תזכורת:

פונקציה של אוילר $\varphi_n = |U_n| = |\{1 \le a \le n : gcd(a,n)=1\}|$

כיוון אם $n = p_1^{e_1} \dots p_r^{e_r}$

אזי $\varphi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i-1)$

בפרט אם p,q שני ראשוניים שונים, $n=pq$, אזי
$\varphi(n)=(p-1)(q-1)$

טענה:

יהי $n=pq$. אזי לחשב את $\varphi(n)$ זה קשה כמו לפרק את n לגורמים ראשוניים

הוכחה:

אם ידוע הפירוק לגורמים ראשוניים p,q אזי $\varphi(n)=(p-1)(q-1)$

להיפך, נניח כי n ו- $\varphi(n)$ ידועים. צריך למצוא את הגורמים p,q. אכן, נשים לב כי $\varphi(n)=pq-p-q+1=n+1-p-q$

$p+q=n+1-\varphi(n)$

הגורמים p,q הם השורשים של הפולינום הריבועי

$$(x-p)(x-q) = x^2-(p+q)x+pq = x^2+(\varphi(n)-n-1)x+n$$

ואם יודעים את $n,\varphi(n)$ אז יודעים את הפולינום הזה. לפי הנוסחא לפולינום ריבועי

$$p,q = \frac{n+1 \pm \sqrt{(\varphi(n)-n-1)^2-4n}}{2}$$

שימוש:

RSA (Rivest-Shamir-Adleman)

A רוצה להקים מערכת הצפנה שמאפשר לכל אחד לשלוח לו

הודעות מוצפנות.

ה"י מוצאת שני ראשוניים גדולים p,q. $n=pq$. ה"י בוחרת מספר זר ל-$\varphi(n)$. לפי אלגוריתם אוקלידס המורחב, ה"י מוצאת x,y כך ש $xe+\varphi(n)y=1=\gcd(e,\varphi(n))$ $\Leftarrow$ $xe\equiv 1 \mod \varphi(n)$

A מפרסמת את n,e (מפתח ציבורי)

ה"י שומרת בסוד את x (המפתח הפרטי)

Bob רוצה לשלוח הודעה $m\in\mathbb{Z}_n$ הוא שולח $c=m^e \pmod n$. A מקבלת c ה"י מעלה את c לחזקה x. $c^x=m^{ex}$. אבל לפי משפט אוילר $m^{\varphi(n)}\equiv 1 \pmod n$

אם m זר ל-n (ובכל מתוך n האיברים של $\mathbb{Z}_n$ רק $n-\varphi(n)=p+q+1$ לא זרים ל-n)

$m^{ex}\equiv m^1 \mod n$

$(ex\equiv 1 \mod \varphi(n))$

$m^{ex}=m\cdot m^{\varphi(n)z}$, $m^{\varphi(n)z}=1$

$n\sim 10^{2000}$ $p+q\sim 10^{1000}$

בהסתברות ש m לא זר ל-n $\frac{10^{1000}}{10^{2000}}\sim\frac{1}{10^{2000}}$ זניחה לחלוטין

פעולות של חבורות:

הגדרה: תהי G חבורה, תהי A קבוצה. הפעולה (שמאלית) של G על A היא העתקה $G\times A\to A$ שמקיימת:

1) לכל $a\in A$, $g_1,g_2\in G$ מתקיים $g_1*(g_2*a)=(g_1g_2)*a$

2) לכל $a\in A$ $e*a=a$

דוגמאות:

1) $G=S_n$ $\quad A=\{1,\dots,n\}$ $\quad \sigma\in S_n$, $a\in A$

$\sigma * a = \sigma(a)$

נבדוק את האקסיומות:

1) $\sigma,\tau\in S_n$ $\quad \sigma*(\tau*a)=\sigma(\tau(a))=(\sigma\circ\tau)(a)=(\sigma\tau)*a$

2) $e\in S_n$ $\quad e*a=e(a)=a$

2) A קבוצה כלשהי, לאו דווקא סופית

$G=S_A=\{f:A\to A:$ חח"ע ועל $\}$ $\quad f*a=f(a)$

3) $G=GL_n(\mathbb{R})$ $\quad A=\mathbb{R}^n$ $\quad g*a=\underset{n\times n}{g}\ \underset{n\times 1}{a}$

