Lectures on Modular Correspondences

by

M. Eichler

Tata Institute of Fundamental Research, Bombay
1957

Lectures on Modular Correspondences

by

M. Eichler

Notes by

S. S. Rangachari

Tata Institute of Fundamental Research, Bombay
1955–56

Introduction

In the theory of modular forms, certain linear operators T_n have been used by Hecke, Petersson, Maass and others for deter-mining the coefficients of modular forms and of corresponding Dirichlet series. Although this idea has already brought rich success, one has to bear in mind that they are only some special correspondences of certain algebraic varieties.

The correspondences which are represented by Hecke's T_n are the so-called modular correspondences. The latter have also applications in the theory of complex multiplication, but we shall not speak about that here. What is common to all these theories, is the general concept of a correspondence which appears as a connection between certain subgroups of the modular group. This observation at once leads to a vast generalization of modular correspondences by replacing modular groups by other groups, say, by groups of units of an order of a normal simple algebra or of certain quadratic forms. But here, we shall restrict ourselves to a very special case, that of units of orders in a quaternion algebra. Our chief task in this connection will be to determine the traces of the representations of T_n and in some case, we shall give them explicitly.

The first three articles are devoted to the necessary algebraic background and in §4, we study the group of units of a maximal order $\mathcal{J}$ in an indefinite quaternion algebra, by exhibiting it as a group of transformations of the upper half plane onto itself. It is proved that this group is finitely generated by using the finite sided nature of the fundamental domain F. The hyperbolic area of this fundamental domain is then computed by using the residue of the zeta function of $\mathcal{J}$ and from this the genus of F by the application of Gauss Bonnet formal.

The second part starts with the definition of correspondences in general and modular correspondences in particular. We prove here the Euler product formula of the Zeta function of the representation of modular correspondence T_n. We then make a study of the representations of T_n by Betti groups of a certain Riemann surface $S_{\mathcal{J}}$ in §8 and herein we give a proof of Lefschetz' fixed point theorem under certain restrictive assumptions, the application of which is required later. §9 deals with the connections between the ideal theory of quadratic subfields and this leads to applications in §10, especially the calculation of the number of fixed points of T_n, with due multiplicity which essentially reduces to the calculation of the trace of the representation of T_n as an endomorphism of the first Betti groups of $S_{\mathcal{J}}$, by the application of Lefschetz, fixed point theorem. From this trace formula follow a host of relations between class numbers of binary quadratic forms.

We then suggest some problems of interest in an appendix on automorphic forms in which we also give the formula for the trace of representation of T_n in the space of modular forms, by using Riemann matrix. This leads to a proof of Hecke's conjecture on the representation of modular forms by ϑ-series.

Contents

Chapter 1

Arithmetic of Quaternion Algebras

1 Algebraic Background

1. Let k be a field of any characteristic (not necessarily zero). Let Q 1
be an algebra over k, generated by the elements $[1, \omega, \Omega, \omega\Omega]$ with the following multiplication table:

$$\omega^2 = p \in k, \Omega^2 = q \in k, \omega\Omega + \Omega\omega = 0.$$

Q is called a *quaternion algebra over k.* Then, any element $\alpha \in \Omega$ can be expressed uniquely as

$$\alpha = a_o + a_1\omega + a_2\Omega + a_3\omega\Omega$$

where $a_i \in k$. We define the *trace* and *norm* of α as

$$\begin{aligned} \text{trace } (\alpha) = & t(\alpha) = 2a_\circ = \alpha + \bar{\alpha} \in k \\ \text{norm } (\alpha) = & n(\alpha) = a_\circ^2 - pa_1^2 - qa_2^2 + pqa_2^3 \\ & = \alpha\bar{\alpha} = \bar{\alpha}\alpha \in k, \end{aligned}$$

where $\bar{\alpha} = a_o - a_1\omega - a_2\Omega - a_3\omega\Omega$ is called the *conjugate of* α. If $\alpha \in Q$, then $\alpha^2 - (\alpha + \bar{\alpha})\alpha + \bar{\alpha}\alpha = 0$, *i.e.*, $\alpha^2 - t(\alpha).\ \alpha + n(\alpha) = 0$; in other words, each element α of Q satisfies a quadratic equation over k.

Theorem 1. *k is the centre of Q.*

Proof. If C is the center of Q by definition $k \subset C$. Conversely if $\alpha \in C$, then $\alpha\beta = \beta\alpha$ for all $\beta \in Q$. □

$$\text{Let} \quad \alpha = a_o + a_1\omega + a_2\Omega + a_3\omega\Omega \qquad \text{and}$$
$$\beta = b_o + b_1\omega + b_2\Omega + b_3\omega\Omega.$$

2 Then

$$\alpha\beta - \beta\alpha = 0 \Longrightarrow (2q(a_3b_2 - a_2b_3) + \Omega(2p(a_1b_3 - a_3b_1))$$
$$\omega\Omega(2(a_1b_2 - a_2b_1)) = 0,$$

i.e., $a_3b_2 - a_2b_1 = 0, a_1b_3 - a_3b_1 = 0, a_1b_2 = 0,$
i.e., $a_1 : a_2 : a_3 = b_1 : b_2 : b_3.$

The left hand side being fixed and the right hand side being arbitrary, this implies that $a_1 = a_2 = a_3 = 0$,i.e. $\alpha = a_o \in k$, i.e., $C \subset k$.

Using this, we shall show incidentally that our definition of a quaternion algebra is fairly general. More explicitly, any element $\omega'(\in Q, \notin k)$ of trace zero and non-zero norm may be taken as the first element of a basis, $[1, \omega', \Omega', \omega'\Omega']$ which we shall construct as follows:

Now,

$$\omega'^2 = -n(\omega') = p' \in k.$$

Let, further more ω'' be an element linearly independent of $1, \omega'$ and which does not commute with ω'. Such ω'' always exists, or else every element of Q would commute with ω' so that ω' would belong to the centre of Q,i.e., $\omega' \in k$(by Theorem 1) which is contradictory to assumption.

Define $\Omega' = \omega'\omega'' - \omega''\omega'(\neq 0$, by the choice of $\omega'')$.

Then

$$\begin{aligned}\omega'\Omega' &= \omega'(\omega'\omega'' - \omega''\omega')\\ &= \omega''\omega'^2 - \omega'\omega''\omega'\\ &= (\omega''\omega' - \omega'\omega'')\omega' \qquad \text{since } \omega'^2 \in k\\ &= -\Omega'\omega' \qquad i.e. \omega'\Omega' + \Omega'\omega' = 0.\end{aligned}$$

3 Further $t(\Omega') = 0$; otherwise $\Omega'^2 = t(\Omega')$. $\Omega' - n(\Omega')$ implies that ω' commutes with Ω' which is not true.

Therefore $t(\Omega') = 0$, i.e., $\Omega'^2 = -n(\Omega') = q' \in k$.

Summing up, we have obtained a set $[1, \omega', \Omega', \omega'\Omega']$ such that

(i) $\omega'^2 = p' \in k$, (ii) $\Omega'^2 = q' \in k$, (iii) $\omega'\Omega' + \Omega'\omega' = 0$. In other words, $[1, \omega', \Omega', \omega'\Omega']$ is a basis for Q over k.

Theorem 2. *If Q has divisors of zero, then $Q \cong \mathfrak{M}_2(k)$ (total matrix algebra of order* 2 *over k).*

Proof. We will find four elements $\varepsilon_1, \varepsilon_2, \eta_1, \eta_2 \in Q$ satisfying the following condition:

i) $\varepsilon_1^2 = \varepsilon_1, \varepsilon_2^2 = \varepsilon_2, \varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1, \varepsilon_2 = 1 - \varepsilon_1$

ii) $\eta_1\eta_2 = \varepsilon_1, \eta_2\eta_1 = \varepsilon_2; \varepsilon_1\eta_1 = \eta_1 = \eta_1\varepsilon_2, \eta_1^2 = 0.$

$$\varepsilon_2\eta_2 = \eta_2 = \eta_2\varepsilon_1; \eta_2^2 = 0.$$

Then we can define the mapping

$$\sigma : \mathfrak{M}_2(k) \to Q$$

as
$$\sigma(e_i) = \varepsilon_i; \sigma(f_i) = \eta_i; \sigma(e) = 1,$$

where

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \ f_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ f_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

σ is easily seen to be an isomorphism onto. □ 4

If $\alpha(\neq 0) \in Q$ is a zero divisor, αy is a zero divisor for all $y \in Q$, so that $n(\alpha y) = 0$, for all $y \in Q$. Then there exists at least one $y \in Q$ for which $t(\alpha y) \neq 0$, for otherwise, $t(\alpha y) = 0$ for all $y \in Q$ and hence for $y = 1, \omega, \Omega, \omega\Omega$, would imply that $\alpha = 0$.

Let $\alpha y = \alpha'$ then $t(\alpha'') = 1$ where $\alpha'' \dfrac{\alpha'}{t(\alpha')} (t(\alpha') \neq 0)$. Putting $\alpha'' = \varepsilon_1$ and $1 - \varepsilon_1 = \varepsilon_2$, we have the equations (i). Consider $\omega' = \varepsilon_1 - \varepsilon_2 (\in Q)$. Then $\omega'^2 = \varepsilon_1 + \varepsilon_2 = 1$, so that $t(\omega') = 0$ and $n(\omega') \neq 0$.

Hence, as seen before, we have a basis $[1, \omega', \Omega', \omega'\Omega']$ for Q over k. Then $t(\Omega') = 0$ while $n(\Omega') \neq 0$, so that Ω' has an inverse.

Define $\eta_1 = \dfrac{\varepsilon_1\Omega'}{\Omega'^2}$ and $\eta_2 = \varepsilon_2\Omega' = \Omega'.\varepsilon_1$ (since $\Omega'\omega' + \omega'\Omega' = 0$). We can easily verify the set of equations (*ii*), for example,

$$\eta_1\eta_2 = \frac{\varepsilon_1\Omega'}{\Omega'^2}\Omega'\varepsilon_1 = \frac{\varepsilon_1\Omega'^2\varepsilon_1}{\Omega'^2} = \varepsilon_1^2 = \varepsilon_1,$$

and similarly others.

5 **2.** Q is said to split over K or K is said to be a *splitting field* of Q if QK/K is isomorphic to $\mathfrak{M}_2(K)$.(QK denoting the tensor product of Q and K).

Theorem 3. *Let Q be a quaternion algebra over a field k of characteristic zero and let K/k be a quadratic extension of k. Then QK/K splits if and only if $K \cong \overline{K} \subset Q(K \neq \overline{K})$.*

Proof. We may, without loss of generality, assume that Q is s-field (skew field) since otherwise k is itself a splitting field. □

1) Let $K = k(a) \cong k(\alpha) = \overline{K} \subset Q(\alpha = \sigma a \in Q)$ (say)).

   We will now show that QK contains divisors and hence that K splits QK.

   Since $\alpha^2 - t(\alpha).\alpha + n(\alpha) = 0, a^2 - t(\alpha).a + n(\alpha) = 0$. In other words, $X^2 - -t(\alpha).X + n(\alpha) = (X - a)(X - \overline{a})$ where $\overline{a} = \sigma\overline{\alpha}$. Therefore $0 = \alpha^2 - t(\alpha).\alpha + n(\alpha) = (\alpha - a)(\alpha - \overline{a})$, the factorization holding in QK. Both the factors cannot vanish, for otherwise, $\alpha \in K$, i.e., $\overline{K} = K$ which not so. Hence QK contains divisors of zero and by Theorem 2, $QK/K \cong \mathfrak{M}_2(K)$.

2) Let QK/K split, where $K = k(a), a = \sqrt{d}$. We shall prove that there exists $\delta \in Q$ such that $\delta^2 = d$. Then $k(\delta) = \overline{K} \cong k(\sqrt{d}) = K$. By hypothesis, there an $\varepsilon \in QK$ such that ε corresponds to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (in $m_2(K)$). Hence $t(\varepsilon) = 0$ and $n(\varepsilon) = 0$. If $Q = k[1, \omega, \Omega, \omega\Omega]$, then $QK = K[1, \omega, \Omega, \omega\Omega]$, so that $\varepsilon = (a_o + \sqrt{d}b_o) + (a_1 + \sqrt{d}b_1)\omega + (a_2 + \sqrt{d}b_2)\Omega + (a_3 + \sqrt{d}b_3)\omega\Omega$ with $a_i, b_i \in k, i.e., \varepsilon = \alpha + \sqrt{d}\beta; \alpha, \beta \in Q$. 6

$(\alpha, \beta \neq 0)$. Now $t(\varepsilon) = t(\alpha) + \sqrt{d}t(\beta) = 0. t(\alpha), t(\beta) \in k$. Hence $t(\alpha) = 0 = t(\beta)$, since $1, \sqrt{d}$ are linearly independent over k.

Further

$$\begin{aligned} n(\varepsilon) &= \left(\alpha + \sqrt{d}\beta\right)\left(\overline{\alpha} + \sqrt{d}\overline{\beta}\right) \\ &= (n(\alpha) + dn(\beta)) + \sqrt{d}\left(\beta\overline{\alpha} + \alpha\overline{\beta}\right) \\ &= 0. \end{aligned}$$

As before $n(\alpha) + dn(\beta) = 0, \beta\overline{\alpha} + \alpha\overline{\beta} = 0$. $n(\alpha), n(\beta) \neq 0$, since α and β are not zero divisors). Putting $\delta = \alpha\beta^{-1}$, we have

$$\begin{aligned} \delta^2 &= (\alpha\beta^{-1})^2 + \alpha\beta^{-1}.\alpha\beta^{-1} \\ &= \frac{\alpha \cdot \overline{\beta}}{\eta(\beta)} \cdot \frac{\alpha \cdot \overline{\beta}}{\eta(\beta)} \\ &= \frac{-\beta\overline{\alpha}}{\eta(\beta)} \cdot \frac{\alpha\overline{\beta}}{\eta(\beta)} \\ &= \frac{-\eta(\alpha)}{\eta(\beta)} = d. \end{aligned}$$

Hence there exists a $\delta \in Q$ such that $\delta^2 = d$. Theorem 3 is thus completely proved.

3. We now state four theorems which we will need in the sequel. For the same, we shall introduce some notations. k^o denotes the rational number field; k an algebraic number field and $\overline{k}_{\mathscr{Y}}$ its completion with respect to a $\mathscr{Y}$- adic valuation. (We include the case of extensions of archimedian valuations also). If Q/k is a quaternion algebra, $Q_{\mathscr{Y}} = Q.\overline{k}_{\mathscr{Y}}$, the tensor product of Q and $\overline{k}_{\mathscr{Y}}$ and similarly $K_{\mathscr{Y}} = K\overline{k}_{\mathscr{Y}}$ where K is a quadratic extension of k.

Theorem 4. a) $Q/ \cong \mathfrak{M}_2(k) \Longleftrightarrow Q_{\mathscr{Y}} \sqrt{k_{\mathscr{Y}}} \cong \mathfrak{M}_2(\overline{k}_{\mathscr{Y}})$ *for every* $\mathscr{Y}$. 7

b) *For every Q/k, there exist only a finite number of primes $\mathscr{Y}$ such that $Q \ncong m_2(\overline{k}_{\mathscr{Y}})$.*

(These exceptional primes are called "characteristic primes").

c) *If $L_{\mathscr{Y}}$ is any quadratic extension of $\overline{k}_{\mathscr{Y}}$ then $L_{\mathscr{Y}}$ is a splitting field for $Q_{\mathscr{Y}}$.*

d) *K is a splitting field for $Q \Longleftrightarrow K_{\mathscr{Y}}$ a splitting field for $Q_{\mathscr{Y}}$ for all characteristic primes.*

We shall not prove theorems 4a, 4b, and 4c, but we will show how Theorem 4d follows as a simple consequence of Theorem 4a. (For proofs of Theorem 4a, Theorem 4c, refer[Deuring, *"Algebren"* page 117, page 113])

(i) Assume that K is a splitting field for Q.

Then, by theorem 4a, the completion $\overline{K}_{\mathscr{Y}}$ is a splitting field for$Q_{\mathscr{Y}}$ for every $\mathscr{Y}$.

α) If $K_{\mathscr{Y}}$ is a field, then the extension $\mathscr{Y}$ of the valuation $\mathscr{Y}$ from k to K is unique, so that $\overline{K}_{\mathscr{Y}} = K_{\mathscr{Y}}$ and hence $K_{\mathscr{Y}}$ is a splitting field for $Q_{\mathscr{Y}} = Q \cdot \overline{K}_{\mathscr{Y}} = Q \cdot K_{\mathscr{Y}} = Q_{\mathscr{Y}}$.

β) If $K_{\mathscr{Y}}$ is not a field, then $K_{\mathscr{Y}} \overline{K}_{\mathscr{Y}_1} + \overline{K}_{\mathscr{Y}_2}$ where $\overline{K}_{\mathscr{Y}_1}$ and $\overline{K}_{\mathscr{Y}_2}$ are completions of K with respect to the extended valuations $\mathscr{Y}_1$ and $\mathscr{Y}_2$ of $\mathscr{Y}$ from k to K. Then $K_{\mathscr{Y}}$ being of rank 2 over $\overline{k}_{\mathscr{Y}}$, $\overline{K}_{\mathscr{Y}_1}$ and $\overline{K}_{\mathscr{Y}_2}$ are of rank 1 each so that $\overline{K}_{\mathscr{Y}_1} \cong k_{\mathscr{Y}} \cong \overline{K}_{\mathscr{Y}_2}$.

8 Hence $Q_{\mathscr{Y}_1} \cong Q_{\mathscr{Y}} \cong Q_{\mathscr{Y}_2}$. But we know that$\overline{K}_{\mathscr{Y}^1}$ and $\overline{K}_{\mathscr{Y}_2}$ are splitting fields of $Q_{\mathscr{Y}_1}$ and $Q_{\mathscr{Y}_2}$ respectively, i.e., $k_{\mathscr{Y}}$ is a splitting field of $Q_{\mathscr{Y}}$, i.e. $\mathscr{Y}$ is not a characteristic prime.

Hence we have the fact that if $\mathscr{Y}$ is a characteristic prime $K_{\mathscr{Y}}$ is a field and by (α), a splitting field for Q.

(ii) Assume that $K_{\mathscr{Y}}$ is a splitting field for $Q_{\mathscr{Y}}$ for all characteristic primes $\mathscr{Y}$

α) If $\mathscr{Y}$ a characteristic prime, then $K_{\mathscr{Y}}$ is a splitting field for $Q_{\mathscr{Y}}$ and hence a priori, a field. Therefore the extension $\mathscr{Y}$ of $\mathscr{Y}$ from k to K is unique and $\overline{K}_{\mathscr{Y}} = K_{\mathscr{Y}}$ so that $Q_{\mathscr{Y}} = Q_{\mathscr{Y}}$ splits over $\overline{K}_{\mathscr{Y}}$.

β) If $\mathscr{Y}$ is not a characteristic prime, then $\overline{k}_{\mathscr{Y}}$ is a splitting field for $Q_{\mathscr{Y}}$, so that (i) if $K_{\mathscr{Y}}$ is a field, $K_{\mathscr{Y}}$ is also a splitting field for $Q_{\mathscr{Y}}$, i.e., $Q_{\mathscr{Y}}$ splits over $\overline{K}_{\mathscr{Y}}$ and (ii) if $K_{\mathscr{Y}}$ is not a field, $K_{\mathscr{Y}} = \overline{K}_{\mathscr{Y}}+\overline{K}_{\mathscr{Y}_2}$

where $\overline{K}_{\mathscr{Y}_1} \cong K_{\mathscr{Y}} \cong \overline{K}_{\mathscr{Y}_2}$, so that $Q_{\mathscr{Y}_1}$ and $Q_{\mathscr{Y}_2}$ split over$\overline{K}_{\mathscr{Y}_1}$and $\overline{K}_{\mathscr{Y}_2}$ respectively.

Therefore in all cases $Q_{\mathscr{Y}}$ splits over $\overline{K}_{\mathscr{Y}}$ for every $\mathscr{Y}$ and hence by Theorem 4a, K is a splitting field over Q.

We shall now give a sketch of the proof of Theorem 4b. ($k = k^\circ$). Now, $\alpha \in Q(\alpha \neq 0)$ is a zero divisor $\Longleftrightarrow n(\alpha) = 0$. Therefore, for proving that Q splits over k, *i.e.* for proving the existence of zero divisors in Q we merely need to find non-trivial solutions of the equation

$$n(\alpha) = a_o^2 - \rho a_1^2 - q a_2^2 + pq a_3^2 = 0.$$

If $\alpha = a_o + a_1\omega + a_2\Omega + a_3\omega\Omega, a_i \in k.$ 9

i) If ρ is a square, choosing $a_o = 0 = a_1, -a_2^2 + pa_3^2 = 0$ can be solved for $a_2, a_3 \in k$.

ii) If ρ is not a square, let $K = k(\sqrt{\rho}) \overset{\sigma}{\cong} k(\omega)$ (since $\omega^2 = \rho$).

Then $n(\alpha) = 0 \Longrightarrow n(\sigma\zeta) - q = 0$ where $\zeta = \dfrac{a_o + \sqrt{\rho}a_1}{a_2 + \sqrt{\rho}a_3} \in K$.

Hence we have the existence of a solution $\zeta \in K$ such that $n(\sigma\zeta) - q = 0$ implies and is implied by the existence of a zero divisor in Q. (The necessary part follows from the fact that if

$$\zeta = x_\circ + \sqrt{p} \cdot x_1, x_o + \omega x_1 + \Omega \text{ is a zero divisor).}$$

We shall now take up the proof of Theorem 4b. Let r be a prime $\neq 2$ and such that p, q are r-adic units. This is the case for almost all r. If $\zeta = x_1 + \sqrt{p} \cdot x_2, n(\sigma\zeta) - q = 0 \Longrightarrow x_1^2 - px_2^2 = q$. We have to find x_1, x_2 in $\overline{k}_r^o$ satisfying this equation

i) If $p = p_1^2, p_1 \in \overline{k}_r^o, x_1 + p_1x_2 = 1, x_1 - p_1x_2 = q$ can be solved non-trivially for $\begin{vmatrix} 1 & -p_1 \\ 1 & p_1 \end{vmatrix} \neq 0$.

ii) If p is not an r-adic square, q can be written as

$$q = y^2 \text{ or } py^2, y \in \overline{k}_r^o.$$

Then

a) $x_1^2 - px_2^2 = y^2$ in which case $x_1 = y, x_2 = 0$ are solutions.

b) $x_1^2 - px_2^2 = py^2$; i.e., $1 + \xi_2^2 = p\xi_1^2, \xi_1 = \dfrac{x_1}{p_y}, \xi_2 = \dfrac{x_2}{y}$

10 Choosing $\xi_2 \in k^o$ such that $1 + \xi_2^2$ is a quadratic non-residue mod r and is an r-adic unit (such ξ_2 always exists, or else it would mean $n + \xi_2^2$ is a residue for all n) then there exists a $\xi_1 \in \bar{k}_r^\circ$ such that $1 + \xi_2^2 = p\xi_1^2$. Since r runs through almost all primes, Q_r splits over$\bar{k}_r^\circ$ for almost all r.

4. We now give two examples of quaternion algebras over the rational number field k, and calculate their characteristic primes.

1) Let Q/k be the quaternion algebra with basis $(1, \omega, \Omega, \omega\Omega)$ such that $\omega^2 = -1, \Omega^2 = -1, (\omega\Omega)^2 = -1$.

To find the characteristic primes p, we have only to find those primes p for which the equation $n(\xi) = 0, \xi \in Q$ has no non-trivial solutions in $\bar{k}_p$.

a) $p = \infty$(in the usual notation). Then $\bar{k}_\infty$ is the field of real numbers. Therefore, if

$$\xi = x_\circ + x_1\omega + x_2\Omega + x_3\omega\Omega, n(\xi) = x_\circ^2 + x_1^2 + x_2^2 + x_3^2 = 0$$

has obviously no non-trivial solutions in real numbers, so that ∞ is a characteristic prime for Q.

b) $p = 2$. $\bar{k}_p$ is the field of 2-adic numbers. Then each $x_i, 0 \leq i \leq 3$, has an expansion of the form

$$x_i = x_{i\circ}2^{-r} + x_{i1}2^{-r+1} + \cdots\cdots$$

so that, multiplying each x_i by a suitable power of 2, we may assume 11 that the new numbers x_i' are all 2−adic integers of which at least one, (say) x_o' is a 2−adic unit.

Then

$$n(\xi) = 0 \Longrightarrow x_\circ'^2 + x_1'^2 + x_2'^2 + x_3'^2 = 0$$

and $$x'_\circ = x'_{\circ\circ} + 2.x_{\circ 1} + \ldots, x'_{\circ\circ} \neq 0.$$

Let $x''_i = x_{i\circ} + 2x_{i1} + x^2 x_{i2}$. Then $n(\xi) = 0$ implies that

$$x''^2_\circ + x''^2_1 + x''^2_2 + x''^2_3 \equiv 0 \pmod{8},$$

where $(x''_\circ, 2) = 1$ so that $x''^2_\circ \equiv 1 \pmod{8}$ and the other squares $x''^2_1, x''^2_2, x''^2_3$ can be congruent to $0, 1$, or 4 mod 8.

Hence

$$\begin{aligned} x''^2_o + x''^2_1 + x''^2_2 + x''^2_3 &\equiv 1 + \cdots + \cdots + \cdots \pmod{8} \\ &\not\equiv 0 \pmod{8} \end{aligned}$$

under the above conditions, so that $n(\xi) = 0$ cannot be solvable in terms of 2-adic numbers. In other words, $p = 2$ is a charac-teristic prime

For the proof of Theorem 4b, we see that only ∞ and 2 are characteristic primes for Q over k.

ii) Consider the quaternion algebra Q over k (rational number field) with basis $(1, \omega, \Omega, \omega\Omega)$ such that $\omega^2 = 2, \Omega^2 = -3$ and hence $(\omega\Omega)^2 = 6$.

Then, if

$$\begin{aligned} \xi &= x_\circ + x_1\omega + x_2\Omega + x_3\omega\Omega \\ n(\xi) &= x^2_\circ - 2x^2_1 + 3x^2_2 - 6x^2_3. \end{aligned}$$

i) $p = \infty$. $n(\xi)$ being an indefinite form in the $x_i - s, n(\xi) = 0$ has always a non-trivial solution in real numbers, so that $p = \infty$ is not a characteristic prime. 12

ii) $p = 2$. The equation $n(\xi) = 0$ can be rewritten as

$$\begin{aligned} n\left(\frac{x_o + \sqrt{-3}x_2}{x_1 + \sqrt{-3}x_3}\right) = 2 &= n\left(\xi_1 + \sqrt{-3}\xi_2\right) \text{ (say) ,} \\ &= n(\mu) \end{aligned}$$

where $$\mu = \xi_1 + \sqrt{-3}\xi_2 \in k(\sqrt{-3}) = K.$$

Since -3 is not a 2-adic square $(\bar{k}_2(\sqrt{-3}) : \bar{k}_2) = 2$ and $n(\mu) = \mu\bar{\mu} = 2 \implies \mu\bar{\mu} \in (2)$(extended ideal in $(\bar{k}_2(\sqrt{-3}))$. (2) being a prime ideal in $(\bar{k}_2(\sqrt{-3})$, either μ or $\bar{\mu}$ is in (2), say μ. Then $\bar{\mu} \in (\bar{2}) = (2)$, since $2 \in k$.Therefore $\mu\bar{\mu} \in (2)^2$ which is impossible, since $2 \notin (2)^2$, so that $n(\mu) = 2$ is not solvable. In other words, $n(\xi) = 0$ is not solvable with $\xi \in (\bar{k}_2(\sqrt{-3})$ or $p = 2$ is a characteristic prime. Similarly it can be proved that $p = 3$ is a characteristic prime and again from the proof of Theorem 4b, it follows that the only characteristic primes for this Q are $p = 2$ and 3.

5. We shall state and prove

Theorem 5. Wedderburn's Theorem: Let Q be a quaternion algebra over the rational number field k and $\alpha, \beta \in Q$. Then α and β satisfy the same quadratic irreducible equation over k (i.e., $t(\alpha) = t(\beta), n(\alpha) = n(\beta)$), if and only if there exists an element $\rho \in Q$, having an inverse ρ^{-1}, such that $\beta = \rho^{-1}\alpha\rho$.

13 *Proof.* We first prove the converse part.

i) Let $\rho \in Q$ be such that $\beta = \rho^{-1}\alpha\rho$. Now α satisfies the equation

$$\alpha^2 - t(\alpha).\alpha + n(\alpha) = 0, \text{ but } \beta^2 = (\rho^{-1}\alpha\rho).(\rho^{-1}\alpha\rho) = \rho^{-1}\alpha^2\rho,$$

and $\rho^{-1}(\alpha^2 - t(\alpha).\alpha + n(\alpha))\rho = 0$ imply that

$$\beta^2 - t(\alpha).\beta + n(\alpha) = 0,$$

i.e., the irreducible equation satisfied by β is the same as that satisfied by α. In other words,

$$t(\alpha) = t(\beta); n(\alpha) = n(\beta).$$

ii) For the direct part, we distinguish two cases:

$$(a) Q \overset{\sigma}{\cong} \mathfrak{M}_2(k); \quad (b) Q \ncong \mathfrak{M}_2(k).$$

(a) Denoting the image of α by σ as α^σ, let $\alpha^\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ $a, b, c, d, \in k$. Then there exists a matrix ρ_1 with elements in a suitable extension of k, such that

$$\rho_1^{-1}\alpha^\sigma\rho_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \alpha_1. \text{ and } \alpha_2$$

being the two distinct solutions of the equation $x^2 - t(\alpha).x + n(\alpha) = 0$. Further, since β satisfies the same equation, we have a matrix ρ_2 such that $\rho_2^{-1}\beta^\sigma\rho_2 = \left(\begin{smallmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{smallmatrix}\right)$.

$$\text{Hence } \rho_1^{-1}\alpha^\sigma\rho_1 = \rho_2^{-1}\beta^\sigma\rho_2.$$

i.e., $\rho^{-1}\alpha^\sigma\rho = \beta^\sigma$ where $\rho = \rho_1\rho_2^{-1}$. Of course, the elements of ρ lie in some extension of k. 14

(b) If $Q \not\cong \mathfrak{M}_2(k)$, then let K be a quadratic extension such that $QK/K \overset{\sigma_1}{\cong} \mathfrak{M}_2(K)$. (For example, we can take $K \cong k(\omega)$). Then, as above, there exists a matrix ρ with elements in an extension of K, such that $\rho^{-1}\alpha^{\sigma_1}\rho = \beta^{\sigma_1}$.

□

In either case, we have obtained a matrix ρ whose elements lie in a finite extension of k, say L $(L = k(1, \lambda_1, \lambda_2, \ldots,))$, satisfying the condition $\rho^{-1}\alpha^{\sigma'}\rho = \beta^{\sigma'}$ (since $QL/L \overset{\sigma'}{\cong} \mathfrak{M}_2(L)$). Let $\rho'(\in QL) = \sigma'^{-1}(\rho)$. Then

$$\rho' = \rho_\circ + \lambda_1\rho_1 + \lambda_2\rho_2 + \cdots, \rho_\circ, \rho_1, \ldots \in Q.$$

Substituting in $\alpha\rho' = \rho'\beta$ we obtain

$$\alpha\rho_\circ + \lambda_1\alpha\rho_1 + \cdots = \rho_\circ\beta + \lambda_1\rho_1\beta + \cdots.$$

Since $\alpha\rho_i \in Q$, expanding each of these in terms of the basis elements $(1, \omega, \Omega, \omega\Omega)$ and using the fact that $1, \lambda_1, \lambda_2, \ldots$ equations $\alpha\rho_0 = \rho_0\beta, \alpha\rho_1 = \rho_1\beta, \ldots.$.

In case (b) for at least one $i, \rho_i \neq 0$, so that ρ_i^{-1} exists and hence $\beta = \rho_i^{-1}\alpha\rho_i; \rho_i \in Q$.

In case (a) we use the fact that $n(\rho') \neq 0$ (since ρ^{-1} exists). Now, $n(\rho') = n(\rho_0) + \lambda_1(\rho_1\bar{\rho_0} + \rho_0\bar{\rho_1}) + \cdots + \lambda_1^2 n(\rho_1) + \cdots + \lambda_2^2 n(\rho_2) + \cdots = 0$.

In this quadratic expression in $\lambda_1, \lambda_2 \ldots$ we replace $\lambda_1, \lambda_2 \cdots$ by 15 indeterminates $x_1, x_2 \ldots$ obtaining a quadratic polynomial $f(x_1, x_2, \ldots)$ with coefficients in k. f does not vanish identically since $f(\lambda_1, \lambda_2, \ldots) = n(\rho') \neq 0$. Now, k being an infinite field, we can always find a set of elements $\bar{\lambda_1}, \bar{\lambda_2}, \ldots \in k$ such that $f(\bar{\lambda_1}, \bar{\lambda_2}, \ldots) \neq 0$.

Let $\zeta = \rho_0 + \bar{\lambda_1}\rho_1 + \cdots$; $\zeta \in Q$ and $n(\zeta) = f(\bar{\lambda_1}, \ldots) \neq 0$ so that ζ^{-1} exists.

$$\begin{aligned}\alpha\zeta &= \alpha\rho_0 + \bar{\lambda_1}\alpha\rho_1 + \cdots \\ &= \rho_0\beta + \bar{\lambda_1}\rho_1\beta + \cdots = \zeta\beta, i.e., \zeta^{-1}\alpha\zeta = \beta\end{aligned}$$

Thus, the proof of our theorem is complete.

2 Orders and Ideals

5. Let k denote the rational number field; $\mathscr{O}$, the ring of rational integers; $\overline{k_p}$, the p-adic completion of k and $\mathscr{O}_P$, the ring of p-adic integers.

Theorem 1. Let Q/k be a quaternion algebra. Then, four elements $\mu_1, \mu_2, \mu_3, \mu_4 \in Q$ are linearly independent over k if and only if the discriminant

$$|t(\mu_i\mu_k)| = D(\mu_1, \mu_2, \mu_3, \mu_4) \neq 0.$$

Proof. Let $Q = k[1, \omega, \Omega, \omega\Omega] = k[\nu_1, \nu_2, \nu_3, \nu_4]$ (say). Then

$$D(\nu_1, \nu_2, \nu_3, \nu_4) = \begin{vmatrix} 2 & 0 & 0 & 0 \\ 0 & 2p & 0 & 0 \\ 0 & 0 & 2q & 0 \\ 0 & 0 & 0 & -2pq \end{vmatrix}^{=-16p^2q^2\neq 0.}$$

16 Now, we have $\mu_i = \sum\limits_{\ell=1}^{4} m_{il}\nu_l; m_{il} \in k, i = 1$ to 4 so that

$$\mu_i\mu_k = \Big(\sum_l m_{il}\nu_l\Big)\Big(\sum_j m_{kj}\nu_j\Big) = \sum_{j,l} m_{il}\nu_l l_j m_{kj}$$

i.e., $$t(\mu_i\mu_k) = \sum_{j,l} m_{il} t(\gamma_l\gamma_j) m_{kj}.$$

Denoting by $(m_{kj})^T$, the transpose of (m_{kj}) we have

$$(t(\mu_i\mu_k) = (m_{il})(t(\nu_l\nu_j))(m_{kj})^T.$$

Hence

$$|t(\mu_i\mu_k)| = |t(\nu_l\nu_j)||m_{ik}|^2,$$

i.e., $$D(\mu_1, \ldots, \mu_4) = -16p^2q^2|m_{ik}|^2.$$

But $\nu_1 \cdots \nu_4$ being linearly independent over $k, |m_{ik}| \neq 0$ implies that $\mu_1 \cdots \mu_4$ are also linearly independent over k and conversely $\mu_1 \cdots \mu_4$ linearly independent implies that $|m_{ik}| \neq 0$, i.e., $D(\mu_1 \cdots \mu_4) \neq 0$. □

6. Let Q be a quaternion algebra over the rational number field k. We now define an order in Q.

Definition. *An* order $\mathcal{J}$ *in Q is a ring of elements of Q with the following properties:*

i) $1 \in \mathcal{J}$,

ii) $\alpha \in \mathcal{J} \Rightarrow t(\alpha)$ *and* $n(\alpha)$ *are integers,*

iii) $\mathcal{J}$ *has* 4 *linearly independent generators over k.*

We can also define an order alternatively as follows:

2) $\mathcal{J}$ *is an* order *if it is a ring of elements of Q such that i)* $1 \in \mathcal{J}$*, ii)* $\mathcal{J}$ *is a finite* $\mathcal{O}$*-module, iii)* $\mathcal{J}$ *has 4 linearly independent generators over k.* 17

For the equivalence of these two definitions, we shall prove in Theorem 2 that $\mathcal{J}$ *an order as in* (1) *is a finite* $\mathcal{O}$*-module. But for the converse, namely if* $\mathcal{J}$ *is a finite* $\mathcal{O}$*-module, then* $\alpha \in \mathcal{J} \Rightarrow n(\alpha)$ *and* $t(\alpha)$ *integral follows from the fact* $\alpha \in \mathcal{J} \Rightarrow \alpha\mathcal{J} \subset \mathcal{J}$ *(for* $\mathcal{J}$ *is a ring), i.e.,* α *is an "integer", i.e.,* α *satisfies a monic polynomial with integral coefficients.*

We shall give some examples of orders in Q. Let Q have the basis $[1, \omega, \Omega, \omega\Omega]$ over k where ω^2 and Ω^2 are integers. Then the finite $\mathscr{O}$-module $[1, \omega, \Omega, \omega\Omega]$ can easily be seen to be an order. If ω^2 and Ω^2 were not integers, (say) $\omega^2 = \dfrac{p'}{q'}, \Omega^2 = \dfrac{p''}{q''}$, then the $\mathscr{O}$-module $[1, q'\omega, q''\Omega, q'q''\omega\Omega]$ is an order in Q.

The definition of an order in a quaternion algebra Q_p over the p-adic number field $\overline{k_P}$ is given exactly as above, except that the ring of integers $\mathscr{O}$ is now replaced by the ring $\mathscr{O}_p$ of p-adic integers.

Theorem 2. An order $\mathscr{J}$ is a finite $\mathscr{O}$-module and has 4 linearly independent generators over $\mathscr{O}$.

Proof. Let $[\mu_1, \ldots, \mu_4]$ be a basis of $\mathscr{J}$ over k.

Then $\mu_i\mu_k = \sum\limits_{j=1}^{4} m_{ik}^j \mu_j, m_{ik}^j \in k$. Let N be the common denominator of all these m_{ik}^j and put $N\mu_i = \mu_i'$. Now $\mu_i'\mu_K' = \sum\limits_{j=1}^{4} Nm_{ik}^j\mu_j'$. Then 18 the $\mathscr{O}$-module $\mathscr{J}' = [1, \mu_1' \ldots, \mu_4']$ is actually an order; for by choice $\mu_i'\mu_k' \in \mathscr{J}'$ and hence $\mathscr{J}'$ is a ring $\ni 1$ and $\mathscr{J}' \subset \mathscr{J}$, so that every element has integral trace and norm. Further $\mathscr{J}'$ is of rank 4 over k. □

If $\mathscr{J}' \neq \mathscr{J}$, there exists an element $\alpha \in \mathscr{J}$ such that $\alpha \notin \mathscr{J}'$. Consider the $\mathscr{O}$-module $\mathscr{J}'' = [\mu_1', \ldots, \mu_4', \alpha, \alpha\mu_1', \ldots \alpha\mu_4', \mu_1'\alpha \cdots \mu_4'\alpha]$. Then $\mathscr{J}''$ is an order. For, $i)1 \in \mathscr{J}'', ii)\mathscr{J}'' \subset \mathscr{J}$ so that every element of $\mathscr{J}''$ has integral trace and norm, $iii)\mathscr{J}''$ is of rank 4. Therefore it is enough to prove that $\mathscr{J}''$ is a ring.

$$\begin{aligned} \alpha\mu_i'.\alpha\mu_k' &= (t(\alpha\mu_i') - \overline{(\alpha\mu_i')}).\alpha\mu_k' \\ &= t(\alpha\mu_i').\alpha\mu_k' - \bar{\mu}_i'\bar{\alpha}\alpha.\mu_k' \in \mathscr{J}'' \end{aligned}$$

since $\underline{t}(\alpha\mu_i) \in \mathscr{O} \subset \mathscr{J}'', n(\alpha)$ is integral and $\bar{\mu}_i' = t(\mu_i') - \mu_i' \in \mathscr{J}'$ so that $n(\alpha).\mu_i'\mu_k' \in \mathscr{J}' \subset \mathscr{J}''.\mathscr{O}$ being a principal ideal domain, we know that the finite $\mathscr{O}$-module $\mathscr{J}''$ has always a linearly independent $\mathscr{O}$-module basis (say) $[\nu_1 \cdots \nu_4]$ similarly $\mathscr{J}' = [\mu_1'' \cdots \mu_4'']$.

Now, $[\nu_1 \cdots \nu_4] \supset [\mu_1'' \cdots \mu_i''] \Rightarrow \mu_i'' = \sum\limits_{k=1}^{4} m_{ik}\nu_k, m_{ik} \in \mathscr{O}$ i.e.,

$D[\mu_1'' \cdots \mu_4''] = D[\nu_1 \cdots \nu_4] \cdot |m_{ik}|^2$. In other words, we have $D(\mathscr{J}') = (\mathscr{J}'').|m_{ik}|^2.D(\mathscr{J}')$ and $D(\mathscr{J}'')$ being integers, $D(\mathscr{J}'')|D(\mathscr{J}')$.

Continuing the above construction further we obtain a system of finite $\mathscr{O}$-modules $\mathscr{J}', \mathscr{J}'', \mathscr{J}''', \ldots$ which are also orders, such that $\mathscr{J} \supset \cdots \supset \mathscr{J}''' \supset \mathscr{J}'' \supset \mathscr{J}' \supset \cdots$ and $D(\mathscr{J})| \cdots D(\mathscr{J}''')|D(\mathscr{J}'')|D(\mathscr{J}')$. This sequence must end after a finite stage, so that $\mathscr{J}^{(n)} = \mathscr{J}$ for some n. In other words, we have proved that $\mathscr{J}$ itself is a finite $\mathscr{O}$-module and consequently has 4 linearly independent $\mathscr{O}_p$-module basis elements.

An order $\mathscr{J}$ is defined to be *maximal* if it is not properly contained in any other order. The above divisibility property of the discriminants incidentally shows that every order is contained in some maximal order. 19

Since the above arguments can be carried over to p-adic integers also, any order $\mathscr{J}_p$ in $Q_p/\overline{k_p}$ is a finite $\mathscr{O}$-module and any order is contained in a maximal order.

Let now $\mathscr{J} = [\mu_1 \cdots \mu_4]$ (an integral basis) be an order in Q/k. Then if $\xi \in \mathscr{J}, \xi \underline{=} m_1\mu_1 + \cdots + m_4\mu_4, \mu_i \in \mathscr{O}$. We associate to $\mathscr{J}$, an order $\mathscr{J}_p$ in $Q_p/\overline{k_p}$ such that if $\xi \in \mathscr{J}_p, \xi = m_1'\mu_1' + \cdots + m_4'\mu_4, m_i' \in \mathscr{O}_p$, i.e., $\mathscr{J}_p = [\mu_1 \cdots \mu_4]$ (an $\mathscr{O}_p$-module). We now establish a connection between $\mathscr{J}$ and $\mathscr{J}_p - s$.

$\mathscr{J} = Q \cap \mathscr{J}_2 \cap \mathscr{J}_3 \cap \mathscr{J}_5 \cap \cdots \cap \mathscr{J}_p \cap \cdots$ where p runs through all primes and $\mathscr{J}_p$ is the p-adic extension of $\mathscr{J}$. For, if $\xi \in \mathscr{J}, \xi = \sum\limits_{i=1}^{4} m_i\mu_i, m_i \in \mathscr{O}$. Therefore $m_i \in k$, and $\mu_i \in \mathscr{O}_p$ for all p, i.e., $\xi \in Q \bigcap\limits_{p} \mathscr{J}_p$.

Conversely if $\xi \in Q \bigcap_p \mathscr{J}_p, \xi = \sum\limits_{i=1}^{4} m_i'\mu_i, m_i'$ are rational p-adic integers for all p and hence are rational integers, i.e., $\xi \in \mathscr{J}$. Therefore $\mathscr{J} = Q \cap \mathscr{J}_2 \cap \mathscr{J}_3 \cap \cdots \cap \mathscr{J}_p \cap \cdots$

Theorem 3. $\mathscr{J}$ is a maximal order in $Q/k \Leftrightarrow \mathscr{J}_p$ is maximal order in $Q_p/\overline{k_p}$ for every p.

For the same, we shall prove

$\mathscr{J}$ is not maximal $\Leftrightarrow \mathscr{J}_P$ is not maximal, for some p.

Proof. i) If $\mathscr{J}$ is not maximal, $\mathscr{J} \subset \mathscr{J}'$ where $\mathscr{J}'$ is maximal, then there exists $\xi \in \mathscr{J}'$, which is $\notin \mathscr{J}$. If $\mathscr{J} = [\mu_1 \cdots \mu_4]$, then Q is generated by $(\mu_1, \ldots, \mu_4)$ over k, so that $\xi = x_1\mu_1 + \cdots + x_4\mu_4$ where at least one 20

x_i (say) x_1, is not integral. Let p be a prime dividing the denominator of x_1. Since $\xi \in \mathcal{J}' \subset \mathcal{J}'_p$, the $\mathcal{O}_p$-module $\mathcal{J}''_p = [\mathcal{J}_p, \xi\mathcal{J}_p, \mathcal{J}_p\xi]$ is an order containing $\mathcal{J}_p$ properly, so that $\mathcal{J}_p$ is not maximal.

ii) Conversely, if $\mathcal{J}_P$ is not maximal for some p then there exists $\xi \in$ some maximal order, which is $\notin \mathcal{J}_p$. If $\mathcal{J}_p = [\mu_1 \cdots \mu_4]$ then Q_p is generated by $[\mu_1 \cdots \mu_4]$ over $\overline{k}_p$ so that : $\xi = x_1\mu_1 + \cdots + x_4\mu_4$ where not all x_i are p-adic integers. □

Let $x_i = x'_i + u'_i$ (u'_i-integral) ($i = 1$ to 4), where some x'_i may vanish; x'_i are rational numbers.

Defining $\xi' = x'_1\mu_1 + \cdots + x'_4\mu_4, \xi = \xi' + \xi''$ where $\xi'' \in \mathcal{J}_p$. Further $\xi' = \xi - \xi'' \in$ maximal order containing $\mathcal{J}_p$. We shall prove that the $\mathcal{O}$-module $\mathfrak{M}' = [\mathcal{J}, \xi'\mathcal{J}, \mathcal{J}\xi'] = [\mu'_1 \cdots \mu'_4]$ (say) is actually an order containing $\mathcal{J}$ properly.

$\mu'_i\mu'_k = \sum\limits_{j=1}^{4} r^j_{ik}\mu'_j$ where r^j_{ik} are p-adic integers, since the $\mathcal{O}_p$-module $[\mu'_1 \cdots \mu'_4] = [\mathcal{J}_p, \xi'\mathcal{J}_p, \mathcal{J}_p\xi']$ is an order. Further they are rational numbers since Q is generated by $(\mu'_1 \cdots \mu'_4)$ over k. Therefore r^j_{ik} are rational p-adic integers. But, their denominators if any, can contain only powers of p by virtue of ξ' so that r^j_{ik} are all rational integers, i.e., $\mu'_i\mu'_k \in \mathfrak{M}'$. 21 In other words, $\mathfrak{M}'$ is a ring. Hence $\mathfrak{M}'$ is a finite $\mathcal{O}$-module of rank 4 over k and also a ring containing 1, so that by our second definition of an order, $\mathfrak{M}'$ is an order. Since $\xi \in \mathfrak{M}'$ and $\notin \mathcal{J}, \mathfrak{M}'$ contains $\mathcal{J}$ properly, i.e., $\mathcal{J}$ is not maximal.

7. We shall now study the maximal orders of Q_p in both the cases $i)Q_p$ is a division algebra over $\overline{k}_p$ and $ii)Q_p/\overline{k}_p \cong \mathfrak{M}_2(\overline{k}_p)$. In case i) we have a uniqueness theorem of orders, namely,

Theorem 4. If $Q_p/\overline{k}_P$ is a division algebra, then there is in Q_p, only one maximal order $\mathcal{J}_p$ and in fact $\mathcal{J}_p = \{\nu \in Q_p : n(\nu) \in \mathcal{O}_p\}$.

We shall prove the following two lemmas from which we deduce the theorem.

