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 אבלי/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 אבלי בעל יחידה וכן $\mathbb{Z}$ חוג אבלי בעל יחידה.

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

טענה: יהי R חוג אבלי בעל יחידה אזי $\langle R[x],+,\text{קונבולוציה}\rangle$ חוג אבלי בעל יחידה.

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

טענה: יהי R חוג אבלי בעל יחידה אזי $R[x_1\ldots x_{n+1}]=(R[x_1\ldots x_n])[x_{n+1}]$.

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

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

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

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

שדה: חוג אבלי בעל יחידה $\mathbb{F}$ המקיים $\mathbb{F}^\times=\mathbb{F}\backslash\{0\}$.

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

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 $(a,b),(c,d)\in R\times(R\backslash\{0\})$ 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 $\nu:R\to S$ 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 $\nu:R\to S$ המקיים $\nu(1_R)=1_S$.

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

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

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

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

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

למה: יהיו R,S חוגים ויהי $\nu:R\to S$ הומומורפיזם אזי (ν אפימורפיזם)$\Longleftrightarrow$($\text{Im}(\nu)=S$).

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

למה: יהיו R,S חוגים ויהי $\nu:R\to S$ הומומורפיזם אזי (ν איזומורפיזם)$\Longleftrightarrow$(ν מונומורפיזם וכן ν אפימורפיזם).

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

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

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

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

משפט: יהי R חוג אבלי בעל יחידה אזי (R שדה)$\Longleftrightarrow$(לכל אידאל $I\subseteq R$ מתקיים $I\in\{\{0\},R\}$).

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

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

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

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

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

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

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

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 אמיתי)$\iff(I \cap R^\times = \varnothing)$.

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.

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

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 אידאל ראשוני)$\iff$(R/I תחום שלמות).
- (I אידאל מקסימלי)$\iff$(R/I 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) מקסימלי)$\iff$((f) ראשוני)$\iff$(f אי־פריק ב־$\mathbb{K}[x]$).

מסקנה: יהי R תחום שלמות אזי ($R[x]$ תחום ראשי)$\iff$(R 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 $f_1 \ldots f_n, d \in \mathbb{K}[x]$ באשר $(f_1 \ldots f_n) = (d)$ וכן d מתוקן אזי $\gcd(f_1 \ldots f_n) = d$.

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 $\deg(r) < \deg(g)$ וכן $f = qg + r$.

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

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

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 אי־פריק)$\iff$(f אי־פריק מעל $\mathbb{Q}[x]$ וכן f פרימיטיבי).

טענה קריטריון אייזנשטיין: יהיו $a_0 \ldots a_n \in \mathbb{Z}$ 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 $a_0 \ldots a_n \in \mathbb{F}[x_1 \ldots x_m]$ ויהי $p \in \mathbb{F}[x_1 \ldots x_m]$ 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 $\mathbb{F}(x_1 \ldots x_m)[x]$.

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 $\operatorname{sols}_{\mathbb{K}}(f) = \{\alpha \in \mathbb{K} \mid f(\alpha) = 0\}$.

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

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

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

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

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

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

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

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.

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 $\nu_{\restriction_{\mathbb{F}}} = \mathrm{Id}_{\mathbb{F}}$.

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

טענה: יהי $\mathbb{F}$ שדה תהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות ויהי $\nu : \mathbb{K}/\mathbb{F} \to \mathbb{L}/\mathbb{F}$ 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 $\bigcap \{\mathbb{K} \subseteq \mathbb{F} \mid \text{שדה } \mathbb{K}\}$ שדה פשוט.

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 $\mathrm{char}(\mathbb{F}) = 0$.
- אם קיים $p \in \mathbb{P}$ עבורו $\mathbb{K} \simeq \mathbb{F}_p$ אז $\mathrm{char}(\mathbb{F}) = p$.

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

טענה: יהי $p \in \mathbb{P}$ ויהי $\mathbb{K}$ שדה המקיים $\mathrm{char}(\mathbb{K}) = p$ 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 $\mathrm{char}(\mathbb{K}) = p$ אזי נגדיר $\mathrm{Fr}_p : \mathbb{K} \to \mathbb{K}$ כך $\mathrm{Fr}_p(a) = a^p$.

