18.786. (Fall 2011) Homework # 4 (due Thu Oct 13)

1. (Neukirch I.9.1) If L/K is a finite Galois extension of algebraic number fields with noncyclic Galois group, then there are at most finitely many nonsplit prime ideals of $\mathcal{O}_K$. (A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is nonsplit if there is only one prime of $\mathcal{O}_L$ dividing $\mathfrak{p}$.)

2. (Neukirch I.9.3) Every quadratic number field $\mathbb{Q}(\sqrt{d})$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$, ζ_n a primitive n-th root of unity.

3. (Neukirch I.10.2) For every finite abelian group A there exists a Galois extension $L/\mathbb{Q}$ with Galois group $\mathrm{Gal}(L/\mathbb{Q}) \simeq A$. (Hint: Prove and use the fact that for every $n \geq 1$, there are infinitely many prime numbers $p \equiv 1 \bmod n$.)

4. Let L and L' be finite (not necessarily Galois) extensions of a number field K (in the algebraic closure of K). Let $\mathfrak{p}$ be a prime of K. Prove that $\mathfrak{p}$ is unramified in both L and L' if and only if $\mathfrak{p}$ is unramified in the composite field LL'.

5. Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K unramified in L. Show that the following are equivalent.
   - $\mathfrak{p}$ splits completely in L.
   - For some prime $\mathfrak{P}$ of L above $\mathfrak{p}$, the Frobenius element $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ is the identity element of $\mathrm{Gal}(L/K)$.

6. Let L/K be a finite Galois extension of number fields again, and let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. Recall we write $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$. For each integer $s \geq 0$, define

$$I_s := \{\sigma \in D_{\mathfrak{P}} : \sigma(a) \equiv a \pmod{\mathfrak{P}^{s+1}},\ \forall a \in \mathcal{O}_L\}.$$

   (Note that I_0 is the inertia group for $\mathfrak{P}$ over K.) Show that I_s is a normal subgroup of $D_{\mathfrak{P}}$ and that there exists $N > 0$ such that $I_s = \{1\}$ for all $s \geq N$.