広域数理科学概論 (4) レポート課題
2016 年 1 月 14 日配布
締め切り：2016 年 1 月 29 日（金）

注意

- 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，代数体 K の整数環を $\mathcal{O}_K$ で表す．

1. R をデデキント整域，$I, J \subset R$ を R の (0) でないイデアルとする．以下の問いに答えよ．
   (a) 次の 2 条件が同値であることを示せ．
      (i) I と J をともに割り切る R の素イデアルは存在しない．
      (ii) $I + J = R$.
   (b) I と J が (a) の同値な条件を満たすとき，R/IJ と $R/I \times R/J$ は環として同型であることを示せ．
2. 虚 2 次体 $K = \mathbb{Q}(\sqrt{-10})$ を考える．以下の問いに答えよ．
   (a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$ を示せ．
   (b) $\mathcal{O}_K$ のイデアル $(5, \sqrt{-10})$ が単項イデアルではないことを示せ．
   (c) K の類数が 2 であることを示せ．
3. 実 2 次体 $K = \mathbb{Q}(\sqrt{6})$ を考える．以下の問いに答えよ．
   (a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ を示せ．
   (b) K の類数が 1 であることを示せ．
   (c) $\mathcal{O}_K^\times = \{\pm(5 + 2\sqrt{6})^n \mid n \in \mathbb{Z}\}$ であることを示せ．
4. $f(X) \in \mathbb{Z}[X]$ をモニックな n 次既約多項式とする．α を $f(X)$ の根として，$\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ を α の共役元とする．以下の問いに答えよ．

(a) 任意の $n-1$ 次以下の多項式 $g(X)$ に対して次の等式が成り立つことを示せ．

$$g(X) = \sum_{i=1}^{n} \frac{g(\alpha^{(i)})}{f'(\alpha^{(i)})} \prod_{j \neq i} (X - \alpha^{(j)}).$$

(b) $K = \mathbb{Q}(\alpha)$ とする．このとき，任意の $\beta \in \mathcal{O}_K$ に対して $f'(\alpha)\beta \in \mathbb{Z}[\alpha]$ であることを示せ．

5. $N = 1769$ を数体篩法で素因数分解することを考える．$f(X) = X^2 + 5$ とおくと，$f(42) = 1769$ である．そこで，環準同型

$$\begin{aligned} \phi\colon \mathbb{Z}[\sqrt{-5}] &\to \mathbb{Z}/1769\mathbb{Z} \\ a + b\sqrt{-5} &\mapsto a + 42b \bmod 1769 \end{aligned}$$

を考える．以下の問いに答えよ．

(a) $(a, b) = (-17, 1), (7, 1)$ に対して，$(a + b\sqrt{-5})$ の素イデアル分解と $a + 42b$ の素因数分解を求めよ．

(b) (a) の結果を利用して，$x^2 \equiv y^2 \pmod{N}$ を満たす相異なる整数 x, y 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．