

0.1 Todo: [The Kuznetsov Trace Formula]

The Kuznetsov trace formula is an analog of the Petersson trace formula for weight zero Maass forms. From ??, $\mathcal{L}(N, \chi)$ admits an orthonormal basis of Maass forms for the point spectrum (these forms are generally not Hecke-Maass eigenforms because they need not be Hecke normalized or even cuspidal in the case of the discrete spectrum). However, by ?? and ?? we make take this orthonormal basis to consist of Hecke-Maass eigenforms and the constant function. Denote this basis by $\{u_j\}_{j \geq 0}$ with $u_0(z) = 1$ and let u_j be of type ν_j for $j \geq 1$. In particular, $\{u_j\}_{j \geq 1}$ is an orthonormal basis of Hecke-Maass eigenforms and each such form admits a Fourier series at the \mathfrak{a} cusp given by

$$(u_j | \sigma_{\mathfrak{a}})(z) = \sum_{n \neq 0} a_{j,\mathfrak{a}}(n) \sqrt{y} K_{\nu_j}(2\pi n y) e^{2\pi i n x}.$$

The Kuznetsov trace formula is an equation relating the Fourier coefficients $a_{j,\mathfrak{a}}(n)$ and $a_{j,\mathfrak{b}}(n)$ of the basis $\{u_j\}_{j \geq 1}$ for two cusps \mathfrak{a} and \mathfrak{b} of $\Gamma_0(N) \backslash \mathbb{H}$ to a sum of integral transforms involving test functions and Salié sums. Similar to the Petersson trace formula, we will compute the inner product of two Poincaré series $P_{n,\chi,\mathfrak{a}}(z, \psi)(z)$ and $P_{m,\chi,\mathfrak{b}}(z, \varphi)(z)$ in two different ways. The first will be geometric in nature while the second will be spectral. We first need to compute the Fourier series of such a Poincaré series. Although we will not need it explicitly, we will work over any congruence subgroup:

Proposition 0.1.1. *Let $m \geq 1$, χ be Dirichlet character with conductor dividing the level, \mathfrak{a} and \mathfrak{b} be cusps of $\Gamma \backslash \mathbb{H}$, and $\psi(y)$ be a smooth function such that $\psi(y) \ll_{\varepsilon} y^{1+\varepsilon}$ as $y \rightarrow 0$. The Fourier series of $P_{m,\chi,\mathfrak{a}}(z, \psi)$ on $\Gamma \backslash \mathbb{H}$ at the \mathfrak{b} cusp is given by*

$$(P_{m,\chi,\mathfrak{a}} | \sigma_{\mathfrak{b}})(z, \psi) = \sum_{t \in \mathbb{Z}} \left(\delta_{\mathfrak{a},\mathfrak{b}} \delta_{m,t} \psi(\text{Im}(z)) + \sum_{c \in \mathcal{C}_{\mathfrak{a},\mathfrak{b}}} \psi(y, m, t, c) S_{\chi,\mathfrak{a},\mathfrak{b}}(m, t, c) \right) e^{2\pi i t z},$$

where $\psi(y, m, t, c)$ is the integral transform given by

$$\psi(y, m, t, c) = \int_{\text{Im}(z)=y} \psi \left(\frac{y}{|cz|^2} \right) e^{-\frac{2\pi i m}{c^2 z} - 2\pi i t z} dz.$$

Proof. From the cocycle condition and ??, we have

$$(P_{m,\chi,\mathfrak{a}} | \sigma_{\mathfrak{b}})(z, \psi) = \delta_{\mathfrak{a},\mathfrak{b}} \psi(\text{Im}(z)) e^{2\pi i m z} + \sum_{\substack{c \in \mathcal{C}_{\mathfrak{a},\mathfrak{b}}, d \in \mathbb{Z} \\ d \pmod{c} \in \mathcal{D}_{\mathfrak{a},\mathfrak{b}}(c)}} \bar{\chi}(d) \psi \left(\frac{\text{Im}(z)}{|cz + d|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + cd} \right)},$$

where a and b are chosen such that $\det \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = 1$ and we have used the fact that

$$\frac{a}{c} - \frac{1}{c^2 z + cd} = \frac{az + b}{cz + d}.$$

Summing over all pairs (c, d) with $c \in \mathcal{C}_{\mathfrak{a},\mathfrak{b}}$, $d \in \mathbb{Z}$, and $d \pmod{c} \in \mathcal{D}_{\mathfrak{a},\mathfrak{b}}(c)$ is the same as summing over all triples (c, ℓ, r) with $c \in \mathcal{C}_{\mathfrak{a},\mathfrak{b}}$, $\ell \in \mathbb{Z}$, and r taken modulo c with $r \in \mathcal{D}_{\mathfrak{a},\mathfrak{b}}(c)$. Indeed, this is seen by writing $d = c\ell + r$. Moreover, since $ad - bc = 1$ we have $a(c\ell + r) - bc = 1$ which further implies that

