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 $R[x_1\dots x_n]$ חוג אבלי בעל יחידה.

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

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

הגדרה: יהי R חוג 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 $R\hookrightarrow S=\{\nu:R\to S\mid$ 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 $R\twoheadrightarrow S=\{\nu:R\to S\mid$ 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)$\iff$($I \cap R^\times = \varnothing$).

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

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

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)$\Longleftrightarrow$($\gcd(f,f')=1$).

טענה: יהי $\mathbb{F}$ שדה אזי ויהי $f\in\mathbb{F}[x]$ באשר $\deg(f)\geq1$ אזי (f ראשוני)$\Longleftrightarrow$(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)$\Longleftrightarrow$(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 $A[S]=\bigcup_{n=1}^{\infty}\left\{f(s_1\ldots s_n)\;\middle|\;\substack{f\in A[x_1\ldots x_n]\\ s_1\ldots s_n\in S}\right\}$.

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 $\mathbb{K}(S)=\bigcup_{n=1}^{\infty}\bigcup_{f,g\in\mathbb{K}[x_1\ldots x_n]}\left\{\frac{f(s_1\ldots s_n)}{g(s_1\ldots s_n)}\;\middle|\;\substack{s_1\ldots s_n\in S\\ g(s_1\ldots s_n)\neq0}\right\}$.

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

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $\alpha_1\ldots\alpha_n\in\mathbb{L}$ אלגבריים מעל $\mathbb{K}$ אזי קיים שדה $\mathbb{L}\subseteq\mathbb{F}$ 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 $\deg(f)\ge1$ 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 $\mathbb{L}\subseteq\mathbb{F}$ המקיים $\mathbb{F}\subseteq\mathbb{K}$ 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 $\deg(f)\ge1$ 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 $\deg(f_\tau)\ge1$ 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 $\mathbb{L}=\overline{\mathbb{K}}$.

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

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

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

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 $u_1\ldots u_m\in\mathbb{L}$ אזי $v\in\mathbb{L}$ באשר v אלגברי מעל $\mathbb{K}(u_1\ldots u_m)$.

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 $j\in[n]$ 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 $f\in\mathbb{K}[x_1\ldots x_m]$ מתקיים כי אם $f(u_1\ldots u_m)=0$ 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 $\mathbb{K}(u_1\ldots u_m)\simeq\mathbb{K}(x_1\ldots x_m)$.

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 $f\in\mathbb{K}\left[x_1,\ldots,x_{|S|}\right]$ 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 $a_1\ldots a_r,b_1\ldots b_s\in\mathbb{L}$ באשר $\{b_1\ldots b_s\}$ בת"א מעל $\mathbb{K}$ וכן b_j תלוי אלגברית ב־$a_1\ldots a_r$ מעל $\mathbb{K}$ לכל $j\in[s]$ אזי $s\leq r$ וכן קיימת $S\subseteq\{a_1\ldots a_r\}$ באשר $|S|=s$ עבורה $\{a_1\ldots a_r,b_1\ldots b_s\}\backslash S$ שקולה אלגברית ל־$\{a_1\ldots a_r\}$ 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 $\mathrm{degtr}_{\mathbb{K}}(\mathbb{L})=|\mathcal{B}|$.

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

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

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 $\mathrm{degtr}_{\mathbb{K}}(\mathbb{K})<\aleph_0$ ויהיו $\mathbb{F},\mathbb{E}\subseteq\mathbb{L}$ שדות באשר $\mathbb{K}\subseteq\mathbb{F}$ וכן $\mathbb{K}\subseteq\mathbb{E}$ אזי $\mathrm{degtr}_{\mathbb{K}}(\mathbb{F}\mathbb{E})\le\mathrm{degtr}_{\mathbb{K}}(\mathbb{F})+\mathrm{degtr}_{\mathbb{K}}(\mathbb{E})$.

שדה פיצול: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ באשר $\deg(f)\ge1$ אזי שדה $\mathbb{F}$ באשר $\mathbb{K}\subseteq\mathbb{F}$ וכן f מתפרק לגורמים ליניאריים מעל $\mathbb{F}$ וכן לכל שדה $\mathbb{L}\subset\mathbb{F}$ מתקיים כי f אינו מתפרק לגורמים ליניאריים 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 $\mathrm{sols}_{\mathbb{L}}(f)\neq\varnothing$ אז f מתפרק לגורמים ליניאריים 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)$\Longleftrightarrow$(לכל $\alpha\in\mathbb{L}$ הפולינום f_α מתפרק לגורמים ליניאריים מעל $\mathbb{L}[x]$).

