SINGULAR HECKE–SHIMURA RINGS AND HECKE OPERATORS ON SIEGEL MODULAR FORMS

ANATOLI ANDRIANOV

Max-Planck-Institut für Mathematik, Bonn

Institut Fourier, Grenoble

St.Petersburg Steklov Mathematical Institute, St.Petersburg

Abstract

Theory of singular Hecke–Shimura rings and Hecke operators on Siegel modular forms for the groups $\Gamma_0^n(q)$ is developed. It is proved, in particular, that, if $n = 2$, the spaces of new cusp forms of integral weights are spanned by common eigenfunctions of all regular Hecke operators, Hecke operators corresponding to elements of singular unramified rings, and to all of the singular Frobenius elements. The classical case of one variable, considered by Atkin and Lehner, is included.

Table of contents

Introduction

The most impressive applications of modular forms to Diophantine number theory during the last decade, the proof of the Fermat's last theorem by Willes and Teylor, would be literally impossible without a reasonable complete theory of Hecke p-operators on modular forms in one variable for all prime numbers p , both for primes which do not divide the level of modular forms (*regular p-operators* due to Hecke [He(37)] and Petersson [Pet(39)]), and for prime divisors of the level (*singular p-operators* studied by Atkin and Lehner [A-L(70)], Li [Li(75)], and others). Without this one could not even define all of the p-factors of Euler products corresponding to modular forms and, therefore, formulate precisely the Shimura–Taniyama conjecture on zeta functions of elliptic curves, which lies in the heart of the Willes–Teylor proof.

One can hardly doubt that the relation between zeta functions of elliptic curves and zeta functions of modular forms in one variable known as Shimura–Taniyama conjecture is only a particular case of some general links of global zeta functions of algebraic varieties and zeta functions of automorphic forms in several variables. Speaking on Abelian varieties in place of elliptic curves, one can expect that modular forms in one variable should be replaced by Siegel modular forms for congruence subgroups of the Siegel modular group $\Gamma^n = Sp_n(\mathbb{Z})$, which expectation is supported by numerical evidences (see, for example, [SM-T(93)]). One of the main obstacle in this direction is complete absence of theory of singular Hecke–Shimura rings and Hecke operators on Siegel modular forms. Here we start to fill this gap.

We develop the theory of *singular*(i.e. related to divisors of levels) Hecke-Shimura rings and Hecke operators on Siegel modular forms for the congruence subgroups of Γ^n of the form $\Gamma_0^n(q)$ (see (2-1)). In particular, it is proved that, if $n = 2$, the spaces of new cusp forms of integral weights are spanned by common eigenfunctions of all regular Hecke operators, Hecke operators corresponding to elements of singular nonramified rings, and to all of the singular Frobenius elements.

Contents. Chapter 1 contains all necessary definitions and facts on Siegel modular forms, general Hecke–Shimura rings, and Hecke operators. Chapter 2 treats specifically regular reducible rings and operators for $\Gamma_0^n(q)$. The proofs in Chapters

1 and 2 are, as a rule, omitted and referred to ours books [An(87)] or [An-Z(90)]. The Chapter 3 is the key chapter. It deals with singular Hecke–Shimura rings for the groups $\Gamma_0^n(q)$. Especially important is §3.3, where, for prime divisors p of q not dividing q/p (*nonramified primes*),canonical embedding of regular reducible p-rings of $\Gamma_0^n(q/p)$ into (*singular*) p-rings of $\Gamma_0^n(q)$ are defined and studied. The embeddings replace parabolic embeddings of regular rings. Chapter 4 contains definitions of old and new cusp forms and considers the questions of their invariance under various Hecke operators and existence of eigenforms. The exposition is essentially based on properties of trace-idempotents, considered in §4.1. Conclusion contains some remarks on possible generalization of the results and their applications.

Acknowledgment. First of all, I wish to thank my colleagues of Institut Fourier (Universite Joseph Fourier, Grenoble, France) and Max-Planck-Institut für Mathematik (Bonn, Germany), where big parts of the present research were carried out and reported, and the paper was prepared, for kind invitations, substantial discussions, and various help. Especially I should like to thank Professor Roland Gillard and Professor Alexei Panchishkin of Institut Fourier, and Professor Yuri Manin of Max-Planck-Institut, who has also taught me to $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX this paper. I am grateful to Fedor Andrianov, who has expertly read the files and initiated a number of improvements.

Last, but foremost, my thanks to my wife, as a small acknowledgment of her patience and moral support.

The research was partly supported by Russian Fund of Fundamental Researches (Grant 96-01-00663).

NOTATION. We fix the letters $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ for the set of positive rational integers, the ring of rational integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively.We set

$$\mathbb{N}_{(q)}=\{n \in \mathbb{N}; \quad \gcd(n, q) = 1\},$$

and

$$\mathbb{N}_q = \{n \in \mathbb{N}; \quad n|q^\infty\},$$

where the expression $n|q^\infty$ means that n divides a power of q.

$\mathbb{A}_n^m$ is the set of all $m \times n$–matrices with entries in a set $\mathbb{A}$. We denote by

$$\mathbb{S}_n = \{M \in \mathbb{Z}_n^n; \quad {}^tM = M\},$$

where ${}^tM$ always denotes the transposed matrix, the set of all integral symmetric matrices of order n, and by

$$\mathbb{E}_n = \{M = (m_{ij}) \in \mathbb{S}_n; \quad m_{ii} \in 2\mathbb{Z}, \quad i = 1, \dots, n\}$$

the set of all *even* matrices of order n.

E_n will denote the unit matrix of order n , and

$$J_n = \begin{pmatrix} 0 & -E_n \\ E_n & 0 \end{pmatrix},$$

where $0 = 0_n$ is the zero matrix of order n.

For brevity we set

$$a(a+1)/2 = \langle a \rangle.$$

Chapter 1

The Background

In this chapter we shall briefly recall basic definitions and properties of symplectic matrices, Siegel modular forms, Hecke-Shimura rings, and Hecke operators for arithmetical discrete subgroups of the real symplectic group $Sp_n(\mathbb{R})$. Majority of the proofs can be found in the books [An(87)], [An-Z(90)], or can be restored by the reader in the course of easy exercises. We make an exception only for *Theorem 1.9*, because it is difficult to point out at explicit reference.

§1.1. Symplectic matrices, groups, and operators

A matrix $M \in \mathbb{C}_{2n}^{2n}$ is said to be *symplectic*, if it satisfies the relation

$$^tM \cdot J_n \cdot M = \mu J_n,$$

with a nonzero scalar $\mu = \mu(M)$ called *the multiplier of* M (see *Notation*).

Lemma 1.1. *Let* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, *where* A, B, C, D *are complex matrices of dimension* $n \times n$, *and* μ *be a nonzero complex number. Then the following conditions are equivalent:*

(1) *M is symplectic of the multiplier $\mu(M) = \mu$;*
(2) *^tM is symplectic of the multiplier $\mu(^tM) = \mu$;*
(3) *M is invertible, and*

$$\mu M^{-1} = \begin{pmatrix} ^tD & -^tB \\ -^tC & ^tA \end{pmatrix};$$

(4) $^tA \cdot C = {}^tC \cdot A, \quad {}^tB \cdot D = {}^tD \cdot B, \quad {}^tA \cdot D - {}^tC \cdot B = \mu E_n;$
(5) $A \cdot {}^tB = B \cdot {}^tA, \quad C \cdot {}^tD = D \cdot {}^tC, \quad A \cdot {}^tD - B \cdot {}^tC = \mu E_n.$

In the course of our arithmetical considerations we shall be interested in discrete subgroups and subsemigroups of the general real positive symplectic group of a genus $n \in \mathbb{N}$ consisting of all real symplectic matrices of order $2n$ with positive multipliers,

$$G^n = GSp_n^+(\mathbb{R}) = \{M \in \mathbb{R}_{2n}^{2n}; \quad {}^tM \cdot J_n \cdot M = \mu(M)J_n, \quad \mu(M) > 0\}.$$

The group G^n is a real Lie group acting as a group of analytical automorphisms on the $n(n+1)/2$ – dimensional complex variety

$$\mathbb{H}_n = \{Z = X + iY \in \mathbb{C}_n^n; \quad {}^tZ = Z, \ Y > 0\},$$

the Siegel upper half-plane of genus n, by the rule

$$G^n \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} : \; Z \to M\langle Z\rangle = (AZ+B)(CZ+D)^{-1}, \quad (Z \in \mathbb{H}_n).$$

The action satisfies

$$(M \cdot M')\langle Z\rangle = M\langle M'\langle Z\rangle\rangle, \qquad (M, M' \in G^n, \; Z \in \mathbb{H}_n).$$

Acting on $\mathbb{H}_n$, the group G^n acts also on functions $F : \mathbb{H}_n \to \mathbb{C}$ by means of *the Petersson operators of integral weights k*,

$$G^n \ni M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} : \; F \to F|_k M = \det(CZ+D)^{-k} F(M\langle Z\rangle), \tag{1-1}$$

satisfying

$$F|_k(M \cdot M') = F|_k M|_k M', \quad F|_k rM = r^{-nk} F|_k M \tag{1-2}$$

for every $F : \; \mathbb{H}_n \to \mathbb{C}, \quad M, M' \in G^n$, and $r \in \mathbb{R} - \{0\}$.

§1.2. Integral matrices and discrete subgroups

We consider the semigroup

$$\Sigma = \Sigma^n = G^n \bigcap \mathbb{Z}^{2n}_{2n}$$

of integral symplectic matrices of order $2n$ with positive multipliers. The inverse M^{-1} of a matrix M of Σ not necessarily belongs to Σ, but the matrix

$$M^* = \mu(M) M^{-1} = J_n^{-1} \cdot {}^t M \cdot J_n \tag{1-3}$$

does, and the map $M \to M^*$ is an antiautomorphism of the semigroup Σ preserving multipliers:$\mu(M^*) = \mu(M)$. Each subgroup of Σ is contained in the maximal subgroup

$$\Gamma = \Gamma^n = Sp_n(\mathbb{Z}) = \{M \in \Sigma^n; \quad \mu(M) = 1\},$$

called *the Siegel modular group of genus n.*

In order to build matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ belonging to Γ, it will be useful to characterize the "second rows" (C, D) of such matrices. A pair (C, D) of square matrices of order n will be called *symmetric*, if it satisfies $C \cdot {}^t D = D \cdot {}^t C$; it will be called *coprime*, if the matrices C and D are integral and the products RC, RD by a matrix R of order n are both integral only if R is integral.

Lemma 1.2. *Let (C, D) be a pair of integral matrices of order n. Then the following conditions are equivalent:*

(1) *There are matrices A, B such that* $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma$;

(2) *The pair (C, D) is symmetric and coprime.*

The modular group $\Gamma = \Gamma^n$ is clearly discrete in G^n.This is also true for every of subgroups of G^n commensurable with Γ. We shall remind that two subgroups $\mathcal{K}$, $\mathcal{K}'$ of a group $\mathcal{G}$ is said to be *commensurable*, if their intersection $\mathcal{K} \cap \mathcal{K}'$ has finite indexes both in $\mathcal{K}$ and $\mathcal{K}'$. The relation of commensurability is reflexive, symmetric, and transitive, and so the set of all subgroups of $\mathcal{G}$ is a disjoint union of *classes of commensurable subgroups. The principal congruence subgroup of level q,*

$$\Gamma(q) = \Gamma^n(q) = \{M \in \Gamma^n; \quad M \equiv E_{2n} \pmod q\},$$

and each of intermediate subgroups K,

$$\Gamma(q) \subset K \subset \Gamma,$$

called *congruence subgroups of level q*, have finite indexes in Γ and therefore are commensurable with Γ. Also, if K is commensurable with Γ, it is also true for every conjugated subgroup $M^{-1} \cdot K \cdot M$ with $M \in \Sigma$. The following easy lemma relates decompositions of double cosets with decompositions of corresponding groups, which is often useful in the theory of Hecke–Shimura rings and Hecke operators.

Lemma 1.3. *Let G be a multiplicative group, K and K' subgroups of G, and $g \in G$. Then the following disjoint decomposition holds*

$$KgK' = \bigcup_{\gamma_i \in g^{-1}Kg \cap K' \backslash K'} Kg\gamma_i.$$

The last lemma implies

Lemma 1.4. *If K is commensurable with Γ^n and $M \in \Sigma^n$,then the double coset KMK is a finite union of left cosets modulo K*

Similar lemmas are also true for right cosets.

§1.3. Modular forms

We shall consider complex-valued functions F on the upper half-plane $\mathbb{H}_n$. Such a function is called *K-automorphic of weight k*, where K is a subgroup of G^n and

$k \in \mathbb{Z}$, if it is invariant under each of the Petersson operators $|_k\gamma$ of weight k with $\gamma \in K$. We shall denote by $\mathcal{A}_k(K)$ the $\mathbb{C}$–linear space of all such functions:

$$\mathcal{A}_k(K) = \{F : \mathbb{H}_n \to \mathbb{C};\ F|_k\gamma = F, \text{ for all } \gamma \in K\}. \tag{1-4}$$

If $M \in G^n$, it follows from (1-4) that the condition $F|_k\gamma = F$ is equivalent with the condition $(F|_kM)|_kM^{-1}\gamma M = F|_kM$. Therefore we have

$$\mathcal{A}_k(M^{-1}KM) = \mathcal{A}_k(K)|_kM, \qquad (M \in G^n).$$

If a subgroup $K \subset G^n$ is commensurable with the modular group $\Gamma = \Gamma^n$, then it contains subgroups of finite index in Γ, and so there are numbers $r \in \mathbb{N}$, called *exponents of* K, such that each of the matrices of the form

$$T(rB) = \begin{pmatrix} E_n & rB \\ 0 & E_n \end{pmatrix}, \qquad \text{with } B \in \mathbb{S}_n,$$

belongs to K. If $F \in \mathcal{A}_k(K)$, where K is a group of exponent r, then, in particular,

$$F|_kT(rB) = F(Z + rB) = F(Z)$$

for every integral symmetric B of order n, and so the function $F = F((z_{ij}))$ is periodic of period r in each of the complex variables $z_{ij} = z_{ji}$.

Lemma 1.5. *Let $F = F((z_{ij}))$ be a function on $\mathbb{H}_n$ which is periodic of period r in each of the variables z_{ij}. Suppose that F is holomorphic on $\mathbb{H}_n$. Then F has an expansion of the form*

$$F = \sum_{A \in r^{-1}\mathbb{E}_n} f(A)e(AZ), \qquad (Z \in \mathbb{H}_n) \tag{1-5}$$

with constant coefficients $f(A)$, where, for a complex square matrix S,

$$e(S) = \exp\bigl(\pi i \cdot \mathrm{Trace}\ S\bigr). \tag{1-6}$$

The series (1-5) *converges absolutely on $\mathbb{H}_n$ and uniformly on each of the subsets*

$$\mathbb{H}_n(\varepsilon) = \{Z = X + iY \in \mathbb{H}_n;\ Y \geq \varepsilon E_n\}$$

with $\varepsilon > 0$.

The series (1-5) and its coefficients $f(A)$ will be called *the Fourier expansion* and *the Fourier coefficients* of F, respectively.

A function $F : \mathbb{H}_n \to \mathbb{C}$ is called *a modular form* (resp.,*a cusp form*) for a subgroup K of G^n commensurable with Γ^n, if it satisfies the following three conditions:

(1) $F \in \mathcal{A}_k(K)$,*i.e.* $F|_k\gamma = F$ for all $\gamma \in K$;

(2) F is holomorphic on $\mathbb{H}_n$;

(3) for each matrix $M \in \Sigma^n$, the coefficients of the Fourier expansion

$$F|_k M = \sum_{A \in r^{-1}\mathbb{E}_n} f_M(A) e(AZ)$$

of the function $F|_k M \in \mathcal{A}_k(M^{-1}KM)$, where r is an exponent of $M^{-1}KM$, satisfy

$$f_M(A) = 0, \qquad \text{unless } A \geq 0 \quad (\text{resp., unless } A > 0).$$

If $n \geq 2$, the condition (3) of the definition of modular forms is a consequence of conditions (1) and (2) (*the Koecher effect*).We let denote by $\mathfrak{M}_k(K)$ and $\mathfrak{N}_k(K)$ the space of all modular forms and all cusp forms of weight k for the group K , respectively. Each of the spaces of modular forms for a group K commensurable with Γ is finite dimensional over $\mathbb{C}$.

§1.4. Petersson scalar product

Every space of cusp forms can be equipped with the structure of a Hilbert space by means of Petersson scalar product, whose definition and properties we shall now recall. By the definition of K–automorphic functions for subgroups K of G^n, the values of such functions on $\mathbb{H}_n$ are determined by their values on a set of representatives of orbits of K on $\mathbb{H}_n$. We shall say that a subset $D = D(K)$ of $\mathbb{H}_n$ is *a fundamental domain of* K *on* $\mathbb{H}_n$, if it is closed in $\mathbb{H}_n$, contains a representative of each K–orbit on $\mathbb{H}_n$, and has no inner points belonging to the same K–orbit. In particular, the upper half-plane is the union of images of the fundamental domain under different transformations by elements of K:

$$\mathbb{H}_n = \bigcup_{\gamma' \in K'} \gamma' \langle D(K) \rangle,$$

where K' is the group of transformations of $\mathbb{H}_n$ corresponding to K, and the images $\gamma'\langle D(K)\rangle$ have pairwise no common inner points.Fundamental domains not necessarily exist, but if a fundamental domain $D(K)$ exists for a group K, it also exists for every group of the form $M^{-1}KM$ with $M \in G^n$ and for every subgroup K_1 of finite index in K, and one can take

$$D(M^{-1}KM) = M^{-1}\langle D(K) \rangle, \tag{1-7}$$

and

$$D(K_1) = \bigcup_{\gamma' \in K_1' \backslash K'} \gamma' \langle D(K) \rangle, \tag{1-8}$$

where K' and K_1' are the corresponding groups of transformations of the upper half-plain.

We turn now to invariant integration on fundamental domains. Recall first that the measure on $\mathbb{H}_n$ given by

$$d^* Z = (det Y)^{-(n+1)} \prod_{1 \leq \alpha \leq \beta \leq n} d x_{\alpha\beta} d y_{\alpha\beta},$$

where $Z = X + iY = (x_{\alpha\beta}) + i(y_{\alpha\beta}) \in \mathbb{H}_n$, and $d x_{\alpha\beta}, d y_{\alpha\beta}$ are the Euclidean measure on $\mathbb{R}$, is G^n–invariant, i.e. it satisfies

$$d^* M\langle Z \rangle = d^* Z \qquad \text{for every } M \in G^n, \tag{1-9}$$

as it follows by a routine check from the formula:

$$Y' = \mu(M)\, {}^t(C\overline{Z} + D)^{-1} Y (CZ + D)^{-1}, \tag{1-10}$$

where $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G^n$, $Z = X + iY \in \mathbb{H}_n$, $M\langle Z \rangle = X' + iY'$, and where the bar means the complex conjugation. It follows from (1-9) and (1-10) that every differential form on $\mathbb{H}_n$ given by

$$\omega_k(F, F')(Z) = F(Z)\overline{F'(Z)}(det\, Y)^k\, d^* Z, \tag{1-11}$$

for arbitrary functions F and F' on $\mathbb{H}_n$, and any integer k, satisfies

$$\omega_k(F, F')(M\langle Z \rangle) = \mu(M)^{nk} \omega_k(F|_k M, F'|_k M)(Z),$$

for each matrix M of G^n, where $|_k$ is the Petersson operator (1-1).

The invariance of the measure $d^* Z$ implies that the volume

$$v(D(K)) = \int_{D(K)} d^* Z \tag{1-12}$$

of a fundamental domain for a subgroup K of G^n does not depend on the choice of fundamental domain and can be refereed as *the volume* $v(K)$ *of* K. More generally, if K is a subgroup of G^n with a fundamental domain $D(K)$, and F, F' are two K–automorphic forms of an integral weight k , such that the integral

$$\int\limits_{D(K)} \omega_k(F, F')(Z)$$

converges absolutely, then it does not depend of the choice of fundamental domain.

Turning to subgroups of G^n commensurable with the modular group, we shall remind first the following lemma, which essentially rests on Minkowski reduction theory of quadratic forms.

Theorem 1.6. *The modular group $\Gamma = \Gamma^n$ has a fundamental domain $D_n = D(\Gamma^n)$ on $\mathbb{H}_n$. The invariant volume $v(\Gamma^n) = v(D_n)$ is finite.*

The lemma and decompositions (1-8) imply that the volume of every subgroup of G^n commensurable with Γ^n is finite.

