

תורת המספרים האלגברית (88798) תשפ"א

תרגיל 3

1. יהי K שדה מספרים ממעלה $n = [K : \mathbb{Q}]$. בהרגיל הזה נראה הוכחה פשוטה של הסופיות של Cl_K שלא משתמשת בשריגים ובמשפט מנקובסקי.

(א) יהי $\alpha_1, \dots, \alpha_n$ בסיס שלם של K . יהי $a \in K$ ונרשום $a = \sum_{i=1}^n c_i \alpha_i$, כאשר $c_i \in \mathbb{Q}$. נתבונן בהעתקה

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow [0, 1]^n \\ \varphi_a(t) &= (\{tc_1\}, \dots, \{tc_n\}), \end{aligned}$$

כאשר $\{y\}$ מסמן את החלק השברי של המספר הרציונלי $y \in \mathbb{Q}$. לדוגמא, $\{\pi\} = 0.14159\dots$. יהיו $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ השיכונים של K לתוך \mathbb{C} . בהוכחה הזאת אין צורך להפריד בין השיכונים הממשיים והאחרים. יהי $L \in \mathbb{N}$. הוכח שקיים מספר שלם $1 \leq t \leq L^n$ ואיבר $b \in \mathcal{O}_K$ כך שמתקיים

$$|N_{K/\mathbb{Q}}(ta - b)| \leq \frac{1}{L^n} \sum_{i=1}^n \cdots \sum_{i_n=1}^n \prod_{j=1}^n |\sigma_j(\alpha_{i_j})|.$$

רמז: חלק כל צלע של הקוביה ה- n -מימדית $[0, 1]^n$ ל- L קטעים שווים, וקבל L^n תת-קוביות. יהיו $t_1, t_2 \in \mathbb{Z}$ כך ש- $\varphi_a(t_1), \varphi_a(t_2)$ שייכים לאותה תת-קוביה, וקח $t = t_1 - t_2$. $b = \sum_{i=1}^n ([t_1 c_i] - [t_2 c_i]) \alpha_i \in \mathcal{O}_K$, $t = t_1 - t_2$.
 (ב) נקבע מספר שלם L כך ש- $H = L^n > \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n \prod_{j=1}^n |\sigma_j(\alpha_{i_j})|$. הוכח שלכל $a \in K$ קיים מספר שלם $1 \leq t \leq H$ ואיבר $b \in \mathcal{O}_K$ כך ש- $|N_{K/\mathbb{Q}}(ta - b)| < 1$.
 זה משפט של קירוב דיופנטי: כל $a \in K$ הינו קרוב לשבר עם מכנה חסום.

(ג) יהי $I \triangleleft \mathcal{O}_K$ אידאל. $0 \neq y \in I$ נבחר איבר $y \neq 0$ כך ש- $|N_{K/\mathbb{Q}}(y)|$ מינימלי. יהי $a \in I$ איבר כלשהו. הוכח שקיימים שלם $1 \leq t \leq H$ ואיבר $b \in \mathcal{O}_K$ כך שמתקיים $ta = by$.

(ד) יהיו I, y כמו בסעיף הקודם. הוכח כי $|N_{K/\mathbb{Q}}(y)| \leq (H!)^n N(I)$.

(ה) הסק, כמו בשיעור, כי Cl_K סופית. שים לב שהחסם $(H!)^n$ המתקבל מן ההוכחה הזאת גרוע בהרבה מחסם מינקובסקי.

2. הוכח בעזרת חסם מינקובסקי שחוגי השלמים של השדות $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ כולם תחומים ראשיים.

3. הוכח כי $\text{Cl}_{\mathbb{Q}(\sqrt{-5})} \simeq \mathbb{Z}/2\mathbb{Z}$. אכן, החוג $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ אינו תחום פריקות יחידה.

4. הוכח שאין $x, y \in \mathbb{Z}$ שמקיימים $y^3 = x^2 + 5$.

רמז: נניח בשלילה שקיימים x, y כזה. הוכח שהם זרים, כי x זוגי, וכי y אי-זוגי. נתבונן באידאלים $I = (x + \sqrt{-5})$, $J = (x - \sqrt{-5})$ של $\mathbb{Z}[\sqrt{-5}]$. שים לב כי $IJ = (y)^3$. הוכח שלאידאלים I, J אין גורם ראשוני משותף. לכן $I = (I')^3$ עבור אידאל $I' \triangleleft \mathbb{Z}[\sqrt{-5}]$. הסק בעזרת התרגיל הקודם כי I' ראשי וקבל סתירה.

5. באופן דומה, הוכח שאם $x, y \in \mathbb{Z}$ מקיימים $y^3 = x^2 + 1$ אזי $(x, y) = (0, 1)$.
זה פותר חצי מן התרגיל האחרון בקובץ התרגילים הראשון.

6. יהיו $x, y, z \in \mathbb{Z}$ מספרים שלמים שמקיימים

$$x^2 + 1 = z = y^3 - 1.$$

הוכח כי $z = 26$.

7. מצא את הסדר של $\text{Cl}_{\mathbb{Q}(\sqrt{6})}$.

בשבועות הקרובים נלמד איך למצוא את הפירוק לגורמים ראשוניים של האידאל $p\mathcal{O}_K$, כאשר p מספר ראשוני ואילו K שדה מספרים. עם הכלים האלה נוכל לטפל בשאלות רבות נוספות הקשורות לחבורות מחלקה.