Lemma 1. *$\nu \in Q_p$ and $n(\nu) \in \mathcal{O}_p \Rightarrow t(\nu) \in \mathcal{O}_p$*

Lemma 2. *$\mathcal{J}_p = \{\nu : n(\nu) \in \mathcal{O}_p\}$ is a ring.*

1) a) If $v \in \overline{k}_p, t(v) = 2v$ and $n(v) = v^2.n(v) \in \mathscr{O}_p \Rightarrow v^2 \in \mathscr{O}_p$, which means that $v \in \mathscr{O}_p$, i.e., $t(v) = 2v \in \mathscr{O}_p$.

b) If $v \notin \overline{k}_p, v$ satisfies the irreducible equation $x^2 - t(v).x + n(v) = 0$. Given that $n(v) \in \mathscr{O}_p$, if $t(v) \notin \mathscr{O}_p$, let $t(v) = \dfrac{\mu}{p^r}, \mu$, a p-adic unit and $r > 1$. Then $v' = p^r.v$ satisfies $x'^2 - \mu.x' + n(v)p^{2r} \equiv (x' - \mu)x' \pmod p$, (replacing x *by* $\dfrac{x'}{p^r}$). μ being a p-adic unit, x' and $x' - \mu$ are coprime mod p and hence by Hensel's lemma, the above equation $x'^2 - \mu.x' + n(v).p^{2r}$ is reducible in $\overline{k}_p$, which is a contradiction to the fact that it is irreducible. Therefore $t(v) \in \mathscr{O}_p$.

2) Let $v_1, v_2 \in Q_p$ such that $n(v_1)$ and $n(v_2)$ are in $\mathscr{O}_p$. Then $n(v_1)|n(v_2)$ or $n(v_2)|n(v_1)$. We may assume that $n(v_1)|n(v_2)$, i.e., $n(v_1^{-1}v_2) \in \mathscr{O}_p$. Then by Lemma (1), $t(v_1^{-1}v_2)$ is also an integer. 22

$$n(v_1 + v_2) = n(v_1(1 + v_1^{-1}v_2)) = n(v_1).(1 + v_1^{-1}v_2).(1 + \overline{v_1^{-1}v_2}).$$

Hence $n(v_1 + v_2) = n(v_1)(1 + t(v_1^{-1}v_2) + n(v_1^{-1}v_2)) \in \mathscr{O}_p$, (since $n(v_1), t(v_1^{-1}v_2), n(v_1^{-1}v_2) \in \mathscr{O}_p$).
or $v_1, v_2 \in \mathscr{J}_p \Rightarrow v_1 + v_2 \in \mathscr{J}_p$. $v_1v_2 \in \mathscr{J}_p$ follows at once, i.e., $\mathscr{J}_p$ is a ring.

Now, $\mathscr{J}_p$ cannot be of rank > 4 since it contains certain rational multiples of every element of Q_p. It cannot be of rank < 4 also, since it contains all orders. Hence $\mathscr{J}_p$ is of rank 4. Therefore, by our first definition of an order, $\mathscr{J}_p$ is an order and it is obviously the only maximal order in Q_p.

Let $Q/k \overset{\sigma}{\cong} \mathfrak{M}_2(k)$. We shall give an example of a maximal order $\mathscr{J}$ and then prove that all maximal orders can be written in the form $\mu^{-1}\mathscr{J}\mu$, $\mu \in Q$ such that $n(\mu) \neq 0$. Define $\mathscr{J} = [\mu_1, \ldots, \mu_4]$ the finite $\mathscr{O}$-module where

$$\mu_1^\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \mu_2^\sigma = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \mu_3^\sigma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \mu_4^\sigma = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Then

$$D(\mathcal{J}) = D[\mu_1 \cdots \mu_4] = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = -1.$$

23 By our second definition of an order, $\mathcal{J}$ is an order, since $\mathcal{J}$ is a ring containing 1 and a finite $\mathscr{O}$-module of rank 4. But $D(\mathcal{J})$ being an unit, $\mathcal{J}$ is a maximal order.

Let $\mu \in Q$ such that $n(\mu) \neq 0$. Consider $\mathcal{J}' = \mu^{-1}\mathcal{J}\mu = [\mu^{-1}\mu_1, \mu, \ldots, \mu^{-1}\mu_4\mu]$. By means of the isomorphism one sees that $\mathcal{J}'$ is again a ring containing 1, a finite $\mathscr{O}$-module of rank 4 and hence an order. Further $\mathcal{J}'$ is maximal since $\mathcal{J}$ is maximal.

[Analogously, if $Q_P/\overline{k_p} \overset{\sigma}{\cong} \mathfrak{M}_2(\overline{k_p})$, we have the order $\mathcal{J}_p$ corresponding to $\mathcal{J}$, which is again maximal, since -1 is a p-adic unit. Further if $\mu \in Q_p$ such that $n(\mu) \neq 0, \mu^{-1}\mathcal{J}_p\mu$ is an order and also maximal.]

Theorem 5. Let $Q/k \overset{\sigma}{\cong} \mathfrak{M}_2(k)$ and let $\mathcal{J}$ be the maximal order defined as before and $\mathcal{J}'$, any other maximal order. Then there exists a $\mu \in Q$ such that $n(\mu) \neq 0$ and $\mathcal{J}' = \mu^{-1}\mathcal{J}\mu$.

Proof. Define $\mathfrak{M}$ to be the $\mathscr{O}$-module $[l_j l'_k, j = 1 \text{ to } 4, k = 1 \; to \; 4]$ if $\mathcal{J} = [l_j]$ and $\mathcal{J}' = [l'_k]$. Then we shall prove

i) $\mathfrak{M} = \mathcal{J}\mu$ for a suitable $\mu \in \mathfrak{M}$.

ii) If $\mathfrak{K} = \{\xi : \mathfrak{M}\xi \subset \mathfrak{M}\}$ then $\mathfrak{K} = \mathcal{J}' = \mu^{-1}\mathcal{J}\mu$.

i) We shall first prove that there exists a $\mu \in \mathfrak{M}$ such that $n(\mu) \neq 0$ and with the additional property that $n(\mu) | n(\nu)$ for all $\nu \in \mathfrak{M}$. □

Let μ_1, μ_2 be any two elements of $\mathfrak{M}$. Let N be chosen sufficiently large so that

$$\mu'_1 = N\mu_1 \sim \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \text{ and } \mu'_2 = N\mu_2 \sim \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix}$$

24 where $m's$ and $n's$ are all integers. By applying suitable elementary

transformation on the left side, μ'_1 goes into

$$ {}^{\varepsilon_1}\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} m'_{11} & m'_{12} \\ 0 & m'_{22} \end{pmatrix} $$

and μ'_2 goes into

$$ {}^{\varepsilon_2}\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} = \begin{pmatrix} n'_{11} & n'_{12} \\ 0 & n'_{22} \end{pmatrix} $$

But $n(\mu'_1).n(\varepsilon_1) = m'_{11}m'_{22} \Rightarrow n(\mu'_1) = m'_{11}m'_{22}$ since ε_1 is unimodular. Similarly $n(\mu'_2) = n'_{11}n'_{22}$.

Let $\gamma_{11} = (m'_{11}, n'_{11})$ and $\gamma_{22} = (m'_{22}, n'_{22})$. Then we can find integers a_1, b_2, a_2, b_2 such that

$$ a_1 m'_{11} + b_1 n'_{11} = \gamma_{11}, \quad a_2 m'_{22} + b_2 n'_{22} = \gamma_{22}. $$

Now, define

$$ \mu' = \alpha_1 \mu'_1 + \alpha_2 \mu'_2 $$

where $$ \alpha_1^\sigma = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \varepsilon_1, \alpha_2^\sigma = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} \varepsilon_2; (\alpha_1, \alpha_2 \in \mathcal{J}) $$

so that $\mu'^\sigma = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} m'_{11} & 0 \\ 0 & m'_{22} \end{pmatrix} + \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} \begin{pmatrix} n'_{11} & n'_{12} \\ 0 & n'_{22} \end{pmatrix} = \begin{pmatrix} \gamma_{11} & * \\ 0 & \gamma_{22} \end{pmatrix}$

Hence $n(\mu') = \gamma_{11}.\gamma_{22}$ which divides $n(\mu'_1)$ and $n(\mu'_2)$. Since $\mu' = \alpha_1 N\mu_1 + \alpha_2 N\mu_2 \in \mathcal{J}.N\mathfrak{M} \subset N\mathfrak{M}, \mu = \dfrac{\mu'}{N} \in \mathfrak{M}$. From the above, it implies that $n(\mu)$ divides $n(\mu_1)$ and $n(\mu_2)$. In other words $n(\mu^{-1}\mu_1)$ and $n(\mu^{-1}\mu_2)$ are integers.

25 If μ_3 is a third element of $\mathfrak{M}$, for μ_3 and μ we can construct a $\nu \in \mathfrak{M}$ such that $n(.\nu^{-1}\mu)$ and $n(\nu^{-1}\mu_3)$ are integers. By virtue of $\mu, n(\nu^{-1}\mu_1)$ and $n(\nu^{-1}\mu_2)$ are also integers. Similarly, given n elements $\mu_i \in \mathfrak{M}(i = 1 \text{ to } n)$, we can find an element $\mu \in \mathfrak{M}$ such that $n(\mu^{-1}\mu_i)$ are all integers.

Let $\mathfrak{M} = [\nu_1 \cdots \nu_4]$. If $\xi = \sum\limits_{i=1}^{4} x_i \nu_i, x_i \in \mathscr{O}$ then we have

$$ n(\xi) = \sum_{i=1}^{4} n(\nu_i) x_i^2 + \sum_{i,j=1}^{4} t(\nu_i \bar{\nu_j}) x_i x_j = \frac{\nu}{s} $$

(say) where s is the common denominator of $n(\nu_i), t(\nu_i\overline{\nu_j})$ and is fixed for all $\xi \in \mathfrak{M}$. Hence we have a g.c.d of all $n(\xi), (\xi \in \mathfrak{M})$ (say) m. Then, if $d =$ g.c.d of $n(\nu_i), t(\nu_i\overline{\nu_j})$, we assert that $d = m$. For m is evidently a multiple of d. Conversely $n(\mu_i), n(\mu_i + \mu_j)\,(= n(\mu_i) + n(\mu_j) + t(\mu_i\overline{\mu_j}))$ are multiples of m implies that $t(\mu_i\overline{\mu_j})$ are multiples of m, i.e., d is a multiple of m so that $d = m$. Now, choose an element $\mu \in \mathfrak{M}$ such that $n(\mu)|n(\mu_1)$ and $n(\mu)|n(\mu_i + \mu_j)\,(i, j = 1 \; to \; 4, i =\neq j)$. Then $n(\mu)|d(= m)$. But $m|n(\mu)$, by definition of m. Hence $n(\mu) = m$. i.e., $n(\mu)|n(\mu')$ for all $\mu' \in \mathfrak{M}$.

Having obtained $\mu \in \mathfrak{M}$ with the property that $n(\mu)|n(\mu')$ for all $\mu' \in \mathfrak{M}$, we assert that there exists a basis $[\mu, \mu_1, \mu_2, \mu_3]$ for $\mathfrak{M}$. For, if $[\nu_1 \cdots \nu_4]$ were some integral base for $\mathfrak{M}$,

$$\mu = \sum_{i=1}^{4} a_i\nu_i = t\sum_{i=1}^{4} a'_i\nu_i$$

(if all a_i are not coprime, t, an integer > 1.)

26 Now, $(a'_1, \ldots, a'_4)$ being a coprime row, it can be completed to a unimodular matrix $\mathcal{U}$ (say) which, on applying to the basis $[\nu_1 \cdots \nu_4]$ gives an integral basis $\left[\frac{\mu}{t}, \mu_1, \mu_2, \mu_3\right]$ for $\mathfrak{M}$. But $n(\mu)|n\left(\frac{\mu}{t}\right) \Rightarrow n(\mu).\lambda = \frac{n(\mu)}{t^2}, \lambda$ being an integer;

i.e., $$t^2.\lambda = 1, \; i.e., t = \pm 1.$$

Therefore we have an integral basis $[\mu, \mu_1, \mu_2, \mu_3]$.

Consider the module $$\begin{aligned} W = \mathfrak{M}\mu^{-1} &= \left[1, \mu, \mu^{-1}, \mu_2\mu^{-1}, \mu_3\mu^{-1}\right] \\ &= [1, \rho_1, \rho_2, \rho_3] \; (say) \end{aligned}$$

Then we prove that $W = \mathcal{J}$.

$\mathcal{J}\mathfrak{M} \subseteq \mathfrak{M} \Rightarrow \mathcal{J}\mathcal{W} \subseteq \mathcal{W} \Rightarrow \mathcal{J} \subseteq \mathcal{W}$. It is enough to show $\mathcal{W} \subseteq \mathcal{J}$. Let $\rho \in \mathcal{W}, \rho = \gamma_0 + \gamma_1\rho_1 + \gamma_2\rho_2 + \gamma_3\rho_3; \gamma_i \in \mathcal{O}$.

Then

$$n(\rho) = (\gamma_0 + \gamma_1\rho_1 + \gamma_2\rho_2 + \gamma_3\rho_3)(\gamma_0 + \gamma_1\overline{\rho}_1 + \gamma_2\overline{\rho}_2 + \gamma_3\overline{\rho}_3)$$

$$= \gamma_0^2 + \gamma_1^2 n(\rho_1) + \cdots + \gamma_0\gamma_1 t(\rho_1) + \cdots + \gamma_1\gamma_2 t(\rho_1\bar{\rho}_2) + \cdots$$

By the choice of $\mu, n(\rho)$ is an integer for every $\rho \in \mathcal{W}$ and since in the above, all the coefficients are integers, it follows that $t(\rho_i)$ and $t(\rho_i\overline{\rho_K})$ are integers. $(i, k = 1, 2, 3)$.

$$\rho_i\rho_k = \rho_i t(\rho_k) - \rho_i\bar{\rho}_k \Rightarrow t(\rho_i\rho_k) = t(\rho_i)t(\rho_k) - t(\rho_i\bar{\rho}_k).$$

i.e., $t(\rho_i\rho_k)$ is an integer.

i.e., $D(\mathcal{W}) = |t(\rho_i\rho_k)|$ is an integer and we have the relation $D(\mathcal{J}) = |M|^2.D(\mathcal{W})$, where $\mu_i = \sum\limits_{j=0}^{3} m_{ij}\rho_j(\rho_\circ) = 1)(m_{ij} \in \mathcal{O}$, for $\mathcal{J} \subseteq \mathcal{W})$, and if $\mathcal{J} = [\mu_1 \cdots \mu_4]$.

27 But $D(\mathcal{J}) = -1 \Rightarrow |M| = \pm 1$, since $D(\mathcal{W})$ is an integer and consequently M^{-1} is integral, i.e., $\rho_j = \sum\limits_{i=1}^{4} \lambda_{ij}\mu_i$ $(j = 0to3, \rho_0 = 1), \lambda_{ij} \in \mathcal{O}$. In other words,

$$\mathcal{W} \subset \mathcal{J},\ i.e.,\ \mathcal{J} = \mathcal{W}.$$

Therefore $\mathcal{J} = \mathfrak{M}\mu^{-1}$ or $\mathfrak{M} = \mathcal{J}.\ \mu$.

ii) Let $\mathcal{J}'' = \mu^{-1}\mathcal{J}\mu = \mu^{-1}\mathfrak{M}$ Then $\mathfrak{M}\mathcal{J}'' = \mathfrak{M}\mu^{-1}\mathcal{J}\mu = \mathcal{J}.\mathfrak{M} = \mathcal{J}\mathcal{J}\mathcal{J}' = \mathcal{J}\mathcal{J}' = \mathfrak{M}$ so that $\mathcal{J}'' \subset \mathfrak{K}$. But $\mathfrak{M}\mathfrak{K} = \mathfrak{M} \Rightarrow \mu^{-1}\mathfrak{M} \subset \mathfrak{K} = \mu^{-1}\mathfrak{M} \Rightarrow \mathcal{J}'\mathfrak{K} = \mathcal{J}''$. Since $1 \in \mathcal{J}''\mathfrak{K} = \mathcal{J}'' \Rightarrow \mathfrak{K} \subset \mathcal{J}''$, i.e., $\mathcal{J}'' = \mathfrak{K}$. Further $\mathfrak{M}\mathcal{J}' = \mathfrak{M} \Rightarrow \mathcal{J}' \subset \mathfrak{K} = \mathcal{J}'' \Rightarrow \mathcal{J}' = \mathcal{J}''$ since $\mathcal{J}''$ is an order and $\mathcal{J}'$ is a maximal order. Thus we have proved our theorem that any maximal order $\mathcal{J}' = \mu^{-1}\mathcal{J}\mu$, for some $\mu \in Q$.

The above theorem holds for Q_p over $\overline{k}_p$ also, i.e., Any maximal order $\mathcal{J}_p$ in $Q_p/\overline{k}_p$ is of the form $\mu^{-1}\mathcal{J}_p\mu$ for some $\mu \in Q_p$, where $\mathcal{J}_p$ is the order in Q_p, corresponding to $\mathcal{J}$ in Q.

8. In the following, we shall introduce ideals for arbitrary orders and study their multiplicative behaviour. In the first step, we shall deal with the local case (p-adic case). The global ideals will be defined as the intersection of p-adic ideals. This procedure turns out to be convenient for our purpose, though from a formal algebraic point of view, a direct definition (Deuring, Algebraic, p.69) of global ideals mess to be preferable. For maximal orders, both definitions can be shown to be equivalent. For non-maximal orders, our definition may be more narrow.

But just those ideals defined in our way will interest us, for example in the application to modular functions.

28 **Definition.** *A* left ideal *with respect to an order $\mathcal{J}$ in $Q_p/\overline{k_p}$ is an $\mathscr{O}_p$ module $\mathfrak{M}$ such that $\mathfrak{M} = \mathcal{J}.\ \mu, \mu \in Q_p$ such that $n(\mu) \neq 0$. $\mathfrak{M}$ can also be written as $\mathfrak{M} = \mu.\mathcal{J}'$ where $\mathcal{J}' = \mu^{-1}\mathcal{J}\mu$. Then $\mathcal{J}$ is called the* left order *of $\mathfrak{M}$ and $\mathcal{J}'$, the* right order *of $\mathfrak{M}$.*

Similarly *right ideals $\nu\mathcal{J}$* can also be defined.

Any left ideal $\mathcal{J}.\mu = \mu\mathcal{J}', \mathcal{J}' = \mu^{-1}\mathcal{J}\mu$ is consequently a right ideal for the order $\mathcal{J}'$

Product of two ideals. If $\mathfrak{M} = \mu.\ \mathcal{J}$ is a right ideal for $\mathcal{J}$ and $\mathfrak{M} = \mathcal{J}.\ \nu$ left ideal for the same order $\mathcal{J}$, then the product $\mathfrak{M}.\mathfrak{N}$ is defined and is equal to $\mu.\ \nu.\ \mathcal{J}' = \mathcal{J}''.\ \mu\nu$ where $\mathcal{J}' = \nu^{-1}\mathcal{J}\nu$, the right order of $\mathfrak{M}$ and $\mathcal{J}'' = \mu.\ \mathcal{J}.\ \mu^{-1}$ the left order of $\mathfrak{M}$.

When multiplication is defined for more than three ideals it is associative, as a consequence of the associativity of Q. Every left (or right) ideal has an inverse (in the following sense).

If $\mathfrak{M} = \mathcal{J} \cdot \mu = \mu.\ \mathcal{J}'$ define $\mathfrak{M}^{-1} = \mu^{-1}\mathcal{J} = \mathcal{J}'.\mu^{-1}$. Then the product $\mathfrak{M}.\ \mathfrak{M}^{-1}$ is defined and $\mathfrak{M}, \mathfrak{M}^{-1} = \mu \cdot \mu^{-1}.\ \mathcal{J} = \mathfrak{J}$. Further, $\mathfrak{M}^{-1}.\ \mathfrak{M}$ is also defined and $\mathfrak{M}^{-1}\mathfrak{M} = \mu^{-1}\mu\mathcal{J}' = \mathcal{J}'$.

Definition. *A* grouping *is a set $G = \{A, B, \ldots\}$ with a given subset $I(G) = I$ of elements called unit elements of G and two mappings i_ℓ and i_r of G into I such that*

29 1. *$A.B$ is defined if and only if $i_r(A) = i_\ell(B)$.*

2. *If $A.B$ and $B.C$ are defined, then $A(BC)$ and $(AB)C$ are defined and are equal.*

3. *$(i_\ell(A)).A$ and $A.(i_r(A))$ are defined and are equal to A.*

4. *For every $A \in G$, there exists A^{-1} in G such that AA^{-1} and $A^{-1}A$ are defined and equal respectively to $i_\ell(A)$ and $i_r(A)$.*

5. *If I_1 and I_2 are elements of I, there exists at least one element $A \in G$ such that*
$$i_\ell(A) = I_1, i_r(A) = I_2.$$

Example of a groupoid

Let G be the set of left and right ideals with respect to the set of all maximal orders $\{\mathcal{J}_j\} = I\,(inQ_p/\overline{k}_p)$ which we take to be the set of unit elements, together with the mappings i_ℓ, i_r given by

$$i_\ell(A) = \mathcal{J}_\ell, \text{ where } A = \mathcal{J}_\ell.\mu$$

and

$$i_r(A) = \mathcal{J}_r, \text{ where } A = \mu\mathcal{J}_r.$$

We now verify that the axioms for a groupoid are satisfied.

1. follows from the definition of multiplication.

2. follows from the associativity of multiplication in Q_p.

3. $i_\ell(A)A = \mathcal{J}_\ell \cdot \mathcal{J}_\ell\mu = \mathcal{J}_\ell \cdot \mu = A$.
   $A(i_rA) = \mu.\mathcal{J}_r \cdot \mathcal{J} = \mu.\mathcal{J}_r = A$.

4. follows from the definition of the inverse.

5. Let $\mathcal{J}_1, \mathcal{J}_2$ be two maximal orders, say

$$\mathcal{J}_1 = \mu_1^{-1}\mathcal{J}\mu_1, \mathcal{J}_2 = \mu_2^{-1}\mathcal{J}\mu_2$$

where

$$\mathcal{J} = \left\{\alpha : \alpha \cong \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, \ldots \in \mathcal{O}_p\right\}$$

Take 30

$$A = \mathcal{J}_1 \cdot \mu_1^{-1}\mu_2 = \mu_1^{-1}\mu_2 \cdot \mathcal{J}^1$$

where

$$\mathcal{J}^1 = (\mu_1^{-1}\mu_2)^{-1} \cdot \mathcal{J}_1\mu_1^{-1}\mu_2 = \mathcal{J}_2$$

Then $i_\ell(A) = \mathcal{J}_1$, $i_r(A) = \mathcal{J}_2$.

If the ideal A is such that $A = \mathcal{J}_\ell, \mu = \mu\mathcal{J}_\ell$, i.e., $\mathcal{J}_\ell = \mathcal{J}_r$ then we say that A is an *ambiguous* ideal or *two-sided*.

If $Q_p/\overline{K}_p$ is a matrix algebra, then since there exists only one maximal order $\mathcal{J}_p$, all ideals are two-sided and they form a group with the unite element $\mathcal{J}_p$.

Definition. *An ideal* $\mathfrak{M}$ *is called an* integral *ideal if* $\mathfrak{M} \subset \mathcal{J}_1$.

$$\mathfrak{M} \subset \mathcal{J}_\ell \Leftrightarrow \mathfrak{M} \subset \mathcal{J}_r$$

(i) Let $\mathfrak{M} \subset \mathcal{J}_\ell$, then since $\mathcal{J}_\ell \mathfrak{M} = \mathfrak{M}, \mathfrak{M}\mathfrak{M} \subset \mathfrak{M}$. But $\mathfrak{M} \cdot \mathcal{J}_r = \mathfrak{M} \Rightarrow \mathfrak{M} \subset \mathcal{J}_r$ since if $\mathscr{K} = \{\xi : \mathfrak{M}\xi \subset \mathfrak{M}, \xi \in Q_p\}$, then $\mathfrak{M}\mathscr{R} = \mathfrak{M} \Rightarrow \mu^{-1}.\mathfrak{M}\mathscr{R} = \mu^{-1}\mathfrak{M}$

i.e., $\mathcal{J}_r \mathfrak{K} = \mathcal{J}_r$ which implies that $\mathfrak{K} \subset \mathcal{J}_r$, or $\mathfrak{M} \subset \mathscr{R} \subset \mathcal{J}_r$.

(ii) If $\mathfrak{M} \subset \mathcal{J}_r$ then $\mathfrak{M} \subset \mathcal{J}_\ell$ is similarly proved.

Definition. *Let $\mathfrak{M} = \mathcal{J}\mu = \mu\mathcal{J}'$ be an ideal. We define the norm of $\mathfrak{M}$ or be $n(\mathfrak{M}) = (n(\mu))$, the principal ideal generated by $n(\mu)$ over $\mathscr{O}_p$.*

If $\mathfrak{M}_1$. $\mathfrak{M}_2$ is defined, then $n(\mathfrak{M}_1\mathfrak{M}_2) = n(\mathfrak{M}_1).\ (\mathfrak{M}_2)$, for, if $\mathfrak{M}_1 = \mu_1\mathcal{J}_1$, $\mathfrak{M}_2 = \mathcal{J}_1\mu_2$, then since $\mathfrak{M}_1\mathfrak{M}_2 = \mu_1\mu_2\mathcal{J}'_1$ we have $n(\mathfrak{M}_1\mathfrak{M}_2) = (n(\mu_1.\mu_2)) = (n(\mu_1).\ n(\mu_2)) = (n(\mu_1)).n(\mu_2)) = n(\mathfrak{M}_1).\ n(\mathfrak{M}_2))$

31 We will now find all integral ideals of a given maximal order, and having norm (p^n).

To do this, we consider two cases:

(1) Let $Q_p/\overline{k}_p$ be a division algebra. Then it has a unique maximal order $\mathcal{J}_p$ and there exists $\pi \in Q_p$ such that $\pi^2 = p$ (since $\overline{k}_p(\sqrt{p})$ being a quadratic extension of $\overline{k}_p$, is a splitting field of Q_p and by Theorem 3, §1). Further $\pi \in \mathcal{J}_p$ since $n(\pi) = -p$.

We now have the

Theorem 6. (i) $\mathscr{P} = \mathcal{J}_p\pi$ *is the only integral ideal with* $n(\mathscr{P}) = (p)$, *and*

(ii) $\mathscr{P}^n = \mathcal{J} \cdot \pi^n$ is the only integral ideal for which $n(\mathscr{P}^n) = (p^n)$.

Proof. (i) Let $\mathscr{P}^1 = \mathcal{J}_p.\pi'$ be another integral ideal such that $n(\pi^1) = p.u_1, u_1$ a unit, i.e., $n(\mathscr{P}) = (p)$. Then $\mathscr{P}^1, \mathscr{P}^{-1} = \mathcal{J}_p\pi'\pi^{-1}$. Let $\pi'\pi^{-1} = \mu$, then $n(\mu) = \dfrac{n(\pi^1)}{n(\pi)} = \dfrac{p.u_1}{-p} = u_2$, a unit. This means that $\mu \in \mathcal{J}_p$ and also $\mu^{-1} \in \mathcal{J}_p$ since $\mu^{-1} = \dfrac{\overline{\mu}}{n(\mu)} = \overline{\mu}.$ unit, and $\overline{\mu} \in \mathcal{J}_p$. Now

$$\mathcal{J}_p\mu \subseteq \mathcal{J}_p \Rightarrow \mathcal{J}_p \subseteq \mathcal{J}_p.\mu^{-1} \subseteq \mathcal{J}_p$$

because $\mu^{-1} \in \mathscr{J}_p$ i.e., $\mathscr{J}_p = \mathscr{J}_p.\ \mu^{-1}$ or $\mathscr{J}_p\mu = \mathscr{J}_p$. So $\mathscr{J}_p.\mu = \mathscr{J}_p = \mathscr{P}^1\mathscr{P}^{-1}$, i.e., $\mathscr{P}^1 = \mathscr{P}$.

(ii) Let $\mathscr{P}^1 = \mathscr{J}_p.\pi'$ be an integral ideal such that $n(\mathscr{P}^1) = (p^n)$. Then $\mathscr{P}^1(\mathscr{P}^n)^{-1} = \mathscr{J}_p\pi'.\ (\pi^n)^{-1}$. If $\mu = \pi'(\pi^n)^{-1}$ then $n(\mu) = unit \Rightarrow \mu, \mu^{-1} \in \mathscr{J}_p$ as before.

$$\mathscr{J}_p\mu = \mathscr{J}_p = \mathscr{P}^1(\mathscr{P}^n)^{-1}, i.e., \mathscr{P}^1 = \mathscr{P}^n.$$

(2) Let $Q_p/\overline{k}_p \cong \mathfrak{M}_2(\overline{k}_p); \mathscr{J}_p = \{\alpha : \alpha \cong \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, \ldots, \in \mathscr{O}_p\}$. 32

We will now find all the integral ideals of $\mathscr{J}_p$ which have the norm (p^n). □

Let $\mathfrak{M}_p = \mathscr{J}_p.\mu_p$ be an integral ideal, i.e., $\mu_p \in \mathscr{J}_p$ and such that $n(\mathfrak{M}_p) = (n(\mu_p)) = (p^n)$, i.e., $n(\mu_p) = p^n.e$, e unit. If ε_p corresponds to an integral matrix and such that $n(\varepsilon_p)$ is a unit, then ε_p^{-1} also corresponds to an integral matrix, i.e., $\underline{\varepsilon_p^{-1} \in \mathscr{J}_p}$ or $\mathscr{J}_p\varepsilon_p = \mathscr{J}_p$ (because $\varepsilon_p \in \mathscr{J}_p$), hence $\mathscr{J}_p\varepsilon_p\mu_p = \mathscr{J}_p\mu_p$. $\overline{\text{Now choose}}$ ε_p such that

$$\varepsilon_p\mu_p \cong \begin{pmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{pmatrix}$$

then $n(\varepsilon_p\mu_p) = m_{11}m_{12} = n(\mu_p) = e.p^n$, e unit. Let $m_{22} = e_{11}.p^{n_1}$, $m_{22} = e_{22}p^{n_2}$, where $n_1 + n_2 = n$, and e_{11}, e_{22} are units.

Now

$$\begin{pmatrix} e_{11}^{-1} & 0 \\ 0 & e_{22}^{-1} \end{pmatrix}\begin{pmatrix} e_{11}p^{n_1} & m_{12} \\ 0 & e_{22}p^{n_2} \end{pmatrix} = \begin{pmatrix} p^{n_1} & e_{11}^{-1}m_{12} \\ 0 & p^{n_2} \end{pmatrix} = \varepsilon'_p\mu_p, \quad \text{say.}$$

In the product

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p^{n_1} & e_{11}^{-1}m_{12} \\ 0 & p^{n_2} \end{pmatrix} = \begin{pmatrix} p^{n_1} & e_{11}^{-1}m_{12} + p^{n_2}.t \\ 0 & p^{n_2} \end{pmatrix}$$

we choose t such that $0 \le m'_{12} < p^{n_2} = e_{11}^{-1}m_{12} + tp^{n_2}$.

Then by the matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \varepsilon'_p\mu_p \to \varepsilon''_p\mu_p \cong \begin{pmatrix} p^{n_1} & m'_{12} \\ 0 & p^{n_2} \end{pmatrix}$.

Now $\mathcal{J}_p\mu_p = \mathcal{J}_p\varepsilon'_p\mu_p = \mathcal{J}_p.\varepsilon''_p\mu_p$. 33

Therefore the set of all integral ideals with norm (p^n) is the set all $\mathcal{J}_p.\mu : \mu \cong \begin{pmatrix} p^{n_1} & m'_{12} \\ 0 & p^{n_1} \end{pmatrix}, n_1 + n_2 = n, 0 \leq m'_{12} < p^{n_2}$. Further $\mu_1 \neq \mu_2 \Rightarrow \mathcal{J}_p.\mu_1 \neq \mathcal{J}_p\mu_2$; for, if $\mathcal{J}_p\mu_1 = \mathcal{J}_p\mu_2$, then $\mathcal{J}_p\mu_1\mu_2^{-1} = \mathcal{J}_p$, i.e., $\mathcal{J}_p\mu = \mathcal{J}_p$, where $\mu = \mu_1\mu_2^{-1}$. From this we obtain $\mathcal{J}_p = \mathcal{J}_p.\mu^{-1}$, or $\mu^{-1} \in \mathcal{J}_p$ since $1 \in \mathcal{J}_p$, *i.e.*, $n(\mu)$ = unit so that

$$\mu \sim \begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix} \qquad \text{(say)}.$$

Now $\mu\mu_2 = \mu_1$ implies that

$$\begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}\begin{pmatrix} p^{n_1} & m_{12} \\ 0 & p^{n_2} \end{pmatrix} = \begin{pmatrix} p^{n'_1} & m'_{12} \\ 0 & p^{n'_2} \end{pmatrix}$$

if $$\mu_2 \sim \begin{pmatrix} p^{n_1} & m_{12} \\ 0 & p^{n_2} \end{pmatrix} \quad \text{and} \quad \mu_1 \sim \begin{pmatrix} p^{n'_1} & m'_{12} \\ 0 & p^{n'_2} \end{pmatrix}$$

Therefore $e_{21}p^{n_1} = 0$ or $e_{21} = 0$ and $e_{11}p^{n_1} = p^{n'_1}, e_{22}.\ p^{n_2} = p^{n'_2}$ imply that $e_{11} = e_{22} = 1$, *i.e*,

$$\mu_1 \sim \begin{pmatrix} 1 & e_{12} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p^{n_1} & m_{12} \\ 0 & p^{n_2} \end{pmatrix} = \begin{pmatrix} p^{n_1} & m_{12} + e_{12}p^{n_2} \\ 0 & p^{n_2} \end{pmatrix}$$

So, $m'_{12} = m_{12} + e_{12}p^{n_2}$ or $m_{12} \equiv m'_{12} \pmod{p^{n_2}}$. But, since $0 \leq m_{12}, m'_{12} < p^{n_2}$ we must have $m_{12} = m'_{12}$.

34 Hence, the number of integral ideals with norm (p^n) is equal to $1 + p + \cdots + p^n$, the number 1 corresponding to the values $n_1 = n, n_2 = 0$, the number p corresponding to the values $n_1 = n - 1, n_2 = 1$ and so on.

9. We will now extend our results from the local case to the global case. Let now Q be a quaternion algebra over the rational number field k, and let $\mathcal{J}$ be any order in Q. We have already seen that $\mathcal{J} = Q \cap \mathcal{J}_2 \cap \mathcal{J}_3 \cdots \cap \mathcal{J}_p \cap \cdots$ Analogously, we define left ideals $\mathfrak{M}$ with respect to the order $\mathcal{J}$ as $\mathfrak{M} = Q \cap \mathcal{J}_2\mu_2 \cap \cdots \cap \mathcal{J}_p\mu_p \cap \cdots$ where $\mathcal{J}_p\mu_p = \mathcal{J}_p$ for almost all p. We then have the following

Theorem 7. (i) $\mathfrak{M}$ *is a finite* $\mathcal{O}$*−module.*

(ii) $\mathfrak{M}_p = \mathcal{J}_p.\ \mu_p$ where $\mathfrak{M}_p$ is the finite $\mathcal{O}_p$–module, with the same basis elements as $\mathfrak{M}$ over $\mathcal{O}$

Proof. (i) We may, without loss of generality, assume that

$$\mathcal{J}_p \mu_p \supseteq \mathcal{J}_p \tag{A}$$

for all p. This is explained as follows:

Now, $\mathcal{J}_p \mu_p = \mathcal{J}_p$ for all except a finite number of primes p, (say) $p_1, \ldots, p_r$. So, let $\mathcal{J}_p \mu_p \not\supseteq \mathcal{J}_p$, $p = p_1, \ldots, p_r$ and let $\mathcal{J}_p \mu_p = [\nu_1 \cdots \nu_4]$ and $\mathcal{J}_p = [L_1\, L_2\, L_3\, L_4]$. □

We can then write $L_i = \sum\limits_{k=1}^{4} m_{ik} \nu_k, m_{ik} \in \overline{k}_p$. Choosing n sufficiently large so that $m_{ik}.p^n$ are p–adic integers, $p^n.L_i \in \mathcal{J}_p \mu_p \Rightarrow \mathcal{J}_p \mu_p \supseteq \mathcal{J}_p.p^n$, i.e., $\mathcal{J}_p \mu'_p \supseteq \mathcal{J}_p, \mu'_p = \dfrac{\mu_p}{p^n}$.

So we have $\mathcal{J}_{p_i} \mu_{p_i} \supseteq \mathcal{J}_{p_i}$ where $\mu'_{p_i} = \dfrac{\mu_p}{{}_{p_i}n_i}$.

Let $m = \prod\limits_{i=1}^{r} pi^{n_i} = pi^{n_i} u_{pi}$(say) u_{pi}, a p_i-adic unit. 35

Then

$$\mathcal{J}_{p_i} \frac{\mu_{p_i}}{m} = \mathcal{J}_{p_i} \cdot \frac{\mu_{p_i}}{{}_{p_i}n_i \cdot u_{p_i}} = \mathcal{J}_{p_i} \cdot \mu'_{p_i} (u_{p_i})^{-1} \supseteq \mathcal{J}_{p_i}$$

for all i, since $\mathcal{J}_{p_i} \mu'_{p_i} \supseteq \mathcal{J}_{p_i}$ and $u_{p_i} \in \mathcal{J}_{p_i}$.

If $\mathfrak{M}' = Q \cap \cdots \cap \mathcal{J}_{p_i} \dfrac{\mu_{p_i}}{m} \cap \cdots$, then $\mathfrak{M}'$ satisfies the condition (A) and if we prove that $\mathfrak{M}'$ is a finite $\mathcal{O}$– module, then since $\mathfrak{M} = m\mathfrak{M}'$, it will follow that $\mathfrak{M}$ itself is a finite $\mathcal{O}$– module.

Now, we assume that $\mathfrak{M}$ itself satisfies condition (A). Then $\mathfrak{M} \supseteq \mathcal{J}$. If $\mathfrak{M} = \mathcal{J}$, there is nothing to prove, so let $\mathfrak{M} \supset \mathcal{J}$ properly, i.e., for at least one $p, \mathcal{J}_p \mu_p \supset \mathcal{J}_p$, properly. We shall now show that $\mathfrak{M}$ can be obtained from $\mathcal{J}$ by a finite number of adjunctions and hence $\mathfrak{M}$ is a finite $\mathcal{O}$– module.

Let $\nu_p \in \mathcal{J}_p \mu_p$ and $\notin \mathcal{J}_p = [L_1\, L_2\, L_3\, \underline{L_4}]$ over $\mathcal{O}_p$ if $\mathcal{J} = [L_1 \cdots L_4]$ over $\mathcal{O}$. Then $\nu_p = L_1 n_1 + \cdots + L_4 n_4, n_i \in \overline{k}_p$ and at least one n_i(say) n_1 is not a p adic integer.

$n_i = n'_i + n''_i, n''_i \in \mathscr{O}_p$(say). Then $n'_1 \neq 0; n'_i$ are rational, $\nu_p = \left(\sum\limits_{j=1}^{4} L_j n'_j\right) + \left(\sum\limits_{j=1}^{4} L_j n''_j\right) = \nu''_p + \nu''_p$ so that $\nu''_p \in \mathscr{J}_p$ and $\nu'_p \notin \mathscr{J}_p$. If $\mathscr{J}' = [\mathscr{J}, \nu'_p]$ then $\mathscr{J}'_p \subset \mathscr{J}_p \subset \mathscr{J}_p \mu_p$. Again if $\mathscr{J}_p \neq \mathscr{J}_p.\mu_p$, as before we adjoin $\nu_p^{(2)'}$ and so on. But $\mathscr{J}_p \mu_p$ being a finite $\mathscr{O}-$ module, there 36 can only be a finite number of $\mathscr{J}'_p$ between $\mathscr{J}_p$ and $\mathscr{J}_p \mu_p$ so that we reach $\mathfrak{M}^{(1)} = [\mathscr{J}, \nu_{p_1}^{(1)'}, \nu_{p_1}^{(2)'} \cdots \nu_{p_1}^{(k)'}]$ whence $\mathfrak{M}_{p_1}^{(1)} = \mathscr{J}_{p_1} \mu_{p_1}$ (putting $p = p_1$, one of the primes for which the inclusion is proper). Now, from the decomposition, $\mathscr{J} = Q \cap_p \mathscr{J}_p$ we obtain on adjunction of these elements to each component,

$$\mathfrak{M}^{(1)} = Q \bigcap_{p \neq p_1} \mathscr{J}_p \cap \mathscr{J}_{p_1} \text{ since } \nu_{p_1}^{(i)'} \in Q \bigcap_{p \neq p_1} \mathscr{J}_p.$$

Doing the same for $\mathfrak{M}^{(1)}$ as we did for $\mathscr{J}$, with respect to prime p_2, we obtain the module

$$\mathfrak{M}^{(2)} = \bigcap_{p \neq p_1, p_2} \mathscr{J}_p \cap \mathscr{J}_{p_1} \mu_{p1} \cap \mathscr{J}_{p_2} \mu_{p_2}$$

i.e., if $\mathscr{J}_{p_2} \mu_{p_2} \supset \mathscr{J}_{p_2}$ properly; consider

$\mathfrak{M}^{(2)} = [\mathfrak{M}^{(1)}, \nu_{p_2}^{(1)'} \cdots \nu_{p_2}^{(s)'}]$ so that as before, the adjunction of these elements keep $Q, \mathscr{J}_p (p \neq p_1, p_2)$ and $\mathscr{J}_{p_1} \mu_{p_1}$ fixed and consequently $\mathfrak{M}^{(2)}$ has the above form. Further $\mathfrak{M}_{p_2}^{(2)} = \mathscr{J}_{p_n} \mu_{p_2}$. Proceeding in this manner, we obtain finally $\mathfrak{M}^{(r)} = Q \cap \mathscr{J}_{p_1} \mu_{p_1} \cap \cdots \cap \mathscr{J}_{p_r} \mu_{p_r} \bigcap\limits_{p \neq p_i \cdots p_r} \mathscr{J}_p = \mathfrak{M}$, by definition.

Thus we have proved that $\mathfrak{M}$ is a finite $\mathscr{O}-$ module.

ii (a) For $p = p_i, i = 1$ to $r, \mathfrak{M}_{p_i} = \mathfrak{M}_{p_i}^{i} = \mathscr{J}_{pi}.\ \mu_{p_i}$ by constructions of $\mathfrak{M}^{(i)}$

(b) For $p \neq p_i, i = 1$ to $r, \mathscr{J}_p \mu_p = \mathscr{J}_p$ so that $\mathfrak{M} \subset \mathscr{J}_p \mu_p = \mathscr{J}_p$, i.e., $\mathfrak{M}_p \subset \mathscr{J}_p$.

37 Further $\mathfrak{M} \supset \mathscr{J} m$ (for some integer m which is a p- adic unit) so that $\mathfrak{M}_p \supset \mathscr{J}_p$. In other words $\mathfrak{M}_p = \mathscr{J}_p = \mathscr{J}_p \mu_p$.

Note. *From the above theorem we may deduce that* $\mathfrak{M} = Q \bigcap\limits_{p} \mathfrak{M}_p$, *which is the analogue of the expression for an order* $\mathcal{J}$ *in p*.19.

Product of ideals

If $\mathfrak{M} = Q \bigcap\limits_{p} \mathcal{J}_p \mu_p$ and $\mathfrak{N} = Q \bigcap\limits_{p} \mathcal{J}'_p \nu_p$ are two ideals where $\mathcal{J}'_p = \mu_p^{-1} \mathcal{J}_p \mu_p$, then the product $\mathfrak{M}\mathfrak{N}$ is defined and is equal to the ideal $Q \bigcap\limits_{p} \mathcal{J}_p \mu_p \mathcal{J}'_p \nu_p = Q \bigcap\limits_{p} \mathcal{J}_p \mu_p \nu_p$.

Theorem 8. *If* $\mathfrak{M} = [\mu_1, \ldots, \mu_4], \mathfrak{N} = [\nu_1 \cdots \nu_4]$ *are two* ideals and the product $\mathfrak{M}\mathfrak{N}$ is defined, then $\mathfrak{M}\mathfrak{N} = [\cdots ik, \ldots]$ *(*the product module*).*

Proof. Let $\mathfrak{M} = Q \bigcap\limits_{p} \mathcal{J}_p \mu_p$ and $\mathfrak{M} = Q \bigcap\limits_{p} \mathcal{J}'_p \nu_p$. Then the ideal product $\mathscr{R} = \mathfrak{M}\mathfrak{N} = \bigcap\limits_{p} \mathcal{J}_p \mu_p \nu_p$. Let $\mathscr{R} = [\rho_1, \rho_2, \rho_3, \rho_4]$. Then $\mathscr{R}_p = (\mathfrak{M}\mathfrak{N})_p = \mathcal{J}_p \mu \nu_p = \mathcal{J}_p \mu \mathcal{J}'_p \nu_p = \mathfrak{M}_p \mathfrak{N}_p$ i.e., $[\rho_k]_p = [\mu_i \nu_j]_p \Rightarrow \mu_i \nu_j = \sum\limits_{k=1}^{4} m_{ij}^{(k)} \rho_k, m_{ij}^{k} \in \mathscr{O}_p$ for all p. □

We know already that $m_{ij}^{(k)} \in k$. Combining these two, we see that $m_{ij}^{k} \in \mathscr{O}$. In other words $\mathscr{R} = [\mu_i \nu_j]$.

We shall consider some special cases of the product of two ideals:

i) $\mathfrak{M} = \mathcal{J}, \Rightarrow \mathfrak{M}\mathfrak{N} = \mathfrak{N}$, i.e., $\mathcal{J}\mathfrak{N} = \mathfrak{N}; \mathcal{J}$ is called the left order of $\mathfrak{N}$.

ii) Defining $\mathcal{J}' = Q \bigcup\limits_{p} \mu_p^{-1} \mathcal{J}_p \mu_p$, where $\mu_p^{-1} \mathcal{J}_p \mu_p = \mathcal{J}_p$ for almost all p, it can be proved as for $\mathfrak{M}$, that $\mathcal{J}'$ is a finite $\mathscr{O}$-module. By definition, $\mathcal{J}'$ is a ring containing 1 and $\mathcal{J}' \supset \mathfrak{M}\mathcal{J}$ for some integer m so that $\mathcal{J}'$ is of rank 4. Therefore, by our second definition of an order, $\mathcal{J}'$ is an order. 38

Now, if $= Q \bigcap\limits_{p} \mathcal{J}_p \mu_p$, then $\mathfrak{M}\mathcal{J}'$ is defined and $\mathfrak{M}\mathcal{J}' = \mathfrak{M}; \mathcal{J}'$ is called the right order for $\mathfrak{M}$.

iii) If $\mathfrak{M} = Q \bigcap\limits_{p} \mathcal{J}_p \mu_p$, we defined its inverse $\mathfrak{M}^{-1} = Q \mu_p^{-1} \mathcal{J}_p$ (a right ideal for $\mathcal{J}$)$\mathfrak{M}^{-1}$ can be rewritten $Q \bigcap\limits_{p} \mathcal{J}'_p \mu_p^{-1}$ (a left ideal for $\mathcal{J}'$). Then $\mathfrak{M}\mathfrak{M}^{-1}$ is defined and $= Q \bigcap\limits_{p} \mathcal{J}_p = \mathcal{J}$.

Similarly $\mathfrak{M}^{-1}\mathfrak{M}$ is defined and $= \mathscr{J}'$.

iv) When the product of more than two ideals is defined, this is easily seen to be associative, for let $\mathfrak{M} = Q \bigcap\limits_p \mathscr{J}_p\mu_p, \mathfrak{N} = Q \bigcap\limits_p \mathscr{J}'_p\nu_p$ and $\vartheta = Q \bigcap\limits_p \mathscr{J}''_p\lambda_p$. If $(\mathfrak{N})$ and $(\mathfrak{M}\mathfrak{N})\vartheta$ are to be defined, then $\mathscr{J}'_p = \mu_p^{-1}\mathscr{J}_p\mu_p$ and $\mathscr{J}''_p = (\mu_p\nu_p)^{-1}\mathscr{J}_p(\mu_p\nu_p)$, so that $(\mathfrak{M}\mathfrak{N})\vartheta = Q \bigcap\limits_p \mathscr{J}_p$ $\mu_p\nu_p\lambda_p$.

