Westlake University
Number Theory, 2024-2025

Exam of 23 December 2024

The duration of the exam is of 4 hours. Notes and books are allowed during the exam but electronic devices is not allowed.

The Exam is composed of six parts and each part contains several questions. In part I the questions are pairwise independent. In the other parts it is possible to use the statement of question (i) to solve question $(i+k)$.

Notation. $B(x,r)$ denotes the open ball of center x and radius $r > 0$ in a metric space. Any absolute value on a field K is intended as non-trivial. If not otherwise specified the letter p denotes a prime number. When clear from the context i denotes a primitive 4-th root of unity (the usual imaginary unit).

Part I: Quick questions

(1) For any prime p find an element $\alpha_p \notin \mathbb{Q}_p$ (lying in some extension of $\mathbb{Q}_p$) which is algebraic over $\mathbb{Q}_p$.

(2) Give an example of a Dedekind domain $\mathcal{O}$ with the following properties: (i) It is local (i.e. it contains only one maximal ideal). (ii) Its residue field has characteristic 0.

(3) Let K be a field. Determine whether $K[T^2, T^3]$ is a Dedekind domain.

(4) Determine whether the following subset of $\mathbb{R}^3$ is a complete lattice:

$$L = \{(x,y,z) \in \mathbb{Z}^3 : \ 2x + 3y + 4z \equiv 0 \pmod 7\}.$$

(5) Let $(K, |\cdot|)$ a non-archimeden field, and let $x, y \in K$. Sow that if $y \in B(x,r)$ then $B(y,r) = B(x,r)$ for any $r > 0$. Deduce that the open balls of K are also closed subsets of K.

(6) Give an explicit example of a non-archimedean (and non-trivial) valued field $(K, |\cdot|)$ which is not a discrete valuation field.

 Turn to the next page

Part II: A dynamical system in $\mathbb{Z}_p$

Let p be a prime number. Consider the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ defined by $f(x) = x^p$.

(1) Show that f is continuous.

(2) Describe the set $f(p^n\mathbb{Z}_p)$ for any $n \geq 1$.

(3) Is f is a contraction[1]?

(4) Find all the fixed points of f.

(5) Show that $a \equiv b \pmod{p^k}$ implies $a^p \equiv b^p \pmod{p^{k+1}}$ for any $a, b \in \mathbb{Z}$ and any $k > 0$.

(6) Show that the sequence $\{a^{p^n}\}_{n\in\mathbb{N}}$ converges in $\mathbb{Z}_p$ for any $a \in \mathbb{Z}$.

(7) Show that $\{a^{p^n}\}_{n\in\mathbb{N}}$ converges to a fixed point of f for any $a \in \mathbb{Z}$.

(8) Characterize (depending on $a \in \mathbb{Z}$) the fixed point of f that is the limit of $\{a^{p^n}\}_{n\in\mathbb{N}}$.

Part III: Non cyclic Galois extensions

Let L/K be a finite Galois extension of number fields such that $\mathrm{Gal}(L/K)$ is not a cyclic group.

(1) Show that any nonsplit[2] prime ideal of $\mathcal{O}_K$ is ramified in L. [*Hint: the Galois group of an extension of finite fields is cyclic...*]

(2) Deduce that K has at most finitely many nonsplit ideals.

Part IV: Arbitrary groups of unit

(1) Show that if a number field K contains a root of unity $\zeta \neq \pm 1$ then it doesn't admit real embeddings in $\mathbb{C}$.

(2) Show that there is no number field K such that $\mathcal{O}_K^\times \cong \mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}^{10}$.

(3) Show that a number field K such that $\mathcal{O}_K^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$ must satisfy $[K : \mathbb{Q}] = 4$

(4) There are some number fields K such that $i \in K$ and $[K : \mathbb{Q}] = 4$, but $\mathcal{O}_K^\times \not\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$. Find such fields.

---

[1] Let (X, d) a metric space. Recall that a contraction is a map $g\colon X \to X$ such that $d(g(x), g(y)) \leq C d(x, y)$ for a real constant $C \in]0, 1[$ and any $x, y \in X$.

[2] Recall that $\mathfrak{p} \subset \mathcal{O}_K$ is called nonsplit if only one prime ideal of $\mathcal{O}_L$ lies over $\mathfrak{p}$

 Turn to the next page

(5) Give an explicit example of number a field K such that $\mathcal{O}_K^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$.

Part V: On the Haar mesure on local fields

Disclaimer: this part requires some very basic knowledge of measure theory.

Let K be a local field with a discrete valuation v, a residue field $k = \mathcal{O}/\mathfrak{p}$ of cardinality $q < \infty$ and such that

$$|x|_v := q^{-v(x)} \quad \forall x \in K^\times .$$

Since K is a locally compact (additive) group, it admits a Haar measure μ. We know that such measure satisfies the following relation for any measurable set S and any $x \in K^\times$:

$$\mu(xS) = |x|_v \mu(S) .$$

Show that $\mu(\mathcal{O}^\times) = (1 - q^{-1})\mu(\mathcal{O})$.

Part VI: Conductor and factorization

Let $K = \mathbb{Q}(\sqrt{d})$ with d square free integer and let $\mathfrak{F}$ be the conductor of $\mathbb{Z}[\sqrt{d}]$.

(1) Show that $\mathfrak{F} = \mathcal{O}_K$ if $d \not\equiv 1 \pmod 4$, and $\mathfrak{F} = 2\mathcal{O}_K$ otherwise.

(2) Find the factorizations of the primes 3 and 5 in $K = \mathbb{Q}(\sqrt{-29})$.