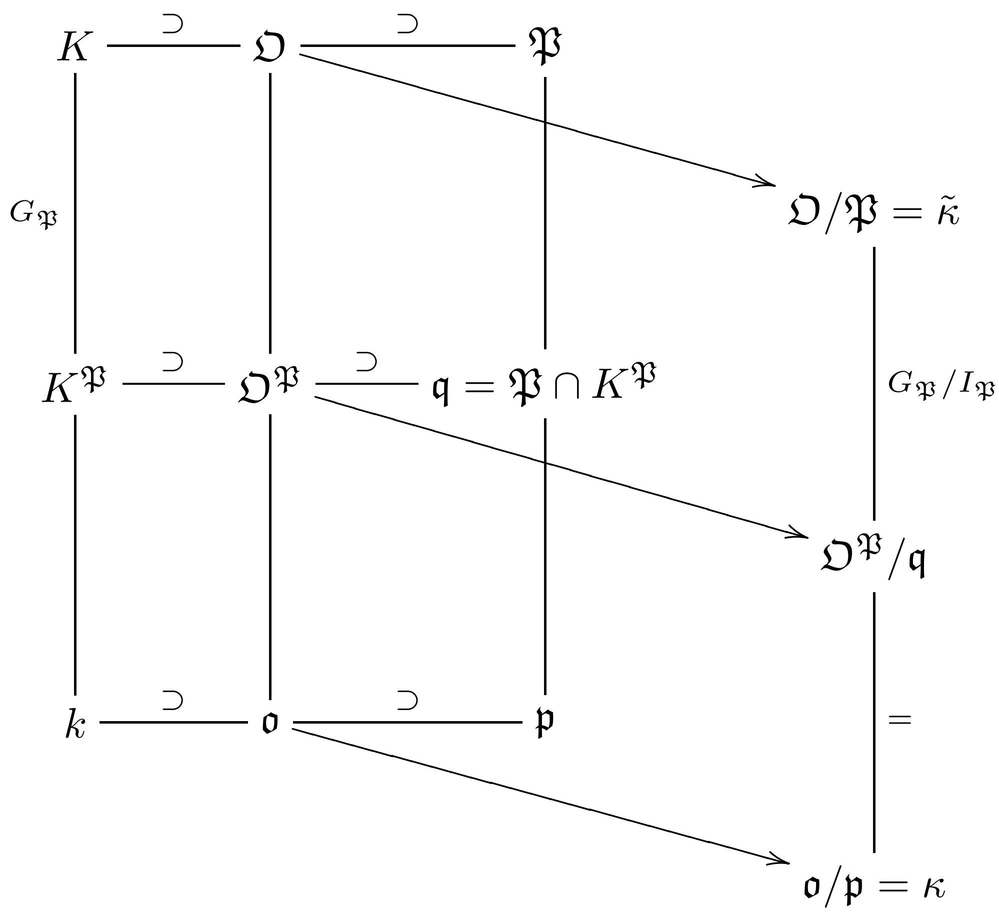
The picture:


K
$\mathfrak{O}$
$\mathfrak{P}$
$\supset$
$G_{\mathfrak{P}}$
$\mathfrak{O}/\mathfrak{P} = \tilde{\kappa}$
$K^{\mathfrak{P}}$
$\mathfrak{O}^{\mathfrak{P}}$
$\mathfrak{q} = \mathfrak{P} \cap K^{\mathfrak{P}}$
$G_{\mathfrak{P}}/I_{\mathfrak{P}}$
$\mathfrak{O}^{\mathfrak{P}}/\mathfrak{q}$
k
$\mathfrak{o}$
$\mathfrak{p}$
$=$
$\mathfrak{o}/\mathfrak{p} = \kappa$

Theorem: In a Noetherian, integrally closed integral domain $\mathfrak{o}$ in which every non-zero prime ideal is *maximal*, every non-zero ideal is *uniquely a product of prime ideals*, and the non-zero fractional ideals form a *group* under multiplication.

Proof: [van der Waerden, Lang] Let $\mathfrak{o}$ be a Noetherian integral domain, integrally closed in its field of fractions, and every non-zero prime ideal is maximal.

