

**חוג:** תהא  $R$  קבוצה ותהיינה  $+, *$  פעולות בינאריות אזי  $(R, +, *)$  המקיים

•  $(R, +)$  חבורה אבלית.

• אסוציאטיביות כפל: לכל  $a, b, c \in R$  מתקיים  $(a * b) * c = a * (b * c)$ .

• חוג הפילוג משמאל: לכל  $a, b, c \in R$  מתקיים  $a * (b + c) = (a * b) + (a * c)$ .

• חוק הפילוג מימין: לכל  $a, b, c \in R$  מתקיים  $(b + c) * a = (b * a) + (c * a)$ .

**סימון:** יהי  $(R, +, *)$  חוג ויהי  $e$  איבר היחידה של  $(R, +)$  אזי  $0_R = e$ .

**חוג אבל/קומוטטיבי/חילופי:** חוג  $(R, +, *)$  המקיים  $a * b = b * a$  לכל  $a, b \in R$ .

**חוג בעל יחידה:** חוג  $(R, +, *)$  עבורו  $(R, *)$  בעל איבר יחידה  $m$  וכן  $m \neq 0_R$ .

**סימון:** יהי  $(R, +, *)$  חוג ויהי  $m$  איבר היחידה של  $(R, *)$  אזי  $1_R = m$ .

**טענה:** יהי  $n \in \mathbb{N}$  אזי  $\mathbb{Z}_n$  חוג אבל בעל יחידה וכן  $\mathbb{Z}$  חוג אבל בעל יחידה.

**טענה:** יהי  $R$  חוג אבל בעל יחידה ויהי  $n \in \mathbb{N}_+$  אזי  $R[x_1 \dots x_n]$  חוג אבל בעל יחידה.

**טענה:** יהי  $R$  חוג אבל בעל יחידה אזי  $\langle R[x], + \rangle$  קונובולוציה, חוג אבל בעל יחידה.

**תחום שלמות:** חוג אבל  $R$  עבורו לכל  $a, b \in R$  המקיימים  $ab = 0$  מתקיים  $(a = 0) \vee (b = 0)$ .

**טענה:** יהי  $R$  תחום שלמות ויהי  $n \in \mathbb{N}_+$  אזי  $R[x_1 \dots x_n]$  תחום שלמות.

**הגדרה:** יהי  $R$  חוג אבל בעל יחידה אזי  $R^\times = \{a \in R \mid \exists h \in R. ah = ha = 1\}$ .

**למה:** יהי  $R$  חוג אבל בעל יחידה אזי  $(R^\times, *)$  חבורה.

**טענה:** יהי  $R$  חוג אבל בעל יחידה אזי  $(R[x])^\times = R^\times$ .

**שדה:** חוג אבל בעל יחידה  $\mathbb{F}$  המקיים  $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ .

**הגדרה:** יהי  $R$  תחום שלמות באשר  $R \neq \{0\}$  אזי  $\sim_{\text{Frac}} = \left\{ ((a, b), (c, d)) \in (R \times (R \setminus \{0\}))^2 \mid ad = bc \right\}$ .

**סימון:** יהי  $R$  תחום שלמות באשר  $R \neq \{0\}$  אזי  $\text{Frac}(R) = R / \sim_{\text{Frac}}$ .

**הגדרה:** יהי  $R$  תחום שלמות באשר  $R \neq \{0\}$  ויהי  $(a, b), (c, d) \in R \times (R \setminus \{0\})$  אזי  $[(a, b)]_{\text{Frac}} + [(c, d)]_{\text{Frac}} = [(ad + cb, bd)]_{\text{Frac}}$ .

וכן  $[(a, b)]_{\text{Frac}} \cdot [(c, d)]_{\text{Frac}} = [(ac, bd)]_{\text{Frac}}$ .

**טענה שדה השברים:** יהי  $R$  תחום שלמות באשר  $R \neq \{0\}$  אזי  $\text{Frac}(R)$  שדה.

**טענה:** יהי  $\mathbb{K}$  שדה אזי  $\mathbb{K}[x]$  תחום שלמות.

**פונקציות רציונליות:** יהי  $\mathbb{K}$  שדה אזי  $\mathbb{K}(x) = \text{Frac}(\mathbb{K}[x])$ .

**מסקנה:** יהי  $\mathbb{K}$  שדה אזי  $\mathbb{K}(x)$  שדה.

**הומומורפיזם בין חוגים:** יהיו  $R, S$  חוגים אזי  $\nu : R \rightarrow S$  המקיימת

• משמרת כפל: לכל  $a, b \in R$  מתקיים  $\nu(ab) = \nu(a) \nu(b)$ .

• משמרת חיבור: לכל  $a, b \in R$  מתקיים  $\nu(a + b) = \nu(a) + \nu(b)$ .

