תרגול 5 שיעור

א. הפיכים של $\mathbb{Z}/m\mathbb{Z}$?

$\bar{a}$ הפיך, $\bar{a}\bar{x} = \bar{1}$, $\bar{a}, \bar{x}, \bar{1} \in \mathbb{Z}/m\mathbb{Z}$

$ax \equiv 1 \pmod m$

$d = \gcd(a,m)$

$d \mid 1$ שקול ל $d = 1$

כלומר $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ הפיך $\Leftrightarrow \gcd(a,m) = 1$.

$ax \equiv b \pmod m$ יש פתרון $\Leftrightarrow d \mid b$ כאשר $d = \gcd(a,m)$

כמה יש הפיכים ב- $\mathbb{Z}/m\mathbb{Z}$? $a = 0, 1, \ldots, m-1$

$\bar{a}$ הפיך אם a זר ל- m. $\gcd(a,m) = 1$

פונקציית אוילר: $\varphi(m) = \#\{a \mid \gcd(a,m) = 1, \ 1 \le a \le m-1\}$

דוגמא: $\varphi(5) = 4$, $\varphi(6) = 2$.

אם p ראשוני אז $\varphi(p) = p-1$.

מתק"מ: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ הינו שדה אם p ראשוני. $\bar{0}, \bar{1}, \ldots, \overline{p-1}$

אם $\bar{0} \neq \bar{a}$ אז ק"מ $\bar{a}$

אם m מורכב: $m = m_1 \cdot m_2$, $1 < m_1, m_2 < m$.

$\bar{0} = \bar{m} = \overline{m_1 m_2} = \bar{m}_1 \cdot \bar{m}_2$ ב- $\mathbb{Z}/m\mathbb{Z} \Rightarrow \bar{m}_1, \bar{m}_2$ מחלקי אפס לכן $\mathbb{Z}/m\mathbb{Z}$ אינו שדה!

מסקנה: $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ הינו הפיך $\Leftrightarrow \gcd(a,m) = 1$

יש בדיוק $\varphi(m)$ הפיכים (units) ב- $\mathbb{Z}/m\mathbb{Z}$.

החוג $\mathbb{Z}/m\mathbb{Z}$ הינו שדה $\Leftrightarrow m$ ראשוני.

משפט אוילר: אם $a \in \mathbb{Z}$, $m > 1$, $\gcd(a,m) = 1$ אז $a^{\varphi(m)} \equiv 1 \pmod m$.

(גרירה משותפת יותר)

מסקנה מהמשפט הקטן של פרמה: אם p ראשוני, $p \nmid a$ אז $a^{p-1} \equiv 1 \pmod p$

דוגמא: $p = 7$, $a = 2$, $2^6 = 64 \equiv 1 \pmod 7$ ו $3^6 \equiv 1 \pmod 7$.

הוכחה: $m = p$, $\varphi(m) = p-1$. $\gcd(a,p) = 1 \Leftrightarrow p \nmid a$ אוילר $\Rightarrow a^{p-1} \equiv 1 \pmod p$ ∎

תכונות ומוגדרים:

הגדרה: **מרכז** של חבורה G הוא $Z(G)=\{a\in G \mid \forall x\in G: ax=xa\}$.

(1) אלמנטי: $Z(x)=Z(Z(x))$

(2) $a\in G$ כך ש- $\forall x\in G \; ax=x=xa$

(3) לכל $a\in G$ קיים $b\in G$ כך ש- $ax=xb=y$.

הגדרה: f כלשהי מוגדרת **היטב** אם $f: X\to Y$ חח"ע ועל.

דוגמאות: $(\mathbb{Z},+)$ חבורה - יחידה: 0, $x^{-1}: -x$

$(\mathbb{Z}/m\mathbb{Z},+)$ *

הגדרה: G **חבורה** אם היא קבוצה כלשהי.

G **אבלית** אם היא חבורה ומתקיים $\forall a,b\in G: ab=ba$.

דוגמא של חבורות: $\mathbb{Z}/m\mathbb{Z}$ - קבוצת השיירים של $x(\mathbb{Z}/m\mathbb{Z})$.

