THE CYCLOTOMIC ZETA FUNCTION

This writeup begins by showing that cyclotomic polynomials are irreducible. Then the "e, f, g" description of rational prime decomposition in a cyclotomic number field is stated, without proof. The cyclotomic zeta function is introduced, and the rational prime decomposition shows that the Nth cyclotomic zeta function is the product of all Dirichlet L-functions modulo N. The cyclotomic zeta function, as initially defined by a sum or a product, is an analytic function of a complex variable s in a right half plane. An easy estimate shows that the sum inherits a pole at $s = 1$ from the basic Euler–Riemann zeta function, with no nontrivial Dirichlet L-function canceling it. This pole is the crux of the proof of Dirichlet's theorem on primes in an arithmetic progression.

Contents

1. Cyclotomic Galois Theory

Let N be a positive integer. The Nth cyclotomic field is

$$K = K_N = \mathbb{Q}(\zeta_N), \quad \text{where } \zeta_N = e^{2\pi i/N}.$$

This field is a Galois extension of $\mathbb{Q}$ because every embedding of K in $\mathbb{C}$ must take ζ_N to some primitive Nth root of unity, i.e., to ζ_N^m for some m coprime to N, making the embedding an automorphism of K. We view the Galois group of K_N as a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$, by identifying each automorphism of K_N, taking ζ_N to ζ_N^m for some m, with $m+N\mathbb{Z}$. What isn't immediately obvious is that the Galois group is *all* of $(\mathbb{Z}/N\mathbb{Z})^\times$.

The Nth cyclotomic polynomial is

$$\Phi_N(X) = \prod_{\substack{0 \le m < N \\ \gcd(m,N)=1}} (X - \zeta_N^m),$$

the monic polynomial in $K_N[X]$ whose roots are the primitive Nth roots of unity. Because each automorphism of K permutes the roots of $\Phi_N(X)$, this polynomial is invariant under the Galois group, so it lies in $\mathbb{Q}[X]$, and further its coefficients are algebraic integers, so it lies in $\mathbb{Z}[X]$. To show that the Galois group of K_N is all of $(\mathbb{Z}/N\mathbb{Z})^\times$ it suffices to show that $\Phi_N(X)$ is irreducible in $\mathbb{Z}[X]$, because its degree $\phi(N)$ (Euler totient function) is $|(\mathbb{Z}/N\mathbb{Z})^\times|$. We show the irreducibility next.

Let $f(X) \in \mathbb{Z}[X]$ be the monic irreducible polynomial of ζ_N. We have $\Phi_n(X) = f(X)g(X)$ for some $g(X) \in \mathbb{Z}[X]$, and we want to show that $f(X) = \Phi_n(X)$. Every complex root of $\Phi_n(X)$ takes the form ζ_N^m where $\gcd(m, N) = 1$, and this root can be obtained from ζ_N by repeatedly raising to various primes $p \nmid N$. Thus it suffices to show that:

For any root ρ of f and for any prime $p \nmid N$, also ρ^p is a root of f.

So, let ρ be a root of f and let $p \nmid N$ be prime. We show that $f(\rho^p) = 0$ by showing that $g(\rho^p) \neq 0$. For, if instead $g(\rho^p) = 0$ then ρ is a root of $g(X^p)$, and so $f(X)$ divides $g(X^p)$ in $\mathbb{Z}[X]$. Letting an overbar denote reduction modulo p, $\overline{f}(X)$ divides $\overline{g}(X)^p$ in the UFD $(\mathbb{Z}/p\mathbb{Z})[X]$, and so $\overline{f}(X)$ and $\overline{g}(X)$ share a nontrivial factor $h(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. Thus $h(X)^2$ divides $\Phi_N(X)$ modulo p. But this is impossible. Indeed, $\Phi_N(X)$ divides $X^N - 1$, which is coprime to its derivative NX^{N-1} modulo p because $p \nmid N$. Hence $X^N - 1$ has no repeated factors modulo p, and consequently neither does $\Phi_N(X)$.

