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 $R\left[x_1\ldots x_n\right]$ חוג אבלי בעל יחידה.

טענה: יהי R חוג אבלי בעל יחידה אזי $\langle R\left[x\right],+,\text{קונבולוציה}\rangle$ 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 תחום שלמות ויהי $n\in\mathbb{N}_+$ אזי $R\left[x_1\ldots x_n\right]$ 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 $\left(R\left[x\right]\right)^\times=R^\times$.

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 $\sim_{\text{Frac}}=\left\{\left((a,b),(c,d)\right)\in\left(R\times\left(R\backslash\{0\}\right)\right)^2\mid ad=bc\right\}$.

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

הגדרה: יהי R תחום שלמות באשר $R\neq\{0\}$ ויהיו $(a,b),(c,d)\in R\times\left(R\backslash\{0\}\right)$ אזי $\left[(a,b)\right]_{\text{Frac}}+\left[(c,d)\right]_{\text{Frac}}=\left[(ad+cb,bd)\right]_{\text{Frac}}$ וכן $\left[(a,b)\right]_{\text{Frac}}\cdot\left[(c,d)\right]_{\text{Frac}}=\left[(ac,bd)\right]_{\text{Frac}}$.

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

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

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

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

הומומורפיזם בין חוגים: יהיו R,S חוגים אזי $\nu:R\to S$ המקיימת
- משמרת כפל: לכל $a,b\in R$ מתקיים $\nu\left(ab\right)=\nu\left(a\right)\nu\left(b\right)$.
- משמרת חיבור: לכל $a,b\in R$ מתקיים $\nu\left(a+b\right)=\nu\left(a\right)+\nu\left(b\right)$.

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

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

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

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

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: $\mathbb{Z}\left[i\right]=\mathbb{Z}+i\mathbb{Z}$.

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 $\ker\left(\nu\right)$ 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 (ν מונומורפיזם)$\vee(\nu=0)$.

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

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

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

טענה: יהי R חוג אבלי בעל יחידה ויהי $I \subseteq R$ אזי (I 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.

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 $\mathbb{Q}[x]$.

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

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

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

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

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

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

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

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

הומומורפיזם הרחבות: יהיו $\mathbb{K},\mathbb{F},\mathbb{L}$ שדות באשר $\mathbb{K}/\mathbb{F}$ הרחבה וכן $\mathbb{L}/\mathbb{F}$ הרחבה אזי שיכון $\nu:\mathbb{K}/\mathbb{F}\to\mathbb{L}/\mathbb{F}$ המקיים $\nu_{\restriction_\mathbb{F}}=\mathrm{Id}_\mathbb{F}$.

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

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

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

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

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

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 $\mathrm{sols}(ax^2+bx+c)=\left\{\frac{-b\pm\sqrt{b^2-4ac}}{2a}\right\}$.

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

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

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

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

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

משפט: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהי $\alpha\in\mathbb{L}$ אלגברי מעל $\mathbb{K}$ אזי קיים ויחיד פולינום מינימלי $f_\alpha\in\mathbb{K}[x]$ עבור α וכן $(f_\alpha)=\{f\in\mathbb{K}[x]\mid f(\alpha)=0\}$.

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

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

חוג נוצר: יהיו A,B חוגים אבליים בעלי יחידה באשר $A\subseteq B$ תהא $S\subseteq B$ ויהי $R\subseteq B$ החוג האבלי בעל יחידה המינימלי המקיים $A\cup S\subseteq R$ 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 ויהיו $\alpha_1\ldots\alpha_n\in\mathbb{L}$ אזי $\mathbb{K}(\alpha_1\ldots\alpha_n)=\bigcup_{n=1}^{\infty}\bigcup_{f,g\in\mathbb{K}[x_1\ldots x_n]}\left\{\frac{f(s_1\ldots s_n)}{g(s_1\ldots s_n)}\,\middle|\,\substack{s_1\ldots s_n\in S\\ g(s_1\ldots s_n)\neq0}\right\}$.

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

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

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

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

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

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

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

משפט מולטיפליקטיביות של דרגה: תהיינה $\mathbb{F}/\mathbb{L},\mathbb{L}/\mathbb{K}$ 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 $\mathbb{K}$)$\iff$(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.

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.

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

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 $\deg(f)\geq 1$ 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 $\deg(f_\tau)\geq 1$ 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 $\nu:\mathbb{K}\to\mathbb{F}$ מונומורפיזם אזי קיים מונומורפיזם $\Phi:\mathbb{L}\to\mathbb{F}$ המקיים $\Phi_{\restriction_{\mathbb{K}}}=\nu$. דורש AC

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

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

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 ($\mathbb{K}(x)=\mathbb{K}(a)$)$\iff$(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 $\varphi\in\mathrm{Aut}(\mathbb{K}(x))$ 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 $u_1 \dots u_m \in \mathbb{L}$ 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.

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 $r \geq s$ וכן קיימת $S \subseteq \{a_1 \dots a_r\}$ באשר $|S| = s$ עבורה $\{a_1 \dots a_r, b_1 \dots b_s\} \backslash S$ 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 $\text{degtr}_{\mathbb{K}}(\mathbb{L}) = |\mathcal{B}|$.

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

שדה פיצול: יהי $\mathbb{K}$ שדה ויהי $f \in \mathbb{K}[x]$ באשר $\deg(f) \geq 1$ אזי שדה $\mathbb{F}$ באשר $\mathbb{K} \subseteq \mathbb{F}$ וכן f מתפרק לגורמים לינאריים מעל $\mathbb{F}$ וכן לכל שדה $\mathbb{F} \subset \mathbb{L}$ מתקיים כי f אינו מתפרק לגורמים לינאריים מעל $\mathbb{L}$.

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 $\mathbb{F}/\mathbb{K} \simeq \mathbb{L}/\mathbb{K}$.

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

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

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 $\overline{\mathbb{K}}/\mathbb{F}$ המקיימת $\mathbb{F}/\mathbb{K} \simeq \mathbb{L}/\mathbb{K}$ אזי $\mathbb{F} = \mathbb{L}$.
- 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.