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $f,g\in\mathbb{K}[x]$ אזי (f,g זרים מעל $\mathbb{K}[x]$)$\Longleftrightarrow$(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 $\mathrm{char}(\mathbb{K})=0$ אזי $\mathbb{L}/\mathbb{K}$ הרחבה ספרבילית.

מסקנה: יהי $p\in\mathbb{P}$ תהא $\mathbb{L}/\mathbb{K}$ הרחבה אלגברית באשר $\mathrm{char}(\mathbb{K})=p$ 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
- $\left|\mathbb{L}\hookrightarrow\overline{\mathbb{K}}\right|\le[\mathbb{L}:\mathbb{K}]$.
- ($\mathbb{L}/\mathbb{K}$ ספרבילית)$\Longleftrightarrow$($\left|\mathbb{L}\hookrightarrow\overline{\mathbb{K}}\right|=[\mathbb{L}:\mathbb{K}]$).

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ויהי $\mathbb{L}\subseteq\mathbb{F}$ שדה באשר $\mathbb{F}\subseteq\mathbb{K}$ 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 $\{\alpha\in\mathbb{L}\mid\mathbb{K}$ ספרבילי מעל $\alpha\}$ שדה.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: תהא G 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 $\left|\left\{ \mathbb{F}\mid\left(\mathbb{K}\subseteq\mathbb{F}\subseteq\mathbb{L}\right)\wedge\left(\text{שדה }\mathbb{F}\right)\right\} \right|=\left|\left\{ H\mid H\leq\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)\right\} \right|$.

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

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

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

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

- $\left(\text{הרחבת גלואה }\mathbb{F}/\mathbb{K}\right)\Longleftrightarrow\left(\mathrm{Gal}\left(\mathbb{L}/\mathbb{F}\right)\trianglelefteq\mathrm{Gal}\left(\mathbb{L}/\mathbb{K}\right)\right)$.
- 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 $\left(\text{טרנזיטיבית RA}\right)\Longleftrightarrow\left(\text{אי־פריק }f\right)$.

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 $\left|\mathrm{Gal}\left(f\right)\right|\mid\deg\left(f\right)!$.

פונקציה סימטרית: יהי $\mathbb{K}$ שדה ויהי $n\in\mathbb{N}_{+}$ אזי $f\in\mathbb{K}\left(x_{1}\ldots x_{n}\right)$ עבורה לכל $\sigma\in S_{n}$ מתקיים $f\left(x_{1}\ldots x_{n}\right)=f\left(x_{\sigma\left(1\right)}\ldots x_{\sigma\left(n\right)}\right)$.

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 ויהי $k\in\mathbb{N}_{+}$ אזי s_{k} פונקציה סימטרית.

משפט: יהי $\mathbb{K}$ שדה יהי $n\in\mathbb{N}_{+}$ ותהא $f\in\mathbb{K}\left(x_{1}\ldots x_{n}\right)$ סימטרית אזי קיימת $g\in\mathbb{K}\left(x_{1}\ldots x_{n}\right)$ עבורה $f=g\left(s_{1},\ldots,s_{n}\right)$.

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 $\left(\mathrm{Arg}\left(z_{i}\right)=\mathrm{Arg}\left(z_{j}\right)\text{ לכל }i,j\in\left[n\right]\right)\Longleftrightarrow\left(\left|\sum_{i=1}^{n}z_{i}\right|=\sum_{i=1}^{n}\left|z_{i}\right|\right)$.

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 $G\leq\mathrm{Aut}\left(\mathbb{L}\right)$ סופית אזי $\left|G\right|\geq\left[\mathbb{L}:\mathbb{L}^{G}\right]$.

מסקנה: יהי $\mathbb{L}$ שדה ותהא $G\leq\mathrm{Aut}\left(\mathbb{L}\right)$ 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 $\mathbb{FE}/\mathbb{E}$ הרחבת גלואה וכן $\left[\mathbb{FE}:\mathbb{E}\right]=\left[\mathbb{F}:\mathbb{F}\cap\mathbb{E}\right]$.

