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.

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 $R[x_1\dots x_n]$ 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 $\mathbb{F}^\times=\mathbb{F}\setminus\{0\}$.

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

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

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

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

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

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

מסקנה: יהי $\mathbb{K}$ 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 $\nu(a+b)=\nu(a)+\nu(b)$.

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.

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

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

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

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

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

אידאל ראשי: יהי R חוג אבלי אזי אידאל $I\subseteq R$ עבורו קיים $a\in R$ המקיים $I=aR$.

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 $I\subseteq J$.

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).

משפט: יהי $\mathbb{K}$ שדה אזי

- לכל אידאל $I\subseteq\mathbb{K}[x]$ מתקיים כי I אידאל ראשי.
- יהי $f\in\mathbb{K}[x]$ אזי ($\langle f\rangle$ מקסימלי)$\iff$($\langle f\rangle$ ראשוני)$\iff$(f אי־פריק ב־$\mathbb{K}[x]$).

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

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 $d\in\mathbb{Z}[x]$.

שורש של פולינום: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]\setminus\{0\}$ אזי $\alpha\in\mathbb{K}$ המקיים $f(\alpha)=0$.

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

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

שורש פשוט: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]\setminus\{0\}$ אזי $\alpha\in\mathbb{K}$ באשר α שורש של f וכן $(x-\alpha)^2\nmid f$.

שורש מרובה: יהי $\mathbb{K}$ שדה ויהי $f\in\mathbb{K}[x]\setminus\{0\}$ אזי $\alpha\in\mathbb{K}$ באשר α שורש של f וכן $(x-\alpha)^2|f$.

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

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

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

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

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

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

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

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 $\langle f_\alpha\rangle=\{f\in\mathbb{K}[x]\mid f(\alpha)=0\}$.

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.

הרחבה נוצרת: תהא $\mathbb{L}/\mathbb{K}$ הרחבה ויהיו $\alpha_1 \dots \alpha_n \in \mathbb{L}$ אזי השדה המינימלי $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ המקיים $\alpha_1 \dots \alpha_n \in \mathbb{F}$ וכן $\mathbb{K} \subseteq \mathbb{F}$.

הרחבה נוצרת: תהא $\mathbb{L}/\mathbb{K}$ הרחבה יהיו $\alpha_1 \dots \alpha_n \in \mathbb{L}$ ויהי $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ השדה המינימלי המקיים $\alpha_1 \dots \alpha_n \in \mathbb{F}$ וכן $\mathbb{K} \subseteq \mathbb{F}$ אזי $\mathbb{F}/\mathbb{K}$.

סימון: תהא $\mathbb{L}/\mathbb{K}$ הרחבה יהיו $\alpha_1 \dots \alpha_n \in \mathbb{L}$ ותהא $\mathbb{F}/\mathbb{K}$ הרחבה הנוצרת על ידי $\alpha_1 \dots \alpha_n$ אזי $\mathbb{K}(\alpha_1 \dots \alpha_n) = \mathbb{F}$.

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

הרחבה פשוטה: תהא $\mathbb{L}/\mathbb{K}$ ויהי $\alpha \in \mathbb{L}$ אזי $\mathbb{K}(\alpha)/\mathbb{K}$.

משפט מבנה של הרחבה פשוטה: תהא $\mathbb{L}/\mathbb{K}$ הרבה 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 $\mathbb{K}(\alpha)/\mathbb{K} \simeq \left(\mathbb{K}[x]/\langle f_\alpha \rangle\right)/\mathbb{K}$.

מסקנה: יהי $\mathbb{K}$ שדה יהי $f \in \mathbb{K}[x] \setminus \{0\}$ אי־פריק ויהיו $\alpha, \beta \in \mathbb{K}$ שורשים של f אזי קיים איזומורפיזם $\nu : \mathbb{K}(\alpha)/\mathbb{K} \to \mathbb{K}(\beta)/\mathbb{K}$ באשר $\nu(\alpha) = \beta$.

למה: תהא $\mathbb{L}/\mathbb{K}$ הרחבה יהיו $\alpha_1 \dots \alpha_n \in \mathbb{L}$ ויהי $\beta \in \mathbb{K}(\alpha_1 \dots \alpha_n)$ אזי קיים $f \in \mathbb{K}[x_1 \dots x_n]$ המקיים $f(\alpha_1 \dots \alpha_n) = \beta$.

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

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

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

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

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

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