Theorem 1.7. *Let K be a subgroup of $G = G^n$ commensurable with the modular group $\Gamma = \Gamma^n$, k an integer, and F , F' two modular forms of weigh k for K. Suppose that at least one of the forms is a cusp form. Then the integral*

$$(F, F') = \nu(K_1')^{-1} \int\limits_{D(K_1)} \omega_k(F, F')(Z), \tag{1-13}$$

where K_1 is a subgroup of finite index of $K \cap \Gamma$, $K_1' = K_1 \cup (-E_n)K_1/(\pm E_n)$ is the transformation group corresponding to K_1, $\nu(K_1') = [\Gamma' : K_1']$ is its index in $\Gamma' = \Gamma/(\pm E_n)$, $D(K_1)$ is a fundamental domain of K_1 on $\mathbb{H}_n$, and ω_k is the differential form (1-11)*, satisfies the following rules:*

(1) *(F, F') converges absolutely and is independent of the choice of fundamental domain;*

(2) *(F, F') is independent neither of the choice of the group K in the commensurability class of Γ with $F, F' \in \mathfrak{M}_k(K)$, nor of the choice of K_1;* (3) *(F, F') is linear in F and conjugate linear in F';*

(4) *$\overline{(F, F')} = (F', F)$;*

(5) *$(F, F) \geq 0$, and $(F, F) = 0$ only if $F = 0$;*

(6) *If M is a matrix of G with rational entries, then*

$$(F|_k M, F'|_k M) = \mu(M)^{-nk}(F, F'), \tag{1-14}$$

where $|_k$ is the Petersson operator (1-1) *, and the functions $F|_k M$, $F'|_k M$ are considered as elements of $\mathfrak{M}_k(M^{-1}KM)$.*

The number (F, F') is called *the (Petersson) scalar product of the forms* F, F'. The product was originally introduced by Petersson in [Pet(39)] for modular forms in one variable and then extended on Siegel modular forms by Maass in [Ma(51)].

The space $\mathfrak{N}_k(K)$ of cusp forms of weight k for a subgroup K of G commensurable with Γ is a finite-dimensional Hilbert space with respect to the Petersson scalar product.

§1.5. Hecke–Shimura rings and Hecke operators

Suppose that G is a multiplicative group, K is a subgroup,and Δ is a subsemigroup of G, containing K. We shall say that the pair (K, Δ) is *finite* (more precisely, *left–finite*), if for every $g \in \Delta$ the double coset KgK consists of a finite number of left cosets Kg'. For such a pair (K, Δ), and a commutative and associative ring $\mathbb{A}$ with the identity we let denote by

$$\mathcal{W} = Lin_{\mathbb{A}}(K\backslash\Delta)$$

the free $\mathbb{A}$–module consisting of all formal finite linear combinations

$$t = \sum_i a_i(Kg_i)$$

with coefficients $a_i \in \mathbb{A}$ of symbols (Kg_i) with $g_i \in \Delta$, which are in one-to-one correspondence with the left cosets Kg of the set Δ modulo the group K. For brevity, we shall refer to these symbols as *left cosets of* Δ *modulo* K.

Next, let us denote by

$$\mathcal{H} = HS_{\mathbb{A}}(K, \Delta)$$

the submodule of $\mathcal{W}$ consisting of all elements which are invariant relative to the natural (right) action of the group K on $\mathcal{W}$:

$$K \ni \gamma : \quad t \to t\gamma = \sum_i a_i(Kg_i\gamma),$$

i.e.,

$$\mathcal{H} = \{t \in \mathcal{W}; \quad t\gamma = t \text{ for all } \gamma \in K\}$$

The multiplication of elements of $\mathcal{H}$ given by the formula

$$(\sum_i a_i(Kg_i)) \cdot (\sum_j b_j(Kh_j)) = \sum_{i,j} a_i b_j(Kg_ih_j)$$

does not depend on the choice of representatives $g_i \in Kg_i$ and $h_j \in Kh_j$, and it turns $\mathcal{H}$ into an associative $\mathbb{A}$–algebra with the identity element $(K) = (K \cdot 1_G)$, called *the Hecke–Shimura ring (HS–ring) of the pair* (K, Δ) *over* $\mathbb{A}$. The elements

$$(g) = (g)_K = \sum_{g_i \in K \backslash KgK} (Kg_i), \tag{1-15}$$

which are in one-to-one correspondence with the two-sided cosets KgK of Δ with respect to K, belong to the ring $\mathcal{H}$ and form a free $\mathbb{A}$–basis of $\mathcal{H}$. For brevity, we shall call these elements *the double cosets of* Δ *modulo* K.

We suppose next that the semigroup Δ acts (from the right) on a (left) $\mathbb{A}$–module V by linear operators

$$|g : v \to v|g, \qquad (v \in V,\ g \in \Delta),$$

satisfying

$$v|g|g' = v|gg', \qquad (v \in V,\ g, g' \in \Delta),$$

and we let denote by

$$\mathfrak{M} = \{v \in V;\ v|\gamma = v \text{ for all } \gamma \in K\}$$

the submodule of K–invariant elements of V. Then for every $v \in \mathfrak{M}$ and every $t = \sum_i a_i(Kg_i)$ of $\mathcal{H} = HS_{\mathbb{A}}(K, \Delta)$ the element

$$v|t = \sum_i a_i v|g_i$$

does not depend on the choice of representatives $g_i \in Kg_i$, it again belong to the submodule $\mathfrak{M}$, and we have

$$v|t|t' = v|tt',$$

for every $v \in \mathfrak{M}$, $t, t' \in \mathcal{H}$. Thus, the correspondence $t \to |t$ is a linear representation of the HS–ring $\mathcal{H}$ on the module $\mathfrak{M}$.The operators $|t$ are called *Hecke operators.*

The Hecke operators were first studied by Hecke in [He(37)] for spaces of modular forms in one variable,although the idea of the operators was originally used by Mordell in [Mo(17)] in order to prove the conjectures of Ramanujan on multiplicative properties of the function $\tau(n)$ and similar functions. General Hecke–Shimura rings over $\mathbb{Z}$ were originally introduced by Shimura at the end of fifties in a formally different, but equivalent, form as an abstraction of rings of Hecke operators.

In the situation which interests us in this paper—the action of Hecke operators on modular forms—the role of G is played by the general real positive symplectic group of genus n, $G^n = GSp_n^+(\mathbb{R})$, introduced in §1.1.; the role of Δ is played by the semigroup Σ^n of integral matrices of G^n; and the role of K is played by a subgroup of G^n commensurable with the modular group Γ^n of genus n. Then, according to Lemma 1.4., the pair (K, Σ) is finite, and so we can define the corresponding HS–ring over arbitrary commutative ring $\mathbb{A}$. In this paper we take $\mathbb{A} = \mathbb{Q}$, the field of rational numbers, for all HS–rings of symplectic groups, and therefore the indication of the ground ring is, as a rule, omitted. In particular, the HS–ring of K,

$$\mathcal{H}(K) = HS(K, \Sigma) \tag{1-16}$$

is the HS–ring of the pair (K, Σ) over $\mathbb{Q}$. In order to define Hecke operators, we shall consider the action of Σ on complex-valued functions F on the upper half-plane $\mathbb{H} = \mathbb{H}^n$, given by the Petersson operators (1-1). Then, by the above, the subspace (1-4) of all K–invariant with weight k functions is invariant under all of the Hecke operators of weight k,

$$|_k T : \, F \to F|_k T = \sum_i a_i F|_k M_i, \qquad (T = \sum_i a_i (K M_i) \in \mathcal{H}(K), \, F \in \mathcal{A}_k(K)),$$

and the linear operators

$$|_k T : \, \mathcal{A}_k(K) \to \mathcal{A}_k(K) \qquad (T \in \mathcal{H}(K)) \tag{1-17}$$

satisfy

$$|_k T|_k T' = |_k T T'.$$

Proposition 1.8. *The subspaces $\mathfrak{M}_k(K)$ and $\mathfrak{N}_k(K)$ of modular forms and cusp forms of $\mathcal{A}_k(K)$ are invariant under all of the Hecke operators* (1-17)*.*

Generally speaking, the whole ring $\mathcal{H}(K)$ is noncommutative. However, it turns out that various questions of the theory of Hecke operators can often be reduced to consideration of suitable commutative subrings.Essential part in the reduction is played by *the star map*

$$T \to T^* \qquad (T \in \mathcal{H}(K)) \tag{1-18}$$

of the ring $\mathcal{H}(K)$, which is defined on the elements of the form (1-15) by

$$(M)^*_K = (M^*)_K, \qquad (M \in \Sigma)$$

where $M \to M^*$ is the antiautomorphism (1-3), and then extended on whole of $\mathcal{H}(K)$ by linearity.

Theorem 1.9. (1) *The star map is a linear antiautomorphism of degree two of the ring $\mathcal{H}(K)$; in particular, it satisfies the rules*

$$(T^*)^* = T,\ (T \cdot T_1)^* = T_1^* \cdot T^* \qquad (T, T_1 \in \mathcal{H}(K)).$$

(2) *The Hecke operators $|_k T$ and $|_k T^*$ are conjugate with respect to the Petterson scalar product* (1-13). *More precisely, if F and F' are two modular forms of weight k for K , and at least one of the forms is a cusp form, then*

$$(F|_k T, F') = (F, F'|_k T^*). \qquad (T \in \mathcal{H}(K))$$

Proof. (1).The linear map

$$\mathcal{H}(K) \to HS(K, \Sigma^{-1}) = \mathcal{H}'$$

given on double cosets by

$$(M)_K \to (M^{-1})_K \qquad (M \in \Sigma)$$

is an antiisomorphism of $\mathbb{Q}$–algebras (see, for example, [An(87), Proposition 3.1.7]). On the other hand , the linear map given on double cosets by

$$(M^{-1})_K \to (\mu(M) M^{-1})_K \qquad (M \in \Sigma)$$

is clearly an isomorphism of $\mathcal{H}'$ onto $\mathcal{H}(K)$.Then the assertion follows, since the star map is the composition of the two maps.

(2). It suffices to consider the case $T = (M)_K$ with $M \in \Sigma$. By Lemma 1.3, the number $\#(K \setminus KMK)$ of the left cosets of KMK modulo K is equal to the index $\nu = [K : K \cap M^{-1}KM]$. The number of the right cosets of KMK modulo K is clearly equal to the number of the left cosets in $KM^{-1}K$ and so equals $\nu' = [K : K \cap MKM^{-1}]$. Let D be a fundamental domain for the group $K \cap M^{-1}KM$ on $\mathbb{H}_n$. Since

$$K \cap MKM^{-1} = M(K \cap M^{-1}KM)M^{-1},$$

it follows, by (1-7), that we can take the set $M\langle D\rangle$ as a fundamental domain for the group $K \cap MKM^{-1}$.Then, by (1-8), we get the following relation for the invariant volumes (1-12):

$$v(D) = \nu v(D(K)), \qquad v(M\langle D\rangle) = \nu' v(D(K)),$$

where $D(K)$ is a fundamental domain for K. By (1-9), we conclude that $v(D) = v(M\langle D\rangle)$, and so $\nu = \nu'$. It follows that the numbers of left and right cosets of KMK modulo K are equal:

$$\#(K \setminus KMK) = \#(KMK/K) \qquad (M \in \Sigma). \tag{1-19}$$

Since each of the left cosets clearly meets each of the right cosets,it follows, by (1-19), that there is a set $M_1, \dots, M_\nu$ of common representatives for left and right cosets of KMK modulo K. Then the set $M_1^*, \dots, M_\nu^*$ is a set of common representatives for left and right cosets of KM^*K modulo K. Finally, by (1-14) and (1-2), we get

$$\begin{aligned}(F|_k(M), F') &= (\sum_i F|_k M_i, F') = \mu(M)^{-nk}(F, \sum_i F'|_k M_i^{-1}) \\ &= (F, \sum_i F'|_k M_i^*) = (F, F'|_k(M)^*).\end{aligned}$$

□

In this paper we practically do not touch, except for §2.4, the important question on action of Hecke operators on Fourier coefficients of modular forms, leaving it to our forthcoming papers on zeta functions. It turns out to be convenient for the applications to normalize the Hecke operators on modular forms for groups K commensurable with Γ^n by certain constant factors. For $T = \sum_i a_i(KM_i) \in \mathcal{H}(K)$ we define *the normalized Hecke operator* $\|_k\ T$ *on* $\mathfrak{M}_k(K)$ by

$$F \|_k\ T = \sum_i a_i \mu(M_i)^{nk-\langle n\rangle} F|_k M_i, \qquad (F \in \mathfrak{M}_k(K)) \tag{1-20}$$

Since, clearly,

$$F \|_k\ (M)_K = \mu(M)^{nk-\langle n\rangle} F|_k(M)_K, \qquad (F \in \mathfrak{M}_k(K),\ M \in \Sigma^n),$$

it follows that the normalized operators map the spaces $\mathfrak{M}_k(K)$ and $\mathfrak{N}_k(K)$ into themselves, the map $T \to \|_k\ T$ is a linear representation of the ring $\mathcal{H}(K)$, and it satisfies

$$(F \|_k\ T, F') = (F, F' \|_k\ T^*), \tag{1-21}$$

if $T \in \mathcal{H}(K)$, and $F, F' \in \mathfrak{N}_k(K)$.We note that Hecke operators considered in the books [An(87)] and [An-Zhu(90),(95)] are the normalized operators.

§1.6. Reducible, regular, and singular subrings

We close this chapter with several simple but useful definitions concerning Hecke–Shimura rings of discrete symplectic groups K commensurable with the modular group Γ^n.

Standard applications of Hecke operators are usually based on relations between eigenvalues of the operators on spaces of modular forms and Fourier coefficients of eigenfunctions. To do this one have first to compute Fourier coefficients of images under Hecke operators in terms of Fourier coefficient of originals. Since a Hecke operator $|_k T$ with $T \in \mathcal{H}(K)$ is a linear combination of the Petersson operators $|_k M$ with $M \in \Sigma$, the problem reduces to that for the Petersson operators. If $F \in \mathfrak{M}_k(K)$, then the only known general situation when the Fourier coefficients of $F|_k M$ can be directly calculated in terms of Fourier coefficients of F is the case when the operator $|_k M$ can be reduced to a "*triangular operator*" $|_k M'$ with a matrix M' belonging to the semigroup

$$\Sigma_0 = \Sigma_0^n = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Sigma \right\} \tag{1-22}$$

of "*triangular*" matrices of Σ. It happens if, say, $M \in K\Sigma_0$, since then

$$F|_k M = F|_k \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (det D)^{-k} F(AZD^{-1} + BD^{-1}),$$

and the Fourier coefficients of the last function can be easily expressed through those of F. These arguments justify the following definition. A nonzero element

$$T = \sum_i a_i(KM_i) \in \mathcal{H}(K), \tag{1-23}$$

where all of the coefficients are nonzero and all of the left cosets are pairwise distinct (*the shortest form*) is said to be *reducible*, if each of the left cosets KM_i contains a "triangular" representative, i. e.

$$KM_i \bigcap \Sigma_0 \neq \emptyset.$$

If T is reducible, one can assume that all of M_i belong to Σ_0, in which case we shall say that T is written in *the triangular form*, or is *triangular*. Since the product of two triangular elements is clearly triangular, it follows that the set

$$R(\mathcal{D}) = \{T \in \mathcal{D}; \quad T \text{ is reducible } \}$$

of all reducible elements contained in a subring $\mathcal{D}$ of $\mathcal{H}(K)$ is a subring, which will be called *the reducible subring* of $\mathcal{D}$.

It follows from definitions that an element $(M)_K$ of $\mathcal{H}(K)$ of the form (1-15) is reducible if and only if $KMK \subset K\Sigma_0$. In this case we shall say that the element M of Σ is *K-reducible.* The set

$$R(K) = \{M \in \Sigma; \quad KMK \subset K\Sigma_0\}$$

of all K–reducible elements of Σ is clearly a subsemigroup of Σ, *the K-reducible semigroup.* If

$$\mathcal{D} = HS(K, \Sigma') \subset \mathcal{H}(K)$$

is the HS–ring of a subsemigroup Σ' of Σ, then the reducible subring $R(\mathcal{D})$ of $\mathcal{D}$ is nothing else but the HS–ring of the pair $(K, \Sigma' \cap R(K))$.

In applications one can usually limit oneself to consideration of appropriate reducible subrings or their simple extensions. We shall see in the following chapter how it looks like in the case of the groups $K = \Gamma_0^n(q)$.

Properties of left and double cosets of matrices M of $\Sigma = \Sigma^n$ for a congruence subgroup of a level $q > 1$ depend very much on common divisors of their multiplier $\mu(M)$ and the level. The two extreme cases, *the regular case*, when

$$\gcd(\mu(M), q) = 1, \tag{1-24}$$

and *the singular case*, when

$$\mu(M)|q^\infty, \tag{1-25}$$

that is each of prime factors of $\mu(M)$ divides q, are of especial importance, since the general case is usually reducible to the particular cases. The reduction is based on the following consequence of the theory of elementary divisors for symplectic groups.

Lemma 1.10. *Let $M \in \Sigma = \Sigma^n$. Suppose that the multiplier $\mu(M)$ is a product of two coprime factors: $\mu(M) = ab$, $\gcd(a, b) = 1$. Then there are matrices M_1, $M_2 \in \Sigma$ such that $M = M_1M_2$, and $\mu(M_1) = a$, $\mu(M_2) = b$. If $M = M_1'M_2'$ is another such factorization, then $M_1' = M_1\gamma$, $M_2' = \gamma^{-1}M_2$ with $\gamma \in \Gamma^n$.*

We shall say that a matrix M of $\Sigma = \Sigma^n$ is *q-regular* (resp., *q-singular*), if it satisfies (1-24) (resp., (1-25)) and denote by

$$\Sigma_{(q)} = \Sigma^n_{(q)} \text{ and } \Sigma_q = \Sigma^n_q \tag{1-26}$$

the sets of all q-regular and q-singular matrices of Σ, respectively. An element of a HS–ring $\mathcal{H}(K)$ is called *q-regular* (resp., *q-singular*) if each of the the cosets entering in the shortest form (1-23) consists of q–regular (resp., q–singular) matrices.The subrings

$$\mathcal{H}_{(q)}(K) = HS(K, \Sigma_{(q)}) \text{ and } \mathcal{H}_q(K) = HS(K, \Sigma_q) \tag{1-27}$$

of all q–regular and q–singular elements of $\mathcal{H}(K)$ are called *the q-regular* and *the q-singular HS–ring of the group K*, respectively. A subring $\mathcal{D}$ of $\mathcal{H}(K)$ is said to be *q-regular* (resp., *q-singular*), if it is contained in $\mathcal{H}_{(q)}(K)$ (resp., $\mathcal{H}_q(K)$). If q is fixed, the indication of q , will be, as a rule, omitted.

Chapter 2

Regular reducible rings and operators for $\Gamma_0^n(q)$

In this chapter we shall remind the regular theory for the groups

$$K = \Gamma_0^n(q) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma^n;\, C \equiv 0 \pmod q \right\} \tag{2-1}$$

with $n, q \in \mathbb{N}$. The numbers n and q are fixed through out the chapter and often are not indicated. For details and omitted proofs see [An(87)] or [An-Z(90)]. The reader may also find there the regular theory for more general congruence subgroups.

§2.1. Global rings

Lemma 2.1. *The set $R^*(K)$ of all q-regular and K-reducible elements of Σ^n for the group* (2-1) *has the form*

$$R^*(K) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Sigma^n_{(q)};\, C \equiv 0 \pmod q \right\}; \tag{2-2}$$

in particular, $R^*(\Gamma^n) = \Sigma^n$.

Proof. For the inclusion $\supset$, see, for example, [An(87), *Lemma 3.3.4*]. The inverse inclusion follows from the definition of K-reducible elements.

□

It follows from the lemma that the (maximal) regular reducible subring of the ring $\mathcal{H}(K)$ is the ring

$$\mathcal{H}_{rr} = \mathcal{H}^n_{rr}(q) = HS(K,\, R^*(K)). \tag{2-3}$$

According to general properties of HS–rings, the elements $(M)_K$ of the form (1-15) associated to different double cosets of $R^*(K)$ modulo K form a free basis of the ring $\mathcal{H}_{rr}$ over $\mathbb{Q}$. In order to describe the basis we shall recall the following lemma on elementary divisors for the symplectic group over $\mathbb{Z}$.

Lemma 2.2. *Each of the double cosets KMK with $M \in R^*(K)$ for the group* (2-1) *contains the unique representative of the form*

$$sd(M) = diag(d_1, \ldots, d_n; e_1, \ldots, e_n), \tag{2-4}$$

where d_i, $e_j \in \mathbb{N}$ with $d_i | d_{i+1}, d_n | e_n, e_{i+1} | e_i, d_i e_i = \mu(M)$. If M, $M' \in R^*(K)$, and the multipliers $\mu(M)$ and $\mu(M')$ are coprime, then

$$sd(MM') = sd(M)sd(M'). \tag{2-5}$$

The diagonal matrix $sd(M)$ is called *the matrix of symplectic divisors of* M, and the positive integers $d_1 = d_1(M), \ldots, d_n = d_n(M)$, $e_1 = e_1(M), \ldots, e_n = e_n(M)$ are *the symplectic divisors of* M.

