)$$

משפטון כא.ב: *Λ הנו שריג $(s-1)$־ממדי ב $\mathbb{R}^s$.*

אם נוכיח את המשפטון נקבל ש Λ יִצור את תת המרחב (1). בפרט נקבל ש Λ הנה חבורה חלופית (חבורית) חפשית שדרגתה $s-1$. הגרעין של λ מֻרכב מכל האברים $x \in K$ המקימים $\|x\|_v = 1$ לכל v. לפי משפטון כא.א, $\mathrm{Ker}(\lambda) = W_K$ הנה חבורה סופית. ביתר דיוק, W_k הנה חבורת כל שרשי היחידה המוכלים ב K. זה יתן לנו את התוצאה הבאה:

משפט כא.ג (משפט האחדות של דיריכלה): *יהי K שדה מספרים, S קבוצה סופית של ערכים מֻחלטים המכילה את כל הערכים המטריים ו $s = |S|$. אזי $K_S \cong W_K \times \mathbb{Z}^{s-1}$.*

למה כא.ד: *לכל i בין 1 ל $s-1$ יהי $\boldsymbol{\xi}_i = (\xi_{i1}, \ldots, \xi_{is})$ וקטור ב L המקים $\xi_{ij} < 0$ עבור $i \neq j$. אזי $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{s-1}$ אינם תלויים לינארית.*

הוכחה: עלינו להוכיח שדרגת המטריצה $X = (\xi_{ij})_{1\le i\le s-1, 1\le j\le s}$ היא $s-1$. לשם כך נסמן ב $\tilde{\boldsymbol{\xi}}_j$ את העמודה ה j־ית של X ונוכיח ש $\tilde{\boldsymbol{\xi}}_1, \ldots, \tilde{\boldsymbol{\xi}}_{s-1}$ אינם תלויים לינארית.

ואכן יהיו $a_1, \ldots, a_{s-1}$ מספרים ממשיים שלא כֻּלם אפס כך ש $\sum_{j=1}^{s-1} a_j \tilde{\boldsymbol{\xi}}_j = 0$. נכפיל לפי הצרך את השויון ב -1 ונתמיר את $1, \ldots, s-1$ כדי להניח ש $a_1 > 0$ ו $a_1 \ge a_j$ עבור $j = 1, \ldots, s-1$. לפי ההנחה $\xi_{1j} < 0$ עבור $j = 2, \ldots, s$. מההנחה ש $\boldsymbol{\xi}_1 \in L$ נובע ש $\sum_{j=1}^{s-1} \xi_{1j} = -\xi_{1,s}$. לכן,

$$0 = \sum_{j=2}^{s-1} a_j \xi_{1j} \ge a_1 \sum_{j=2}^{s-1} \xi_{1j} = -a_1 \xi_{1s} > 0.$$

זוהי סתירה. ∎

הוכחת משפטון כא.ב: נתחיל את הוכחת המשפטון בהערה שבכל תחום חסום של $\mathbb{R}^s$ יש רק מספר סופי של אברים של Λ. ואכן, אם $\lambda(x)$ חסום עבור x השיך לתת קבוצה A של K_S, אזי $\|x\|_v$ חסום לכל v. לכן, לפי למה יט.ב, A סופית.

מההערה ומטענה כ.א נובע ש Λ היא תת חבורה סגורה ובדידה של $\mathbb{R}^s$. לכן, לפי למה כ.ד, ש Λ הנו שריג. בפרט Λ הוא תת חבורה חפשית של $\mathbb{R}^s$. הואיל ו Λ מוכלת במרחב ה $(s-1)$־ממדי, $\dim(\Lambda) \le s-1$. כדי לסים את הוכחת המשפטון עלינו עוד להצביע על $s-1$ וקטורים ב Λ שאינם תלויים לינארית מעל $\mathbb{R}$. לצרך זה נבנה לכל i בין 1 ל $s-1$ וקטור $\boldsymbol{\xi}_i = (\xi_{i1}, \ldots, \xi_{is})$ ב Λ המקים $\xi_{ij} < 0$ עבור $i \neq j$. אזי $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{s-1}$ יקיְמו את תנאי למה כא.ד ולכן לא יהיו תלויים לינארית.

בלי הגבלת הכלליות נניח ש $i = 1$. $v_0 \in S$. לפי למה יט.ד קים $c_0 > 0$ כך שלכל מחלק $\mathfrak{c}$ קים $y \in K^\times$ המקים

$$(2) \qquad v \neq v_1 \quad \Longleftarrow \quad 1 \le \|y\mathfrak{c}\|_v \le c_0.$$

לכל $v \in V(K)$ יהי P_v האידאל המתאים של O_K. נסמן $S' = S \cup \{v \in V(K) \mid NP_v \le c_0\}$. זוהי קבוצה סופית (כי מעל כל מספר ראשוני מונחים רק מספר סופי של אידאלים של O_K). אם $v \in V(K) \smallsetminus S'$, אזי $NP_v > c_0$. מצד שני, קים $k \ge 0$ שלם כך ש $\|y\mathfrak{c}\|_v = NP_v^k$ (לפי (5) בסעיף יח). לכן, לפי (2), $k = 0$. כלומר

$$(3) \qquad v \in V(K) \smallsetminus S' \quad \Longleftarrow \quad \|y\mathfrak{c}\|_v = 1.$$

נסמן עתה ב C את קבוצת כל המחלקים $\mathfrak{c}$ של K שעבורם $\mathfrak{c}(v) \ge 1$ לכל $v \in V(K)$ ו $\mathfrak{c}(v) = 1$ לכל $v \in V(K) \smallsetminus S$. מ (2) ו (3) נובע שלכל $\mathfrak{c} \in C$ קים $y \in K^\times$ כך ש

$$\begin{aligned} (4a)\quad & v \neq v_1 \implies 1 \le \|y\mathfrak{c}\|_v \le c_0. \\ (4b)\quad & v \in V(K) \smallsetminus S \implies 1 \le \|y\|_v \le c_0 \\ (4c)\quad & v \in V(K) \smallsetminus S' \implies \|y\|_v = 1. \end{aligned}$$

נסמן ב Y את קבוצה כל ה y־ים המתאימים למחלקים השיכים ל C. נגדיר העתקה של Y לתוך $\mathbb{R}^{S' \smallsetminus S}$ על ידי $\varphi\colon Y \to$ $\varphi(y) = (\|y\|_v \mid v \in S' \smallsetminus S)$. הקבוצה $S' \smallsetminus S$ סופית. לכל $v \in S' \smallsetminus S$ המספר $\|y\|_v$ חסום מלעיל ומלרע (לפי $(4b)$) ושוה לחזקה שלמה של NP_v (לפי (5) בסעיף יח). לכן, $\varphi(Y)$ סופית. יהיו $y_1, \ldots, y_m$ נציגים של סיבֵי φ ב Y. נסמן $b = \min(\|y_j\|_v \mid v \in S' \smallsetminus S,\ j = 1, \ldots, m)$. אזי $b > 0$.

נבחר מחלק $\mathfrak{c}$ ב C כך ש $\mathfrak{c}(v) > \frac{c_0}{b}$ לכל $v \in S$. יהי y אבר של $K^\times$ המקים את (4). לפי הפסקה הקודמת קים j כך ש $\varphi(y) = y_j$. כלומר $\|y\|_v = \|y_j\|_v$ לכל $v \in S' \smallsetminus S$. לפי $(4c)$, $\|y\|_v = 1 = \|y_j\|$ לכל $v \in V(K) \smallsetminus S'$. לכן קים $u \in K_S$ כך ש $y = uy_j$. לכל $v \neq v_1$ נסיק מ $(4a)$ ומהגדרת b ש $\|u\mathfrak{c}\|_v = \frac{1}{\|y_j\|_v}\|y\mathfrak{c}\|_v \le \frac{c_0}{b}$. לכן, לפי בחירת $\mathfrak{c}$, $\|u\|_v \le \frac{c_0}{b \cdot \mathfrak{c}(v)} < 1$. במלים אחרות, $\log \|u\|_v < 0$ לכל $v \in S \smallsetminus \{v_1\}$. הוקטור $(\log \|u\|_{v_1}, \log \|u\|_{v_2}, \ldots, \log \|u\|_{v_s})$ יקים את הדרישות. ∎

משפט כא.ה: *יהי E עקֻם אלפטי מעל שדה מספרים K. אזי $E(K)/2E(K)$ הנה חבורה סופית.*

הוכחה: בתור הסגור השלם של $\mathbb{Z}$ ב K, O_K הנו חוג דדקינד (משפטון ג.ד). כמו כן, חבורת מחלקות האידאלים השבורים של O_K סופית (משפט יז.ג). בנוסף, לכל תת קבוצה סופית S של אידאלים מרביים של O_K חבורת אחדות־S, $U_{K,S}$, נוצרת סופית (משפט כא.ג). אותן טענות נכונות לכל הרחבה סופית L של K. לכן, K מהוה חוג ארתמטי ביחס ל O_K במונחים של סעיף ד. משפטון ז.א אומר ש E ו K מקַימים את התנאים (1) ו (2) של סעיף ה ביחס ל $m = 2$. יתר על כן, משפטון זה מגדיר קבוצה סופית, $\mathrm{Bad}_K(E)$, של מחלקים ראשוניים ואומר שיש ל E העמדה טובה ביחס לכל מחלק ראשוני של K שאינו שיָך ל $\mathrm{Bad}_K(E)$. בזה הראינו שקבוצה המחלקים הראשוניים של K מקַימת את הדרישות (1)־(5) של סעיף ד. מתוצאה ז.ב נובע ש $E(K)/2E(K)$ היא חבורה סופית. ∎

בסעיף זה נגדיר פונקציה גבה על $\mathbb{P}^n(K)$ לכל n טבעי ולכל שדה מספרים K. הואיל ועבור כל עקֹם אלפטי E מעל K נִתן לשכן את $E(K)$ בתוך $\mathbb{P}^2(K)$, נגדיר באֹפן כזה גם פונקצית גבה על $E(K)$. בסעיף הבא נוכיח שפונקצית הגבה של $E(K)$ תקיֵם את התנאים בהגדרה א.א. בכך תֻשלם הוכחת משפט מורדל־וייל לעקֻמים אלפטיים מעל שדות מספרים.