$\begin{pmatrix}1&2\\3&4\end{pmatrix}*\begin{pmatrix}\pi\\-1\end{pmatrix}=\begin{pmatrix}\pi-2\\3\pi-4\end{pmatrix}$

4) הגדרה: יהי V מרחב וקטורי n-מימדי מעל שדה $\mathbb{F}$. דגל שלם ב-V הינו סדרה של תת מרחבים

$(0)=V_0\subsetneq V_1\subsetneq\dots\subsetneq V_n=V$

כך ש $\dim_{\mathbb{F}}V_k=k$

למשל: $V=\mathbb{R}^3$ $\quad V_1=\left\langle\begin{pmatrix}1\\0\\0\end{pmatrix}\right\rangle$ $\quad V_2=\left\langle\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\rangle$

תהי A הקבוצה של כל הדגלים על $V=\mathbb{R}^n$

$G=GL_n(\mathbb{R})$ נחשוב על כל איבר $g\in G$ כהעתקה לינארית

$g:\mathbb{R}^n\to\mathbb{R}^n$ $\quad a=(V_1,\dots,V_n)$ $\quad g*a=(g(V_1),g(V_2),\dots,g(V_n))$

דוגמא: a דגל למשל $a=\left(V_1=\left\langle\begin{pmatrix}1\\0\\0\end{pmatrix}\right\rangle, V_2=\left\langle\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\rangle\right)$

$g=\begin{pmatrix}2&3&0\\1&1&0\\1&1&1\end{pmatrix}$ $\quad g*a=\left(\left\langle\begin{pmatrix}2\\1\\1\end{pmatrix}\right\rangle,\left\langle\begin{pmatrix}2\\1\\1\end{pmatrix},\begin{pmatrix}3\\1\\1\end{pmatrix}\right\rangle\right)$

4) תהי G חבורה $A=G$ $g*a=ga$. נבדוק את האקסיומות

1) $g_1*(g_2*a)=g_1*(g_2a)=g_1g_2a=g_1g_2*a$

2) $e*a=ea=a$

פעולה של G על עצמה על ידי כפל משמאל.

5) $G=A$ $g*a=ag$

$$g_1*(g_2*a)=g_1*(ag_2)=ag_2g_1 \neq ag_1g_2=(g_1g_2)*a$$

זו לא פעולה אם G לא אבלית

6) פעולה של חבורה G על עצמה על ידי הצמדה. G חבורה כלשהי. $A=G$ $g*a=gag^{-1}$. נבדוק אקסיומות

1) $g_1*(g_2*a)=g_1*(g_2ag_2^{-1})=g_1g_2ag_2^{-1}g_1^{-1}=(g_1g_2)a(g_1g_2)^{-1}=g_1g_2*a$

2) $e*a=eae^{-1}=a$

7) $G=\mathbb{R}$ עם פעולת חיבור. A קבוצה של הפו' הרציפות $f:\mathbb{R}\to\mathbb{R}$

יהי $r\in\mathbb{R}$, f פו' $(r*f)(x)=f(xe^r)+r$. נבדוק אקסיומות?

1) $(r_1*(r_2*f))(x)=(r_2*f)(xe^{r_1})+r_1=(f(xe^{r_1}e^{r_2})+r_2)+r_1=$

$=f(xe^{r_1+r_2})+r_1+r_2=((r_1+r_2)*f)x$

2) לכל $x\in\mathbb{R}$ $(0*f)(x)=f(xe^0)+0=f(x)$

הגדרה: פעולה של G על A נקראת טרנזיטיבית אם לכל זוג של איברים $a_1,a_2\in A$ קיים $g\in G$ כך ש $g*a_1=a_2$

דוגמאות:

1) $G=S_n$, $A=\{1,\dots,n\}$ לכל $a_1,a_2\in A$, יהי $\sigma=(a_1,a_2)$ חילוף.

