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 $R/\ker(\nu) \simeq \mathrm{Im}(\nu)$.

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

מסקנה: יהי R תחום שלמות אזי ($R[x]$ תחום ראשי)$\Longleftrightarrow$(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)$\Longleftrightarrow$(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 $\mathrm{sols}_{\mathbb{K}}(f) = \{\alpha \in \mathbb{K} \mid f(\alpha) = 0\}$.

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

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

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

שורש מרובה: יהי $\mathbb{K}$ שדה ויהי $f \in \mathbb{K}[x] \setminus \{0\}$ אזי $\alpha \in \mathrm{sols}_{\mathbb{K}}(f)$ 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)$\iff(\gcd(f,f')=1)$.

טענה: יהי $\mathbb{F}$ שדה אזי ויהי $f\in\mathbb{F}[x]$ באשר $\deg(f)\ge1$ 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 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 $\mathrm{char}(\mathbb{F})\neq2$ ויהיו $a,b,c\in\mathbb{F}$ באשר $a\neq0$ אזי $\mathrm{sols}\left(ax^2+bx+c\right)=\left\{\frac{-b\pm\sqrt{b^2-4ac}}{2a}\right\}$.

טענה: יהי $\mathbb{F}$ שדה אינסופי באשר $\mathrm{char}(\mathbb{F})\neq2$ 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 $\alpha\in\mathbb{L}$ 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.

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 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 $A[S]=\bigcup_{n=1}^{\infty}\left\{f(s_1\dots s_n)\;\middle|\;\substack{f\in A[x_1\dots x_n]\\ s_1\dots s_n\in S}\right\}$.

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

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

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 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 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 $\mathbb{F} \subseteq \mathbb{L}$ המקיים $\alpha \in \mathbb{F}$ וכן $\mathbb{F}/\mathbb{K}$ הרחבה סופית).

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $\alpha_1 \ldots \alpha_n \in \mathbb{L}$ אלגבריים מעל $\mathbb{K}$ אזי קיים שדה $\mathbb{F} \subseteq \mathbb{L}$ המקיים $\alpha_1 \ldots \alpha_n \in \mathbb{F}$ 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 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 $\alpha_0, \alpha_1 \ldots \alpha_n \in \mathbb{K}$ 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 $\alpha_0, \alpha_1 \ldots \alpha_n \in \mathbb{L}$ המקיימים $f = \alpha_0 \cdot \prod_{i=1}^{n}(x - \alpha_i)$.

מסקנה: יהי $\mathbb{K}$ שדה ויהיו $f_1 \ldots f_m \in \mathbb{K}[x] \setminus \{0\}$ 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: $\left|\overline{\mathbb{Q}}\right|=\aleph_0$.

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 $\deg(a)\ge 1$ אזי a טרנסצנדנטי מעל $\mathbb{K}$ וכן $\mathbb{K}(x)/\mathbb{K}(a)$ הרחבה אלגברית מדרגה $\deg(a)$.

מסקנה: יהי $\mathbb{K}$ שדה ותהא $a\in\mathbb{K}(a)$ אזי $(\mathbb{K}(x)=\mathbb{K}(a))\Longleftrightarrow$(קיימים $\alpha,\beta,\gamma,\delta\in\mathbb{K}$ המקיימים $\alpha\delta-\beta\gamma\neq0$ וכן $a=\frac{\alpha x+\beta}{\gamma x+\delta}$).

מסקנה: יהי $\mathbb{K}$ שדה אזי $\mathrm{Aut}(\mathbb{K}(x))=\left\{\frac{\alpha x+\beta}{\gamma x+\delta}\;\middle|\;(\alpha,\beta,\gamma,\delta\in\mathbb{K})\wedge(\alpha\delta-\beta\gamma\neq0)\right\}$.

