

חוקי הגזירה (באמצעות הקודים יעזר כמה בדיוק, יהיו ואז שגו נרץ להגזיר)
 ציון - (0.1 תפלים + 0.9 מבחן, מבחן) וגם
 הרק וויס - barak@post.tau.ac.il

פיחוק לגורמים ראשוניים

מטרה - להגדיר ראשוניים ולהוכיח שכל טבעי ניתן לפירוק למכפלה של ראשוניים בצורה יחידה.
 כדי להוכיח זאת, נבין באופן כללי יותר על חזרים.

הגדרה - $A \subseteq \mathbb{C}$ נקראת חוג אם: היא מכילה את 1 ואת 0
 סגורה תחת חיבור, חיסור, וכפל
 * - יש להגדרה יותר מופשטת, אנוני נסתפק בהמשך זה

דוגמאות - $\mathbb{Z}$ - שלמים

$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ = "השלמים האוסטריים"
 אם $\alpha \in \mathbb{Z}$ שגוי ריבוע של מספר שלם, נסמן ב- $\sqrt{2}$ את אחד הסורטים של α ,
 ונסמן $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ (הזירה - כל הצבה כלואה היא יחידה)

הגדרה - A חוג, $a \in A$ נקרא הפך אם $a \neq 0$, $a^{-1} \in A$.
 קבוצת כל ההפכים ב- A נסמן ב- A^* . הזירה - A^* סגור לכפל, מכאן $\neq 1$,
 ושאר עליונות הפכים

דוגמאות - ב- $\mathbb{Z}$ ההפכים הם ± 1

$\mathbb{Z}[i]^* = \{1, -1, i, -i\}$

הוכחה: יהי $\alpha + b i \in \mathbb{Z}[i]^*$

מהגדרה -

מסמלות

אז

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} \in \mathbb{Z}[i]$$

$$a \left(\frac{a-bi}{a^2+b^2} \right) = \frac{a^2}{a^2+b^2} - \frac{ab}{a^2+b^2} i \in \mathbb{Z}[i]$$

$$\frac{a^2}{a^2+b^2} \in \mathbb{Z}$$

זה מתקיים רק אם $a=0$ או $b=0$.
 נציב ונראה שנקבל בדיוק את מה שרצינו $(\pm 1, \pm i)$

- נסתכל על החוג $\mathbb{Z}[\sqrt{2}]$.

נראה שכל המספרים $\{n \mid n \in \mathbb{Z}\} \cup \{(n+1)\sqrt{2} \mid n \in \mathbb{Z}\}$ הפכים ב- $\mathbb{Z}[\sqrt{2}]$.
 הוכחה: $(1+\sqrt{2})(-1+\sqrt{2}) = 2-1 = 1 \rightarrow 1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$

ומסמלות כלפינו, נקבל $\{(n+1)\sqrt{2} \mid n \in \mathbb{Z}\} \cup \{1\} \subseteq \mathbb{Z}[\sqrt{2}]^*$

הגדרה - A חוג. יהיו $a, b \in A$. נאמר ש- a מחלק את b (אז $a|b$) אם קיים $c \in A$ כך ש- $ac = b$

טענה

- אם $b \in A$, $a \neq 0$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A^*$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

$$a|ub+vc$$

- אם $a \in A$, אז $a|b$ אם ורק אם $a|1$

הוכחה - נבדוק ישירות מההגדרה

הצגה - A חזו', $a, b \in A$. נאמר ש- b חזר ש a

אם יום $\varepsilon \in A^*$ ק' ש- $b = \varepsilon a$
 $a \in A$ נקרא א'-פרק אם $a \notin A^*$, וכל מרחק של a הוא זה
 ש- a או הפרק $\forall a, b \in A$
 $p \in A$ "קרא" ראשוני אם $p \notin A^*$, $p \neq 0$, $p | a \rightarrow p | b$ או $p | a \leftarrow p | b$
 * נוכח בהוכחה שהמרחק וההצטרף של איבריך וראשוני נקראים (כמו ב-Z), אבל לא כולם

שאלה - יהי A חוג, $A \in \mathcal{A}$ ראשוני ו- p אי-זר. $a \in A$ חזרתי p ו- $a \in A^*$.
הוכח: a אינו ערכי- p .

