

הרצאה 14

שאלה אין לחשוב על איברים של שוג סופיים?

למשל, אם q הוא אינרטיאלי של $\mathbb{Z}/p\mathbb{Z}$ שזה האיבר
 זה מתקין שיקרא מילואו q . אם q לא חדר וכהנני
 אדם.

צוגה יהי F שזה סופי אינרטיאלי הסוג שלו הינו
 חזקה של האינרטיאלי. אם $q = p$ חזקה של
 האינרטיאלי קיים שזה יחיד (זו נוי אינרטיאלי) מסוג
 \mathbb{F}_q אלו

שאלה איך לבנות את \mathbb{F}_q ?

איך לבנות את \mathbb{F}_4 שיתו $\mathbb{Z}/4\mathbb{Z}$ לא
 שזה!

אינרטיאלי לא חדר
 $[0] = [2] - [2] = [0]$

שאלה ושוג בג'אן שוג F , און
 לאו ברירה סופי!

לבנות שוג קטורים יחד, אמנילים F ?

\mathbb{C} "ממילי" \mathbb{R} ←

$\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} : a, b \in \mathbb{Q}\}$ ← "ממילי" \mathbb{Q}

הרעיון ה(לוא) יהי F שגו כלשהו. טעני $F[x]$ הינו
 מחום אינלייני; אכן מחום ראשי, אכן גבתי!

$$\{ \text{שזוג} \} \subseteq \{ \text{מחום אינלייני} \} \subseteq \{ \text{מחום ראשי} \} \subseteq \{ \text{מב"י} \} \subseteq \{ \text{מחום גלג} \} \subseteq \{ \text{מחום אלמיג} \}$$

יהי $f \in F[x]$ פולינום אי-בריק. אכן, q גם איבר הראשוני
 לני $F[x]$ גבתי, ולכן כל איבר אי-בריק הוא ראשוני. אכן,

$$0 \neq (q) \text{ איגורל ראשוני לא-אבסי ולכן מקסימלי}$$

לני $F[x]$ מחום ראשי, אכן $\dim F[x] = 1$, אכן השורג

$$(0) \subseteq (q) \text{ של איגורליב ראשוניים הינו מאגר מקסימלי.}$$

אכן הינו $F[x]/(q)$ הינו שגה.

$$\begin{array}{ccc} F & \longrightarrow & F[x]/(q) \\ \alpha & \longmapsto & \alpha + (q) \end{array} \quad \text{הזוג יש לני סיכון}$$

נה החייז כי $\deg q \geq 1$ אי-בריק. אכן לא הינו,

אכן לא פולינום קבוע. אכן, אבס $a, b \in F$, $a \neq b$

$$a - b \notin (q)$$

כל האיגורליב של (q) היב
 סי, אלו פולינומים ממעלה $\leq \deg q$.

הערה 2 לאינן נחלקים האזורים של $F[x]/(g)$?

יהי $f \in F[x]$ פולינום כלשהו. סוף $F[x]$ גומים
 אינרצ'ני, הנומיה היא המעלה של פולינום כלפי.

$$f = qg + r$$

ואם $\deg r < \deg g = n$ (הקטיון) $(n = \deg g)$

$$f + (g) = r + (g) \Leftrightarrow f - r = qg \in (g)$$

כלומר, בכל מחלקה של $F[x]/(g)$ יש פולינום ממעלה

$< n$. הפולינום היחיד שיהי סגור סוף r_1, r_2

עדי פולינומים ממעלה $< n$ באוגה מחלקה, אינן

$$r_1 = r_2 \Leftrightarrow r_1 - r_2 = 0 \Leftrightarrow \deg(r_1 - r_2) < n \Leftrightarrow r_1 - r_2 \in (g)$$

מסקנה: אם כל איבר של $F[x]/(g)$ ניתן להצג

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} + (g) \quad \text{בצורה גבוהה}$$

$$a_0, \dots, a_{n-1} \in F$$

עכשיו $F = \mathbb{F}_p =$ גופו p ראשוני. יהי $g \in \mathbb{F}_p[x]$

פולינום אי-זריק ממעלה n אלפי $\mathbb{F}_p[x]/(g)$ הינה

$$\mathbb{F}_p[x]/(g) = \{ a_0 + \dots + a_{n-1}x^{n-1} + (g) : a_i \in \mathbb{F}_p \} \quad \text{... וז"ע}$$

$$|\mathbb{F}_p[x]/(g)| = p^n$$

$$\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(g)$$

$g = x^2 + x + 1 \in \mathbb{F}_2[x]$ הפולינום $F = \mathbb{F}_2^{\mathbb{Z}/2\mathbb{Z}}$
 ... וז"ע

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1) = \{ 0+(g), 1+(g), x+(g), x+1+(g) \}$$

$$= \{ \bar{0}, \bar{1}, \bar{x}, \overline{x+1} \}$$

המספרים הם המספרים $\bar{0}, \bar{1}, \bar{x}, \overline{x+1}$

$$\overline{x} \cdot \overline{x+1} = \overline{(x^2+x)} = \overline{(-1)} = \bar{1}$$

$$\overline{x} \cdot \overline{\bar{x}} = \overline{x^2} = \overline{(-x-1)} = \overline{x+1}$$

$g \in \mathbb{F}_2[x]$ הפולינום $\in \mathbb{F}_2[x]$ הפולינום $\mathbb{F}_2[x]/(g)$ הפולינום $\mathbb{F}_2[x]/(g)$ הפולינום $\mathbb{F}_2[x]/(g)$ הפולינום

