Dedekind Domains

Definition 1 A **Dedekind domain** is an integral domain that has the following three properties:

(i) Noetherian,
(ii) Integrally closed,
(iii) All non-zero prime ideals are maximal. □

Example 1 Some important examples:

(a) A PID is a Dedekind domain.
(b) If A is a Dedekind domain with field of fractions K and if $K \subset L$ is a finite separable field extension, then the integral closure, B, of A in L is a Dedekind domain.
(c) A localization of a Dedekind domain at any multiplicative set is also a Dedekind domain. □

Example (b) is the most important. It includes the ring of algebraic integers in any finite extension of $\mathbb{Q}$. Proofs that all three examples above are Dedekind domains amount to collecting various known or straightforward results. For example, in (b), Noetherian follows from the trace form argument, which proves B is contained in a finitely generated A module. That all non-zero primes of B are maximal is part of the Going Up theory, comparing prime ideals in B and A. B is integrally closed by transitivity of integral extensions.

The first main result about Dedekind domains is that every proper ideal is uniquely a product of powers of distinct prime ideals. One way to approach this is to start with primary decomposition. Properties (i) and (iii) are enough to show that every proper ideal is uniquely a product of primary ideals with distinct radicals. Then condition (ii) is brought in to show that the only primary ideals are powers of primes. This is accomplished by localizing at a prime and proving that any *local* Dedekind domain is a PID, in fact, a rather special kind of PID. Anyway, in a PID the only primary ideals are powers of primes. Standard results comparing prime and primary ideals before and after localization then gives what you want, namely that the only primary ideals in a Dedekind domain are powers of primes.

In the end, one wants to factor more than the ideals in a Dedekind domain A. One wants to study what are called fractional ideals, which are A-submodules of the field of fractions K of A of the form $(1/c)I \subset K$ where $I \subset A$ is an ideal. We prove that these fractional ideals form a group under a product operation extending the product operation on ideals, and we factor them as products of primes, with both positive and negative exponents. After factoring ideals by the method outlined above, one more little argument is needed which identifies the inverse of a prime ideal as a fractional ideal. After that, it is easy to factor fractional ideals and show they form a group. All this becomes quite important in algebraic number theory.

The classical approach to prime factorization and study of fractional ideals in Dedekind domains proceeds more directly than via primary decomposition. But one sees very similar steps along the way. Also, the Noetherian hypothesis is used in similar ways. Recall for example that in a Noetherian ring any ideal contains a finite product of powers of distinct prime ideals. If all non-zero primes are maximal, any prime containing the ideal must occur in this product. So this is a start toward showing that an ideal is a product of powers of the distinct primes that contain it. Use of primary decomposition places the study of Dedekind domains in the context of a decomposition theory for ideals valid in arbitrary Noetherian rings.

This handout is organized as follows. First, we give several preliminary paragraphs. This is supposed to be review. The longest preliminary section discusses some standard facts about ideals and localization. If you've never thought these things through, now is a good time, because you won't fully understand otherwise. Basic results about localization get used all the time. It is important to be familiar enough with the properties of localization that you quickly understand how it gets used and helps in many situations you encounter. It's like linear algebra or basic group theory. You get so familiar with basic results that it doesn't require any energy to use those results whenever convenient and useful.

After the preliminaries, we prove the basic result that a local Dedekind domain is a PID. Combined with the preliminaries, this immediately gives unique factorization of ideals as products of powers of distinct primes in any Dedekind domain. Then a few trivial preliminaries about fractional ideals are given. Following that, we identify the inverse of a fractional ideal in the Dedekind domain situation, and prove fractional ideals form a group and satisfy unique factorization. Many rather simple, but somewhat dramatic, corollaries follow. At the end, we present some really cool results about factoring ordinary integer prime ideals in rings of algebraic integers in finite extensions of $\mathbb{Q}$.