$$p|b \wedge p|a \nmid p|ab \leftarrow ab \in P \quad -\text{ש } p \nmid b \in A \quad \text{קיים } p|a \leftarrow a \in P$$

$$\leftarrow a=b \cdot p \leftarrow a \cdot b = p \quad \text{ש } p \nmid c \in A \quad \text{קיים } p|a \quad \text{במקרה } -\text{ש } p = p \cdot b$$

$$\quad \quad \quad b \in A^* \quad \leftarrow 1 = cb \quad \leftarrow p = p \cdot b$$

$$\quad \quad \quad b^{-1} \in A^* \quad \leftarrow p \text{ חסר } a$$

a חסר של p $b^{-1} \in A^*$

במקרה ש- $p|b$ $c \in A$ p''_c $p|b$ $p|ac = ap_c = p$

a חסר $\leftarrow c = a^{-1}$ $\leftarrow ac=1$

סוג - $A = \mathbb{Z}$, $a \in A$ שמים 0, וסיון ב- A^* , אפטר, ערשום
במכשור של אלו-עירקים.

הוכחה - באמצעות δ $\forall \epsilon \in \mathbb{N}$, הסוציאליות מתקיימת - $\delta = 10$.

$\left\{ a \in \mathbb{Z} \mid a \equiv 1 \pmod{2} \right\} \leftarrow |a| = 2$ - 0'ס
 $\left\{ a \in \mathbb{Z} \mid a \equiv 1 \pmod{2} \right\} \leftarrow |a| \geq 3$ - נחמ

אם a כבר איז פאראן אין M ערשט
אחרת a איז נעם אן און $a \leq b$ און $b \leq a$ און $a = b$
וואס צו זאגן $a < b$ און $b < a$ און $a = b$ איז א פארטרעג
און a איז נעם אן און $a \leq b$ און $b \leq a$ און $a = b$ איז א פארטרעג
און a איז נעם אן און $a \leq b$ און $b \leq a$ און $a = b$ איז א פארטרעג

דבר (החתם) הא' צוקצוק $b = b_1 \dots b_r$, b_i אי פריק'ס
 $c = c_1 \dots c_s$, c_j אי פריק'ס
 $a = b_1 \dots b_r c_1 \dots c_s$ מ'פאלט אי פריק'ס.

הצורה - נאמר שהפירוק של a כתפלה של אי-פריקים הוא יחיד עד כדי סדרה
 $a = a_1 \dots a_r$ כאשר a_i אי-פריקים, ואם b כל שוויון
 מהצורה $b_1 \dots b_s = a_1 \dots a_r$ כאשר a_i ו- b_j אי-פריקים, מתקיים
 $r = s$ ונשאור שישו סדרם a_i ו- b_j חדר של b_i .

למטה - גוף A חוצ' בו α מספר חוף מים והימים אסטר ערסום למכפלה α ש' פרק'.
אזי הפרק חס' יחיד $\leftrightarrow$ כל אי-פרק A - A הוא רשומי

רעיון ההוכחה - אינדוקציה על המספר המניימלי של אותם או ביקים, קודם לט או ירא במכשיר
ש' פ'יקים

$\leftarrow$ יהי P א' - פריק, נכיר P ראשוני
 נניח $a, b \in A$ - $ab \in P$, $a \notin P$, $b \notin P$ (ההנחה)
 קיים $c \in A$ כן $c = ab$, נרמק את c במכפלת אי פריק:
 $c = a_1 \cdot b_1 \cdot \dots \cdot a_j \cdot b_j \cdot \dots \cdot a_k \cdot b_k$
 (אם a או b הפכים, הטענה מיוזגת (מכפילים את שני האגפים בהפכיה)
 שכי לחיצות בכתיבת אותה A - במכפלת א' - פריקים, קיים P'
 חגר של P , המופיע בגיטוי $a_1 \cdot b_1 \cdot \dots \cdot a_j \cdot b_j \cdot \dots \cdot a_k \cdot b_k$ ש $a' = a_1$, $b' = a_1$
 $\leftarrow$ איש קיים $c \in A$ כן $a = P'c$ ~~מ~~
 וקיים $c \in A^*$ כן $a = P'c$

