(1) Let \( m \neq 1 \) be a square-free integer and \( K = \mathbb{Q}(\sqrt{m}) \). The embeddings \( K \to \mathbb{C} \) are given by \( \sigma_1(a + b\sqrt{m}) = a + b\sqrt{m} \) and \( \sigma_2(a + b\sqrt{m}) = a - b\sqrt{m} \).

If \( m \not\equiv 1 \mod 4 \) then \( R_K = \mathbb{Z} + \mathbb{Z}\sqrt{m} \) by Lemma 3.6, so \( \beta_1 = 1, \beta_2 = \sqrt{m} \) is a \( \mathbb{Z} \)-basis of \( R_K \). Hence

\[
d_K = \det \begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = 4m.
\]

If \( m \equiv 1 \mod 4 \) then \( R_K = \mathbb{Z} + \mathbb{Z}\frac{1 + \sqrt{m}}{2} \) by Lemma 3.6, so \( \beta_1 = 1, \beta_2 = \frac{1 + \sqrt{m}}{2} \) is a \( \mathbb{Z} \)-basis of \( R_K \). Hence

\[
d_K = \det \begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \frac{1 + \sqrt{m}}{2} \\ 1 & \frac{1 - \sqrt{m}}{2} \end{pmatrix}^2 = m.
\]

Therefore we have shown that

\[
d_{\mathbb{Q}(\sqrt{m})} = \begin{cases} 4m & \text{if } m \not\equiv 1 \mod 4, \\ m & \text{if } m \equiv 1 \mod 4. \end{cases}
\]

(2) Let \( a \in \mathbb{Z} \) be such that \( a^2 \equiv m \mod p \), and consider the ideals \( P_1 = (p, \sqrt{m} + a) \) and \( P_2 = (p, \sqrt{m} - a) \) of \( R_{\mathbb{Q}(\sqrt{m})} \).

**Claim:** \( P_1P_2 = (p) \)

**Proof of claim.** We have

\[
P_1P_2 = (p^2, p(\sqrt{m} + a), p(\sqrt{m} - a), m - a^2).
\]

It is clear that \( p^2, p(\sqrt{m} + a), p(\sqrt{m} - a) \in (p) \). Furthermore \( m - a^2 \in (p) \) because \( a^2 \equiv m \mod p \). This shows that \( P_1P_2 \subseteq (p) \).

To show the converse we first observe that \( p^2, p(\sqrt{m} + a), p(\sqrt{m} - a) \in P_1P_2 \). Since \( p \nmid m \) and \( a^2 \equiv m \mod p \), it follows that \( p \nmid a \). Furthermore \( p \) is odd, so \( p \nmid 2a \). Therefore \( 2a \) and \( p \) are coprime, so there exist \( u, v \in \mathbb{Z} \) such that \( u \cdot 2a + v \cdot p = 1 \). Multiplying this by \( p \) gives \( p = u \cdot 2a + v \cdot p^2 \in P_1P_2 \). This implies \( (p) \subseteq P_1P_2 \).

**Claim:** \( P_1 \) and \( P_2 \) are prime ideals of \( R_{\mathbb{Q}(\sqrt{m})} \)

**Proof of claim.** Using Lemmas 8.5 and 8.2 we have

\[
\mathbf{N}(P_1)\mathbf{N}(P_2) = \mathbf{N}(P_1P_2) = \mathbf{N}((p)) = p^{[K:\mathbb{Q}]} = p^2.
\]

Furthermore it is easy to see that \( \mathbf{N}(P_1) = \mathbf{N}(P_2) \) (observe that the automorphism \( \tau \) of \( K \) maps \( P_1 \) onto \( P_2 \) and therefore induces an isomorphism \( R_K/P_1 \cong R_K/P_2 \)). It follows that \( \mathbf{N}(P_1) = \mathbf{N}(P_2) = p \). By Question (3)(a) this implies that \( P_1 \) and \( P_2 \) are prime ideals.

