In this exam, if $K$ is a number field or a local field, we will denote by $\mathcal{O}_K$ the ring of integers of $K$.

**Exercise 1.** The following questions do not need lengthy justifications.

1. Let $\alpha$ be a complex root of the polynomial $X^2 - X + 3$, and let $K = \mathbb{Q}(\alpha)$. Which are the prime numbers that ramify in $K$?
2. How would you compute the class number or class group of an explicit number field $1$?
3. Give the definition of the Dedekind $\zeta$ function of a number field. What can you say (qualitatively) about its behaviour at $1$?
4. Give the definition of the Dirichlet $L$-function associated to a character of $(\mathbb{Z}/N\mathbb{Z})^\ast$. Give the definition of Artin $L$-functions (you may exclude some primes). Is there a relationship between these two notions?
5. What can you say about the behaviour of Artin $L$-functions at $1$? How can one prove it (just give a brief idea)? Give one way to apply this.
6. Let $K$ be a local field. Give the definition of a finite, tamely ramified extension of $K$. How can one describe the tamely ramified extensions of $K$?
7. Let $K$ be a local field. Give a family of central simple algebras that generate the Brauer group of $K$.

**Problem 1**

Let $K$ be a number field, and let $L$ be a finite Galois extension of $K$, with group $G$. Let $H$ be a subgroup of $G$, and let $E = L^H$ be the fixed field of $H$ in $L$.

1. Give the statement of the Cebotarev density theorem for the extension $L/K$. In particular, what is the analytic density of the set $D(L/K)$ of primes of $\mathcal{O}_K$ that are totally split in $L$?
2. Show that if $L \subset M$, then $D(M/K) \subset D(L/K)$.
3. Let $M$ be another finite Galois extension of $K$, and let $C$ be an algebraic closure of $K$ containing $L$ and $M$. Let $LM$ be the subfield of $C$ generated by $L$ and $M$. Show that the extension $LM/K$ is finite Galois.
4. Show that if there exists a finite set $S$ of primes in $\mathcal{O}_K$ such that $D(M/K) \subset D(L/K) \cup S$, then $D(LM/K)$ and $D(M/K)$ only differ by a finite set.

---

1. This is an open-ended question, you simply need to give some methods you know.
5. What can you deduce from the previous question and the Cebotarev density theorem?

6. Using the previous question, show the following: if $P$ is a monic polynomial in $\mathcal{O}_K[X]$ such that for almost all primes $p$ in $\mathcal{O}_K$, the reduction of $P$ modulo $p$ splits into linear factors, the $P$ is a product of linear factors.

7. Let $D'(E/K)$ be the set of primes $p$ in $\mathcal{O}_K$ such that there exists a prime $\mathfrak{q}$ in $\mathcal{O}_E$ above $p$ with $\epsilon_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$. Let $p$ be a prime in $\mathcal{O}_K$, let $\mathfrak{p}$ be prime in $\mathcal{O}_L$ above $p$, and let $D_\mathfrak{p}$ be the decomposition group of $\mathfrak{p}$. Show that $p \in D'(E/K)$ if and only if there exists a conjugate of $D_\mathfrak{p}$ in $G$ that is contained in $H$.

8. What can you say about the analytic density of $D'(E/K)$?

9. Let $H'$ be a subgroup of $G$, and let $E' = L^{H'}$. Show that $E$ and $E'$ are isomorphic as extensions of $K$ if and only if $H$ and $H'$ are conjugate in $G$.

10. Under the previous notations, assume that $G = S_6$ is the symmetric group on 6 elements,

$$H = \{1, (12)(34), (13)(24), (14)(23)\}$$

and

$$H' = \{1, (12)(34), (12)(56), (34)(56)\}.$$ 

Show that $E$ and $E'$ are not isomorphic as extensions of $K$, but that $D'(E/K) = D'(E'/K)$.

**Problem 2**

Let $p$ be an odd prime number.

**Part 1.**

1. Show that the function

$$\mathbb{Z} \to \mathbb{Z}_p, x \mapsto (1 + p)^x$$

extends to a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$, and give a power series representing $f$.

2. Show that the closure of the subgroup of $(\mathbb{Z}_p^*, \times)$ generated by $1 + p$ is $1 + p\mathbb{Z}_p$. What is the image of $f$?

3. Give an inverse of $f : \mathbb{Z}_p \to 1 + p\mathbb{Z}_p$, and show that $f$ is an isomorphism of topological groups from $\mathbb{Z}_p$ to $1 + p\mathbb{Z}_p$.

4. Show that the group $\mathbb{Q}_p^*$ is isomorphic to

$$\mathbb{Z} \times \mathbb{Z}/(p - 1)\mathbb{Z} \times \mathbb{Z}_p.$$ 

5. Making use of the reciprocity map, show that there is no Galois extension of $\mathbb{Q}_p$ with group $(\mathbb{Z}/p\mathbb{Z})^3$. 

2
Part 2.

1. Let $N = p^s - 1$, where $s$ is a positive integer. Let $\zeta_N$ a primitive $N$-th root of unity in an algebraic closure of $\mathbb{Q}_p$. Show that the extension $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$ is Galois, compute its Galois group and that of its residual extension.

2. Same question with $N = p$. One might first compute the minimal polynomial of $\zeta_N - 1$.

3. Same question with $N = p^t$. One might first compute the minimal polynomial of $\zeta_N^{p^t} - 1$.

4. Let $K$ be a cyclic extension of $\mathbb{Q}_p$ with degree a power of $p$. Show that the Galois group of $K(\zeta_N)$ over $\mathbb{Q}$, for $N$ of the form $(p^s - 1)p^t$ with $s, t > 0$, has a quotient of the form $(\mathbb{Z}/p\mathbb{Z})^3$ as long as $K$ is not included in $\mathbb{Q}(\zeta_N)$.

5. Show that if $K$ is an abelian extension of $\mathbb{Q}_p$ with degree a power of $p$, then $K$ is included in a cyclotomic extension.