$\mathscr{J}''_p = \nu_p^{-1}\mu_p^{-1}\mathscr{J}_p\mu_p\nu_p = \nu_p^{-1}\mathscr{J}'_p\nu_p$ implies that $\mathfrak{N}\vartheta$ is defined and $= Q \bigcap\limits_p \mathscr{J}_p\nu_p\lambda_p$. Consequently $\mathfrak{M}(\mathfrak{N}\vartheta)$ is also defined and $Q \bigcap\limits_p \mathscr{J}_p\mu_p\nu_p\lambda_p$ i.e., $(\mathfrak{M}\mathfrak{N})\vartheta = \mathfrak{M}(\mathfrak{N}\vartheta)$.

Form the above considerations, it follows at once that the set of ideals defined above with the set of all orders $\mathscr{J}' = Q \bigcap\limits_p \mu_p^{-1}\mathscr{J}_p\mu_p$ $(\mu_p^{-1}\mathscr{J}_p\mu_p = \mathscr{J}_p$ for almost all p), as the class of unit elements forms a groupoid. This particular choice of orders becomes necessary for the fifth axiom of the groupoid.

39 **Norm of an ideal :** Let $\mathfrak{M}$ be an ideal, $\mathfrak{M} = Q \bigcap\limits_p \mathscr{J}_p\mu_p, \mathscr{J}_p\mu_p = \mathscr{J}_p$ for almost all p. Then we define the norm $n(\mathfrak{M})$ of $\mathfrak{M}$, to be the principal ideal $\prod\limits_p (n(\mu_p))$ where by this we mean the ideal $(\prod\limits_{i=1}^{r} p_i^{n_i})$ generated over $\mathscr{O}.n(\mu_{p_i}) = p_i^{n_i}.\ u_i,)$ a p_i adic unit, and $p_1, \ldots p_r$ being the primes for which $\mathscr{J}_p\mu_p \neq \mathscr{J}_p$. For primes other than $p_i, n(\mu_p)$ is a unit. We may also define $n(\mathfrak{M}) = (m)$ generated over $\mathscr{O}$, where m is the g.c.d of all $n(\mu), \mu \in \mathfrak{M}$.

But if $\mathfrak{M} = [\nu_1 \cdots \nu_4]$, then m =g.c.d. of the coefficients of the quadratic from

$$n(\mu) = \sum_{i=1}^{4} n(\nu_i)x_i^2 + \sum_{i=1}^{4} t(\nu_i\bar{\nu}_j)x_ix_j.$$

For $m = \prod\limits_p$ g.c.p adic divisor of the same coefficients $= \prod\limits_p n(\mu_p)$, since $n(\mu_p)$ = g.c.p-adic divisor of the coefficients of the above quadratic form with x'_i s p - adic integers instead of being rational integers, for $\mathscr{J}_p\mu_p = \mathfrak{M}_p = [\nu_1 \cdots \nu_4]_p$.

Hence, both the definitions are equivalent.

Integral ideals A left ideal $\mathfrak{M}$ for an order $\mathcal{J}$ is said to be integral if $\mathfrak{M} \subseteq \mathcal{J}$. This is equivalent to saying that $\mathfrak{M} \subseteq \mathcal{J}'$ (right order of $\mathfrak{M}$), for $\mathfrak{M} \subseteq \mathcal{J} \Rightarrow \mathfrak{M}_p \subseteq \mathcal{J}_p$ for all p, i.e., $\mathfrak{M}_p \subseteq \mathcal{J}'_p$, since $\mathcal{J}'_p$ is a right order for $\mathfrak{M}_p$. In other words, $\mathfrak{M} \subseteq \mathcal{J}'$.

$\mathfrak{M}$ integral $\Rightarrow$ $(n(\mathfrak{M}))$ an integral ideal, since each $n(\mu), \mu \in \mathfrak{M} \subset \mathcal{J}$ is an integer, the g.c.d. is also an integer. Let $\mathcal{J}$ be maximal order in 40
Q/k, then

$$\mathcal{J}' = Q \cap \cdots \cap \mu_p^{-1} \mathcal{J}_p \mu_p \cap \cdots$$

(where $\mu_p^{-1} \mathcal{J}_p \mu_p = \mathcal{J}_p$ for almost al p), is also maximal; for $\mathcal{J}$ maximal $\Leftrightarrow \mathcal{J}_p$ maximal for every p, i.e., $\mathcal{J}'_p = \mu_p^{-1} \mathcal{J}_p \mu_p$ is maximal for every p, or $\mathcal{J}'_p$ is maximal. Conversely, we have the

Theorem 9. *If $\mathcal{J}''$ is any maximal order, then*

$$\mathcal{J}'' = Q \cap \cdots \cap \mathcal{J}''_p \cap \cdots$$

where $\mathcal{J}''_p = \mathcal{J}_p$ for almost all p.

Proof. We have $\mathcal{J}'' = Q \cap \cdots \cap \mathcal{J}''_p \cap \cdots$. Since $\mathcal{J}''$ is maximal, $\mathcal{J}''_p$ is maximal for every p, and hence there exists a $\mu''_p \in Q_p$, such that $n(\mu''_p) \neq 0$ and such that $\mathcal{J}''_p = \mu_p^{''-1} \mathcal{J}_p \mu'_p$. We have now only to show that $\mathcal{J}''_p = \mu_p^{''-1} \mathcal{J}_p \mu''_p = \mathcal{J}_p$ for almost all p. □

Let $\mathcal{J} = [L_1, \ldots, L_4], \mathcal{J}'' = [L''_1, \ldots, L''_4]$. We can write

$$L''_i = \sum_{k=1}^{4} c_{ik} L_k, c_{ik} \in k.$$

Let p be a prime which does not divide the denominator of any c_{ik}. Then c_{ik} are all p- adic integers, *i.e.*, $\mathcal{J}''_p \subset \mathcal{J}_p$. But $\mathcal{J}''_p$ is maximal, so that $\mathcal{J}''_p = \mathcal{J}_p$.

Since almost all primes p satisfy the above condition, the proof is complete.

10. Zeta Function of an Order $\mathcal{J}$

We define the zeta function $\zeta(s)$, of an order $\mathscr{J}$(where s is a complex number for which $\mathscr{R}(s) > 1$) as

$$\zeta(s) = \sum_{\mathfrak{M}} \frac{1}{(n(\mathfrak{M}))^{2s}}$$

41 where $\mathfrak{M}$ runs though all the integral left ideals of the order $\mathscr{J}$. Further we can write

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^{2s}}$$

where a_n is the number of integral left ideals for $\mathscr{J}$ with norm n; (The finiteness of a_n will be proved in §3, Lemma 1)

If

$$n = p_1^{r_1} - -p_k^{r_k}, \text{ then } a_n = a_{p_1}^{\overset{(p)}{r_1}} \cdots a_{p_k}^{\overset{(p_k)}{r_k}}$$

where $a_{p_1}^{\overset{(p)}{r_1}}$ is the number of p_i adic integral left ideals for $\mathscr{J}_{p_i}$, with the norm $p_i^{r_i}$. This follows from $\mathfrak{M} = Q \bigcap\limits_{p} \mathfrak{M}_p$ established in Theorem 7. Formally we may write

$$\zeta(s) = \prod_p \Big(\sum_{r=o}^{\infty} \frac{a_{p^r}^{(p)}}{(p^r)^{2s}} \Big)$$

the product being extended over all rational primes p. This result is a simple consequence of the equation for a_n. Actually, one can prove the convergence of this infinite product in the domain of convergence $\zeta(s)$.

We will now restrict ourselves to maximal orders. So let $\mathscr{J}$ be a maximal order. Then

$$a_{p^r}^{(p)} = \begin{cases} 1 & \text{if } Q_p \text{ is a division algebra ,} \\ i + p + \cdots p^r = \frac{1-p^{r+1}}{1-p}, & \text{if } Q_p \cong \mathfrak{M}_2(\overline{k}_p) \end{cases}$$

Let $p_1, \ldots, p_t$ denote the characteristic primes, which we know to be finite in number. Then

$$\zeta(s) = \prod_{i=1}^{t} \left(\sum_{r=0}^{\infty} \frac{1}{(p_i^r)^{2s}} \right) \cdot \prod_{\substack{p \neq p_i \\ i=1,\ldots,r}} \left(\sum_{r=0}^{\infty} \frac{1 - p^{r+1}}{\frac{1-p}{(p^r)^{2s}}} \right)$$

$$= \prod_{i=1}^{t}\left(\frac{1}{1-p_i^{-2s}}\right)\prod_{p\neq p_i}\left(\frac{1}{(1-p^{-2s})(1-p^{1-2s})}\right)$$

i.e., 42

$$\boxed{\zeta(s) = \zeta_o(2s)\zeta_o(2s-1)\prod_{i=1}^{t}(1-p_i^{1-2s})}$$

where

$$\zeta_o(s) = \prod_p (1-p^{-s})^{-1}$$

$\mathscr{R}(s) > 1$, is the Riemann zeta function.

In particular, when $t = 0$, i.e., when there do not exist any characteristic primes, we have

$$\zeta(s) = \zeta_o(2s).\zeta_o(2s-1).$$

Extending $\zeta(s)$ to the whole plane (this is possible since $\zeta_o(s)$ can be extended), it follows that $\zeta(s)$ has a simple pole at $s = 1$ with the residue

$$=(\zeta_o(2s))_{s=1}\prod_{i=1}^{t}\left(1-\frac{1}{p_i}\right)(res.\zeta_o(2s-1)_{s=1})$$

$= \dfrac{\pi^2}{6}.\dfrac{1}{2}\prod_{i=1}^{t}\left(1-\dfrac{1}{p_i}\right)$ since $\zeta_o(2s-1)$ has the expansion $\dfrac{1}{(2s-1)-1} + \cdots = \dfrac{1}{2(s-1)} + \cdots$ at the point $2s-1 = 1$, i.e., at $s = 1$

Note. *In the special case of orders $\mathscr{J}$ not necessarily maximal, but satisfying the following conditions*

1. $\mathscr{J}_p$ is maximal for all characteristic primes.

2. $\mathscr{J}_p \cong \begin{pmatrix}\mathscr{O}_p & \mathscr{O}_p\\ p\mathscr{O}_p & \mathscr{O}_p\end{pmatrix}$ for a finite number of primes. 43

3. $\mathscr{J}_p$ is maximal (say) $= \begin{pmatrix}\mathscr{O}_p & \mathscr{O}_p\\ \mathscr{O}_p & \mathscr{O}_p\end{pmatrix}$, for the rest,

We can proved that zeta function for this order is of form

$$\zeta(s) = \zeta_o(2s)\,\zeta_o(2s-1)\prod_p(1+p^{1-2s})\prod_p(1-p^{1-2s})$$

where the second product is taken over all characteristic primes, and the first over the prime for which $\mathcal{J}_p$ is of type (2). This is a consequence of the fact that $a^{(p)}_{p^r} = 2.\ \dfrac{1-p^{r+1}}{1-p} - 1$, for primes of the type (2) (M.Eichler, Zur zahlentheorie der Quat.Alg.Uselle's Journal, 1956, P.132)

Another application of the p-adic theory we shall see later in the relations between the ideals of quaternion algebras and there quadratic subfields.

3 Class of Ideals

11. Let $\mathcal{J}$ be a given, and let $\mathfrak{M}$ and $\mathfrak{N}$ be two left ideals for $\mathcal{J}$. We say that $\mathfrak{M}$ is left equivalent to $\mathfrak{N}$, (we write $\mathfrak{M} \sim \mathfrak{N}$) is there exist a μ-such that $n(\mu) \neq 0$ and $\mathfrak{M} = \mathfrak{N}\mu$, i.e., if $\mathfrak{N}^{-1}\mathfrak{M}$ is a principal ideal. The above defined relation is evidently an equivalence relation, and we obtain thus left equivalence classes of left ideals with respect to the order $\mathcal{J}$. We can similarly define right equivalence for right ideals with respect to the order $\mathcal{J}$ and obtain right equivalence classes. We will now prove the following

44 **Theorem 1.** The number of left classes with respect to an order $\mathcal{J}$ is finite and is equal to the number of right classes for $\mathcal{J}$. Further, this (say, h which is called the class number) is independent of the order $\mathcal{J}$; (in the class of unit elements of the groupoid of ideals).

Proof. Assuming that the number of left classes in finite, by means of the mapping $\mathfrak{M} \leftrightarrow \mathfrak{M}^{-1}$, the left ideal classes for $\mathcal{J}$ correspond in a $(1,1)$ manner to the right ideal classes for $\mathcal{J}$, and hence the number of right classes being equal to the number of left classes, is finite. Let now $\mathfrak{M}_1, \ldots \mathfrak{M}_h$ be a system of representatives for the left classes, then by axiom 5 for a groupoid, there exists an ideal $\mathfrak{N}$ which has $\mathcal{J}$ as a right order, and $\mathcal{J}'$ as a left order, where $\mathcal{J}' = Q\bigcap\limits_p \mu_p^{-1}\mathcal{J}\mu_p, \mu_P^{-1}\mathcal{J}_P\mu_P = \mathcal{J}_P$

for almost all p. The products $\mathfrak{N}\mathfrak{M}_1, \ldots, \mathfrak{N}\mathfrak{M}_h$ are then defined and are left ideals for the order $\mathcal{J}'$. No two of these can be left equivalent, for if $\mathfrak{N}\mathfrak{M}_i = \mathfrak{N}.\mathfrak{M}_j\varrho$, where $n(\varrho) \neq 0$ then we would have $\mathfrak{M}_i = \mathfrak{M}_j\varrho$ which is a contradiction. If h' denotes the class member for $\mathcal{J}'$ this means that $h' \geq h$. Similarly $h \geq h'$, i.e., $h = h'$. □

To prove that the number of left classes is finite, we require two lemmas.

Lemma 1. *For any order $\mathcal{J}$, there are only a finite numbers of integral left ideals with a given norm n.*

Lemma 2. *Let $\mathfrak{M}$ be a right ideal for a given order $\mathcal{J}$. Then there exist a $\mu \in \mathfrak{M}$ such that $0 < |n(\mu)| < C_{\mathcal{J}}.|n(\mathfrak{M})|$ where $C_{\mathcal{J}}$ is a constant depending only on $C_{\mathcal{J}}$.*

We will first prove the theorem assuming the lemmas to the true, and 45
then prove the lemmas.

Proof of the theorem. Let $\mathfrak{M}$ be any left ideal for $\mathcal{J}$, consequently $\mathfrak{M}^{-1}$ is a right ideal for $\mathcal{J}$ and $\mathfrak{M}\mathfrak{M}^{-1} = \mathcal{J}$. Applying lemma 2 to $\mathfrak{M}^{-1}$ there exists a $\mu \in \mathfrak{M}^{-1}$, such that

$$0 < |n(\mu)| < C_{\mathcal{J}}.n(\mathfrak{M}^{-1}) - c_{\mathcal{J}}|n(\mathfrak{M})|^{-1}$$

Consider the left ideal $\mathfrak{N} = \mathfrak{M}\mu, \mathfrak{N} \subseteq \mathcal{J}$ since $\mu \in \mathfrak{M}^{-1}$. This means that $\mathfrak{N}$ is an integral ideal in the left class of $\mathfrak{M}$ and $|n(\mathfrak{N})| = |n(\mathfrak{M}).n(\mu)| < C_{\mathcal{J}}$. Since there are only a finite number of integers in the interval $[-C_{\mathcal{J}}, C_{\mathcal{J}}]$ and since by lemma 1, there exists only a number of integral left ideals with a given norm, the number of $\mathfrak{N}_s$ is finite, it follows that the number of left classes is finite.

Proof of lemma 1. (a) If $\mathcal{J}$ is maximal, Lemma 1 has already been proved to be true. (§2, Zeta function of an order).

(b) So, one let $\mathcal{J}$ be any order. Then there exists a maximal order $\bar{\mathcal{J}}$ for which $\mathcal{J} \subset \bar{\mathcal{J}}$, i.e., $\mathcal{J}_p \subset \bar{\mathcal{J}}_p$ for all p, $\bar{\mathcal{J}}_p$ being maximal for all p because $\bar{\mathcal{J}}$ is so.

To the ideal $\mathfrak{M}_p = \mathscr{J}\mu_p$ we make correspond the ideal $\bar{\mathfrak{M}}_p = \bar{\mathscr{J}}_p\mu_p$ which is again integral since $\mu_p \in \mathscr{J}_p \subset \bar{\mathscr{J}}_p$. Further $n(\bar{\mathfrak{M}}_p) = n(\mathfrak{M}_p)$. Therefore for proving that there are only a finite number of $\mathfrak{M}_p$ with a given norm it suffices to show that only a finite number of $\mathfrak{M}_p$ correspond to the same $\bar{\mathfrak{M}}_p$.

46 Let $\bar{\mathscr{J}}_p\mu_i^{(i)} = \bar{\mathscr{J}}_p\mu_p$ where $\mathscr{J}_p\mu_p^{(i)}$ are the ideals associated with $\bar{\mathscr{J}}_p\mu_p$. Then $\mu_p^{(i)}\mu_p^{-1} = \epsilon_p^{-(i)}$, a unit in $\bar{\mathscr{J}}_p$. Denote by $\bar{\mathscr{O}}_p$ and $\mathscr{O}_p$ respectively the unit groups of $\bar{\mathscr{J}}_p$ and $\mathscr{J}_p$. Then $\bar{\mathscr{O}}_p \supset \mathscr{O}_p$ and we shall prove that $\mathscr{O}_p/\mathscr{O}_p$ is finite.

Choose n sufficiently large so that $\mathcal{P}^n.\bar{\mathscr{J}}_p \subset \mathscr{J}_p$. (The subsequent arguments hold good for the global orders $\mathscr{J} \subset \bar{\mathscr{J}} \subset Q/k$ also expect that we have to choose an integer m sufficiently large such that $m.\bar{\mathscr{J}} \subset \mathscr{J}$). This implies that the ring generated by 1, $p^n\bar{\mathscr{J}}_p$ (say) $[1, p^n\bar{\mathscr{J}}_p] \subseteq \mathscr{J}_p$ for $1 \in \mathscr{J}_p$. Let $2\mathfrak{Y}_p$ be the group of units $\{\varepsilon\}$ of the ring $[1, p^n.\bar{\mathscr{J}}_p]$ which are of the type $\varepsilon = 1(p^n.\bar{\mathscr{J}}_p)$ Then $\bar{\mathscr{O}}_p \supseteq \mathscr{O}_p \supseteq 2\mathfrak{Y}_p$. Now, the mapping

$$\mathfrak{Y}_p\alpha \to p^n\bar{\mathscr{J}}_p + \alpha, (\alpha \in \bar{\mathscr{O}}_p)$$

gives $a(1,1)$ image of $\bar{\mathscr{O}}_p/\mathfrak{Y}_p$ in the system of residue classes $\{p^n.\bar{\mathscr{J}}_p + \alpha\}$; so that $\bar{\mathscr{O}}_p/\mathfrak{Y}_p$ is finite which in its turn implies that $\bar{\mathscr{O}}_p/\mathscr{O}_p$ is finite (say) of order r. We have then the cost decomposition, $\bar{\mathscr{O}}_p = \bigcup\limits_{\nu=1}^{r} \mathscr{O}_p\eta_\nu$. Hence $\bar{\varepsilon}_p^{(i)} \in \mathscr{O}_p$ implies that $\bar{\varepsilon}_p^{(i)} \in \mathscr{O}_p\eta_\nu$ (say), i.e., $\varepsilon_p^i = \varepsilon_p^{(i)}\eta_{\nu_i}, \varepsilon_p^{(i)} \in \mathscr{O}_p$ i.e., $\mu_p^{(i)} = \varepsilon_p^{(i)}\eta_{\nu_i}\mu_p$ or $\mathscr{J}_p\mu_p^{(i)} = \mathscr{J}_p.(\eta_{\nu_i}\mu_p)$ since, we deduce that $\mathscr{J}_p\mu_p^{(i)}$ are finite in number.

Proceeding to the global case the number of integral left ideals for
47 the order $\mathscr{J}$ with norm n is given by $\prod\limits_{i=1}^{s} a^{(i)}_{p_i^{r_i}}$ if $n = p_1^{r_1}\cdots p_s^{r_s}$ and $a^{(i)}_{p_i^{r_i}}$ denotes the number of integral left ideals for the order $\mathscr{J}_{p_i}$ with norm $p_i^{r_i}$, which has been proved to be finite in the previous paragraph.

Thus our contention in completely established.

Proof of lemma 2. Let $\mathfrak{M} = Q\bigcap\limits_{p}\mu_p$. $\mathscr{J}_p = [\nu_1, \nu_2, \nu_3, \nu_4]$ and $\mathscr{J} = [L_1, L_2, L_3, L_4]$. Then, if $\nu_i = \sum_{k=1}^{4} m_{ik}L_k, m_{ik} \in k$, we will prove that absolute value of $|m_{ik}| = n(\mathfrak{M})^2$. We shall above first that $(|m_{ik}|)_p =$

$(n(\mu_p)^2)_p$. Then it would follow that

$$(n(\mathfrak{M})^2) = \prod_p (n\mu_p))^2 = \prod_p (|m_{ik}|)_p = (|m_{ik}|).$$

i.e., $n(\mathfrak{M})^2 = |m_{ik}|$. rational unit = absolute value of $|m_{ik}|$. Since $\overline{l}_K \in \mathcal{J}_p$, we can write $\overline{L}_k = \sum\limits_{l=1}^{4} L_1 c_{lk}, c_{lk} \in \mathcal{O}_p$. Then $(t(L_i\overline{L}_k)) = (t(L_iL_k))(c_{ik})$ and since $L_1, \ldots, \overline{L}_4$ also form a basis for $\mathcal{J}_p$ over $\mathcal{O}_p, (c_{ik})$ is p-unimodular, i.e., $|c_{ik}|$ is a p-adic unit. Now $D(\mu_p\mathcal{J}_p) = D(\mathfrak{M}_p) = |m_{ik}|^2.D(\mathcal{J}_p)$ from the basis representation of the ν_i-s. Since $[\mu_pL_1, \ldots, \mu_pL_4]$ form a basis for $\mathfrak{M}_p$, and since $t(\mu_pL_i.\overline{\mu_pL_j}) = n(\mu_p).\ t(L_i\overline{L}_j)$, we have $D(\mathfrak{M}_p) = n(\mu_p)^4.\ |t(L_i\overline{L}_j)| = n(u_p)^4.\ D(\mathcal{J}_p)\mu_p.\ u_p$, a p-adic unit, i.e., $|m_{ik}|D(\mathcal{J}_p) = n(\mu_p)^4.\ D(\mathcal{J}_p).\ u_p$, and $D(\mathcal{J}_p) \neq 0$ so that $(|m_{ik}|)_p = (n(\mu_p)^2)_p$.

Our object now is to find $\mu \in \mathfrak{M}$, $\mu = \nu_1t_1 \cdots + \nu_4t_4\ t_i \in \mathcal{O}$ such that $0 < |n(\mu)| < C_{\mathcal{J}}|n(\mathfrak{M})|$. Let $\nu = \nu_1X_1 + \cdots + \nu_4X_4\ X_i \in \mathcal{O}$, be any element of $\mathfrak{M}$. Substituting $\nu_i = \sum\limits_{k=1}^{4} m_{ik}L_k$ in this expression, we obtain 48
$\nu = L_1L_1 + \cdots + L_4L_4$ where

$$L_j = \sum_{i=1}^{4} X_i m_{ij} j = 1, \ldots, 4$$

are linear forms in $X_1, \ldots, X_4$ with rational coefficients. By Minkowski's Theorem on linear forms, since absolute value of $|m_{ik}| = n(\mathfrak{M})^2 = (\sqrt{|n(\mathfrak{M})|})^4$, there exist integers $t_1, \ldots, t_4$ such that

$$|L_j| = \left|\sum_{i=1}^{4} t_i m_{ij}\right| < \sqrt{|n(\mathfrak{M})|}.$$

If $\mu = \nu_1t_1 + \cdots + \nu_4t_4$, then $\mu \in \mathfrak{M}$, and since $n(\mu) = \sum_{i=1}^{4} n(L_i)L_i^2 + \sum_{i,j=1,i\neq j}^{4} t(L_i\overline{L}_j).L_iL_j$ we have $0 < |n(\mu)| < C_{\mathcal{J}}.\ |n(\mathfrak{M})|$, where $C_{\mathfrak{J}}$ is a constant depending only on the order $\mathcal{J}$.

12. The quaternion algebras over the rational number field k can be divided into two classes according as the quadratic form given by the norm is definite or indefinite. In the first case way that the algebra is definite, and in the second case that it is indefinite.

If the algebra Q is definite, the class number h is in general greater than 1. If Q is indefinite, it can be proved that $h = 1$ for maximal orders. (For a proof see M.Eichler, *Math.Zeit*, 1938). Furthermore, it can be proved that $h = 1$ for even a wider class of orders, i.e., for orders of the type $\mathscr{J}$, where

49 1. $\mathscr{J}_p$ is maximal for almost all p, or without loss of generality,

$$\mathscr{J}_p \cong \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ \mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$$

2. $\mathscr{J}_p$ is maximal for all characteristic primes p.

3. For the remaining finite number of primes,

$$\mathscr{J} p \cong \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ p\mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$$

(For a proof of this, see M.Eichler, *Math.Zeit*, 1952.

We will give a proof of the above result in a special case.

Note. *We call such an order an order of the type* $(q_1, q_2), q_1, q_2$ *being the product of primes of types* (2) *and* (3) *respectively.*

Theorem 2. *Let* $Q/k \cong \mathfrak{M}_2(k)$ *(i.e.,* there do not exist any characteristic primes) and let $\mathfrak{J} \cong \begin{pmatrix} \mathscr{O} & \mathscr{O} \\ m\mathscr{O} & \mathscr{O} \end{pmatrix}$, m a rational integer be an order of Q. Then all left ideals for $\mathscr{J}$ are principal,*i.e.,* $h = 1$.

We required the following two lemmas:

Lemma 1. *Let* $\mathfrak{M} = Q \bigcap_p \mathscr{J}_p \mu_p$ *be any left ideal for* $\mathscr{J}$*; then there exists a* $\varrho \in Q$ *such that* $\mathfrak{M}.\ \varrho = \mathfrak{N}$ *is integral,* $n(\varrho) \neq 0$ *and such that* $(n(\mathfrak{N}), m) = 1$.

Lemma 2. *An ideal* $\mathfrak{N}$ *whose norm is coprime to m is necessarily principal.*

Assuming the lemmas to be true, we will establish the theorem. By 50 lemmas 1 and 2, every left ideal $\mathfrak{M}$ for the order $\mathscr{J}$ is left equivalent to a principal ideal, and hence there is only one class, viz., the class of principal ideals, i.e., $h = 1$.

Proof of lemma 1. Let the primes p for which $p|m$ be denoted by $p_1, \ldots, p_r$. We have to find a $\mu \in Q, n(\mu) \neq 0$ such that μ_p. μ^{-1} is a unit in $\mathscr{J}_p$ for all $p|m$. If $n(\mu_{pi}) = p_i^{n_i} u_i$ (u_i, a p-adic unit), $i = 1, \ldots, r$, let n be integer greater than max $(1, n_1 + 1 - s_1, \ldots, n + 1 - s_r)$ where $\mu_{p_i} = p_i^{s_i}.\ \mu'_{p_i}, \mu'_{p_i} \in \mathscr{J}_{p_i}$. Let $\mathscr{J} = [\nu_1, \nu_2, \nu_3, \nu_4]$, then we have

$$\mu_{p_i} = \sum_{j=1}^{4} \mu_{p_i}^{(i)} \nu_j, \mu_{p_i}^{(j)} \in \overline{k}_{p_i}, i = 1, \ldots, r.$$

Now by Ostrowski's Theorem on approximation, for each $j = 1, \ldots$, r we can find a $\mu^{(j)} \in k$ such that

$$\mu^{(j)} \equiv \mu_{p_i}^{(j)} (p_i^n . \mathscr{O}_{p_i}), i = 1, \ldots, r.$$

Let $\mu = \sum\limits_{j=1}^{4} \mu^{(j)} \nu_j$, then $\mu \in Q$, and we use the notation $\mu \equiv \mu_p$ (mod $p^n \mathscr{O}_p$), $(p = p_1, \ldots, p_r)$. Now $n(\mu) \neq 0$, for otherwise we would have $0 = n(\mu) \equiv n(\mu_p)(p^n \mathscr{O}_p)$, i.e., $n(\mu_p) = p^n$. (some p-adic integer), $p = p_1, \ldots, p_r$ which is a contradiction to the choice of n.

Now $\mu_{p_i} = p_i^{s_i}.\ \mu'_{p_i}, \mu'_{p_i} \in \mathscr{J}_{p_i}, n = max(1, n + 1 - s_1, \ldots, n_r + 1 - s_r)$ and $\mu = \mu_{p_i} + p_i^n \varrho_i, \varrho_i \in \mathscr{J}_{p_i}$. Then

$$\begin{aligned} \mu\mu_{p_i}^{-1} &= 1 + p_i^n \varrho_i \frac{\overline{\mu}_{p_i}}{n(\mu_{p_i})} \\ &= 1 + p_i^n \varrho_i \frac{p_i^{s_i} . \overline{\mu'}_{pi}}{p_i^{n_i} u_i} = 1 + p_i^{n+s_i-n_i} \left(\frac{\overline{\mu'}_{p_i}}{u_i} \right) \\ &= 1 + p_i \lambda_i, \lambda_i \in \mathscr{J}_{p_i}, \end{aligned}$$

because $\dfrac{\overline{\mu}_{p_i}}{u_i} \in \mathscr{J}_{p_i}$, and $n + s_i - n_i \geq 1$ by choice of n. Hence $\mu\mu_{p_i}^{-1} \in \mathscr{J}_{p_i}$ 51 also since $n(\mu\mu_{p_i}^{-1})$ is a p_i-adic unit, it follows that $\mu\mu_{p_i}^{-1}$ is a unit of

$\mathcal{J}_{p_i}$ for $i = 1, \ldots, r$. Consider now the ideal $\mathfrak{M}\mu^{-1} = Q \bigcap\limits_p \mathcal{J}_p \mu_p \mu^{-1} = \mathfrak{N}'$(say), then $\mathfrak{N}'_p = \mathcal{J}$ for all $p|m$, also for almost all p. Now $(n(\mathfrak{N}')) = \prod_p (n(\mathfrak{N}'_p))$, and since $n(\mathfrak{N}'_p)$ is a p-adic unit for all $p|m$, it follows that $n(\mathfrak{N}')$ is coprime to m.

Let $q_1, \ldots, q_s$ be the primes for which $\mathfrak{N}'_p \neq \mathcal{J}_p$, then we choose r_i such that $q_i^{r_i}\mathfrak{N}'_{q_i} \subseteq \mathcal{J}_{q_i}$. Let $n = q_1^{r_1} \cdots q_s^{r_s}$, then $n.\mathfrak{N}'_{q_i} \subseteq \mathcal{J}_{q_i}$, $i = 1, \ldots, s$ and $n.\mathfrak{N}'_p = n.\ \mathcal{J}_p = \mathcal{J}$ for $p \neq q_i$. since n is a p-adic unit. Therefore the ideal $\mathfrak{M}.\mu^{-1}n = \mathfrak{N}'.n = \mathfrak{N}$, or $\mathfrak{M}\varrho = \mathfrak{N}$, $\varrho = \mu^{-1}.\ n$, is integral, and $n(\mathfrak{N}) = n^2.\ n(\mathfrak{N}')$ is coprime to m since both factors are coprime to m.

Proof of lemma 2. (1) If $m = 1$, we know that there exists $\mu \in \mathfrak{N}$ such that $n(\mu)|n(\nu)$ for all $\nu \in \mathfrak{N}$ and then we proved (in $Th/5$§2) that $\mathfrak{N} = \mathcal{J}.\ \mu$, i.e., $\mathfrak{N}$ is principal, or $h = 1$.

(2) $m > 1$. In this case we proceed in a similar fashion. Consider all $\nu \in \mathfrak{N}$ such that $(n(\nu), m) = 1$. There exist such ν, since $n(\mathfrak{N}) =$
52 g.c.d. $n(\nu)\nu \in \mathfrak{N}$. If there exist two such elements ν_1, ν_2, then we can find units ε_1, ε_2 such that

$$\varepsilon_1\nu_1 = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad \varepsilon_2\nu_2 = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

We only show how to find the unit ε_1, and then ε_2 can be constructed in the same way. Let

$$\varepsilon_1 = \begin{pmatrix} e_{11} & e_{12} \\ me_{21} & e_{22} \end{pmatrix}, \nu_1 = \begin{pmatrix} n_{11} & n_{12} \\ m.n_{21} & n_{22} \end{pmatrix}$$

Then

$$\varepsilon_1\nu_1 = \begin{pmatrix} * & * \\ m(e_{21}n_{11} + e_{22}n_{21}) & * \end{pmatrix}$$

In order that ε_1 be a unit and $\varepsilon_1\nu_1$ be of the required form, we must have

$$e_{11}e_{22} - me_{21}e_{12} = 1,$$
$$e_{21}n_{11} + e_{22}n_{21} = 0.$$

Put $e_{21} = \dfrac{n_{21}}{(n_{21}, n_{11})}, -e_{22} = \dfrac{n_{11}}{(n_{21}, n_{11}}$), then $(e_{21}, e_{22}) = 1$, further $(me_{21}, e_{22}) = 1$, because $(n_{11}, m.n_{21}) = 1$ since $(n(\nu_1), m) = 1$, so there exists integers a and b such that $be_{22} - ame_{21} = 1$, then put $b = e_{11}, a = e_{12}$, and we easily see that the required conditions are satisfied.

Proceeding as before, we obtain $\nu \in \mathfrak{N}$ such that $n(\nu)|n(\nu_1)$ and $n(\nu_2)$. Continuing thus, since the denominators of $n(\nu)$ are bounded, we obtain after a finite number of steps, a $\nu \in \mathfrak{N}$ such that $n(\nu)$ divides the norms of all elements in $\mathfrak{N}$ and then $n(\nu) = n(\mathfrak{N})$. 53

It is enough to show that $\mathcal{J}_p.\nu = \mathcal{J}_p.\nu_p$ for all p, where $\mathfrak{N} = Q \bigcap\limits_p \mathcal{J}_p \nu_p$, for this would mean that

$$(\mathcal{J}.\nu)_p = \mathcal{J}_p.\nu = \mathcal{J}_p \nu_p = \mathfrak{N}_p$$

for all p, i.e., $\mathcal{J}.\nu = \mathfrak{N}$.

Now $\nu = L_p.\ \nu_p$, $L_p \in \mathcal{J}_p$ so that $n(\nu) = n(L_p).n(\nu_p)$. But $n(\nu)$ =(p-adic unit). $n(\nu_p)$ by definition of norm and this means that $n(L_p)$ = p-adic unit, i.e., $L_p^{-1} \in \mathcal{J}_p \Rightarrow L_p$ a unit in $\mathcal{J}_p$. in other words, $\mathcal{J}_p.\ \nu = \mathcal{J}_p.\ \nu_p$.

13. We will prove an important lemma concerning an order $\mathcal{J}$ of type (q_1, q_2) presently.

Lemma 3. $\underline{D(\mathcal{J}) = q_1^2 q_2^2}$.

Proof. We have $(D) = \prod\limits_p (D)_p$. But for all primes of the type (1) $(D)_p = (D(\mathcal{J}_p))_p = \mathcal{O}_p$ so that our purpose, it is enough to consider the primes dividing q_1 and q_2. □

(i) In the case of characteristic primes $p|q_1, \mathcal{J}_p$ is maximal and we construct a special basis $[1, \omega, \Omega, \omega\Omega]$ such that

$D(\mathcal{J}_p) = D[1, \omega, \Omega, \omega\Omega] = p^2.u; u$, a p-adic unit.

Let K be an unramified quadratic extension of $\bar{k}_p$ and $[1, \omega]$ a base for the maximal order (or the ring of integers in $\bar{K}$). Then, by theorem 4.c of §1, $\bar{K}$ is a splitting field for Q_p and hence $\bar{K} \cong K \subset Q$ by theorem 3 of §1 so that we may look upon $[1, \omega]$ as an integral base for integers in K.

Then we choose an element $\Omega \in Q_p$ such that $\Omega^2 \in \bar{k}_p$, $\Omega^{-1}\omega\Omega = \bar{\omega}$. 54

But Ω^2 cannot be the norm of an element of $\overline{K}$, for then it would mean that Q_p is a matrix algebra. Since every unit of k_p is a norm of an element of $\overline{K}$ and p is not, $\Omega^2 = p.\ \mathcal{U}$ with $\mathcal{U}, a$ unit. We shall now prove that $[1, \omega, \Omega, \omega\Omega]$ is the maximal order in Q_p. That it is an order, follows by construction. Further

$$D[1, \omega, \Omega, \omega\Omega] = \begin{vmatrix} 2 & t(\omega) & 0 & 0 \\ t(\omega) & t(\omega^2) & 0 & 0 \\ 0 & 0 & 2p & pt(\omega) \\ 0 & 0 & pt(\omega) & 2p.n(\omega) \end{vmatrix}$$

Now,

$$D[1, \omega] = \begin{vmatrix} t(1.1) & t(1.\omega) \\ t(\omega.1) & t(\omega.\omega) \end{vmatrix} = \begin{vmatrix} 2 & t(\omega) \\ t(\omega) & t(\omega^2) \end{vmatrix}$$

is a p-adic unit, since the extension is unramified (follows by Dedekind's theorem). Furthermore,

$\begin{vmatrix} t(1.1) & t(1, \bar{\omega}) \\ t(\omega.1) & t(\omega, \bar{\omega} \end{vmatrix} = D[1, \omega].u$; u, a p-adic unit, so that $[1, \omega, \Omega, \omega\Omega] = p^2.\ u_o$ being a p-adic unit. It remains to prove now that $[1, \omega, \Omega, \omega\Omega]$ is maximal. For the same it is enough to show that if $\xi = x_o + \cdots + x_3\omega\Omega$ is an element of Q_p such that $n(\xi) \in \mathscr{O}_p$, then x_i are all in $\mathscr{O}_p$. Now $\xi = \xi_1 + \xi_2\Omega$, where $\xi_1 = x_o + x_1\omega$ and $\xi_2 = x_2 + x_3\omega$; $n(\xi) = n(\xi_1) - pn(\xi_2)$ is a p-adic integer.

55 Since $\xi_1 \in K$, either $\xi_1 \in \mathscr{O}$ (ring of integers in K) or $\xi_1^{-1} \in \mathfrak{R} = (p)$ by virtue of K being unramified, i.e., $\xi_1 = p^{-r_1}.\ u_1; u_1$,a unit of $\mathscr{O}$. Similarly, either $\xi_2 \in \mathscr{O}$ or $\xi_2 = p^{-r_2}u_2; u_2$, a unit. Therefore $n(\xi) = p^{-2r_1}.n(u_1) - p^{-2r_2}.\ n(u_2)$. Since $n(u_1)$ and $n(u_2)$ are p-adic units, this cannot happen. Hence ξ_1 and ξ_2 are both in $\mathscr{O}$, i.e., x_0, x_1, x_2, x_3 are all p-adic integers, since $[1, \omega]$ forms a base of $\mathscr{O}$ over $\mathscr{O}_p$.

(ii) In the case of primes $p|q_2$,

$$\mathscr{J}_p \cong \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ p\mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$$

so that we have a basis

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right]$$

Therefore

$$D[\mathcal{J}_p] = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = -p^2 = p^2 \text{ a } p\text{-adic unit .}$$

Hence our assertion is completely established.

Chapter 2

Theory of Units

4 Units

1. Let $\mathscr{J}$ be an order in the quaternion algebra Q/k; then a necessary and sufficient condition that an element ε in $\mathscr{J}$ be a unit in $\mathscr{J}$ is that $n(\varepsilon)$ be a unit in $\mathscr{O}$. It is easy to see that the units in $\mathscr{J}$ form a group which we denote by $\mathscr{O}_{\mathscr{J}}$. In the case of definite algebras Q/k, we have the following 56

Theorem 1. If Q/k is definite, then $\mathscr{O}_{\mathscr{J}}$ is of finite order.

Proof. Let $\mathscr{J} = [L_1 \cdots L_4]$ and $\varepsilon = e_1L_1 + \ldots + e_4L_4$, a unit in $\mathscr{J}$.

$$n(\varepsilon) = e_1^2 n(L_1) + \cdots + e_1e_2t(L_1\bar{L}_2) + \cdots = 1.$$

Q being definite, the quadratic form given by the norm is definite and consequently the equation $n(\varepsilon) = 1$ with real coefficients $e_1, \ldots, e_4$ represent an ellipsoid in R_4. Hence there are only a finite number of lattice points on this surface. In other words there are only a finite number of integral $e_1 \cdots e_4$ for which $n(\varepsilon) = 1$, i.e., $\mathscr{O}_{\mathscr{J}}$ is of finite order. □

Note. *In fact, we have the converse part also to be true in this case, namely, if Q is indefinite, $\mathscr{U}_{\mathscr{J}}$ is infinite. (We shall not give the proof here).*

We shall now consider unit groups of order of $Q/k \cong \mathfrak{M}_2(k)$. Let $\mathcal{J}$ be the maximal order $\begin{pmatrix} \mathscr{O} & \mathscr{O} \\ \mathscr{O} & \mathscr{O} \end{pmatrix}$. Then the group of units $\mathscr{U} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \right.$
57 $\left. a, b, c, d \in \mathscr{O} \text{ and } ad - bc = \pm, 1 \right\}$ is simply the unimodular group Γ of $(2, 2)$ matrices and the subgroup $\mathscr{U}_1$ of proper units of $\mathcal{J}$ (i.e., $ad - bc = 1$) is nothing but the modular group Γ_1, which is a normal subgroup of Γ of index 2.

We know that Γ_1 as a group acting on the upper half plane is discontinuous and we have a fundamental domain (say) D_1. If $\mathcal{J}_o$ is any order $\subset \mathcal{J}$, then the group of proper units of $\mathcal{J}_o$, say $\mathscr{U}_0 \subset \mathscr{U}_1$. Consequently $\mathscr{U}_0$ as a group acting on the upper half plane, is discontinuous and let D_0 be its fundamental domain.

Now, $\mathscr{U}_0$ is of finite index in $\mathscr{U}$. Just as we had in the p-adic case (§3, Proof of lemma 1) we have a coset decomposition

$$\mathscr{U}_1 = \bigcup_{i=1}^{h} \mathscr{U}_0 \varepsilon_i$$

Then it can easily be-seen that D_0 can be taken to be $\bigcup\limits_{i=1}^{h} \varepsilon_i D_1$; $\varepsilon_i D_1$, the image of D_1, by means of ε_i.

We shall take up the remaining case, namely when Q is indefinite and also a division algebra.

If $Q = [1, \omega, \Omega, \omega\Omega], \omega^2 = p, \Omega^2 = q, (\omega\Omega)^2 = -pq$, since Q is indefinite, at least one of the three $p, q, -pq$ is positive and we assume without loss of generality that $p > 0$.

Since Q splits over $K \cong k(\sqrt{p})$, we have the following isomorphism of QK onto $\mathfrak{M}_2(K) \cong \mathfrak{M}_2(k(\sqrt{p}))$.

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \omega \to \begin{pmatrix} \sqrt{p} & 0 \\ 0 & -\sqrt{p} \end{pmatrix}, \Omega \to \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \text{ and } \omega\Omega \to \begin{pmatrix} o & \sqrt{p} \\ -q\sqrt{p} & 0 \end{pmatrix}$$

58 Consequently, any element $\xi \in Q, \xi = X_1 + X_2\omega + X_3\Omega + X_4\omega\Omega$ has the image $\begin{pmatrix} X_1 + X_2\sqrt{p} & X_3 + X_4\sqrt{p} \\ q(X_3 - X_4\sqrt{p}) & X_1 - X_2\sqrt{p}) \end{pmatrix}$, i. e., $\begin{pmatrix} \xi_1 & \xi_2 \\ q\bar{\xi}_2 & \bar{\xi}_1 \end{pmatrix}$ if $\xi_1 = X_1 +$

$X_2\sqrt{p}, \xi_2 = X_3 + X_4\sqrt{p}; \xi_1, \xi_2 \in k(\sqrt{p})$ and $\bar{\xi}_1, \bar{\xi}_2$ denote the algebraic conjugates of ξ_1, ξ_2 in $k(\sqrt{p})$.

2. We wish to prove the existence of fundamental domains for unit groups of orders in this case also and for the same, we require the following two lemmas.

Let $\mathscr{J}$ be an order and $\mathscr{J} = [L_1 \cdots L_4]$. Consider all $\xi = L_1x_1 + \cdots + L_4x_4, x_i$- real and $n(\xi) = 1$. ($n(\xi)$ means simply the quadratic from with real variables $x_1 \cdots x_4$). Then the set M_c is defined as $\{\xi : |x_i| \leq c\} \cap \{\xi : n(\xi) = 1\}$. In other words it is the intersection of the cube $|x_i| \leq c$ in R_4 with the surface $n(\xi) = 1$.

Lemma 1. *Let $\xi = L_1x_1 + \cdots + L_4x_4$, x_i - real and $n(\xi) = 1$. Then there exists only a finite number of units (say) $\varepsilon_1 \ldots \varepsilon_n$ so that if for any $\xi \in M_c, \xi$ and $\varepsilon\xi \in M_c, \varepsilon$, an unit of $\mathscr{J}$, then ε is one of $\varepsilon_1 \ldots \varepsilon_n$. (This lemma is true even if Q is not a division algebra).*

Lemma 2. *Q/k is a division algebra and $\xi = \sum_{j=1}^{4} L_jx_j, x_j$- real and $n(\xi) = 1$. Then there exists a constant C independent of ξ, and a unit ε of $\mathscr{J}$, such that $\varepsilon\xi = \eta \in M_c$.*

Proof of lemma 1. Let $\eta = \varepsilon\xi = \sum_{j=1}^{4} L_jy_j, \varepsilon$, a unit of $\mathscr{J}$. Then we have $\varepsilon = \eta\xi^{-1} = \eta.\xi = L_1e_1 + \cdots + L_4e_4$ (say) where $e_i \in \mathscr{O}$. Further e_i are bilinear forms in the coefficients of ξ and η. If ξ and $\eta = \varepsilon\xi \in M_c$, 59 then $|x_i| \leq c, |y_j| \leq c$ so that $|e_i| \leq c'$ (c' depending on c only), e_i being integers, there can be a finite number of them satisfying the above condition and hence our lemma.

Proof of lemma 2. Let $\beta = \alpha\xi, \alpha \in \mathscr{J} = [L_1 \ldots L_4]$. If $\alpha = \sum_{i=1}^{4} \alpha_iL_i$, then $\beta = \sum_{i=1}^{4} \alpha_iL_i\xi$. But $L_i.\xi = \sum_{j=1}^{4} L_iL_jX_j = \sum_{j,k} \lambda_{ij}^{(k)}X_jL_k$ if $L_iL_j = \sum_{k=1}^{4} \lambda_{ij}^{(k)}L_k$.

i. e.,
$$L_i\xi = \sum_{k=1}^{4} c_{ik}L_k, c_{ik} - \text{ real.}$$

Then we know that $|(c_{ik})| = (n(\xi))^2$. Hence $\beta = \sum\limits_{i,k} a_i c_{ik} L_k = \sum\limits_{k=1}^{4} b_k L_k$ if $b_k = \sum\limits_{i=1}^{4} a_i c_{ik}, b_k$ are linear forms in $a_1 \cdots a_4$ and their determinant $|c_{ik}| = n(\xi)^2 = 1$.

Applying Minkowski's Theorem on linear forms to b_k, we can find integral values for $a_1, \ldots, a_4$ not all zero such that $|b_k| \leq 1$, $k = 1$ to 4. Putting $\alpha = \sum\limits_{i=1}^{4} a_i L_i$ $(\alpha \in \mathcal{J})$ and $\beta = \alpha\xi$ we have since $|b_k| \leq 1, n(\alpha) = n(\beta) < \gamma$, where γ is a constant. Further $a_1 \cdots a_4$ not all zero imply that $\alpha \neq 0$ and hence $n(\alpha) \neq 0$ from the fact that Q is a division algebra.

Now, $\alpha \in \mathcal{J}$ and $n(\alpha) < \gamma$ imply that since there can exist only a finite number of integral ideals $\alpha_1\mathcal{J} \ldots \alpha_h\mathcal{J}$ with norms bounded by $\gamma, \alpha\mathcal{J} = \alpha_j\mathcal{J}$, i, e., $\alpha = \alpha_j\varepsilon, \varepsilon$, a unit of $\mathcal{J}$. Therefore $\beta = \alpha_j\varepsilon\xi$, i.e., $\alpha_j^{-1}\beta = \varepsilon\xi = \eta$ (say). Since coefficients of β are bounded and since α_j come from a finite set, the coefficients of η are bounded (say) are by c, and further $n(\eta) = 1$. Hence $\eta \in M_c$ and thus Lemma 2 is proved. 60

Lemma 3. *In Lemmas 1 and 2, we can replace $L_1 \cdots L_4$ by any four linearly independent elements $k_1, \ldots k_4$ of Q/k.*

This follows from the fact that $[L_1 \cdots L_4]$ and $k_1, \ldots, k_4$ are connected by means of non-singular transformation and accordingly the proofs of Lemmas 1 and 2 go through except for the fact that the constant c has to be replaced by another c'.