משפט: יהי $p \in \mathbb{P}$ ויהי $\mathbb{K}$ שדה המקיים $\mathrm{char}(\mathbb{K}) = p$ אזי Fr_p מונומורפיזם.

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

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 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: $\mathbb{C}/\mathbb{R}$ 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 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 תהיינה $\mathbb{K}/\mathbb{F}, \mathbb{L}/\mathbb{F}$ הרחבות יהי $\nu : \mathbb{K}/\mathbb{F} \to \mathbb{L}/\mathbb{F}$ 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 באשר $A \subseteq B$ תהא $S \subseteq B$ ויהי $R \subseteq B$ החוג האבלי בעל יחידה המינימלי המקיים $A \cup S \subseteq R$ אזי 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 $A[S] = \bigcup_{n=1}^{\infty} \left\{ f(s_1 \ldots s_n) \;\middle|\; \begin{smallmatrix} f \in A[x_1 \ldots x_n] \\ s_1 \ldots s_n \in S \end{smallmatrix} \right\}$.

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 $\mathbb{K}(S) = \bigcup_{n=1}^{\infty} \bigcup_{f,g \in \mathbb{K}[x_1 \dots x_n]} \left\{ \frac{f(s_1 \dots s_n)}{g(s_1 \dots s_n)} \;\middle|\; \substack{s_1 \dots s_n \in S \\ g(s_1 \dots s_n) \neq 0} \right\}$.

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

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 α טרנסצנדנטי מעל $\mathbb{K}$ אז $\mathbb{K}(\alpha)/\mathbb{K} \simeq \mathbb{K}(x)/\mathbb{K}$.
- אם α אלגברי מעל $\mathbb{K}$ אז $\mathbb{K}(\alpha)/\mathbb{K} \simeq \left(\mathbb{K}[x]/(f_\alpha)\right)/\mathbb{K}$.

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 $\nu : \mathbb{K}(\alpha)/\mathbb{K} \to \mathbb{K}(\beta)/\mathbb{K}$ 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 $\left\{x^i + (f)\right\}_{i=0}^{n-1}$ בסיס של $\mathbb{F}[x]/(f)$.

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: תהיינה $\mathbb{F}/\mathbb{L}, \mathbb{L}/\mathbb{K}$ 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 (α אלגברי מעל $\mathbb{K}$)$\Longleftrightarrow$(קיים שדה $\mathbb{L} \subseteq \mathbb{F}$ 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 $\mathbb{L} \subseteq \mathbb{F}$ המקיים $\alpha_1 \dots \alpha_n \in \mathbb{F}$ וכן $\mathbb{F}/\mathbb{K}$ הרחבה סופית.

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

טענה: יהיו $p, q \in \mathbb{P}$ שונים אזי $\mathbb{Q}\left(\sqrt{q}\right) \not\simeq \mathbb{Q}\left(\sqrt{p}\right)$.

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

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

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

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 $|\mathbb{L}| \le \max\{|\mathbb{K}|, \aleph_0\}$.

שדה סגור אלגברית: שדה $\mathbb{K}$ עבורו לכל $f \in \mathbb{K}[x]$ באשר $\deg(f) \ge 1$ 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 $\deg(f) \ge 1$ אזי קיימת הרחבה סופית $\mathbb{L}/\mathbb{K}$ המקיימת $\mathrm{sols}_{\mathbb{L}}(f) \neq \varnothing$.

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 $f_j = \alpha_{j,1} \cdot \prod_{i=1}^{n} (x - \alpha_{j,i+1})$ 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 $\deg(f_\tau) \ge 1$ לכל $\tau \in \mathcal{T}$ אזי קיימת הרחבה אלגברית $\mathbb{L}/\mathbb{K}$ המקיימת $\mathrm{sols}_{\mathbb{L}}(f_\tau) \neq \varnothing$ 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 $\Phi_{\restriction_{\mathbb{K}}} = \nu$. דורש AC

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

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 $\nu:\mathbb{L}/\mathbb{K}\to\overline{\mathbb{K}}/\mathbb{K}$.

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

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

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

משפט: יהי $\mathbb{K}$ שדה ותהא $a\in\mathbb{K}\left(x\right)$ באשר $\deg\left(a\right)\ge1$ אזי a טרנסצנדנטי מעל $\mathbb{K}$ וכן $\mathbb{K}\left(x\right)/\mathbb{K}\left(a\right)$ הרחבה אלגברית מדרגה $\deg\left(a\right)$.