Preliminary 1 Primary decomposition. If A is a Noetherian integral domain in which all non-zero prime ideals are maximal, then every proper ideal I is uniquely a product of primary ideals, $I = Q_1 Q_2 \cdots Q_r$, with distinct radicals. The radicals $P_j = \operatorname{rad} Q_j$ are exactly the prime ideals which contain I, all of which are minimal over I, since there are no proper inclusions among non-zero prime ideals. The primary components are given by $Q_j = \{a \in A \mid as \in I \text{ for some } s \notin Pj\}$. It is obvious from the definition of P_j-primary ideal that Q_j is thus the smallest P_j-primary ideal that contains I, since $as \in I, s \notin P_j$, implies that a belongs to any P_j-primary ideal that contains I. We summarize this discussion, with an added hypothesis, in the next statement.

Prelim 1.1 Suppose A is a Noetherian domain in which all non-zero primes are maximal and suppose for each prime P the only P-primary ideals are powers of P. Then every proper ideal I is uniquely the product of powers of distinct prime ideals. If $I \subset P$, then the P-primary component of I is P^e, where e is the greatest integer such that $I \subset P^e$.

The powers P^n of a prime ideal in any Noetherian domain are distinct. To prove this, localize at P to reduce to the case A local. Then $PP^n = P^n$ would imply $P^n = (0)$ by Nakayama's Lemma. (See the next paragraphs for details about the behavior of primes and powers of primes under localization.)

Preliminary 2 Primary ideals and localization. Given any ring homomorphism $i : A \to B$, there are two important operations on ideals, **contraction** $c : \{\text{ideals in } B\} \to \{\text{ideals in } A\}$ and **extension** $e : \{\text{ideals in } A\} \to \{\text{ideals in } B\}$. Contraction is defined by $J^c = i^{-1}(J) \subset A$ for an ideal $J \subset B$. Extension is defined by $I^e = i(I)B \subset B$ for an ideal $I \subset A$. If $S \subset A$ is a multiplicative set and $i : A \to S^{-1}A$ is the natural homomorphism to the localization of A at S, then the following results are easily verified, although there are many small details to check. (A few, but certainly not all, of the statements below hold for arbitrary ring homomorphisms $A \to B$.)

Prelim 2.1 For any ideal $J \subset S^{-1}A$, $J^{ce} = J \subset S^{-1}A$. If J is prime [resp. primary] then J^c is prime [resp. primary]. For any J, $\operatorname{rad}(J^c) = (\operatorname{rad} J)^c$.

Prelim 2.2 For any ideal $I \subset A$, $I^{ec} = \{a \in A \mid as \in I \text{ for some } s \in S\} \subset A$. If I is prime [resp. primary] and $I \cap S = \emptyset$, then I^e is prime [resp. primary]. For any I, $\operatorname{rad}(I^e) = (\operatorname{rad} I)^e$.

Prelim 2.3 Extension and contraction define bijections between the prime ideals of $S^{-1}A$ and the prime ideals of A disjoint from S. Extension and contraction define bijections between the primary ideals of $S^{-1}A$ and the primary ideals of A disjoint from S. These bijections commute with the operation of taking radicals of primary ideals.

For any ring homomorphism $A \to B$, it is obvious that extension commutes with the operation of products of ideals, that is $(I_1 I_2)B = (I_1 B)(I_2 B)$, hence extension also commutes with the operation of nth powers of an ideal.

Prelim 2.4 Suppose $P \subset A$ is a maximal ideal such that in the localization $A_{(P)}$ the only $PA_{(P)}$-primary ideals are powers of $PA_{(P)}$. Then the only P-primary ideals of A are powers of P.

PROOF Since P is maximal, the powers P^n are indeed P-primary. By the hypothesis, these powers extend to give all the $PA_{(P)}$-primary ideals in $A_{(P)}$. Because of the bijection of Prelim 2.3, there can be no other P-primary ideals in A. ∎

Preliminary 3 A module condition for integrality. Suppose $A \subset B$ is a ring extension, and suppose $b \in B$. Suppose there exists an $A[b]$-module M which is faithful as an $A[b]$-module and finitely generated as an A-module. (Faithful means the $A[b]$-annihilator of M is (0).) Then b is integral over A. Namely, if M is generated by $\{x_j\}$ as A-module, write $bx_i = \sum_j a_{ij} x_j$. By the adjugate matrix trick, $\det(bI - (a_{ij}))$ annihilates M. Hence $\det(bI - (a_{ij})) = 0$, which is a monic polynomial equation for b over A.