$G * a_1 = G(a_1) = a_2$

2) A , $G = S_A$ ונתון. הרעיון: יהיו $a_1, a_2 \in A$

$$f(x) = \begin{cases} a_2 & x = a_1 \\ a_1 & x = a_2 \\ x & x \neq a_1, a_2 \end{cases}$$

$f * a_1 = a_2$

לכן הפעולה הנתונה טרנזיטיבית

3) פעולה של $GL_n(\mathbb{R})$ על $\mathbb{R}^n$. לכל $g \in GL_n(\mathbb{R})$

$$g * \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

ואם $a_2 \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ לא קיים שום $g \in GL_n(\mathbb{R})$ כך ש

$$g * \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = a_2$$

לכן הפעולה לא טרנזיטיבית

נשים לב: ואם $a_1, a_2 \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ אזי יש $g \in GL_n(\mathbb{R})$ כך ש $g * a_1 = a_2$

4) פעולה על דגלים כן טרנזיטיבית. אכן: יהיו $a_1, a_2 \in A$ שני דגלים $a_1 = (V_1, \ldots, V_n)$ $a_2 = (W_1, \ldots, W_n)$

נבחר בסיס v_1 של V_1 נרחיב אותו לבסיס v_1, v_2 של V_2 וכך הלאה. נקבל בסיס $v_1, \ldots, v_n$ של $\mathbb{R}^n$ כך ש $V_k = \langle v_1, \ldots, v_k \rangle$ לכל k. באופן דומה, נקבל בסיס ל-W

$W_k = \langle w_1, \ldots, w_k \rangle$

תהי $g \in GL_n(\mathbb{R})$ המטריצה המתאימה להעתקה $\mathbb{R}^n \to \mathbb{R}^n$ $v_i \to w_i$ לכל $i = 1, .., n$. אזי $g(V_i) = W_i$ לכל i לכן $g * a_1 = a_2$. הפעולה אכן טרנזיטיבית

5) פעולה של G על עצמה על ידי כפל משמאל

יהיו $a_1,a_2\in A=G$ $g=a_2a_1^{-1}$ $g*a_1=a_2$. טרנזיטיבי

6) פעולה של G על עצמה על ידי הצמדה $g*a=gag^{-1}$

$g*e=geg^{-1}=e$ לא טרנזיטיבי (אם $|G|>1$)

7) טרנזיטיביות

הגדרה: תהי G חבורה שפועלת על קבוצה A. לכל $g\in G$ נגדיר פונ'

$f_g:A\to A$ $f_g(a)=g*a$

טענה:

לכל $g\in G$, הפו' f_g חח"ע ועל

הוכחה:

נראה כי $f_{g^{-1}}$ הינה הופכי דו צדדי של f_g

ואכן לכל a $f_g(f_{g^{-1}}(a))=g*g^{-1}*a=e*a=a$

באופן דומה $f_{g^{-1}}(f_g(a))=a$

לכן f_g חח"ע ועל, ובפרט $f_g\in S_A$

מקבלים העתקה $G\xrightarrow{\varphi}S_A$ ($g\mapsto f_g$) העתקה זו

מתאימה לכפל בשני הצדדים $\varphi(\underbrace{g_1g_2}_{\text{כפל של } G})=\underbrace{\varphi(g_1)\varphi(g_2)}_{\text{כפל של } S_A}$

הגדרה: תהי G חבורה שפועלת על קבוצה A. נגדיר יחס על A.

$a_1\sim a_2 \iff \exists g\in G: g*a_1=a_2$

טענה:

זה יחס שקילות

הוכחה:

רפלקסיביות: $e*a=a$ לכן $a\sim a$ לכל $a\in A$

סימטריות: נניח $a_1\sim a_2$, לכן קיים $g\in G$ כך ש $g*a_1=a_2$

לכן $a_1=g^{-1}*a_2$ וקיבלנו $a_2\sim a_1$

טרנזיטיביות: נניח $a_1\sim a_2, a_2\sim a_3$. קיימים $g_1,g_2\in G$ כך ש

$g_1*a_1=a_2$, $g_2*a_2=a_3$

$g_2g_1*a_1=g_2*(g_1*a_1)=g_2*a_2=a_3 \Rightarrow a_1\sim a_3$

היחס הזה מפריד את A למחלקות שקילות.

מחלקות השקילות נקראות מסלולים של הפעולה.