(3) (a) Assume that \( A \) is a non-zero ideal of \( R_K \) which is not a prime ideal. If \( A = R_K \) then \( \mathbf{N}(A) = 1 \), i.e. in this case \( \mathbf{N}(A) \) is not a prime number. If \( A \neq R_K \) then by Theorem 4.7 we can write \( A = P_1 \cdots P_n \) with \( n \geq 2 \) where \( P_1, \ldots, P_n \) are non-zero prime ideals of \( R_K \). By Lemma 8.5 we obtain \( \mathbf{N}(A) = \mathbf{N}(P_1) \cdots \mathbf{N}(P_n) \). Now for all \( i \) we have \( \mathbf{N}(P_i) \in \mathbb{N} \) and \( \mathbf{N}(P_i) \neq 1 \) because \( P_i \neq R_K \). This shows that in this case \( \mathbf{N}(A) \) is a composite number, i.e. again \( \mathbf{N}(A) \) is not a prime number.
(b) Let $K = \mathbb{Q}(\sqrt{2})$ and $A = (3)$, i.e. $A$ is the principal ideal of the ring $R_K$ generated by 3. We claim that $A$ is a prime ideal of $R_K$ such that $N(A)$ is not a prime number.

By Lemma 8.2 we have $N(A) = 3^{[K:\mathbb{Q}]} = 9$, so $N(A)$ is not a prime number.

To show that $A$ is a prime ideal, we must show that if

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \in A$$

where $a + b\sqrt{2}, c + d\sqrt{2} \in R_K$ then $a + b\sqrt{2} \in A$ or $c + d\sqrt{2} \in A$. Now $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \in A$ implies $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 3 \cdot (u + v\sqrt{2})$ for some $u + v\sqrt{2} \in R_K$. Since $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ it follows that

$$ac + 2bd = 3u,$$
$$ad + bc = 3v.$$

If $b \equiv 0 \pmod{3}$ then these two equations imply $ac \equiv ad \equiv 0 \pmod{3}$. Therefore either $a \equiv 0 \pmod{3}$ and so $a + b\sqrt{2} \in A$, or $c \equiv d \equiv 0 \pmod{3}$ and so $c + d\sqrt{2} \in A$.

Now assume that $b \not\equiv 0 \pmod{3}$. From the two formulas $ac + 2bd = 3u$ and $ad + bc = 3v$ we can deduce $be^2 + bd^2 \equiv 0 \pmod{3}$. This implies $c^2 + d^2 \equiv 0 \pmod{3}$. Therefore $c^2 \equiv d^2 \equiv 0 \pmod{3}$ and hence $c \equiv d \equiv 0 \pmod{3}$. This shows that $c + d\sqrt{2} \in A$.

(4) If $z > 1$ is a real number then

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z} < 1 + \frac{1}{z - 1},$$

(compare the computation in the notes after Definition 7.1). Also

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z} > \int_{1}^{\infty} x^{-z} dx = \frac{1}{z - 1}.$$ 

These two inequalities imply $1 < (z - 1)\zeta(z) < z$ for all $z > 1$. Letting $z \to 1^+$ gives

$$1 \leq \lim_{z \to 1^+} (z - 1)\zeta(z) \leq \lim_{z \to 1^+} z = 1,$$

hence $\lim_{z \to 1^+} (z - 1)\zeta(z) = 1$.

(5) Let $m > 1$. The polynomial $X^m - 1$ has roots $\zeta_m^i$ for $i = 0, 1, \ldots, m - 1$, therefore $X^m - 1 = \prod_{i=0}^{m-1} (X - \zeta_m^i)$. Dividing this equation by $X - 1$ gives

$$X^{m-1} + X^{m-2} + \cdots + X + 1 = \prod_{i=1}^{m-1} (X - \zeta_m^i).$$

Letting $X = 1$ shows that

$$m = \prod_{i=1}^{m-1} (1 - \zeta_m^i).$$

Write $n = p_1^{a_1} \cdots p_r^{a_r}$ where $p_1, \ldots, p_r$ are distinct prime numbers and $a_k \in \mathbb{N}$. Applying the above formula to $m = n$ gives