Preliminary 4 Local Noetherian domains with principal maximal ideal. Call such a domain A, with maximal ideal (t). Then t is irreducible, since if $t = rs$, with r, s not units, then $r, s \in (t)$, so we get an equation $t = t^2 x$, which implies $1 - tx = 0$, contradicting the fact that t is not a unit in A. In fact, up to unit factors, t is clearly the only irreducible (non-unit) in A, since any non-unit $a = tu$ for some u, and if a is irreducible, u must be a unit. Since A is a Noetherian domain, all non-zero, non-units a are products of finitely many irreducible elements, hence products of powers of t and units. More directly, if (a) were maximal so that a is not such a product, then $a = tb$ and $(a) \subsetneqq (b)$, so $b = t^m u$ and $a = t^{m+1} u$, a contradiction. We summarize:

Prelim 4.1 If A is a Noetherian local domain with principal maximal ideal (t), then every non-zero element of A can be uniquely written $a = t^n u$ for some $n \geq 0$ and some unit u. The only non-zero ideals in A are the powers of the maximal ideal, that is, the principal ideals (t^n). In particular A is a PID.

The rings described in Prelim 4.1 are also called **discrete valuation rings**. The function $\nu(a) = n$, where $a = t^n u$, u a unit, has nice properties which makes it something called a valuation. But that's another story.

That finishes the first preliminaries. Now we come to the key result that implies unique factorization of ideals in a Dedekind domain as products of powers of distinct primes.

Proposition 1 *A local Dedekind domain is a discrete valuation ring, in particular a PID. Thus, by Prelim 2.4, in any Dedekind domain the only primary ideals are powers of primes.*

PROOF If A is our local Dedekind domain, with maximal ideal P, choose $(t) \subset P$ to be maximal among proper principal ideals contained in P. We will show $(t) = P$. If not, choose $r > 1$ least

such that $P^r \subset (t)$. Choose $b \in P^{r-1}$, $b \notin (t)$. Then, in the field of fractions of A, $b/t \notin A$. By the choice of b, we get $(b/t)P \subset A$ since $bP \subset P^r \subset (t)$. Since $(b/t)P \subset A$ is clearly now an ideal, either $(b/t)P = A$ or $(b/t)P \subset P$.

Suppose $(b/t)P = A$. Then $1 = bx/t$ for some $x \in P$, which implies $(t) \subset (x)$. By maximality of $(t) \subset P$, we would have $(t) = (x)$ hence $x = ct$ and $1 = bc$, contradicting the fact that $b \in P$ cannot be a unit. But if $(b/t)P \subset P$, then by Preliminary 3, $b/t \notin A$ is integral over A, contradicting the assumption that A is integrally closed. Thus $(t) = P$. ∎

Preliminary 5 Fractional ideals. Let A be a Noetherian domain with field of fractions K. By a fractional ideal $\Gamma \subset K$ we mean a non-zero A-submodule of K that satisfies any of the four equivalent conditions below. (It is an easy to see that the conditions are equivalent via $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.)

(i) $c\Gamma \subset A$ for some $c \in A$, $c \neq 0$. (Of course $c\Gamma = I$ is then an ideal in A, and $\Gamma = (1/c)I$.)
(ii) $c\Gamma \subset A$ for some $c \in K$, $c \neq 0$.
(iii) $\Gamma \subset (1/c)A$ for some $c \in K$.
(iv) $\Gamma \subset K$ is a finitely generated A-submodule of K

Prelim 5.1 The product $\Gamma\Delta$ of two fractional ideals is a fractional ideal, where the product means $\{\sum_i x_i y_i \mid x_i \in \Gamma, y_i \in \Delta\}$.

Prelim 5.2 If Γ is a fractional ideal then so is $(A : \Gamma) = \{x \in K \mid x\Gamma \subset A\}$.

For 5.1, just multiply two appropriate c's from condition (i). For 5.2, just take c to be any non-zero element of Γ.