Theorem 2.3. *The star map* (1-18) *is identical on the double cosets* $(M)_K$ *contained in the regular reducible ring* $\mathcal{H}_{rr}$ *of the group* (2-1)*:*

$$(M)^*_K = (\mu(M)M^{-1})_K = (M)_K, \qquad (M \in R^*(K)); \tag{2-6}$$

in partiqular, the ring $\mathcal{H}_{rr}$ *is commutative.*

A problem of explicit multiplication rules for specific elements of $\mathcal{H}_{rr}$ can be quite complicated, except for certain special cases, which, in partiqular, allow one to bring about an impotant reduction of the problem.

Note, first of all, that, for every $M \in \Sigma$ and $r \in \mathbb{N}$, one has the rules

$$[r](M)_K = (M)_K[r] = (rM)_K, \tag{2-7}$$

where

$$[r] = [r]_K = (rE_{2n})_K = (K(rE_{2n})); \tag{2-8}$$

in particular, the element [1] is the unity element of $\mathcal{H}(K)$. Next we have the following

Proposition 2.4. *Let us suppose that the quotients of the divisors* $e_1(M)/d_1(M)$ *and* $e_1(M')/d_1(M')$ *of two matrises* M, $M' \in R^*(K)$ *are coprime. Then the following relation holds:*

$$(M)_K(M')_K = (MM')_K. \tag{2-9}$$

If a diagonal matrix $diag(d_1, \dots, d_n; e_1, \dots, e_n)$ is the matrix of symplectic divisors of a matrix $M \in R^*(K)$, we shall write

$$T(d_1, \dots, d_n; e_1, \dots, e_n) = (sd(M))_K = (M)_K, \tag{2-10}$$

and for a number $a \in \mathbb{N}$ prime to q we denote by $T(a) = T_K(a)$ the sum of all different double cosets $(M)_K$ with $M \in R^*(K)$ and $\mu(M) = a$:

$$T(a) = \sum_{KMK \subset R^*(K), \mu(M)=a} (M)_K. \tag{2-11}$$

Then, by (2-5), (2-7), and (2-9), we get the relations

$$T(d_1, \dots, e_n)T(d'_1, \dots, e'_n) = T(d_1d'_1, \dots, e_ne'_n), \tag{2-12}$$

provided that the numbers e_1/d_1 and e'_1/d'_1 are coprime, and the relations

$$T(a)T(b) = T(ab), \quad \text{if } a,\ b \text{ are coprime and prime to } q. \tag{2-13}$$

For a prime number p not dividing q ,we define *the matrix of symplectic p-divisors of M* by

$$sd_p(M) = diag(p^{\nu_p(d_1)}, \dots, p^{\nu_p(e_n)}), \tag{2-14}$$

where $\nu_p(r)$ is the p-order of r. The matrix (2-14) is clearly the matrix of symplectic divisors of a matrix $M_p \in R^*(K)$ (for example, $M_p = sd_p(M)$):

$$sd_p(M) = sd(M_p), \qquad (M, M_p \in R^*(K), \gcd(p,\, q) = 1). \tag{2-15}$$

The relations (2-9) imply the factorization

$$(M)_K = \prod_p (M_p)_K, \tag{2-16}$$

where p runs over all prime divisors of $\mu(M)$.

The p-components $(M_p)_K$ of double cosets $(M)_K \in \mathcal{H}_{rr}$ span clearly a subring $\mathcal{H}_p$, *the (reducible) p-ring*, which can be interpreted by itself as the HS–ring of the pair

$$\big(K,\, R_p(K) = \{M \in R(K);\, \mu | p^\infty\}\big) :$$

$$\mathcal{H}_p = \mathcal{H}_p^n(q) = HS(K,\, R_p(K)). \tag{2-17}$$

The factorization (2-16) imply the following

Theorem 2.5. *The ring $\mathcal{H}_{rr}$ is generated by the p-rings $\mathcal{H}_p$ for all primes p not dividing q.*

The factorization of elements of $\mathcal{H}_{rr}$ into p-factors can be naturally reformulated in terms of Euler decomposition of formal symplectic zeta functions. For example, it follows from (2-13) that

$$T(\prod_i p_i^{\nu_i}) = \prod_i T(p_i^{\nu_i}),$$

if p_i runs over a finite set of different prime numbers not dividing q, which implies the following (formal) Euler decomposition of the formal Dirichlet series over $\mathcal{H}_{rr}$ with the coefficients $T(a)$ for a prime to q:

$$\sum_{a \in \mathbb{N},\, \gcd(a,q)=1} \frac{T(a)}{a^s} = \prod_{\substack{p \text{ prime}, \\ p \nmid q}} \Big(\sum_{\delta=0}^{\infty} T(p^\delta) \cdot p^{-\delta s} \Big). \tag{2-18}$$

We shall see in the next section that each of the formal power series

$$Z_p(v) = Z_p^n(v) = \sum_{\delta=0}^{\infty} T(p^\delta)v^\delta \tag{2-19}$$

is formally a rational fraction over the ring $\mathcal{H}_p$.

§2.2. Local rings

Theorem 2.6. *Let p be a prime number not dividing q. Then the following assertions holds:*

(1) *If $T = \sum_i a_i(KM_i)$ is an element of $\mathcal{H}_p^n(q)$ with triangular representatives M_i , then the map $T \to i(T) = \sum_i a_i(\Gamma^n M_i)$ is an isomorphism of $\mathcal{H}_p^n(q)$ onto $\mathcal{H}_p^n(1)$;*

(2) *The ring $\mathcal{H}_p^n(q)$ is generated over $\mathbb{Q}$ by the $n+1$ elements*

$$\begin{cases} T^n(p) = T(\underbrace{1,\ldots,1}_{n};\underbrace{p,\ldots,p}_{n}), \\ T_i^n(p^2) = T(\underbrace{1,\ldots,1}_{n-i},\underbrace{p,\ldots,p}_{i};\underbrace{p^2,\ldots,p^2}_{n-i},\underbrace{p,\ldots,p}_{i}), \qquad (i=1,\ldots,n); \end{cases} \tag{2-20}$$

(3) *The elements* (2-20) *are algebraically independent over $\mathbb{Q}$.*

The problem to express elements of the ring $\mathcal{H}_p = \mathcal{H}_p^n(q)$ in terms of generators (2-20) is not easy one. But it can be considerably simplified, if one uses another realization of the rings given by spherical polynomials.

Since the ring $\mathcal{H}_p$ is reducible, each of the left cosets KM with $K = \Gamma_0^n(q)$ and $M \in R_p(K)$ contains a triangular representative

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \qquad \text{with } {}^tAD = p^\delta E_n, \qquad (p^\delta = \mu(M)). \tag{2-21}$$

Since the group K contains the subgroup

$$V^n = \left\{ v(U) = \begin{pmatrix} {}^tU^{-1} & 0 \\ 0 & U \end{pmatrix}; \quad U \in GL_n(\mathbb{Z}) \right\}, \tag{2-22}$$

one can replace the matrix D in (2-21) by any of the matrices UD with $U \in GL_n(\mathbb{Z})$ and so assume that D is an upper triangular matrix of the form

$$D = (d_{ij}), \text{ where } d_{ij} = 0 \text{ , if } i > j, \text{ and } d_{ii} = p^{d_i}, \qquad (i,j = 1,\ldots,n). \tag{2-23}$$

We set then

$$\omega(KM) = x_0^{\delta} \prod_{i=1}^{n} (x_i p^{-i})^{d_i},$$

where $x_0, x_1, \ldots, x_n$ are algebraically independent over $\mathbb{Q}$. By extending the map ω by linearity on the whole ring $\mathcal{H}_p$, we obtain a linear map

$$\omega = \omega_p : \quad \mathcal{H}_p \to \mathbb{Q}[x_0, \ldots, x_n] \tag{2-24}$$

of the ring $\mathcal{H}_p$ into the ring of polynomials in $n+1$ independent variables over $\mathbb{Q}$, *the spherical map*. The polynomials $\omega(T)$ with $T \in \mathcal{H}_p$ are called *the spherical polynomials*.

Theorem 2.7. *The spherical mapping ω_p is an isomorphism of the ring $\mathcal{H}_p = \mathcal{H}_p^n(q)$ with the subring $\mathbb{Q}^W[x_0, \ldots, x_n]$ of $\mathbb{Q}[x_0, \ldots, x_n]$ consisting of all polynomials invariant with respect to the group $W = W_n$ of $\mathbb{Q}$–automorphisms of the rational function field $\mathbb{Q}(x_0, \ldots, x_n)$ generated by all permutations in the variables $x_1, \ldots, x_n$ and by the automorphisms $\tau_1, \ldots, \tau_n$ satisfying*

$$\tau_i(x_0) = x_0 x_i, \quad \tau_i(x_i) = x_i^{-1}, \quad \tau_i(x_j) = x_j \quad (j \neq 0,\, i).$$

The ring $\mathbb{Q}^W[x_0, \ldots, x_n]$ is generated over $\mathbb{Q}$ by $n+1$ polynomials

$$t = t^n(x_0, \ldots, x_n) = x_0 \prod_{i=1}^{n} (1 + x_i),$$

$$\rho_a = \rho_a^n(x_0, \ldots, x_n) = {x_0}^2 x_1 \ldots x_n r_a^n(x_1, \ldots, x_n) \qquad (a = 0, 1, \ldots, n-1),$$

where

$$\sum_{a=0}^{2n} (-1)^a r_a^n(x_1, \ldots, x_n) v^a = \prod_{i=1}^{n} (1 - x_i v)(1 - x_i^{-1} v).$$

With the help of spherical map one can prove the following formulae for the formal power series (2-19):

$$Z_p^1(v) = Q_p^1(v)^{-1}, \quad \text{where } Q_p^1(v) = [1] - T^1(p)v + p[p]v^2; \tag{2-25}$$

$$Z_p^2(v) = Q_p^2(v)^{-1}([1] - p^2[p]v^2),$$

where

$$Q_p^2(v) = [1] - T^2(p)v + q_2(p)v^2 - p^3[p]T^2(p)v^3 + p^6[p^2]v^4 \tag{2-26}$$

with $q_2(p) = pT(1,p,p^2,p) + p(p^2+1)[p]$; and for general n,

$$Z_p^n(v) = Q_p^n(v)^{-1}N_p^n(v),$$

where

$$Q_p^n(v) = \sum_{i=0}^{m}(-1)^i q_i^n(p)v^i \qquad (m = 2^n) \tag{2-27}$$

is the polynomial of degree $m = 2^n$ over $\mathcal{H}_p^n(q)$ satisfying

$$\begin{aligned}\omega(Q_p^n)(v) &= \sum_{i=0}^{m}(-1)^i \omega(q_i^n(p))v^i \\ &= (1 - x_0 v)\prod_{r=1}^{n}\prod_{1\le i_1<\cdots<i_r\le n}(1 - x_0 x_{i_1}\cdots x_{i_r}v),\end{aligned}$$

$\omega = \omega_p$ being the spherical mapping (2-24), and where $N_p^n(v)$ is a polynomial over $\mathcal{H}_p^n(q)$ of degree at most $2^n - 2$. The coefficients $q_i^n(p)$ satisfy the rules

$$q_{m-i}^n(p) = (p^{\langle n\rangle}[p])^{(m/2)-i}q_i^n(p), \qquad (0 \le i \le m = 2^n),$$

$$q_0^n(p) = [1], \quad \text{and } q_m^n(p) = (p^{\langle n\rangle}[p])^{m/2}.$$

The formula (2-25) goes back to Hecke and was formally proved along with the formula for $Z_p^2(v)$ in [Sh(63)] and [Sa(63)]. The general case was considered in [An(69)] and [An(70)].

§2.3. Parabolic embeddings

It is often useful to split elements of a symplectic HS–ring on certain elementary components. Howerever, in general, the components do not belong to the original ring. According to our approach, they live in HS–rings of the "triangular" subgroup

$$\Gamma_0 = \Gamma_0^n = \left\{\begin{pmatrix} A & B \\ 0 & D\end{pmatrix} \in \Gamma^n\right\}$$

of the modular group $\Gamma = \Gamma^n$.

It is easy to see that the pair $(\Gamma_0,\, \Sigma_0)$, where $\Sigma_0 = \Sigma_0^n$ is defined by (1-22), is finite, and therefore one can introduce the corresponding Hecke–Shimura ring over $\mathbb{Q}$,

$$\mathcal{L} = \mathcal{L}^n = HS(\Gamma_0^n,\, \Sigma_0^n), \tag{2-28}$$

along with its q-regular and q-singular subrings

$$\mathcal{L}_{(q)} = \mathcal{L}^n_{(q)} = HS(\Gamma^n_0,\, \Sigma^n_{0,(q)}), \qquad \mathcal{L}_q = \mathcal{L}^n_q = HS(\Gamma^n_0,\, \Sigma^n_{0,q}), \tag{2-29}$$

for $q \in \mathbb{N}$, where

$$\Sigma_{0,(q)} = \Sigma^n_{0,(q)} = \Sigma^n_0 \bigcap \Sigma^n_{(q)}, \qquad \Sigma_{0,q} = \Sigma^n_{0,q} = \Sigma^n_0 \bigcap \Sigma^n_q$$

(see (1-22) and (1-26)).

Let $\mathcal{D}$ be a reducible subring of the ring $\mathcal{H}(K)$ (see (1-16)) for $K = \Gamma^n_0(q)$, and let $T = \sum_i a_i(KM_i)$ be an element of $\mathcal{D}$ written in the triangular form. Since $K \cap \Sigma_0 = \Gamma_0$, the map

$$j\,:\, T \to j(T) = \widehat{T} = \sum_i a_i(\Gamma_0 M_i)$$

does not depend on the choice of triangular representatives $M_i \in KM_i$, the image $\widehat{T}$ belongs to $\mathcal{L}$, and $\widehat{T} = 0$, if and only if $T = 0$. It follows from the definition of multiplication in HS–rings, that the map $T \to \widehat{T}$ is a linear ring homomorphism. Thus, we get the homomorphic inclusion

$$j: \quad \mathcal{D} \hookrightarrow \widehat{\mathcal{D}} \subset \mathcal{L} \tag{2-31}$$

of the ring $\mathcal{D}$ into $\mathcal{L}$, which will be referred as *parabolic embedding.*

We now turn to multiplicative properties of the ring $\mathcal{L}$. Contrary to reduced rings we have considered earlier, the ring $\mathcal{L}$ is not commutative and contains zero divisors. Howerever, some important properties remain valid and, as a matter of fact, we shall need only certain subrings and submodules of $\mathcal{L}$ with good properties.

Note, first of all, that *the star map*

$$X \to X^* \qquad (X \in \mathcal{L}) \tag{2-32}$$

of the ring $\mathcal{L}$, which is defined on double cosets by

$$(M)^*_{\Gamma_0} = (\mu(M)M^{-1})_{\Gamma_0} \tag{2-33}$$

and then extended on whole of $\mathcal{L}$ by linearity, is again a linear antiautomorphism of the second order of the ring $\mathcal{L}$. The same is obviously true for the subrings $\mathcal{L}_{(q)}$ and $\mathcal{L}_q$. The images of double cosets $(M)_K \in \mathcal{H}^n_{rr}(q)$ under parabolic embedding (2-30) are invariant under the star map:

$$j((M)_K)^* = j((M)_K) \qquad (M \in R^*(K)). \tag{2-34}$$

Note that the image $j((M)_K)$ is not necessarily a double coset modulo Γ_0, but a sum of such cosets.

Next, by analogy with (2-7), we have the relations

$$\widehat{[r]}(M)_{\Gamma_0} = (M)_{\Gamma_0}\widehat{[r]} = (rM)_{\Gamma_0}, \qquad (r \in \mathbb{N},\ M \in \Sigma_0), \tag{2-35}$$

where

$$\widehat{[r]} = [r]_{\Gamma_0} = (\Gamma_0(rE_{2n})); \tag{2-36}$$

in particular, the element $\widehat{[1]}$ is the unity element of the ring $\mathcal{L}$.

It turns out that the ring $\mathcal{L}$ contains not only HS–rings of the symplectic group, but also subrings which are naturally isomorphic to certain subrings of HS–rings of the general linear group. This allows one to reduce certain questions of the theory of Hecke–Shimura rings and Hecke operators for symplectic group to similar questions for general linear group.

Let us consider the elements of $\mathcal{L} = \mathcal{L}^n$ defined by

$$\widehat{\Pi}(a) = \widehat{\Pi}^n(a) = \left(\begin{pmatrix} E_n & 0 \\ 0 & aE_n \end{pmatrix}\right)_{\Gamma_0} \tag{2-37}$$

with $a \in \mathbb{N}$. The elements have the following decomposition into left cosets modulo Γ_0^n:

$$\widehat{\Pi}(a) = \sum_{B \in \mathbb{S}/a\mathbb{S}} \left(\Gamma_0 \begin{pmatrix} E & B \\ 0 & aE \end{pmatrix}\right), \tag{2-38}$$

where $E = E_n$ and $\mathbb{S} = \mathbb{S}_n$ (see Notation).It follows that

$$\widehat{\Pi}(a)\widehat{\Pi}(b) = \widehat{\Pi}(ab) \qquad (a, b \in \mathbb{N}) \tag{2-39}$$

The elements $\widehat{\Pi}(a)$ will be called *the Frobenius elements of the ring* $\mathcal{L}$.

We now consider centralizers of Frobenius elements in the rings $\mathcal{L}$, $\mathcal{L}_{(q)}$, and $\mathcal{L}_q$:

$$\begin{aligned} \widehat{C}^n &= \left\{X \in \mathcal{L};\quad \widehat{\Pi}(a)X = X\widehat{\Pi}(a), \quad a \in \mathbb{N}\right\}, \\ \widehat{C}^n_{(q)} &= \left\{X \in \mathcal{L}_{(q)};\quad \widehat{\Pi}(a)X = X\widehat{\Pi}(a), \quad a \in \mathbb{N}, \quad \gcd(a,q) = 1\right\}, \\ \widehat{C}^n_q &= \left\{X \in \mathcal{L}_q;\quad \widehat{\Pi}(a)X = X\widehat{\Pi}(a), \quad a|q^\infty\right\}. \end{aligned} \tag{2-40}$$

The following theorem is proved in [An(87)] and [An-Z(90)] only for rings $\mathcal{L}_{(q)}$, but the same proof with obvious modifications goes through also for the rings $\mathcal{L}$ and $\mathcal{L}_q$.

Theorem 2.8. *The ring $\widehat{C}$ (resp.,$\widehat{C}_{(q)}$, $\widehat{C}_q$) is spanned over $\mathbb{Q}$ by all of the double cosets modulo Γ_0 of the matrices of Σ_0 (resp., $\Sigma_{0,(q)}, \Sigma_{0,q}$) of the form*

$$M = U(\mu, D) = \begin{pmatrix} \mu \cdot {}^t D^{-1} & 0 \\ 0 & D \end{pmatrix}, \tag{2-41}$$

satisfying the condition

$$\mu | d(D)^2, \tag{2-42}$$

where $d(D)$ is the greatest common divisor of entries of D. For every such M, the double coset $(M)_{\Gamma_0}$ has the following decomposition into left cosets:

$$(M)_{\Gamma_0} = \sum_{D', B} (\Gamma_0 U(\mu, D') \begin{pmatrix} E & B \\ 0 & E \end{pmatrix}), \tag{2-43}$$

where D' runs a set of representatives of the left cosets modulo the group

$$\Lambda = \Lambda^n = GL_n(\mathbb{Z}), \tag{2-44}$$

contained in the double coset $\Lambda D \Lambda$, and B runs over a set of representatives for the additive group $\mathbb{S} = \mathbb{S}_n$ modulo the subgroup $\mu^{-1} \cdot {}^t D' \mathbb{S} D'$.

Let now

$$X = \sum_i a_i \left(\Gamma_0 \begin{pmatrix} \mu_i \cdot {}^t D_i^{-1} & B_i \\ 0 & D_i \end{pmatrix} \right)$$

be an element of the ring $\mathcal{L}$. We set

$$\Omega(X) = \sum_i a_i \{\mu_i\} (\Lambda D_i), \tag{2-45}$$

where the coefficients $a_i\{\mu_i\}$ are considered as elements of the semigroup ring $\mathbb{Q}[\mathbb{N}]$ of the semigroup of positive integers over the field $\mathbb{Q}$. It is easy to see that in fact $\Omega(X)$ belongs to the HS–ring of the pair (Λ, Δ), where

$$\Delta = \Delta^n = \{ D \in \mathbb{Z}_n^n; \quad \det D \neq 0 \}, \tag{2-46}$$

over $\mathbb{Q}[\mathbb{N}]$, and the map

$$\Omega : \quad \mathcal{L} \to HS_{\mathbb{Q}[\mathbb{N}]}(\Lambda, \Delta) \tag{2-47}$$

is a $\mathbb{Q}$–linear ring homomorphism.