**גרעין:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $\ker(\nu) = \nu^{-1}[\{0\}]$ .

**למה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $\ker(\nu), \text{Im}(\nu)$  חוגים.

**למה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $(\ker(\nu) = 0) \iff (\nu \text{ מונומורפיזם})$ .

**למה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $(\text{Im}(\nu) = S) \iff (\nu \text{ אפימורפיזם})$ .

**סימון:** יהיו  $R, S$  חוגים איזומורפיים אזי  $R \simeq S$ .

**למה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $(\nu \text{ איזומורפיזם}) \iff (\nu \text{ מונומורפיזם וכן } \nu \text{ אפימורפיזם})$ .

**חוג השלמים של גאוס:**  $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ .

**אידאל:** יהי  $R$  חוג אבל אזי  $I \subseteq R$  המקיימת  $I \cdot R \subseteq I$  וכן  $I + I \subseteq I$ .

**טענה:** יהי  $R$  חוג אבל ויהי  $I \subseteq R$  אידאל אזי  $(I, +) \leq (R, +)$ .

**טענה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם אזי  $\ker(\nu)$  אידאל.

**משפט:** יהי  $R$  חוג אבל בעל יחידה אזי  $(R \text{ שדה}) \iff (I \subseteq R \text{ אידאל } I \subseteq R \text{ מתקיים } I \in \{\{0\}, R\})$ .

**מסקנה:** יהיו  $\mathbb{K}, \mathbb{F}$  שדות ויהי  $\nu : \mathbb{F} \rightarrow \mathbb{K}$  הומומורפיזם אזי  $(\nu \text{ מונומורפיזם}) \vee (\nu = 0)$ .

**הגדרה:** יהי  $R$  חוג אבל ויהי  $I \subseteq R$  אידאל אזי  $R/I = \{a + I \mid a \in R\}$ .

**טענה:** יהי  $R$  חוג אבל ויהי  $I \subseteq R$  אידאל ויהיו  $a, b, c, d \in R$  באשר  $a + I = c + I$  וכן  $b + I = d + I$  אזי  $(ab) + I = (cd) + I$ .

**הגדרה:** יהי  $R$  חוג אבל ויהי  $I \subseteq R$  אידאל ויהיו  $a, b \in R$  אזי  $(a + I)(b + I) = (ab) + I$ .

**משפט חוג מנה:** יהי  $R$  חוג אבל ויהי  $I \subseteq R$  אידאל אזי  $R/I$  חוג אבל.

**טענה:** יהי  $R$  חוג אבלי יהי  $I \subseteq R$  אידאל ונגדיר  $p : R \rightarrow R/I$  כך  $p(a) = a + I$  אזי  $p$  הינו אפימורפיזם חוגים וכן  $\ker(p) = I$ .

**למה:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם חוגים אזי  $R/\ker(\nu)$  חוג.

**משפט:** יהיו  $R, S$  חוגים ויהי  $\nu : R \rightarrow S$  הומומורפיזם חוגים אזי  $R/\ker(\nu) \simeq \text{Im}(\nu)$ .

**טענה:**  $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$ .

**אידאל אמיתי:** יהי  $R$  חוג אבלי בעל יחידה אזי אידאל  $I \subseteq R$  המקיים  $I \neq R$ .

**טענה:** יהי  $R$  חוג אבלי בעל יחידה ויהי  $I \subseteq R$  אזי  $(I \cap R^\times = \emptyset) \iff (I \text{ אמיתי})$ .

**אידאל נוצר:** יהי  $R$  חוג אבלי בעל יחידה ותהא  $S \subseteq R$  אזי  $(S) = \{\sum_{i=1}^n r_i s_i \mid (n \in \mathbb{N}_+) \wedge (r \in R^n) \wedge (s \in S^n)\}$ .

**טענה:** יהי  $R$  חוג אבלי בעל יחידה ותהא  $S \subseteq R$  אזי  $(S)$  אידאל.

**אידאל ראשי:** יהי  $R$  חוג אבלי אזי אידאל  $I \subseteq R$  עבורו קיים  $a \in R$  המקיים  $I = (a)$ .

**אידאל ראשוני:** יהי  $R$  חוג אבלי אזי אידאל  $I \subseteq R$  עבורו לכל  $a, b \in R$  המקיימים  $ab \in I$  מתקיים  $(a \in I) \vee (b \in I)$ .

**אידאל מקסימלי:** יהי  $R$  חוג אבלי אזי אידאל  $I \subseteq R$  עבורו לכל אידאל  $J \subseteq R$  לא מתקיים  $I \subsetneq J$ .

**משפט:** יהי  $R$  חוג אבלי בעל יחידה ויהי  $I \subseteq R$  אידאל אזי

- $(I \text{ אידאל ראשוני}) \iff (R/I \text{ תחום שלמות})$ .
- $(I \text{ אידאל מקסימלי}) \iff (R/I \text{ שדה})$ .

**תחום ראשי:** חוג אבלי בעל יחידה  $R$  עבורו לכל אידאל  $I \subseteq R$  מתקיים כי  $I$  ראשי.

**איבר אי־פריק:** יהי  $R$  חוג אבלי בעל יחידה אזי  $r \in R$  עבורו לכל  $a, b \in R$  המקיימים  $r = ab$  מתקיים  $(a \in R^\times) \vee (b \in R^\times)$ .

