First, some motivation from number theory. One subject of interest in number theory is determining integral points on an elliptic curve, i.e. solutions $(x, y) \in \mathbb{Z}^2$ of an equation of the form

$$y^2 = x^3 + Ax + B,$$

where A and B are integers.

Now, if the right hand side factored over $\mathbb{Z}$, this would be fairly straightforward, as we would have something like

$$y^2 = (x - a)(x - b)(x - c)$$

with everything integers. Depending on whether the terms on the right hand side are coprime, we could determine that some of them are squares, and we could study solutions modulo various primes to get more information and eventually determine the possible values of x and y.

Unfortunately, it is rare in practice that such an equation would factor in $\mathbb{Z}$. However, we do know that there will be a finite extension of $\mathbb{Q}$, namely $\mathbb{Q}(a, b, c)$ in which the right hand side does split. If we are still interested in integer solutions, it might make sense to look at this equation in $\mathbb{Z}[a, b, c]$, but the problem is that such a ring is not in general a UFD or PID, which is what in principle makes the previous special case easy to hand.

(one can check that in $\mathbb{Z}[\sqrt{-5}]$, $2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, that all those values are irreducible, but that these factorizations do not just differ by a unit)

This means we cannot really make use of GCDs and other tricks to figure out if various components of the product must be squares or to put other constraints on the problem.

Fortunately, there is a sort of "second best" available to us in this setting. Notice that in the above factorization, a, b, and c are algebraic integers, so $\mathbb{Z}$ is integral over $\mathbb{Z}[a, b, c]$ which we saw leads to a number of useful results relating the primes of $\mathbb{Z}[a, b, c]$ to the primes of $\mathbb{Z}$ (e.g. going up and going down). It turns out we will get much more mileage by considering not just $\mathbb{Z}[a, b, c]$, but the whole integral closure of $\mathbb{Z}$ in $\mathbb{Q}(a, b, c)$. If $K = \mathbb{Q}(a, b, c)$, that integral closure is called the ring of integers of K and denoted $\mathcal{O}_K$.

(small note: even these smaller rings, there is a lot of useful data, and often the same results hold but with exceptions involving the primes which divide the index of $\mathbb{Z}[a, b, c]$ in $\mathcal{O}_K$)

It turns out that the ring $\mathcal{O}_K$ is what is called a dedekind domain, a ring in which every nonzero proper ideal factors uniquely as a product of maximal ideals (up to rearranging). So while $\mathcal{O}_K$ is not in general a UFD, which has unique factorization of elements themselves, we can study the relation of ideals

$$(y)^2 = (x - a)(x - b)(x - c)$$

So, for instance, of all of the ideals on the right are pairwise coprime, we know they must be squares of coprime ideals in $\mathcal{O}_K$. When we know enough about $\mathcal{O}_K$, an analysis of this factorization can allow us to determine all the possible solutions or show that none exist.

Here is another useful application: it is possible to prove Fermat's Last Theorem in a various special cases with this technique. Recall that Fermat's last theorem claims that the equation

$$x^n + y^n = z^n$$

Has no nontrivial integer solutions (x, y, z) for any exponent $n \geq 3$. One can immediately reduce this to showing the result for $n = 4$ and all odd primes and (x, y, z) relatively prime. The case of $n = 4$ can be treated by elementary methods, and is the only case Fermat is known to have been able to prove of "his" theorem. Then if p is an odd prime and $\zeta = \zeta_p$, the left hand side of the equation factors into

$$(x + y)(x + \zeta y)(x + \zeta^2 y)...(x + \zeta^{p-1} y) = z^p$$

One can prove that for $K = \mathbb{Q}(\zeta)$, $\mathcal{O}_K = \mathbb{Z}[\zeta]$ but the latter is a UFD for only finitely many primes. However, we can still treat this as an equation in ideals, and if we are lucky and know enough about the ideals in $\mathbb{Z}[\zeta]$ it is possible to show that this has no solutions for what are called "regular primes", though

to discuss that in detail involves developing much more machinery from algebraic number theory. For those with such a background, Keith Conrad has a good exposition on his website.

