

חוקי נורמי (קומפוטציה)

- (1) Acc (אינדוקציה) $I_1 \subseteq I_2 \subseteq \dots$ בשיטת אינדוקציה טיפוסית
- (2) עקרון האינדוקציה
- (3) כל אינדוקציה נובעת מ-10

צמצום

(1) חוק סופר \mathbb{Z}
 $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \dots$
 גודל יורד וזה אינסופי אבל שרשרת קצרה

אקסיומ: הוכחה כי החוק (אינדוקציה) שלבים קטן [אם לא נוסח]

הוכחה: עבור $0 < a < b < 1$ נגדו: $f(a,b) = |a|$
 $I_{a,b} \subseteq I_{a,b}$ מוכח [אם לא נוסח]

$$I_{0,1} \subseteq I_{0,1/2} \subseteq I_{0,1/3} \subseteq I_{0,1/4} \dots$$

שיטת אינדוקציה

הוכחה

הוכחה: (1) מניח שאנחנו רוצים להוכיח
 R כל R נורמי קב [אם לא נוסח]

(= (אם לא נוסח) (אם לא נוסח))

הוכחה: נניח R הוא גוף נורמי (כל האינדוקציה) $P(x) = x^2 - 2$
 יש אינדוקציה באמצעות $P(x) = x^2 - 2$ ו- $P(x) = x^2 - 2$

הוכחה: נניח \mathbb{Z} הוא אינדוקציה (אם לא נוסח) $\mathbb{Z} \neq \emptyset$

זכור: $I \subseteq I+Ra$ $I \subseteq I+Rb$ $I \subseteq I+Rc$ $I \subseteq I+Rd$ $I \subseteq I+Re$ $I \subseteq I+Rf$ $I \subseteq I+Rg$ $I \subseteq I+Rh$ $I \subseteq I+Ri$ $I \subseteq I+Rj$ $I \subseteq I+Rk$ $I \subseteq I+Rl$ $I \subseteq I+Rm$ $I \subseteq I+Rn$ $I \subseteq I+Ro$ $I \subseteq I+Rp$ $I \subseteq I+Rq$ $I \subseteq I+Rr$ $I \subseteq I+Rs$ $I \subseteq I+Rt$ $I \subseteq I+Ru$ $I \subseteq I+Rv$ $I \subseteq I+Rw$ $I \subseteq I+Rx$ $I \subseteq I+Ry$ $I \subseteq I+Rz$

$(I+Ra) \cap (I+Rb) = I + R(a-b)$
 $(I+Ra) \cap (I+Rb) \cap (I+Rc) = I + R(a-b-c)$
 $(I+Ra) \cap (I+Rb) \cap (I+Rc) \cap (I+Rd) = I + R(a-b-c-d)$

מרחב וקטורי V מעל F . I אידיאל של $F[x]$.
 $I = \langle p_1, \dots, p_n \rangle$
 $I = \langle q_1, \dots, q_m \rangle$
 $I = \langle r_1, \dots, r_k \rangle$

קבוצת I מכילה את כל הפולינומים שמתחלקים ב- I .
 $I = \langle p_1, \dots, p_n \rangle = \langle q_1, \dots, q_m \rangle = \langle r_1, \dots, r_k \rangle$

צורת גלואט: $F[x], \mathbb{Z}$

$\sqrt{2} = \sqrt{2}$
 $\sqrt{2} = \sqrt{2}$

תהיה תוספת: זה לא אמר. נראה שיש להוכיח יותר.
 $(\sqrt{2})^2 = 2$. אם נחברו לפי המכונה

תהיה - אחת פתיחה יותר (תהיה $\sqrt{2}$)
 אחת שלמה אחת מהו (תהיה $\sqrt{2}$)

צורת גלואט: אחת מהו אחת מהו

הקדמה: $\gcd(a,b)$ עם אזור d כך ש- $a|bd$ ו- $b|ad$ $\therefore \gcd(a,b) | d$

תכונות

- * \gcd לא תלכסם ק"פ
- * אם a ו- b קוים d אז $d | \gcd(a,b)$ (ה- \gcd הוא-המ-מכיל-המקסימלי)
- * $d < a$ ו- $d < b$ והוא (המקסימלי) ש- $d | a$ ו- $d | b$ (המקסימלי המשותף)
- תכונות: $\gcd(a,b) = \gcd(b, a \bmod b)$ (ל- $a > b$)
- * אם a ו- b זרים אז $\gcd(a,b) = 1$

חוקים

חוק (א) חוק (ב) חוק (ג) חוק (ד) (PID) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

משפט: חוק (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

במקרה (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

(2) $\langle a \rangle = a\mathbb{Z}$

(3) $F[x]$

(4) $F[x]$

חוק (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח) $d = xa + yb$ $\gcd(a,b) = \langle a, b \rangle$

משפט: חוק (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

חוק (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

משפט: חוק (א) חוק (ב) חוק (ג) חוק (ד) חוק (ה) חוק (ו) חוק (ז) חוק (ח)

הכל
 אגלה, יורו אחרות פירוק וזהה על ההצגה והאנשים הם באישי.