Of course all ideals of A are fractional ideals. The unit ideal A itself acts as a unit for the product operation, $A\Gamma = \Gamma$. The notion of fractional ideal is especially important if A is a Dedekind domain.

Proposition 2 *If A is a Dedekind domain then all fractional ideals are invertible. In fact,*

$$\Gamma(A : \Gamma) = A.$$

Proof We will first prove $P(A : P) = A$ for a non-zero prime ideal $P \subset A$. To begin, we show $(A : P)$ *properly* contains A. Pick any non-zero element $a \in P$, and find primes (not necessarily distinct) with $P_1 \cdots P_r \subset (a) \subset P$. Then P must occur among the P_j. We assume r is least. Of course, if $(a) = P$ then $1/a \in (A : P)$ and we are done. Otherwise, say $P = P_1$ and choose $b \in P_2 \cdots P_r$ but $b \notin (a)$. Then $x = b/a \notin A$. However, $bP \subset (a)$, so $(b/a)P \subset A$ and $b/a \in (A : P)$, as desired.

Now, $P(A : P)$ is clearly an ideal of A containing P. Since P is maximal, either $P(A : P) = P$ or $P(A : P) = A$. But we just produced $x \notin A$ with $x \in (A : P)$. Then $xP \subset P$ would imply x integral over A by Preliminary 3. This contradicts A integrally closed. Therefore, we have established $P(A : P) = A$.

Next, we observe any ideal $I = P_1 P_2 \cdots P_s$ is invertible. Namely, pick off one prime at a time by multiplying I by the product $(A : P_s) \cdots (A : P_1) = \Delta$. It now also follows that $\Delta = (A : I)$, because $\Delta I = A$ immediately gives $\Delta \subset (A : I)$ and multiplying the inclusion $I(A : I) \subset A$ by Δ gives $(A : I) \subset \Delta$.

Finally, if Γ is any fractional ideal, we have $(c)\Gamma = I \subset A$, an ideal, for some $c \in A$. Thus, $\Gamma = (A : (c))I$ and $\Gamma^{-1} = (c)(A : I)$, which is quickly identified with $(A : \Gamma)$. ∎

Corollary 1 *Every fractional ideal Γ is uniquely expressible as a product $\prod_i P_i^{f_i}$ taken over all primes in A, where the f_i are integers with only finitely many non-zero. The set of fractional ideals forms a group under multiplication, and this group is isomorphic to a free abelian group with generators corresponding to the prime ideals.*

PROOF Existence of a factorization comes from $\Gamma = (c)^{-1}I \subset A, c \in A$, along with factorizations of I and (c) as products of positive powers of primes. For uniqueness, just multiply two factorizations by enough positive powers of finitely many primes to get two factorizations of an ideal in A. But we know ideals have unique factorizations. Also, we've proved $\Gamma(A : \Gamma) = A$, so inverses exist. Associativity of the product operation on fractional ideals is trivial. ■

Before continuing with the main development of ideas, we prove here that every fractional ideal is a *projective* A-module. It obviously suffices to consider ideals, because as modules fractional ideals are isomorphic to ideals.

Corollary 2 *If $I \subset A$ is an ideal then I is a direct summand of a free module A^n, some n. Hence all ideals are projective A modules.*

PROOF Since $A = I(A : I)$, write $1 = \sum_i x_i y_i$ with $x_i \in I$ and $y_i \in (A : I)$. Define $p : A^n \to I$ by $p(a_1, \ldots, a_n) = \sum_i x_i a_i$. If $z \in I$, define $s(z) = (y_1 z, \ldots, y_n z) \in A^n$. Then $ps(z) = z$, so p is surjective and s splits an exact sequence $0 \to N \to A^n \to I \to 0$. ■

Corollary 3 $\Delta = \prod_i P_i^{e_i} \subset \prod_i P_i^{f_i} = \Gamma$ *if and only if $e_i \geq f_i$, all i.*

PROOF Just multiply by Γ^{-1}. We know a fractional ideal is an ideal, that is, contained in A, if and only if all exponents are non-negative. ■

Given a prime P, define $\nu_P(\Gamma) = e$ if P^e is the power of P occurring in the factorization of Γ. For a non-zero element $r \in K$, define $\nu_P(r) = \nu_P((r))$.

