

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 חוג אבל בעל יחידה אזי $R[x_1 \dots x_{n+1}] = (R[x_1 \dots x_n])[x_{n+1}]$.

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 $R \neq \{0\}$ ויהיו $(a, b), (c, d) \in R \times (R \setminus \{0\})$ 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 $\mathbb{K}(x)$ 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 $\nu(a + b) = \nu(a) + \nu(b)$.

הומומורפיזם בין חוגים בעלי יחידה: יהיו R, S חוגים בעלי יחידה אזי הומומורפיזם בין חוגים $\nu : R \rightarrow S$ המקיים $\nu(1_R) = 1_S$.

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.

קבוצת המונומורפיזמים/שיכונים: יהיו R, S חוגים אזי $\nu : R \rightarrow S$ הומומורפיזם חח"ע $R \hookrightarrow S = \{\nu : R \rightarrow S \mid \nu \text{ הומומורפיזם חח"ע}\}$.

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

קבוצת האפימורפיזמים: יהיו R, S חוגים אזי $\nu : R \rightarrow S$ הומומורפיזם על $R \twoheadrightarrow S = \{\nu : R \rightarrow S \mid \nu \text{ הומומורפיזם על}\}$.

למה: יהיו R, S חוגים ויהי $\nu : R \rightarrow S$ הומומורפיזם אזי $(\text{Im}(\nu) = S) \iff \nu$ 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 $I + I \subseteq I$ וכן $I \cdot R \subseteq I$.

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 $(R \text{ שדה}) \iff (I \subseteq R \text{ אידאל לכל } I \text{ מתקיים } I \in \{\{0\}, R\})$.

מסקנה: יהיו \mathbb{F}, \mathbb{K} שדות ויהי $\nu : \mathbb{F} \rightarrow \mathbb{K}$ הומומורפיזם אזי $\nu \in (\mathbb{F} \hookrightarrow \mathbb{K}) \cup \{0\}$.

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

טענה: יהי R חוג אבלי יהי $I \subseteq R$ אידיאל 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 אבלי יהי $I \subseteq R$ אידיאל ויהיו $a, b \in R$ אזי $(a + I)(b + I) = (ab) + I$.

משפט חוג מנה: יהי R חוג אבלי ויהי $I \subseteq R$ אידיאל אזי R/I חוג אבלי.

טענה: יהי R חוג אבלי יהי $I \subseteq R$ אידיאל 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 $R/\ker(\nu) \simeq \text{Im}(\nu)$.

אידיאל אמייתי: יהי R חוג אבלי בעל יחידה אזי אידיאל $I \subseteq R$ המקיים $I \neq R$.

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

אידיאל 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) אידיאל.

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

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

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

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

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

• $(I \text{ אידיאל ראשוני}) \iff (R/I \text{ תחום שלמות}).$

• $(I \text{ אידיאל מקסימלי}) \iff (R/I \text{ שדה}).$

תחום ראשי: חוג אבלי בעל יחידה R עבורו לכל אידיאל $I \subseteq R$ 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 $I \subseteq R$ אידיאל אזי קיים אידיאל 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 $\mathbb{Q}[x]$.

טענה קריטריון אייזנשטיין המוכלל: יהי \mathbb{F} שדה יהיו $a_0 \dots a_n \in \mathbb{F}[x_1 \dots x_m]$ ויהי $p \in \mathbb{F}[x_1 \dots x_m]$ אי־פריק 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 $\mathbb{F}[x_1 \dots x_m][x]$.

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 $(\alpha \in \text{sols}_{\mathbb{K}}(f)) \iff ((x - \alpha) | f)$.

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 $f \in \mathbb{F}[x]$ כאשר $\deg(f) \geq 1$ אזי f ראשוני $\iff f$ 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 כאשר \mathbb{L} הרחבה של \mathbb{K} אזי \mathbb{L}/\mathbb{K} .

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

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

הומומורפיזם הרחבות: יהי \mathbb{F} שדה ותהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות אזי שיכון $\nu: \mathbb{K} \hookrightarrow \mathbb{L}$ המקיים $\nu|_{\mathbb{F}} = \text{Id}_{\mathbb{F}}$.

סימון: יהי \mathbb{F} שדה ותהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות אזי $\{\nu: \mathbb{K} \hookrightarrow \mathbb{L} \mid \nu|_{\mathbb{F}} = \text{Id}_{\mathbb{F}}\}$.

טענה: יהי \mathbb{F} שדה ותהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות ויהי $\nu: \mathbb{K}/\mathbb{F} \rightarrow \mathbb{L}/\mathbb{F}$ אזי ν העתקה לינארית מעל \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 $(\mathbb{F} \simeq \mathbb{Q}) \vee (\exists p \in \mathbb{P}. \mathbb{F} \simeq \mathbb{F}_p)$.

מסקנה: 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 $|\mathbb{K}| = p^n$.

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 $\text{char}(\mathbb{F}) \cdot a = 0$.

טענה: יהי $p \in \mathbb{P}$ ויהי \mathbb{K} שדה המקיים $\text{char}(\mathbb{K}) = p$ אזי $(x+y)^p = x^p + y^p$ לכל $x, y \in \mathbb{K}$.

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 Fr_p מונומורפיזם.

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

טענה: יהי \mathbb{F} שדה אינסופי כאשר $\text{char}(\mathbb{F}) \neq 2$ אזי \mathbb{F}^\times אינה ציקלית.

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 $\alpha \in \mathbb{L}$ כאשר α אינו אלגברי מעל \mathbb{K} .

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

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

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה אזי (\mathbb{L}/\mathbb{K}) הרחבה אלגברית \iff (לכל חוג $R \subseteq \mathbb{L}$ המקיים $\mathbb{K} \subseteq R$ מתקיים כי R שדה).

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 α 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 α הינו f_α .

מסקנה: תהא \mathbb{L}/\mathbb{K} הרחבה ויהי $\alpha \in \mathbb{L}$ אלגברי מעל \mathbb{K} אזי f_α אי־פריק.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה יהי $\alpha \in \mathbb{L}$ אלגברי מעל \mathbb{K} ויהי $f \in \mathbb{K}[x]$ אי־פריק מתוקן המקיים $f(\alpha) = 0$ אזי $f = f_\alpha$.

טענה: יהי \mathbb{F} שדה ותהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות יהי $\nu: \mathbb{K}/\mathbb{F} \rightarrow \mathbb{L}/\mathbb{F}$ הומומורפיזם ויהי $\alpha \in \mathbb{K}$ אלגברי מעל \mathbb{F} אזי $\nu(\alpha)$ אלגברי

מעל \mathbb{F} וכן $f_{\nu(\alpha)} = f_\alpha$.