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

הרחבה טרנסצנדנטית פשוטה: הרחבה $\mathbb{L}/\mathbb{K}$ עבורה קיים $\alpha\in\mathbb{L}$ טרנסצנדטי 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 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 $\nu,\psi\in\mathbb{K}(x)$ עבורן $f(\nu,\psi)=0$.

עקומה רציונלית: יהי $\mathbb{K}$ שדה תהא $f:\mathbb{K}^2\to\mathbb{K}$ 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/טרנסצנדנטיים 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 $f\in\mathbb{K}\left[x_1,\dots,x_{|S|}\right]$ 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 $\mathbb{K}\left(\{u_\alpha\}_{\alpha\in\mathcal{I}}\right)\simeq\mathbb{K}\left(\{x_\alpha\}_{\alpha\in\mathcal{I}}\right)$.

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.

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

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 $\mathbb{K}(B)$ 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 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 $a_1\dots a_r,b_1\dots b_s\in\mathbb{L}$ 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 $s\le r$ וכן קיימת $S\subseteq\{a_1\dots a_r\}$ באשר $|S|=s$ עבורה $\{a_1\dots a_r,b_1\dots b_s\}\backslash S$ שקולה אלגברית ל־$\{a_1\dots a_r\}$ מעל $\mathbb{K}$.

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

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

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

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

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

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

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

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 $\mathbb{F}\cdot\mathbb{K}=\mathbb{E}$.

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבת שדות באשר $\operatorname{degtr}_{\mathbb{K}}(\mathbb{K})<\aleph_0$ ויהיו $\mathbb{F},\mathbb{E}\subseteq\mathbb{L}$ שדות באשר $\mathbb{K}\subseteq\mathbb{F}$ וכן $\mathbb{K}\subseteq\mathbb{E}$ אזי $\operatorname{degtr}_{\mathbb{K}}(\mathbb{F}\mathbb{E})\leq\operatorname{degtr}_{\mathbb{K}}(\mathbb{F})+\operatorname{degtr}_{\mathbb{K}}(\mathbb{E})$.

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 $|\mathbb{F}|=p^n$.

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

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

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

הרחבה נורמלית: הרחבה אלגברית $\mathbb{L}/\mathbb{K}$ עבורה לכל פולינום אי־פריק $f\in\mathbb{K}[x]$ מתקיים כי אם $\operatorname{sols}_{\mathbb{L}}(f)\neq\varnothing$ 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 $\mathbb{L}\subset\mathbb{F}$.

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)$\iff$(לכל $\alpha\in\mathbb{L}$ הפולינום f_α מתפרק לגורמים לינאריים מעל $\mathbb{L}[x]$).

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

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה נורמלית יהי $f\in\mathbb{K}[x]$ אי־פריק ויהיו $g,h\in\mathbb{L}[x]$ אי־פריקים באשר $g,h|f$ מעל $\mathbb{L}[x]$ אזי $\deg(g)=\deg(h)$.

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

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

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

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 $\operatorname{char}(\mathbb{K})=0$ אזי $\mathbb{L}/\mathbb{K}$ הרחבה ספרבילית.

מסקנה: יהי $p\in\mathbb{P}$ תהא $\mathbb{L}/\mathbb{K}$ הרחבה אלגברית באשר $\operatorname{char}(\mathbb{K})=p$ ויהי $\alpha\in\mathbb{L}$ אזי (f_α בעל שורש מרובה)$\iff$(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)$\iff$($\left|\mathbb{L}\hookrightarrow\overline{\mathbb{K}}\right|=[\mathbb{L}:\mathbb{K}]$).

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)$\iff$($\mathbb{L}/\mathbb{F},\mathbb{F}/\mathbb{K}$ ספרביליות).

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

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

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

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

טענה: יהי $p\in\mathbb{P}$ תהא $\mathbb{L}/\mathbb{K}$ הרחבה אלגברית באשר $\operatorname{char}\left(\mathbb{K}\right)=p$ 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 $\operatorname{char}\left(\mathbb{K}\right)\nmid\left[\mathbb{L}:\mathbb{K}\right]$ 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 $\operatorname{char}\left(\mathbb{K}\right)=0$ אז $\mathbb{K}$ שדה משוכלל.
- אם $\operatorname{char}\left(\mathbb{K}\right)=p$ אז ($\mathbb{K}$ שדה משוכלל)$\iff$(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.

