תרגיל(קצת תורת המספרים$\mathbb{Z}$)

1. אם d הוא מחלק משותף של a,b אזי $d \mid \gcd(a,b)$
2. אם m הוא כפולה משותפת של a,b אזי $\operatorname{lcm}(a,b) \mid m$

פתרון

1. ראינו בתרגיל הראשון(משפט הgcd) שקיימים u,v שלמים כך ש= $\gcd(a,b)$ $d \mid \gcd(a,b) \Leftarrow au+bv$
2. נחלק את m ב$\operatorname{lcm}(a,b)$ עם שארית: קיימים q,r שלמים $m=\operatorname{lcm}(a,b)\,q+r$

$$0 \le r < |\operatorname{lcm}(a,b)|$$

$$r = m - \operatorname{lcm}(a,b)\,q$$

לכן r מתחלק בa,b, כלומר r הוא כפולה משותפת. אם $r \neq 0$ אזי סתירה למינימליות של $\operatorname{lcm}(a,b)$. לכן $r=0$ ולכן הטענה מתקיימת.

הגדרה

בהנתן שתי חבורות $\begin{matrix}(G,*_G,e_G)\\(H,*_H,e_H)\end{matrix}$ נאמר שH <u>תת חבורה</u> של G, ונסמן $H \le G$, אם מתקיימים:

א. $H \subseteq G$ (H תת קבוצה של G)

ב. לכל $a,b \in H$ מתקיים $a *_H b = a *_G b$

טענה

נשים לב ש$e_H = e_G$:
יהי $h \in H$

$$h *_G e_H = h *_H e_H = h$$

נכפיל בh^{-1} משמאל

$$e_H = e_G *_G e_H = \left(h^{-1} *_G h\right) *_G e_H = \left(h^{-1} *_G h\right) = e_G$$

G תת חבורה?

- נתונה תת קבוצה H של G וצריך לבדוק האם H מקיימת את הקסיומות החבורה תחת $*_G$
- נתונות שתי חבורות ובודקים האם אחת מוכלת בשניה ושהפעולה תואמת

דוגמאות

1. $(\mathbb{Z},+,0)\le(\mathbb{Q},+,0)\le(\mathbb{R},+,0)$
2. $(\mathbb{Z}_8,+,0)$. האם $\mathbb{Z}_8 \le \{0,1\}$? <u>לא!</u> $1+1\equiv 2\,(\mathrm{mod}8)\notin\{0,1\}$ לכן לא מתקיימת סגירות.
3. האם $(\mathbb{Z},+,0)\le(\mathbb{N},+,0)$? לא! לא מתקיימת אקסיומת האיבר ההפכי. 1 לא הפיך כי $-1\notin\mathbb{N}$
4. $\mathbb{Z}_8\le\{0,4\}$? כן. ניתן לעבור על האקסיומות ולבדוק.
<u>טענה</u>: $H\le K$ וגם $G\le H \Leftarrow G\le k$
5. $\mathbb{Z}_6\le\mathbb{Z}_3$? לא! הפעולה אחרת: $\begin{array}{c}1+2=0\,(\mathrm{mod}3)\\ 1+2\equiv 3\,(\mathrm{mod}6)\end{array}$. בצורה דומה $\mathbb{Z}\not\le\mathbb{Z}_n$
6. $(\mathbb{C}^*,\cdot,1)$. מעגל היחידה:

$$S^1:=\{z\in\mathbb{C}^*||z|=1\}\le\mathbb{C}^*$$

$\{z\in S^1\big|z^n=1\}:\Omega_n$ שורשי היחידה ה-nים ב-$\mathbb{C}^*$.

$$\Omega_n\le S^1\le\mathbb{C}^*$$

$$-1\in\Omega_2$$

$$-i,i\in\Omega_4$$

לכל $z\in S^1$ קיימת הצגה $\mathrm{cis}x=\cos x+i\sin x$. קיימת זהות: $\mathrm{cis}\,(x)\cdot\mathrm{cis}\,(y)=\mathrm{cis}\,(x+y)$ $\Leftarrow$ סגירות.