Corollary 4 *For* finitely many *given primes P_i and integers e_i, there exist elements $r \in K$ with $\nu_{P_i}(r) = e_i$.*

PROOF We will choose $r = a/b$, where $a, b \in A$, so that a takes care of the $e_i \geq 0$ and b takes care of $e_j < 0$. Choose $t_i \in P_i - P_i^2$. By the Chinese Remainder Theorem, choose $a \in A$ so that $a \equiv t_i^{e_i} \bmod P_i^{e_i+1}$ for the $e_i \geq 0$ and so that $a \equiv 1 \bmod P_j$ for the $e_j < 0$. Similarly choose $b \in A$ so that $\nu_{P_j}(b) = |e_j|$ for those $e_j < 0$ and $\nu_{P_i}(b) = 0$ for those $e_i \geq 0$. Then $r = a/b$ works. ■

Corollary 5 *A Dedekind Domain with only finitely many prime ideals is a PID.*

PROOF Call the primes P_i. Given an ideal I, choose $a \in A$ with $\nu_{P_i}(a) = \nu_{P_i}(I)$. Then $(a) = I$ since these two ideals have the same factorization. ■

Note that the sum $\Delta + \Gamma$ and intersection $\Delta \cap \Gamma$ of fractional ideals is a fractional ideal. Clearly sum is an analogue of greatest common divisor and intersection is an analogue of least common multiple. The sum is the smallest fractional ideal containing both Δ and Γ. The intersection is the largest fractional ideal contained in both Δ and Γ.

Corollary 6 *If $\Delta = \prod_i P_i^{e_i}$ and $\Gamma = \prod_i P_i^{f_i}$ then $\Delta + \Gamma = \prod_i P_i^{\min\{e_i, f_i\}}$ and $\Delta \cap \Gamma = \prod_i P_i^{\max\{e_i, f_i\}}$.*

PROOF Just use the inclusion criterion three Corollaries above, along with the characterization of the sum and intersection as smallest and largest fractional ideals with certain properties. ■

Corollary 7 *Every fractional ideal, in particular every ideal of A, can be generated by two elements.*

PROOF Multiply by an element of A to reduce to the case of an ideal I. Write $I = \prod_i P_i^{f_i}$ as a finite product and choose $a \in A$ with $\nu_{P_i}(a) = fi$. Now write $(a) = I \prod_i Q_i^{e_i}$, also a finite product, where the Q_i are different from all P_i. Choose $b \in A$ with $\nu_{P_i}(b) = f_i + 1$ and $\nu_{Q_i}(b) = 0$. Then $I = (a) + (b)$. ■

Remark 1 Combined with the proof above that all ideals are projective A-modules, we see this last result implies every ideal is a direct summand of A^2. □

For later use, we record one more observation.

Corollary 8 *If Q is a prime ideal in a Dedekind domain B, then Q^i/Q^{i+1} is a one-dimensional vector space over B/Q.*

PROOF Take $x \in Q^i - Q^{i+1}$. Then $Q^i = (x) + Q^{i+1}$ since these ideals have the same factorization. ■

One can prove this last important result by more direct methods, just using the theorem that the local Dedekind domain $B_{(Q)}$ is a PID, which was the starting point for the factorization theory. Namely, choose $t \in Q - Q^2$, so $(t)B_{(Q)} = QB_{(Q)}$. Then if $z \in Q^i$, we get $z = t^i y/s \in B_{(Q)}$ for some $s \notin Q$. Since (s) and Q^{i+1} are comaximal ideals in B, we can write $1 = as + b$, with $b \in Q^{i+1}$. Then $z = azs + bz = at^i y + bz$. Hence $Q^i = (t^i) + Q^{i+1}$.

We now take $A = \mathbb{Z}$, the integers, with field of fractions $\mathbb{Q}$, the rationals, and we take B to be the integral closure of $\mathbb{Z}$ in a finite extension E of $\mathbb{Q}$. We investigate how prime ideals $(p) \subset \mathbb{Z}$ factor in B.

