- You have 90 minutes to complete the exam.
- Follow the instructions on the cover page of the Tsinghua University Examination Paper.
- This is a closed-book exam. No notes, books, calculators, computers, or electronic aids are allowed.
- All the answers must be written in English on the Tsinghua University Examination Paper. Please write neatly and indicate the problem number. Answers which are illegible for the reader cannot be given credit.
- For the proofs, make sure your arguments are as clear as possible. You will not get full credit for incomplete proofs.
- In case of an emergency, please follow the instructions of the proctor. In any situation, you are not allowed to leave the room with your exam paper.
- Good Luck!

1. Set
$$f(X) \coloneqq X^3 - X - 1 \in \mathbb{Q}[X]$$
and let $L/\mathbb{Q}$ denote the (smallest) splitting field of $f$. Note that the discriminant $\Delta$ of $f$ is $-23$.

Let $v$ be a place of $\mathbb{Q}$ (a prime or $\infty$) and let $w$ be a place of $L$ above $v$. Set
$$G \coloneqq \mathrm{Gal}(L/\mathbb{Q}) \quad \text{and} \quad G_v \coloneqq \mathrm{Gal}(L_w/\mathbb{Q}_v).$$

(a) (10 points) Show that $f(X) \in \mathbb{Q}[X]$ is irreducible.
Note: by (a) and $\sqrt{\Delta} \notin \mathbb{Q}$, one can conclude $[L : \mathbb{Q}] = 6$.

**Solution:** We have $f \in \mathbb{Z}[X]$ and its image $f_2$ in $\mathbb{F}_2[X]$ is irreducible since $f_2$ has no root in $\mathbb{F}_2$. Hence $f$ is irreducible in $\mathbb{Z}[X]$ and thus in $\mathbb{Q}[X]$ by Gauss' lemma.

(b) (20 points) Let $K \coloneqq \mathbb{Q}(\sqrt{-23})$. One can show $K \subset L$, which you may assume from now. Show that $L/K$ is unramified at every place.
Note: by (b) and $h_K = 3$, one can see that $L$ is the Hilbert class field of $K$.

**Solution:** Since $K$ has no real place, $L/K$ is unramified at every infinite place. Moreover, $L/K$ is Galois, so it suffices to show that for every finite place of $K$, there exists an unramified place of $L$ above it.

Set $M \coloneqq \mathbb{Q}[X]/(f)$. This is a degree 3 subextension of $L/\mathbb{Q}$ by (a). Since $[L : \mathbb{Q}] = 6$ and $[K : \mathbb{Q}] = 2$, we see that $M$ and $K$ are linearly disjoint over $\mathbb{Q}$ and $L = KM$. Hence it is enough to show that for every prime $p$, there exists an unramified prime of $\mathcal{O}_M$ above $p$.

Let $f_p$ denote the image of $f \in \mathbb{Z}[X]$ in $\mathbb{F}_p[X]$. Then the discriminant of $f_p$ is $-23 \in \mathbb{F}_p$. Hence if $p \neq 23$, $f_p$ is separable. In this case, the set of irreducible factors $f_p$ corresponds to the set of primes of $\mathcal{O}_M$ above $p$, and each such prime of $\mathcal{O}_M$ is unramified in $M/\mathbb{Q}$.

Finally, assume $p = 23$. Then $f_{23}(X) = (X - 3)(X - 10)^2$ in $\mathbb{F}_{23}[X]$. By Hensel's lemma, there exists $\alpha \in \mathbb{Z}_{23}$ such that $f(\alpha) = 0$ and $\alpha \equiv 3 \pmod{23}$. So $M = \mathbb{Q}[X]/(f) \to \mathbb{Q}_{23} : X \mapsto \alpha$ defines an unramified prime of $\mathcal{O}_M$ above 23.

(c) (15 points) Find $\#G_v$ for $v = 2, 23, \infty$. You must provide a proof to get full credit.

**Solution:** We keep the notation as above. If $v = 2$, then $w$ is unramified in $L/\mathbb{Q}$ by (b) and the fact that 2 is unramified in $K/\mathbb{Q}$. Hence $G_2$ is a cyclic subgroup of $G$. On the other hand, we saw that $f_2$ is irreducible in (a). Hence $2\mathcal{O}_M$ is a prime ideal with residue field $\mathbb{F}_8$. Hence $3 \mid \sharp G_2$. So we conclude $\boxed{\#G_2 = 3}$.

If $v = 23$, the proof of (b) shows that the residue field of $w$ is $\mathbb{F}_{23}$ and the residue degree $f(w/23)$ is 1. Since 23 ramifies in $K/\mathbb{Q}$, the ramification index $e(w/23)$ is 2. Hence $G_{23}$ agrees with the inertia subgroup at $w$ and $\boxed{\#G_{23} = 2}$.

If $v = \infty$, then $w$ is a complex place and $G_\infty = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. So $\boxed{\#G_\infty = 2}$.