$$|\mathrm{cis}x|=\cos^2 x+\sin^2 x=1$$

נראה סגירות ב-Ω_n:

$$a,b\in\Omega_n\Rightarrow a^n=b^n=1$$

$$(ab)^n=a^nb^n=1\cdot1=1$$

$$\Rightarrow ab\in\Omega_n$$

איבר יחידה:

$$1\in\Omega_n$$

לכל n(כי $1^n=1$)
אסוצ': נובעת מ-$\mathbb{C}^*$
<u>הפכי</u>: אם $a\in\Omega_n$ אזי $a^n=1$

$$\left(a^{-1}\right)^n=(a^n)^{-1}=1^{-1}=1$$

ולכן $a^{-1}\in\Omega_n$.

משפט קיצור הדרך I:

תהי $G\subseteq H\neq\emptyset$. אזי $H\leq G$ אם ורק אם:

א. $\forall a,b\in H\ a*_G b\in H$(סגירות)

ב. $\forall a\in H\ a^{-1}\in H$(ההפכי של a ב-G)

משפט קיצור הדרך II:

תהי $G\subseteq H\neq\emptyset$, אזי $H\leq G$ אם ורק אם $\forall a,b\in H\ a*_G b^{-1}\in H$

תרגיל

הראו שהתת חבורות היחידות של $(\mathbb{Z},+,0)$ הן מהצורה $n\mathbb{Z}$ כאשר $n\geq 0$

הערות

$$n\mathbb{Z}=\{nk|k\in\mathbb{Z}\}=\{...,-2n,-n,0,n,2n,3n,...\}$$

כלומר כל המספרים השלמים שמתחלקים ב-n. לדוגמה

$$2\mathbb{Z}=\{...,-4,-2,0,2,4,6,...\}$$

כש-$n=0$ נקבל $0\mathbb{Z}=\{0\}$

$$-n\mathbb{Z}=n\mathbb{Z}$$

<u>טרמינולוגיה</u>: $G=\{e\}$ נקראת החבורה הטריויאלית.

פתרון תרגיל

שני חלקים:

א. $n\mathbb{Z}\leq\mathbb{Z}$ לכל $n\geq 0$. נשתמש בקיצור דרך II:

$$0,n\in n\mathbb{Z}\Rightarrow n\mathbb{Z}\neq\emptyset$$

יהיו $a,b\in n\mathbb{Z}$, צריך להוכיח $a-b\in n\mathbb{Z}$:

$$a,b\in n\mathbb{Z}\Rightarrow n\mid a,b\Rightarrow n\mid a-b\Rightarrow a-b\in n\mathbb{Z}$$

לכן $n\mathbb{Z}\leq\mathbb{Z}$

ב. $\mathbb{Z} \geq H \Leftarrow$ קיים m כך ש$H = m\mathbb{Z}$

תהי $\mathbb{Z} \geq H$ נניח $H \neq \{0\}$ונשים לב שבכל $n\mathbb{Z}$, $n > 0$ מתקיים n הוא המספר השלם החיובי הקטן ביותר.]

יהי $m \in H$ המספר החיובי הקטן ביותר. נראה שבהכרח $H = m\mathbb{Z}$.