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

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 $\mathbb{FE}=\mathbb{L}$ 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 $k \in \mathbb{N}$ ויהיו $p_1 \ldots p_k \in \mathbb{P}$ שונים ויהי $e \in \mathbb{N}_+^k$ אזי נגדיר $\mu : \mathbb{N} \to \{0, \pm 1\}$ כך $\mu\left(\prod_{i=1}^k p_i^{e_i}\right) = \left\{\begin{smallmatrix} (-1)^k & e=\mathbb{1} \\ 0 & \text{else} \end{smallmatrix}\right.$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

למה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה פשוטה סופית יהי $\alpha \in \mathbb{L}$ עבורו $\mathbb{L} = \mathbb{K}(\alpha)$ יהי $\mathbb{F}$ שדה באשר $\mathbb{K} \subseteq \mathbb{F} \subset \mathbb{L}$ יהי $f_\alpha \in \mathbb{F}[x]$ הפולינום המינימלי של α יהי $m \in \mathbb{N}$ ויהי $\zeta \in \mathbb{F}^{m+1}$ באשר $f_\alpha = \sum_{i=0}^m \zeta_i \cdot x^i$ אזי $\mathbb{K}(\zeta) = \mathbb{F}$.

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי $(\text{פשוטה } \mathbb{L}/\mathbb{K}) \Longleftrightarrow (|\{\mathbb{F} \mid (\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}) \wedge (\text{שדה } \mathbb{F})\}| < \aleph_0)$.

טענה: יהי $\mathbb{K}$ שדה סופי יהי $r \in \mathbb{N}_+$ ויהיו $f_1 \ldots f_r \in \mathbb{K}[x]$ אי־פריקים מתוקנים שונים אזי $\prod_{i=1}^r f_i$ ספרבילי.

טענה: יהי $\mathbb{K}$ שדה סופי יהי $r \in \mathbb{N}_+$ יהיו $f_1 \ldots f_r \in \mathbb{K}[x]$ אי־פריקים מתוקנים שונים ויהיו $d_1 \ldots d_r \in \mathbb{K}[x]$ באשר $\deg(f_i) = d_i$ לכל $i \in [r]$ אזי קיימים מעגלים זרים $C_1 \ldots C_r \in S_{\deg(f)}$ עבורם $\prod_{i=1}^r C_i \in \text{Gal}\left(\prod_{i=1}^r f_i\right)$ וכן $\text{len}(C_i) = d_i$ לכל $i \in [r]$.

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

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

הגדרה: יהי $k\in\mathbb{N}$ אזי $\Omega_0^{(0)}=\{0,1\}$ 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: $\mathbb{K}_{\text{sc}}=\bigcup_{k=0}^{\infty}\Omega_k^{(0)}$.

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ריבועית אזי קיים $a\in\mathbb{L}$ עבורו $\mathbb{L}=\mathbb{K}(a)$ וכן $a^2\in\mathbb{K}$.

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 $i\in[n-1]$.

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

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

מצולע משוכלל: יהי $n\in\mathbb{N}_{\geq3}$ אזי $\text{RegPol}_n=\left\{\zeta_n^0,\ldots,\zeta_n^{n-1}\right\}$.

מסקנה: יהי $n\in\mathbb{N}_{\geq3}$ אזי $(\text{RegPol}_n\subseteq\mathbb{K}_{\text{sc}})\Longleftrightarrow$(קיים שדה $\mathbb{L}$ הנוצר מסדרת הרחבות ריבועיות של $\mathbb{Q}$ עבורו $\zeta_n\in\mathbb{L}$).

מסקנה: יהי $n\in\mathbb{N}_{\geq3}$ באשר $\text{RegPol}_n\subseteq\mathbb{K}_{\text{sc}}$ אזי קיים $r\in\mathbb{N}$ עבורו $\varphi(n)=2^r$.

משפט: יהי $n\in\mathbb{N}_{\geq3}$ אזי $(\text{RegPol}_n\subseteq\mathbb{K}_{\text{sc}})\Longleftrightarrow$(קיימים $r,r_1\ldots r_k\in\mathbb{N}$ עבורם $2^{2^{r_i}}+1\in\mathbb{P}$ לכל $i\in[k]$ וכן $n=2^r\cdot\prod_{i=1}^{k}p_i$).

