

Solution 1.

The painful ‘nitty gritty’ proof:

Note that $\mathbb{Q}[x, y]$ is a UFD (as $\mathbb{Q}[x]$ is a UFD, $\mathbb{Q}[x, y] \cong \mathbb{Q}[x][y]$ and a polynomial ring over a UFD is a UFD), furthermore in a UFD a non-zero principal ideal is prime iff its generator is irreducible. Thus, it suffices to show that $x^2 - y^3$ is irreducible over $\mathbb{Q}[x, y]$. We will view $A = \mathbb{Q}[x, y]$ as $\mathbb{Q}[y][x]$, i.e the polynomial ring in one indeterminate x over the ring $\mathbb{Q}[y]$. Suppose $x^2 - y^3$ is reducible then there exist polynomials $p_1, p_2 \in A$ such that $x^2 - y^3 = p_1 p_2$. As $\mathbb{Q}[y]$ is an integral domain we have that either both p_1 and p_2 have degree 1 or one of them has degree 2 and the other degree 0. We deal with the latter case first. Assuming without loss of generality that p_1 has degree 0, we have

$$x^2 - y^3 = q_1(y)(q_2(y)x^2 + q_3(y)x + q_4(y)),$$

here $p_1 = q_1(y)$, and $q_1(y), q_2(y), q_3(y), q_4(y) \in \mathbb{Q}[y]$. Now looking at the degree of $q_1(y)$ in $\mathbb{Q}[y]$ and the coefficient of x^2 we have that $q_1(y)$ (and consequently p_1) is a unit.

If both p_1 and p_2 have degree 1 then

$$\begin{aligned} x^2 - y^3 &= (q_1(y)x + q_2(y))(q_3(y)x + q_4(y)) \\ &= q_1(y)q_3(y)x^2 + (q_1(y)q_4(y) + q_2(y)q_3(y))x + q_2(y)q_4(y) \end{aligned}$$

for some $q_1(y), q_2(y), q_3(y), q_4(y) \in \mathbb{Q}[y]$. So $q_1(y)q_3(y) = 1$ forcing $q_1(y)$ and $q_3(y)$ to be units; also $q_2(y)q_4(y) = y^3$ and using unique factorization in $\mathbb{Q}[y]$ we have that either, (without loss of generality) $q_2(y) = k$, $q_4(y) = \frac{1}{k}y^3$ or (again without loss of generality) $q_2(y) = ky$, $q_4(y) = \frac{1}{k}y^2$, for some $k \in \mathbb{Q}^\times$. Both cases lead to a contradiction when we note that $q_1(y)q_4(y) + q_2(y)q_3(y) = 0$ and that $q_1(y), q_3(y)$ are units.

Thus, $\mathfrak{p} = x^2 - y^3$ is irreducible over A and A/\mathfrak{p} is an integral domain. To see that it is not integrally closed consider the polynomial $T^3 - \bar{x}$, this has a root in $\text{Frac}(A/\mathfrak{p})$, namely $\frac{\bar{x}}{\bar{y}}$, (\bar{x}, \bar{y} denote the image of x, y respectively in A/\mathfrak{p}). However, clearly $\frac{\bar{x}}{\bar{y}}$ is not in A/\mathfrak{p} .

The slick proof (sketch):

The map $x \rightarrow t^3$ and $y \rightarrow t^2$ induces a ring homomorphism $\phi : \mathbb{Q}[x, y] \rightarrow \mathbb{Q}[t]$. Now note that an element in $\mathbb{Q}[x, y]$ differs from an element in $(x^2 - y^3)$ by a polynomial $p(x, y)$ of degree at most 2 in y , furthermore the exponents of $\phi(x^r y^s)$ are distinct for $0 \leq s \leq 2$. These two facts show that $\ker(\phi) = (x^2 - y^3)$, thus $\mathbb{Q}[x, y]/(x^2 - y^3)$ is isomorphic to a subring of $\mathbb{Q}[t]$ which being an integral domain implies that $(x^2 - y^3)$ is prime. \square

Solution 2.

Let A, B, α, β be as stated in the problem. It suffices to show (by Proposition 2.11, Milne) that there exists a finitely generated A -submodule, say M , of B such that $\alpha M \subset M$. Now as $\alpha \in A[\beta] \cap A[\beta^{-1}]$ we have that

$$\begin{aligned} \alpha &= a_n \beta^n + a_{n-1} \beta^{n-1} + \cdots + a_0 \\ \text{and } \alpha &= b_m \beta^{-m} + b_{m-1} \beta^{-m+1} + \cdots + b_0 \end{aligned}$$

where $a_0, \dots, a_n, b_0, \dots, b_m \in A$. Let M be the A -module generated by $\{\beta^n, \beta^{n-1}, \dots, 1, \beta^{-1}, \dots, \beta^{-m}\}$. We claim that $\alpha M \subset M$. It suffices to show that $\alpha\beta^i \in M$ for $-m \leq i \leq n$. Clearly, $\alpha \cdot 1 = \alpha \in M$. If $-m \leq i < 0$ then using the first representation for α we have that

$$\alpha\beta^i = a_n\beta^{n+i} + a_{n-1}\beta^{n-1+i} + \dots + a_0\beta^i$$

every term in this sum lies in M . Similarly, if $0 < i \leq n$ then using the second representation for α we have that

$$\alpha\beta^i = b_m\beta^{-m+i} + b_{m-1}\beta^{-m+1+i} + \dots + b_0\beta^i$$

every term in this sum too lies in M . Thus, $\alpha M \subset M$ as required. \square

Solution 3.

