A pre-analysis discussion of zeta functions

December 15, 2013

Today we are going to introduce the Dedekind zeta function of a number field F, and give a "formula" for it in the case $F = \mathbb{Q}(\zeta_p)$.

Let F be a number field, with ring of integers $\mathcal{O}$. Recall that we've been talking about ideals $I \subset \mathcal{O}$: these are just abelian subgroups which are furthermore closed under "scalar multiplication" by the elements of $\mathcal{O}$. We motivated these things as being "generalized elements" of the ring $\mathcal{O}$, with an eye towards the salvage of unique prime factorization. But one thing I didn't mention last time, but that should be said at some point (and why not now), is that ideals have an independent motivation from the perspective of ring theory. Namely, an ideal I in a (commutative) ring R is exactly what you can "mod out" by and still get a ring R/I. To be more precise, for any subset $I \subset R$ you can define R/I to be the set of equivalence classes of elements $r \in R$ under the equivalence relation $r \simeq r'$ if and only if $r - r'$ is in I. And you can try to define addition and multiplication by picking representatives and adding or multiplying in R. Then this will be independent of the representatives and therefore define a ring structure on R/I if and only if I is an ideal.

For example, if you think about it, in ordinary arithmetic, when you work "mod n" you're really working modulo the ideal generated by n: treating two integers as equal if their difference is multiple of n. So again, ideals are the natural things to "mod out" by if you want to stay in the world of rings. Another way of saying this is that the ideals are exactly the *kernels* of ring homomorphisms: for example, I is the kernel of $R \to R/I$.

Moving on, and coming back to our ring of integers $\mathcal{O} \subset F$, recall also that the set of nonzero ideals of $\mathcal{O}$ is "tamed" by the norm function,

$$N(I) = \#(\mathcal{O}/I).$$

What I mean by this is that the set of ideals of norm $\leq N$ is finite, where N is any fixed natural number. Another important property of the norm function, which will be relevant shortly, is that it is multiplicative:

$$N(IJ) = N(I)N(J).$$

Here inside the norm we have the product of ideals, and outside the norm we have the product of natural numbers. I don't think there's a direct explanation for this multiplicativity. But briefly, one can deduce it as follows. First, if I and J are "relatively prime", meaning the sum $I + J$ is the unit ideal $\mathcal{O}$, then the formula holds for the simple reason that the natural map $\mathcal{O}/(IJ) \to \mathcal{O}/I \times \mathcal{O}/J$ is an isomorphism. (This requires nothing of the nature of the ring $\mathcal{O}$: look up the "Chinese remainder theorem".) Now, powers of distinct maximal ideals are always relative prime, so by the existence of factorizations into

maximal ideals we can then reduce the multiplicativity claim to the statement that if P is maximal then $N(P^k) = N(P)^k$ for all $k \in \mathbb{N}$. This, in turn, holds because $\mathcal{O}/P^k$ is "built out of" k copies of $\mathcal{O}/P$. Not in the sense that $\mathcal{O}/P^k$ is the product of k copies of $\mathcal{O}/P$, but in the sense that there are k more drastic quotients $\mathcal{O}/P^i$ for $0 \leq i < k$, and the kernel of each natural map $\mathcal{O}/P^{i+1} \to \mathcal{O}/P^i$ is isomorphic to $\mathcal{O}/P$. This is a consequence of the unique maximal ideal factorization in $\mathcal{O}$. Anyway, that's all we'll say about the multiplicativity of N.

So, moving on, we can now give the main definition.

Definition 0.1. *Let F be a number field, with integer ring $\mathcal{O}$. Define the* Dedekind zeta function *of F to be*

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{N(I)^s},$$

the sum being over all nonzero ideals of $\mathcal{O}$.

We'll eventually want to think of s as a complex variable, but for now let's just consider the above sum "formally". To be more precise about this, note that we can rewrite the above definition as

$$\zeta_F(s) = \sum_{n \in \mathbb{N}} a_n \cdot n^{-s},$$

where a_n denotes the number of nonzero ideals of $\mathcal{O}$ whose norm equals n. For now our perspective will be that this zeta function is just a particular way of keeping track of all these numbers a_n at the same time. This would be a familiar idea ("generating series") if we were to use something like X^n instead of n^{-s}. But for our purposes n^{-s} is a more convenient expression. It converts addition in s to multiplication, whereas X^n converts multiplication in X to multiplication.

The simplest case is $F = \mathbb{Q}$. Then the above definition reduces to the Riemann zeta function:

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) = \sum_{n \in \mathbb{N}} n^{-s}.$$

So the $a_n = 1$ in this case. That's not very interesting.

The goal of this lecture will be to prove the following. First we'll give the statement, then we'll describe the undefined terms.

