Solution 1.
Note that $\mathbb{Z}$ is Noetherian, hence by the Hilbert basis theorem $\mathbb{Z}[x]$ is also Noetherian. Furthermore $\mathbb{Z}$ is a UFD and a polynomial ring over a UFD is also a UFD (cf. Dummit and Foote 3rd edition, Theorem 7, p.304), hence $\mathbb{Z}[x]$ is a UFD. But UFDs are integrally closed (cf. Dummit and Foote 3rd edition, p. 693), hence $\mathbb{Z}[x]$ is integrally closed. However, $\mathbb{Z}[x]$ is not a Dedekind domain as the ideal (x) is clearly prime in $\mathbb{Z}[x]$ but not maximal as $(x) \subsetneq (x, 5) \subsetneq \mathbb{Z}[x]$. □

Solution 2. Note that by the structure theorem on free modules over PIDs we have that if G is a free $\mathbb{Z}$-module of rank n and H a $\mathbb{Z}$-submodule of G with rank $s \leq n$, then there exists a basis $u_1, \ldots, u_n$ for G and positive integers $\alpha_1, \ldots, \alpha_s$ such that $\alpha_1 u_1, \ldots, \alpha_s u_s$ is a basis for H. From this it is clear that G/H (G and H by virtue of being $\mathbb{Z}$-modules are free abelian groups, so I am looking at the quotient group here) is the direct product of finite cyclic groups of order $\alpha_1, \ldots, \alpha_s$ and $n - s$ infinite cyclic groups. Hence, $|G : H = |G/H|$ is finite if and only if $n = s$.

Also note that with R as stated in the problem as $1 \in R$ we have that $\mathbb{Z} \subseteq R$.

$(a \Rightarrow b)$

Note that O_K is a free $\mathbb{Z}$-module (i.e a free abelian group) of rank $n = [K : \mathbb{Q}]$ and R is a $\mathbb{Z}$-submodule of O_K (i.e subgroup). But subgroups of free abelian groups are free abelian themselves. Moreover, a subgroup of a free abelian group has finite index iff the rank of the subgroup is equal to the rank of the group (by the remark we made at the very beginning). Thus, the rank of R is also n. This means that there exists a basis $\{e_1, \ldots, e_n\}$ for R over $\mathbb{Z}$, however these elements must stay linearly independent over $\mathbb{Q}$ too (if a non trivial linear combination of them over $\mathbb{Q}$ was 0 then we could clear denominators to obtain a non trivial linear combination that was 0 over $\mathbb{Z}$). But K is a vector space of dimension n over $\mathbb{Q}$ thus the set $\{e_1, \ldots, e_n\}$ is a basis for K over $\mathbb{Q}$. Hence, R contains a basis of K over $\mathbb{Q}$.

$(b \Rightarrow c)$

So assume R contains a basis $\{e_1, \ldots, e_n\}$ of K over $\mathbb{Q}$. Clearly as $R \subseteq O_K$ and $K = Frac(O_K)$ we have that $Frac(R) \subseteq K$. Conversely if $k \in K$ then $k = \sum_{i=1}^{n} a_i e_i$ where $a_i \in \mathbb{Q}$ but each $a_i e_i \in Frac(R)$ as $\mathbb{Z} \subseteq R$ (and consequently $\mathbb{Q} \subseteq Frac(R)$). Thus, $k \in Frac(R)$.

$(c \Rightarrow a)$

So assume that the field of fractions of R is K. Now note that O_K contains a basis $\{e_1, \ldots, e_n\}$ of O_K over $\mathbb{Z}$ (it's a free abelian group of rank n), further note that by virtue of being a subgroup of O_K, R too is a free abelian group. Now each $e_i \in O_K \subseteq K = Frac(R)$ thus each $e_i = \frac{a_i}{b_i}$ where $a_i, b_i \in R$ and $b_i \neq 0$. Thus $(b_1 b_2 \ldots b_n) e_i = (b_1 \ldots b_{i-1} b_{i+1} \ldots b_n) a_i \in R$. We now claim that the $(b_1 \ldots b_n) e_i$ are linearly independent over $\mathbb{Z}$, indeed, if there was a non trivial linear combination of them over $\mathbb{Z}$ that was 0 then working in K we could multiply by the inverse of $(b_1 \ldots b_n)$ to obtain a non trivial linear combination of e_is over $\mathbb{Z}$ that was 0. Thus

