Exercise sheet 8

Units, Decomposition Of Prime Ideals

*1. (a) Let M be a bounded subset of a finite dimensional real vector space V. Construct another bounded subset $N \subset V$ such that for any complete lattice $\Gamma \subset V$ with $V = \Gamma + M$, the subset $\Gamma \cap N$ generates Γ.

(b) Deduce that, in principle, for every number field K one can effectively find generators of $\mathcal{O}_K^\times$.

2. Prove that for any odd prime number p the following are equivalent:

(a) $p \equiv 1 \bmod (4)$.

(b) p splits in $\mathbb{Z}[i]$.

(c) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

*3. Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{2}\,)$ is $\mathbb{Z}[\sqrt[3]{2}\,]$ and compute its discriminant.

4. In the number field $K := \mathbb{Q}(\sqrt[3]{2})$, what are the possible decompositions of $p\mathcal{O}_K$ for rational primes p?

5. Consider a Dedekind ring A with quotient field K, a finite separable extension L/K of degree n, and let B be the integral closure of A in L. Assume that $L = K(\alpha)$, where the minimal polynomial $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ of α over K lies in $A[X]$ and is *Eisenstein at* a prime ideal $\mathfrak{p}$ of A, that is, all $a_i \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Show that $\mathfrak{p}B = \mathfrak{q}^n$ with $\mathfrak{q} := \mathfrak{p}B + \alpha B$ prime, so that $\mathfrak{p}$ is totally ramified in B.

(*Hint:* Prove that $\mathfrak{p}B \subset \mathfrak{q}^j$ for all $1 \leqslant j \leqslant n$ by induction on j.)

6. Consider the polynomial ring $A := k[x]$ over a field k of characteristic $p > 0$. Take an element $t \in k^\times$ and let y be a zero of the polynomial

$$f(Y) \ := \ Y^p - x^{p-1}Y - t \ \in \ A[Y]$$

in an algebraic closure of $K := \mathrm{Quot}(A)$.

(a) Show that f is invariant under the substitions $Y \mapsto Y + \alpha x$ for all $\alpha \in \mathbb{F}_p$.

(b) Show that f is separable and irreducible over K.

(c) Show that $L := K(y)/K$ is galois with Galois group isomorphic to $(\mathbb{F}_p, +)$.

*(d) Show that the integral closure B of A in L is equal to

$$\begin{cases} A[z] & \text{for } z := \frac{x}{y-s} \text{ if } t = s^p \text{ for some } s \in k, \\ A[y] & \text{if } t \text{ does not lie in the subfield } k' := \{a^p \mid a \in k\}. \end{cases}$$

(e) Determine the behavior of the prime $\mathfrak{p} := Ax \subset A$ in B.

(f) Discuss the action of $\mathrm{Gal}(L/K)$ on the residue field extension at $\mathfrak{p}$.