כפי שהגדרנו את הפונקטור $\mathbb{P}^2$, כן נגדיר גם את הפונקטור $\mathbb{P}^n$. לכל שדה L יהיה $\mathbb{P}^n(L)$ קבוצת מחלקות השקילות של כל ה $(n+1)$־יות $(x_0,\dots,x_n)$ של אברי L שלא כֻלם אפס. שתי $(n+1)$־יות $(x_0,\dots,x_n)$ ו $(x'_0,\dots,x'_n)$ של אברי L **שקולות זו לזו** אם קיָם $a\in L^\times$ כך ש $x'_i=ax_i$ עבור $i=0,\dots,n$. נסמן את מחלקת השקילות של $(x_0,\dots,x_n)$ ב $(x_0{:}\cdots{:}x_n)$. אם L' הנו הרחבה של L, אזי אפשר לשכן את $\mathbb{P}^n(L)$ באֹפן טבעי ב $\mathbb{P}(L')$ על ידי שמתאימים למחלקת השקילות של $(n+1)$־יה $(x_0,\dots,x_n)$ ב L^{n+1} את מחלקת השקילות של $(x_0,\dots,x_n)$ ב $(L')^{n+1}$.

דֻגמה כב.א: גבה על $\mathbb{P}^n(\mathbb{Q})$. יהיו $x_0,\dots,x_n\in\mathbb{Q}$ שלא כֻלם אפס. נסמן $\mathbf{p}=(x_0{:},\dots{:}x_n)$. על ידי כפל במכנה משֻתף של $x_0,\dots,x_n$ נוכל להניח שכֻלם שיָכים ל $\mathbb{Z}$. על ידי כפל בהפוך של המחלק המֻשתף הגדול ביותר של $x_0,\dots,x_n$ נוכל להניח ש $\gcd(x_0,\dots,x_n)=1$. לאחר תִקון זה נגדיר

$$.H(\mathbf{p})=\max(|x_0|,\dots,|x_n|) \qquad (1)$$

הגדרה זו תואמת להגדרת הגבה ח.ב על $\mathbb{Q}$. ואכן, בהגדרה הנ"ל מציגים כל אבר x של $\mathbb{Q}^\times$ כשבר $\frac{a}{b}$ מצֻמצם ומגדירים $H(x)=\max(|a|,|b|)$. השִכון הרגיל של $\mathbb{Q}$ ב $\mathbb{P}^1(\mathbb{Q})$ מעתיק את x לנקֻדה $(1:x)$ השווה גם ל $(a{:}b)$. לכן, $H(x)=H(1:x)$.

מ (1) עולה גם ש

$$\#\{\mathbf{p}\in\mathbb{P}^n(\mathbb{Q})\mid\ H(\mathbf{p})\le c\}\le(2c+1)^{n+1} \qquad (2)$$

לכל $c>0$. זוהי אחת התכונות הנדרשות בהגדרה א.א. ∎

בדֻגמה כא.ב השתמשנו בעֲרכים מֻחלטים ממשיים כדי להגדיר פונקצית גבה על $\mathbb{P}^n(\mathbb{Q})$. כדי להגדיר פונקצית גבה על $\mathbb{P}^n(K)$ עבור שדה מספרים כלשהוא, נשתמש בערכים המחלטים המתֻקנים $\|\ \|_w$ שהֻגדרו בסעיף יח.

הגדרה כב.ב: לכל נקֻדה $\mathbf{p}=(x_0{:}\cdots{:}x_n)$ של $\mathbb{P}^n(K)$ נגדיר

$$.\ H_K(\mathbf{p})=\prod_{v\in V(K)}\max(\|x_0\|_v,\dots,\|x_n\|_v) \qquad (3)$$

למה כב.ג: *תהי* $\mathbf{p} \in \mathbb{P}^n(K)$.

(א) *הגדרת הגׂבה* $H_K(\mathbf{p})$ *אינה תלויה בבחירת הקואורדינטות ההומוגניות עבור* $\mathbf{p}$.

(ב) $H_K(\mathbf{p}) \geq 1$.

(ג) *לכל הרחבה סופית* L *של* K *מתקיֵם* $H_L(\mathbf{p}) = H_K(\mathbf{p})^{[L:K]}$.

הוכחת א: יהיו $x_0, \dots, x_n$ קואורדינטות הומוגניות של $\mathbf{p}$ ויהי $a \in K^\times$. לפי נֻסחת המכפלה (משפטון יח.ג), $\prod_{v \in V(K)} \|a\|_v = 1$. לכן

$$\begin{aligned}\prod_{v \in V(K)} \max(\|ax_0\|_v, \dots, \|ax_n\|_v) &= \prod_{v \in V(K)} \|a\|_v \max(\|x_0\|_v, \dots, \|x_n\|_v) \\ &= \prod_{v \in V(K)} \max(\|x_0\|_v, \dots, \|x_n\|_v)\end{aligned}$$

כפי שצריך להוכיח.

הוכחת ב: נבחר את הקואורדינטות של $\mathbf{p}$ כך שאחת מהן שוה ל 1. אזי, לכל $v \in V(K)$ יתקיֵם $\max(\|x_0\|_v, \dots, \|x_n\|_v) \geq 1$ ולכן $H_K(\mathbf{p}) \geq 1$.

הוכחת ג: יהי $v \in V(K)$ ונִתן ל w לעבר על כל האברים של $V(L)$ המחלקים את v. כמו כן נסמן ב p את המספר הראשוני המונח מתחת ל v. לכל $x \in K^\times$ מתקיֵם $\|x\|_v = |x|^{[\hat{K}_v:\mathbb{Q}_p]}$ (סעיף יח), $|x|_w = |x|_v$ ו $\prod_{w|v} \|x\|_w = \|x\|_v^{[L:K]}$ (למה יח.ד). לכן,

$$\begin{aligned}\prod_{w|v} \max(\|x_0\|_w, \dots, \|x_n\|_w) &= \prod_{w|v} \max(|x_0|_2^{[\hat{L}_w:\mathbb{Q}_p]}, \dots, |x_n|_2^{[\hat{L}_w:\mathbb{Q}_p]}) \\ &= \Big(\prod_{w|v} \max(|x_0|_v, \dots, |x_n|_v)^{[\hat{L}_w:\hat{K}_v]}\Big)^{[K_v:\mathbb{Q}_p]} \\ &= \Big(\max(|x_0|_v, \dots, |x_n|_v)^{\sum_{w|v}[\hat{L}_w:\hat{K}_v]}\Big)^{[K_v:\mathbb{Q}_p]} \\ &= \max(|x_0|_v, \dots, |x_n|_v)^{[L:K][K_v:\mathbb{Q}_p]} \\ &= \max(\|x_0\|_v, \dots, \|x_n\|_v)^{[L:K]}\end{aligned}$$

לכן,

$$\begin{aligned}H_L(\mathbf{p}) &= \prod_{v \in V(K)} \prod_{w|v} \max(\|x_0\|_w, \dots, \|x_n\|_w) \\ &= \prod_{v \in V(K)} \max(\|x_0\|_v, \dots, \|x_n\|_v)^{[L:K]} = H_K(\mathbf{p})^{[L:K]}\end{aligned}$$

כנטען. ∎

הערה כב.ד: השואה עם הגדרה כב.א. במקרה ש $K = \mathbb{Q}$ מתלכדת ההגדרה כב.ב עם ההגדרה כב.א. ואכן, לכל $\mathbf{p} \in \mathbb{P}^n(\mathbb{Q})$ נבחר קואורדינטות הומוגניות $x_0, \ldots, x_n$ כך ש $x_i \in \mathbb{Z}$ עבור $i = 0, \ldots, n$ ו $\gcd(x_0, \ldots, x_n) = 1$. אזי, לכל $v \in V(\mathbb{Q})$ לא ארכימדי $\|x_i\| \leq 1$ לכל i ו $\|x_i\| = 1$ עבור לפחות i אחד. לכן, $\max(\|x_0\|_v, \ldots, \|x_n\|_v) = 1$. מכאן ש,

$$.H_{\mathbb{Q}}(\mathbf{p}) = \max(|x_0|, \ldots, |x_n|) = H(\mathbf{p})$$

בפרט נובע מ (2) ש

$$\#\{\mathbf{p} \in \mathbb{P}^n(\mathbb{Q}) \mid H_{\mathbf{Q}}(\mathbf{p}) \leq c\} \leq (2c+1)^{n+1} \tag{4}$$

לכל $c > 0$. אחת ממטרותינו היא להכליל את אי השויון (4) ל H_K. ∎

הגדרה כב.ה: גבה מֻחלט. תהי $\mathbf{p} = (x_0 : \cdots : x_n)$ נקֻדה של $\mathbb{P}^n(\tilde{\mathbb{Q}})$. נבחר שדה מספרים K כך ש $\mathbf{p} \in \mathbb{P}^n(K)$ ונגדיר את **הגבה המֻחלט** של $\mathbb{P}$ על ידי הנֻסחה

$$. H(\mathbf{p}) = H_K(\mathbf{p})^{\frac{1}{[K:\mathbb{Q}]}} \tag{5}$$

באשר באגף ימין השרש החיובי של $H_K(\mathbf{p})$ הוא זה שנלקח (אם $[K:\mathbb{Q}]$ זוגי). מלמה כב.ג(ג) נובע שאגף ימין אינו תלוי ב K ולכן ההגדרה (5) טובה. ∎

נבדֹק עתה כיצד משתנה הגֹבה של נקֻדה תחת מורפיזם של מרחבים פרויקטיביים.