אחר R אחר באישי.

אחר R אחר באישי.
 אחר R אחר באישי.

אחר R אחר באישי.
 אחר R אחר באישי.

אחר R אחר באישי.

אחר R אחר באישי.

אחר R אחר באישי.

$$M = \{ \dots \}$$

$$\{ \dots \}$$

$$M = \{ \dots \}$$

$$M = \{ \dots \}$$

$$M = \{ \dots \}$$

$$M = \{ \dots \}$$

אחר

$$x \in M \quad \text{ב} \quad \geq$$

$$M+Ra \ni x = m' + ra$$

$$x \cdot d = (m' + ra)d = \underbrace{m'd}_M + \underbrace{rad}_M \in M$$

כ"כ $d \in (M:a)$

ע"כ קיימת $d \in M$ ויש d המכיל את a (כלומר $d \in (M:a)$)

לכן

שאלה: האם $\mathbb{Z}[i]$ הוא דומיננט? $\mathbb{Z}[i]$

התשובה היא כן, וזאת בגלל שיש $N(x) = a^2 + b^2$ (כאשר $x = a + bi$)

$x = ab$
 $N(x) = N(a)N(b)$

המשפט הזה נקרא משפט גאוס. לדוגמה, $2 = (1+i)(1-i)$ (כאשר 2 אי-פרימ

$N(1+i) = 2$

$\mathbb{Z}[i] \rightarrow$ $p \equiv 3 \pmod{4}$ אינו מתפצל (כלומר p אי-פרימ)

$p^2 = N(p) = N(a) \cdot N(b)$ (כאשר $p = a + bi$)
 $p = a \cdot b$ ו- p אי-פרימ $\Leftrightarrow N(a) = p$

כלומר $N(a) = a^2 + b^2 = p \equiv 3 \pmod{4}$ אינו אפשרי (כלומר $a = \alpha + \beta i$)

$\exists x^2 + y^2 \mid x, y \in \mathbb{Z} \neq 3$

לכן $\mathbb{Z}[i]$ הוא דומיננט

השאלה היא: האם $\mathbb{Z}[i]$ הוא דומיננט?

$p \equiv 1 \pmod{4}$ מתפצל p (כלומר p אי-פרימ)

$x^2 \equiv -1 \pmod{p}$ - יש פתרון $x \in \mathbb{Z}$ עבור $p \equiv 1 \pmod{4}$ (כלומר p אי-פרימ)

לכן

לכל $a \in \mathbb{Z}$

יש $d \in \mathbb{Z}$ כך ש-

$I = \bigcup_{i \in \mathbb{Z}} I_i$

כאשר $I_i = a + i\mathbb{Z}$

כלומר $\mathbb{Z}[i]$ הוא דומיננט

$S \subseteq M+Ra$

$(M:a) =$

כלומר

$(M:a)$

כלומר $\mathbb{Z}[i]$ הוא דומיננט

יבג
הוכחה: p הוא מספר ראשוני של $a+ib$ ו- $a, b \in \mathbb{Z}$.

$$N(a+ib) = (a+ib)(a-ib) = p$$

הוכחה: $x^2 \equiv -1 \pmod{p}$ ו- $x \in \mathbb{Z}$.

$$p \mid x^2 + 1 = (x+i)(x-i)$$

כלומר $p \mid x+i$ או $p \mid x-i$.

$$p \mid \overline{x+i} = x-i$$

$$\Leftrightarrow p \mid x \Leftrightarrow p \mid (x-i)(x+i) = 2x$$

$$p \mid 1 = (x^2+1) - x^2$$

כלומר $p \mid 1$ וזה סתירה.

$$p^2 = N(p) = N(c) \cdot N(d)$$

↓

כלומר $c \mid p$

$$c \cdot \bar{c} = N(c) = p$$

כלומר $c \mid p$ ו- $\bar{c} \mid p$.

לכן