In fact, even for the case $n = 2$, where it is well-known that $x^2 + y^2 = z^2$ has solutions (pythagorean triple) it is possible to employ these techniques to determine all the solutions. To do this, one works in the ring $\mathbb{Q}(i)$, where it can be shown that $\mathcal{O}_K = \mathbb{Z}[i]$. The latter ring is well-known to be a UFD, and in fact a PID, the factorization

$$(x - iy)(x + iy) = z^2$$

quickly leads to a great deal of information; it will turn out that there are two cases, depending on the GCD of the two terms on the left and that by studying these carefully one can classify all the solutions of this equation. More details are presented in the first chapter of Marcus's *Number Fields* (partly in the exercises; other sources may have the full details).

So now our goal is to more carefully state what a Dedekind domain is, verify the useful property mentioned above (unique factorization of ideals into products of prime ideals), and then give examples of two kinds of dedekind domain.

Essentially, Dedekind domains should generalize PIDs (or UFDs) by weakening factorization of elements to factorization of ideals. In fact, one definition of a dedekind domain is essentially a ring that is locally a PID. This means that all of the nice properties enjoyed by PIDs which happen to also be local hold for dedekind domains. Even for properties which are not local in general, they sometimes lift or have useful analogs in dedekind domains. In some cases, these are enough to make up for the deficiencies of these rings relative to PIDs and UFDs.

Definition. A **dedekind domain** is an integral domain A which satisfies one of the following:

DD1) Every nonzero proper ideal factors uniquely into a product of maximal ideals

DD2) A is noetherian, and the localization at each maximal ideal is a DVR

DD3) A is noetherian, integrally closed, and dimension 1

Showing these are equivalent is a difficult task, and we will work from easiest to most difficult. The equivalence of DD2 and DD3 boils down to Prop 9.2 in A&M. That DD2 implies DD1 should be highly plausible, and its proof even follows our intuition: the factorization of ideals in A behaves extremely well locally, given what we know about DVRs, and so we can patch this together into good factorizations globally.

Showing DD1 implies DD2 or DD3 is much more difficult - it is not at all clear why simply the existence of a factorization of any ideal into primes would imply noetherianity or the other properties in DD2 or DD3. This is not done in A&M or even the algebraic number theory books I looked at, but there is a good exposition in Zariski-Samuel.

Here is a summary of the main algebraic facts:

Lemma. *The following are true:*

1) if $(A, \mathfrak{m})$ is a noetherian local domain of dimension 1, then A is integrally closed if and only if A is a DVR.

2) if A is a domain and for each maximal ideal $\mathfrak{m}$ we identify $A_{\mathfrak{m}}$ with its natural inclusion in $Frac(A)$, then

$$A = \bigcap_{\mathfrak{m}\ max.} A_{\mathfrak{m}}.$$

3) given a multiplicatively closed set S, there is a 1-1 correspondence between prime ideals of A not meeting S, and prime ideals of $S^{-1}A$.

4) if A is a DVR then A has dimension 1.

5) if $\mathfrak{p}$ is a prime ideal and $\mathfrak{p} \supseteq \prod \mathfrak{a}_i$ or $\mathfrak{p} \supseteq \cap \mathfrak{a}_i$ for some finite collection of ideals $\mathfrak{a}_i$, then $\mathfrak{p} \supseteq \mathfrak{a}_j$ for some j.

6) given a multiplicatively closed set S, there is a 1-1 correspondence between primary ideals of A not meeting S, and primary ideals of $S^{-1}A$.

7) given a map $\phi : M \to N$ of A-modules, ϕ is surjective if the localized map $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for all maximal $\mathfrak{m}$.

8) If an ideal $\mathfrak{a}$ is contained in a union of finitely many prime ideals, then $\mathfrak{a}$ is contained in one of those prime ideals.

Proof.

1) Prop 9.2 in A&M.

2) Well, by construction it is clear that $A \subseteq A_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$, so $A \subseteq \cap A_{\mathfrak{m}}$. To see this cannot be proper, suppose that $x/y \in K - A$, so we seek a maximal ideal $\mathfrak{m}$ such that $x/y \notin A_{\mathfrak{m}}$. Consider the colon ideal $(y : x) = \{a \in A \mid bx \in (y)\}$; it must be proper, because if $1 \in (y : x)$ then $x \in (y)$ meaning we can write $x = ay$ then $x/y = ay/y = a/1 \in A$, contradiction.