הגדרה כב.ו: **מורפיזם** ממעלה d בין מרחבים פרויקטיביים מעל שדה K הנה העתקה

$$\varphi\colon \mathbb{P}^n \to \mathbb{P}^m$$

כך שלכל שדה הרחבה L של K ולכל נקֻדה $\mathbf{p} = (x_0 : \cdots : x_n)$ מתקיֵם

$$\varphi(\mathbf{p}) = (f_0(\mathbf{p}) : \cdots : f_m(\mathbf{p})) \tag{6}$$

באשר $f_0, \ldots, f_n \in K[X_0, \ldots, X_n]$ הם פולינומים הומוגניים ממעלה d בלי אפס משֻתף ב $\mathbb{P}^n(\tilde{K})$ חוץ מ $(0, \ldots, 0)$. נעיר שלא כל האברים $f_i(\mathbf{p})$ שוים לאפס. יתר על כן, אגף ימין של (6) אינו תלוי בבחירות הקואורדינטות של $\mathbf{p}$. לכן, φ מֻגדר היטב. נסמן את אגף ימין של (6) גם ב $\mathbf{f}(\mathbf{p})$. ∎

משפטון כב.ו (משפט האפסים של הלברט): *יהיו K שדה, $\mathbf{X} = (X_1, \dots, X_n)$ nריה של משתנים ו I אידאל של $K[\mathbf{X}]$.*

(א) *אם I הנו אידאל נאות של $K[\mathbf{X}]$, אזי יש לכל הפולינומים ב I אפס משֻׁתף ב $\tilde{K}^n$.*

(ב) *יהי $g \in K[\mathbf{X}]$ אידאל המתאפס על $V(I)(\tilde{K})$ (= אסף כל האפסים המשֻׁתפים של הפולינומים ב I ב K^n). אזי קיָם e טבעי כך ש $g^e \in I$.*

הוכחת א: נבחר בעזרת הלמה של צורן אידאל מרבי M של $K[\mathbf{X}]$ המקיף את I. לכל j בין 1 ל n נסמן $x_j = X_j + M$. אזי $K[\mathbf{x}]$ הנו תחום שלמות וההעתקה $X_j \mapsto x_j$ משרה סדרה מדֻיקת קצרה $0 \to M \to K[\mathbf{X}] \to K[\mathbf{x}] \to 0$. יהי $t_1, \dots, t_r$ בסיס נעלות להרחבה $K(\mathbf{x})/K$. נבחר פולינום שונה מאפס $p \in K[\mathbf{t}]$ כך ש x_j שלם מעל $K[\mathbf{t}, p(\mathbf{t})^{-1}]$, $j = 1, \dots, n$. עתה נבחר $a_1, \dots, a_r \in \tilde{K}$ כך ש $g(\mathbf{a}) \neq 0$ ונרחיב את היִחוד $\mathbf{t} \to \mathbf{a}$ לאתר $\varphi\colon K(\mathbf{x}) \to \tilde{K} \cup \{\infty\}$. מבחירת $\mathbf{a}$ נובע שהצמצום של φ ל $K[\mathbf{x}]$ הנו הומומורפיזם לתוך $\tilde{K}$. בפרט, $\mathbf{x}' \in \tilde{K}^n$ הנו אפס משֻׁתף של כל הפולינומים ב M ולכן גם של כל הפולינומים ב I.

הוכחת ב: נוסיף ל $X_1, \dots, X_n$ את המשתנה Y. נתבונן באידאל I' של $K[\mathbf{X}, Y]$ הנוצר על ידי I ו $1 - g(\mathbf{X})Y$. אם $(\mathbf{x}', y')$ הנו אפס של I' ב $\tilde{K}^{n+1}$, אזי $\mathbf{x}'$ הנו אפס של I ולכן, לפי ההנחה, גם של g. מכאן ש $1 = 1 - g(\mathbf{x}')y'$, ולכן $(\mathbf{x}', y')$ אינו אפס של I'. סתירה זו מוכיחה שאין לאידאל I' שום אפס ב $\tilde{K}^{n+1}$. מחלק א נובע אפוא ש $I' = K[\mathbf{X}, Y]$. במִלים אחרות, קיָמים $h_0, h_1 \in K[\mathbf{X}, Y]$ ו $i \in I$, כך ש $h_0(\mathbf{X}, Y)(1 - g(\mathbf{X})Y) + h_1(\mathbf{X}, Y)i(\mathbf{X}) = 1$. נציב $Y = \frac{1}{g(\mathbf{X})}$ בשויון זה כדי לקבל $h_1\Big(\mathbf{X}, \frac{1}{g(\mathbf{X})}\Big)i(\mathbf{X}) = 1$. עתה נבחר מספר טבעי e כך ש $g(\mathbf{X})^e h_1\Big(\mathbf{X}, \frac{1}{g(\mathbf{X})}\Big) \in K[\mathbf{X}]$. מהשויון האחרון עולה ש $g(\mathbf{X})^e = \Big(g(\mathbf{X})^e h_1\big(\mathbf{X}, \frac{1}{g(\mathbf{X})}\big)\Big)i(\mathbf{X}) \in I$. ∎

למה כב.ח: *יהי K שדה מספרים, d מספר טבעי ו $f_0, \dots, f_m \in K[X_0, \dots, X_n]$ פולינומים הומוגניים ממעלה d. נניח שאין ל $f_0, \dots, f_m$ אפס משֻׁתף ב $\mathbb{Q}^{n+1}$ פרט ל $(0, \dots, 0)$. אזי קיים e טבעי, $e \geq d$, וקיָמים פולינומים הומוגניים $g_{ij} \in K[X_0, \dots, X_n]$ ממעלה $e - d$, $i = 0, \dots, n$ ו $j = 0, \dots, n$ כך ש $X_i^e = \sum_{j=0}^m g_{ij} f_j$, $i = 0, \dots, n$. יתר על כן, e ו $\mathbf{g}$ תלויים אך ורק במקדמי f_i.*

הוכחה: עבור כל i הפולינום X_i מתאפס על האפס המשֻׁתף היחיד $(0, \dots, 0)$ של $f_0, \dots, f_m$. משפטון כב.ז(ב) נותן אפוא מספר טבעי e (אשר נִתן להניח עליו שאינו תלוי ב i ושהוא גדול או שוה ל d) ופולינומים $g_{ij} \in K[\mathbf{X}]$, $j = 0, \dots, m$ כך ש

$$X_i^e = \sum_{j=0}^m g_{ij}(\mathbf{X}) f_j(\mathbf{X}) \;. \tag{7}$$

נרשֹם כל אחד מה g_{ij}־ים כסכום המרכיבים ההומוגניים שלו ונשוה את החלק ההומוגני של (7) ממעלה e כדי להניח ש g_{ij} הומוגני ממעלה $e-d$. עתה נראה את (7) כמערכת של משואות לינאריות שמשתניהם הם מקדמי g_{ij} ומקדמיהם מתקבלים ממקדמי f_j. למערכת זו יש פתרון הנִתן לחשוב בעזרת נֻסחת קרֶמר מתוך המקדמים של ה f_j־ים. ∎

משפטון כב.ט: *יהי* $\varphi\colon \mathbb{P}^n \to \mathbb{P}^m$ *מורפיזם ממעלה* d *מעל* $\tilde{\mathbb{Q}}$*. אזי קיָמים קבועים* c_1, c_2 *(התלויים ב* φ*) כך שלכל* $\mathbf{p} \in \mathbb{P}^n(\tilde{\mathbb{Q}})$ *מתקיֵם* $c_1 H(\mathbf{p})^d \le H(\varphi(\mathbf{p})) \le c_2 H(\mathbf{p})^d$.

הוכחה: נניח ש φ נתון כמו בהגדרה כב.ו. תהי $\mathbf{p} = (x_0{:}\ldots{:}x_n)$ נקֻדה ב $\mathbb{P}^n(\tilde{\mathbb{Q}})$. נבחר שדה מספרים K המכיל את כל הקואורינטות x_i ואת כל המקדמים של הפולינומים f_j. לכל $v \in V(K)$ נסמֵן

$$\|\mathbf{x}\|_v = \max(\|x_0\|_v, \ldots, \|x_n\||_v)$$
$$\|\mathbf{f}(\mathbf{x})\|_v = \max(\|f_0(\mathbf{x})\|_v, \ldots, \|f_m(\mathbf{x})\|_v)$$
$$\|\varphi\|_v = \max(\|a\|_v \mid a \text{ is a coefficient of some } f_i)$$

לפי (3), $H_K(\mathbf{p}) = \prod_{v\in V(K)} \|\mathbf{x}\|_v$ ו $H_K(\varphi(\mathbf{p})) = \prod_{v\in V(K)} \|\mathbf{f}(\mathbf{p})\|_v$. נעיר ש $H_K(\varphi(\mathbf{p}))$ אינו תלוי בבחירת הקואורדינטות ההומוגניות עבור $\mathbf{p}$. ואכן, אם $a \in K^\times$, אזי לפי נֻסחת המכפלה

$$\prod_{v\in V(K)} \|\mathbf{f}(a\mathbf{x})\|_v = \prod_{v\in V(K)} \|a\|_v^d \|\mathbf{f}(\mathbf{x})\|_v = \prod_{v\in V(K)} \|\mathbf{f}(\mathbf{p})\|_v \ .$$

בהתאם לכך נגדיר

$$H_K(\varphi) = \prod_{v\in V(K)} \|\varphi\|_v = H_K(a_0{:}a_1{:}\cdots)$$

באשר ה a_j־ים הם המקדמים של ה f_i־ים. הגדרות דומות נגדיר עבור הערך המֻחלט הלא מתֻקן $|\ |_v$.

