Continuing the pre/review of the simple (!?) case...

Examples: Riemann's formula

$$\sum_{p^m<X} \log p \;=\; X \;-\; (b+1) \;-\; \lim_{T\to\infty} \sum_{|\mathrm{Im}\,(\rho)|<T} \frac{X^\rho}{\rho} \;+\; \sum_{n\geq 1} \frac{X^{-2n}}{2n}$$

Gauss' *Quadratic Reciprocity*:

$$\left(\frac{q}{p}\right)_2 \cdot \left(\frac{p}{q}\right)_2 \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}$$

Continuing: *factorization* of Dedekind zeta-functions into Dirichlet L-functions. Equivalently, *behavior of primes in extensions.*

Example: behavior of primes in the extension $\mathbb{Z}[i]$ of $\mathbb{Z}$

Prime numbers p in $\mathbb{Z}$, which we'll call *rational primes* to distinguish them, do not usually *stay prime* in larger rings: for example

$$5 \;=\; (2+i)\cdot(2-i)$$

Expanding on the two-squares theorem:

Theorem: A rational prime p stays prime in $\mathbb{Z}[i]$ if and only if $p = 3 \bmod 4$. A rational prime $p = 1 \bmod 4$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 2 *ramifies*, in the sense that $2 = (1+i)(1-i)$ and $1+i$ and $1-i$ differ by a unit.

Terminology: Primes that *stay* prime are *inert*, and primes that *factor* (with no factor repeating) are *split*. A prime that factors and has *repeated factors* is *ramified*.

So far, for split p, and for ρ a $\sqrt{-1}$ in $\mathbb{F}_p$,

$$\mathbb{Z}[i]/p \approx \mathbb{F}_p[x]/\langle x^2+1\rangle \approx \mathbb{F}_p[x]/\langle x-\rho\rangle \oplus \mathbb{F}_p[x]/\langle x+\rho\rangle$$

By the cyclic-ness of $\mathbb{F}_p^\times$, p has a $\sqrt{-1}$ exactly when $p = 1 \bmod 4$. That is, $p = 1 \bmod 4$ is *split*, specifically, $p \cdot \mathbb{Z}[i]$ is of the form $p_1 p_2 \cdot \mathbb{Z}[i]$ for *distinct* (non-associate) prime elements p_i of $\mathbb{Z}[i]$.

Lemma For an ideal I in a PID R, suppose there is an isomorphism

$$\varphi : R \longrightarrow R/I \approx D_1 \times D_2$$

to a product of integral domains D_i (with $0 \neq 1$ in each). Then $I = \ker\varphi$ is generated by a product $p_1 p_2$ of two distinct (non-associate) prime elements p_i.

Proof: In a *principal* ideal domain, every non-zero prime ideal is *maximal*. Let φ_i be the further composition of φ with the projection to D_i. Then $\ker \varphi_i$ of $\varphi_i : R \to D_i$ is a prime ideal containing I, and

$$\ker \varphi = \ker \varphi_1 \cap \ker \varphi_2$$

$\ker \varphi_1 \neq \ker \varphi_2$, or else $I = \ker \varphi_1 = \ker \varphi_2$ would already be prime, and R/I would be an integral domain, not a product. Let $\ker \varphi_i = p_i \cdot R$ for non-associate prime elements p_1, p_2 of R. Then

$$I = p_1 R \cap p_2 R = \{r \in R : r = a_1 p_1 = a_2 p_2 \text{ for some } a_1, a_2 \in R\}$$

p_1 and p_2 are distinct, so $p_2 | a_1$ and $p_1 | a_2$, and $I = p_1 p_2 \cdot R$. ///

Description of behaviors in an extension, in terms of behavior in the ground ring, is a *reciprocity law.*

Quadratic symbol as Dirichlet character: conductor The *quadratic symbol* that tells whether or not -1 is a square mod p is

$$\left(\frac{-1}{p}\right)_2 = \left\{ \begin{array}{ll} 0 & (p=2) \\ +1 & (\text{when } -1 \text{ is a square mod } p) \\ -1 & (\text{when } -1 \text{ is not a square mod } p) \end{array} \right\} \quad (\text{prime } p)$$

