

# תורת המספרים האלגברית (88798) תשפ"א

## תרגיל 4

1. יהי  $K = \mathbb{Q}(\sqrt{65})$ .

(א) הוכח כי  $3\mathcal{O}_K$  ראשוני וכי  $2\mathcal{O}_K = P_1P_2$ , כאשר  $P_1, P_2 \triangleleft \mathcal{O}_K$  הינם אידיאלים ראשוניים שונים.

(ב) יהי  $S = \{x \in \mathcal{O}_K : N_{K/\mathbb{Q}}(x) = \pm 2\}$ . הוכח כי  $P_1, P_2$  ראשיים אם ורק אם  $S \neq \emptyset$ .

(ג) יהיו  $\mathbb{R} \hookrightarrow K \xrightarrow{\sigma_1, \sigma_2} \mathbb{R}$  שני השיכונים של  $K$  ב- $\mathbb{R}$ , ונגדיר  $\lambda : \mathcal{O}_K \setminus \{0\} \rightarrow \mathbb{R} \times \mathbb{R}$  על ידי  $\lambda(x) = (\log |\sigma_1(x)|, \log |\sigma_2(x)|)$ .

מצא איבר הפיך  $u \in \mathcal{O}_K^\times$  שאינו שורש יחידה. התת-חבורה  $\langle u \rangle \subset \mathcal{O}_K^\times$  פועלת על  $S$  על ידי כפל. היעזר בפעולה הזאת כדי לקבוע  $c > 0$  מפורש כך שאם  $S$  לא ריק, אזי קיים  $x \in S$  שמקיים

$$\lambda(x) \in \{(y_1, y_2) \in \mathbb{R} \times \mathbb{R} : |y_1| < c, |y_2| < c\}.$$

(ד) מצא מספר שלם מפורש  $N$  כך אם  $x = a + b\sqrt{65} \in S$  הינו האיבר מן הסעיף הקודם, אזי בהכרח  $|a|, |b| < N$ .

(ה) כיוון ש- $x \in \mathcal{O}_K$ , ותיארנו את החוג  $\mathcal{O}_K$  בקובץ התרגילים הראשון, בהכרח  $a, b \in \frac{1}{2}\mathbb{Z}$ . לכן יש רק מספר סופי של אפשרויות עבור  $x$ , אם הוא קיים. בדוק את הנורמות של כולם והוכח כי  $S = \emptyset$ . מומלץ לכתוב תוכנה של כמה שורות, כי מספר האפשרויות גדול מדי בשביל בדיקה ידנית.

(ו) הוכח כי  $P_1^2, P_2^2$  ראשיים.

(ז) הוכח בעזרת חסם מינקובסקי כי  $\text{Cl}_K \simeq \mathbb{Z}/2\mathbb{Z}$ .

2. בתרגיל הזה נראה משפחה של שדות מספרים עם חבורות מחלקה גדולות כרצונינו. יהי  $p$  מספר ראשוני שמקיים  $p \equiv 11 \pmod{12}$ . יהי  $K = \mathbb{Q}(\sqrt{-p})$ . נניח כי  $p > 3^m$ . לפי המפשט של דיריכלה על ראשוניים בסדרות אריתמטיות, לכל  $m$  קיימים  $p$  כאלה. הוכח כי  $\text{Cl}_K$  מכילה איברים מסדר גדול מ- $m$ , ובפרט  $|\text{Cl}_K| > m$ .

3. לכל שדה מספרים  $K$ , תהי  $d_K$  הדיסקרימיננטה של  $K$ . לכל  $n$  טבעי, נגדיר  $d(n) = \min\{|d_K| : [K : \mathbb{Q}] = n\}$ . הוכח כי  $\lim_{n \rightarrow \infty} d(n) = \infty$ .

4. בכל השאלות בהמשך, יהי  $A$  תחום דדקינד, יהי  $K = \text{Frac } A$ , תהי  $L/K$  הרחבה סופית וספרבילית, ויהי  $B$  הסגור השלם של  $A$  ב- $L$ . הוכח כי  $B$  הינו תחום דדקינד.

5. יהיו  $A, B, K, L$  כמו בשאלה הקודמת, ויהי  $\mathfrak{p} \triangleleft A$  אידיאל ראשוני. נסמן  $k = A/\mathfrak{p}$ . יהי  $n = [L : K]$ . בשאלה הזאת נוכיח כי  $\dim_k B/\mathfrak{p}B = n$ .

(א) יהי  $m = \dim_k B/\mathfrak{p}B$ . הוכח כי  $m < \infty$ .

(ב) יהי  $\bar{\beta}_1, \dots, \bar{\beta}_m$  בסיס של  $B/\mathfrak{p}B$  כמרחב וקטורי מעל  $k$ . לכל  $1 \leq i \leq m$  נבחר הרמה  $\beta_i \in B$  של  $\bar{\beta}_i$ . אנחנו רוצים להוכיח כי  $\beta_1, \dots, \beta_m$  הינו בסיס של  $L$  מעל  $K$ , ולכן  $m = n$ . נוכיח קודם כי  $\beta_1, \dots, \beta_m$  בלתי תלויים לינארית מעל  $K$ . נניח בשלילה שלא. הוכח שקיימים  $a_1, \dots, a_m \in A$ , לא כולם אפס, כך ש-  $a_1\beta_1 + \dots + a_m\beta_m = 0$ .

(ג) יהי  $I = (a_1, \dots, a_m) \triangleleft A$ . הוכח שקיים  $x \in I^{-1}$  כך ש-  $x \notin I^{-1}\mathfrak{p}$ . הוכח כי  $xa_i \in A$  לכל  $i$  וכי

$$\overline{xa_1}\bar{\beta}_1 + \dots + \overline{xa_m}\bar{\beta}_m = 0 \in B/\mathfrak{p}B$$

הינה תלות לינארית לא־טריוויאלית, בסתירה.

(ד) נשאר להוכיח כי  $\beta_1, \dots, \beta_m$  פורשים את  $L$ . נגדיר את  $\mathfrak{h} = A^{-1}N$  מודולים  $N = B/M$  ואת  $M = A\beta_1 + \dots + A\beta_m \subseteq B$ . הוכח כי  $\mathfrak{p}N = N$  וכי  $N$  נוצרת סופית.

(ה) יהי  $N = A\nu_1 + \dots + A\nu_s$ . הוכח שקיימים  $a_{ij} \in \mathfrak{p}$  כך ש-  $\nu_i = \sum_{j=1}^s a_{ij}\nu_j$ . נגדיר את המטריצה  $C = (a_{ij}) - I_s$ . הוכח כי  $(\det C)\nu_i = 0$  לכל  $i$ .

(ו) הסק כי  $(\det C)B \subseteq M$ . הוכח כי  $\det C \equiv \pm 1 \pmod{\mathfrak{p}}$  ובפרט  $\det C \neq 0$ . הוכח כי  $L = (\det C)L = K\beta_1 + \dots + K\beta_m$ .

6. יהי  $I \triangleleft B$ . הוכח שקיים  $\theta \in B$  כך ש-  $L = K(\theta)$  וכי  $\mathcal{F}_\theta$  זר ל-  $I$ .

7. הוכח כי  $\text{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/3\mathbb{Z}$ .