Problems for Math 6370, Fall 2016

As always, if a problem or hint is incorrectly stated, the problem becomes to formulate it correctly, and then solve the corrected version.

1. Basics of local fields

(1) For what primes p does $x^2 - 7$ have a root in $\mathbb{Q}_p$?

(2) Let A be a Dedekind domain with fraction field K, and let B be the integral closure of A in a finite separable extension L/K. Recall that (for any finite separable extension of fields) the trace form $\mathrm{tr}\colon L \times L \to K$ is non-degenerate. In our setting, integrality properties of this duality are one way to measure ramification of the extension. We define the *inverse different* by

$$\mathcal{D}_{B/A}^{-1} = \{\alpha \in L : \mathrm{tr}(\alpha B) \subset A\}.$$

Check that this is a fractional ideal of L containing B. The *different* $\mathcal{D}_{B/A}$ (often written as $\mathcal{D}_{L/K}$) is then defined to be its inverse, which is therefore an integral ideal of B.

(a) Show that if $B = A[\beta]$, then $\mathcal{D}_{B/A} = (f'(\beta))$ where $f(X) \in A[X]$ is the minimal polynomial of β. (Hint: let $\beta_1, \ldots, \beta_n$ be the conjugates of β in $\overline{L}$. Show that

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(\beta_k)(X - \beta_k)} = \sum_{i=1}^{\infty} X^{-i} \,\mathrm{tr}_{L/K}\left(\frac{\beta^{i-1}}{f'(\beta)}\right).$$

Deduce that $\mathrm{tr}_{L/K}(\frac{\beta^{i-1}}{f'(\beta)})$ is zero for $i = 1, \ldots, n-1$, is 1 for $i = n$, and is integral for all i. Conclude that $\left\{\frac{\beta^i}{f'(\beta)}\right\}_{i=0,\ldots,n-1}$ is an $\mathcal{O}_K$-basis of $\mathcal{D}_{L/K}^{-1}$.)

(b) Show that $\mathcal{D}_{L/K} = \prod_w \mathcal{D}_{L_w/K_v}$, where the product is taken over the (equivalence classes) of discrete valuations (or, if you prefer, prime ideals) w of L.

(c) In light of the previous part, we turn to a purely local analysis. Let L/K be a finite Galois extension of local fields, with rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. Assume the extension of residue fields is separable. Let v_L be the *normalized* valuation on L (that is, $v_L\colon L \twoheadrightarrow \mathbb{Z} \cup \infty$). Recall the lower ramification groups $G(L/K)_i$. Show that

$$v_L(\mathcal{D}_{L/K}) = \sum_{i=1}^{\infty} (\#G(L/K)_i - 1).$$

(Hint: we showed in class that the hypothesis of part (a) always applies.) In particular, $\mathcal{D}_{L/K} = \mathcal{O}_L$ if and only if L/K is unramified.

(3) Let ζ be a primitive p^n root of unity, and let $K = \mathbb{Q}_p(\zeta)$. Recall that the mod p^n cyclotomic character gives an injection $\kappa\colon G(K/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$, characterized by $\sigma(\zeta) = \zeta^{\kappa(\sigma)}$.

(a) Show that for all $i \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, $\frac{1-\zeta^i}{1-\zeta}$ is a *unit* in $\mathcal{O}_K$. Conclude that $v_K(p) = p^{n-1}(p-1)v_K(1-\zeta)$ (hint: evaluate the p^n cyclotomic polynomial at 1).

(b) Deduce that κ is in fact an isomorphism, and that $1 - \zeta$ is a uniformizer of $\mathcal{O}_K$.

(c) Compute the lower ramification groups $G(K/\mathbb{Q}_p)_i$. (Hint: the previous part implies $\mathcal{O}_K = \mathbb{Z}_p[\zeta]$.) Compute the different $\mathcal{D}_{K/\mathbb{Q}_p}$.

(4) Let $K = \mathbb{Q}_2[\sqrt{-1}, \sqrt{2}]$. Find a uniformizer for K, and compute the lower ramification groups and different of $K/\mathbb{Q}_2$.

(5) Let (K, v) be a complete discretely valued non-archimedean field (normalize so that $v(K \setminus 0)) = \mathbb{Z}$). Recall that a polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ is Eisenstein if $v(a_i) > 0$ for all i, and $v(a_0) = 1$.

(a) Let $f(X)$ be Eisenstein. Show that $f(X)$ is irreducible, and that $K[X]/(f(X))$ is a totally ramified extension of K.

(b) Conversely, show that every totally ramified extension (of finite degree) of K is obtained by adjoining the root of an Eisenstein polynomial.

(6) (Krasner's Lemma) Let (K, v) be a complete discretely valued field. Assume all polynomials and field extensions that show up in this exercise are separable (eg, you could take K to have characteristic zero).

