1. Let $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, and let ε be the fundamental unit. Thus $\mathcal{O}_K^* \cong \mu_2 \oplus \langle \varepsilon \rangle$ with $\varepsilon > 1$. There are two embeddings of K in $\mathbb{R}$: id and $\sigma : K \hookrightarrow \mathbb{R}$, where $\sigma(a+\sqrt{d}b) = a - \sqrt{d}b$.

But then

$$R_K = \left| \text{minor of } \begin{bmatrix} \log(\varepsilon) & \log|\sigma(\varepsilon)| \end{bmatrix} \right|$$

Since $|\sigma(\varepsilon)| = |\varepsilon| = \varepsilon$, we have $R_K = \log \varepsilon$.

2. a) $d_K = d(1, \theta, \theta^2) = \operatorname{disc}(x^3 - 11) = -3^3 \cdot 11^2$.

The primes that ramify in the extension $K/\mathbb{Q}$ are those dividing the discriminant.

Thus 3 and 11 are the ramified primes.

b) The class $[\mathfrak{b}]$ contains an integral ideal $\mathfrak{a}$ such that

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

$$= \frac{3!}{3^3} \cdot \frac{4}{\pi} \sqrt{3^3 \cdot 11^2} < 17,$$

by the Minkowski Bound theorem.

3. $p=2$: $\mathcal{O}_K/(2) \cong \frac{\mathbb{Z}[X]}{(2, X^3-11)} \cong \frac{\mathbb{F}_2[X]}{(X^3-1)} = \frac{\mathbb{F}_2[X]}{(X-1)(X^2+X+1)} \cong \mathbb{F}_2 \oplus \mathbb{F}_4$.

So $(2) = \mathfrak{p}_2 \mathfrak{p}_2'$ where $N(\mathfrak{p}_2) = 2$, $N(\mathfrak{p}_2') = 4$.

$p=5$: $X^3 - 11 \equiv (X-1)(X^2+X+1) \bmod 5$, so

$\mathcal{O}_K/(5) \cong \mathbb{F}_5 \oplus \mathbb{F}_{5^2}$.

Hence $(5) = \mathfrak{p}_5 \cdot \mathfrak{p}_5'$, $N(\mathfrak{p}_5) = 5$, $N(\mathfrak{p}_5') = 5^2$.

$p=7$: $X^3 - 11$ is irred. mod 7.

Hence $\mathcal{O}_K/(7) \cong \mathbb{F}_{7^3}$ and $\mathfrak{p}_7 = (7)$ is a prime ideal of norm 7^3.

$p=13$: $X^3 - 11$ irred. mod 13 $\Rightarrow$ (13) is prime in $\mathcal{O}_K$,

$N(\mathfrak{p}_{13}) = 13^3$

4. a) Compute minimal poly. of $\theta + k$:

$X = \theta + k \Rightarrow (X-k)^3 = 11$, so

$X^3 - 3X^2 + 3X - (k^3 + 11)$

is the minimal poly of $\theta + k$ over $\mathbb{Q}$.

Hence $N_{K/\mathbb{Q}}(\theta + k) = k^3 + 11$.

Similarly, get $N_{K/\mathbb{Q}}(\theta^2 - k) = k^3 + 121$

b) If $x \in R$ is such that $N_{K/\mathbb{Q}}(x) = 7$, where 7 is prime, then (x) is a prime ideal in $\mathcal{O}_K$ such that $N((x)) = 7$.

By a), $N_{K/\mathbb{Q}}(\theta) = 11$, $N_{K/\mathbb{Q}}(\theta - 2) = 3$.

Hence (θ) resp. $(\theta - 2)$ are prime ideals of norm 11 resp. 3.

$\mathfrak{p}_{11}$ " " $\mathfrak{p}_3$.

c) We have $(\theta - 2)^3 = 11 - 6\theta^2 + 12\theta - 8$

$= 3(1 + 4\theta - 2\theta^2)$.

The matrix of $1 + 4\theta - 2\theta^2$ is

$$\begin{pmatrix} 1 & 4 & -2 \\ -22 & 1 & 4 \\ 44 & -22 & 1 \end{pmatrix},$$

which has determinant 1. Hence $1 + 4\theta - 2\theta^2$ is a unit, and thus $\mathfrak{p}_3^3 = (\theta - 2)^3 = (3)$

Thus we know that $\mathfrak{p}_3$ is the only prime ideal dividing (3).

Similarly, $\mathfrak{p}_{11}^3 = (\theta)^3 = (11)$, so $\mathfrak{p}_{11}$ is the only prime ideal dividing (11).

d) By the above, Cl_K is generated by

$[\mathfrak{p}_2]$, $[\mathfrak{p}_2']$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$ and $[\mathfrak{p}_{11}]$,

as these are the prime ideals in $\mathcal{O}_K$ of norm < 17.

Now $[\mathfrak{p}_3] = 1 = [\mathfrak{p}_{11}]$ as $\mathfrak{p}_3$ and $\mathfrak{p}_{11}$ are principal.

Since $\mathfrak{p}_2 \mathfrak{p}_2' = (2)$ is principal, $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$ in Cl_K.

So the possible generators are $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$.

