הרצאה 4

26 באפריל 2019

1 דוגמאות של חבורות

1.1 דוגמה 1 - U_n

$U_n = \{o \leq a < n | gcd(a,n) = 1\}$עם הפעולה כפל $mod(n)$.

למשל: $U_{10} = \{1,3,6,9\}$

עוד דוגמה מעניינת: $U_{12} = \{1,5,7,11\}$. בחבורה זו מתקיימת התכונה המעניינת: כל איבר הוא ההופכי של עצמו. לחבורה כזו יש שם מיוחד: חבורת קליין.

1.2 טענה: U_nחבורה

קל יחסית להוכיח אסוציאטיביות. נרצה להוכיח כי קיים הופכי.

1.2.1 הוכחה

צריך להוכיח כי מתקיים שלכל $a \in U_n$ קיים $k \in U_n$ כך ש-$k \cdot a = 1$.

נזכר כי מתקיים $(a,n) = 1 \iff \exists k,l \in U_n : ka + ln = 1$

מכיוון שאנחנו עושים כפל מודולו n, מתקיים: $ka = 1 - ln \equiv_n 1$. נשאלה השאלה: האם $k \in U_n$, כלומר מהגדרת U_n האם מתקיים $(k,n) = 1$? וזה בהחלט מתקיים כי המשפט המקורי (שכתבנו מה"זווית" של a תקף גם מהזווית של k) הוא אמ"מ, ולכן k זר ל-n.

להוכחה זו חסר רק להראות כי מכפלה של 2 מספרים ב-U_n היא גם ב-U_n (סגירות לפעולה). כלומר: אם $(a,n) = 1$ וגם $(b,n) = 1$ אזי $(ab,n) = 1$.

לפי הנתון, ולפי משפט (מהתזכורת מקודם) קיימים k,l כך ש-$ka + ln = 1$, כך גם עבור b קיימים k', l' כך ש-$k'b + l'n = 1$. נכפול את 2 המשוואות:

$kk'ab + (kal' + lk'b + ll'n)n = 1$ ולכן שוב מהמשפט, זהו צירוף של ab ושל n ולכן $(ab,n) = 1$.

2 דוגמה נוספת - U_7

$U_7 = \{1,2,3,4,5,6\}$ עם הפעולה כפל מודולו 7.

מתקיים: $(U_7, \cdot mod(n)) = (Z_7^*, \cdot)$.

הקדמה להמשך הסמסטר: Z_p הוא שדה (כלומר חבורה גם ביחס לכפל וגם ביחס לחיבור) כאשר p ראשוני.

3 הגודל של U_n

הגודל של U_n מסומן $|U_n|$ וגם $\Phi(n)$ וסדרת מספרים זו נקראת מספרי אויילר.

עבור 7 מתקיים $\Phi(7)=6$, ובכללי עבור p ראשוני $\Phi(p)=p-1$.

עוד דוגמה: $\Phi(1024)=\Phi(2^{10})=512$ שכן כל המספרים האי זוגיים עד 1024 זרים ל1024 (הוא מכפלה רק של 2)

דוגמה נוספת: $\Phi(120)$. מי זר ל-120 ? מתקיים $120=2^3\cdot 3\cdot 5$. כמה מספרים מתחלקים ב-2 או ב-3 או ב-5 ? נחסיר אותם מ-120, אך נשים לב שיש כפילויות (כאלה שמתחלקים גם ב-3 וגם ב-2 למשל). למעשה צריך להשתמש במשפט ההכלה וההפרדה. $120-120\cdot\frac{1}{2}-120\cdot\frac{1}{3}-120\cdot\frac{1}{5}+120\cdot\frac{1}{2}\cdot\frac{1}{3}+120\cdot\frac{1}{2}\cdot\frac{1}{5}+120\cdot\frac{1}{3}\cdot\frac{1}{5}-120\cdot\frac{1}{2}\cdot\frac{1}{3}\cdot\frac{1}{5}=32$

4 בניה של חבורות מחבורות קודמות

4.1 סכום ישר

חבורת כל הזוגות במספרים הממשיים:

$$(\mathbb{R}^2,+)=\{(x,y)|x\in\mathbb{R},y\in\mathbb{R}\}=\mathbb{R}\oplus\mathbb{R}$$

כאשר החיבור הישר מקיים: $(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$.

4.2 הגדרה

תהיינה G,H חבורות.

נסמן $G\oplus H=\{(g,h)|g\in G,h\in H\}$

ועבור פעולת הכפל מתקיים: $(g_1,h_1)\cdot(g_2,h_2)=(g_1g_2,h_1h_2)$.