Theorem 0.2. *Let $F = \mathbb{Q}(\zeta_p)$ for a prime p. Then*

$$\zeta_F(s) = \zeta(s) \cdot \prod_{\chi} L(s, \chi),$$

where the product is over all non-trivial characters $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$.

Actually a similar statement holds with any natural number n instead of p, but as usual we're focusing on the prime case, which is simpler to analyze and contains many of the important ideas anyway.

If you expand this out, it amounts to an interesting formula for the a_n in terms of the values of the characters χ. It's fun to work this out in explicit examples, for instance $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ or

$\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$. (OK, 4 isn't prime, but no big deal.)

Now let's explain what $L(s, \chi)$ is. But first, we should talk about what these characters χ are. A character χ of $(\mathbb{Z}/p\mathbb{Z})^\times$ is just a group homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$. One can analyze these as follows. Recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$. If g denotes a generator, then it follows that any character χ is determined just by its value on g. And the only condition that value has to satisfy, is that it should be a $(p-1)^{st}$ root of unity. So, given a choice of generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, characters χ of $(\mathbb{Z}/p\mathbb{Z})^\times$ are just the same thing as $(p-1)^{st}$ roots of unity in $\mathbb{C}$. Now, in the above formula we're taking only the nontrivial characters χ, which amounts to excluding 1 as a $(p-1)^{st}$ root of unity. One thing to keep in mind is that since $p-1$ is not usually prime, it is not the case that a $(p-1)^{st}$ root of unity which is not 1 is necessarily primitive as a $(p-1)^{st}$ root of unity. For example, if p is odd, then there is a unique character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ whose image is $\{\pm 1\}$: this is the so-called *quadratic character* (mod p). It's determined by the fact that it sends one (or any) generator to -1. Of course, it's only "primitive" if $p = 3$.

OK, so now we can define $L(s, \chi)$ for a character χ of $(\mathbb{Z}/p\mathbb{Z})^\times$. It is a "twisted" form of the Riemann zeta function $\zeta(s) = \sum_{n \in \mathbb{N}} n^{-s}$. The definition is

$$L(s, \chi) = \sum_{n \in \mathbb{N}} \chi(n) \cdot n^{-s}.$$

Here by $\chi(n)$ for a natural number n we mean the following. If p doesn't divide n, then n (mod p) defines an element of $(\mathbb{Z}/p\mathbb{Z})^\times$, so the meaning is obvious. On the other hand, if p does divide n, we just set $\chi(n) = 0$. In other words, the above is really a sum over the n relatively prime to p, in which case the character χ makes sense.

Now, to verify the above theorem is to understand the numbers a_n for $F = \mathbb{Q}(\zeta_p)$, i.e. it is to understand the distribution of the values of $N(I)$ as I ranges over nonzero ideals of $\mathbb{Z}[\zeta_p]$. The first step in this understanding is to realize that, instead of thinking about $N(I)$ for arbitrary ideals, we can just think just about $N(P)$ for maximal ideals P. This is a consequence of unique maximal ideal factorization in $\mathbb{Z}[\zeta_p]$ and the multiplicativity of the norm. In terms of zeta functions, this is encoded in the *Euler product expansion*

$$\zeta_F(s) = \prod_{P \text{ maximal}} \frac{1}{1 - N(P)^{-s}},$$

valid for an arbitrary number field F. To see that this equality is true, imagine expanding the inner terms using the geometric series identity. Then the product on the right becomes

$$\prod_P (1 + N(P)^{-s} + N(P)^{-2s} + \ldots).$$

Now, imagine expanding this product out. You will get a term in the expansion every time you choose, for every maximal ideal P, a term of the sum $1 + N(P)^{-s} + N(P)^{-2s} + \ldots$. These terms are indexed by integers $k \geq 0$, and the k^{th} term is $N(P)^{-ks}$. Also, to actually get a valid term in the formal expansion it needs to be the case that for all but finitely many P this integer k you chose is 0, corresponding to the term 1. Thus we see that the terms of the expansion are the expressions

$$\left(N(P_1^{k_1}) \cdot \ldots \cdot N(P_r^{k_r})\right)^{-s}$$

where $P_1, \ldots, P_r$ is a choice of finitely many maximal ideals and $k_i \geq 0$ is a corresponding exponent for every P_i. By unique maximal ideal factorization in $\mathcal{O}$ and multiplicativity of the norm, this is just the same as writing $N(I)^{-s}$ for all nonzero ideals I. And that gives the Dedekind zeta function. So we've verified (formally) the Euler product expansion

$$\zeta_F(s) = \prod_{P \text{ maximal}} \frac{1}{1 - N(P)^{-s}}.$$

Similarly we have Euler product expansions

$$\zeta(s) = \prod_{\ell} \frac{1}{1 - \ell^{-s}}$$

and

$$L(s, \chi) = \prod_{\ell} \frac{1}{1 - \chi(\ell) \cdot \ell^{-s}}.$$

These are also just a formal consequence of unique prime factorization in $\mathbb{Z}$ and the multiplicativity of χ. Note that we have decided to index the primes by ℓ instead of p, since we're saving p for the notation $\mathbb{Q}(\zeta_p)$.