First: given non-zero ideal $\mathfrak{a}$, there is a product of non-zero prime ideals *contained in* $\mathfrak{a}$. If not, by Noetherian-ness there is a *maximal* $\mathfrak{a}$ failing to contain a product of primes, and $\mathfrak{a}$ is not prime. Thus, there are $b, c \in \mathfrak{o}$ neither in $\mathfrak{a}$ such that $bc \in \mathfrak{a}$. Thus, $\mathfrak{b} = \mathfrak{a} + \mathfrak{o}b$ and $\mathfrak{c} = \mathfrak{a} + \mathfrak{o}c$ are strictly larger than $\mathfrak{a}$, and $\mathfrak{b}\mathfrak{c} \subset \mathfrak{a}$.

Since $\mathfrak{a}$ was maximal among ideals not containing a product of primes, both $\mathfrak{b}, \mathfrak{c}$ contain such products. But then their product $\mathfrak{b}\mathfrak{c} \subset \mathfrak{a}$ does, contradiction.

Second: for maximal $\mathfrak{m}$, the $\mathfrak{o}$-module $\mathfrak{m}^{-1} = \{x \in k : x\mathfrak{m} \subset \mathfrak{o}\}$ is strictly larger than $\mathfrak{o}$. Certainly $\mathfrak{m}^{-1} \supset \mathfrak{o}$, since $\mathfrak{m}$ is an ideal. We claim that $\mathfrak{m}^{-1}$ is strictly larger than $\mathfrak{o}$. Indeed, for $m \in \mathfrak{m}$ and a (smallest possible) product of primes $\mathfrak{p}_j$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset m\mathfrak{o}$.

Since $m\mathfrak{o} \subset \mathfrak{m}$ and $\mathfrak{m}$ is prime, $\mathfrak{p}_j \subset \mathfrak{m}$ for at least one $\mathfrak{p}_j$, say $\mathfrak{p}_1$. Since every (non-zero) prime is maximal, $\mathfrak{p}_1 = \mathfrak{m}$.

By minimality, $\mathfrak{p}_2 \ldots \mathfrak{p}_n \not\subset m\mathfrak{o}$. That is, there is $y \in \mathfrak{p}_2 \ldots \mathfrak{p}_n$ but $y \notin m\mathfrak{o}$, or $m^{-1}y \notin \mathfrak{o}$. But $y\mathfrak{m} = y\mathfrak{p}_1 \subset m\mathfrak{o}$, so $m^{-1}y\mathfrak{m} \subset \mathfrak{o}$, and $m^{-1}y \in \mathfrak{m}^{-1}$ but not in $\mathfrak{o}$.

Third: maximal $\mathfrak{m}$ is invertible. By this point, $\mathfrak{m} \subset \mathfrak{m}^{-1}\mathfrak{m} \subset \mathfrak{o}$. By maximality of $\mathfrak{m}$, either $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$ or $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$.

The Noetherian-ness of $\mathfrak{o}$ implies that $\mathfrak{m}$ is finitely-generated. A relation $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$ would show that $\mathfrak{m}^{-1}$ stabilizes a non-zero, finitely-generated $\mathfrak{o}$-module. Since $\mathfrak{o}$ is integrally closed in k, this would give $\mathfrak{m}^{-1} \subset \mathfrak{o}$, but we have seen otherwise. Thus, we have the inversion relation $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$ for maximal $\mathfrak{m}$.

Fourth: every non-zero ideal $\mathfrak{a}$ has inverse $\mathfrak{a}^{-1} = \{y \in k : y\mathfrak{a} \subset \mathfrak{o}\}$. If not, there is maximal $\mathfrak{a}$ *failing* this, and $\mathfrak{a}$ cannot be a maximal ideal, by the previous step. Thus, $\mathfrak{a}$ is *properly* contained in some maximal ideal $\mathfrak{m}$. Certainly $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{o}$. Integral-closedness of $\mathfrak{o}$ and $\mathfrak{m}^{-1} \neq \mathfrak{o}$, $\mathfrak{m}^{-1} \supset \mathfrak{o}$ show that $\mathfrak{m}^{-1}\mathfrak{a} \not\subset \mathfrak{a}$.