טענה: תהא $\alpha\in(-\pi,\pi]$ יהי $n\in\mathbb{N}_{\geq2}$ ויהיו $o,a_0,a_n\in\mathbb{K}_{\text{sc}}$ שונים באשר $\sphericalangle_{\text{line}(o,a_0),\text{line}(o,a_n)}=\alpha$ אזי (קיים $a\in\mathbb{K}_{\text{sc}}^{n-1}$ עבורו לכל $i\in[n]$ מתקיים $\sphericalangle_{\text{line}(o,a_{i-1}),\text{line}(o,a_i)}=\frac{\alpha}{n}$)$\Longleftrightarrow$(קיים $m\in\mathbb{N}_+$ עבורו $n=2^m$).

טענה: $\mathbb{K}_{\text{sc}}/\mathbb{Q}$ הרחבת גלואה.

טענה: יהי $p\in\mathbb{P}$ אזי (קיים שדה $\mathbb{L}$ עבורו $\mathbb{L}/\mathbb{K}_{\text{sc}}$ הרחבה ממעלה p)$\Longleftrightarrow$($p\neq2$).

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

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

מסקנה: יהי $n\in\mathbb{N}_+$ יהי $\mathbb{K}$ שדה באשר $\text{char}(\mathbb{K})=0$ וכן $\zeta_n\in\mathbb{K}$ ויהי $a\in\mathbb{K}^\times\backslash\left\{b^d\mid(b\in\mathbb{K}^\times)\wedge(d\in\mathbb{N}_{\geq2})\wedge(d|n)\right\}$ אזי $|\text{Gal}(x^n-a)|=n$.

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

מסקנה: יהי $p\in\mathbb{P}$ יהי $n\in\mathbb{N}_+$ באשר $\gcd(n,p)=1$ יהי $\mathbb{K}$ שדה באשר $\text{char}(\mathbb{K})=p$ וכן $\zeta_n\in\mathbb{K}$ ויהי $a\in\mathbb{K}^\times\backslash\left\{b^d\mid(b\in\mathbb{K}^\times)\wedge(d\in\mathbb{N}_{\geq2})\wedge(d|n)\right\}$ אזי $|\text{Gal}(x^n-a)|=n$.

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

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 $\text{Gal}(\mathbb{L}/\mathbb{K})$ 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 $\text{Gal}(\mathbb{L}/\mathbb{K})$ אזי

- לכל $\alpha\in\mathbb{L}$ מתקיים $\mathcal{L}(\alpha)^\sigma=\zeta_n\cdot\mathcal{L}(\alpha)$.
- לכל $\alpha\in\mathbb{L}$ מתקיים $\mathcal{L}(\alpha)^n\in\mathbb{K}$.
- קיים $\alpha\in\mathbb{L}$ המקיים $\mathcal{L}(\alpha)\neq0$.

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

הרחבה רדיקלית: הרחבה $\mathbb{L}/\mathbb{K}$ עבורה קיים $k\in\mathbb{N}$ וקיימים 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 $a\in\mathbb{F}_i$ עבורם קיים $\alpha\in\text{sols}_{\mathbb{F}_i}(x^n-a)$ המקיים $\mathbb{F}_i=\mathbb{F}_{i-1}(\alpha)$.

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

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

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

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

מסקנה: יהי $\mathbb{K}$ שדה באשר $\text{char}(\mathbb{K})=0$ 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)$\Longleftrightarrow$($n\leq4$).

טענה: יהי $p\in\mathbb{P}_{>2}$ ויהי $f\in\mathbb{Q}[x]$ אי־פריק באשר $\deg(f)=p$ וכן $|\text{sols}_{\mathbb{R}}(f)|=p-2$ אזי $\text{Gal}(f)\simeq S_p$.

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

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

משוואה פתירה ברדיקלים ממשיים: יהי $\mathbb{R}\subseteq\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ עבורו קיימת הרחבה ממשית רדיקלית $\mathbb{L}/\mathbb{K}$ המקיימת $\text{sols}_{\overline{\mathbb{K}}}(f)\subseteq\mathbb{L}$ 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 $\mathbb{L}\nsubseteq\mathbb{K}$ 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 $\text{sols}_{\mathbb{K}}(x^p-a)=\varnothing$ אזי x^p-a אי־פריק מעל $\mathbb{K}(\zeta_p)$.

