Universität Basel

Analytic Algebraic Number Theory
November 11, 2019

Exercise sheet #8

Exercises marked with a ✎ are to be handed in before **Monday November 18** at noon, in the mailbox at Spiegelgasse 1. Each of these is worth a number of points, as indicated.
Questions marked with a $\star$ are more difficult.

Exercise 1 – Let A be a Dedekind ring with field of fractions K. We assume that K has characteristic 0. Let L/K be a finite Galois extension with Galois group G, and B be the integral closure of A in L.

Let $\mathfrak{p}$ be a maximal ideal in A, and $\mathfrak{q}$ be a maximal ideal of B such that $\mathfrak{q} \cap \mathrm{A} = \mathfrak{p}$ (i.e., $\mathfrak{q}$ appears in the factorisation of $\mathfrak{p}\mathrm{B}$ as a product of prime ideals in B). We say that $\mathfrak{q}$ lies above $\mathfrak{p}$.

We assume that $\mathrm{A}/\mathfrak{p}$ is finite or of characteristic p.

1.1. Prove that $\ell := \mathrm{B}/\mathfrak{q}$ is a finite Galois extension of $k := \mathrm{A}/\mathfrak{p}$. What is the degree of that extension?

1.2. Let $\mathrm{D}_\mathfrak{q}$ be the subgroup of G formed by elements $\sigma \in \mathrm{G}$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$. Show that the reduction map $\mathrm{A} \to \mathrm{A}/\mathfrak{p}$ induces a surjective group morphism $\rho_\mathfrak{q} : \mathrm{D}_\mathfrak{q} \to \mathrm{Gal}(\ell/k)$.

1.3. Let $\mathrm{I}_\mathfrak{q}$ denote the kernel of $\rho_\mathfrak{q}$. Prove that, for all $\sigma \in \mathrm{G}$, we have $\mathrm{D}_{\sigma(\mathfrak{q})} = \sigma \mathrm{D}_\mathfrak{q} \sigma^{-1}$ where $\sigma \mathrm{D}_\mathfrak{q} \sigma^{-1} = \{\sigma\tau\sigma^{-1},\ \tau \in \mathrm{D}_\mathfrak{q}\}$, and $\mathrm{I}_{\sigma(\mathfrak{q})} = \sigma \mathrm{I}_\mathfrak{q} \sigma^{-1}$.

1.4. Show that $\mathrm{D}_\mathfrak{q}/\mathrm{I}_\mathfrak{q} \simeq \mathrm{Gal}(\ell/k)$ and deduce that $\#\mathrm{I}_\mathfrak{q}$ is equal to the multiplicity $e(\mathfrak{q}/\mathfrak{p})$ with which $\mathfrak{q}$ appears in $\mathfrak{p}\mathrm{B}$ (i.e., the ramification index of $\mathfrak{p}$ in L).

1.5. Assume that G is abelian. Prove that $\mathrm{D}_\mathfrak{q} = \mathrm{D}_{\mathfrak{q}'}$ for all maximal ideals $\mathfrak{q}, \mathfrak{q}'$ of B lying over $\mathfrak{p}$.

Exercise 2 – For this exercise, we work in the setting of Section VII.3 of the lecture notes:

$$\begin{array}{ccccc}
\mathfrak{q} & \subset & \mathcal{O}_\mathrm{L} & \hookleftarrow & \mathrm{L} \\
\Big| & & \Big| \text{ integral closure} & & \Big| \ \mathrm{Gal(L/K)=G} \\
\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_\mathrm{K} & \subset & \mathcal{O}_\mathrm{K} & \hookleftarrow & \mathrm{K}.
\end{array}$$

Here $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_\mathrm{K}$ and $\mathfrak{q}$ is a prime ideal appearing in the factorisation of $\mathfrak{p}\mathcal{O}_\mathrm{L}$. We assume that $\mathfrak{p}$ does not ramify in L. Recall that there is a Frobenius automorphism $(\mathfrak{q}, \mathrm{L/K}) \in \mathrm{Gal(L/K)}$.

Let F/K be a subextension of L/K. Let $\mathfrak{p}'$ be the maximal ideal $\mathfrak{q} \cap \mathcal{O}_\mathrm{F}$ of $\mathcal{O}_\mathrm{F}$.

2.1. Let $d := [\mathcal{O}_\mathrm{F}/\mathfrak{p}' : \mathcal{O}_\mathrm{K}/\mathfrak{p}]$. Prove that the two elements $(\mathfrak{q}, \mathrm{L/F})$ and $(\mathfrak{q}, \mathrm{L/K})^d$ of Gal(L/K) coincide.

2.2. If F/K is Galois, prove that the restriction $(\mathfrak{q}, \mathrm{L/K})|_\mathrm{F}$ coincides with $(\mathfrak{p}', \mathrm{F/K})$ in Gal(F/K).

Exercise 3 (The quadratic reciprocity law) – Let q be an odd prime number. We let $\mathrm{L} := \mathbb{Q}(\zeta_q)$ denote the q-th cyclotomic field. Recall that $\mathrm{L}/\mathbb{Q}$ is an abelian extension of degree $\varphi(q) = q - 1$, whose Galois group $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ is isomorphic to $\mathbb{F}_q^\times$.