$$n = \prod_{i=1}^{n-1} (1 - \zeta_n^i).$$
Applying the above formula to \( m = p_k^{a_k} \) and using that \( \zeta_{p_k^{a_k}} = \zeta^{n/p_k} \) gives

\[
p_k^{a_k} = \prod_{i=1}^{p_k^{a_k} - 1} (1 - \zeta^{n/p_k^{a_k} - 1}) = \prod_{j} (1 - \zeta_n^j)
\]

where the product is over those \( j \in \{1, \ldots, n-1\} \) for which \( \zeta_n^j \) has order a power of \( p_k \). Hence

\[
n = p_1^{a_1} \cdots p_r^{a_r} = \prod_{j} (1 - \zeta_n^j)
\]

where the product is over those \( j \in \{1, \ldots, n-1\} \) for which \( \zeta_n^j \) has prime power order.

It follows that

\[
1 = \prod_{j} (1 - \zeta_n^j)
\]

where the product is over those \( j \in \{1, \ldots, n-1\} \) for which \( \zeta_n^j \) is not of prime power order. Since \( n \) has at least two distinct prime factors this product contains the factor \( 1 - \zeta_n \). Hence \( (1 - \zeta_n)^{-1} = \prod_{j \neq 1} (1 - \zeta_n^j) \) where the product is over those \( j \in \{2, \ldots, n-1\} \) for which \( \zeta_n^j \) has not prime power order. Since \( 1 - \zeta_n \in R_{Q(\zeta_n)} \) and \( (1 - \zeta_n)^{-1} = \prod_{j \neq 1} (1 - \zeta_n^j) \in R_{Q(\zeta_n)} \), it follows that \( 1 - \zeta_n \) is a unit in \( R_{Q(\zeta_n)} \).

(6) Let \( n \in \mathbb{N} \). We recall that \([Q(\zeta_n) : Q] = \phi(n)\) where \( \phi \) is Euler’s \( \phi \)-function. Indeed, for \( n = 1 \) this is clear, for \( n > 1 \) and \( n \equiv 2 \pmod{4} \) this is Theorem 10.1.1, and for \( n \equiv 2 \pmod{4} \) it follows from the other cases because we have (using that \( n/2 \) is odd) \([Q(\zeta_n) : Q] = [Q(\zeta_{n/2}) : Q] = \phi(n/2) = \phi(n)\).

**Claim:** If \( n > 1 \) is an even integer then \( \mu_{Q(\zeta_n)} = \{ \zeta_n^i : 0 \leq i \leq n-1 \} \).

**Proof.** The inclusion \( \{ \zeta_n^i : 0 \leq i \leq n-1 \} \subseteq \mu_{Q(\zeta_n)} \) is clear.

Conversely let \( \epsilon \in \mu_{Q(\zeta_n)} \). Let \( m \in \mathbb{N} \) be the order of \( \epsilon \). Then \( \epsilon = \zeta_n^i \) for some integer \( i \) with \( (i, m) = 1 \). It follows that \( \zeta_m \in \mu_{Q(\zeta_n)} \) (because if \( u \cdot i + v \cdot m = 1 \) for \( u, v \in \mathbb{Z} \) then \( \zeta_m = \zeta_n^i = (\zeta_n^{1/m})^u \cdot (\zeta_n^{1/m})^v = \epsilon^i \)). Now let \( l = \text{gcd}(m, n) \). Then \( (l/m, l/n) = 1 \), so there exist \( x, y \in \mathbb{Z} \) such that \( 1 = x \cdot l/m + y \cdot l/n \). It follows that \( \zeta_l = \zeta_n^{1} = (\zeta_n^{1/m})^x \cdot (\zeta_n^{1/n})^y = \zeta_m^x \cdot \zeta_n^{y} \in Q(\zeta_n) \).

