Recap: about Dedekind domains...

Theorem: A Noetherian, integrally closed, integral domain with every non-zero prime ideal maximal, ... *has unique factorization:* non-zero ideals are uniquely products of prime ideals, and non-zero fractional ideals form a *group*.

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.

Lemma: $S^{-1}\mathfrak{o}$ is Dedekind. Primes of $S^{-1}\mathfrak{o}$ are $S^{-1}\mathfrak{p}$ for primes $\mathfrak{p}$ of $\mathfrak{o}$ not meeting S. Factorization is

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

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

Continuing ...

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 $f(\mathfrak{P}/\mathfrak{p}) = [\tilde{\kappa} : \kappa]$. When K/k is Galois,

$$e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \;=\; |G_{\mathfrak{P}}| \qquad\qquad e(\mathfrak{P}/\mathfrak{p}) \;=\; |I_{\mathfrak{P}}|$$

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

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

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

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

Proof: We first treat the case that $\mathfrak{o}$ and $\mathfrak{O}$ are PIDs, and then reduce to this case by localizing. As usual, Sun-Ze's theorem gives

$$\mathfrak{O}/\mathfrak{p}\mathfrak{O} \approx \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$$

For $\mathfrak{o}$ a PID, $\mathfrak{O}$ is a free $\mathfrak{o}$-module of rank $[K : k]$. Then $\mathfrak{O}/\mathfrak{p}\mathfrak{O}$ is a $\kappa = \mathfrak{o}/\mathfrak{p}$-vectorspace of dimension $[K : k]$. Each $\mathfrak{O}/\mathfrak{P}^e$ is a κ-vectorspace, and the sum of their dimensions is $[K : k]$. The κ-dimension of $\mathfrak{O}/\mathfrak{P}$ is $f(\mathfrak{P}/\mathfrak{p})$. The slightly more complicated $\mathfrak{O}/\mathfrak{P}^e$ require slightly more effort.

The chain of κ-vectorspaces

$$\{0\} = \mathfrak{P}^e/\mathfrak{P}^e \subset \mathfrak{P}^{e-1}/\mathfrak{P}^e \subset \ldots \subset \mathfrak{P}^2/\mathfrak{P}^e \subset \mathfrak{P}/\mathfrak{P}^e \subset \mathfrak{O}/\mathfrak{P}^e$$

has consecutive quotients

$$\big(\mathfrak{P}^i/\mathfrak{P}^e\big)/\big(\mathfrak{P}^{i+1}/\mathfrak{P}^e\big) \approx \mathfrak{P}^i/\mathfrak{P}^{i+1}$$

Using the fact that $\mathfrak{O}$ is a PID, let ϖ generate $\mathfrak{P}$. Visibly, $\mathfrak{P}^{i+1}/\mathfrak{P}^i \approx \mathfrak{O}/\mathfrak{P}$ by the map

$$x + \mathfrak{O}\varpi \quad \longrightarrow \quad \varpi^i x + \mathfrak{O}\varpi^{i+1} \qquad\qquad \text{(multiplication by } \varpi^i\text{)}$$

In general, for a chain $\{0\} = V_o \subset V_1 \subset \ldots \subset V_{e-1} \subset V_e$ of finite-dimensional vectorspaces, we have

$$\dim V_e \;=\; \dim(V_1/V_o) + \dim(V_2/V_1) + \ldots + \dim(V_e/V_{e-1})$$

In the case at hand, the dimensions of the consecutive quotients are all $f(\mathfrak{P}/\mathfrak{p})$, so

$$\dim_\kappa \mathfrak{O}/\mathfrak{P}^e \;=\; e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p})$$

and $[K : k] \;=\; \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p})$. The transitivity of Galois on $\mathfrak{P}|\mathfrak{p}$ gives equality among the e, fs in the Galois case.

Now reduce to the case that $\mathfrak{o}$ is a PID, by *localizing* at $\mathfrak{p}$, thus leaving a single prime. We must show that localizing at $S = \mathfrak{o} - \mathfrak{p}$ does not change the e, fs.

