

## 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  $\nu_j$  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  $m \geq 1$ ,  $\chi$  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  $(c, \ell, r)$  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  $(c, \ell, r)$  with the prescribed properties and the second line holds since  $\chi$  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

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

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

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

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

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

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

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

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  $\nu_j$  with Fourier coefficients  $a_j(n)$ . Then for any positive integers  $n, m \geq 1$ , we have*

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

## 0.2 Misc.

In particular, we also have the discriminant

$$D_{\mathcal{O}_K/\mathbb{Z}} = d_{\mathcal{O}_K/\mathbb{Z}}(\alpha_1, \dots, \alpha_n) \mathbb{Z},$$

for any integral basis  $\alpha_1, \dots, \alpha_n$  of  $K$ . Since  $(\mathbb{Z}^*)^2$  is the trivial group,  $d_{\mathcal{O}_K/\mathbb{Z}}(\alpha_1, \dots, \alpha_n)$  is a well-defined nonzero integer by ????. We then define the **discriminant**  $\Delta_K$  of  $K$  by

$$\Delta_K = d_{\mathcal{O}_K/\mathbb{Z}}(\alpha_1, \dots, \alpha_n),$$

which is well-defined. Moreover,  $\Delta_K$  is nonzero by ?? and

$$\Delta_K = \det(M(\alpha_1, \dots, \alpha_n))^2,$$

by ??.

We now discuss the factorization of prime integral ideals in extensions of number fields. First, we need to introduce the concept of prime integral ideals above primes. Let  $K$  be a number field and let  $\mathfrak{p}$  be a prime integral ideal. Then  $\mathfrak{p} \cap \mathbb{Z}$  is a prime integral ideal of  $\mathbb{Q}$ . Indeed, it is clear that  $\mathfrak{p} \cap \mathbb{Z}$  is an integral ideal of  $\mathbb{Q}$ . It is proper because  $1 \notin \mathfrak{p} \cap \mathbb{Z}$  as  $\mathfrak{p}$  does not contain units. It is nonzero because any integral ideal contains its norm (as we have noted) and hence  $N(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$ . To show that  $\mathfrak{p} \cap \mathbb{Z}$  is prime, suppose  $a, b \in \mathbb{Z}$  are such that  $ab \in \mathfrak{p} \cap \mathbb{Z}$ . Then  $ab \in \mathfrak{p}$  and since  $\mathfrak{p}$  is prime either  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . But then  $a \in \mathfrak{p} \cap \mathbb{Z}$  or  $b \in \mathfrak{p} \cap \mathbb{Z}$  as desired. We have now shown that  $\mathfrak{p} \cap \mathbb{Z}$  is a prime integral ideal of  $\mathbb{Q}$ . Hence

$$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z},$$

for some prime integer  $p$ . Accordingly, we say that  $\mathfrak{p}$  is **above**  $p$ , or equivalently,  $p$  is **below**  $\mathfrak{p}$ . Moreover, if  $\mathfrak{p}$  is above  $p$ , then  $\mathfrak{p}$  must be a prime factor of  $p\mathcal{O}_K$ . Indeed,  $p\mathbb{Z} \subseteq \mathfrak{p}$  so that  $p\mathcal{O}_K \subseteq \mathfrak{p}$  and then the fact  $\mathfrak{p}$  is prime implies that some prime factor of  $p\mathcal{O}_K$  is contained in  $\mathfrak{p}$ . Since prime integral ideals are maximal, this prime factor must be  $\mathfrak{p}$  itself. We illustrate these relations by the extension

$$\begin{array}{c} \mathfrak{p} \subset \mathcal{O}_K \subset K \\ | \\ p\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q}. \end{array}$$

Since  $\mathfrak{p}$  and  $p\mathbb{Z}$  are maximal in  $\mathcal{O}_K$  and  $\mathbb{Z}$  respectively, we have the residue fields  $\mathcal{O}_K/\mathfrak{p}$  and  $\mathbb{F}_p$ . It turns out that  $\mathcal{O}_K/\mathfrak{p}$  is a finite dimensional vector space over  $\mathbb{F}_p$ . To see this, consider the homomorphism

$$\phi : \mathbb{Z} \rightarrow \mathcal{O}_K/\mathfrak{p} \quad a \mapsto a \pmod{\mathfrak{p}}.$$

