June 23rd, 2016

Number Theory II

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

Exercise sheet 10[1]

Exercise 1. (i) Suppose that L_1, L_2 are number fields, say of degrees (over $\mathbb{Q}$) d_1, d_2, respectively. Suppose that p is a prime number which decomposes as $p\mathcal{O}_{L_1} = P^{d_1}$ and that is *unramified* in $L_2/\mathbb{Q}$, meaning that all primes of $\mathcal{O}_{L_2}$ dividing $p\mathcal{O}_{L_2}$ have ramification index equal to 1.

Show that L_1 and L_2 are linearly disjoint.

Let $m \geq 3$ be an integer and suppose

$$m = \prod_{i=1}^{k} p_i^{a_i}$$

for distinct prime numbers $p_1, \ldots, p_k$. Let $\zeta_m = \exp(\frac{2\pi i}{m})$ be a primitive mth root of unity in $\mathbb{C}$ and set $K = \mathbb{Q}(\zeta_m)$.

(ii) Show that if $p \neq q$ are different prime numbers and $r, s \geq 1$, then the fields $\mathbb{Q}(\zeta_{p^r})$ and $\mathbb{Q}(\zeta_{q^s})$ are linearly disjoint.

(iii) Show that the field K is the compositum of $\mathbb{Q}(\zeta_{p_i^{a_i}})$ for $1 \leq i \leq k$.

(iv) You have seen in class that the element $(1 - \zeta_{p^r})$ generates a prime ideal of $\mathbb{Z}[\zeta_{p^r}]$ when p is prime and $r \geq 1$. Prove that if m has at least two prime factors, then

$$(1 - \zeta_m) \in \mathcal{O}_K^\times$$

Exercise 2. Let $m \in \mathbb{Z}_{\geq 2}$ be a natural number and define $K = \mathbb{Q}(\zeta_m)$.

(i) Fix a prime number $\ell \nmid m$ and let P be a prime of $\mathcal{O}_K$ above ℓ with residue field $\mathcal{O}_K/P = \mathbb{F}_P$. Choose $\sigma_\ell \in \mathrm{Gal}(K/\mathbb{Q})$ to be such that its reduction modulo P is the canonical generator of the Galois group $\bmod \ell$, namely

$$\left[\overline{\sigma_\ell} \colon x \longmapsto x^\ell\right] \in \mathrm{Gal}\big(\mathbb{F}_P/\mathbb{F}_\ell\big)$$

Show that the order of $\overline{\sigma_\ell}$ in $\mathrm{Gal}\big(\mathbb{F}_P/\mathbb{F}_\ell\big)$ and of σ_ℓ in G coincide.

Hint: Prove that there are no two mth roots of unity which are congruent modulo P.

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

(ii) Prove that a prime $\ell \nmid m$ factors in $\mathcal{O}_K$ as

$$\ell\mathcal{O}_K = P_1 \dots P_g$$

with $f(P_i/\ell) = f$ where f is the multiplicative order of ℓ modulo m.

Exercise 3. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \equiv 2, 3 \pmod 4$ and $d > 0$.

(i) Suppose that we fix a complex embedding ι of K in $\mathbb{C}$. Show that there exists a unique unit ε in $\mathcal{O}_K^\times$ with $\Re\big(\iota(\varepsilon)\big) > 1$ such that every unit $u \in \mathcal{O}_K^\times$ can be uniquely written as

$$u = \pm\varepsilon^n \quad \text{with } n \in \mathbb{Z}.$$

We call it the fundamental unit (relative to ι)

(ii) Let $\varepsilon = a + b\sqrt{d}$ be the fundamental unit and write inductively

$$\varepsilon^n = a_n + b_n\sqrt{d} \quad \text{for } n \geq 1 :$$

show that $b_n < b_{n+1}$ for all n. Use this result to find the fundamental unit of $\mathbb{Z}[\sqrt{2}]$ and of $\mathbb{Z}[\sqrt{7}]$.

Exercise 4. Let $K = \mathbb{Q}(\sqrt[3]{2})$, and let $\iota\colon K \hookrightarrow \mathbb{R}$ be a real embedding.

(i) Show that the quotient $\mathcal{O}_K^\times/\mu_K$ admits a unique generator ε which verifies $\iota(\varepsilon) > 1$. Call it the fundamental unit.

(ii) Use the bound (if you want a proof, see Lemma 5.13 of Milne's book)

$$|\mathrm{disc}(1, \alpha, \alpha^2)| < 4\iota(\varepsilon^3) + 24$$

to prove that $(\alpha - 1)^{-1}$ is the fundamental unit, where $\alpha = \sqrt[3]{2}$.