

פירוקי - עבר - חיבורים

הסדרה: $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ עבר.

הסדרה: $z \in \mathbb{C}$ יקרא שלם אלגברי, אם z הוא שורש של
 פולינום ממעלה n בעבר, $z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 = 0$, $a_0, \dots, a_{n-1} \in \mathbb{Z}$

אנוני: יהי $\mathbb{Q}$ שלם אלגברי, אזי $z \in \mathbb{Z}$.

אנוני: $\{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}] \subset \mathbb{O}_d = \{z \in \mathbb{Q}[\sqrt{d}] \mid z \text{ שלם אלגברי}\}$

אנוני: יהי $d \neq 1$ מספר שלם חיובי ~ חיבורים.

$$\mathbb{O}_d = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \not\equiv 1 \pmod{4} \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & d \equiv 1 \pmod{4} \end{cases}, \text{ שז}$$

אנוני: $z \neq 0$ $\rightarrow$ $\mathbb{O}_d$ בנוי סביב $\tilde{N}(z) = \pm 1$

אנוני: $\mathbb{O}_d^* = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}$ - ע. $\varepsilon \in \mathbb{O}_d^*$ אנוני $\varepsilon \neq \pm 1$ ($d \geq 2$)
 (ε יקרא יחידה היחידה של $\mathbb{Q}[\sqrt{d}]$)

אנוני: נניח כי $z \in \mathbb{O}_d$ כך ש- $|N(z)| = p$ כאשר $p \in \mathbb{Z}$ ראשוני, אזי z אי-פריק.

אנוני: $d < 0$, $\mathbb{O}_d$ הוא חבור פריקו - יחידה $\tilde{N}$
 $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$

חברים אוקלידיים:

הסדרה: $\mathbb{O}_d$ חברים אוקלידיים אם לכל $a, b \in \mathbb{O}_d$, $b \neq 0$, $a = c \cdot b + t$, $c, t \in \mathbb{O}_d$ כך ש- $|N(t)| < |N(b)|$.

אנוני: $\mathbb{O}_d$ הוא חברים אוקלידיים $\tilde{N}$ לכל $z \in \mathbb{Q}[\sqrt{d}]$ $e \in \mathbb{O}_d$ כך ש- $|N(z-e)| < 1$.

שאלה! נניח $z \in \mathbb{Q}[\sqrt{-d}]$ כזו ש $z = a/b$ פשוט
 כאשר $a, b \in \mathbb{Z}$

טענה: נניח כי $d < 0, d \not\equiv 1 \pmod{4}$ אז חז' אוקלידי.
 אז $d = -1, -2$

טענה: נניח כי $d \equiv 1 \pmod{4}, d < 0$ אז חז' אוקלידי.
 אז $d = -3, -7, -11$

טענה: אז חז' אוקלידי אז $d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13,$
 $17, 19, 21, 29, 33, 37, 41, 57, 73$.

טענה: לכל $a, b \in \mathbb{Z}$ קיים $\gcd(a, b)$ כאשר $(a, b) \neq (0, 0)$.
 אוקלידי

(אם גזום בריקו יתקדם כאשר אס' אוקלידי, אוקלידי ביק)

טענה: יהי $d \in \mathbb{Z}$ אי-ריבוי (= ראשוני - בריק ואין שיתוף)
 אז קיים ס' ראשוני כי אם גזום בריקו יתקדם.
 יחיד $N = p$ בק-ע $p \mid \pi$.
 כאשר כי " π מונח מל p ".

טענה: יהי $p \in \mathbb{Z}$ ראשוני - אז יש $d \in \mathbb{Z}$ אי-ריבוי, הומוגן $h \sim p$.

טענה: יהי $d \in \mathbb{Z}$ אי-ריבוי, יהי $p \in \mathbb{Z}$ ראשוני. היחיד הראשוני
 גזום $p - \pi, \pi$ אז $N(\pi) = \pm p, \pm p^2$

תישים חבורת החיבורה של חוג השלמים $\mathbb{Z}$;
השדה המקסימלי $\mathbb{Q}$.

אם $d \leq 0$ אז החבורה מסתגרת.
אחרת, נבחר את d שלב ונחזיר את
אורך החבורה m .

נחשב את p_{m-1} ו- q_{m-1} יקבלו שסדרות היסודי
הוא $p_{m-1} + q_{m-1}\sqrt{d}$ ולכן
$$Od^+ = \{ \pm (p_{m-1} + q_{m-1}\sqrt{d})^n \mid n \in \mathbb{Z} \}$$

נבחר שיוון כלשהו אינו סוג של קצובה $\mathbb{Z}[\sqrt{d}]$ הוא
תחום פריק יחידה.

נזכיר שיש קצובה מסוימים אחרים פריקים ע"י מילוי
פריקים.

הראוי כי $\mathbb{Z}[\sqrt{d}]$ אינו תחום פריק יחידה (כבר נראה אחרת)

~~נבחר את $\sqrt{d} = x + y\sqrt{d}$ שיהיה $x, y \in \mathbb{Z}$ כפריק.~~

~~נבחר $N(x + y\sqrt{d}) = x^2 - dy^2$:~~

קראו: הראוי כי $\mathbb{Z}[\sqrt{13}]$ אי-פריק. ה- $\mathbb{Z}[\sqrt{13}]$ והוכח כי $\mathbb{Z}[\sqrt{13}]$
אינו תחום פריק יחידה.

נניח כי $1 + \sqrt{13} = u \cdot v$ $N(1 + \sqrt{13}) = 14 = N(u) \cdot N(v) \iff$

$N(u), N(v) = \pm 1, \pm 2, \pm 7, \pm 14$

אם $N(u) = \pm 14$ אז $N(v) = \pm 1$ מכאן u הפך ל- $1 + \sqrt{13}$ ו- v הפך.

אם $N(u) = \pm 7$ $a^2 - 13b^2 = \pm 7$ וזה לא יתכן.

בן ראוי $N(u) = \pm 2$ $a^2 - 13b^2 = \pm 2$ אין פתרון ב- $\mathbb{Z}$.

הם פריקים וחבריהם של $\mathbb{Z}[\sqrt{13}]$ הם $1 + \sqrt{13}$ ו- $1 - \sqrt{13}$.

14 הוא אינו $\pm$ ראשוני או $\pm$ ראשוני בריבוע ולכן

ניתן לפרוק ע"י סגירה כי $\mathbb{Z}[\sqrt{13}] \neq 0 - 13$

כי אם כן, אז קראו את אי-פריק הפעמים $\pm p, \pm p^2$

כאשר $\mathbb{Z}$ שלם ראשוני.

קבץ $\mathcal{A}$ איז אים פאר פריק אויף $\mathcal{A}$, $\mathcal{A} \subseteq \mathcal{Z}$;
 - אים $\mathcal{A} \neq \emptyset$ ו- $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 שפירט אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

- אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 שפירט אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

- אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

אם $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

אם $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$

אם $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$
 אים $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$ $\mathcal{A} \subseteq \mathcal{Z}$