Exercise 1. Let $\mathbb{A}(d)$ be any quadratic ring and let
\[ \omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \mod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4. \end{cases} \]
Prove that for every element $x \in \mathbb{A}(d)$ there are $a, b \in \mathbb{Z}$ such $x = a + b\omega$.

Solution. We first need to notice that $d \equiv 0 \mod 4$ is not possible since $d$ is square-free. Now we take $x \in \mathbb{A}(d)$, so, for $a$ and $b$ rationals, $x = a + b\sqrt{d}$ and because it is an element of the quadratic ring, $2a$ and $a^2 - b^2d$ are integers.

Our first step will be to conclude that $2b$ is also an integer. For this, we notice that $4b^2d$ is also an integer, so by taking $b = p/q$ with $(p, q) = 1$ and $q > 1$, the above will imply that $q^2|4p^2d$ but since $(p^2, q^2) = 1$ and $d$ is square-free, $q^2|4$. In that case, either $q = 1$ or $q = 2$ and this allows us to conclude that $2b$ is an integer as desired.

Knowing this, we define the integers $u = 2a$ and $v = 2b$. We have then $u^2 \equiv v^2d \mod 4$. We analyze now the different cases:

- If $d \equiv 2 \mod 4$, we will have
  \[ u^2 \equiv 2v^2 \mod 4, \]
  and in consequence, $u^2$ will be even making also $u$ even; in that case $v^2$ is also even and $v$ in consequence. In such a case, $a$ and $b$ will be integers, thus
  \[ a + b\omega = a + b\sqrt{d} = x \]
  as desired.

- If $d \equiv 3 \mod 4$, we will have
  \[ u^2 \equiv 3v^2 \mod 4. \]
  We need to notice that either $u$ and $v$ are both even or both odd; if they are odd, then
  \[ u^2 \equiv 1 \equiv v^2 \mod 4 \]
  leading to
  \[ 1 \equiv 3 \mod 4, \]
  a contradiction; thus both are even, again $a$ and $b$ are integers and we conclude the same as before.
If \( d \equiv 1 \mod 4 \), we will have
\[
  u^2 \equiv v^2 \mod 4.
\]
Again, they, \( u \) and \( v \), are both even or both odd. In any of these cases \( u - v \) is even so we take \( a' = (u - v)/2 \) and \( b' = v \), both integers, and we have
\[
  a' + b' \omega = \frac{u - v}{2} + v \left( \frac{1 + \sqrt{d}}{2} \right)
  = \frac{u}{2} + \frac{v}{2} \sqrt{d}
  = a + b \sqrt{d}
  = x.
\]

**Exercise 2.** Let \( \mathbb{Q}(\sqrt{d}) \) is a quadratic number field.

(a) Show that the norm is multiplicative, i.e., if \( x, y \in \mathbb{Q}(\sqrt{d}) \) then we have \( N(xy) = N(x)N(y) \).

*Solution.* It is enough to proof that \( \overline{xy} = \overline{x} \overline{y} \), since if it is the case
\[
  N(xy) = (xy)(\overline{xy})
  = x\overline{y} \overline{x}y
  = \overline{x} \overline{y} \overline{x}y
  = N(x)N(y).
\]
We prove then our claim: For \( x = a + b\sqrt{d} \) and \( y = e + f\sqrt{d} \) and since \( xy = ae + bfd + (be + af)\sqrt{d} \),
\[
  \overline{xy} = (a - b\sqrt{d})(e - f\sqrt{d})
  = ae + bfd - (be + af)\sqrt{d}
  = \overline{xy}.
\]

(b) Show that if \( n \in \mathbb{N} \) and \( x \in \mathbb{Q}(\sqrt{d}) \) then \( N(nx) = n^2 N(x) \).

*Solution.* If \( n \in \mathbb{N} \), we need to notice that \( \overline{n} = n \). Thus, \( N(n) = n^2 \) and
\[
  N(nx) = N(n)N(x)
  = n^2 N(x).
\]

(c) Show that if \( d \leq 1 \) then \( N(x) \geq 0 \) for any \( x \in \mathbb{Q}(\sqrt{d}) \).
Solution. Taking \( x = a + b\sqrt{d} \) with \( a \) and \( b \) rationals, we can write
\[
N(x) = a^2 - b^2d \\
= a^2 + b^2|d| \\
\geq 0
\]

(d) Show that if \( x \in \mathbb{A}(d) \) is a unit, then \( N(x) = \pm 1 \).

Solution. If \( x \) is a unit, then there is an element \( y \in \mathbb{A}(d) \) such that \( xy = 1 \), thus
\[
N(x)N(y) = N(xy) = N(1) = 1.
\]

But \( N(x) \) and \( N(y) \) are integers because \( x \) and \( y \) are elements of \( \mathbb{A}(d) \) so the only possibilities are \( N(x) = N(y) = -1 \) or \( N(x) = N(y) = 1 \).