טענה: יהי $p\in\mathbb{P}$ ויהי $\mathbb{F}$ שדה באשר $\operatorname{char}\left(\mathbb{F}\right)=p$ 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 $\mathbb{L}=\mathbb{K}\left(\alpha\right)$.

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

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 $\mathbb{L}=\mathbb{K}\left(\alpha\right)$.

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

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

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

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

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

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 $\operatorname{char}\left(\mathbb{K}\right)=0$ יהי $f\in\mathbb{K}\left[x\right]$ 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 $\operatorname{Gal}\left(\mathbb{L}/\mathbb{K}\right)=\operatorname{Aut}\left(\mathbb{L}/\mathbb{K}\right)$.

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

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

פעולת גלואה: תהא $\mathbb{L}/\mathbb{K}$ הרחבת גלואה אזי נגדיר $\operatorname{GA}:\operatorname{Gal}\left(\mathbb{L}/\mathbb{K}\right)\times\mathbb{L}\to\mathbb{L}$ כך $\operatorname{GA}\left(\sigma,\alpha\right)=a^\sigma$.

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

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

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

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

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

שדה אינבריאנטים/שימורים של שדה ביחס לחבורה: יהי $\mathbb{L}$ שדה ותהא $H\leq\operatorname{Aut}\left(\mathbb{L}\right)$ 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 $H\leq\operatorname{Aut}\left(\mathbb{L}\right)$ תת־חבורה סופית אזי $\mathbb{L}/\mathbb{L}^H$ הרחבה גלואה וכן $\operatorname{Gal}\left(\mathbb{L}/\mathbb{L}^H\right)=H$.

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

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

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

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

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

מסקנה: יהי $\mathbb{L}$ שדה ותהיינה $H,G\le\mathrm{Aut}\left(\mathbb{L}\right)$ 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 $(\mathbb{F}\subseteq\mathbb{K})\Longleftrightarrow(\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)\subseteq\mathrm{Gal}\left(\mathbb{L}/\mathbb{F}\right))$.

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

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

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

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

- $(\text{הרחבת גלואה }\mathbb{F}/\mathbb{K})\Longleftrightarrow(\mathrm{Gal}\left(\mathbb{L}/\mathbb{F}\right)\trianglelefteq\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right))$.
- אם $\mathbb{F}/\mathbb{K}$ הרחבת גלואה אז $\mathrm{Gal}\left(\mathbb{F}/\mathbb{K}\right)\simeq{}^{\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)}/_{\mathrm{Gal}\left(\mathbb{L}/\mathbb{F}\right)}$.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}\left[x\right]$ 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 $f\in\mathbb{K}\left[x\right]$ בעל שורשים פשוטים ויהי $\mathbb{L}$ שדה הפיצול של f אזי $\mathrm{Gal}\left(f\right)=\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)$.

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

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

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

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

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

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

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

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 $\mathbb{K}$.

טענה: יהי $n\in\mathbb{N}_{+}$ ויהיו $z_{1}\ldots z_{n}\in\mathbb{C}\backslash\left\{0\right\}$ אזי $(\mathrm{Arg}\left(z_{i}\right)=\mathrm{Arg}\left(z_{j}\right)\text{ לכל }i,j\in\left[n\right])\Longleftrightarrow(\left|\sum_{i=1}^{n}z_{i}\right|=\sum_{i=1}^{n}\left|z_{i}\right|)$.

מסקנה: יהיו $a_{1}\ldots a_{n},d_{1}\ldots d_{n}\in\mathbb{N}_{+}$ אזי $\mathbb{Q}\left(\sqrt[d_{1}]{a_{1}},\ldots,\sqrt[d_{n}]{a_{n}}\right)=\mathbb{Q}\left(\sum_{i=1}^{n}\sqrt[d_{i}]{a_{i}}\right)$.