Now  $\ker \phi = \mathfrak{p} \cap \mathbb{Z}$  and hence  $\ker \phi = p\mathbb{Z}$  since  $\mathfrak{p}$  is above  $p$ . By the first isomorphism theorem,  $\phi$  induces an injection  $\phi : \mathbb{F}_p \rightarrow \mathcal{O}_K/\mathfrak{p}$  and since  $\mathcal{O}_K/\mathfrak{p}$  is field (with  $N(\mathfrak{p})$  elements), it must be a finite field containing  $\mathbb{F}_p$ . Necessarily  $\mathcal{O}_K/\mathfrak{p}$  is a finite dimensional vector space over  $\mathbb{F}_p$ . Accordingly, we define the **inertia degree**  $f_p(\mathfrak{p})$  of  $\mathfrak{p}$  by

$$f_p(\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p].$$

That is,  $f_p(\mathfrak{p})$  is the dimension of the residue field  $\mathcal{O}_K/\mathfrak{p}$  as a vector space over  $\mathbb{F}_p$ . Then we have

$$N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_p|^{f_p(\mathfrak{p})} = p^{f_p(\mathfrak{p})}.$$

In particular, the norm of a prime integral ideal is a power of the prime below it. As we have already noted,  $\mathfrak{p}$  is a prime factor of  $p\mathcal{O}_K$ .

Then it suffices to show  $\lambda_1, \dots, \lambda_m$  is a basis for  $L/K$  so that  $m = n$ . We claim  $\lambda_1, \dots, \lambda_m$  are linearly independent over  $K$ . If not, as  $K$  is the field of fractions of  $\mathcal{o}$ , we may multiply by a nonzero element of  $\mathcal{o}$  to ensure they are linearly independent over  $\mathcal{o}$  as well. Then there are  $\alpha_i \in \mathcal{o}$ , for  $1 \leq i \leq m$  and not all zero, such that

$$\alpha_1 \lambda_1 + \dots + \alpha_m \lambda_m = 0.$$

Let  $\mathfrak{a}$  be the integral ideal of  $\mathcal{o}$  generated by the  $\alpha_i$ . By uniqueness of the prime factorization of integral ideals,  $\mathfrak{a}^{-1}\mathfrak{p} \subset \mathfrak{a}^{-1}$  so that there exists a nonzero  $\alpha \in \mathfrak{a}^{-1} - \mathfrak{a}^{-1}\mathfrak{p}$ . Thus  $\alpha\mathfrak{a} \not\subseteq \mathfrak{p}$  and so the elements  $\alpha\alpha_1, \dots, \alpha\alpha_m$  generating  $\alpha\mathfrak{a}$  lie in  $\mathcal{o}$  and at least one of them does not lie in  $\mathfrak{p}$ . Therefore their reductions

$\overline{\alpha\alpha_1}, \dots, \overline{\alpha\alpha_m}$  modulo  $\mathfrak{p}$  are not all zero and so the nontrivial linear dependence above implies a nontrivial linear dependence

$$\overline{\alpha\alpha_1\lambda_1} + \dots + \overline{\alpha\alpha_m\lambda_m} = 0.$$

This contradicts the fact that  $\overline{\lambda_1}, \dots, \overline{\lambda_m}$  is a basis. Therefore  $\lambda_1, \dots, \lambda_m$  are linearly independent over  $K$ . To show that they span  $L/K$ ,

Since  $\mathcal{O}_K$  is a free abelian group of rank  $n$  so is any fractional ideal by ???. Therefore fractional ideals are complete lattices in  $K$  as a vector space over  $\mathbb{Q}$ . In particular,  $\mathcal{O}_K$  is a complete lattice in  $K$ .

