Problem set 7 – Math 699 – Algebraic number theory

(1) Let $L/K/F$ be a tower of extensions of number fields. Let $\mathfrak{p}$ be a prime of F, let $\mathfrak{P}_K$ be a prime of K above $\mathfrak{p}$, and let $\mathfrak{P}_L$ be a prime of L above $\mathfrak{P}_K$. Suppose L/F is Galois and that $\mathfrak{P}_L$ is unramified in L/F. Let $\mathrm{Frob}(\mathfrak{P}_L/\mathfrak{p})$ denote the Frobenius element of $\mathfrak{P}_L$ in $\mathrm{Gal}(L/F)$; similarly for $\mathrm{Frob}(\mathfrak{P}_L/\mathfrak{P}_K)$.

(a) Show that

$$\mathrm{Frob}(\mathfrak{P}_L/\mathfrak{P}_K) = \mathrm{Frob}(\mathfrak{P}_L/\mathfrak{p})^{f(\mathfrak{P}_K/\mathfrak{p})},$$

where $f(\mathfrak{P}_K/\mathfrak{p})$ denote the inertial degree of $\mathfrak{P}_K$ in K/F.

(b) If K/F is also Galois, show that

$$\mathrm{Frob}(\mathfrak{P}_K/\mathfrak{p}) = \mathrm{Frob}(\mathfrak{P}_L/\mathfrak{p})|_K.$$

(2) Recall that when K/F is an abelian extension of number fields (so that conjugacy classes in its Galois group are singletons), for a prime $\mathfrak{p}$ of F, all Frobenius elements $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ for $\mathfrak{P}/\mathfrak{p}$ are equal. We denote this common element by $\mathrm{Frob}(\mathfrak{p})$.

Let $n \in \mathbf{Z}_{\geq 3}$, let $K_n = \mathbf{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, and let $F = \mathbf{Q}$. Recall that $\mathrm{Gal}(K_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$ where $\sigma \in \mathrm{Gal}(K_n/\mathbf{Q})$ is sent to the unique element $a_\sigma \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$. Let $F = \mathbf{Q}$.

(a) Recall that p is unramified in K_n if and only if $p \nmid n$. Show that $\mathrm{Frob}(p) = p \in (\mathbf{Z}/n\mathbf{Z})^\times$.

(b) For the rest of this problem, let ℓ be an odd prime. Show that $(\mathbf{Z}/\ell\mathbf{Z})^\times$ has a unique index 2 subgroup and that it consists of the squares in $(\mathbf{Z}/\ell\mathbf{Z})^\times$.

(c) Recall from class that $\mathbf{Q}(\sqrt{\ell^*})$ is a (from part (b), *the*) quadratic extension of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_\ell)$, where $\ell^* = (-1)^{(\ell-1)/2}\ell$. Use Question (1) of this problem set to show that p splits in $\mathbf{Q}(\sqrt{\ell^*})$ if and only if p is a square in $(\mathbf{Z}/\ell\mathbf{Z})^\times$.

(d) From the criterion of prime factorization in quadratic fields (Question (1) of Problem Set 5), realize that you have given a nice, conceptual proof of the law of quadratic reciprocity. Snap!

(3) Recall that when K/F is a Galois, but not abelian, extension of number fields, for a prime $\mathfrak{p}$ of F, we still have the notation $\mathrm{Frob}(\mathfrak{p})$, but we mean the conjugacy class $\{\mathrm{Frob}(\mathfrak{P}) : \mathfrak{P}|\mathfrak{p}\} \subseteq \mathrm{Gal}(K/F)$. We'll use $\mathrm{Frob}_{K/F}(\mathfrak{p})$ to emphasize to which

extension we are referring (another, more standard, notation is $\left(\frac{K/F}{\mathfrak{p}}\right)$, referred to as the *Artin symbol* of $\mathfrak{p}$ in K/F).

Let K_1, K_2 be two number fields, both containing the number field F, and let $L = K_1K_2$ be their composite (i.e. the smallest field containing both of them). Suppose K_i are Galois are F.