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 $c=\alpha a^{2}+\beta b^{2}$.

משפט ארטין: יהי $\mathbb{L}$ שדה ותהא $G\le\mathrm{Aut}\left(\mathbb{L}\right)$ סופית אזי $\left|G\right|\ge\left[\mathbb{L}:\mathbb{L}^{G}\right]$.

מסקנה: יהי $\mathbb{L}$ שדה ותהא $G\le\mathrm{Aut}\left(\mathbb{L}\right)$ סופית אזי $G=\mathrm{Aut}\left(\mathbb{L}/\mathbb{L}^{G}\right)$.

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 $\mathbb{F}\mathbb{E}/\mathbb{E}$ הרחבת גלואה וכן $\left[\mathbb{F}\mathbb{E}:\mathbb{E}\right]=\left[\mathbb{F}:\mathbb{F}\cap\mathbb{E}\right]$.

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 $\mathrm{Gal}\left(\mathbb{F}\mathbb{E}/\mathbb{E}\right)\simeq\mathrm{Gal}\left(\mathbb{E}/\left(\mathbb{E}\cap\mathbb{F}\right)\right)$.

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 $\mathbb{F}\mathbb{E}=\mathbb{L}$ אזי $\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)\simeq\mathrm{Gal}\left(\mathbb{E}/\mathbb{K}\right)\times\mathrm{Gal}\left(\mathbb{F}/\mathbb{K}\right)$.

טענה: יהיו $p,q\in\mathbb{P}$ באשר $p<q$ תהא $\mathbb{L}/\mathbb{K}$ הרחבת גלואה ממעלה pq ויהי $f\in\mathbb{K}\left[x\right]$ באשר $\deg\left(f\right)=p$ 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 $\left(d|n\right)\Longleftrightarrow\left(\mathbb{F}_{p^{d}}\subseteq\mathbb{F}_{p^{n}}\right)$.

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

הגדרה: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_{q}$ שדה אזי נגדיר $\pi_{q}:\mathbb{N}_{+}\to\mathbb{N}$ כך $\pi_{q}\left(n\right)=\left|\left\{f\in\mathbb{F}_{q}\left[x\right]\mid\left(\deg\left(f\right)=n\right)\wedge\left(\text{מתוקן ואי־פריק }f\right)\right\}\right|$.

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

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

פונקציית מוביוס: יהי $k\in\mathbb{N}$ יהיו $p_{1}\ldots p_{k}\in\mathbb{P}$ שונים ויהי $e\in\mathbb{N}_{+}^{k}$ אזי נגדיר $\mu:\mathbb{N}\to\left\{0,\pm1\right\}$ כך $\mu\left(\prod_{i=1}^{k}p_{i}^{e_{i}}\right)=\left\{\begin{smallmatrix}\left(-1\right)^{k} & e=\mathbb{1}\\ 0 & \text{else}\end{smallmatrix}\right.$.

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

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

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

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

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

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

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

הרחבה 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 $\mathbb{K}\left(\zeta_n\right)=\mathbb{F}$.

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

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

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

- $\text{Gal}\left(\mathbb{K}\left(\zeta_n\right)/\mathbb{K}\right)$ אבלית.
- קיימת $H\le\left(\mathbb{Z}_n\right)^\times$ עבורה $H\cong\text{Gal}\left(\mathbb{K}\left(\zeta_n\right)/\mathbb{K}\right)$.
- אם $n\in\mathbb{P}$ אז $\text{Gal}\left(\mathbb{K}\left(\zeta_n\right)/\mathbb{K}\right)$ ציקלית.

הרחבה ציקלוטומית: יהי $n\in\mathbb{N}_+$ אזי $\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}$.

