18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 10, due Thursday, May 4

This will be the last problem set; it will be followed by a take-home final exam due on the last day of classes (May 18), whose scope will be equal to that of these problem sets, i.e., roughly chapters 1-3 of Janusz.

Handy notation: for L a finite extension of $\mathbb{Q}_p$ and $i \geq 0$, let $U_i(L)$ be the subgroup of $\mathfrak{o}_L^*$ consisting of units congruent to 1 modulo $\mathfrak{m}_L^i$.

1. Let K be a finite extension of $\mathbb{Q}_p$, and let L be a finite Galois extension of K; the purpose of this exercise is to prove that $G = \mathrm{Gal}(L/K)$ is solvable. (For more details, see Serre's *Local Fields.*)

   (a) For each integer $i \geq -1$, let G_i be the set of $g \in G$ such that for all $x \in \mathfrak{o}_L$, $g(x) - x \in \mathfrak{m}_L^{i+1}$. Prove that G_i is a subgroup of G.

   (b) Prove that G_0 is the inertia subgroup of G.

   (c) Let π be a uniformizer of L. Show that for each $i \geq 0$, the function $g \mapsto g(\pi)/\pi$ induces an injective homomorphism $G_i/G_{i+1} \to U_i(L)/U_{i+1}(L)$.

   (d) Deduce from (c) that G_0/G_1 is cyclic of order prime to p, and for $i > 0$, G_i/G_{i+1} is abelian of exponent p. Then note that $G_i = \{e\}$ for i large, so G is in fact solvable.

   (e) Show that if G is abelian, then the map $G_0/G_1 \hookrightarrow \kappa_L^*$ given in (c) actually maps into κ_K^*. This will be useful later.

2. Here's the non-Galois version of what I said in class on April 25.

   (a) Let L/K be a finite extension of number fields and let M/K be a Galois extension containing L. Put $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$, and let $\mathfrak{q}$ be a prime of $\mathfrak{o}_M$ above $\mathfrak{p}$. Prove that there is a bijection between the double cosets $H/G\backslash G(\mathfrak{q})$ and the primes of $\mathfrak{o}_L$ above $\mathfrak{p}$, taking a double coset representative g to $L \cap g(\mathfrak{q})$.

   (b) Let L/K be a finite extension of number fields. Deduce from (a) that a prime ideal of K, which does not ramify in L, is totally split in L if and only if it is totally split in the Galois closure of L/K.

   (c) (Optional, not to be turned in) Think about how to extract e and f from this group-theoretic setup.

3. (a) (Galois; optional, but you're encouraged to at least look this up) Let G be a solvable group which acts faithfully and transitively on a finite set of *prime* cardinality. Prove that no non-identity element of G has two fixed points.

(b) (Schmidt) Let L/K be an extension of number fields of prime degree, whose Galois closure is solvable. Prove that if $\mathfrak{p}$ is a prime ideal of K which does not ramify in L, and there are at least two primes of L above $\mathfrak{p}$ of relative degree 1, then $\mathfrak{p}$ splits completely in L.

4. (a) Let K be an abelian extension of $\mathbb{Q}$ unramified away from a single prime p. Prove that there is a unique prime of K above p, and that this prime is totally ramified. (Hint: where does the inertia field ramify?)

   (b) Let G be a p-group. The *Frattini subgroup* F of G is the intersection of the maximal proper subgroups of G. Prove that G/F is the maximal quotient of G which is abelian of exponent p.

   (c) Let K be a Galois extension of $\mathbb{Q}$ of prime power degree, which is unramified away from a single prime p (not necessarily the same prime as the one dividing the degree). Prove that there is a unique prime of K above p, and that this prime is totally ramified. (Hint: use Frattini to reduce to (a).)