   So there exists a maximal ideal $\mathfrak{m}$ containing $(y : x)$. By construction, $x/y \notin A_{\mathfrak{m}}$, because if we could write

$$\frac{x}{y} = \frac{a}{b} \quad b \notin m$$

   then we would have

$$xb = ay$$

   which is to say $bx \in (y)$ and hence $b \in (y : x)$, contrary to our choice of $\mathfrak{m}$.

3) Prop 3.11(iv) in A&M.

4) This is shown in the remarks preceeding 9.2 in A&M.

5) Prop 1.11(ii) in A&M. As stated it only applies to intersections, but it is clear from the proof that the result holds for products as well.

6) Prop 4.8(ii) in A&M.

7) Prop 3.9(iii), surjective version, in A&M.

8) Prop 1.11(i) in A&M.

Showing that DD3 implies DD2 is essentially the content of Prop 9.2 in A&M, so it requires only (1) from the Lemma. The converse needs both Prop 9.2, via (1) and (4), and a few facts which enable us to lift information from the localizations to A, from (2) and (3).

Theorem. *DD2 is equivalent to DD3*

Proof. First, DD2 implies DD3. Noetherian: already part of DD2

Dimension 1: For all maximal ideals $\mathfrak{m}$, $A_{\mathfrak{m}}$ is a DVR, which by (4) has dimension 1. By lifting back a chain of length 1 in any such localization, using (3), we see that $\dim A \geq 1$. Conversely, if $\dim A > 1$, we can find some primes $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subseteq \mathfrak{p}_2$, but then take a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}_2$, and by the dimension constraint on $A_{\mathfrak{m}}$, we see that in the local ring, $\mathfrak{p}_0 = \mathfrak{p}_1$ or $\mathfrak{p}_1 = \mathfrak{p}_2$, so again by (3) we have $\mathfrak{p}_0 = \mathfrak{p}_1$ or $\mathfrak{p}_1 = \mathfrak{p}_2$ in A, contradiction. Thus A has dimension 1

Integrally closed: $A_{\mathfrak{m}}$ is a DVR, hence integrally closed by (1). Integral closure is preserved by intersection, and hence by (2), $A = \cap A_{\mathfrak{m}}$ is integrally closed.

Then DD3 implies DD2. Observe that, because A is a domain of dimension 1, for any maximal ideal $\mathfrak{m}$, the chain $0 \subseteq \mathfrak{m}$ is the largest possible chain containing $\mathfrak{m}$. Localizing this, we see that $A_\mathfrak{m}$ has dimension 1. Noetherianity, being an integral domain, and integral closure are preserved by localizing, while we know $A_\mathfrak{m}$ is local, and so by (1) we see that $A_\mathfrak{m}$ is a DVR.

To show DD2 implies DD1, we just follow our intuition that the local factorizations of an ideal (which will be powers of some maximal ideal, since $A_\mathfrak{m}$ is a DVR) can be put together to give a factorization in the original ring. From this, we can already guess that we will need (6), since it tells us that powers of primes behave well under localization, while (7) shows us how we can glue the local information together. It turns out (5) will be important as well, but one only sees this during the proof; essentially, (7) will ask that we combine all local factorizations, which a priori could involve infinitely many ideals in the factorization, but it is not possible to take a product of infinitely many ideals. However, combining (5) with the fact that every ideal contains a product of prime ideals in a noetherian ring will allow us to conclude that only finitely many primes are actually involved.

Theorem. *DD2 implies DD1*

Proof. Since we have assumed A is a DVR, it has dimension 1 by (4).

Let I be a nonzero ideal of A. By noetherianity, I contains a product $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ of nonzero prime ideals $\mathfrak{p}_i$. From this, we can see that I is contained in only finitely many maximal ideals, because if we had a maximal ideal $\mathfrak{m}$ with

$$\mathfrak{m} \supseteq I \supseteq \prod_{i=1}^{r} \mathfrak{p}_i^{f_i},$$

then $\mathfrak{m} \supseteq \mathfrak{p}_i^{f_i}$ for some i by (5), and taking radicals we get $\mathfrak{m} \supseteq \mathfrak{p}_i$, but $\mathfrak{p}_i$ is a nonzero prime ideal and hence maximal because A has dimension 1, so $\mathfrak{m} = \mathfrak{p}_i$.

