פעולה בינארית בקבוצה S: כלל המתאים לכל זוג איברים של S (כל קומבינציה + כל איברים)

פעולה בינארית קומוטטיבית:[1] אם לכל $a,b \in S$ מתקיים $a \cdot b = b \cdot a$
(ה- $(\cdot)$ ב- S הקבוצה)

אסוציאטיבית: -ו- -ו- אם לכל $a,b,c \in S$ מתקיים $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

חבורה: תהי הקבוצה G ופעולה בינארית $(\cdot)$, זוג $\langle G, \cdot \rangle$ תיקרא חבורה אם מתקיים: 1) פעולה[1] קומוטטיבית
2) איבר אדיש $e \in G$: אדיש e זהו איבר מקיים, לכל $a \in G$ $e \cdot a = a$
3) איבר הופכי a^{-1}: לכל $a \in S$ קיים $a^{-1} \in G$ כך ש $a \cdot a^{-1} = e$, $a^{-1} \cdot a = e$

חבורה אבלית:[2] חבורה $\langle G, \cdot \rangle$ תיקרא אבלית אם לכל $g,h \in G$ מתקיים, $gh = hg$

חוג: תהי R הקבוצה ופעולות בינאריות $\cdot$ (כפל), $+$ (חיבור) כך שמתקיים: 1) $(R, +)$ חבורה[2] אבלית
2) קומוטטיביות[1] של פעולה כפל $(\cdot)$
3) פילוג[3] לפעולות כפל $(\cdot)$: לכל $a,b,c \in R$ מתקיים: א) $a(b+c) = ab + ac$
ב) $(b+c)a = ba + ca$ ← תנאי נוסף חובה כיוון כפל לא בהכרח קומוטטיבי

שדה: חוג, קומוטטיבי (לפעולות כפל), עם 1 (אדיש כפלי) ולכל איברי קבוצה $R - \{0\}$ קיים הופכי כפלי
הגדרה שקולה; R קבוצה וקיים פעולות פעולות בינאריות על R $\cdot$, $+$ כך שמתקיים: 1) $\langle R, + \rangle$ חבורה אבלית
2) $\langle R - \{0\}, \cdot \rangle$ חבורה אבלית
3) פילוג[3] לפעולות כפל $(\cdot)$:

הגדרה שקולה; R קבוצה וקיים פעולות פעולות בינאריות על R $\cdot$, $+$ כך שמתקיים: 1) $a \cdot b = b \cdot a$
לכל $a,b,c \in R$ 2) $(a+b)+c = a+(b+c)$
3) קיים איבר $0 \in R$ כך שלכל $a \in R$ $a + 0 = a$
4) לכל $a \in R$ קיים $-a \in R$ יחיד כך ש $a + (-a) = 0$
5) $a \cdot b = b \cdot a$
6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
7) אדיש כפלי 1
8) הופכי כפלי: לכל $a \in R - \{0\}$ $a \cdot a^{-1} = a^{-1} \cdot a = 1$
9) פילוג[3] לפעולות כפל $(\cdot)$:

הערה:[4] אם a,b שייכים לשדה ומתקיים $ab = 0$ אז לפחות אחד מהאיברים אפס.
הערה: הערה[4] נכונה רק לשדות. טענה אינה נכונה בחוגים.

מטריצה מסדר $n \times m$ מעל שדה F: טבלה m שורות n עמודות וכל איבר שייך לשדה F $(F^{m \times n})$

קוסט שמאלי של חבורה $\langle G, \cdot \rangle$ ואיבר $a \in G$: $\{ax \in G \mid x \in G\}$

$\mathbb{Z}_n$: קבוצת קוסטים של $\mathbb{Z}$, כאשר קוסט $C_n = \{n \cdot x \in \mathbb{Z} \mid x \in \mathbb{Z}\}$ ו $\mathbb{Z}_n = \{C_n \mid n \in \mathbb{Z}\}$

$\langle \mathbb{Z}_n, \cdot_n, +_n \rangle$: חוג, קומוטטיבי[1], עם 1.