Exercise 3. Let \( n, k \) and \( a \) be natural numbers with \( a > 1 \). Show that the integral solutions to Pell’s equation can be computed recursively by
\[
x_{nk}(a) + y_{nk}(a)\sqrt{a^2 - 1} = (x_n(a) + y_n(a)\sqrt{a^2 - 1})^k.
\]

Conclude that, writing \( x_s = x_s(a) \) and \( y_s = y_s(a) \), that
\[
y_{nk} = \sum_{i=1}^{k} \binom{k}{i} (x_n)^{k-i}(y_n)^{i}(a^2 - 1)^{(i-1)/2}.
\]

Solution. By definition,
\[
x_{nk} + y_{nk}\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^{nk} \\
= ((a + \sqrt{a^2 - 1})^n)^k \\
= (x_n + y_n\sqrt{a^2 - 1})^k.
\]

Now, by using the binomial theorem
\[
x_{nk} + y_{nk}\sqrt{a^2 - 1} = \sum_{i=0}^{k} \binom{k}{i} (x_n)^{k-i}(y_n)^{i}(a^2 - 1)^{i/2};
\]
since \( \sqrt{a^2 - 1} \) is irrational and \( (a^2 - 1)^{i/2} \) will be an integer whenever \( i \) is even,
\[
y_{nk} = \sum_{i=1}^{k} \binom{k}{i} (x_n)^{k-i}(y_n)^{i}(a^2 - 1)^{(i-1)/2}.
\]
Exercise 4. Let \( A(d) \) be any quadratic ring and let \( y \in A(d) \). Show that if \( y^2 \in \Q \), then \( y^2 \in \Z \). Furthermore, show that if \( d > 1 \), \( y^2 \in \N \).

Solution. We write \( y = a + b\sqrt{d} \), with \( a, b \in \Q \); if \( y^2 \) is a rational number we will have

\[
a^2 + b^2d + 2ab\sqrt{d} \in \Q.
\]

Thus \( a = 0 \) or \( b = 0 \). In that case,

\[
y^2 = -a^2 + b^2d = -N(y)
\]

or

\[
y^2 = a^2 - b^2d = N(y).
\]

Since \( y \) is an element of the quadratic ring, \( N(y) \) is an integer so in either case, we have to conclude that \( y^2 \in \Z \). In particular, if \( d > 1 \), we have \( y \in \R \) and thus \( y^2 \geq 0 \); we have then \( y^2 \in \N \).

Exercise 5. Let \( A(d) \) be any imaginary quadratic ring.

(a) Show that the only possible units are

\[\pm 1, \pm i, \frac{\pm 1 \pm i\sqrt{3}}{2}.\]

Solution. Since the ring is imaginary, for any element \( u \), \( N(u) \geq 0 \) and thus, \( u \) is a unit if and only if \( N(u) = 1 \). Let \( a \) and \( b \) be integers such that \( u = a + bw \); if \( b = 0 \), \( u \) is a unit if and only if \( u = 1 \) or \( u = -1 \). With this, we will \( b \) different than \( 0 \).

Allow \( d < -4 \), then

\[N(u) = a^2 + b^2|d|\]

or

\[N(u) = \frac{(2a + b)^2}{4} + \frac{b^2}{4}|d|.
\]

In either case, because \( b^2 \geq 1 \), the norm \( N(u) > 1 \). We need to conclude that an element \( u \) in the quadratic ring with \( b \neq 0 \) cannot be a unit.

We restrict, then, our attention to the cases \( d = -1 \), \( d = -2 \) and \( d = -3 \) (excluding \( d = -4 \) because it is divided by a perfect square)

- When \( d = -1 \), \( N(u) = a^2 + b^2 \), so if we assume \( u \) a unit, we have

\[
1 = a^2 + b^2 \geq a^2 + 1.
\]

Thus \( a = 0 \), \( b^2 = 1 \) and in consequence \( u = \pm \sqrt{-1} \).

- When \( d = -2 \),

\[
N(u) = a^2 + 2b^2 \geq a^2 + 2 > 1.
\]

So there are no units with \( b \neq 0 \).
• When $d = -3$,

$$
1 = N(u)
= \frac{(2a + b)^2}{4} + \frac{b^2}{4}.
$$

So

$$(2a + b)^2 + 3b^2 = 4;$$

we need to notice that $b^2 > 1$ is a contradiction with the above, we conclude $b^2 \leq 1$, but $b$ is already not zero so we will have $b^2 = 1$; in that case $(2a + b)^2 = 1$ and this will yield four possibilities: $a = 0$ and $b = 1$, $a = 0$ and $b = -1$, $a = 1$ and $b = -1$ or $a = -1$ and $b = 1$. In turn

$$
u = \pm 1 \pm \frac{\sqrt{-3}}{2}.
$$

With the cases exhausted, the proof is complete.

(b) Use this to prove that the fact that $5h + 2$ is a unit, for $h \in \mathbb{A}(d)$, is contradictory.

Solution. We notice first that the case where $\pm i$ are possible as units happens when $d = -1$, in that case $\omega = \sqrt{d}$ so we will have $\pm \omega$ as these units.

Also, if

$$
\frac{\pm 1 \pm \sqrt{-3}}{2}
$$

happen, we will have $d = -3$, so $\omega = (1 + \sqrt{-3})/2$; in that case the possible units are $\omega, -\omega, 1 - \omega$ and $-1 + \omega$. In that light, if $e + f\omega$ is a unit of the quadratic ring $\mathbb{A}(d)$ for any square-free integer $d$, then $e = 1, e = -1$ or $e = 0$.

Now, if $h = a + b\omega$ is any element of the quadratic ring, with $a$ and $b$ integers,

$$
5h + 2 = (5a + 2) + 5b\omega
$$

but $5a + 2 \neq 1$, $5a + 2 \neq -1$, and $5a + 2 \neq 0$, thus $5h + 2$ is not a unit of the quadratic ring. Since $h$ was taken arbitrary, $5h + 2$ being a unit is contradictory.