יהי $v \in V(K)$. אם v מטרי נסמן $\varepsilon(v) = 1$ ואם v אולטרה מטרי נסמן $\varepsilon(v) = 0$. כמו כן נסמן $n_v = [K_v : \mathbb{Q}_v]$. אזי

$$|t_1 + \cdots + t_n| \le n^{\varepsilon(v)} \max(|t_1|_v, \ldots, |t_n|_v) \qquad (8)$$

לכל $t_1, \ldots, t_n \in K$.

שארית ההוכחה מתחלקת לשני חלקים.

חלק א: *חסם מלעיל.* נסמן ב $c_2 = c_{d,n}$ את מספר המונומים ב $X_0, \ldots, X_n$ ממעלה d (נִתן להראות שמספר זה הנו $\binom{n+d}{n}$). יהי $f_i = \sum a_{\mathbf{j}} X_0^{j_0} \cdots X_n^{j_n}$ באשר $a_{\mathbf{j}} \in K$ ו $\mathbf{j} = (j_0, \ldots, j_n)$ עובר על כל ה $(j+1)$־יות של מספרים שלמים אי שליליים המקיְמים $j_0 + \cdots + j_n = d$. תהי $\mathbf{p} = (x_0{:}\ldots{:}x_n)$ נקֻדה של $\mathbb{P}^n(K)$. אזי

$$|f_i(\mathbf{x})|_v \le \sum |a_j|_v |x_0|_v^{j_0} \cdots |x_n|_v^{j_n} \le c_2^{\varepsilon(v)} |\varphi|_v |\mathbf{x}|_v^d \ . \qquad (9)$$

לכן $|\varphi(\mathbf{x})|_v \le c_2^{\varepsilon(v)}|\varphi|_v|\mathbf{x}|_v^d$. נסמן ב $V_\infty(K)$ את אסף הערכים המֻחלטים המטריים של K, כלומר אלו המונחים מעל הערך המֻחלט $|\,|_\infty$ של $\mathbb{Q}$. לפי למה יח.ב(ג), $\sum_{v\in V(K)}\varepsilon(v)n_v = \sum_{v\in V_\infty(K)}\varepsilon(v)n_v = [K:\mathbb{Q}]$.
לכן

$$\begin{aligned}
H_K(\varphi(\mathbf{p})) &= \prod_{v\in V(K)}\|\varphi(\mathbf{x})\|_v = \prod_{v\in V(K)}|\varphi(\mathbf{x})|_v^{n_v} \\
&= c_2^{\sum_{v\in V(K)}\varepsilon(v)n_v}\prod_{v\in V(K)}|\varphi|_v^{n_v}\prod_{v\in V(K)}|\mathbf{x}|_v^{n_v d} \\
&= c_2^{[K:\mathbb{Q}]}H_K(\varphi)H_K(\mathbf{p})^d
\end{aligned}$$

אם נוציא את השרש ה $[K:\mathbb{Q}]$-י משני אגפי אי השויון נקבל $H(\varphi(\mathbf{p})) \le c_2 H(\varphi)H(\mathbf{p})^d$, כפי שהיה להוכיח.

חלק ב: *חסם מלרע.* הוכחת חלק א לא הסתמכה על כך שלפולינומים $f_0,\dots,f_m$ אין אפס משֻתף ב $\mathbb{Q}^{n+1}$ מחוץ ל $(0,\dots,0)$. אולם עתה בבֹאינו להוכיח את אי השויון השמאלי של המשפטון עלינו להשתמש בהנחה זו. בהתאם להנחה זו נותנת למה כב.ח מספר טבעי e שאינו פחות מ d ופולינומים הומוגניים $g_{ij}\in K[X_0,\dots,X_n]$ ממעלה $e-d$ כך ש $X_i^e = \sum_{j=0}^m g_{ij}f_j$, $i=0,\dots,n$. יתר על כן, e ו $H_K(\mathbf{g})$ תלויים אך ורק ב $\mathbf{f}$.
יהי $v\in V(K)$. כמו ב (9) נובע ש $|g_{ij}(\mathbf{x})|_v \le c_{e-d,n}^{\varepsilon(v)}|\mathbf{g}|_v|\mathbf{x}|_v^{e-d}$. לכן,

$$\begin{aligned}
|x_i|_v^e &= \Big|\sum_{j=0}^m g_{ij}(\mathbf{x})f_i(\mathbf{x})\Big| \\
&\le (m+1)^{\varepsilon(v)}\max\big(|g_{i0}(\mathbf{x})|_v|f_0(\mathbf{x})|_v,\dots,|g_{im}(\mathbf{x})|_v|f_m(\mathbf{x})|_v\big) \\
&\le (m+1)^{\varepsilon(v)}|\mathbf{g}(\mathbf{x})|_v|\mathbf{f}(\mathbf{x})|_v \\
&\le (m+1)^{\varepsilon(v)}c_{e-d,n}^{\varepsilon(v)}|\mathbf{g}|_v|\mathbf{x}|_v^{e-d}|\mathbf{f}(\mathbf{x})|_v
\end{aligned}$$

אם נִתן ל i לעבֹר מ 0 ועד n באגף שמאל של השויון האחרון, נקבל

$$|\mathbf{x}|_v^e \le (m+1)^{\varepsilon(v)}c_{e-d,n}^{\varepsilon(v)}|\mathbf{g}|_v|\mathbf{x}|_v^{e-d}|\mathbf{f}(\mathbf{x})|_v \,.$$

ולכן, $|\mathbf{x}|_v^d \le \big((m+1)c_{e-d,n}\big)^{\varepsilon(v)}|\mathbf{g}|_v|\mathbf{f}(|\mathbf{x})|_v$. מכאן נובע ש

$$\begin{aligned}
H_K(\mathbf{p})^d &= \prod_{v\in V(K)}\|\mathbf{x}\|_v^d \\
&\le \prod_{v\in V(K)}\big((m+1)c_{e-d,n}\big)^{\varepsilon(v)n_v}\prod_{v\in V(K)}|\mathbf{g}|_v^{n_v}\prod_{v\in V(K)}|\mathbf{f}(\mathbf{x})|_v^{n_v} \\
&= \big((m+1)c_{e-d,n}\big)^{[K:\mathbb{Q}]}H_K(\mathbf{g})H_K(\varphi(\mathbf{p}))
\end{aligned}$$

הקבוע החיובי c_1 המֻגדר על ידי $c_1^{-1} = (m+1)c_{e-d,n}H_K(\mathbf{g})^{\frac{1}{[K:\mathbb{Q}]}}$ מקיֵם $c_1 H(\mathbf{p})^d \le H(\varphi(\mathbf{p}))$, כנדרש.

∎

כל מטריצה $A \in \mathrm{GL}_{n+1}(\tilde{\mathbb{Q}})$ מגדירה אוטומורפיזם $A\colon \mathbb{P}^n \to \mathbb{P}^n$ ממעלה 1. התוצאה הבאה הנה אפוא מקרה פרטי של משפטון כב.ט.

תוצאה כב.י: *לכל מטריצה $A \in \mathrm{GL}_{n+1}(\tilde{\mathbb{Q}})$ קיָמים קבועים c_1, c_2 (התלויים באברי A) כך שלכל $\mathbf{p} \in \mathbb{P}^n(\tilde{\mathbb{Q}})$*

$$. \; c_1 H(\mathbf{p}) \le H(A\mathbf{p}) \le c_2 H(\mathbf{p})$$

עתה נחקֹר את הקשר בין הגבה של פולינום והגבה של שרשיו.

הגדרה כב.יא: לכל $x \in \tilde{\mathbb{Q}}$ נסמן $H(x) = H(1:x)$. אם x שיָך לשדה מספרים K נסמן $H_K(x) = H_K(1:x)$. ∎

משפטון כב.יא: *יהי*

$$f(T) = a_d T^d + a_{d-1}T^{d-1} + \cdots + a_0 = a_0(T-\alpha_1)\cdots(T-\alpha_d) \in \tilde{\mathbb{Q}}[T]$$

פולינום ממעלה d (דהיינו $a_0 \ne 0$). אזי

$$2^{-d}\prod_{j=1}^{d} H(\alpha_j) \le H(a_0 : \cdots : a_d) \le 2^{d-1}\prod_{j=1}^{d} H(\alpha_j) \tag{10}$$

הוכחה: ראשית נעיר שאי השויון (10) אינו משתנה אם מחליפים את $f(T)$ ב $\frac{1}{a_d}f(T)$. לכן מספיק להוכיח את (10) תחת ההנחה ש $a_d = 1$.