R has rank at least n as a free $\mathbb{Z}$-module (or equivalently as a free abelian group), but R is a subgroup of O_K, which has rank n, thus R must also have rank n. But subgroups of finitely generated free abelian groups have same the same rank as the group they are lying in iff they are of finite index, thus, $[O_K : R]$ is finite.

Now we assume that R is a subring of O_K satisfying these conditions.

(i) By our remarks earlier R is a finitely generated free abelian group and every ideal in R being a subgroup (under addition) is also a free abelian group and thus must be finitely generated as a group, giving us that the ideal is finitely generated. Thus, every ideal in R is finitely generated which is equivalent to R being Noetherian.

(ii) Let $\mathfrak{p}$ be nonzero prime ideal in R. And let $x \in \mathfrak{p}$ such that $x \neq 0$. As $x \in \mathfrak{p} \subset R \subseteq O_K$ we have that x is integral over $\mathbb{Z}$ and thus must satisfy an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where each $a_i \in \mathbb{Z}$, furthermore $\mathbb{Z} \subseteq R$. We can take n to be minimal which gives us that $a_n \neq 0$, but from the equation we also have that $a_n \in \mathfrak{p}$. So $\mathfrak{p} \cap \mathbb{Z}$ is a non zero prime ideal of $\mathbb{Z}$ but in $\mathbb{Z}$ nonzero prime ideals are maximal, thus $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ is a field and in particular must be a finite field of characteristic p, for some prime p. Since K is a finite algebraic extension of $\mathbb{Q}$, $R/\mathfrak{p}$ must be contained in a finite algebraic extension of $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ (another way of seeing the same thing is by noting that the canonical ring homomorphism from $\mathbb{Z}$ to $R/\mathfrak{p}$ has kernel $\mathfrak{p} \cap \mathbb{Z}$, and that R is finitely generated over $\mathbb{Z}$ and thus $R/\mathfrak{p}$ must be finitely generated over $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$). In other words $R/\mathfrak{p}$ must be contained in a finite field of characteristic p, making $R/\mathfrak{p}$ a finite integral domain (the integral domain follows just from $\mathfrak{p}$ being prime). Finite integral domains are fields hence $\mathfrak{p}$ must be maximal.

(iii) Suppose $R \neq O_K$, then there exists $x \in O_K$ such that $x \notin R$. But by deifinition of the ring of integers x satisifies a relation of the form $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathbb{Z} \subseteq R$. Furthermore, $x \in O_K \subseteq K = Frac(R)$ thus the polynomial $X^n + a_1 X^{n-1} + \cdots + a_n$ lies in $R[X]$ and has a root in $Frac(R)$ which doesn't lie in R, thus R is not integrally closed.

□

Solution 3.
Consider the ideal $\mathfrak{a} = (2, 1 + \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$. Note that if we can show that $\mathfrak{a}$ is a prime ideal we will be done as clearly $\mathfrak{a} \neq (2)$ but $\mathfrak{a}^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = (2)\mathfrak{a}$ and if we did have unique factorization of ideals this would mean that $\mathfrak{a} = (2)$. We claim that $\mathfrak{a}$ is a maximal ideal (and hence prime). Consider any $m + n\sqrt{-3} \notin \mathfrak{p}$ then clearly one of m, n is even and the other odd (if both were even they'd be contained in (2), if both were odd then $m + n\sqrt{-3} - 1 - \sqrt{-3}$ would be contained in (2)). But now clearly $1 \in (\mathfrak{a}, m + n\sqrt{-3})$, hence $\mathfrak{a}$ is maximal as required. □

Solution 4.
In this problem integral domain will always mean a non-trivial, commutative ring with

unity.