$ar \equiv 1 \pmod{c}$. So we may take a to be the inverse for r modulo c . Then

$$\begin{aligned}
\sum_{\substack{c \in \mathcal{C}_{a,b}, d \in \mathbb{Z} \\ d \pmod{c} \in \mathcal{D}_{a,b}(c)}} \bar{\chi}(d) \psi \left(\frac{\text{Im}(z)}{|cz + d|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + cd} \right)} &= \sum_{(c, \ell, r)} \bar{\chi}(c\ell + r) \psi \left(\frac{\text{Im}(z)}{|cz + c\ell + r|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + c^2 \ell + cr} \right)} \\
&= \sum_{(c, \ell, r)} \bar{\chi}(r) \psi \left(\frac{\text{Im}(z)}{|cz + c\ell + r|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + c^2 \ell + cr} \right)} \\
&= \sum_{\substack{c \in \mathcal{C}_{a,b} \\ r \in \mathcal{D}_{a,b}(c)}} \sum_{\ell \in \mathbb{Z}} \bar{\chi}(r) \psi \left(\frac{\text{Im}(z)}{|cz + c\ell + r|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + c^2 \ell + cr} \right)} \\
&= \sum_{\substack{c \in \mathcal{C}_{a,b} \\ r \in \mathcal{D}_{a,b}(c)}} \bar{\chi}(r) \sum_{\ell \in \mathbb{Z}} \psi \left(\frac{\text{Im}(z)}{|cz + c\ell + r|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + c^2 \ell + cr} \right)},
\end{aligned}$$

where on the right-hand side it is understood that we are summing over all triples (c, ℓ, r) with the prescribed properties and the second line holds since χ has conductor dividing the level and $d \in \mathcal{D}_{a,b}(c)$ is determined modulo c . Now let

$$I_{c,r}(z, \psi) = \sum_{\ell \in \mathbb{Z}} \psi \left(\frac{\text{Im}(z)}{|cz + c\ell + r|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + c^2 \ell + cr} \right)}.$$

We apply the Poisson summation formula to $I_{c,r}(z, \psi)$. This is allowed since the summands are absolutely integrable by ??, as they exhibit polynomial decay of order $\sigma > 1$ because $\psi(y) \ll_{\varepsilon} y^{1+\varepsilon}$ as $y \rightarrow 0$, and $I_{c,r}(z, \psi)$ is holomorphic because $(P_{m,\chi,a}|\sigma_b)(z, \psi)$ is. By the identity theorem it suffices to apply the Poisson summation formula for $z = iy$ with $y > 0$. So let $f(x)$ be given by

$$f(x) = \psi \left(\frac{y}{|cx + r + icy|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 x + cr + ic^2 y} \right)}.$$

As we have just noted, $f(x)$ is absolutely integrable on \mathbb{R} . We compute the Fourier transform:

$$\hat{f}(t) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i t x} dx = \int_{-\infty}^{\infty} \psi \left(\frac{y}{|cx + r + icy|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 x + cr + ic^2 y} \right)} e^{-2\pi i t x} dx.$$

Complexify the integral to get

$$\int_{\text{Im}(z)=0} \psi \left(\frac{y}{|cz + r + icy|^2} \right) e^{2\pi i m \left(\frac{a}{c} - \frac{1}{c^2 z + cr + ic^2 y} \right)} e^{-2\pi i t z} dz.$$

Now make the change of variables $z \rightarrow z - \frac{r}{c} - iy$ to obtain

$$e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c} - 2\pi t y} \int_{\text{Im}(z)=y} \psi \left(\frac{y}{|cz|^2} \right) e^{-\frac{2\pi i m}{c^2 z} - 2\pi i t z} dz.$$

As the remaining integral is $\psi(y, m, t, c)$, it follows that

$$\hat{f}(t) = \psi(y, m, t, c) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c} - 2\pi t y}.$$

By the Poisson summation formula and the identity theorem, we have

$$I_{c,r}(z, \psi) = \sum_{t \in \mathbb{Z}} (\psi(y, m, t, c) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c}}) e^{2\pi i t z},$$

for all $z \in \mathbb{H}$. Substituting this back into the Eisenstein series gives a form of the Fourier series:

$$\begin{aligned}
(P_{m,\chi,a}|\sigma_b)(z, \psi) &= \delta_{a,b} \psi(\text{Im}(z)) e^{2\pi i m z} + \sum_{\substack{c \in \mathcal{C}_{a,b} \\ r \in \mathcal{D}_{a,b}}} \bar{\chi}(r) \sum_{t \in \mathbb{Z}} \psi(y, m, t, c) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c}} e^{2\pi i t z} \\
&= \sum_{t \in \mathbb{Z}} \left(\delta_{a,b} \delta_{m,t} \psi(\text{Im}(z)) + \sum_{\substack{c \in \mathcal{C}_{a,b} \\ r \in \mathcal{D}_{a,b}}} \bar{\chi}(r) \psi(y, m, t, c) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c}} \right) e^{2\pi i t z} \\
&= \sum_{t \in \mathbb{Z}} \left(\delta_{a,b} \delta_{m,t} \psi(\text{Im}(z)) + \sum_{c \in \mathcal{C}_{a,b}} \psi(y, m, t, c) \sum_{r \in \mathcal{D}_{a,b}} \bar{\chi}(r) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c}} \right) e^{2\pi i t z}.
\end{aligned}$$

We will simplify the innermost sum. Since a is the inverse for r modulo c , the innermost sum above becomes

$$\sum_{r \in \mathcal{D}_{a,b}} \bar{\chi}(r) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{r}{c}} = \sum_{r \in \mathcal{D}_{a,b}} \bar{\chi}(\bar{a}) e^{2\pi i m \frac{a}{c} + 2\pi i t \frac{\bar{a}}{c}} = \sum_{r \in \mathcal{D}_{a,b}} \chi(a) e^{\frac{2\pi i (am + \bar{a}t)}{c}} = S_{\chi,a,b}(m, t, c).$$

So at last, we obtain our desired Fourier series:

$$(P_{m,\chi,a}|\sigma_b)(z) = \sum_{t \in \mathbb{Z}} \left(\delta_{a,b} \delta_{m,t} \psi(\text{Im}(z)) + \sum_{c \in \mathcal{C}_{a,b}} \psi(y, m, t, c) S_{\chi,a,b}(m, t, c) \right) e^{2\pi i t z}.$$

