応用数理概論 (2) レポート課題
2022 年 1 月 21 日配布
提出期限：2022 年 2 月 4 日（金）17:00

注意

- 以下の 6 問のうち，2 問以上解答すること．
- 8 号館 6 階東側エレベーターホールのレポート入れに提出すること．
- 1 枚目に科目名・学修番号・氏名を書くこと．
- レポートが複数枚にわたるときは，左上をホッチキス等で綴じること．
- A4 レポート用紙を使用すること．

問題

以下の問題では，代数体 K の整数環を $\mathcal{O}_K$ で表し，K の単数（$\mathcal{O}_K$ の単元）全体を $\mathcal{O}_K^\times$ で表す．

1. 複素数 α を $X^3 - X + 1$ の一つの根として，$K = \mathbb{Q}(\alpha)$ とする．判別式
$$D(1, \alpha, \alpha^2) = \det[\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{i+j})]_{0 \le i,j \le 2}$$
を求めよ．
2. $\mathbb{Q}(\sqrt{-6})$ の類数を求めよ．
3. $K = \mathbb{Q}(\sqrt{7})$ とする．$\mathcal{O}_K^\times$ について，以下の問いに答えよ．
   (a) ある $\varepsilon_0 \in \mathcal{O}_K^\times$ が存在して，
   $$\mathcal{O}_K^\times = \{\pm\varepsilon_0^n \mid n \in \mathbb{Z}\} \qquad (*)$$
   が成り立つことを示せ．
   (b) $(*)$ を満たす ε_0 を一つ求めよ．
4. R を体でない Dedekind 環として，K を R の商体とする．$K^\times = K \setminus \{0\}$ とおく．$\mathfrak{p}$ を R の (0) でない素イデアルとする．$a \in K^\times$ に対して，分数イデアル (a) が
$$(a) = \mathfrak{p}^e \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_r^{f_r}$$
と素イデアル分解されるとき，$v_\mathfrak{p}(a) = e$ と定義する．ただし，$\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ は $\mathfrak{p}$ と異なる R の (0) でない相異なる素イデアルであり，$e, f_1, \ldots, f_r \in \mathbb{Z}$ とする．このように関数 $v_\mathfrak{p} \colon K^\times \to \mathbb{Z}$ を定義するとき，以下の性質が成り立つことを示せ．
   (a) 任意の $a, b \in K^\times$ に対して，$v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$ が成り立つ．
   (b) 任意の $a, b \in K^\times$ に対して，$a + b \neq 0$ ならば，$v_\mathfrak{p}(a + b) \ge \min\{v_\mathfrak{p}(a), v_\mathfrak{p}(b)\}$ が成り立つ．
5. p を素数，e を正の整数として，$q = p^e$ とする．$\mathbb{F}_q$ を q 個の元を持つ有限体とする．このとき，$\mathbb{F}_q$ と $\mathcal{O}_K/\mathfrak{p}$ が体として同型になるような代数体 K と $\mathcal{O}_K$ の素イデアル $\mathfrak{p}$ が存在することを示せ．

6. $N = 2501$ を数体篩法で素因数分解することを考える．$f(X) = X^2 + 1$ とおくと，$f(50) = 2501$ である．そこで，環準同型

$$\begin{aligned} \phi\colon \mathbb{Z}[\sqrt{-1}] &\to \mathbb{Z}/N\mathbb{Z} \\ a + b\sqrt{-1} &\mapsto a + 50b \bmod N \end{aligned}$$

を考える．以下の問いに答えよ．

(a) $(a, b) = (-2, 1), (22, 19)$ に対して，$(a + b\sqrt{-1})$ の素イデアル分解と $a + 50b$ の素因数分解を求めよ．

(b) (a) の結果を利用して，$x^2 \equiv y^2 \pmod{N}$ を満たす相異なる $x, y \in \mathbb{Z}$ を一組求めよ．

(c)（ユークリッドの互除法を用いて）$\gcd(x - y, N)$ を計算することで，N を素因数分解せよ．