Since $\mathfrak{m}^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$, it has inverse $\mathfrak{f}$. Thus, $(\mathfrak{f}\mathfrak{m}^{-1})\mathfrak{a} = \mathfrak{f}(\mathfrak{m}^{-1}\mathfrak{a}) = \mathfrak{o}$, and $\mathfrak{f}\mathfrak{m}^{-1}$ is an inverse for $\mathfrak{a}$, contradiction.

Fifth: ideals $\mathfrak{a}$ have *unique* inverses. For fractional ideal $\mathfrak{f}$ such that $\mathfrak{f}\mathfrak{a} = \mathfrak{o}$, certainly $\mathfrak{f} \subset \{y \in k : y\mathfrak{a} \subset \mathfrak{o}\}$. On the other hand, for $y\mathfrak{a} \subset \mathfrak{o}$, multiply by $\mathfrak{f}$ to obtain $y\mathfrak{a}\mathfrak{f} \subset \mathfrak{f}$. Since $\mathfrak{a}\mathfrak{f} = \mathfrak{o} \ni 1$, $y \in \mathfrak{f}$.

Sixth: every *fractional* ideal $\mathfrak{f}$ is uniquely *invertible*, and $\mathfrak{a} \subset \mathfrak{b}$ implies $\mathfrak{a}^{-1} \supset \mathfrak{b}^{-1}$. Let $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{f} \subset \mathfrak{o}$. Then $c\mathfrak{f}$ has unique inverse $\mathfrak{k}$, and $\mathfrak{f}$ has unique inverse $c^{-1}\mathfrak{k}$. For $\mathfrak{a} \subset \mathfrak{b}$, visibly $\{x \in k : x\mathfrak{a} \subset \mathfrak{o}\} \supset \{x \in k : x\mathfrak{b} \subset \mathfrak{o}\}$, so inversion is inclusion-reversing.

Seventh: every ideal $\mathfrak{a}$ is a product of prime ideals. If not, let $\mathfrak{a}$ be maximal among failures. It is not prime, so is properly contained in maximal $\mathfrak{m}$. Then $\mathfrak{a} \subset \mathfrak{m}$ gives $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{o}$. Invertibility of fractional ideals gives $\mathfrak{m}^{-1}\mathfrak{a} \neq \mathfrak{o}$ and $\mathfrak{m}^{-1}\mathfrak{a} \neq \mathfrak{a}$. Thus, $\mathfrak{m}^{-1}\mathfrak{a}$ is a proper ideal strictly larger than $\mathfrak{a}$, and is a product of primes. Multiplication by $\mathfrak{m}$ expresses $\mathfrak{a}$ as a product, contradiction.

Eighth: for *fractional* ideals $\mathfrak{a}, \mathfrak{b}$, the **divisibility** property $\mathfrak{a}|\mathfrak{b}$, meaning there is an *ideal* $\mathfrak{c}$ such that $\mathfrak{c} \cdot \mathfrak{a} = \mathfrak{b}$, is equivalent to $\mathfrak{a} \supset \mathfrak{b}$. Indeed, on one hand, $\mathfrak{c} \subset \mathfrak{o}$ gives $\mathfrak{b} = \mathfrak{c}\mathfrak{a} \subset \mathfrak{o}\mathfrak{a} = \mathfrak{a}$. On the other hand, for $\mathfrak{a} \supset \mathfrak{b}$, since inversion is inclusion-reversing, $\mathfrak{a}^{-1} \subset \mathfrak{b}^{-1}$, so $\mathfrak{c} \subset \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{o}$.

Ninth: unique factorization of ideals into primes. The definition of prime ideal $\mathfrak{p}$ gives $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ only when $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$, for ideals $\mathfrak{a}, \mathfrak{b}$. That is, $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$. Given two factorizations

$$\mathfrak{p}_1 \ldots \mathfrak{p}_m \;=\; \mathfrak{a} \;=\; \mathfrak{q}_1 \ldots \mathfrak{q}_n$$

$\mathfrak{p}_1$ must divide some $\mathfrak{q}_j$, thus, $\mathfrak{p}_1 \;=\; \mathfrak{q}_j$. Renumber so $\mathfrak{p}_1 \;=\; \mathfrak{q}_1$. Using *invertibility*, multiply by $\mathfrak{p}_1^{-1}$, obtaining $\mathfrak{p}_2 \ldots \mathfrak{p}_m = \mathfrak{q}_2 \ldots \mathfrak{q}_n$ and use induction.

