HOMEWORK 1: MATH 223B (GALOIS COHOMOLOGY AND CLASS FIELD THEORY)

1. Exercises

1.1. Review of algebraic number theory.

Exercise 1.1. ***(16 pts)*** *Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal and fix a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying above it $\mathfrak{P}|\mathfrak{p}$ (i.e. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$). Write $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ and $k_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$ for the residue fields, and denote by $L_\mathfrak{P}$ and $K_\mathfrak{p}$ the completions of L and K at $\mathfrak{P}$ and $\mathfrak{p}$ respectively. We recall, since $\mathcal{O}_L$, is Dedekind, we have a unique factorization*

$$\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i} \tag{1.1}$$

into prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ for integers $e_i \geq 1$.

(1) *Define the* decomposition group *of $\mathfrak{P}$ by*

$$D(\mathfrak{P}|\mathfrak{p}) = \{\, \sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P} \,\}.$$

(a) ***(1 pt)*** *Prove that $D(\mathfrak{P}|\mathfrak{p})$ is a subgroup of G.*
(b) ***(1 pt)*** *Show that G acts transitively on the set of primes of L above $\mathfrak{p}$ and that the stabilizer of $\mathfrak{P}$ is $D(\mathfrak{P}|\mathfrak{p})$. Deduce that*

$$g = [G : D(\mathfrak{P}|\mathfrak{p})].$$

(2) ***(2 pts)*** *Show that all the integers e_i in (1.1) are equal to a single integer $e := e(\mathfrak{B}|\mathfrak{p})$. In particular, the decomposition (1.1) becomes*

$$\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e}.$$

Show that there exists a single integer $f = f(\mathfrak{P}/\mathfrak{p})$ such that $[k_{\mathfrak{P}_i} : k_\mathfrak{p}] = f$ for all i. Deduce the fundamental relation

$$[L : K] = e\, f\, g.$$

(3) *Consider the reduction map*

$$\mathrm{red}_\mathfrak{P} : \mathcal{O}_L \longrightarrow k_\mathfrak{P}.$$

(a) ***(1 pt)*** *For $\sigma \in D(\mathfrak{P}|\mathfrak{p})$, show that σ induces a well-defined automorphism $\overline{\sigma}$ of $k_\mathfrak{P}$ by*

$$\overline{\sigma}(\mathrm{red}_\mathfrak{P}(x)) = \mathrm{red}_\mathfrak{P}(\sigma(x)).$$

(b) ***(1 pt)*** *Deduce a group homomorphism*

$$\phi_\mathfrak{P} : D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p}).$$

(c) ***(1 pt)*** *Define the* inertia group *by*

$$I(\mathfrak{P}|\mathfrak{p}) = \ker(\phi_\mathfrak{P}) = \{\, \sigma \in D(\mathfrak{P}|\mathfrak{p}) : \overline{\sigma} = \mathrm{id} \text{ on } k_\mathfrak{P} \,\}.$$

Prove that $I(\mathfrak{P}|\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}|\mathfrak{p})$.

(4) ***(2 pts)*** *Prove that $\phi_{\mathfrak{P}}$ is surjective and that there is a short exact sequence*

$$1 \longrightarrow I(\mathfrak{P}|\mathfrak{p}) \longrightarrow D(\mathfrak{P}|\mathfrak{p}) \xrightarrow{\phi_{\mathfrak{P}}} \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow 1.$$

Deduce in particular that

$$|D(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})\, f(\mathfrak{P}|\mathfrak{p}), \qquad |I(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p}), \qquad |\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})| = f(\mathfrak{P}|\mathfrak{p}).$$

(5) (a) ***(2 pt)*** *Show that the natural embedding $K \hookrightarrow K_{\mathfrak{p}}$ extends to an embedding $L \hookrightarrow L_{\mathfrak{P}}$ and that restriction induces a canonical isomorphism*

$$D(\mathfrak{P}|\mathfrak{p}) \;\cong\; \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

(b) ***(2 pt)*** *Under this identification, interpret $I(\mathfrak{P}|\mathfrak{p})$ as the subgroup of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ acting trivially on the residue field $k_{\mathfrak{P}}$.*

(6) *Assume $\mathfrak{p}$ is unramified in L, i.e. $e(\mathfrak{P}|\mathfrak{p}) = 1$. Then $I(\mathfrak{P}|\mathfrak{p}) = 1$ and $\phi_{\mathfrak{P}}$ is an isomorphism. Let $\mathrm{Frob}_{\mathfrak{p}} \in D(\mathfrak{P}|\mathfrak{p})$ be the unique element whose image in $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is the $|k_{\mathfrak{p}}|$-power map.*

(a) ***(1 pt)*** *Show that $\mathrm{Frob}_{\mathfrak{p}}$ is characterized by*

$$\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \textit{for all } x \in \mathcal{O}_L.$$

(b) ***(1 pt)*** *Show that if $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$, then*

$$\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}') = \tau\, \mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P})\, \tau^{-1}.$$

In particular, the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G is independent of the choice of $\mathfrak{P}|\mathfrak{p}$.