די טריוואלי להראות שזו חבורה.

4.2.1 דוגמה

עבור החבורה $(Z_2,+)$ נביא לדוגמה את הסכום הישר עם עצמה: $(Z_2,+)\oplus(Z_2,+)$. כמה איברים יהיו בו ? כמו במכפלה קרטזית - 4 איברים: $Z_2\oplus Z_2=\{(1,0),(0,1),(0,0),(1,1)\}$.

האם החבורה הזו איזומורפית ל-Z_4 ? למרות שגם ב- Z_4 יש 4 איברים, לא מתקיימת איזומורפיות שכן ב-Z_4 לא מתקיימת תכונת חבורת קליין שכן מתקיימת בסכום הישר.

מסתבר שU_{12} איזומורפית ל-$Z_2\oplus Z_2$!

4.2.2 דוגמה

נביא לדוגמה את $Z_2\oplus Z_3$. יהיו בה 6 איברים: $Z_2\oplus Z_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

לדוגמה: $(0,2)+(1,2)=(1,1)$.

מה ההופכי של $(1,2)$? מתקיים $-(1,2)=(1,1)$.

מפתיע לגלות, כי $Z_2\oplus Z_3$ איזומורפית ל-Z_6.

4.2.3 טענה

אם $(a,b)=1$ אזי $Z_a\oplus Z_b\cong Z_{ab}$. זאת נוכיח בהמשך על ידי המושג תת חבורה שנגדיר כעת.

5 תת חבורה

בהינתן חבורה G, תת חבורה H היא תת קבוצה שהיא חבורה לגבי הפעולה ב-G. נסמן: $H < G$.

5.1 דוגמה

עבור החבורה $Z_6 = \{0,1,2,3,4,5\}$ קיימות תתי החבורות:
$H = \{0\}, H = \{0,2,4\}, H = \{0,3\}$

5.2 טענה

תת קבוצה לא ריקה H של G היא תת חבורה אם ורק אם H סגורה לפעולה (לכל $h_1, h_2 \in H$ מתקיים $h_1 \cdot h_2 \in H$) וסגורה להופכי (אם $h \in H$ אז גם $h^{-1} \in H$).

5.3 משפט לגראנז'

אם $H < G$ אזי מתקיים $|H|||G|$ (הגודל של H מחקל את הגודל של G).
מסקנה: לחבורה מסדר ראשוני יש רק שתי תתי חבורות - הטריויאליות.

5.4 הגדרה - סדר של איבר

תהא G חבורה, $g \in G$. הסדר של g שמסומן ב-$o(g)$ הוא ה-k הראשון כך ש-$g^k = g \cdot g \cdot g \cdots g = e$
נגדיר את הכפל $g^k = g \cdot g \cdots g$, ואם הפעולה היא חיבור: $g^k = g + g + g \cdots + g = k \cdot g$

5.5 משפט

סדר של איבר מחלק את סדר החבורה: $o(g)||G|$

5.6 חבורת החזקות של איבר

יהא g איבר מסדר k.
נגדיר: $< g >= \{g^0 = e, g^1 = g, \cdots g^{k-1}\}$. נשים לב שיש כאן k איברים.

5.6.1 טענה

מתקיים $< g >< G$ כלומר $< g >$ תת חבורה של G.
נוכיח:
סגירות לכפל: $g^i, g^j \in < g >$, נראה כי $g^i g^j \in < g >$. מתקיים $g^i g^j = g^{i+j}$. זה כמעט טוב לנו.
מתקיים: $g^{i+j} = g^{(i+j)(modk)} \in < g >$ ולכן יש סגירות לכפל.
סגירות להופכי: $(g^i)^{-1} = g^{k-i}$. מתקיים: $g^i g^{k-i} = g^k = e$ ולכן תמיד קיים הופכי ב $< g >$.

5.7 משפט

אם G סופית, אז לכל איבר $g \in G$ יש סדר, כלומר יש k כך ש-$g^k = e$.

5.7.1 הוכחה

נסמן $|G| = n$. נתבונן ב-$g, g^2, g^3 \cdots g^k, g^{k+1}$.

אם אחד מהם שווה e - זה מוכיח את הנדרש.

אחרת יש ל-g^i רק $n-1$ אפשרויות, ולכן לפי עקרון שובך היונים יש לפחות 2 בעלי אותו הערך. כלומר $g^i = g^j$ ובפירוט: $gg \cdots g = gggg \cdots g$. אם נצמצם ב g^j נקבל: $e = g^{j-i}$. ולכן קיימת חזקה שמביאה לנו את e כנדרש.