

תצבורת:

חוג R נקרא תחום קיקורג אם R הוא תחום שלמות וגם:

(1) R נטרי

(2) R סגור בשלמות

(3) כל איגאל ראשוני לא אפסי של R הוא מקסימלי, ויש איגאלים כאלה.

גולמא: k שגה מספרים, $\dim_k k < \infty$

$$O_k = \{ \alpha \in k : \exists \text{ מס' } \alpha \}$$

"חוג השלמים של k " הוא תחום קיקורג

משפט:

יהי R תחום קיקורג, יהי $I \neq R$ (0) איגאל (לא בהכרח אמיתי). אז $I = P_1 \cdot \dots \cdot P_r$

מתפרק במכפלה של איגאלים ראשוניים של R , ובהכרח הבה יחיד צד כדי

החלפת סדר האגזמים.

המשק הבוכחה:

יהי $I \neq R$ איגאל (לא בהכרח אמיתי)

בוכחנו בפעם הקודמת כי I הוא מכפלה של ראשוניים.

נשאר להוכיח יחידות: נניח שיש לנו שני פירוקים

$$I = P_1 \cdot \dots \cdot P_r = Q_1 \cdot \dots \cdot Q_s$$

וינזוקנו על r

$r=0$: $I = (1) = R = Q_1 \cdot \dots \cdot Q_s \subseteq Q_1$ אז

אם המכפלה של n ה- Q 'ים לא כיקה

ובה לא יתכן כי Q_1 איגאל אמיתי. לכן המכפלה של ה- Q 'ים עם כיקה

$r > 0$: יהי $I = P_1 \cdot \dots \cdot P_r = Q_1 \cdot \dots \cdot Q_s$ כמו שאמרנו קודם

$$Q_1 \cdot \dots \cdot Q_s = P_1 \cdot \dots \cdot P_r \subseteq P_r$$

האיגאל P_r ראשוני, לכן $Q_i \in P_r$ עבור $1 \leq i \leq r$ (ובכל P_i, Q_i שניהם מקסימליים, לכן $P_r = Q_i$)

נכפיל את שני האיגלים בקבוצה $\{x \in \text{Frac } R : x P_r \subseteq R\}$. $Q_i^{-1} = P_r^{-1}$

$$I P_r^{-1} = P_1 \cdot \dots \cdot P_{r-1} = Q_1 \cdot \dots \cdot Q_{i-1} \cdot Q_{i+1} \cdot \dots \cdot Q_s$$

הוכחנו כי $R \not\subseteq I P_r^{-1} \neq (0)$ אוילי לא אמיתי.

באינדוקציה אני הפירוקים $P_r \cdot \dots \cdot P_{r-1} = Q_1 Q_2 \dots$ זהים עד כדי התלפזת

הסבר (בפרט $r=s$).

בצורה המשפט הנ"ל הוא בהפלאה ה"נכונה" של המשפט היסודי של האריתמטיקה.

כאילו שתחומי גזיקנק אינם בהכרח תחומי פריקות יחידה. לגדולתו, $\mathbb{Z}[\sqrt{5}]$.

מתי הם כן תחומי פריקות יחידה?

טענה:

יהי R תחום גזיקנק. אזי R תפ"י $\Leftrightarrow R$ תחום ראשי

הוכחה:

(\Rightarrow) נכון לכל חוג

(\Rightarrow) מספיק להוכיח שכל איגאל ראשוני של R הוא ראשי.

אכן, מכפלה של איגלים ראשיים בחוג תלסוכי היא ראשית $(ab) = (a)(b)$. אכן הוכחנו

אז R תחום גזיקנק, אז כל איגאל הוא מכפלה של ראשוניים.

יהי $R \not\subseteq P \neq (0)$ ראשוני. יהי $a \in P$. מניחים כי R תפ"י, לכן $a = p_1 \cdot \dots \cdot p_r$

מתברר למכפלה של אי פריקים. אבל P ראשוני, לכן $p_i \in P$ עבור i מתאים.