Let Q be an indefinite quaternion algebra over k. We shall take for k_1, k_2, k_3, k_4 the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ respectively. (This is possible even if Q be a division algebra, because it splits over $K \simeq k(\sqrt{p})\,(p > 0)$).

Let $\mathscr{H}$ be the space of all $(2, 2)$ real matrices with determinant 1. In particular $\mathscr{H}$ contains all elements ξ of Q with $n(\xi) = 1$. We now map $\mathscr{H}$ onto the complex upper half plane S.

If $\xi = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$ with $x_{11}x_{22} - x_{12}x_{21} = 1$, define the mapping $\varphi : \mathscr{H} \to S$ by $\varphi(\xi) = \xi(i) = \dfrac{x_{11}i + x_{12}}{x_{21}i + x_{22}}$.

Since $\operatorname{Im}(\xi(i)) = \dfrac{1}{x_{21}^2 + x_{22}^2}$, $\varphi(\xi)$ is onto; for

$$\begin{pmatrix} a/\sqrt{b} & \sqrt{b} \\ 1/-\sqrt{b} & 0 \end{pmatrix}(i) = a + ib.$$

Lemma 4. *The set* $M_c = \left\{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} x_{ij}$ *real and* $|x_{ij}| \leq c$, $x_{11}x_{22} - x_{12}x_{21} = 1\right\} \subset \mathscr{H}$ *is mapped by* φ *onto finite part of the upper half plane* 61 S *and conversely, any domain in* S *consisting of* $\left\{\tau : |\tau| < C_1, \operatorname{Im}\tau > c_2\right\}$ *has an inverse contained in* M_c *for some* c*.*

Proof. Now $|x_{ij}| < c \Longrightarrow |x_{11}i + x_{12}| < 2c$ and $|x_{12}i + x_{22}| < 2c$. Further $0 \leq d < |x_{21}i + x_{22}| < 2\,c$, for

$$\left|(x_{22} - x_{21}i)(x_{11}i + x_{12})\right| = \left|(x_{22}x_{12} + x_{11}x_{21}) + i\right| \leq C'$$

implies that if $\left|x_{21}i + x_{22}\right|$ were arbitrarily small, $|x_{11}i + x_{12}|$ would increase arbitrarily, which is not true. □

Hence $\operatorname{Im}(\xi(i)) = \dfrac{1}{\left|(x_{21}i + x_{22})\right|^2} > \dfrac{1}{c^2}$ so that M_c is mapped onto a finite part of the upper half plane. Conversely if $\tau = \dfrac{x_{11}i + x_{12}}{x_{21}i + x_{22}}$ is such that $x_{11}x_{22} - x_{12}x_{21} = 1$, $|\tau| < c_1$ and $\operatorname{Im}\tau > c_2$, then $\dfrac{1}{x_{21}^2 + x_{22}^2} > c_2 \Longrightarrow \left|x_{21}\right| < c_3, \left|x_{22}\right| < c_3$. Further $\dfrac{x_{11}^2 + x_{12}^2}{x_{21}^2 + x_{22}^2} < c_1^2 \Longrightarrow x_{11}^2 + x_{12}^2 < \dfrac{c_1^2}{c_2} \Longrightarrow \left|x_{11}\right| < c_4, \left|x_{12}\right| < c_4$. Choosing $c = \max(c_3, c_4)$, it follows that $\left|x_{ij}\right| < c, i, j = 1, 2$. From here onwards, we shall use the notation M_c for the image of M_c by means of φ, in the upper half plane S. If $\xi, \eta \in \mathscr{H}$, then we shall prove that $\varphi(\eta\xi) - (\eta\xi)(i) = \eta(\xi(i))$. For, let $\xi = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$

and $\eta = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$. Then

$$\begin{aligned}(\eta\xi)(i) &= \frac{(y_{11}x_{11} + y_{12}x_{21})i + (y_{11}x_{12} + y_{12}x_{22})}{(y_{21}x_{11} + y_{22}x_{21})i + (y_{21}x_{12} + y_{22}x_{22})} \\ &= \frac{y_{11}\left(\frac{x_{11}i+x_{12}}{x_{21}i+x_{22}}\right) + y_{12}}{y_{21}\left(\frac{x_{11}i+x_{12}}{x_{21}i+x_{22}}\right) + y_{22}} = \frac{y_{11}\xi(i) + y_{12}}{y_{21}\xi(i) + y_{22}}\end{aligned}$$

62 $\xi(i)$ being a point of the upper half plane S and since $\mathscr{H}$ acts as a group of mapping on S, $\frac{y_{11}\xi(i) + y_{12}}{y_{21}\xi(i) + y_{22}} = \eta(\xi(i))$. Thus we have the important passage from a mapping of $\mathscr{H} : \xi \to \eta\xi$ to a mapping of the upper half plane: $\xi(i) \to \eta(\xi(i))$ by means of φ. This enables us to carry over our lemmas for $\mathscr{H}$ to those for S, as follows:

Lemma 1′ Given a finite domain M_c in S, there exists only a finite number of units $\varepsilon_1, \ldots, \varepsilon_n$ in order $\mathscr{J}$ of Q such that if τ and $\varepsilon(\tau)$ are in $M_c(\varepsilon$, a unit of $\mathscr{J})$ then ε is one of $\varepsilon_1 \cdots \varepsilon_n$.

Lemma 2′ If Q is a division algebra, then there exists an M_c in S such that for any $\tau \in S$, we can find at least one unit ε of $\mathscr{J}$ such that $\varepsilon(\tau) \in M_c$.

If $\mathscr{H}$ is the group of proper units of an order $\mathscr{J}$ in Q $\mathscr{O} \subset \mathscr{H}$and using the lemma 1′ we shall construct a fundamental domain for $\mathscr{O}$ in S. We will further prove using lemma 2′ that $D$is bounded in the case of a division algebra Q and in general D has only a finite number of neighbours.

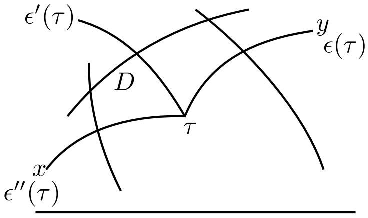
Note. *One may also proceed alternatively for proving the existence of a fundamental domain for $\mathscr{O}$ in S, as follows:_If $\mathfrak{L}$ is the inverse image of the point i, by means of φ, in $\mathscr{H}$, then $\mathfrak{L}$ is the proper orthogonal group and consequently a compact subgroup of the topological group $\mathscr{H}$. Then it can be proved that the mapping $f : \frac{\mathscr{H}}{\mathfrak{L}} \to S$ defined by*
63 *$f(\xi\mathfrak{L}) = \varphi(\xi) = \xi(i)$ is one-one open and continuous. The latter part follows from the fact that φ is open and continuous. From Lemma 1′, we*

obtain $\mathscr{O}$ is discrete in $\mathscr{H}$ and $\bar{\mathcal{L}}$ being compact, it follows that $\mathscr{O}$ has a discontinuous representation in $\dfrac{\mathscr{H}}{\mathcal{L}}$. $\dfrac{\mathscr{H}}{\mathcal{L}}$ being homeomorphic to S, this implies that $\mathscr{O}$ acts as a discontinuous group of mapping on the upper half plane S and thus we have the existence of a fundamental domain for $\mathscr{O}$ in S.

We shall now sketch a method of constructing of a fundamental domain for the group $\mathscr{O}$ in S. For the same we consider the upper half plane S as a metric space with the hyperbolic metric d, i.e., $d(x, y)$ is invariant under the group of hyperbolic motions.

Choose a point τ in S, which is not a fixed point for any $\varepsilon \neq 1 (\varepsilon \in \mathscr{O})$. Such a τ exists, for if not, then for $\tau \in S$ there would exist an $\varepsilon \in \mathscr{O}$ such that $\varepsilon(\tau) = \tau$. If $\tau \in M_c$, then $\varepsilon(\tau) = \tau \in M_c$. But such $\epsilon - s$ are infinite in number, a contradiction to Lemma 1.

Consider τ and $\varepsilon(\tau), \varepsilon \neq 1, \varepsilon \in \mathscr{O}$. Since $\tau \neq \varepsilon(\tau)$, we can draw the perpendicular bisector of the hyperbolic line joining τ and $\varepsilon(\tau)$. Then the hyperbolic plane S is divided into two half -planes, one consisting of points nearer to τ than $\varepsilon(\tau)$, the other vice-versa. Carrying out a similar construction for all $\varepsilon(\neq 1)$ of $\mathscr{O}$, we finally obtain a domain D, which is the intersection of all open half planes containing the point τ. In other words D consists of points which are nearer to τ than to any other $\varepsilon(\tau)$. **64** That D is non-empty follows from Lemma $1'$. We shall prove now that D is a fundamental domain (except for some boundary points) for $\mathscr{O}$ in S. Accordingly, we shall verify the following:



i) $D \cap \varepsilon D = (\phi)$ for every $\varepsilon(\neq 1) \in \mathscr{O}$. ($\varepsilon D$ denotes the image of D by means of the transformation ε).

ii) $\bigcup\limits_{\varepsilon \in \mathscr{O}} \overline{\varepsilon D} = S$.

Proof. i) If $D \cap \varepsilon D \neq (\phi)$ for some ε, there exists a $\sigma \in D \cap \varepsilon D$ so that σ and $\varepsilon^{-1}(\sigma) \in D$. Since ε preserves the hyperbolic distance, we have

$$d(\tau, \varepsilon^{-1}(\sigma)) < d(\varepsilon^{-1}(\tau), \varepsilon^{-1}(\sigma)) = d(\tau, \sigma)$$

and
$$d(\tau, \sigma) < d(\varepsilon(\tau), \sigma) = d(\tau, \varepsilon^{-1}(\sigma))$$

which are contradictory.

ii) Let ρ be any point of S. Then there exists at least one $\varepsilon(\tau)$ which is nearer to ρ than $\varepsilon'(\tau), \varepsilon' \neq \varepsilon$. For, if not, in a neighbourhood of ρ we would have an infinity of $\varepsilon(\tau)$ which contradicts Lemma 1′. Therefore ρ lies in εD. If $\varepsilon(\tau)$ and $\eta(\tau)$ are equidistant from ρ and are nearer to ρ than any other $\varepsilon'(\tau)\,(\varepsilon \neq \varepsilon, \eta)$ is from ρ, then ρ lies on the boundary of εD and ηD. Thus, we have the second assertion. □

Theorem 1. *In case Q is a division algebra, the fundamental domain D is bounded*

65 *Proof.* If not, there will be a boundary point τ of D on the real line (τ can be the point at ∞ as well). Let $\{\tau_i\}$ be a sequence of elements of D having τ as a limit point and choose a subsequence $\{\tau_{n_i}\}$ converging to τ. Then, by Lemma 2′, there exists an M_c for which $\varepsilon_{n_i}(\tau_{n_i}) \in M_c; \varepsilon_{n_i} \in \mathscr{O}$. Further $\varepsilon_{n_i}(\tau_{n_i}) \in \varepsilon_{n_i} D$ so that $\varepsilon_{n_i}(\tau_{n_i}) \in M_c \cap \varepsilon_{n_i} D$. But $M_c \cap \varepsilon D$ is non-empty only for a finite number of $\varepsilon \in \mathscr{O}$ from Lemma 1′, so that $\varepsilon_{n_i}(\tau_{n_i}) \in M_c \cap \varepsilon D$ for $n_i \geq n_o$ (say), for a fixed ε. □

Now, $\varepsilon_{n_i}(\tau_{n_i}) = \varepsilon(\lambda_i), \lambda_i \in D \implies \tau_{n_i} = \lambda_i$ since no two distinct points of D are equivalent. Therefore $\varepsilon_{n_i} = \varepsilon$.

Since $\tau_{n_i} \to \tau$, $\varepsilon(\tau_{ni}) \to \varepsilon(\tau)$. But $\varepsilon(\tau_{n_i}) \in M_c$ so that $\varepsilon(\tau) \in M_c$ for M_c is closed. This is contradictory to Lemma 4 for ε is a real transformation and τ is a real point.

Theorem 2. D has only a finite number of neighbours in either case whether Q is a matrix or division algebra.

From this it would follow that there are only a finite number of $\varepsilon_i D$, $\varepsilon_i \in \mathscr{O}$ which have boundary points in common with D. In other words there exists a fundamental polygon D with a finite number of sides.

Proof. Suppose D does not have a finite number of neighbours. Then it has an infinite number, i. e., D has an infinite number of sides $\{c_i\}$ (say). Let $\varepsilon_i(\tau)$ be the reflections of τ at these c_i respectively. Then we have to distinguish two cases. □

(i) $\{\varepsilon_i(\tau)\}$ have a finite limit point τ (say)

(ii) $\{\varepsilon_i(\tau)\}$ have a limit point at infinity (i. e., real).

In case (i) we choose a subsequence $\{\varepsilon_{n_i}(\tau)\}$ (say) which converges to τ. Then we may select a neighbourhood N of τ contained in some M_c. By the nature of τ, there exists an infinity of $\varepsilon_{n_i}(\tau)$ inside N and hence in M_c, which is contradictory to Lemma $1'$. **66**

In case (ii), we easily see that this arises only if Q is a matrix algebra, since D is bounded otherwise, by (b). Then $\mathscr{U}$ is a subgroup of the modular group Γ_1, so that if the coset decomposition given by $\Gamma_1 = \sum\limits_{i=1}^{n} \mathscr{U}.\varepsilon_i$ we may get a fundamental domain for $\mathscr{U}$ as $F = \sum\limits_{i=1}^{n} \varepsilon_i D_1, D_1$ being a fundamental domain for the modular group Γ_1. D and F are topologically equivalent and we know that F has only a finite number of sides and in fact only a finite number (say n) of real boundary points or parabolic cusps (a parabolic cusp is a fixed point of infinite order), since D_1 has ∞ as the only parabolic cusp.

5 Topological Properties of Units

3. We have already seen that the fundamental domain D has only a finite number of neighbours $\varepsilon_1 D_1, \ldots, \varepsilon_n D$ say. In this connection we have the

Theorem 1. *The units $\varepsilon_1, \ldots, \varepsilon_n$ generate the whole group $\mathscr{O}$.*

Proof. Let P be a point of D, and Q a point of εD. Join P and Q by an arc. This are is contained in M_c for some c, and M_c intersects only finite number of $\eta D' - s, \eta \in \mathscr{U}$, so that the are PQ is covered by a finite number of the $\eta D's$. Then the neighbours of any ηD are given by $\eta\varepsilon_i D, i = 1, \ldots, n$. □

67 We can go from D to εD as follows:

$$D, \varepsilon_{i_1} D, \varepsilon_{i_1}.\varepsilon_{i_2} D, \ldots, \varepsilon_{i_1}.\varepsilon_{i_2} \cdots \varepsilon_{i_k} D = \varepsilon D,$$

where $i_1, \ldots, i_k$ lie between 1 and n. This means $\varepsilon = \varepsilon_{i_1} \cdots \varepsilon_{i_k}$. (It may be remarked here that there exist certain relations between $\varepsilon_1 \ldots, \varepsilon_n$ which we will later obtain explicitly).

(i) In the case that Q is a division algebra the fundamental domain D is bounded, and by identifying the pairs of equivalent sides we obtain a closed surface which we denote by $S_{\mathcal{J}}$. This surface can also be seen to be the same as the upper half plane modulo $\mathscr{O}$, i, e,. $\mathscr{H}/\mathcal{L}$ modulo $\mathscr{O}$ which is the same as the space of double cosets $\mathscr{U}\xi\mathcal{L}$. It can also be seen that S is an infinite sheeted covering surface of $S_{\mathcal{J}}$

(ii) In the case when Ω is a matrix algebra, we have at most a finite number of parabolic cusps, and the surface $S_{\mathcal{J}}$ is obtained by identification of pairs of equivalent sides together with the adjunction of these cusps.

(iii) $S_{\mathcal{J}}$ as a manifold is orientable.

This follows from the fact that the $\varepsilon' s$ considered as hyperbolic motions have positive determinant.

(iv) *Canonical form for the surface*$S_{\mathcal{J}}$

In the fundamental domain D is denoted by $a_1 \cdots a_n$ where a_i are the sides, then we wish to obtain this in the canonical from $a_1 c_1 c_1^{-1} b_1 c_2 c_2^{-1} a_1^{-1} \cdots b_1^{-1} \cdots c_k c_k^{-1} \cdots a_g b_g^{-1}$ where a_1^{-1} is the side equivalent to a_1 with the opposite orientation.

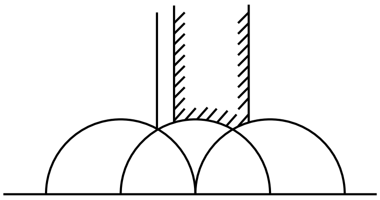


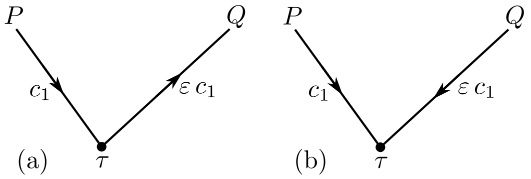
Figure a fundamental domain for the whole modular group in canonical form.

(There may be more than one pair $c_1 c_1^{-1}$ between a_1, b_1 and similarly 68 at other places also). The surface obtained from this reduced from is then called the canonical form for $S_{\mathcal{J}}$

The canonical from is obtained in two steps.

(i) Reduction of *elliptic vertices*. (i, e,. the vertices which are fixed points of elliptic transformations).

Let τ be a vertex which is a fixed point, i. e., τ is the intersection of a pair of equivalent sides, say c_1 and εc_1. We have the following two possibilities in the orientation of the sides.



Case (a) is ruled out since the orientation of εc_1 induced by the orientation of c_1 would be opposite to that already present in εc_1

We have then only the case (b), and in this case we may consider $c_1 (\varepsilon c)^{-1}$ as an inseparable unit.

(ii) Having dispensed with the case of elliptic vertices we now consider the polygon D as one without fixed points. We now employ the classical procedure to obtain canonical form $a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g$ $b_g a_g^{-1} b_g^{-1}$. [For this see C. L. Siegel, Ausgewahlte Fragen der Funktionentheorie, *I* (Göttingen). Pages 106 - 110, or Nevanlinna, " Uniformisierung", Chapter 7 §3].

69 However, in our case, there do not exist free sides even in the case of a matrix algebra.

Combining both (i) and (ii), the required canonical form is obtained.

We now have the

Theorem 2. *If ε_a is the transformation which takes a to the side $a^{-1}(\varepsilon_a \in \mathscr{U})$, we have the following relations:*

$$I\ \varepsilon_{b_g}\varepsilon_{a_g}^{-1}\varepsilon_{d_g}^{-1}\varepsilon_{a_g}\cdots\varepsilon_{b_1}\varepsilon_{a_1}^{-1}\varepsilon_{b_1}\varepsilon_{a_1}\cdot\eta_{c_k}\cdots\eta_{c_1}=1;$$

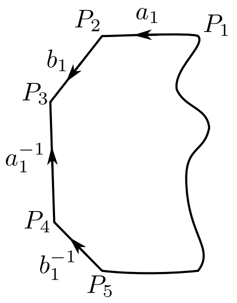
and $\eta_{c_i}^{n_i}=1$ for all i.

II(a) If Q is a division algebra, and if τ is a parabolic vertex, or cusp and if $\varepsilon_\tau(\tau)=\tau$, then ε_τ is of infinite order. Here $\eta_{c_i}=B_i^{-1}\varepsilon_{c_i}B_i$ and $B_i's$ are products of the ε_a' and $\varepsilon_b's$.

Proof. To prove I we split it into two cases:

Let no fixed points exists between P_1 and P_5. Consequently we have the following relations:

$$\varepsilon_{a_1}(P_1)=P_4, \varepsilon_{a_1}(P_2)=P_3,$$
$$\varepsilon_{b_1}(P_3)=p_4, \varepsilon_{b_1}(P_2)=P_5,$$
i, e,. $$\varepsilon_{a_1}^{-1}.\varepsilon_{b_1}^{-1}\varepsilon_{a_1}(P_1)=P_2$$
and hence $$\varepsilon_{b_1}.\varepsilon_{a_1}^{-1}\varepsilon_{b_1}^{-1}\varepsilon_{a_1}(P_1)=P_5.$$



Assuming that there are no fixed points, and proceeding as above, we obtain

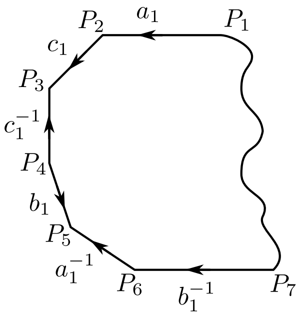
$$\varepsilon_{b_g}\varepsilon_{a_g}^{-1}\varepsilon_{b_g}^{-1}\varepsilon_{a_g}\cdots\varepsilon_{b_1}\varepsilon_{a_1}^{-1}\varepsilon_{b_1}^{-1}\varepsilon_{a_1}(P_1)=P_1,$$

and since P_1 is not a fixed point, we have **70**

$$\varepsilon_{b_g}\varepsilon_{a_g}^{-1}\varepsilon_{b_g}^{-1}\varepsilon_{a_g}\cdots\varepsilon_{b_1}\varepsilon_{a_1}^{-1}\varepsilon_{b_1}^{-1}\varepsilon_{a_1} = 1.$$

(ii) In the case that there exist elliptic vertices, we may suppose, for example, that one such lies between a_1 and b_1. In this case we have

$$\begin{aligned}
&\varepsilon_{a_1}(P_1) = P_6, \quad \varepsilon_{a_1}(P_2) = P_5,\\
&\varepsilon_{c_1}(P_3) = P_3, \quad \varepsilon_{c_1}(P_2) = P_4,\\
&\varepsilon_{b_1}(P_4) = P_7, \quad \varepsilon_{b_1}(P_5) = P_6,\\
\text{i.e.,}\quad &\varepsilon_{b_1}\varepsilon_{c_1}\varepsilon_{a_1}^{-1}\varepsilon_{b_1}^{-1}\varepsilon_{a_1}(P_1) = P_7.
\end{aligned}$$



□

Proceeding in this manner, we obtain

$$\varepsilon_{b_g}\varepsilon_{a_g}^{-1}\varepsilon_{b_g}^{-1}\varepsilon_{a_g}\cdots\varepsilon_{b_k}\varepsilon_{c_k}\varepsilon_{a_k}^{-1}\varepsilon_{a_k}^{-1}\varepsilon_{a_k}\cdots\varepsilon_{b_1}.\varepsilon_{c_1}\varepsilon_{a_1}^{-1}\varepsilon_{b_1}^{-1}\varepsilon_{a_1} = 1.$$

With an obvious notation, we write the above equation in the form

$$A_{k+1}\varepsilon_{c_k}A_k\varepsilon_{c_{k-1}}\cdots A_2\varepsilon_{c_1}A_1 = 1.$$

We may rewrite this as follows:

$$A_{k+1}\cdot A_k\cdot\cdot A_1(A_k\cdot\cdot A_1)^{-1}\varepsilon_{c_k}(A_k\cdot\cdot A_1)\cdot\cdot(A_2A_1)^{-1}\varepsilon_{c_2}(A_2A_1)\cdot A_1^{-1}\varepsilon_{c_1}A_1 = 1.$$

Let $\eta_{c_i} = (A_i A_{i-1} \cdot \cdot A_1)^{-1} \varepsilon_{c_i} (A_i \cdot \cdot A_1)$, then the above relation can be written in the form

$$\varepsilon_{b_g} \varepsilon_{a_g}^{-1} \varepsilon_{b_g}^{-1} \varepsilon_{a_g}{}^{\vdots} \varepsilon_{b_1} \varepsilon_{a_1}^{-1} \varepsilon_{b_1}^{-1} \varepsilon_{a_1} \eta_{c_k} \cdots \eta_{c_1} = 1.$$

Let now the transformations $\varepsilon_{c_1}, \ldots, \varepsilon_{c_k}$ have $\tau_1, \ldots, \tau_k$ as their fixed points (we suppose that no τ_i is a cusp). We can then find a neighbourhood of τ_i which is contained in some M_c. If now ε_{c_i} is not of finite **71** order, then $\varepsilon_{c_i}, \varepsilon_{c_i}^2, \ldots$, are all distinct, and $\varepsilon_{c_i}^n(\tau_i) = \tau_i$ for all n, and this contradicts Lemma 1. Hence ε_{c_i} is of finite order n_i, and then we have

$$\varepsilon_{c_1}^{n_1} = \cdots = \varepsilon_{c_k}^{n_k} = 1.$$

From this equation it follows that $\eta_{c_1}^{n_1} = \cdots = \eta_{c_k}^{n_k} = 1$. (b) Since the above argument breaks down in the case of a parabolic vertex or a rational fixed point $\tau_o, (\tau_o \neq 0, \infty)$, we cannot conclude that ε_c which fixes τ_o is of finite order. We now prove that it is necessarily of infinite order.

Since $\tau_o \neq \infty$, we obtain a transformation η such that $\eta(\tau_o) = \infty$. We only have to take $\eta = \begin{pmatrix} -1/\tau_o & 0 \\ 1 & -\tau_o \end{pmatrix}$.

Then $\eta \varepsilon_c \eta^{-1} = \varepsilon'_c$ has $\eta(\tau_o) = \infty$ as fixed point ε'_c must then necessarily have the form $\varepsilon'_c = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, and on multiplication by $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$, we may assume that $a > 0, d > 0$.

Further $\varepsilon'_c \neq 1$, for otherwise $\varepsilon_c = 1$. Suppose $\varepsilon_c^n = 1$. Then $\varepsilon_c'^n = 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^n & B_n \\ 0 & d^n \end{pmatrix}$, i. e., $a^n = d^n = 1$, or $a = d = 1$, for $a > 0$ and $d > 0$. Now $B_n = nb = 0$ implies that $b = 0$, or $\varepsilon'_c = 1$ which is a contradiction.

Theorem 3. (1) *For any two $\varepsilon_{c_i}, \varepsilon_{cj}, \eta^{-1} \varepsilon_{c_i} . \eta \neq \varepsilon_{cj}$ for any η.*

(2) *If ε has the fixed point τ, then there exists an η such that*

$$\eta^{-1} \varepsilon \eta = \varepsilon_{c_i} \textit{ for some } i.$$

72 *Proof.* 1. $\eta^{-1}\varepsilon_{c_i}\eta$ has $\eta^{-1}(\tau_i)$ as fixed point, and ε_{c_j} has τ_j as fixed point, and in order to prove 1, we need only to show that $\eta^{-1}(\tau_i) \neq \tau_j$. But this since the elliptic vertices τ_i and τ_j belong to the same fundamental domain, and hence they cannot be equivalent.

2. Let η^{-1} be the transformation which takes τ into the fundamental domain; then since $\varepsilon(\tau) = \tau, \eta^{-1}\varepsilon\eta$ has $\eta^{-1}(\tau)$ as fixed point, i. e., it leaves a point of the fundamental domain fixed, this means that $\eta^{-1}\varepsilon\eta = \varepsilon_{c_i}$ for some i.

□

6 The Hyperbolic Area of the Fundamental Domain

(We shall see from the calculation that the hyperbolic area is independent of the choice of the fundamental domain).

4. Let Q be an indefinite quaternion algebra over the rational number field k. Let $\mathcal{J}$ be an order in Q, with class number 1 and we suppose that there exists at least one unit ε of $\mathcal{J}$ such that $n(\varepsilon) = -1$. This allows us write any integral ideal $\mathfrak{M} = \mathcal{J}\alpha$ and where $n(\alpha) > 0$, for if $n(\alpha) < 0$, we may write $\mathcal{J}\alpha = \mathcal{J} \cdot \epsilon\alpha$ and $n(\varepsilon\alpha) > 0)0)$.

The zeta-function of the order $\mathcal{J}$ is now given by

$$\zeta(s) = \sum_{\mathfrak{M}} \frac{1}{(n(\mathfrak{M}))^{2s}} = \sum_{n(\alpha)\geq 1} \frac{1}{(n(\alpha))^{2s}}$$

(the summation extending over all $\alpha \in \mathcal{J}$ such that no two α-s are left associate with to the unit group a of $\mathcal{J}$).

We shall now consider an order $\mathcal{J}$ of the type (q_1, q_2). Then $\mathcal{J}$ has 73 class number 1 and contains a unit of norm -1, namely $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (in case $q_1 = 1$). For such an order $\mathcal{J}$, we saw that the zeta-function was given by (§2, 10, Zeta -function of an Order).

$$\zeta(s) = \zeta_0(2s)\,\zeta_0(2s-1)\prod_{p|q_1}(1 - p^{1-2s})\prod_{p|q_2}(1 + p^{1-2s})$$

where $\zeta_0(s)$ is the Riemann zeta - function. Then $\zeta(s)$ has a simple pole at $s = 1$ with residue $\frac{\pi^2}{12}\prod_{p|q_1}\left(1-\frac{1}{p}\right)\prod_{p|q_2}\left(1+\frac{1}{p}\right)$. Since we have $\prod_{p|q_1q_2} p = \sqrt{|D|}$ (by Lemma 3 of §3), the above may be written as $\underset{s\to 1}{\mathrm{Lt}}(s-1)\zeta(s) = \frac{\pi^2}{12\sqrt{|D|}}\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1)$. We shall now try to obtain this residue is an alternative manner.

Let $\mathcal{J} = [L_1 \ldots L_4]$. If $\xi \in Q$, then $\xi = L_1x_1 + \cdots + L_4x_4X_i$, rational. We can look upon ξ as a point $(x_1, \ldots, x_4)$ of R_4, the Euclidean space of four dimensions. Then all the lattice points of R_4 correspond to elements of $\mathcal{J}$. By the above correspondence, every unit η of $\mathcal{J}$ such that $n(\eta) = 1$ gives rise to a linear transformation of the space R_4 and obviously this group of transformations is discontinuous on R_4. Hence we may construct a fundamental domain F for Q in R_4. This is also be obtained from a fundamental domain D we constructed for $\mathfrak{Q}$ in the upper half, in §4, by the inverse mapping φ^{-1}; $(\varphi : R_4 \to S)$.

F is a cone and in case Q is a division algebra, this fundamental domain F is of finite volume. Though in the case matrix algebra, F stretches out to infinity, the volume is $< \infty$ in both cases.

74 From the definition of the fundamental domain F, we may write

$$\zeta(s) = \sum_{n(\xi)\geq 1} \frac{1}{(n(\xi))^{2s}}$$
$$\xi \in \text{ lattice points of } F$$

We shall now prove the following:

$$\underset{s\to 1}{\mathrm{Lt}}(s-1)\zeta(s) = \underset{s\to 1}{\mathrm{Lt}}(s-1)\underset{\substack{n(\xi)\geq 1\\ F}}{\int\cdots\int}\frac{dx_1\ldots dx_4}{(n(\xi))^{2s}}$$

(i) Let Q be a division algebra.

Then the fundamental domain F is bounded by a finite number of smooth surfaces and let $S = F \cap n(\xi) \leq 1$. If S_t is the domain obtained by expanding S in the ratio $1 : t^{1/4}$, i.e., $S_t = (n(\xi) \leq \sqrt{t}) \cap F$, then we have, by a classical theorem, if z_t denotes the number of lattice points of

S_t (for S_t is compact), then

$$\operatorname*{Lt}_{s\to 1}\frac{Z_t}{t} = \underset{n_F(\xi)\leq 1}{\int\cdots\int} dx_1\ldots dx_4 = \text{ Volume of } S.$$

[Refer Weber, *Lehrbuch der Algebra*, II, P, 712]. But by a theorem of Dirichlet, if $(T(\sqrt{t}))$ denotes the number of integral ideals with norm $\leq\sqrt{t}$, then $\operatorname*{Lt}_{t\to\infty}\frac{T(\sqrt{t})}{t} = \operatorname*{Lt}_{s\to 1}(s-1)(\zeta(s))$. [Refer, Ibid, P. 724].

Now it is easily seen that $T(\sqrt{t}) = z_t$ so that combining the above two, we obtain the following:

$$\operatorname*{Lt}_{s\to 1}(s-1)\zeta(s) = \underset{n(\zeta_F)\leq 1}{\int\cdots\int} dx_1\cdots dx_4.$$

By a transformation of co-ordinates from $(x_1\ldots x_4)$ to (x,y,t,φ) we can prove that the above integral reduces to

$$\underset{t^2\leq 1}{\int\cdots\int} f dxdy\, d\phi. t^3 dt = \left(\int f(x,y,\varphi)dxdyd\varphi\right)\frac{1}{4}$$

The same transformation when applied to $\underset{n(\xi)_F\geq 1}{\int\cdots\int}\frac{dx-1\ldots x_4}{(n(\xi))^{2s}}$ leads 75 to $\underset{t^2\geq 1}{\int\cdots\int} f(x,y,\varphi).\frac{t^3}{t^{4s}}dxdy, d\varphi dt$ so that

$$\begin{aligned}\operatorname*{Lt}_{s\to 1}(s-1)\underset{n(\xi)_F\geq 1}{\int\cdots\int}\frac{dx_1\ldots dx_4}{(n(\xi))^{2s}} &= \left(\int f(x,y,\varphi)dxdyd\varphi\right)\operatorname*{Lt}_{s\to 1}(s-1)\int_{t^2\leq 1}\frac{dt}{t^{4s-3}}\\ &= \left(\int fdxdyd\varphi\right)\operatorname*{Lt}_{s\to 1}\frac{(s-1)}{4s-4}\\ &= \left(\frac{1}{4}\int fdxdyd\varphi\right)\end{aligned}$$

where $f(x, y, \varphi)$ does not interest us here.

$$= \underset{n(\xi)_F \leq 1}{\int \cdots \int} dx_1 \ldots dx_4$$

$$= \underset{s \to 1}{\mathrm{Lt}} (s-1)\zeta(s)$$

(ii) In the case of Q being a matrix algebra, the same considerations are not valid so that we consider truncated domains $F_c = \varphi^{-1}(D_c)$ where $D_c = \{\tau : 0 < \dfrac{1}{c} \leq \operatorname{Im} \tau \leq c\} \cap D$ and then make $c \to \infty$. D_c and $F_c \cap n(\xi) \leq 1$ are compact.

Let $\zeta^c(s)$ be the zeta-function corresponding to the truncated domain F_c.

i.e., $$\zeta^c(s) = \sum_{\substack{n(\xi) \geq 1 \\ \xi \in \text{ lattice points of} E_c}} \frac{1}{(n(\xi))^{2s}}$$

Now, applying (i) for the function $\zeta^{(c)}(s)$,

$$\underset{s \to 1}{\mathrm{Lt}} (s-1)\zeta^{(c)}(s) = \underset{s \to 1}{\mathrm{Lt}} (s-1) \underset{n(\xi)_{F_c} \geq 1}{\int \cdots \int} \frac{dx_1 \ldots dx_4}{(n(\xi))^{2s}}$$
$$= \underset{s \to 1}{\mathrm{Lt}} (s-1) L_c (say).$$

76 $\zeta^{(c)}(s)$ and L_c being monotone increasing with the limits existing uniformly in s as $c \to \infty$, in the equality $\underset{c \to \infty}{\mathrm{Lt}} \underset{s \to 1}{\mathrm{Lt}} (s-1)\zeta^{(c)}(s) = \underset{c \to \infty}{\mathrm{Lt}} \underset{s \to 1}{\mathrm{Lt}} (s-1)L_c$, the limits can be interchanges on both sides, so that

$$\underset{s \to 1}{\mathrm{Lt}} (s-1) \underset{c \to \infty}{\mathrm{Lt}} \zeta^{(c)}(s) = \underset{s \to 1}{\mathrm{Lt}} (s-1) \underset{c \to \infty}{\mathrm{Lt}} L_c.$$

$$\underset{c \to \infty}{\mathrm{Lt}} L_c = \underset{c \to \infty}{\mathrm{Lt}} \underset{n(\xi_{Fc}) \geq 1}{\int \cdots \int} \frac{dx_1 \ldots dx_4}{(n(\xi))^{2s}}$$
$$= \underset{n(\xi_F) \geq 1}{\int \cdots \int} \frac{dx_1 \ldots dx_4}{(n(\xi))^{2s}}$$

and $\quad \underset{c\to\infty}{\text{Lt}}\, \zeta^{(c)}(s) = \zeta(s).$

Hence we have, finally

$$\underset{s\to 1}{\text{Lt}}\,(s-1)L(s) = \underset{s\to 1}{\text{Lt}}\,(s-1)\underset{n(\xi)_F\geq 1}{\int\cdots\int}\frac{dx_1\ldots dx_4}{(n(\xi))^{2s}}$$

Our problem now is to evaluate the integral

$$\underset{s\to 1}{\text{Lt}}\,(s-1)\underset{n(\xi_F)\geq 1}{\int\cdots\int}\frac{dx_1dx_2dx_3dx_4}{n(\xi)^{2s}}$$

Any element $\xi\in Q$ can be written as

$$\xi = L_1x_1+\cdots+L_4x_4 \cong \begin{pmatrix}\xi_{\underline{1}} & \xi_{\underline{2}}\\ q\xi_2 & \xi_1\end{pmatrix} = \begin{pmatrix}y_{11} & y_{12}\\ y_{21} & y_{22}\end{pmatrix}(say).$$

Making the change of coordinates from $x_1,\ldots,x_4$ to $y_{11},\ldots,y_{22}$ we obtain

$$dx_1\cdots dx_4 = \left|\frac{\partial(x_i)}{\partial(y_ik)}\right|.dy_{11}\cdots dy_{22}.$$

If ξ is an integer and $2n(\xi) = \sum\limits_{i,k} f_{ik}x_ix_k$, then $|f_ik| = D(\tau)$, where $\mathcal{J} = [L_1,\ldots,L_4]$.

But $2n(\xi) = 2(y_{11}y_{22}-y_{21}y_{12})$ in the new coordinate system, and the determinant of this quadratic form is 1, and $1 = \left|f_{ik}\right|\left|\frac{\partial(x_i)}{\partial(y_{ik})}\right|^2$. This 77 means that $\left|\frac{\partial(x_i)}{\partial(y_{ik})}\right| = \frac{1}{\sqrt{|D|}}$.

We may now write

$$\underset{s\to 1}{\text{Lt}}\,(s-1)\zeta(s) = \frac{1}{\sqrt{|D|}}\underset{n(\xi_F)\geq 1}{\int\cdots\int}\frac{dy_{11}\cdots dy_{22}}{n(\xi)^{2s}};\, n(\xi) = y_{11}y_{22}-y_{21}y_{12}.$$

We now make another change of coordinates from which it is easier to compute the value of the integral. Consider the transformation

$$\begin{pmatrix}y_{11} & y_{12}\\ y_{21} & y_{22}\end{pmatrix}\to\tau = x+iy = \frac{y_{11}i+y_{12}}{y_{21}i+y_{22}}$$

Since $n(\xi) > 0$, we have $\mathrm{Im}(\tau) > 0$. Now

$$x + iy = \frac{(y_{12}y_{22} + y_{11}y_{21}) + i(y_{11}y_{22} - y_{21}y_{12})}{(y_{21}^2 + y_{22}^2)}$$

that is, $$x = \frac{y_{11}y_{22} + y_{21}y12}{y_{21}^2 + y_{22}^2}; y = \frac{y_{11}y_{22} - y_{12}y_{21}}{y_{21}^2 + y_{22}^2} = t^2 \text{ (say)}$$

that is, $$y_{21}^2 + y_{22}^2 = \frac{t^2}{y}.$$

Now put

$$y_{21} = \frac{-t}{\sqrt{y}} \sin\varphi, Y_{22} = \frac{-t}{\sqrt{y}} \cos\varphi.$$

Solving for y_{11}, y_{12} from the simulations equations

$$y_{11}\cos\varphi + y_{12}\sin\varphi = t\sqrt{y},$$
$$-y_{11}\sin\varphi + y_{12}\cos\varphi = \frac{tx}{\sqrt{y}},$$

we have

$$y_{12} = t\sqrt{y}\sin\varphi + \frac{tx}{\sqrt{y}}\cos\varphi,$$
$$y_{11} = t\sqrt{y}\cos\varphi + \frac{tx}{\sqrt{y}}\sin\varphi.$$

78 Writing these equations in the matrix form, we have

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \tag{1}$$

We denote the Jacobian $\left|\frac{\partial(y_{ik})}{\partial(x, y, \varphi, t)}\right|$ of the transformation by $J(x, y, \varphi, t)$. $J(x, y, \varphi, t)$. has the following three properties

1. $J(x, y, \varphi, t) = t^3 J_1(x, y, \varphi)$.

2. $J_1(x, y, \varphi) = J_1(x, y)$.

3. $J(x, y)dxdy = \varrho_1 d\omega$, where $d\omega$ is the $d\omega$, where is the hyperbolic are element, and ϱ_1 is a constant independent of the algebra.

That property 1 is true is seen by direct computation.

As for 2, multiplying (1) on the right by $\begin{pmatrix} \cos\psi & \sin\psi \\ -\sin\psi & \cos\psi \end{pmatrix}$ the y_{ij}'s undergo a linear transformation with determinant 1, and we have

$$J_1(x, y, \varphi + \psi) = J_1(x, y, \varphi)$$

for every ψ. Hence $J_1(x, y) = J_1(x, y, \varphi)$.

To prove 3, it is enough to show that the are element $J_1(x, y)dxdy$ is invariant with respect to all hyperbolic motions.

Let τ be replaced by $\dfrac{z_{11}\tau + z_{12}}{z_{21}\tau + z_{22}} = h(\tau)$, say, where $z_{11}, \ldots, z_{22}$ are real and $\begin{vmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{vmatrix} = 1$. The y_{ik} then undergo a linear transformation of determinant 1. Therefore $dy_{11} \cdots dy_{22} = Jdxdyd\varphi dt$ is invariant. Hence

$$\operatorname*{Lt}_{s\to 1}(s-1)\zeta(s) = \operatorname*{Lt}_{s\to 1}(s-1)\frac{1}{\sqrt{|D|}}\int\cdots\int_{t_F^2\leq 1}\frac{J(x, y)dxdydyd\varphi dt^2}{t^{4s}}\cdot\frac{t^2}{2}$$

Making the transformation $t^2 \to t$, we see that the above equals 79

$$\operatorname*{Lt}_{s\to 1}(s-1)\frac{\rho_1}{2\sqrt{|D|}}\int_1^\infty\frac{dt}{t^{2s-1}}\int_0^{2\pi}d\mathscr{S}\int_D\int d\omega,$$

where $D$is the fundamental domain in the upper half plane obtained as the image of F under the map (1). Now

$$\operatorname*{Lt}_{s\to 1}(s-1)\frac{\varrho_1\pi}{2(s-1)\sqrt{|D|}}\int_D\int d\omega = \frac{\rho_1\pi}{s\sqrt{|D|}}\int_D\int d\omega.$$

But the left hand side being the residue of the zeta-function at $s = 1$ its value is given by

$$\frac{\pi^2}{|2\sqrt{|D|}}\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1)$$

and hence $$\varrho\int\int_D d\omega=\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1)$$

where $\varrho=\dfrac{6\rho_1}{\pi}$.(From this it follows that the hyperbolic area of the fundamental domain is independent of the choice of the fundamental domain).

5. From the above expression for the area, we will find a relation between the genus and the hyperbolic are of D using the Gauss Bonnet formula.

The Gauss-Bonnet formula can be stated as follows; For a simply connected domain D in the plane bounded by a closed curve C composed of k smooth arcs making at the vertices exterior angles $\alpha_1,\ldots,\alpha_k$,

$$\int\int_D d\omega=\int_c Kds-2\pi+\sum_{i=1}^k\alpha_i;$$

80 where K represents the geodesic curvature of the arcs. Applying this formula to the fundamental polygon D in the hyperbolic plane, we see that

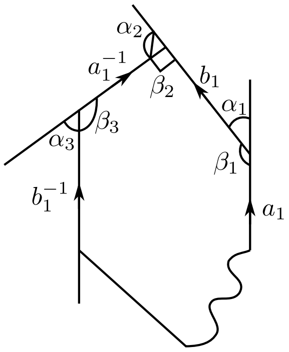
$$\int\int_D d\omega=\sum_{i=1}^k\alpha_i-2\pi.$$

for $\int_C Kds=0$ since C consists of pair of equivalent sides oppositely oriented.

We have now to consider the following two cases:

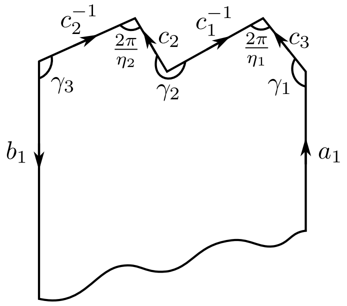
1. D has no elliptic vertices. Since the angles $\beta_1,\ldots$ together make up a full neighbourhood of one point in the closed surface $S_{\mathcal{J}}$ obtained by identification of pairs of equivalent sides, we have $\sum\limits_i\beta_i=2\pi$, and here $k=4g$, hence we obtain

$$\begin{aligned}[H]\int\int_D d\omega&=\sum_i(\pi-\beta_i)-2\pi\\&=4g\pi-4=\pi(g-1).\end{aligned}$$



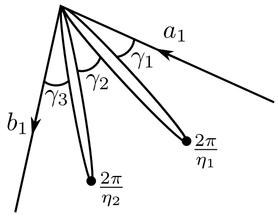
2. *D* has elliptic varieties.

Let the number of elliptic verities between a_1 and b_1 be h_1, between a_2 and b_2 be h_2, and so on. Here is included the case in which some of the elliptic vertices are parabolic cusps. In this case $(\pi - \beta_1)$ must be replace by



$$(\pi - \gamma_1) + \left(\pi - \frac{2\pi}{n_1}\right) + (\pi - \gamma_2) + \left(\pi - \frac{2\pi}{n_2}\right) + \cdots + (\pi - r_{h_1+1})$$
$$= \pi - \sum_{i=1}^{h_1+1} \gamma_i + 2\pi \sum_{i=1}^{h_1} \left(1 - \frac{1}{n_i}\right)$$

where $n_1, \ldots$ are the orders of the substitutions leaving the respective **81**
vertices fixed. In the case of a parabolic cusp, the angle $\dfrac{2\pi}{n_i}$ has to be replaced by 0.



We have therefore

$$\int\int_D d\omega = \sum_{h=h_1,h_2,\ldots}\left(\pi - \sum_{i=1}^{h+1}\gamma_i\right) + 2\pi\sum_{\text{e.v.}}\left(1-\frac{1}{n_1}\right)$$
$$= 4\pi(g-1) + 2\pi\sum_{\text{e.v.}}\left(1-\frac{1}{n_i}\right)$$

where e.v. stands for elliptic vertices including those which are parabolic cusps in which case $\dfrac{1}{n_i}$ has to be replaced by 0. In the final form, we obtain

$$\rho\iint_D d\omega = \rho\left\{4\pi(g-1) + 2\pi\sum_{e.v.}\left(1-\frac{1}{n_i}\right)\right\}$$
$$= \prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1).$$

Since the constant ρ is independent of the algebra, we can obtain its value by considering the particular case where Q is a matrix algebra, $\mathscr{J} = \begin{pmatrix}\mathscr{O} & \mathscr{O}\\ \mathscr{O} & \mathscr{O}\end{pmatrix}$, and then $\mathscr{O}$ is the modular group. Here $q_1 = 1, q_2 =$ 1and D is the fundamental domain for the modular group. The elliptic vertices are i, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, ∞ (∞ begin a parabolic cup). The orders of the corresponding hyperbolic motions are $2, 3, \infty$ respectively, Further $g = 0$, since the closed surface $s_{\mathscr{J}}$ is here the sphere. Hence we obtain

$$\rho\left\{-4\pi + 2\pi\left(1-\frac{1}{2}+1-\frac{1}{3}+1\right)\right\} = 1, \text{ or } \rho = \frac{3}{\pi}.$$

Thus we arrive the complete formula

$$g = 1 - \frac{1}{2}\left(\sum_{\text{e.v.}}\left(1 - \frac{1}{n_i}\right) + \sum_{\text{parabolic cusps}} 1 + \frac{1}{12}\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1)\right).$$

Chapter 3

Theory of Correspondences

7 Correspondences

1. In this article we shall define so - called correspondences of Riemann surfaces, and study a class of special correspondences of the surfaces $s_{\mathcal{J}}$ to be defined below. They are certain operators and form a ring. In §7 We shall study various representations of this ring. These representations are of topological, function theoretical or of arithmetical nature. We shall determine the traces of some of them and this will load to several interesting arithmetical results. **82**

Let S and S' be two closed Riemann surfaces and let f be an analytic (algebraic) mapping. in general multi-valued, of S onto S'. If P is a point of S, then $f(P)$ is a set of points of S, then $f(P)$ is a set of points $P'_1, \ldots, P'_d$,., of S', said to this f we associate the correspondence which we may write as

$$C : C(P) = P'_1 + \cdots + P'_d, (\text{ formal sum };$$

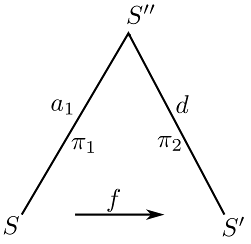
where it may happen that some P'_i is equal to some P'_j.