Thus \( Q(\zeta_l) \subseteq Q(\zeta_n) \). The inclusion \( Q(\zeta_n) \subseteq Q(\zeta_l) \) is obvious because \( n \mid l \), hence \( Q(\zeta_n) = Q(\zeta_l) \) and therefore \( \phi(n) = \phi(l) \). Since \( n \mid l \) and \( l \) is even, this implies that \( l = n \) and thus \( m \mid n \). Hence \( \zeta_m = \zeta_n^n \) for some \( j \in \mathbb{Z} \). It follows that \( \epsilon = \zeta_n^i = \zeta_m^j \). Thus we have shown that \( \mu_{Q(\zeta_n)} \subseteq \{ \zeta_n^i : 0 \leq i \leq n-1 \} \).

Now let \( n > 1 \) be an integer such that \( n \equiv 2 \pmod{4} \). If \( n \) is divisible by \( 4 \) then \( \mu_{Q(\zeta_n)} = \{ \zeta_n^i : 0 \leq i \leq n-1 \} \) by the claim. If \( n \) is odd then

\[
\mu_{Q(\zeta_n)} = \mu_{Q(\zeta_{2n})} = \{ \zeta_{2n}^i : 0 \leq i \leq 2n-1 \} = \{ \pm \zeta_n^i : 0 \leq i \leq n-1 \}
\]

where for the second equality we use the claim and for the first and third equalities we use that \( \zeta_{2n} = -\zeta_n^{(n+1)/2} \). Thus we have shown that

\[
\mu_{Q(\zeta_n)} = \begin{cases} 
\{ \pm \zeta_n^i : 0 \leq i \leq n-1 \} & \text{if } n \text{ is odd,} \\
\{ \zeta_n^i : 0 \leq i \leq n-1 \} & \text{if } n \text{ is divisible by } 4
\end{cases}
\]

as required.
(7) (a) By Theorem 10.2 we know that \( \mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) \). Note that
\[
\zeta_5 = \sqrt[4]{5} - \frac{1}{4} + \frac{\sqrt[4]{5} + 5}{8}i.
\]
Since \( \zeta_5^{-1} = \overline{\zeta_5} \) it follows that
\[
\zeta_5 + \zeta_5^{-1} = \frac{\sqrt[4]{5} - 1}{2}.
\]
From this it is obvious that \( \mathbb{Q}(\zeta_5) = \mathbb{Q}(\sqrt[4]{5}) \).

(b) The group of units \( R_{\mathbb{Q}(\sqrt[4]{5})}^\times \) is generated by \( \{\pm 1\} \) and a fundamental unit. To find a fundamental unit \( \varepsilon = a + b\sqrt[4]{5} \) of \( \mathbb{Q}(\sqrt[4]{5}) \) we can use the method from Question (7) on Problem Sheet 1. Since \( 5 \equiv 1 \pmod{4} \), we must try \( a = \frac{1}{2}, \frac{3}{2}, \ldots \) until we find an \( a \) for which there exists a \( b \) such that \( a + b\sqrt[4]{5} \in R_{\mathbb{Q}(\sqrt[4]{5})}^\times \), i.e. \( a + b\sqrt[4]{5} \in R_{\mathbb{Q}(\sqrt[4]{5})}^\times \) and \( N(a + b\sqrt[4]{5}) = \pm 1 \). For \( a = \frac{1}{2} \) we find \( N(\frac{1}{2} + \sqrt[4]{5}) = \frac{1}{4} - 5b^2 \) and this is equal to \(-1\) for \( b = \frac{1}{2} \). Therefore \( \varepsilon = \frac{1 + \sqrt[4]{5}}{2} \) is a fundamental unit of \( \mathbb{Q}(\sqrt[4]{5}) \).