הגדרה: R חוג. $(R)^\times = R^\times = \{x\in R \mid \exists y\in R: xy=yx=1\}$ קבוצת ההפיכים של R.

דוגמא: $\mathbb{Z}_x^\times$ חבורה.

טענה: לכל חוג R, $\mathbb{Z}_x^\times$ היא חבורה.

הוכחה: $x\in R^\times$ ו $y\in R^\times$. אזי קיימים $x',y'\in R$ כך ש- $xx'=1$, $yy'=1$.

$$(xy)(y'x') = x(yy')x' = x1x' = xx' = 1$$

לכן $xy\in R^\times$ ⇐ יש הפכיות ✓

משפט: $x(\mathbb{Z}/m\mathbb{Z})$ חבורה, $\#\mathbb{Z}_m^\times = \varphi(m)$.

⇐

חוק צמצום בחבורה:

אזי $a,b,c\in G$, G חבורה ומתקיים $ac=bc$ אזי $a=b$.

הוכחה: נתון $ac=bc$. נכפיל ב- c^{-1} מימין: $(ac)c^{-1}=(bc)c^{-1}$

$a(cc^{-1})=b(cc^{-1})$

$a=b$ ← $ae=be$

אזי $x\in R$ אזי קיים $y\in x$ כך ש- $xy=1=yx$ (R חוג) אזי $x\in R^\times$ ✓ (2)

מתקיים: $1\cdot 1=1$ לכן $1\in R^\times$ ✓ (1) $[\forall x\in R^\times \; x\cdot 1=x \Rightarrow \exists x\in R \; x\cdot 1=x]$

לכן $x\in R^\times \Rightarrow$ יש הפכיות ✓

$$1=xx'=x1x=x(yx)x'=(xy)(xx')$$

הוכחה: יהיו $x,y\in R^\times$. אזי קיימים $x',y'\in R$ כך ש- $xx'=1$, $yy'=1$.

טענה: לכל חוג R, $\mathbb{Z}_x^\times$ היא חבורה.

הגדרה: R חוג. $(R)^\times = R^\times = \{x\in R \mid \exists y\in R: xy=yx=1\}$ קבוצת ההפיכים של R.

דוגמא של חבורות: $x(\mathbb{Z}/m\mathbb{Z})$ - קבוצת השיירים של $\mathbb{Z}/m\mathbb{Z}$.

G **אבלית** אם היא חבורה ומתקיים $\forall a,b\in G: ab=ba$.

הגדרה: G **חבורה** אם היא קבוצה כלשהי.

$(\mathbb{Z}/m\mathbb{Z},+)$ *

דוגמאות: $(\mathbb{Z},+)$ חבורה - יחידה: 0, $x^{-1}: -x$

הגדרה: f כלשהי **מוגדרת היטב** אם $f: X\to Y$ חח"ע ועל.

(1) לכל $a\in G$ קיים $b\in G$ כך ש- $ax=y=xb$.

(2) $a\in G$ כך ש- $\forall x\in G \; ax=x=xa$

(3) אלמנטי: $Z(x)=Z(Z(x))$

הגדרה: **מרכז** של חבורה G הוא $Z(G)=\{a\in G \mid \forall x\in G: ax=xa\}$.

הגדרה: **תבונה** היא קבוצה a עם **פעולה** אחת $\cdot$ כש- הפעולה: $x\cdot y\to f_x$

תשעד תגלס 5:

טענה: תהי G חבורה אבלית סופית מסדר (וגדל) n. יהי $a\in G$

אזי, $a^n=1$.