If for $P' \in S'$, $f^{-1}(P')$ consists of $P_1, P_2, \ldots, P_d$, then f^{-1} gives rise to the correspondence

$$C^* : C^*(P') = P_1 + \cdots P_d.$$

We may view the correspondence as follows:

Let S'' be the Riemann surface of the multi-valued function f, then S'' is compact and is covering surface of both S and S' with d' and d sheets respectively. Let π_1 and π_2

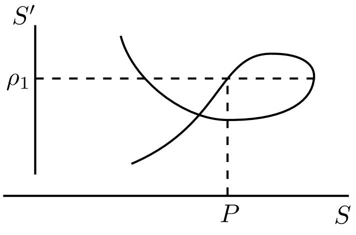


83 be the corresponding projection maps. Then $f(P) = \pi_2\pi_1^{-1}(P)$ is the set of points $P'_1, \ldots P'_d$, and similarly $f^{-1}(P') = \pi_1\pi_2^{-1}(P')$. (It is easily seen that both f and f^{-1} are onto).

As an example of a correspondence we consider the following figure:

Here $d' = 2$, $d = 3$.

In the case that S' is homomorphic to S, we show that we can make the set of correspondences of S onto itself into a ring. So let ν be a homomorphism of S' on S, i.e, $S'^{\nu} = S$. If C is a correspondence between S and S' defined by $C(P) = P'_1, + \ldots + P'_{d'}$ then the correspondence $\nu C : S \to S$ is defined by



$$C(P) = (P'_1)^{\nu} + \cdots + (P'_{d'})^{\nu}.$$

For such correspondence we can can define addition, (in fact, addition, can be such defined for any two correspondences between S and

S') and multiplication in the following way: Let D_1, D_2 be two correspondences from $S \rightarrow S$. Then we define $(D_1 + D_2)(P) = D_1(P) + (D_2)(P), (D_1D_2)(P) = D_1(D_2(P))$, and for any rational integer n, (nD) $(P) = n.D(P)$ so that $(D_1 - D_2) = D_1 + (-1)D_2)$. There exists a zero correspondence, it maps each P on the empty se, and the unit element is the identity map. Multiplication is associative and distributive with respect to addition, so that the correspondence of S on S form a ring $\mathscr{R}$.

We now prove the existence of an involution in $\mathscr{R}$. Consider the mapping $C \rightarrow C^*$ which is a $1 - 1$ mapping of $\mathscr{R}$ onto $\mathscr{R}$. This mapping has the properties **84**

1. $(C_1 + C_2)^* = C_1^* + C_2^*$

2. $(C_1C_2)^* = C_2^*C_1^*$

3. $C^{**} = C$,

so that it is an involution in $\mathscr{R}$.

(This involutorial anti-automorphism is named after Rosati.)

2. We will now study the correspondence from $S_{\mathcal{J}} \rightarrow S_{\mathcal{J}}$, where $\mathcal{J}$and $\mathcal{J}'$ are orders in Q/k. (For explanations and notations, see §5). To be precise, let Q be an indefinite quaternion algebra over the rational number field k, and $\mathcal{J}$ an order in Q. Let $Q_{\mathcal{J}}$ denote the proper unit group of $\mathscr{J}$, then $Q_{\mathcal{J}} = \left\{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \varepsilon, \quad n(\varepsilon) = 1\right\}$, where $\alpha, \ldots, \delta$ lie in a real quadratic extension of k which is isomorphic to a subfield of Q. Each element ϵ of $Q_{\mathcal{J}}$ gives rise to a linear transformations $z \rightarrow \varepsilon(z), \varepsilon \in Q_{\mathcal{J}}$.

Remark. Since $\pm\varepsilon \in Q_{\mathcal{J}}$ give rise to the same element of $\Gamma_{\mathcal{J}}, \Gamma_{\mathcal{J}}$ is not a faithful representation of $Q_{\mathcal{J}}$. It can be proved that $\Gamma_{\mathcal{J}}$ is a faithful representation $Q_{\mathcal{J}}/_{(\pm E)}$.

The closed Riemann surface $S_{\mathcal{J}}$ associated with the group Q_J can be considered as the compactifications of the quotient space of the upper half plane modulo $\Gamma_{\mathcal{J}}$, i.e., $S_{\mathcal{J}} : \{\Gamma_{\mathcal{J}}.z, z$ in the upper half plane $\}$. Similarly if $\mathcal{J}'$ is another order, we have the surface $S_{\mathcal{J}'}$, and we will consider some special correspondences between $S_{\mathcal{J}}$ and $S_{\mathcal{J}}$. **85**

Since $\mathscr{O}_{\mathcal{J}} \cap \mathscr{O}_{\mathcal{J}'}$ is of finite index in both $\mathscr{O}_{\mathcal{J}}$ and $\mathscr{O}_{\mathcal{J}'}$ (for a proof under similar situation, see *P*.46). say d' and d, the same holds for $\Gamma_{\mathcal{J}}$ and $\Gamma_{\mathcal{J}'}$. Consequently we have the coset decompositions.

$$\Gamma_{\mathcal{J}} = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}'}\epsilon_i = \sum_{i=1}^{d} (\Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}'})\varepsilon'_i$$

Let $S_{\mathcal{J}\cap\mathcal{J}'}$ be the surface associated with $\mathscr{O} \cap \mathscr{O}_{\mathcal{J}}$, so that $S_{\mathcal{J}\cap\mathcal{J}'}$: $\{\Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}'}z\}$, and $S_{\mathcal{J}} \cap \mathcal{J}'$, is a covering surface of both $S_{\mathcal{J}}$ and $S_{\mathcal{J}'}$ sheets d' and d respectively. Then the points lying over $\Gamma_{\mathcal{J}}.z$ are precisely

$$\Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}'}.z_i, z_i = \varepsilon_i(z), i = 1, \ldots, d'.$$

The correspondence $C_{S_{\mathcal{J}}\to S_{\mathcal{J}'}}$ is defined as

$$C_{S_{\mathcal{J}}\to S_{\mathcal{J}'}}(\Gamma_{\mathcal{J}}.Z) = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}'}z_i$$

C^* is given by

$$C^*_{S_{\mathcal{J}'}\to S_{\mathcal{J}}}(\Gamma_{\mathcal{J}'} \cdot z) = \textstyle\sum_{i=1}^{d} \Gamma_{\mathcal{J}} \cdot \varepsilon'_i(z).$$

$$\begin{tikzcd} & S_{\tau\cap\tau''} \arrow[dl, dash, "d'"'] \arrow[dr, dash, "d"] & \\ S_{\tau} & & S_{\tau'} \end{tikzcd}$$

We now restrict our attention to orders $\mathcal{J}', \mathcal{J}$ such that $\mathcal{J}' \cong \mathcal{J}$ so that there exists $\nu \in Q$ such that $\mathcal{J} = \nu^{-1}\Gamma_{\mathcal{J}}\nu$. Then $\Gamma_{\mathcal{J}'} = \nu^{-1}\Gamma_{\mathcal{J}}\nu$ and $C_{S_{\mathcal{J}}\to\mathcal{J}'}(\tau_{\mathcal{J}.Z})z = \sum_{i=1}^{d} \nu^{-1}\Gamma_{\mathcal{J}^{\nu}}.Z_i$, and

$$\nu C_{S_{\mathcal{J}}} \to S_{\mathcal{J}'}(\Gamma_{\mathcal{J}}.z) = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}} \cdot \nu\epsilon_i z,$$

since $\Gamma_{\mathcal{J}}.\nu\epsilon_j = \Gamma_{\mathcal{J}} \cdot \nu\varepsilon_i, \varepsilon, \varepsilon \in \Gamma_{\mathcal{J}}$ (for from a later lemma, it would
86 follow that $\mathcal{J}\nu\varepsilon_i\varepsilon = \mathcal{J}\nu\varepsilon_j$) we can look upon $\nu C_{S_{\mathcal{J}} \to S_{\mathcal{J}'}}$ as a correspondence of $S_{\mathcal{J}}$ with itself, i.e.,

$$C(\Gamma_{\mathcal{J}} \cdot z) = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}} \cdot \nu\varepsilon_i \cdot \Gamma_{\mathcal{J}} \cdot z,$$

so that $C = \sum\limits_{i=1}^{d'} \Gamma_{\mathcal{J}} \cdot \nu\varepsilon_i$ may be considered as an operator on $S_{\mathcal{J}}$.

Therefore correspondences can be written as left operators

3. Before defining modular correspondences, we shall prove an important lemma, which will enable us to pass from the topological aspect of correspondences to its algebraic counterpart. An element $\nu \in \mathcal{J}$ is said to be *primitive* if there exists no rational integer $t > 1$ such that $\dfrac{\nu}{t} \in \mathcal{J}$.

Lemma. *Let $\mathcal{J}$ be an order of the type (q_1, q_2) and $n\chi | q_1, q_2$. If $\mathcal{J}' = \nu^{-1}\mathcal{J}\nu$ and $\Gamma_{\mathcal{J}} = \sum\limits_{i=1}^{d} \Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}}.\varepsilon_i$, then all primitive (integral) left ideals with norm n are of the form $\mathcal{J}\nu\varepsilon_i (i = 1$ to $d')$*

Proof. For such an order $\mathcal{J}$, the class number is 1, so that every ideal is principal. □

We shall not prove the lemma in its most general form but for simplicity, assume that there are no characteristic primes, i.e., $q_1 = 1$. We may then take the order $\mathcal{J} = \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ q_2\mathcal{O} & \mathcal{O} \end{pmatrix}$ (q_2 being square free).

Let μ be a primitive left ideal for the order $\mathcal{J}$ with norm n, so that in the reduced form, $\mu = \mathcal{J}\begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix}$; $n_1, n_3 = n$ $n_1 > 0$ and $n_3 > 0$, n_2 is reduced modulo n_3, μ being primitive $(n_1, n_2, n_3,) = 1$.

For our lemma, it is enough to show that there exists a unit ε such that 87

$$\varepsilon \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \varepsilon_i; \text{For } \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$$

being a primitive element with norm $n, \varepsilon' \nu = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \epsilon_j$ for some ε' and ε_j, so that $\mathscr{J} \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix} = \mathscr{J} \nu \varepsilon_j^{-1} \cdot \varepsilon_i$. In fact, we shall only prove that there exists units $\varepsilon, \eta, \in \Gamma_{\mathscr{J}}$ such that $\varepsilon \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \eta$ for, then writing $\eta = \eta_\circ \varepsilon_i, \eta_\circ \in \Gamma_{\mathscr{J}} \cap \Gamma_{\mathscr{J}'}, \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \eta_\circ = \varepsilon_\circ \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}, \epsilon \cdot \in \Gamma_{\mathscr{J}}$ we have

$$\varepsilon_\circ^{-1} \varepsilon \quad \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \varepsilon_i.$$

Let $(n_2, n_3) = n_4$. Then $(n_1, n_4) = 1$. Choosing γ such that $(\gamma, n_3) = 1$, we see that $q_3 n_1 \gamma$ and n_4 being coprime, we may find a unimodular matrix. $\begin{pmatrix} a & b \\ q_2 n_1 \gamma & n_4 \end{pmatrix}$. With this matrix, we form the product

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ q_1 n_1 \gamma & n_4 \end{pmatrix} = \begin{pmatrix} n_1 n_3 a & nb \\ q_2 n_1 \gamma & n_4 \end{pmatrix}.$$

Again, since $(a, q_2, n_1 \gamma) = 1$, i.e., $(a, q_2 \gamma) = 1$ and $(q_2 \gamma., n_3) = 1$, there exists a unimodular matrix $\begin{pmatrix} A & B \\ -q_2 \gamma & n_3 \end{pmatrix}$ so that

$$\begin{pmatrix} A & B \\ -q_2 \gamma & n_3 a \end{pmatrix} \begin{pmatrix} n_1 n_3 a & nb \\ q_2 n_1 \gamma & n_4 \end{pmatrix} = \begin{pmatrix} n_1 & Anb + Bn \\ 0 & n_3 \end{pmatrix} \sim \begin{pmatrix} n_1 & Bn_4 \\ 0 & n_3 \end{pmatrix}$$

88 where "$\sim$" means that each matrix goes over into the other by multiplication on the left by a unit of the type $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, t begin a multiple of n_3. Further

$$\begin{pmatrix} n_1 & Bn_4 \\ 0 & n_3 \end{pmatrix} \sim \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix}$$

for we may choose for γ, then element given by

$$\gamma \frac{n_2}{n_4} . q_2 + \Lambda n_3 = 1$$

$(q_2.\dfrac{n_2}{n_4}$ and n_3 are co-prime, since $(n, q_2) = 1$ implies $(n_3, q_2) = 1$). Incidentally $(q_2\gamma, n_3) = 1$ is satisfied. Now, $Bq_2\gamma + An_3a = 1$ implies that

$$B(1 - \Lambda n_3) + An_3a.\frac{n_2}{n_4} = \frac{n_2}{n_4} \Rightarrow Bn_4 \equiv n_2 \pmod{n_3}$$

which is what we required.

We have yet to show that any primitive ideal $\mathcal{J}\mu$ of norm n can occur only once among $\mathcal{J}\nu\varepsilon_i$, $i = 1$ to d'. For, if $\mathcal{J}\nu\varepsilon = \mathcal{J}\nu\varepsilon'$, $\varepsilon, \varepsilon'$ two among $\varepsilon_1, \ldots, \varepsilon_d$, then it follows that $\nu\varepsilon = \varepsilon''\nu\varepsilon'$, i.e., $\varepsilon\varepsilon'^{-1} = \nu^{-1}\varepsilon''\nu \in \Gamma_{\mathcal{J}'}$ and also in $\Gamma_{\mathcal{J}}$ so that $\varepsilon\varepsilon'^{-1} \in \Gamma_{\mathcal{J}'} \cap \Gamma_{\mathcal{J}}$. The units that give rise to the same ideal lie in the same coset modulo $\Gamma_{\mathcal{J}} \cap \Gamma_{\mathcal{J}'}$, and conversely. Therefore there can be only d' distinct ideals of the type $\mathcal{J}\nu\varepsilon_i$, $i = 1$ to d'.

Let ν be a primitive element of norm $n, (n, q_1q_2) = 1$ of the order $\mathcal{J}$. Let $\mathcal{J}' = \nu^{-1}\mathcal{J}\nu$, then we have the correspondence of $S_{\mathcal{J}}$ onto itself defined by

$$C_n = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}}\nu\varepsilon_i$$

(ϵ_i as defined in the above lemma). By the above lemma, 89

$$C_n = \sum_{i=1}^{d'} \Gamma_{\mathcal{J}} \cdot \nu_i$$

where $\mathcal{J}\nu_i$, $i = 1, \ldots, d'$ are precisely all the primitive integral ideals of norm n. (We may define C_n even when $(n, q_1q_2) \neq 1$). We call C_n a *primitive modular correspondence. A modular correspondence* T_n, for $(n, q_1q_2) = 1$, is defined by

$$T_n = \sum_i \Gamma_{\mathcal{J}} \cdot \mu_i$$

where $\mathcal{J}\mu_i$ runs over all the integral left ideals with norm n. (We know that this number is finite). We can now write

$$T_n = \sum_{t^2/n} \frac{C_n}{t^2}$$

for if $\mu \in \mathcal{J}$ is an element whose norm is n, then we can write $\mu = \nu t, t \geq 1$, and ν is primitive $n(\nu) = n/t^2$ and then

$$\Gamma_{\mathcal{J}}\mu = \Gamma_{\mathcal{J}}, \nu t = \Gamma_{\mathcal{J}}.\nu$$

as an operator. Conversely if ν is a primitive element of norm $\dfrac{n}{t^2}$ then $\mu = \nu.t$ is an element of norm n, and $\Gamma_{\mathcal{J}}.\nu t = \Gamma_{\mathcal{J}}\nu$ as an operator.

4. *Some properties of* T_n : Let T_n^* denote the inverse operator of T_n. Then

1) $T_n^* = T_n$ (This will imply that the ring of operators T_n is commutative).

2) $T_n.T_m = T_{nm}$ if $(n, m) = 1$.

3) $T_{p^s} \cdot T_p t = \sum\limits_{\sigma=o}^{\min(s,t)} p^{\sigma}.T_p s + t - 2\sigma$

4) $T_n.T_m = \sum_{d|(n,m)} d.\dfrac{T_{nm}}{d^2}$

90 for any n, m. We shall prove these now.

1) We shall show first that $C_n^* = C_n$ and this will imply that $T_n^* = T_n$, for since $T_n = \sum\limits_{t^2|n} C_{n/t^2}$, we have

$$T_n^* = \sum_{t^2|n} C^*_{n/t^2} = \sum_{t^2|n} C_{\frac{n}{t^2}} = T_n.$$

Proof of $C_n = C_n^*$.

Let τ, σ be two complex variables in the upper half plane.

By definition $C_n(\Gamma_{\mathcal{J}}\tau) = \sum\limits_i \Gamma_{\mathcal{J}}\nu_i\tau$. The elements in $C_n^*(\Gamma_{\mathcal{J}})\sigma$ contain those $\Gamma_{\mathcal{J}}.\tau$ for which $C_n(\Gamma_{\mathcal{J}}\tau)$ contains $\Gamma_{\mathcal{J}}.\sigma$, i.e., If $\Gamma_{\mathcal{J}}\tau \in C_n^*$ $(\Gamma_{\mathcal{J}}\sigma)$ then $\Gamma_{\mathcal{J}}\sigma = \Gamma_{\mathcal{J}}\nu\tau$ for some $\nu \in \mathcal{J}$ of norm n. This means that $\varepsilon\sigma = \nu\tau$ or $\overline{\nu}\varepsilon\sigma = n(\nu).\tau$ or $\Gamma_{\mathcal{J}}, \overline{\nu}\varepsilon\sigma = \Gamma_{\mathcal{J}}.\tau$ as an operator in the complex plane. By lemma in para 3, as ε runs over $\Gamma_{\mathcal{J}}$, $\mathcal{J}\overline{\nu}\varepsilon$ runs over all primitive left $\mathcal{J}$- ideals of norm n. Hence

$$C_n^*(\Gamma_{\mathcal{J}}\sigma) \not\supseteq \sum \Gamma_{\mathcal{J}} \cdot \nu\sigma = C_n(\Gamma_{\mathcal{J}}\sigma)$$

and by symmetry, the other way, so that $C_n = C_n^*$.

2) $T_n.T_m = T_{nm}$ if $(n, m) = 1$.

Let $T_n = \sum\limits_i \Gamma_{\mathcal{J}}.\nu_i, n(\mathcal{J}\,\nu_i) = n$ and

$$T_m = \sum_k^i \Gamma_{\mathcal{J}} \cdot \mu_k,\ n(\mathcal{J}\mu_k) = m$$

hence $$T_n.T_m = \sum_{i,k} \Gamma_{\mathcal{J}}\nu_i\Gamma_{\mathcal{J}}\mu_k = \sum_{i,k} \Gamma_{\mathcal{J}}\nu_i\mu_k.$$

Since the number of integral ideals of norm $n.m$ is $\sum\limits_{d|nm} d = \sum\limits_{d|n} d. \sum\limits_{d'|m} d'$ (for $(n, m) = 1$) (this follows from the factorization of ideals), and conversely since any integral ideal $\mathcal{J}\nu_i\mu_k$ is of norm $n.m$ if we prove that all these are distinct, our proof will be finished. So consider any 91 two ideals $\mathcal{J}\nu_i\mu_k, \mathcal{J}\nu_{i'}\mu_{k'}$, where $i \neq i'$ or $k \neq k'$. If $k \neq k'$, let p be a prime dividing m, then $(\mathcal{J}\nu_i\mu_k)_p = \mathcal{J}_p\mu_k$, because $n(\nu_i) = n$ and $(n, m) = 1$, i.e., n is a p-adic unit or ν_i is a unit in $\mathcal{J}_p$.

Similarly $(\mathcal{J}\nu_i, \mu_{k'})_p = \mathcal{J}_p\mu_{k'}$. Now, since $k \neq k', \mathcal{J}_p\mu_k \neq \mathcal{J}_p\mu_{k'} \Rightarrow \mathcal{J}\nu_i\mu_k \neq \mathcal{J}\nu_{i'}\mu_{k'}$. If $k = k', i \neq i', \mathcal{J}_p\nu_i \neq \mathcal{J}_p\nu_{i'}$, for at least one $p|n$ (for, otherwise $\mathcal{J}_p\nu_i = \mathcal{J}_p\nu_{i'}$, for all $p, \Rightarrow \mathcal{J}\nu_i = \mathcal{J}\nu_{i'}$), and then $\mu_k = \mu_{k'}$ is a unit in $\mathcal{J}_p, \Rightarrow \mathcal{J}_p\mu_i\mu_k \neq \mathcal{J}_p\nu_i, \mu_{k'}$; for otherwise $\mathcal{J}_p\nu_i = \mathcal{J}_p\nu_{i'}$.

3) $T_ps.T_pt = \sum\limits_{\sigma=o}^{\min(s,t)} p^\sigma.T_ps + t - 2\sigma$

We will first prove that

$$T_ps.T_p = T_{p^{s+1}} + p.T_{p^{s-1}}$$

and then obtain the required result by induction.

Let

$$T_{p^s} = \sum_i \Gamma_{\mathcal{J}}.\nu_i, n(\mathcal{J}\nu_i) = p^s$$

and $$T_p = \sum_k \Gamma_{\mathcal{J}}\mu_k, n(\mathcal{J}\mu_k) = p;$$

so that $$T_{p^s}.T_p = \sum_{i,k} \Gamma_{\mathcal{J}}\nu_i\mu_k = \sum_{\text{primitive}} + \sum_{\text{imprimitive}}.$$

Because an integral ideal of prime power norm is uniquely decomposable into prime factors if it is primitive, there occur, among the $\mathcal{J}\nu_i\mu_k$
92 all integral primitive left ideals of norm p^{s+1} exactly once. But, if $\mathcal{J}\nu_i\mu_k$ is imprimitive it means that $\frac{\nu_i\mu_k}{\mathfrak{p}} \in \mathcal{J}$, i.e., $\nu_i\mu_k = \nu'_i.p = \nu'_i\bar{\mu}_k\mu_k \Rightarrow \nu_i = \nu'_i\bar{\mu}_k$. Since the number of integral left ideals of norm p is $p+1$, there occur among $\mathcal{J}\nu_i\mu_k$, all ideals $p\nu'_i\mathcal{J}$ of norm $p^{s+1}, (p+1)$ times each. Therefore, $T_{p^s}.T_p = C_{p^{s+1}} + (p+1)T_{p^{s-1}}$.

Next, we have

$$T_{p^{s+1}} = C_{p^{s+1}} + T_{p^{s-1}}.$$

For,

$$\begin{aligned} T_{p^{s+1}} &= \sum_{\text{prim. part}} + \sum_{\text{impr. part}} \\ &= C_{p^{s+1}} + \sum \mathfrak{p}\Gamma_{\mathcal{J}}\eta \end{aligned}$$

where the second sum is taken over all integral ideals η with norm p^{s-1}. The above sum therefore equals $C_{p^{s+1}} + T_{p^s-1}$.

From both the formulae, it follows that

$$\boxed{T_{p^s} = T_{p^{s+1}} + p.T_{p^{s-1}}}$$

We now use complete induction on t, i.e., assuming the result to be true for $n \leq t$, we prove it true for $t+1$. (Without loss of generality, we assume that $t \leq s$). Now,

$$T_{p^s}.T_{p^t} = \sum_{\sigma=o}^{t} p^{\sigma}.T_{p^{s+t-2\sigma}}.$$

Multiplying both sides by T_p, and substituting we have

$$T_{p^s}(T_{p^t+1} + p.T_{p^{t-1}}) = \sum_{\sigma=o}^{t} p^{\sigma}(T_{p^{s+t+1-2\sigma}} + p.T_{p^{s+1-1-2\sigma}})$$

$$T_{p^s}T_{p^{t+1}} = -p.T_{p^s}.T_{p^{t-1}} + \sum_{\sigma=o}^{t} p^{\sigma}T_{p^{s+t+1-2\sigma}} + \sum_{\sigma=o}^{t} p^{\sigma+1}T_{p^{s+t-1-2\sigma}}$$

$$= -p\left\{\sum_{\sigma=o}^{t-1} p^{\sigma}.T_{p^{s+t-1-2\sigma}}\right\} +'' \quad '' \quad + \cdots$$

$$= \sum_{\sigma=o}^{t} p^{\sigma}.T_{p^{s+t+1-2\sigma}} + p^{t+1}T_{p^{s-1-t}}$$

$$= \begin{cases} \sum_{\sigma=o}^{t+1} p^{\sigma}.T_{p^{s+t+1-2\sigma}}, & \text{if } t < s. \\ \sum_{\sigma=o}^{t} p^{\sigma}.T_{p^{s+t+1-2\sigma}}, & \text{if } t = s, \end{cases}$$

because $T_{p^{-1}} = 0$ by convention. 93

Therefore, in either case,

$$T_{p^s}.T_{p^{t+1}} = \sum_{\sigma=o}^{\min(s,t+1)} p^{\sigma}.T_{p^{s+t+1-2\sigma}}$$

$$T_n.T_m = \sum d|n, md.T_{nm/d^2} \tag{4}$$

This follows as a direct consequence of the properties (2) and (3). We may now define the operator T_n for $(n, q_1q_2) > 1$. Firstly, we shall define T_p, $p|q_1q_2$ and then extend it to n.

1. $\underline{p|q_1}$. In this case, $\mathscr{J}_p$ is a maximal order in the division algebra Q_p, so that there exists only one integral ideal

$$\mathscr{P}\mathscr{J}_p\pi = \mathscr{J}_p\bar{\pi} = \bar{\pi}\mathscr{J}_p = \pi\mathscr{J}_p$$

   with norm p and hence the ideal $\mathscr{J}\pi = \bar{\pi}\mathscr{J}$ is the only integral ideal with norm P.

   We define $T_p = \Gamma_{\mathscr{J}}\pi = \bar{\pi}\Gamma_{\mathscr{J}}$. Consequently $T_p.T_p = \Gamma_{\mathscr{J}}\pi\bar{\pi}\Gamma_{\mathscr{J}} = I$. Also $T_{p^s}.T_p = \Gamma_{\mathscr{J}}\pi^s.\Gamma_{\mathscr{J}}\pi = \Gamma_{\mathscr{J}}\pi^{s+1} = T_{p^{s+1}}$.

2. $\underline{p\big|q_2}$. $\mathscr{J}_p \cong \begin{pmatrix}\mathscr{O}_p & \mathscr{O} \\ p\mathscr{O}_p & \mathscr{O}_p\end{pmatrix}$. We define $T_{p^n} = \sum_{\nu}\Gamma_{\mathscr{J}}\nu$ where $\mathscr{J}\nu$ are 94 ambiguous ideals with norm p^n. But we have already shown that actually there is only one such ambiguous ideal. Now $\mathscr{J}\nu = \nu\mathscr{J}$, where $\nu = \begin{pmatrix}0 & 1 \\ p & 0\end{pmatrix}$. Hence $\mathscr{J}\nu^s = \nu^s\mathscr{J}$ and $n(\nu^s) = p^s$. From this, we may deduce that there exists only one integral ambiguous ideal of norm p^s.

As before

$$T_{p^s}.T_p = \Gamma_{\mathcal{J}}.\nu^s.\Gamma_{\mathcal{J}}.\nu = \Gamma_{\mathcal{J}}.\nu^{s+1} = T_{p^{s+1}}.$$

Hence

$$T_p.T_p = T_{p^2} = \Gamma_{\mathcal{J}} \cdot \nu^2 = \Gamma_{\mathcal{J}} \begin{pmatrix} p & 0 \\ O & p \end{pmatrix} = I.$$

Note: We may deduce some interesting results from the above multiplicative properties of T_n, regarding the representations of the ring of operators $\mathscr{R}$ of T_n.

5. Let $R(T_n)$ be the representation matrix of T_n of some fixed degree. Then, we have the following product formulae from (2) and (3).

1) If n, m are coprime to q_1q_2 and $(n, m) = 1$, then $R(T_nT_m) = R(T_{nm})$.

2) If $p\chi q_1q_2, R(T_{p^s}.T_p) = R(T_{p^{s+1}}) + p.R(T_{p^{s-1}})$.

For $p\big|q_1q_2$, from the facts that $T_{p^2} = I$ and $T_{p^s}.T_p = T_{p^{s+1}}$, we have $R(T_p.T_p) = R(T_{p^2}) = I$ and $R(T_{p^s}.T_p) = R(T_{p^{s+1}})$.

Consider now the ζ-function associated with this representation, as follows:

$$\zeta_R(s) = \sum_{n=1}^{\infty} \frac{(R(T_n))}{n^s}.$$

95 A special representation is the one-rowed matrix $R(T_n) = R_1(T_n) =$ number of integral ideals with norm $n = \sum\limits_{d|n} d$ (if $(n, q_1q_2) = 1$).

Hence

$$\zeta'_{R_1}(s) = \sum_{(n,q_1q_2)=1} \frac{\sum_{d|n} d}{n^s}$$

(omitting in ζ_{R_1} those n which are divisible by q_2).

This is easily seen to be the same as the ζ- function, associated with the order $\mathcal{J}$ but for those terms, corresponding to the factors of q_2. We have seen that $\zeta_{R_1}(s)$ possesses a functional equation. But it is still an unsolved problem whether $\zeta_R(s)$ for an arbitrary R, possesses a functional equation.

We shall prove, using the multiplicative properties of $R(T_n)$ that $\zeta(s)$ possesses an Euler product. It is easily seen that

$$\zeta_R(s) = \sum_{n=1}^{\infty} \frac{R(T_n)}{n^s} = \prod_p (I + \frac{R(T_p)}{p^s} + \frac{R(T_{p^2})}{p^{2s}} + \cdots$$

i) In case $p \nmid q_1 q_2$, we shall show that

$$\sum_{n=o}^{\infty} \frac{R(T_{p^n})}{p^{n,\mathscr{S}}} = (I - R(T_p)p^{-s} + p^{1-2s})^{-1}.$$

For,

$$\begin{aligned}
&\left(I + \frac{R(T_p)}{p^s} + \frac{R(T_{p^2})}{p^{2s}} + \cdots\right)(I - R(T_p).p^{-s} + p^{1-2s}) \\
&= \sum_{n=o}^{\infty} \frac{R(T_{p^n})}{p^{ns}} - \sum_{n=o}^{\infty} R(T_{p^{n+1}}).p^{-(n+1)s} \\
&- \sum_{n=o}^{\infty} R(T_{p^{n-1}}).p^{-(n+1)s+1} + \sum_{n=o}^{\infty} R(T_{p^n}).p^{-ns+1-2s} \\
&= I + \sum_{n=1}^{\infty} R(T_{p^n}).p^{-ns} - \sum_{n=o}^{\infty} R(T_{p^{n+1}}).p^{-(n+1)s} \\
&- \sum_{n=1}^{\infty} R(T_{p^{n-1}}).p^{-(n+1)s+1} + \sum_{n=1}^{\infty} R(T_p^{n-1})p^{-ns+1-s} \\
&= I.
\end{aligned}$$

ii) $\underline{p|q_1 q_2}$. 96

$$\begin{aligned}
\sum_{n=0}^{\infty} R(T_{p^n}).p^{-ns} &= I + R(T_p).p^{-s} + R(T_{p^2}).p^{-2s} + \cdots \\
&= I + R(T_p).p^{-s} + p^{-2s} + R(T_p).p^{-3s} + \cdots \\
&= (1 + p^{-2s} + p^{-4s} \cdots)(I + R(T_p)p^{-s}) \\
&= \frac{I + R(T_p).p^{-s}}{1 - p^{-2s}}.
\end{aligned}$$

Hence we have the Euler product

$$\zeta_R(s) = \prod_{p|q_1q_2} \frac{I + R(T_p).p^{-s}}{1 - p^{-2s}} \prod_{p+q_1q_2} (I - R(T_p).p^{-s} + p^{1-2s})^{-1}$$

8 Representations of the Modular Correspondence by the Betti Groups

6. The chief task hereafter will be the determination of the traces of certain representations $R(\mathfrak{M})$, ($\mathfrak{M}$, the ring of correspondences or T_n operators) because the traces determine the representations uniquely. For some $R(\mathfrak{M})$, the calculation of the trace leads to topological considerations, for others traces are not yet known. For example, we shall be concerned with the trace of the representation of T_n by the Betti groups of $S_{\mathcal{J}}$.

Let $S_{\mathcal{J}}$ be the Riemann surface associated with an order $\mathcal{J}$ and $S'_{\mathcal{J}}$ a homeomorph of $S_{\mathcal{J}}$. Let C be a correspondence of $S_{\mathcal{J}}$, onto itself defined by means of the covering surface S''. It is easy to see from the definition of a correspondence, that C takes cycles to cycles and boundaries to boundaries, so that C induces an endomorphism of the Betti groups of dimension $0, 1$ and 2.

$$\begin{tikzcd}
 & S'' \arrow[dl, dash, "d'"'] \arrow[dr, dash, "d"] & \\
S_{\mathcal{J}} \arrow[rr, leftrightarrow] & & S_{\mathcal{J}'}
\end{tikzcd}$$

97 Let T_n be a modular correspondence. Then $T_n = \sum_{t^2/n} c_{\frac{n}{t^2}} C_{-s}$ being primitive correspondences and hence can be looked upon as topological mappings of $S_{\mathcal{J}}$ onto itself. Now, if we extend the notion of covering surface to include disconnected pieces also, then T_n may also be looked

upon as a correspondence in the topological sense. By the above paragraph, T_n induces an endomorphism of the Betti groups $B^r(S), r = 0$, 1, 2 ; consequently, we have the traces of these endomorphisms, (say) $tr^o(T_n), tr^1(T_n)$ and $tr^2(T_n)$. Here, $tr^1(T_n)$= number of sheets of S'' over S = number of sheets of S'' over S', both being equal since $T_n = T_n^*$. Further

$$tr^o(T_n) = tr^2(T_n) = \sum_{d|n} d \text{ if } (n, q_1 q_2) = 1).$$

For calculating $tr^1(T_n)$, we apply Lefschetz's fixed-point theorem, namely

Theorem.

$$\left.\begin{array}{l}\textit{The number } f(T_n) \textit{ of fixed}\\ \textit{points of } T_n \textit{ with due mul-}\\ \textit{tiplicity}\end{array}\right\} \begin{array}{l} = tr^o(T_n) - tr^1(T_n) + tr^2(T_n)\\ = 2\sum_{d|n} d - tr^1(T_n).\end{array}$$

We will calculate explicitly the left hand side so that we obtain $tr^1(T_n)$ at once by the above equation.

7. We shall sketch a proof of Lefschetz's fixed - point theorem 98 in our case where T_n are multi-valued analytic orientation preserving mappings, by defining the multiplicities suitably, as the original proof is rather lengthy and is not found in elementary text-books on topology.

We may define the multiplicity of a fixed point $\Gamma_{\mathcal{J}}.\tau^o$, for a branch $\Gamma_{\mathcal{J}}\nu_i$. This branch in the neighbourhood of this point can be expanded as,

$$\begin{aligned}\tau_i = \nu_i(\tau) &= \nu_i(\tau^o) + c_1(\tau - \tau^o)^{\frac{a}{b}} + c_2(\tau - \tau^o)^{\frac{a+1}{b}} + \cdots\\ &= \tau^o + c_1(\tau - \tau^o)^{\frac{a}{b}} + c_2(\tau - \tau^o)^{\frac{a+1}{b}} + \cdots\end{aligned}$$

(since $\nu_i(\tau^o) = \tau^o$), where τ is a local uniformizing parameter and b being the common denominator of all the exponents. Further $c_1 \neq 0$. The multiplicity of $\Gamma_{\mathcal{J}}\tau^o$ as a fixed point is min $.(a, b)$.

The general plan of the proof is to define a special linear mapping φ on the image of (a triangulation of) $S_{\mathcal{J}}$, by means of T_n, so that the mapping $\varphi(T_n)$ is homotopic to T_n. Further φ has to be boundary preserving. Since the number of fixed points is invariant under homotopic deformations, it is enough to calculate this number for $\varphi(T_n)$.

We first cut up $S_{\mathcal{J}}$ into a finite number of triangles τ^2_i (superscript meaning dimension), the fixed points being among the vertices. We may choose the triangulation so fine that the following conditions are satisfied:

Let $\{\tau^j_i\}$ $(j - 0, 1, 2)$ denote the simplices of the triangulation.

99 1) The image $T_n(\tau^2_i)$ consist of a number of simply connected domains $\overline{\tau}^2_{ik}$ bounded by Jordan curves without double points.

2) All images of each vertex are situated in the interior of some other triangle, except for the fixed points.

3) All images of all points of a τ^2_i lie in such triangles τ^2_k which have no point in common with τ^2_i, except for those τ^2_i which contain a fixed point.

Let $T_n(\tau^r_i) = \sum\limits_k \overline{\tau}^r_{ik}$ where $\overline{\tau}^r_{ik}$ are, by (1), simply connected domains $(r = 2)$, arcs of curves $(r = 1)$ and points $(r = o)$. We shall now define a linear mapping φ on $\overline{\tau}^r_{ik}$ so that

$$\varphi_n(\tau^r_i) = \phi(T_n(\tau^r_i)) = \sum_k \varphi(\overline{\tau}^r_{ik})$$

The definition of $\varphi(\sigma^r)$ $(r = 0, 1, 2)$ $(\sigma^r$ are cycles $\overline{\tau}^r_{ik})$ differs according as σ^r contains a fixed point or not.

i) Suppose first that σ^r does not contain a fixed point.

Then

$$\varphi(\sigma^2) = \frac{1}{3}\sum_j \varepsilon_j \tau^2_j$$

where ε_j is the number of vertices of τ^2_j lying in σ^2.

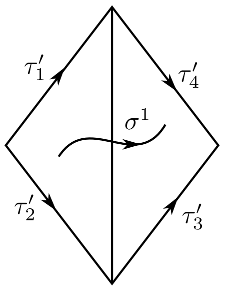
$$\varphi(\sigma^1) = \begin{cases} 0 & \text{if } \mathcal{N} \text{ lies entirely inside a } \tau^2_i. \\ \frac{1}{6}\left(\tau'_1 + \tau'_2 + \cdots + \tau'_4\right) & \text{if } \sigma' \text{ crosses one boundary} \end{cases}$$

once between two τ^2_i, the sides being denoted as in the figure

Finally

$$\varphi(\sigma^o) = \frac{1}{3}(\tau^o_{k,1} + \tau^o_{k,2} + \tau^o_{k,3}$$

where $\tau^o_{k,j}$ are the vertices of a triangle τ^2_k in which σ^o lies.



By linearity, **100**

$$\varphi(\sigma^r_1 + \sigma^r_2) = \varphi(\sigma^r_1) + \varphi(\sigma^r_2) \qquad (*)$$

φ is extended to all σ^r. $(r = 0, 1, 2)$.

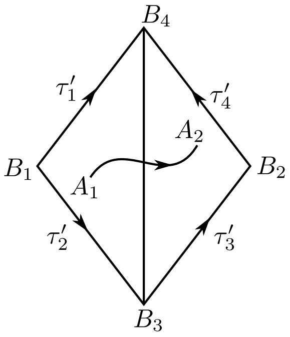
We need not define $\varphi(\sigma^r)$ for $r = 0, 1$ when σ^r has a point in common with a vertex τ^o_i because of the assumptions made on. *p*.99

It is verified easily that the above definition of φ on $\sigma^r(r = 0, 1, 2)$ is consistent with linearity. It is also seen that

$$\varphi(Bd(\sigma^r)) = Bd\,(\varphi(\sigma^r)).$$

For example, when $r = 1$, $Bd\sigma^1 = A_2 - A_1$ and

$$\begin{aligned}\varphi(Bd\sigma^1) &= \varphi(A_2) - \varphi(A_1)\\ &= \frac{1}{3}(B_2 + \cancel{B_3} + \cancel{B_4} - \cancel{B_3} - \cancel{B_4} - B_1)\\ &= \frac{1}{3}(B_2 - B_1).\end{aligned}$$



Now, $\varphi(\sigma') = \dfrac{1}{6}(\tau_1' + \tau_2' + \tau_3' + \tau_4')$ so that

$$\begin{aligned} Bd\varphi(\sigma') &= \frac{1}{6}(\cancel{B_4} - B_1 + \cancel{B_3} + B_1 + B_2 - \cancel{B_3} + B_2 - \cancel{B_4}) \\ &= \frac{1}{3}(B_2 - B_1), \end{aligned}$$

i.e., $\underline{(}Bd(\varphi(\sigma^1 = \varphi(Bd(\sigma^1)$.

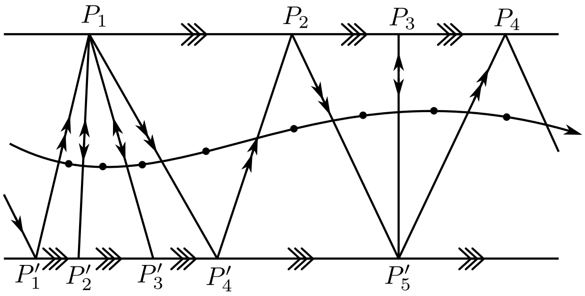
It is to be noted that the above definition of φ is not to be applied if $Bd\,\sigma^r$ passes through a vertex of a τ_i^2, which case we deal with later.

Then, we have the following lemma (if σ' does not pass through a fixed point).

101 **Lemma .** *For a closed curve σ' without double points (in the usual sense), $\varphi(\sigma')$ is a cycle homotopic with σ', (the triangulation being sufficiently fine).*

Proof. If the τ_i^2 are sufficiently small, then the strip of simplices through which σ' passes does not contain any double points. Then $\varphi(\sigma')$ can be obtained as follows: (2 arrows indicating traversed twice in the same direction).

$$\varphi(\sigma') = \frac{1}{3}\Big[(P_1P_2) + (P_2P_3) + \cdots + (P_1'P_2') + (P_2'P_3') \\ + \cdots + (P_1'P_1) + (P_1P_4') + (P_4'P_2)\cdots\Big]$$

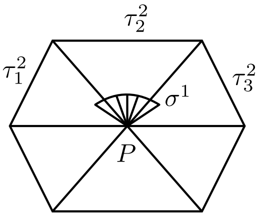


and the lemma follows. σ' passing through a fixed point will be taken up in case (*ii*) after defining φ in the neighbourhood of a fixed point. (*ii*) $\sigma^r (r = 0, 1, 2)$ *contains a fixed point* P (say). □

Because of linearity, it suffices to define φ for such σ^ν which are contained in the union of all τ_i^2 having P as a vertex and this is called the star of P.

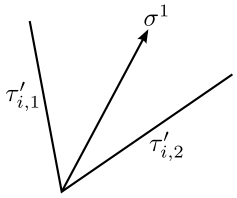
We then define $\varphi(\sigma^2) = \dfrac{1}{6} \sum\limits_j \epsilon_j \tau_j^2$ where ε_j is the number of sides originating from P which pass through σ^2. **102**

Applying the linearity property $(*)$ we can assume without loss of generality that σ' has no common points except P with any $\tau'_{i,j} (j = 1, 2)$ (τ_i^2 being the triangles through which σ' passes) originating from P. We then define



$$\varphi(\sigma') = \frac{1}{3} \left(\tau'_{i,1} + \tau'_{i,2}\right);$$

$\tau'_{i,j}$ being the sides originating from P of τ_i^2 through which σ' passes. Finally $\varphi(P) = P$.



As before, consistency with linearity is verified and also the commutativity with the boundary mapping. Now, the above lemma is valid even if σ' passes through a fixed point, with the above definition and is easily seen to be true.

We have then in either case $\varphi(T_n(\sigma^r)) \sim T_n(\sigma^r)\,(r = 0, 1, 2)$. For $r = 0$ and 2, this follows from the definition of φ which is homotopic to the identity, and for $r = 1$, $\varphi(\sigma') \sim \sigma'$ from our lemma.

It can be seen that at this stage the condition that σ' should not have double points can be dropped for otherwise we can split it into pieces in each of which there is no double point, and the above relation holds good for the sum.

Since $Bd(T_n(\tau_i^r)) = T_n(Bd(\tau_i^r))$ and $Bd(\varphi(\sigma^r)) = \varphi(Bd(\sigma^r))$ we have $Bd(\varphi_n(\tau_i^r)) = \varphi_n(Bd(\tau_i^r))$.

This enables us to apply the Euler-Poincar'e-Hopf formula

$$s^o(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n) = f(\varphi_n) = t\pi^o(\varphi_n) - t\pi^1(\varphi_n) + t\pi^2(\varphi_n)$$

(σ^i denoting the traces of endomorphisms in the chain groups).

103 We know $T_n \sim \varphi_n$ so that $f(T_n) = f(\varphi_n)$. Therefore it is enough to compute for the linear mappings φ_n, the number

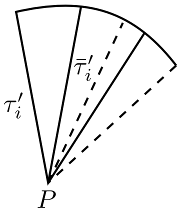
$$f(\varphi_n) = s^o(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n).$$

Because of the condition (3) on the triangulation, it is enough to consider the effect of φ_n on the simplices τ_i^r belonging to the stars of fixed points.

From the expansion, $\tau_i = \tau_o + c_1(\tau - \tau)^{\frac{a}{b}} + c_2(\tau - \tau)^{\frac{a+1}{b}} + \cdots, c_1 \neq 0$, it is seen that star of P is mapped "b" times on Riemann surface of "a" sheets lying over the neighbourhood of P, the ramification (of order a) being at P. In case $a = b$, and $|c_1| = 1$, the mapping is approximately a rotation and the image of the star of P is of the same size as the star of P. If $a > b$ or $a = b$ and $|c_1| < 1$, the image of the star of P lies entirely inside of the star of P. If $a < b$ or $a = b$ and $|c_1| > 1$, the image of the star of P lies entirely outside the star of P. We shall treat the above cases one by one.

i) $a = b$ and $|c_1| = 1$.

Let the image of τ'_i be the dotted line $\overline{\tau}'_i$. We may subdivide the star of P so fine ($\overline{\tau}'_i$ need not be straight lines) that $\overline{\tau}'_1$ lies inside a sector both of whose sides differ from τ'_i. By such a procedure, we have, by definition of traces



$$s^o(\varphi_n) = b, s^1(\varphi_n) = 0, s^2(\varphi_n) = 0$$

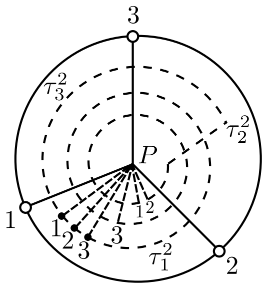
regarding the star of P. The first one follows from the fact that φ_n maps P, "b'' times on itself. Hence the multiplicity of the fixed point P is given by **104**

$s^o(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n)$ (restricted to the star P)

$$= b - 0 + 0 = b = \min(a, b).$$

ii) $a > b$ or $a = b$ and $|c_1| < 1$.

In this case, the image of the star of P lies completely inside the star of P and we may deform φ_n homotopically so as to make almost all images $\overline{\tau}^2_{ik}$ of τ^2_i, sectors with an angle nearly zero at P and the rest covering almost an angle 2π. Further, we may take these to lie in τ^2_1 (say) in a sufficiently small neighbourhood (see figure).



(The broken lines show the $\overline{\tau}^r_{ik}$).

$$(a = 3, b = 2),$$

Only “a'' of the $\overline{\tau}^2_{ik}$ (with $i \neq 1$) are sectors of an angle nearly 2π. By our definition of φ, the coefficient of τ_i^2 in $\varphi_n(\overline{\tau}^2_{ik})$ is 0 or $\dfrac{1}{3}$ according as $\overline{\tau}^2_{ik}$ is a small or large sector.

Hence the contribution of the star of P to $s^2(\varphi_n)$ is $\dfrac{a}{3}$.