(a) Let L/K be a finite Galois extension containing elements α and β. If

$$v(\alpha - \sigma(\alpha)) < v(\beta - \alpha)$$

for all $\sigma \in G(L/K) \setminus G(L/K(\alpha))$, show that $\alpha \in K(\beta)$. (The hypothesis says: "β is closer to α than α is to any of its conjugates.")

(b) Define a valuation on $K[X]$ by $v(\sum a_n X^n) = \min(v(a_n))$. Fix a degree d irreducible monic polynomial $f(X)$. Show that there is a constant c such that for any other degree d monic polynomial g, $v(f - g) > c$ implies that g is also irreducible, and $K[X]/(g) \cong K[X]/(f)$.

(c) Let K be a non-archimedean local field of characteristic zero. Show that in a fixed algebraic closure $\overline{K}$ of K, there are only finitely many extensions of bounded degree. (Hint: reduce to the case of totally ramified extensions; then use the previous exercise, showing that all totally ramified extensions come from adjoining roots of Eisenstein polynomials; finiteness follows from a compactness argument and Krasner's Lemma.) Remind yourself that the conclusion of this exercise is false for global fields!

(7) Classify quadratic extensions of $\mathbb{Q}_p$, for all primes p.

2. Basics of global fields

(1) Let K be a number field. Refine the weak approximation theorem as follows: if S is a finite set of finite places of K, if $\alpha_v \in K_v$ is given for all $v \in S$, and if $\varepsilon > 0$, then there exists an $\alpha \in K$ such that $|\alpha - \alpha_v|_v < \varepsilon$ for all $v \in S$ and $|\alpha|_v \leq 1$ for all finite places $v \notin S$ (i.e., α can be chosen to be integral away from S).

(2) Let K be a number field, and equip $\mathbb{A}_K$ and $\mathbb{A}_K^\times$ with their restricted direct product topologies.

(a) Show that the topology on $\mathbb{A}_K^\times$ is not the subspace topology for the inclusion $\mathbb{A}_K^\times \subset \prod_v K_v^\times$ (the latter with the usual direct product topology).

(b) Show that the topology on $\mathbb{A}_K^\times$ is not the subspace topology for the inclusion $\mathbb{A}_K^\times \subset \mathbb{A}_K$.

(c) Show that the topology on $\mathbb{A}_K^\times$ is the natural colimit topology on $\bigcup_S \mathbb{A}_K^{\times S}$ (i.e., a set in the union is open if and only if its intersection with each $\mathbb{A}_K^{\times S}$ is open).

(d) Show that the topology on $\mathbb{A}_K^\times$ is the subspace topology for the inclusion $\mathbb{A}_K^\times \xrightarrow{x \mapsto (x, x^{-1})} \mathbb{A}_K \times \mathbb{A}_K$.

(3) Let K be a number field, and set $n = [K : \mathbb{Q}]$. Recall the Minkowski bound: for every element of the class group of K, there is a representative ideal I whose norm satisfies

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s D_K^{1/2},$$

where s is the number of complex places of K, and D_K is the (absolute) discriminant of K.

(a) Compute the class groups of $K = \mathbb{Q}(\sqrt{-5})$ and $L = \mathbb{Q}(\sqrt{-31})$.

(b) Show that $K(\sqrt{-1})$ and $L(\alpha)$, where α satisfies $\alpha^3 + \alpha + 1 = 0$, are everywhere unramified extensions of K and L, respectively (hint for L: what is the discriminant of a cubic polynomial?). They are in fact the maximal abelian unramified extensions, and it is part of class field theory (the theory of the Hilbert class field) that the Galois groups of these extensions are isomorphic to the respective class groups.

(4) Let K be a number field. Show there exists a finite extension L/K such that all ideals of K become principal in L. (Hint: for every ideal I of K, I^{h_K} is principal.) This is a soft statement; again, the theory of the Hilbert class field will yield something sharper.

(5) A number field K is said to be *totally real* if all of its archimedean places are real, i.e. all embeddings $K \hookrightarrow \mathbb{C}$ actually land in $\mathbb{R}$. A number field is said to be *CM* ("complex multiplication") if it is a totally imaginary quadratic extension of a totally real field.
   (a) Show that the CM number fields are precisely the totally imaginary number fields on which complex conjugation is well-defined, i.e. complex conjugation on $\mathbb{C}$ induces an automorphism of K for each choice of embedding $K \hookrightarrow \mathbb{C}$, and this automorphism is independent of the choice of embedding.
   (b) Give an example of a number field that is neither CM nor totally real.
   (c) Let K/F be a quadratic CM extension of a totally real field F. Show that $O_K^\times$ and $O_F^\times$ have the same rank. Show that the index $[O_K^\times : \mu_\infty(K)O_F^\times]$ is either 1 or 2. (Hint: $\varepsilon \mapsto \varepsilon/\bar{\varepsilon}$ defines a homomorphism $O_K^\times \to \mu_\infty(K)$; show this induces an inclusion $O_K^\times/(\mu_\infty(K)O_F^\times) \hookrightarrow \mu_\infty(K)/\mu_\infty(K)^2$.)