□

We can now derive the first half of the Kuznetsov trace formula by computing the inner product between $P_{n,\chi,a}(z, \psi)$ and $P_{m,\chi,b}(z, \varphi)$:

$$\begin{aligned}
\langle P_{n,\chi,a}(\cdot, \psi), P_{m,\chi,b}(\cdot, \varphi) \rangle &= \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}_{\Gamma_0(N)}} P_{n,\chi,a}(z, \psi) \overline{P_{m,\chi,b}(z, \varphi)} d\mu \\
&= \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}_{\Gamma_0(N)}} \sum_{\gamma \in \Gamma_b \backslash \Gamma_0(N)} \chi(\gamma) P_{n,\chi,a}(z, \psi) \overline{\varphi(\text{Im}(\sigma_b^{-1} \gamma z))} e^{-2\pi i m \overline{\sigma_b^{-1} \gamma z}} d\mu \\
&= \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}_{\Gamma_0(N)}} \sum_{\gamma \in \Gamma_b \backslash \Gamma_0(N)} P_{n,\chi,a}(\gamma z, \psi) \overline{\varphi(\text{Im}(\sigma_b^{-1} \gamma z))} e^{-2\pi i m \overline{\sigma_b^{-1} \gamma z}} d\mu \\
&= \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}_{\sigma_b^{-1} \Gamma_0(N) \sigma_b}} \sum_{\gamma \in \Gamma_b \backslash \Gamma_0(N)} P_{n,\chi,a}(\gamma \sigma_b z, \psi) \overline{\varphi(\text{Im}(\sigma_b^{-1} \gamma \sigma_b z))} e^{-2\pi i m \overline{\sigma_b^{-1} \gamma \sigma_b z}} d\mu \\
&= \frac{1}{V_{\Gamma_0(N)}} \int_{\mathcal{F}_{\sigma_b^{-1} \Gamma_0(N) \sigma_b}} \sum_{\gamma \in \Gamma_\infty \backslash \sigma_b^{-1} \Gamma_0(N) \sigma_b^{-1}} P_{n,\chi,a}(\sigma_b \gamma z, \psi) \overline{\varphi(\text{Im}(\gamma z))} e^{-2\pi i m \overline{\gamma z}} d\mu \\
&= \frac{1}{V_{\Gamma_0(N)}} \int_{\Gamma_\infty \backslash \mathbb{H}} (P_{n,\chi,a}|\sigma_b)(z, \psi) \overline{\varphi(\text{Im}(z))} e^{-2\pi i m \bar{z}} d\mu,
\end{aligned}$$

where in the third line we have used the automorphy of $P_{n,\chi,a}(z, \psi)$, in the forth and fifth lines we have made the change of variables $z \rightarrow \sigma_b z$ and $\gamma \rightarrow \sigma_b \gamma \sigma_b^{-1}$ respectively, and in the sixth line we have unfolded. Now substitute in the Fourier series of $P_{n,\chi,a}(z, \psi)$ at the b cusp to obtain

$$\frac{1}{V_{\Gamma_0(N)}} \int_{\Gamma_\infty \backslash \mathbb{H}} \sum_{t \in \mathbb{Z}} \left(\delta_{a,b} \delta_{n,t} \psi(\text{Im}(z)) + \sum_{c \in \mathcal{C}_{a,b}} \psi(y, n, t, c) S_{\chi,a,b}(n, t, c) \right) \overline{\varphi(\text{Im}(z))} e^{2\pi i t z - 2\pi i m \bar{z}} d\mu,$$

which is equivalent to

$$\frac{1}{V_{\Gamma_0(N)}} \int_0^\infty \int_0^1 \sum_{t \geq 1} \left(\delta_{a,b} \delta_{n,t} \psi(y) + \sum_{c \in \mathcal{C}_{a,b}} \psi(y, n, t, c) S_{\chi,a,b}(n, t, c) \right) \overline{\varphi(y)} e^{2\pi i(t-m)x} e^{-2\pi(t+m)y} \frac{dx dy}{y^2}.$$

By the dominated convergence theorem, we can interchange the sum and the two integrals. Then ?? implies that the inner integral cuts off all of the terms except the diagonal $t = m$. This leaves

$$\frac{1}{V_{\Gamma_0(N)}} \int_0^\infty \left(\delta_{a,b} \delta_{n,m} \psi(y) + \sum_{c \in \mathcal{C}_{a,b}} \psi(y, n, m, c) S_{\chi,a,b}(n, m, c) \right) \overline{\varphi(y)} e^{-4\pi m y} \frac{dy}{y^2}.$$

Interchanging the integral and the remaining sum by the dominated convergence theorem again, we arrive at

$$\langle P_{n,\chi,a}(\cdot, \psi), P_{m,\chi,b}(\cdot, \varphi) \rangle = \delta_{a,b} \delta_{n,m} (\psi, \varphi)_{n,m} + \sum_{c \in \mathcal{C}_{a,b}} S_{\chi,a,b}(n, m, c) V(n, m, c, \psi, \varphi),$$

where we have set

$$(\psi, \varphi)_{n,m} = \frac{1}{V_{\Gamma_0(N)}} \int_0^\infty \psi(y) \overline{\varphi(y)} e^{-2\pi(n+m)y} \frac{dy}{y^2},$$

and

$$V(n, m, c; \psi, \varphi) = \frac{1}{V_{\Gamma_0(N)}} \int_0^\infty \int_{\text{Im}(z)=y} \psi\left(\frac{y}{|cz|^2}\right) \overline{\varphi(y)} e^{-\frac{2\pi i m}{c^2 z} - 2\pi i n z - 4\pi m y} \frac{dz dy}{y^2}.$$