2. Dirichlet Characters and e, f, g

Let N be a positive integer. A *Dirichlet character modulo N* is defined *initially* as a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

Any such character determines a least positive divisor M of N such that the character factors as

$$\chi = \chi_o \circ \pi_M : (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\pi_M} (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi_o} \mathbb{C}^\times.$$

The integer M is the *conductor* of χ, and the character χ_o is *primitive*. Note that if $n \in \mathbb{Z}$ is not coprime to N but is coprime to M then $\chi_o(n + M\mathbb{Z})$ is defined and nonzero. Perhaps confusingly at first, we also use the symbol χ to denote χ_o lifted to a multiplicative function on the integers,

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}, \quad \chi(n) = \begin{cases} \chi_o(n + M\mathbb{Z}) & \text{if } \gcd(n, M) = 1, \\ 0 & \text{if } \gcd(n, M) > 1. \end{cases}$$

Thus (the lifted) $\chi(n)$ need not equal (the original) $\chi(n + N\mathbb{Z})$, and in particular $\chi(n)$ need not equal 0 even when $\gcd(n, N) > 1$. Especially, if $N > 1$ then the trivial character $\mathbf{1}$ modulo N has conductor $M = 1$, and the trivial character $\mathbf{1}_o$ modulo 1 is identically 1 on $(\mathbb{Z}/1\mathbb{Z})^\times = \{\overline{0}\}$, and this character lifts to the constant function $\mathbf{1}(n) = 1$ for all $n \in \mathbb{Z}$, even though the original character $\mathbf{1}$ modulo N is undefined on cosets $n + N\mathbb{Z}$ where $\gcd(n, N) > 1$.

Fix a rational prime p.

- Let $p^d \parallel N$ and $N_p = N/p^d$ and $e = \phi(p^d)$.
- Let f denote the order of $p + N_p\mathbb{Z}$ in $(\mathbb{Z}/N_p\mathbb{Z})^\times$.
- Let $g = \phi(N_p)/f$.

Thus altogether $efg = \phi(N)$. Note that $N_p = N$ and $e = 1$ for all primes p other than the finitely many prime divisors of N. Conversely, $e > 1$ for $p \mid N$, excepting the case $N = 2 \bmod 4$ and $p = 2$. Just below we will see good reason to exclude the case $N = 2 \bmod 4$, after which $e > 1$ precisely when $p \mid N$.

Let $\zeta_f = e^{2\pi i/f}$. The multiplicative subgroup $\langle p + N_p\mathbb{Z}\rangle$ of $(\mathbb{Z}/N_p\mathbb{Z})^\times$ has f characters, taking p to ζ_f^k for $k = 0, \ldots, f-1$. Each such character lifts to $\phi(N_p)/f = g$ Dirichlet characters modulo N_p. Any Dirichlet character modulo N that is not defined modulo N_p takes p to 0. That is, for $k = 0, \dots, f-1$ there exist g Dirichlet characters modulo N that take p to ζ_f^k, and any Dirichlet character modulo N that doesn't take p to any ζ_f^k takes p to 0.

3. Cyclotomic Arithmetic

Again let N be a positive integer, now stipulating that $N \neq 2 \bmod 4$, and consider the cyclotomic number field

$$K = \mathbb{Q}(\zeta_N), \qquad \zeta_N = e^{2\pi i/N}.$$

The case $N = 2 \bmod 4$ is excluded because here $\gcd(2, N/2) = 1$ and so $-\zeta_{N/2}$ has order $2 \cdot N/2 = N$, which is to say that the field $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N/2})$ is redundant. For example, $-\zeta_3$ has order 6 but lies in $\mathbb{Q}(\zeta_3)$. Another way to see the redundancy is to reason geometrically (again with $N = 2 \bmod 4$) that $\zeta_{N/2}^{\lceil (N/2)/2 \rceil} = \zeta_{N/2}^{N/4+1/2}$ is just more than halfway around the circle, so that its negative must be ζ_N, and then to confirm this analytically by computing $-\zeta_{N/2}^{(N+2)/4} = -\zeta_N^{(N+2)/2} = -\zeta_N^{N/2+1} = \zeta_N^{N/2}\zeta_N^{N/2+1} = \zeta_N$.

We state some results without proof. For any rational prime p, let e and f and g be as above. Then p factors in $\mathcal{O}_K$ as

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e, \qquad [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = f \text{ for each } i.$$

Some particular cases are as follows.