105 For $s'(\varphi_n)$, by definition of φ in the neighbourhood of fixed point, the coefficient of $\tau'_{i,j}$ in $\varphi_n(\tau'_{i,j})$ is 0 or $\dfrac{1}{3}$ according as $i \neq 1$ or $i = 1$.

Furthermore, for each side $\tau^1_{i,3}$ of τ^2_i opposite to P say $\tau^1_i, \varphi(\overline{\tau}^1_{ik}) = 0$ or $\dfrac{1}{3}$ times the boundary of the star of P according as $\overline{\tau}^i_{ik}$ is small or large. Hence the contribution of the star of P to $s'(\varphi_n)$ is $(a + 2b)/3$.

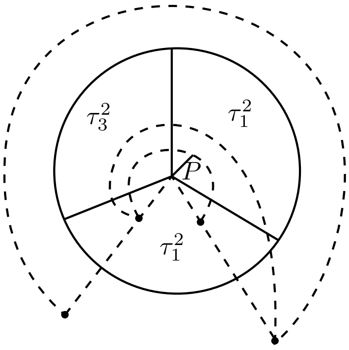
Lastly $\varphi(P) = b.P.$ and for other vertices $\tau^o_{i,k}$ of the triangles τ^2_i, φ $(\overline{\tau}^o_{ik,j}) = \dfrac{1}{3}$ (sum of the vertices of τ^2_i). Hence the contribution to $s^o(\varphi_n)$ of these is $\dfrac{2b}{3}$, i.e., in the star of P, $s^o(\varphi_n) = b + \dfrac{2b}{3}$.

Therefore

$$\begin{aligned} s^0(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n) &= \frac{a}{3} - \left(\frac{a}{3} + \frac{2b}{3}\right) + \left(b + \frac{2b}{3}\right) \\ &= b = \min(a, b). \end{aligned}$$

(iii) $a < b$ or $a = b$ and $|c_1| > 1$.

Here the image lies completely outside the star of P. For simplicity, we consider only one large triangle. This is cut up into three parts as shown in the diagram. For a large $\overline{\tau}^2_{ik}$, the coefficients of τ^2_i in $\varphi(\overline{\tau}^2_{ik})$ is 1 and for small sectors, the coefficient is zero. So the contribution of the neighbourhood of P to $s^2(\varphi_n)$ is a.



Now, the sides $\tau^1_{ik}(j = 1, 2)$ of τ^2_i originating in P are divided into two parts. The sides $\tau^{(1)}_{1,j}$ have coefficients $\dfrac{1}{2}$ in $\varphi(\overline{\tau}^1_{ik,j})$, so that the contribution from these is b while other sides of τ^2_i have no contribution. 106

Lastly, the only contribution to $s^o(\varphi_n)$ of the star of P is given by P and that is b. Hence we obtain

$$s^o(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n) = a - b + b = a = \min(a, b).$$

For the full traces s^o, s^1 and s^2, summing up, for each fixed point the multiplicity being $\min(a, b)$, we obtain finally the result that

$$\left.\begin{array}{l}\text{the number of fixed points}\\ \text{with due multiplicity}\end{array}\right\} = s^o(\varphi_n) - s^1(\varphi_n) + s^2(\varphi_n).$$

Chapter 4

Ideal Theories in Q and in Quadratic Subfields

The following considerations serve as a tool for calculating the number of fixed points of correspondences. Besides, there are other applications. **107**

9 Connections Between Ideals in Q and in Quadratic Subfields

1. We consider an order $\mathcal{J}$ of the type (q_1, q_2) for which we know that the class number is 1. Further, for such an order, any left integral ideals $\mathfrak{M}$ such that $(n(\mathfrak{M}), q_2) = 1$ can be written in the form $\mathfrak{M} = \mathcal{J}\begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix}$ (here $q_1 = 1), n_2$ being reduced $\mod n_3$. But, suppose $(n(\mathfrak{M}), q_2) \neq 1$. Then $n(\mathfrak{M}) = p^r.u, p|q_2$ and u, a p-adic unit. We consider in the following structure of $\mathfrak{M}_p$ for $p|q_2$.

Theorem 1. For $\mathfrak{M}_p = \mathcal{J}_p.v$, we have the following normal forms. *i.e.,*

(1) *There exists a unit ε of $\mathcal{J}_p$ such that*

$\varepsilon v = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}, r = a + b$ *and c is reduced* $\mod p^a$.

or

(2) *There exists a unit* ε' *of* $\mathcal{J}_p$ *so that* $\varepsilon'\nu = \begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix}, r = a + b + 1$ *and c is reduced* $\mod p^{a+1}$.

Proof. Let the generator ν be $\begin{pmatrix} n_{11} & n_{12} \\ pn_{21} & n_{22} \end{pmatrix}$. We now distinguish two cases:

(i) $\dfrac{n_{21}}{n_{11}}$ is a p-adic integer, or

(ii) $\dfrac{n_{21}}{n_{11}}$ is not a p-adic integer.

□

108 **Case (i).** *Our object is to find a unit* $\varepsilon = \begin{pmatrix} e_{11} & e_{12} \\ pe_{21} & e_{22} \end{pmatrix}$ *such that* $\varepsilon\nu$ *is of type* 1).

Now

$$\varepsilon\nu = \begin{pmatrix} e_{11}\ n_{11} + e_{12}\ pn_{21} & e_{11}n_{12} + e_{12}n_{22} \\ p(e_{21}n_{11} + e_{22}n_{21}) & pe_{21}\ n_{12} + e_{22}n_{22} \end{pmatrix}$$

Letting $n_{11} = p^s.u_1$ and putting $e_{21} = \dfrac{n_{21}}{p^s}$ we have $e_{22} = -\dfrac{n_{11}}{p^s}$. Since pe_{21} and e_{22} are coprime as p-adic integers (e_{22} being a unit) this row can be completed to a p-unimodular matrix ε. Now

$$\varepsilon\nu = \begin{pmatrix} p^a.u_1^{/} & c' \\ 0 & p^b.u'_2 \end{pmatrix}.$$

Again

$$\begin{pmatrix} u_1'^{-1} & 0 \\ 0 & u_2'^{-1} \end{pmatrix} \varepsilon\nu = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix},$$

$a + b = r$. For reducing $c \mod p^a$, we may multiply $\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}$ to the left by a unit $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ for a suitable t.

Case (ii). *$n_{11} = p^s.u_1$ and $n_{21} = p^1.u_2$ (say). Now, by hypothesis, $s > 1$. Putting*

$$e_{11} = p.\frac{n_{21}}{p^{l+1}}, e_{12} = -n_{11}\frac{1}{p^{l+1}},$$

we may complete $(e_{11}\, e_{12})$ to a unimodular matrix ε belonging to $\mathcal{J}_p$ and we have

$$\varepsilon\nu = \begin{pmatrix} 0 & u'_2.p^a \\ u'_1.p^{b+1} & c' \end{pmatrix}, a + b + 1 = r.$$

As before, $\begin{pmatrix} u_2'^{-1} & 0 \\ 0 & u_2'^{-1} \end{pmatrix} \varepsilon\nu = \begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix}$ and on multiplication to 109 the left by a unit of the form $\begin{pmatrix} 1 & 0 \\ pt & 1 \end{pmatrix}$, we can reduce $c \mod p^{a+1}$.

Note: As a consequence, the number of integral ideals with respect to the order $\mathcal{J}_p, (p|q_2)$ with norm p^r = number of ideals in the first normal form + number in the second normal form, and this is evidently given by

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

(This result was assumed in §2).

Using the above normal form, we shall now find the structure of all integral ambiguous ideals for the order $\mathcal{J}_p$; $p|q_2$.

Theorem 2. *If $\mathcal{J}_p\pi = \pi\mathcal{J}_p$ is an ambiguous ideal for $\mathcal{J}_p$, then either $\mathcal{J}_p\pi = \mathcal{J}_p \begin{pmatrix} p^r & 0 \\ 0 & p^r \end{pmatrix}$ or $\mathcal{J}_p\pi = \mathcal{J}_p \begin{pmatrix} 0 & p^r \\ p^{r+1} & 0 \end{pmatrix}$ according as $n(\pi)$ is an even or odd power of p.*

Proof. Let $\pi_o = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$. Then $\mathcal{J}_p\pi_o = \pi_o\mathcal{J}_p$, for, if $x \in \mathcal{J}_p$,

$$\pi_o^{-1}x\pi_o = \begin{pmatrix} 0 & \frac{1}{p} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ px_{21} & x_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} = \begin{pmatrix} x_{22} & x_{21} \\ px_{12} & x_{11} \end{pmatrix} \in \mathcal{J}_p.$$

Further, since

$$\begin{pmatrix} p^r & 0 \\ 0 & p^r \end{pmatrix} = p^r \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & p^r \\ p^{r+1} & 0 \end{pmatrix} = p^r \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix},$$

□

110 the corresponding ideals $\mathcal{J}_p\begin{pmatrix} p^r & 0 \\ 0 & p^r \end{pmatrix}$ and $\mathcal{J}_p\begin{pmatrix} 0 & p^r \\ p^{r+1} & 0 \end{pmatrix}$ are ambiguous.

I) Let π be of the first normal form, i.e., $\pi = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}$, c reduced mod p^b, and $a + b = s$. Then we shall prove that $a = b$ so that $s = 2r$ and $c = 0$.

$$\mathcal{J}_p\pi = \pi\mathcal{J}_p \Longrightarrow \pi^{-1}x\pi \in \mathcal{J}_p$$

for any $x \in \mathcal{J}_p$. i.e.,

$$\begin{pmatrix} p^a & -p^{-a}c^{-b} \\ 0 & p^{-b} \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} \\ px_{21} & x_{22} \end{pmatrix}\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}$$
$$= \begin{pmatrix} x_{11} - p^{1-b}x_{21}c & p(x_{11}c - p^{1-b}c^2x_{21} + p^bx_{12} - cx_{22}) \\ p^{1+a-b}x_{21} & p^{1-b}x_{21}c + x_{22} \end{pmatrix}$$

is in $\mathcal{J}_p$.

Consequently, we have

i) $(1 + a - b) \geq 1 \Longrightarrow a \geq b$

ii) $x_{11} - p^{1-b}x_{21}c = \lambda$, a p-adic integer and also $p^{-a}c(x_{11} - p^{1-b}cx_{21}) + p^{-a}(p^bx_{12} - cx_{22}) = \lambda_1$, a p-adic integer. i.e., $c\lambda + p^bx_{12} - cx_{22} = p^a.\lambda_1 \Longrightarrow c(\lambda - x_{22}) = p^b.\lambda'_1$ since $a \geq b(\lambda'_1$ an integer).

Choosing x_{11}, x_{21} and x_{22} in such a manner that $\lambda - x_{22}$ is a p-adic unit, we conclude that $p^b|c \Longrightarrow c = 0$, since c is reduced $\mod p^b$.

iii) Putting $c = 0$, $p^{b-a}x_{12}$ an integer $\Longrightarrow b \geq a$.

From (i) and (iii) we conclude $a = b = r$.

II) If π is of the second normal form, $\pi = \begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix}$, c reduced mod $p^{a+1}a + b + 1 = s$.

$$\mathcal{J}_p\pi = \pi\mathcal{J}_p \Longrightarrow \pi_o\mathcal{J}_p\pi = \pi_o\pi\mathcal{J}_p.$$

111 But

$$\pi_o\mathscr{J} = \mathscr{J}_p\pi_o \text{ so that}$$

$$\mathscr{J}_p\pi_o\pi = \pi_o\pi\mathscr{J}_p \text{ and } \pi_o\pi = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix} = \begin{pmatrix} p^{b+1} & c \\ 0 & p^{a+1} \end{pmatrix}$$

which is of the first normal form, since c is reduced module p^{a+1}, and $(a+1)+(b+1) = s+1$. By $(i) s+1$ is even and $= 2r+2$ (say) so that $s = 2r+1$ and $a = b = r, c = 0$. In other words,

$$\begin{pmatrix} 0 & p^r \\ p^{r+1} & c \end{pmatrix}.$$

Note. *We had assumed this lemma in §7 for defining T_p when $p|q_2$.*

2. Now, we shall consider quadratic subfields K of Q and connect the ideal theory of K with that of Q.

Let $K = k(\sqrt{d})$ (d without square factor) be a quadratic sub-field of Q and $\mathscr{O}_o$ the maximal order in K (the ring of all integers). Then we know that $\mathscr{O}_o = [1, \omega_o]$ where

$$\omega_o = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv \quad \pmod 4 \end{cases}$$

If $\mathscr{O}$ be any order in K (i.e., a subring of $\mathscr{O}_o$), then $\mathscr{O}$ has a basis $[1, f\omega_\sigma]$, f, a rational integer. This f, we call the *conductor* of the order $\mathscr{O}$. If D_o denotes the discriminant of the order $\mathscr{O}_o$ and D that of $\mathscr{O}$, then $D = f^2 D_o$ and since

$$D_o \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

i.e., $D_o \equiv 0, 1 \pmod 4), D \equiv 0, f^2 \pmod 4 \implies D \equiv 0, 1 \pmod 4$ (since $f^2 \equiv 0, 1 \pmod 4$)). 112

We now prove the following :

Lemma 1. *Given a quadratic subfield $K \subset Q$, we can find an order $\mathscr{J}$ of Q such that $\mathscr{J} \supset \mathscr{O}_o$.*

Proof. Let $\mathscr{O}_o = [1, \omega_o]$. Consider an element $\Omega \in Q$ and $\notin K$, so that $(1, \omega_o, \Omega, \Omega\omega_o)$ are linearly independent over k. Then we prove that $\mathscr{J} = [1, \omega_o, m\Omega, m\Omega\omega_o]$ is an order for a sufficiently large integer m.

For, m can be chosen so large that $tr(m\Omega), tr(m\Omega\omega_o)$ and $n(m\Omega)$ are integers. Now, it is enough to show that $m\omega_o\Omega\, m\omega_o\Omega\omega_o$ and $m\Omega\omega_o\Omega$ lie in $\mathscr{J}$. This can be shown as follows:

$$\begin{aligned}\overline{m\omega_o\Omega} = \overline{\Omega}\;\overline{(m\omega_o)} &= (\mathrm{tr}(\Omega) - \Omega)(\mathrm{tr}(m\omega_o) - m\omega_o)\\ &= \mathrm{tr}(\Omega) - \Omega\,\mathrm{tr}(m\omega_o) - \mathrm{tr}(m\omega_o) - \mathrm{tr}(\Omega)m\omega_o + m\Omega\omega_o\end{aligned}$$

is an element of $\mathscr{J}$, since each component lies in $\mathscr{J}$. Hence the conjugate of $\overline{m\omega_o\Omega}$ also lies in $\mathscr{J}$. Similarly others. □

Note. *The above lemma can be proved in the same way even if k is replaced by $\overline{k}_p$ and Q by Q_p. If $K_p = K \otimes \overline{k}_p$, then the max. order in $K_p = [1, \omega_o]$ (i.e., that $\mathscr{O}_p$-module generated by $1, \omega_o$).*

Definition. *1) If $K \subset Q$ and $\mathscr{O} \subset \mathscr{J}, \mathscr{O}$ is* optimally imbedded *in $\mathscr{J}$ if $\mathscr{J} \cap K = \mathscr{O}$.*

It follows immediately from the definition that $\mathscr{O}$ is optimally imbedded in $\mathscr{J}$ if and only if $\mathscr{O}_p$ is so in $\mathscr{J}_p$ for every p.

113 **Definition.** *Consider rational integers, $D \equiv 0, 1 \pmod 4$. We define a modified Legendre symbol for these as follows:*

$$\left\{\frac{D}{p}\right\} = \begin{cases} 1 & \textit{if } \frac{D}{p^2} \textit{ integral and} \equiv 0, 1 \pmod 4\\ 0 & \textit{if } p | D \textit{ but not the former case}\\ \left(\frac{D}{p}\right) & \textit{if } p \nmid D.\end{cases}$$

Theorem 3. *Let K be a quadratic subfield of Q and $\mathscr{O}$, an order in K with discriminant D. Then there exists an order $\mathscr{J}$ in Q of type (q_1, q_2) in which $\mathscr{O}$ is optimally imbedded, if and only if,*

$$\prod_{p|q_1}\left(\left\{\frac{D}{p}\right\} - 1\right) \prod_{p|q_2}\left(\left\{\frac{D}{p}\right\} + 1\right) \neq 0.$$

We shall first prove the theorem in the local case and then extend it to the global case, i.e., for every p, there exists and order $\mathscr{J}_p$ of type (q_1, q_2) containing $\mathscr{O}_p$ optimally, under the above condition and vice-versa.

We split the proof into there parts.

(i) $p|q_1$, (ii) $p \nmid q_1q_2$, (iii) $p|q_2$.

Case (i). P/q_1. *(a) Given that* $\mathscr{O}_p \subset \mathscr{J}_p$ *optimally, to prove* $\left\{\dfrac{D}{p}\right\} \neq 1$.

Let $\mathscr{O}_o$ be the unique maximal order in K, so that $\mathscr{O} \subset \mathscr{O}_\circ$. Since $\mathscr{O}_p \subset \mathscr{O}_{op} \subset \mathscr{J}_p, (\mathscr{J}_p$ here is the unique maximal order in Q_p) and both the imbeddings being optimal, $\mathscr{O}_p = [1, f\omega_o]_p = \mathscr{O}_{op} = [1, \omega_o]_p$ or $p \nmid f$. Now, $\dfrac{D}{p^2} = \dfrac{f^2D_o}{p^2} = \dfrac{f^2d}{p^2}$ or $\dfrac{4f^2d}{p^2}$, according as $d \equiv 1 \pmod 4$ or $d \not\equiv 1 \pmod 4$. (D_o is the discriminant of $\mathscr{O}_o$ and $K = k(\sqrt{d})), d$ being square-free, in either case, (except for the latter one, when $p = 2)\dfrac{D}{p^2}$ is not an integer. In case $p = 2$, when $d \not\equiv 1 \pmod 4$, $\dfrac{D}{p^2} = f^2d \not\equiv 1, 0 \pmod 4$ for $2 \nmid f => f^2 \equiv 1 \pmod 4$ and $f^2d \equiv 0 \pmod 4 \implies 4|d$ **114** which is impossible.

Hence we have $\left\{\dfrac{D}{p}\right\} = 0$ or $\left(\dfrac{D}{p}\right)$.

Now that $\left(\dfrac{D}{p}\right) \neq 1$, in case $\left\{\dfrac{D}{p}\right\} = \left(\dfrac{D}{p}\right)$. [1]

b) Conversely, if $\left\{\dfrac{D}{p}\right\} \neq 1$, to prove that $\mathscr{O}_p \subset \mathscr{J}_p$ optimally. Since we know that $\mathscr{O}_p \subset \mathscr{O}_{op} \subset_{opt} \mathscr{J}_p$, it is sufficient to prove that $\mathscr{O}_p = \mathscr{O}_{op}$ or $p \nmid f$.

Suppose $p|f$, $\dfrac{D}{p^2} = \dfrac{f^2D_o}{p^2} \equiv 0, 1 \pmod 4$ for $D_o \equiv 0, 1 \pmod 4$. But this would mean that $\left\{\dfrac{D}{p}\right\} = 1$, which contradicts our hypothesis.

[1] For, $\left(\dfrac{D}{p}\right) = \left(\dfrac{D_o}{p}\right) \neq 1$, in case $\left\{\dfrac{D}{p}\right\} = \left(\dfrac{D}{p}\right)$.

Case (ii). *$p \nmid q_1q_2$. Given an order $\mathcal{J}_p \sim \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ \mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$, to show that there always exists an order $\mathcal{J}'_p \sim \mathcal{J}_p$ such that $\mathscr{O}_p \subset \mathcal{J}'_p$ optimally.*

Proof. Let $\mathscr{O}_p = [1, \omega]_p, \omega = f\omega_o$. Without loss of generality we may take $\omega = \begin{pmatrix} 0 & b \\ c & e \end{pmatrix} jb, c, e \in \overline{k}_p$. □

If $(b, c, e) = 1, \mathscr{O}_p \subset \mathcal{J}_p$ optimally vice-versa. In order to secure this, we will consider the element

$$\omega' = \pi^r \begin{pmatrix} 0 & b \\ c & e \end{pmatrix} \pi^{-r} = \begin{pmatrix} 0 & p^{-rb} \\ p^r c & e \end{pmatrix} \text{ where } \pi = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

and r being chosen a positive or negative integer so as to make one among $p^{-r}b$, $p^r c$, a unit. Thus $(p^{-r}b, p^r c, e) = 1$, implies that $[1, \omega']_p \subset \mathcal{J}_p$ optimally or $[1, \omega]_p \subset \pi^{-r}\mathcal{J}_p\pi^r (\sim \mathcal{J}_p)$ optimally.

115 **Case (iii).** *(a) $p|q_2$. Given that $\mathcal{J}_p \sim \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ p\mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$ and $\mathscr{O}_p \subset \mathcal{J}_p$ optimally. To show that $\left\{\frac{D}{p}\right\} \neq -1$.*

Proof. If $\mathscr{O}_p = [1, \omega]_p$ and $\omega = \begin{pmatrix} 0 & b \\ pc & e \end{pmatrix}$, ω satisfies the equation $\lambda^2 - e\lambda - pbc = 0$. Then $D = e^2 + 4pbc$. □

We have now two cases to consider

$$\alpha) p|D, \qquad \beta) p \nmid D.$$

In α), $\left\{\frac{D}{p}\right\}$ is either 1 or 0, so that we are through.

In β) $\left\{\frac{D}{p}\right\} = \left(\frac{D}{p}\right)$ and $D = e^2 + 4$ pbc $\equiv e^2 \pmod{p}$) shows that $\left(\frac{D}{p}\right) = 1$, i.e., $\left\{\frac{D}{p}\right\} \neq -1$, in either case.

Before going to the converse part of the above, we shall prove a lemma which will be useful in the sequel.

Lemma 2. *Let $\omega', \omega''(\in Q_p)$ satisfy the same quadratic polynomial over $\bar{k}_p$. Then, if $[1, \omega'']_p \subset \mathscr{J}_p$ optimally, $[1, \omega']_p$ is optimally imbedded in an order isomorphic with $\mathscr{J}_p$.*

Proof. a) By Wedderburn's Theorem, there exists an $\alpha \in Q_p$ such that $\alpha^{-1}\omega''\alpha = \omega'$ so that $[1, \omega'']_p \subset \mathscr{J}_p$ optimally implies that $[1, \omega']_p \subset \alpha^{-1}\mathscr{J}_p\alpha = \mathscr{J}'_p \sim \mathscr{J}_p$ optimally.

b) Conversely, let us suppose that $\left\{\dfrac{D}{p}\right\} \neq -1$. To prove that the order $\mathscr{O}_p \subset \mathscr{J}_p \sim \mathscr{J}_p = \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_P \\ p\mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$ optimally.

□

Let $\mathscr{O}_p = [1, \omega]_p$ where $\omega = \begin{pmatrix} 0 & b \\ c & e \end{pmatrix}, b, c, e \in \bar{k}_p$. Here again, we have two cases to distinguish:

$$(\alpha) p \nmid D, (\beta) p | D.$$

In case (α), $\left\{\dfrac{D}{p}\right\} = \left(\dfrac{D}{p}\right) = 1$ and in (β), $\left\{\dfrac{D}{p}\right\} = 1$ or 0.

(α) D being a quadratic residue mod p, $\sqrt{D}$ is a p-adic integer. Now, ω satisfies the equation 116

$$\left(\omega - \frac{e - \sqrt{D}}{2}\right)\left(\omega - \frac{e + \sqrt{D}}{2}\right) = 0,$$

since $D = d^2 + 4bc$. If $p \neq 2, \dfrac{e}{2}$ and $\dfrac{\sqrt{D}}{2}$ being p-adic integers ($e = tr\omega \in \mathscr{O}_p).\omega' = \omega - \dfrac{e - \sqrt{D}}{2} \in \mathscr{O}_p$.

In $p = 2, D$ being a quadratic residue mod 8, $\dfrac{\sqrt{D}}{2}$ is a 2-adic integer and so is $\dfrac{e}{2}$ so that $\omega' = \omega - \dfrac{e - \sqrt{D}}{2} \in \mathscr{O}_2$.

Hence the above equation can be written in the form $\omega' = (\omega' - \sqrt{D}) = 0$. Now, if $\omega'' = \begin{pmatrix} 0 & 0 \\ pc' & \sqrt{D} \end{pmatrix}$ where c' is a unit then $[1, \omega'']_p \subset$

$\mathcal{J}_p$ optimally and further ω'', ω' satisfy the same equation, so that by our lemma, we are through. 117

$(\beta) p|D$. i) $p \nmid e$, in which case, $[1, \omega]_p \subset \mathcal{J}_p$ optimally.

ii) $p|e$. Firstly, let us suppose $\left\{\dfrac{D}{p}\right\} = 0$. Now, since $D = e^2 + 4bc, p|e \implies p|4bc$, or $p|b.c$ if $p \neq 2$. Let $e = p.s$ and $b.c = p.n$, so that if $\omega' = \begin{pmatrix} 0 & b' \\ pc' & p.s \end{pmatrix}$ where $b'c' = n$ and one among b', c' is a unit. Then $[1, \omega']_p \subset \mathcal{J}_p$ and ω', ω satisfy the same equation. Our lemma is applicable and we are through.

In case $p = 2, p^2|D$ so that this will be discussed in the following :

Secondly, $\left\{\dfrac{D}{p}\right\} = 1$ or $\dfrac{D}{p^2}$ integral and $\equiv 0, 1 \pmod 4$. Now, $\dfrac{D}{p^2} = \dfrac{e^2 + 4bc}{p^2}$ is an integer and $p|e$ imply that $p^2|4bc$ or $p^2|bc$ if $p \neq 2$. Let $bc = p^2.n$ and $e = p.s$. Then the element $\omega'' = \begin{pmatrix} 0 & b \\ pc & p.s \end{pmatrix}$ where one among b, c is a unit, is such that $[1, \omega'']_p \subset \mathcal{J}_p$ optimally and ω'', ω satisfy the same equation. The application of our lemma gives the required result. Even if $p = 2$, the above argument can be applied, for

$$\frac{D}{4} = \frac{e^2}{4} + bc = 0, 1 \pmod 4 \implies bc \equiv 0, 1 \pmod 4.$$

Since $p|bc$, being even, $bc \equiv 0. \pmod 4$ or $p^2|bc$, which is essentially what we require in the above.

Thus the proof is complete for the local case. For going from the local to the global case, we distribute the primes into 2 classes.

1) p$|q_1 q_2 f$, 2) $p \nmid q_1 q_2 f$.

Class (1). Let these primes being finite in number be $p_1, \ldots, p_m$. Then, by what has already been proved, there exists an order $\mathcal{J}_{p_\nu}$ for each ν such that $\mathcal{O}_{p_\nu} \subset \mathcal{J}_{p_\nu}$ optimally. If we call $\mathcal{J}_{p_\nu} \cap Q = \mathcal{J}_\nu$, then $\mathcal{J}_{\nu p_\nu} = \mathcal{J}_{p_\nu}$ so that we may write $\mathcal{O}_{p_\nu} \subset \mathcal{J}_{\nu_{p_\nu}}$.

Class (2). These primes which constitute almost all p, we denote by p_o. By our previous lemma, there is a maximal order $\mathcal{J}_o$ such that $\mathcal{O}_o \subset$

$\mathscr{J}_o(\mathscr{O}_o$ being the maximal order in K). Therefore $\mathscr{O}_{op_o} \subset \mathscr{J}_{op_o}$ and since $p_o \nmid f, \mathscr{O}_{p_o} = \mathscr{O}_{op_o} \subset \mathscr{J}_{op_o}$ optimally. $\mathscr{J}_{op_o} = \mu^{-1}_{p_o}\mathscr{J}_{p_o}\mu_{p_o}$ (say).

Consider now $\mathscr{J} = Q \bigcap\limits_{p_\nu} \mathscr{J}_{\nu_{\nu_o}}$. $\mathscr{J}$ is an order of Q for which $(\mathscr{J})_{p_\nu} = \mathscr{J}_{p_\nu}$ and $(\mathscr{J})_{p_o} = \mathscr{J}_{p_o}$, i.e., $\mathscr{J}$is an order of type (q_1, q_2) and $\mathscr{O}_p \subset (\mathscr{J})_p$ optimally for every p, implies that $\mathscr{O} \subset \mathscr{J}$ optimally, by a previous lemma.

Thus our theorem is completely established.

Theorem 4. *Let $\mathscr{J}_1$ and $\mathscr{J}_2$ be* 2 *orders in Q, of type* (q_1, q_2), $\mathscr{O}$ *an order of a subfield K of Q, optimally imbedded in both $\mathscr{J}_1$ and $\mathscr{J}_2$. Then there exists an ideal $\mathscr{U}$ of $\mathscr{O}$ such that $\mathscr{J}_1\mathscr{O} = \mathscr{O}\mathscr{J}_2$.* 118

Conversely, *if $\mathscr{O} \subset \mathscr{J}_1$ optimally and if $\mathscr{J}_1\mathscr{U} = \mathscr{U}\mathscr{J}_2$, then $\mathscr{O} \subset \mathscr{J}_2$ optimally.*

Proof. The second part is rather easy and we shall do it first. □

Now, $\mathscr{J}_1\mathscr{U} = \mathscr{J}_1(\mathscr{U}\mathscr{O}) = (\mathscr{J}_1\mathscr{U})\mathscr{O} = \mathscr{U}\mathscr{J}_2\mathscr{O} = \mathscr{U}\mathscr{J}_2$ implies that $\mathscr{O} \subset \mathscr{J}_2$. If this imbedding were not optimal, $\mathscr{O}_p \subset \mathscr{O}'_p \underset{\text{0pt}}{\subset} (\mathscr{J}_2)_p$ for at least one p.

$\mathscr{U}_p$ being principal is is $\mathscr{O}_p\alpha_p$ (say) and $(\mathscr{J}_1\mathscr{U}_p = (\mathscr{J}_1)_p\alpha_p$ and similarly $(\mathscr{U}\mathscr{J}_2)_p = \alpha_p(\mathscr{J}_2)_p$ so that

$$(\mathscr{J}_1\mathscr{U})_p = (\mathscr{U}\mathscr{J}_2)_p \Rightarrow \alpha_p^{-1}(\mathscr{J}_1)_p\alpha_p = (\mathscr{J}_2)_p.$$

Then, $\mathscr{O}'_p \subset (\mathscr{J}_2)_p$ optimally $\Rightarrow \alpha_p\mathscr{O}'_p\alpha_p^{-1} \subset (\mathscr{J}_1)_p$ optimally which is a contradiction to the fact that $\mathscr{O} \subset \mathscr{J}_1$ optimally, since $\mathscr{O}_p \neq \alpha_p \mathscr{O}'_p\alpha_p^{-1}$.

For the first part, we observe that it is sufficient to prove it in the local case, for, then it would imply that there exist $\beta_p \in \mathscr{O}_p$ such that $(\mathscr{J}_1)_p\beta_p = \beta_p(\mathscr{J}_2)_p$ for every p and β_p are units for almost all p. Then the required ideal will be given $\mathcal{U} = \bigcap\limits_p \mathscr{O}_p\beta_p$.

For proving the theorem in the local case, we split the primes into three parts.

i) $p \mid q_1$, ii) $p \nmid q_1q_2$, iii) $p \mid q_2$.

Case (i). $p \mid q_1$. *This in trivial, for* $(\mathscr{J}_1)_p = (\mathscr{J}_2)_p = \mathscr{J}_p$ *so that* $\beta_p = 1$. 119

Case (ii). $p \nmid q_1\ q_2$. *Without loss of generality we may assume that* $(\mathcal{J}_1)_p = \begin{pmatrix}\mathcal{O}_p & \mathcal{O}_p\\ \mathcal{O}_p & \mathcal{O}_p\end{pmatrix}$*; now since* $\mathcal{J}_{2p} \simeq \mathcal{J}_{1p}$*,there exists* $\alpha \in Q_p$ *such that* $\mathcal{J}_{2p} = \alpha^{-1}\mathcal{J}_{1p}\alpha$*. We will reduce* α *to a normal form* $\alpha' = \begin{pmatrix}1 & 0\\ 0 & p^r\end{pmatrix}$ *by multiplication by units of* $\mathcal{J}_{1p}$ *on the left and right, say* $\alpha' = \varepsilon_1^{-1}\alpha\varepsilon_2^{-1}$*, i.e.,* $\alpha = \varepsilon_1\alpha'\varepsilon_2$ *then* $\mathcal{J}_{1p}\alpha = \mathcal{J}_{1p}\alpha'\varepsilon_2$ *and* $\mathcal{J}_{2p} = \varepsilon_2^{-1}(\alpha^{1-1}\mathcal{J}_{1p}\alpha')$ $\varepsilon_2 = \varepsilon_2^{-1}\mathcal{J}'_{2p}\ \varepsilon_2$*; where* $\mathcal{J}'_{2p} = \alpha'^{-1}\mathcal{J}_{1p}\alpha'$*.*

Let $\mathcal{O}'_p = \varepsilon_2\mathcal{O}_p\varepsilon_2^{-1}$, then

$$\mathcal{O}_p \underset{0pt}{\subset} \mathcal{J}_{1p} \Rightarrow \mathcal{O}'_p \underset{0pt}{\subset} \varepsilon_2\mathcal{J}_{1p}\varepsilon_2^{-1} = \mathcal{J}_{1p},$$
$$\mathcal{O}_p \underset{0pt}{\subset} \mathcal{J}_{2p} \Rightarrow \mathcal{O}'_p \underset{0pt}{\subset} \varepsilon_2\mathcal{J}_{2p}\varepsilon_2^{-1} = \mathcal{J}'_{2p},$$

The conditions of the theorem being satisfied for $\mathcal{J}_{1p}, \mathcal{J}'_{2p}, \mathcal{O}'_p$, we show that there exists an $\mathcal{O}_p$ -ideal $\mathcal{U}'_p$ such that

$$\mathcal{J}_{1p}\mathcal{U}'_p = \mathcal{U}'_p\mathcal{J}'_{2p},$$

from this we would obtain on putting $\mathcal{U}'_p = \varepsilon_2\mathcal{U}_p\varepsilon_2^{-1}$ that $\mathcal{J}_{1p}\varepsilon_2\mathcal{U}_p\varepsilon_2^{-1} = \varepsilon_2\mathcal{U}_p\varepsilon_2^{-1}.\ \varepsilon_2\mathcal{J}_{2p}\varepsilon_2^{-1}$; i.e., $\mathcal{J}_{1p}\mathcal{U}_p = \varepsilon_2\mathcal{U}_p\mathcal{J}_{2p}$, or $\mathcal{J}_{1p}\mathcal{U}_p = \mathcal{U}_p\mathcal{J}_{2p}$ since ε_2 is a unit in $\mathcal{J}_{1p}$.

120 Therefore we may assume that α itself is of the form

$$\alpha = \begin{pmatrix}1 & 0\\ 0 & p^r\end{pmatrix}, \mathcal{J}_{2p} = \begin{pmatrix}\mathcal{O}_p & p^r\mathcal{O}_p\\ p^{-r}\mathcal{O}_p & \mathcal{O}_p\end{pmatrix}.$$

Now,

$$\mathcal{O}_p = [1, \omega]_p \text{ with } \omega = \begin{pmatrix}0 & b\\ c & d\end{pmatrix}.$$

Since ω is optimally contained in $\mathcal{J}_{1p}$ (i.e., $\mathcal{O}_p \subset \mathcal{J}_{1p}$ optimally) we have $(b, c, d) = 1$ and since ω is optimally contained in $\mathcal{J}_{2p}$, we have $(p^{-1}b, p^r c, d) = 1$. It is enough to find $\beta \in \mathcal{O}_p$ such that

$$\mathcal{J}_{1p}\beta = \beta\mathcal{J}_{2p} \tag{1}$$

Now (1) will be satisfied if $\beta\alpha^{-1} = \varepsilon$ is a unit in $\mathcal{J}_{1p}$. For, then

$$\mathcal{J}_{1p}\beta = \mathcal{J}_{1p}\alpha = \beta\alpha^{-1}\mathcal{J}_{1p}\alpha = \beta\mathcal{J}_{2p}.$$

So let $\beta = u + v\omega$, $u, v \in \mathscr{U}_p$, then

$$\beta = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} + \begin{pmatrix} 0 & vb \\ vc & vd \end{pmatrix} = \begin{pmatrix} u & vb \\ vc & u+vd \end{pmatrix}$$

so that $$\beta\alpha^{-1} = \begin{pmatrix} u & vb \\ vc & u+vd \end{pmatrix} \begin{pmatrix} 1 & \\ o & p^{-r} \end{pmatrix} = \begin{pmatrix} u & p^{-r}vb \\ vc & p^{-r}(u+vd) \end{pmatrix}$$

Put $v = 1$, $u = -d + p^r.\ u_1$, then

$$|\beta\alpha^{-1}| = (-d + p^r u_1)u_1 - p^{-r}bc.$$

If

(i) $(d, p) = 1$, we can choose u_1 such that $|\beta\alpha^{-1}| =$ unit.

(ii) $(d, p) \neq 1$, i.e., $p \mid d$, then $(p^{-r}bc, p) = 1$, and taking $u_1 = 0$, $|\ \beta\alpha^{-1}\ |$ is again a unit. 121

Case (iii). *$p \mid q_2$. We assume $\mathcal{J}_{1p} = \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ p\mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$, and since $\mathcal{J}_{2p} \cong \mathcal{J}_{1p}$ there is an $\alpha \in Q_p$ such that $\mathcal{J}_{1p}\alpha = \alpha\mathcal{J}_{2p}$. We have already seen that by multiplication on the left by a unit in $\mathcal{J}_{1p}$, α can be reduced to one of the normal forms*

$$\eta_1\alpha = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix} c \textit{ reduced} \mod p^b,$$

or $$\begin{pmatrix} 0 & p^a \\ p^{b+1} & 0 \end{pmatrix} c \textit{ reduced} \mod p^{a+1}, \eta_1 - \textit{ unit.}$$

It is enough to consider the first normal form, for if $\eta_1\alpha$ is in the second normal form, by multiplication on the left by

$$\pi = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \text{ we obtain}$$

$$\pi\eta_1\alpha = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix} = \begin{pmatrix} p^{b+1} & c \\ 0 & p^{a+1} \end{pmatrix}$$

so that by suitable multiplication on the left and right by powers of π, we may assume that $\alpha = \pi^{r_1}\eta_1\alpha\pi^{r_2}$ has the same norm as α, and that it is in the first normal form.

We have now to consider the following cases:

(i) $b = 0$. If $b = 0$, then $c = 0$, and

$$\pi^{r_1}\eta_1\alpha\pi^{r_2} = \begin{pmatrix} p^a & 0 \\ 0 & 1 \end{pmatrix}.$$

By multiplication on the right by π and on the left by π^{-1}, we have

$$\begin{pmatrix} 0 & \frac{1}{p} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p^a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^a \end{pmatrix}$$

122 (ii) $a = 0$. $\pi^{r_1}\eta_1\alpha\pi^{r_2} = \begin{pmatrix} 1 & c \\ 0 & p^b \end{pmatrix}$, and we have

$$\pi^{r_1}\eta_1\alpha\pi^{r_2} \begin{pmatrix} 1 & -c \\ 0 & p^b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p^b \end{pmatrix}$$

(iii) $a > 0$, $b > 0$. We may assume that $(c, p) = 1$, otherwise $\alpha|p$ instead of α would serve the same purpose. Multiplying on the left by a unit, and on the right by π^{-1}, we obtain $\begin{pmatrix} 1 & c' \\ 0 & p^{b'} \end{pmatrix}$, and again multiplying on the right by $\begin{pmatrix} 1 & -c' \\ 0 & 1 \end{pmatrix}$, we arrive at $\begin{pmatrix} 1 & 0 \\ 0 & p^{b'} \end{pmatrix}$.

Hence in all cases, α is of the form $\alpha = \varepsilon_1\pi^{r_1} \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \pi^{r_2}\varepsilon_2$. The transformed orders will now be of the form

$$\mathcal{J}'_{2p} = \varepsilon_2\pi^{r_2}\mathcal{J}_{2p}.\pi^{-r_2}\varepsilon_2^{-1}, \varepsilon_2 \text{ unit in } \mathcal{J}_{1p}.$$
$$\mathcal{O}'_p = \varepsilon_2\pi^{r_2}\mathcal{O}_p\pi^{-r_2}\varepsilon_2^{-1}, \text{ then since}$$

$$\mathscr{O}_p \underset{0pt}{\subset} \mathscr{J}_{1_p},\ \text{we have } \mathscr{O}'_p \underset{0pt}{\subset} \mathscr{J}'_{2p},\ \text{also}$$
$$\mathscr{O}'_p \underset{0pt}{\subset} \mathscr{J}_{1p} \text{ since } \mathscr{J}_{1p} = \varepsilon_2\pi^{r_2}\mathscr{J}_{1_p}\pi^{-r_2}\varepsilon_2^{-1}$$

As in case (ii) we change notations and prove the theorem under the assumption
$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix};$$
$\mathscr{O}_p = [1,\omega]_p$ is optimally imbedded in $\mathscr{J}_{1p} = \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ \mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$ and in $\mathscr{J}_{2p} = \begin{pmatrix} \mathscr{O}_p & p^r & \mathscr{O}_p \\ p^{1-r} & \mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$. ω is optimal in $\mathscr{J}_{1p} \Rightarrow (b,c,d) = 1$, again since ω is 123 optimal in $\mathscr{J}_{2p} \Rightarrow (p^{-r}b, p^r.c, d) = 1$. As before we take $\beta = u+\omega, \omega = \begin{pmatrix} 0 & b \\ pc & d \end{pmatrix}$ and show that β can be so chosen that $\beta\alpha^{-1}$ is a unit of $\mathscr{J}_{1p}$. Now as before $|\beta\alpha^{-1}| = (-d+p^r u_1)u_1 - p^{1-r}b.c$; where $u = -d + p^r u_1$.

(i) If $(p,d) = 1$, then u_1 can be chosen such that $|\beta\alpha^{-1}|=$ unit.

(ii) If $(p,d) = p, i.e., p \mid d$; we consider $\beta(\pi\alpha)^{-1}$, if we put $u_1 = 0$, $(-d+\omega)(\pi\alpha)^{-1} = \begin{pmatrix} -d & b \\ pc & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \dfrac{1}{p} \end{pmatrix}\begin{pmatrix} 0 & \dfrac{1}{p} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p^{-r}b & \dfrac{-d}{p} \\ 0 & c \end{pmatrix}$ or $|(-d+\omega)(\pi\alpha)^{-r}| = p^{-r}b.c.$

Now since $(p^{-r}b,p) = 1$, and $(c,p) = 1$, we have $(p^{-r}bc,p) = 1$, i.e., $p^{-r}bc$ is a $p-$adic unit, so that $\beta = \epsilon\pi\alpha, \epsilon$, unit in $\mathscr{J}_{1p}$. In this case, again we have $\mathscr{J}_{1p}\beta = \mathscr{J}_{1p}\pi\alpha = \pi\mathscr{J}_{[}1p]\alpha = \pi\alpha\mathscr{J}_{2p} = \beta\mathscr{J}_{2p}$. In order to complete the proof of the theorem, we have only to show that β is a unit of $\mathscr{O}_p$ for almost all p and it is enough to verify this in the case $p \nmid q_1q_2$.

This is secured by taking among the primes $p \nmid q_1q_2$, only those for which both b and c are p-adic units. Then
$$|\beta| = |\begin{pmatrix} u & b \\ c & u+d \end{pmatrix}| = p^r.u_1(p^r.u_1 - d) - bc$$
is always a $p-$ adic unit. Or, β is a unit of $\mathscr{O}_p$.

Thus in $\mathcal{J}_{1p}\beta_p = \beta_p\mathcal{J}_{2p}, \beta_p$ is a unit for almost all p so that the global ideal $\mathscr{O} = \bigcap_p \mathscr{O}_p\beta_p$ serves our purpose.

124 **Remark.** The theorem proved above is a very important one for our further applications and it has been proved in various connections and in various forms by several mathematicians dating from Legendre, Gauss, Minkowski and Emmy Noether to Hasse, Chevalley and Siegel. Chevalley and Hasse proved an analogous result in the theory of algebras while Siegel required a similar form for the theory of quadratic forms.

3. Let $\mathscr{O}$ be an order of a quadratic subfield K of Q optimally imbedded in an order $\mathcal{J}$ of Q of type (q_1, q_2). Let D denote the discriminant of $\mathscr{O}$. We have then the following

Theorem 5. *An ambiguous prime ideal v with norm p is generated by an $\mathscr{O}$ -ideal $\mathscr{U}$ if and only if* $\left\{\frac{D}{p}\right\} = 0.$

Proof. Since all global ideals are defined as intersections of local ones, it is sufficient to prove the theorem for the p-adic case. □

For the proof in the local case, we have three possibilities :
(i) $p \nmid q_1q_2$, (ii) $p|q_1$, (iii) $p|q_2$.

Case (i). $p+q_1q_2$. *In this case, we shall prove that there do not exist any proper* $(i.e., \vartheta_p \neq \mathcal{J}_p.p^r)$ *ambiguous ideals ϑ_p at all so that the above problem does not arise.*

$\mathcal{J}_p \cong \begin{pmatrix} \mathscr{O}_p & \mathscr{O}_p \\ \mathscr{O}_p & \mathscr{O}_p \end{pmatrix}$; if $\vartheta_p = \mathcal{J}_p\pi$ is ambiguous, and if we assume π to be without loss of generality, of the form, $\pi = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix} a + b = s; c$ reduced $mod p^p$, then $\mathcal{J}_p\pi = \pi\mathcal{J}_p$ implies that 125

$$\begin{pmatrix} p^{-a} & -cp^{-(a+b)} \\ 0 & p^{-b} \end{pmatrix}\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}$$
$$= \begin{pmatrix} p^{-a}x_1 - cx_3p^{-(a+b)} & p^{-a}x_2 - cx_4p^{-(a+b)} \\ p^{-b}x_3 & p^{-b}x_4 \end{pmatrix}\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}$$

$$= \begin{pmatrix} x_1 - cx_3p^{-b} & cp^{-a}x_1 - c^2x_3p^{-(a+b)} + p^{b-a}x_2 - cx_4p^{-a} \\ p^{a-b}x_3 & cp^{-b}x_3 + x_4 \end{pmatrix}$$

must be an integral matrix for all $x_1, x_2, x_3, x_4 \in \mathscr{O}_p$. Choosing x_3 to be a unit, $a \geq b$ and x_1 to be divisible by p, $p^b|c$, which implies $c = 0$ since c is reduced modulo p^b. Hence, if we further choose x_2 to be a unit, $b \geq a$ so that $a = b$ and $c = 0$, *i.e.*, $\pi = \begin{pmatrix} p^r & 0 \\ 0 & p^r \end{pmatrix}$ where $a = b = r$ and $2r = s$. Hence $\vartheta_p = \mathscr{J}_p.p^r$.

Case (ii). $p|q_1$. *If $\mathscr{O}_\circ$ is the maximal order of K,*

$$\mathscr{O}_p \subset \mathscr{O}_{op} \subset \mathscr{J}_p \Rightarrow \mathscr{O}_p = \mathscr{O}_{op} \text{ and } \left\{\frac{D}{p}\right\} = \left(\frac{D}{p}\right) \neq 1,$$

by theorem 1. Therefore if $\left(\frac{D}{p}\right) = \frac{D_o}{p} = 1$, *where D_o is the discriminant of $\mathscr{O}_0$ so that K_p is unramified over $\bar{k}_p$ which implies that there cannot exist any $\mathscr{O}_j p$-ideal generating ϑ_p. On the other hand, if* $\left(\frac{D_0}{p}\right) = 0$, *then K_p is ramified over $\bar{k}_p$, there exists an $\mathscr{O}_p$ -ideal $\mathscr{U}_p$ such that $p\mathscr{O}_p = \mathcal{U}_p^2$ and $N(\mathscr{U}_p) = p$ and by the uniqueness of such an ideal $\vartheta_p = \mathscr{J}_p.\ \mathscr{U}_p$.*

Case (iii). $p|q_2$. *Again, by theorem 1,* $\left\{\frac{D}{R}\right\} \neq -1$.

a) $\dfrac{D}{p^2}$ integral and $\equiv 0, 1 \pmod 4$. $\mathscr{O}_p = [1, p^{r_\omega}] \underset{0pt}{\subset} \mathscr{J}_p$ where $\mathscr{O}_{op} =$ 126
$[1, \omega]$ (say). Let $\vartheta_p = \mathscr{J}_p\delta$, $\delta \in \mathscr{O}_p$, then $n(\delta) = p$ and $\delta = a + bp^{r_\omega}$; $a, b \in \mathscr{O}_p$. Hence $n(\delta)$ is either a unit or $\equiv 0 \pmod{p^2}$ in either case we obtain a contradiction.

b) $\left\{\dfrac{D}{p}\right\} = \left(\dfrac{D}{p}\right) = 1$.