(6) Let $K/\mathbb{Q}$ be a finite Galois extension, and let $\sigma_0, \dots, \sigma_r$ be a set of representatives of embeddings $K \hookrightarrow \mathbb{C}$ modulo complex conjugation. Use the following outline to show that there exists a unit ε of O_K such that the conjugates $\{\sigma_i(\varepsilon)\}_{i=1,\dots,r}$ generate a finite-index subgroup of $O_K^\times$ (such an ε is called a Minkowski unit).
   (a) Assume for the time being that we can construct a unity ε such that $|\sigma_0(\varepsilon)| > 1$ but $|\sigma_i(\varepsilon)| < 1$ for all $i > 0$. Regard K as a subfield of $\mathbb{C}$ via σ_0, so we can think of the σ_i as elements of $\mathrm{Gal}(K/\mathbb{Q})$. It suffices to show the regulator of $\sigma_1(\varepsilon), \dots, \sigma_r(\varepsilon)$ is non-zero (recall that the regulator of $t_1, \dots, t_r$ is $|\det(\log|\sigma_i(t_j)|)|$). The matrix $(a_{ij})_{i,j=1,\dots,r}$ with entries $a_{ij} = \log|\sigma_i^{-1}\sigma_j(\varepsilon)|$ then has $a_{ii} > 0$, $a_{ij} \le 0$ for all $i \ne j$, and $\sum_i a_{ij} > 0$ for all j. Conclude by showing that any real matrix satisfying these three properties has non-zero determinant.
   (b) Now we show that a unit ε as in the last part exists. Recall that the unit theorem shows that injective homomorphism $O_K^\times/\mu_\infty(K) \to \mathbb{R}^r$ given by
   $$\log(x) = (\log|\sigma_i(x)|)_{i=1,\dots,r}$$
   has image equal to a lattice (of rank r) in $\mathbb{R}^r$. As such, the image must intersect the "quadrant" (2^r-ant?) where all coordinates are negative. Take such an ε in this image. By construction, $\log|\sigma_i(\varepsilon)| < 0$ for $i = 1, \dots, r$; and then necessarily $\log|\sigma_0(\varepsilon)| > 0$.

3. Group and Galois cohomology

All modules for a profinite group are implicitly discrete, unless otherwise specified.

(1) (Cohomology of pro-cyclic groups) Let $G = \widehat{\mathbb{Z}}$ (the profinite completion of $\mathbb{Z}$), and let F be a (topological) generator of G. Show that for any torsion G-module M, $H^1(G, M) \cong M/(F-1)M$. Show that $H^i(G, M) = 0$ for $i \ge 2$. (We will use this result frequently, as the case $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ will often show up for us.)

(2) Recall that H^0 and H^1 admit concrete group-theoretic interpretations. In this important exercise, we show that H^2 does as well. Let G be a profinite group, and let M be a (for simplicity) finite G-module. Consider the set of extensions (of profinite groups)
   $$1 \to M \to E \to G \to 1,$$
   where M is a normal subgroup of E such that the given G-action on M agrees with the G-action induced by E-conjugation (i.e., lift $g \in G$ to E and allow it to act on M by conjugation–this action is well-defined since M is abelian). Regard two extensions E and E' as equivalent if there is an isomorphism $E \xrightarrow{\sim} E'$ inducing the identity on M and G. Denote by $\mathrm{Ext}(G, M)$ the set of such equivalence classes.
   (a) Show that there is a natural isomorphism $\mathrm{Ext}(G, M) \cong H^2(G, M)$. Hint: given $\phi \in Z^2(G, M)$, let $E = M \times G$ as a set, and endow it with the group law $(m, g)\cdot(m', g') = (m + g(m') + \phi(g, g'), gg')$.

Conversely, given an extension, fix a continuous section (not a group homomorphism) of $E \to G$ (we showed existence in class), and use it to reverse the previous step.

(b) Verify that the trivial element of $H^2(G, M)$ corresponds to the semi-direct product $M \rtimes G$.

(c) Supposed we have an extension E corresponding to a cohomology class ϕ_E. If $f\colon H \to G$ is a homomorphism of profinite groups, show that f lifts to E if and only if $f^*(\phi_E) = 0$.

(d) Classically, the cohomology group $H^2(G, \mathbb{C}^\times)$ is known as the Schur multiplier. Explain the connection between the Schur multiplier and obstructions to lifting projective representations $G \to \mathrm{PGL}_n(\mathbb{C})$ to honest representations $G \to \mathrm{GL}_n(\mathbb{C})$. (Note: $H^2(G, \mathbb{C}^\times) = H^2(G, \mu_\infty(\mathbb{C})) \cong \varinjlim_n H^2(G, \frac{1}{n}\mathbb{Z}/\mathbb{Z})$.)