- The primes p such that $p = 1 \bmod N$ decompose completely in $\mathcal{O}_K$,
$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_{\phi(N)} \quad \text{and} \quad \mathcal{O}_K/\mathfrak{p}_i \approx \mathbb{Z}/p\mathbb{Z} \text{ for each } i,$$
with $(e, f, g) = (1, 1, \phi(N))$. Here the cyclotomic polynomial $\Phi_N(X)$ has $\phi(N)$ distinct roots $\overline{r}_1, \dots, \overline{r}_{\phi(N)}$ in $\mathbb{Z}/p\mathbb{Z}$, and the prime divisors of $p\mathcal{O}_K$ are
$$\mathfrak{p}_i = \langle r_i, p \rangle \subset \mathcal{O}_K, \quad i = 1, \dots, \phi(N).$$
- The primes p that are primitive roots modulo N undergo pure residue field growth from $\mathbb{Q}$ to K,
$$p\mathcal{O}_K = \mathfrak{p} \quad \text{and} \quad [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = \phi(N),$$
with $(e, f, g) = (1, \phi(N), 1)$.
- The primes p that divide N are the primes that ramify, here using the fact that the case $N = 2 \bmod 4$ is excluded. The extreme case of ramification is
$$p\mathcal{O}_K = \mathfrak{p}^{\phi(N)} \text{ and } [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = 1 \quad \text{if } N = p^d \text{ for some } d \geq 1.$$
with $(e, f, g) = (\phi(N), 1, 1)$. Here the prime divisor of $p\mathcal{O}_K$ is
$$\mathfrak{p} = (1 - \zeta_{p^d})\mathcal{O}_K.$$

4. Cyclotomic Galois Theory and Cyclotomic Arithmetic

As shown above, the Galois group of $K = \mathbb{Q}(\zeta_N)$ is

$$G = \{\zeta_N \longmapsto \zeta_N^m : m + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Recall the decomposition $N = N_p \cdot p^d$ where $p^d \parallel N$. We freely make the identifications

$$G = (\mathbb{Z}/N\mathbb{Z})^\times = (\mathbb{Z}/N_p\mathbb{Z})^\times \times (\mathbb{Z}/p^d\mathbb{Z})^\times.$$

Fix a rational prime p. The inertia and decomposition subgroups of p in G are

$$I_p = \{1\} \times (\mathbb{Z}/p^d\mathbb{Z})^\times, \qquad D_p = \langle p + N_p\mathbb{Z}\rangle \times (\mathbb{Z}/p^d\mathbb{Z})^\times.$$

Thus $I_p \subset D_p$ and $|I_p| = e$ and $|D_p| = ef$.

The inertia field $K_{I,p}$ and the decomposition field $K_{D,p}$ of p are the intermediate fields of $K/\mathbb{Q}$ corresponding to the inertia and decomposition subgroups of G. Thus $\mathbb{Q} \subset K_{D,p} \subset K_{I,p} \subset K$.

- The decomposition field is so named because p decomposes there as
$$p\mathcal{O}_D = \mathbf{p}_{1,D} \cdots \mathbf{p}_{g,D}$$
with the $\mathbf{p}_{i,D}$ ideals. For each i there is no residue field growth, meaning that $[\mathcal{O}_D/\mathbf{p}_{i,D} : \mathbb{Z}/p\mathbb{Z}] = 1$, and visibly there is no ramification. The degree $[K_{D,p} : \mathbb{Q}] = g$ matches the number of factors of p. Because g is the index $[G : D_p]$, it is called the *decomposition index* of p in K.
- The inertia field is so named because each $\mathbf{p}_{i,D}$ remains inert in $\mathcal{O}_I$, which is to say that $\mathbf{p}_{i,D}\mathcal{O}_I$ takes the form $\mathbf{p}_{i,I}$ rather than decomposing further. Here there *is* residue field growth, specifically
$$[\mathcal{O}_I/\mathbf{p}_{i,I} : \mathcal{O}_D/\mathbf{p}_{i,D}] = f \quad \text{for } i = 1, \ldots, g,$$
and again there is no ramification. The degree $[K_{I,p} : K_{D,p}] = f$ matches the uniform residue field extension degree shown in the display, and f is called the *inertial degree* of p in K.
- Finally, each $\mathbf{p}_{i,I}$ ramifies totally in $\mathcal{O}_K$,
$$\mathbf{p}_{i,I}\mathcal{O}_K = \mathfrak{p}_i^e \quad \text{for } i = 1, \ldots, g.$$
Here there is no further decomposition and with no further residue field growth, $[\mathcal{O}_K/\mathfrak{p}_i : \mathcal{O}_I/\mathbf{p}_{i,I}] = 1$ for each i. The degree $[K : K_{I,p}] = e$ matches the ramification exponent in the display, and e is called the *ramification degree* of p in K.

To summarize, as we climb from $\mathbb{Q}$ through $K_{D,p}$ and $K_{I,p}$ to K, the prime p decomposes, then the residue fields grow, then each factor of p ramifies.