Tenth: unique factorization of *fractional ideals*. Given fractional $\mathfrak{a}$, take $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$. Let $c\mathfrak{o} = \mathfrak{q}_1 \ldots \mathfrak{q}_n$. Then

$$\mathfrak{a} \;=\; (\mathfrak{p}_1 \ldots \mathfrak{p}_m) \cdot (\mathfrak{q}_1 \ldots \mathfrak{q}_n)^{-1} \;=\; \frac{\mathfrak{p}_1 \ldots \mathfrak{p}_m}{\mathfrak{q}_1 \ldots \mathfrak{q}_n}$$

Cancel any common factors. ///

The **order** $\mathrm{ord}_\mathfrak{p}\mathfrak{a}$ at prime $\mathfrak{p}$ of a (non-zero) fractional ideal $\mathfrak{a}$ is the integer exponent of $\mathfrak{p}$ appearing in a factorization of $\mathfrak{a}$:

$$\mathfrak{a} \;=\; \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}\,\mathfrak{a}} \cdot (\text{primes distinct from } \mathfrak{p})$$

Similarly for $\alpha \in k^\times$, $\mathrm{ord}_\mathfrak{p}\alpha = \mathrm{ord}_\mathfrak{p}\alpha\mathfrak{o}$.

Elements or fractional ideals are **(locally) integral at** $\mathfrak{p}$, when their $\mathfrak{p}$-orders are non-negative. An element is a $\mathfrak{p}$-**unit** when its $\mathfrak{p}$-ord is 0.

Corollary: For Dedekind $\mathfrak{o}$, an element $\alpha \in k$ is in $\mathfrak{o}$ if and only if it is $\mathfrak{p}$-integral everywhere locally. A fractional ideal $\mathfrak{f}$ is a genuine ideal if and only if it is $\mathfrak{p}$-integral everywhere locally.

Proof: Unique factorization: if $\mathfrak{f} = (\mathfrak{p}_1 \ldots \mathfrak{p}_m) \cdot (\mathfrak{q}_1 \ldots \mathfrak{q}_n)^{-1}$ is inside $\mathfrak{o}$, then $\mathfrak{p}_1 \ldots \mathfrak{p}_m \subset \mathfrak{q}_1 \ldots \mathfrak{q}_n$. ///

Lemma: Localization $S^{-1}\mathfrak{o}$ is Dedekind. The primes of $S^{-1}\mathfrak{o}$ are $S^{-1}\mathfrak{p}$ for primes $\mathfrak{p}$ of $\mathfrak{o}$ not meeting S. Factorization of fractional ideals behaves like

$$S^{-1}\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}\Big) \;=\; \prod_{\mathfrak{p}:\,\mathfrak{p}\cap S=\phi} (S^{-1}\mathfrak{p})^{e(\mathfrak{p})}$$

Proof: The integral domain property is preserved, because $S^{-1}\mathfrak{o}$ sits inside the field of fractions. Noetherian-ness is preserved: there are fewer ideals in $S^{-1}\mathfrak{o}$ than in $\mathfrak{o}$. Integral closedness: for $\alpha \in k$ integral over $S^{-1}\mathfrak{o}$, multiply out the denominators (from S) of the coefficients, obtaining an equation of the form

$$s \cdot \alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_o \;=\; 0 \qquad\qquad \text{(with } s \in S\text{)}$$

Thus,

$$(s\alpha)^n + (c_{n-1}s)\cdot(s\alpha)^{n-1} + \ldots + (c_1 s^{n-1})(s\alpha) + (s^n c_o) \;=\; 0$$

By integral closedness, $s\alpha \in \mathfrak{o}$, and $\alpha \in S^{-1}\mathfrak{o}$.