Write $pB = \prod_{i=1}^d Q_i^{e_i}$, a finite product of distinct prime powers. By the Chinese Remainder Theorem, $B/pB = \prod_i B/Q_i^{e_i}$ as rings. We can also regard both sides of this equation as $\mathbb{Z}/(p)$ vector spaces, hence they have the same dimension as $\mathbb{Z}/(p)$ vector spaces. Note that $pB \subset Q_i^{e_i}$, so $B/Q_i^{e_i}$ is indeed a $\mathbb{Z}/(p)$ vector space.

Proposition 3 *Let $n = |E : \mathbb{Q}|$ be the degree of E over the rational numbers. Let $f_i = |B/Q_i : \mathbb{Z}/(p)|$, where $pB = \prod_{i=1}^d Q_i^{e_i}$. Then $n = \sum_{i=1}^d e_i f_i$.*

PROOF We know that *additively* $B \cong \mathbb{Z}^n$, so B/pB has dimension n as a $\mathbb{Z}/(p)$-vector space. We show that each $B/Q_i^{e_i}$ has dimension $e_i f_i$ as a $\mathbb{Z}/(p)$-vector space. The Proposition follows since $B/pB = \prod_i B/Q_i^{e_i}$ as rings.

Study B/Q^e by exploiting the filtration $B/Q^e \supset Q/Q^e \supset Q^2/Q^e \supset \cdots \supset Q^e/Q^e = (0)$.

Each successive quotient $(Q^j/Q^e)/(Q^{j+1}/Q^e) = Q^j/Q^{j+1}$ is a one-dimensional vector space over B/Q, hence has dimension $f = |B/Q : \mathbb{Z}/(p)|$ over $\mathbb{Z}/(p)$. Therefore B/Q^e has dimension ef over $\mathbb{Z}/(p)$ and the Proposition is proved. ■

Proposition 4 *Suppose $\mathbb{Q} \subset E$ is a finite* Galois *extension, $p \in \mathbb{Z}$ prime. Then $pB = \prod_{i=1}^{d} Q_i^e$, that is, all prime power exponents are the same. Moreover, $n = def$, where d is the number of distinct primes in B lying over (p), $f = |B/Q : \mathbb{Z}/(p)|$ for any such prime Q, and e is the common exponent of all prime factors.*

PROOF We know the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ acts transitively on the primes above (p). Thus if we write $pB = \prod_{i=1}^{d} Q_i^{e_i}$ and apply Galois automorphisms, we conclude all e_i must be the same by unique factorization of the ideal pB. Also, all the fields B/Q_i are isomorphic, so all the f_i must be the same. Thus $n = \sum_{i=1}^{d} e_i f_i = def$. ∎

Remark 2 Recall that if Q is one prime in B over (p) then we have the decomposition group $G^Z = G^Z(Q) \subset G$, consisting of automorphisms σ with $\sigma(Q) = Q$. Thus $d = |G : G^Z|$. Also, we have a surjection $G^Z \to \mathrm{Gal}(B/Q : \mathbb{Z}/(p))$, where this last group has order $f = |B/Q : \mathbb{Z}/(p)|$. The inertia group of Q is defined to be $G^T = G^T(Q) = \ker(G^Z \to \mathrm{Gal}(B/Q : \mathbb{Z}/(p)))$. From $G \supset G^Z \supset G^T \supset \{1\}$, we see $d = |G : G^Z|$, $f = |G^Z : G^T|$, and, necessarily $e = |G^T|$, since $n = def = |G|$. □

Remark 3 There is a useful uniqueness observation about the decomposition $B/pB = \prod_i B/Q_i^{e_i}$ as rings. Each factor $B/Q_i^{e_i}$ has a single prime ideal, hence cannot be further decomposed as a direct product of rings. Anytime a ring can be written as a finite direct product of other rings that are indecomposable, then the decomposition is unique in the sense that two such decompositions will have the same number of factors, which match up isomorphically in pairs. The proof is easy, in fact there is an easy more general uniqueness statement about decomposing modules over a direct product ring. In the case of a factor like B/Q^e, the integer e is uniquely characterized as the smallest power of the prime ideal which is (0). □