חוג נוצר: יהיו A, B חוגים אבליים בעלי יחידה כאשר $A \subseteq B$ 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 כאשר $A \subseteq B$ 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 כאשר $A \subseteq B$ 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 ותהא $S \subseteq \mathbb{L}$ אזי $\mathbb{K}(S) = \bigcup_{n=1}^{\infty} \bigcup_{f,g \in \mathbb{K}[x_1 \dots x_n]} \left\{ \frac{f(s_1 \dots s_n)}{g(s_1 \dots s_n)} \mid \begin{matrix} s_1 \dots s_n \in S \\ g(s_1 \dots s_n) \neq 0 \end{matrix} \right\}$

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 $\mathbb{K}(\alpha)$.

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

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

• אם α 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 $\alpha_1 \dots \alpha_n \in \mathbb{L}$ אלגבריים מעל \mathbb{K} ויהי $\beta \in \mathbb{K}(\alpha_1 \dots \alpha_n)$ אזי קיים $f \in \mathbb{K}[x_1 \dots x_n]$ המקיים $f(\alpha_1 \dots \alpha_n) = \beta$.

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 $[\mathbb{L} : \mathbb{K}] < \infty$.

למה: יהי \mathbb{F} שדה יהי $n \in \mathbb{N}_+$ ויהי $f \in \mathbb{F}[x]$ באשר $\deg(f) = n$ אזי $\{x^i + (f)\}_{i=0}^{n-1}$ בסיס של $\mathbb{F}[x]/(f)$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה סופית אזי \mathbb{L}/\mathbb{K} הרחבה נוצרת סופית.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה אזי $\mathbb{L}/\mathbb{K} \iff \mathbb{L}/\mathbb{K}$ הרחבה אלגברית נוצרת סופית.

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

משפט מולטיפליקטיביות של דרגה: תהינה $\mathbb{F}/\mathbb{L}, \mathbb{L}/\mathbb{K}$ הרחבות אזי $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}]$.

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

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

מסקנה: תהינה $\mathbb{F}/\mathbb{L}, \mathbb{L}/\mathbb{K}$ הרחבות אלגבריות אזי \mathbb{F}/\mathbb{K} הרחבה אלגברית.

טענה: יהיו $p, q \in \mathbb{P}$ שונים אזי $\mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q})$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה סופית ויהי $f \in \mathbb{K}[x]$ אי-פריק באשר $\gcd(\deg(f), [\mathbb{L} : \mathbb{K}]) = 1$ אזי f אי-פריק מעל $\mathbb{L}[x]$.

סגור אלגברי בשדה: תהא \mathbb{L}/\mathbb{K} הרחבה אזי $\overline{\mathbb{K}_{\mathbb{L}}} = \{\alpha \in \mathbb{L} \mid \mathbb{K} \text{ אלגברי מעל } \alpha\}$.

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

טענה: יהי \mathbb{F} שדה אזי $|\mathbb{F}[x]| = \max\{|\mathbb{F}|, \aleph_0\}$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה אלגברית אזי $|\mathbb{L}| \leq \max\{|\mathbb{K}|, \aleph_0\}$.

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

טענה המשפט היסודי של האלגברה: \mathbb{C} שדה סגור אלגברית.

הרחבה סגורה אלגברית: הרחבה אלגברית \mathbb{L}/\mathbb{K} באשר \mathbb{L} סגור אלגברית.

פולינום מתפרק לגורמים לינאריים: יהי \mathbb{K} שדה אזי $f \in \mathbb{K}[x]$ עבורו קיימים $\alpha_0, \alpha_1 \dots \alpha_n \in \mathbb{K}$ המקיימים $f = \alpha_0 \cdot \prod_{i=1}^n (x - \alpha_i)$.

טענה: יהי \mathbb{K} שדה סגור אלגברית ויהי $f \in \mathbb{K}[x] \setminus \{0\}$ אזי f מתפרק לגורמים לינאריים.

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

למה: יהי \mathbb{K} שדה סגור אלגברית ותהא \mathbb{L}/\mathbb{K} הרחבה אלגברית אזי $\mathbb{L} = \mathbb{K}$.

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

למה: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x] \setminus \{0\}$ אזי קיימת הרחבה סופית \mathbb{L}/\mathbb{K} עבורה קיימים $\alpha_0, \alpha_1 \dots \alpha_n \in \mathbb{L}$ המקיימים

$$f = \alpha_0 \cdot \prod_{i=1}^n (x - \alpha_i)$$

מסקנה: יהי \mathbb{K} שדה ויהיו $f_1 \dots f_m \in \mathbb{K}[x] \setminus \{0\}$ אזי קיימת הרחבה סופית \mathbb{L}/\mathbb{K} עבורה קיימת $\alpha \in M_{m \times (n+1)}(\mathbb{L})$ המקיימת

$$f_j = \alpha_{j,1} \cdot \prod_{i=1}^n (x - \alpha_{j,i+1}) \quad \text{לכל } j \in [m]$$

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

$$\text{sols}_{\mathbb{L}}(f_\tau) \neq \emptyset \quad \text{לכל } \tau \in \mathcal{T}$$

משפט: יהי \mathbb{K} שדה אזי קיימת הרחבה סגורה אלגברית \mathbb{L}/\mathbb{K} .

משפט שטייניץ: תהא \mathbb{L}/\mathbb{K} הרחבה אלגברית יהי \mathbb{F} שדה סגור אלגברית ויהי $\nu: \mathbb{K} \hookrightarrow \mathbb{F}$ אזי קיים מונומורפיזם $\Phi: \mathbb{L} \hookrightarrow \mathbb{F}$ המקיים

$$\Phi|_{\mathbb{K}} = \nu \quad \text{דורש AC}$$

מסקנה: תהינה $\mathbb{F}/\mathbb{K}, \mathbb{L}/\mathbb{K}$ הרחבות סגורות אלגבריות אזי $\mathbb{F}/\mathbb{K} \simeq \mathbb{L}/\mathbb{K}$.

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

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

טענה: $\overline{\mathbb{Q}} = \mathbb{Q}$.

טענה: $|\overline{\mathbb{Q}}| = \aleph_0$.

טענה: יהי \mathbb{F} שדה אינסופי אזי \mathbb{F}^\times אינה ציקלית.

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

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

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

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

מסקנה: יהי \mathbb{K} שדה יהי $\varphi: \mathbb{K}(x)/\mathbb{K} \rightarrow \mathbb{K}(x)/\mathbb{K}$ אוטומורפיזם ויהי $a \in \mathbb{K}(x)$ אזי $\deg(a) = \deg(\varphi(a))$.

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

משפט לורות': יהיו \mathbb{L}, \mathbb{K} שדות באשר \mathbb{L}/\mathbb{K} הרחבה לא טריוואלית וכן $\mathbb{K}(x)/\mathbb{L}$ הרחבה טרנסצנדנטית פשוטה.

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

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

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

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

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

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

קבוצה בלתי תלויה אלגברית/טרנסצנדנטית בלתי תלויים אלגברית זה בזה (בת"א): תהא \mathbb{L}/\mathbb{K} הרחבה אזי $u_1 \dots u_m \in \mathbb{L}$ עבורם לכל $f \in \mathbb{K}[x_1 \dots x_m]$ 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.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת שדות ותהא $S \subseteq \mathbb{L}$ באשר $\mathbb{L} = \mathbb{K}(S)$ אזי קיים בסיס טרנסצנדנטי \mathcal{B} של \mathbb{L}/\mathbb{K} המקיים $\mathcal{B} \subseteq S$.