**איבר ראשוני:** יהי  $R$  חוג אבלי בעל יחידה אזי  $r \in R$  עבורו לכל  $a, b \in R$  המקיימים  $r|ab$  מתקיים  $(r|a) \vee (r|b)$ .

**משפט:** יהי  $\mathbb{K}$  שדה אזי

- $\mathbb{K}[x]$  תחום ראשי.
- יהי  $f \in \mathbb{K}[x]$  אזי  $(f) \iff (f) \iff (f \text{ ראשוני}) \iff (f \text{ אי־פריק ב-}\mathbb{K}[x])$ .

**מסקנה:** יהי  $R$  תחום שלמות אזי  $(R[x]) \iff (R \text{ תחום ראשי}) \iff (R \text{ שדה})$ .

**משפט:** יהי  $R$  חוג אבלי בעל יחידה ויהי  $I \subseteq R$  אידאל אזי קיים אידאל מקסימלי  $M \subseteq R$  עבורו  $I \subseteq M$ . דורש AC

**מחלק משותף מקסימלי:** יהי  $\mathbb{K}$  שדה ויהיו  $f_1 \dots f_n, d \in \mathbb{K}[x]$  באשר  $(d) = (f_1 \dots f_n)$  וכן  $d$  מתוקן אזי  $\gcd(f_1 \dots f_n) = d$ .

**משפט חלוקה עם שארית:** יהי  $R$  חוג אבלי בעל יחידה ויהיו  $f, g \in R[x]$  באשר המקדם המוביל של  $g$  הפיך אזי קיימים ויחידים  $q, r \in R[x]$  באשר  $f = qg + r$  וכן  $\deg(r) < \deg(g)$ .

**פולינומים זרים:** יהי  $\mathbb{F}$  שדה אזי  $f, g \in \mathbb{F}[x]$  המקיימים  $\gcd(f, g) = 1$ .

**פולינום פרימיטיבי:** יהיו  $a_0 \dots a_n \in \mathbb{Z}$  אזי  $\sum_{i=0}^n a_i x^i$  המקיים  $\gcd(a_1 \dots a_n) = 1$ .

**משפט:** יהי  $f \in \mathbb{Z}[x] \setminus \{0\}$  ויהיו  $g, h \in \mathbb{Q}[x]$  באשר  $f = gh$  אזי קיימים  $r, s \in \mathbb{Q}$  המקיימים  $sh, rg \in \mathbb{Z}[x]$  וכן  $f = (rg)(sh)$ .

**מסקנה גאוס:** יהי  $f \in \mathbb{Z}[x]$  מתוקן ויהי  $d \in \mathbb{Q}[x]$  אי־פריק מתוקן באשר  $d|f$  אזי  $d \in \mathbb{Z}[x]$ .

**למה גאוס:** יהי  $f \in \mathbb{Z}[x]$  אזי  $(f \text{ אי־פריק}) \iff (f \text{ אי־פריק מעל } \mathbb{Q}[x] \text{ וכן } f \text{ פרימיטיבי})$ .

**טענה קריטריון אייזנשטיין:** יהיו  $a_0 \dots a_n \in \mathbb{Z}$  ויהי  $p \in \mathbb{P}$  המקיים  $p \nmid a_n$  וכן  $p|a_i$  לכל  $i < n$  וכן  $p^2 \nmid a_0$  אזי  $\sum_{i=0}^n a_i x^i$  אי־פריק מעל  $\mathbb{Q}[x]$ .

**שורש של פולינום:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי  $\alpha \in \mathbb{K}$  המקיים  $f(\alpha) = 0$ .

**סימון:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי  $\text{sols}_{\mathbb{K}}(f) = \{\alpha \in \mathbb{K} \mid f(\alpha) = 0\}$ .

**משפט בז'ור:** יהי  $\mathbb{K}$  שדה יהי  $f \in \mathbb{K}[x]$  ויהי  $\alpha \in \mathbb{K}$  אזי  $((x - \alpha) | f) \iff (\alpha \in \text{sols}_{\mathbb{K}}(f))$ .

**מסקנה:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי  $|\text{sols}_{\mathbb{K}}(f)| \leq \deg(f)$ .

**שורש פשוט:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי  $\alpha \in \text{sols}_{\mathbb{K}}(f)$  המקיים  $(x - \alpha)^2 \nmid f$ .

**שורש מרובה:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי  $\alpha \in \text{sols}_{\mathbb{K}}(f)$  המקיים  $(x - \alpha)^2 | f$ .

**נגזרת של פולינום:** יהי  $\mathbb{K}$  שדה יהי  $n \in \mathbb{N}$  ויהיו  $a_0 \dots a_n \in \mathbb{K}$  אזי  $(\sum_{i=0}^n a_i x^i)' = \sum_{i=1}^n a_i x^{i-1}$ .

**משפט:** יהי  $\mathbb{K}$  שדה ויהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אזי (כל השורשים של  $f$  הם פשוטים)  $\iff (\gcd(f, f') = 1)$ .

**טענה:** יהי  $\mathbb{F}$  שדה אזי ויהי  $f \in \mathbb{F}[x]$  באשר  $\deg(f) \geq 1$  אזי  $(f \text{ ראשוני}) \iff (f \text{ אי־פריק})$ .

