

Algebraic Number Theory (88-798)

5779 Semester A

Question Sheet 4

- (1) Find all the pairs $(x, y) \in \mathbb{Z}^2$ such that $5x^2 = y^4 + 5y^2$.
- (2) Prove that 26 is the only natural number that is the successor of a perfect square and the predecessor of a perfect cube.
- (3) Let $d > 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$. If $D = d_K$, then show that $x, y \in \mathbb{Z}$ are solutions of Pell's equation $x^2 - Dy^2 = \pm 4$ if and only if $\frac{1}{2}(x + y\sqrt{D}) \in \mathcal{O}_K^*$.
- (4) Say that a solution (x, y) of Pell's equation is positive if $x \geq 0$ and $y \geq 0$. Show that there exists a positive solution (x, y) that is minimal in the sense that if (x', y') is any other positive solution, then $x' \geq x$ and $y' \geq y$. If (x, y) is this minimal positive solution, then show that

$$u = \frac{1}{2}(x + y\sqrt{D})$$

is a fundamental unit of $K = \mathbb{Q}(\sqrt{d})$. (In other words, $\mathcal{O}_K^* = \{\pm u^k : k \in \mathbb{Z}\}$.)

- (5) The following problem appeared in 1917 in H.E. Dudeney's classic puzzle book *Mathematical Amusements*. When I first solved it, I thought I must have made a mistake because the solution differs by several orders of magnitude from the actual number of participants in the Battle of Hastings. Don't be troubled by that.

Read the following text from an ancient manuscript about the Battle of Hastings, which took place in 1066 between William the Conqueror and his Normans, who had just invaded England, and the Saxons led by King Harold II. Determine how many men were in the Saxon army.

“The men of Harold stood well together, as was their wont, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon war hatchet would break his lance and cut through his coat of mail. After Harold joined his men and threw himself into the fray the Saxons were one mighty square of men shouting the battle cries ‘Ut!’ ‘Olicrosse!’ and ‘Godemite!’ ”

- (6) 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 $L \cap L' = \mathbb{Q}$.

- (7) 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 $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}\}$ is a \mathbb{Q} -basis of $\mathbb{Q}(\zeta_n)$. Prove that $d(1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}) = \pm \ell^{a-1(a\ell-a-1)}$.

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 $K = \text{Frac}(A)$, 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 $\text{Gal}(LL'/L') = \{\sigma_1, \dots, \sigma_n\}$ and $\text{Gal}(LL'/L) = \{\tau_1, \dots, \tau_m\}$, then prove that $\text{Gal}(LL'/K) = \{\sigma_i \tau_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$.

(8) 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 $d(x_1, \dots, x_n) = d$ and $d(y_1, \dots, y_m) = d'$. 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 $\{x_i y_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ 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 $a = \sum_{i=1}^n \sum_{j=1}^m a_{ij} x_i y_j$, 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 $d(z_1, \dots, z_n)B \subset Az_1 + \cdots + Az_n$ for any basis $\{z_1, \dots, z_n\}$ of L as a K -vector space.

(9) Prove also that $da_{ij} \in A$ for each pair (i, j) and conclude that $a_{ij} \in A$.

(10) Prove that $d(x_1 y_1, \dots, x_n y_m) = d^m (d')^n$.

(11) Let L/K be a Galois extension of number fields, and suppose that $\text{Gal}(L/K)$ 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.)

(12) 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 .

(13) 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 $G = \text{Gal}(N/K)$ and $H = \text{Gal}(N/L) \subset G$. 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:

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

- (14) 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 $\sigma \in G$.
- (15) 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 .
- (16) Let $p \in \mathbb{Z}$ be an odd prime number such that $p \equiv 2 \pmod{3}$. 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 $p \equiv 1 \pmod{n}$.