Let $\vartheta_p = \mathscr{J}_p\alpha_p, \alpha_p \in \mathscr{O}_p$; we, may assume without loss of generality $\mathscr{O}_p = \left[1, \begin{pmatrix} 0 & b \\ pc & d \end{pmatrix}\right]$. Since there is only one ambiguous prime ideal of norm p, namely $\mathscr{J}_p\pi, \mathscr{J}_p\alpha_p = \mathscr{J}_p\pi$ or $\alpha_p\pi^{-1}$ is a unit of $\mathscr{J}_p$.

Now, $D = d^2 - 4pbc$ and $p \nmid D \Rightarrow p \nmid d$ so that if $\alpha_p \in \mathscr{O}_p$, *i.e.*, $\alpha_p = u + v\omega$ where $\omega = \begin{pmatrix} 0 & b \\ pc & d \end{pmatrix}$ then $\alpha_p \pi^{-1} = \begin{pmatrix} bv & u/p \\ u + vd & cv \end{pmatrix}$ is a unit $\Rightarrow p|u$ and $p|u + vd$, *i.e.*, $p|vd$ or $p|v$. In other words, $|\alpha_p \pi^{-1}| \equiv 0(mod p)$ so that $\alpha_p \pi^{-1}$ cannot be a unit.

c) $\left\{\dfrac{D}{p}\right\} = 0. \left(\dfrac{D}{p^2} \not\equiv 0, 1 \pmod 4\right).$

$D = d^2 - 4pbc \equiv 0 \pmod p \Rightarrow d \equiv 0 \pmod p$. Further $p \nmid bc$ for otherwise, $\dfrac{D}{p^2} \equiv \dfrac{d^2}{p^2} \pmod 4$ and $\equiv 0, 1 \pmod 4$ which is a contradiction to the hypothesis.

Consider $\omega\pi^{-1} = \begin{pmatrix} 0 & b \\ pc & d \end{pmatrix} \begin{pmatrix} 0 & 1/p \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & o \\ d & c \end{pmatrix}$ is a unit of $\mathscr{J}_p$ by virtue of $p|d$, $p \nmid bc$ so that $\mathscr{J}_p\omega = \mathscr{J}_p\pi$. In other words, the unique ambiguous prime ideal of norm p is $\vartheta_p = \mathscr{J}_p\omega$.

Note. *Let ϑ be an ambiguous ideal with norm n and let $n = p_1^{\varrho_1} \cdots p_k^{\varrho_k}$. Then we know that $\vartheta = \bigcap_p \varepsilon_p$; $\vartheta_p = \mathscr{J}_p$ for almost all p and for the rest $n(\vartheta_{pi}) = p_i^{\mathscr{U}}$.*

127 ϑ_p being ambiguous for all primes $p \nmid q_1q_2$, ϑ_p is a rational ideal; i.e., $\vartheta_p = \mathscr{J}_p\lambda_p$; λ_p, a p-adic number and since $\vartheta_p = \mathscr{J}_p$ for almost all p, λ_p is a p-adic unit for all but a finite number of $p \nmid q_1q_2$. Among the primes p_i that occur in the factorization of n, let $p_1 \cdots p_l$ (suitably rearranged) by those which divide q_1q_2 and for these, $\vartheta_{pi} = \mathscr{J}_{pi}\pi_i^{\varrho_i}$ $(i = 1$ to $l)$ where $n(\pi_i) = p_i$ so that we may write symbolically $\vartheta = \mathscr{J}.r.\delta_1^{\varrho_1} \cdots \delta_l^{\varrho_l}$ where $\delta_i = \mathscr{J}_{p_i}\pi_i(p_i/q_1q_2n)$ and r is a rational number. Since $\mathscr{J}_{p_i}\pi_i^2 = \mathscr{J}_{p_i}.p_i$, the indices $\varrho_1 \ldots \varrho_l$ can be reduced mod 2; i.e., $\varrho_i = 0, 1$.

From the above factorization we immediately deduce that the total number of proper ambiguous ideals i.e., upto multiplication by a rational number) is 2^x, x being the number of primes $p|q_1q_2$.

From theorem 3, deduce that $2^{x'}$ is the number of ambiguous ideals generated by means of $\mathscr{O}-$ ideals where x' is the number of primes p for which $\left\{\dfrac{D}{p}\right\} = 0$ among those which divide $q_1 q_2$. Therefore the order of the quotient group is $2^{x-x'} = \prod\limits_{p|q_1}\left(1 - \left\{\dfrac{D}{p}\right\}\right)\prod\limits_{p|q_2}\left(1 + \left\{\dfrac{D}{p}\right\}\right)$.

4. We shall now prove the last theorem of this section, which sums up previous ones and which will be applied later for computing the traces of correspondences.

If $\mathscr{O}$ is an order of a subfield $K \subset Q$ such that if $\mathscr{O} \underset{\text{0pt}}{\subset} \mathscr{J}$ and ε, a unit of $\mathscr{J}$, then $\varepsilon^{-1}\mathscr{O}\varepsilon \underset{\text{0pt}}{\subset} \mathscr{J}$. Thus, with each order $\mathscr{O} \underset{\text{0pt}}{\subset} \mathscr{J}$, a whole class of orders $\{\varepsilon^{-1}\mathscr{O}\varepsilon\}$ is optimally contained in $\mathscr{J}$. Of course, $\varepsilon^{-1}\mathscr{O}\varepsilon \subset \varepsilon^{-1}\ K\varepsilon \sim K$. We shall restrict our attention to only proper classes of orders $\{\varepsilon^{-1}\mathscr{O}\varepsilon; n(\varepsilon) = +1\}$.

Theorem 6. *The number of proper classes of orders $\{\varepsilon^{-1}\mathscr{O}\varepsilon\}$ optimally* 128
imbedded in an order $\mathscr{J}$ of type (q_1, q_2) (where class number of ideals is 1) *and isomorphic to a given order $\mathscr{O}_\circ \subset K \subset Q$ (Q indefinite and K, imaginary) is equal to the following product*

$$\prod_{p|q_1}\left(1 - \left\{\frac{D}{p}\right\}\right)\ \prod_{p|q_2}\left(1 + \left\{\frac{D}{p}\right\}\right)h(D),$$

D being the discriminant of $\mathscr{O}_\circ$ and $h(D)$, the class number of $\mathscr{O}_\circ$-ideals.

Proof. $\mathscr{O}_\circ$ is the given fixed order, optimally imbedded in $\mathscr{J}$ and $\mathscr{O}$, any other order, isomorphic to $\mathscr{O}_\circ$, and optimally imbedded in $\mathscr{J}$. Since the class number of $\mathscr{J}$-ideals is 1, there exists an $\alpha \in Q$ such that $\mathscr{O} = \alpha\mathscr{O}_\circ\alpha^{-1}$. □

Now, defining $\mathscr{J}' = \alpha^{-1}\mathscr{J}\alpha$, we find that

$$\mathscr{O} \underset{\text{0pt}}{\subset} \mathscr{J} \Rightarrow \alpha^{-1}\mathscr{O}\alpha \underset{\text{0pt}}{\subset} \mathscr{J}' \text{ or } \mathscr{O}_\circ \underset{\text{0pt}}{\subset} \mathscr{J}'.$$

$\mathscr{O}_\circ$ being contained optimally in both $\mathscr{J}$ and $\mathscr{J}'$ of type (q_1, q_2), by our previous theorem, there exists an $\mathscr{O}_\circ$ -ideal $\mathscr{U}$ such that $\mathscr{J}\mathscr{U} = \mathscr{U}\mathscr{J}'$. In other words, $\mathscr{J}\mathscr{U}\alpha^{-1}\alpha = \mathscr{U}\alpha^{-1}\mathscr{J}\alpha$ or $\mathscr{J}\mathscr{U}\alpha^{-1} = \vartheta$ is an ambiguous $\mathscr{J}-$ideal. Without loss of generality, we may assume that ϑ contains in its decomposition, no ideal generated by an $\mathscr{O}_\circ$ -ideal, for if $\vartheta = b\vartheta'\ b$ is generated by an $\mathscr{O}_\circ$ -ideal, we may combine b with $\mathscr{U}$ with have ϑ' instead of ϑ.

We now make correspond to the pair $(\mathscr{O}, \mathscr{O}_\circ)$, the pair of ideals $(\vartheta, \mathscr{U})$. α is not uniquely determined by the condition $\alpha\mathscr{O}_\circ\alpha^{-1} = \mathscr{O}$. In fact

i) α can be replaced by $\alpha\mu$, $\mu \in K$, in which case $\mathscr{U} \to \mathscr{U}\mu$ and $\vartheta \to \vartheta$.

129 ii) α can even be replaced by $\alpha\mu\omega$ where $\omega \in Q$ and $\infty^{-1}K\omega = K^\sigma$, σ being the only automorphism of K/k different from the identity, so that $\omega^{-1}\mathscr{O}_\circ\omega = \mathscr{O}_\circ$ and $\mathscr{O} \to \mathscr{O}$.

But here for $\mathscr{U}$, we cannot take the ideal $\mathscr{U}'\omega^{-1}\mu^{-1}$ (where $\mathcal{J}\mathscr{U}' = \mathscr{U}'\mathcal{J}''$; $\mathcal{J}'' = (\alpha\mu\omega)^{-1}\mathcal{J}(\alpha\mu\omega)$) since it is no longer an $\mathscr{O}_\circ$ -ideal.

$\mathscr{U} \sim \mathscr{U}/ \Rightarrow$ there exists $\mu' \in K$ such that $\mathscr{U}\mu' = \mathscr{U}$, in which case $\vartheta' = \mathcal{J}\mathscr{U}'.\ \omega^{-1}\mu^{-1}\alpha^{-1} = \mathcal{J}\mathscr{U}\mu'.\ \omega^{-1}\mu^{-1}\alpha^{-1} = \vartheta = \mathcal{J}\mathscr{U}\alpha^{-1}$ if and only if $\eta = \mu'\omega^{-1}\mu^{-1}$ is a unit of $\alpha^{-1}\mathcal{J}\alpha = \mathcal{J}'$.

Consequently, if we now make correspond to every pair of classes of orders $((\mathscr{O}), (\mathscr{O}_\circ))$ ($\mathscr{O}$ optimally imbedded in $\mathcal{J}$ and isomorphic to $\mathscr{O}_\circ$) the pair $(\vartheta, (\mathscr{U}))$ ($(\mathscr{U})$ denoting the class of $\mathscr{O}_\circ$ -ideals equivalent to $\mathscr{U}$, and ϑ is an integral ambiguous $\mathcal{J}$ -ideal not divisible by an $\mathcal{J}$-ideal generated by an $\mathscr{O}_\circ$ -ideal), then to a pair $((\mathscr{O}), (\mathscr{O}_\circ))$ there correspond exactly one or two pairs $(\vartheta, (\mathscr{U}))$ according as there does or does not exist a unit of the type $\mu'\omega^{-1}\mu^{-1}$ in $\mathcal{J}'$.

We shall now consider the converse map. Let $(\vartheta, (\mathscr{U}))$ be a pair, ϑ ambiguous and $(\mathscr{U})$, an $\mathscr{O}_\circ$ -ideal class such that there exists an $\alpha \in Q$ such that $\mathcal{J}\mathscr{U} = \vartheta\alpha$. We may suppose that ϑ does not contain any $\mathscr{O}_\circ$ - ideal. Then, we associate to the pair $(\vartheta, (\mathscr{U}))$ the pair $(\mathscr{O}, \mathscr{O}_\circ)$ where $\mathscr{O} = \alpha\mathscr{O}_\circ\alpha^{-1}$. Now, $\vartheta\alpha = \mathcal{J}\mathscr{U}$, holds even if we replace α 130 by $\varepsilon\alpha$, ε being a unit of $\mathcal{J}$. But then $\mathscr{O} \to \varepsilon\alpha\mathscr{O}_\circ\alpha^{-1}\varepsilon^{-1} = \varepsilon\mathscr{O}\varepsilon^{-1}$ so that $\varepsilon\mathscr{O}\varepsilon^{-1}$ would properly be equivalent with $\mathscr{O}$ only if there exists a proper unit ε_+ such that $\varepsilon\mathscr{O}\varepsilon^{-1} = \varepsilon_+\mathscr{O}\varepsilon_+^{-1}$. Therefore, the mapping $(\vartheta, \mathscr{U})) \to ((\mathscr{U}, (\mathscr{O}_\circ))((\mathscr{O})$ being the proper class of $\mathscr{O}$) is in general two - valued or single-valued if and only if there does not exist or does exist a unit $\varepsilon \in \mathscr{J}$ of norm -1 with the property that $\varepsilon\mathscr{O}\varepsilon^{-1} = \varepsilon_+\mathscr{O}\varepsilon_+^{-1}$ for a unit ε_+ of norm 1.

We now observe the following :

The existence of $\eta = \mu'\omega^{-1}\mu^{-1}$, a unit in $\mathscr{J}' \Longleftrightarrow$ the existence of ε, a unit of $\mathscr{J}$ with $n(\varepsilon) = -1$ such that $\varepsilon\mathscr{O}\varepsilon^{-1} = \varepsilon_+\mathscr{O}\varepsilon_+^{-1}$ for some ε_+ a unit of $\mathscr{J}$ with norm 1.

Now, $n(\eta) = n(\mu')(\mu')(n(\omega))^{-1}n(\mu^{-1}) = n(\mu'')$. $(n(\omega))^{-1}$ if $\mu'' = \mu'$. $\mu^{-1} \in Q$. Therefore $n(\eta)$ and $n(\omega)$ are of the same sign. But $n(\omega)$ is < 0 for otherwise, $K = k(\delta)$ with $\delta^2 < 0$ implies that $n(\delta) > 0$ and if $n(\omega) > 0$, then $Q = k[1, \delta, \omega, \delta\omega]$ would be definite, contradictory to our hypothesis. Therefore $n(\eta) = -1$. Let ε be any unit of $\mathscr{J}$ of norm -1. Then, if $\varepsilon_+ = \varepsilon\alpha\eta\alpha^{-1}$, we have

$$\begin{aligned}\varepsilon_+\mathscr{O}\varepsilon_+^{-1} &= \varepsilon\alpha\eta\alpha^{-1}\mathscr{O}\alpha\eta^{-1}\alpha^{-1}\varepsilon^{-1} = \varepsilon\alpha\eta\mathscr{O}_\circ\eta^{-1}\alpha^{-1}\varepsilon^{-1}\\ &= \varepsilon\mathscr{O}\varepsilon^{-1}(\text{ since } \eta\mathscr{O}_\circ\eta^{-1} = \mathscr{O}_\circ).\end{aligned}$$

Conversely, if for an ε of norm -1, $\varepsilon\mathscr{O}\varepsilon^{-1} = \varepsilon_+\mathscr{O}\varepsilon_+^{-1}$ then take for $\eta = \alpha^{-1}\varepsilon\varepsilon_+\alpha$.

We may therefore conclude the following:

The direct mapping $((\mathscr{O}), (\mathscr{O}_\circ)) \to (\vartheta, (\mathscr{U}))$ is single valued if and only if the inverse mapping is single-valued. The sets being finite, combining this fact with both the mappings by an enumerative argument, 131 we obtain a $1-1$ correspondence in the above. The classes of orders $(\mathscr{O})$ which are optimally imbedded in $\mathscr{J}$ and isomorphic with $(\mathscr{O}_\circ)$ is equal to the number of pairs $((\mathscr{O}), (\mathscr{O}_\circ))$ which in turn is thus equal to the number of pairs, $(\vartheta, (\mathscr{U}))$. But by the deduction from Theorem 5, the number of ambiguous ideals not containing $\mathscr{O}_\circ$ - ideals is given by

$$\prod_{p|q_1}\left(1 - \left\{\frac{D}{p}\right\}\right) \prod_{p|q_2}\left(1 + \left\{\frac{D}{p}\right\}\right)$$

and the number of ideal classes $\{\mathscr{U}\}$ is $h(D)$, so that the required number is given by

$$\prod_{p|q_1}\left(1 - \left\{\frac{D}{p}\right\}\right) \prod_{p|q_2}\left(1 + \left\{\frac{D}{p}\right\}\right) h(D).$$

Note. *If Q is definite, the above arguments have to be slightly modified and the number of units of $\mathscr{J}$ being finite, we can show by a slightly different argument, that the number of classes is given by*

$$\frac{\textit{number of units in}\mathscr{J}}{2}\prod_{p|q_1}\left(1-\left\{\frac{D}{p}\right\}\right)\prod_{p|q_2}\left(1-+\left\{\frac{D}{p}\right\}\right)h(D)$$

(if again, the class number of $\mathscr{J}$ -ideals is 1).

10 Applications, Especially to the Calculation of the Number of Fixed Points of a Correspondence T_n

5. We shall first take up the number of elliptic vertices of the fundamental domain of the proper unit group of an order $\mathscr{J}$ of type (q_1, q_2) of an indefinite quaternion algebra Q over the rational number field k. We will take up the calculation of parabolic cusps, later, since this does not require any of the theorems we have proved so far.

132 **1.** If τ is an elliptic vertex and $\varepsilon(\tau) = \tau$, then ε is a transformation of finite order, $\varepsilon^n = 1$ (say). But $\varepsilon \in Q$ satisfies $\varepsilon^2 - s.\ \varepsilon + 1 = 0$. Now, if D is the discriminant of this equation, then ε lies in the field $K = k(\sqrt{D})$ and $D < 0$ implies that $n = 3, 4$ or 6. When $n = 4, D = -4$ and when $n = 3$ or 6, $D = -3$. If $\mathscr{O} = [1, \varepsilon]$, then $\mathscr{O}$ is a maximal order optimally contained in $\mathscr{J}$ and $D(\mathscr{O}) = D$.

As we have already seen in §5, to an elliptic vertex τ of δ (actually $\Gamma.\tau$), there corresponds a class $\eta^{-1}\varepsilon\eta\,(n(\eta) = 1, \eta \in \Gamma)$ and to each such class, there corresponds the proper class of orders $\eta^{-1}\mathscr{O}\eta$. It is easily seen that this correspondence is one-one so that the number of elliptic vertices is equal to the number of isomorphic classes of orders $(\mathscr{O})$, optimally contained in $\mathscr{J}$. By theorem 4, this number is given by

$$\prod_{p|q_1}\left(1-\left\{\frac{D}{p}\right\}\right)\prod_{p|q_2}\left(1+\left\{\frac{D}{p}\right\}\right)h(D), D = D(\mathscr{O}).$$

i) If $n = 4$, $D = -4$ and this number is

$$\prod_{p|q_1}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-4}{p}\right)\right).1$$

since the modified Legendre symbol is the ordinary Legendre symbol and $h(D) = 1$.

ii) If $n = 3$ or 6, $D = -3$ and this number is then

$$\prod_{p|q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-3}{p}\right)\right).1$$

for the same reason as before.

Representation of a Natural Number as a Sum of Three Squares.

6 Let d be a negative rational integer and $K = k(\sqrt{d})$ ($-d$ squarefree). Let $Q = k(1, i, j, k)$ be the Hamiltonian quaternion algebra over the rational number field k. Then Q is definite and $K \subset Q$. 133

Now, the order $\mathcal{J} = (i, j, k, \frac{1+i+j+k}{2})$ is maximal in Q so that $q_2 = 1$. The only characteristic prime of Q is 2 and the class number of $\mathcal{J}$ is 1. The units in $\mathcal{J}$ are 24 in number and are given by

$$\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}.$$

For the maximal order $\mathscr{O}_\circ = [1, \omega] \subset K, \omega = \sqrt{d}$ if $d \not\equiv 1 \pmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. Taking the basis representation of ω, we have

i) $\omega = X_1 i + X_2 j + X_3 k$, if $d \not\equiv 1 \pmod 4$, or

ii) $\omega = \frac{1 + X_1 i + X_2 j + X_3 k}{2}$, if $d \equiv 1 \pmod 4$.

But, in either case,

$$X_1^2 + X_2^2 + X_3^2 = -d.$$

It is easily seen that every representation of $-d$ as a sum of three squares as above as above, is in one-one correspondence with a class of orders $(\mathscr{O})$, isomorphic with the class $(\mathscr{O}_\circ)$ and optimally contained in $\mathcal{J}$, so that this number is given by (from Note to Theorem 4, §9)

$$12(1-(\frac{D}{2}))h(D),\ D = D(\mathscr{O}_\circ) = 4d \text{ or } d$$

according as $d \not\equiv 1 \pmod 4$ or $d \equiv 1 \pmod 4$.

7. We shall now take up the third application, namely the calculation of fixed points of a correspondence T_n. The fixed points are of two typed, i) finite and ii) infinite. Firstly, we shall consider the finite ones, i.e., points $\Gamma_{\mathcal{J}}.\tau$ on $S_{\mathcal{J}}$ where $\operatorname{Im}\tau > 0$. In case

$$n = m^2, T_n = \sum_{n(\mathcal{J}\nu_i)=m} \Gamma_{\mathcal{J}}.\nu_i = T_n^* + \Gamma_{\mathcal{J}}.m \text{ where } T_n^* = \sum_{\mathcal{J}\nu_i \neq \mathcal{J}m} \Gamma_{\mathcal{J}}\nu_i.$$

134 For $\Gamma_{\mathcal{J}}.m$, all points are fixed points and Lefschetz' theorem is not applicable, so that we consider only T_n^*. In case $n \neq m^2$, if $\Gamma_{\mathcal{J}}\tau_\circ$ is a fixed point, then $\Gamma_{\mathcal{J}}.\nu(\Gamma_{\mathcal{J}}.\tau_\circ) = \Gamma_{\mathcal{J}}\nu(\tau_\circ) = \Gamma_{\mathcal{J}}(\tau_\circ)$ or $\nu(\tau_\circ) = \varepsilon(\tau_\circ)$ for some ν of norm n and $\varepsilon \in \Gamma_{\mathcal{J}}$. In other words, $\varepsilon^{-1}\nu(\tau_\circ) = \tau_\circ$. Since $\Gamma_{\mathcal{J}}.\varepsilon^{-1}\nu = \Gamma_{\mathcal{J}}\nu$, without loss of generality, we may take $\nu(\tau_\circ) = \tau_\circ$.

Let $\nu = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; a, b, c, d are all real and $n(\nu) = n$. $t(\nu) = a + d = +t$ (say).

Now, $\nu(\tau_\circ) = \tau_\circ \Rightarrow \dfrac{a\tau_\circ + b}{c\tau_\circ + d} = \tau_\circ$ or $\tau_\circ$ satisfies the equation $\tau^2 - \dfrac{a-d}{c}\tau - b/c = 0$. Since $\operatorname{Im}\tau_\circ > 0$, it follows that the discriminant of this equation $\dfrac{t^2-4n}{c^2} < 0$ so that $t^2 - 4n < 0$ is a necessary condition for a solution of $\nu(\tau) = \tau$ existing in the finite part of the upper half plane. If $\nu' = u + v\nu$, u and v rational, then $\nu'(\tau) = \tau$ has the same set of solutions as $\nu(\tau) = \tau$.

Associate to any $\nu(\in Q)$ of norm n such that $\nu(\tau_\circ) = \tau_\circ$ the order $\mathscr{O} = \mathcal{J} \cap k(\nu)$, which, by definition, is optimally imbedded in $\mathcal{J}$.

Now,

$$\nu\tau_\circ = \tau_\circ \Rightarrow \eta^{-1_\nu}(\eta(\tau_\circ)) = \eta(\tau_\circ) \text{ if } \eta \in \Gamma_{\mathcal{J}}$$

so that $$\left(\Gamma_{\mathcal{J}}.\eta^{-1_{\nu\eta}}\right)(\Gamma_{\mathcal{J}}.\tau_\circ) = \Gamma_{\mathcal{J}}.\eta\tau_\circ = \Gamma_{\mathcal{J}}\tau_\circ$$

Therefore to one fixed point $\Gamma_{\mathcal{J}}.\tau_\circ$, we may make correspond a whole class of orders $\left\{\eta^{-1}\mathscr{O}\eta; \eta \in \Gamma_{\mathcal{J}}\right\}$, which are optimally imbedded in $\mathcal{J}$, and which contain a ν of norm n.

Conversely, given a class of orders $\left\{\eta^{-1}\mathscr{O}\eta; \mathscr{O} = \mathcal{J} \cap k(\nu)\right\}$ (for which $D(\mathscr{O}) = \Delta < 0$ and $\mathscr{O}$ containing a ν of norm n), then the solution of $\nu(\tau) = \tau$ is a fixed point. 135

So we have now a one-one correspondence between finite fixed points $\Gamma_{\mathcal{J}}.\tau_\circ$ and classes of quadratic subfields K of Q for which there is a $\nu \in K \cap \mathcal{J}$, of norm n and discriminant of K is < 0.

Let $\mathscr{O} = \mathcal{J} \cap K = \left[1, \dfrac{x+\nu}{f}\right]$; x, f integers and $f > 0$.

Here $t = tr(\nu)$ satisfies $(t^2 - 4n) < 0$ and $\Delta = \dfrac{t^2 - 4n}{f^2} \equiv 0, 1$ (mod 4). By t, f and n, the class of $\mathscr{O}$ is uniquely determined and we have as many fixed points as there are such isomorphic classes with a negative discriminant. By Theorem 4 of §9, the number of such classes is given by the following sum over all admissible Δ,

$$\sum_{\substack{t,f\\ \Delta<0}} \prod_{p|q_1}\left(1 - \left\{\frac{\Delta}{p}\right\}\right) \prod_{p|q_2}\left(1 + \left\{\frac{\Delta}{p}\right\}\right) h(\Delta).$$

Let $W(\Delta)$ denote the number of units $in\mathscr{O}.(\mathscr{O} \subset K$ and K being imaginary, this is finite). Then, for all units $\varepsilon \in \mathscr{O}, \nu$ and $\varepsilon\nu$ have different traces but correspond to the same fixed point (except for $tr(\nu) = 0, \varepsilon = -1$) so that we would have counted each fixed point $W(\Delta)$ times in the above sum, with the exception of those ν for which $tr(\nu) = 0$ in which case the fixed points belonging to ν would have been counted only $\dfrac{1}{2}W(\Delta)$ times (since here for the unit $\varepsilon = -1$, $\varepsilon\nu = \overline{\nu}$). Even with this correction the above sum would not yet be the number of fixed points, as the following consideration shows:

The sum would be the correct number of fixed points, if a $\Gamma_{\mathcal{J}}\tau_\circ$ occurs only in one branch $\Gamma_{\mathcal{J}}\nu_i$ of the correspondence $T_n = \sum\limits_i \Gamma_{\mathcal{J}}.\nu_i$

But, in fact $\Gamma_{\mathcal{J}}.\tau_\circ$ may be fixed by more than one branch $\Gamma_{\mathcal{J}}.\nu_i$. **136**
Let $\Gamma_{\mathcal{J}}.\nu_1, \Gamma_{\mathcal{J}}.\nu_2$ be two branches fixing $\Gamma_{\mathcal{J}}.\tau_\circ$. Let $\mathscr{O}_1 = \left[1, \dfrac{x_1 + \nu_2}{f_2}\right]$ and $\mathscr{O}_2 = \left[1, \dfrac{x_2 + \nu_2}{f_2}\right]$ be the orders associated with these two branches. Then, if $(t_2, f_2) \neq (t_1, f_1)$, the fixed point $\Gamma_{\mathcal{J}}.\tau_\circ$ would have been counted twice in the above sum, as it should be. But it may happen that $(t_1, f_1) = (t_2, f_2)$, *i.e.*, $t_1 = t_2$ and $f_1 = f_2$ and yet $\Gamma_{\mathcal{J}}.\nu_1 \neq \Gamma_{\mathcal{J}}.\nu_2$. In other words, $\nu_1 = \overline{\nu_2}$ and $\nu_1 \neq \varepsilon\nu_2(\varepsilon$, a proper unit). Therefore the number of fixed points of T_n is twice the above sum except for the terms $t = 0$ which should be kept unchanged. So the number of fixed points is finally given by,

$$F = \sum_{t,f} \prod_{p|q_1} \left(1 - \left\{\frac{\Delta}{p}\right\}\right) \prod_{p/q_2} \left(1 + \left\{\frac{\Delta}{p}\right\}\right) \frac{h(\Delta)}{\omega(\Delta)} \qquad (*)$$

$(\Delta = (T^2 - 4n)f^{-2} \equiv 0, 1 \pmod 4)$ and where $\omega(\Delta) = \dfrac{1}{2}$ number of units of $\mathscr{O}(\Delta) = \dfrac{1}{2}W(\Delta)$.

ii) $n = m^2$. In this case, we have $T_n = T_n^* + \Gamma_{\mathcal{J}}.m$. We only calculate the number of fixed points of T_n^*. The considerations are the same as above with the exception that those $\nu = \varepsilon.m$ must not be counted for ε, a unit of $\mathscr{O}$.

$\varepsilon = \pm 1$ would that $t = \pm 2m \Rightarrow t^2 - 4n = 0$ which had already been excluded. But ε may be a third, fourth or sixth root of unity.

a) $\varepsilon^4 = 1.t(\nu) = mt(\varepsilon) = 0$ since either $\varepsilon^2 - 1 = 0$ or $\varepsilon^2 + 1 = 0$. $f = m$
137 and $(t^2 - 4n)f^{-2} = -4$ so that $h(-4) = 1$ and $\omega(-4) = 2$. The number of fixed points of order 4 is given by $(*)$ with these special values.

i.e., $$= \frac{1}{2} \prod_{p|q_1} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p|q_2} \left(1 + \left(\frac{-4}{p}\right)\right)$$

b) $\varepsilon^3 = 1$ or $\varepsilon^6 = 1$. Either $\varepsilon^2 + \varepsilon + 1 = 0$ or $\varepsilon^2 - \varepsilon + 1 = 0$, so that $t(\nu) = mt(\varepsilon) = \pm m$ and $f = m; (t^2 - 4n)f^{-2} = -3$. Further $h(-3) = 1$ and $\omega(-3) = 3$ in either case. The number of fixed points of order 3 and 6 is given by 2(∗) since both are equal.

i.e., $$= \frac{2}{3}\prod_{p|q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-3}{p}\right)\right).$$

Hence the total number of fixed points of T_n^* is obtained by subtracting the above terms from (∗). In other words, it is given by

$$\sum_{\substack{t,f\\ f>0 \text{ integral}}} \prod_{p|q_1}\left(1-\left\{\frac{\Delta}{p}\right\}\right)\prod_{p/q_2}\left(1+\left\{\frac{\Delta}{p}\right\}\right)\frac{h(\Delta)}{\omega(\Delta)} - \frac{1}{2}\prod_{p/q_1}\left(1-\left(\frac{-4}{p}\right)\right).$$

$$\Delta = (t^2-4n)f^{-2} \equiv 0,1 \pmod 4) \prod_{p/q_2}\left(1+\left(\frac{-4}{1p}\right)\right)$$

$$-\frac{2}{3}\prod_{p|q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-3}{p}\right)\right) - 2\sqrt{n} < t < 2\sqrt{n}$$

8. We shall now compute all the parabolic cusps of fundamental domain D of the proper unit group $\mathscr{O}_{\mathscr{J}}$ of an order $\mathscr{J}$ of the type (q_1, q_2) (here $q_1 = 1$ since otherwise, D is bounded). In fact, if k is the number of prime divisors of q_2, these cusps are the points $\tau = i\infty, \dfrac{1}{q'}, q'|q_2(q' \neq q_2)$; 2^k in number.

The proof consists of two parts: (i) these points are inequivalent with respect to the group $\mathscr{O}_{\mathscr{J}}$ or $\Gamma_{\mathscr{J}}$. (ii) any rational cusp is equivalent to one these by means os elements of $\Gamma_{\mathscr{J}}$.

(i) a) The points $\tau = i\,\infty$ and $\dfrac{1}{q'}, q'|q_2(q' \neq q_2)$ are inequivalent. 138

If not, there will exist $\begin{pmatrix} a & b \\ q_2c & d\end{pmatrix} \in \mathscr{O}_{\mathscr{J}}$ such that $\dfrac{a\tau+b}{q_2c\tau+d} = \dfrac{1}{q'}$ ((τ being the points $i\infty$), *i.e.*, $\dfrac{a}{q_2c} = \dfrac{1}{q'}$ which is impossible since q' is a proper divisor of q_2 and a, c are integers.

b) The points $\dfrac{1}{q'}$ and $\dfrac{1}{q^*}(q' \neq q^*)$ are inequivalent. Let $q_2 = q'q''$. Supposing $\dfrac{a+bq'}{q_2c+dq'} = \dfrac{1}{q^*}$ which ⇒ $\dfrac{a+bq'}{cq''+d} = \dfrac{q'}{q^*}$, *i.e.*, $q^*(a+bq') =$

$q'(cq''+d)$. Therefore there exists $p|q^*$ which divides either q' or $cq''+d$. But $(cq_2, d) = 1 \Rightarrow (cq'', d) = 1$, so that if $p|q'$ in which case $p|q''$ and $p|cq'' + d$, which is not possible simultaneously.

Hence $q^*|q'$- Without loss of generality, we could have assumed $q^* \geq q'$ or else we can argue with the inverse transformation. Thus we arrive at a contradiction unless $q^* = q'$.

(ii) Any parabolic cusp (which is of the form $\frac{\alpha}{\beta}$, $(\alpha,\beta) = 1$) is equivalent to $i\infty$, $\frac{1}{q'}$; $q'|q_2$.

(a) Let $\frac{\alpha}{\beta}$ be a parabolic cusp $(\alpha,\beta) = 1$. If $q_2|\beta$ let $\beta = q_2c$. Then $\frac{\alpha}{\beta} \sim i\infty$ for $\frac{\alpha\tau + b}{q_2c\tau + d} = \frac{\alpha}{q_2c}$ if $\tau = i\infty$; (b, d) being chosen in such a way that $\begin{pmatrix} \alpha & b \\ q_2c & d \end{pmatrix} \in \Gamma_{\mathcal{J}}$ which is possible, since $(\alpha,\beta) = (\alpha, q_2c) = 1$.

(b) $q_2 \nmid \beta$. Let $(\beta, q_2) = q'$ and $\beta = q'\beta''$. Then $(\beta'', q_2) = 1$; $q_2 = q'q''$.
Our object is to find $\begin{pmatrix} a & b \\ q_2c & d \end{pmatrix} \in \Gamma_{\mathcal{J}}$ such that $\frac{a\alpha + b\beta}{q_2c\alpha + d\beta} = \frac{1}{q'}$.
$(\alpha,\beta) = 1$ and $(\alpha q'',\beta'') = 1 \Rightarrow$ there exists integers $a_\circ, b_\circ, c_\circ, d_\circ$
139 such that $a_\circ\alpha + b_\circ\beta = 1$ and $c_\circ q''\alpha + d_\circ\beta'' = 1$ or $q_2c_\circ\alpha + d_\circ\beta = q'$.
Now $q''c\alpha + d\beta'' = 1$ if $q''c = q''c_\circ + q''t\beta''$ and $d = d_\circ - q''t\alpha$, with arbitrary t. We determine t in such a way that $d \equiv \alpha \pmod{q'}$. This is possible because $(\alpha q'', q') = 1$.

Now, $a_\circ\alpha \equiv 1 \pmod{q'}$ and $d \equiv \alpha \pmod{q'}$ imply that $a_\circ d \equiv 1 \pmod{q'}$.

Similarly $a_\circ, b_\circ$ may be replaced by $a = a_\circ + s\beta$ and $b = b_\circ - s\alpha$.

We choose s in such a way that $\begin{vmatrix} a & b \\ q_2c & d \end{vmatrix} = 1$. For the same, we have

$$\begin{vmatrix} a & b \\ q_2c & d \end{vmatrix} = \begin{vmatrix} a & q'b \\ q''c & d \end{vmatrix} = \begin{vmatrix} a_\circ + s\beta & q'(b_\circ - s\alpha) \\ q''c & d \end{vmatrix}$$

$$= \begin{vmatrix} a_\circ & q'b_\circ \\ q''c & d \end{vmatrix} + s\begin{vmatrix} \beta & -q\alpha \\ q''c & d \end{vmatrix}$$

$$= a_\circ d - q_2b_\circ c + q's(\text{ since } q_2c\alpha + d\beta = q').$$

$a_\circ d \equiv 1 \pmod{q'} \Rightarrow a_\circ d - q_2 b_\circ c \equiv 1 \pmod{q'} = 1 - sq'$ (say). Thus s can be determined.

Collecting the above results, we have $\begin{vmatrix} \alpha & b \\ q_2 c & d \end{vmatrix} = 1$; $a\alpha + b\beta = 1$ and $q_2 c\alpha + d\beta = q'$ and thus

$$\frac{a\alpha + b\beta}{q_2 c\alpha + d\beta} = \frac{1}{q'}.$$

After having found the parabolic cusps, we have still got to compute the multiplicity of each such fixed point.

a) The point $\tau = i\infty$. In this case, the local uniformiser is given by $\zeta = e^{2\pi i\tau}$

i) $\sqrt{n} \not\equiv 0 \pmod 1$. Let $T_n = \sum\limits_i \Gamma_{\mathcal{J}} \nu_i$, where $\nu_i = \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix} n_1, n_3 > 0; n_1 n_3 = n$ and $0 \leq n_2 < n_3$.

Now, $\nu_i(\tau) = \dfrac{n_1}{n_3}\tau + \dfrac{n_2}{n_3}$ and the local uniformiser ζ is mapped into 140 $\zeta_i = \zeta(\nu_i(\tau)) = e^{2\pi i \dfrac{n_1\tau + n_2}{n_3}} = \zeta^{\frac{n_1}{n_3}} e^{2\pi i n_2/n_3}$ Let $(n_1, n_3) = d$ and $n_1 = n'_1 d, n_3 = dn'_3$. Then $\zeta_i = \zeta^{\frac{n'_1}{n'_3}} . e^{2\pi i n_2/dn_3}$ Consider the functions $e^{2\pi\gamma/n'_3} . \zeta^{n'_1/n'_3} (0 \leq r < n'_3)$. These are all analytic continuations of one another and they represent one branch of the correspondence T_n and we have for the multiplicity for this branch $\min(n'_1, n'_3)$. But $0 \leq n_2 < d.n'_3$ implies that we have d branches with the same n'_1, n'_3 and the total multiplicity corresponding to these branches is $d \min(n'_1, n'_3) = \min(n_1, n_3)$. This being the same for all branches whenever n_1, n_3 range through divisors of n such that $n_1 n_3 = n$, we obtain for the totally multiplicity of the fixed point $\Gamma_{\mathcal{J}}.\tau$, $2 \sum\limits_{\substack{d|n \\ d<\sqrt{n}}} d$.

ii) $\sqrt{n} \equiv 0 \pmod 1$. If $n = m^2$, $T_n = T^*_n + \Gamma_{\mathcal{J}} m$. The above argument applies for T^*_n and we have multiplicity $2 \sum\limits_{\substack{d|n \\ d<\sqrt{n}}} d$ and corresponding to the term $\Gamma_{\mathcal{J}}.m$, we have $\zeta_i = e^{2\pi i n_2/m.}\zeta^{m/m}$ and a similar argument as in (i) shows the multiplicity to be m, but it is actually only $m-1$ since we should not take into account the term corresponding to $n_2 = 0$, *i.e.*, $\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$ this being the identity map.

Hence the total multiplicity is here given by,

$$2 \sum_{\substack{d|n \\ d<\sqrt{n}}} d + \sqrt{n} - 1.$$

(b) $\tau = \dfrac{1}{q'}, q'|q_2; q' \neq q_2$.

141 Firstly, we shall calculate the local uniformising parameter at $\Gamma_{\mathcal{J}}.\dfrac{1}{q'}$ and then see that the multiplicity is exactly the same as that for $i\infty$.

If $\lambda = \begin{pmatrix} 1 & 0 \\ -q' & 1 \end{pmatrix}$, then $\lambda\left(\dfrac{1}{q'}\right) = \infty$. We wish to fine a primitive transformation $\rho \in \Gamma_{\mathcal{J}}$ such that $\rho(\dfrac{1}{q'}) = \dfrac{1}{q'}$. Let σ be a transformation fixing ∞, i.e., $\sigma = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ and all the transformations $\lambda^{-1}\sigma\lambda$ fix $\dfrac{1}{q'}$. Now,

$$\lambda^{-1}\sigma\lambda = \begin{pmatrix} 1 & 0 \\ q' & 1 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -q' & 1 \end{pmatrix} = \begin{pmatrix} 1-q's & s \\ -q'^2 s & 1+q's \end{pmatrix}$$

is an element of $\Gamma_{\mathcal{J}}$ implies that $q''|s$ (where $q'' = \dfrac{q_2}{q'}$) and since we require a primitive transformation of this type, we may take $s = q''$.

Consider now $\zeta = e^{2\pi i \frac{\lambda(\tau)}{q''}}$; τ, a point in a neighbourhood of $\dfrac{1}{q'}$. Now, $\dfrac{1}{q''}\lambda\rho(\tau) = \dfrac{1}{q''}\sigma\lambda(\tau) = \dfrac{1}{q''}\dfrac{\lambda(\tau)+q''}{1} = \dfrac{\lambda(\tau)}{q''} + 1$, by our choice of σ, so that ζ remains unaltered. In other words, ζ takes any neighbourhood of $\Gamma_{\mathcal{J}}.\dfrac{1}{q'}$ in $\mathcal{S}_{\mathcal{J}}$ to the unit circle and hence is a local uniformiser at $\Gamma_{\mathcal{J}}.\dfrac{1}{q'}$.

Let $T_n = \sum i\Gamma_{\mathcal{J}}.\nu_i; \nu_i = \begin{pmatrix} n_1 & n_2 \\ 0 & n_3 \end{pmatrix}; n_1, n_3 > 0; n_1 n_3 = n.0 \leq n_2 < n_3$.

(In case n is a square, T_n^* has to be considered). If $\Gamma_{\mathcal{J}}.\nu_i\left(\dfrac{1}{q'}\right) = \Gamma_{\mathcal{J}}.\dfrac{1}{q'}$ then $\nu_i\left(\dfrac{1}{q'}\right) = \varepsilon_i\left(\dfrac{1}{q'}\right); \varepsilon_i^{-1}\nu_i\left(\dfrac{1}{q'}\right) = \dfrac{1}{q'}$.

Call $\nu_i' = \varepsilon_i^{-1}\nu_i$. Since now $\lambda\left(\dfrac{1}{q'}\right) = \infty$, then $\lambda\nu_i'\lambda^{-1} = \mu_i$ fix ∞, and hence are of the form $\begin{pmatrix} s_1 & s_2 \\ 0 & s_3 \end{pmatrix}$

$$\begin{aligned} \nu_i' = \mu_i\lambda &= \begin{pmatrix} 1 & 0 \\ q' & 1 \end{pmatrix}\begin{pmatrix} s_1 & s_2 \\ 0 & s_3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -q' & 1 \end{pmatrix} \\ &= \begin{pmatrix} s_1 - s_2 q' & s_2 \\ q'(s_1 - s_2 q') - q' s_3 & s_3 + q' s_2 \end{pmatrix} \end{aligned}$$

in $\mathcal{J}$ implies that $(s_1 - s_2 q') - s_3 \equiv 0 \pmod{q})''$. Such an s_2 can always be found out since $(q', q'') = 1$. and s_2 takes each residue class $\mod s_3$ exactly once. 142

We shall prove that as $\left\{\mathcal{J}\nu_i'\right\}$run through a system of distinct integral left ideals of norm n, $\left\{\mathcal{J}\nu_i'\right\}$also run through a system of distinct integral ideals of norm n; for $\mathcal{J}\nu_i' = \mathcal{J}\nu_j' \Rightarrow$ for primes $p|n$ (and hence $p \nmid q_1 q_2$),

$$(\mathcal{J}\mu_i)_p = \mathcal{J}_p\lambda\nu_i'\lambda^{-1} = \mathcal{J}_p\nu_i'\lambda^{-1} = \mathcal{J}_p\lambda\nu_j'\lambda^{-1} = \mathcal{J}_p\mu_j$$

(for λ is a unit of $\mathcal{J}p$).

For primes $p \nmid n$, $(\mathcal{J}\nu_i')_p = \mathcal{J}_p = (\mathcal{J}\nu_j')_p$ and also $(\mathcal{J}\mu_i)_p = \mathcal{J}_p = (\mathcal{J}\mu_j)_p$.

Hence in all cases

$$\begin{aligned} \mathcal{J}\nu_i' = \mathcal{J}\nu_j' \Longleftrightarrow (\mathcal{J}\nu_i')_p \\ = (\mathcal{J}\nu_j')_p \Longleftrightarrow (\mathcal{J}\mu_i)_p = (\mathcal{J}\mu_j)_p \Longleftrightarrow \mathcal{J}\mu = \mathcal{J}\mu_j. \end{aligned}$$

The local uniformising parameter ζ at $\dfrac{1}{q'}$ goes over to $\nu_i'\left(\dfrac{1}{q'}\right)$ and in fact

$$\begin{aligned} \nu'_i(\zeta'_q) = e^{2\pi i\lambda(\nu'_i(\tau))/q''} &= e^{2\pi i\mu_i\lambda(\tau)/q''}\\ &= e^{2\pi i\frac{\mathscr{S}_1}{\mathscr{S}_3}\frac{\lambda(\tau)}{q''}} e^{2\pi i\frac{\mathscr{S}_1}{\mathscr{S}_3 q''}} = \zeta_{q'}^{\mathscr{S}_1/\mathscr{S}_3} e^{2\pi i\mathscr{S}_2/\mathscr{S}_3 q''} \end{aligned}$$

So, $\zeta_{q'}$ behave similar to ζ_∞ under the correspondences and the sum of multiplicities of the branches is the same as that for ζ_∞.

143 The parabolic cusps being 2^{k_2} in number, the number of parabolic cusps with due multiplicity is given by $2\sum_{\substack{d|n\\ d<\sqrt{n}}} d+\gamma_n$

where $\gamma_n = \begin{cases} 0 & \text{if } \sqrt{n}\not\equiv 0 \pmod 1\\ \sqrt{n}-1 & \text{if } \sqrt{n}\equiv 0 \pmod 1. \end{cases}$

(i) If $\sqrt{n}\not\equiv 0 \pmod 1$ we had obtained by Lefschetz' fixed point theorem, $tr^1(T_n) = 2\sum_{d/n} d$- (number of finite fixed points of T_n) - (number of infinite fixed points of T_n).

$$\text{i.e., } \mathrm{tr}^1(T_n) = 2\sum_{d|n} d - \sum_{\substack{t,r\\ f>o,\Delta=(t^2-4n)f^{-2}\equiv 0,1 \pmod 4\\ -2\sqrt{n}<t<2\sqrt{n}}} \prod_{1-|q_1}\left(1-\left\{\frac{\Delta}{\mu}\right\}\right)\frac{h(\Delta)}{\omega(\Delta)} - \left(2^{k_2+1}\sum_{\substack{\alpha/n\\ \alpha<\sqrt{n}}}\right)$$

(ii) If $\sqrt{n}\equiv 0 \pmod 1$, $T_n = T_n^* + \Gamma_{\mathcal{J}}.m$ so that (in case $q_1 = 1$).

$tr^1(T_n) = tr^1(T_n^*) + tr^1(T_n^*) + 2g$. By the application of Lefschetz' fixed point theorem for the mapping T_n^*,

$$\left.\begin{array}{l}\text{total number of fixed points (finite and}\\ \text{infinite) of } T_n^* \text{ with due multiplicity}\end{array}\right\} = 2\left(\sum_{d|n} d-1\right) - tr^1(T_n^*).$$

Therefore

$$\operatorname{tr}^1(T_n^*) = 2\sum_{d|n} d - 2 - \text{(finite fixed points) - (infinite fixed points)}$$

$$= 2\sum_{d|n} d - 2 - \sum_{t,f}\prod_{p|q_1}\left(1-\left\{\frac{\Delta}{p}\right\}\right)\prod_{p|q_2}\left(1+\left\{\frac{\Delta}{p}\right\}\right)\frac{h}{\omega}(\Delta)$$

$$+\frac{1}{2}\prod_{p|q_1}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{p|q_2}(1+\left(\frac{-4}{p}\right)+\frac{2}{3}\prod_{p|q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-3}{p}\right)\right)$$

$$-2^{k_2}\left(2\sum_{\substack{d|n\\ d<\sqrt{n}}} d + \sqrt{n}-1\right)(\text{ in case } q_1 = 1).$$

From §6, we have a formula for genus and using the expression for the number of elliptic vertices we obtain for g, 144

$$2g = 2-\frac{1}{2}\prod_{p|q_1}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-4}{p}\right)\right)$$

$$-\frac{2}{3}\prod_{p|q_1}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{p|q_2}\left(1+\left(\frac{-3}{p}\right)\right)-2^{k_2}+\frac{1}{6}\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1).$$

On adding the above two, we obtain finally

$$\operatorname{tr}^1(T_n) = 2\sum_{d|n} d - (2^{k_2+1}\sum_{\substack{d_n\\ d<\sqrt{n}}} d,\ \text{in case } q_1 = 1)$$

$$-\sum\prod_{p|q_1}(1-\left\{\frac{\Delta}{p}\right\})\prod_{p|q_2}\left(1+\left\{\frac{\Delta}{p}\right\}\right)\frac{h}{\omega}(\Delta)+\gamma_n$$

$$\text{where } \gamma_n = \begin{cases} 0 \text{ if } \sqrt{n}\not\equiv \ (\text{mod } 1)\\ (-2^k 2\sqrt{n},\ \text{in case } q_1 = 1) + \frac{1}{6}\prod_{p|q_1}(p-1)\prod_{p|q_2}(p+1),\\ \qquad\qquad\qquad\qquad \text{if } \sqrt{n}\equiv 0 \ (\text{mod } 1).\end{cases}$$

Of course, all these formulae hold good only for n such that $(n, q_1.q_2) = 1$.