It follows that
\[
R_{\mathbb{Q}(\zeta_5)}^\times = R_{\mathbb{Q}(\sqrt[4]{5})}^\times = \{\pm 1\} \times \varepsilon^\mathbb{Z} = \{\pm 1\} \times \left( \frac{1 + \sqrt[4]{5}}{2} \right)^\mathbb{Z}.
\]

(c) By definition the group \( C^+ \) of cyclotomic units of \( \mathbb{Q}(\zeta_5) \) is generated by \(-1\) and by the units \( \xi_a \) for all \( a \in \mathbb{Z} \) with \( (a, 5) = 1 \). An easy computation shows that \( \xi_{a+5} = -\xi_a \) and \( \xi_{-a} = -\xi_a \). Furthermore \( \xi_1 = 1 \). It follows that \( C^+ \) is generated by \(-1\) and \( \xi_2 \). We have
\[
\xi_2 = \zeta_5^{(1-2)/2} \cdot \frac{\zeta_5^2 - 1}{\zeta_5 - 1} = -\zeta_5^2 \cdot (\zeta_5 + 1) = -(\zeta_5^{-2} + \zeta_5^2) = \ldots = 1 + \sqrt[4]{5} \cdot \frac{1}{2}.
\]
Hence
\[
C^+ = \{\pm 1\} \times \xi_2^\mathbb{Z} = \{\pm 1\} \times \left( \frac{1 + \sqrt[4]{5}}{2} \right)^\mathbb{Z}.
\]

(d) By parts (b) and (c) we have \( R_{\mathbb{Q}(\zeta_5)}^\times = C^+ \), therefore it follows from Theorem 11.4 that
\[
h_{\mathbb{Q}(\zeta_5)}^\times = [R_{\mathbb{Q}(\zeta_5)}^\times : C^+] = 1.
\]

(8) Let \( p \) be a prime number and \( f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X] \). We will use Hensel’s lemma to show that the equation \( f(X) = 0 \) has \( p - 1 \) solutions in \( \mathbb{Z}_p \). Note that \( f'(X) = (p - 1)X^{p-2} \).

For every \( a \in \mathbb{Z}_p \) there exists an \( \bar{a} \in \mathbb{Z} \) such that \( a \equiv \bar{a} \pmod{p} \). It easily follows that \( \mathbb{Z}_p/p^2\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \), so \( \mathbb{Z}_p/p^2\mathbb{Z}_p \) is a field with \( p \) elements. Now let \( \alpha \in \mathbb{Z}_p/p^2\mathbb{Z}_p \) be a non-zero element. Choose \( a_1 \in \mathbb{Z} \subseteq \mathbb{Z}_p \) such that \( a_1 \) reduces to \( \alpha \) in \( \mathbb{Z}_p/p^2\mathbb{Z}_p \). Since \( \alpha \neq 0 \) it follows that \( p \mid a_1 \) and therefore by Euler’s theorem \( a_1^{p-1} \equiv 1 \pmod{p} \). Hence \( a_1 \) satisfies \( f(a_1) \equiv 0 \pmod{p} \). Furthermore \( f'(a_1) = (p - 1)a_1^{p-2} \neq 0 \pmod{p} \) since \( p - 1 \neq 0 \pmod{p} \) and \( a_1 \neq 0 \pmod{p} \). Therefore by Hensel’s lemma (Theorem 14.1) there exists a unique \( a \in \mathbb{Z}_p \) such that \( f(a) = 0 \) and \( a \equiv a_1 \pmod{p} \). The last condition implies that \( a \) reduces to \( \alpha \) in \( \mathbb{Z}_p/p^2\mathbb{Z}_p \) because \( a_1 \) reduces to \( \alpha \).
We have shown that for every non-zero $\alpha \in \mathbb{Z}_p/p\mathbb{Z}_p$ there exists a unique solution $a \in \mathbb{Z}_p$ of $f(X) = 0$ which reduces to $\alpha$. As there are $p-1$ choices for $\alpha$, we have therefore found $p-1$ solutions of the equation $f(X) = 0$.