### 0.3 Todo: [Lattices]

Let  $K$  be a number field of degree  $n$ . By ???, there is a nondegenerate symmetric bilinear form on  $K$  given by

$$\text{Tr} : K \times K \rightarrow \mathbb{Q} \quad (\kappa, \lambda) \mapsto \text{Tr}(\kappa\lambda).$$

We call this bilinear form the **trace form** on  $K$ . The trace form makes  $K$  into a nondegenerate inner product space over  $\mathbb{Q}$ . Since  $\mathcal{O}_K$  is a free abelian group of rank  $n$  so is any fractional ideal by ???. Therefore fractional ideals are complete lattices in  $K$  as a vector space over  $\mathbb{Q}$ . In particular,  $\mathcal{O}_K$  is a complete lattice in  $K$ . For a fractional ideal  $\mathfrak{f}$ , note that the dual lattice  $\mathfrak{f}^\vee$  is

$$\mathfrak{f}^\vee = \{\kappa \in K : \text{Tr}(\kappa\alpha) \in \mathbb{Z} \text{ for all } \alpha \in \mathfrak{f}\}.$$

We call  $\mathfrak{f}^\vee$  the **dual ideal** of  $\mathfrak{f}$ . The following proposition shows that the dual ideal  $\mathfrak{f}^\vee$  is indeed a fractional ideal:

**Proposition 0.3.1.** *Let  $K$  be a number field and  $\mathfrak{f}$  be a fractional ideal. Then  $\mathfrak{f}^\vee$  is a fractional ideal and*

$$\mathfrak{f}^\vee = \mathfrak{f}^{-1}\mathcal{O}_K^\vee.$$

*Proof.* By ???,  $\mathfrak{f}^\vee$  is a finitely generated  $\mathbb{Z}$ -module. Therefore it is a finitely generated  $\mathcal{O}_K$ -submodule of  $K$  if it is preserved under multiplication by  $\mathcal{O}_K$ . Let  $\alpha \in \mathcal{O}_K$  and  $\beta \in \mathfrak{f}^\vee$ . Then we must show  $\alpha\beta \in \mathfrak{f}^\vee$ . To see this, observe that  $\text{Tr}(\alpha\beta\mathfrak{f}) \subseteq \text{Tr}(\beta\mathfrak{f}) \subseteq \mathbb{Z}$  since  $\alpha\mathfrak{f} \subseteq \mathfrak{f}$  and  $\beta \in \mathfrak{f}^\vee$ . Therefore  $\alpha\beta \in \mathfrak{f}^\vee$  and hence  $\mathfrak{f}^\vee$  is a fractional ideal proving the first statement. To prove the second we will show containment in both directions. For the forward containment, first suppose  $\alpha \in \mathfrak{f}^\vee$  and  $\beta \in \mathfrak{f}$ . Then  $\text{Tr}(\alpha\beta\mathcal{O}_K) \subseteq \text{Tr}(\alpha\mathfrak{f}) \subseteq \mathbb{Z}$  since  $\beta\mathcal{O}_K \subseteq \mathfrak{f}$  and  $\alpha \in \mathfrak{f}^\vee$ . Hence  $\alpha\beta \in \mathcal{O}_K^\vee$  so that  $\mathfrak{f}^\vee\mathfrak{f} \subseteq \mathcal{O}_K^\vee$  and therefore  $\mathfrak{f}^\vee \subseteq \mathfrak{f}^{-1}\mathcal{O}_K^\vee$ . This proves the forward containment. For the reverse containment, suppose  $\alpha \in \mathfrak{f}^{-1}\mathcal{O}_K^\vee$  and  $\beta \in \mathfrak{f}$ . Then  $\text{Tr}(\alpha\beta\mathfrak{f}) \subseteq \text{Tr}(\beta\mathcal{O}_K) \subseteq \mathbb{Z}$  since  $\alpha\mathfrak{f} \subseteq \mathcal{O}_K$  and  $\beta \in \mathfrak{f}$ . This shows  $\alpha\beta \in \mathfrak{f}^\vee$  and hence  $\mathfrak{f}^{-1}\mathcal{O}_K^\vee \subseteq \mathfrak{f}^\vee$  proving the reverse containment and completing the proof.  $\square$

We define the **different**  $\mathfrak{D}$  of  $K$  by

$$\mathfrak{D}_K = (\mathcal{O}_K^\vee)^{-1}.$$

This is an integral ideal. Indeed, first note that  $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$ . It follows from ??? that  $\mathfrak{D}_K$  is an integral ideal and

$$\mathfrak{D}_K = \{\kappa \in K : \kappa\mathcal{O}_K^\vee \subseteq \mathcal{O}_K\}.$$