הוכחה: כותבים $G=\{g_1,\dots,g_n\}$. נסתכל על $\{ag_1,ag_2,\dots,ag_n\}$ -

כולם שונים זה מזה. אחרת n אומרים שיש G שונים. לכן ההקבוצה

$\{ag_1,\dots,ag_n\}=G=\{g_1,\dots,g_n\}$. מכיוון ש-$G$ אבלית: $ag_1\cdot ag_2\cdot\dots\cdot ag_n=g_1\cdot\dots\cdot g_n$

G אבלית ⇓

$a^n g_1\cdot\dots\cdot g_n=g_1\cdot\dots\cdot g_n$

מהצמצום ⇓

$a^n=1$ ■

הוכחת משפט אוילר:

$(\mathbb{Z}/m\mathbb{Z})^*$ מתקיים: $\varphi(m)=\#(\mathbb{Z}/m\mathbb{Z})^*$. יהי $a\in\mathbb{Z}$, a זר ל-m,

אזי, $\bar{a}\in(\mathbb{Z}/m\mathbb{Z})^*$ ולפי הטענה $\bar{1}=\bar{a}^{\varphi(m)}$ ⇔ $a^{\varphi(m)}\equiv 1\ (m)$ ■

הגדרה: $\mathrm{ord}(x)$ של איבר בחבורה - $G\ni x$. כותבים: $\{e=x^0,x=x^1,x^2=\dots$

עד שמקבלים פעם ראשונה $e=x^k$. אזי k נקרא הסדר של x: $\mathrm{ord}(x):=k$ (k

אם אין k כזה כותבים $\mathrm{ord}(x)=\infty$.

דוגמאות: • $G=(\mathbb{Z}/7\mathbb{Z})^+$: $\mathrm{ord}_+(\bar{2})=3$ [$\bar{2}+\bar{2}=\bar{4}$, $\bar{2}+\bar{2}+\bar{2}=\bar{6}$ סה"כ

$\mathrm{ord}_+(\bar{3})=2$; $\mathrm{ord}_+(\bar{1})=0$

$G=(\mathbb{Z}/8\mathbb{Z})^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$:

$\mathrm{ord}(1)=1$ ⇐ $\bar{1}=\bar{1}^1$

$\mathrm{ord}(3)=2$ ⇐ $\bar{1}=\bar{3}^2$

$\mathrm{ord}(5)=2$ ⇐ $\bar{1}=\bar{5}^2$

$\mathrm{ord}(7)=2$ ⇐ $\bar{1}=\bar{7}^2$

טענה: יהי $G\ni x$. $\mathrm{ord}(x)=k<\infty$. יהי $m\in\mathbb{Z}$ כך ש-$x^m=1$ אזי: $\mathrm{ord}(x)\mid m$

הוכחה: כותבים $m=kq+r$ ($0\le r<k$).

אזי $x^r=x^r\cdot 1=x^r\cdot(x^k)^q=x^{r+kq}=x^m=1$

לכן כיוון ש-k הוא המינימלי שעבורו $x^k=1$. נקבל $r=0$ ⇒ $m=kq$ ■

מסקנה: יהי G חבורה סופית אבלית, $G\ni x$, אזי: $\mathrm{ord}(x)\mid\#G$

הוכחה: לפי הטענה $x^{\#G}=1$, והמסקנה מ"ד תתקיים.

דוגמא: $\mathbb{F}_7^* = (\mathbb{Z}/7\mathbb{Z})^*$. $\#\mathbb{F}_7^* = 6$

מהו אוסף כל $\mathbb{F}_7^*$ שמסדר 4.

תרגיל: $\mathbb{F}_7^* = \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$.

- $\bar{1}, \bar{2}, 2^2=4, 2^3=8=\bar{1}$ $\quad \text{ord}(2)=3$
- $\bar{1}, \bar{3}, 3^2=\bar{9}, 3^3=\bar{27}, 3^4=\bar{81}, 3^5=\bar{243}, 3^6=\bar{1}$ $\quad \text{ord}(3)=6$.

הגדרה: תהי G חבורה. $g \in G$. $\{g^n | n \in \mathbb{Z}\}$ שקולה ל G אומרים g הוא יוצר (generator) של G.

אם G יש יוצר אומרים ש G חבורה ציקלית.

דוגמא: * $(\mathbb{Z}, +)$ - חבורה ציקלית עם יוצרים 1, -1

* $(\mathbb{Z}/m\mathbb{Z}, +)$ - ציקלית

* מה ידוע $(\mathbb{Z}/m\mathbb{Z})^*$?

הכוונה ש $(\mathbb{Z}/7\mathbb{Z})^*$ ציקלית עם יוצר 3.