**פולינום ציקלוטומי:** יהי  $p \in \mathbb{P}$  אזי נגדיר  $\Phi_p \in \mathbb{Q}[x]$  כך  $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ .

**טענה:** יהי  $p \in \mathbb{P}$  אזי  $\Phi_p$  אי־פריק.

**סימון:** יהי  $p \in \mathbb{P}$  אזי  $\mathbb{F}_p = \mathbb{Z}_p$ .

**שדה הרחבה:** יהי  $\mathbb{K}$  שדה אזי שדה  $\mathbb{L}$  המקיים  $\mathbb{K} \subseteq \mathbb{L}$ .

**סימון:** יהיו  $\mathbb{K}, \mathbb{L}$  שדות באשר  $\mathbb{L}$  הרחבה של  $\mathbb{K}$  אזי  $\mathbb{L}/\mathbb{K}$ .

**הערה:** יהיו  $\mathbb{K}, \mathbb{L}$  שדות באשר  $\mathbb{L}/\mathbb{K}$  אזי נתייחס לביטוי  $\mathbb{L}/\mathbb{K}$  כאובייקט.

**הומומורפיזם הרחבות:** יהיו  $\mathbb{K}, \mathbb{F}, \mathbb{L}$  שדות באשר  $\mathbb{K}/\mathbb{F}$  הרחבה וכן  $\mathbb{L}/\mathbb{F}$  הרחבה אזי שיכון  $\nu: \mathbb{K}/\mathbb{F} \rightarrow \mathbb{L}/\mathbb{F}$  המקיים  $\nu|_{\mathbb{F}} = \text{Id}_{\mathbb{F}}$ .

**שדה פשוט:** שדה  $\mathbb{F}$  עבורו לא קיים שדה  $\mathbb{K}$  המקיים  $\mathbb{K} \subset \mathbb{F}$ .

**טענה:** יהי  $\mathbb{F}$  שדה אזי  $\{\mathbb{K} \subseteq \mathbb{F} \mid \mathbb{K} \text{ שדה}\} \cap \{\mathbb{K} \subseteq \mathbb{F} \mid \mathbb{K} \text{ שדה פשוט}\} = \{\mathbb{F}\}$ .

**מסקנה:** יהי  $\mathbb{F}$  שדה אזי קיים ויחיד שדה פשוט  $\mathbb{K} \subseteq \mathbb{F}$ .

**משפט:** יהי  $\mathbb{F}$  שדה פשוט אזי  $(\mathbb{F} \simeq \mathbb{Q}) \vee (\exists p \in \mathbb{P}. \mathbb{F} \simeq \mathbb{F}_p)$ .

**מציין של שדה:** יהי  $\mathbb{F}$  שדה ויהי  $\mathbb{K} \subseteq \mathbb{F}$  שדה פשוט אזי

• אם  $\mathbb{K} \simeq \mathbb{Q}$  אז  $\text{char}(\mathbb{F}) = 0$ .

• אם קיים  $p \in \mathbb{P}$  עבורו  $\mathbb{K} \simeq \mathbb{F}_p$  אז  $\text{char}(\mathbb{F}) = p$ .

**טענה:** יהי  $\mathbb{F}$  שדה המקיים  $\text{char}(\mathbb{F}) > 0$  אזי לכל  $a \in \mathbb{F}$  מתקיים  $\text{char}(\mathbb{F}) \cdot a = 0$ .

**מורפיזם פרובניוס:** יהי  $p \in \mathbb{P}$  ויהי  $\mathbb{K}$  שדה המקיים  $\text{char}(\mathbb{K}) = p$  אזי נגדיר  $\text{Fr}_p: \mathbb{K} \rightarrow \mathbb{K}$  כך  $\text{Fr}_p(a) = a^p$ .

**משפט:** יהי  $p \in \mathbb{P}$  ויהי  $\mathbb{K}$  שדה המקיים  $\text{char}(\mathbb{K}) = p$  אזי  $\text{Fr}_p$  מונומורפיזם.

**טענה:** יהי  $\mathbb{F}$  שדה באשר  $\text{char}(\mathbb{F}) \neq 2$  ויהיו  $a, b, c \in \mathbb{F}$  באשר  $a \neq 0$  אזי  $\text{sols}(ax^2 + bx + c) = \left\{ \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right\}$ .

**איבר אלגברי מעל שדה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבת שדות אזי  $\alpha \in \mathbb{L}$  עבורו קיים  $f \in \mathbb{K}[x] \setminus \{0\}$  המקיים  $f(\alpha) = 0$ .

**איבר טרנסצנדנטי מעל שדה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבת שדות אזי  $\alpha \in \mathbb{L}$  באשר  $\alpha$  אינו אלגברי מעל  $\mathbb{K}$ .

**הרחבה אלגברית:** הרחבה  $\mathbb{L}/\mathbb{K}$  עבורה לכל  $\alpha \in \mathbb{L}$  מתקיים כי  $\alpha$  אלגברי מעל  $\mathbb{K}$ .