Proposition 2.9. *The restriction $\Omega\big|_{\widehat{C}}$ of the homomorphism Ω to the centralizer $\widehat{C}$ of Frobenius elements in $\mathcal{L}$ is a monomorphism; in partiqular, $\widehat{C}$ is a commutative integral domain.*

Note that HS–ring of the pair $(\Lambda^n,\, \Delta^n)$ over any commutative ring without zero divisors is commutative and contains no zero divisors.

Let us turn now to local triangular rings. For each prime number p, the local subring $\mathcal{L}_p = \mathcal{L}_p^n$ of the ring $\mathcal{L}$ consists of those linear combinations of left (or double) cosets of $\mathcal{L}$ whose multipliers are powers of p.

According to Proposition 2.9, the local centalizers

$$\widehat{C}_p = \big\{X \in \mathcal{L}_p; \quad \widehat{\Pi}(p)X = X\widehat{\Pi}(p)\big\} = \widehat{C} \cap \mathcal{L}_p \tag{2-48}$$

are commutative integral domains.

Theorem 2.10. *The ring $\widehat{C}$ (resp., $\widehat{C}_{(q)}$, $\widehat{C}_q$) is generated by the subrings $\widehat{C}_p$, where p runs over all prime numbers (resp.,all prime numbers not dividing q, all prime numbers dividing q).*

Although the ring $\mathcal{L}_p$ is noncommutative and contains zero divisors, it turns out that each element of $\mathcal{L}_p$ can be "projected" into commutative integral domain $\widehat{C}_p$ and, moreover, each element of $\widehat{\mathcal{H}}_p = \mathcal{H}_p(1)$ can be restored by its projections:

Proposition 2.11. *Let $X = \sum_i a_i(\Gamma_0 M_i)$ be an element of $\mathcal{L}_p$ with $\mu(M_i) = p^{\nu_i}$, and let d be an integer satisfying $d \geq \nu_i$ for all i. Then*

$$X\widehat{\Pi}(p)^d \in \widehat{C}_p. \tag{2-49}$$

If, moreover, $X \in \widehat{\mathcal{H}}_p$, then

$$\Pi_+^{-d} \cdot X\widehat{\Pi}(p)^d = X, \tag{2-50}$$

where $\Pi_+^{-d} = \widehat{\Pi}(p)^{(-d)}$ are independent of X elements of the extension $\widehat{C}'_p = \widehat{C}\big[[p]^{-1}\big]$ of the ring $\widehat{C}_p$.

The elements Π_+^{-d} are so-called "negative powers" of Frobenius elements. For their definition and properties see, for example, [An(87), §3.5.1].

It is clear from the definitions that the image $\widehat{\mathcal{H}}_p(q)$ of a p-ring of the group $\Gamma_0^n(q)$ is contained in $\mathcal{L}_p$. Moreover, it follows from the first part of Theorem 2.6, that the parabolic embedding of the ring $\mathcal{H}_p(q)$ into the ring $\mathcal{L}_p$ can be presented as a composition of the isomorphism of $\mathcal{H}_p^n(q)$ onto $\mathcal{H}_p(1)$ defined in the theorem and the parabolic embedding of the ring $\mathcal{H}_p(1)$, in particular the image

$$\widehat{\mathcal{H}}_p(q) = \widehat{\mathcal{H}}_p = \widehat{\mathcal{H}}_p(1) \tag{2-51}$$

is independent of the choice of q not divisible by p.

As to the relations between introduced local rings for different primes, we have the following

Proposition 2.12. *Let p and p' be two different prime numbers. Then each element of $\widehat{\mathcal{H}}_p$ commutes with each element of $\widehat{C}_{p'}$.*

We close this section with the following theorem which is crucial for our forthcoming constructions.

Theorem 2.13. *The Frobenius element $\widehat{\Pi}(p) = \widehat{\Pi}^n(p)$, where p is a prime number, satisfies the equation*

$$\sum_{j=0}^{m}(-1)^j\widehat{q_j^n}(p)\widehat{\Pi}(p)^{m-j} = 0, \qquad (m = 2^n), \tag{2-52}$$

where $\widehat{q_j^n}(p) \in \widehat{\mathcal{H}}_p$ are images under parabolic embedding of coefficients of the polynomial (2-27) *over the ring $\mathcal{H}_p(q)$ for a q not divisible by p.*

§2.4. Regular reducible Hecke operators and triangular operators

We consider first the representation of the regular reducible ring $\mathcal{H}_{rr}(q) = \mathcal{H}_{rr}^n(q)$ on the space $\mathfrak{N}_k(K)$ of cusp forms of weight k for the group $K = \Gamma_0^n(q)$ given by Hecke operators, as they were defined in §1.5.

According to Theorem 2.3 and Theorem 1.9(2), the Hecke operators on $\mathfrak{N}_k(K)$ corresponding to elements of $\mathcal{H}_{rr}(q)$ commute with each other and are selfadjoint with respect to the Petersson scalar product. Since the space of cusp forms is finite-dimensional, this implies the following theorem.

Theorem 2.14. *The space $\mathfrak{N}_k(K)$ has an orthogonal basis consisting of common eigenfunctions for all of the Hecke operators $|_kT$ and $\|_kT$ with $T \in \mathcal{H}_{rr}(q)$.*

Hecke operators for the group $\Gamma_0 = \Gamma_0^n$ not necessarily map the spaces $\mathfrak{M}_k(K)$ into themselves. Therefore, in order to apply the relations between elements of HS–rings of the groups K and Γ_0 cited in §2.3, one has first to extend the spaces.

Every function F of $\mathfrak{M}_k(K)$ satisfies, in particular, the relations

$$F|_kM = (\det D)^{-k}F(M\langle Z\rangle) = F \text{ for each } M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_0. \tag{2.53}$$

Besides, it can be decomposed into an absolutely convergent on $\mathbb{H}_n$ Fourier series of the form

$$F(Z) = \sum_{A\in\mathbb{E}_n\,,\,A\geq 0} f(A)e(AZ) \tag{2.54}$$

(see Notation and (1-6)) with constant Fourier coefficients $f(A)$. These remarks allows one to define the space $\mathcal{T}_k = \mathcal{T}_k^n$ of *modular forms of weight k for the group* Γ_0 as the space of all absolutely convergent on $\mathbb{H}_n$ Fourier series of the form (2-54), which satisfy the relations (2-53). Note that the space $\mathcal{T}_k$ depends only on parity of k. It is clear that

$$\mathfrak{M}_k(K) \subset \mathcal{T}_k. \tag{2-55}$$

The HS–ring $\mathcal{L}$ of the group Γ_0 defined by (2-28) naturally acts on $\mathcal{T}_k$,say, by normalized Hecke operators:

$$\mathcal{L} \ni T = \sum_i a_i(\Gamma_0 M_i) : F \to F\|_k T = \sum_i a_i \mu(M_i)^{nk-\langle n\rangle} F|_k M_i. \tag{2-56}$$

The mapping $T \to \|_k T$ is a linear representation of $\mathcal{L}$ on $\mathcal{T}_k$, which is compatible with the parabolic embedding

$$\mathcal{H}_{rr}(q) \to \widehat{\mathcal{H}}_{rr}(q) \subset \mathcal{L},$$

defined by (2-30), in the sense that

$$F\|_k T = F\|_k \widehat{T} \qquad (F \in \mathfrak{M}_k(K), \quad T \in \mathcal{H}_{rr}(q)). \tag{2-57}$$

The following lemma shows that the normalized Hecke operators corresponding to elements of the centralizer C of Frobenius elements $\Pi(a)$ (see (2-38) and (2-40)) have an especially simple action on Fourier coefficients of functions in $\mathcal{T}_k$.

Lemma 2.15. *Let F be a function of $\mathcal{T}_k$ with Fourier coefficients $f(A)$, and let $M = U(\mu, D)$ be a matrix of Σ_0 of the form* (2-41) *satisfying* (2-42). *Then the Fourier coefficients $(f\|_k(M)_{\Gamma_0})(A)$ of the function $F\|_k(M)_{\Gamma_0}$ can be given by the formula*

$$\begin{aligned}(f\|_k(M)_{\Gamma_0})(A) \\ = \mu^{nk-n(n+1)}|\det D|^{n+1} \sum_{D' \in \Lambda\backslash\Lambda D\Lambda} (\det D)^{-k} f(\mu^{-1} D' A \cdot {}^t D').\end{aligned} \tag{2-58}$$

In particular,

$$(f\|_k \widehat{\Pi}(a))(A) = f(aA) \qquad (a \in \mathbb{N},\ A \in \mathbb{E}_n). \tag{2-59}$$

As an illustration of the technique of parabolic embeddings we shall prove here a rationality theorem originally proved for the group Γ^n by Zharkovskaya in [Zha(75)].

Theorem 2.16. *Let*

$$F=\sum_{A\in\mathbb{E}_n\,,\,A\geq 0} f(A)e(AZ)\in\mathfrak{M}_k(K)$$

be an eigenfunction for all Hecke operators $\|_k T$ *with* $T\in\mathcal{H}_p^n(q)$, *where* p *is a prime number not dividing* q:

$$F\|_k T=\lambda(T)F \qquad (T\in\mathcal{H}_p^n(q)).$$

Then each of the formal power series

$$\sum_{\delta=0}^{\infty} f(p^\delta A)v^\delta \qquad \text{with } A\in\mathbb{E}_n$$

is formally a rational fraction with the denominator

$$(\lambda Q_p^n)(v)=\sum_{i=0}^{m}(-1)^i\lambda(q_i^n(p))v^i \qquad (m=2^n),$$

where $Q_p^n(v)$ *is the polynomial* (2-27), *and with a numerator of degree at most* 2^n-1.

*Proof.*We have

$$\begin{aligned}\left(\sum_{i=0}^{m}(-1)^i\lambda(q_i^n(p))v^i\right)\left(\sum_{\delta=0}^{\infty} f(p^\delta A)v^\delta\right)&=\sum_{i,\delta}(-1)^i(f\|_k q_i^n(p))(p^\delta A)v^{i+\delta}\\&=\sum_{i,\delta}(-1)^i(f\|_k\widehat{q_i^n}(p)\widehat{\Pi}(p)^\delta)(A)v^{i+\delta},\end{aligned}$$

where we have used (2-57) and (2-59). If $i+\delta=r\geq m$, then

$$\sum_{i+\delta=r}(-1)^i\widehat{q_i^n}(p)\widehat{\Pi}(p)^\delta=\sum_{i=0}^{m}\big((-1)^i\widehat{q_i^n}(p)\widehat{\Pi}(p)^{m-i}\big)\widehat{\Pi}(p)^{r-m}=0,$$

by (2-52).

□

Chapter 3

Singular Hecke–Shimura rings for $\Gamma_0^n(q)$

Our theory of singular HS–rings for the groups $\Gamma_0^n(q)$ rests on two fundamental facts: the first is that the centralizer of the Frobenius element $\Pi(p)$ in the reducible p-subring for $\Gamma_0^n(q)$, where p is a prime divisor of q, is naturally isomorphic to the centralizer of $\widehat{\Pi}(p)$ in the triangular ring $\mathcal{L}_p$, which follows from *Theorem 3.3* and *Theorem 2.8*; the second is that the elements $\Pi(p)$ with primes p dividing q but not dividing q/p are invertible, which is based on properties of neutral HS–rings considered in §3.2. These circumstances will allow us to construct in §3.3 natural embeddings of regular reducible p-rings for $\Gamma_0^n(q/p)$ into p-subring for $\Gamma_0^n(q)$, provided that $p|q$ and $p^2 \nmid q$, which replace parabolic embeddings of regular rings considered in §2.3.

§3.1. Centralizers of Frobenius elements

We let denote by

$$\begin{aligned} &\mathcal{S}(q) = \mathcal{S}^n(q) \subset \mathcal{H}_q(K) \qquad \text{and} \\ &\mathcal{S}_p(q) = \mathcal{S}_p^n(q) = \{\sum_i a_i(KM_i) \in \mathcal{S}(q); \quad \mu(M_i)|p^\infty\}, \end{aligned} \tag{3-1}$$

where p is a prime divisor of q, *the (maximal) reducible subring* of the singular HS–ring $\mathcal{H}_q(K)$ of the group $K = \Gamma_0^n(q)$ and *the singular reducible p-ring*. In this section we shall show that *the singular Frobenius elements*

$$\Pi(a) = \Pi_K^n(a) = \left(\begin{pmatrix} E_n & 0 \\ 0 & aE_n \end{pmatrix}\right)_K \quad \text{with } a|q^\infty \tag{3-2}$$

belong to the ring $\mathcal{S}(q)$ and determine their centralizer in the ring.

It turns out that the centralizer is naturally isomorphic to the centralizer $\widehat{C}_q^n$ of the corresponding elements $\widehat{\Pi}(a)$ in the q-singular subring $\mathcal{L}_q^n$ of the triangular ring $\mathcal{L}^n$ (see *Theorem 3.3*). This is crucial for our approach to singular HS–rings and operators for the group K.

We shall start with two simple lemmas on rational matrices (see [Si(63)]).

Lemma 3.1. *Let R be a rational matrix of order n. Then there is an integral matrix D of order n with nonzero determinant, which satisfies the following conditions:*

(1) *the matrix DR is integral;*
(2) *if a product $D'R$ is integral, then $D' = TD$ with an integral matrix T.*

Proof. If $R = 0$, one can take $D = E_n$. If $R \neq 0$, then it can be diagonalized by left and right multiplications by matrices of the group $\Lambda = GL_n(\mathbb{Z})$:

$$URV = R' = diag\big(a_1/b_1, \ldots, a_r/b_r, 0, \ldots, 0\big), \qquad (U, V \in \Lambda),$$

where a_i, b_j are positive integers satisfying $\gcd(a_i, b_i) = 1$ for $i = 1, \ldots, r$. Note that when $S = (s_i, \ldots, s_n)$ is an integral matrix with columns s_i, then the product SR' is again an integral matrix if and only if the columns s_i are divisible by b_i for $i = 1, \ldots, r$, which is equivalent to the condition that S is divisible from the right by the matrix $B = diag(b_1, \ldots, b_r, 1, \ldots, 1)$. Let us set $D = BU$ .Then the matrix $DR = BR'V^{-1}$ is integral, and if a product $D'R$ is integral, then the matrix $D'U^{-1}R'$ is integral, which implies that $D'U^{-1} = TB$ with an integral matrix T, that is $D' = TBU = TD$.

□

A matrix D satisfying the conditions (1) and (2) of the lemma is called *a (left) denominator of the matrix R*. It follows from the definition that all denominators of R form the single left coset ΛD modulo the group $\Lambda = \Lambda^n$, which can be called *the denominator of R*.

Lemma 3.2. *If R is a rational matrix of order n and D is a denominator of R, then the pair (DR, D) is coprime.*

Proof. If $DR = SC_1$ and $D = SD_1$ with integral matrices S, C_1, D_1, then $R = D_1^{-1}C_1$, and so the matrix D_1R is integral. It follows that $D_1 = TD$ with an integral matrix T. Therefore, $ST = E$, and so $S \in \Lambda$.

□

Theorem 3.3. *Let n, q be positive integers and $q > 1$. Then the following assertions hold:*

(1) *Each double coset $(M)_K$ of a matrix $M = U(\mu, D)$ of the form* (2-41)*, which is contained in $\Sigma^n_{0,q}$ and satisfies the condition* (2-42)*, has the following decomposition into left cosets modulo the group $K = \Gamma^n_0(q)$:*

$$(M)_K = \sum_{D', B} \big(KU(\mu, D') \begin{pmatrix} E & B \\ 0 & E \end{pmatrix}\big), \tag{3-3}$$

where D' runs a set of representatives of the left coset modulo the group $\Lambda = \Lambda^n$ contained in the double coset $\Lambda D \Lambda$, and B runs over a set of representatives for the additive group $\mathbb{S} = \mathbb{S}_n$ modulo the subgroup $\mu^{-1} \cdot {}^tD'\mathbb{S}D'$. In particular, the singular Frobenius elements (3-2) *have the decomposition*

$$\Pi(a) = \Pi^n_K(a) = \big(U(a, aE)\big)_K = \sum_{B \in \mathbb{S}/a\mathbb{S}} \big(K \begin{pmatrix} E & B \\ 0 & aE \end{pmatrix}\big); \tag{3-4}$$

(2) *All double cosets* $(M)_K$ *of matrices* $M = U(\mu, D)$ *in* $\Sigma^n_{0,q}$ *satisfying* (2-42) *span over* $\mathbb{Q}$ *a subring* $C_q = C^n_q$ *of the ring* $\mathcal{S}(q) = \mathcal{S}^n(q)$*;*

(3) *Restriction of the parabolic embedding*

$$j: \quad \mathcal{S} \to \mathcal{L}_q \tag{3-5}$$

on the subring C_q *is an isomorphism of* C_q *onto the centralizer* $\widehat{C}_q$ *of the Frobenius elements contained in* $\mathcal{L}_q$*. In particular ,* C_q *is a commutative integral domain, which is generated by the local subrings*

$$C_p = \{T = \sum_i a_i(KM_i) \in C_q; \quad \mu(M_i)|p^\infty\} \tag{3-6}$$

for all prime numbers p *dividing* q*;*

(4) *The ring* C_q *(resp.,* C_p*) can be characterized as the centralizer in* $\mathcal{S}(q)$ *(resp.,* $\mathcal{S}_p(q)$*) of the Frobenius elements* (3-2) *(resp.,* $\Pi(p)$*).*

We prove first two lemmas.

Lemma 3.4. *Each element of the form* $U(\mu, D) \in \Sigma^n_0$ *satisfying the condition* (2-42) *is* K*–reducible.*

Proof. By *Lemma 2.1*, one can assume that $q > 1$. It suffices to prove that , for every matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$, there is a matrix $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in K$ such that

$$\gamma' U(\mu, D)\gamma = \begin{pmatrix} * & * \\ c'Aa + d'Dc & * \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \tag{3-7}$$

where $A = \mu \cdot {}^tD^{-1}$. Since $a \cdot {}^td \equiv 1 \pmod q$, it follows that $\det a$ is prime to q, and so the matrix a is invertible. Set

$$R = -Dca^{-1}A^{-1} = -\mu^{-1}Dca^{-1} \cdot {}^tD.$$

By *Lemma 1.1(4)*, the matrix R is symmetric. Since $\mu | d(D)^2$, it follows that the matrix $\det a \cdot R$ is integral. Since $\det a$ is prime to q and $c \equiv 0 \pmod q$, we conclude that $\det a \cdot R \equiv 0 \pmod q$. Let d' be a denominator of R and $c' = d'R$. Then $d' | \det a \cdot E$, whence $\det d' | (\det a)^n$, and so $\det d'$ is prime to q. Further, since $(\det a)c' = d' \cdot (\det a)R \equiv 0 \pmod q$, we have $c' \equiv 0 \pmod q$. The pair (c', d') is coprime, by *Lemma 3.2*, and is symmetric, since R is symmetric. By *Lemma 1.2*, there are matrices a',b' such that the matrix $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma^n$. Then $\gamma' \in K$, and γ' satisfies (3-7).

□

Lemma 3.5. *Each of left cosets modulo K contained in the double coset KMK of a matrix $M = U(\mu, D) \in \Sigma_{0,q}$ of the form (2-41) satisfying (2-42) contains a representative of the form*

$$\begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix} \qquad \text{with } D' \in \Lambda D \Lambda. \tag{3-8}$$

Proof. Let us take a representative

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} M \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in KM \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ of the form } \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$, which exists, by previous lemma. Then $c'Aa + d'Dc = 0$, where $A = \mu \cdot {}^tD^{-1}$, and so $(d')^{-1}c' = -\mu^{-1}Dca^{-1} \cdot {}^tD$. On the other hand, we have

$$\begin{aligned} D' &= c'Ab + d'Dd = d'\big((d')^{-1}c'Ab + Dd\big) \\ &= d'(-\mu^{-1}Dca^{-1}\,{}^tDAb + Dd) = d'D(-ca^{-1}b + d) \\ &= d'D \cdot {}^ta^{-1}({}^tad - {}^ta \cdot {}^ta^{-1} \cdot {}^tcb) = d'D \cdot {}^ta^{-1}. \end{aligned}$$

Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in K$, it follows that $\det d'$ and $\det a$ are coprime with q, and so are coprime with μ, because $\mu | q^\infty$. On the other hand, the matrix $\mu \cdot {}^tD^{-1}$ is integral, and so $\det D | \mu^n | q^\infty$. Since the integral matrices d' and D have coprime determinants, it is an easy consequence of the theory of elementary divisors for the general linear group over $\mathbb{Z}$ (see, for example, [An(87),Chapter 3]), that one can write $d'D = D_1 d_1$, where D_1 and d_1 are integral matrices having the same elementary divisors as D and d', respectively. Then we have the relation

$$D' = d'D \cdot {}^ta^{-1} = D_1 d_1 \cdot {}^ta^{-1}.$$

Since all of the elementary divisors of matrices D' and D are prime to those of d_1 and a, the last relation implies that all of the elementary divisors of the matrix $d_1 \cdot {}^ta^{-1}$ are equal to 1. It follows that the matrices D',D_1, and D have the same elementary divisors, and so $D' \in \Lambda D \Lambda$.