Note. (i) *In case $g = 0$, this trace is always 0. So the trace formula implies relations between the class numbers $h(\Delta)$ of different imaginary quadratic fields. An example is given in the case $q_1 = q_2 = 1$, where Γ is the full modular group.*

$$2\sum_{\substack{d|n\\ d\geq\sqrt{n}}} - \sum_{\Delta=(t^2-4n)f^2} \frac{h(\Delta)}{\omega(\Delta)} + \gamma_n = 0,$$

$$\text{where } \gamma_n = \begin{cases} 0 & \text{if } \sqrt{n} \not\equiv 0 \pmod 1 \\ -\sqrt{n} + \frac{1}{6} & \text{if } \sqrt{n} \equiv 0 \pmod 1 \end{cases}$$

(ii) *One may obtain other class number relations among which the following one is most remarkable:*

$$\sum_{t\equiv\frac{n+1}{2} \pmod 2} \frac{h}{\omega}(t^2-4n)f^{-2}) = \frac{1}{3}\sum_{d|n} d - \sum_{\substack{d|n\\ d\leq\sqrt{n}}} *d(n \equiv 1 \pmod 2))$$

(M. Eichler, Jour. of the Ind. Math. Soc., 1956).

145 *Using the above two relations, one can compute the class numbers of imaginary quadratic fields, by a recursion scheme.*

(iii) *These and similar class number relations are quoted in Dickson's "History of the Theory of Numbers", Vol. III, Chap. VI. They have been proved by application of the theory of elliptic modular function. Here we have seen that they originate from the topological background of that theory. The topological methods are even more powerful since they lead also to class number relations derived from quaternion algebras $Q \not\cong \mathfrak{M}_2(k)$ which cannot be obtained from the theory of modular functions.*

Our consideration from a natural branch of algebraic number theory, which contains yet a number of open problem. One of these is the investigation of the algebraic geometric aspects of the correspondences T_n of those algebraic curves which are uniformized by the groups $\Gamma_{\mathcal{J}}$. In case of $\Gamma_{\mathcal{J}}$ being the classical modular group, these investigations lead to the theory of complex multiplication.

Another question is the following one: the eigenvalues of the representations of T_n by the first homology group, are integers from a totally real algebraic number field. What is the meaning of this field?

In case of $Q \cong \mathfrak{M}_2(k)$ it has been proved (M. Eichler, Quaternare Formen und die Rienannsche Vermutung fur die Kongruenzzetafunktion, Archiv der Mathematik, V, 1957, p.355 – 366) that the absolute values of the eigenvalues of T_n, for n, a prime are $\leq 2n^{\frac{1}{2}}$, up to a finite number of exceptions at most. For an arbitrary n, there exists for every $\varepsilon > 0$, a constant C_ε such that values are $\leq C_\varepsilon n^{\frac{1}{2}+\varepsilon}$.

Chapter 5

Automorphic Forms

11 Automorphic Forms

1. Let Γ be a group of (2, 2) real matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc > 0$. **146** Furthermore, assume that Γ considered as a group of transformations on the upper half plane, is a "discontinuous group of the first kind", i.e., it possesses a fundamental domain F, which is bounded by a finite number of sides and has only a finite number of parabolic cusps.

Definition. *An automorphic form $\varphi(\tau)$ belonging to the group Γ and of degree $-2f(2f$ integral) is a meromorphic function $\varphi(\tau)$ in* $\operatorname{Im}\tau > 0$, *with the property that*

$$\varphi(\tau) = \varphi\left(\frac{a\tau + b}{c\tau + d}\right)\left(\frac{ad - bc}{(c\tau + d)^2}\right)^f \quad \textit{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

$\varphi(\tau)$ is an integral form if it is regular in the upper half plane including the parabloiccusps of F.

By virtue of the transformation formula of $\varphi(\tau)$, one can associate to $\varphi(\tau)$, the differential $\varphi(\tau).d\tau^f$, of degree f, on the Riemann surface obtained by identifying the sides of F and adjoining the cusps.

We shall now give some examples of automorphic forms.

1. Poincare Series

The series $\varphi(\tau) = \sum\limits_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma} \dfrac{1}{(c\tau + d)^{2f}} \circ f\left(\dfrac{a\tau + d}{c\tau + d}\right)$ for a suitable $f(\tau)$, is called a *Poincare theta-series* and is an automorphic form of degree $-2f$ for the group Γ.

147 Some special cases of Poincare Series are discussed in

(i) H. Weyl - Die Idee der Riemannschen Fläche, 1955, (Page 151)

(ii) Ford - Automorphic Functions

(iii) C. L. Siegel - Ausgewahlte Fragen der Funktionentheorie-II (Göttingen) (Page 50). One of the important special cases of Poincare Series is the so-called Einstein series, for which $f(\tau) \equiv 1$. It was first studied by Hecke (Theorie der Eisensteinschen Reihe Hamburger Abhandlungen, 1927), in the case of principal congruence subgroups of the modular group.

2. Theta-series.

2. Let $F(\underline{X}) = \sum\limits_{i,k=1}^{4f} f_{ik} X_i X_k$ be a positive definite quadratic form in an even number $4f$ of variables, with integral coefficients and further $f_{ii} \equiv 0 \pmod 2, (-1)^{2f} |f_{ik}| = a$ square. Consider now the series

$$\vartheta_F(\tau) = \sum_{\underline{X} \text{ integral}} e^{\pi i \tau F(\underline{X})}.$$

Then this convergent series defines an automorphic form of degree $-2f$ for the group $\Gamma(q) : (\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ modular and $c \equiv \pmod q$) where q is the smallest integer for which $q.(f_{ik})^{-1}$ is integral with even diagonal elements. That it is a modular from was proved by Hermite.

The above series can obviously be written in the from: $\vartheta(\tau) = \sum\limits_{n=1}^{\infty} c_n e^{2\pi \text{ in } c}, c_n$ being the number of representations of n by $\frac{1}{2} F(\underline{X})$. When F is definite, c_n is finite, and from the theory of modular correspondences, we can get some information about c_n.

148 **3.** One can also form a theta series with weights which are homoge-

neous polynomials of a certain type. Consider

$$\vartheta(\tau, P_\nu, F) = \sum_{\underline{\text{X}} \text{ integral}} P_\nu(\underline{\text{X}}) e^{\pi i \tau F(\underline{\text{X}})}$$

where $P(X_1 \ldots X_{4f})$ is a homogeneous polynomial of degree ν in $4f$ variables and satisfies the Laplacian $\sum\limits_{i,k} f_{ik} \dfrac{\partial^2 P_\nu}{\partial X_i \partial X_k} = 0$ associated with the form $F(\underline{\text{X}})$. Then it was proved by B. Schoeneberg (Math. Annalen, 1939, Vol. 116, Das Verhalten von mehrfachen thetareihen fur Modulsubstitutionen) that the series represent a modular form of degree -$(2f + \nu)$ for the group $\Gamma(q)$, q being defined as before.

3. We may also define theta-series associated with $F(X)$ with integral coefficient from a totally real algebraic number field K.

But now, this will be an automorphic form with respect to a subgroup of the corresponding Hilbert group. For example, in a particular case, when $K = k(\sqrt{d}), d > 0$,

$$\vartheta(\tau_1, \tau_2) = \sum_{\underline{\text{X}} \text{ integral in } K} e^{2\pi i(\tau_1 F(\bar{X}) + \tau_2 \overline{F(\underline{\text{X}})})}$$

($\underline{\text{X}}$ being a vector with $4f$ components and $\nu \to \bar{\nu}$ denoting the non identity automorphism of K/k).

It can be shown then that $\vartheta(\tau_1, \tau_2)$ converges absolutely and uniformly in $\operatorname{Im}\tau_1 > 0, \operatorname{Im}\tau_2 > 0$.

Definition. *An analytic function $\varphi(\tau_1, \tau_2)$of 2 complex variables, meromorphic in* $\operatorname{Im}\tau_1 > 0, \operatorname{Im}\tau_2 > 0$, *is* automorphic form *of degree $-2f$ for the group $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a, b, c, d integers in K and $ad - bc$, a unit of K)), if* 149

$$\varphi(\tau_1, \tau_2) = \varphi(\varepsilon(\tau_1), \bar{\varepsilon}(\tau_2)) . \frac{1}{(\gamma\tau_1 + \delta)^{2f} (\bar{\gamma}\tau_2 + \bar{\delta})^{2f}}$$

where $\quad \varepsilon = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma.$

It can be shown then that the above defined theta-series is an automorphic form of degree $-2f$ for a subgroup of the Hilbert modular group of K. Such forms are called Hilbert modular forms.

4. Now, let $\vartheta(\tau_1, \tau_2)$ be an arbitrary Hilbert modular form of degree $-2f$ (with respect to the whole Hilbert modular group).

We shall now reduce $\vartheta(\tau_1, \tau_2)$ to an automorphic form $\varphi(\tau)$ in one variable τ, by the following procedure.

Putting $\tau_1 = \tau$ and $\tau_2 = \dfrac{-1}{\tau}, r > 0$, a rational number so that $\operatorname{Im}(\tau_1) > 0$ implies $\operatorname{Im}(\tau_2) > 0$, we shall replace τ_1, τ_2 by $\tau' = \varepsilon(\tau)$ and $\tau'' = \bar{\varepsilon}(\dfrac{-1}{r\tau})$. We then seek for conditions on ε such that $\tau'' = -\dfrac{1}{r\tau'}$. In other words,

$$\frac{\bar{\alpha}\left(-\frac{1}{\gamma\tau} + \bar{\beta}\right)}{\bar{\gamma}(-\frac{1}{\gamma\tau}) + \bar{\delta}} = \frac{-(\gamma\tau + \delta)}{\gamma(\alpha\tau + \beta)} or, \pm \begin{pmatrix} \gamma\bar{\beta} & -\bar{\alpha} \\ \gamma\bar{\delta} & -\bar{\gamma} \end{pmatrix} = \begin{pmatrix} -\gamma & -\delta \\ \gamma\alpha & \gamma\beta \end{pmatrix}$$

so that $\varepsilon = \begin{pmatrix} \alpha & \bar{\beta} \\ \gamma\bar{\beta} & -\bar{\alpha} \end{pmatrix}$. If r is an integer and if α, β are also integers, then ε is a unit in some order of an indefinite quaternion algebra defined by

$$Q = [1, \omega, \Omega, \omega\Omega]$$

with $\omega^2 = d > 0$ and $\Omega^2 = r > 0$. We shall call the unit group of this order by Γ. Define now $\varphi(\tau) = \vartheta(\tau, \dfrac{-1}{\gamma\tau}).\ \tau^{-2f}$, then $\varphi(\tau)$ is an
150 automorphic from of degree - $4f$with respect to the group Γ, for

$$\begin{aligned}
\varphi(\varepsilon(\tau)) &= \vartheta\left(\varepsilon(\tau), -\frac{1}{\gamma\varepsilon(\tau)}\right)(\varepsilon(\tau))^{-2f} \\
&= \vartheta\left(\varepsilon(\tau), \bar{\varepsilon}\left(-\frac{1}{\gamma\tau}\right)\right)(\varepsilon(\tau))^{-2f} \\
&= \vartheta\left(\tau, -\frac{1}{\gamma\tau}\right)(\gamma\tau + \delta)^{2f}\left(\bar{\gamma}\left(\frac{-1}{\gamma\tau}\right) + \bar{\delta}\right)^{2f}(\varepsilon(\tau))^{-2f} \\
&= \vartheta\left(\tau, -\frac{1}{\gamma\tau}\right)(\gamma\tau + \delta)^{2f}\left(\frac{\beta}{\tau} + \alpha\right)^{2f}\left(\frac{(\gamma\tau + \delta)}{(\alpha\tau + \beta)}\right)^{2f}
\end{aligned}$$

$$
\begin{aligned}
&= \vartheta\left(\tau, -\frac{1}{\gamma\tau}\right)(\gamma\tau+\delta)^{4f}\,\tau^{-2f}\\
&= \varphi(\tau)\,(\gamma\tau+\delta)^{4f}
\end{aligned}
$$

The Hilbert modular form $\vartheta(\tau_1, \tau_2)$ being periodic of periods $\alpha, \overline{\alpha}(\alpha$ being an integer in $K = k(\sqrt{d})(d > 0))$ it has a series expansion of the form

$$\vartheta(\tau_1, \tau_2) = \sum_{\substack{\nu,\overline{\gamma}>0\\ \nu\in\theta^{-1}}} c_\gamma e^{2\pi i(\tau_1\gamma+\tau_2\overline{\nu})} (\theta \text{ is the different of } K)$$

so that on replacing $\tau_1 = \tau, \quad \tau_2 = -\dfrac{1}{r\tau}$, we have

$$\vartheta\left(\tau, -\frac{1}{\gamma\tau}\right) = \sum_{\substack{\nu,\overline{\nu}>o\\ \gamma\in\theta^{-1}}} C_\gamma e^{2\pi i(\nu\tau-\overline{\nu}(\frac{1}{\gamma\tau}))}$$

Consider the substitution $\tau \rightarrow \lambda(\tau)$ where $\lambda = \begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{pmatrix}$. Then $\vartheta(\varepsilon^2\tau_1, \overline{\varepsilon}^2\tau_2) = \vartheta(\tau_1, \tau_2)$ implies that

$$
\begin{aligned}
\sum_\nu c_\nu e^{\pi i(\tau_1\varepsilon^2\nu+\tau_2\overline{\varepsilon}^2\nu)} &= \sum_\nu c_{\nu\varepsilon^{-2}} e^{2\pi i(\tau_1\nu+\tau_2\overline{\nu})}\\
&= \sum_\nu c_\nu e^{2\pi i(\tau_1\nu+\tau_2\overline{\nu})}
\end{aligned}
$$

and by uniqueness of the expansion, on comparison of coefficients, $c_\nu = c_{\nu\varepsilon^{-2}}$ for every unit ε of K.

We may therefore write **151**

$$\vartheta\left(\tau, -\frac{1}{r\tau}\right) = \sum_{(\nu)} c_{(\nu)} P_\nu(\tau)$$

where (γ) denotes the class of all $\nu\varepsilon^{-2}$ and $P_\nu(\tau) = \sum_\varepsilon e^{2\pi i\left(\nu\varepsilon^2\tau-\tau\varepsilon^2\frac{1}{r\tau}\right)}$ the summation over ε running over all powers of $\varepsilon_\circ$, the fundamental unit of K.

From the definition of $P_\nu(\tau)$, we have the following product formula,

$$P_\nu(\tau).P_\mu(\tau) = \sum_{s=-\infty}^{\infty} P_{\nu+\mu\varepsilon_\circ}2s(\tau)$$

where $\varepsilon_\circ$ is the fundamental unit of K. For,

$$P_\nu(\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi i}\left(\nu\varepsilon_\circ^{2n}\tau - \overline{\nu}\varepsilon_\circ^{2n}\left(\frac{1}{r\tau}\right)\right)$$

and
$$P_\mu(\tau) = \sum_{m=-\infty}^{\infty} e^{2\pi i}\left(\mu\varepsilon_\circ^{2m}\tau - \mu\varepsilon_\circ^{2m}.\left(\frac{1}{r\tau}\right)\right),$$

so that

$$\begin{aligned} P_\nu(\tau)P_\mu(\tau) &= \sum_{n,m} e^{2\pi i((\nu\varepsilon_\circ^{2n}+\mu\varepsilon_\circ^{2m})\tau-\overline{(\nu\varepsilon_\circ^{2n}+\mu\varepsilon_\circ^{2m})}(\frac{1}{r\tau}))} \\ &= \sum_{s=-\infty}^{\infty}\sum_{n} e^{2\pi i((\nu+\mu\varepsilon_\circ^{2s})\varepsilon_\circ^{2n}(\tau)-\overline{(\nu+\mu\varepsilon_\circ^{2s})}\varepsilon_\circ^{-2n}(\frac{1}{r\tau}))} \\ &= \sum_{s=-\infty}^{\infty} P_{\nu+\mu\varepsilon_\circ^{2s}}(\tau) \text{ where } \varepsilon_\circ^{2s}.\varepsilon_\circ^{2n} = \varepsilon_\circ^{2m}. \end{aligned}$$

If Γ denotes the unit group of an order of the quaternion algebra Q we introduced before, then we had seen that the function $f(\tau) = \tau^{-2f}\vartheta\left(\tau, -\frac{1}{r\tau}\right)$ is an automorphic form of degree $-4f$ for Γ.

Now, the above expression for $\vartheta\left(\tau, \frac{-1}{r\tau}\right)$ leads at once to the following:

$$\varphi(\tau) = \tau^{-2f}\sum_{(\nu)} c_{(\nu)}p_\nu(\tau)$$

152 with $P_\nu - s$ having the above property. A natural question arises now namely, is it true that *any* from $\psi(\tau)$ for the group Γ has an expansion of the above type and if so, is such an expansion unique? This question is still unsolved.

Petersson metric.

5. We shall now introduce the inner product (φ,ψ) in the space of automorphic forms of degree $-2f$, which was first defined by Peterson in 1939 (Math. Annalen, Vol. 116, page 406). If Q is a division algebra, φ and ψ may be arbitrary, but in case of Q being a matrix algebra or when Γ is a subgroup pf the module of the modular group, either φ or ψ must be a cusp form. (This condition becomes necessary for the convergence of the integral we are going to define). For two such forms, φ,ψ,

$$(\varphi,\psi) = \int_F \varphi(\tau)\,\overline{\psi(\tau)}\,y^{2f}\,\frac{dxdy}{y^2}$$

where F is a fundamental domain in the hyperbolic plane for the concerned group.

Now, if F_1 is any domain in the hyperbolic plane and if we replace F_1 by εF_1, then the above integral taken over F_1 or εF_1 is the same where $\varepsilon = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. For

$$\begin{aligned}(\varphi,\psi) &= \int_{F_1} \varphi(\tau).\overline{\psi(\tau)}.y^{2f}\frac{dx\,dy}{y^2}\\ &= \int_{F_1}\varphi(\varepsilon(\tau))\left(\frac{ad-bc}{(c\tau+d)^2}\right)^f \overline{(\psi(\varepsilon)(\tau))}\left(\frac{\overline{ad-bc}}{(c\tau+d)^2}\right)^f y^{2f}\\ &\qquad\qquad\cdot\left(\frac{|c\tau+d|^2}{ad-bc}\right)^f\frac{dx'\,dy'}{y'^2}\end{aligned}$$

where
$$\begin{aligned} y' &= \operatorname{Im}(\varepsilon(\tau)) = \operatorname{Im}\tau.\frac{ad-bc}{|c\tau+d|^2} = y.\frac{ad-bc}{|c\tau+d|^2}\\ &= \int\limits_{\varepsilon F_1}\varphi(\tau)\overline{\psi(\tau)}.y^{2f}.\frac{dx'\,dy}{y'^2},\ \tau' = \varepsilon(\tau).\end{aligned}$$ 153

Thus, if the fundamental domain is split up as $F = F_1 \cup \cdots \cup F_n$ and if $F' = \varepsilon_1 F_1 \cup \cdots \cup \varepsilon_n F_n$ where $\varepsilon_i \in \Gamma$, then (φ,ψ) taken over F or F' is the same.

12 Representation of T_n by Automorphic Forms

6. Let $T_n = \sum\limits_i \Gamma_j \gamma_i, \gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ with $n(\gamma_i) = n$. If $\varphi(\tau)$ is an automorphic form fo degree $-2f$ for the group Γ_τ, we define

$$\varphi(\tau).T_n = n^f. \sum_i \varphi(\frac{a_i\tau + b_i}{c_i\tau + d_i}).(c_i\tau + d_i)^{-2f} = \psi(\tau) \text{ (say)}.$$

Then $\psi(\tau)$ is again an automorphic form of degree $-2f$ for the group Γ_τ. Further one can show that an integral forms goes to an integral forms by T_n and a cusp form to a cusp form. The cusp forms are of special interest to us. Now, since the cusp forms of degree $-2f$ form a finite dimensional vector space, let $\varphi_1(\tau), \ldots, \varphi_d(\tau)$ be one basis for the same.Then

$$\varphi_i(\tau).T_n = \sum_{j=1}^{d} c_{ij}\varphi_j(\tau) \text{ (say) or}$$

$$\begin{pmatrix} \varphi_1(\tau) \\ \vdots \\ \varphi_d(\tau) \end{pmatrix} T_n = (c_{ij}) \begin{pmatrix} \varphi_1(\tau) \\ \vdots \\ \varphi_d(\tau). \end{pmatrix}$$

In order words, this gives rise to a representation of the ring of modular correspondences
$mathfrakR = \{T_n\}$, namely $T_n \to (c_{ij}) = R_f(T_n)$.

154 We shall now prove that the above representation matrix is hermitian if we choose the basis $\varphi_1, \ldots, \varphi_d$ to be orthonormal with respect to the Petersson metric. It is enough to show that

$$(\varphi \circ T_n, \psi) = (\varphi, \psi \circ T_n).$$

For, then $\varphi_1, \ldots, \varphi_d$ being orthonormal, $(\varphi_i, \varphi_j) = \delta_{ij}$, so that if

$$\varphi_i \circ T_n = \sum_{j=1}^{d} m_{ij}\varphi_j, \quad \text{then}$$

$$(\varphi_i \circ T_n, \varphi_k) = (\varphi_i, \varphi_k \circ T_n) \quad \text{implies that}$$

$$\left(\sum_j m_{ij}\varphi_j, \varphi_k\right) = \left(\varphi_i, \sum_j m_{m_{kj}}\varphi_j\right) \quad \text{or} \quad m_{ik} = \bar{m}_{ki}.$$

i.e., the matrix (m_{ij}) is hermitian so that all its eigen-values are real. Now, because of the product formula for T_n, it is sufficient to prove that

$$(\varphi \circ T_p, \psi) = (\varphi, \psi \circ T_p)$$

$$(\varphi \circ T_p, \psi) = \sum_i \int_F \varphi(v_i(\tau)).\overline{\psi(\tau)}.y^{2f}\frac{dxdy}{y^2}(c_i\tau + d_i)^{-2f}$$

where F is a fundamental domain for Γ.

If $\Gamma(p)$ be the group of matrices $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma$ with the property $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \pmod{p}$

$$(\varphi \circ T_p, \psi)_\Gamma = \frac{1}{g(p)}(\varphi \circ T_n, \psi)_{\Gamma(p)}$$

where $g(p)$ is the index of $\Gamma(p)$ in Γ.

Now $\varphi_i(\tau) = \varphi(v_i(\tau)).(c_i\tau + d_i)^{-2f}$ is an automorphic forms of degree $-2f$ for the group $v_i^{-1}\Gamma v_i$ and since $g(p)$ is also the index of $\Gamma(p)$ is each $v_i^{-1}\Gamma v_i$, we have 155

$$(\varphi \circ T_p, \psi) = \frac{1}{g(p)}\sum_i(\varphi_i, \psi)_{\Gamma(p)}.$$

On replacing τ by $v_i^{-1}(\tau) = \bar{v}_i(\tau)$ and observing that for a suitable system of v_i, when v_i runs over a system of non-associated integral elements of $\mathcal{J}$ of norm $p, \bar{v}_i$ also does the same, we obtain

$$\frac{1}{g(p)}\sum_i(\varphi_i, \psi)_{\Gamma(p)} = \frac{1}{g(p)}\sum_i(\varphi, \psi_i)_{\Gamma(p)}$$

where $\psi_i = \dfrac{\psi(\bar{v}_i(\tau))}{(-c_i\tau + a_i)^{2f}}$. Then

$$\frac{1}{g(p)}\sum_i(\varphi, \psi_i)_{\Gamma(p)} = \frac{1}{g(p)}(\varphi, \psi \circ T_p)_{\Gamma(p)} = (\varphi, \psi \circ T_p)$$

Consider integral modular forms $\varphi(\tau)$ of degree $-2f = -2$. Then $\varphi(\tau)d\tau = du$ becomes a differential holomorphic at all points of the surface $S_{\mathcal{J}}$ except perhaps at the vertices and cusps. In the neighbourhood of an elliptic vertex of order n, for the differential du to be holomorphic, we required that $\dfrac{\varphi(\tau)}{(\tau-\tau_\circ)^{n-1}}$ be holomorphic, since

$$\varphi(\tau).d(\tau-\tau_\circ) = \frac{\varphi(\tau).d(\tau-\tau_\circ)^n}{n(\tau-\tau_\circ)^{n-1}}.$$

In the neighbourhood of the cusps, for example, at $\infty, \varphi(\tau)d\tau = \psi(\tau)d(e^{2\pi i\tau})$ $(e^{2\pi i\tau}$ is the local uniformizer) and for the differential du to be holomorphic we require that $\psi(\tau)$ be holomorphic or $\varphi(\tau)e^{2\pi i\tau}$ be holomorphic. In other words, $\varphi(\tau)$ must have a zero at ∞.

156 Similarly at all cusps. Therefore we can look upon the space of cusp forms of degree -2 belonging to the group $\Gamma_{\mathcal{J}}$ as the space of differentials of the first kind on the surface $S_{\mathcal{J}}$. The space of cusps forms being invariant under T_n, we have a representation of T_n in the space of differentials of the first kind on $S_{\mathcal{J}}$. We shall now find explicitly the trace of this representation.

Let $\varphi_1(\tau)d\tau, \ldots, \varphi_g(\tau)d\tau$ be a base for the space of differentials of the first kind and $c_1, \ldots, c_{2g}$ be a system of representatives of a basis for the first homology group. Then, setting $\nu_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j, \end{pmatrix}$

$$\begin{aligned}\int_{c_i} \varphi_k(\tau).T_n d\tau &= \sum_j \int_{c_i} \varphi_k\left(\frac{a_j\tau+b}{c_j\tau+d_j}\right).d\left(\frac{a_j\tau+b}{c_j\tau+d_j}\right)\\ &= \sum_i \int\limits_{\nu_j(c_i)} \varphi_k(\tau)d\tau = \int\limits_{c_i.T_n} \varphi_k(\tau)d\tau.\end{aligned}$$

Let $\varphi_k(\tau)\circ T_n = \sum\limits_{t=1}^{g} m_{kt}\varphi_t$ and $c_i \circ T_n = \sum\limits_{j=1}^{2g} c_j M_{ij}$ with M_{ji} integers. Then $\sum\limits_{t=1}^{g} m_{kt}r_{ti} = \sum\limits_{j=1}^{2g} r_{kj}M_{ji}$ where $R = \left(\int\limits_{c_i} \varphi_k(\tau)d\tau\right) = (r_{ki})$ is the period matrix (Riemann matrix) of $S_{\mathcal{J}}$. From above we have

$$mR = RM \text{ or } \overline{mR} = \bar{R}M$$

since the elements M are integers.

On denoting the $(2g, 2g)$ matrix $\begin{pmatrix} R \\ \overline{R} \end{pmatrix}$ ($\overline{R}$ denoting the conjugate of R) by p, we have $\begin{pmatrix} m & 0 \\ 0 & \overline{m} \end{pmatrix} P = PM$ or $2tr(m) = tr(M)$, since P is known to be non-singular. In other words, 157

$$\boxed{2tr_1(T_n) = \mathrm{tr}^1(T)_n.}$$

Note . *Even when $2f > 2$ (but Γ has to be the full modular group), a formula for $tr(R_f(T_n))$ has been found by Selberg (Report of the International Colloquium on Zeta-sanctions, page 85). In our case, this method gives*

$$\mathrm{tr}(R_f(T_n)) = \frac{1}{n^{f-1}}\Bigg[- 2^{k_2+1} \sum_{\substack{d|n \\ d\leq \sqrt{n}}} d^{2f-1-} \sum_{t,f} \prod_{p|q_1} \left(1 - \left\{\frac{\Delta}{p}\right\}\right)$$
$$\prod_{p|q_2} \left(1 + \left\{\frac{\Delta}{p}\right\}\right) \frac{h(\Delta)}{\omega(\Delta)} \cdot \frac{\eta^{2f-1-}\overline{\eta}^{2f-1}}{\eta - \overline{\eta}}$$

where $\eta = \frac{1}{2}(t + \sqrt{\Delta})$.

(The trace need not be an integer).

Appendix I

1. We shall, in this appendix, discuss a certain algebraic cohomology and obtain a mapping forms of degree $-2f$ on certain cohomology classes. 158

Let $\varphi(\tau)$ be an automorphic form of degree $-2f$ with respect to a group Γ of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $(a, b, c, d$ real).

Consider $\Phi(\tau) = \dfrac{1}{(2f-2)!} \int_{\tau_0}^{\tau} (\tau - \sigma)^{2f-2} \varphi(\sigma) d\sigma$ where $\tau_\circ$ is a fixed point in $\operatorname{Im}(\tau) > 0$. The integral exists and by direct verification $\dfrac{d^{2f-1}\Phi(\tau)}{d\tau^{2f-1}} = \varphi(\tau)$.

Let now $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Then, we have, on putting $\sigma = \alpha(\sigma)$,

$$\Phi(\alpha(\tau)).\frac{(c\tau+d)^{2f-2}}{(ad-bc)^{f-1}} = \frac{1}{(2f-2)!} \int\limits_{\alpha^{-1}(\tau_\circ)}^{\tau} \left(\frac{a\tau+b}{c\tau+d} - \frac{a\sigma'+b}{c\sigma+d} \right)^{2f-2}.$$

$$\varphi(\sigma) \frac{(c\sigma'+d)^{2f}}{(ad-bc)^{f}} \frac{(c\tau+d)^{2f-2}}{(ad-bc)^{f-1}} \frac{ad-bc}{(c\sigma'+d)^2} d\sigma'$$

$$= \frac{1}{(2f-2)!} \int\limits_{\alpha^{-1}(\tau_\circ)}^{\tau} (\tau-\sigma)^{2f-2} \varphi(\sigma') d\sigma'$$

$$= \frac{1}{(2f-2)!} \left[\int\limits_{\alpha^{-1}(\tau_\circ)}^{\tau} + \int\limits_{\tau_\circ}^{\tau} \right]$$

$$= C(\alpha;\tau) + \Phi(\tau)$$

where $C(\alpha;\tau) = \frac{1}{(2f-2)!} \int\limits_{\alpha^{-1}(\tau_\circ)}^{\tau} (\tau-\sigma')^{2f-2}\varphi(\sigma')d\sigma'$ and hence a polynomial of degree $\leq 2f-2$.

159 Defining $\Phi(\tau).\alpha = \Phi(\alpha(\tau))\dfrac{(c\tau+d)^{2f-2}}{(ad-bc)^{f-1}}$ and

$$C(\tau).\alpha = C(\alpha(\tau))\frac{(c\tau+d)^{2f-2}}{(ad-bc)^{f-1}} \tag{*}$$

we may write the above as $\Phi(\tau).\alpha = C(\alpha;\tau) + \Phi(\tau)$. In other words,

$$C(\alpha,\tau) = \Phi(\tau).\alpha - \Phi(\tau),$$

and consequently for $\alpha,\beta \in \Gamma$,

$$\begin{aligned} C(\alpha\beta;\tau) = \Phi.\alpha\beta - \Phi &= (\Phi.\alpha - \Phi).\beta + (\Phi.\beta - \Phi) \\ &= C(\alpha;\tau).\beta + u(\beta;\tau). \end{aligned}$$

We may now assume for the same of simplicity that the elements of Γ have determinant 1.

We shall now go into the algebraic meaning behind these formulae.

Let $\mathfrak{M}$ be a representation module of the group Γ. A mapping $\alpha \to C(\alpha)$ of Γ into the representation module m we shall call a 1-*cochain,* and if this cochain satisfies the equation

$$C(\alpha\beta) = C(\alpha).\beta + C(\beta),$$

then it is *closed* or a 1-*cocycle*. Special cocycles $C(\alpha) = m.(\alpha - 1)$, ($m$ being fixed element of $\mathfrak{M}$ and 1 denotes the unit matrix) are called *coboundaries*. Now, the cocycles forms an additive group Z and the coboundaries from a subgroup B of Z and the quotient group Z/B is the *first cohomology group* of Γ in $\mathfrak{M}$ and its elements are called *cohomology classes*.

160 Take for $\mathfrak{M}$, the vector space of polynomial of degree $\leq 2f-2$ and the representation of Γ in m defined as above by $(*)$. Then, associated

with every $\varphi(\tau)$ we have the following mapping $\varphi(\tau) \to \{C(\alpha, \tau)\}$ and the cochain $C(\alpha) : \alpha \to C(\alpha; \tau)$ is a cocycle, as we had seen already. Thus, to a modular form of degree $-2f$, there corresponds a cocycle $C(\alpha)$. This cocycle still depends on the constant τ_0 occurring in the definition of $\Phi(\tau)$. A change of $\tau_\circ$ would add a coboundary to $C(\alpha)$, for, suppose

$$\Phi_1(\tau) = \frac{1}{(2f-2)!}\int\limits_{\tau_1}^{\tau}(\tau-\sigma)^{2f-2}\varphi(\sigma)d\sigma$$

$$= \frac{1}{(2f-2)!}\left(\int\limits_{\tau_1}^{\tau_\circ} + \int\limits_{\tau_\circ}^{\tau}\cdots\right)$$

$$= p(\tau) + \Phi(\tau) \text{ where } p(\tau) = \frac{1}{(2f-2)!}\int\limits_{\tau_1}^{\tau_\circ}(\tau-\sigma)^{2f-2}\varphi(\sigma)d\sigma$$

is a polynomial in τ of degree $\leq 2f-2$. Therefore

$$\Phi_1 \circ \alpha = p(\tau).\alpha + \Phi(\tau).\alpha$$

and if $$\Phi_1 \circ \alpha - \Phi_1 = C_1(\alpha; \tau),$$

then $C_1(\alpha; \tau) = p(\tau).(\alpha - 1) + C(\alpha; \tau)$ or $C_1(\alpha; \tau) - C(\alpha; \tau) = p(\tau).(\alpha - 1)$ which shows that the cocycle $C_1(\alpha) - C(\alpha)$ is a coboundary.

Consequently, we have now a well-defined mapping $\varphi(\tau) \to$ (a cohomology class). We may even prove that this mapping is onto. For, let C be a representative of the cohomology class $\overline{C}$ and $C(\alpha)$ (for $\alpha \in \Gamma$) = $C(\alpha; \tau)$, a polynomial of degree $\leq 2f-2$.

Consider now the series $\psi(\tau) = \sum\limits_{\alpha\in\tau} \dfrac{c(\alpha;\tau)}{(c\tau+d)^{2n}} e^{2\pi i\mu\alpha(\tau)}$, ($\mu$ a positive integer). Then the series converges for n sufficiently large (only if Γ is the unit group of $\mathcal{J} = \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ q_2\mathcal{O} & \mathcal{O}\end{pmatrix}$), and if $\beta = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma$, we have 161

$$(\psi(\tau).\beta)(c'\tau + d')^{-2n} = \psi(\beta(\tau)).(c'\tau + d')^{2f-2-2n}$$

$$= \sum_{\alpha\in\Gamma} \frac{C(\alpha; \tau).\beta}{(C''\tau + d'')^{2n}} e^{2\pi i\mu\alpha\beta(\tau)}$$

where $\alpha\beta = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in \Gamma, C$ being a cocycle,

$$\begin{aligned}(\psi(\tau).\beta)(c'\tau + d')^{-2n} &= \sum_{\alpha\beta \in \Gamma} \frac{C(\alpha\beta;\tau)}{(C''\tau + d'')^{2n}} e^{2\pi i \mu \alpha\beta(\tau)} \\ &\qquad - C(\beta;\tau) \sum_{\alpha\beta} \frac{e^{2\pi i \mu \alpha\beta(\tau)}}{(C''\tau + d'')^{2n}} \\ &= \psi(\tau) - C(\beta;\tau)\chi(\tau)\end{aligned}$$

$\chi(\tau)$ being a genuine Poincare series, is modular form of degree $-2n$. Putting $\Phi(\tau) = \dfrac{\psi(\tau)}{\chi(\tau)}$, we obtain

$$\frac{\psi(\beta(\tau))}{\chi(\beta(\tau))}(c'\tau + d')^{2f-2} = \Phi(\tau) - C(\beta;\tau).$$

In other words,

$$\Phi(\tau) \cdot \beta = \Phi(\tau) - C(\beta;\tau).$$

On differentiating $\Phi(\tau), (2f - 1)$ times and calling $\varphi(\tau) = \dfrac{d^{2f-1}\Phi(\tau)}{d\tau^{2f-1}}$ we have the required modular form $\varphi(\tau)$ of degree $-2f(\varphi(\tau))$ will have poles in general) and we easily see that C is the cocycle associated with $\varphi(\tau)$. Again, it is to be noted that the form $\varphi(\tau)$ is independent of the representative cocycle C in the class $\overline{C}$.

162 We have thus established a two-way mapping (not necessarily one-one), between the space of modular forms of degree $-2f$, and with have the property that they have no logarithmic singularities and the cohomology classes defined above.

Remarks. (1) *In the above correspondence, though the mapping $\varphi \rightarrow \overline{C}$ is unique, the converse mapping $\overline{C} \longrightarrow \varphi$ is not uniquely defined. For securing one-one nature, we take the space of classes of forms of degree $-2f$ modulo $(2f - 1)t\underset{\cdot\cdot}{h}$ derivatives of forms of degree $+(2f - 2)$, because the periods of the integrals of these derivatives are 0. The rank of the modulo of integral forms taken modulo the space of $(2f - 2)th$ derivatives of forms of degree $2f - 2$*

can be calculated by application of Riemann-Roch theorem (Refer M.Eichler, Eine Verallgemienerung der Abelsche Integral, Mathenatische Zeitschrift, 1957*).*

(2) *The above procedure can be generalized to forms not necessarily integral but the singularities must be such that no logarithmic terms can occur. (Ibid).*

2. We now study the behaviour of $C(\alpha)$ under the correspondences T_n. Let ν_i be defined as usual and $\alpha \in \Gamma_{\mathcal{J}}$. Then $\nu_i\alpha = \alpha'\nu_j, \alpha' \in \Gamma_{\mathcal{J}}$, with j and α' depending on i and α. We defined now,

$$\begin{aligned}\Psi(\tau) = \Phi(\tau).T_n &= \sum_{i=1}^{d_n} \Phi(\tau).\nu_i\\ &= \sum_{i=1}^{d_n} \frac{(C_i\tau + d_i)^{2f-2}}{(a_id_i - b_ic_i)^{f-1}}\Phi\left(\frac{(a_i\tau + b_i)}{(c_i\tau + d_i)}\right).\end{aligned}$$

To the pair i, α, there exist $j = j(i, \alpha)$ and $\alpha' = \alpha'(i, \alpha)$, such that $\nu_i\alpha = \alpha'\nu_j$. Consequently,

$$\begin{aligned}\Psi(\tau).\alpha &= \sum_{i=1}^{d_n}(\Phi(\tau).\alpha').\nu_j = C'(\alpha;\tau) + \Psi(\tau) \text{ with}\\ C'(\alpha) &= \sum_{i=1}^{d_n} C(\alpha').\nu_j = C(\alpha).T_n \text{ (definition)}.\end{aligned}$$

Thus T_n are made endomorphisms of the first cohomology group of $\Gamma_{\mathcal{J}}$ in the module $\mathfrak{M}$ of polynomial of degree $\leq 2f - 2$. We have only to show that $C'(\alpha)$ is closed if $C(\alpha)$ is closed and that coboundaries are mapped onto coboundaries. Indeed, if $C(\alpha) = C(\alpha - 1)$, then 163

$$C'(\alpha) = \sum_i C.(\alpha' - 1)\nu_j = \sum_i C.(\nu_i\alpha - \nu_j) = \left(\sum_i C.\nu_i\right)(\alpha - 1)$$

Now $\nu_i\alpha\beta = \alpha'\nu_i\beta = \alpha'\beta'\nu_k$ (say). Then

$$C'(\alpha\beta) = \sum_i C(\alpha'\beta').\nu_k$$

$$
\begin{aligned}
&= \sum_i (C(\alpha').\beta' + C(\beta')).v_k \\
&= \sum_i C(\alpha')v_i.\beta + \sum_i C(\beta')v_k
\end{aligned}
$$

or in other words, $C'(\alpha\beta) = C'(\alpha).\beta + C'(\beta)$ where one has to bear in mind that j and k are function of i which assume all values from 1 to d_n.

It is easy to verify that the above-defined endomorphisms are in fact independent of the special choice of the v_i.

Then, the natural question is to ask for the trace of this endomorphisms and this has been calculated even for more general discontinuous groups Γ, by M.Eichler (Verallegemeinerung der Ablesche Integrale, Mathematische Zeitschrift, 1957)

Appendix II

3. We shall now speak about some ideas of Heche and their possible generalizations. 164

Let $\Gamma(Q) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right.$ with $c \equiv 0(Q)$ and $\Gamma_1(Q) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right.$ $\left.(\text{mod } Q)\right\}$ be subgroups of the modular group. It can easily be seen that $\Gamma(Q)/\Gamma_1(Q) \cong$ multiplicative groups of prime residue classes modulo Q. (This quotient group can also be interpreted as $G(K_1/K)$ where $G(K_1/K)$ denotes the Galio group of the field K_1 of functions invariant under $\Gamma_1(Q)$ over K, field of functions invariant under $\Gamma(Q)$).

Consider the space of modular forms of degree $-2f$ for the groups $\Gamma_1(Q)$. Let $\varphi_1(\tau), \ldots, \varphi_\alpha(\tau)$ form a basis of this space. Then, for every $\alpha \in \Gamma(Q)$,

$$\varphi_i(\tau).\alpha = \sum_{j=1}^{d} C_{ij}(\alpha)\varphi_j(\tau)$$

gives a representation $\alpha \to c_{ij}(\alpha)$ of the quotient group $\Gamma(Q)/\Gamma_1(Q)$. This finite group being abelian, this representation splits into one- dimensional ones so that for a suitable basis $\psi_1(\tau), \ldots, \psi_d(\tau)$, we have

$$\psi_i(\tau).\alpha = \chi_i(\alpha).\psi_i(\tau),$$

and the representation is given by $\alpha \to \chi(\alpha) = \begin{pmatrix} \chi(\alpha) \cdots 0 \\ \vdots \\ 0 \cdots \chi_\alpha(\alpha) \end{pmatrix}$; $\chi_i - s$ denoting characters of the group $\Gamma(Q)/\Gamma_1(Q)$.

In this connection, the study of forms φ with a given character, was made by Hecke (Uber Modulfunktionen und die Dirichlerschen Reihen mit Eulerscher Produktentwicklug, *I* and *II*, Math. Annalen, 1937.) For example, it can be shown that the theta-series

$$\vartheta_F(\tau) = \sum_{\underline{X}} e^{\pi i\tau \underline{X}' F \underline{X}}$$

165 where $\underline{X}' F \underline{X}$ is a positive definite even quadratic form, is a modular form with the character $\chi(a) = \left(\dfrac{(-1)^f |F|}{a}\right)$ (we denote $\chi(\alpha)$ by $\chi(a)$ where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$).

The modular correspondences T_n are defined as in Hecke's paper and this ring of operator takes holomorphic forms to holomorphic forms and cusp forms to cusp forms.

4. Let $\varphi_1(\tau), \ldots, \varphi_\alpha(\tau)$ be basis of forms of degree $-2f$ with respect to the the group $\Gamma_1(\Omega)$ with character χ. Then we have

$$\begin{pmatrix} \varphi_1(\tau) \\ \vdots \\ \varphi_d(\tau). \end{pmatrix} T_n = R_f(T_n). \begin{pmatrix} \varphi_1(\tau) \\ \vdots \\ \varphi_d(\tau). \end{pmatrix} \text{ or if } \varphi(\tau) = \begin{pmatrix} \varphi_1(\tau) \\ \vdots \\ \varphi_d(\tau). \end{pmatrix}$$

$$\varphi\tau.T_n = R_f(T_n).\varphi(\tau).$$

Now, let the Fourier expansion of $\varphi(\tau)$ be $\sum\limits_{n=\circ}^{\infty} c_n e^{2\pi i n\tau/Q}$ c_n being column vectors.

Consider $\varphi(\tau).T_p$, p a prime. By definition, $T_p = \sum\limits_i \Gamma(Q).\nu_i$ and for ν_i, we may take

$$\left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} 0 \leq r < p \right\}$$

so that $$\varphi(\tau).T_n = \overline{\chi}(p) \sum_{n=0}^{\infty} p^f c_n e^{2\pi i\ np\tau/Q} + 1 \sum_{r=\circ}^{p-1} \sum_{n=0}^{\infty} \frac{1}{p^{f^c n}} e^{2\pi i \frac{n}{\alpha} \frac{n}{Q} \frac{t+r}{p}}$$

$$= \overline{\chi}(p) p^f \sum_{n=0}^{\infty} \frac{c_n}{p} e^{2\pi i\ np\tau/Q} + p^{1-f} \sum_{n=0}^{\infty} c_{np} e^{2\pi i n\tau/Q}$$

with the prescription that $c_{n/p} = 0$ if $p \nmid n$. **166**

But $\varphi(\tau).T_p = R_f(T_p).\varphi(\tau) = \sum\limits_{n=0}^{\infty} R_f(T_p).c_n e^{2\pi i\ np\tau/Q}$ and on comparing the coefficients of $e^{2\pi i\tau/Q}$ on both sides, we obtain the famous formula fo Hecke,

$$R_f(T_p).c_1 = p^{1-f}.c_p \text{ or } c_p = p^{f-1}R_f(T_p).c_1$$

Using the product formula for T_n, we may obtain the same for arbitrary n, as: $C_n = n^{f-1}R_f(T_n).c_1$.

This helps us to pass from zeta-functions associated with $R_f(T_n)$ to those associated with modular forms; for, if

$$\zeta_R(s) = \sum_{n=1}^{\infty} \frac{R_f(T_n)}{n^s} \text{ and } \zeta_M(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}, \text{ then } \zeta_M(s) = n^{f-1}c_1\zeta_R(s).$$

In the case of subgroup of the modular group we have a functional equation for $\zeta_M(s)$ obtained from the behaviour of $\vartheta(\tau)$ (in this particular case) under the substitution $\tau \to \frac{-1}{\tau}$ and this gives a functional equation for $\zeta_R(s)$. But for groups of orders of division algebras, this is an open problem.

5. We now make one more application of our modular correspondences.

Consider the theta-series $\vartheta(\tau) = \sum\limits_{\underline{X}} e^{\pi i\tau \underline{X}'F\underline{X}}$ with a positive form $\underline{X}'F\underline{X}$. This is a modular form for a suitable subgroup of the modular group. There is a nature question whether every modular form can be expressed as a linear combination of such theta-series. The general question is still unsolved. But, in a special case, Hecke conjectured in 1936 that all integral modular forms of degree -2 and stufe q(a prime) can be expressed as a linear combination of theta-series associated with **167** quaternary forms. We succeeded in proving this conjecture, a couple of years ago, (M.Eichler, Crelle's Journal, 1956, Uber Darstellbarkeit von Modulformen durch Thetareihen) and proof is based on the equality of the trace of the representation of correspondence T_n, by means of cusp forms of degree -2 and stufe q and by means of ϑ-series associated with norm forms of a difinite quaternion algebra. Even in case $2f > 2$, Hecke's conjecture can be generalized by considering the ϑ-series with spherical harmonies and if we use Selber's trace formula and compare the two traces, we obtain the following result; all cusp forms of stufe q (a prime) are representable as a sum of cusp forms for the whole modular group and generalized ϑ-series with spherical harmonics for definite quaternion algebras of discriminant q^2.