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

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

$$\zeta_{\mathbb{Z}[i]}(s) = \zeta(s) \cdot L(s, \chi) \qquad \chi(p) = \left(\tfrac{-1}{p}\right)_2$$

$$\zeta_{\mathbb{Z}[\sqrt{2}]}(s) = \zeta(s) \cdot L(s, \chi) \qquad \chi(p) = \left(\tfrac{2}{p}\right)_2$$

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

Next, $\mathbb{Z}[\omega]$ with ω an eighth root of unity. First, look at the eighth cyclotomic polynomial $x^4 + 1$.

Comment: The change of variables $x \to x + 1$ gives $x^4 + 4x^3 + 6x^2 + 4x + 2$, so *Eisenstein's criterion and Gauss' Lemma* prove irreducibility of $x^4 + 1$ in $\mathbb{Q}[x]$.

A peculiar feature of the polynomial $x^4 + 1$:

Claim: $x^4 + 1$ is *reducible* modulo every prime p.

$p = 2$ is easy. For $p > 2$, for $x^4 + 1 = 0$ to have a root in $\mathbb{F}_p$ requires existence of an element of order 8 in $\mathbb{F}_p^\times$, so $8|p - 1$, and $p = 1 \bmod 8$. For $x^4 + 1 = 0$ to have a root in $\mathbb{F}_{p^2}$ requires existence of an element of order 8 in $\mathbb{F}_{p^2}\times$, so $8|p^2 - 1$.

Interestingly-enough, $\mathbb{Z}/8^\times$ is not cyclic, but is isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. Thus, $p^2 = 1 \bmod 8$ for all odd p. That is, at worst, $x^4 + 1 = 0$ has a root in $\mathbb{F}_{p^2}$ for all odd p. ///

Comment For f a monic polynomial in $\mathbb{Z}[x]$ irreducibility of its image in $\mathbb{F}_p[x]$ certainly implies its irreducibility in $\mathbb{Z}[x]$. We might hope that there'd be a sort of converse, namely, that irreducible monics in $\mathbb{Z}[x]$ would be irreducible mod *some* prime p... but $x^4 + 1$ is a counter-example.

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 $\left(\frac{-2}{p}\right)_2$.

Claim:

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

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

By Euler's criterion, computing mod p,

$$\left(\frac{-2}{p}\right)_2 = (-2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)_2 \cdot \left(\frac{2}{p}\right)_2$$

The characters of $\mathbb{Z}/8^\times$

$p\backslash\chi$	triv	$\left(\frac{-1}{*}\right)$	$\left(\frac{2}{*}\right)$	$\left(\frac{-2}{*}\right)$
1 mod 8	1	1	1	1
3 mod 8	1	−1	−1	1
5 mod 8	1	1	−1	−1
7 mod 8	1	−1	1	−1

For $3, 5, 7$ there are exactly two -1's in each row.

As earlier, for rational prime $p > 2$,

$$\mathfrak{o}/p \;\approx\; \mathbb{Z}[x]/\langle x^4+1, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^4+1\rangle$$

$$\approx \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } p = 1 \bmod 8) \\ \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } p = 3, 5, 7 \bmod 8) \end{cases}$$

Observe: Prime splitting determined by congruence conditions!!!

Since $x^4 + 1 = (x+1)^4 \bmod 2$, for $p = 2$ something more complicated happens:

$$\mathbb{F}_2[x]/(x+1)^4 \;\neq\; \text{product of fields}$$

Indeed, we already saw that, in the PIDs $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$, inside the intermediate fields, 2 is *ramified.* A little later we'll have means to see that the above computation implies 2 is *totally ramified* in the extension $\mathfrak{o} = \mathbb{Z}[\omega]$ of $\mathbb{Z}$, namely, $2\mathfrak{o} = \mathfrak{p}^4$.

Write $\chi_D(p) = \left(\frac{D}{p}\right)_2$ for $D = -1, 2, -2$.