מסקנה: יהי $\mathbb{K}$ שדה ותהא $a\in\mathbb{K}\left(a\right)$ אזי $(\mathbb{K}\left(x\right)=\mathbb{K}\left(a\right))\Longleftrightarrow$(קיימים $\alpha,\beta,\gamma,\delta\in\mathbb{K}$ המקיימים $\alpha\delta-\beta\gamma\ne0$ וכן $a=\frac{\alpha x+\beta}{\gamma x+\delta}$).

מסקנה: יהי $\mathbb{K}$ שדה אזי $\mathrm{Aut}\left(\mathbb{K}\left(x\right)\right)=\left\{ \frac{\alpha x+\beta}{\gamma x+\delta}\;\middle|\;\left(\alpha,\beta,\gamma,\delta\in\mathbb{K}\right)\wedge\left(\alpha\delta-\beta\gamma\ne0\right)\right\}$.

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

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

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

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

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

איבר תלוי אלגברית מעל שדה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $u_{1}\ldots u_{m}\in\mathbb{L}$ אזי $v\in\mathbb{L}$ באשר v אלגברי מעל $\mathbb{K}\left(u_{1}\ldots u_{m}\right)$.

איבר בלתי תלוי אלגברית מעל שדה (בת"א): תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $u_{1}\ldots u_{m}\in\mathbb{L}$ אזי $v\in\mathbb{L}$ באשר v אינו תלוי אלגברית ב־$u_{1}\ldots u_{m}$ מעל $\mathbb{K}$.

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

למה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה יהיו $u_{1}\ldots u_{m},v_{1}\ldots v_{n},w\in\mathbb{L}$ באשר w תלוי אלגברית ב־$v_{1}\ldots v_{n}$ מעל $\mathbb{K}$ וכן v_{j} תלוי אלגברית ב־$u_{1}\ldots u_{m}$ מעל $\mathbb{K}$ לכל $j\in\left[n\right]$ אזי w תלוי אלגברית ב־$u_{1}\ldots u_{m}$ מעל $\mathbb{K}$.

קבוצה בלתי תלויה אלגברית/טרנסצנדנטיים בלתי תלויים אלגברית זה בזה (בת"א): תהא $\mathbb{L}/\mathbb{K}$ הרחבה אזי $u_{1}\ldots u_{m}\in\mathbb{L}$ עבורם לכל $f\in\mathbb{K}\left[x_{1}\ldots x_{m}\right]$ מתקיים כי אם $f\left(u_{1}\ldots u_{m}\right)=0$ אז $f=0$.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $u_{1}\ldots u_{m}\in\mathbb{L}$ בת"א מעל $\mathbb{K}$ אזי $\mathbb{K}\left(u_{1}\ldots u_{m}\right)\simeq\mathbb{K}\left(x_{1}\ldots x_{m}\right)$.

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 $f\in\mathbb{K}\left[x_{1},\ldots,x_{\left|S\right|}\right]$ מתקיים כי אם $f\left(S\right)=0$ אז $f=0$.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה תהא $\mathcal{I}$ קבוצה ותהא $\left\{ u_{\alpha}\right\} _{\alpha\in\mathcal{I}}\subseteq\mathbb{L}$ בת"א מעל $\mathbb{K}$ אזי $\mathbb{K}\left(\left\{ u_{\alpha}\right\} _{\alpha\in\mathcal{I}}\right)\simeq\mathbb{K}\left(\left\{ x_{\alpha}\right\} _{\alpha\in\mathcal{I}}\right)$.

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 $\mathcal{B}\not\subset\mathcal{A}$.

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 $\mathbb{L}/\mathbb{K}\simeq\mathbb{K}\left(\left\{ x_{\alpha}\right\} _{\alpha\in\mathcal{I}}\right)/\mathbb{K}$.

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 $\mathbb{K}\left(B\right)$ וכן לכל $\beta\in B$ מתקיים כי β אלגברי מעל $\mathbb{K}\left(A\right)$.