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 אלגברית: תהא \mathbb{L}/\mathbb{K} הרחבה אזי $A, B \subseteq \mathbb{L}$ עבורן לכל $\alpha \in A$ מתקיים כי α אלגברי מעל $\mathbb{K}(B)$ וכן לכל $\beta \in B$ מתקיים כי β 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 L/K הרחבה ויהי $A, B \subseteq L$ בסיסים טרנסצנדנטיים של L/K אזי $|A| = |B|$.

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

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

טענה: $\overline{C(x)} \simeq C$.

טענה: קיים שדה $K \subseteq C$ באשר $K \simeq R$ וכן $K \neq R$.

טענה: $Aut(R/Q) = \{e\}$ וכן $|Aut(C/Q)| = 2^{2^{\aleph_0}}$.

שדה קומפוזיט: יהי L שדה ויהי $F, K \subseteq L$ שדות אזי השדה המינימלי $E \subseteq L$ המקיים $F, K \subseteq E$.

סימון: יהי L שדה יהיו $F, K \subseteq L$ ויהי E שדה קומפוזיט של F, K אזי $F \cdot K = E$.

טענה: תהא L/K הרחבת שדות באשר $\deg_{tr_K}(K) < \aleph_0$ ויהיו $F, E \subseteq L$ שדות באשר $K \subseteq F$ וכן $K \subseteq E$ אזי $\deg_{tr_K}(FE) \leq \deg_{tr_K}(F) + \deg_{tr_K}(E)$.

שדה פיצול: יהי K שדה ויהי $f \in K[x]$ באשר $\deg(f) \geq 1$ אזי שדה F באשר $K \subseteq F$ וכן f מתפרק לגורמים לינאריים מעל F וכן

לכל שדה $L \subset F$ מתקיים כי f אינו מתפרק לגורמים לינאריים מעל $L[x]$.

משפט: יהי K שדה ויהי $f \in K[x]$ אזי קיים f -שדה פיצול וכן לכל שדות פיצול F, L של F, L מתקיים $F/K \simeq L/K$.

טענה: יהי $n \in \mathbb{N}_+$ ויהי $p \in \mathbb{P}$ אזי קיים ויחיד שדה F באשר $|F| = p^n$.

טענה: יהי $n \in \mathbb{N}_+$ ויהי $p \in \mathbb{P}$ אזי $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$.

הרחבה ריבועית: יהי K שדה יהי $f \in K[x]$ באשר $\deg(f) = 2$ ויהי L שדה הפיצול של f אזי L/K .

טענה: תהא L/K הרחבה ריבועית באשר $L \neq K$ אזי $[L : K] = 2$.

הרחבה נורמלית: הרחבה אלגברית L/K עבורה לכל פולינום אי-פריק $f \in K[x]$ מתקיים כי אם $\text{sols}_L(f) \neq \emptyset$ אז f מתפרק

לגורמים לינאריים מעל $L[x]$.

משפט: תהא L/K הרחבה סופית באשר \overline{K}/L הרחבה אזי התב"ש

• L/K הרחבה נורמלית.

• קיים $f \in K[x]$ עבורו L שדה הפיצול של f .

• לכל הרחבה \overline{K}/F אם $F/K \simeq L/K$ אז $F = L$.

• לכל אוטומורפיזם $\nu : \overline{K}/K \rightarrow \overline{K}/K$ מתקיים $\nu(L) = L$.

מסקנה: תהא L/K הרחבה נורמלית ויהי $F \subseteq L$ שדה באשר $K \subseteq F$ אזי L/F הרחבה נורמלית.

מסקנה: תהא L/K הרחבה סופית אזי קיימת הרחבה סופית נורמלית F/K עבורה $L \subset F$.

מסקנה: יהי K שדה ויהי $F, L \subseteq \overline{K}$ שדות באשר $K \subseteq F$ וכן $K \subseteq L$ וכן $F/K, L/K$ הרחבות נורמליות אזי $(L \cdot F)/K$ הרחבה

נורמלית וכן $(L \cap F)/K$ הרחבה נורמלית.

מסקנה: תהא L/K הרחבה מדרגה 2 אזי L/K הרחבה נורמלית.

מסקנה: יהי F שדה סופי ותהא L/F הרחבה סופית אזי L/F הרחבה נורמלית.

טענה: תהא L/K הרחבה אלגברית אזי $(L/K \text{ נורמלית}) \iff (\forall \alpha \in L \text{ הפולינום } f_\alpha \text{ מתפרק לגורמים לינאריים מעל } L[x])$.

טענה: תהא L/K הרחבה ויהי $f, g \in K[x]$ אזי $(f, g \text{ זרים מעל } K[x]) \iff (f, g \text{ זרים מעל } L[x])$.

טענה: תהא L/K הרחבה נורמלית יהי $f \in K[x]$ אי-פריק ויהיו $g, h \in L[x]$ אי-פריקים באשר $g, h \mid f$ מעל $L[x]$ אזי

$\deg(g) = \deg(h)$.

פולינום ספרבילי: יהי K שדה אזי $f \in K[x]$ באשר f בעל שורשים פשוטים מעל $\overline{K}[x]$.

פולינום אי-ספרבילי טהור: יהי K שדה אזי $f \in K[x]$ באשר f בעל שורש יחיד מעל $\overline{K}[x]$.

איבר ספרבילי מעל שדה: תהא L/K הרחבה אלגברית אזי $\alpha \in L$ עבורו f_α ספרבילי.

הרחבה ספרבילית: הרחבה אלגברית L/K עבורה לכל $\alpha \in L$ מתקיים כי α ספרבילי מעל K .

מסקנה: תהא L/K הרחבה אלגברית יהי $\alpha \in L$ ספרבילי מעל K ותהא $F \subseteq L$ באשר $K \subseteq F$ אזי α ספרבילי מעל F .

מסקנה: תהא L/K הרחבה אלגברית באשר $\text{char}(K) = 0$ אזי L/K הרחבה ספרבילית.

מסקנה: יהי $p \in \mathbb{P}$ תהא L/K הרחבה אלגברית באשר $\text{char}(K) = p$ ויהי $\alpha \in L$ אזי f_α בעל שורש מרובה \iff (קיים $g \in K[x]$

עבורו $f_\alpha(x) = g(x^p)$).

משפט: יהי $n \in \mathbb{N}$ ותהא L/K הרחבה סופית אזי

• $|L \hookrightarrow \overline{K}| \leq [L : K]$.

• $(|L \hookrightarrow \overline{K}| = [L : K]) \iff (L/K \text{ ספרבילית})$.

