ALGEBRAIC NUMBER THEORY HOMEWORK 1 SOLUTION

- The solution is sometimes a sketch but you should fill in all the details.
- Comments can be sent to maliu@zju.edu.cn

§1.1. If \(N(\alpha) = \alpha \bar{\alpha} = 1\) then clearly \(\alpha\) is a unit. Conversely if \(\alpha \beta = 1\) for some \(\beta \in \mathbb{Z}[i]\), then \(N(\alpha)N(\beta) = 1\) hence \(N(\alpha) = N(\beta) = 1\).

§1.2. The assertion follows from the fact that \(\mathbb{Z}[i]\) is a UFD. Indeed, for a prime divisor \(\delta | \gamma\), we have either \(\delta^n \parallel \alpha\) or \(\delta^n \parallel \beta\) because \(\alpha, \beta\) are relatively prime.

§1.3. Since \((x,y,z) = 1\), \(x + iy\) and \(x - iy\) are relatively prime in \(\mathbb{Z}[i]\). Indeed, they obviously do not have a common prime divisor of the form \(p \equiv 3 \mod 4\). If they have a common prime divisor of the form \(a + ib\) with \(a^2 + b^2 = p \equiv 1 \mod 4\), then by conjugation \(a + ib\) and \(a - ib\) both divide \(x + iy\) (as well as \(x - iy\)), which implies that \(p|x \pm iy\), which again contradicts \((x,y,z) = 1\).

Thus by §1.2 we may write \(x + iy = (u + iv)^2\) and \(x - iy = (u - iv)^2\) up to units, which implies that \(x = u^2 - v^2\) and \(y = 2uv\) up to permutation of \(x,y\). The conditions on \(u,v\) can be easily checked.

§1.5. Consider the norm map \(N: \mathbb{Z}[\sqrt{-d}] \to \mathbb{N}, \alpha = a + b\sqrt{-d} \mapsto N(\alpha) = a^2 + b^2d\). If \(\alpha\) is a unit, say, \(\alpha \beta = 1\), then \(N(\alpha) = 1\) which forces that \(a = \pm 1, b = 0\).

§2.1. Let \(Tr, N\) be the trace and norm map from \(\mathbb{Q}(\sqrt{6})\) to \(\mathbb{Q}\). Denote \(a = \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}}\). Then
\[Tr(a) = -6, \quad N(a) = 3\]
hence \(a\) is a root of \(x^2 + 6x + 3 = 0\), which implies that \(a\) is an algebraic integer.

§2.4. For \(\alpha = a + b\sqrt{D} \in K\), we have \(\alpha \in \mathcal{O}_K\) if and only if
\[Tr(a) = 2a \in \mathbb{Z}, \quad N(a) = a^2 - b^2D \in \mathbb{Z}\]
From this it follows easily that
\[\mathcal{O}_K = \mathbb{Z}[\frac{1 + \sqrt{D}}{2}] \lor \mathbb{Z}[\sqrt{D}]\]
if \(D \equiv 1 \mod 4\) or \(D \equiv 2, 3 \mod 4\). In the first case
\[d = \left| \frac{1}{1 + \sqrt{D}} \frac{1}{1 - \sqrt{D}} \right|^2 = D,\]
and in the second case
\[ d = \left| \begin{array}{cc} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{array} \right|^2 = 4D. \]

\[ \square \]

§2.7. Following the hint, expand the determinant \( \det(\sigma_i \omega_j) = P - N \) where \( P, N \) are the sums corresponding to even and odd permutations respectively. Then \( d_K = (P - N)^2 = (P + N)^2 - 4PN \). Let \( L \) be the Galois closure of \( K \). Choose any extension of \( \sigma_i \) to \( \tilde{\sigma}_i \in \text{Gal}(L/\mathbb{Q}) \). Then one has coset decomposition
\[ \text{Gal}(L/\mathbb{Q}) = \bigcup_{i=1}^{n} \tilde{\sigma}_i \text{Gal}(L/K) = \bigcup_{i=1}^{n} \text{Gal}(L/K) \tilde{\sigma}_i. \]

Using this fact one can deduces that \( P + N \) and \( PN \) are invariant under \( \text{Gal}(L/\mathbb{Q}) \), which implies that \( P + N \) and \( PN \) are rational integers. It follows that \( d_K \) is a square modulo 4, i.e. \( \equiv 0 \) or \( 1 \mod 4 \). \( \square \)