May 24th, 2016

Number Theory II

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

Exercise sheet 6[1]

Exercise 1. Let be $P \subset Q \subset U$ be three prime ideals in $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$ where $\mathcal{O}_K$, $\mathcal{O}_L$ and $\mathcal{O}_M$ are the rings of integers of the number fields $K \subset L \subset M$. Prove that the ramification index and the residue class degree are multiplicative in towers: i.e.

$$e(U/P) = e(U/Q)e(Q/P)$$

$$f(U/P) = f(U/Q)f(Q/P).$$

Exercise 2. Let L/K be an extension of number fields of degree n, with ring of integers $\mathcal{O}_K$ and $\mathcal{O}_L$. Fix an element α in $\mathcal{O}_L$ such that $L = K(\alpha)$. For a prime P of $\mathcal{O}_K$ we use the following notation: given a polynomial $f \in \mathcal{O}_K[X]$, let $\overline{f}$ be the corresponding polynomial in $(\mathcal{O}_K/P)[X]$ obtained by reducing the coefficients of f modulo P. Let h be the minimal polynomial of α over K . We consider $\overline{h} \in (\mathcal{O}_K/P)[X]$ and its factorization in monic irreducible distinct factors

$$\overline{h} = \overline{h}_1^{e_1} \cdots \overline{h}_g^{e_g}.$$

Assume that p does not divide $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$, where p is the prime of $\mathbb{Z}$ lying under P. Then the prime decomposition of $P\mathcal{O}_L$ is given by

$$Q_1^{e_1} \cdots Q_g^{e_g}$$

where Q_i is the ideal $(P, h_i(\alpha))$ in $\mathcal{O}_L$ generated by P and $h_i(\alpha)$, with h_i a monic lift of $\overline{h_i}$; in other words

$$Q_i = P\mathcal{O}_L + (h_i(\alpha)).$$

Also $f(Q_i/P)$ is equal to the degree of $\overline{h_i}$.

Exercise 3. Let ζ be a primitive p^rth root of unity, where p is a prime number bigger or equal than 3. We consider $K = \mathbb{Q}(\zeta)$ and denote by $n = [\mathbb{Q}(\zeta) : \mathbb{Q}]$. Proceeding as in exercise 2 of Exercise sheet 3 one can prove that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$; so we assume this. The goal of this exercise is to show, in two different ways, that the ideal $(1 - \zeta)$ is a prime ideal of the ring $\mathbb{Z}[\zeta]$.

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on June 3rd.

(i) Prove that

$$\prod_{1\leq k\leq p^r,(k,p)=1} (1-\zeta^k) = p$$

(ii) Show that $(1-\zeta) \mid (1-\zeta^k)$ in $\mathbb{Z}[\zeta]$ for every $1 \leq k \leq p^r$, with $(k,p)=1$.

(iii) Conclude, using theorem 3.34 of Milne's book, that $(1-\zeta)$ is prime.

(iv) Prove that $(1-\zeta)$ is prime, looking at the factorization in $\overline{\mathbb{F}_p}[X]$ of the reduction of the minimal polynomial of ζ.

Exercise 4. Let $K = \mathbb{Q}(\sqrt[3]{2})$.

(i) Determine the factorization into prime ideals of the ideals $3\mathcal{O}_K$, $5\mathcal{O}_K$ and $11\mathcal{O}_K$.

(ii) Is there a prime number p such that $p\mathcal{O}_K = P^2Q$ with $Q \neq P$? (Hint: Consider the Galois closure of $K/\mathbb{Q}$)

Exercise 5. Let L/K be an extension of number fields of degree n which is Galois. Let P be a prime of $\mathcal{O}_K$ and Q a prime of $\mathcal{O}_L$ which lies over P. Supposing that $P\mathcal{O}_L = Q$, prove that

$$Gal(L/K) \cong Gal((\mathcal{O}_L/Q)/(\mathcal{O}_K/P)).$$

(Hint: Choose an element $\overline{\alpha}$ such that $\mathcal{O}_L/Q = \mathcal{O}_K/P[\overline{\alpha}]$).

Now take $L = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ and $K = \mathbb{Q}$; prove using the above result that it does not exist a prime number p such that $p\mathcal{O}_L$ is prime.