(e) Exhibit a finite group with a non-trivial Schur multiplier and a corresponding projective representation that does not lift to an honest representation.

(3) Compute $H^2(\mathbb{Z}/p, \mathbb{Z}/p)$ for any prime p. Reconcile this calculation with the previous exercise and your knowledge of groups of order p^2. Do the same for $H^2(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$ and groups of order p^3. For the latter, you may assume the Künneth formula (see exercise 5).

(4) (An alternative description of group cohomology)

(a) Let $\mathcal{A}$ be an abelian category. For any object M of $\mathcal{A}$, the (covariant) functor $\mathrm{Hom}(M, \bullet)$ is left-exact. If $\mathcal{A}$ has enough injectives, this lets us define the derived functors $\mathrm{Ext}^i(M, \bullet)$. Similarly, for any $N \in \mathcal{A}$, $\mathrm{Hom}(\bullet, N)$ is a (contravariant) left-exact functor, and if $\mathcal{A}$ has enough projectives, we can define its derived functors $\mathrm{Ext}^i(\bullet, N)$. Assume $\mathcal{A}$ does have enough injectives and projectives, and check that the two resulting definitions of $\mathrm{Ext}^i(M, N)$ agree.

(b) If G is profinite, and M is a discrete G-module, then $M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$, so $H^i(G, M) = \mathrm{Ext}^i_G(\mathbb{Z}, M)$ (the Ext is taken in the category of discrete G-modules).

(c) If G is finite (or more generally, discrete), then the category of $\mathbb{Z}[G]$-modules has enough projectives, so we can also define $H^i(G, M)$ as the i^{th} cohomology group of the complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, M)$, where $P_\bullet$ is any projective resolution of $\mathbb{Z}$.

(5) (Another description of group cohomology) Let G be a discrete group, and let M be a $\mathbb{Z}[G]$-module. One can also define $H^i(G, M) = H^i(BG, \mathcal{M})$, where BG is a $K(G, 1)$, and in the second group M is regarded as the local system on BG associated to the $G = \pi_1(BG, *)$-module M. (Note: there are a few ways to define cohomology with coefficients in a local system: one can take sheaf cohomology in the usual sense, or, better for purposes of this exercise, the following. Let X be a reasonable topological space with fundamental group Π. Let $\Pi \to \mathrm{Aut}(M)$ be a local system on X, and let $X' \to X$ be a Galois covering space trivializing M, with $\Pi' \trianglelefteq \Pi$. Then the homologies of the complexes $C_\bullet(X') \otimes_{\mathbb{Z}[\Pi/\Pi']} M$ and $\mathrm{Hom}_{\mathbb{Z}[\Pi/\Pi']}(C_\bullet(X'), M)$ give the homology and cohomology groups of X with coefficients in M. Here we write $C_\bullet$ for singular chains.) This exercise elaborates on this connection.

(a) Let $EG \to BG$ be the universal cover of BG. The singular chain complex $C_\bullet(EG)$ (with integer coefficients) is a free ($\mathbb{Z}[G]$-module) resolution of $\mathbb{Z}$.

(b) The cohomology of $\mathrm{Hom}_G(C_\bullet(EG), M)$ computes both $H^i(G, M)$ and $H^i(BG, M)$.

(c) Realizing EG as a simplicial complex with one n-simplex $[g_0, \ldots, g_n]$ for each tuple $(g_0, \ldots, g_n) \in G^{n+1}$ and G-action carrying $[g_0, \ldots, g_n]$ isomorphically to $[gg_0, \ldots, gg_n]$ (see Hatcher I.B.7), $H^i(BG, M)$ is also the cohomology of $\mathrm{Hom}_G(C^\Delta_\bullet(EG), M)$, $C^\Delta_\bullet$ denoting the simplicial chain complex; we recover (and provide the best conceptual explanation for) the description of $H^\bullet(G, M)$ as the cohomology of the cochain complex whose degree n term is the inhomogeneous cochains $G^n \to M$, with the funny (but now explained) boundary map given in class.

(d) Now many of the constructions we carried out in class can be explained in terms of algebraic topology: construct restriction, corestriction, and inflation maps from this perspective. Construct the "Hochschild-Serre" spectral sequence of group cohomology from the Serre spectral sequence of the fibration $BG \to B(G/H)$.