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

טענה: יהי $\alpha\in\mathbb{K}_{\text{sc}}$ ויהי $f_\alpha\in\mathbb{Q}[x]$ הפולינום המינימלי של α אזי f_α פתיר ברדיקלים.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ ויהי $n\in\mathbb{N}_+$ אזי (f פתיר ברדיקלים)$\Longleftrightarrow$($f(x^n)$ פתיר ברדיקלים).

חבורה טרנזיטיבית: יהי $n\in\mathbb{N}_+$ אזי חבורה $H\le S_n$ עבורה לכל $i,j\in[n]$ קיים $\sigma\in H$ המקיים $\sigma(i)=j$.

משפט: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ ספרבילי אזי (f אי־פריק)$\Longleftrightarrow$($\text{Gal}(f)$ חבורה טרנזיטיבית).

דיסקרמיננטה: יהי $\mathbb{K}$ שדה יהי $n\in\mathbb{N}$ יהי $f\in\mathbb{K}[x]$ מתוקן באשר $\deg(f)=n$ ויהי $\alpha\in\overline{\mathbb{K}}^n$ באשר $\text{sols}_{\overline{\mathbb{K}}}(f)=\{\alpha_i\mid i\in[n]\}$ אזי $\text{disc}(f)=\prod_{\substack{i,j\in[n]\\ i<j}}(\alpha_i-\alpha_j)^2$.

טענה: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ מתוקן אזי ($\text{disc}(f)\neq 0$)$\Longleftrightarrow$(f ספרבילי).

טענה: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]$ מתוקן אזי $\text{disc}(f)\in\mathbb{K}$.

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

טענה: יהי $\mathbb{K}$ שדה באשר $\text{char}(\mathbb{K})\neq 2$ ויהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי אזי ($\text{Gal}(f)\le A_n$)$\Longleftrightarrow$($\text{disc}(f)\in\square_{\mathbb{K}}$).

טענה: תהא $\mathbb{L}/\mathbb{Q}$ הרחבה ציקלית ממעלה 4 אזי לא קיים $\alpha\in\mathbb{L}$ עבורו $\alpha^2\in\mathbb{Q}_{<0}$.

מסקנה: יהי $f\in\mathbb{Q}[x]$ אי־פריק באשר $\deg(f)=4$ וכן $\text{disc}(f)<0$ אזי $\text{Gal}(f)$ אינה ציקלית.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי באשר $\deg(f)=3$ אזי

- אם $|\text{sols}_{\mathbb{K}}(f)|=3$ אז $\text{Gal}(f)\simeq\{0\}$.
- אם $|\text{sols}_{\mathbb{K}}(f)|=1$ אז $\text{Gal}(f)\simeq\mathbb{Z}_2$.
- אם f אי־פריק וכן $\text{disc}(f)\in\square_{\mathbb{K}}$ אז $\text{Gal}(f)\simeq A_3$.
- אם f אי־פריק וכן $\text{disc}(f)\notin\square_{\mathbb{K}}$ אז $\text{Gal}(f)\simeq S_3$.

הרזולבנטה הקובית: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי באשר $\deg(f)=4$ ויהי $\alpha\in\overline{\mathbb{K}}^4$ באשר $\text{sols}_{\overline{\mathbb{K}}}(f)=\{\alpha_i\mid i\in[4]\}$ אזי $\mathcal{H}(f)(x)=(x-(\alpha_1+\alpha_2)(\alpha_3+\alpha_4))(x-(\alpha_1+\alpha_3)(\alpha_2+\alpha_4))(x-(\alpha_1+\alpha_4)(\alpha_2+\alpha_3))$.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי באשר $\deg(f)=4$ אזי $\mathcal{H}(f)\in\mathbb{K}[x]$.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי באשר $\deg(f)=4$ אזי $\text{disc}(\mathcal{H}(f))=\text{disc}(f)$.