יהי $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$. נוכיח את אי השויון

$$. \; \frac{1}{2^d}\prod_{j=1}^{d}\max(1, |\alpha_j|_v) \le \max_{0\le i\le d}|a_i|_v \le \frac{1}{2^{d-1}}\prod_{j=1}^{d}\max(1,|\alpha_j|_v) \tag{13}$$

נעיר ש $\prod_{v\in V(K)} 2^{-dn_v} = \prod_{v\in V_\infty(K)} 2^{-dn_v} = 2^{-d[K:\mathbb{Q}]}$. לכן, אם נוכיח את (13), נוכל להעלותו בחזקת n_v להכפיל על כל $v \in V(K)$ ולקחת את השרש ה $[K:\mathbb{Q}]$ כדי לקבל את אי השויון (10).

נוכיח את (13) באנדוקציה על d. במקרה ש $d=1$, $f(T) = T - a_0 = T - \alpha_1$ כך ש $a_0 = \alpha_1$ ואי השויון (13) מקבל את הצורה $2^{-1}\max(1,|\alpha_1|_v) \le \max(1,|a_1|_v) \le \max(1,|\alpha_1|_v)$ שהיא נכונה.

נניח עתה שהוכחנו כבר את (13) לכל שדה מספרים K ולכל הפולינומים ב $K[T]$ ממעלה $d-1$. נבחר אנדקס k כך ש

$$|\alpha_k|_v \ge |\alpha_j|_v, \qquad j = 0, \ldots$$

ונתבונן בפולינום

$$\begin{aligned} g(T) &= (T-\alpha_1)\cdots(T-\alpha_{k-1})((T-\alpha_{k+1})\cdots(T-\alpha_d) \\ &= b_{d-1}T^{d-1} + b_{d-2}T^{d-2} + \cdots + b_0 \end{aligned}$$

שבו $b_{d-1} = 1$. פולינום זה מקיֵם $f(T) = (T-\alpha_k)g(T)$. השואת המקדמים של שני האגפים נותנת

$$a_i = b_{i-1} - \alpha_k b_i \tag{14}$$

לכל i אם קובעים $b_{-1} = b_d = 0$. שארית ההוכחה מתחלקת לשני חלקים.

חלק א: *חסם מלעיל.*

$$\begin{aligned} \max_{0\le i\le d} |a_i|_v &= \max_{0\le i\le d} |b_{i-1} - \alpha_k b_i|_v \\ &\le \max_{0\le i\le d} (|b_{i-1}|_v, \||\alpha_k|_v |b_i|_v) && \text{אי שויון המשֻׁלש} \\ &\le 2(v) \max_{0\le i\le d} |b_i|_v \cdot \max(|\alpha_k||_v, 1) \\ &\le 2(v)^{d-1} \prod_{i=0}^{d-1} \max(|\alpha_i|_v, 1) \cdot \max(|\alpha_k|_v, 1) && \text{הנחת האנדוקציה} \\ &= 2(v)^{d-1} \prod_{i=0}^{d} \max(|\alpha_i|_v, 1) \end{aligned}$$

חלק ב: *חסם מלרע.* נחלק את הוכחת החלק השמאלי של (13) לשני מקרים. נניח קודם ש $|\alpha_k|_v \le 2$. אזי

$$. \prod_{j=1}^{d} \max(|\alpha_j|_v, 1) \le \max(|\alpha_k|_v, 1)^d \le 2^d$$

הואיל ו $a_0 = 1$, $\max_{0\le i\le d} |a_i|_v \ge 1$. לכן

$$.2^{-d} \prod_{j=1}^{d} \max(|\alpha_j|_v, 1) \le 1 \le \max_{0\le i\le d} |a_i|_v$$

כנדרש.

עתה נניח ש $|\alpha_k|_v > 2$. אזי, $\frac{1}{2}|\alpha_k|_v > 1$ ולכן $\frac{1}{2}|\alpha_k|_v > |\alpha_k| - 1$. נחבר j כך ש

$|b_j|_v = \max_{0\le i\le d}|b_i|_v$. אזי,

$$\begin{aligned}
\max_{0\le i\le d}|a_i|_v &= \max_{0\le i\le d}|b_{i-1}-\alpha_k b_i|_v\\
&\ge |b_{j-1}-\alpha_k b_j|_v\\
&\ge |\alpha_k|_v|b_j|_v - |b_{j-1}|_v && \text{אי שויון המשֻלש}\\
&\ge (|\alpha_k|_v - 1)|b_j|_v && \text{כי } |b_j|_v \ge |b_{j-1}|_v\\
&\ge \frac{1}{2}|\alpha_k|_v \max_{0\le i\le d}|b_i|_v\\
&\ge \frac{1}{2}\max(\||\alpha_k|_v,1)\frac{1}{2^{d-1}}\prod_{i=0}^{d-1}\max(|\alpha_i|_v,1)\\
&= \frac{1}{2^d}\prod_{i=0}^{d}(|\alpha_i|_v,1)
\end{aligned}$$

בזה הסתיְמה הוכחת אי (13). ∎

השִמוש הראשון של פונקצית הגֹבה יהיה להראות שב $\mathbb{P}^n(\tilde{\mathbb{Q}})$ יש רק מספר סופי של נקֻדות עם גבה חסום. לשם כך עלינו להראות קודם שהגבה אינו משתנה תחת הפעלה של אוטומורפיזם של $\tilde{\mathbb{Q}}$.

למה כב.יב: *יהיו* $\mathbf{p}\in\mathbb{P}(\tilde{\mathbb{Q}})$ *ו* $\sigma\in\mathrm{Gal}(K)$*. אזי* $H(\mathbf{p}^\sigma)=H(\mathbf{p})$.

הוכחה: יהי K שדה מספרים המכיל קואורדינטות הומוגניות $x_0,\dots,x_n$ עבור bfp. האוטומורפיזם σ משרה איזומורפיזם $\sigma\colon K\to K^\sigma$ והעתקה חד חד ערכית $V(K)\to V(K^\sigma)$ המעתיקה כל $v\in V(K)$ לאבר $v^\sigma\in V(K^\sigma)$ המֻגדר על ידי $|x^\sigma|_{v^\sigma}=|x|_v$ לכל $x\in K$. כמו כן משרה σ איזומורפיזם $\sigma\in\hat{K}_v\to\hat{K}_{v^\sigma}$ ומתקיֵם $n_{v^\sigma}=n_v$. לכן,

$$\|x^\sigma\|_{v^\sigma}=|x^\sigma|_{v^\sigma}^{n_{v^\sigma}}=|x|_v^{n_v}=\|x\|_v\,.$$

מכאן נובע ש

$$\begin{aligned}
H_{K^\sigma}(\mathbf{p}^\sigma) &= \prod_{w\in V(K^\sigma)}\max_{0\le i\le n}\|x_i^\sigma\|_w\\
&= \prod_{v\in V(K)}\max_{0\le i\le n}\|x_i^\sigma\|_{v^\sigma}\\
&= \prod_{v\in V(K)}\max_{0\le i\le n}\|x_i\|_v = H_K(\mathbf{p})
\end{aligned}$$

אם נוציא את השרש ה $[K:\mathbb{Q}]$-י משני האגפים ונשתמש בשויון $[K:\mathbb{Q}]=[K^\sigma:\mathbb{Q}]$, נקבל ש $H(\mathbf{p}^\sigma)=H(\mathbf{p})$, כפי שהיה להוכיח. ∎

משפטון כב.יג (Northcott [Nor1,2]): *יהיו c ו d קבועים. אזי הקבוצה*

$$\{\mathbf{p} \in \mathbb{P}^n(\tilde{\mathbb{Q}}) \mid \; H(\mathbf{p}) \leq c \text{ and } [\mathbb{Q}(\mathbf{p}) : \mathbf{Q}] \leq d\}$$

סופית. בפרט, לכל שדה מספרים K הקבוצה $\{\mathbf{p} \in \mathbb{P}^n(K) \mid \; H(\mathbf{p}) \leq c\}$ סופית.

הוכחה: תהי $\mathbf{p} = (x_0 : \cdots : x_n)$ נקֻדה ב $\mathbb{P}^n(\mathbb{Q})$. בלי הגבלת הכלליות נניח ש x_j עבור איזה שהוא j. אזי $K = \mathbb{Q}(\mathbf{p}) = \mathbb{Q}(x_0, \ldots, x_n)$. לכל $v \in V(K)$ נבחר $i(v)$ בין 0 ל 1 כך ש $\|x_i\|_v \geq \|x_{i(v)}\|_v$ לכל i. בפרט, $1 \geq \|x_{i(v)}\|$. לכן,

$$\begin{aligned} H_K(\mathbf{p}) &= \prod_{v \in V(K)} \max(\|x_0\|_v, \ldots, \|x_n\|_v) \\ &= \prod_{v \in K} \|x_{i(v)}\|_v \\ &\geq \max_{0 \leq i \leq n} \prod_{v \in V(K)} \max(\|x_i\|_v, 1) \\ &= \max_{0 \leq i \leq n} H_K(x_i) \end{aligned}$$

מכאן נובע ש $\max_{0 \leq i \leq n} H(x_i) \leq H(\mathbf{p})$. לכן, אם $H(\mathbf{p}) \leq c$, גם $\max_{0 \leq i \leq n} H_K(x_i) \leq c$ כמו כן, אם $[K : \mathbf{Q}] \leq d$, אזי $\max_{0 \leq i \leq n}[\mathbf{Q}(x_i) : \mathbf{Q}] \leq d$. מספיק אפוא להוכיח שהקבוצה

$$A_{c,d} = \{x \in \tilde{\mathbb{Q}} \mid \; H(x) \leq c \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] \leq d\}$$

סופית. במִלים אחרות, העמדנו את המשפטון על המקרה $n = 1$.