Example 2 Consider a quadratic extension $\mathbb{Q}[\sqrt{d}]$, where d is a square-free integer. Then $r + s\sqrt{d}$ with $s \neq 0$ is integral over $\mathbb{Z}$ if and only if the trace $2r$, and the norm $r^2 - ds^2$ are integers. (Trace and norm are the coefficients of the minimal polynomial.) It follows rather quickly that if $d \equiv 2, 3 (\mathrm{mod} 4)$ then the ring of algebraic integers in $\mathbb{Q}[\sqrt{d}]$ is $B = \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1 (\mathrm{mod} 4)$ then $B = \mathbb{Z}[(1 + \sqrt{d})/2]$. Note $b = (1 + \sqrt{d})/2$ is a root of the quadratic equation $x^2 - x - (d-1)/4$.

Let's determine how the ideals $2B$ and $3B$ factor in the ring B of integers in $\mathbb{Q}[\sqrt{13}]$ and $\mathbb{Q}[\sqrt{11}]$. First in the case $\sqrt{13}$, $B = \mathbb{Z}[b]$, where b is a root of $x^2 - x - 3$. Therefore, $B/2B \cong \mathbb{Z}/(2)[x]/(x^2 - x - 3)$, which is a quadratic extension field of $\mathbb{Z}/(2)$. Thus, $2B = Q$ is a prime ideal in B. In the $n = def$ formula, $d = 1$, $f = 2$ and $e = 1$. Continuing, $B/3B \cong \mathbb{Z}/(3)[x]/(x^2 - x - 3) = \mathbb{Z}/(3)[x]/(x^2 - x) = \mathbb{Z}/(3) \times \mathbb{Z}/(3)$. Thus, $3B = Q_1 Q_2$ is a product of two primes in B. In the $n = def$ formula, $d = 2$, $f = 1$, and $e = 1$.

Next, we have $B = \mathbb{Z}[\sqrt{11}] \subset \mathbb{Q}[\sqrt{11}]$. Thus $B/2B \cong \mathbb{Z}/(2)[x]/(x^2 - 11) = \mathbb{Z}/(2)[x]/(x-1)^2$. Lying over the prime 2 in B is a single prime Q. We have $2B = Q^2$. In the $n = def$ formula, $d = 1$, $f = 1$, and $e = 2$. Finally, $B/3B \cong \mathbb{Z}/(3)[x]/(x^2 - 11) = \mathbb{Z}/(3)[x]/(x^2 + 1)$, a quadratic extension of $\mathbb{Z}/(3)$. Thus $3B = Q$ is prime. In the $n = def$ formula, $d = 1$, $f = 2$, and $e = 1$. □

The method above 'works' whenever $B = \mathbb{Z}[\alpha]$. If $f(x) \in \mathbb{Z}[x]$ is the minimal monic polynomial of α then $B/pB \cong \mathbb{Z}/(p)[x]/(f(x))$, and the structure of this ring is obtained by factoring $f(x)$ mod p. However, not all rings of integers in number fields can be expressed in the form $\mathbb{Z}[\alpha]$, and even when this is possible it may be difficult to establish. Further examples of the form $B = \mathbb{Z}[\alpha]$ are

$\mathbb{Z}[\sqrt[3]{2}]$ and $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive pth root of unity, p prime. That these are all the integers in the corresponding extensions of $\mathbb{Q}$ is not easy, but can be shown with enough trace and norm calculations.

As further examples of prime factorizations, $3\mathbb{Z}[\sqrt[3]{2}] = Q^3$, since $x^3 - 2 = (x+1)^3 \bmod 3$, and $5\mathbb{Z}[\sqrt[3]{2}] = Q_1Q_2$, since $x^3 - 2 = (x-3)(x^2+3x-1) \bmod 5$. Here, $\mathbb{Q}[\sqrt[3]{2}]$ is not normal over $\mathbb{Q}$, and in the last example we get $n = 3 = e_1f_1 + e_2f_2 = 1 + 2$. Continuing, $11\mathbb{Z}[\zeta_5] = Q_1Q_2Q_3Q_4$ and $5\mathbb{Z}[\zeta_{11}] = Q_1Q_2$, reflecting the facts that all 5th roots of unity are in $\mathbb{Z}/(11)$ and that the 11th roots of unity are first found in the degree 5 extension of $\mathbb{Z}/(5)$.