A factorization $\mathfrak{p}\mathfrak{O} = \prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$ gives a corresponding

$$(S^{-1}\mathfrak{p})(S^{-1}\mathfrak{O}) = \prod_{\mathfrak{P}} (S^{-1}\mathfrak{P})^{e(\mathfrak{P}/\mathfrak{p})}$$

The primes of $\mathfrak{O}$ surviving to $S^{-1}\mathfrak{O}$ are exactly those lying over $\mathfrak{p}$, seen as follows. For $\mathfrak{P}$ to lie over $\mathfrak{p}$ means that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$. Since $S \subset \mathfrak{o}$, and $\mathfrak{p} \cap S = \phi$, $\mathfrak{P} \cap S = \phi$ for $\mathfrak{P}$ lying over $\mathfrak{p}$. For all other $\mathfrak{P}$, $\mathfrak{P} \cap \mathfrak{o}$ is a prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of $\mathfrak{o}$. Taking Galois norms shows that $\mathfrak{q} \neq \{0\}$, so $S \cap \mathfrak{q} \neq \phi$, and $S^{-1}\mathfrak{P} = \mathfrak{O}$.

Thus, the ramification indices $e(\mathfrak{P}/\mathfrak{p})$ are unchanged by localizing.

Next, show that the residue field extension degrees are unchanged by localization. First, *claim/recall* that $\mathfrak{o}/\mathfrak{p} \quad \approx \quad S^{-1}\mathfrak{o}/S^{-1}\mathfrak{p}$. Indeed, $\mathfrak{o} \to S^{-1}\mathfrak{o} \to S^{-1}\mathfrak{o}/S^{-1}\mathfrak{p}$ has kernel $\mathfrak{o} \cap S^{-1}\mathfrak{p}$. For $sx \in \mathfrak{p}$ with $s \in S$ and $x \in \mathfrak{o}$, then $x \in \mathfrak{p}$ by primality of $\mathfrak{p}$ and $S \cap \mathfrak{p} = \phi$. This gives injectivity.

For surjectivity, given $\frac{x}{s} + S^{-1}\mathfrak{p}$, find $y \in \mathfrak{o}$ such that $y - \frac{x}{s} \in S^{-1}\mathfrak{p}$. It suffices to have $sy - x \in \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, $s\mathfrak{o} + \mathfrak{p} = \mathfrak{o}$, so there is $z \in \mathfrak{o}$ such that $sz - 1 \in \mathfrak{p}$. Multiplying through by x gives $(xz)s - x \in x\mathfrak{p} \subset \mathfrak{p}$, proving surjectivity.

Similarly, *claim* that $\mathfrak{O}/\mathfrak{P} \approx S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$ for $\mathfrak{P}|\mathfrak{p}$. The kernel of

$$\mathfrak{O} \longrightarrow S^{-1}\mathfrak{O} \longrightarrow S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$$

is $\mathfrak{O} \cap S^{-1}\mathfrak{P}$. For $sx \in \mathfrak{P}$ with $x \in \mathfrak{O}$ and $s \in S$, then either $s \in \mathfrak{P}$ or $x \in \mathfrak{P}$. Since $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$ and $S \subset \mathfrak{o}$, $\mathfrak{P} \cap S = \phi$. Thus, $x \in \mathfrak{P}$, and $\mathfrak{O}/\mathfrak{P} \to S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$ is *injective*.

For surjectivity, given $\frac{x}{s} + S^{-1}\mathfrak{P}$, find $y \in \mathfrak{O}$ such that $y - \frac{x}{s} \in S^{-1}\mathfrak{P}$. It suffices to have $sy - x \in \mathfrak{P}$. Since $\mathfrak{p}$ is maximal, $s\mathfrak{o} + \mathfrak{p} = \mathfrak{o}$, so there is $z \in \mathfrak{o}$ such that $sz - 1 \in \mathfrak{p} \subset \mathfrak{P}$. Multiplying through by x gives $(xz)s - x \in x\mathfrak{P} \subset \mathfrak{P}$, proving surjectivity.

