Exercise sheet 9
Fundamental units, Galois correspondence, and cyclotomic fields

Exercise 1. [Continued fractions]

Let $d > 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$.

Compute the first terms of the continued fraction expansion for $\sqrt{d}$ and deduce the fundamental unit of $\mathcal{O}_K^*$ for $d = 6, 7, 10, 11$.

Exercise 2. [Some results on cyclotomic fields]

(a) For any odd $n \geq 3$, count the number of quadratic subfields of $\mathbb{Q}(\zeta_n)$ in terms of $(\mathbb{Z}/n\mathbb{Z})^*$ (begin with the prime case).

(b) Prove that for every $m, n \geq 1$, $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_\ell)$ where ℓ is the lcm of m and n. Prove next that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$ where d is the gcd of m and n.

(c) (*Gauss-Wantzel*) We admit that the numbers of $\mathbb{C}$ constructible with straightedge and compass are exactly the numbers α such that there is a number field K containing α and a tower of subfields

$$\mathbb{Q} = K_0 \subset \cdots \subset K_n = K$$

where for every $i \in \{0, \cdots, n-1\}$, $[K_{i+1} : K_i] = 2$.

Prove that a primitive n-th root of unity is constructible with straightedge and compass if and only if

$$n = 2^k p_1 \cdots p_r$$

where the p_i's are pairwise distincts Fermat prime number (i.e. prime numbers of the shape $2^{2^m} + 1$.).

(d) For any $n \geq 1$ and any prime p, let α be such that $n = p^\alpha n'$ with n' coprime to p. Describe the ramification and inertia indices of p in $\mathbb{Q}(\zeta_n)$ in terms of the order of n' in $(\mathbb{Z}/p\mathbb{Z})^*$.

Exercise 3.

The goal of this exercise is to prove that for every $n > 1$, there is infinitely many prime numbers $p \equiv 1 \mod n$ (the weak case of Dirichlet's theorem).

(a) Prove that it is enough to prove that for every $n > 2$, there is at least one prime number $p \equiv 1 \mod n$. This is what we will do now.

(b) Let Φ_n be the n-th cyclotomic polynomial. Prove that for every $n > 2$, $|\Phi_n(n)| > 1$ and that $\Phi_n(n)$ divides $n^n - 1$.

(c) Let p be a prime divisor of $\Phi_n(n)$. Prove that it is prime to n, let t be the order of n in $(\mathbb{Z}/p\mathbb{Z})^*$.

(d) Prove that t divides n and that if $t < n$ then $\Phi_n(n)$ divides $(n^n - 1)/(n^t - 1)$. Deduce that $t = n$ and $p \equiv 1 \mod n$.