Algebraic Number Theory (88-798)
5777 Semester B
Question Sheet 4
Due 5/6/2017, יא בסיון תשע"ז

(1) Find all the pairs $(x, y) \in \mathbb{Z}^2$ such that $5x^2 = y^4 + 5y^2$.
(2) Let L and L' be finite Galois extensions of $\mathbb{Q}$ and suppose that $\gcd(d_L, d_{L'}) = 1$. Let LL' be the compositum. Prove that $[LL' : \mathbb{Q}] = [L : \mathbb{Q}][L' : \mathbb{Q}]$.
    Hint: Prove that $L \cap L' = \mathbb{Q}$.
(3) Let $n = \ell^a$ be a power of the prime number ℓ, and let ζ_n denote a primitive n-th root of unity. Consider the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Show that $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_n)$. Prove that $d(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}) = \pm\ell^{\ell^{a-1}(a\ell-a-1)}$.
    Hint: Let $\Phi_n(X) \in \mathbb{Z}[X]$ be the minimal polynomial of ζ_n. Consider the element $\Phi_n'(\zeta_n)$.
    item Let A be an integral domain, let $K = \mathrm{Frac}(K)$, and let L and L' be two Galois extensions of K such that $L \cap L' = K$. Suppose that $[L : K] = n$ and $[L' : K] = m$. If $\mathrm{Gal}(LL'/L') = \{\sigma_1, \ldots, \sigma_n\}$ and $\mathrm{Gal}(LL'/L) = \{\tau_1, \ldots, \tau_m\}$, then prove that $\mathrm{Gal}(LL'/K) = \{\sigma_i\tau_j | 1 \le i \le n, 1 \le j \le m\}$.
(4) Let B and B' be the integral closures of A in L and L', respectively. Suppose that

$$\begin{aligned} B &= Ax_1 + Ax_2 + \cdots Ax_n \\ B' &= Ay_1 + Ay_2 + \cdots + Ay_m \end{aligned}$$

and that $d(x_1, \ldots, x_n) = d$ and $d(y_1, \ldots, y_m) = d'$. Suppose that d and d' (which are elements of A) are relatively prime, in the sense that $dA + d'A = A$. The aim of this exercise and the next one is to prove that $\{x_iy_j | 1 \le i \le n, 1 \le j \le m\}$ is an integral basis of LL'.

Let $\mathcal{O}$ be the integral closure of A in LL'. Let $a \in \mathcal{O}$. Show that we may write $a = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_iy_j$, with $a_{ij} \in K$. We need to prove that all the a_{ij} actually lie in A. For every j, define $b_j = \sum_{i=1}^{n} a_{ij}x_i$. Prove that $d'b_j \in B$ and hence that $d'a_{ij} \in A$ for each pair i, j.

Hint: Use the same idea that we used to prove that $d(z_1, \ldots, z_n)B \subset Az_1 + \cdots + Az_n$ for any basis $\{z_1, \ldots, z_n\}$ of L as a K-vector space.
(5) Prove also that $da_{ij} \in A$ for each pair (i, j) and conclude that $a_{ij} \in A$.
(6) Prove that $d(x_1y_1, \ldots, x_ny_m) = d^m(d')^n$.
(7) Let L/K be a Galois extension of number fields, and suppose that $\mathrm{Gal}(L/K)$ is not cyclic. Prove that there are only finitely many prime ideals of K that are non-split in L. (Recall that a prime ideal of K is called non-split in L if only one prime ideal of L lies above it.)
(8) Let L/K be an extension of number fields, and let N/K be its normal closure. In other words, $N \supset L \supset K$ is the smallest extension such that N/K is Galois. The aim of this

and the next three exercises is to show that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ splits completely in L if and only if it splits completely in N. Show that if $\mathfrak{p}$ splits completely in N, then it splits completely in L.

(9) Let G be a group and let $U, V \subset G$ be two subgroups. If $g, h \in G$, we say that $g \sim h$ if there exist $u \in U$ and $v \in V$ such that $h = ugv$. Then $\sim$ is an equivalence relation, and the equivalence classes UgH are called double cosets. The set of double cosets is written $U\backslash G/V$. (Note that if U is trivial, then the double cosets are just the usual left cosets of V.)

Set $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(N/L) \subset G$. Choose a prime ideal $\mathcal{P}_N$ of N dividing $\mathfrak{p}$, and let $G_{\mathcal{P}_N} \subset G$ be its decomposition subgroup. Let $A_{\mathfrak{p}}$ be the set of prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}$. Show that the following map is a bijection:

$$\begin{array}{rcl} H\backslash G/G_{\mathcal{P}_N} & \to & A_{\mathfrak{p}} \\ \sigma(\in G) & \mapsto & \sigma(\mathcal{P}_N) \cap \mathcal{O}_L \end{array}$$

(10) Suppose now that $\mathfrak{p}$ splits completely in L. For any $\sigma \in G$, show that $H\sigma G_{\mathcal{P}_N} = H\sigma$. Conclude that $\sigma G_{\mathcal{P}_N} \subseteq H\sigma$ for all $\sigma \in G$.

(11) Let $\tilde{H} = \bigcap_{\sigma \in G} \sigma^{-1} H \sigma$. Show that $G_{\mathcal{P}_N} \subset \tilde{H}$ and that $\tilde{H} \subset H$ is a normal subgroup. Conclude that either $\tilde{H} = H$ or $\tilde{H}$ is trivial, and in both cases show that $\mathfrak{p}$ splits completely in N.

(12) Let $p \in \mathbb{Z}$ be an odd prime number such that $p \equiv 2 \mod 3$. If $L = \mathbb{Q}(\sqrt[3]{2})$, prove that $p\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2$, where $f(\mathcal{P}_1|p) = 1$ and $f(\mathcal{P}_2|p) = 2$.

Hint: Use the previous exercises. You may also use the following facts without proof:

(a) If m is a cube-free integer, then $\mathbb{Q}(\sqrt[3]{m})$ has discriminant $-27m^2$.

(b) Let n be an integer, and let ζ_n be a primitive n-th root of unity ($(\zeta_n)^n = 1$ and $(\zeta_n)^m \neq 1$ for $1 \leq m < n$). An odd prime number p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \mod n$.