$F \in K$ $x+(g)$ $\mathbb{F}_2[x]/(g)$ $\mathbb{F}_2[x]/(g)$

$g \in \mathbb{F}_2[x] \subseteq K[x]$ הפולינום $K = \mathbb{F}_2[x]/(g)$ הפולינום

$$g(x) = b_0 + b_1 x + \dots + b_n x^n$$

$$g(x+g) = b_0 + b_1(x+g) + \dots + b_n(x+g)^n =$$

$$(b_0 + b_1 x + \dots + b_n x^n) + g = g + g = 0 + g = 0_K.$$

הצורה $K = F[x]/(g)$ של F היא אלגוריתם של F וקטורי, נחלק F

$$\dim_F K = \deg g = n < \infty \quad | \quad F \subseteq K$$

בסיס $\{1+g, x+g, x^2+g, \dots, x^{n-1}+g\}$ הינו

בסיס K על F וכל $\alpha \in K$ נכתב כסכום בסיס

$$\alpha = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + g \quad a_i \in F$$

הקבוצה $R \subseteq S$ מוקימה. S היא אלגברת

של R על F היא אלגברת פולינומית $R[x]$

כלומר, קיים $b_0 + b_1 x + \dots + b_n x^n \in R[x]$ כך

$$b_0 + b_1 s + \dots + b_n s^n = 0_s$$

כל $s \in S$ הוא אלגברי מעל R , הוא נקרא אלגברי

(למעשה)

Lindemann (1873) π, e
 π, e אינם אלגבריים מעל \mathbb{Q}

Alan Baker
Transcendental Number
Theory

אסימטריה בהוכחה בגחילוב הוסבר
בזמנה של איליני 2.

$\sum_{n=1}^{\infty} \frac{1}{n^3}$ (אפרי, 1977) $\zeta(3)$

? $\sum_{n=1}^{\infty} \frac{1}{n^5}$ האם פשוטה

$$\zeta(m) = \sum_{n=1}^{\infty} \frac{1}{n^m}$$

$$\zeta(2) = \frac{\pi^2}{6}$$

$$\zeta(4) = \frac{\pi^4}{90}$$

טענה נחשבו $K = F[x]/(g)$ - F שדה
כאשר K שדה F שדה

הוכחה $\dim_F K = n = \deg g$ $\beta \in K$ יחידי

גורמים $1, \beta, \beta^2, \dots, \beta^n$
שדה F שדה

כאן קיימת גורם $a_0 + a_1\beta + a_2\beta^2 + \dots + a_n\beta^n = 0$, כאשר

$\beta \in F$ $a_i \in F$ β יחידי שדה F שדה
 $a_0 + a_1x + \dots + a_nx^n$

הסקנה אי אכאז אקבא עגז שמניא אאז יד אע וזי
 $\mathbb{Q}[x]/(f)$ עגזי פוליוזיב אן-פרייז $\mathbb{Q}[x]$.

תצור אמולויב.

הקנה R חוק R -מודול (אמולוי) היינו חבורה אבליק M
 (אזי חזקה +)

עב נפל סקלרו $M \rightarrow R \times M$ בן e .

$$\begin{array}{l} r, s \in R \\ m, n \in M \end{array} \quad \text{אנא} \quad \left\{ \begin{array}{l} (r+s)m = rm + sm \quad (1) \\ r(m+n) = rm + rn \quad (2) \\ r(sm) = (rs)m \quad (3) \\ 1_R \cdot m = m \quad (4) \end{array} \right.$$

זקנהא יהיו $R \subset S$ חוקים (R גג-חוק של S) אאזי א-א-
 יש מבנה טבעי של R-מודול.

חבור : חבור של S
 נפל סקלרו : r (נפל גיין S).

מקנה פול $F \subseteq K$ כמו אמולוי. אאזי א-א- יש מבנה טבעי.

של F-מודול, נאמר של מרוב וקטוריאלי F , כמו שגאלין.

האופן שבו יוגדר נכס, יהי $f: R \rightarrow S$ הומומורפיזם
 של S ונגד S כהוגו $S \rightarrow R$ מוגדר

$$\underbrace{r \cdot s}_{\text{כנס } S} = \underbrace{f(r) \cdot s}_{\text{כנס } S}$$

הקבוצה R חוקי, M מודול R והאנניטור M $\subseteq R$ היא

$$\text{Ann}_R(M) = \{r \in R : r \cdot m = 0_M \quad \forall m \in M\} \subseteq R$$

היא $\text{Ann}_R(M) \triangleleft R$ היא $\{0, 1\}$ היא

הוכחה סגירות $\{0, 1\}$: יהי $r, s \in \text{Ann}_R(M)$ היא

$$\begin{aligned} (-1)m = -m \quad (r-s)m &= rm - sm = 0_M - 0_M = 0_M \\ r-s &\in \text{Ann}_R(M) \quad \text{כנס} \end{aligned}$$

$$\begin{aligned} (ar)m &= a(rm) = a \cdot 0_M = 0_M && r \in \text{Ann}_R(M) \\ (ra)m &= r(am) = 0_M && a \in R \end{aligned}$$

$\text{Ann}_R(M) \triangleleft R$ היא $\{0, 1\}$ היא $ar, ra \in \text{Ann}_R(M)$ כנס

השאלה היא: האם M הוא S -מודול פשוט?

התשובה היא: כן.

$$(r + \text{Ann}_R(M))m = rm$$

(כל $r \in R$)

אם $\text{Ann}_R(M) = (0)$ אז M הוא R -מודול פשוט.