Thus, we can localize at $S = \mathfrak{o} - \mathfrak{p}$ without changing the e, fs, thereby assuming without loss of generality that $\mathfrak{o}$ and $\mathfrak{O}$ are PIDs, being Dedekind with finitely-many primes. ///

Proposition: The e, f's are *multiplicative in towers*, that is, for separable extensions $k \subset E \subset K$ and corresponding primes $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{P}$,

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}) \cdot e(\mathfrak{P}/\mathfrak{q}) \qquad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{q})$$

Proof: This follows from the ideas of the previous proof, together with the fact from field theory that for fields $\kappa \subset \kappa' \subset \tilde{\kappa}$, $\dim_\kappa \tilde{\kappa} = \dim_\kappa \kappa' \cdot \dim_{\kappa'} \tilde{\kappa}$ ///

Remark: The incidental fact that localization at $\mathfrak{p}$ does not alter the $e(\mathfrak{P}/\mathfrak{p})$s and $f(\mathfrak{P}/\mathfrak{p})$'s for $\mathfrak{P}|\mathfrak{p}$ will be re-used on several later occasions. For example:

Proposition: For $\alpha \neq 0$ in the integral closure $\mathfrak{O}$ of $\mathbb{Z}$ in a number field K, the Galois norm and ideal norm are essentially the same:

$$|N_{\mathbb{Q}}^K(\alpha)| \;=\; N(\alpha\mathfrak{O})$$

with *ideal* norm $N(\mathfrak{A}) = \#\mathfrak{O}/\mathfrak{A}$ for ideals $\mathfrak{A}$ in $\mathfrak{O}$.

A stronger assertion has a simpler proof. To set it up, define a variant notion of *ideal* norm N_k^K from fractional ideals of $\mathfrak{O}$ to fractional ideals of $\mathfrak{o}$, first on primes $\mathfrak{P}$ of $\mathfrak{O}$, by

$$\text{(ideal-norm)}\; N_k^K\mathfrak{P} \;=\; \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} \qquad \text{(for } \mathfrak{P}|\mathfrak{p})$$

and extend this to the group of fractional ideals by multiplicativity:

$$\text{(ideal-norm)}\, N_k^K \Big(\prod_{\mathfrak{P}} \mathfrak{P}^{\ell_{\mathfrak{P}}}\Big) \;=\; \prod_{\mathfrak{P}} (N_k^K \mathfrak{P})^{\ell_{\mathfrak{P}}}$$

Proposition: With $\mathfrak{o} \subset k$ and $\mathfrak{O} \subset K$ as usual, for $0 \neq \alpha \in \mathfrak{O}$,

$$\text{(ideal-norm)}\, N_k^K(\alpha\mathfrak{O}) \;=\; \mathfrak{o} \cdot \text{(Galois norm)}\, N_k^K(\alpha)$$

Proof: Without loss of generality, we can take K/k Galois, since extending to the Galois closure E of K over k has the effect of raising everything to the $[E:K]$ power. With $G = \mathrm{Gal}(K/k)$,

$$\prod_{\sigma\in G} \sigma\mathfrak{P} \;=\; \prod_{\sigma\in G/G_{\mathfrak{P}}} (\sigma\mathfrak{P})^{ef} \;=\; \Big(\prod_{\mathfrak{P}_i|\mathfrak{p}} \mathfrak{P}_i^e\Big)^f \;=\; \mathfrak{p}^f \cdot \mathfrak{O}$$

Thus, for an ideal $\mathfrak{A}$ of $\mathfrak{O}$, $\prod_{\sigma\in G} \sigma\mathfrak{A} \;=\; \text{(ideal-norm)}\, N_k^K \mathfrak{A} \cdot \mathfrak{O}$

On the other hand,

$$\prod_{\sigma\in G} \sigma(\alpha\mathfrak{O}) \;=\; \Big(\prod_{\sigma\in G} \sigma(\alpha)\Big)\cdot\mathfrak{O} \;=\; (\text{Galois-norm})\, N_k^K(\alpha)\cdot\mathfrak{O}$$

Combining these,

$$(\text{ideal-norm})\ N_k^K(\alpha\mathfrak{O})\cdot\mathfrak{O} \;=\; (\text{Galois-norm})\ N_k^K(\alpha)\cdot\mathfrak{O}$$

The ideal norm $N_k^K(\alpha\mathfrak{O})$ is in $\mathfrak{o}$, by definition, and $N_k^K(\alpha)$ is in $\mathfrak{o}$. Unique factorization into prime ideals in $\mathfrak{O}$ proves

$$(\text{ideal-norm})\ N_k^K(\alpha\mathfrak{O})\cdot\mathfrak{o} \;=\; (\text{Galois-norm})\ N_k^K(\alpha)\cdot\mathfrak{o}$$

as claimed. ///

Equality of ideal and Galois norms eliminates ambiguities in comparing the following general definition to simpler instances.