Yes, $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ is an algebraic integer as it is a root of the monic polynomial $x^2 + 6x + 3$. (Furthermore, $\frac{3+2\sqrt{6}}{1-\sqrt{6}} = \frac{3+2\sqrt{6}}{1-\sqrt{6}} \cdot \frac{1+\sqrt{6}}{1+\sqrt{6}} = \frac{15+5\sqrt{6}}{-5} = -3 - \sqrt{6}$ which being the sum of two algebraic integers must also be an algebraic integer.) \square

Solution 4.

We will assume $d \neq 0, 1$ and squarefree throughout. An element of $\mathbb{Q}[\sqrt{d}]$ is integral over \mathbb{Z} (and hence in the ring of integers of $\mathbb{Q}[\sqrt{d}]$ iff its minimum polynomial over \mathbb{Q} has coefficients in \mathbb{Z} (Proposition 2.9, Milne). The minimum polynomial of $\alpha = r + s\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, $r, s \in \mathbb{Q}$, $s \neq 0$ is given by

$$X^2 - 2rX + (r^2 - s^2d)$$

Thus α is in the ring of integers iff

$$2r \in \mathbb{Z}, \quad r^2 - s^2d \in \mathbb{Z}$$

Suppose α is in the ring of integers, then $4(r^2 - s^2d) = (2r)^2 - (2s)^2d \in \mathbb{Z}$, and as $2r \in \mathbb{Z}$ we have that $(2s)^2d \in \mathbb{Z}$, but as d is squarefree and $2s \in \mathbb{Q}$ we have that $(2s)^2 \in \mathbb{Z}$, consequently we have that $2s \in \mathbb{Z}$. Furthermore

$$4(r^2 - s^2d) = (2r)^2 - (2s)^2d \equiv 0 \pmod{4}$$

If $d \equiv 2, 3 \pmod{4}$ then (as squares are always $\equiv 0$ or $\equiv 1 \pmod{4}$) we get that $(2r)^2 \equiv (2s)^2 \equiv 0 \pmod{4}$. Consequently $2r$ and $2s$ are even rational integers, making r and s rational integers. If $d \equiv 1 \pmod{4}$ then (proceeding as above) we get that either $(2r)^2 \equiv (2s)^2 \equiv 0 \pmod{4}$ and consequently $r, s \in \mathbb{Z}$; or that $(2r)^2 \equiv (2s)^2 \equiv 1 \pmod{4}$ and $r = \frac{2m+1}{2}, s = \frac{2n+1}{2}, m, n \in \mathbb{Z}$.

We have so far thus shown that if $d \equiv 2, 3 \pmod{4}$ then

$$\alpha \in \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}$$

and if $d \equiv 1 \pmod{4}$ then

$$\alpha \in \left\{ \frac{2m+1 + (2n+1)\sqrt{d}}{2} \mid m, n \in \mathbb{Z} \right\} \cup \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}$$

the latter of which is also equivalent to saying that

$$\alpha \in \left\{ m + n \left(\frac{1 + \sqrt{d}}{2} \right) \mid m, n \in \mathbb{Z} \right\}$$

Conversely if $\alpha \in \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}$ then clearly α is in the ring of integers of $\mathbb{Q}[\sqrt{d}]$, and if $d \equiv 1 \pmod{4}$ then for $\beta = \frac{n(1+\sqrt{d})}{2}, n \in \mathbb{Z}$, set

$$f(x) = X^2 - nX + \frac{n^2(1-d)}{4}$$

and note that $\frac{n^2(1-d)}{4} \in \mathbb{Z}$ as $d \equiv 1 \pmod{4}$. Now $f(\beta) = 0$ and thus β is integral over \mathbb{Z} and consequently the set

$$\left\{ m + n \left(\frac{1 + \sqrt{d}}{2} \right) \mid m, n \in \mathbb{Z} \right\}$$

is also contained in the ring of integers if $d \equiv 1 \pmod{4}$.

To sum up, the ring of integers for $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod{4}$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod{4}$. \square

Solution 5.

Let A, K and $f(x)$ be as stated in the problem. Then

$$f(x) = p_1(x)p_2(x)$$

for some $p_1(x), p_2(x) \in K[x]$ where $p_1(x)$ and $p_2(x)$ are not units. Furthermore, we may assume that $p_1(x)$ and $p_2(x)$ are monic. Let L be a splitting field of $f(x)$ over K . Then

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

for some $\alpha_i \in L, 1 \leq i \leq n$. Now each α_i is integral over A (it is a root of the monic polynomial $f(x) \in A[x]$, thus the ring $R = A[\alpha_1, \dots, \alpha_n]$ is integral over A . Also, each coefficient of $p_1(x)$ and $p_2(x)$ lies in R and is thus also integral over A , but these coefficients also lie in K and as A is integrally closed we have that they lie in A and thus $p_1(x), p_2(x) \in A[x]$ as required. \square