(4) By (a) we have $N_{K/\mathbb{Q}}(\theta - 1) = 10$,

so $(\theta - 1)$ is divisible by a prime ideal of norm 2 and a prime ideal of norm 5. Since these primes are unique, we find

$$\mathfrak{p}_2 \mathfrak{p}_5 = (\theta - 1).$$

Hence $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}$, so Cl_K is generated by $[\mathfrak{p}_2]$

5. Suppose that $\mathfrak{p}_2' = (\theta^2 - 5)$.

Then $(2) = \mathfrak{p}_2 \mathfrak{p}_2' = \mathfrak{p}_2 (\theta^2 - 5)$,

so $\mathfrak{p}_2 = \left(\frac{2}{\theta^2 - 5}\right)$. But $\frac{2}{\theta^2 - 5}$ is not integral over $\mathbb{Z}$ (since the minimal polynomial is not monic), hence $\frac{2}{\theta^2 - 5} \notin \mathcal{O}_K$. ↯

6. a) $\mathcal{O}_K^* \cong \mu_2 \oplus \mathbb{Z}$ by Dirichlet's unit theorem (as there is one real embedding and one conjugate pair of complex embeddings of K)

That v is a unit was shown in 4 c).

b) Since $\mathfrak{p}_3 = (\theta - 2)$, $2 \equiv \theta \bmod \mathfrak{p}_3$.

Hence $x = \pm v^\delta (\theta^2 - 5) \equiv \pm (1 + 8 - 8)^\delta (4 - 5)$

$\equiv \pm (-1) \bmod \mathfrak{p}_3$.

Since $x \equiv \square \bmod \mathfrak{p}_3$, and since $\mathcal{O}_K/\mathfrak{p}_3 \cong \mathbb{Z}/3$, in which $1 \in \mathbb{Z}/3$ is the only square, we must have $x \equiv 1 \bmod \mathfrak{p}_3$. Thus $x = -v^\delta(\theta^2 - 5)$.

c) $N_{K/\mathbb{Q}}(\theta + 3) = 2 \cdot 19$, so $(\theta + 3)$ is divisible by a prime ideal $\mathfrak{p}_{19}$ of norm 19.

d) We have $\theta \equiv -3 \bmod \mathfrak{p}_{19}$,

so $x \equiv -(1 + 4(-3) - 2(-3)^2)^\delta ((-3)^2 - 5)$

$= -9^\delta \cdot 4 \bmod \mathfrak{p}_{19}$.

We know $x \equiv \square \bmod \mathfrak{p}_{19}$.

Now both 9^δ and 4 are squares in $\mathcal{O}_K/\mathfrak{p}_{19} \cong \mathbb{Z}/19$.

But -1 is not a square mod 19:

$\left(\frac{-1}{19}\right) = (-1)^{\frac{19-1}{2}} = -1$.

This is a contradiction, so $\mathfrak{p}_2$ cannot be principal.

Hence $Cl_K \cong \mathbb{Z}/2\{[\mathfrak{p}_2]\}$.

(6)

7. Clearly $3 = 0^2 + 3 \cdot 1^2$ is of the given form.

On the other hand, $x^2 + 3y^2 = 2$ has no integer solutions. So we may assume that $p > 3$ is an odd prime.

Then $p = n^2 + 3m^2 \iff (p)$ splits in the extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$

$\iff -3$ is a square mod p,

i.e., $\left(\frac{-3}{p}\right) = 1$.

Now, by quadratic reciprocity,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = \begin{cases} 1 \cdot \left(\frac{p}{3}\right), & p \equiv 1 \ (4) \\ (-1)\cdot(-1)\left(\frac{p}{3}\right), & p \equiv 3 \ (4). \end{cases}$$

Hence $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ for all $p > 3$,

and $\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \ (3)$, since 1 is the only square mod 3.

8. We know: For any ideal $\alpha \subseteq \mathcal{O}_K$,

$$1 \le N(\alpha) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

Hence $$\sqrt{|d_K|} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}$$

Let $f_n = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}$.

Then $f_2 > 1$ while

$$\frac{f_{n+1}}{f_n} = \frac{(n+1)!}{(n+1)^{n+1}}\left(\frac{\pi}{4}\right)^{-\frac{n+1}{2}} \cdot \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}$$

$$= \sqrt{\frac{\pi}{4}}\left(1+\frac{1}{n}\right)^n > 1.$$

So f_n is an increasing sequence with $f_2 > 1$. Hence, if $[K:\mathbb{Q}] > 1$ we have $|d_K| > 1$. It follows that d_K is divisible by some rational prime, i.e., the extension $K/\mathbb{Q}$ is ramified.

9. Suppose that $\mathfrak{p} \subset \mathcal{O}_K$ is inert in L/K, so $\mathfrak{P} := \mathfrak{p}\mathcal{O}_L$ is prime.

- Since $\mathfrak{p}$ is nonsplit, the decomposition group $G_{\mathfrak{P}}$ equals the Galois group $\mathrm{Gal}(L/K)$.
- Since $\mathfrak{p}$ is inert, it is in particular unramified, so the inertia group $I_{\mathfrak{P}}$ is trivial.

But then the map

$$G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}\left(k(\mathfrak{P})/k(\mathfrak{p})\right)$$

is an isomorphism.

- Hence $\mathrm{Gal}(L/K) \cong \mathrm{Gal}\left(k(\mathfrak{P})/k(\mathfrak{p})\right)$.

Now $k(\mathfrak{P})/k(\mathfrak{p})$ is a finite extension of finite fields, hence $\mathrm{Gal}\left(k(\mathfrak{P})/k(\mathfrak{p})\right)$ is cyclic.

10. Since $\mathfrak{p} \subseteq \mathcal{O}_K$ is unramified,

$I_{\mathfrak{q}} = 0$. Hence $G_{\mathfrak{q}} \cong \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \subseteq \mathrm{Gal}(L/K)$.

Now $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ is cyclic of order $[k(\mathfrak{q}) : k(\mathfrak{p})]$. Thus there is a unique element

$$\mathrm{Frob}_{\mathfrak{q}} \in \mathrm{Gal}(L/K)$$

corresponding to the generator of $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ that acts as the Frobenius endomorphism on $k(\mathfrak{q})$.