Now $\mathfrak{o}$ must have *finite residue fields.* It suffices that its field of fractions k is either a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(x)$.

And revert to using the *ideal norm* unadorned N to refer to the ideal norm $N\mathfrak{a} = \#\mathfrak{o}/\mathfrak{a}$.

Dedekind zeta functions: Even though the subscript should make a reference to the ring $\mathfrak{o}$ rather than k, the ring $\mathfrak{o}$ is essentially implied by specifying the field k. (This is not quite true for functions fields, but never mind.)

$$\zeta_k(s) \;=\; \sum_{0\neq\mathfrak{a}\subset\mathfrak{o}} \frac{1}{N\mathfrak{a}^s}$$

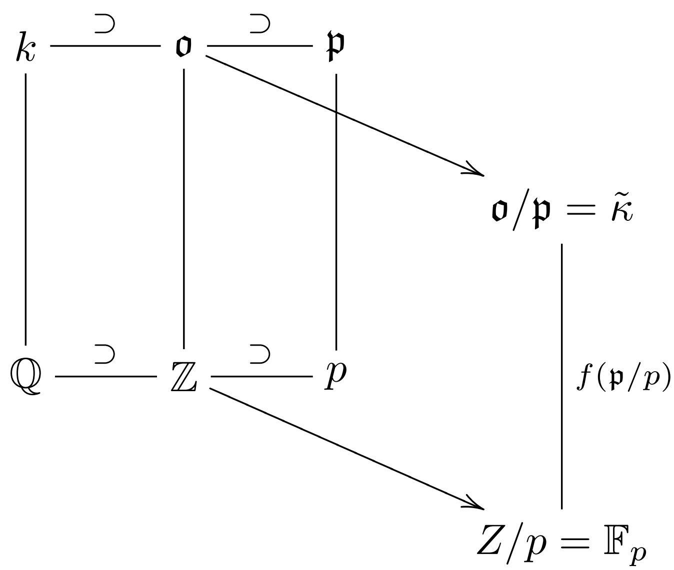
The Dedekind property and the same analysis as for $\mathbb{Z}$ suggests (convergence?!) the Euler product

$$\zeta_k(s) \;=\; \sum_{0\neq\mathfrak{a}\subset\mathfrak{o}} \frac{1}{N\mathfrak{a}^s} \;=\; \prod_{\mathfrak{p}\text{ prime in }\mathfrak{o}} \frac{1}{1-N\mathfrak{p}^{-s}}$$

Understanding splitting/factorization of primes in extensions of $\mathbb{Z}$ or of $\mathbb{F}_q[x]$ gives

Proposition: The Euler product expression for $\zeta_k(s)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.

Proof: Treat the number field case. Group the Euler factors according to the associated rational primes. **The picture:**



With $p\mathfrak{o} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ with residue field extension degrees f_i, and $\sum_i e_i f_i = [k:\mathbb{Q}]$, with $\sigma = \mathrm{Re}(s)$,

$$\Big|\frac{1}{1 - N\mathfrak{p}^{-s}}\Big| \;=\; \frac{1}{1 - p^{-f\sigma}} \;\le\; \Big(\frac{1}{1 - p^{-\sigma}}\Big)^f$$

Thus,

$$\Big|\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}}\Big| \;\le\; \Big(\frac{1}{1 - p^{-\sigma}}\Big)^{[k:\mathbb{Q}]}$$

and the Euler product for $\zeta_k(s)$ is dominated by the Euler product for $\zeta_{\mathbb{Q}}(\sigma)^{[k:\mathbb{Q}]}$, nicely convergent for $\mathrm{Re}(s) > 1$. ///

Remark: The estimate

$$|\zeta_k(s)| \;\;\le\;\; \zeta_{\mathbb{Q}}(\sigma)^{[k:\mathbb{Q}]} \qquad\qquad (\text{as } \sigma = \mathrm{Re}(s) \to 1^+)$$

suggests a pole of order $[k:\mathbb{Q}]$ at $s = 1$, **but**, in fact, the pole is of order 1 for all number fields k. [Below]