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 ותהיינה $A,B\subseteq\mathbb{L}$ 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 $a_{1}\ldots a_{r},b_{1}\ldots b_{s}\in\mathbb{L}$ באשר $\left\{ b_{1}\ldots b_{s}\right\}$ בת"א מעל $\mathbb{K}$ וכן b_{j} תלוי אלגברית ב־$a_{1}\ldots a_{r}$ מעל $\mathbb{K}$ לכל $j\in\left[s\right]$ אזי $s\le r$ וכן קיימת $S\subseteq\left\{ a_{1}\ldots a_{r}\right\}$ באשר $\left|S\right|=s$ עבורה $\left\{ a_{1}\ldots a_{r},b_{1}\ldots b_{s}\right\} \backslash S$ שקולה אלגברית ל־$\left\{ a_{1}\ldots a_{r}\right\}$ מעל $\mathbb{K}$.

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

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

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

משפט: תהיינה $\mathbb{F}/\mathbb{K},\mathbb{L}/\mathbb{F}$ הרחבות אזי $\text{degtr}_{\mathbb{K}}(\mathbb{L})=\text{degtr}_{\mathbb{K}}(\mathbb{F})+\text{degtr}_{\mathbb{F}}(\mathbb{L})$.

טענה: $\overline{\mathbb{C}(x)}\simeq\mathbb{C}$.

שדה פיצול: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ באשר $\deg(f)\geq1$ אזי שדה $\mathbb{F}$ באשר $\mathbb{K}\subseteq\mathbb{F}$ וכן f מתפרק לגורמים לינאריים מעל $\mathbb{F}$ וכן לכל שדה $\mathbb{L}\subset\mathbb{F}$ מתקיים כי f אינו מתפרק לגורמים לינאריים מעל $\mathbb{L}[x]$.

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

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

הרחבה נורמלית: הרחבה אלגברית $\mathbb{L}/\mathbb{K}$ עבורה לכל פולינום אי־פריק $f\in\mathbb{K}[x]$ מתקיים כי אם $\text{sols}_{\mathbb{L}}(f)\neq\varnothing$ אז f מתפרק לגורמים לינאריים מעל $\mathbb{L}[x]$.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית באשר $\overline{\mathbb{K}}/\mathbb{L}$ הרחבה אזי התב"ש
- $\mathbb{L}/\mathbb{K}$ הרחבה נורמלית.
- קיים $f\in\mathbb{K}[x]$ עבורו $\mathbb{L}$ שדה הפיצול של f.
- לכל הרחבה $\overline{\mathbb{K}}/\mathbb{F}$ אם $\mathbb{L}/\mathbb{K}\simeq\mathbb{F}/\mathbb{K}$ אז $\mathbb{F}=\mathbb{L}$.
- לכל אוטומורפיזם $\nu:\overline{\mathbb{K}}/\mathbb{K}\to\overline{\mathbb{K}}/\mathbb{K}$ מתקיים $\nu(\mathbb{L})=\mathbb{L}$.

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

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

שדה קומפוזיט: יהי $\mathbb{L}$ שדה ויהיו $\mathbb{F},\mathbb{K}\subseteq\mathbb{L}$ שדות אזי השדה המינימלי $\mathbb{E}\subseteq\mathbb{L}$ המקיים $\mathbb{F},\mathbb{K}\subseteq\mathbb{E}$.

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

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

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה מדרגה 2 אזי $\mathbb{L}/\mathbb{K}$ הרחבה נורמלית.

מסקנה: יהי $\mathbb{F}$ שדה סופי ותהא $\mathbb{L}/\mathbb{F}$ הרחבה סופית אזי $\mathbb{L}/\mathbb{F}$ הרחבה נורמלית.

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה אלגברית אזי ($\mathbb{L}/\mathbb{K}$ הרחבה נורמלית)$\Longleftrightarrow$(לכל $\alpha\in\mathbb{L}$ הפולינום f_α מתפרק לגורמים לינאריים מעל $\mathbb{L}[x]$).

איבר ספרבילי מעל שדה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה אלגברית אזי $\alpha\in\mathbb{L}$ עבורו f_α בעלת שורשים פשוטים.

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

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

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

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

משפט: יהי $n\in\mathbb{N}$ ותהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי
- $\left|\mathbb{L}\hookrightarrow\overline{\mathbb{K}}\right|\leq[\mathbb{L}:\mathbb{K}]$.
- ($\mathbb{L}/\mathbb{K}$ ספרבילית)$\Longleftrightarrow$($\left|\mathbb{L}\hookrightarrow\overline{\mathbb{K}}\right|=[\mathbb{L}:\mathbb{K}]$).