   (d) Let $K/\mathbb{Q}$ be an abelian extension of 2-power degree unramified outside 2. Prove that $K \subseteq \mathbb{Q}(\zeta_{2^m})$ for some m. (Hint: first reduce to the case where K is totally real, by replacing K with the maximal real subfield of $K(\sqrt{-1})$. Then for m large, count quadratic subextensions of $K(\zeta_{2^m})$ to prove that $K(\zeta_{2^m})/\mathbb{Q}$ is cyclic, and then deduce the claim.) Optional: is this still true when K is only Galois, not just abelian?

5. The *Kronecker-Weber theorem* asserts that every finite abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$. The *local Kronecker-Weber theorem* asserts that every finite abelian extension of $\mathbb{Q}_p$ is contained in some $\mathbb{Q}_p(\zeta_n)$. Prove that local KW implies global KW, as follows.

   (a) Given an abelian extension K of $\mathbb{Q}$, use local KW to prove that there exists $n = \prod p^{e_p}$ such that for each p which ramifies in K, and each prime $\mathfrak{p}$ of K above p, we have
   $$K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{p^{e_p} m_p})$$
   for some m_p coprime to p.

   (b) Prove that the Galois group of $K(\zeta_n)$ is isomorphic to the product of its inertia groups, and deduce $K(\zeta_n) = \mathbb{Q}(\zeta_n)$. (Hint: first show that the Galois group contains the product, using the fact that $\mathbb{Q}(\zeta_{p^n})$ does not ramify outside p. Then use Minkowski's theorem to get equality.)

6. Put $K = \mathbb{Q}_p(\zeta_p)$.

   (a) Prove that as abelian groups,
   $$K^* = (1-\zeta_p)^{\mathbb{Z}} \times \zeta_{p-1}^{\mathbb{Z}/(p-1)\mathbb{Z}} \times U_1(K).$$

   .

(b) Prove that $U_1(K)^p = U_{p+1}(K)$, so that

$$(K^*)^p = (1-\zeta_p)^{p\mathbb{Z}} \times \zeta_{p-1}^{\mathbb{Z}/(p-1)\mathbb{Z}} \times U_{p+1}(K).$$

(Hint: the case $p = 2$ was on an earlier homework.)

7. I'm going to use a little Kummer theory later, so here is a review.

   (a) (Look it up, but don't turn it in) Let n be a positive integer, and let K be a field of characteristic coprime to n. Suppose that K contains the primitive n-th roots of unity. Then every Galois extension of K with Galois group $\mathbb{Z}/n\mathbb{Z}$ has the form $K(x^{1/n})$ for some $x \in K^*$ which is not a d-th power in K for any $d > 1$ dividing n.

   (b) Let n be a positive integer, and let K be a field of characteristic coprime to n, but now don't suppose that K contains the primitive n-th roots of unity. Define the homomorphism $\omega : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^*$ by the property $g(\zeta_n) = \zeta_n^{\omega(g)}$. Put $M = K(\zeta_n, a^{1/n})$ for some $a \in K(\zeta_n)^*$. Prove that M/K is abelian if and only if for all $g \in \mathrm{Gal}(K(\zeta_n)/K)$, $g(a)/a^{\omega(g)}$ is an n-th power in $K(\zeta_n)$.

8. Prove local Kronecker-Weber as follows. (This follows Washington's *Introduction to Cyclotomic Fields*.)

   (a) Let e be an integer coprime to p. Prove that $\mathbb{Q}_p((-p)^{1/e})$ is Galois over $\mathbb{Q}_p$ if and only if $e|p-1$. (Hint: remember from an earlier pset that $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.)

   (b) Let $K/\mathbb{Q}_p$ be a finite abelian extension of q-power order, for some prime $q \neq p$. Let L be the maximal unramified subextension of K, and put $e = [K : L]$. Prove that $K(\zeta_e) = L(\zeta_e, (-pu)^{1/e})$ for some $u \in \mathfrak{o}^*_{L(\zeta_e)}$, and that $L(\zeta_e, u^{1/e})/\mathbb{Q}_p$ is unramified.

   (c) In the notation of (b), let p^n be the cardinality of the residue field of $L(\zeta_e, u^{1/e})$. Prove that $K \subseteq \mathbb{Q}_p(\zeta_{p(p^n-1)})$.