In the examples above when $pB = p\mathbb{Z}[\alpha]$ is not prime, it is easy to find generators of the various primes above (p) in $\mathbb{Z}[\alpha]$. If $f(x)$ is the minimal polynomial for α then for each irreducible factor $f_j(x)$ of $f(x) \bmod p$, $Q_j = (p, f_j(\alpha))$ will generate one of the primes of B above (p). This is pretty clear from the formula $B/pB \cong \mathbb{Z}/(p)[x]/(f(x))$, because then $B/Q_j \cong \mathbb{Z}/(p)[x]/(f(x), f_j(x)) = \mathbb{Z}/(p)[x]/(f_j(x))$, which is a field.

Since all non-zero primes in a Dedekind domain B are minimal non-zero primes, it is clear that if B is a UFD then all primes and hence all ideals are principal. Thus UFD and PID are equivalent for Dedekind domains. It is generally difficult to determine if a given B is a PID. If B is the ring of integers in a number field, then an element of B is a unit if and only if its norm is $+1$ or -1 in $\mathbb{Z}$. Here is an example of how norms can sometimes be used to show an ideal can't be principal. With $B = \mathbb{Z}[\sqrt{-5}]$, we get $3B = Q_1Q_2$, where, say, $Q_1 = (3, 1-\sqrt{-5})$. Now $N(3) = 3^2 = 9$, and $N(1-\sqrt{-5}) = (1-\sqrt{-5})(1+\sqrt{-5}) = 6$. If $Q_1 = (z)$, then necessarily $N(z) = +3$ or -3, since both 9 and 6 must be multiples of $N(z)$, and $N(z)$ can't be $+1$ or -1. But $N(a+b\sqrt{-5}) = a^2 + 5b^2$, so clearly neither $+3$ nor -3 can be norms. Another view of this same argument is to note the two factorizations $6 = 2 \cdot 3 = (1-\sqrt{-5}) \cdot (1+\sqrt{-5})$. Since 2 and 3 are not norms, all four factors must be irreducible. Therefore $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

For a final example, we start with a different ground ring, the polynomial ring $A = \mathbb{Q}[x]$. The integral closure of A in a finite field extension $\mathbb{Q}(x)[y]/(f(x,y))$ of $\mathbb{Q}(x)$ will be a Dedekind domain B. Here $f(x,y) \in \mathbb{Q}[x,y]$ is an irreducible polynomial in which y occurs. Consider specifically $f(x,y) = y^3 - x^2 + 1$. It can be shown that $B = \mathbb{Q}[x,y]/(f(x,y))$ is an integrally closed domain. [See the handout on Plane Algebraic Curves.] Therefore B is the integral closure of $\mathbb{Q}[x]$ in the field $\mathbb{Q}(x)[y]/(f(x,y))$. We find factorizations $xB = Q_1Q_2$, $(x-1)B = Q^3$, and $(x^2-5)B = Q$ is prime. Namely, $B/xB \cong \mathbb{Q}[x,y]/(x, f(x,y)) = \mathbb{Q}[y]/(y^3+1)$, which is a product of two fields. Similarly, $B/(x-1)B \cong \mathbb{Q}[y]/(y^3)$ and $B/(x^2-5)B \cong \mathbb{Q}[y]/(y^3-4)$.

Replace $f(x,y)$ by $g(x,y) = y^3 - x^2 - 2$, and you find in the corresponding integral closure that $(x^2+3)B = Q_1Q_2Q_3$. Namely, $B/(x^2+3)B \cong \mathbb{Q}[x,y]/(x^2+3, g(x,y)) = \mathbb{Q}[\sqrt{-3}][y]/(y^3+1)$, which is a product of three fields, each isomorphic to $A/P = \mathbb{Q}[x]/(x^2+3) = \mathbb{Q}[\sqrt{-3}]$.