We will need some preliminary definitions and results in order to approach this problem.

Let R be *any* integral domain, let $K = Frac(R)$.

We will say that an ideal $\mathfrak{a}$ of R is *invertible* if there exists some R-submodule (denote it by $\mathfrak{a}^{-1}$) of K such that $\mathfrak{a}\mathfrak{a}^{-1} = R$. Here multiplication is defined in the usual way for submodules, i.e if M and N are R-submodules of K then

$$MN = \{\sum_i m_i n_i \,|\, m_i \in M, n_i \in N\}$$

Note that under this definition, products of R-submodules of K are in turn R-submodules of K. Furthermore it is quite clear that every nonzero *principal* ideal is invertible.

We will take the following approach. First, we will show that if the product of finitely many ideals in an integral domain is invertible then each ideal in the product is invertible. Then we will show that in an integral domain if an ideal $\mathfrak{a}$ can be written as a product of finitely many *invertible* prime ideals then this is the unique representation of $\mathfrak{a}$ as a product of prime ideals. Using these facts we will then show that if B is as stated in the problem then any nonzero *invertible* prime ideal $\mathfrak{p}$ of B is maximal. Finally, we will then show that every prime ideal of B is invertible and hence maximal and the fact that B is a Dedekind domain will follow easily from this.

In keeping with our outline we now show that if the product of finitely many ideals in an integral domain R is invertible then each ideal in the product is invertible. Let $\mathfrak{b} = \prod_i \mathfrak{a}_i$ (where the product is finite), and let $\mathfrak{b}$ be invertible, i.e there is some $\mathfrak{b}^{-1}$ such that $\mathfrak{b}\mathfrak{b}^{-1} = R$, this means that

$$\mathfrak{b}^{-1}\mathfrak{b} = R = \mathfrak{b}^{-1}\prod_i \mathfrak{a}_i = \mathfrak{a}_j(\mathfrak{b}^{-1}\prod_{i \neq j} \mathfrak{a}_i)$$

hence each $\mathfrak{a}_i$ is invertible, as required.

Now we need to show that in an integral domain R if $\mathfrak{a} = \prod_i \mathfrak{p}_i$ (again this is a finite product) where each $\mathfrak{p}_i$ is an invertible prime ideal, then this is the unique factorization of $\mathfrak{a}$ into prime ideals. So suppose $\mathfrak{a}$ is as stated and $\mathfrak{a} = \prod_j \mathfrak{q}_j$, where the $\mathfrak{q}_j$s are prime ideals. Let $\mathfrak{p}_1$ be minimal amongst the $\mathfrak{p}_i$s (with respect to inclusion). Now as

$$\mathfrak{a} = \prod_i \mathfrak{p}_i = \prod_j \mathfrak{q}_j$$

we have that $\prod_j \mathfrak{q}_j$ is contained in $\mathfrak{p}_1$ then as $\mathfrak{p}_1$ is a prime ideal we have that some $\mathfrak{q}_j$, say $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Similarly, some $\mathfrak{p}_r$ is contained in $\mathfrak{q}_1$ and we have that $\mathfrak{p}_r \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1$, but as $\mathfrak{p}_1$ is minimal we have that $\mathfrak{p}_r = \mathfrak{q}_1 = \mathfrak{p}_1$. Now as we had assumed that the $\mathfrak{p}_i$s are invertible we may multiply $\mathfrak{a}$ by $\mathfrak{p}_1^{-1}$ and continue in a similar fashion to obtain that each $\mathfrak{q}_j$ is equal to some $\mathfrak{p}_i$. Thus, $\mathfrak{a}$ has a unique factorization into prime ideals.