טענה: אם n הוא ראשוני אז חוג $\langle \mathbb{Z}_n, \cdot, + \rangle$ הינו שדה.
הוכחה: כדי להוכיח זאת מספיק להראות $\langle \{1,2,\dots,n-1\}, \cdot_n \rangle$[5] חבורה. (נראה בכמה דרכים)

עקרון סדר טוב:[6] תהי $\emptyset \neq S \subseteq \mathbb{N}$ אז קיים איבר מינימלי ב S

למה של אוקלידס:[7] יהי $n \in \mathbb{Z}$, $m \in \mathbb{N}$ אז קיימים $r \in \{0,1,\dots,m-1\}$, $q \in \mathbb{Z}$ כך ש $n = qm + r$
הוכחה: עבור $r \geq 0$: $n = q \cdot m + r \Leftarrow r = n - qm$
נראה שקיים פתרון עבור $n > 0$: $q = 0$ $r = n$
$n < 0$: $q = n$ $r = n - nm = \overbrace{n(1-m)}^{+}$
נגדיר קבוצה $R = \{r \in \mathbb{Z} \mid r \geq 0, n = qm + r, q \in \mathbb{Z}\}$, $R \neq 0$ כי קיים פתרון 1 לפחות
לפי עקרון[6] הסדר הטוב קיים איבר מינימלי $r_0 \in R$ שהוא פתרון $n = q_0 m + r_0$
נראה $r_0 \leq m-1$ הוכחה / $n = q_0 m + r_0 \Rightarrow n = (q_0+1)m + (r_0 - m)$ $\in R$
נניח בשלילה $r_0 > m$ אז $r_0 - m$ גם פתרון
קיבלנו סתירה r_0 הוא פתרון מינימלי

למה של בזו:[8] יהי $a,b\in\mathbb{N}$ אז קיימים $x,y\in\mathbb{Z}$ כך ש $ax+by=\gcd(a,b)$ ($\gcd(a,b)=d$ מחלק משותף הגדול ביותר $d|a \wedge d|b$)

הוכחה $X=\{ax+by \mid x,y\in\mathbb{Z},\ ax+by\geq 1\} \neq \emptyset$ (כי $x=0$, $y=1$)

לפי עקרון[6] הסדר הטוב קיים x_0,y_0 כך ש $t=ax_0+by_0$ מינימלי

נותר להראות $t|a$ וגם $t|b$:

נראה $t|a$: לפי למה[7] של אוקלידס קיים $q\in\mathbb{Z}$ ו $r\in\{0,1,\dots,t-1\}$ כך ש $a=qt+r$

אם אכן $r\geq 1$ כי אז $r\in X$ ו $r<t$ סתירה לכך ש t איבר מינימלי $r=a-qt$

לכן $r=0$ לכן $a=qt$ $t|a$ $a-q(ax_0+by_0)$

בדומה אפשר להראות $t|b$.

טענה:[5] $\langle \{1,2,\dots,n-1\},\cdot_n \rangle^{\times}$ חבורה עם n ראשוני.

הוכחה: 1) פעולת כפל הומטוטי מוגדרת

2) לכל $a\in X$ $1\cdot_n a=a\cdot_n 1=a$

3) לפי למה[3] של בזו: לכל $a\in X$ $\alpha\cdot a+\beta\cdot n=\gcd(a,\overset{n\text{ ראשוני}}{n})=1$ $\Leftarrow$ $\alpha\cdot_n a=1$

מטריצות מעל שדה: טבלה $\overset{\text{שורות}}{m}\times\overset{\text{עמודות}}{n}$ של איברים משדה מסוים

הערה: מערכת משוואות ניתן לתאר בעזרת מטריצות (ולפתור בעזרת דירוג)

הערה: מערכת משוואות מעל שדה סופי לא אתכן שיהיה אינסוף פתרונות אלא מספר סופי כי שדה סופי (שכן יש למערכת 3 מקרים: אין פתרון, פתרון יחיד, אינסוף)