נגדר הפעולה טרנזיטיבית. אם $a_1\sim a_2$ לכל $a_1,a_2\in A$

כלומר, אם יש רק מחלקת שקילות אחת.

דוגמא:

לפעולה של $GL_n(\mathbb{R})$ על $\mathbb{R}^n$ יש שתי מחלקות שקילות

(מסלולים) $\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$, $\mathbb{R}^n \setminus \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$

סימון: יהי $a\in A$. המסלול של a הינו $G*a=\{g*a : g\in G\}$

הגדרה: תהי G חבורה שפועלת על קבוצה A, יהי $a\in A$ המייצב

של a הינו $G_a=\{g\in G : g*a=a\}$

טענה:

לכל פעולה ולכל $a\in A$, המייצב G_a הינו תת חבורה של G

הוכחה:

$e\in G_a$ לכל a לכן $G_a\neq\emptyset$. נבדוק סגירות לכפל ולהפכיים

כפל: נניח $g_1,g_2\in G_a$ לכן $g_1*a=a$, $g_2*a=a$

$g_1g_2*a=g_1*(g_2*a)=g_1*a=a$

לכן $g_1 g_2 \in G_a$

הפכים: יהי $g \in G_a$. כלומר, $g*a=a$. נכפיל g^{-1} ונקבל
$g^{-1}*a=a$

לכן $g^{-1} \in G_a$

דוגמה:

פעולה של $G=S_A$ על A, $G_a=Stab(a)$

תרגיל:

$G=GL_n(\mathbb{R})$, A קבוצת הדגלים $a=(\langle e_1\rangle,\langle e_1,e_2\rangle,\dots)$

$G_a=\{$ מטריצות משולשיות עליונות $\}$

משפט: (משפט מסלול-מייצב)

תהי G חבורה שפועלת על הקבוצה A. יהי $a\in A$. אזי יש התאמה חח״ע ועל

$$\underbrace{G/G_a}_{\text{הקבוצה של מחלקות שמאליות של } G_a \text{ ב-} G} \longleftrightarrow \underbrace{G*a}_{\text{המסלול של } a}$$

$\{b\in A \mid \exists g: g*a=b\}$

$G*a \subseteq A$

הוכחה:

נגדיר $\varphi: G/G_a \to G*a$ $\quad \varphi(gG_a)=g*a$

קודם כל נבדוק ש φ מוגדרת היטב. אם $gG_a=xG_a$

כלומר g,x שייכים לאותה מחלקת שקילות, כלומר, קיים $h\in G_a$ כך ש $x=gh$. אבל אז, $x*a=(gh)*a=g*(h*a)\underset{h\in G_a}{=}g*a$

קיבלנו $x*a=g*a$ ולכן φ מוגדרת היטב

φ על: יהי $b\in G*a$. לפי הגדרת המסלול זה אומר שקיים $g\in G$ כך ש $\varphi(gG_a)=g*a=b$. לכן φ על

φ חח"ע: נניח $\varphi(g_1G_a)=\varphi(g_2G_a)$. זה אומר ש $g_1*a=g_2*a$ נפעיל g_1^{-1} $.a=g_1^{-1}g_2*a$ לכן $g_1^{-1}g_2\in G_a$ זה אומר ש g_1,g_2 שייכים לאותה מחלקה משמאל של G_a. כלומר $g_1G_a=g_2G_a$ זה אומר כי φ חח"ע.

תוצאה:

תהי G חבורה סופית שפועלת על קבוצה A. העוצמה של כל מסלול מחלקת את $|G|$

הוכחה:

יהי $a\in A$, יהי $G*a$ המסלול שלו. הוכחנו שהמייצב G_a הינו תת חבורה של G. לפי לגרנז' $|G_a|\,\big|\,|G|$

$$|G_a|[G:G_a]=|G| \Rightarrow [G:G_a]\,\big|\,|G|$$

לפי משפט מסלול מייצב, $[G:G_a]:=|G/G_a|=|G*a|$

הגדרה: תהי G חבורה שפועלת על A. איבר $a\in A$ נקרא נקודת שבת של הפעולה אם $g*a=a$ לכל $g\in G$ $\iff G*a=\{a\}$

$\Updownarrow$

$|G*a|=1$

סימון $Fix(A)$ הקבוצה של כל נקודות השבת.

