February 14, 2022

NUMBER THEORY I, 14/2/2022

3h. Each question is 4 points (total 32 points).

Exercise 1. (1) Find an integral basis and the discriminant of $K = \mathbb{Q}[\sqrt{13}]$, where by *integral basis* we mean a $\mathbb{Z}$-basis of the ring of algebraic integers $\mathcal{O}_K$ of K.

(2) Let p be an odd prime and $\mathbb{Q}(\zeta_p)$ the p-th cyclotomic field, where ζ_p is a primitive p-th root of unity. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, the fixed field of the subgroup $2\mathbb{Z}/(p-1)\mathbb{Z} \subseteq \mathbb{Z}/(p-1)\mathbb{Z}$ corresponds, by Galois theory, to a quadratic subfield $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. Using that, for number fields $K \subseteq L$, we have $d_K \mid d_L$ (where d_K and d_L are the discriminants of K and L, respectively) and the explicit formulas for $d_{\mathbb{Q}(\zeta_p)}$ and $d_{\mathbb{Q}(\sqrt{p^*})}$, prove that $p^* = p$ if $p \equiv 1 \pmod 4$ and $p^* = -p$ if $p \equiv 3 \pmod 4$.

Exercise 2. (1) Find the units of the ring of integers $\mathcal{O}_K$ of the field $K = \mathbb{Q}[i]$ and the isomorphism class of the group $\mathcal{O}_K^\times$, where $i^2 = -1$.

(2) Find the fundamental unit of the field $K = \mathbb{Q}[\sqrt{2}]$.

Exercise 3. (1) Show that $\mathbb{Q}[\sqrt{5}]$ has class number equal to 1.

(2) Let $K/\mathbb{Q}$ be a number field. Assume that p is a prime number which does not divide the class number of K, and let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. Show that if $\mathfrak{a}^p$ is principal, then $\mathfrak{a}$ is principal.

Exercise 4. (1) Find a prime number number ℓ_1 which is split and a prime number ℓ_2 which is inert in the quadratic field $\mathbb{Q}[\sqrt{5}]$

(2) Let ℓ be an odd prime and $\mathbb{Q}[\zeta_\ell]$ the ℓ-th cyclotomic field, where ζ_ℓ is a primitive p-th root of unity. Put $\lambda = 1 - \zeta_\ell$. Show that the principal ideal (λ) of $\mathbb{Z}[\zeta_\ell]$ satisfies the equality of ideals $(\lambda)^{\ell-1} = (\ell)$ in the ring of integers $\mathbb{Z}[\zeta_\ell]$ of $\mathbb{Q}[\zeta_\ell]$, and show that there is only one prime ideal of $\mathbb{Z}[\zeta_\ell]$ which divides (ℓ).