טענה: יהי $\mathbb{K}$ שדה יהי $f\in\mathbb{K}[x]$ מתוקן ספרבילי באשר $\deg(f)=4$ אזי

- אם קיימים $g,h\in\mathbb{K}[x]$ אי־פריקים באשר $\deg(g)=\deg(h)=2$ וכן $f=gh$ וכן $\frac{\text{disc}(g)}{\text{disc}(h)}\in\square_{\mathbb{K}}$ אז $\text{Gal}(f)\simeq\mathbb{Z}_2$.
- אם קיימים $g,h\in\mathbb{K}[x]$ אי־פריקים באשר $\deg(g)=\deg(h)=2$ וכן $f=gh$ וכן $\frac{\text{disc}(g)}{\text{disc}(h)}\notin\square_{\mathbb{K}}$ אז $\text{Gal}(f)\simeq\mathbb{Z}_2\times\mathbb{Z}_2$.
- אם f אי־פריק אז קיים $H\in\{S_4,A_4,D_4,\mathbb{Z}_4,\mathbb{Z}_2\times\mathbb{Z}_2\}$ עבורו $\text{Gal}(f)\simeq H$.

טענה: יהי $q\in\mathbb{N}$ עבורו קיים שדה $\mathbb{F}_q$ יהי $n\in\mathbb{N}_+$ ונגדיר $f\in\mathbb{F}_q(t_0\ldots t_{n-1})[x]$ כך $f(x)=x^{q^n}+\sum_{i=0}^{n-1}t_ix^{q^i}$ אזי $\text{Gal}(f)\simeq\text{GL}_n(\mathbb{F}_q)$.

משפט קאפלאנסקי: יהיו $a,b\in\mathbb{Q}$ עבורם x^4+ax^2+b אי־פריק מעל $\mathbb{Q}[x]$ אזי

- אם $b\in\square_{\mathbb{Q}}$ אז $\text{Gal}(f)\simeq\mathbb{Z}_2\times\mathbb{Z}_2$.
- אם $b\notin\square_{\mathbb{Q}}$ וכן $b(a^2-4b)\in\square_{\mathbb{Q}}$ אז $\text{Gal}(f)\simeq\mathbb{Z}_4$.
- אם $b\notin\square_{\mathbb{Q}}$ וכן $b(a^2-4b)\notin\square_{\mathbb{Q}}$ אז $\text{Gal}(f)\simeq D_8$.

שדה ממשי פורמלי: שדה $\mathbb{K}$ המקיים $\text{char}(\mathbb{K})=0$ 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 $\text{char}(\mathbb{K})=0$ 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 $\mathrm{char}(\mathbb{K})=0$ אזי (קיים יחס $<_{\mathbb{K}}$ עבורו $\langle\mathbb{K},<_{\mathbb{K}}\rangle$ שדה סדור)$\iff$(קיימות $\mathbb{K}_+,\mathbb{K}_-\subseteq\mathbb{K}$ המקיימות $\mathbb{K}=(\mathbb{K}_+\uplus\mathbb{K}_-)\cup\{0\}$ 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 $f\in\mathbb{K}[x]$ באשר $\deg(f)\in\mathbb{N}_{\mathrm{odd}}$ אזי $\mathrm{sols}_{\mathbb{K}}(f)\neq\varnothing$.

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

מסקנה: $\mathbb{R}$ שדה ממשי סגור.

הכפלה באיבר: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ויהי $a\in\mathbb{L}$ אזי נגדיר $\Lambda_{\mathbb{L}/\mathbb{K},a}:\mathbb{L}\to\mathbb{L}$ כך $\Lambda_{\mathbb{L}/\mathbb{K},a}(\gamma)=a\cdot\gamma$.

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ויהי $a\in\mathbb{L}$ אזי $\Lambda_{\mathbb{L}/\mathbb{K},a}$ העתקה לינארית מעל $\mathbb{K}$.

נורמה של הרחבה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי נגדיר $N_{\mathbb{L}/\mathbb{K}}:\mathbb{L}\to\mathbb{K}$ כך $N_{\mathbb{L}/\mathbb{K}}(a)=\det\left(\Lambda_{\mathbb{L}/\mathbb{K},a}\right)$.

למה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי

- לכל $a,b\in\mathbb{L}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(ab)=N_{\mathbb{L}/\mathbb{K}}(a)\cdot N_{\mathbb{L}/\mathbb{K}}(b)$.
- לכל $a\in\mathbb{K}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(a)=a^{[\mathbb{L}:\mathbb{K}]}$.
- לכל $a\in\mathbb{L}$ מתקיים $(a=0)\iff\left(N_{\mathbb{L}/\mathbb{K}}(a)=0\right)$.