טכניק שכל $\mathbb{Z}a+b$ קיימים $\mathbb{Z}k+l$ - $\gcd(a,b) \mid ka+lb$

הוכחה 1 - נסמן $I = \{ka+lb \mid k,l \in \mathbb{Z}\}$

- נשים לב שהקבוצה סגורה סחיבור - $x,y \in I \rightarrow x+y \in I$

- וסגורה מכפלה ב- $\mathbb{Z}$ - $x \in I, y \in \mathbb{Z} \rightarrow xy \in I$

(כלומר, I אידיאל)

- אם $a,b \neq 0$, I מכילה חיוביים, ו- I מכילה את a ואת b

- נסמן $c = \min \{x \in I \mid x > 0\}$

נראה מיד כי $I = c\mathbb{Z}$
 נסמן $d = \gcd(a,b)$, נראה ש- $d \mid c$
 $d \mid x \leftarrow d \mid a, d \mid b, x = ka+lb \in I$
 בפרט $d \mid c \leftarrow d \mid c$
 מצד שני, $c \in I$, $c \mid a$, $c \mid b$
 $c \mid b \leftarrow b \in I$
 ולפי $I = c\mathbb{Z}$

$c\mathbb{Z} \subseteq I \leftarrow \forall x \in \mathbb{Z}, cx \in I \leftarrow c \in I$
 נקח $x \in I$, כדי להראות ש- x כפולה של c , נבצע חלקה עם שארית:
 $x = cq + r, 0 \leq r < c$
 $x = cq$ או $r = 0$
 $I \subseteq c\mathbb{Z}$
 ומהכלל דו כיוונית $I = c\mathbb{Z}$

מסקנה - אם $d = \gcd(a,b)$ ו- n מחלק משותף של a,b אז $n \mid d$

הוכחה - $d = ka+lb$ אם $n \mid a$ ו- $n \mid b$ אז $n \mid d$

הוכחה 2 - השלשוריתם האוקלידי $\gcd(a,b)$

בהיכ $a > 0$. נסמן $a = r_0, b = r_1$. נבצע חלקה עם שארית:

$$b = q_0 a + r_1, \quad 0 \leq r_1 < r_0 = a$$

$$r_0 = q_1 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_{j-1} = q_j r_j + r_{j+1}, \quad 0 \leq r_{j+1} < r_j$$

ממשיכים. בצעד j :
 ממשיכים לבצע חלקה עם שארית עד שמקבלים שארית 0. כלומר יש אחרון $r_{k+1} = 0$
 ו- $r_k \neq 0$.

$$\gcd(a,b) = r_k$$

הוכחה - טכניק - $\gcd(r_{j-1}, r_j) = \gcd(r_j, r_{j+1})$ ($0 \leq j \leq k$) - ש

$$\gcd(a,b) = \gcd(r_1, 0) = \dots = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k$$

$$r_{j-1} = q_j r_j + r_{j+1} \quad \rightarrow \quad r_{j+1} = r_{j-1} - q_j r_j$$

דוגמה לאלגוריתם אוקלידס:

המחלקים המשותפים: $\pm \{3, 5, 15\}$

$$a = 270, b = -105$$

$$a = 270 = r_0, b = r_{-1} = -105$$

$$b = q_0 a + r_1$$

$$270 = 1 \cdot 105 + 165$$

$$165 = 1 \cdot 105 + 60$$

$$105 = 1 \cdot 60 + 45$$

$$60 = 1 \cdot 45 + 15$$

$$45 = 3 \cdot 15 + 0$$

$$\rightarrow r_0 = 270, r_1 = 165$$

$$\rightarrow r_2 = 105$$

$$\rightarrow r_3 = 60$$

$$\rightarrow r_4 = 45$$

$$\rightarrow 15 = \gcd(270, -105)$$

נוסח מטריצוני של אלגוריתם אוקלידס

אפשר לכתוב:

$$r_{j-1} = q_j r_j + r_{j+1}$$

אם הנמצא

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_j \end{bmatrix} \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix}$$

מטריצה הפיכה בשלמים.