מסקנה: תהא \mathbb{L}/\mathbb{K} הרחבה סופית ויהי $\mathbb{F} \subseteq \mathbb{L}$ שדה באשר $\mathbb{K} \subseteq \mathbb{F}$ אזי $(\mathbb{L}/\mathbb{K}) \iff (\mathbb{L}/\mathbb{F}, \mathbb{F}/\mathbb{K})$ ספרביליות).

מסקנה: יהיו $\alpha_1 \dots \alpha_m \in \overline{\mathbb{K}}$ אזי $(\mathbb{K}(\alpha_1 \dots \alpha_m)/\mathbb{K}) \iff (\alpha_1 \dots \alpha_m)$ ספרביליים מעל \mathbb{K} .

מסקנה: יהי \mathbb{K} שדה ותהיינה $\mathbb{L}/\mathbb{K}, \mathbb{F}/\mathbb{K}$ הרחבות ספרביליות אזי $(\mathbb{L} \cdot \mathbb{F})/\mathbb{K}$ ספרבילית.

מסקנה סגור ספרבילי בשדה: תהא \mathbb{L}/\mathbb{K} הרחבה אזי $\{\alpha \in \mathbb{L} \mid \mathbb{K} \text{ ספרבילי מעל } \alpha\}$ שדה.

סגור ספרבילי: יהי \mathbb{K} שדה אזי $\overline{\mathbb{K}}_s = \{\alpha \in \overline{\mathbb{K}} \mid \mathbb{K} \text{ ספרבילי מעל } \alpha\}$.

טענה: יהי $p \in \mathbb{P}$ תהא \mathbb{L}/\mathbb{K} הרחבה אלגברית באשר $\text{char}(\mathbb{K}) = p$ ויהי $\alpha \in \mathbb{L}$ אזי קיים $r \in \mathbb{N}$ עבורו α^{p^r} ספרבילי מעל \mathbb{K} .

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה סופית באשר $[\mathbb{L} : \mathbb{K}] \nmid \text{char}(\mathbb{K})$ אזי \mathbb{L}/\mathbb{K} ספרבילית.

שדה משוכלל: שדה \mathbb{K} עבורו לכל הרחבה \mathbb{L}/\mathbb{K} מתקיים כי \mathbb{L} ספרבילי.

משפט: יהי \mathbb{K} שדה ויהי $p \in \mathbb{P}$ אזי

• אם $\text{char}(\mathbb{K}) = 0$ אז \mathbb{K} שדה משוכלל.

• אם $\text{char}(\mathbb{K}) = p$ אז $(\mathbb{K} \text{ שדה משוכלל}) \iff (\text{לכל } \alpha \in \mathbb{K} \text{ קיים } \beta \in \mathbb{K} \text{ עבורו } \beta^p = \alpha)$.

מסקנה: יהי \mathbb{F} שדה סופי אזי \mathbb{F} שדה משוכלל.

טענה: יהי $p \in \mathbb{P}$ ויהי \mathbb{F} שדה באשר $\text{char}(\mathbb{F}) = p$ אזי $\bigcap_{i=0}^{\infty} \mathbb{F}^{p^i}$ שדה משוכלל.

איבר פרימיטיבי: תהא \mathbb{L}/\mathbb{K} הרחבה אזי $\alpha \in \mathbb{L}$ עבורו $\mathbb{L} = \mathbb{K}(\alpha)$.

משפט האיבר הפרימיטיבי: יהי \mathbb{K} שדה אינסופי ותהא \mathbb{L}/\mathbb{K} הרחבה סופית ספרבילית אזי קיים $\alpha \in \mathbb{L}$ עבורו $\mathbb{L} = \mathbb{K}(\alpha)$.

למה: יהי \mathbb{K} שדה ותהא $G \subseteq \mathbb{K}^\times$ חבורה סופית אזי G ציקלית.

מסקנה: יהי \mathbb{F} שדה סופי אזי \mathbb{F}^\times ציקלית.

משפט האיבר הפרימיטיבי: יהי \mathbb{K} שדה סופי ותהא \mathbb{L}/\mathbb{K} הרחבה סופית אזי קיים $\alpha \in \mathbb{L}$ עבורו $\mathbb{L} = \mathbb{K}(\alpha)$.

טענה: יהי $p \in \mathbb{P}$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ אזי $(x^n - 1)$ ספרבילי מעל $\mathbb{K}[x]$ $\iff (p \nmid n)$.

שורשי היחידה: יהי $p \in \mathbb{P}$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ באשר $\gcd(n, p) = 1$ אזי $\mu_n = \text{sols}_{\overline{\mathbb{K}}}(x^n - 1)$.

טענה: יהי $p \in \mathbb{P}$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ באשר $\gcd(n, p) = 1$ אזי μ_n חבורה ציקלית.

שורש יחידה פרימיטיבי: יהי $p \in \mathbb{P}$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ באשר $\gcd(n, p) = 1$ אזי $g \in \mu_n$ באשר g יוצר

של μ_n .

טענה: תהא $\mathbb{K}(\alpha)/\mathbb{K}$ הרחבה פשוטה ויהי $f_\alpha \in \mathbb{K}[x]$ הפולינום המינימלי של α אזי $|\text{Aut}(\mathbb{L}/\mathbb{K})| = |\text{sols}_{\mathbb{K}(\alpha)}(f_\alpha)|$.

הרחבת גלואה: הרחבה סופית \mathbb{L}/\mathbb{K} באשר \mathbb{L}/\mathbb{K} נורמלית וספרבילית.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהי $\mathbb{F} \subseteq \mathbb{L}$ שדה באשר $\mathbb{K} \subseteq \mathbb{F}$ אזי \mathbb{L}/\mathbb{F} הרחבת גלואה.

טענה: יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = 0$ יהי $f \in \mathbb{K}[x]$ ויהי \mathbb{F} שדה פיצול של f אזי \mathbb{F}/\mathbb{K} הרחבת גלואה.

טענה: יהי \mathbb{F} שדה סופי ויהי \mathbb{L} שדה באשר \mathbb{L}/\mathbb{F} הרחבה סופית אזי \mathbb{L}/\mathbb{F} הרחבת גלואה.

משפט: תהא \mathbb{F}/\mathbb{K} הרחבה סופית ספרבילית אזי קיימת הרחבת גלואה \mathbb{L}/\mathbb{K} עבורה קיים הומומורפיזם $\nu : \mathbb{F}/\mathbb{K} \rightarrow \mathbb{L}/\mathbb{K}$.

חבורת גלואה של הרחבת גלואה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $\text{Gal}(\mathbb{L}/\mathbb{K}) = \text{Aut}(\mathbb{L}/\mathbb{K})$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $\text{Gal}(\mathbb{L}/\mathbb{K})$ חבורה.

סימון: יהי \mathbb{L} שדה יהי $a \in \mathbb{L}$ ויהי $\sigma \in \text{Aut}(\mathbb{L})$ אזי $a^\sigma = \sigma(a)$.

פעולת גלואה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי נגדיר $\text{GA} : \text{Gal}(\mathbb{L}/\mathbb{K}) \times \mathbb{L} \rightarrow \mathbb{L}$ כך $\text{GA}(\sigma, \alpha) = \alpha^\sigma$.