יהי אפוא x אבר של $A_{c,d}$. יהיו $x_1, \ldots, x_e$ הצמודים של x מעל $\mathbb{Q}$ ויהי

$$f(T) = (T - x_1) \cdots (T - x_e) = T^e + a_{e-1}T^{e-1} + \cdots + a_0$$

הפולינום האי פריק של x מעל $\mathbb{Q}$. לפי משפטון כב.יא ולפי למה כב.יב,

$$. \; H(a_0, \ldots, a_{e-1}, 1) \leq 2^{e-1} \prod_{j=1}^{e} H(x_i) = 2^{e-1} H(x)^e \leq (2c)^e$$

לפי דֻגמה כב.א, מספר הנקֻדות $\mathbf{a} \in \mathbb{Q}^n$ שגבהן אינו עולה של $(2c)^e$ חסום. לכן, יש רק מספר סופי של פולינומים מתֻקנים אי פריקים $f \in \mathbb{Q}[X]$ ממעלה שאינה עולה על d ששרשיהם בעלי גבה חסום על ידי c. מכאן ש $A_{c,d}$ קבוצה סופית. ∎

כג. גֹבה על עֲקֻמים אלִפטיים

נשתמש כאן בגבה שהגדרנו בסעיף כב כדי להגדיר גבה על עקמים אלפטיים שיקַיֵם את התנאים המפרטים בהגדרה א.א. בכך נשלים את הוכחת משפט מורדל־וייל לעקמים אלפטיים מעל שדה מספרים.

הגדרה כג.א: ה O הגדול. תהיינה f ו g פונקציות ממשיות על קבוצה A. נרשֹם $f = g + O(1)$ אם קיָם קבועים c כך ש $|f(x) - g(x)| \le c$ לכל $x \in A$. נרשֹם $f \le g + O(1)$ אם קיָם קבוע c כך ש $f \le g + c$ לכל $x \in A$. לבסוף נרשם $f \ge g + O(1)$ אם קיָם קבוע c כך ש $f \ge g + c$ לכל $x \in A$. ∎

יהי עתה E עקם אלפטי מעל שדה מספרים K. נִתן לראות כל f בשדה הפונקציות $\tilde{K}(E)$ של E מעל $\tilde{K}$ כפונקציה $f\colon E(\tilde{K}) \to \mathbb{P}^1(\tilde{K})$ המֻגדרת באפן הבא: כל נְקֻדה $\mathbf{p}$ של $E(\tilde{K})$ מתאימה באפן חד חד ערכי לחוג הערכה בדידה $O_{\mathbf{p}}$ של $E(\tilde{K})$ ששדה השאריות שלה הנו $\tilde{K}$ (ראה סעיף יג.א). נסמן ב $\varphi_{\mathbf{p}}$ את האתר המתאים לשדה שאריות זה (אתר זה נקבע באפן חד ערכי אחרי בחירת נקֻדה יוצרת ל E). נגדיר

$$f(\mathbf{p}) = \begin{cases} (1 : \varphi_{\mathbf{p}}(f)) & \text{if } \varphi_{\mathbf{p}}(f) \neq \infty \\ (0 : 1) & \text{if } \varphi_{\mathbf{p}}(f) = \infty \end{cases}$$

היה זה מתקבל על הדעת להגדיר פונקצית גֹבה על $E(\tilde{K})$ בעזרת ההגדרה $H_f(\mathbf{p})) = H(f(\mathbf{p}))$. אולם פונקצית הגבה H קרובה להיות כפלית (כפי שראינו במשפטון כב.ט) בעוד שהגדרה א.א דורשת שהפונקציה תתנהג באפן חבורי. ההגדרות הבאות יתקנו מצב עניָנים זה:

הגדרה כג.ב: נגדיר פונקציה $h\colon \mathbb{P}^n(\tilde{\mathbb{Q}}) \to \mathbb{R}$ על ידי $h(\mathbf{p}) = \log H(\mathbf{p})$ ונקרא לה **פונקצית הגבה** (**הלוגרִתמית המֻפשטת**). היא מקיֶמת $h(\mathbf{p}) \ge 0$ לכל $\mathbf{p} \in E(\tilde{\mathbb{Q}})$. ∎

הגדרה כג.ג: יהי E עקֹם אלפטי מעל שדה מספרים K ותהי $f \in \tilde{K}(E)$. נגדיר פונקציה $h_f\colon E(\tilde{K}) \to \mathbb{R}$ על ידי $h_f(\mathbf{p}) = h(f(\mathbf{p}))$ ונקרא לה **פונקציה הגבה** על E (ביחס ל f). ∎

במונחים אלו מקבלים המשפטונים כב.ט ו כב.יא את הצורה הבאה:

משפטון כג.ד:

(א) *יהי* $\varphi\colon \mathbb{P}^n \to \mathbb{P}^m$ *מורפיזם ממעלה* d *מעל* $\tilde{\mathbb{Q}}$*. אזי* $h(\varphi(\mathbf{p})) = dh(\mathbf{p}) + O(1)$.

(ב) *יהי* $f(T) = a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0 = a_0(T - \alpha_1) \cdots (T - \alpha_d)$ *פולינום עם מקדמים ב* $\tilde{\mathbb{Q}}$ *ממעלה* d*. אזי* $h(a_0 : \cdots : a_d) = \sum_{j=1}^{d} h(\alpha_j) + O(1)$.

משפטון כב.ט משתנה באפן הבא:

משפטון כג.ה: *יהיו* E *עקם אלפטי מעל שדה מספרים* K *ו* $f \in K(E)$*. אזי לכל קבוע* c *הקבוצה*

$$\{\mathbf{p} \in E(K) \mid h_f(\mathbf{p}) \le c\}$$

סופית.

הוכחה: הואיל ו $f \in K(E)$, משרה f העתקה $f\colon E(K) \to \mathbb{P}^1(K)$. מספר האברים בכל סיב של f חסום על ידי $[K(E) : K(f)]$. יתר על כן, f מעתיקה את הקבוצה $A = \{\mathbf{p} \in E(K) \mid h_f(\mathbf{p}) \le c\}$ לקבוצה $B = \{\mathbf{q} \in \mathbb{P}^2(K) \mid H(\mathbf{q}) \le e^c\}$. לפי משפטון כב.יג, B סופית. לכן, גם A סופית. ∎

נאמר שפונקציה רציונלית f על עקם אלפטי E מעל שדה K הנה **זוגית** אם $f(-\mathbf{p}) = f(\mathbf{p})$ לכל $\mathbf{p} \in E(\tilde{K})$. אם העקֹם מֻגדר על ידי משואת ויירשטרס ואם (x, y) היא נקֻדה יוצרת של E מעל K, אזי $\mathrm{Gal}(K(x,y)/K(x))$ היא חבורה מעגלית מסדר 2 עם יוצר σ המֻגדר על ידי $\sigma(y) = -y$. לכן, לכל פונקציה רציונלית f ולכל $\mathbf{p} \in E(\tilde{K})$ מתקיֵם $f(-\mathbf{p}) = (\sigma f)(\mathbf{p})$. בפרט, f זוגית, אם ורק אם $\sigma f = f$, כלומר אם $f \in K(x)$.

משפט כג.ח נותן קשר יסודי בין פונקציות גבה לבין כלל החבור על עקֻמים אלפטיים. נתחיל בקשר בין פונקצית הגבה לבין כלל השכפול.

למה כג.ו: *יהי E עקֹם אלפטי מעל שדה מספרים K. אזי* $h_x(2\mathbf{p}) = 4h_x(\mathbf{p}) + O(1)$.

הוכחה: נגדיר העתקה $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ על ידי

$$\varphi(z_0 : z_1) = (z_1^4 - 2Az_0^2z_1^2 + 8Bz_0^3z_1 + z_0^4A^2 : 4z_0z_1^3 + 4Az_0^3z_1 + rz_0^4B) \qquad (1)$$

שני הפולינומים המופיעים בסגרים באגף ימין של (1) הנם הומוגניים ממעלה 4. האפס המשֻתף לשניהם הנו $(0,0)$. ואכן, יהי (z_0, z_1) אפס משֻתף לשני הפולינומים. אם $z_0 = 0$, אזי $z_1 = 0$. אם $z_0 \ne 0$ נרשם $x_1 = \frac{z_1}{z_0}$ ונקבל ש $x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2 = 0$ ו $4x_1^3 + 4Ax_1 + 4B = 0$, בסתירה למסקנה ו.ב.

תהי עתה $\mathbf{p} = (x_1, y_1)$ נקֻדה ב $E(K)$. אזי, $2\mathbf{p} = (x_2, y_2)$, באשר $x_2 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4x_1^3 + 4Ax_1 + 4B}$ (נֻסחה $(7d5)$ של סעיף ז). לפי משפטון כג.ד(א),

$$h_x(2\mathbf{p}) = h(1{:}x_2) = 4h(1{:}x_1) + O(1) = 4h(\mathbf{p}) + O(1),$$

כפי שהיה להוכיח. ∎

בלמה הבאה נפתח נֻסחאות הנובעות מנֻסחאות החבור.