דוגמא:

תזכורת G חבורה. המרכז של G הינו $Z(G)=\{g\in G \mid gh=hg \ \text{לכל}\ h\in G\}$ הוכחנו בתרגול ש $Z(G)$ הינו תת חבורה של G.

תהי G פועלת על עצמה על ידי הצמדה. $A=G$. $g*a=gag^{-1}$

אזי $a\in Fix(A)$ $\iff$ $g*a=a$ לכל $g\in G$ $\iff$ $gag^{-1}=a$ לכל g

$\iff$ $ga=ag$ לכל $g\in G$ $\iff$ $a\in Z(G)$

לכן $Z(G)=Fix(A)$

הגדרה: יהי p מס' ראשוני. חבורה סופית G נקראת p-חבורה אם $|G|$ הינו חזקה של p. $|G|\in\{p,p^2,\dots\}$

טענה:

תהי G p-חבורה (סופית) שפועלת על קבוצה סופית A. אזי
$|Fix(A)|\equiv|A| \mod p$

הוכחה:

יהי $|G|=p^n$. לפי התוצאה ממשפט מסלול-מייצב, אזי העוצמה של כל מסלול מחלקת את $|G|=p^n$. כלומר העוצמה של כל מסלול הינו אחד מהאפשרויות הבאות $1,p,p^2,\dots,p^n$

המשלים $A\setminus Fix(A)$ הינו האיחוד של כל המסלולים מעוצמות $p,\dots,p^n$ ($a\in Fix(A) \iff |G*a|=1$). זה אומר שהעוצמה של המשלים מתחלקת ב-p. ולכן, $|A|-|Fix(A)|=\underbrace{|A\setminus Fix(A)|}_{\text{מתחלק ב-}p}$ לכן $|A|\equiv|Fix(A)| \mod p$

מסקנה 1:

תהי G p-חבורה סופית. אזי $Z(G)$ לא טריוויאלית

הוכחה:

G פועלת על עצמה על ידי הצמדה. ראינו $Fix(A)=Z(G)$ עבור הפעולה הזאת. $A=G$. לפי הטענה $|Fix(A)|\equiv|A| \mod p$

$|Z(G)|\equiv 0 \mod p \Leftarrow |Z(G)|\equiv p^n \mod p \Leftarrow |Z(G)|\equiv|G| \mod p$

ידוע כי $e\in Z(G)$ לכן $|Z(G)|>0$ לכן $|Z(G)|\ge p>1$ לכן $Z(G)\neq\{e\}$

משפט: (קושי)

תהי G חבורה סופית, p מספר ראשוני, נניח כי $p \mid |G|$

אזי קיים $g\in G$ כך ש $o(g)=p$

הוכחה:

$$A=\{(g_1,\dots,g_p)\in G^p \mid g_1g_2\cdots g_p=e\}$$

נשים לב ש $|A|=|G|^{p-1}$ (בוחרים $g_1,\dots,g_{p-1}$ באופן חופשי ומוסיפים את ההופכי שלהם)

נגדיר $G=\mathbb{Z}_p$ על A:

$$[n]*(g_1,\dots,g_p)=(g_{n+1},\dots,g_p,g_1,g_2,\dots,g_n)$$

(מעבירים כל קומפוננטה n מקומות שמאלה)

$(g_1,\dots,g_p)\in Fix(A) \iff g_1=\dots=g_p$

$\shortparallel$

$(g_2,\dots,g_p,g_1)$

$g^p=e \iff (g,\dots,g)\in A$ לכן, $|Fix(A)|=|\{g\in G \mid g^p=e\}|$

לפי הטענה, $|Fix(A)|\equiv |A| \bmod p$. $|Fix(A)|=\underbrace{|G|^{p-1}}_{\text{מתחלק ב-}p}$

כי $p \mid |G|$

ולכן $|Fix(A)|\equiv 0 \bmod p$. ברור כי $(e,\dots,e)\in Fix(A)$

לכן $|Fix(A)|>0$ בפרט $|Fix(A)|\ge p>1$

לכן קיים $g\neq e$ כך ש $(g,\dots,g)\in Fix(A)$ ול. $o(g)=p$