למה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $\text{GA} \in \text{Gal}(\mathbb{L}/\mathbb{K}) \curvearrowright \mathbb{L}$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה יהי $\alpha \in \mathbb{L}$ ונגדיר $f \in \mathbb{L}[x]$ כך $f(x) = \prod_{\beta \in \text{Orb}(\alpha)} (x - \beta)$ אזי $f \in \mathbb{K}[x]$ וכן f אי־פריק מעל

$\mathbb{K}[x]$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהי $\mathbb{F} \subseteq \mathbb{L}$ שדה באשר $\mathbb{K} \subseteq \mathbb{F}$ אזי $\text{Gal}(\mathbb{L}/\mathbb{F}) \leq \text{Gal}(\mathbb{L}/\mathbb{K})$.

משפט: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $[\text{Gal}(\mathbb{L}/\mathbb{K})] = [\mathbb{L} : \mathbb{K}]$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבה סופית אזי $([\mathbb{L} : \mathbb{K}] = |\text{Aut}(\mathbb{L}/\mathbb{K})|) \iff (\mathbb{L}/\mathbb{K} \text{ הרחבת גלואה})$.

שדה אינבריאנטים/שימורים של שדה ביחס לחבורה: יהי \mathbb{L} שדה ותהא $H \leq \text{Aut}(\mathbb{L})$ תת־חבורה אזי

$\mathbb{L}^H = \{a \in \mathbb{L} \mid \forall h \in H. a^h = a\}$.

משפט: יהי \mathbb{L} שדה ותהא $H \leq \text{Aut}(\mathbb{L})$ תת־חבורה סופית אזי \mathbb{L}/\mathbb{L}^H הרחבה גלואה וכן $\text{Gal}(\mathbb{L}/\mathbb{L}^H) = H$.

מסקנה: תהא \mathbb{L}/\mathbb{K} הרחבה גלואה ותהא $H \leq \text{Gal}(\mathbb{L}/\mathbb{K})$ תת־חבורה אזי $[\mathbb{L}^H : \mathbb{K}] = [\text{Gal}(\mathbb{L}/\mathbb{K}) : H]$.

מסקנה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $\mathbb{L}^{\text{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$.

טענה: יהי $q \in \mathbb{P}$ ויהי $n \in \mathbb{N}_+$ אזי $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ חבורה ציקלית וכן Fr_p יוצר של $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

טענה: תהא $G = \text{Gal}(\mathbb{L}/\mathbb{K})$ חבורה סופית אזי קיימת הרחבת גלואה \mathbb{L}/\mathbb{K} עבורה $G = \text{Gal}(\mathbb{L}/\mathbb{K})$.

טענה המשפט היסודי של תורת גלואה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה אזי $|\{H \mid H \leq \text{Gal}(\mathbb{L}/\mathbb{K})\}| = |\{\mathbb{F} \mid (\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}) \wedge (\mathbb{F} \text{ שדה})\}|$.

מסקנה: יהי \mathbb{L} שדה ותהיינה $H, G \leq \text{Aut}(\mathbb{L})$ אזי $(\mathbb{L}^G \subseteq \mathbb{L}^H) \iff (H \subseteq G)$.

מסקנה: יהי \mathbb{L} שדה ויהיו $\mathbb{F}, \mathbb{K} \subseteq \mathbb{L}$ שדות אזי $(\text{Gal}(\mathbb{L}/\mathbb{K}) \subseteq \text{Gal}(\mathbb{L}/\mathbb{F})) \iff (\mathbb{F} \subseteq \mathbb{K})$.

מסקנה: תהא \mathbb{L}/\mathbb{K} הרחבה ספרבילית סופית אזי $|\{\mathbb{F} \mid (\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}) \wedge (\mathbb{F} \text{ שדה})\}| \in \mathbb{N}$.

מסקנה: $\{\mathbb{F} \mid (\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}) \wedge (\mathbb{F}/\mathbb{K} \text{ הרחבה אלגברית})\} = \{\mathbb{C}\}$.

משפט: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהיו $\mathbb{F}, \mathbb{E} \subseteq \mathbb{L}$ שדות באשר $\mathbb{K} \subseteq \mathbb{F}, \mathbb{E}$ אזי $(\text{Gal}(\mathbb{L}/\mathbb{F}), \text{Gal}(\mathbb{L}/\mathbb{E})) \iff (\mathbb{F}/\mathbb{K} \simeq \mathbb{E}/\mathbb{K})$ צמודות ב- $(\text{Gal}(\mathbb{L}/\mathbb{K}))$.

משפט: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהי $\mathbb{F} \subseteq \mathbb{L}$ שדה באשר $\mathbb{K} \subseteq \mathbb{F}$ אזי

• $(\text{Gal}(\mathbb{L}/\mathbb{F}) \trianglelefteq \text{Gal}(\mathbb{L}/\mathbb{K})) \iff (\mathbb{F}/\mathbb{K} \text{ הרחבת גלואה})$.

• אם \mathbb{F}/\mathbb{K} הרחבת גלואה אז $\text{Gal}(\mathbb{F}/\mathbb{K}) \simeq \text{Gal}(\mathbb{L}/\mathbb{K})/\text{Gal}(\mathbb{L}/\mathbb{F})$.

טענה: יהי \mathbb{K} שדה יהי $f \in \mathbb{K}[x]$ בעל שורשים פשוטים ויהי \mathbb{L} שדה הפיצול של f אזי \mathbb{L}/\mathbb{K} הרחבת גלואה.

חבורת גלואה של פולינום: יהי \mathbb{K} שדה יהי $f \in \mathbb{K}[x]$ בעל שורשים פשוטים ויהי \mathbb{L} שדה הפיצול של f אזי $\text{Gal}(f) = \text{Gal}(\mathbb{L}/\mathbb{K})$.

פעולת השורשים: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ בעל שורשים פשוטים אזי נגדיר $\text{RA} : \text{Gal}(f) \times \text{sols}_{\mathbb{K}}(f) \rightarrow \text{sols}_{\mathbb{K}}(f)$ כך $\text{RA}(\sigma, \alpha) = \sigma(\alpha)$.

למה: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ בעל שורשים פשוטים אזי $\text{RA} \in \text{Gal}(f) \curvearrowright \text{sols}_{\mathbb{K}}(f)$.

משפט: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ בעל שורשים פשוטים אזי $(\text{RA טרנזיטיבית}) \iff (f \text{ אי-פריק})$.

מסקנה: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ אי-פריק בעל שורשים פשוטים אזי $|\text{Gal}(f)| \mid \deg(f)!$ וכן $\deg(f) \mid |\text{Gal}(f)|$.