למה כג.ז: *יהי E עקֹם אלפטי מעל שדה K בעל אפיון שונה מ 2 ומ 3 הנתן על ידי משואת ויירשטרס $Y^2 = X^3 + AX + B$. יהיו $\mathbf{p} = (x_1, y_1)$ ו $\mathbf{q} = (x_1, y_2)$ נקֻדות שונות מאפס של $E(\tilde{K})$ המקיֵמות $\mathbf{p} \ne -\mathbf{q}$. יהיו $\mathbf{p} + \mathbf{q} = (x_3, y_3)$ ו $\mathbf{p} - \mathbf{q} = (x_4, y_4)$. אזי,*

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}$$

$$x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x + 1 + x_2)^2 - 4x_1x_2}$$

הוכחה: לפי $(7a)$ של סעיף ז, $-\mathbf{q} = (x_2, -y_2)$. עתה נפעיל את נֻסחת החבור $(7c2)$ של סעיף ז על $\mathbf{p}+\mathbf{q}$ ועל $\mathbf{p}-\mathbf{q}$:

$$\begin{aligned}
x_3 + x_4 &= \frac{A(x_1{+}x_2) + 2B + x_1x_2^2 + x_2x_1^2 - 2y_1y_2}{(x_1-x_2)^2} + \frac{A(x_1{+}x_2) + 2B + x_1x_2^2 + 2y_1y_2}{(x_1-x_2)^2} \\
&= \frac{2A(x_1+x_2) + 4B + 2x_1x_2^2 + 2x_2x_1^2}{(x_1-x_2)^2} \\
&= \frac{2(x_1+x_2)(A + x_1x_2) + 4B}{(x_1+x_2)^2 - 4x_1x_2}
\end{aligned}$$

כדי להוכיח את הנֻסחה עבור x_3x_4 נפתח תחִלה

$$\begin{aligned}
x_1^2x_2 + x_1x_2^2 - x_1^3 - x_2^3 &= x_2(x_1^2 - x_2^2) - x_1(x_1^2 - x_2^2) \\
&= (x_2 - x_1)(x_1^2 - x_2^2) = -(x_2-x_1)^2(x_1+x_2)
\end{aligned}$$

ו

$$\begin{aligned}
2x_1x_2(x_1+x_2)^2 - 4x_1^3x_2 - 4x_1x_2^3 &= 2x_1x_2(x_1^2 + 2x_1x_2 + x_2^2 - 2x_1^2 - xx_2^2) \\
&= -2x_1x_2(x_1^2 - 2x_1x_2 + x_2^2) \\
&= -2x_1x_2(x_1-x_2)^2
\end{aligned}$$

כמו כן נשתמש בקשר $y_i^2 = x_i^3 + Ax_i + B$ עבור $i = 3, 4$ כדי לחשב:

$$\begin{aligned}
x_3x_4(x_1-x_2)^4 &= \big(A(x_1+x_2) + 2B + x_1x_2(x_1+x_2) - 2y_1y_2\big) \\
&\quad \cdot \big(A(x_1+x_2) + 2B + x_1x_2(x_1+x_2) + 2y_1y_2\big) \\
&= \big(A(x_1+x_2) + 2B + x_1x_2(x_1+x_2)\big)^2 - 4y_1^2y_2^2 \\
&= A^2(x_1+x_2)^2 + 4B^2 + x_1^2x_2^2(x_1+x_2)^2 \\
&\quad + 4AB(x_1+x_2) + 2Ax_1x_2(x_1+x_2)^2 + 4Bx_1x_2(x_1+x_2) \\
&\quad - 4(x_1^3 + Ax_1 + B)(x_2^3 + Ax_2 + B) \\
&= A^2(x_1^2 + 2x_1x_2 + x_2^2) + 4B^2 + x_1^2x_2^2(x_1+x_2)^2 \\
&\quad + 4AB(x_1+x_2) + 2Ax_1x_2(x_1+x_2)^2 + 4Bx_1x_2(x_1+x_2) \\
&\quad - 4x_1^3x_2^3 - 4Ax_1^3x_2 - 4B(x_1^3 + x_2^3) - 4Ax_1x_2^3 \\
&\quad - 4A^2x_1x_2 - 4AB(x_1+x_2) - 4B^2 \\
&= A^2(x_1-x_2)^2 - 2Ax_1x_2(x_1-x_2)^2 \\
&\quad - 4B(x_1+x_2)(x_1-x_2)^2 + x_1^2x_2^2(x_1-x_2)^2
\end{aligned}$$

אם נחלק את שני האגפים ב $(x_1-x_2)^2$ נקבל

$$\begin{aligned} x_2x_4(x_1-x_2)^2 &= A^2-2Ax_1x_2-4B(x_1+x_2)+x_1^2x_2^2 \\ &= (x_1x_2-A)^2-4B(x_1+x_2) \end{aligned}$$

כפי שהיה להוכיח. ∎

למה כג.ח: *יהי E עקֹם אלפטי מעל שדה מספרים K. אזי לכל $\mathbf{p},\mathbf{q}\in E(\tilde{K})$,*

$$. \, h_x(\mathbf{p}+\mathbf{q})+h_f(\mathbf{p}-\mathbf{q})=2h_x(\mathbf{p})+2h_x(\mathbf{q})+O(1) \qquad (2)$$

הקבוע של ה $O(1)$ תלוי ב E אולם אינו תלוי בנקֻדות $\mathbf{p}$ ו $\mathbf{q}$.

הוכחה: נבחר ל E משואת ויירשטרס מעל K כמו בלמה כו.ה ונתחיל את הוכחת המשפט עבור הפונקציה x.

יהי תחילה $\mathbf{q}=0$. אזי $h_x(\mathbf{q})=\log H(0:1)=\log 1=0$ ולכן

$$. \, h_x(\mathbf{p}+\mathbf{q})+h_x(\mathbf{p}-\mathbf{q})=2h_x(\mathbf{p})+2h_x(\mathbf{q})$$

אותה הנֻסחה נכונה במקרה ש $\mathbf{p}=0$. המקרה שבו $\mathbf{p}=\pm\mathbf{q}$ מכֻסה על ידי למה כג.ו.

נניח עתה ש $\mathbf{p},\mathbf{q}\neq 0$ וגם $\mathbf{p}\neq\pm\mathbf{q}$. יהיו (x_1,y_1) קואורדינטות אפיניות עבור $\mathbf{p}$ ו (x_2,y_2) קואורדינטות אפיניות עבור $\mathbf{q}$. אזי

$$\begin{aligned} x(\mathbf{p})&=(1:x_1) \qquad & x(\mathbf{q})&=(1:x_2) \\ x(\mathbf{p}+\mathbf{q})&=(1:x_3) \qquad & x(\mathbf{p}+\mathbf{q})&=(1:x_4) \end{aligned}$$

. יִתרת ההוכחה מתחלקת לכמה חלקים.

חלק א: *תרשים חלופי.* נגדיר העתקה $\varphi\colon\mathbb{P}^2\to\mathbb{P}^2$ על ידי

$$. \, \varphi(t:u:v)=(u^2-4tv:2u(At+v)+4Bt^2:(v-At)^2-4Btu) \qquad (3)$$

לפי למה כג.ה

$$\begin{aligned} \varphi(1:x_1+x_2:x_1x_2) &= \big((x_1+x_2)^2-4x_1x_2:2(x_1+x_2)(A+x_1x_2)+4B \\ &\qquad :(x_1x_2-A)^2-4B(x_1+x_2)\big) \qquad (4) \\ &= (1:x_2+x_4:x_3x_4) \end{aligned}$$

כמו כן נגדיר העתקות $\Phi\colon E\times E\to E\times E$, $\alpha\colon E\times E\to\mathbb{P}^1\times\mathbb{P}^1$ ו $\beta\colon\mathbb{P}^1\times\mathbb{P}^1\to\mathbb{P}^2$ על ידי

$$\begin{aligned}\Phi(\mathbf{p},\mathbf{q})&=(\mathbf{p}+\mathbf{q},\mathbf{p}-\mathbf{q})\\ \alpha(\mathbf{p},\mathbf{q})&=(x(\mathbf{p}),x(\mathbf{q}))\\ \beta\big((a_1{:}b_1),(\mathbf{a}_2{:}b_2)\big)&=(a_1a_2:a_1b_2+a_2b_1:b_1b_2)\end{aligned}$$

מ (4) עולה שהתרשים הבא חִלופי:

$$\begin{tikzcd} E\times E \arrow[r, "\Phi"] \arrow[d, "\alpha"'] & E\times E \arrow[d, "\alpha"] \\ \mathbb{P}^1\times\mathbb{P}^1 \arrow[d, "\beta"'] & \mathbb{P}^1\times\mathbb{P}^1 \arrow[d, "\beta"] \\ \mathbb{P}^2 \arrow[r, "\varphi"] & \mathbb{P}^2 \end{tikzcd} \tag{5}$$

חלק ב: *ההעתקה φ הנה מורפיזם.* ואכן, לפי (3), שלש הקואורדינטות של $\varphi(t{:}u{:}v)$ הנם פונקציות הומוגניות ממעלה 2 של u,t,v. מספיק אפוא להוכיח שאין לפונקציות אלו אפס משֻתף ב $\tilde{K}^3$ פרט ל $(0,0,0)$. ואכן, נניח ש

$$u^2-4tv=0\quad 2u(At+v)+4Bt^2=0\quad (v-At)^2-4Btu=0 \tag{6}$$

אם $t=0$, אזי $u=v=0$. נניח אפוא ש $t\neq 0$ ונציב $x=\frac{u}{2t}$. אזי נובע מהשויון השמאלי של (6) ש $x^2=\frac{v}{t}$. נחלק את השויון האמצעי של (6) ב $4t^2$ ואת השויון הימְני ב t^2 כדי לקבל,

$$\begin{aligned}&x^3+Ax+B=4x(A+x^2)+B=0\\ &x^4-4Ax^2-8Bx+A^2=(x^2-A)^2-8Bx=0\end{aligned} \tag{7}$$

בסתירה לכך שהפולינומים באגף ימין של (7) זרים זה לזה (מסקנה ו.ג). כדי להשיג סתירה זו השתמשנו בכך שהדסקרימיננטה $4A^3+27B^2$ של E שונה מאפס.

