June 30rd, 2016

Number Theory II

Prof. H. Esnault, Dr. V. Di Proietto

Exercise sheet 11[1]

Exercise 1. We are going to find a proof of the quadratic reciprocity law (at least for odd primes). Let $p > 2$ be an odd prime and $K = \mathbb{Q}(\zeta_p)$. Set also $G = \mathrm{Gal}(K/\mathbb{Q})$.

(i) We have seen that G is isomorphic to $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$: prove that there exists an isomorphism sending the class $\bar{\ell} \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ of each prime ℓ to σ_ℓ in the notation of point (i) of Exercise 2 of Exercise sheet 10.

(ii) Show that K contains a unique quadratic field $F = \mathbb{Q}(\sqrt{d})$ and determine d in terms of p.

(iii) Fix an odd prime $\ell \neq p$. Show that the following conditions are equivalent:
   a) The restriction $\sigma_\ell|_F$ is trivial;
   b) ℓ is a square in $\mathbb{F}_p^\times$;
   c) ℓ factors as $\ell\mathcal{O}_F = PP'$.

(iv) Combine points (ii) and (iii) to prove the quadratic reciprocity law (for odd primes): a prime $\ell > 2$ is a square in $\mathbb{F}_p^\times$ if and only if

$$\begin{cases} p \text{ is a square in } \mathbb{F}_\ell^\times & \text{if one between } p, \ell \text{ is } \equiv 1 \pmod 4 \\ p \text{ is not a square in } \mathbb{F}_\ell^\times & \text{if both } p, \ell \text{ are } \equiv 3 \pmod 4. \end{cases}$$

Exercise 2. Let $K \subseteq L$ be an extension of number fields.

(i) Let $f(X)$ be a polynomial in $\mathbb{Z}[X]$, with $\deg(f) \geq 1$, show that there are infinitely many primes $p \in \mathbb{Z}$ such that $f(X)$ has a root modulo p.

(ii) Deduce from (i) that there exist infinitely many primes in K which split completely in L. *Hint: Consider the extension $M/\mathbb{Q}$, where M is the Galois closure of $L/\mathbb{Q}$. Use Exercise 2 of Exercise sheet 6 applied to $M/\mathbb{Q}$ and (i).*

Exercise 3. Deduce from Exercise 2 that there exist infinitely many primes in the arithmetic progression $1 + km$ for every $m \in \mathbb{Z}$, in other words that there exist infinitely many primes $p \equiv 1 \pmod m$, for every $m \in \mathbb{Z}$.

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on July 8th.

Exercise 4. Let L/K be a Galois extension of number field, with $G = \mathrm{Gal}(L/K)$. Let $P \subset \mathcal{O}_K$ be a prime ideal.

(i) If P is totally ramified in every intermediate extension of L, but not in L, then there are no intermediate extension. (The group G is cyclic of prime order).

(ii) If P is unramified in every intermediate extension, but it is ramified in L, then there exist $\mathrm{id} \neq H \trianglelefteq G$ minimal, which means that it is contained in every non trivial subgroup of G.

(iii) If P splits completely in every intermediate extension, but does not splits in L, there exists a minimal $H \trianglelefteq G$. Give an example.