This quadratic symbol is determined by p mod 4. That is, the *conductor* of this symbol is 4. That is, this quadratic symbol is a *Dirichlet character* mod 4:

$$\left(\frac{-1}{p}\right)_2 = \begin{cases} 0 & (p=2) \\ +1 & (\text{when } p = 1 \bmod 4) \\ -1 & (\text{when } p = 3 \bmod 4) \end{cases}$$

Factoring $\zeta_{\mathbb{Z}[i]}(s)$ The zeta function of $\mathfrak{o} = \mathbb{Z}[i]$ is a sum over non-zero elements of $\mathfrak{o}$ modulo units: (note that the *ideal* norm is expressible in terms of the *Galois* norm here)

$$\zeta_{\mathfrak{o}}(s) = \sum_{0 \neq \alpha \in \mathfrak{o} \bmod \mathfrak{o}^\times} \frac{1}{|N\alpha|^s} \qquad \text{(Galois norm)}$$

Since $|\mathfrak{o}^\times| = 4$, this is also

$$\zeta_{\mathfrak{o}}(s) = \frac{1}{4} \sum_{0 \neq \alpha \in \mathfrak{o}} \frac{1}{(N\alpha)^s} = \frac{1}{4} \sum_{m,n \in \mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+n^2)^s}$$

Easy estimates prove convergence for $\mathrm{Re}(s) > 1$. As in the Euler factorization of $\zeta_{\mathbb{Z}}(s)$, unique factorization in $\mathfrak{o} = \mathbb{Z}[i]$ gives

$$\zeta_{\mathfrak{o}}(s) = \prod_{\text{primes } \pi \bmod \mathfrak{o}^\times} \frac{1}{1 - \frac{1}{|N\pi|^s}} \qquad (\text{for } \mathrm{Re}(s) > 1)$$

With $\chi(p) = \left(\frac{-1}{p}\right)_2$, we claim a factorization

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$$

To this end, group the Euler factors according to the rational primes the Gaussian prime divides:

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_{\text{rational } p} \; \prod_{\pi|p} \frac{1}{1 - \dfrac{1}{|N\pi|^s}}$$

The prime $p = 2$ is *ramified*: $\pi = 1 + i$ is the unique prime dividing 2, and $2 = (1+i)^2/i$. Since $\chi(2) = 0$,

$$\prod_{\pi|2} \frac{1}{1 - \dfrac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \dfrac{1}{|N(1+i)|^s}} \;=\; \frac{1}{1 - \dfrac{1}{2^s}}$$

$$= \frac{1}{1 - \dfrac{1}{2^s}} \cdot 1 \quad = \quad 2^{th} \text{ factor of } \zeta_{\mathbb{Z}}(s) \;\times\; 2^{th} \text{ factor of } L(s,\chi)$$

Primes $p = 3 \bmod 4$ stay prime in $\mathfrak{o}$, and $\chi(p) = -1$, so

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} = \frac{1}{1 - \frac{1}{|Np|^s}} = \frac{1}{1 - \frac{1}{p^{2s}}} = \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 + \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi(p)}{p^s}} = p^{th} \text{ factor of } \zeta_(s) \times p^{th} \text{ factor of } L(s,\chi)$$

Primes $p = 1 \bmod 4$ factor as $p = p_1 p_2$, and $\chi(p) = +1$. Note that $p^2 = Np = Np_1 \cdot Np_2$, so since the p_i are not units, $Np_i = p$. Then

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} = \frac{1}{1 - \frac{1}{|Np_1|^s}} \times \frac{1}{1 - \frac{1}{|Np_2|^s}} = \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi(p)}{p^s}} = p^{th} \text{ factor of } \zeta_{\mathbb{Z}}(s) \times p^{th} \text{ factor of } L(s,\chi)$$

Putting this together, $\quad \zeta_{\mathfrak{o}}(s) = \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$.

Example: extension $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{Z}$

A little work shows that the ring $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ is *Euclidean*, so a *PID*.

The group of units $\mathfrak{o}^\times$ is highly non-trivial: has non-torsion element $1+\sqrt{2}$. In fact, $\mathfrak{o}^\times$ is generated by $1+\sqrt{2}$ and -1.

Theorem: A rational prime p stays prime in $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ if and only if $p = 3, 5 \bmod 8$. A rational prime $p = \pm 1 \bmod 8$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 2 *ramifies*, in the sense that $2 = (\sqrt{2})^2$.