5. The Dedekind Zeta Function and its Euler Product

The ring of integers of K is

$$\mathcal{O}_K = \mathbb{Z}[\zeta_N].$$

Define the *norm* of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ to be

$$\mathrm{N}\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|.$$

Thus we tacitly assert without proof that the quotient is finite. We further assert without proof that the norm is strongly multiplicative. The relation $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = f$ with f as above says that

$$\mathrm{N}\mathfrak{p} = p^f \quad \text{where } \mathfrak{p} \mid p \text{ and } f \text{ is the inertial degree of } p \text{ in } K.$$

Definition 5.1. *The* **Nth cyclotomic Dedekind zeta function** *is*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathrm{N}\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

The sum is taken over the nonzero ideals of $\mathcal{O}_K$, and the product is taken over the maximal ideals.

We show that $\zeta_K(s)$ cannot converge for all positive real s but is analytic on $\mathrm{Re}(s) > 1$. Indeed, $\mathrm{N}\mathfrak{p} = p^f$ gives $p \leq \mathrm{N}\mathfrak{p} \leq p^{\phi(N)}$, from which $(1-p^{-\phi(N)s})^{-1} \leq (1-\mathrm{N}\mathfrak{p}^{-s})^{-1} \leq (1-p^{-s})^{-1}$ for $s > 0$, and then, because at most $\phi(N)$ ideals $\mathfrak{p}$ divide a rational prime p,

$$(1-p^{-\phi(N)s})^{-1} \leq \prod_{\mathfrak{p}|p}(1-\mathrm{N}\mathfrak{p}^{-s})^{-1} \leq (1-p^{-s})^{-\phi(N)}, \quad s > 0.$$

Because $\prod_p(1-p^{-\phi(N)s})^{-1} = \sum_{n\geq 1} n^{-\phi(N)s}$ diverges at $s = 1/\phi(N)$, so does $\prod_p \prod_{\mathfrak{p}|p}(1-\mathrm{N}\mathfrak{p}^{-s})^{-1} = \zeta_K(s)$. Similarly, because $\prod_p(1-p^{-s})^{-\phi(N)} = \zeta(s)^{\phi(N)}$ converges absolutely and uniformly on compacta in $\mathrm{Re}(s) > 1$, so does $\zeta_K(s)$; here we are using the fact that $|\mathrm{N}\mathfrak{a}^{-s}| = \mathrm{N}\mathfrak{a}^{-\mathrm{Re}(s)}$.

Next we obtain another expression for $\zeta_K(s)$. For any p, compute that

$$\prod_{\mathfrak{p}|p}(1-\mathrm{N}\mathfrak{p}^{-s})^{-1} = (1-p^{-fs})^{-g} = \prod_{k=0}^{f-1}(1-\zeta_f^k p^{-s})^{-g} = \prod_{\chi}(1-\chi(p)p^{-s})^{-1},$$

where the product is taken over all characters χ modulo N, each character understood to be the underlying primitive character extended to a multiplicative function on $\mathbb{Z}$. As discussed above, $\chi(p) = \zeta_f^k$ for g characters χ modulo N, independently of k, these characters being defined modulo N_p, while the characters χ modulo N that are not defined modulo N_p take p to 0 and thus contribute a trivial factor of 1 to the last product in the previous display. Overall, then, we have

$$\zeta_K(s) = \prod_p \prod_\chi (1-\chi(p)p^{-s})^{-1} = \prod_\chi \prod_p (1-\chi(p)p^{-s})^{-1},$$

which is to say that the Nth cyclotomic Dedekind zeta function factors as the product of all Dirichlet L-functions modulo N,

$$\boxed{\zeta_K(s) = \prod_\chi L(\chi, s).}$$

The boxed expression for $\zeta_K(s)$ in the previous display arises naturally in the proof of Dirichlet's theorem on primes in an arithmetic progression. We have seen that the function $L(1,s) = \zeta(s)$, which is initially defined only for $\mathrm{Re}(s) > 1$, extends to a meromorphic function on $\{\mathrm{Re}(s) > 0\}$ whose only singularity is a simple pole at $s = 1$, and that $L(\chi, s)$ for $\chi \neq 1$ extends to an analytic function on $\{\mathrm{Re}(s) > 0\}$. Thus the cyclotomic zeta function $\zeta_K(s)$ extends meromorphically to $\{\mathrm{Re}(s) > 0\}$ with its only possible pole at $s = 1$. There really is such a pole, because otherwise the defining sum expression for $\zeta_K(s)$ would converge for all $s > 0$, but we have shown above that this is impossible. The pole of $\zeta_K(s)$ at $s = 1$ is the crux of Dirichlet's theorem.