Let $K = \mathbf{Q}[\sqrt{d}]$ be a quadratic field with squarefree $d \in \mathbf{Z}$. We call $\alpha \in K$ an *integer* of K if the quadratic polynomial

$$f_\alpha(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}$$

has integral coefficients. Writing $\alpha = r + s\sqrt{d}$ with $r, s \in \mathbf{Q}$, we have $f_\alpha(X) = X^2 - 2rX + (r^2 - ds^2)$, so α is an integer of $\mathbf{Q}[\sqrt{d}]$ when $2r \in \mathbf{Z}$ and $r^2 - ds^2 \in \mathbf{Z}$.

Example 1. If a and b are in $\mathbf{Z}$ then $a + b\sqrt{d}$ is an integer of $\mathbf{Q}[\sqrt{d}]$.

Example 2. If $\alpha = \frac{1+\sqrt{5}}{2}$ then $f_\alpha(X) = X^2 - X - 1 \in \mathbf{Z}[X]$, so $\frac{1+\sqrt{5}}{2}$ is an integer of $\mathbf{Q}[\sqrt{5}]$.

Theorem 1. *When d is a squarefree integer and $K = \mathbf{Q}[\sqrt{d}]$, the integers of K are*

$$\begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{d}, & \text{if } d \equiv 2, 3 \bmod 4. \\ \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

We don't have the case $d \equiv 0 \bmod 4$ since those d are not squarefree!

Proof. First we check that any number in the indicated set, depending on $d \bmod 4$, is an integer of $\mathbf{Q}[\sqrt{d}]$. This is clear when $d \equiv 2, 3 \bmod 4$ by Example 1. When $d \equiv 1 \bmod 4$, a number of the form $\alpha = a + b\frac{1+\sqrt{d}}{2} = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}$ with $a, b \in \mathbf{Z}$ has

$$f_\alpha(X) = X^2 - (2a + b)X + \left(a^2 + ab + b^2\frac{1-d}{4}\right) \in \mathbf{Z}[X].$$

Conversely, we now show that any integer of $\mathbf{Q}[\sqrt{d}]$ has to be a number in the indicated set, depending on $d \bmod 4$. Suppose $r + s\sqrt{d}$ is an integer of $\mathbf{Q}[\sqrt{d}]$. Then $2r \in \mathbf{Z}$ and $r^2 - ds^2 \in \mathbf{Z}$. Set $a = 2r$, so $a \in \mathbf{Z}$ and $r = a/2$. Therefore $a^2/4 - ds^2 \in \mathbf{Z}$, so $a^2 - d(2s)^2 \in 4\mathbf{Z}$, which implies $d(2s)^2 \in \mathbf{Z}$. Since d is squarefree, the only way $d(2s)^2$ could be in $\mathbf{Z}$ is if $2s \in \mathbf{Z}$: a denominator in $2s$ when this fraction is written in reduced form can't be cancelled out in $d(2s)^2$ because primes in d appear just once. Set $b = 2s$, so $b \in \mathbf{Z}$ and $s = b/2$. Thus

$$r + s\sqrt{d} = \frac{a}{2} + \frac{b}{2}\sqrt{d} \quad \text{and} \quad a^2 - db^2 \in 4\mathbf{Z}.$$

We can write the second condition as $a^2 \equiv db^2 \bmod 4$.

If a is even then $db^2 \equiv 0 \bmod 4$, which implies b is even (there is at most one 2 appearing in d and db^2 needs at least two 2's in it), so $\frac{a}{2} + \frac{b}{2}\sqrt{d} \in \mathbf{Z} + \mathbf{Z}\sqrt{d}$.

If a is odd then $a^2 \equiv 1 \bmod 4$, so $db^2 \equiv 1 \bmod 4$. This implies b is odd (if it were even then $db^2 \equiv 0 \bmod 4$) and therefore $d \equiv 1 \bmod 4$.

So any integer in $\mathbf{Q}[\sqrt{d}]$ either is in $\mathbf{Z} + \mathbf{Z}\sqrt{d}$ or has the form $\frac{a}{2} + \frac{b}{2}\sqrt{d}$ with odd a and b and $d \equiv 1 \bmod 4$.

Thus if $d \not\equiv 1 \bmod 4$ then $r + s\sqrt{d} \in \mathbf{Z} + \mathbf{Z}\sqrt{d}$.

If $d \equiv 1 \bmod 4$ and $r + s\sqrt{d}$ is not in $\mathbf{Z} + \mathbf{Z}\sqrt{d}$ then for some odd a and b we have

$$r + s\sqrt{d} = \frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} \in \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}.$$

Since $\sqrt{d} = -1 + 2\frac{1+\sqrt{d}}{2} \in \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}$ we have $\mathbf{Z} + \mathbf{Z}\sqrt{d} \subset \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}$, so every integer of $\mathbf{Q}[\sqrt{d}]$ is in $\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}$ when $d \equiv 1 \bmod 4$.

■