   (d) Let p be an odd prime. Prove that there is no extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$. (Hint: let K be such an extension, apply Kummer theory (both parts of problem 7) to describe $K(\zeta_p)$ over $\mathbb{Q}_p(\zeta_p)$, then use problem 6.)

   (e) Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. (Hint: in the second case, reduce to showing that there is no extension of $\mathbb{Q}_2$ containing $\mathbb{Q}_2(\sqrt{-1})$ with Galois group $\mathbb{Z}/4\mathbb{Z}$.)

   (f) Deduce local Kronecker-Weber from all this. (This is similar to 4(d); for $p = 2$, use the fact that there are cyclotomic extensions of $\mathbb{Q}_2$ with group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^n\mathbb{Z})^2$ for any n.)

9. (Optional, not to be turned in) In this problem and the next, we give a direct proof of Kronecker-Weber (not going through the local version), modulo an important theorem which we did not discuss from the theory of cyclotomic fields. This argument is due to Franz Lemmermeyer.

(a) Let $K/\mathbb{Q}$ be a cyclic extension of degree p unramified outside p. Put $F = \mathbb{Q}(\zeta_p)$; by Kummer theory, we can write $KF = F(\mu^{1/p})$ for some $\mu \in \mathfrak{o}_F$. Prove that for any prime $\mathfrak{q}$ of F, if $v_{\mathfrak{q}}(\mu) \not\equiv 0 \pmod{p}$, then $\mathfrak{q}$ splits completely in F. (Hint: look at the decomposition group of $\mathfrak{q}$ and use the previous problem.)

(b) Deduce from (b) that the ideal (μ) is a p-th power. (Hint: the prime $(1-\zeta)$ does not fit the criterion in (b).)

(c) Write g_a for the element of $\mathrm{Gal}(F/\mathbb{Q})$ corresponding to $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Then *Stickelberger's theorem* (see, e.g., Washington's *Introduction to Cyclotomic Fields*) implies that for any fractional ideal $\mathfrak{a}$ of F, the fractional ideal

$$\prod_{a=1}^{p-1} g_a^{-1}(\mathfrak{a}^a)$$

is principal. (Yes, that's really the a-th power where a is viewed as an *integer*, not as an element of $(\mathbb{Z}/p\mathbb{Z})^*$. Weird, isn't it?) Use Stickelberger's theorem to prove that the ideal (μ) is the p-th power of a *principal* ideal.

(e) Remember from an earlier pset that every unit in $\mathfrak{o}_F$ is equal to a power of ζ times a unit in the ring of integers of the maximal real subfield of F. Using this, deduce that μ is a power of ζ times a p-th power, and hence $KL = \mathbb{Q}(\zeta_{p^2})$; that is, $K \subseteq \mathbb{Q}(\zeta_{p^2})$.

10. (Optional, not to be turned in) This exercise concludes the direct proof of Kronecker-Weber begun in the previous exercise.

(a) Let $K/\mathbb{Q}$ be a cyclic extension of p-power order, for p prime, in which some prime $q \neq p$ ramifies. Prove that p must divide $q-1$. (Hint: use problem 1(e) above.)

(b) Let $K/\mathbb{Q}$ be an abelian extension which ramifies at some prime q not dividing $[K : \mathbb{Q}]$. Prove that there there exists an abelian extension $K'/\mathbb{Q}$ such that:

- $K \subseteq K'(\zeta_q)$;
- $[K' : \mathbb{Q}]$ divides $[K : \mathbb{Q}]$;
- every prime that ramifies in K' also ramifies in K;
- q does not ramify in K'.

(Hint: first reduce to the case $\zeta_q \in K$. In that case, take K' to be the inertia field of K for a prime above q.)

(c) From other problems in this pset, we know that a cyclic extension of $\mathbb{Q}$ of p-power order unramified away from p is cyclotomic. Use (b) to deduce from this that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.