(9) Existence of $a$: We will construct a sequence $a_0, a_1, a_2, \ldots$ in $\mathbb{Z}_p$ such that for all $i \geq 0$ we have

(i) $f(a_i) \equiv 0 \pmod{p^{2M+1+i}}$,

(ii) $a_i \equiv a_{i-1} \pmod{p^{M+i}}$ if $i \geq 1$.

Clearly the given $a_0 \in \mathbb{Z}_p$ satisfies (i) and (ii).

Now suppose that we have constructed $a_0, a_1, \ldots, a_i$ satisfying (i) and (ii). We want to find $a_{i+1} \in \mathbb{Z}_p$ for which (i) and (ii) hold. In order for (ii) to be satisfied we must have $a_{i+1} = a_i + \lambda p^{M+i}$ for some $\lambda \in \mathbb{Z}_p$. We will show that there exists $\lambda$ such that $f(a_i + \lambda p^{M+i}) \equiv 0 \pmod{p^{2M+2+i}}$.

Note that

$f(a_i + \lambda p^{M+i}) \equiv f(a_i) + f'(a_i)\lambda p^{M+i} \pmod{p^{2M+2+i}}$.

Hence we will have $f(a_i + \lambda p^{M+i}) \equiv 0 \pmod{p^{2M+2+i}}$ if and only if

$f(a_i) + f'(a_i)\lambda p^{M+i} \equiv 0 \pmod{p^{2M+2+i}}$.

By assumption $f(a_i) \equiv 0 \pmod{p^{2M+2+i}}$. Since $a_i \equiv a_0 \pmod{p^{M+1}}$ we have $f'(a_i) \equiv f'(a_0) \pmod{p^{M+1}}$, so in particular $f'(a_i) \equiv 0 \pmod{p^{M}}$. It follows that the previous congruence is equivalent to

$f(a_i) + f'(a_i)\lambda p^{M+i} \equiv 0 \pmod{p^{2M+2+i}}$.

Now $f'(a_i) \not\equiv 0 \pmod{p^{M+1}}$, hence $L(a_i)/p^{M+1} \not\equiv 0 \pmod{p}$. Therefore $f'(a_i)/p^{M+1}$ is a unit in $\mathbb{Z}_p$, so there exists a $\lambda \in \mathbb{Z}_p$ such that the previous congruence is satisfied. It follows that $a_{i+1} = a_i + \lambda p^{M+i}$ satisfies condition (i).

By (ii) the sequence $a_0, a_1, a_2, \ldots$ is a Cauchy sequence in $\mathbb{Z}_p$. Hence we can define $a = \lim_{i \to \infty} a_i \in \mathbb{Z}_p$. Then (again by (ii)) we have $a \equiv a_0 \pmod{p^{M+i}}$. Furthermore $f(a) = f(\lim_{i \to \infty} a_i) = \lim_{i \to \infty} f(a_i) = 0$ where the last equality comes from (i). This shows the existence of $a \in \mathbb{Z}_p$ with the required properties.

Uniqueness of $a$: Suppose that $a' \in \mathbb{Z}_p$ satisfies $f(a') = 0$ and $a' \equiv a_0 \pmod{p^{M+1}}$. We must show that $a' = a$.

First we make the following observation. We showed above that for every $i \geq 0$ there exists $a_{i+1} \in \mathbb{Z}_p$ such that conditions (i) and (ii) are satisfied. It follows from the above that $a_{i+1}$ must be of the form $a_{i+1} = a_i + \lambda p^{M+i}$ and that $\lambda$ is unique modulo $p$. Therefore $a_{i+1}$ is unique modulo $p^{M+2+i}$.

Now we claim that for all $i \geq 0$ we have $a' \equiv a_i \pmod{p^{M+1+i}}$. For $i = 0$ this is true by assumption. Suppose that we have shown $a' \equiv a_i \pmod{p^{M+1+i}}$ for some $i \in \mathbb{N} \cup \{0\}$. Since $f(a') \equiv 0 \pmod{p^{2M+2+i}}$, it follows that $a'$ satisfies conditions (i) and (ii) for $i+1$, hence by the uniqueness result stated in the previous paragraph it follows that $a' \equiv a_{i+1} \pmod{p^{M+2+i}}$.