3.1. Prove that the only prime number which ramifies in $\mathrm{L}/\mathbb{Q}$ is q.

3.2. Show that G has a unique subgroup H of index 2, and that H corresponds to the subgroup of squares in $\mathbb{F}_q^\times$ in the isomorphism $\mathrm{G} \simeq \mathbb{F}_q^\times$.

3.3. Deduce that L has a unique subfield K with $[\mathrm{K} : \mathbb{Q}] = 2$.

3.4. Prove that $\mathrm{K} = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{(q-1)/2}q$. *Hint: which primes can ramify in* $\mathrm{K}/\mathbb{Q}$*?*

We identify $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ with $\{\pm 1\}$ via the unique group morphism $\theta : \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \to \{\pm 1\}$.

Let p be an odd prime which is distinct from q. For any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_\mathrm{L}$ which appears in the decomposition of $p\mathcal{O}_\mathrm{L}$ as a product of prime ideals of $\mathcal{O}_\mathrm{L}$, we let $\sigma_p := (\mathfrak{p}, \mathrm{L}/\mathbb{Q}) \in \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ be the Frobenius automorphism associated to $\mathfrak{p}$.

3.5. Prove that σ_p is well-defined (i.e., that the definition of σ_p does not depend on the choice of $\mathfrak{p}$). Show that the restriction $\sigma_p|_\mathrm{K}$ is $(\mathfrak{p} \cap \mathcal{O}_\mathrm{K}, \mathrm{K}/\mathbb{Q}) \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$.

Recall from Exercise 2 on Sheet #7 the definition of the Legendre symbol $\left(\frac{a}{p}\right) \in \{\pm 1, 0\}$.

3.6. Show that $\sigma_p|_\mathrm{K} = \mathrm{id}$ if and only if p is a square in $\mathbb{F}_q^\times$. Deduce that $\theta(\sigma_p|_\mathrm{K}) = \left(\frac{p}{q}\right)$.

For any maximal ideal π of $\mathcal{O}_\mathrm{K}$ appearing in the decomposition of $p\mathcal{O}_\mathrm{K}$, we let $\tau_p \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ denote the Frobenius automorphism $(\pi, \mathrm{K}/\mathbb{Q}) \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. One easily checks, as in **3.5**, that this definition is independent of π.

3.7. Prove that $\theta(\tau_p) = 1$ if and only if p splits in K, and that $\theta(\tau_p) = -1$ if and only if p is inert.

3.8. Deduce from Exercise 2 on Sheet #7 that $\theta(\tau_p) = \left(\frac{q^*}{p}\right)$.

3.9. Recall why $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

3.10. Conclude the proof of the quadratic reciprocity law: *For all odd prime numbers $p \neq q$, we have*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Exercise 4 (A Fermat–Pell equation) {✎ : 9 points} – The goal of this exercise is to find the smallest solution in positive integers $(x, y) \in \mathbb{N}^2$ of the Diophantine equation

$$x^2 - 509 \cdot y^2 = 1.$$

We work in the quadratic number field $\mathrm{K} = \mathbb{Q}(\sqrt{509})$, and we let $\alpha := (1 + \sqrt{509})/2$. *You may want to use a computer to help with some of the calculations.*

4.1. Compute the discriminant Δ_K and the Minkowski bound $\mathrm{M}_\mathrm{K} = (4/\pi)^{r_2} \cdot n!/n^n \cdot |\Delta_\mathrm{K}|^{1/2}$ for K.

4.2. Describe the splitting of the primes $2, 3, 5, 7, 11$ in K. Deduce a set of generators for $\mathrm{Cl}(\mathcal{O}_\mathrm{K})$. *Hint: you should obtain* 4 *generators.*

4.3. Factor the ideals $(2 - \alpha)$, $(3 - \alpha)$, $(8 + \alpha)$ and $(11 + \alpha)$ as products of prime ideals. Deduce from these factorisations some relations between the generators of $\mathrm{Cl}(\mathcal{O}_\mathrm{K})$.

4.4. Conclude that $\mathrm{Cl}(\mathcal{O}_\mathrm{K})$ is trivial.

4.5. Consider the element $\eta = -5^{-3}(2 - \alpha)(11 + \alpha)^3 \in \mathrm{K}$. With as little computation as possible, prove that η is a unit in $\mathcal{O}_\mathrm{K}$.

4.6. Compute η and $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\eta)$.

4.7. Let $\epsilon_0 = a + b\alpha > 1$ denote the fundamental unit of $\mathcal{O}_\mathrm{K}$, with $a, b \in \mathbb{Z}_{\geqslant 0}$. Prove that $a \geqslant 1$ and that $b \geqslant 4$ (by proving that $b = 0, 1, 2, 3$ would not give rise to a unit $\neq \pm 1$). Deduce that $\epsilon_0 > 4\alpha$.

4.8. Check that η^6 is the smallest power of η which lies in $\mathbb{Z}[\sqrt{509}]$ and has norm 1.

4.9. Prove that $\eta = \epsilon_0$. *Hint: estimate* $\log \eta / \log \epsilon_0$.

4.10. Deduce from the above the smallest pair of integers $(x, y) \in \mathbb{N}^2$ such that $x^2 - 509y^2 = 1$.
