1. In this exercise we will prove the following Theorem due to Hermite:
   Theorem. For every integer D there are at most finitely many number fields $K/\mathbb{Q}$ satisfying $\mathrm{disc}(K) = D$.
   a) Show that for every $D \in \mathbb{Z}$ there exists a constant $d_0(D)$ such that
   $$\mathrm{disc}(K) = D \implies [K\colon \mathbb{Q}] \leqslant d_0(D).$$
   Deduce that it suffices to show that for any $d, r_1 \in \mathbb{N}$ and for any $D \in \mathbb{Z}$ the set of number fields $K/\mathbb{Q}$ satisfying $[K\colon \mathbb{Q}] = d$, $|\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})| = r_1$, and $\mathrm{disc}(K) = D$ is finite.
   b) Let $d \leqslant d_0(D)$, $0 \leqslant r_1 \leqslant d$ such that $2|d - r_1$, and $V_{d,r_1} = \mathbb{R}^{r_1} \times \mathbb{C}^{\frac{d-r_1}{2}}$. Given $X, Y > 0$, we denote by $B_{X,Y}$ the set given, if $r_1 \geqslant 1$, by
   $$B_{X,Y} = \left\{v \in V_{d,r_1}\colon |v_1| < X, |v_i| < Y^{-1} \text{ for } i = 2, \ldots, r_1 + r_2,\right\}$$
   and, if $r_1 = 0$, by
   $$B_{X,Y} = \left\{v \in V_{d,r_1}\colon |\mathrm{Re}(v_1)| < 1, |\mathrm{Im}(v_1)| < X, |v_i| < Y^{-1} \text{ for } i = 2, \ldots, r_2\right\}.$$
   Show that for all r_1, d as above there exist $C(r_1, d) > 0$ such that
   $$\forall X, Y > 0 \quad \mathrm{vol}(B_{X,Y}) = \begin{cases} C(r_1, d)XY^{1-d} & \text{if } r_1 \geqslant 1, \\ C(r_1, d)XY^{2-d} & \text{else.} \end{cases}$$
   c) Let D, d, r_1 as above and let $K/\mathbb{Q}$ be a number field of degree d satisfying $|\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})| = r_1$ and $\mathrm{disc}(K) = D$. Note that $\sigma_\infty(K) \subseteq V_{d,r_1}$. Suppose that $X, Y > 1$ are chosen such that $\mathrm{vol}(B_{X,Y}) > 2^{\frac{d+r_1}{2}}\sqrt{|D|}$. Show that there exists $z \in \mathcal{O}_K \smallsetminus \{0\}$ such that $\sigma_\infty(z) \in B_{X,Y}$. Show that $|\sigma_1(z)| \geqslant 1$.
   d) Let z as above and let $L = \mathbb{Q}(z) \subseteq K$. Show that the map $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \to \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ given by $\sigma \longmapsto \sigma|_L$ is well-defined and $[K\colon L]$-to-1.
   Hint: Since L has characteristic 0, we know that $K = L(y)$ for some $y \in K$ and $\mathrm{Hom}_{\mathbb{Q}(z)}(K, \mathbb{C})$ is in 1-to-1 correspondence with the roots of the minimal polynomial of y over L.
   e) Let z as above. Show that $\mathbb{Q}(z) = K$.
   Hint: Suppose first that $r_1 = d$, i.e., K is totally real, and look at the fiber above σ_1 under the restriction map above and provide a proof by contradiction. Then generalize to $r_1 \geqslant 1$ and, finally, if $r_1 = 0$, you want to show that $\mathrm{Im}(\sigma_1(z)) \neq 0$.
   f) Deduce that for every $D \in \mathbb{Z}$ the set of number fields of discriminant D is finite.
2. Let $K/\mathbb{Q}$ be a number field of degree d and let $\mathrm{Log}_\infty\colon K^\times \to \mathbb{R}^{r_1+r_2}$ be he group homomorphism given by
   $$\mathrm{Log}_\infty(z)_i = \begin{cases} \log|\sigma_i z| & \text{if } i \leqslant r_1, \\ 2\log|\sigma_i z| & \text{otherwise.} \end{cases} \qquad (z \in K^\times).$$
   Show that $\mathrm{Log}_\infty|_{\mathcal{O}_K^\times}$ has finite kernel and discrete image.
   Hint: Consider a compact set $C \subseteq \mathbb{R}^{r_1+r_2}$ and note that, given $z \in K^\times$, the condition $\mathrm{Log}_\infty(z) \in C$ restricts the size of $\sigma_i(z)$. Now use that integers are one apart.