From $a' \equiv a_i \pmod{p^{M+1+i}}$ for all $i$ it follows that $a' = \lim_{i \to \infty} a_i = a$, as required.

(10) Let $f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34)$.

Claim 1: The equation $f(X) = 0$ has solutions in $\mathbb{R}$.

Proof. Clearly the solutions of $f(X) = 0$ in $\mathbb{R}$ are $X = \pm\sqrt{2}, \pm\sqrt{17}, \pm\sqrt{34}$.

Claim 2: The equation $f(X) = 0$ has solutions in $\mathbb{Q}_{17}$.
Proof. Let \( g(X) = X^2 - 2 \). Then \( a_1 = 6 \in \mathbb{Z} \subset \mathbb{Z}_{17} \) satisfies \( g(a_1) = 34 \equiv 0 \) (mod 17) and \( g'(a_1) = 12 \not\equiv 0 \) (mod 17). Therefore by Hensel’s lemma (Theorem 14.1) there exists \( a \in \mathbb{Z}_{17} \) such that \( g(a) = 0 \). This implies that \( f(a) = (a^2 - 2)(a^2 - 17)(a^2 - 34) = 0 \), i.e. \( f(X) = 0 \) has a solution in \( \mathbb{Z}_{17} \subset \mathbb{Q}_{17} \). □

Claim 3: The equation \( f(X) = 0 \) has solutions in \( \mathbb{Q}_p \) for every prime number \( p \) with \( p \neq 2 \) and \( p \neq 17 \).

Proof. We have \( \left( \frac{34}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{17}{p} \right) \), therefore at least one of the Legendre symbols \( \left( \frac{2}{p} \right), \left( \frac{17}{p} \right), \left( \frac{34}{p} \right) \) is equal to 1. Let \( c \in \{2, 17, 34\} \) be such that \( \left( \frac{c}{p} \right) = 1 \) and let \( g(X) = X^2 - c \). Then by the definition of the Legendre symbol there exists \( a_1 \in \mathbb{Z} \subset \mathbb{Z}_p \) such that \( g(a_1) = 0 \). This implies that \( f(a) = (a^2 - 2)(a^2 - 17)(a^2 - 34) = 0 \), i.e. \( f(X) = 0 \) has a solution in \( \mathbb{Z}_p \subset \mathbb{Q}_p \). □

Claim 4: The equation \( f(X) = 0 \) has solutions in \( \mathbb{Q}_2 \).

Proof. Let \( g(X) = X^2 - 17 \). Let \( a_0 = 1 \in \mathbb{Z} \subset \mathbb{Z}_2 \) and \( M = 1 \in \mathbb{N} \cup \{0\} \). Then \( g(a_0) = -16 \equiv 0 \) (mod \( 2^{2M+1} \)), \( g'(a_0) = 2 \equiv 0 \) (mod \( 2^{2M} \)) and \( g''(a_0) = 2 \not\equiv 0 \) (mod \( 2^{2M+1} \)). Therefore by the generalisation of Hensel’s lemma stated in Question (9) there exists \( a \in \mathbb{Z}_2 \) such that \( g(a) = 0 \). This implies that \( f(a) = (a^2 - 2)(a^2 - 17)(a^2 - 34) = 0 \), i.e. \( f(X) = 0 \) has a solution in \( \mathbb{Z}_2 \subset \mathbb{Q}_2 \). □

Claim 5: The equation \( f(X) = 0 \) has no solutions in \( \mathbb{Q} \).

Proof. In the proof of Claim 1 we listed all solutions of \( f(X) = 0 \) in \( \mathbb{R} \). Clearly all of these solutions are irrational, therefore \( f(X) = 0 \) has no solutions in \( \mathbb{Q} \). □