**טענה:**  $\mathbb{C}/\mathbb{R}$  הרחבה אלגברית.

**פולינום מינימלי של איבר אלגברי:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהי  $\alpha \in \mathbb{L}$  אלגברי מעל  $\mathbb{K}$  אזי פולינום מתוקן  $f \in \mathbb{K}[x] \setminus \{0\}$  בעל דרגה

מינימלית המקיים  $f(\alpha) = 0$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהי  $\alpha \in \mathbb{L}$  אלגברי מעל  $\mathbb{K}$  אזי קיים ויחיד פולינום מינימלי  $f_\alpha \in \mathbb{K}[x]$  עבור  $\alpha$  וכן

$(f_\alpha) = \{f \in \mathbb{K}[x] \mid f(\alpha) = 0\}$ .

**סימון:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהי  $\alpha \in \mathbb{L}$  אלגברי מעל  $\mathbb{K}$  אזי הפולינום המינימלי של  $\alpha$  הינו  $f_\alpha$ .

**מסקנה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה יהי  $\alpha \in \mathbb{L}$  אלגברי מעל  $\mathbb{K}$  אזי  $f_\alpha$  אי-פריק.

**חוג נוצר:** יהיו  $A, B$  חוגים אבליים בעלי יחידה באשר  $A \subseteq B$  תהא  $S \subseteq B$  ויהי  $R \subseteq B$  החוג האבלי בעל יחידה המינימלי המקיים

$R \cup S \subseteq R$ .

**סימון:** יהיו  $A, B$  חוגים אבליים בעלי יחידה באשר  $A \subseteq B$  תהא  $S \subseteq B$  ויהי  $R \subseteq B$  החוג הנוצר מ- $A$  על ידי  $S$  אזי  $A[S] = R$ .

**טענה:** יהיו  $A, B$  חוגים אבליים בעלי יחידה באשר  $A \subseteq B$  ותהא  $S \subseteq B$  אזי  $A[S] = \bigcup_{n=1}^{\infty} \left\{ f(s_1 \dots s_n) \mid \begin{matrix} f \in A[x_1 \dots x_n] \\ s_1 \dots s_n \in S \end{matrix} \right\}$ .

**הרחבה נוצרת:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה תהא  $S \subseteq \mathbb{L}$  ויהי  $\mathbb{F} \subseteq \mathbb{L}$  השדה המינימלי המקיים  $\mathbb{K} \subseteq \mathbb{F}$  וכן  $S \subseteq \mathbb{F}$  אזי  $\mathbb{F}/\mathbb{K}$ .

**סימון:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה תהא  $S \subseteq \mathbb{L}$  ותהא  $\mathbb{F}/\mathbb{K}$  הרחבה הנוצרת על ידי  $S$  אזי  $\mathbb{K}(S) = \mathbb{F}$ .

**טענה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהיו  $\alpha_1 \dots \alpha_n \in \mathbb{L}$  אזי  $\mathbb{K}(\alpha_1 \dots \alpha_n) = \bigcup_{n=1}^{\infty} \bigcup_{f, g \in \mathbb{K}[x_1 \dots x_n]} \left\{ \frac{f(s_1 \dots s_n)}{g(s_1 \dots s_n)} \mid \begin{matrix} s_1 \dots s_n \in S \\ g(s_1 \dots s_n) \neq 0 \end{matrix} \right\}$ .

**טענה:**  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ .

**הרחבה פשוטה:** תהא  $\mathbb{L}/\mathbb{K}$  ויהי  $\alpha \in \mathbb{L}$  אזי  $\mathbb{K}(\alpha)/\mathbb{K}$ .

**משפט מבנה של הרחבה פשוטה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהי  $\alpha \in \mathbb{L}$  אזי

• אם  $\alpha$  טרנסצנדנטי מעל  $\mathbb{K}$  אז  $\mathbb{K}(\alpha)/\mathbb{K} \simeq \mathbb{K}(x)/\mathbb{K}$ .

• אם  $\alpha$  אלגברי מעל  $\mathbb{K}$  אז  $\mathbb{K}(\alpha)/\mathbb{K} \simeq (\mathbb{K}[x]/(f_\alpha))/\mathbb{K}$ .

**מסקנה:** יהי  $\mathbb{K}$  שדה יהי  $f \in \mathbb{K}[x] \setminus \{0\}$  אי-פריק ויהיו  $\alpha, \beta \in \mathbb{K}$  שורשים של  $f$  אזי קיים איזומורפיזם  $\nu: \mathbb{K}(\alpha)/\mathbb{K} \rightarrow \mathbb{K}(\beta)/\mathbb{K}$

באשר  $\nu(\alpha) = \beta$ .

**למה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה יהיו  $\alpha_1 \dots \alpha_n \in \mathbb{L}$  ויהי  $\beta \in \mathbb{K}(\alpha_1 \dots \alpha_n)$  אזי קיים  $f \in \mathbb{K}[x_1 \dots x_n]$  המקיים  $f(\alpha_1 \dots \alpha_n) = \beta$ .