We now show that if B is as stated in the problem then every nonzero *invertible* prime ideal $\mathfrak{p}$ of B is maximal. Let $a \in B$ such that $a \notin \mathfrak{p}$. We will show that $\mathfrak{p} + (a) = B$, hence showing that $\mathfrak{p}$ is maximal. Assume to the contrary that $\mathfrak{p} + (a)$ is a proper ideal. Then, consider the proper ideals $\mathfrak{p} + (a)$ and $\mathfrak{p} + (a)^2$. As we have factorization into prime ideals in B, we get that $\mathfrak{p} + (a) = \prod_{i=1}^{n} \mathfrak{p}_i$ and $\mathfrak{p} + (a)^2 = \prod_{j=1}^{m} \mathfrak{q}_j$. Let $\overline{B} = B/\mathfrak{p}$ and let the 'bar' denote the image in $\overline{B}$ of elements/ideals of B. Note that as $\mathfrak{p}$ is prime $\overline{B}$ is an integral domain, furthermore note that as each $\mathfrak{p}_i$ and each $\mathfrak{q}_j$ is a prime ideal containing $\mathfrak{p}$ we have that each $\overline{\mathfrak{p}}_i$ and each $\overline{\mathfrak{q}}_j$ is a prime ideal of $\overline{B}$. We now have that

$$\overline{(a)} = \prod_{i=1}^{n} \overline{\mathfrak{p}}_i$$

and that

$$\overline{(a)}^2 = \prod_{j=1}^{m} \overline{\mathfrak{q}}_j$$

but $\overline{(a)}^2 = \overline{(a)(a)}$ so we have that

$$\overline{(a)}^2 = \prod_{i=1}^{n} \overline{\mathfrak{p}}_i^2 = \prod_{j=1}^{m} \overline{\mathfrak{q}}_j$$

Now $\overline{(a)}^2$ is a nonzero principal ideal (it's generated by $\overline{a}^2 \neq \overline{0}$) and thus invertible. But now by our very first result this means that each $\overline{\mathfrak{p}}_i$ (and $\overline{\mathfrak{q}}_j$ for that matter) is invertible. This in turn means that $\overline{(a)}^2$ has a factorization in invertible prime ideals, but now by our second result this means that this factorization into prime ideals is unique. So the $\overline{\mathfrak{q}}_j$s are the $\overline{\mathfrak{p}}_i$s (each repeated twice). But note that as each $\mathfrak{p}_i$ and each $\mathfrak{q}_j$ contained $\mathfrak{p}$ in B we have that the preimage of $\overline{\mathfrak{p}}_i$ is exactly $\mathfrak{p}_i$ and that the preimage of $\overline{\mathfrak{q}}_j$ is exactly $\mathfrak{q}_j$. We thus have that the $\mathfrak{q}_j$s are equal to the $\mathfrak{p}_i$s (each repeated twice). We thus have that $\prod_{i=1}^{n} \mathfrak{p}_i^2 = (\mathfrak{p} + (a))^2 = \prod_{j=1}^{m} \mathfrak{q}_j = \mathfrak{p} + (a)^2$. But $(\mathfrak{p} + (a))^2 = \mathfrak{p} + (a)^2$ implies that $\mathfrak{p} \subseteq \mathfrak{p} + (a)^2 = (\mathfrak{p} + (a))^2 \subseteq \mathfrak{p}^2 + (a)$. Thus any $x \in \mathfrak{p}$ may be written as $x = y + az$ where $y \in \mathfrak{p}^2$ and $z \in B$, but this in turn implies that $az \in \mathfrak{p}$ and as $a \notin \mathfrak{p}$ we have that $z \in \mathfrak{p}$ (as $\mathfrak{p}$ is a prime ideal). Consequently we have that $\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p}(a)$, but clearly $\mathfrak{p}^2 + \mathfrak{p}(a) \subseteq \mathfrak{p}$. Hence, $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}(a)$. But now note that (in what seems to be a long long time ago in a galaxy far far away) we had assumed $\mathfrak{p}$ to be invertible, thus multiplying by $\mathfrak{p}^{-1}$ we get that

$$\mathfrak{p}\mathfrak{p}^{-1} = B = \mathfrak{p}^{-1}(\mathfrak{p}^2 + \mathfrak{p}(a)) = B\mathfrak{p} + B(a) = \mathfrak{p} + (a)$$

which is a contradiction as we had assumed $\mathfrak{p} + (a)$ to be a proper ideal, thus $\mathfrak{p} + (a)$ blows up to the whole ring B as required. (Note that the secondlast equality follows because the way we had defined our submodule multiplication, the operation was associative, distributed nicely over sums etc.)