(d) (5 points) Let $\mathbb{I}_L$ denote the idèle group of $L$ and let $\mathcal{C}_L \coloneqq \mathbb{I}_L/L^\times$ denote the idèle class group of $L$. Consider the induced map

$$\varepsilon\colon H^2(G, \mathbb{I}_L) \to H^2(G, \mathcal{C}_L).$$

Is $\varepsilon$ surjective? You must provide a proof to get full credit.

**Solution:** The map $\varepsilon$ is described as

$$H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(G_v, (L_w)^\times) = \bigoplus_v \frac{1}{\#G_v}\mathbb{Z}/\mathbb{Z} \xrightarrow{\Sigma} \frac{1}{\#G}\mathbb{Z}/\mathbb{Z} = H^2(G, \mathcal{C}_L),$$

where $v$ runs over all the places of $\mathbb{Q}$. Since the least common multiple of $\#G_v$'s is $6 = \#G$ by (c), we conclude that $\varepsilon$ is surjective.

2. Fix a prime $p$. Let $K$ be a number field and let $K_\infty/K$ be an infinite Galois extension with

$$\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p.$$

We call such an extension a $\mathbb{Z}_p$-*extension*.

All the nonzero closed subgroups of $\mathbb{Z}_p$ are precisely $p^n\mathbb{Z}_p$ ($n \geq 0$). For each $n \geq 0$, let $K_n$ be the unique subextension of $K_\infty/K$ with $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}$ (so $K = K_0$).

Let $v = v_0$ be a place of $K$ and choose a place $v_n$ of $K_n$ inductively such that $v_{n+1} \mid v_n$. Let $L_n$ denote the completion $(K_n)_{v_n}$ of $K_n$ with respect to $v_n$ and set

$$L_\infty \coloneqq \bigcup_{n\geq 0} L_n.$$

In particular, $\mathrm{Gal}(L_\infty/L_0) \subset \mathrm{Gal}(K_\infty/K)$ is the decomposition group at $v$. Let $I_v \subset \mathrm{Gal}(L_\infty/L_0)$ denote the inertia group at $v$.

(a) (10 points) Show that there exists at least one place of $K$ that is ramified in $K_\infty/K$.

**Solution:** Assume the contrary. Then $K_\infty/K$ is an abelian extension in which every place is unramified, so it should be contained in the Hilbert class field $H$ of $K$. Since $[K_\infty : K] = \infty$ and $[H : K] < \infty$, we get contradiction.

(b) (10 points) Show that if $v$ is an infinite place, then $K_\infty/K$ is unramified at $v$ (i.e., $L_\infty = L_0$).

**Solution:** If $v$ is an infinite place, then $\#\,\mathrm{Gal}(L_\infty/L_0)$ is 1 or 2. On the other hand, $\mathbb{Z}_p$ is torsion-free. Hence $\#\,\mathrm{Gal}(L_\infty/L_0) = 1$ and $L_\infty = L_0$.

(c) (10 points) Assume that $v$ is a finite place that is above a rational prime $\ell \neq p$. Show that $K_\infty/K$ is unramified at $v$.
Hint: $\mathcal{O}_{L_0}^\times$ contains an open subgroup that is isomorphic to $\mathcal{O}_{L_0}$ as topological groups.

**Solution:** Write $k_n$ for the residue field of $L_n$ and set $k_\infty \coloneqq \bigcup_{n\geq 0} k_n$. Since $L_\infty/L_0$ is abelian, the local Artin map induces the commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}_{L_0}^\times & \longrightarrow & L_0^\times & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{Art}_{L_\infty/L_0}} & & \downarrow & & \\
1 & \longrightarrow & I_v & \longrightarrow & \mathrm{Gal}(L_\infty/L_0) & \longrightarrow & \mathrm{Gal}(k_\infty/k_0) & \longrightarrow & 0.
\end{array}$$

Here $\alpha \coloneqq (\mathrm{Art}_{L_\infty/L_0})|_{\mathcal{O}_{L_0}^\times} : \mathcal{O}_{L_0}^\times \to I_v$ is continuous and surjective. (If we write $I(L_n/L_0)$ for the inertia group for $L_n/L_0$, then $\mathrm{Art}_{L_n/L_0}|_{\mathcal{O}_{L_0^\times}} : \mathcal{O}_{L_0}^\times \to$

$I(L_n/L_0)$ is surjective. Since $I_v = \varprojlim_n I(L_n/L_0)$ and $\mathcal{O}_{L_0}$ is complete with respect to the norm topology, $\alpha$ is surjective.)