פולינום סימטרי אלמנטרי: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}_+$ ויהי $k \in [n]$ אזי $s_k \in \mathbb{K}[x_1 \dots x_n]$ המוגדר

$$s_k(x_1, \dots, x_n) = \sum_{a \in [n]^k} \prod_{i=1}^k x_{a_i}$$

טענה: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}_+$ ויהיו $\alpha_1 \dots \alpha_n \in \mathbb{K}$ אזי $x^n + \sum_{i=0}^{n-1} (-1)^{n-i} \cdot s_{n-i}(\alpha_1, \dots, \alpha_n) \cdot x^i$ אזי $\prod_{i=1}^n (x - \alpha_i) = x^n + \sum_{i=0}^{n-1} (-1)^{n-i} \cdot s_{n-i}(\alpha_1, \dots, \alpha_n) \cdot x^i$.

מסקנה: יהי \mathbb{K} שדה ויהיו $\alpha_1 \dots \alpha_n$ בת"א מעל \mathbb{K} אזי $\text{Gal}(\prod_{i=1}^n (x - \alpha_i)) \simeq S_n$.

משפט: יהי \mathbb{K} שדה ויהיו $\alpha_1 \dots \alpha_n$ בת"א מעל \mathbb{K} אזי $s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)$ בת"א מעל \mathbb{K} .

טענה: יהי $n \in \mathbb{N}_+$ ויהיו $z_1 \dots z_n \in \mathbb{C} \setminus \{0\}$ אזי $(\sum_{i=1}^n |z_i| = \sum_{i=1}^n |z_j|) \iff (i, j \in [n] \text{ לכל } \text{Arg}(z_i) = \text{Arg}(z_j))$.

מסקנה: יהיו $a_1 \dots a_n, d_1 \dots d_n \in \mathbb{N}_+$ אזי $\mathbb{Q}(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_n}) = \mathbb{Q}(\sqrt[n]{a_i})$.

טענה: יהי \mathbb{F} שדה סופי יהיו $\alpha, \beta \in \mathbb{F}^\times$ ויהי $c \in \mathbb{F}$ אזי קיימים $a, b \in \mathbb{F}$ עבורם $c = \alpha a^2 + \beta b^2$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהיו $\mathbb{F}, \mathbb{E} \subseteq \mathbb{L}$ שדות באשר $\mathbb{K} \subseteq \mathbb{F}$ וכן $\mathbb{K} \subseteq \mathbb{E}$ וכן \mathbb{F}/\mathbb{K} הרחבת גלואה אזי \mathbb{FE}/\mathbb{E} הרחבת גלואה וכן $[\mathbb{FE} : \mathbb{E}] = [\mathbb{F} : \mathbb{F} \cap \mathbb{E}]$.

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהיו $\mathbb{F}, \mathbb{E} \subseteq \mathbb{L}$ שדות באשר $\mathbb{K} \subseteq \mathbb{F}$ וכן $\mathbb{K} \subseteq \mathbb{E}$ וכן \mathbb{F}/\mathbb{K} הרחבת גלואה אזי

$$\text{Gal}(\mathbb{FE}/\mathbb{E}) \simeq \text{Gal}(\mathbb{E}/(\mathbb{E} \cap \mathbb{F}))$$

טענה: תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ויהיו $\mathbb{F}, \mathbb{E} \subseteq \mathbb{L}$ שדות באשר $\mathbb{K} \subseteq \mathbb{F}$ וכן $\mathbb{K} \subseteq \mathbb{E}$ וכן $\mathbb{F}/\mathbb{K}, \mathbb{E}/\mathbb{K}$ הרחבות גלואה וכן $\mathbb{E} \cap \mathbb{F} = \mathbb{K}$.

וכן $\mathbb{FE} = \mathbb{L}$ אזי $\text{Gal}(\mathbb{L}/\mathbb{K}) \simeq \text{Gal}(\mathbb{E}/\mathbb{K}) \times \text{Gal}(\mathbb{F}/\mathbb{K})$.

טענה: יהיו $p, q \in \mathbb{P}$ באשר $p < q$ תהא \mathbb{L}/\mathbb{K} הרחבת גלואה ממעלה pq ויהי $f \in \mathbb{K}[x]$ באשר $\deg(f) = p$ אזי \mathbb{L} אינו שדה פיצול של f .

טענה: יהי $p \in \mathbb{P}$ אזי $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

טענה: יהי $p \in \mathbb{P}$ ויהיו $d, n \in \mathbb{N}_+$ אזי $(\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}) \iff (d \mid n)$.

טענה: יהי $p \in \mathbb{P}$ ויהי $f \in \mathbb{F}_p[x]$ אי-פריק אזי $\mathbb{F}_{p^{\deg(f)}}$ הינו שדה הפיצול של f .

הגדרה: יהי $q \in \mathbb{P}$ באשר \mathbb{F}_q שדה אזי נגדיר $\pi_q : \mathbb{N}_+ \rightarrow \mathbb{N}$ כך $\pi_q(n) = |\{f \in \mathbb{F}_q[x] \mid (\deg(f) = n) \wedge (f \text{ מתוקן ואי-פריק})\}|$.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהי $n \in \mathbb{N}_+$ אזי $\pi_q(n) > 0$.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהי $n \in \mathbb{N}_+$ אזי $q^n = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} (d \cdot \pi_q(d))$.

פונקציית מוביוס: יהי $k \in \mathbb{N}$ יהי $p \in \mathbb{P}^k$ ויהי $e \in \mathbb{N}_+^k$ אזי נגדיר $\mu : \mathbb{N} \rightarrow \{0, \pm 1\}$ כך $\mu = \begin{cases} (-1)^k & \forall i \in [k], e_i = 1 \\ 0 & \text{else} \end{cases}$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\sum_{\substack{d \in \mathbb{N} \\ d \mid n}} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$.

טענה נוסחת ההיפוך של מוביוס: תהא $f : \mathbb{N}_+ \rightarrow \mathbb{C}$ ויהי $n \in \mathbb{N}_+$ אזי $f(n) = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} \left(\mu(d) \cdot \left(\sum_{\substack{a \in \mathbb{N} \\ a \mid \frac{n}{d}}} f(a) \right) \right)$.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהי $n \in \mathbb{N}_+$ אזי $\pi_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d$

משפט הפולינומים הראשוניים: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה אזי $\pi_q(n) \sim \frac{q^n}{n}$

שורשי היחידה: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}_+$ אזי $\text{sols}_{\mathbb{K}}(x^n - 1)$

שורש יחידה פרימיטיבי: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}_+$ אזי שורש יחידה g מסדר n באשר g יוצר של $\text{sols}_{\mathbb{K}}(x^n - 1)$

סימון: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}_+$ ויהי g שורש יחידה פרימיטיבי מסדר n אזי $\zeta_n = g$

הרחבת מעגל: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}_+$ אזי שדה הפיצול של $x^n - 1$ מעל \mathbb{K}

טענה: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}_+$ ותהא \mathbb{F}/\mathbb{K} הרחבת מעגל מסדר n אזי $\mathbb{K}(\zeta_n) = \mathbb{F}$

למה: יהי $p \in \mathbb{P}$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ אזי $\mathbb{K}(\zeta_n) = \mathbb{K}(\zeta_{\gcd(n,p)})$

למה: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}_+$ אזי $\mathbb{K}(\zeta_n)/\mathbb{K}$ הרחבת גלואה.