Now for $\mathfrak{m}$ an arbitrary prime ideal, consider $I_\mathfrak{m}$ in $A_\mathfrak{m}$; by DD2, $A_\mathfrak{m}$ is a DVR and hence we can write $I_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}^{f_\mathfrak{m}}$ for a nonnegative integer $e_\mathfrak{m}$ (the notation leaves something to desired). Then we have

$$I \subseteq I^{ec} \subseteq (\mathfrak{m}_\mathfrak{m}^{f_\mathfrak{m}})^c = \mathfrak{m}^{f_\mathfrak{m}}.$$

The last equality is (6), the correspondence for primary ideals. Thus we have an inclusion

$$I \to \bigcap_{\mathfrak{m} \text{ max.}} \mathfrak{m}^{f_\mathfrak{m}}.$$

But by choice, the inclusion is surjective when localized at all maximal ideals. Thus by (7), the inclusion itself is a surjection.

By the earlier remarks, I is contained in only finitely many maximal ideals, say $\mathfrak{m}_i$, $1 \leq i \leq s$ and so for any other $\mathfrak{m}$, $f_\mathfrak{m}$ must be zero, meaning the above intersection is actually finite:

$$I = \bigcap_{i=1}^{s} \mathfrak{m}_i^{f_{\mathfrak{m}_i}}.$$

As all the ideals are maximal, they are also coprime. Hence, by the chinese remainder theorem, we may replace the intersection by the product, which gives the desired factorization of I as a product of maximal ideals,

$$I = \prod_{i=1}^{s} \mathfrak{m}_i^{f_{\mathfrak{m}_i}}.$$

This is clearly unique, since if we had any other factorization, pick a maximal ideal $\mathfrak{m}$ where they differ and localize both at $\mathfrak{m}$ to obtain a contradiction.

The most difficult direction is DD1 implies DD2 or DD3. In particular, it is difficult to see how one might extract noetherianity simply from the existence of a factorization for each ideal. One clue that such a ring could be noetherian is that a decomposition of an ideal as a product of maximal ideals is the same as a

primary decomposition, and we know that ideals of noetherian rings always admit primary decompositions.

In fact, a much weaker version DD1* of DD1 would suffice: if A is a domain for which each nonzero ideal can be written as a product of prime ideals, A is a dedekind domain in one of the sense described above. It requires substantially more work to prove this. Not only do we weaken the factorization from maximal ideals to prime ideals, but we also lose the uniqueness statement, which we will see later is crucial. For all the cases I know of, one DD1 or DD1* are viewed as corrolaries of DD2/DD3, even though they are equivalent; dedekind domains show up often in number theory, but in the number theory textbooks I checked, none included the converse. Zariski-Samuel contains a complete proof that DD1* implies DD3 (Vol. 1, Ch. V, Theorem 13, pg 275).

Theorem. *DD1 implies DD2*

Proof. DVR: recall that every ideal of a localized ring $S^{-1}A$ is of the form $S^{-1}I$ where I is an ideal of A. So let $I_{\mathfrak{m}}$ be a nonzero ideal of $A_{\mathfrak{m}}$. By hypothesis, we can factor

$$I = \prod_{i=1}^{r} \mathfrak{m}_i^{e_i}.$$

Now, if $\mathfrak{m}_i \neq \mathfrak{m}$, then $\mathfrak{m}_i$ becomes the unit ideal when we localize at $\mathfrak{m}$, so after localizing

$$I_{\mathfrak{m}} = \mathfrak{m}_{\mathfrak{m}}^{k},$$

for some k (e.g. if $\mathfrak{m} = \mathfrak{m}_1$ then $k = e_1$, and if $\mathfrak{m}$ doesn't equal any $\mathfrak{m}_i$ then $I_{\mathfrak{m}} = A_{\mathfrak{m}}$). This allows us to define a valuation on $A_{\mathfrak{m}}$ by $v(x) = k$ when $(x) = \mathfrak{m}_{\mathfrak{m}}^{k}$.

Noetherity: it suffices to prove this for the nonzero prime ideals, since a product of finitely generated ideals is again finitely generated. Let $\mathfrak{m}$ be some nonzero prime.