**טענה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה אזי  $\mathbb{L}$  הינו מרחב וקטורי מעל  $\mathbb{K}$ .

**דרגה של הרחבה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה אזי  $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$ .

**הרחבה סופית:** הרחבה  $\mathbb{L}/\mathbb{K}$  המקיימת  $[\mathbb{L} : \mathbb{K}] < \infty$ .

**טענה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהי  $\alpha \in \mathbb{L}$  אלגברי מעל  $\mathbb{K}$  אזי  $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg(f_\alpha)$ .

**טענה:** יהי  $\mathbb{K}$  שדה סופי אזי קיים  $p \in \mathbb{P}$  עבורו  $\mathbb{F}_p \subseteq \mathbb{K}$ .

**מסקנה:** יהי  $\mathbb{K}$  שדה סופי אזי קיים  $p \in \mathbb{P}$  וקיים  $n \in \mathbb{N}$  עבורם  $|\mathbb{K}| = p^n$ .

**משפט מולטיפליקטיביות של דרגה:** תהיינה  $F/L, L/K$  הרחבות אזי  $[F : K] = [F : L] \cdot [L : K]$ .

**משפט:** תהא  $L/K$  הרחבה ויהי  $\alpha \in L$  אזי  $(\alpha$  אלגברי מעל  $K) \iff (\alpha$  קיים שדה  $F \subseteq L$  המקיים  $\alpha \in F$  וכן  $F/K$  הרחבה סופית).

**מסקנה:** תהא  $L/K$  הרחבה ויהיו  $\alpha_1 \dots \alpha_n \in L$  אלגבריים מעל  $K$  אזי קיים שדה  $F \subseteq L$  המקיים  $\alpha_1 \dots \alpha_n \in F$  וכן  $F/K$  הרחבה סופית.

**מסקנה:** תהיינה  $F/L, L/K$  הרחבות אלגבריות אזי  $F/K$  הרחבה אלגברית.

**סגור אלגברי בשדה:** תהא  $L/K$  הרחבה אזי  $\alpha$  אלגברי מעל  $K$   $\iff \alpha \in \overline{K}$ .

**מסקנה:** תהא  $L/K$  הרחבה אזי  $\overline{K}$  שדה.

**שדה סגור אלגברית:** שדה  $K$  עבורו לכל  $f \in K[x]$  באשר  $\deg(f) \geq 1$  קיים  $\alpha \in K$  המקיים  $f(\alpha) = 0$ .

**הרחבה סגורה אלגברית:** הרחבה  $L/K$  כאשר  $L$  סגור אלגברית.

**טענה:** יהי  $K$  שדה סגור אלגברית ויהי  $f \in K[x] \setminus \{0\}$  אזי קיימים  $\alpha_0, \alpha_1 \dots \alpha_n \in K$  המקיימים  $f = \alpha_0 \cdot \prod_{i=1}^n (x - \alpha_i)$ .

**טענה:** תהא  $L/K$  הרחבה סגורה אלגברית ויהי  $F \subseteq L$  המקיים  $K \subseteq F$  אזי  $L/F$  הרחבה סגורה אלגברית.

**למה:** יהי  $K$  שדה סגור אלגברית ותהא  $L/K$  הרחבה אלגברית אזי  $L = K$ .

**למה:** יהי  $K$  שדה ויהי  $f \in K[x]$  באשר  $\deg(f) \geq 1$  אזי קיימת הרחבה סופית  $L/K$  המקיימת  $\text{sols}_L(f) \neq \emptyset$ .

**למה:** יהי  $K$  שדה ויהי  $f \in K[x] \setminus \{0\}$  אזי קיימת הרחבה סופית  $L/K$  עבורה קיימים  $\alpha_0, \alpha_1 \dots \alpha_n \in L$  המקיימים  $f = \alpha_0 \cdot \prod_{i=1}^n (x - \alpha_i)$ .

**מסקנה:** יהי  $K$  שדה ויהיו  $f_1 \dots f_m \in K[x] \setminus \{0\}$  אזי קיימת הרחבה סופית  $L/K$  עבורה קיימת  $\alpha \in M_{m \times (n+1)}(L)$  המקיימת  $f_j = \alpha_{j,1} \cdot \prod_{i=1}^n (x - \alpha_{j,i+1})$  לכל  $j \in [m]$ .

**משפט:** יהי  $K$  שדה תהא  $\mathcal{T}$  קבוצה ויהיו  $\langle f_\tau \in K[x] \mid \tau \in \mathcal{T} \rangle$  באשר  $\deg(f_\tau) \geq 1$  לכל  $\tau \in \mathcal{T}$  אזי קיימת הרחבה אלגברית  $L/K$  המקיימת  $\text{sols}_L(f_\tau) \neq \emptyset$  לכל  $\tau \in \mathcal{T}$ .

**משפט:** יהי  $K$  שדה אזי קיימת הרחבה סגורה אלגברית  $L/K$ .

**משפט שטייניץ:** תהא  $L/K$  הרחבה אלגברית יהי  $F$  שדה סגור אלגברית ויהי  $\nu : K \rightarrow F$  מונומורפיזם אזי קיים מונומורפיזם  $\Phi : L \rightarrow F$  דורש AC.