(a) Show that L is Galois over F and the natural map

$$\mathrm{Gal}(L/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

given by $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ is injective.

(b) Show that under this map $\mathrm{Frob}_{L/F}(\mathfrak{p}) \mapsto \mathrm{Frob}_{K_1/F}(\mathfrak{p}) \times \mathrm{Frob}_{K_2/F}(\mathfrak{p})$.

(c) Show that $\mathfrak{p}$ splits completely in L/F if and only if it splits completely in both L_1/F and L_2/F.

(d) In 1880, Frobenius proved the following (well, he proved something more general called the Frobenius density theorem): let K/F be Galois and let $\mathrm{Spl}(K/F)$ be the set of all primes of F that split completely in K, then $\mathrm{Spl}(K/F)$ has density $\frac{1}{[K:F]}$ in the set of all primes.[1] Use this to show the following amazing theorem: a Galois extension K/F is determined by the set $\mathrm{Spl}(K/F)$. What?!

(e) The previous part screams for us to ask: what sets of prime ideals can arise as $\mathrm{Spl}(K/F)$ as K runs over finite Galois extensions of F?

Let $F = \mathbf{Q}$. The Kronecker–Weber theorem states that every abelian extension K of $\mathbf{Q}$ is contained in some cyclotomic extension $\mathbf{Q}(\zeta_{\mathfrak{f}})$.[2] Using this theorem,

[1] Here by density, we mean what's called the *natural density*: if $\mathcal{P}$ is a set of prime ideals of F, then its natural density is

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in \mathcal{P} : \mathcal{N}_{F/\mathbf{Q}}(\mathfrak{p}) \le X\}}{\#\{\mathfrak{p} : \mathcal{N}_{F/\mathbf{Q}}(\mathfrak{p}) \le X\}}$$

(if the limit exists). Frobenius originally proved his theorem with the notion of *Dirichlet density*, if I remember correctly, but it holds with the stronger notion of natural density, which is also more, well, natural. The more well-known density theorem is the Chebotarëv density theorem, a strengthening of Frobenius' density theorem (and in fact, it was a conjecture of Frobenius). It states that the density of prime ideals $\mathfrak{p}$ of F whose Frobenius conjugacy class $\mathrm{Frob}(\mathfrak{p})$ is a fixed conjugacy class C of the Galois group G of K/F is $\frac{\#C}{\#G}$ (i.e. the Frobenii are equidistributed with respect to the counting measure on G). If you apply this to $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ you get Dirichlet's theorem on primes in arithmetic progression.

[2] The least $\mathfrak{f}$ for which this is true is called the *conductor* of $K/\mathbf{Q}$, not to be confused with the notion of conductor we came across earlier concerning subrings of the rings of integers. (Technical comment: usually one considers the conductor to be not just an ideal, but to also have an infinite component which for extensions of $\mathbf{Q}$ is just whether or not ∞ "divides" the conductor. The conductor is divisible by infinity if and only if K is *not* contained in the maximal totally real subfield of $\mathbf{Q}(\zeta_{\mathfrak{f}})$. Thus the infinite component is just about whether the real place of $\mathbf{Q}$ must become complex or not.)

show that the sets $\mathrm{Spl}(K/\mathbf{Q})$ that arise as K runs over abelian extensions of $\mathbf{Q}$ consist of the congruence conditions mod n as n varies over integers ≥ 3 and the congruence conditions form a proper subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$.

(4) In this exercise, you'll show that the conductor of a quadratic field $K/\mathbf{Q}$ is equal to (the absolute value of) its discriminant. Let K_n denote $\mathbf{Q}(\zeta_n)$.

(a) Let $D = |\Delta_K|$. Show that K_D contains $K = \mathbf{Q}(\sqrt{\Delta_K})$.

(b) Question (1) of Problem Set 5 tells you how rational primes factor in K. Show that the factorization behaviour of primes in K is given by a congruence conditions modulo D and not modulo any smaller integer.

(c) Conclude from the above problems that K_D is the smallest cyclotomic field containing K.