□

Proof of Theorem 3.3. (1). Let us take a representative of the form (3-8) in a left coset $KM \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$. then we have

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} M \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix} = \begin{pmatrix} {}^t\eta^{-1} & 0 \\ 0 & \eta \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} {}^t\nu^{-1} & 0 \\ 0 & \nu \end{pmatrix},$$

where $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in K$, η, $\nu \in \Lambda$. It follows that

$$M = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} * & a_1Ab_2 + a_1Bd_2 + b_1Dd_2 \\ * & * \end{pmatrix},$$

where the matrices
(3-9)

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} \begin{pmatrix} {}^t\eta^{-1} & 0 \\ 0 & \eta \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} {}^t\nu^{-1} & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

belong to K. This implies the relation $a_1Ab_2 + a_1Bd_2 + b_1Dd_2 = 0$, whence

$$B = -(Ab_2d_2^{-1} + a_1^{-1}b_1D) = AS,$$

where $S = -(b_2d_2^{-1} + A^{-1}a_1^{-1}b_1D)$. Note that, since the matrices (3-9) belong to K, we have ${}^ta_1d_1 \equiv 1 \pmod q$ and ${}^ta_2d_2 \equiv 1 \pmod q$, and so $\det a_1$, $\det d_2$ are prime to q. In particular, the matrices a_1 and d_2 are invertible, because $q > 1$. Also, if p is a prime number and $p | \det a_1 \det d_2$, then $p \nmid q$ and so $p \nmid \det A$. It follows that the matrix $S = A^{-1}B$ is p-integral, because the matrix B is integral. But if $p | \det A$, then $p|q$ and so $p \nmid \det a_1 \det d_2$. Also the matrix $S = -(b_2d_2^{-1} + \mu^{-1} \cdot {}^tDa_1^{-1}bD)$ is p-integral, by the condition (2-42). We conclude that S is an integral matrix, and so

$$B' = {}^t\eta^{-1}B\nu = {}^t\eta^{-1}AS\nu = A' \cdot {}^t\nu S\nu = A'S'$$

with an integral symmetric matrix S'.

Finally, it is clear that two matrices $\begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix}$ and $\begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix}$ of the form (3-8), where $B' = A'S'$ and $B_1 = A_1S_1$ with S, $S_1 \in \mathbb{S}$, belong to the same left coset modulo K, if and only if they belong to the same left coset modulo Γ_0^n:

$$\begin{pmatrix} \alpha & \alpha\beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} A_1 & A_1S_1 \\ 0 & D_1 \end{pmatrix} = \begin{pmatrix} A' & A'S' \\ 0 & D' \end{pmatrix},$$

where α, $\delta \in \Lambda$, ${}^t\alpha\delta = E$, $\beta \in \mathbb{S}$, which is equivalent to the relations

$$\delta D_1 = D' \quad \text{and } \alpha A_1S_1 + \alpha\beta D_1 = A'S'.$$

The first relation means that $\Lambda D_1 = \Lambda D'$, and so one can assume that $D_1 = D'$ and $\delta = E$. Then the second turns into

$$A'S_1 + \beta D' = A'S', \quad \text{i.e. } S' - S_1 = (A')^{-1}\beta D' = \mu^{-1} \cdot {}^tD'\beta D'.$$

(2). If $(M)_K = (U(\mu, D))_K$ and $(M_1)_K = (U(\mu_1, D_1))_K$ are two double cosets of C_q, written in the form (3-3), then their product is a sum of the left cosets of the products

$$U(\mu, D')\begin{pmatrix} E & B \\ 0 & E \end{pmatrix} U(\mu_1, D'_1)\begin{pmatrix} E & B_1 \\ 0 & E \end{pmatrix}$$
$$= U(\mu\mu_1, D'D'_1)\begin{pmatrix} E & \mu_1^{-1} \cdot {}^tD_1 B D_1 + B_1 \\ 0 & E \end{pmatrix},$$

which belong to the double coset of the matrix $U(\mu\mu_1, D'D'_1)$, since the matrix $\mu^{-1} \cdot {}^tD_1BD_1$ is integral, by the condition (2-42) for $U(\mu_1, D_1)$. Also,

$$\mu\mu_1 | (\det D \det D_1)^2 = (\det D' \det D'_1)^2 = (\det D'D'_1)^2.$$

(3). The statements follow from parts (1), (2), *Theorem 2.8, Proposition 2.9*, and *Theorem 2.10.*

(4). Since the ring C_q is commutative and contains the elements (3-2), it suffices to prove that every element T of $\mathcal{S}(q)$ which commutes with the elements (3-2) belongs to C_q. The image under the parabolic embedding $\widehat{T}$ of T in $\mathcal{L}_q$ commutes with each of Frobenius elements of the ring $\mathcal{L}_q$ and therefore belongs to $\widehat{C}_q$. Then, by *Theorem 2.8*, $\widehat{T}$ is a linear combination of the left cosets modulo Γ_0 of matrices of the form

$$U(\mu, D')\begin{pmatrix} E & B \\ 0 & E \end{pmatrix}$$

with integral symmetric B and integral D' satisfying the condition $\mu | (\det D')^2 | q^\infty$. By the definition of parabolic embeddings, the element T is a linear combination of left cosets of the same matrices modulo K. Then T belongs to C_q, by the part (1). The case of C_p with a prime p dividing q is considered similarly.

□

§3.2. Neutral rings

The neutral ring

(3-10) $$\mathcal{N}(q) = \mathcal{N}^n(q) = HS(K, \Gamma^n)$$

of the group $K = \Gamma_0^n(q)$ is contained both in the regular ring $\mathcal{H}_{(q)}(K)$ and in the singular ring $\mathcal{H}_q(K)$ (see (1-27)), since

$$\Gamma^n = \Sigma^n_{(q)} \bigcap \Sigma^n_q.$$

Although the neutral ring does not play essential part in the regular theory, it is important in the singular case. In this section we shall prove several properties of the neutral ring and its subrings of the form

(3-11) $$\mathcal{N}(q_1, q) = \mathcal{N}^n(q_1, q) = HS(K, \Gamma_0^n(q_1)),$$

where q_1 divides q.

Lemma 3.6. *Two matrices* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *and* $M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$ *of the group* $\Gamma = \Gamma^n$ *belong to the same left coset* $KM = KM'$ *modulo the group* K*, if and only if their "second rows" are "proportional" modulo* q*,*

$$(C', D') \simeq (C, D) \pmod{q}, \tag{3-12}$$

in the sense that

$$(C', D') \equiv d(C, D) \pmod{q} \tag{3-13}$$

with an integral matrix d *of order* n *invertible modulo* q*.*

Proof. If $KM' = KM$, then $M' = \gamma M$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$, which implies the relation

$$(C', D') = (cA + dC, cB + dD) \equiv d(C, D) \pmod{q}.$$

But if (3-13) is satisfied, then the matrix

$$\begin{aligned} \gamma = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} &= \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} {}^tD & -{}^tB \\ -{}^tC & {}^tA \end{pmatrix} \\ &= \begin{pmatrix} * & * \\ C' \cdot {}^tD - D' \cdot {}^tC & * \end{pmatrix} \end{aligned}$$

belongs to K, since $C' \cdot {}^tD - D' \cdot {}^tC \equiv d(C \cdot {}^tD - D \cdot {}^tC) = 0 \pmod{q}$. □

Lemma 3.7. *The indices*

$$\nu(q) = \nu_n(q) = \left[\Gamma^n : \Gamma_0^n(q)\right] \tag{3-14}$$

satisfy the relations

$$\nu(q_1 q_2) = \nu(q_1)\nu(q_2), \ \textit{if} \ \gcd(q_1, q_2) = 1. \tag{3-15}$$

Proof. It is well known that the natural map $\Gamma^n \to Sp_n(\mathbb{Z}/q\mathbb{Z})$ is an epimorphism (see, for example, [An(87), *Lemma 3.3.2*]). It follows that the index $\nu(q)$ can be interpreted as the index in the group $Sp_n(\mathbb{Z}/q\mathbb{Z})$ of the subgroup

$$\left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in Sp_n(\mathbb{Z}/q\mathbb{Z}) \right\}. \tag{3-16}$$

The group and the subgroup are sets of solutions of finite systems of polynomial congruences modulo q, and the relations (3-15) follow from the Chinese remainder theorem.

$\square$

In order to formulate next lemma, we need certain notation. We set

$$I_{r,n} = \{(i_1, \ldots, i_r) \in \mathbb{N}^r; \quad 1 \le i_1 < \cdots < i_r \le n\}. \tag{3-17}$$

For $\mathbf{i} = (i_1, \ldots, i_r) \in I_{r,n}$ we denote by $\widehat{\mathbf{i}}$ the set $(j_1, \ldots, j_{n-r}) \in I_{n-r,n}$ which is complementary to $(i_1, \ldots, i_r)$ in $(1, \ldots, n)$. Further, to each $\mathbf{i} = (i_1, \ldots, i_r) \in I_{r,n}$ we associate the permutation

$$\sigma(\mathbf{i}) : (i_1, \ldots, i_r, j_1, \ldots, j_{n-r}) \to (1, \ldots, r, r+1, \ldots, n) \tag{3-18}$$

of the set $(1, \ldots, n)$, where $(j_1, \ldots, j_{n-r}) = \widehat{\mathbf{i}}$, and the matrix

$$M(\mathbf{i}) = M(\sigma(\mathbf{i})) \tag{3-19}$$

of the permutation, where the matrix of a permutation σ of the set $(1, \ldots, n)$ is the matrix $M(\sigma) = (\delta_{\sigma^{-1}(i),j})$ with $\delta_{i,i} = 1$ and $\delta_{i,j} = 0$, if $i \neq j$, for $i, j = 1, \ldots, n$. Finally, for $\mathbf{i} \in I_{r,n}$ and a positive integer p , we set

(3-20)
$$V_p(\mathbf{i}) = \{V = (v_{\alpha\beta)} \in \mathbb{Z}_n^r; \quad 0 \le v_{\alpha\beta} < p, \text{ if } i_\alpha < j_\beta, \text{ and } v_{\alpha\beta} = 0, \text{ if } i_\alpha > j_\beta\},$$

where $(j_1, \ldots, j_{n-r}) = \widehat{\mathbf{i}}$.

Lemma 3.8. *Let p be a prime divisor of q, which does not divide q/p, and let a,b be two integers satisfying $ap - bq_1 = 1$, where $q_1 = q/p$. Then the set*

$$\bigcup_{r=0}^{n} W_n^r(p, q), \tag{3-21}$$

where $W_n^0(p, q) = \{E_{2n}\}$, and, for $r > 1$,

$$W_n^r(p, q) = \{M_r \cdot U_{\mathbf{i}}(V, D); \quad \mathbf{i} \in I_{r,n}, \quad V \in V_p(\mathbf{i}), \quad D \in \mathbb{S}_r/p\mathbb{S}_r\} \tag{3-22}$$

with

$$M_r = \begin{pmatrix} aE_r & 0 & bE_r & 0 \\ 0 & E_{n-r} & 0 & 0 \\ q_1E_r & 0 & pE_r & 0 \\ 0 & 0 & 0 & E_{n-r} \end{pmatrix},$$

and

$$U_{\mathbf{i}}(V,\,D)=\begin{pmatrix}E_r & V & D & 0\\ 0 & E_{n-r} & 0 & 0\\ 0 & 0 & E_r & 0\\ 0 & 0 & -{}^tV & E_{n-r}\end{pmatrix}\begin{pmatrix}M(\mathbf{i}) & 0\\ 0 & {}^tM(\mathbf{i})^{-1}\end{pmatrix}$$

is a complete set of representatives for different left cosets $\Gamma_0^n(q)\setminus\Gamma_0^n(q_1)$.

Proof. We shall show first that matrices of the set (3-21) belong to different left cosets modulo $K=\Gamma_0^n(q)$. Let $M=\begin{pmatrix}A & B\\ C & D\end{pmatrix}$ and $M'=\begin{pmatrix}A' & B'\\ C' & D'\end{pmatrix}$ be two of the matrices. Suppose that $KM=KM'$. Then, by *Lemma 3.6*, their second rows are proportional modulo p, that is

$$C'\equiv dC \pmod q,\qquad D'\equiv dD \pmod q \tag{3-23}$$

with an integral matrix d of order n invertible modulo q. It follows that the matrices C, C' have the same rank r modulo p, and so M, M' both belong to the same set $W_n^r(p,\,q)$. If

$$C=\begin{pmatrix}q_1E_r & q_1V\\ 0 & 0\end{pmatrix}M(\mathbf{i}),\quad C'=\begin{pmatrix}q_1E_r & q_1V'\\ 0 & 0\end{pmatrix}M(\mathbf{i}'),\ \text{and } d=\begin{pmatrix}d_1 & d_2\\ d_3 & d_4\end{pmatrix},$$

where d_1 is the block of dimension $r\times r$, then the congruences imply the congruence

$$\big(q_1E_r,\,q_1V'\big)M(\mathbf{i}')\equiv d_1\big(q_1E_r,\,q_1V\big)M(\mathbf{i}) \pmod q. \tag{3-24}$$

It follows that the matrix d_1 is invertible modulo p. If $q_1(E_r,\,V)M(\mathbf{i})=(t_1,\dots,t_n)$, then

$$q_1(E_r,\,V)=(t_1,\dots,t_n)M(\mathbf{i})^{-1}=(t_{i_1},\dots,t_{i_r},t_{j_1},\dots,t_{j_{n-r}}),$$

where $(i_1,\dots,i_r)=\mathbf{i}$ and $(j_1,\dots,j_{n-r})=\widehat{\mathbf{i}}$, by the definition of the matrix $M(\mathbf{i})$, and so, by the definition of the set $V_p(\mathbf{i})$ (see (3-20)), the system $\mathbf{i}=(i_1,\dots,i_r)$ is in the sense of lexicographic order the least system of indices of columns of the matrix $(t_1,\dots,t_n)$ which are linearly independent modulo p. Thus, the congruence (3-24) implies that $\mathbf{i}'=\mathbf{i}$, and so $d_1\equiv E_r \pmod p$, and $V'\equiv V \pmod p$. By (3-30), the last congruence means that $V'=V$. Then the second congruence (3-23) implies the congruence

$$\begin{pmatrix}q_1D' & 0\\ -{}^tV & E_{n-r}\end{pmatrix}{}^tM(\mathbf{i})^{-1}\equiv\begin{pmatrix}E_r & d_2\\ d_3 & d_4\end{pmatrix}\begin{pmatrix}q_1D & 0\\ -{}^tV & E_{n-r}\end{pmatrix}{}^tM(\mathbf{i})^{-1} \pmod p.$$

by comparing corresponding blocks, we conclude that $d_2\equiv 0 \pmod p$, and $q_1D'\equiv q_1D-d_2{}^tV\equiv q_1D \pmod p$. It follows that $D'=D$.

In order to conclude the proof of the lemma, it is sufficient to show that the number of elements of the set (3-21) is equal to the index $[\Gamma_0^n(q_1) : \Gamma_0^n(q)]$. Note first that the number of elements of the set (3-20) for $\mathbf{i} = (i_1, \dots, i_r) \in I_{r,n}$ is $p^{j_1+\cdots+j_{n-r}-\langle n-r \rangle}$ (see *Notation*), where $(j_1, \dots, j_{n-r}) = \widehat{\mathbf{i}}$, since the number of i_α satisfying $i_\alpha < j_\beta$ with a fixed β is equal to $j_\beta - \beta$. It follows that the number of elements of the set (3-21) is equal to

$$\sum_{r=0}^{n}\big(p^{-\langle n-r\rangle} \sum_{1\le j_1<\cdots<j_{n-r}\le n} p^{j_1+\cdots+j_{n-r}}\big)p^{\langle r\rangle} = \sum_{r=0}^{n} p^{\langle r\rangle}\frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)} = \prod_{i=1}^{n}(1+p^i), \tag{3-25}$$

where

$$\varphi_0(x) = 1, \quad \varphi_r(x) = (x-1)(x^2-1)\dots(x^r-1), \quad (r \in \mathbb{N}) \tag{3-26}$$

and we have used the identity in two variables x, t:

$$\prod_{i=1}^{n}(1+tx^i) = \sum_{r=0}^{n} t^r x^{\langle r\rangle}\frac{\varphi_n(x)}{\varphi_r(x)\varphi_{n-r}(x)},$$

and its consequences

$$\sum_{1\le i_1<\cdots<i_r\le n} x^{i_1+\cdots+i_r} = x^{\langle r\rangle}\frac{\varphi_n(x)}{\varphi_r(x)\varphi_{n-r}(x)}, \qquad (1 \le r \le n). \tag{3-27}$$

On the other hand, according to *Lemma 3.7*, we can write

$$[\Gamma_0^n(q_1) : \Gamma_0^n(q)] = \nu_n(q)/\nu_n(q_1) = \nu_n(p), \tag{3-28}$$

and

$$\begin{aligned} \nu_n(p) &= [\Gamma^n : \Gamma_0^n(p)] = \#(Sp_n(\mathbb{Z}/p\mathbb{Z}))/p^{\langle n\rangle}\#(GL_n(\mathbb{Z}/p\mathbb{Z})) \\ &= p^{n^2}\prod_{i=1}^{n}(p^{2i}-1)/p^{\langle n\rangle}p^{\langle n-1\rangle}\prod_{i=1}^{n}(p^i-1) = \prod_{i=1}^{n}(p^i+1). \end{aligned} \tag{3-29}$$

(see, for example, [Ar(57), *Chapters 3,4*]). The comparison of formulas (3-28) and (3-29) with (3-25) concludes the proof of the lemma.

$\square$

Proposition 3.9. *Let p be a prime number dividing q, but not dividing $q_1 = q/p$. Then the following assertions hold:*

(1) *The ring*

$$\mathcal{N}_p(q) = \mathcal{N}_p^n(q) = \mathcal{N}^n(q_1,\, q) \tag{3-30}$$

consists of linear combinations of $n+1$ different double cosets

$$\xi_r(p) = \xi_r^n(p) = (M_r)_K, \tag{3-31}$$

where $M_0 = E_{2n}$, and $M_1, \ldots, M_n$ were introduced in Lemma 3.8. Each double coset KM_rK can be characterized as the set of all matrices $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of $\Gamma_0^n(q_1)$ with the block C of rank r modulo p.

(2) *Each double coset* (3-31) *has the following decomposition into left cosets:*

$$\xi_r(p) = \sum_{M \in W_n^r(p,q)} (KM), \tag{3-32}$$

where $W_n^r(p,\, q)$ is the set (3-22). *In particular, the number of different left cosets in $\xi_r(p)$ is*

$$\#(W_n^r(p,\, q)) = p^{\langle r\rangle} \frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)}, \tag{3-33}$$

where $\varphi_r(x)$ are the polynomials (3-26).

(3) *The double cosets* (3-31) *are invariant with respect to the star antiautomorphism* (1-18)*:*

$$\xi_r^*(p) = \xi_r(p), \qquad (r = 0, 1, \ldots, n). \tag{3-34}$$

In particular, the ring $\mathcal{N}_p(q)$ is commutative.

(4) *If p and p' are two different prime divisors of q and p^2 does not divide q, then each element of $\mathcal{N}_p(q)$ commutes with the Frobenius element $\Pi(p')$.*

Proof. First of all, note that, since $K \subset \Gamma_0^n(p)$, the function

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \to r_p(C), \qquad (M \in \Sigma^n) \tag{3-35}$$

where $r_p(C)$ is the rank of C modulo p, takes a constant value on every left and double coset of the group K; in particular, its value on $W_n^r(p,\, q)$ and on KM_rK is r. Thus, the double cosets ξ_r are pairwise distinct. Since

$$W_n^r(p,\, q) \subset M_r\Gamma_0^n \subset KM_rK,$$

it follows from *Lemma 3.8*, that each of ξ_r has the decomposition (3-32), and there are no other double cosets in $\mathcal{N}_p(q)$, but $\xi_0, \xi_1, \dots, \xi_n$.

