Dr. Andrey Soldatenkov
Jan Hesmert

Humboldt Universität zu Berlin
Summer term 2020

Algebraic Number Theory

Exercise sheet 11

Solutions should be submitted online before 6.07.20 via the Moodle page of the course:
`https://moodle.hu-berlin.de/course/view.php?id=95156`

Exercise 11.1. (3 + 3 points) Let $K = \mathbb{Q}(\mu)$, where μ is a primitive n-th root of unity for arbitrary n. Let $F \in \mathbb{Z}[X]$ be the monic minimal polynomial of μ.

1. Let $X^n - 1 = F(X)G(X)$ for some $G \in \mathbb{Z}[X]$. Taking derivatives of both sides, deduce that $N_{K/\mathbb{Q}}(F'(\mu))$ divides some power of n.
2. Deduce that the prime factors of d_K are among the prime factors of n. Conclude that if p ramifies in K, it divides n.

Exercise 11.2. (3 points) Let $K = \mathbb{Q}(\mu)$ for μ a primitive p-th root of unity, where $p > 2$ is prime. Recall that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{F}_p^\times$. Consider the index 2 subgroup $(\mathbb{F}_p^\times)^2 \subset \mathbb{F}_p^\times$ and the corresponding quadratic field $F \subset K$. Identify this quadratic field (i.e. find $d \in \mathbb{Z}$, such that $F \simeq \mathbb{Q}(\sqrt{d})$).

Exercise 11.3. (5 points) Consider the group $(\mathbb{Z}/p^k\mathbb{Z})^\times$. Is this group is always cyclic? Prove that there exists a natural homomorphism $(\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p^{k-1}\mathbb{Z})^\times$, and that it is surjective. Prove that it induces an isomorphism of prime-to-p parts $\mathbb{Z}/(p-1)\mathbb{Z}$ of both groups and eventually identifies those parts with $\mathbb{F}_p^\times$. Using this, construct a splitting of the group surjection $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$, where $\mathbb{Z}_p$ are p-adic integers.