ידוע ש$m \in H$, ובגלל הסגירות $m+m \in H$, וגם $-m \in H$, ואז באינדוקציה אפשר להראות $km \in H$ לכל $k \in \mathbb{Z} \Leftarrow m\mathbb{Z} \subseteq H$

יהי $t \in H$. נראה $m \mid t$. נחלק עם שארית: קיימים q, r שלמים כך ש$t = mq + r$

$$0 \leq r < |m|$$

אם $r \neq 0$:

$$r = t - mq$$

$$\Rightarrow r \in H$$

סתירה למינימליות m

$$\Rightarrow r = 0$$

$$\Rightarrow m \mid t$$

$$\Rightarrow t \in m\mathbb{Z}$$

$$\Rightarrow H \subseteq m\mathbb{Z}$$

$$\Rightarrow H = m\mathbb{Z}$$

תרגיל

אם G חבורה סופית, $\emptyset \neq H \subseteq G$ אזי

$$\Leftrightarrow \emptyset \neq H \subseteq G$$

$$\forall x, y \in H \;\; x *_G y \in H$$

פתרון

⇐מתקיים לפי אקסיומת הסגירות.
⇐:נשאר להוכיח ש$\forall a \in H \Rightarrow a^{-1} \in H$ (לפי קיצור הדרך I).
יהי $a \in H$, ניצור סדרה של איברים $a, a^2, a^3, a^4, ...(\in H)$. לא ייתכן שכל האיברים בסדרה שונים כי החבורה סופית ⇐ קיים k, j כך ש$k > j$ וגם $a^k = a^j$ ⇐ נכפיל בa^{-j} את שני הצדדים (בG)

$$e = a^{k-j} = a \cdot a^{k-j-1} = a^{k-j-1} \cdot a$$

$$\Rightarrow a^{-1} = a^{k-j-1} \in H$$

משפט 1

אם $H, K \leq G$ אזי $H \cap K \leq G$

משפט 2

אם נתון אוסף $\{H_i\}_{i \in I}$ של ת"ח של G אזי $\bigcap\limits_{i \in I} H_i \leq G$

תרגיל

הראו ש$z\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}\,(a,b)\,\mathbb{Z}$.

פתרון

יהי $x \in a\mathbb{Z} \cap b\mathbb{Z} \Leftrightarrow b \mid x$ וגם $a \mid x \Leftrightarrow x$ כפולה משותפת של $a, b \Leftrightarrow \text{lcm}\,(a,b) \mid x \Leftrightarrow x \in \text{lcm}\,(a,b) \Leftrightarrow a\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}\,(a,b)\,\mathbb{Z}$.

תת חבורה ציקלית

תהי G חבורה, יהי $a \in G$:

$$\langle a \rangle := \{a^n | n \in \mathbb{Z}\}$$

נטען ש$\langle a \rangle \leq G$. נקרא ל$\langle a \rangle$ התת"ח הציקלית הנוצרת ע"י a.

הוכחה

לפי משפט קיצור הדרך II:
$\langle a \rangle \neq \emptyset$ כי $a \in \langle a \rangle$. צ"ל $\forall x, y \in \langle a \rangle \; xy^{-1} \in \langle a \rangle$

$$x = a^m, y = a^n, xy^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle$$

הגדרה

נאמר שחבורה G היא ציקלית אם קיים $a \in G$ כך ש$G = \langle a \rangle$

תרגיל

אם G סופית אזי $\langle a \rangle = \{a^n | n \in \mathbb{N}\}$

פתרון

$$a, a^2, a^3, ...$$

$$a^k = a^j \Rightarrow a^{k-j}$$

צ"ל $a^{-j} \in B$ לכל $j \in \mathbb{N}$. $\left(a^{-j}\right) = \left(a^j\right)^{-1}$

$$a^j, a^{2j}, a^{3j}, ...$$

ונקבל כמו בתרגיל קודם $\left(a^j\right)^{-1} \in B$

דוגמאות

$$(\mathbb{Z}_6, +, 0)$$

$$\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$$

$$\langle 2 \rangle = \{2, 4, 0\}$$

$$\langle 3 \rangle = \{0, 3\}$$

$$\langle 5 \rangle = \{0, 5, 4, 3, 2, 1\}$$

1,5 יוצרים של החבורה $\mathbb{Z}_6$, לכן $\mathbb{Z}_6$ ציקלית.

$\mathbb{Z}$ ציקלית: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$\langle m \rangle = m\mathbb{Z}$