This is the first half of the Kuznetsov trace formula. For the second half, ?? gives

$$P_{n,\chi,a}(\cdot, \psi) = \sum_{j \geq 0} \langle P_{n,\chi,a}(\cdot, \psi), u_j \rangle u_j(z) + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \left\langle P_{n,\chi,a}(\cdot, \psi), E_a\left(\cdot, \frac{1}{2} + ir\right) \right\rangle E_a\left(z, \frac{1}{2} + ir\right) dr,$$

and

$$P_{m,\chi,a}(\cdot, \varphi) = \sum_{j \geq 0} \langle P_{m,\chi,a}(\cdot, \varphi), u_j \rangle u_j(z) + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \left\langle P_{m,\chi,a}(\cdot, \varphi), E_a\left(\cdot, \frac{1}{2} + ir\right) \right\rangle E_a\left(z, \frac{1}{2} + ir\right) dr.$$

By orthonormality, it follows that

$$\begin{aligned} \langle P_{n,\chi,a}(\cdot, \psi), P_{m,\chi,a}(\cdot, \varphi) \rangle &= \sum_j \langle P_{n,\chi,a}(\cdot, \psi), u_j \rangle \overline{\langle P_{m,\chi,a}(\cdot, \varphi), u_j \rangle} \\ &\quad + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \left\langle P_{n,\chi,a}(\cdot, \psi), E_a\left(\cdot, \frac{1}{2} + ir\right) \right\rangle \overline{\left\langle P_{m,\chi,a}(\cdot, \varphi), E_a\left(\cdot, \frac{1}{2} + ir\right) \right\rangle} dr. \end{aligned}$$

Now we must simplify the remaining inner products. Let $f \in \mathcal{L}(N, \chi)$ with Fourier series

$$f(z) = a^+(0) y^{\frac{1}{2}+\nu} + a^-(0) y^{\frac{1}{2}-\nu} + \sum_{n \neq 0} a(n) \sqrt{y} K_\nu(2\pi|n|y) e^{2\pi i n x}.$$

By unfolding the integral in the Petersson inner product and cutting off everything except the diagonal using ?? exactly as in the case for $\langle P_{n,\chi,a}(\cdot, \psi), P_{m,\chi,a}(\cdot, \varphi) \rangle$, we see that

$$\langle P_{n,\chi,a}(\cdot, \psi), f \rangle = \frac{1}{V_\Gamma} \int_0^\infty \overline{a(n) \sqrt{y} K_\nu(2\pi n y)} \psi(y) e^{-4\pi m y} \frac{dy}{y^2}.$$

Now set

$$\omega_\nu(n, \psi) = \frac{1}{V_\Gamma} \int_0^\infty \sqrt{y} K_\nu(2\pi|n|y) \overline{\psi(y)} e^{-4\pi my} \frac{dy}{y^2}.$$

Then it follows from the Fourier series of cusp forms and Eisenstein series that

$$\langle P_{n,\chi,a}(\cdot, \psi), u_j \rangle = \overline{a_j(n)} \omega_{\nu_j}(n, \psi),$$

for $j \geq 1$ and

$$\left\langle P_{n,\chi,a}(\cdot, \psi), E_a\left(\cdot, \frac{1}{2} + ir\right) \right\rangle = \overline{\tau_a\left(n, \frac{1}{2} + ir\right)} \omega_{ir}(n, \psi).$$

In particular, $\langle P_{n,\chi,a}(\cdot, \psi), u_0 \rangle = 0$. So we obtain

$$\begin{aligned} \langle P_{n,\chi,a}(\cdot, \psi), P_{m,\chi,a}(\cdot, \varphi) \rangle &= \sum_{j \geq 1} \overline{a_j(n)} a_j(m) \overline{\omega(n, \psi)} \omega(m, \varphi) \\ &\quad + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \overline{\tau_a\left(n, \frac{1}{2} + ir\right)} \tau_a\left(m, \frac{1}{2} + ir\right) \overline{\omega(n, \psi)} \omega(m, \varphi) dr. \end{aligned}$$

This is the second half of the Kuznetsov trace formula. Equating the first and second halves we get the **Kuznetsov trace formula**:

$$\begin{aligned} \delta_{n,m}(\psi, \varphi) + \sum_{\substack{c \geq 1 \\ c \equiv 0 \pmod{N}}} \frac{1}{c} S_\chi(n, m, c) V(n, m, c, \psi, \varphi) &= \sum_{j \geq 1} \overline{a_j(n)} a_j(m) \overline{\omega(n, \psi)} \omega(m, \varphi) \\ &\quad + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \overline{\tau_a\left(n, \frac{1}{2} + ir\right)} \tau_a\left(m, \frac{1}{2} + ir\right) \overline{\omega(n, \psi)} \omega(m, \varphi) dr. \end{aligned}$$

The left-hand side is called the **geometric side** and the right-hand side is called the **spectral side**. We collect our work as a theorem:

Theorem 0.1.1 (Kuznetsov trace formula). *Let $\{u_j\}_{j \geq 1}$ be an orthonormal basis of Hecke-Maass eigenforms for $\mathcal{L}(N, \chi)$ of types ν_j with Fourier coefficients $a_j(n)$. Then for any positive integers $n, m \geq 1$, we have*

$$\begin{aligned} \delta_{n,m}(\psi, \varphi) + \sum_{\substack{c \geq 1 \\ c \equiv 0 \pmod{N}}} \frac{1}{c} S_\chi(n, m, c) V(n, m, c, \psi, \varphi) &= \sum_{j \geq 1} \overline{a_j(n)} a_j(m) \overline{\omega(n, \psi)} \omega(m, \varphi) \\ &\quad + \sum_a \frac{1}{4\pi} \int_{-\infty}^\infty \overline{\tau_a\left(n, \frac{1}{2} + ir\right)} \tau_a\left(m, \frac{1}{2} + ir\right) \overline{\omega(n, \psi)} \omega(m, \varphi) dr. \end{aligned}$$

0.2 Todo: [Cyclotomic Number Fields]

Let ω be a primitive n -th root of unity. We call $\mathbb{Q}(\omega)$ the n -th **cyclotomic field**. Note that $\mathbb{Q}(\omega)$ is independent of the choice of primitive root ω since $\mathbb{Q}(\omega)$ contains all n -th roots of unity. As ω is a root of $x^n - 1$, we see that $\mathbb{Q}(\omega)/\mathbb{Q}$ is a finite extension of degree at most n . In particular, $\mathbb{Q}(\omega)$ is a number field. More generally, we say that a number field K is **cyclotomic** if K is the n -th cyclotomic field for some $n \geq 1$. That is, $K = \mathbb{Q}(\omega)$ for some primitive n -th root of unity ω . In any case, our aim is to study the structure of cyclotomic number fields $\mathbb{Q}(\omega)$. Our first step is to compute the degree of $\mathbb{Q}(\omega)$ which is the

degree of the minimal polynomial of ω over \mathbb{Q} . Accordingly, we define the n -th **cyclotomic polynomial** $\Phi_n(x)$ by

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (x - \omega^k).$$

That is, $\Phi_n(x)$ is the polynomial whose roots are the primitive n -th roots of unity. It is clearly monic, of degree $\varphi(n)$, and divides $x^n - 1$. As every n -th root of unity is a primitive d -th root of unity for some $d \mid n$, we also find that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x). \quad (1)$$

Clearly $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. When $n = p$ for a prime p , Equation (1) implies

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

More generally, writing $n = p^k$ and inducting on k using Equation (1) gives

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + 1. \quad (2)$$

Observe from Equation (2) that $\Phi_{p^k}(x)$ has coefficients in \mathbb{Z} . This is true for a general cyclotomic polynomial $\Phi_n(x)$ in addition to irreducibility over \mathbb{Z} as the following proposition shows:

Proposition 0.2.1. *$\Phi_n(x)$ has coefficients in and is irreducible over \mathbb{Z} .*

Proof. We first show $\Phi_n(x)$ has coefficients in \mathbb{Z} and we will argue by induction. The claim is true for $n = 1$ since $\Phi_1(x) = x - 1$. So assume by induction that it is true for all $1 \leq d < n$. In view of Equation (1), we have

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d \mid n \\ d < n}} \Phi_d(x),$$

and $\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)$ has coefficients in \mathbb{Z} . Therefore $\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)$ divides $x^n - 1$ in $\mathbb{Q}[x]$ and hence in $\mathbb{Z}[x]$ as well by Gauss's lemma. Thus $\Phi_n(x)$ has coefficients in \mathbb{Z} as desired. We now show $\Phi_n(x)$ is irreducible over \mathbb{Z} . So suppose

$$\Phi_n(x) = f(x)g(x),$$

for monic polynomials $f(x), g(x) \in \mathbb{Z}[x]$ (recall $\Phi_n(x)$ is monic) with $f(x)$ irreducible. Then it suffices to show $f(x) = \Phi_n(x)$. Now let ω be a root of $f(x)$. Then ω is also a root of $\Phi_n(x)$ and necessarily a primitive n -th roots of unity. Since $f(x)$ is monic and irreducible it is necessarily the minimal polynomial of ω over \mathbb{Q} . Now let p be any prime not dividing n . Then ω^p is also a primitive n -th root of unity and hence a root of either $f(x)$ or $g(x)$. Suppose ω^p is a root of $g(x)$. Then ω is a root of $g(x^p)$, and since $f(x)$ is the minimal polynomial of ω over \mathbb{Q} , $f(x)$ divides $g(x^p)$ in $\mathbb{Q}[x]$. By Gauss's lemma, it follows that $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$ too. Therefore

$$g(x^p) = f(x)h(x),$$

for a monic polynomial $h(x) \in \mathbb{Z}[x]$. Reducing this factorization modulo p , we obtain

$$\bar{g}(x^p) \equiv \bar{g}(x)^p \equiv \bar{f}(x)\bar{h}(x) \pmod{p},$$

where the first congruence holds since $\bar{g}(x^p) = \bar{g}(x)^p$ in $\mathbb{F}_p[x]$ (recall Fermat's little theorem and that the characteristic of \mathbb{F}_p is p). As $p \geq 2$, this equivalence shows that $\bar{f}(x)$ and $\bar{h}(x)$ must have a common factor.

