18.786 PROBLEM SET 3

(1) Construct (with proofs) an abelian extension E/F of number fields such that E does not embed into any cyclotomic extension of F, i.e., there does not exist an integer n such that E embeds into $F(\zeta_n)$.

(2) Let $K \neq \mathbb{C}$ be a local field of characteristic $\neq 2$. For $a, b \in K^\times$, $H_{a,b}$ denotes the corresponding Hamiltonian algebra over K. You can assume all good properties of Hilbert symbols in this problem (since we have not proved them yet for residue characteristic 2 and $K \neq \mathbb{Q}_2$).
   (a) Show that $H_{a,b} \simeq H_{a,c}$ if and only if $b = c \in K^\times/N(K[\sqrt{a}]^\times)$.
   (b) Show that the isomorphism class of $H_{a,b}$ depends only on the Hilbert symbol (a, b).
   (c) Give another proof of (a slight extension of) that exercise from last week: every $x \in K$ admits a square root in $H_{a,b}$ for all pairs $a, b \in K^\times$.
   (d) Show that any noncommutative 4-dimensional division algebra H over K is a Hamiltonian algebra. Deduce that there is a unique 4-dimensional division algebra over K.

(3) In this problem, we will examine how far the tame symbol (defined in the first problem set) can take us in local class field theory.
   (a) Let $n > 1$ be an integer and let K be a field of characteristic prime to n. Let $\mu_n \subseteq K^\times$ denote the subgroup of nth roots of unity. Suppose that $|\mu_n| = n$, i.e., K admits a primitive nth root of unity.[1].

   Construct a canonical isomorphism:

$$\mathrm{Hom}(\mathrm{Gal}(K), \mu_n) \simeq K^\times/(K^\times)^n$$

   where Hom indicates the abelian group of continuous morphisms.[2]
   (b) Now suppose that K is a nonarchimedean local field. Let q denote the order of the residue field $k = \mathcal{O}_K/\mathfrak{p}$ of K. Suppose that n divides $q - 1$ (e.g., $n = 2$ and q is odd) for the remainder of this problem.

   Show that every element of μ_n lies in the ring of integers of K. Show that the mod $\mathfrak{p}$ reduction map:

Updated: February 25, 2016.

[1]I.e., suppose that there exists an isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$, but we do not fix such an isomorphism at the onset. In what follows, *canonical* means that you should not choose an isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ in making your constructions (though you are welcome to use it in the course of proving claims about your constructions)

[2]A small hint: first identify the left hand side with the set of Galois extensions L/K equipped with an embedding $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$ (up to isomorphism).

$$\mu_n \to \{x \in k^\times \mid x^n = 1\}$$

is an isomorphism. Deduce that $|\mu_n| = n$.

(c) Construct a canonical isomorphism between $k^\times/(k^\times)^n$ and μ_n.

(d) Show that the composition:

$$K^\times \times K^\times \xrightarrow{\text{tame symbol}} k^\times \to k^\times/(k^\times)^n \simeq \mu_n$$

induces a bimultiplicative pairing:

$$K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mu_n$$

that is non-degenerate in the sense that the induced map:

$$K^\times/(K^\times)^n \to \mathrm{Hom}(K^\times, \mu_n)$$

is an isomorphism.

(4) (a) Let L/K be an unramified extension of local fields of degree n. Show that $K^\times/N(L^\times)$ is cyclic of order n.

(b) Let L/K be a totally ramified extension of degree n. Assume n divides $q-1$, with q the order of the residue field of K (which is also the residue field of L).

Show that the canonical map:

$$\mathcal{O}_K^\times/N(\mathcal{O}_L^\times) \to K^\times/N(L^\times)$$

is an isomorphism. Show that the reduction map:

$$\mathcal{O}_K^\times/N(\mathcal{O}_L^\times) \to k^\times/(k^\times)^n$$

is well-defined and an isomorphism. Deduce that $K^\times/N(L^\times)$ canonically isomorphic to μ_n.

(c) Briefly, what is the relationship between this problem and the previous one?

(5) In the next exercise (which is long but locally easy), assume any standard results you like from Galois theory. The point is to get a bit more comfortable with the profinite Galois group.

Let G be a finite group and K a field. A *G-torsor* over[3] K is a commutative K-algebra L with an action of G by K-automorphisms, such that the canonical map:

$$L \underset{K}{\otimes} L \to \prod_{g \in G} L$$

$$a \otimes b \mapsto ((g \cdot a) \cdot b)_{g \in G}$$

is an isomorphism of K-algebras. Here in the formula on the right, we are giving the coordinates of the result of applying our function, and $g \cdot a$ means we act on $a \in L$ by $g \in G$, while the second $\cdot$ is multiplication in the algebra L.

(a) Show that any G-torsor L is étale as a K-algebra.

[3] In algebraic geometry, we would rather say *over* $\mathrm{Spec}(K)$.

(b) Show that $L = \prod_{g\in G} K$ is a G-torsor over K, where the G-action permutes the coordinates. This G-torsor is called the *trivial* G-torsor.

(c) If L is Galois extension of K (in particular, L is a field) with Galois group G, show that L is a G-torsor over K.

(d) We now fix a separable closure K^{sep} of K. Let us say a *rigidification* of a G-torsor L as above is the datum of a map $i : L \to K^{sep}$ of K-algebras. Show that every G-torsor L admits a rigidification.

(e) Note that G acts on the set of rigidifications of L through its action on L. Show that this action is simple and transitive.

(f) Given a rigidified G-torsor $i : L \to K^{sep}$, show that the only automorphism φ of L as a K-algebra that commutes with both the G-action and with i (i.e., $i(\varphi(a)) = i(a)$ for all $a \in L$) is the identity.

(g) Let $\mathrm{Gal}(K) := \mathrm{Aut}_{K-\mathsf{alg}}(K^{sep})$ be the absolute Galois group of K, considered as a profinite group.

Show that the set of continuous homomorphisms $\chi : \mathrm{Gal}(K) \to G$ are in canonical bijection with the set of isomorphism classes of rigidified G-torsors over K.

As a hint, here is one direction in the construction: given χ, we take L to be the subalgebra of $\prod_{g\in G} K^{sep}$ consisting of elements of the form $(a_g)_{g\in G}$ such that for every $\gamma \in \mathrm{Gal}(K)$, $\gamma \cdot a_g = a_{\chi(\gamma)\cdot g}$ (here $\gamma \cdot a_g$ indicates the action of $\mathrm{Gal}(K)$ on K^{sep}), and the rigidification to be projection onto the coordinate corresponding to $1 \in G$.

(h) For a continuous homomorphism $\chi : \mathrm{Gal}(K) \to G$, show that the resulting K-algebra L is a field if and only if χ is surjective, and in this case, is the Galois subfield of K^{sep} with Galois group G corresponding (under infinite Galois theory) to this quotient G of $\mathrm{Gal}(K)$.

(i) Show that the trivial homomorphism $\chi : \mathrm{Gal}(K) \to G$ corresponds to the G-torsor $\prod_{g\in G} K$ with rigidification induced by the projection onto the coordinate for $1 \in G$.

(j) (Not for credit.) If you know the fundamental group $\pi_1(X, x)$ of a (sufficiently nice) topological space X, then formulate a notion of G-torsor over X and show that if X is connected, a G-torsor with a lift of the basepoint is the same as a homomorphism $\pi_1(X, x) \to G$.

(k) (Not for credit.) Invent the étale fundamental group for schemes. Formulate all the main results of Grothendieck's SGA I. Bonus non-credit for proving all those results.

18.786 Number Theory II: Class Field Theory
Spring 2016