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

מסקנה: יהיו $\alpha_1\ldots\alpha_m\in\overline{\mathbb{K}}$ אזי ($\mathbb{K}(\alpha_1\ldots\alpha_m)/\mathbb{K}$ ספרבילית)$\Longleftrightarrow$($\alpha_1\ldots\alpha_m$ 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 $\{\alpha\in\mathbb{L}\mid\alpha \text{ ספרבילי מעל } \mathbb{K}\}$ שדה.

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

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 ($\mathbb{K}$ שדה משוכלל)$\Longleftrightarrow$(לכל $\alpha\in\mathbb{K}$ קיים $\beta\in\mathbb{K}$ עבורו $\beta^p=\alpha$).

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

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

משפט האיבר הפרימטיבי: 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 $\mathbb{L} = \mathbb{K}(\alpha)$.

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

טענה: יהי $p \in \mathbb{P}$ יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K}) = p$ 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 $\mathrm{char}(\mathbb{K}) = p$ ויהי $n \in \mathbb{N}_+$ באשר $\gcd(n,p) = 1$ אזי $g \in \mu_n$ באשר g יוצר של μ_n.

הרחבת גלואה: הרחבה סופית 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 $\mathrm{char}(\mathbb{K}) = 0$ 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 $\nu : \mathbb{F}/\mathbb{K} \to \mathbb{L}/\mathbb{K}$.

חבורת גלואה של הרחבת גלואה: תהא $\mathbb{L}/\mathbb{K}$ הרחבת גלואה אזי $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \{f : \mathbb{L}/\mathbb{K} \to \mathbb{L}/\mathbb{K} \mid \text{אוטומורפיזם } f\}$.

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

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

סימון: יהי $\mathbb{L}$ שדה יהי $a \in \mathbb{L}$ ויהיו $\sigma, \tau \in \mathrm{Aut}(\mathbb{L})$ אזי $a^{\sigma\tau} = (a^{\sigma})^{\tau}$.

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

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

שדה אינבריאנטים/שימורים של שדה ביחס לחבורה: יהי $\mathbb{L}$ שדה ותהא $H \le \mathrm{Aut}(\mathbb{L})$ תת־חבורה אזי $\mathbb{L}^H = \left\{a \in \mathbb{L} \mid \forall h \in H. a^h = a\right\}$.

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

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

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

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

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

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

מסקנה: יהי $\mathbb{L}$ שדה ותהיינה $H, G \le \mathrm{Aut}(\mathbb{L})$ אזי $(H \subseteq G) \Longleftrightarrow (\mathbb{L}^G \subseteq \mathbb{L}^H)$.

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

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

מסקנה: $\{\mathbb{F} \mid (\text{הרחבה אלגברית } \mathbb{F}/\mathbb{R}) \wedge (\text{שדה } \mathbb{F})\} = \{\mathbb{C}\}$.

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 $(\mathbb{F} \simeq \mathbb{E}) \Longleftrightarrow$($\mathrm{Gal}(\mathbb{L}/\mathbb{F}), \mathrm{Gal}(\mathbb{L}/\mathbb{E})$ צמודות ב־$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$).

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

- ($\mathbb{F}/\mathbb{K}$ הרחבת גלואה)$\Longleftrightarrow$($\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ נורמלית ב־$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$).
- אם $\mathbb{F}/\mathbb{K}$ הרחבת גלואה אז $\mathrm{Gal}(\mathbb{F}/\mathbb{K}) \simeq {}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}/_{\mathrm{Gal}(\mathbb{L}/\mathbb{F})}$.

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 $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

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

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

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

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

פולינום סימטרי אלמנטרי: יהי $\mathbb{K}$ שדה יהי $n \in \mathbb{N}_+$ ויהי $k \in [n]$ אזי $s_k \in \mathbb{K}[x_1 \ldots x_n]$ המוגדר $s_k(x_1, \ldots, x_n) = \sum_{\substack{a \in [n]^k \\ \text{עולה ממש } a}} \prod_{i=1}^{k} x_{a_i}$.

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

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

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