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

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

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

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

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

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

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

טענה: יהי $m\in\mathbb{N}_{\text{odd}}\backslash\left\{1\right\}$ אזי $\Phi_{2m}\left(x\right)=\Phi_m\left(-x\right)$.

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

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

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

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

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

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

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

טענה: יהיו $m,d\in\mathbb{N}$ ויהי $p\in\mathbb{P}$ באשר $p|\Phi_d\left(m\right)$ וכן $p\nmid d$ אזי $p\equiv1\mod d$.

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

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

הגדרה: תהא $\Omega^{(0)}\subseteq\mathbb{C}$ אזי $\Omega^{(1)}=\left\{\text{line}_{a,b}\;\middle|\;a,b\in\Omega^{(0)}\right\}$.

הגדרה: תהא $\Omega^{(0)}\subseteq\mathbb{C}$ אזי $\Omega^{(2)}=\left\{\partial B_{\text{dist}(a,b)}\left(c\right)\;\middle|\;a,b,c\in\Omega^{(0)}\right\}$.

הגדרה: יהי $k\in\mathbb{N}$ אזי $\Omega_0^{(0)}=\left\{0,1\right\}$ וכן $\Omega_{k+1}^{(0)}=\bigcup\left\{S_1\cap S_2\;\middle|\;S_1,S_2\in\left(\Omega_k^{(1)}\cup\Omega_k^{(2)}\right)\right\}$.

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 $\mathbb{L}_1,\ldots,\mathbb{L}_n$ עבורם $\mathbb{L}_1/\mathbb{K}$ הרחבה ריבועית וכן $\mathbb{L}_{i+1}/\mathbb{L}_i$ הרחבה ריבועית לכל $i\in\left[n-1\right]$.

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

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

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

מצולע משוכלל: יהי $n\in\mathbb{N}_{\ge3}$ אזי $\text{RegPol}_n\left\{\zeta_n^0,\ldots,\zeta_n^{n-1}\right\}$.

מסקנה: יהי $n\in\mathbb{N}_{\ge3}$ אזי $(\mathrm{RegPol}_n\subseteq\mathbb{K}_{\text{sc}})\Longleftrightarrow$(קיים שדה $\mathbb{L}$ הנוצר מסדרת הרחבות ריבועיות של $\mathbb{Q}$ עבורו $\zeta_n\in\mathbb{L}$).

מסקנה: יהי $n\in\mathbb{N}_{\ge3}$ באשר $\mathrm{RegPol}_n\subseteq\mathbb{K}_{\text{sc}}$ אזי קיים $r\in\mathbb{N}$ עבורו $\varphi(n)=2^r$.

משפט: יהי $n\in\mathbb{N}_{\ge3}$ אזי $(\mathrm{RegPol}_n\subseteq\mathbb{K}_{\text{sc}})\Longleftrightarrow$(קיימים $r,r_1\ldots r_k\in\mathbb{N}$ 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 $\sphericalangle_{\mathrm{line}_{a,b},\mathrm{line}_{b,c}}=\frac{\alpha}{3}$.

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

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

מסקנה: יהי $n\in\mathbb{N}_+$ יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K})=0$ וכן $\zeta_n\in\mathbb{K}$ ויהי $a\in\mathbb{K}^\times\backslash\left\{b^d\mid(b\in\mathbb{K}^\times)\wedge(d\in\mathbb{N}_{\ge2})\wedge(d|n)\right\}$ אזי $|\mathrm{Gal}(x^n-a)|=n$.

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

מסקנה: יהי $p\in\mathbb{P}$ יהי $n\in\mathbb{N}_+$ באשר $\gcd(n,p)=1$ יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K})=p$ וכן $\zeta_n\in\mathbb{K}$ ויהי $a\in\mathbb{K}^\times\backslash\left\{b^d\mid(b\in\mathbb{K}^\times)\wedge(d\in\mathbb{N}_{\ge2})\wedge(d|n)\right\}$ אזי $|\mathrm{Gal}(x^n-a)|=n$.