**מסקנה:** תהיינה  $F/K, L/K$  הרחבות סגורות אלגבריות אזי  $F \simeq L$ .

**סימון:** יהי  $K$  שדה ותהא  $L/K$  הרחבה סגורה אלגברית אזי  $\overline{K} = L$ .

**מסקנה:** תהא  $L/K$  הרחבה אלגברית אזי קיים מונומורפיזם  $\nu : L/K \rightarrow \overline{K}/K$ .

**דרגה של פונקציה רציונלית:** יהי  $K$  שדה תהא  $a \in K(x)$  ויהיו  $f, g \in K[x]$  באשר  $a = \frac{f}{g}$  וכן  $\gcd(f, g) = 1$  אזי  $\deg(a) = \max\{\deg(f), \deg(g)\}$ .

**משפט:** יהי  $K$  שדה ותהא  $a \in K(x)$  באשר  $\deg(a) \geq 1$  אזי  $a$  טרנסצנדנטי מעל  $K$  וכן  $K(x)/K(a)$  הרחבה אלגברית מדרגה  $\deg(a)$ .

**מסקנה:** יהי  $K$  שדה ותהא  $a \in K(a)$  אזי  $(K(x) = K(a)) \iff (\alpha, \beta, \gamma, \delta \in K \text{ המקיימים } \alpha\delta - \beta\gamma \neq 0 \text{ וכן } a = \frac{\alpha x + \beta}{\gamma x + \delta})$ .

**מסקנה:** יהי  $K$  שדה אזי  $\text{Aut}(K(x)) = \left\{ \frac{\alpha x + \beta}{\gamma x + \delta} \mid (\alpha, \beta, \gamma, \delta \in K) \wedge (\alpha\delta - \beta\gamma \neq 0) \right\}$ .

**מסקנה:** יהי  $K$  שדה יהי  $\varphi \in \text{Aut}(K(x))$  ויהי  $a \in K(x)$  אזי  $\deg(a) = \deg(\varphi(a))$ .

**הרחבה טרנסצנדנטית פשוטה:** הרחבה  $L/K$  עבורה קיים  $\alpha \in L$  טרנסצנדנטי המקיים  $L = K(\alpha)$ .

**משפט לורוט:** יהיו  $L, K$  שדות כאשר  $L/K$  הרחבה לא טריוואלית וכן  $K(x)/L$  הרחבה טרנסצנדנטית פשוטה.

**פרמטריזציה רציונלית:** יהי  $K$  שדה ותהא  $f : K^2 \rightarrow K$  אזי פונקציות רציונליות  $\nu, \psi \in K(x)$  עבורן  $f(\nu, \psi) = 0$ .

**עקומה רציונלית:** יהי  $K$  שדה תהא  $f : K^2 \rightarrow K$  אזי עקומה  $\{f(x, y) = 0\}$  עבורה קיימת פרמטריזציה רציונלית.

**איבר תלוי אלגברית מעל שדה:** תהא  $L/K$  הרחבה ויהיו  $u_1 \dots u_m \in L$  אזי  $v \in L$  כאשר  $v$  אלגברי מעל  $K(u_1 \dots u_m)$ .

**איבר בלתי תלוי אלגברית מעל שדה (בת"א):** תהא  $L/K$  הרחבה ויהיו  $u_1 \dots u_m \in L$  אזי  $v \in L$  כאשר  $v$  אינו תלוי אלגברית ב- $u_1 \dots u_m$  מעל  $K$ .

**למה:** תהא  $L/K$  הרחבה יהיו  $u_1 \dots u_m, v \in L$  כאשר  $v$  תלוי אלגברית ב- $u_1 \dots u_m$  מעל  $K$  וכן  $v$  בת"א ב- $u_1 \dots u_{m-1}$  מעל  $K$  אזי  $u_m$  תלוי אלגברית ב- $u_1 \dots u_{m-1}, v$  מעל  $K$ .

**למה:** תהא  $L/K$  הרחבה יהיו  $u_1 \dots u_m, v_1 \dots v_n, w \in L$  כאשר  $w$  תלוי אלגברית ב- $v_1 \dots v_n$  מעל  $K$  וכן  $v_j$  תלוי אלגברית ב- $u_1 \dots u_m$  מעל  $K$  לכל  $j \in [n]$  אזי  $w$  תלוי אלגברית ב- $u_1 \dots u_m$  מעל  $K$ .