A prime $\mathfrak{p}$ meeting S becomes the whole ring $S^{-1}\mathfrak{o}$. For $\mathfrak{p}$ not meeting S, if $(x/s)(y/t) = z/u$ with $x, y \in \mathfrak{o}$, $z \in \mathfrak{p}$, and $s, t, u \in S$, then $u \cdot xy = st \cdot z$. Since $z \in \mathfrak{p}$ and $u \notin \mathfrak{p}$, $xy \in \mathfrak{p}$. Thus, $S^{-1}\mathfrak{p}$ is prime. Likewise, non-zero primes are *maximal*.

If $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$ for primes $\mathfrak{p}, \mathfrak{q}$, then $s\mathfrak{p} = \mathfrak{q}$ for some $s \in S \subset \mathfrak{o}$. Unique factorization of $s \cdot \mathfrak{o}$ shows $s \in \mathfrak{o}^\times$ and $\mathfrak{p} = \mathfrak{q}$.

Finally, with S containing 1 and closed under multiplication, $S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a}) \cdot (S^{-1}\mathfrak{b})$ for all fractional ideals $\mathfrak{a}, \mathfrak{b}$, from the definition of the multiplication $\mathfrak{a} \cdot \mathfrak{b}$. This gives the factorization in the localization. ///

When we only care about finitely-many primes...:

Proposition: Dedekind with finitely-many primes $\Rightarrow$ PID.

Proof: Let the primes be $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Since $\mathfrak{p}_j^2 \neq \mathfrak{p}_j$, there is $\varpi_j \in \mathfrak{p}_j - \mathfrak{p}_j^2$. Given $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$, Sun-Ze's theorem gives a solution in $\mathfrak{o}$ of

$$x = \varpi_j^{e_j} \bmod \mathfrak{p}_j^{e_j+1} \qquad \text{(for } j = 1, \ldots, n\text{)}$$

The principal ideal $x\mathfrak{o}$ has a prime factorization, with the same exponents as $\mathfrak{a}$. ///

Corollary: The localization of Dedekind $\mathfrak{o}$ at a prime $\mathfrak{p}$ is a PID, with unique prime $(\mathfrak{o} - \mathfrak{p})^{-1} \cdot \mathfrak{p}$. ///

Big Corollary: For Dedekind $\mathfrak{o}$ in field of fractions k, the integral closure $\mathfrak{O}$ in a finite separable extension K/k is Dedekind.

Proof: Use the theorem characterizing Dedekind domains. $\mathfrak{O}$ is an integral domain and is integrally closed. By the Lying-Over theorem, primes $\mathfrak{P}$ in $\mathfrak{O}$ over non-zero, hence maximal, primes $\mathfrak{p}$ in $\mathfrak{o}$ are maximal.

Conversely, any prime $\mathfrak{P}$ of $\mathfrak{O}$ meets $\mathfrak{o}$ in a prime ideal $\mathfrak{p}$. As observed earlier, $\mathfrak{p}$ cannot be 0, because Galois norms from $\mathfrak{P}$ are in $\mathfrak{o} \cap \mathfrak{P}$ and are non-zero. Thus, $\mathfrak{p}$ is maximal, and by Lying-Over $\mathfrak{P}$ is maximal.

Noetherian-ness follows from the earlier result that $\mathfrak{O}$ is finitely-generated over $\mathfrak{o}$, using the non-degeneracy of the *trace pairing* corresponding to the finite separable extension K/k. ///

Ramification, residue field extension degrees: e, f, g

Prime $\mathfrak{p}$ in $\mathfrak{o}$ factors in an integral extension as $\mathfrak{p}\mathfrak{O} = \prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$. The exponents $e(\mathfrak{P}/\mathfrak{p})$ are **ramification** indices.

The residue field extensions $\tilde{\kappa} = \mathfrak{O}/\mathfrak{P}$ over $\kappa = \mathfrak{o}/\mathfrak{p}$ have degrees $f(\mathfrak{P}/\mathfrak{p}) = [\tilde{\kappa} : \kappa]$.

Theorem: For fixed $\mathfrak{p}$ in $\mathfrak{o}$,

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \quad = \quad [K : k]$$

For K/k Galois, the ramification indices e and residue field extension degrees f depend only on $\mathfrak{p}$ (and K/k), and in that case

$$e \cdot f \cdot (\text{number of primes } \mathfrak{P}|\mathfrak{p}) \quad = \quad [K : k]$$