נתפ"י כל איבר אי פריק הוא ראשוני. לכן, $(p_i) \subseteq P$ איגלים ראשוניים לא אפס"ם,

לכן מקסימליים, לכן $(p_i) = P$ ולכן P ראשי.

בצורה יהי R תחום גזיקנק. איגאל שברי של R הוא תת-מוחזק נוצר סופית של $\text{Frac } R$ (או אפס)

טענה/תוצאה:

יהי a איגאל שברי, אזי $a = Q_1^{-1} \cdot \dots \cdot Q_r^{-1} \cdot P_1 \cdot \dots \cdot P_s$ כאשר P_i, Q_i ראשוניים

מכי R החבורה של כל האיגלים השבריים, תחת כפל.

אם ρ הוא רוציג'ר, למסוף ρ הטרענר:

נגיר את J_R לכיות החכורה האכלית החופשית הנוצרת על ידי האיגאלים הראשונים
כלו אפסיים של R .

תבי P_R תת החכורה של האיגאלים הראשונים R_x , $x \in \text{Frac } R$

$$P_R = \{ \sum_{i=1}^n r_i(s)^{-1} : r_i \in R \}, \quad x = \frac{r}{s}, \quad xR = (r)(s)^{-1}$$

הצורה: $Cl_R = J_{P_R}/P_R$ נקראת חכורת החתלקות של R . נשים לב כי

$$Cl_R = \{ \sum \xi_i \} \Leftrightarrow R \text{ תחום ראשי} \Leftrightarrow Cl_R = 0$$

לכן הסכר של Cl_R (מסמנים h_R) הוא מקינה של חנה רחוק מלהיות תפי

משפט: (Ceburn, 1963)

תפי G חכורה אכלית. אזי קיים תחום בקיקנר R עם $Cl_R \cong G$

משפט: (מאה ה-18)

יפי k שדה מספרים. אזי Cl_k סופית. נסמן $h_k = |Cl_k|$.

נתבונן בשדות מספרים ריבועיים $k = \mathbb{Q}(\sqrt{d})$:

פי מקרים:

(1) $d < 0$, k שדה ריבועי מקומה.

משפט: (הצורה של גאוס מהמאה ה-19, Heegner 1952, Stark 1967)

יפי $d < 0$, $k = \mathbb{Q}(\sqrt{d})$. אזי $h_k = 1 \Leftrightarrow d \in \{ -1, -2, -3, -7, -11, -19, -43, -67, -163 \}$

(בוכחוו כי $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$ הפשמים של גאוס, שהוא תחום נוקספי ולקן תחום ראשי)

(2) סלד, $k = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ שדה ריבועי ממשי

האם יש אינסוף שדות ריבועיים ממשיים כך $h_k = 1$?

ההצורה (Cohen-Lenstra heuristics 1983) אומרת שדכור 75.446% של הראשונים p ,

שדה $k = \mathbb{Q}(\sqrt{p})$ מתקיים $h_k = 1$

נושא הקבץ מ'יון של מוקפים נוצרים סופית מעל תחום ראשי

הגדרה: יהיו M, N מוקפים מעל תחום R .

$$M \times N = \{(m, n) : m \in M, n \in N\}, \quad \begin{cases} (m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \\ r(m, n) = (rm, rn) \end{cases}$$

טענה:

יהי M מוקף מעל תחום R . יהיו M_1, M_2 תת מוקפים. נניח ש:

$$(1) \quad M_1 + M_2 = \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\} = M$$

$$(2) \quad M_1 \cap M_2 = (0)$$

$$\text{אזי } M \cong M_1 \times M_2$$

הוכחה:

נגדיר $f: M_1 \times M_2 \rightarrow M$ ברור שזה הוא של מוקפים.
 $(m_1, m_2) \mapsto m_1 + m_2$

f על כמעט (1), f חזק כמעט (2).