Now, we're trying to show that

$$\zeta_{\mathbb{Q}(\zeta_p)}(s) = \zeta(s) \cdot \prod_{\chi \neq 1} L(s, \chi).$$

The idea will be to match up the Euler product expansions on both sides. For this, we need to be able to group the maximal ideals in $\mathbb{Z}[\zeta_p]$ into groups which are instead labeled by the primes ℓ, to match the left-hand side with the right-hand side. Such a grouping is provided by the following proposition.

Proposition 0.3. *Let F be a number field with ring of integers $\mathcal{O}$, and let P be a maximal ideal of $\mathcal{O}$. Then for a prime number ℓ, the following are equivalent:*

1. *The ring $\mathcal{O}/P$ (actually a field) has characteristic ℓ, meaning $\ell = 0$ in $\mathcal{O}/P$.*
2. *The maximal ideal P contains the principal ideal (ℓ) of $\mathcal{O}$.*
3. *The maximal ideal P divides the principal ideal (ℓ).*
4. *The maximal ideal P occurs in the unique maximal ideal factorization of (ℓ).*

Proof. The statement in 1 is equivalent to saying that ℓ lies in P. This is also equivalent to saying that $(\ell) \subset P$, which is statement 2. But in general for ideals in a ring of integers, to contain is to divide (we stated this concurrently with the unique maximal ideal factorization), so that's also the same as 3. Finally, the equivalence of 3 with 4 follows from the uniqueness of maximal ideal factorizations. □

So every maximal ideal P determines a prime ℓ, namely the ℓ such that the finite field $\mathcal{O}/P$ has characteristic ℓ. In such a case, we say that "P lies above ℓ", and write $P|\ell$. Thus, if $(\ell) = P_1^{e_1} \ldots P_g^{e_g}$ is the maximal ideal factorization of (ℓ), then the maximal ideals lying above ℓ are exactly the P_i. But we won't use that characterization; we'll actually only use statement 2 above, which is much more elementary.

Anyway, via the separate Euler products of $\zeta_{\mathbb{Q}(\zeta_p)}(s)$, $\zeta(s)$, and $L(s,\chi)$, we see that our theorem about $\zeta_{\mathbb{Q}(\zeta_p)}$ will follow if we can show that for $\ell \neq p$ we have

$$\prod_{P|\ell} \frac{1}{1-N(P)^{-s}} = \prod_{\chi} \frac{1}{1-\chi(\ell)\cdot \ell^{-s}},$$

and for $\ell = p$ we have

$$\prod_{P|p} \frac{1}{1-N(P)^{-s}} = \frac{1}{1-p^{-s}}.$$

Note that in the case $\ell \neq p$ we are now taking the product over *all* characters $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$: for the trivial character $\chi = 1$ we're picking up the Euler factor at ℓ for $\zeta(s)$. On the other hand, for $\ell = p$ the only Euler factor at p on the right-hand side of our desired equation is contributed by $\zeta(s)$, so that explains why the second equation is the correct one.

So, we need to prove these two equalities. In other words, we need to understand the norms of maximal ideals P of $\mathbb{Z}[\zeta_p]$, when these are classified in terms of the prime ℓ which they lie above. Now, there are different ways of going about this. Though the "Galois" method is probably the best (and we'll talk about it at some point), here we'll adopt a "polynomial" method, which is maybe the most explicit. What we'll see is that the question of classifying the maximal ideals P of $\mathbb{Z}[\zeta_p]$ lying above ℓ is equivalent to problem 2 on your first problem set, about factoring $\Phi_p(X)$ in $\mathbb{F}_\ell[X]$.

The key is the following: there is a natural ring isomorphism

$$\mathbb{Z}[\zeta_p]/\ell \simeq \mathbb{F}_\ell[X]/\Phi_p(X).$$

To prove this, consider the surjective ring homomorphism $\mathbb{Z}[X] \to \mathbb{Z}[\zeta_p]$ defined by $X \mapsto \zeta_p$. When we mod out by ℓ, this gives a surjective ring homomorphism $\mathbb{F}_\ell[X] \to \mathbb{Z}[\zeta_p]/\ell$. Then since $\Phi_p(\zeta_p) = 0$, this induces a surjective ring homomorphism $\mathbb{F}_\ell[X]/\Phi_p(X) \to \mathbb{Z}[\zeta_p]/\ell$. But both sides have the same dimension (namely, $p-1$) as $\mathbb{F}_\ell$-vector spaces, so this must be an isomorphism. That gives the desired isomorphism.