3. In what follows, we let K be a quadratic number field of discriminant Δ and we denote $D = |\Delta|$. Given $n \in \mathbb{N}$ we denote by ζ_n a choice of a primitive n-th root of unity.
   a) Given $p \in \mathbb{N}$ an odd prime, let $p^* = (-1)^{\frac{p-1}{2}} p$. Show that $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.
   Hint: The multiplicative group in a finite field is cyclic.
   b) Prove that K is a subfield of $\mathbb{Q}(\zeta_D)$.
   Hint: Suppose first that D is square-free and use Sh. 10, Ex. 5.

   Recall that $K \subseteq \mathbb{Q}(\zeta_D)$ gives rise to a surjective group homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

   By identifying $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \cong (\mathbb{Z}/D\mathbb{Z})^\times$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \{-1, 1\}$, we obtain from this homomorphism a character

$$\chi_K \colon (\mathbb{Z}/D\mathbb{Z})^\times \to \{-1, 1\},$$

   which we call the quadratic character associated to K.
   d) Prove that

$$\chi_K(-1) = \begin{cases} 1 & \text{if} \quad \text{if } \Delta > 0, \\ -1 & \text{if} \quad \text{otherwise.} \end{cases}$$

   e) Let p be a prime coprime to D. Show that, under the surjective group homomorphism described above, the Frobenius element $(p, K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q})$ is the image of the Frobenius element $(p, \mathbb{Q}(\zeta_D)/\mathbb{Q}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$.
   f) Show that, for any prime p with $(p, D) = 1$, we have

$$\chi_K(p) = \begin{cases} 1 & \text{if } p \text{ splits in } K, \\ -1 & \text{otherwise.} \end{cases}$$

4. The goal of this exercise is to count fundamental units of real quadratic fields. To this end, given $d \geqslant 2$ a square-free integer, we identify $K = \mathbb{Q}(\sqrt{d})$ with its image in $\mathbb{R}$ given by choosing the unique root satisfying $\sqrt{d} > 0$ and we enumerate the $\mathbb{Q}$-embeddings of K as

$$\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1 = \mathrm{id}_K, \sigma_2 \colon \sqrt{d} \mapsto -\sqrt{d}\}.$$

   a) Let $d > 1$ a square-free integer. Show that $\mathbb{Q}(\sqrt{d})$ contains a unique fundamental unit ε_d satisfying $\varepsilon_d > 1$.
   b) Show that there are $m, n \in \mathbb{N}$ such that $\varepsilon_d = \frac{m + n\sqrt{d}}{2}$.
   Hint: First show that such an equality holds with $m, n \in \mathbb{Z}$ and then use the norm to show that $mn > 0$.

   In what follows, we let $\mathbb{R}$:

$$U_{\text{fun}} = \{\varepsilon_d \colon d > 1 \text{ squarefree}\}, \qquad U_{\text{all}} = \{\varepsilon_d^k \colon d > 1 \text{ squarefree}, k > 1\}.$$

   Thus, U_{fun} contains all fundamental units of real quadratic fields.
   c) For any $X > 2$, prove that $]1, X] \cap U_{\text{fun}}$ is a finite set. We write $f(X)$ for its cardinality.
   d) Let $d > 1$ be a squarefree integer and $u \in \mathcal{O}_K^\times$. We write $u = a + b\sqrt{d}$ for some half-integers $a, b \in \frac{1}{2}\mathbb{Z}$; cf. Sh. 1, Ex. 2. Prove that $1 < u < X$ if and only if $1 < a < (X^2 \pm 1)/(2X)$.

e) Given $a \in \frac{1}{2}\mathbb{Z}$ satisfying the above inequalities and a sign $\sigma \in \{\pm 1\}$, prove that there is a unique choice of $b \in \frac{1}{2}\mathbb{Z}$ and squarefree $d > 1$ such that $a + b\sqrt{d}$ is a unit of norm σ.
Hint: $a^2 + \sigma = b^2 d$.

f) Counting the number of possibilities for a and σ, deduce that

$$\left|]1, X] \cap U_{\text{all}} \right| = 2X + O(1) \quad \text{as } X \to \infty.$$

We write $a(X)$ for $\left|]1, X] \cap U_{\text{all}} \right|$.

g) Prove that $a(X) = \sum_{k=1}^{\infty} f(X^{1/k})$ for X large enough, where the sum is actually finite.

h) Let $\mu \colon \mathbb{N} \to \{-1, 0, 1\}$ denote the Möbius function given by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\omega(n)$ denotes the number of pairwise distinct prime factors of n. Recall that

$$\forall n \in \mathbb{N} \quad \sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Show that

$$f(X) = \sum_{k=1}^{\infty} \mu(k) a(X^{1/k})$$

for sufficiently large X.

i) Conclude that $f(X) = 2X + o(X)$ as $X \to \infty$. In particular, we have

$$\lim_{X \to \infty} \frac{\left|]1, X] \cap U_{\text{fun}} \right|}{X} = 2.$$