Notice that $\mathfrak{m}_{\mathfrak{m}} \neq \mathfrak{m}_{\mathfrak{m}}^2$ in $A_{\mathfrak{m}}$ because in that setting, the $\mathfrak{m}_{\mathfrak{m}}$ is finitely generated and hence Nakayama's lemma applies. Then by the correspondence for primary ideals, $\mathfrak{m} \neq \mathfrak{m}^2$. Let $x \in \mathfrak{m} - \mathfrak{m}^2$. Factoring the ideal (x), by prime ideals, this means we must have

$$(x) = \mathfrak{m} \prod_{i=1}^{r} \mathfrak{m}_i^{e_i},$$

where $\mathfrak{m}_i \neq \mathfrak{m}$ for any i, by considering (x) in $A_{\mathfrak{m}}$.

By (8), $\mathfrak{m}$ is not contained in $\cup \mathfrak{m}_i$, since then we would have $\mathfrak{m} \supseteq \mathfrak{m}_j$ for some j, and hence $\mathfrak{m} = \mathfrak{m}_j$ by maximality, a contradiction. So let $y \in \mathfrak{m} - \cup \mathfrak{m}_i$.

Claim: $\mathfrak{m} = (x, y)$. It is clear that $\mathfrak{m}$ contains (x, y), but in fact no other maximal ideal contains (x, y). If we had such a maximal ideal $\mathfrak{m}'$, then since $\mathfrak{m}' \supseteq (x)$, but is not $\mathfrak{m}$, it contains, and thus equals, some $\mathfrak{m}_j$. But by construction, no such $\mathfrak{m}_j$ contains y, and so $\mathfrak{m}'$ does not exist. Then in consideration of the factorization of (x, y), it must be a power $\mathfrak{m}^k$, but because it contains x, k must equal 1.

(in fact, it is true that any ideal in a dedekind domain is generated by at most two elements, and the proof is quite similar to the one above, but working just with the maximal ideals simplifies it slightly)

With these characterizations of dedekind domains, our next goal is to study a small application of dedekind domains in algebraic number theory. We will show that the integral closure of a dedekind domain in a finite extension of fields is again a dedekind domain.

Theorem. *Let A be a dedekind domain with fraction field K and L a finite separable extension of K. Then the integral closure B of A in L is a dedekind domain.*

Proof. It is easiest to verify DD3.

Noetherianity: By Prop 5.17, B a submodule of a finitely generated A-module, so B noetherian A-module by Prop 6.2, thus *a fortiori* a noetherian B-module (or apply Prop 7.8 with $B = C$).

Integral closure: Nothing to prove by construction of B.

Dimension: Let $\mathfrak{p}$ be a nonzero prime ideal in B. From Cor 5.8, it will be maximal if $A \cap \mathfrak{p}$ is maximal; since the latter is always prime, it is enough to know that it is nonzero since A has dimension 1 by assumption. Taking any nonzero $x \in \mathfrak{p}$, apply the integrality of B over A to find a monic polynomial it satisfies,

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0.$$

We may refine this polynomial so that the constant term is not zero - simply factor out and cancel x (as it is nonzero) until this is the case. Then such a polynomial gives a relation

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x = -a_0.$$

Everything on the LHS is in (x), so $-a_0 \in (x) \subseteq (\mathfrak{p})$ is a nonzero element of A in $\mathfrak{p}$, which is all we needed to verify the dimension claim.

From which we obtain two classes of dedekind domains, one arising in number theory, and another in geometry.

Corollary. *The integral closure of $\mathbb{Z}$ in a finite extension of $\mathbb{Q}$ is a dedekind domain. Given a field k and indeterminate x, the integral closure of $k[x]$ in a finite extension of $k(x)$ is a dedekind domain*

Proof. Both $\mathbb{Z}$ and $k[x]$ are clearly dedekind domains under any of the above definitions. This follows in both cases from the fact that these rings are PIDs.

DD1: Any ideal I is of the form (x), and we know that x can be factored uniquely into a product of irreducibles, which induces a factorization of $(x) = I$. Further, since these rings are PIDs, irreducible elements generate maximal ideals.

DD2: Take any maximal ideal $\mathfrak{m} = (m)$, and we can see that $A_{\mathfrak{m}}$ is the valuation ring induced by the valuation sending each element to the power of m which divides it (which is unique because A is a PID, hence UFD).

DD3: They are both PIDs, hence noetherian, and we've seen previously that they are integrally closed in their respective fields of fractions. Moreover, we know that in a PID, all nonzero primes are maximal, so they have dimension 1.