Proof: The $p = 2$ case is clear. With $p > 2$,

$$\mathfrak{o}/p \;=\; \mathbb{Z}[\sqrt{2}]/p \;\approx\; \mathbb{Z}[x]/\langle x^2 - 2, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^2 - 2\rangle$$

When 2 is a non-square mod p, $x^2 - 2$ is irreducible in $\mathbb{F}_p[x]$, and $\mathfrak{o}/p$ is a field, so p is prime. When 2 is a square mod $p > 2$, there are two *distinct* square roots ρ_1, ρ_2, and by Sun-Ze's theorem

$$\mathbb{F}_p[x]/\langle x^2 - 2\rangle \;\approx\; \mathbb{F}_p[x]/\langle x - \rho_1\rangle \oplus \mathbb{F}_p[x]/\langle x - \rho_2\rangle$$

The earlier Lemma shows that p factors in $\mathfrak{o}$ as a product of two distinct (non-associate) primes, so p *splits.* ///

In fact, taking any representatives ρ in $\mathbb{Z}$ for a square root of 2 mod p, the isomorphism shows that the *pairs* $p, \rho - \sqrt{2}$ and $p, \rho + \sqrt{2}$ generate the two prime ideals into which $p \cdot \mathfrak{o}$ factors.

Group the Euler factors of the Dedekind zeta function for $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ by rational primes:

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_p \Big(\prod_{\pi | p} \frac{1}{1 - |N\pi|^{-s}} \Big) \;=\; (\text{ramified}) \cdot (\text{split}) \cdot (\text{inert})$$

The only ramified prime is 2. Split primes are $p = \pm 1 \bmod 8$, and $p = \pi_1 \cdot \pi_2$ implies

$$p^2 \;=\; Np \;=\; N\pi_1 \cdot N\pi_2$$

so the norms of any two prime factors are p. Inert primes are $p = 3, 5 \bmod 8$, they remain prime in $\mathfrak{o}$, and $Np = p^2$. Thus,

$$\zeta_{\mathfrak{o}}(s) \quad = \quad \prod_{\pi | 2} \frac{1}{1 - |N\pi|^{-s}}$$

$$\times \prod_{p = \pi_1 \pi_2} \frac{1}{1 - |N\pi_1|^{-s}} \cdot \frac{1}{1 - |N\pi_2|^{-s}}$$

$$\times \prod_{p = 3,5 \bmod 8} \frac{1}{1 - |Np|^{-s}}$$

With $\chi(p) = \left(\frac{2}{p}\right)_2$, this is

$$\zeta_{\mathfrak{o}}(s) = \frac{1}{1-2^{-s}} \times \prod_{p=\pm 1 \bmod 8} \frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{-s}}$$

$$\times \prod_{p=3,5 \bmod 8} \frac{1}{1-p^{-s}} \cdot \frac{1}{1+p^{-s}}$$

$$= \prod_p \frac{1}{1-p^{-s}} \cdot \frac{1}{1-\chi(p)p^{-s}} = \zeta(s) \cdot L(s,\chi)$$

Example: eighth roots of unity

Let $\omega = \frac{1+i}{\sqrt{2}}$ be a primitive eighth root of unity, and $\mathfrak{o} = \mathbb{Z}[\omega]$.

The non-trivial characters mod 8 are $\left(\frac{-1}{p}\right)_2$, $\left(\frac{2}{p}\right)_2$, and $\left(\frac{-2}{p}\right)_2$. The ring $\mathbb{Z}[\sqrt{-2}]$ is Euclidean. The same argument shows not only

$$\zeta_{\mathbb{Z}[\sqrt{-2}]}(s) \;=\; \zeta(s) \cdot L(s, \left(\frac{-2}{p}\right)_2)$$

but also **Claim:**

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta(s) \cdot L(s, \left(\frac{-1}{p}\right)_2) L(s, \left(\frac{2}{p}\right)_2) \cdot L(s, \left(\frac{-2}{p}\right)_2)$$

Without determining whether $\mathfrak{o}$ is a PID, or what its units are, let's grant ourselves that it is a *Dedekind domain*, in that *every non-zero ideal factors uniquely into prime ideals.*