Ok, we are almost done. Let $\mathfrak{p}$ be *any* nonzero prime ideal of B and let x be a nonzero element of $\mathfrak{p}$. Now as we have factorization into prime ideals in B we have that

$$(x) = \prod_i \mathfrak{p}_i \subseteq \mathfrak{p}$$

Now as (x) is principal it is also invertible and by our very first result this implies that each $\mathfrak{p}_i$ is invertible which as a consequence of our most recent result implies that each $\mathfrak{p}_i$ is maximal. Now as $\mathfrak{p}$ is prime and $\prod_i \mathfrak{p}_i \subseteq \mathfrak{p}$ we have that one of the $\mathfrak{p}_i$s, say $\mathfrak{p}_1$ is contained in $\mathfrak{p}$ but as we just showed $\mathfrak{p}_1$ is maximal and hence $\mathfrak{p} = \mathfrak{p}_1$. Thus, $\mathfrak{p}$ is maximal as required.

Also note that we have also just shown that along with every prime ideal being maximal it is also invertible (as $\mathfrak{p} = \mathfrak{p}_1$ which is invertible).

Now to finally show that B is a Dedekind domain all that is left for us to show is that B is Noetherian and integrally closed.

For Noetherian (it's short, I promise) we will first show that if an ideal in B is invertible then it is finitely generated. We will then show that every ideal is invertible, hence showing that B is Noetherian. So let $\mathfrak{a}$ be an invertible ideal then as $\mathfrak{a}\mathfrak{a}^{-1} = B$ we have in particular that $\sum_{i=1}^n x_i y_i = 1$ for some $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{a}^{-1}$. We claim that $x_1, \ldots, x_n$ generate $\mathfrak{a}$, as for any $a \in \mathfrak{a}$ we have that $ay_i \in B$ (this follows from how we defined $\mathfrak{a}^{-1}$ right at the beginning of this solution). And thus $\sum_{i=1}^n (ay_i)x_i = a$, as required. To see that every ideal in B is invertible, note that earlier we had shown that every prime ideal in B is invertible, as any ideal can be written as a product of prime ideals, it follows easily that every ideal is in turn invertible (just multiply through by the 'inverse' of each prime ideal in the factorization). Hence, B is Noetherian.

To see that B is integrally closed, let $a \in Frac(B)$ be integral over B, i.e there exist $c_1, \ldots, c_n \in B$ such that

$$a^n + c_1 a^{n-1} + \cdots + c_n = 0 \tag{1}$$

Now let M be the B-submodule of $Frac(B)$ generated by $a, a^2, \ldots, a^{n-1}$. Note that $aM \subseteq M$ (this follows from (1)). Now as $a \in Frac(B)$ we have that $a = \frac{p}{q}$ where $p, q \in B$ and $q \neq 0$. So we have that $q^{n-1}M \subseteq B$ but this means that the submodule $q^{n-1}M$ is an ideal of B which means that it must be invertible (we proved this when we were showing B is Noetherian). So if we set $\mathfrak{b} = q^{n-1}M$ then there exists a $\mathfrak{b}^{-1}$, such that $\mathfrak{b}\mathfrak{b}^{-1} = B$. Now as we already noted $aM \subseteq M$ so

$$aq^{n-1}M\mathfrak{b}^{-1} \subseteq q^{n-1}M\mathfrak{b}^{-1}$$

but this gives us that

$$a\mathfrak{b}\mathfrak{b}^{-1} = aB \subseteq \mathfrak{b}\mathfrak{b}^{-1} = B$$

hence, $a \in B$. □

Remark: It seems that with this proof we can actually drop the uniqueness condition from the original problem as the uniqueness falls out of the existence of a factorization into prime ideals (see second step in the outline).