משפט: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}_+$ אזי

• $\text{Gal}(\mathbb{K}(\zeta_n)/\mathbb{K})$ אבלית.

• קיימת $H \leq (\mathbb{Z}_n)^\times$ עבורה $H \cong \text{Gal}(\mathbb{K}(\zeta_n)/\mathbb{K})$

• אם $n \in \mathbb{P}$ אז $\text{Gal}(\mathbb{K}(\zeta_n)/\mathbb{K})$ ציקלית.

הרחבת ציקלוטומית: יהי $n \in \mathbb{N}_+$ אזי $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

פולינום ציקלוטומי: יהי $n \in \mathbb{N}_+$ ויהי $f_{\zeta_n} \in \mathbb{Q}[x]$ הפולינום המינימלי של ζ_n מעל \mathbb{Q} אזי נגדיר כך $\Phi_n = f_{\zeta_n}$

טענה: יהי $n \in \mathbb{N}_+$ אזי $\Phi_n(x) = \prod_{\substack{i \in [n] \\ \gcd(i,n)=1}} (x - \zeta_n^i)$

טענה: יהי $p \in \mathbb{P}$ אזי $\frac{x^p-1}{x-1}$ אי-פריק מעל $\mathbb{Q}[x]$

טענה: יהי $p \in \mathbb{P}$ אזי $\Phi_p(x) = \frac{x^p-1}{x-1}$

טענה: יהיו $p_1 \dots p_k \in \mathbb{P}$ שונים ויהיו $e_1 \dots e_k \in \mathbb{N}_+$ אזי $\Phi_{\prod_{i=1}^k p_i^{e_i}}(x) = \Phi_{\prod_{i=1}^k p_i} \left(x^{\prod_{i=1}^k p_i^{e_i-1}} \right)$

טענה: יהי $n \in \mathbb{N}_+$ ויהי $p \in \mathbb{P}$ באשר $p \nmid n$ אזי $\Phi_{pn}(x) \Phi_n(x) = \Phi_n(x^p)$

טענה: יהי $n \in \mathbb{N}_+$ אזי $\Phi_n(0) = \begin{cases} -1 & n=1 \\ 1 & n>1 \end{cases}$

טענה: יהי $\{1\} \neq \text{odd}$ אזי $\Phi_{2m}(x) = \Phi_m(-x)$

משפט: יהי $n \in \mathbb{N}_+$ אזי $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

טענה: תהא \mathbb{K}/\mathbb{Q} הרחבת סופית באשר $\mathbb{K} \subseteq \mathbb{C}$ אזי $|\mathbb{K} \cap \{\zeta_n \mid n \in \mathbb{N}\}| < \aleph_0$

טענה: יהיו $n, m \in \mathbb{N}_+$ זרים אזי Φ_m אי-פריק מעל $\mathbb{Q}(\zeta_n)$

טענה: יהיו $n, m \in \mathbb{N}_+$ זרים אזי $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$

טענה: יהיו $n, m \in \mathbb{N}_+$ אזי $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}\left(\zeta_{\frac{nm}{\gcd(n,m)}}\right)$

טענה: יהיו זרים $n, m \in \mathbb{N}_+$ אזי $\text{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}(\zeta_n)) \simeq \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

טענה: יהיו זרים $n, m \in \mathbb{N}_+$ אזי $\text{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}) \simeq \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

טענה: יהיו $m, d \in \mathbb{N}$ ויהי $p \in \mathbb{P}$ באשר $p \nmid \Phi_d(m)$ וכן $p \nmid d$ אזי $p \equiv 1 \pmod d$

טענה: תהא G חבורה אבלית סופית אזי קיים שדה $\mathbb{L} \subseteq \mathbb{C}$ עבורו \mathbb{L}/\mathbb{Q} הרחבת גלואה וכן $\text{Gal}(\mathbb{L}/\mathbb{Q}) \simeq G$

טענה: יהי $n \in \mathbb{N}_+$ אזי $|\{\mathbb{K} \subseteq \mathbb{R} \mid \mathbb{K} \text{ שדה}\} \wedge (\mathbb{K}/\mathbb{Q} \text{ הרחבת גלואה}) \wedge (\text{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}_n)\}| \geq \aleph_0$

הגדרה: תהא $\Omega^{(0)} \subseteq \mathbb{C}$ אזי $\Omega^{(1)} = \{\text{line}_{a,b} \mid a, b \in \Omega^{(0)}\}$

הגדרה: תהא $\Omega^{(0)} \subseteq \mathbb{C}$ אזי $\Omega^{(2)} = \{\partial B_{\text{dist}(a,b)}(c) \mid a, b, c \in \Omega^{(0)}\}$

הגדרה: יהי $k \in \mathbb{N}$ אזי $\Omega_k^{(0)} = \{0, 1\}$ וכן $\Omega_{k+1}^{(0)} = \bigcup \left\{ S_1 \cap S_2 \mid S_1, S_2 \in \left(\Omega_k^{(1)} \cup \Omega_k^{(2)} \right) \right\}$

שדה המספרים הניתנים לבנייה בעזרת סרגל ומחוגה: $\mathbb{K}_{\text{sc}} = \bigcup_{k=0}^{\infty} \Omega_k^{(0)}$

סדרת הרחבות ריבועיות: יהי \mathbb{K} שדה ויהי $n \in \mathbb{N}$ אזי שדות $\mathbb{L}_1, \dots, \mathbb{L}_n$ עבורם \mathbb{L}_1/\mathbb{K} הרחבת ריבועית וכן $\mathbb{L}_{i+1}/\mathbb{L}_i$ הרחבת ריבועית

לכל $i \in [n-1]$

שדה נוצר מסדרת הרחבות ריבועיות: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}$ ותהא $\mathbb{L}_1, \dots, \mathbb{L}_n$ סדרת הרחבות ריבועיות של \mathbb{K} אזי \mathbb{L}_n

משפט: \mathbb{K}_{sc} שדה וכן \mathbb{L} שדה נוצר מסדרת הרחבות ריבועיות של \mathbb{Q} $\mathbb{K}_{\text{sc}} = \bigcup \{\mathbb{L} \mid \mathbb{L} \text{ שדה}\}$

מסקנה: יהי $a \in \mathbb{K}_{\text{sc}}$ אזי $\{\sqrt{a}, -\sqrt{a}\} \subseteq \mathbb{K}_{\text{sc}}$

מצולע משוכלל: יהי $n \in \mathbb{N}_{\geq 3}$ אזי $\{\zeta_n^0, \dots, \zeta_n^{n-1}\} \subseteq \text{RegPol}_n$

מסקנה: יהי $n \in \mathbb{N}_{\geq 3}$ אזי $(\text{RegPol}_n \subseteq \mathbb{K}_{\text{sc}}) \iff \langle \text{קיים שדה } \mathbb{L} \text{ הנוצר מסדרת הרחבות ריבועיות של } \mathbb{Q} \text{ עבורו } \zeta_n \in \mathbb{L} \rangle$

מסקנה: יהי $n \in \mathbb{N}_{\geq 3}$ באשר $\text{RegPol}_n \subseteq \mathbb{K}_{\text{sc}}$ אזי קיים $r \in \mathbb{N}$ עבורו $\varphi(n) = 2^r$

משפט: יהי $n \in \mathbb{N}_{\geq 3}$ אזי $(\text{RegPol}_n \subseteq \mathbb{K}_{\text{sc}}) \iff$ (קיימים $r, r_1 \dots r_k \in \mathbb{N}$ עבורם $2^{2^{r_i}} + 1 \in \mathbb{P}$ לכל $i \in [k]$ וכן $n = 2^r \cdot \prod_{i=1}^k p_i$).