Also, by Proposition 0.3.1 we can express the dual ideal  $\mathfrak{f}^\vee$  of a fractional ideal  $\mathfrak{f}$  in terms of the different as

$$\mathfrak{f}^\vee = \mathfrak{f}^{-1}\mathfrak{D}_K^{-1}.$$

It turns out that the norm of the different is the absolute value of the discriminant:

---

**Proposition 0.3.2.** *Let  $K$  be an algebraic number field of degree  $n$ . Then we have an isomorphism*

$$\mathcal{O}_K/\mathfrak{D}_K \cong \mathcal{O}_K^\vee/\mathcal{O}_K,$$

as  $\mathcal{O}_K$ -modules. In particular,

$$N(\mathfrak{D}_K) = |\Delta_K|.$$

*Proof.* By ??,  $\mathcal{O}_K \subseteq \mathfrak{D}_K^{-1}$ . Then the second isomorphism theorem implies

$$\mathcal{O}_K/\mathfrak{D}_K \cong \mathfrak{D}_K^{-1}/\mathcal{O}_K \cong \mathcal{O}_K^\vee/\mathcal{O}_K,$$

which proves the first statement. For the second, this isomorphism shows that  $N(\mathfrak{D}_K) = |\mathcal{O}_K^\vee/\mathcal{O}_K|$ . Now let  $\alpha_1, \dots, \alpha_n$  be an integral basis for  $\mathcal{O}_K$ . Then  $\alpha_1^\vee, \dots, \alpha_n^\vee$  is a basis for  $\mathcal{O}_K^\vee$  and by definition of the dual basis we have

$$\alpha_i^\vee = \sum_{1 \leq j \leq n} \text{Tr}(\alpha_i \alpha_j) \alpha_j.$$

But then the base change matrix from  $\alpha_1, \dots, \alpha_n$  to  $\alpha_1^\vee, \dots, \alpha_n^\vee$  is  $(\text{Tr}(\alpha_i \alpha_j))_{i,j}$ . The claim follows by ?? and the definition of  $\Delta_K$ .  $\square$

As a corollary, we can compute the norm of dual ideals:

**Corollary 0.3.1.** *Let  $K$  be a number field and  $\mathfrak{f}$  be a fractional ideal. Then*

$$N(\mathfrak{f}^\vee) = \frac{N(\mathfrak{f}^{-1})}{|\Delta_K|}.$$

*Proof.* This follows immediately from the second statement of Proposition 0.3.2, complete multiplicativity of the norm, and that  $\mathfrak{f}^\vee = \mathfrak{f}^{-1} \mathfrak{D}_K^{-1}$ .  $\square$

We have already remarked that the different is an integral ideal and that  $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$ . Therefore we have an inclusion of complete lattices

$$\mathcal{D}_K \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\vee.$$

What Proposition 0.3.2 shows is that each complete lattice in chain has index  $|\Delta_K|$  in the next one. In particular,  $\mathcal{O}_K^\vee$  is strictly larger than  $\mathcal{O}_K$  if and only if  $|\Delta_K| \geq 2$ . So we can think of the different  $\mathcal{D}_K$  as a measure of the failure of  $\mathcal{O}_K$  to be self-dual since  $N(\mathcal{D}_K) = 1$  if and only if  $\mathcal{O}_K^\vee = \mathcal{O}_K$ .

## 0.4 The Ideal Norm

For a number field  $K$ , we can define a norm for integral ideals of  $\mathcal{O}_K$  which will be immensely useful. Since  $\mathcal{O}_K$  is a free abelian group of rank  $n$  so is any integral ideal  $\mathfrak{a}$  by ?. Therefore  $\mathcal{O}_K/\mathfrak{a}$  is finite by ?. Accordingly, we define the **norm**  $N(\mathfrak{a})$  of  $\mathfrak{a}$  by

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

We also define the norm of the zero ideal to be zero. Moreover, Lagrange's theorem implies that  $N(\mathfrak{a}) \in \mathfrak{a}$  for any integral ideal  $\mathfrak{a}$ . As we might hope, the norms of  $\alpha$  and  $\alpha \mathcal{O}_K$  are essentially the same for any  $\alpha \in \mathcal{O}_K$ :