(6) Let G be a profinite group, and let H be an open subgroup of G. Fix a section $t\colon H\backslash G \to G$. Define a map $V\colon G \to H^{\mathrm{ab}}$ (the abelianization of H) by

$$V(g) = \prod_{H\backslash G \ni x} t(x)gt(xg)^{-1}.$$

(a) Show V is independent of the choice of section t.
(b) Show that V is a group homomorphism, and therefore factors $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. This is called the *transfer* ("V" is for *Verlagerungen*).
(c) Show that $(G^{\mathrm{ab}})^\vee \cong H^2(G, \mathbb{Z})$.
(d) Via the above isomorphism, the transfer identifies to the dual of the corestriction map

$$\mathrm{cor}\colon H^2(H, \mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

(Hint: we gave an alternative description of corestriction as the composite

$$H^i(H, M) \xrightarrow{\sim} H^i(G, \mathrm{Ind}_H^G M) \xrightarrow{\mathrm{tr}} H^i(G, M).)$$

(7) (See Serre, *Topics in Galois Theory*) A natural question in (inverse) Galois theory is, given a field K, a surjection of (finite) groups $G \to H$, and a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong H$, does there exist a Galois extension $M/L/K$ such that the surjection $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ can be identified with $G \to H$? This is known as the embedding problem. This exercise will show how even the simplest cases of the embedding problem depend on subtle arithmetic properties of the field K. Assume $\mathrm{char}(K) \neq 2$, and let $K(\sqrt{\alpha})$ be a quadratic extension of K ($\alpha \in K$). We will show that $K(\sqrt{\alpha})$ can be embedded in a cyclic degree four extension L/K if and only if α is a sum of two squares in K.
(a) Let G be a (finite) group equipped with a surjection $\epsilon\colon G \to \mathbb{Z}/2$. Let $H = \ker(\epsilon)$, and suppose we are also given a homomorphism $\chi\colon H \to \mathbb{Z}/2$, with kernel H_χ. Show that the following are equivalent: (a) H_χ is normal in G, and G/H_χ is cyclic of order 4; (b) $\mathrm{cor}(\chi) = \epsilon$. (Use that corestriction is the dual of the transfer, which can be computed explicitly.)
(b) Let $L = K(\sqrt{\alpha}, \sqrt{a + b\sqrt{\alpha}})$ for some $a, b \in K$. Use the previous part to show that L/K is cyclic of degree 4 if and only if $a^2 - \alpha b^2 = \alpha c^2$ for some $c \in K^\times$.
(c) If $a^2 - \alpha b^2 = \alpha c^2$ and $b^2 + c^2 \neq 0$, observe that

$$\alpha = \left(\frac{ab}{b^2 + c^2}\right)^2 + \left(\frac{ac}{b^2 + c^2}\right)^2.$$

Use this (and a similar algebraic manipulation for the converse) to finish the problem.

4. Local Class Field Theory

(1) Let K be a finite extension of $\mathbb{Q}_p$. What is the maximal abelian tamely ramified extension of K (give generators for the field)? What is the maximal abelian totally tamely ramified extension of K? What norm subgroup does this correspond to under the correspondence of local class field theory?
(2) Let K be a finite extension of $\mathbb{Q}_p$. Assume that K contains a primitive n^{th} root of 1. Define the Hilbert symbol

$$(\cdot,\cdot)_n\colon K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

by $(a, b)_n = \mathrm{inv}_K(\delta(a) \cup \delta(b))$, where δ is the Kummer theory boundary map, and, to be precise, by inv_K here we mean the isomorphism $H^2(G_K, \mu_n \otimes \mu_n) \xrightarrow{\sim} \mu_n$ induced by the usual invariant map. (An aside: note that $(\cdot,\cdot)_n$ factors through Milnor K-theory.)
(a) Show $(a, b)_n = 1$ if and only if b is a norm from $K[\sqrt[n]{a}]$.
(b) Show that the Hilbert symbol can be computed in terms of the reciprocity map r_K via

$$r_K(b)(a^{1/n}) = (a, b)_n a^{1/n}.$$

(c) Take $n = \#\mu_\infty(K)$, and assume that n is coprime to the residue characteristic p of K. This assumption implies that reduction to the residue field k gives an isomorphism $\mu_n(K) \xrightarrow{\sim} \mu_n(k)$ (in contrast, note, eg, that if $K = \mathbb{Q}_p(\zeta_p)$, then $\zeta_p = 1 + (\zeta_p - 1)$ is in the kernel of reduction). Show that

$$(a, b)_n = (-1)^{v(a)v(b)} \frac{b^{v(a)}}{a^{v(b)}},$$

where v is the normalized valuation on K, and the right-hand side is to be interpreted as the Teichmuller lift of its image in k. (Hint: use bilinearity and skew-symmetry to reduce to checking a few basic cases. Note that the calculation of $(u, \varpi)_n$ for $u \in O_K^\times$ depends on our normalization of local class field theory: in class, and here, we take uniformizers to geometric frobenii. To compute $(\varpi, \varpi)_n$, rewrite it as $(-1, \varpi)_n(-\varpi, \varpi)_n$, and use parts (a) and (b) to evaluate each of these factors.)

(d) Similarly define $(a, b)_2$ for $K = \mathbb{R}$. Compute it explicitly.

