Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie

SoSe 2019

Exercise Sheet 7

If you want your solutions to be corrected, you should hand them in by Monday, June 3.
Please write your name and immatriculation number on top of every exercise

Exercise 7.1 (1+2+2 points) Let $\mathbb{Q} \subseteq K \subseteq L$ be number fields and $\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \mathcal{O}_L$ the corresponding rings of integers. Let also $p \in \mathbb{Z}$ be a prime, $P \subseteq \mathcal{O}_K$ a prime ideal that lies over p and $Q \subseteq \mathcal{O}_L$ a prime ideal that lies over P.

a) Show that Q lies over p.

b) Show that the ramification index is multiplicative: $e_Q(p) = e_Q(P) \cdot e_P(p)$.

c) Show that the inertia degree is multiplicative: $f_Q(p) = f_Q(P) \cdot f_P(p)$.

Exercise 7.2 (2+1+4+4 points) Let $\Phi_n(X) \in \mathbb{Z}[X]$ be the d-th cyclotomic polynomial. By definition, this is the minimal polynomial of ζ_n over $\mathbb{Q}$. Since Φ_n has integer coefficients, we can define analogous cyclotomic polynomials $\Phi_n(X)$ with coefficients in any ring A, thanks to the canonical map $\mathbb{Z} \to A$.

a) Prove that $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Let k be a field of characteristic zero, or of positive characteristic p such that $p \nmid n$.

b) Prove that $X^n - 1$ is squarefree in $k[X]$.

c) Prove that the roots of $\Phi_n(X)$ in k correspond to primitive n-th roots of unity: by definition, these are the elements of the multiplicative group k^* of order exactly n.

Now consider a finite field $\mathbb{F}_p$ such that $p \nmid n$. Recall that every finite extension $K/\mathbb{F}_p$ is Galois, with Galois group generated by the Frobenius automorphism $F\colon K \to K, \alpha \mapsto \alpha^p$.

d) Let $g_i(X)$ be an irreducible factor of $\Phi_n(X)$ in $\mathbb{F}_p[X]$, and let $\mathbb{F}_p(\alpha) = \mathbb{F}_p[X]/(g_i(X))$ be the corresponding field extension. Prove that $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = f$, where f is the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

Exercise 7.2 (1+3+3+4 points) Here we consider splitting of primes in cyclotomic extensions $\mathbb{Q}(\zeta_n)$. Let $p \in \mathbb{Z}$ be a prime: since the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, we know that the ramification indexes and the inertia degrees for p are all the same: this means that p splits in $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ as

$$p\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathfrak{p}_1^e \dots \mathfrak{p}_r^e, \qquad f_{\mathfrak{p}_i}(p) = f$$

We want to compute e, f, r.

a) Show that $e \cdot f \cdot r = \varphi(n)$.

Suppose first that $n = p^k$.

b) Consider the factorization of $X^{p^k} - 1$ in $\mathbb{F}_p[X]$ and conclude that $e = \varphi(p^k), f = 1, r = 1$.

Suppose now that $n = m$ with p, m coprime.

c) Using Exercise 7.2.b and Exercise 7.2.d show that $e = 1$ and that f is the order of p in the group $(\mathbb{Z}/n\mathbb{Z})^*$.

Now suppose that $n = p^k \cdot m$, with p, m coprime.

d) Consider the intermediate extensions $\mathbb{Q}(\zeta_m), \mathbb{Q}(\zeta_{p^k}) \subseteq \mathbb{Q}(\zeta_n)$ and conclude that $e = \varphi(p^k)$ and that f is the order of p in the group $(\mathbb{Z}/n\mathbb{Z})^*$. You will need Exercise 7.1.