הגדרות לאלגברה מודרנית

חבורה : קבוצה G עם פעולה * בין איבריה כך שמתקיימות 4 דרישות :

1. סגירות לכפל
2. קיום איבר אדיש
3. אסוציאטיביות $(a*b)*c=a*(b*c)$
4. קיום הופכי לכל איבר

תת חבורה : קבוצה לא ריקה H המוכלת או שווה לחבורה G ומהווה חבורה בעצמה עבור אותה פעולה של G. תנאי מספיק לתת חבורה : סגירות לכפל וקיום הופכי ואם G סופית אז רק סגירות.

חבורה אבלית (קומטטיבית) : חבורה בה לכל שני איברים a,b מתקיים : $a*b=b*a$

חבורה ציקלית : חבורה אשר כל איבר בה הוא חזקה של איבר קבוע $<g>$ הנקרא יוצר של החבורה.

תת חבורה נורמלית : G חבורה, N תת חבורה נורמלית של G $(N\Delta G)$ אם $g\in G, n\in N \Rightarrow g^{-1}ng\in N$

סדר של חבורה : אם החבורה סופית, אזי סדר החבורה הוא מספר איבריה. אם החבורה אינסופית, אזי סדר החבורה הוא 0. $O(G)=|G|$ or 0

סדר של איבר : המספר K הקטן ביותר כך ש $a^k=e$

קוסט ימני : G חבורה, H תת חבורה. לכל $a\in G$ נגדיר $Ha=\{ha|h\in H\}$ וזהו קוסט (מחלקה) ימני.

כפל קוסטים : $(Ha)*(Hb)=(Hab)$

אינדקס : האינדקס של תת חבורה H של חבורה G הוא מס הקוסטים הימניים של H ב-G. $|G:H|$

שוויון קוסטים : $Ha=Hb \iff a*b^{-1}\in H$

הצמדת איברים : G חבורה, $a,b\in G$ אזי a,b יקראו צמודים אם קיים $x\in G$ כך ש : $x^{-1}ax=b$

תמורה : פונקציה חח״ע ועל מקבוצה סופית כלשהי לעצמה

מעגל באורך k : תמורה ב S_n שמסומנת $F=(a_1,a_2,a_3,\ldots,a_k)$ כך ש : $F(a_i)=a_{i+1}$ ו $F(a_k)=F(a_1)$ ו $F(b)=b$ לכל $b\neq a_i$

סדר של מעגל באורך k : k

סדר של תמורה : הכמק״ב של סדרי המעגלים הזרים המרכיבים אותה

חילוף (טרנספוזיציה) : מעגל באורך 2

תמורה זוגית : תמורה אשר ניתן לרשום אותה כמכפלה של מספר זוגי של חילופים וכדומה לאי זוגית

הומומורפיזם של חבורות : G_1,G_2 חבורות, פונקציה $\Phi:G_1\to G_2$ נקראת הומומורפיזם אם : $\Phi(a*b)=\Phi(a)*\Phi(b)$ לכל $a,b\in G_1$.

אפימורפיזם : הומומורפיזם על.

מונומורפיזם : הומומורפיזם חח״ע.

איזומורפיזם : הומומורפיזם חח״ע ועל.

גרעין של הומומורפיזם : $Ker(\Phi)=\{a\in G_1|\Phi(a)=e_2\}$ קבוצת כל האיברים ב G_1 ש Φ שולחת ל- e_2

תמונה של הומומורפיזם : $Im(\Phi)=\{b\in G_2|\Phi(a)=b$ כך ש $a\in G_1$ קיים$\}$

חבורת מנה : G חבורה, $N\Delta G$, אזי G/N מוגדר כאוסף הקוסטים של N ב- G עם הפעולה כפל קוסטים.

כפל חבורות : H,K חבורות, אזי $H*K=\{h*k|h\in H, k\in K\}$

חוג : קבוצה R עם שתי פעולות, + חיבור, * כפל, כך שמתקיימות 4 דרישות :
1. R חבורה אבלית לגבי + (איבר נטרלי יסומן ב- 0, הפכי של a יסומן ב $-a$)
2. R סגורה לגבי כפל
3. אסוציאטיביות $a(bc)=(ab)c$
4. דיסטריבוטיביות $a*(b+c)=ab+ac$

חוג עם יחידה : חוג שיש בו איבר נטרלי לגבי כפל אשר יסומן ב- 1.

חוג קומטטיבי : חוג שבו הכפל קומטטיבי

מחלק אפס : איבר $a\neq 0$ בחוג R יקרא מחלק אפס אם קיים $b\neq 0$ ב - R כך ש $ab=0$ או $ba=0$.

תחום שלמות : חוג קומטטיבי עם יחידה ללא מחלקי אפס

איבר הפיך : $a\in R$ הפיך אם קיים $b\in R$ כך ש : $ab=ba=1$

חוג עם חילוק : חוג עם יחידה שבו כל איבר שונה מאפס הוא הפיך

שדה : חוג קומטטיבי עם חילוק

מציין של שדה : המספר m הקטן ביותר כך ש $\underbrace{1+1+1+\ldots+1}_{m \text{ פעמים}}=0$ סימון : $Char(F)$

הומומורפיזם של חוגים : פונקציה $\Phi:R_1\text{->}R_2$ עבור R_1,R_2 חוגים כך ש :
$$\Phi(a+b)=\Phi(a)+\Phi(b)$$
$$\Phi(ab)=\Phi(a)\Phi(b)$$

אידיאל : R חוג. $I\neq 0$ תת קבוצה ב- R שמקיימת :
1. סגירות לחיסור
2. קיום בליעה : $a\in I,x\in R \Rightarrow ax\in I\ ,\ xa\in I$

קוסט של אידיאל : $a\in I$ אזי הקוסט של a הוא $I+a=\{x+b|x\in I\}$

חיבור קוסטים : $(I+a)+(I+b)=(I+a+b)$

אידיאל ראשי : R חוג קומטטיבי, $a\in R$, נסמן $(a)=\{ax|x\in R\}$ אידיאל ראשי

אידיאל מקסימלי : אידיאל אשר מכיל כל אידיאל אחר בחוג מלבד החוג עצמו ואינו החוג עצמו.

אידיאלים טריוויאלים : אידיאל האפס $I=\{0\}$ וכל החוג. $I=R$

מעלה של פולינום : מסומן $deg(F)$ החזקה n הגבוהה ביותר בפולינום עם מקדם שונה מאפס. a_nX^n
מעלת פולינום האפס אינה מוגדרת.

קוסט של פולינום : אם $f(x)$ פולינום ממעלה n אזי קוסט של $f(x)$ יראה כך : $(f(x)+g(x))$ כאשר $g(x)$ פולינום ממעלה קטנה מ- n או פולינום ה-0.

פולינום אי-פריק : $f(x)\in F(x)$ יקרא אי-פריק אמ"מ מחלקיו היחידים הם איברי F וכפולותיו באיברי F.

מחלק משותף מקסימלי של פולינומים : $0\neq f(x),g(x)\in F(x)$ אזי $d(x)\in F(x)$ יקרא ממ"מ של $f(x),g(x)$ אם :
1. $d(x)|f(x)\ ,\ d(x)|g(x)$
2. כל פולינום אחר שמחלק את $f(x),g(x)$ יהיה ממעלה קטנה או שווה ל – $d(x)$.
3. $d(x)$ מתוקן, כלומר מקדם החזקה הגבוהה ביותר הוא 1.