**קבוצה בלתי תלויה אלגברית/טרנסצנדנטיים בלתי תלויים אלגברית זה בזה (בת"א):** תהא  $L/K$  הרחבה אזי  $u_1 \dots u_m \in L$  עבורם לכל  $f \in K[x_1 \dots x_m]$  מתקיים כי אם  $f(u_1 \dots u_m) = 0$  אז  $f = 0$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהיו  $u_1 \dots u_m \in \mathbb{L}$  בת"א מעל  $\mathbb{K}$  אזי  $\mathbb{K}(u_1 \dots u_m) \simeq \mathbb{K}(x_1 \dots x_m)$ .  
**קבוצה בלתי תלויה אלגברית (בת"א):** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה אזי  $\mathcal{B} \subseteq \mathbb{L}$  עבורה לכל  $S \subseteq \mathcal{B}$  סופית ולכל  $f \in \mathbb{K}[x_1, \dots, x_{|S|}]$  מתקיים כי אם  $f(S) = 0$  אז  $f = 0$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה תהא  $\mathcal{I}$  קבוצה ותהא  $\{u_\alpha\}_{\alpha \in \mathcal{I}} \subseteq \mathbb{L}$  בת"א מעל  $\mathbb{K}$  אזי  $\mathbb{K}(\{u_\alpha\}_{\alpha \in \mathcal{I}}) \simeq \mathbb{K}(\{x_\alpha\}_{\alpha \in \mathcal{I}})$ .  
**בסיס טרנסצנדנטי של הרחבה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה שאינה אלגברית אזי  $\mathcal{B} \subseteq \mathbb{L}$  בת"א מעל  $\mathbb{K}$  עבורה לכל  $\mathcal{A} \subseteq \mathbb{L}$  בת"א מעל  $\mathbb{K}$  מתקיים  $\mathcal{B} \not\subseteq \mathcal{A}$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה שאינה אלגברית אזי קיים ל- $\mathbb{L}/\mathbb{K}$  בסיס טרנסצנדנטי.  
**הרחבה טרנסצנדנטית:** הרחבה  $\mathbb{L}/\mathbb{K}$  עבורה קיימת קבוצה  $\mathcal{I}$  המקיימת  $\mathbb{L}/\mathbb{K} \simeq \mathbb{K}(\{x_\alpha\}_{\alpha \in \mathcal{I}})/\mathbb{K}$ .  
**מסקנה משפט הפיצול:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה אזי קיים שדה  $\mathbb{F}$  באשר  $\mathbb{L}/\mathbb{F}, \mathbb{F}/\mathbb{K}$  הרחבות המקיים כי  $\mathbb{F}/\mathbb{K}$  הרחבה טרנסצנדנטית וכן  $\mathbb{L}/\mathbb{F}$  הרחבה אלגברית.

**קבוצות שקולות אלגבריות:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה אזי  $A, B \subseteq \mathbb{L}$  עבורן לכל  $\alpha \in A$  מתקיים כי  $\alpha$  אלגברי מעל  $\mathbb{K}(B)$  וכן לכל  $\beta \in B$  מתקיים כי  $\beta$  אלגברי מעל  $\mathbb{K}(A)$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ותהא  $A \subseteq \mathbb{L}$  אזי קיימת  $M \subseteq A$  בת"א מעל  $\mathbb{K}$  באשר  $A, M$  שקולות אלגברית מעל  $\mathbb{K}$ . דורש AC  
**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ותהינה  $A, B \subseteq \mathbb{L}$  באשר  $B \subseteq A$  וכן  $B$  בת"א אזי קיימת  $M \subseteq A$  בת"א מעל  $\mathbb{K}$  באשר  $B \subseteq M$  וכן  $A, M$  שקולות אלגברית מעל  $\mathbb{K}$ . דורש AC

**למה משפט ההחלפה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהיו  $a_1 \dots a_r, b_1 \dots b_s \in \mathbb{L}$  באשר  $\{b_1 \dots b_s\}$  בת"א מעל  $\mathbb{K}$  וכן  $b_j$  תלוי אלגברית ב- $a_1 \dots a_r$  מעל  $\mathbb{K}$  לכל  $j \in [s]$  אזי  $r \geq s$  וכן קיימת  $S \subseteq \{a_1 \dots a_r\}$  באשר  $|S| = s$  עבורה  $\{a_1 \dots a_r, b_1 \dots b_s\} \setminus S$  שקולה אלגברית ל- $\{a_1 \dots a_r\}$  מעל  $\mathbb{K}$ .

**משפט:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ותהינה  $A, B \subseteq \mathbb{L}$  בת"א שקולות אלגברית מעל  $\mathbb{K}$  אזי  $|A| = |B|$ .

**מסקנה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה ויהיו  $\mathcal{A}, \mathcal{B} \subseteq \mathbb{L}$  בסיסים טרנסצנדנטיים של  $\mathbb{L}/\mathbb{K}$  אזי  $|\mathcal{A}| = |\mathcal{B}|$ .

**דרגה טרנסצנדנטית של הרחבה:** תהא  $\mathbb{L}/\mathbb{K}$  הרחבה שאינה אלגברית ויהי  $\mathcal{B}$  בסיס טרנסצנדנטי של  $\mathbb{L}/\mathbb{K}$  אזי  $\deg_{\mathbb{K}}(\mathbb{L}) = |\mathcal{B}|$ .

**משפט:** תהינה  $\mathbb{F}/\mathbb{K}, \mathbb{L}/\mathbb{F}$  הרחבות אזי  $\deg_{\mathbb{K}}(\mathbb{L}) = \deg_{\mathbb{K}}(\mathbb{F}) + \deg_{\mathbb{F}}(\mathbb{L})$ .