חלק ג: *נסחת קֵרוב.* נסמן $\gamma=\alpha\circ\beta$. מהתרשים החלופי (5) נסיק ש

$$\begin{aligned}h(\gamma(\mathbf{p}+\mathbf{q},\mathbf{p}-\mathbf{q}))&=h(\sigma(\Phi(\mathbf{p},\mathbf{q})))\\ &=h(\varphi(\gamma(\mathbf{p},\mathbf{q})))\\ &=2h(\gamma(\mathbf{p},\mathbf{q}))+O(1)\\ &=2h_x(\mathbf{p})+2h_x(\mathbf{q})+O(1)\end{aligned} \tag{8}$$

עבור $i = 1, 2$ יהי $\mathbf{r}_i = (a_i, b_i)$ נקֻדה של $E(\tilde{K})$. אזי $h_x(\mathbf{r}_i)) = h(x(\mathbf{r}_i)) = h(a_i)$. נפעיל את משפטון כג.ד(ב) על הפולינום $(T + a_1)(T + a_2) = T^2 + (a_1 + a_2)T + a_1 a_2$ כדי לקבל

$$\begin{aligned} h(\gamma(\mathbf{r}_1, \mathbf{r}_2)) &= h(1 : a_1 + a_2 : a_1 a_2) \\ &= h(1 : a_1) + h(1 : a_2) + O(1) \\ &= h_x(\mathbf{r}_1) + h_x(\mathbf{r}_2) + O(1) \end{aligned} \tag{9}$$

השויון האחרון נובע ממשפטון כג.ד הואיל ו γ הנו מורפיזם ממעלה 2. הפעלה של (9) על שני האגפים של (8) נותנת:

$$h_x(\mathbf{p} + \mathbf{q}) + h_x(\mathbf{p} - \mathbf{q}) = 2h_x(\mathbf{p}) + 2h_x(\mathbf{q}) + O(1)$$

כפי שהיה להוכיח. ∎

למה כג.ט: *יהי E עקֹם אלפטי מעל שדה מספרים K ויהיו $f, g \in K(E)$ פונקציות זוגיות. אזי*

$$\deg(f) h_f = \deg(g) h_g + O(1) \ .$$

הוכחה: הואיל ו f פונקציה זוגית, היא שַיֶכת ל $K(x)$. לכן קיָם מורפיזם $\rho\colon \mathbb{P}^1 \to \mathbb{P}^1$ כך ש $f = \rho \circ x$. לפי משפטון כג.ד(א),

$$\begin{aligned} h_f(\mathbf{p}) &= h(f(\mathbf{p})) = h(\rho(x(\mathbf{p}))) \\ &= \deg(\rho) h(x(\mathbf{p})) + O(1) \\ &= \deg(\rho) h_x(\mathbf{p}) + O(1) \end{aligned} \tag{10}$$

הואיל ו $\deg(x) = 2$, נקבל ש $\deg(f) = 2\deg(\rho)$. לכן, $2h_f(\mathbf{p}) = \deg(f) h_x(\mathbf{p}) + O(1)$. באפן דומה, $2h_g(\mathbf{p}) = \deg(g) h_x(\mathbf{p}) + O(1)$. אם נכפיל את המשואה הלפני אחרונה ב $\deg(g)$, את האחרונה ב $\deg(f)$ ונחסר את השויון השני מהראשון, נקבל $2\deg(g) h_f(\mathbf{p}) - 2\deg(f) h_g(\mathbf{p}) = O(1)$. חלֻקה ב 2 והעברת אגפים נותנת את הנסחה (10). ∎

תוצאה כג.י: *יהי E עקֹם אלפטי מעל שדה מספרים K ותהי $f \in K(E)$ פונקציה זוגית.*

(א) *תהי $\mathbf{q} \in E(\tilde{K})$. אזי $h_f(\mathbf{p} + \mathbf{q}) \le 2h_f(\mathbf{p}) + O(1)$, באשר ה $O(1)$ תלוי ב E, f ו $\mathbf{q}$ אולם לא ב $\mathbf{p}$.*

(ב) *יהי $m \in \mathbb{Z}$. אזי, $h_f(m\mathbf{p}) = m^2 h_f(\mathbf{p}) + O(1)$, באשר ה $O(1)$ תלוי ב E, f וב m (אולם לא ב $\mathbf{p}$).*

הוכחת א: עבור כל $\mathbf{p} \in E(\tilde{K})$ מתקיֵם $h_f(\mathbf{p} - \mathbf{q}) \ge 0$. כמו כן, $h_f(\mathbf{q})$ הנו קבוע שאינו תלוי ב $\mathbf{q}$. לכן, לפי למה כג.ח, $h_f(\mathbf{p} + \mathbf{q}) = 2h_f(\mathbf{p}) + 2h_f(\mathbf{q}) - h_f(\mathbf{p} - \mathbf{q}) + O(1) \le 2h_f(\mathbf{p}) + O(1)$, כפי שהיה להוכיח.

הוכחת ב: הואיל ו f פונקציה זוגית, מספיק להוכיח את (ב) רק במקרה ש $m \geq 0$. המקרים $m = 0, 1$ שגרתיים. נניח עתה באנדוקציה ש $m \geq 1$ ושנֻסחת הקרוב נכונה עבור $m - 1$ ו m. אזי, לפי למה ככ.ח,

$$\begin{aligned} h_f\big((m+1)\mathbf{p}\big) &= h_f(m\mathbf{p} + \mathbf{p}) \\ &= -h_f\big((m-1)\mathbf{p}\big) + 2h_f(m\mathbf{p}) + 2h_f(\mathbf{p}) + O(1) \\ &= -(m-1)^2 h_f(\mathbf{p}) + 2m h_f(\mathbf{p}) + 2h_f(\mathbf{p}) + O(1) \\ &= (m+1)^2 h_f(\mathbf{p}) + O(1) \end{aligned}$$

והאנדוקציה הֻשלמה. ∎

יש בידינו עתה את כל הכלים כדי להוכיח את משפט מורדל־וייל לעקֻמים אלפטיים מעל שדות מספרים.

משפט כג.יא (משפט מורדל־וייל): *יהי E עקֹם אלפטי מעל שדה מספרים K. אזי $E(K)$ הנה חבורה אבלית נוצרת סופית.*

הוכחה: לפי משפט כא.ה, החבורה $E(K)/2E(K)$ סופית. כדי להוכיח ש $E(K)$ נוצרת סופית עלינו להוכיח שפונקציה הגבה h_x על $E(K)$ מקיֶמת את התנאי (2) של הגדרה א.א.

ואכן, תוצאה כג.י(א), נותנת לכל $\mathbf{p} \in E(K)$ קבוע c_1 כך ש $h_x(\mathbf{p} + \mathbf{q}) \leq 2h(\mathbf{p}) + c_1$ לכל $\mathbf{p} \in E(K)$. בזה מתקיֵם תנאי $(2a)$ של הגדרה א.א.

תוצאה כג.י(ב) נותנת קבוע c_2 כך ש $h_x(m\mathbf{p}) \geq 4h(\mathbf{p}) - c_2$. בזה מתקיֵם תנאי $(2b)$ של הגדרה א.א.

לבסוף, לכל קבוע c_3 הקבוצה $\{\mathbf{p} \in E(K) \mid h_x(\mathbf{p}) \leq c_3\}$ סופית, כפי שתנאי $(2c)$ דורש.

ממשפטון א.ב עולה ש $E(K)$ נוצרת סופית. ∎

References

[Bou] N. Bourbaki, *Commutative Algebra, Chapters 1–7,* Springer, Berlin, 1989.

[Cas] J.W.S. Cassels, *Lectures on Elliptic Curves,* London Mathematical Society, Student Texts **24**, Cambridge University Press, Cambridge, 1991.

[CaF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[Hus] D. Husemölller, *Elliptic Curves,* Graduate Texts in Mathematics **111**, Springer, New York, 1987.

[La1] S. Lang, *Introduction to algebraic geometry,* Interscience Publishers, New York, 1958.

[La2] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Reading, 1970.

[La3] S. Lang, *Fundamentals of Diophantine Geometry,* Springer-Verlag, New York, 1983.

[Nor1] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties* Proceedings of the Cambridge Philosophical Society **45** (1949), 502–509.

[Nor2] D. G. Northcott, *A further inequality in the theory of arithmetic on algebraic varieties,* Proceedings of the Cambridge Philosophical Society **45** (1949), 510–518.

[Ser] J.-P. Serre, *Corps locaux,* Actualités scientifiques et industrielles **1296**, Hermann, Paris 1968.

[Sil] J.H. Silverman,

[Ser] J.-P. Serre, *Corps locaux,* Actualités scientifiques et industrielles **1296**, Hermann, Paris 1968.

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves,* Graduate texts in Mathematics **106**, Springer, New York, 1986.