הגדרה: R -מוקף M נקרא ציקלי אם הוא נוצר על ידי איבר אחד. כלומר, קיים

$$M = Rm = \{rm : r \in R\}$$

טענה:

יהי R תחום כלשהו. יהי M R -מוקף (שמאלי) אזי M ציקלי \Leftrightarrow קיים איבר $a \in M$ שמהו $I \subseteq R$

כך ש $M \cong R/I$ (כמוקפים). (מכנה כמוקף של R/I נתון על ידי $\{r(a+I) = ra+I\}$)

הוכחה:

(\Rightarrow) R/I נוצר על ידי $1+I$. $(r+I = r(1+I))$. לכן R/I ציקלי.

(\Leftarrow) יהי M ציקלי, יהי $m \in M$ יוצר. כלומר, $M = Rm$. נגדיר הצתקה

$$f: R \rightarrow M \quad (f(r) = rm) \leftarrow \text{הסתכל על } R \text{ כמוקף מעל עצמו}$$

ברור שזה הוא של R -מוקדם.

f של M כי M יוצר את M . לפי משפט איז'ר, עבור מוקדם

$$M = f(R) \cong R / (\ker f)$$

וגן $\ker f$ הוא חת מוקדם של R . כלומר, איננו שואלי.

תוצאה:

$$G \cong \mathbb{Z} / n\mathbb{Z} \text{ או } G \cong \mathbb{Z}$$

הוכחה:

מבורה אנליטית $= \mathbb{Z}$ -מוקדם. לפי הטענה הקודמת, G ציקלית $\Leftrightarrow G \cong \mathbb{Z} / I$ כמבורה אנליטית ($= \mathbb{Z}$ -מוקדם) כאשר I קוץ של \mathbb{Z} .

$$I = n\mathbb{Z} \quad \text{או} \quad \mathbb{Z} / I \cong \mathbb{Z} \Leftrightarrow I = (0)$$

טענה:

יהי R תחום ראשי, יהי $a, b \in R$. אזי $\exists \text{gcd}$ הוא gcd של $a, b \Leftrightarrow (a, b) = (g)$.

הוכחה:

קריטי.

טענה:

יהיו $a, b \in R$ כאשר R תחום ראשי. יהי gcd של a, b . אזי קיימים

$$x, y \in R \text{ כך } \text{gcd} = xa + yb$$

הוכחה:

$(a, b) = (g)$ לפי הטענה הקודמת

טענה:

יהי R תחום ראשי, יהי $c_1, \dots, c_n \in R$. יהיה gcd כך ש-

$$\text{gcd}(c_1, \dots, c_n) = 1 \Leftrightarrow (c_1, \dots, c_n) = R$$

ז"ל קיימת מטריצה $A \in M_n(R)$ כך ש: (1) $\det A = 1$, (2) העמודה הראשונה

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

גאינקוקציה של n .

$n=2$: קיימים $x, y \in R$ כך $-e = xc_1 + yc_2 = 1$. יהי $A = \begin{pmatrix} c_1 & -y \\ c_2 & x \end{pmatrix}$

גדלים: יהי $(g) = (c_1, \dots, c_{n-1})$. אז g לא בהכרח הכי קטן. אז $\gcd(g, c_n) = 1$ לכן.

קיימים $x, y \in R$ כך $e = gx + c_n y = 1$. יותר נכון, יהיו

$$c_1 = g d_1, c_2 = g d_2, \dots, c_{n-1} = g d_{n-1}$$

אז $\gcd(d_1, \dots, d_{n-1}) = 1$. גאינקוקציה קיימת מטכריצה $A' \in M_{n-1}(R)$ כך e

$\det A' = 1$ וזה העמודה הראשונה היא: $\begin{pmatrix} d_1 \\ \vdots \\ d_{n-1} \end{pmatrix}$. תהי:

$$A = \begin{pmatrix} c_1 & \begin{matrix} \text{מ-2 עמודות} \\ \text{יתרונות} \\ \delta e \end{matrix} & \begin{matrix} \vdots \\ d_1 y \\ \vdots \\ d_{n-1} y \end{matrix} \\ \vdots & & \vdots \\ c_n & 0 \dots 0 & x \end{pmatrix}$$