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

רזולבנטת 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 $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ אזי נגדיר $\mathcal{L}:\mathbb{L}\to\mathbb{L}$ 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 $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ 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 $\mathcal{L}(\alpha)\neq0$.

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 $\beta\in\mathrm{sols}_{\mathbb{L}}(x^n-b)$ המקיים $\mathbb{L}=\mathbb{K}(\beta)$.

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

- $\mathbb{K}=\mathbb{F}_0$ וכן $\mathbb{L}=\mathbb{F}_k$.
- לכל $i\in[k]$ קיים $n\in\mathbb{N}_+$ וכן קיים $a\in\mathbb{L}_i$ עבורם קיים $\alpha\in\mathrm{sols}_{\mathbb{L}_i}(x^n-a)$ 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 $\mathrm{sols}_{\overline{\mathbb{K}}}(f)\subseteq\mathbb{L}$ אזי f.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה רדיקלית באשר $\mathrm{char}(\mathbb{K})=0$ אזי קיים שדה $\mathbb{L}\subseteq\mathbb{F}$ עבורו $\mathbb{F}/\mathbb{K}$ הרחבה נורמלית רדיקלית.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה נורמלית רדיקלית באשר $\mathrm{char}(\mathbb{K})=0$ אזי $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ פתירה.

משפט: יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K})=0$ ויהי $f\in\mathbb{K}[x]$ אזי (f פתיר ברדיקלים)$\Longleftrightarrow$($\mathrm{Gal}(f)$ פתירה).

מסקנה: יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K})=0$ יהי $n\in\mathbb{N}_+$ ויהיו $a_0\ldots a_n$ בת"א מעל $\mathbb{K}$ אזי ($\sum_{i=0}^n a_ix^i$ פתיר ברדיקלים)$\Longleftrightarrow$($n\le4$).

משפט: יהי $p\in\mathbb{P}_{>2}$ ויהי $f\in\mathbb{Q}[x]$ אי־פריק פתיר ברדיקלים באשר $\deg(f)=p$ אזי $|\mathrm{sols}_{\mathbb{R}}(f)|\in\{1,p\}$.

הרחבה ממשית רדיקלית: הרחבה רדיקלית $\mathbb{L}/\mathbb{K}$ המקיימת $\mathbb{L}\subseteq\mathbb{R}$.

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

למה: יהי $p\in\mathbb{P}$ ויהיו $\mathbb{K},\mathbb{L},\mathbb{F}$ שדות עבורם $\mathbb{K}/\mathbb{F},\mathbb{L}/\mathbb{F}$ הרחבות גלואה וכן $[\mathbb{L}:\mathbb{F}]=p$ וכן $\mathbb{L}\not\subseteq\mathbb{K}$ אזי $\mathbb{LK}/\mathbb{K}$ הרחבת גלואה וכן $[\mathbb{LK}:\mathbb{K}]=p$.

למה: יהי $p\in\mathbb{P}$ יהי $\mathbb{K}$ שדה ויהי $a\in\mathbb{K}$ עבורו $\mathrm{sols}_{\mathbb{K}}(x^p-a)=\varnothing$ אזי x^p-a אי־פריק מעל $\mathbb{K}(\zeta_p)$.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית נורמלית באשר $\mathbb{L}\subseteq\mathbb{R}$ אזי ($\mathbb{L}/\mathbb{K}$ הרחבה ממשית רדיקלית)$\Longleftrightarrow$($\exists s\in\mathbb{N}:\mathrm{Gal}(\mathbb{L}/\mathbb{K})=2^s$).

סימון: יהי R חוג אזי $\square_R=\left\{a^2\mid a\in R\right\}$.