(3) Let K be a finite extension of $\mathbb{Q}_p$. For all primes ℓ, and all integers r, compute the Galois cohomology groups $H^2(G_K, \mathbb{Q}_\ell/\mathbb{Z}_\ell(r))$. (For any Galois module M, we write $M(r)$ for its twist by the r^{th} power of the cyclotomic character; for example, $\mathbb{Q}/\mathbb{Z}(1) = \mu_\infty$.)

(4) Use the previous exercise (the case $r = 0$) to show that any (continuous) projective representation $G_K \to \mathrm{PGL}_n(\mathbb{C})$ lifts to a genuine representation $G_K \to \mathrm{GL}_n(\mathbb{C})$.

(5) (a) Compute $H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/p^n)$ (as an abstract group) for all n. What is the image of the reduction map

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/p^{n+1}) \to H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/p^n)?$$

(b) The natural maps

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Z}_p) \to \varprojlim_n H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/p^n)$$

and

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$$

are isomorphisms (these groups with p-adic coefficients are defined via continuous cochains; you may assume these isomorphisms, or prove them if you like). Use the last part to compute (as an abstract $\mathbb{Q}_p$ vector space) $H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$.

(c) For any continuous representation of G_K (here K can be any field) on a $\mathbb{Q}_p$-vector space V, show that $H^1(G_K, V)$ (again defined via continuous cocycles) is in bijection with isomorphism classes of extensions

$$0 \to V \to E \to \mathbb{Q}_p \to 0$$

of (continuous) $\mathbb{Q}_p$-representations of G_K.

(d) Construct explicit homomorphisms $G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{Q}_p)$ that, under the correspondence of part (c), give a basis of $H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$.

(6) (Norm Limitation Theorem) Let $L/K/\mathbb{Q}_p$ be finite extensions. Let M be the largest abelian extension of K contained in L. Show that $N_{L/K}(L^\times) = N_{M/K}(M^\times)$. Thus, local class field theory gives us little direct information about non-abelian extensions of local fields.

(7) Recall that in problem (6) of the Group Cohomology assignment, we defined the transfer morphism $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ for any open subgroup H of a profinite group G. Establish the following compatibility property of the reciprocity maps of local clas field theory: the diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{r_K} & G_K^{\mathrm{ab}} \\ \downarrow & & \downarrow V \\ L^\times & \xrightarrow{r_L} & G_L^{\mathrm{ab}} \end{array}$$

commutes for any finite extension L/K.

5. Global Class Field Theory

Many of these problems are based on the exercises Tate wrote for the Cassels-Fröhlich volume; you'll find more problems, and extensions of some of these problems, there as well.

(1) (Apropos of the Grunwald-Wang theorem)
   (a) Show that 16 is an 8^{th} power in $\mathbb{Q}_v$ for all $v \neq 2$. (Hint: Show that $\mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}$ is unramified at all odd primes p, and deduce that for all such p, one of $1 + \sqrt{-1}$, $\sqrt{2}$, or $\sqrt{-2}$ lies in $\mathbb{Q}_p$.) That 16 is not an 8^{th} power in $\mathbb{Q}$ has been known for thousands of years.
   (b) Show that 16 is an 8^{th} power everywhere locally in $\mathbb{Q}(\sqrt{7})$, but not an 8^{th} power globally.
   (c) Relate the previous two counter-examples to the statement of the Grunwald-Wang theorem.

(2) (Local norms not global norms)
   (a) Let L/K be a finite *cyclic* extension of number fields. Show that $a \in K$ lies in $N_{L/K}(L)$ if and only if for each place w of L, a lies in $N_{L_w/K_{w|_K}}(L_w)$. (Hint: consider the map $H^2(G(L/K), L^\times) \to H^2(G(L/K), \mathbb{A}_L^\times)$.)
   (b) Let $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Show that 5^2 is not a norm for $L/\mathbb{Q}$, but that it is a norm for $L_w/\mathbb{Q}_{w|_\mathbb{Q}}$ for all places w of L.

(3) Recall that the Hilbert class field H_K of a number field K is the maximal abelian extension of K that is unramfied at all finite places of K and split completely at all infinite places (that is, above every real place of K, H_K has only real places). If we remove the archimedean condition, the resulting field H'_K is called the "narrow" Hilbert class field.
   (a) Which open subgroups of C_K correspond under global class field theory to H_K and H'_K?
   (b) Let $K = \mathbb{Q}(\sqrt{3})$. Compute H_K and H'_K.
   (c) Recall the fields $K = \mathbb{Q}(\sqrt{-5})$ and $L = \mathbb{Q}(\sqrt{-31})$ from "Basics of Global Fields." From your earlier work, you can now complete the description of H_K and H_L.
   (d) For general K, describe the set of primes of K that split completely in H_K/K.
   (e) Show that every ideal in K becomes principal in H_K, assuming the following (tricky!) result in finite group theory: if G is a finite group and $H = [G, G]$ its commutator subgroup, then the transfer map $V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is trivial. (First globalize exercise 7 from "Local Class Field Theory.")