The formula (3-33) follows from the identities (3-27), since the number of elements of a set $V_p(\mathbf{i})$ with $\mathbf{i} \in I_{r,n}$ is clearly $p^{j_1+\cdots+j_{n-r}-\langle n-r\rangle}$, where $(j_1, \dots, j_{n-r}) = \widehat{\mathbf{i}}$.

Further, by the above,

$$M_r^* = M_r^{-1} = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ -q_1 E_r & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix} \in K M_r K,$$

which implies (3-34).

Finally, if $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_0^n(q_1)$, S and S' are matrices of $\mathbb{S}_n$ satisfying the congruence $AS' \equiv B + SD \pmod{p'}$, then the matrix

$$\begin{aligned} M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} &= \begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix}^{-1} \\ &= \begin{pmatrix} A + SC & (-(A+SC)S' + B + SD)/p \\ p'C & -CS' + D \end{pmatrix} \end{aligned}$$

belongs to $\Gamma_0^n(q_1)$, $r_p(C') = r_p(C)$, and it satisfies the relation

$$\begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix} M = M' \begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix}.$$

It is easy to see that, for every two matrices M, $M_1 \in \Gamma_0^n(q_1)$ with different left cosets KM, KM_1, the left cosets KM', KM_1' are also different. It follows that

$$\begin{aligned} \Pi(p')\xi_r(p) &= \sum_{\substack{M \in K\backslash\Gamma_0^n(q_1), r_p(C(M))=r, \\ S \in \mathbb{S}_n/p\mathbb{S}_n}} \left(K \begin{pmatrix} E & S \\ 0 & p'E \end{pmatrix} M \right) \\ &= \sum_{\substack{M' \in K\backslash\Gamma_0^n(q_1), r_p(C(M'))=r, \\ S' \in \mathbb{S}_n/p\mathbb{S}_n}} \left(KM' \begin{pmatrix} E & S' \\ 0 & p'E \end{pmatrix} \right) = \xi_r(p)\Pi(p'), \end{aligned}$$

where $C(M)$, and $C(M')$ denote the lower left $n \times n$–blocks of the corresponding matrices.

$\square$

Lemma 3.10. *With the notations and assumptions of Proposition 2.9, products of elements* (3.31) *of the ring* $\mathcal{N}_p(q)$ *by the element* $\xi_n(p)$ *can be given by the following formulas*

$$\xi_n(p)\xi_r(p) = \sum_{s=0}^{r} p^{\langle n-r\rangle+(r-s)(n-r+s)} sm_p(s,\, n-r+s)\xi_{n-r+s}(p), \tag{3-36}$$

where $r = 0, 1, \dots, n$ *and* $sm_p(a,\, b)$ *stands for the number of symmetric matrices of order* b *and rank* a *over the field of* p *elements.*

Proof. By *Proposition 3.9* and the definition of multiplication in HS–rings, the product $\xi_n(p)\xi_r(p)$ is the sum of left cosets of all products

$$\begin{pmatrix} aE_n & aD+bE_n \\ q_1E_n & q_1D+pE_n \end{pmatrix} M_r \begin{pmatrix} E_r & V & D' & 0 \\ 0 & E_{n-r} & 0 & 0 \\ 0 & 0 & E_r & 0 \\ 0 & 0 & -{}^tV & E_{n-r} \end{pmatrix} \begin{pmatrix} M(\mathbf{i}) & 0 \\ 0 & {}^tM(\mathbf{i})^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ \check{D}_1 & 0 & * & * \\ q_1^2D_3 & q_1E_{n-r} & * & * \end{pmatrix} \begin{pmatrix} E_r & V & D' & 0 \\ 0 & E_{n-r} & 0 & 0 \\ 0 & 0 & E_r & 0 \\ 0 & 0 & -{}^tV & E_{n-r} \end{pmatrix} \begin{pmatrix} M(\mathbf{i}) & 0 \\ 0 & {}^tM(\mathbf{i})^{-1} \end{pmatrix},$$

where $D = \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix}$, $D' \in \mathbb{S}_n/p\mathbb{S}_n$, $V \in V(\mathbf{i})$ with $\mathbf{i} \in I_{r,n}$, and where $\check{D}_1 = q_1^2D_1 + q_1(a+p)E_r$. Such a product belongs to a double coset $KM_{r'}K$ if and only if the rank of the matrix

$$\begin{pmatrix} \check{D}_1 & 0 \\ q_1^2D_3 & q_1E_{n-r} \end{pmatrix}$$

modulo p is r' (see (3-35) and further). On the other hand, the rank is clearly equal to $n-r+s$, where s stands for the rank $r_p(\check{D}_1)$. Since the matrix $\check{D}_1$ runs together with D_1 over all symmetric matrices of order r modulo p, we conclude that the number of the products belonging to $KM_{n-r+s}K$ is

$$sm_p(s,\, r)p^{\langle n-r\rangle+r(n-r)}\#(W_n^r(p,\, q)) = sm_p(s,\, r)p^{\langle n\rangle}\frac{\varphi_n(p)}{\varphi_r(p)\varphi_{n-r}(p)}$$

(see (3-33)). On dividing the number by the number $\#(W_n^{n-r+s}(p,\, q))$ of left cosets in $\xi_{n-r+s}(p)$, we see that the coefficient at $\xi_{n-r+s}(p)$ in the product $\xi_n(p)\xi_r(p)$ is equal to

$$sm_p(s,\, r)p^{\langle n\rangle-\langle n-r+s\rangle}\frac{\varphi_{n-r+s}(p)\varphi_{r-s}(p)}{\varphi_r(p)\varphi_{n-r}(p)}$$

$$= p^{\langle r-s\rangle+(r-s)(n-r+s)} sm_p(s,\, s)\frac{\varphi_r(p)\varphi_{n-r+s}(p)\varphi_{r-s}(p)}{\varphi_s(p)\varphi_{r-s}(p)\varphi_r(p)\varphi_{n-r}(p)}$$
$$= p^{\langle r-s\rangle+(r-s)(n-r+s)} sm_p(s,\, n-r+s),$$

where we have twice used the formula

$$sm_p(a,\, b) = sm_p(a,\, a)\frac{\varphi_b(p)}{\varphi_a(p)\varphi_{b-a}(p)} \qquad (0 \le a \le b) \tag{3-37}$$

(see, for example, [An(87), *Lemma 3.5.20*]) and the obvious relation $\langle a+b\rangle = \langle a\rangle + \langle b\rangle + ab$.

$\square$

Note that the numbers $sm_p(a,\, b)$ can be explicitly calculated with the help of formulas (3-37) and the formula

$$sm_p(a,\, a) = \sum_{i=0}^{a}(-1)^i p^{\langle i-1\rangle+\langle a-i\rangle}\frac{\varphi_a(p)}{\varphi_i(p)\varphi_{a-i}(p)}, \tag{3-38}$$

which is equivalent to the first identity of *Lemma 3.5.21* of [An(87)].

Lemma 3.11. *With the notation and assumptions of Proposition 2.9, the element $\xi^n_n = \xi^n_n(p)$ is invertible in the ring $\mathcal{N}^n_p(q)$. In particular,*

$$(\xi^1_1)^{-1} = \big((1-p)\xi^1_0 + \xi^1_1\big)/p; \tag{3-39}$$
$$(\xi^2_2)^{-1} = \big((1-p)\xi^2_0 + (1-p)\xi^2_1 + \xi^2_2\big)/p^3. \tag{3-40}$$

Proof. The formulas (3-36) show that the matrix of the operator of multiplication by ξ^n_n in the basis $\xi^n_0, \xi^n_1, \dots, \xi^n_n$ of the space $\mathcal{N}^n_p(q)$ has zeros above the second diagonal and nonzero elements $p^{\langle r\rangle+r(n-r)}sm_p(0,\, n-r) = p^{\langle r\rangle+r(n-r)}$ for $r = 0, 1, \dots, n$ on this diagonal. For example, for $n = 1$ and $n = 2$, we get the matrices

$$\begin{pmatrix} 0 & 1 \\ p & p-1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & p^2 & p^2-1 \\ p^3 & p^2(p-1) & p^2(p-1) \end{pmatrix},$$

respectively. Such a matrix is clearly invertible, which proves that ξ^n_n is invertible. The formulas (3-39) and (3-40) follow by inversion of the matrices.

$\square$

In contrast to *Lemma 3.8*, where q/q_1 and q_1 are coprime, in the case when q and its divisor q_1 have the same prime factors, the left cosets $\Gamma^n_0(q)\setminus\Gamma^n_0(q_1)$ admit a very simple description, which we shall need in the case when q/q_1 is a prime number.

Proposition 3.12. *Let p be a prime number such that p^2 divides q. Then the following assertions hold:*

(1) *The set*

$$\left\{ \begin{pmatrix} E_n & 0 \\ q_1 C & E_n \end{pmatrix} ; \quad C \in \mathbb{S}_n / p\mathbb{S}_n \right\},$$

where $q_1 = q/p$, is a complete set of representatives for different left cosets of the group $K_1 = \Gamma_0^n(q_1)$ modulo the subgroup $K = \Gamma_0^n(q)$;

(2) *The element*

$$\tau(p) = \tau^n(p,\, q) = p^{-\langle n \rangle} \sum_{M_i \in K \backslash K_1} (K M_i)$$
$$= p^{-\langle n \rangle} \sum_{C \in \mathbb{S}_n / p\mathbb{S}_n} \left(K \begin{pmatrix} E_n & 0 \\ q_1 C & E_n \end{pmatrix} \right) \in \mathcal{N}(q_1,\, q) \tag{3-41}$$

satisfies the relation

$$\Pi(p)\tau(p) = \Pi(p),$$

where $\Pi(p)$ is the Frobenius element of the multiplier p ;

(3) *The element $\tau(p)$ commutes with every of Frobenius elements $\Pi(p')$ with primes $p' \neq p$ dividing q;*

(4) *The element $\tau(p)$ satisfies*

$$\tau^*(p) = \tau(p),$$

where $*$ is the antiautomorphism (1-18).

Proof. The "second rows" of different matrices of the set are clearly not proportional modulo q in the sense of (3-13), and so, by *Lemma 3.6*, the matrices belong to different left cosets modulo K. If $\begin{pmatrix} * & * \\ q_1 C' & D \end{pmatrix} \in K_1$, then the matrix D is invertible modulo q_1, and therefore, since $q | q_1^2$, it has also an inverse D' modulo q. It follows that the pair $(q_1 C',\, D)$ is proportional modulo q to the pairs

$$\left(q_1 D' C',\, D' D\right) \equiv \left(q_1 C,\, E_n\right) \pmod{q},$$

which concludes the proof of the part (1).

Since all of the products

$$\begin{pmatrix} E & B \\ 0 & pE \end{pmatrix} \begin{pmatrix} E & 0 \\ q_1 C & E \end{pmatrix} \begin{pmatrix} E & B \\ 0 & pE \end{pmatrix}^{-1} = \begin{pmatrix} E + q_1 BC & -(q_1/p)BCB \\ qC & E - q_1 CB \end{pmatrix},$$

where $E = E_n$, and $B,\, C \in \mathbb{S}_n$, belong to the group K, it follows that

$$\Pi(p)\tau(p) = p^{-\langle n\rangle} \sum_{B,C\in\mathbb{S}/p\mathbb{S}} \left(K\begin{pmatrix} E & B\\ 0 & pE\end{pmatrix}\begin{pmatrix} E & 0\\ q_1C & E\end{pmatrix}\right)$$

$$= \sum_{B\in\mathbb{S}/p\mathbb{S}} \left(K\begin{pmatrix} E & B\\ 0 & pE\end{pmatrix}\right) = \Pi(p),$$

where $\mathbb{S} = \mathbb{S}_n$, which proves the part (2).

One can assume that all of the matrices C in (3-41) are divisible by p'. Then we have

$$p^{\langle n\rangle}\Pi(p')\tau(p) = \sum_{\substack{B\in\mathbb{S}/p'\mathbb{S},\\ C\in\mathbb{S}/p\mathbb{S}}} \left(K\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix}\begin{pmatrix} E & 0\\ q_1p'C & E\end{pmatrix}\right)$$

$$= \sum_{B,\,C} \left(K\begin{pmatrix} E+q_1p'BC & -q_1BCB\\ q_1(p')^2C & E-q_1p'CB\end{pmatrix}\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix}\right)$$

$$= p^{\langle n\rangle}\tau(p)\Pi(p'),$$

since the matrix

$$\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix}\begin{pmatrix} E & 0\\ q_1p'C & E\end{pmatrix}\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix}^{-1} = \begin{pmatrix} E+q_1p'BC & -q_1BCB\\ q_1(p')^2C & E-q_1p'CB\end{pmatrix}$$

belongs to K_1 and runs a complete system of representatives for $K\backslash K_1$, when C runs a set $\mathbb{S}/p\mathbb{S}$.

The part (4) easily follows from definitions.

□

In next section we shall see how the neutral rings work in singular theory.

§3.3. Unramified embeddings of local rings

A q-singular prime number p is said to be *unramified*, if it does not divide the number $q_1 = q/p$, otherwise it is called *ramified*. In this section we shall show that the Frobenius elements $\Pi(p)$ for unramified primes numbers p are invertible in an extension of the singular HS–ring $\mathcal{H}_q(K)$ of the group $K = \Gamma_0^n(q)$. This will allow us to define a natural homomorphic embeddings of the (regular) p-rings

$$\mathcal{H}_p(q_1) = \mathcal{H}_p^n(q_1) = HS\big(\Gamma_0^n(q_1),\, R_p(\Gamma_0^n(q_1))\big) \tag{3-42}$$

of the groups $\Gamma_0^n(q_1)$ into the extension. The embeddings replace parabolic embeddings of the regular theory and have a number of similar properties.

Lemma 3.13. *Let p be a nonramified prime divisor of q . Then the matrix*

$$H(p) = H^n(p,\, q) = \begin{pmatrix} apE_n & bE_n \\ qE_n & pE_n \end{pmatrix}, \tag{3-43}$$

where a, b are rational integers satisfying $ap - bq_1 = 1$, is a symplectic matrix with the multiplier $\mu(H(p)) = p$, which satisfies the following rules:

$$H(p)^2 = \gamma_p \cdot (pE_{2n}) \qquad \textit{with } \gamma_p \in K, \tag{3-44}$$

$$KH(p)K = H(p)K. \tag{3-45}$$

The *proof* is a routine exercise on multiplication of block matrices, which we leave to the reader.

Lemma 3.14. *Let p be a q–singular unramified prime number. Then the double coset*

$$\Omega(p) = \Omega^n(p,\, q) = \big(H^n(p,\, q)\big)_K \in \mathcal{H}_q(K) \tag{3-46}$$

has the following properties:

$$\Omega(p) = \big(KH(p)\big); \tag{3-47}$$

$$\Omega(p)^2 = [p], \tag{3-48}$$

where $[p]$ has the form (2-8)*;*

$$\Omega(p)^* = \Omega(p), \tag{3-49}$$

where star stands for the antiautomorphism (1-18)*;*

$$\Pi(p) = \Omega(p)\xi_n(p), \tag{3-50}$$

where $\Pi(p)$ and $\xi_n(p) = \xi_n^n(p)$ were defined by (3-2) *and* (3-31)*, respectively;*

$$\Omega(p)\Omega(p') = \Omega(p')\Omega(p), \tag{3-51}$$

if p' is another unramified prime;

$$\Omega(p)\Pi(p') = \Pi(p')\Omega(p), \tag{3-52}$$

if p' is a singular prime number different from p.

Proof. The decomposition (3-47) follows from (3-45). The relation (3-48) follows from (3-47) and (3-44). By definition of star map and (3-44), we have

$$\Omega(p)^* = \big(pH(p)^{-1}\big) = \big(\gamma_p H(p)\big) = \Omega(p).$$

By (3-47), (3-32), and (3-4), we get

$$\begin{aligned}\Omega(p)\xi_n(p) &= \sum_{B\in\mathbb{S}_n/p\mathbb{S}_n} \left(KH(p)M_n\begin{pmatrix} E_n & B\\ 0 & E_n\end{pmatrix}\right)\\ &= \sum_{B}\left(KH(p)M_n\begin{pmatrix} E & 0\\ 0 & pE\end{pmatrix}^{-1}\begin{pmatrix} E & B\\ 0 & pE\end{pmatrix}\right) = \Pi(p),\end{aligned}$$

since the matrix

$$H(p)M_n\begin{pmatrix} E & 0\\ 0 & pE\end{pmatrix}^{-1} = \begin{pmatrix} (a^2+bq_1)E & (ab+b)E\\ q(a+1)E & (q_1b+p)E\end{pmatrix},$$

where $E = E_n$ and $q_1 = q/p$, belongs to K.

Further, one can easily verify that the matrix $H(p)H(p')H(p)^{-1}H(p')^{-1}$ belongs to K, which implies (3-51).

Finally, one can easily check that the product

$$H(p)\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix} H(p)^{-1}\begin{pmatrix} E & B'\\ 0 & p'\end{pmatrix}^{-1}$$

with $B,\ B' \in \mathbb{S}_n$ belongs to the group K, if

$$B' \equiv aB - p^{-1}bE \pmod{p'}.$$

It follows that

$$\begin{aligned}\Omega(p)\Pi(p') &= \sum_{B\in\mathbb{S}_n/p'\mathbb{S}_n}\left(KH(p)\begin{pmatrix} E & B\\ 0 & p'E\end{pmatrix}\right)\\ &= \sum_{B'\in\mathbb{S}_n/p'\mathbb{S}_n}\left(K\begin{pmatrix} E & B'\\ 0 & p'E\end{pmatrix}H(p)\right) = \Pi(p')\Omega(p).\end{aligned}$$

□

Now we shall take a small break in order to remind a simple construction which we shall need later. If $\mathbb{A}$ is an associative ring with the unity element, and $a_1, \dots, a_r$

are not zero divisors belonging to the center of $\mathbb{A}$, then one can produce the smallest extension of $\mathbb{A}$, where all of the elements $a_1, \dots, a_r$ are invertible, using the standard procedure of localization with respect to the multiplicative system

$$S = \left\{a_1^{n_1} \cdots a_r^{n_r}; \quad n_1, \dots, n_r = 0, 1, \dots\right\}.$$

We shall denote the extension by

$$\mathbb{A}\left[S^{-1}\right] = \mathbb{A}\left[a_1^{-1}, \dots, a_r^{-1}\right].$$

(The notation has been already used in *Proposition 2.11.*)

Proposition 3.15. *Let p be a prime divisor of q not dividing the quotient q/p, then the Frobenius element $\Pi(p) = \Pi_K^n(p)$ is invertible in the extension*

$$\mathcal{H}_p'(K) = \mathcal{H}_p(K)\left[[p]^{-1}\right]$$

of the ring $\mathcal{H}_p(K)$, and

$$\Pi(p)^{-1} = [p]^{-1} \cdot \xi_n(p)^{-1} \cdot \Omega(p). \tag{3-53}$$

Proof. The statement follows from (3-50), (3-48), and *Lemma 3.11.*

□

With the help of the inverse Frobenius element (3-53) we are now going to define a homomorphism of the local p–subring $\mathcal{L}_p = \mathcal{L}_p^n$ of the triangular ring (2-28), where p is a q–singular unramified prime number, into an extension of the local p–ring of the group $K = \Gamma_0^n(q)$.

Let $X \in \mathcal{L}_p$. According to *Proposition 2.11*, "projections" $X \cdot \widehat{\Pi}(p)^d$ belongs to the centralizer $\widehat{C}_p$ of $\widehat{\Pi}(p)$ in $\mathcal{L}_p$,

$$X \cdot \widehat{\Pi}(p)^d \in \widehat{C}_p, \tag{3-54}$$

if d is sufficiently big. By *Theorem 3.3 (3), (4)*, the ring $\widehat{C}_p$ is the isomorphic image under the parabolic embedding (2-30) of the centralizer C_p of $\Pi(p) = \Pi_K(p)$ in the ring $\mathcal{S}_p(q)$,

$$j(C_p) = \widehat{C}_p,$$

and so there is unique element

$$i\left(X \cdot \widehat{\Pi}(p)^d\right) \in C_p, \tag{3-55}$$

where i stands for the inverse of j on $\widehat{C}_p$. We put then

$$\widetilde{X} = \Pi(p)^{-d} \cdot i\left(X \cdot \widehat{\Pi}(p)^d\right) \in C_p' = C_p\left[\Pi(p)^{-1}\right] \in \mathcal{H}_p'(K), \tag{3-56}$$

where $\Pi(p)^{-d} = \left(\Pi(p)^{-1}\right)^d$.