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי $\left(N_{\mathbb{L}/\mathbb{K}}\right)_{\restriction_{\mathbb{L}^\times}}:\mathbb{L}^\times\to\mathbb{K}^\times$ וכן $\left(N_{\mathbb{L}/\mathbb{K}}\right)_{\restriction_{\mathbb{L}^\times}}$ הומומורפיזם חבורות.

משפט חישוב של נורמה בעזרת פולינום מינימלי: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי

- לכל $a\in\mathbb{L}$ מתקיים $M_{\Lambda_{\mathbb{L}/\mathbb{K},a}}(x)=f_a(x)$.
- לכל $a\in\mathbb{L}$ מתקיים $P_{\Lambda_{\mathbb{L}/\mathbb{K},a}}(x)=f_a(x)^{[\mathbb{L}:\mathbb{K}(a)]}$.
- לכל $a\in\mathbb{L}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(a)=(-1)^{[\mathbb{L}:\mathbb{K}]}\cdot f_a(0)^{[\mathbb{L}:\mathbb{K}(a)]}$.

איברים צמודים: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ויהי $a\in\mathbb{K}$ אזי $\mathrm{sols}_{\overline{\mathbb{K}}}(f_a)$.

משפט חישוב של נורמה בעזרת איברים צמודים: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ספרבילית אזי

- לכל $a\in\mathbb{L}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(a)=\left(\prod_{s\in\mathrm{sols}_{\overline{\mathbb{K}}}(f_a)}s\right)^{[\mathbb{L}:\mathbb{K}(a)]}$.
- לכל $a\in\mathbb{L}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(a)=\prod_{\varphi\in\left(\mathbb{L}/\mathbb{K}\hookrightarrow\overline{\mathbb{K}}/\mathbb{K}\right)}\varphi(a)$.
- אם $\mathbb{L}/\mathbb{K}$ הרחבת גלואה אז לכל $a\in\mathbb{L}$ מתקיים $N_{\mathbb{L}/\mathbb{K}}(a)=\prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{K})}\sigma(a)$.

מסקנה טרנזיטיביות של נורמה: יהיו $\mathbb{K},\mathbb{F},\mathbb{L}$ שדות באשר $\mathbb{L}/\mathbb{F},\mathbb{F}/\mathbb{K}$ הרחבות סופיות אזי $N_{\mathbb{L}/\mathbb{K}}=N_{\mathbb{F}/\mathbb{K}}\circ N_{\mathbb{L}/\mathbb{F}}$.

עקבה של הרחבה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי נגדיר $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}:\mathbb{L}\to\mathbb{K}$ כך $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)=\mathrm{trace}\left(\Lambda_{\mathbb{L}/\mathbb{K},a}\right)$.

למה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית אזי $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ פונקציונל לינארי.

משפט חישוב של עקבה בעזרת פולינום מינימלי: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית יהי $a\in\mathbb{L}$ ויהי $m\in\mathbb{N}$ ויהי $\zeta\in\mathbb{K}^{\{0\ldots m\}}$ באשר $f_a=\sum_{i=0}^m\zeta_i\cdot x^i$ אזי $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)=-[\mathbb{L}:\mathbb{K}(a)]\cdot\zeta_{m-1}$.

משפט חישוב של עקבה בעזרת איברים צמודים: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית ספרבילית אזי

- לכל $a\in\mathbb{L}$ מתקיים $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)=[\mathbb{L}:\mathbb{K}(a)]\cdot\sum_{s\in\mathrm{sols}_{\overline{\mathbb{K}}}(f_a)}s$.
- לכל $a\in\mathbb{L}$ מתקיים $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)=\sum_{\varphi\in\left(\mathbb{L}/\mathbb{K}\hookrightarrow\overline{\mathbb{K}}/\mathbb{K}\right)}\varphi(a)$.
- אם $\mathbb{L}/\mathbb{K}$ הרחבת גלואה אז לכל $a\in\mathbb{L}$ מתקיים $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)=\sum_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{K})}\sigma(a)$.