(4) (Ray class fields and "classical" class field theory) Let $\mathfrak{n}$ be a non-zero ideal of O_K, with support $S(\mathfrak{n})$, and for any finite set of (finite) primes S of K, let $I_K^S = I^S$ denote the subgroup of ideals generated by the primes not in S. Let $K_{\mathfrak{n},1}$ denote the set of elements $\alpha \in K^\times$ such that $v(\alpha - 1) \geq v(\mathfrak{n})$ for all $v|\mathfrak{n}$ (here v abusively denotes both the normalized valuation and the corresponding prime ideal).
   (a) Show that the divisor map $K^\times \to I_K$ induces a map $K_{\mathfrak{n},1} \to I_K^{S(\mathfrak{n})}$. Show that $K_{\mathfrak{n},1}$ can alternatively be described as the set of all quotients $\alpha/\beta \in K^\times$ with $\alpha, \beta \in O_K$, $\alpha - \beta \in \mathfrak{n}$, and $(\alpha) + \mathfrak{n} = (\beta) + \mathfrak{n} = O_K$. (Hint: check that every ideal class of K can be represented by an integral ideal in I_K^S, for any finite set S.)
   (b) The quotient $\mathrm{Cl}_\mathfrak{n}(K) = I_K^{S(\mathfrak{n})}/K_{\mathfrak{n},1}$ is known as the ray class group of conductor $\mathfrak{n}$. Show that

$$\mathrm{Cl}_\mathfrak{n}(K) \cong \mathbb{A}_K^\times / (K^\times K_\infty^\times U(\mathfrak{n})),$$

   where $U(\mathfrak{n})$ is the subgroup of $\prod_{v|\infty} O_v^\times$ consisting of elements congruent to 1 modulo $\mathfrak{n}$.
   (c) A finite abelian extension L/K is said to have conductor dividing $\mathfrak{n}$ if for all finite places $w|v$ of L/K, the local reciprocity map $K_v^\times \to \mathrm{Gal}(L_w/K_v)$ vanishes on the subgroup of $O_v^\times$ of elements congruent to 1 modulo $\mathfrak{n}$ (i.e. $1 + \mathfrak{p}_v^{v(\mathfrak{n})}$). Show that there is a *maximal* abelian extension $H_\mathfrak{n}/K$ of conductor I in which all infinite places split completely, and show that the reciprocity map induces an isomorphism $\mathrm{Cl}_\mathfrak{n}(K) \xrightarrow{\sim} \mathrm{Gal}(H_\mathfrak{n}/K)$.
   (d) When $K = \mathbb{Q}$ and $\mathfrak{n} = n$, compute the ray class field $H_n/\mathbb{Q}$.

(5) (Wait to do this problem until we have discussed the Čebotarev density theorem.) Let L/K be a finite extension of number fields, not necessarily Galois. Let S be a finite (or more generally density zero) set of primes of K. Denote by $\mathrm{Spl}_S(L/K)$ the set of primes $v \notin S$ such that v splits completely in L, and by $\mathrm{Spl}'_S(L/K)$ the set of primes $v \notin S$ such that v has a split factor in L (the two sets are equal if L/K is Galois).
   (a) When L/K is Galois, what is the (Dirichlet) density of $\mathrm{Spl}_S(L/K)$?
   (b) A (not necessarily abelian) Galois extension L/K is determined by the set $\mathrm{Spl}_S(L/K)$! More precisely, if L and M are Galois over K, then
   $$L \subset M \iff \mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L).$$
   (Hint: check that $\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K)$, and then use the previous part.)
   (c) If a polynomial $f(X) \in K[X]$ splits into linear factors mod $\mathfrak{p}$ for all but finitely many prime ideals $\mathfrak{p}$ of K, then f splits into linear factors in K. (Hint: consider the splitting field of f.)
   (d) (Not an exercise: see Cassels-Fröhlich exercise 6.2-6.4 if you want to pursue this) In fact, if an irreducible polynomial $f(X) \in K[X]$ has a root mod $\mathfrak{p}$ for almost all $\mathfrak{p}$, then it has a root in K. But in general one has to be very careful with non-Galois extensions in this setting: for instance, the set $\mathrm{Spl}'_S(L/K)$ does not always determine the extension L/K, even up to K-isomorphism, when L/K is not Galois.

(6) Complete the detailed outline given in Exercise 4 of Cassels-Fröhlich of the proof of the Hasse-Minkowski theorem (stated there as Exercise 4.8).