For $p = 1 \bmod 8$, applying the ideal norm to $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ gives $N\mathfrak{p}_i = p$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \left(\frac{1}{1 - p^{-s}}\right)^4$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi_{-1}(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_{-2}(p)}{p^s}}$$

$=$ Euler p-factors from $\zeta(s)$, $L(s, \chi_{-1})$, $L(s, \chi_2)$, $L(s, \chi_{-2})$

For $p = 3, 5, 7 \bmod 8$, $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$ gives $N\mathfrak{p}_i = p^2$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1 - p^{-2s}}\Big)^2$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 + \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 + \frac{1}{p^s}} \qquad \text{(in } \textit{some} \text{ order!?!)}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi_{-1}(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_{-2}(p)}{p^s}} \qquad \text{(order?)}$$

$$= \text{ Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_{-1}),\ L(s,\chi_2),\ L(s,\chi_{-2})$$

We *could* have treated $p = 3, 5, 7$ separately, tracking *which* two-out-of-three characters took values -1, but this would not have accomplished much. Except for the Euler 2-factors, we've proven

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta(s) \cdot L(s, \big(\tfrac{-1}{p}\big)) \cdot L(s, \big(\tfrac{2}{p}\big)) \cdot L(s, \big(\tfrac{-2}{p}\big))$$

Example: fifth roots of unity

Let ω be a primitive fifth root of unity, and $\mathfrak{o} = \mathbb{Z}[\omega]$.

The group $\mathbb{Z}/5^\times$ has four characters: the trivial one, an order-two character χ_2, and two order-four characters χ_1, χ_3.

(**Note:** This indexing is incompatible with earlier...)

Claim:

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta(s) \cdot L(s,\chi_1) \cdot L(s,\chi_2) \cdot L(s,\chi_3)$$

Without determining whether $\mathfrak{o}$ is a PID, or what its units are, if necessary, grant that it is a *Dedekind domain*, ...

As earlier, for rational prime p, with $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ the fifth cyclotomic polynomial,

$$\mathfrak{o}/p \;\approx\; \mathbb{Z}[x]/\langle \Phi_5, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle \Phi_5\rangle$$

$$\approx \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } 5|p-1) \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } 5|p^2-1 \text{ but } 5 \not| p-1) \\ \mathbb{F}_{p^4} & (\text{for } 5|p^4-1 \text{ but } 5 \not| p^2-1) \end{cases}$$

$$\approx \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } p = 1 \bmod 5) \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } p = -1 \bmod 5) \\ \mathbb{F}_{p^4} & (\text{for } p = 2, 3 \bmod 5) \end{cases}$$

Observe: Prime splitting determined by congruence conditions!!!

For p splitting completely $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, norms are $N\mathfrak{p}_i = p$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1-p^{-s}}\Big)^4$$

$$= \;\frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_1(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_3(p)}{p^s}}$$

$=$ Euler p-factors from $\zeta(s)$, $L(s,\chi_1)$, $L(s,\chi_2)$, $L(s,\chi_3)$

For p splitting *half-way* $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$, norms are $N\mathfrak{p}_i = p^2$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1 - p^{-2s}}\Big)^2$$

$$= \;\frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 + \dfrac{1}{p^s}} \cdot \frac{1}{1 + \dfrac{1}{p^s}}$$

$$= \;\frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_1(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_3(p)}{p^s}}$$

$$= \;\text{Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_2),\ L(s,\chi_1),\ L(s,\chi_3)$$

... in that order, except that we can't distinguish the order-four characters χ_1,χ_3.

For p *inert* $p\mathfrak{o} = \mathfrak{p}$, the norm is $N\mathfrak{p} = p^4$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} = \frac{1}{1 - p^{-4s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 + \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{i}{p^s}} \cdot \frac{1}{1 + \frac{i}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_1(p)}{p^s}} \cdot \frac{1}{1 - \frac{\chi_3(p)}{p^s}}$$

$$= \text{ Euler } p\text{-factors from } \zeta(s),\ L(s, \chi_2),\ L(s, \chi_1),\ L(s, \chi_3)$$

... not distinguishing the order-four characters χ_1,χ_3.

This proves the claimed factorization, except for $p = 5$. The interested reader might show that $5\mathfrak{o} = (\omega - 1)^4$, and then it's easy to see the complete factorization of the Dedekind zeta.