(c) ***(1 pt)*** *If L/K is abelian i.e $\mathrm{Gal}(L/K)$ is abelian, deduce that the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in G$ (for $\mathfrak{p}$ unramified) is independent of the choice of $\mathfrak{P}|\mathfrak{p}$ as an* element *of G (not just up to conjugacy).*

Exercise 1.2 (10 pts). *Let $q \neq p$ be odd primes and set $K = \mathbb{Q}(\zeta_q)$, for ζ_q a non-trivial qth root of unity.*

(1) ***(1 pt)*** *Show that*

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

(2) ***(3 pts)*** *Set $H \subset (\mathbb{Z}/q\mathbb{Z})^\times$ be the subgroup of squares, and let $K^+ = K^H$ denote the fixed field. Prove that*

$$K^+ = \mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}} q}\right).$$

(Hint: *Compare discriminants.)*

(3) ***(2 pts)*** *Show that p splits completely in K^+ if and only if the image of Frob_p lies in H.*

(4) ***(3 pts)*** *Deduce that*

$$\left(\frac{q}{p}\right) = 1 \quad \Longleftrightarrow \quad p \textit{ splits in } \mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}} q}\right).$$

(5) ***(1 pt)*** *Use (1) and (3), to show that*

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

1.2. **Some group theory.**

Exercise 1.3 (**11 pts**). *If M is an abelian group then we define its Potryagin dual to be $M^* := \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$.*

(1) ***(2 pts)*** *Construct isomorphisms of the form*
$$(\mathbb{Z}/n\mathbb{Z})^\vee \simeq \mathbb{Z}/n\mathbb{Z}$$
$$(\mathbb{Q}_p/\mathbb{Z}_p)^\vee \simeq \mathbb{Z}_p,$$
for p a prime number and $n \geq 1$ an integer. Show that
$$\mathbb{Q}^\vee \simeq 0.$$

(2) ***(3 pts)*** *Suppose that M is a torsion abelian group endowed with the discrete topology. Endow M^* with topology given by pointwise convergence (I.e consider the embedding $M \hookrightarrow M^{\mathbb{Q}/\mathbb{Z}}$, where $M^{\mathbb{Q}/\mathbb{Z}}$ is given the product topology and give M the subspace topology). Prove that M^* is a commutative profinite group (Hint: write M^* as a directed limit or union of its finite subgroups).*

(3) ***(2 pts)*** *For M a torsion abelian group check that the natural evaluation map*
$$\mathrm{ev}_M : M \to (M^*)^*$$
$$m \mapsto (\chi \mapsto \chi(m))$$
is an isomorphism of abelian groups. We let let **TorAb** *be the category of* discrete torsion *abelian groups. Let* **ProFinAb** *be the category of* profinite *(equivalently: compact, Hausdorff, totally disconnected topological) abelian groups (with morphisms being continuous homomorphisms). The above duality upgrades to a contravariant equivalence*
$$\mathbf{TorAb}^{\mathrm{op}} \simeq \mathbf{ProFinAb}.$$
of categories. This is known as Pontryagin duality.

(4) ***(2 pts)*** *Prove that Pontryagin dual of a torsion-free profinite abelian group is a divisible abelian group.*

(5) ***(2 pts)*** *Combine (1), (4), and Exercise 1.4 below, to deduce that any commutative torsion free profinite group is isomorphic to a (possibly-infinite) product of copies of $\mathbb{Z}_p$ for some prime numbers p.*

Exercise 1.4 (**12 pts**). *Let A be a divisible abelian group, i.e. for every $a \in A$ and every integer $n \geq 1$ there exists $b \in A$ with $nb = a$.*

(1) ***(2 pts)*** *Show that a finite divisible abelian group is trivial.*

(2) ***(2 pts)*** *Show that A a divisble abelian group is a $\mathbb{Q}$-vector space if and only if it is torsion-free.*

(3) ***(1 pt)*** *Let*
$$A_{\mathrm{tors}} := \{a \in A \mid \exists n \geq 1 \text{ with } na = 0\}.$$
Show that A_{tors} is a divisible subgroup of A.

(4) ***(1 pt)*** *Prove that A_{tors} decomposes canonically as a direct sum of its p-primary components*
$$A_{\mathrm{tors}} = \bigoplus_p A[p^\infty], \qquad A[p^\infty] := \{a \in A \mid \exists n \text{ with } p^n a = 0\}.$$

(5) ***(1 pt)*** *Fix a prime p. Show that every divisible p-primary (in the sense that for every element a there exists $n \geq 0$ such that $p^n a = 0$) abelian group D contains a nonzero element of order p^n for all $n \geq 1$ unless $D = 0$.*

(6) ***(2 pts)*** *Prove that any divisible p-primary abelian group is a direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$.*

(7) ***(1 pt)*** *Show that there exists a (non-canonical) decomposition*
$$A \cong A_{\mathrm{tors}} \oplus A/A_{\mathrm{tors}}.$$

(8) ***(1 pt)*** *Show that A/A_{tors} is torsion-free and divisible, hence a $\mathbb{Q}$-vector space by (3).*

(9) ***(2 pts)*** *Deduce that there exist cardinals κ and $\{\lambda_p\}_p$ such that*

$$A \;\cong\; \mathbb{Q}^{(\kappa)} \;\oplus\; \bigoplus_p \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{(\lambda_p)},$$

where p varies over all prime numbers.

(Hint: Use that divisible abelian groups are injective objects in the category of abelian groups, so short exact sequences with divisible terms split. For the p-primary case, reduce to showing that a nonzero divisible p-group contains a copy of $\mathbb{Q}_p/\mathbb{Z}_p$ and then use Zorn's lemma to obtain a maximal direct sum of such copies.)