Assume $I_v \neq 0$. Since $I_v$ is a closed subgroup of $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$, we can write $I_v = p^n\mathbb{Z}_p$ for some $n \geq 0$. Take an open subgroup $H \subset \mathcal{O}_{L_0}^\times$ that is topologically isomorphic to $\mathcal{O}_{L_0}$. Since $\ell \neq p$, $p$ is invertible in $\mathcal{O}_{L_0}$ and thus $p^m\mathcal{O}_{L_0} = \mathcal{O}_{L_0}$ for each $m \geq 0$. This implies that the composite

$$H \hookrightarrow \mathcal{O}_{L_0}^\times \xrightarrow{\alpha} I_v = p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p/p^{n+m}\mathbb{Z}_p = \mathbb{Z}/p^m\mathbb{Z}$$

is the zero map for every $m \geq 0$. Hence $H \subset \mathrm{Ker}\,\alpha$ and $\alpha$ induces a surjection $\mathcal{O}_{L_0}^\times/H \twoheadrightarrow I_v = p^n\mathbb{Z}_p$. Since $\#(\mathcal{O}_{L_0}^\times/H) < \infty$, we get contradiction. So $I_v = 0$.

(d) (10 points) Show that there exists $n \geq 0$ such that if a place of $K_n$ is ramified in $K_\infty$, then it is totally ramified in $K_\infty$.

**Solution:** Since $K$ is a number field, there are only finitely many places of $K$ above $p$. This together with (b) and (c) implies that there are only finitely many places of $K$ that are ramified in $K_\infty/K$. Let $v^{(1)}, \dots, v^{(s)}$ be those places of $K$. For $i = 1, \dots, s$, the inertia group $I_{v^{(i)}}$ is a nonzero closed subgroup of $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$, so write $I_{v^{(i)}} = p^{n^{(i)}}\mathbb{Z}_p \subset \mathbb{Z}_p$. Set $n \coloneqq \max\{n^{(1)}, \dots, n^{(s)}\}$. Then this $n$ works. In fact, if $v'$ is a place of $K_n$ that is ramified in $K_\infty$, $v'$ is above $v^{(i)}$ for some $i$. If we write $I'$ for the inertia subgroup of $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}_p$ at $v'$, we have

$$I' = I_{v^{(i)}} \cap \mathrm{Gal}(K_\infty/K_n) = p^{n^{(i)}}\mathbb{Z}_p \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}_p = \mathrm{Gal}(K_\infty/K_n).$$

This means that $v'$ is totally ramified in $K_\infty/K_n$.

(e) (10 points) Assume that $K_\infty/K$ is a cyclotomic $\mathbb{Z}_p$-extension, i.e., $K_\infty \subset K(\mu_{p^\infty}) \coloneqq \bigcup_m K(\mu_{p^m})$. Show that if $v$ is a finite place, $v$ does not split completely in $K_\infty/K$.

**Solution:** Set $M \coloneqq K \cap \mathbb{Q}_(\mu_{p^\infty})$. Then we have

$$\mathrm{Gal}(K_\infty/K) \subset \mathrm{Gal}(K(\mu_{p^\infty})/K) = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/M) \subset \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$$

with $\mathrm{Gal}(K_\infty/K) = \mathbb{Z}_p$ and $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Since $\mathbb{Z}_p^\times$ contains an open subgroup that is topologically isomorphic to $\mathbb{Z}_p$, we see that $\mathrm{Gal}(K_\infty/K)$ has finite index in $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and thus in $\mathrm{Gal}(K(\mu_{p^\infty})/K)$. In particular $[K(\mu_{p^\infty}) : K_\infty] < \infty$.

If $v$ is a finite place, then $K_v = L_0$ is a non-archimedean local field and thus contains only finitely many roots of unity. In particular, $[K_v(\mu_{p^\infty}) : K_v] = \infty$. Since $[K_v(\mu_{p^\infty}) : L_\infty] \leq [K(\mu_{p^\infty}) : K_\infty] < \infty$, we conclude $[L_\infty : L_0] = \infty$. In particular, $L_\infty \supsetneq L_0$. This means that the decomposition group of $K_\infty/K$ at $v$ is nontrivial, namely, $v$ does not split completely in $K_\infty/K$.

3. This is a bonus problem. Your final exam score does not exceed 100.

(a) (5 points) Write down the statement of the existence and uniqueness (i.e., characterizing properties) of the local Artin map $\mathrm{Art}_K$ in Local Class Field Theory for a non-archimedean local field $K$.

You may write "There exists a unique ... such that ... ."

**Solution:** There exists a unique continuous group homomorphism

$$\mathrm{Art}_K \colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that

- $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K$ for every uniformizer $\pi$ (where $\mathrm{Frob}_K$ is a fixed topological generator of $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \widehat{\mathbb{Z}}$);
- for every finite abelian extension $L/K$, $\mathrm{Art}_K(N_{L/K}(L^\times))|_L = 1$ and $\mathrm{Art}_K\,|_L$ induces an isomorphism

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\cong} \mathrm{Gal}(L/K).$$

(b) (5 points) Write down the fundamental exact sequence in Class Field Theory (i.e., the exact sequence involving the Brauer groups) for a global field $K$.

**Solution:** The restrictions and the local invariant maps induce an exact sequence

$$0 \to \mathrm{Br}_K \xrightarrow{(\mathrm{Res}_v)} \bigoplus_{v \in S_K} \mathrm{Br}_{K_v} \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z},$$

where $S_K$ denotes the set of places of $K$.