In other words, $\bar{g}(x^p)$ has a multiple root and therefore $\bar{g}(x)$ does as well. Reducing the factorization for $\Phi_n(x)$ modulo p gives

$$\overline{\Phi_n}(x) \equiv \bar{f}(x)\bar{g}(x) \pmod{p}.$$

Then $\overline{\Phi_n}(x)$ has a multiple root since $\bar{g}(x)$ does. Since $\overline{\Phi_n}(x)$ divides $x^n - 1$ (because $\Phi_n(x)$ does and $x^n - 1$ is itself reduced modulo p), it follows that $x^n - 1$ has a multiple root over \mathbb{F}_p . This is impossible since $x^n - 1$ has n distinct roots as p does not divide n (recall that the derivative of $x^n - 1$ is nx^{n-1} which is relatively prime to p). It follows that ω^p cannot be a root of $g(x)$ and is therefore a root of $f(x)$. Now let $k \in (\mathbb{Z}/n\mathbb{Z})^*$ and write $k = p_1 p_2 \cdots p_k$ as a product of primes not dividing n . Then $\omega^k = \omega^{p_1 p_2 \cdots p_k}$ is a root of $f(x)$ and hence every primitive n -th root of unity is a root of $f(x)$. Thus $f(x) = \Phi_n(x)$ which proves $\Phi_n(x)$ is irreducible over \mathbb{Z} . \square

Since $\Phi_n(x)$ is monic, Proposition 0.2.1 implies that $\Phi_n(x)$ is the minimal polynomial of ω over \mathbb{Q} and hence of every primitive n -th root of unity over \mathbb{Q} . It follows that the degree of $\mathbb{Q}(\omega)$ is $\varphi(n)$ because this is the degree of $\Phi_n(x)$. This implies $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_n(x)$ over \mathbb{Q} because if one primitive n -th root of unity belongs to a field then they all do (as they are powers of each other). In particular, $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal and hence Galois. Moreover, every primitive n -root of unity is an algebraic integer since $\Phi_n(x)$ also has coefficients in \mathbb{Z} by Proposition 0.2.1. We now turn to the question of the ring of integers of $\mathbb{Q}(\omega)$. For convenience write $\mathcal{O}_\omega = \mathcal{O}_{\mathbb{Q}(\omega)}$ and set

$$\mathfrak{p}_\omega = (1 - \omega)\mathcal{O}_\omega.$$

We will first prove a useful lemma which shows that \mathfrak{p}_ω is a prime of $\mathbb{Q}(\omega)$ and more in the case n is a prime power:

Lemma 0.2.1. *Let $\mathbb{Q}(\omega)$ be the cyclotomic number field generated by a primitive p^e -th root of unity ω with for some prime p and $e \geq 1$. Then*

$$p\mathcal{O}_\omega = \mathfrak{p}_\omega^{\varphi(p^e)}.$$

In particular, \mathfrak{p}_ω is a prime above p with $f_p(\mathfrak{p}_\omega) = 1$. Moreover, $1, \omega, \dots, \omega^{\varphi(p^e)-1}$ is a basis for $\mathbb{Q}(\omega)/\mathbb{Q}$ with

$$d_{\mathbb{Q}(\omega)/\mathbb{Q}}(1, \omega, \dots, \omega^{\varphi(p^e)-1}) = \pm p^{\varphi(p^e)e - p^{e-1}}.$$

Proof. In view of the definition of $\Phi_{p^e}(x)$ and Equation (2), we have

$$x^{p^{e-1}(p-1)} + x^{p^{e-1}(p-2)} + \cdots + 1 = \prod_{k \in (\mathbb{Z}/p^e\mathbb{Z})^*} (x - \omega^k).$$

Setting $x = 1$ gives

$$p = \prod_{k \in (\mathbb{Z}/p^e\mathbb{Z})^*} (1 - \omega^k).$$

In the case $e = 1$, ω is a primitive p -th root of unity. Then $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \omega) = p$ by ?? since $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois. In any case, the factors $1 - \omega^k$ are clearly algebraic integers because ω is (as a consequence of Proposition 0.2.1). Then

$$\varepsilon_k = \frac{1 - \omega^k}{1 - \omega} = \omega^{k-1} + \omega^{k-2} + \cdots + 1,$$

is also an algebraic integer and satisfies $1 - \omega^k = \varepsilon_k(1 - \omega)$. Moreover,

$$\varepsilon_k^{-1} = \frac{1 - \omega}{1 - \omega^k} = \frac{1 - \omega^{k\bar{k}}}{1 - \omega^k} = \omega^{k(\bar{k}-1)} + \omega^{k(\bar{k}-2)} + \cdots + 1,$$

is also an algebraic integer. This means ε_k is a unit in \mathcal{O}_ω . So upon setting $\varepsilon = \prod_{k \in (\mathbb{Z}/p^e\mathbb{Z})^*} \varepsilon_k$, we conclude that

$$p = \varepsilon(1 - \omega)^{\varphi(p^e)},$$

and therefore

$$p\mathcal{O}_\omega = \mathfrak{p}_\omega^{\varphi(p^e)}.$$

Since the degree of $\mathbb{Q}(\omega)$ is $\varphi(p^e)$, the fundamental equality implies that \mathfrak{p}_ω is prime (otherwise any prime factor has ramification index at least $\varphi(p^e)$) and that $f_p(\mathfrak{p}_\omega) = 1$. This proves the first two statements. For the last two statements, $1, \omega, \dots, \omega^{\varphi(p^e)-1}$ is a basis for $\mathbb{Q}(\omega)/\mathbb{Q}$ since ω is a primitive element for $\mathbb{Q}(\omega)/\mathbb{Q}$. Now let $\omega_1, \dots, \omega_{\varphi(p^e)}$ be the conjugates of ω with $\omega_1 = \omega$. Then

$$\Phi_{p^e}(x) = \prod_{1 \leq i \leq \varphi(p^e)} (x - \omega_i).$$

Now ?? and ?? (since $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois) give the first and last equalities in the following chain respectively:

$$d(1, \lambda, \dots, \lambda^{\varphi(p^e)}) = \pm \prod_{\substack{1 \leq i, j \leq \varphi(p^e) \\ i \neq j}} (\omega_i - \omega_j)^2 = \pm \prod_{1 \leq i \leq \varphi(p^e)} \Phi'_{p^e}(\omega_i) = \pm N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi'_{p^e}(\omega)).$$