מסקנה: יהי $\alpha \in (-\pi, \pi]$ אזי לא קיימים $a, b, c \in \mathbb{K}_{\text{sc}}$ עבורם $\angle_{\text{line}_{a,b}, \text{line}_{b,c}} = \frac{\alpha}{3}$.

הרחבה ציקלית: הרחבת גלואה \mathbb{L}/\mathbb{K} באשר $\text{Gal}(\mathbb{L}/\mathbb{K})$ ציקלית.

משפט: יהי $n \in \mathbb{N}_+$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = 0$ וכן $\zeta_n \in \mathbb{K}$ ויהי $a \in \mathbb{K}$ אזי $\text{Gal}(x^n - a)$ ציקלית וכן $|\text{ord}(\text{Gal}(x^n - a))| = n$.

מסקנה: יהי $n \in \mathbb{N}_+$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = 0$ וכן $\zeta_n \in \mathbb{K}$ ויהי $a \in \mathbb{K}^\times \setminus \{b^d \mid (b \in \mathbb{K}^\times) \wedge (d \in \mathbb{N}_{\geq 2}) \wedge (d|n)\}$ אזי $|\text{Gal}(x^n - a)| = n$.

משפט: יהי $p \in \mathbb{P}$ יהי $n \in \mathbb{N}_+$ באשר $\gcd(n, p) = 1$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ וכן $\zeta_n \in \mathbb{K}$ ויהי $a \in \mathbb{K}$ אזי $\text{Gal}(x^n - a)$ ציקלית וכן $|\text{ord}(\text{Gal}(x^n - a))| = n$.

מסקנה: יהי $p \in \mathbb{P}$ יהי $n \in \mathbb{N}_+$ באשר $\gcd(n, p) = 1$ יהי \mathbb{K} שדה באשר $\text{char}(\mathbb{K}) = p$ וכן $\zeta_n \in \mathbb{K}$ ויהי

$$|\text{Gal}(x^n - a)| = n \text{ אזי } a \in \mathbb{K}^\times \setminus \{b^d \mid (b \in \mathbb{K}^\times) \wedge (d \in \mathbb{N}_{\geq 2}) \wedge (d|n)\}.$$

מסקנה: תהא G חבורה ציקלית סופית אזי קיים $n \in \mathbb{N}_+$ וכן קיים שדה \mathbb{K} וכן קיים $a \in \mathbb{K}$ עבורם $G = \text{Gal}(x^n - a)$.

רזולבנט לגראנז': יהי $n \in \mathbb{N}_+$ תהא \mathbb{L}/\mathbb{K} הרחבה ציקלית מסדר n באשר $\zeta_n \in \mathbb{K}$ ויהי σ יוצר של $\text{Gal}(\mathbb{L}/\mathbb{K})$ אזי נגדיר $\mathcal{L} : \mathbb{L} \rightarrow \mathbb{L}$ כך $\mathcal{L}(\alpha) = \sum_{i=0}^{n-1} \zeta_n^{-i} \cdot \alpha^{\sigma^i}$.

למה: יהי $n \in \mathbb{N}_+$ תהא \mathbb{L}/\mathbb{K} הרחבה ציקלית מסדר n באשר $\zeta_n \in \mathbb{K}$ ויהי σ יוצר של $\text{Gal}(\mathbb{L}/\mathbb{K})$ אזי

- לכל $\alpha \in \mathbb{L}$ מתקיים $\mathcal{L}(\alpha)^\sigma = \zeta_n \cdot \mathcal{L}(\alpha)$.

- לכל $\alpha \in \mathbb{L}$ מתקיים $\mathcal{L}(\alpha)^n \in \mathbb{K}$.

- קיים $\alpha \in \mathbb{L}$ המקיים $\mathcal{L}(\alpha) \neq 0$.

משפט: יהי $n \in \mathbb{N}_+$ תהא \mathbb{L}/\mathbb{K} הרחבה ציקלית מסדר n באשר $\zeta_n \in \mathbb{K}$ אזי קיים $b \in \mathbb{K}^\times$ עבורו קיים $\beta \in \text{sols}_{\mathbb{L}}(x^n - b)$ המקיים $\mathbb{L} = \mathbb{K}(\beta)$.

הרחבה רדיקלית: הרחבה \mathbb{L}/\mathbb{K} עבורה קיים $k \in \mathbb{N}$ וקיימים $\mathbb{F}_0 \dots \mathbb{F}_k$ שדות המקיימים

- $\mathbb{L} = \mathbb{F}_k$ וכן $\mathbb{K} = \mathbb{F}_0$.

- לכל $i \in [k]$ קיים $n \in \mathbb{N}_+$ וכן קיים $a \in \mathbb{L}_i$ עבורם קיים $\alpha \in \text{sols}_{\mathbb{L}_i}(x^n - a)$ המקיים $\mathbb{L}_i = \mathbb{L}_{i-1}(\alpha)$.

משוואה פתירה ברדיקלים: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ עבורו קיימת הרחבה רדיקלית \mathbb{L}/\mathbb{K} המקיימת $\text{sols}_{\mathbb{K}}(f) \subseteq \mathbb{L}$ אזי $f = 0$.

משפט: תהא \mathbb{L}/\mathbb{K} הרחבה רדיקלית אזי קיים שדה $\mathbb{F} \subseteq \mathbb{L}$ עבורו \mathbb{F}/\mathbb{K} הרחבה נורמלית רדיקלית.

משפט: תהא \mathbb{L}/\mathbb{K} הרחבה נורמלית רדיקלית אזי $\text{Gal}(\mathbb{L}/\mathbb{K})$ פתירה.

משפט: יהי \mathbb{K} שדה ויהי $f \in \mathbb{K}[x]$ אזי $f = 0$ (פתירה ברדיקלים) $\iff \text{Gal}(f)$ פתירה.

מסקנה: יהי \mathbb{K} שדה יהי $n \in \mathbb{N}_+$ ויהיו $a_1 \dots a_n$ בת"א מעל \mathbb{K} אזי $x^n + \sum_{i=1}^n a_i x^i = 0$ (פתירה ברדיקלים) $\iff (n \leq 4)$.