Theorem 3.16. *Let p be a q–singular unramified prime number, i.e. $p|q$, but $p^2 \nmid q$. Then the following assertions hold:*

(1) *For every $X \in \mathcal{L}_p = \mathcal{L}_p^n$ the element $\widetilde{X}$ defined by* (3-56) *is independent of the choice of $d \in \mathbb{N}$ satisfying* (3-54)*;*

(2) *The map*

$$X \to \widetilde{X} \in C_p\big[\Pi(p)^{-1}\big] \qquad (X \in \mathcal{L}_p) \tag{3-57}$$

is a $\mathbb{Q}$–linear ring homomorphism;

(3) *The restriction of the map* (3-57) *on the image $\widehat{\mathcal{H}}_p(q_1) \in \mathcal{L}_p$ of the local HS–ring* (3-42) *of the group $\Gamma_0^n(q_1)$ with $q_1 = q/p$ under the parabolic embedding* (2-30) *is an isomorphic embedding of the ring $\widehat{H}_p(q_1)$ into $C_p\big[\Pi(p)^{-1}\big]$.*

Proof. (1) If d_1 is another exponent satisfying (3-54), and, say, $d_1 > d$, then

$$\begin{aligned}\Pi^{-d_1} \cdot i(X\widehat{\Pi}^{d_1}) &= \Pi^{-d_1} \cdot i(X\widehat{\Pi}^{d} \cdot \widehat{\Pi}^{d_1-d}) = \Pi^{-d_1} \cdot i(\widehat{\Pi}^{d_1-d} \cdot i(X\widehat{\Pi}^{d}))\\ &= \Pi^{-d_1}\Pi^{d_1-d} \cdot i(X\widehat{\Pi}^{d}) = \Pi^{-d} \cdot i(X\widehat{\Pi}^{d}),\end{aligned}$$

where $\Pi = \Pi(p)$

(2) If X, $X_1 \in \mathcal{L}_p$, and d satisfies (3-54) both for X and X_1, then we have

$$\begin{aligned}\widetilde{XX_1} &= \Pi^{-2d} \cdot i(XX_1\widehat{\Pi}^{2d}) = \Pi^{-2d} \cdot i(X(X_1\widehat{\Pi}^{d})\widehat{\Pi}^{d})\\ &= \Pi^{-2d} \cdot i((X\widehat{\Pi}^{d}) \cdot (X_1\widehat{\Pi}^{d})) = \Pi^{-d} \cdot i(X\widehat{\Pi}^{d}) \cdot \Pi^{-d} \cdot i(X_1\widehat{\Pi}^{d}),\end{aligned}$$

since $i(X\widehat{\Pi}^d)$ belongs to C_p and therefore commutes with Π and Π^{-1}.

(3) If X is a nonzero element of the ring $\widehat{\mathcal{H}}_p(q_1)$, then $X\widehat{\Pi}(p)^d \neq 0$, by *Proposition 2.11* and (2-51), and so $\widetilde{X} \neq 0$, since the element $\Pi(p)^{-d}$ is not a zero divisor in $\mathcal{H}_p'(K)$.

□

It follows from the definition of parabolic embeddings and the last part of *Theorem 3.16*, that the map

$$T \to \widehat{T} \to \widetilde{T} \in C_p\big[\Pi(p)^{-1}\big] \qquad (T \in \mathcal{H}_p(q_1)) \tag{3-58}$$

is a composition of two isomorphic embeddings and therefore is an isomorphic embedding by itself. We shall say that the map (3-58) is *unramified embedding of the ring $\mathcal{H}_p^n(q_1)$* and its image

$$\mathcal{H}_p^n(q) = \mathcal{H}_p^n(q) = \widetilde{\mathcal{H}_p^n}(q_1) \tag{3-59}$$

will be called *the unramified (singular) p–ring of the group $K = \Gamma_0^n(q)$.*

Theorem 3.17. *Let p be a q–singular unramified prime number. Then the following assertions hold:*

(1) *Every element of the p–ring* (3-59) *commutes with every element of the regular reducible ring* (2-3)*;*

(2) *Every element of the p–ring* (3-59) *commutes with every element of others unramified p'–rings $\mathcal{H}_{p'}(q)$ as well as with every of singular Frobenius elements $\Pi(a)$ with $a|q^\infty$;*

(3) *The element $\Pi(p)$ satisfies the equation*

$$\sum_{j=0}^{m} \widetilde{q_j^n}(p)\Pi(p)^{m-j} = 0, \qquad (m = 2^n) \tag{3-60}$$

whose coefficients $\widetilde{q_j^n}(p) \in \mathcal{H}_p(q)$ are images under the map (3-58) *of the corresponding coefficients $q_j^n(p) \in \mathcal{H}_p(q_1)$ of the polynomial* (2-27) *with $q_1 = q/p$ in place of q; the coefficients $\widetilde{q_j^n}(p)$ satisfy the relations*

$$\begin{gathered} \widetilde{q_{m-i}^n}(p) = \big(p^{\langle n\rangle}[p]_K\big)^{(m/2)-i}\widetilde{q_i^n}(p), \qquad (0 \le i \le m), \\ \widetilde{q_0^n}(p) = [1]_K, \quad \widetilde{q_m^n}(p) = \big(p^{\langle n\rangle}[p]_K\big)^{m/2}. \end{gathered} \tag{3-61}$$

Proof. By *Theorem 2.3* and *Theorem 2.5*, it is sufficient to prove the part (1) for a local regular reducible ring $\mathcal{D}$ instead of $\mathcal{H}_{rr}(q)$. In this case it follows from *Proposition 2.12* that each element of $\mathcal{D}$ commutes with each element of C_p. In particular, it commutes with $\Pi(p)$ and so with $\Pi(p)^{-1}$. It follows that each element of $\mathcal{D}$ commutes with every element of the ring $C_p\big[\Pi(p)^{-1}\big]$, which contains the p–ring $\mathcal{H}_p(q)$. The part (1) is proved.

Since all of $\mathcal{H}_p(q)$, $\mathcal{H}_{p'}(q)$, and $\Pi(a)$ for unramified p, p', and $a|q^\infty$ are contained in a commutative extension of the ring C_q, the part (2) follows.

The relation (3-60) follows from (2-52) by applying to both parts the homomorphism (3-57). Similarly, the relations (3-61) follow from the corresponding relations for the coefficients of the polynomial (2-27), and obvious relations

$$\widetilde{[p^\delta]_{K_1}} = \widetilde{[p^\delta]_{\Gamma_0}} = [p^\delta]_K, \tag{3-62}$$

where $K_1 = \Gamma_0^n(q_1)$, and $\delta = 0, 1, \ldots$.

□

The unramified embeddings (3-58) and the homomorphisms (3-57) make it possible to transfer all of the factorizations of polynomials over local HS–rings of the group $\Gamma = \Gamma^n$ with factors over HS–rings $\mathcal{L}_p$ of the triangular subgroups, obtained, for example, in [An(87),§3.5], into corresponding factorizations of polynomials over

p–rings $\mathcal{H}_p(q)$ with factors over rings $C'_p = C_p\bigl[\Pi(p)^{-1}\bigr]$, if p is unramified. It is interesting to note that, although the order of factors over $\mathcal{L}_p$ is strictly fixed, the order of their images is not significant, since their coefficients belong to the commutative ring C'_p.

Let p be an unramified prime, and let

$$\widetilde{Q_p}(v) = \widetilde{Q_p^n}(v) = \sum_{i=0}^{m}(-1)^i\widetilde{q_i^n}(p)v^i \qquad (m = 2^n) \tag{3-63}$$

be the polynomial over the p–ring $\mathcal{H}_p(q)$, whose coefficients are images of corresponding coefficients of the polynomial (2-27) over $\mathcal{H}_p(q_1)$ under the unramified embedding. Then *Proposition 3.5.11* of [An(87)] implies the factorization

$$\widetilde{Q_p}(v) = Q'(v)([1] - \Pi(p)v),$$

where $Q'(v)$ is a polynomial of degree $2^n - 1$ over C'_p, which follows also from (3-60). For small n more explicit results can be obtained:

Proposition 3.18. *Let p be a q–singular unramified prime number, and let $n = 1$. Then the polynomial $\widetilde{Q_p^1}$ has the following factorization over the ring $(C_p^1)'$:*

$$\begin{aligned}\widetilde{Q_p^1}(v) &= [1] - \widetilde{T^1}(p)v + p[p]v^2\\ &= \bigl([1] - p[p]\Pi(p)^{-1}v\bigr)\bigl([1] - \Pi(p)v\bigr),\end{aligned} \tag{3-64}$$

where $[1] = [1]_K$, $[p] = [p]_K$ with $K = \Gamma_0^1(q)$, and where $T^1(p) \in \mathcal{H}_p^1(q_1)$ has the form (2-20)*. In particular, the middle coefficient $\widetilde{T^1}(p)$ can be written in the form*

$$\begin{aligned}\widetilde{T^1}(p) &= p[p]\Pi(p)^{-1} + \Pi(p)\\ &= (1-p)\Omega(p) + \Pi(p)^* + \Pi(p),\end{aligned} \tag{3-65}$$

where $\Omega(p) = \Omega^1(p, q)$ is the element (3-46)*, and where star stands for the antiautomorphism* (1-18)*.*

Proof. Applying the map (3-57) coefficient-wise to the factorization of $\widehat{Q_p^1}(v)$ given in *Proposition 3.5.13* of [An(87)], we get

$$\widetilde{Q}_p = \bigl([1] - \widetilde{\Pi}_0^1(p)v\bigr)\bigl([1] - \Pi(p)v\bigr),$$

which proves (3-64), since

$$\widetilde{\Pi}_0^1(p) = \Pi(p)^{-1}\cdot i\bigl(\Pi_0^1(p)\widehat{\Pi}(p)\bigr) = \Pi(p)^{-1}\cdot p[p],$$

by (3-62) and relation (3.4.13) of [An(87)]. The formulas (3-65) follow from (3-64), (3-53), and (3-39), since

$$\xi_1(p)\Omega(p) = \xi_1(p)^*\Omega(p)^* = \bigl(\Omega(p)\xi_1(p)\bigr)^* = \Pi(p)^*,$$

by (3-34) and (3-49).

□

For $n = 2$ formulas are more complicated:

Proposition 3.19. *Let p be a q–singular unramified prime number and $n=2$. Then the polynomial $\widetilde{Q}^2_p(v)$ has the following factorization over $C_p\big[\Pi(p)^{-1}\big]$:*

(3-66)
$$\begin{aligned}\widetilde{Q}^2_p(v) &= [1]-\widetilde{T}^2(p)v+\widetilde{q}_2(p)v^2-p^3[p]\widetilde{T}^2(p)v^3+p^6[p^2]v^4\\ &=\big([1]-p^3[p]\Pi(p)^{-1}v\big)\big([1]-p\Pi(p)^{-1}\Pi_1(p^2)v+p^3[p]v^2\big)\big([1]-\Pi(p)v\big),\end{aligned}$$

where $[p^\delta]=[p^\delta]_K$ *with* $K=\Gamma^2_0(q)$, $T^2(p)$ *and* $q_2(p)$ *were defined in* (2-20) *and* (2-26), *and where*

(3-67) $$\Pi_1(p^2)=\big(diag(p,1,p,p^2)\big)_K\in C_p.$$

Proof. It follows from the factorization of the polynomial $\widehat{Q}^2_p(v)$ given by *Proposition 3.5.14* of [An(87)], where $\Pi^{(2)}_{2,0}$ (a misprint) must be replaced by $\Pi^{(0)}_{2,0}$, that

$$\widetilde{Q}^2_p(v)=\big([1]-\widetilde{\Pi}_-v\big)\big([1]-\widetilde{\Pi}v+p(\widetilde{\Pi}^{(1)}_{2,0}+\widetilde{\Pi}^{(0)}_{2,0})v^2\big)\big([1]-\widetilde{\Pi}_+v\big),$$

where we have used the notation of the proposition. Using (3-56) and the relations (3.4.14), (3.5.23), and (3.5.25) of [An(87)], we obtain

$$\begin{aligned}\widetilde{\Pi}_- &= \Pi(p)^{-1}\cdot i(\Pi_-\Pi_+)=p^3[p]\Pi(p)^{-1},\\ \widetilde{\Pi} &= \Pi(p)^{-1}\cdot i(\Pi\Pi_+)=\Pi(p)^{-1}\cdot i(p\Pi^{(0)}_{1,1})=p\Pi(p)^{-1}\cdot\Pi_1(p^2),\\ \widetilde{\Pi}^{(1)}_{2,0}+\widetilde{\Pi}^{(0)}_{2,0} &= \Pi(p)^{-2}\cdot i(\Pi^{(1)}_{2,0}\Pi^2_+ +\Pi^{(0)}_{2,0}\Pi^2_+)=\Pi(p)^{-2}\cdot i(p^2[p]\Pi^2_+)=p^2[p],\end{aligned}$$

and

$$\widetilde{\Pi}_+=\Pi(p)^{-1}\cdot i(\Pi_+\Pi_+)=\Pi(p).$$

□

We shall say that an element T of a HS–ring of the group $K=\Gamma^n_0(q)$ is *symmetric* if it is invariant under the star map (1-18):

(3-68) $$T^*=T.$$

It looks likely that local p–rings $\mathcal{H}_p(q)$ in unramified cases consist of symmetric elements, as it was in regular cases according to *Theorem 2.3*. Since the rings $\mathcal{H}_p(q)$ together with $\mathcal{H}_p(q/p)$ are commutative polynomial rings, it would sufficient to check (3-68) for a set of generators, say, for

(3-69) $$\widetilde{T}(p)=\Pi(p)^{-1}\cdot i\big(\widehat{T}^n(p)\widehat{\Pi}(p)\big),\qquad \widetilde{T}^n_j(p^2)=\Pi(p)^{-2}\cdot i\big(\widehat{T}^n_j(p^2)\Pi(p)^2\big),$$

where $j=1,\dots,n$ (see *Theorem 2.6* for $\mathcal{H}^n_p(q/p)$). However, the check seems to be quite informal, requires detailed information on products of double cosets in the corresponding HS– rings, and extent of necessary computations grows tremendously with increase of n. Therefore we shall restrict ourselves only to the cases $n=1$ and $n=2$.

Proposition 3.20. *Let p be a q–singular unramified prime number. Then the p–rings $\mathcal{H}_p^1(q)$ and $\mathcal{H}_p^2(q)$ consist of symmetric elements.*

Proof. By (2-20) and (3-62), we have

$$\widetilde{T}_1^1(p^2) = [p]_{\Gamma_0^1(q)} \qquad \text{and } \widetilde{T}_2^2(p^2) = [p]_{\Gamma_0^2(q)},$$

which elements are clearly symmetric. The element $\widetilde{T}^1(p)$ is symmetric, by formulas (3-65) and (3-49), which concludes the story for $n = 1$. If $n = 2$, as we have seen, it is sufficient to show that elements

$$\widetilde{T}(p) = \widetilde{T}^2(p) \text{ and } \widetilde{q}_2(p) = p\widetilde{T}_1^2(p^2) + p(p^2+1)[p]_{\Gamma_0^2(q)} \tag{3-70}$$

(see (2-26)) are symmetric, which is far from being easy and requires more information on multiplication of certain double cosets in the ring

$$\mathcal{H}_p^2(q_1,\, q) = HS\big(K,\, \Sigma_p^2(q_1)\big), \tag{3-71}$$

where $K = \Gamma_0^2(q)$, $q_1 = q/p$, and

$$\Sigma_p^2(q_1) = \left\{ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Sigma_p^2; \quad C \equiv 0 \pmod{q_1} \right\}. \tag{3-72}$$

More concretely, we shall need formulas for products of double cosets of multiplier 1 by double cosets of multiplier 1 and p.

As to products of double cosets of multiplier 1, the cosets belong to the neutral subring $\mathcal{N}^2(q_1,\, q)$ of the ring (3-71) and, by *Lemma 3.10*, we have the formulas

$$\begin{gathered} \xi \cdot \xi_1 = \xi_1 \cdot \xi = p^2\xi_1 + (p^2-1)\xi, \\ \xi^2 = p^3[1] + p^2(p-1)\xi_1 + p^2(p-1)\xi, \end{gathered} \tag{3-73}$$

where $\xi_1 = \xi_1^2(p)$, $\xi = \xi_2^2(p)$ are the elements (3-31), which imply the relations

$$\xi^{-1}\xi_1 = \big((1-p^2)[1] + \xi_1\big)/p^2, \tag{3-74}$$

since

$$\xi\big((1-p^2)[1] + \xi_1\big)/p^2 = \big((1-p^2)\xi + p^2\xi_1 + (p^2-1)\xi\big)/p^2 = \xi_1.$$

In order to consider double cosets of multiplier p we have first to present in a convenient form representatives of all left cosets KM, where $M \in \Sigma_p^2(q_1)$ and

$\mu(M) = p$. For that one can multiply a system of representatives for cosets $K\backslash\Gamma_0^2(q_1)$ by a system of representatives for cosets

$$\Gamma_0^2(q_1)\backslash \left\{M \in \Sigma_p^2(q_1); \quad \mu(M) = p\right\}. \tag{3-75}$$

As to the first system, we shall take the system of representatives described in *Lemma 3.8*, that is the union of the three sets:$W^0 = \{E_4\}$,

$$W^1 = M_1 \left\{ \begin{pmatrix} \varepsilon & \delta \cdot {}^t\varepsilon^{-1} \\ 0 & {}^t\varepsilon^{-1} \end{pmatrix}; \varepsilon = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \delta = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}, \quad c, d \bmod p \right\}$$
$$= M_1 \cdot R_1,$$

and

$$W^2 = M_2 \left\{ \begin{pmatrix} E & B \\ 0 & E \end{pmatrix}; \quad B \in \mathbb{S}_2/p\mathbb{S}_2 \right\} = M_2 \cdot R_2,$$

where $E = E_2$,

$$M_1 = \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ q_1 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \text{and } M_2 = \begin{pmatrix} aE & bE \\ q_1 E & pE \end{pmatrix} \tag{3-76}$$

with a and b satisfying $ap - bq_1 = 1$.

Since p does not divide q_1, we could take, by *Lemma 2.1*, as representatives for the cosets (3-75) the set of triangular representatives for cosets

$$\Gamma_0^2\backslash \left\{M \in \Sigma_{0,p}^2; \quad \mu(M) = p\right\},$$

which can be described using *Lemma 3.3.32* and *Lemma 3.2.7* of [An(87)] as the union of three sets:

$$\{D_0\}, \quad D_1 \cdot R_1, \quad \text{and } D_2 \cdot R_2,$$

where

$$D_0 = diag(p,p,1,1), \quad D_1 = diag(1,p,p,1), \quad D_2 = diag(1,1,p,p).$$

But it will be more convenient for further calculations to modify the representatives on replacing the matrices D_0 and D_1 by matrices $D_0' = M_2 D_0$ and

$$D_1' = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} M_1 \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} D_1 = M_1' D_1 \quad \text{with } I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

respectively, where M_1 and M_2 are the matrices (3-76). Note that

$$D_0' = H(p) \quad \text{and } D_1' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & pa & 0 & b \\ 0 & 0 & p & 0 \\ 0 & q & 0 & p \end{pmatrix}, \tag{3-77}$$

where $H(p) = H^2(p, q)$ is the matrix (3-43) for $n = 2$.