It remains to show $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi'_{p^e}(\omega)) = \pm p^{p^{(e-1)(ep-e-1)}}$. To this end, Equation (2) implies

$$(x^{p^{e-1}} - 1)\Phi_{p^e}(x) = x^{p^e} - 1,$$

and differentiating gives

$$(p^{e-1} - 1)x^{p^{e-1}-1}\Phi_{p^e}(x) + (x^{p^{e-1}} - 1)\Phi'_{p^e}(x) = p^e x^{p^e-1}.$$

Now set $x = \omega$ and let $\xi = \omega^{p^{e-1}}$ to obtain

$$(\xi - 1)\Phi'_{p^e}(\omega) = p^e \omega^{-1},$$

where ξ is a primitive p -th root of unity. As $N_{\mathbb{Q}(\xi)/\mathbb{Q}}(1 - \xi) = p$ from our previous work, we compute

$$\begin{aligned} N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \xi) &= \prod_{k \in (\mathbb{Z}/p^e\mathbb{Z})^*} (1 - \xi^k) \\ &= \omega^{p+2p+\dots+(p^{e-1}-1)p} \left(\prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (1 - \xi^k) \right)^{p^{e-1}} \\ &= \omega^{\frac{p^n(p^{n-1}-1)}{2}} \left(\prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (1 - \xi^k) \right)^{p^{e-1}} \\ &= \left(\prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (1 - \xi^k) \right)^{p^{e-1}} \\ &= N_{\mathbb{Q}(\xi)/\mathbb{Q}}(1 - \xi)^{p^{e-1}} \\ &= p^{p^{e-1}}, \end{aligned}$$

where the first and second to last equalities follow by ?? since $\mathbb{Q}(\omega)/\mathbb{Q}$ and $\mathbb{Q}(\xi)/\mathbb{Q}$ are Galois. Thus $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\xi - 1) = \pm p^{p^{e-1}}$. Our previous identity is equivalent to

$$\Phi'_{p^e}(\omega) = \frac{p^e \omega^{-1}}{(\xi - 1)},$$

and multiplicativity of the norm together with ?? give

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi'_{p^e}(\omega)) = \frac{p^{\varphi(p^e)e} N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega^{-1})}{N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\xi - 1)} = \pm p^{\varphi(p^e)e - p^{e-1}}.$$

This completes the proof. □

With Lemma 0.2.1 we can prove \mathcal{O}_ω is monogenic in full generality:

Proposition 0.2.2. *Let $\mathbb{Q}(\omega)$ be the cyclotomic number field generated by a primitive n -th root of unity ω . Then $\mathbb{Q}(\omega)$ is monogenic where*

$$\mathcal{O}_\omega = \mathbb{Z}[\omega].$$

Proof. The claim is trivial when $n = 1$ so assume $n \geq 2$. We will now prove the claim when $n = p^e$ for a prime p and $e \geq 1$. By Lemma 0.2.1, $1, \omega, \dots, \omega^{\varphi(p^e)-1}$ is a basis for $\mathbb{Q}(\omega)/\mathbb{Q}$ and

$$d_{\mathbb{Q}(\omega)/\mathbb{Q}}(1, \omega, \dots, \omega^{\varphi(p^e)-1}) = \pm p^{\varphi(p^e)e - p^{e-1}}.$$

Then ?? implies

$$p^{\varphi(p^e)e - p^{e-1}} \mathcal{O}_\omega \subseteq \mathbb{Z}[\omega] \subseteq \mathcal{O}_\omega.$$

Moreover, $\mathbb{F}_{\mathfrak{p}_\omega} \cong \mathbb{F}_p$ since \mathfrak{p}_ω is a prime above p with $f_p(\mathfrak{p}_\omega) = 1$ by Lemma 0.2.1. Therefore $\mathcal{O}_\omega = \mathbb{Z} + \mathfrak{p}_\omega$ which implies

$$\mathcal{O}_\omega = \mathbb{Z}[\omega] + \mathfrak{p}_\omega.$$

Multiplying by $1 - \omega$ gives $\mathfrak{p}_\omega = (1 - \omega)\mathbb{Z}[\omega] + \mathfrak{p}_\omega^2$. Combining with the previous identity results in

$$\mathcal{O}_\omega = \mathbb{Z}[\omega] + \mathfrak{p}_\omega^2,$$

because $(1 - \omega)\mathbb{Z}[\omega] \subseteq \mathbb{Z}[\omega]$. Iterating this procedure gives

$$\mathcal{O}_\omega = \mathbb{Z}[\omega] + \mathfrak{p}_\omega^t,$$

for any $t \geq 1$. Taking $t = \varphi(p^e)(\varphi(p^e)e - p^{e-1})$ shows

$$\mathcal{O}_\omega = \mathbb{Z}[\omega] + p^{\varphi(p^e)e - p^{e-1}} \mathcal{O}_\omega = \mathbb{Z}[\omega],$$

because $p\mathcal{O}_\omega = \mathfrak{p}_\omega^{\varphi(p^e)}$ by Lemma 0.2.1 and that $p^{\varphi(p^e)e - p^{e-1}} \mathcal{O}_\omega \subseteq \mathbb{Z}[\omega]$. This proves the claim in the case n is a prime power. For the general case, let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n . Then $\omega_i = \omega^{\frac{n}{p_i^{e_i}}}$ is a primitive $p_i^{e_i}$ -th root of unity for $1 \leq i \leq r$ and $\omega = \omega_1 \cdots \omega_r$. This factorization of ω implies

$$\mathbb{Q}(\omega) = \mathbb{Q}(\omega_1) \cdots \mathbb{Q}(\omega_r).$$

In addition, since $p_1^{e_1}, \dots, p_r^{e_r}$ are pairwise relatively prime we have

$$\mathbb{Q}(\omega_1) \cdots \mathbb{Q}(\omega_{i-1}) \cap \mathbb{Q}(\omega_i) = \mathbb{Q},$$

for all i . **Todo:** [xxx] □

0.3 The Ideal Norm

Let us now prove some properties about the ideal norm. We first show that it respects localization:

Proposition 0.3.1. *Let \mathcal{O}/\mathfrak{o} be a Dedekind extension of separable extension L/K and let $D \subseteq \mathfrak{o} - \{0\}$ be a multiplicative subset. Then for any fractional ideal \mathfrak{F} of \mathcal{O} , we have*

$$N_{\mathcal{O}D^{-1}/\mathfrak{o}D^{-1}}(\mathfrak{F}D^{-1}) = N_{\mathcal{O}/\mathfrak{o}}(\mathfrak{F})D^{-1}.$$

Proof. Since the ideal norm is multiplicative, it suffices to prove the claim in the case of a prime \mathfrak{P} of \mathcal{O} . Then we must show

$$N_{\mathcal{O}D^{-1}/\mathfrak{o}D^{-1}}(\mathfrak{P}D^{-1}) = N_{\mathcal{O}/\mathfrak{o}}(\mathfrak{P})D^{-1}.$$

This is immediate from ?? and the definition of the ideal norm. □

The ideal norm is also compatible with the field trace:

Proposition 0.3.2. *Let \mathcal{O}/\mathfrak{o} be a Dedekind extension of degree n separable extension L/K . Then for any $\lambda \in \mathcal{O}$, we have*

$$N_{\mathcal{O}/\mathfrak{o}}(\lambda\mathcal{O}) = N_{L/K}(\lambda)\mathfrak{o}.$$

Proof. In light of Proposition 0.3.1, it suffices to assume \mathcal{O}/\mathfrak{o} is a local Dedekind extension. Therefore \mathfrak{o} is a discrete valuation ring, \mathcal{O} is a principal ideal domain, and \mathcal{O}/\mathfrak{o} admits an integral basis $\alpha_1, \dots, \alpha_n$ making \mathcal{O} a free \mathfrak{o} -module of rank n . Let \mathfrak{p} be the unique prime of \mathfrak{o} and π be a uniformizer so that $\mathfrak{p} = \pi\mathfrak{o}$. Since the ideal norm and the field norm are both multiplicative and \mathcal{O} and \mathfrak{o} are both unique factorization domains, we may assume that λ is prime. Then $\lambda\mathcal{O} = \mathfrak{P}$ for some prime \mathfrak{P} of \mathcal{O} . So on the one hand,

$$N_{\mathcal{O}/\mathfrak{o}}(\lambda\mathcal{O}) = \mathfrak{p}^{f_{\mathfrak{p}}(\mathfrak{P})}.$$

As \mathfrak{o} is a discrete valuation ring, we have the prime factorization $N_{L/K}(\lambda) = \mu\pi^f$. So on the other hand,

$$N_{L/K}(\lambda)\mathfrak{o} = \mathfrak{p}^f.$$

It now suffices to show that $f = f_{\mathfrak{p}}(\mathfrak{P})$. Todo: [xxx] □

The different and discriminant are related to each other via the ideal norm. In particular, the ideal norm of the different is the discriminant:

Proposition 0.3.3. *Let \mathcal{O}/\mathfrak{o} be a Dedekind extension of a degree n separable extension L/K . Then*

$$\mathfrak{d}_{\mathcal{O}/\mathfrak{o}} = N_{\mathcal{O}/\mathfrak{o}}(\mathfrak{D}_{\mathcal{O}/\mathfrak{o}}).$$

Proof. In view of ??, we may assume \mathcal{O}/\mathfrak{o} is a local Dedekind extension. Therefore \mathfrak{o} is a discrete valuation ring, \mathcal{O} is a principal ideal domain, and \mathcal{O}/\mathfrak{o} admits an integral basis $\alpha_1, \dots, \alpha_n$ making \mathcal{O} a free \mathfrak{o} -module of rank n . Then $\mathfrak{d}_{\mathcal{O}/\mathfrak{o}}$ is a principal integral ideal where

$$\mathfrak{d}_{\mathcal{O}/\mathfrak{o}} = d_{\mathcal{O}}(\mathcal{O})\mathfrak{o}.$$

As \mathcal{O} is a principal ideal domain, every fractional ideal is also principal. So on the one hand, $\mathfrak{d}_{\mathcal{O}/\mathfrak{o}} = \lambda\mathcal{O}$ for some nonzero $\lambda \in L$ and $\lambda\alpha_1, \dots, \lambda\alpha_n$ is a basis of L/K contained in $\mathfrak{d}_{\mathcal{O}/\mathfrak{o}}$. Moreover,

$$d_{L/K}(\lambda\alpha_1, \dots, \lambda\alpha_n) = N_{L/K}(\lambda)^2 d_{L/K}(\alpha_1, \dots, \alpha_n),$$

by ?? and that base change matrix from $\alpha_1, \dots, \alpha_n$ to $\lambda\alpha_1, \dots, \lambda\alpha_n$ is the multiplication by λ map. Todo: [xxx] □