Now, we know that the maximal ideals P lying above ℓ are the same as the maximal ideals P containing ℓ. These are thus in bijection with the maximal ideals of the quotient $\mathbb{Z}[\zeta_p]/\ell$. By the above isomorphism, that's also the same as the maximal ideals of $\mathbb{F}_\ell[X]/\Phi_p(X)$. But in general, for a field E and a polynomial $f(X) \in E[X]$, the maximal ideals of $E[X]/f(X)$ are in bijection with the irreducible factors f_i of f in $E[X]$. So in our case, we see that the maximal ideals P_i lying above ℓ are in bijection with the irreducible factors f_i of $\Phi_p(X)$ in $\mathbb{F}_\ell[X]$. Moreover, under this bijection, the ring $\mathbb{Z}[\zeta_p]/P_i$ is isomorphic to $\mathbb{F}_\ell[X]/f_i$. In particular, $N(P_i)$ equals $\ell^{deg(f_i)}$, since $\mathbb{F}_\ell[X]/f_i$ is an $\mathbb{F}_\ell$-vector space of dimension $deg(f_i)$.

In summary, the factorization of ℓ into maximal ideals in $\mathbb{Z}[\zeta_p]$ completely mirrors the factorization of $\Phi_p(X)$ into irreducible polynomials in $\mathbb{F}_\ell[X]$. And you figured out how that goes on your problem set: if $\ell \neq p$, then if f denotes the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$, there are $\frac{p-1}{f}$ irreducible factors, each having degree f. But if $\ell = p$, then there's only one irreducible factor, and it has degree 1. Translating back into maximal ideals, we see that when $\ell \neq p$ there are exactly $\frac{p-1}{f}$ maximal ideals of $\mathbb{Z}[\zeta_p]$ lying above ℓ, and each has norm ℓ^f; whereas if $\ell = p$ then there is a unique maximal ideal of $\mathbb{Z}[\zeta_p]$ lying above

p, and it has norm p. (We can also see this explicitly: the unique maximal ideal factorization of (p) is $(p) = (1-\zeta_p)^{p-1}$, provided by our old friend again...)

We conclude that for $\ell \neq p$,

$$\prod_{P|\ell} \frac{1}{1-N(P)^{-s}} = (\frac{1}{1-\ell^{-fs}})^{\frac{p-1}{f}},$$

and for $\ell = p$

$$\prod_{P|p} \frac{1}{1-N(P)^{-s}} = \frac{1}{1-p^{-s}}.$$

So we're done when $\ell = p$. But when $\ell \neq p$, we still need to show that

$$(\frac{1}{1-\ell^{-fs}})^{\frac{p-1}{f}} = \prod_{\chi} \frac{1}{1-\chi(\ell)\cdot\ell^{-s}}.$$

Actually, something more general is true: if X is a formal variable, then

$$(\frac{1}{1-X^{f}})^{\frac{p-1}{f}} = \prod_{\chi} \frac{1}{1-\chi(\ell)\cdot X}.$$

Undoing the reciprocals, this is just a polynomial identity:

$$(1-X^{f})^{\frac{p-1}{f}} = \prod_{\chi}(1-\chi(\ell)X).$$

To verify it, note that the polynomials have the same degree (there are $p-1$ characters $\chi : (\mathbb{Z}/p\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ because that's the number of $(p-1)^{st}$ roots of unity in $\mathbb{C}$) and the same constant coefficient, so it suffices to see that they have the same roots, with multiplicity. On the left hand side, the roots are the f^{th} roots of unity, and each occurs with multiplicity $\frac{p-1}{f}$. On the right hand side, the roots are the values $\chi(\ell)^{-1}$ as χ ranges over all characters of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Each such value is indeed an f^{th} root of unity, since ℓ has order f in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. So it suffices to see that each f^{th} root of unity is of the form $\chi(\ell)^{-1}$ for exactly $\frac{p-1}{f}$ characters χ of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. This is easy to see by picking a generator to identify characters with $(p-1)^{st}$ roots of unity.

So we have proved the theorem:

$$\zeta_{\mathbb{Q}(\zeta_p)}(s) = \zeta(s)\cdot\prod_{\chi\neq 1} L(s,\chi).$$

It reflects our explicit understanding of how primes ℓ factor in $\mathbb{Z}[\zeta_p]$, which in turn came from the fact that the effect of Frobenius on roots of unity is very easy to understand.

The next order of business will be to "do analysis" on both sides of this equation separately. Then we can compare the answers and get some interesting facts!