משפט קאפלאנסקי: יהיו $a,b\in\mathbb{Q}$ עבורם x^4+ax^2+b אי־פריק מעל $\mathbb{Q}[x]$ אזי $\mathrm{Gal}\left(x^4+ax^2+b\right)\simeq\begin{cases}\mathbb{Z}_2\times\mathbb{Z}_2 & b\in\square_{\mathbb{Q}}\\ \mathbb{Z}_4 & b\left(a^2-4b\right)\in\square_{\mathbb{Q}}\\ D_8 & \text{else}\end{cases}$.

שדה ממשי פורמלי: שדה $\mathbb{K}$ המקיים $\mathrm{char}(\mathbb{K})=0$ וכן לכל $n\in\mathbb{N}_+$ ולכל $a\in\square_{\mathbb{K}}^n$ מתקיים $\sum_{i=1}^n a_i\neq-1$.

שדה ממשי סגור: שדה ממשי פורמלי $\mathbb{K}$ עבורו לכל שדה ממשי פורמלי $\mathbb{L}$ המקיים $\mathbb{L}/\mathbb{K}$ הרחבה סופית מתקיים $\mathbb{L}=\mathbb{K}$.

למה: יהי $\mathbb{K}$ שדה ממשי סגור יהי $n\in\mathbb{N}_+$ ויהי $a\in\square_{\mathbb{K}}^n$ אזי $\sum_{i=1}^n a_i\in\square_{\mathbb{K}}$.

שדה סדור: יהי $\mathbb{K}$ שדה באשר $\mathrm{char}(\mathbb{K})=0$ ויהי $<_{\mathbb{K}}$ יחס סדר חזק קווי מעל $\mathbb{K}$ המקיים

- קומפטביליות עם חיבור: לכל $x,y,z\in\mathbb{K}$ המקיימים $x<_{\mathbb{K}}y$ מתקיים $x+z<_{\mathbb{K}}y+z$.
- קומפטביליות עם כפל: לכל $x,y\in\mathbb{K}$ המקיימים $x<_{\mathbb{K}}y$ ולכל $z\in\mathbb{K}$ המקיים $0<_{\mathbb{K}}z$ מתקיים $x\cdot z<_{\mathbb{K}}y\cdot z$.

אזי $\langle \mathbb{K}, <_{\mathbb{K}} \rangle$.

משפט: יהי $\mathbb{K}$ שדה באשר $\mathrm{char}\left(\mathbb{K}\right)=0$ אזי (קיים יחס $<_{\mathbb{K}}$ עבורו $\langle \mathbb{K}, <_{\mathbb{K}} \rangle$ שדה סדור)$\Longleftrightarrow$(קיימות $\mathbb{K}_+, \mathbb{K}_- \subseteq \mathbb{K}$ המקיימות $\mathbb{K}=\left(\mathbb{K}_+ \uplus \mathbb{K}_-\right) \cup \{0\}$ וכן $1 \in \mathbb{K}_+$ וכן $\mathbb{K}_-=-\mathbb{K}_+$ וכן לכל $a,b \in \mathbb{K}_+$ מתקיים $\{a+b, ab\} \subseteq \mathbb{K}_+$).

משפט: יהי $\mathbb{K}$ שדה ממשי סגור אזי קיים ויחיד יחס סדר חזק $<_{\mathbb{K}}$ מעל $\mathbb{K}$ עבורו $\langle \mathbb{K}, <_{\mathbb{K}} \rangle$ שדה סדור.

משפט: יהי $\mathbb{K}$ שדה ממשי סגור ויהי $f \in \mathbb{K}\left[x\right]$ באשר $\deg\left(f\right) \in \mathbb{N}_{\mathrm{odd}}$ אזי $\mathrm{sols}_{\mathbb{K}}\left(f\right) \neq \varnothing$.

משפט: יהי $\mathbb{K}$ שדה ממשי פורמלי אזי ($\mathbb{K}$ שדה ממשי סגור)$\Longleftrightarrow$($\mathbb{K}\left(\sqrt{-1}\right)$ שדה סגור אלגברית).

מסקנה: $\mathbb{R}$ שדה ממשי סגור.