Problem. Let d be a squarefree integer and let

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Show that the set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\omega_d]$.

Solution. It is easy to see that $\mathbb{Z}[\omega_d] = \{a + b\,\omega_d : a, b \in \mathbb{Z}\}$ as $\omega_d^2 = d$ if $d \equiv 2,3 \pmod 4$ and $\omega_d^2 = (d-1)/4 + \omega_d$ if $d \equiv 1 \pmod 4$. Now let $\alpha = p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Let $q \neq 0$ and let $x^2 + ax + b \in \mathbb{Q}[x]$ be the irreducible polynomial of α over $\mathbb{Q}$. Plugging in α we get

$$0 = \alpha^2 + a\alpha + b = (p + q\sqrt{d})^2 + a(p + q\sqrt{d}) + b = (p^2 + q^2 d + ap + b) + (2pq + aq)\sqrt{d}.$$

Comparing the coefficients we get

$$p^2 + q^2 d + ap + b = 0 \quad \text{and} \quad 2pq + aq = 0.$$

Because $q \neq 0$ we obtain $a = -2p$ and $b = p^2 - q^2 d$. Thus α is an algebraic integer if and only if $2p$ and $p^2 - q^2 d$ are both integers. We now treat the cases $d \equiv 2,3 \pmod 4$ and $d \equiv 1 \pmod 4$ separately.

Suppose that $d \equiv 2,3 \pmod 4$. Note that $\mathbb{Z}[\sqrt{d}]$ consists only of algebraic integers for if $p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ (with $q \neq 0$), then $2p$ and $p^2 - q^2 d$ are clearly integers.

Now let $p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ be an algebraic integer. If $q = 0$, then p must be integer and so $p + q\sqrt{d} = p \in \mathbb{Z}[\sqrt{d}]$. If $q \neq 0$, then $a = 2p$ and $b = p^2 - q^2 d$ are both integers. Substituting a into b we get that $a^2/4 - q^2 d = (a^2 - 4q^2 d)/4$ is an integer. In particular, $4q^2 d$ is an integer. This implies that q is a half-integer. To see this take $q = r/s$, where r and s are coprime integers. Then $s^2 \,|\, 4r^2 d$ and so $s^2 \,|\, 4d$. Because d is squarefree it follows that $s^2 \,|\, 4$ and so $s \,|\, 2$. Let $q = c/2$, where c is an integer. Then we have

$$a^2 - c^2 d \equiv 0 \pmod 4.$$

Because $d \equiv 2,3 \pmod 4$, it follows that $a^2 \equiv c^2 \equiv 0 \pmod 4$ for if $c^2 \equiv 1 \pmod 4$, then $a^2 \equiv 2,3 \pmod 4$, a contradiction as 0 and 1 are the only quadratic residues mod 4. Hence a and c are both even and as a consequence $p = a/2$ and $q = c/2$ are both integers. Thus $p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Now suppose that $d \equiv 1 \pmod 4$. Let $a + b\omega_d \in \mathbb{Z}[\omega_d]$. Then

$$a + b\omega_d = \left(\frac{2a+b}{2}\right) + \frac{b}{2}\sqrt{d}.$$

Let $p + q\sqrt{d} = a + b\omega_d$, where $p, q \in \mathbb{Q}$. If $b = 0$, then $a + b\omega_d = a$ is clearly an algebraic integer. Now if $b \neq 0$, then $q \neq 0$ and

$$2p = 2a + b \quad \text{and} \quad p^2 - q^2 d = \frac{4a^2 + b^2 + 4ab}{4} - \frac{b^2 d}{4} = a^2 + ab + b^2\left(\frac{1-d}{4}\right)$$

are both integers. Hence, $a + b\omega_d$ is an algebraic integer.

Now suppose that $p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer. Again if $q = 0$, then p must be an integer and so $p + q\sqrt{d} = p \in \mathbb{Z}[\omega_d]$. If however $q \neq 0$, then $a = 2p$ and $b = p^2 - q^2 d$ must be integers. Just as before q must be half-integer so let $q = c/2$, where c is an integer. Again we have

$$a^2 - c^2 d \equiv 0 \pmod 4.$$

Because $d \equiv 1 \pmod 4$ we get $a^2 = c^2 \pmod 4$. This implies that $a \equiv c \pmod 2$ and so we have

$$p + q\sqrt{d} = \frac{a}{2} + \frac{c}{2}\sqrt{d} = \frac{a-c}{2} + c\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\omega_d].$$