מסקנה טרנזיטיביות של עקבה: יהיו $\mathbb{K},\mathbb{F},\mathbb{L}$ שדות באשר $\mathbb{L}/\mathbb{F},\mathbb{F}/\mathbb{K}$ הרחבות סופיות אזי $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}=\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}\circ\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}$.

מסקנה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה סופית באשר $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}=0$ אזי $\mathbb{L}/\mathbb{K}$ אינה ספרבילית.

טענה: יהיו $n,d\in\mathbb{N}_+$ באשר $d|n$ ויהי $a\in\mathbb{Q}_{>0}$ באשר x^n-a אי־פריק אזי $[\mathbb{Q}(\sqrt[d]{a}):\mathbb{Q}]=d$.

טענה: יהיו $n,d\in\mathbb{N}_+$ באשר $d|n$ יהי $a\in\mathbb{Q}_{>0}$ באשר x^n-a אי־פריק ויהי $\mathbb{F}$ שדה באשר $\mathbb{Q}\subseteq\mathbb{F}\subseteq\mathbb{Q}(\sqrt[d]{a})$ וכן $[\mathbb{F}:\mathbb{Q}]=d$ אזי $\mathbb{F}=\mathbb{Q}(\sqrt[d]{a})$.

טענה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה באשר $\mathbb{L}$ שדה סופי אזי $N_{\mathbb{L}/\mathbb{K}}$ על וכן $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ על.

טענה: יהי $\mathbb{K}$ שדה יהי $n\in\mathbb{N}_+$ יהי $f\in\mathbb{K}[x]$ באשר $\deg(f)=n$ ויהיו $\alpha_1\ldots\alpha_n\in\overline{\mathbb{K}}$ עבורם $\mathrm{sols}_{\overline{\mathbb{K}}}(f)=\{\alpha_i\mid i\in[n]\}$ אזי לכל $g\in\mathbb{K}[x]$ מתקיים $N_{\mathbb{K}(\alpha_1)/\mathbb{K}}(g(\alpha_1))=\prod_{i=1}^n g(\alpha_i)$.

טענה: יהי $\mathbb{K}$ שדה יהי $n\in\mathbb{N}_+$ יהי $\zeta\in\mathbb{K}^{\{0\ldots n\}}$ באשר $\zeta_n=1$ וכן $\sum_{i=0}^n\zeta_ix^i$ אי־פריק ספרבילי יהיו $\alpha_1\ldots\alpha_n\in\overline{\mathbb{K}}$ עבורם $\mathrm{sols}_{\overline{\mathbb{K}}}\left(\sum_{i=0}^n\zeta_ix^i\right)=\{\alpha_i\mid i\in[n]\}$ ויהיו $\eta,\beta\in\mathbb{K}$ אזי $N_{\mathbb{K}(\alpha_1)/\mathbb{K}}(\eta\alpha_1+\beta)=\sum_{i=0}^n(-1)^i\zeta_{n-i}\beta^{n-i}\eta^i$.

טענה: יהי $\mathbb{K}$ שדה יהי $n\in\mathbb{N}_+$ יהי $\zeta\in\mathbb{K}^{\{0\ldots n\}}$ באשר $\zeta_n=1$ וכן $\sum_{i=0}^n\zeta_ix^i$ אי־פריק ספרבילי יהיו $\alpha_1\ldots\alpha_n\in\overline{\mathbb{K}}$ עבורם $\mathrm{sols}_{\overline{\mathbb{K}}}\left(\sum_{i=0}^n\zeta_ix^i\right)=\{\alpha_i\mid i\in[n]\}$ אזי $\mathrm{Tr}_{\mathbb{K}(\alpha_1)/\mathbb{K}}\left(\alpha_1^2\right)=\zeta_{n-1}^2-2\zeta_{n-2}$.

טענה: יהי $\mathbb{K}$ שדה יהי $n \in \mathbb{N}_+$ יהי $f \in \mathbb{K}[x]$ באשר $\deg(f) = n$ ויהיו $\alpha_1 \ldots \alpha_n \in \overline{\mathbb{K}}$ עבורם $\mathrm{sols}_{\overline{\mathbb{K}}}(f) = \{\alpha_i \mid i \in [n]\}$ אזי $\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}} \cdot N_{\mathbb{K}(\alpha_1)/\mathbb{K}}(f'(\alpha_1))$.