**Proposition 0.4.1.** *Let  $K$  be a number field. Then for any  $\alpha \in \mathcal{O}_K$ , we have*

$$N(\alpha\mathcal{O}_K) = |N(\alpha)|.$$

*Proof.* Let  $\alpha_1, \dots, \alpha_n$  be an integral basis for  $K$ . Writing

$$\alpha = \sum_{1 \leq i \leq n} a_i \alpha_i,$$

with  $a_i \in \mathbb{Z}$ , we see that  $a_1\alpha_1, \dots, a_n\alpha_n$  is a basis for  $\alpha\mathcal{O}_K$ . In particular, the base change matrix from  $\alpha_1, \dots, \alpha_n$  to this basis is a diagonal matrix with the  $a_i$  on the diagonal. Then on the one hand, we have  $N(\alpha\mathcal{O}_K) = |a_1 \cdots a_n|$  by ???. On the other hand, in terms of the basis  $a_1\alpha_1, \dots, a_n\alpha_n$  the map  $T_\alpha$  is given by

$$T_\alpha = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},$$

and so  $N(\alpha) = a_1 \cdots a_n$ . Hence

$$N(\alpha\mathcal{O}_K) = |N(\alpha)|,$$

as desired. □

The norm of an integral ideal is also completely multiplicative:

**Proposition 0.4.2.** *Let  $K$  be a number field and let  $\mathfrak{a}$  and  $\mathfrak{b}$  be integral ideals. Then*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

*Proof.* First suppose  $\mathfrak{a}$  and  $\mathfrak{b}$  are relatively prime. Then the Chinese remainder theorem implies

$$\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \oplus \mathcal{O}_K/\mathfrak{b},$$

and hence  $|\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{b}|$  so that  $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ . As distinct prime integral ideals are relatively prime (because they are maximal), it suffices to show  $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$  for all prime integral ideals  $\mathfrak{p}$  and  $n \geq 0$ . We will prove this by induction. The base case is clear so assume that the claim holds for  $n - 1$ . By the third isomorphism theorem, we have

$$\mathcal{O}_K/\mathfrak{p}^{n-1} \cong (\mathcal{O}_K/\mathfrak{p}^n)/(\mathfrak{p}^{n-1}/\mathfrak{p}^n).$$

Using ??, it follows that

$$|\mathcal{O}_K/\mathfrak{p}^{n-1}| = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathfrak{p}^{n-1}/\mathfrak{p}^n|} = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathcal{O}_K/\mathfrak{p}|}.$$

Thus  $N(\mathfrak{p}^n) = N(\mathfrak{p}^{n-1})N(\mathfrak{p})$  and our induction hypothesis implies  $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$  as desired. □

At last we can define the norm to fractional ideals. Let  $\mathfrak{f}$  be a fractional ideal. By ??, there exist unique integral ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  such that  $\mathfrak{f} = \mathfrak{a}\mathfrak{b}^{-1}$ . We define the **norm**  $N(\mathfrak{f})$  of  $\mathfrak{f}$  by

$$N(\mathfrak{f}) = \frac{N(\mathfrak{a})}{N(\mathfrak{b})}.$$

From this definition and Proposition 0.4.2 it follows that the norm of a fractional ideal is completely multiplicative. Then upon writing  $\mathfrak{f}\mathfrak{b} = \mathfrak{a}$ , we have  $N(\mathfrak{f})N(\mathfrak{b}) \in \mathfrak{a}$  and hence  $N(\mathfrak{f}) \in \mathfrak{f}$  after multiplying by  $\frac{1}{N(\mathfrak{b})}$  because  $\frac{1}{N(\mathfrak{b})}\mathfrak{a} \subseteq \mathfrak{f}\mathcal{O} \subseteq \mathfrak{f}$ . That is, every fractional ideal contains its norm. We have now established a homomorphism

$$N : I_K \rightarrow \mathbb{Q}^* \quad \mathfrak{f} \mapsto N(\mathfrak{f}),$$

which we call the **ideal norm** of  $K$ .