(7) (Higher-power reciprocity laws) Throughout this exercise fix an integer $n > 1$, a number field K containing the n^{th} roots of unity, and let S denote the set of places of K consisting of those dividing n and the archimedean places (the latter will only be relevant in the case $n = 2$). For any $a \in K^\times$, let $S(a)$ denote the union of S with the places dividing a. Define a pairing
   $$K^\times \times (\mathbb{A}_K^S)^\times \to \mu_n(K)$$
   by
   $$(a, \beta) \mapsto \left(\frac{a}{\beta}\right) = \delta(a)(r_K(\beta))^{-1},$$
   where δ is the Kummer theory boundary map, and r_K is the reciprocity map (normalized so that uniformizers map to geometric Frobenii).
   (a) If $\beta_v = 1$ for all $v \in S(a)$, show that $\left(\frac{a}{\beta}\right)$ depends only on the ideal $\beta\mathcal{O}_K$ (that is, the ideal whose prime factorization is given by the valuations $v(\beta_v)$ for all v). We then write $\left(\frac{a}{\beta\mathcal{O}_K}\right)$ and can speak of this "power residue symbol" $\left(\frac{a}{I}\right)$ for any fractional ideal of K supported away from $S(a)$.
   (b) Let I be a non-zero integral ideal of $\mathcal{O}_K$ coprime to n, and let $a \in \mathcal{O}_K$ be coprime to nI. Then
   $$\left(\frac{a}{I}\right) \equiv a^{(N(I)-1)/n} \pmod{I}.$$
   (First check the case where I is prime. This is where you have to pay attention to how we have normalized the reciprocity map.) In particular, if a' is another element of $\mathcal{O}_K$ coprime to nI, and $a \equiv a' \pmod{I}$, then $\left(\frac{a}{I}\right) = \left(\frac{a'}{I}\right)$. Moreover, if $\zeta \in \mu_n(K)$, then taking $a = \zeta$ the above formula holds in $\mathcal{O}_K$, not only modulo I. When $n = 2$, $K = \mathbb{Q}$, and p is an odd prime, check that that we recover the Legendre symbol $\left(\frac{a}{p}\right)$ and the formula for $\left(\frac{-1}{p}\right)$.
   (c) We now prove the general power reciprocity law. Recall first from the previous problem set the (local) Hilbert symbol: at a place v of K, we will now write $(\cdot,\cdot)_v$ for what was denoted $(\cdot,\cdot)_n$ in the last homework. For all $a, b \in K^\times$, show that
   $$\prod_v (a, b)_v = 1.$$

(Use part of the local-global sequence for $Br(K)$.)

(d) The power residue law. For $a, b \in K^\times$, define $\left(\frac{a}{b}\right) = \left(\frac{a}{(b)^{S(a)}}\right)$, where $(b)^{S(a)}$ is the ideal generated by b but excluding any prime factors in $S(a)$. Assume that $S(a) \cap S(b) = S$, and show that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} \prod_{v \in S} (b, a)_v = \prod_v (b, a)_v = 1.$$

Conclude that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S} (a, b)_v.$$

(e) Finally, check that this recovers quadratic reciprocity by computing $(p, q)_2$ for odd primes p and q. (Hint: show that $\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2$ is unramified if and only if $p \equiv 1 \pmod 4$; moreover show that if $p \equiv q \equiv 3 \pmod 4$, then the local reciprocity map $r_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2}$ is non-trivial at q.) A somewhat messier calculation also recovers the formula for $\left(\frac{2}{p}\right)$; and more generally we recover all the classical higher reciprocity laws of Gauss and Eisenstein (see Cassels-Fröhlich for details).

(8) Let $d > 1$ be a square-free integer such that $d \equiv 1 \pmod 4$, and let p be a prime not dividing $2d$.

(a) Show that p can be expressed as $p = x^2 + dy^2$ for $x, y \in \mathbb{Z}$ if and only if p splits completely in $H_K/\mathbb{Q}$, where H_K is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-d})$; equivalently, if p splits in $K/\mathbb{Q}$ into a product of (distinct) principal ideals of O_K. Deduce that the density of such p is $\frac{1}{2h_K}$.

(b) Which integer primes can be expressed in the form $p = x^2 + 5y^2$ with $x, y \in \mathbb{Z}$?

(c) Now we ask the weaker question of which primes can be expressed in the form $x^2 + dy^2$ with $x, y \in \mathbb{Q}$. Show that $p \in N_{\mathbb{Q}(\sqrt{-d})/\mathbb{Q}} \mathbb{Q}(\sqrt{-d})^\times$ if and only if

- $p \in N_{\mathbb{Q}_2(\sqrt{-d})/\mathbb{Q}_2} \mathbb{Z}_2[\sqrt{-d}]^\times$;
- and $p \in (\mathbb{Z}_\ell^\times)^2$ for all primes $\ell | d$;
- and p splits in $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$.

(d) Use the reciprocity theorem to show that in the previous part the condition that p splits in $\mathbb{Q}(\sqrt{-d})$ is implied by the other two conditions. Deduce that the density of primes representable as $x^2 + dy^2$ is $\frac{1}{2^{r+1}}$, where r is the number of prime factors of d. (In particular, $h_K \geq 2^r$.)