If we multiply each of three sets of the chosen system of representatives for cosets $K\backslash\Gamma_0^2(q_1)$ by each of three sets of the modified system of representatives for cosets (3-75) and take into account formulas (3-77), we obtain a complete system of representatives of different left cosets of the set

$$\{M \in \Sigma_p^2(q_1); \quad \mu(M) = p\}$$

modulo K in the form of union of the following nine sets:

$$\begin{aligned} &S_1 = \{H\}, && S_2 = \{D_1' R_1\}, && S_3 = \{D_2 R_2\}, \\ &S_4 = \{M_1 R_1 H\}, && S_5 = \{M_1 R_1 D_1' R_1\}, && S_6 = \{M_1 R_1 D_2 R_2\}, \\ &S_7 = \{M_2 R_2 H\}, && S_8 = \{M_2 R_2 D_1' R_1\}, && S_9 = \{M_2 R_2 D_2 R_2\}. \end{aligned}$$

Let $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ be a matrix of Γ_0^n, then the matrices

$$H^{-1} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} H = \begin{pmatrix} apA + qB - bq_1 D & bA + pB - bD \\ -aqA - q_1 qB + aqD & -q_1 bA - qB + apD \end{pmatrix}$$

and

$$D_2^{-1} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} D_2 = \begin{pmatrix} A & pB \\ 0 & D \end{pmatrix}$$

belong to K. As to the matrix $(D_1')^{-1} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} D_1'$, one can easily check after routine multiplication of the matrices that it belongs to K if $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in R_2$ or

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in R_1' = \left\{ \begin{pmatrix} \varepsilon & \delta \cdot {}^t\varepsilon^{-1} \\ 0 & {}^t\varepsilon^{-1} \end{pmatrix}; \quad \varepsilon = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \delta = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}, c, d \bmod p \right\}.$$

Therefore we have the inclusions:

$$\begin{aligned} &S_1 \subset KHK, \quad S_2 \subset KD_1'K, \quad S_3 \subset KD_2K, \\ &S_4 = \{M_1 H H^{-1} R_1 H\} \subset KM_1 HK, \\ &S_6 = \{M_1 D_2 D_2^{-1} R_1 D_2 R_2\} \subset KM_1 D_2 K, \\ &S_7 = \{M_2 H H^{-1} R_2 H\} \subset KM_2 HK, \\ &S_8 = \{M_2 D_1' (D_1')^{-1} R_2 D_1' R_1\} \subset KM_2 D_1' K, \\ &S_9 = \{M_2 D_2 D_2^{-1} R_2 D_2 R_2\} \subset KM_2 D_2 K. \end{aligned} \tag{3-78}$$

As to the set S_5, we divide the set R_1 into the subset R_1' defined above and the complementary subset

$$R_1'' = \left\{ \begin{pmatrix} I & \delta I \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} E & \delta' \\ 0 & E \end{pmatrix}; \quad \delta' = I\delta I = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \quad d \bmod p \right\}.$$

Then we have

(3-79)
$$\begin{aligned} S_5 &= \{M_1 R_1' D_1' R_1\} \bigcup \{M_1 R_1'' D_1' R_1\} \\ &= \{M_1 D_1' (D_1')^{-1} R_1' D_1' R_1\} \bigcup \left\{ M_1 \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} D_1' (D_1')^{-1} \begin{pmatrix} E & \delta' \\ 0 & E \end{pmatrix} D_1' R_1 \right\} \\ &= S_5' \bigcup S_5'' \\ &\subset K M_1 D_1' K \bigcup K M_1 \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} D_1' K. \end{aligned}$$

On the other hand, if we multiply corresponding double cosets using decompositions (3-47), (3-32), (3-4), (3-50), and the relation

$$D_1' = HQM_1 \quad \text{with} \quad Q = H^{-1} D_1' M_1^{-1} = \begin{pmatrix} * & * \\ Q_{2,1} & * \end{pmatrix} \in K,$$

since $Q_{2,1} = \begin{pmatrix} -q(a+1) & 0 \\ 0 & 0 \end{pmatrix}$, we obtain the following decompositions:

$$\begin{aligned} &\Omega = (KH), && \Omega\xi_1 = \sum_{M \in S_2} (KM), && \Omega\xi = \sum_{M \in S_3} (KM), \\ &\xi_1\Omega = \sum_{M \in S_4} (KM), && \xi_1\Omega\xi_1 = \sum_{M \in S_5} (KM), && \xi_1\Omega\xi = \sum_{M \in S_6} (KM) \\ &\xi\Omega = \sum_{M \in S_7} (KM), && \xi\Omega\xi_1 = \sum_{M \in S_8} (KM), && \xi\Omega\xi = \sum_{M \in S_9} (KM), \end{aligned} \tag{3-80}$$

where $\Omega = \Omega^2(p, q)$ is the double coset (3-46), $\xi_1 = \xi_1^2(p)$ and $\xi = \xi_2^2(p)$ are the cosets (3-31). By comparing the decompositions (3-80) with inclusions (3-78) and (3-79), we get the relations

$$\Omega\xi_1 = (D_1')_K, \qquad \Omega\xi = (D_2)_K, \qquad \xi_1\Omega = (M_1 H)_K, \qquad \xi_1\Omega\xi = (M_1 D_2)_K,$$

$$\xi\Omega = (M_2 H)_K, \qquad \xi\Omega\xi_1 = (M_2 D_1')_K, \qquad \xi\Omega\xi = (M_2 D_2)_K,$$

and

$$\xi_1 \Omega \xi_1 = \Phi + \Psi, \tag{3-81}$$

where

$$\Phi = \sum_{M \in S_5'} (KM) = (P)_K, \quad \text{and } \Psi = \sum_{M \in S_5''} (KM) = (P')_K \tag{3-82}$$

with

$$P = M_1 D_1' = \begin{pmatrix} * & * \\ P_{2,1} & * \end{pmatrix}, \quad \text{and } P' = M_1 \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} D_1' = \begin{pmatrix} * & * \\ P_{2,1}' & * \end{pmatrix},$$

where

$$P_{2,1} = \begin{pmatrix} q_1 & 0 \\ 0 & q \end{pmatrix}, \qquad P_{2,1}' = \begin{pmatrix} 0 & q(a+p) \\ 0 & 0 \end{pmatrix}.$$

Note that the double cosets Φ and Ψ are different, since the blocks $P_{2,1}$ and $P_{2,1}'$ have different ranks modulo p.

With the knowledge of all ten double cosets of multiplier p of the ring (3-71) together with their decompositions into left cosets we can deduce all necessary properties of the double cosets. First of all, by (3-34) and (3-49), we have

$$\Phi^* + \Psi^* = \xi_1^* \Omega^* \xi_1^* = \xi_1 \Omega \xi_1 = \Phi + \Psi,$$

whence

$$\Phi^* = \Phi \quad \text{and } \Psi^* = \Psi, \tag{3-83}$$

since $\Phi^* \neq \Psi$, by the same reason that we have used to show that $\Phi \neq \Psi$. Verification of the following three relations is nothing else but a standard but tiresome exercise on multiplication of double cosets in HS–rings, which we leave to the reader:

$$\xi \Psi = p\Phi + (p-1)\xi\Omega\xi_1; \tag{3-84}$$

$$\Omega\Psi = \Psi\Omega; \tag{3-85}$$

$$\Pi_1(p^2) = \Omega\Phi, \tag{3-86}$$

where $\Pi_1(p^2)$ is the element (3-67). From (3-84) follows the relation

$$\xi^{-1}\Phi = (\Psi + (1-p)\Omega\xi_1)/p, \tag{3-87}$$

since

$$\xi(\Psi + (1-p)\Omega\xi_1)/p = (p\Phi + (p-1)\xi\Omega\xi_1 + (1-p)\xi\Omega\xi_1)/p = \Phi.$$

Finally, by (3-74), (3-87), and (3-81), we obtain

$$\begin{aligned}\xi^{-1}\Psi &= \xi^{-1}(\xi_1\Omega\xi_1 - \Phi) = ((1-p^2)[1] + \xi_1)\Omega\xi_1/p^2 - (\Psi + (1-p)\Omega\xi_1)/p \\ &= (\Phi + (1-p)\Psi + (1-p)\Omega\xi_1)/p^2.\end{aligned} \tag{3-88}$$

Returning to elements (3-70), we can now present them in symmetric form. By (3-66), we have

$$\begin{aligned}\widetilde{T}^2(p) &= p^3[p]\Pi^{-1} + p\Pi^{-1}\Pi_1(p^2) + \Pi \\ &= p^3\xi^{-1}\Omega + p\xi^{-1}\Omega^{-1}\Omega\Phi + \Omega\xi,\end{aligned}$$

where we have used the relations (3-53), (3-86), and (3-50). By (3-40) and (3-87), last expression can be rewritten in the form

$$\begin{aligned}\widetilde{T}^2(p) &= (\xi + (1-p)\xi_1 + (1-p)[1])\Omega + (\Psi + (1-p)\Omega\xi_1) + \Omega\xi \\ &= \xi\Omega + \Omega\xi + (1-p)(\xi_1\Omega + \Omega\xi_1) + \Psi + (1-p)\Omega,\end{aligned} \tag{3-89}$$

which is symmetric, by (3-34), (3-49), and (3-83). Again by (3-66), we have

$$\begin{aligned}\widetilde{q_2}(p) &= p^4[p]\Pi^{-1}\Pi^{-1}\Pi_1(p^2) + p\Pi^{-1}\Pi_1(p^2)\Pi + 2p^3[p] \\ &= p^4\xi^{-1}\Omega\xi^{-1}\Omega^{-1}\Omega\Phi + p\Omega\Phi + 2p^3[p],\end{aligned}$$

where we have used the relations (3-53), (3-48), (3-86), and *Theorem 3.3(4)*. By (3-87), (3-85), and (3-88), the last expression can be rewritten in the form

(3-90)

$$\begin{aligned}\widetilde{q_2}(p) &= p^3\xi^{-1}\Omega(\Psi + (1-p)\Omega\xi_1) + p\Omega\Phi + 2p^3[p] \\ &= p^3\xi^{-1}\Psi\Omega + p^3(1-p)[p]\xi^{-1}\xi_1 + p\Omega\Phi + 2p^3[p] \\ &= p(\Phi + (1-p)\Psi + (1-p)\Omega\xi_1)\Omega + p(1-p)[p]((1-p^2)[1] + \xi_1) \\ &+ p\Omega\Phi + 2p^3[p] \\ &= p(\Phi\Omega + \Omega\Phi) + p(1-p)(\Psi\Omega + \Omega\xi_1\Omega + [p]\xi_1) + p(p^3 + p^2 - p + 1)[p],\end{aligned}$$

which is symmetric, by (3-49), (3-83), (3-85), and (3-34).

□

Chapter 4

Old forms, new forms, eigenforms

In this chapter we shall define old and new cusp forms for the group $\Gamma_0^n(q)$ and prove, in particular, that the spaces of new forms of genus $n \leq 2$ are spanned by common eigenfunctions of all Hecke operators corresponding to elements of the regular reducible ring $\mathcal{H}_{rr}^n(q)$, of the singular unramified ring

$$\mathcal{H}_{su}^n(q) = \prod_{p|q, p^2\nmid q} \mathcal{H}_p^n(q) \tag{4-1}$$

generated by all singular unramified p–rings, and to all of the singular Frobenius elements $\Pi(a)$ (see *Theorem 4.15*). If $n = 1$, the result for regular operators belongs to Petersson (see [Pet(39)]); action of singular Frobenius elements was considered by Atkin and Lehner in [A-L(70)].

We restrict ourselves here only to the case of cusp forms. One can also consider old and new Eisenstein–Klingen series, but it is another story.

§4.1. Trace–idempotents

We shall intoduce here a simple but useful abstract tool.

Let G be a multiplicative group and $\Gamma \subset G$ a subgroup of finite index $\nu = [G : \Gamma]$. Let us consider the element of HS–ring $\mathcal{H} = HS_{\mathbb{Q}}(\Gamma, G)$ given by

$$\tau = \tau(\Gamma\backslash G) = \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (\Gamma g_i). \tag{4-2}$$

Lemma 4.1. *The element* (4-2) *satisfies the following rules:*

$$\tau g = \nu^{-1} \sum_{g_i \in \Gamma\backslash G} (\Gamma g_i g) = \tau, \qquad (g \in G) \tag{4-3}$$

$$\tau \cdot (g)_\Gamma = \tau \cdot \sum_{g_j \in \Gamma\backslash \Gamma g \Gamma} (\Gamma g_j) = \#(\Gamma\backslash \Gamma g \Gamma) \cdot \tau, \tag{4-4}$$

and $\tau^2 = \tau$.

Proof. Since $\{g_i g\}$ is just another system of representatives for $\Gamma\backslash G$, the relation (4-3) follows. The relation (4-4) is a consequence of (4-3). The last relation follows from (4-3) and definition of products in HS–rings.

□

We shall call the element $\tau = \tau(\Gamma\backslash G)$ *the trace–idempotent of the pair* (Γ, G)

Suppose now that the group G acts on a $\mathbb{Q}$–vector space V by linear operators

$$|g: \quad v \to v|g, \qquad (v \in V,\, g \in G)$$

satisfying

$$v|g|g' = v|gg' \qquad (v \in V,\, g, g' \in G).$$

Denote by $V(\Gamma)$ and $V(G)$ the subspaces of Γ–invariant and G–invariant elements of V, respectively. Then $V(G) \subset V(\Gamma)$, and HS–ring $\mathcal{H}$ acts on the space $V(\Gamma)$ by Hecke operators. Since the element (4-2) is an idempotent, it follows that the space $V(\Gamma)$ is the direct sum of subspaces

$$V_1(\Gamma) = V(\Gamma)|\tau, \qquad V_2(\Gamma) = \{v \in V(\Gamma); \quad v|\tau = 0\}:$$

$$V(\Gamma) = V_1(\Gamma) + V_2(\Gamma), \qquad V_1(\Gamma) \bigcap V_2(\Gamma) = \{0\}.$$

Lemma 4.2. $V_1(\Gamma) = V(G)$.

Proof. The inclusion $\subset$ follows from (4-3). The inverse inclusion is obvious.

□

Finally, let us assume that the space V is equipped with a nondegenerate Hermitian scalar product $(v,\, v')$ satisfying

$$(v|g,\, v') = (v,\, v'|g^{-1}) \qquad (v, v' \in V,\, g \in G).$$

Then the subspace $V_2(\Gamma)$ can be characterised as the orthogonal complement to the subspace $V(G)$ in $V(\Gamma)$:

Lemma 4.3. $V_2(\Gamma) = V(G)^{\perp} = \{v \in V(\Gamma); \quad (v,\, V(G)) = 0\}$.

Proof. Let $v \in V_2(\Gamma)$ and $v' = v'|\tau \in V(G) = V_1(\Gamma)$. Then we have

$$(v,\, v') = (v,\, v'|\tau) = \nu^{-1} \sum_{g_i \in \Gamma \backslash G} (v,\, v'|\tau g_i^{-1})$$
$$= \nu^{-1} \sum_{g_i \in \Gamma \backslash G} (v|g_i,\, v'|\tau) = (v|\tau,\, v') = 0,$$

and so $v \in V(G)^{\perp}$.Conversely, if $v \in V(G)^{\perp}$, then we have

$$(v|\tau,\, v|\tau) = \nu^{-1} \sum_{g_i \in \Gamma \backslash G} (v|\tau,\, v|g_i)$$
$$= \nu^{-1} \sum_{g_i \in \Gamma \backslash G} (v|\tau g_i^{-1},\, v) = (v|\tau,\, v) = 0,$$

and so $v|\tau = 0$.

□

Summing up, we obtain the following theorem:

Theorem 4.4. *With the above notation and assumptions, the subspace $V(G) \subset V(\Gamma)$ and its ortogonal complement $V(G)^{\perp}$ can be characterized by*

$$V(G) = V(\Gamma)|\tau(\Gamma\backslash G), \qquad V(G)^{\perp} = \{v \in V(\Gamma);\, , v|\tau(\Gamma\backslash G) = 0\}\,. \tag{4-5}$$

§4.2. Definition of old and new forms

We are considering the representation of the HS–ring $\mathcal{H}(K) = HS_{\mathbb{Q}}(K, \Sigma^n)$ of the group $K = \Gamma_0^n(q)$ on the space

$$\mathfrak{N} = \mathfrak{N}(q) = \mathfrak{N}_k^n(q) = \mathfrak{N}_k(K)$$

of cusp forms of a fixed integral weight k for the group K given by the Hecke operators (1-17) or normalized Hecke operators (1-20). For definiteness, we shall speak on the operators (1-17),although all the definitions, results and proofs (with relations (1-21) in place of *Theorem 1.9(2)*) remains valid also for normalized operators. The space $\mathfrak{N}$ is equipped with the Petersson scalar product (1-13), which is Hermitian, nondegenerate, and satisfies relations (1-14).

Let p be a prime divisor of q, and let $\Pi(p)$ and $\Pi^*(p)$ be the corresponding Frobenius element (3-2) and its dual with respect to the antiautomorphism (1-18). We shall define *the subspace of p–old forms* of $\mathfrak{N}$ by

$$\mathbf{O}_p = \mathbf{O}_k^n(q)_p = \sum_{i=0}^{m-1} \mathfrak{N}(q/p)|\Pi^*(p)^i, \qquad (m = 2^n), \tag{4-6}$$

if p is unramified (i.e. $p^2 \nmid q$), and by

$$\mathbf{O}_p = \mathbf{O}_k^n(q)_p = \mathfrak{N}(q/p) + \mathfrak{N}(q/p)|\Pi^*(p), \tag{4-7}$$

if p is ramified (i.e. $p^2|q$), where

$$\mathfrak{N}(q/p) = \mathfrak{N}_k(\Gamma_0^n(q/p)), \tag{4-8}$$

and $| = |_k$ stand for the Hecke operators (1-17).

Let

$$\tau(p) = \tau^n(p, q) = [K' : K]^{-1} \sum_{M_i \in K\backslash K'} (KM_i), \tag{4-9}$$

where $K' = \Gamma_0^n(q/p)$, be the trace–idempotent (4-2) of the pair (K, K'),then, by *Theorem 4.4*, we can write

$$\mathbf{O}_p = \sum_{i=0}^{m-1} \mathfrak{N}|\tau(p) \cdot \Pi^*(p)^i, \qquad (m = 2^n) \tag{4-10}$$

if p^2 does not divide q, and

$$\mathbf{O}_p = \mathfrak{N}|\tau(p) + \mathfrak{N}|\tau(p)\Pi^*(p), \tag{4-11}$$

if p^2 divides q.

The space

$$\mathbf{O} = \mathbf{O}_k^n(q) = \sum_{p \text{ prime}, p|q} \mathbf{O}_p \tag{4-12}$$

will be called *the (global) subspace of old forms* of $\mathfrak{N}$.

We shall define *the subspace* $\mathbf{N}_p$ *of p–new forms* and *the subspace* $\mathbf{N}$ *of (global) new forms* as orthogonal complements with respect to Petersson scalar product of the subspace of p–old forms and the subspace of old forms, respectively:

$$\mathbf{N}_p = \mathbf{N}_k^n(q)_p = \{F \in \mathfrak{N}; \quad (F, \mathbf{O}_p) = 0\}, \tag{4-13}$$

$$\mathbf{N} = \mathbf{N}_k^n(q) = \{F \in \mathfrak{N}; \quad (F, \mathbf{O}) = 0\}. \tag{4-14}$$

Then we have

$$\mathbf{N} = \bigcap_{p \text{ prime}, p|q} \mathbf{N}_p, \tag{4-15}$$

and, by *Theorem 4.4* and *Theorem 1.9(2)* each of the subspaces $\mathbf{N}_p$ can be presented in the form

$$\mathbf{N}_p = \left\{F \in \mathfrak{N}; \quad F|\Pi(p)^i\tau(p) = 0, \quad i = 0, 1, \dots, 2^n - 1\right\}, \tag{4-16}$$

if p^2 does not divide q, or in the form

$$\mathbf{N}_p = \{F \in \mathfrak{N}; \quad F|\tau(p) = 0, \quad F|\Pi(p)\tau(p) = 0\}, \tag{4-17}$$

if p^2 divides q.

§4.3. Invariant subspaces and eigenforms

Here we shall consider the questions of invariance of subspaces of old and new forms under Hecke operators and show that under certain conditions the subspaces of new forms are spanned by common eigenfunctions of the operators. We preserve the notation introduced in §4.2.

Lemma 4.5. *Let p and p' be two prime numbers, such that p divides q, but p' does not divide q. Then the following statements hold:*

(1) *The subspace $\mathfrak{N}(q/p) \subset \mathfrak{N}$ is invariant under each of the Hecke operators $|T$ with $T \in \mathcal{H}_{p'}(q)$;*

(2) *Every element of the ring $\mathcal{H}_{p'}(q)$ commutes with the Frobenius element $\Pi(p)$ and with its dual $\Pi^*(p)$.*

Proof. By *Theorem 2.6*, the rings $\mathcal{H}_{p'}(q)$ and $\mathcal{H}_{p'}(q/p)$ are isomorphic, and, if $T \in \mathcal{H}_{p'}(q)$, $T' \in \mathcal{H}_{p'}(q/p)$ is a pair of elements related by the isomorphism, then their images $\widehat{T}$ and $\widehat{T}'$ under parabolic embedding (2-30) coincide. It follows that

$$\begin{aligned}\mathfrak{N}(q/p)|T = \mathfrak{N}(q/p)|\widehat{T} &= \mathfrak{N}(q/p)\widehat{T}' \\ &= \mathfrak{N}(q/p)|T' \subset \mathfrak{N}(q/p),\end{aligned}$$

which proves the first part.

As to the second part, by *Proposition 2.12(1)*, we have

$$\widehat{\Pi T} = \widehat{\Pi}\widehat{T} = \widehat{T}\widehat{\Pi} = \widehat{T\Pi} \qquad (\Pi = \Pi(p))$$

for every $T \in \mathcal{H}_{p'}(q)$, whence $\Pi T = T\Pi$. It follows that

$$T^*\Pi^* = (\Pi T)^* = (T\Pi)^* = \Pi^* T^*,$$

which together with *Theorem 2.3* concludes the proof of the lemma.

□

Theorem 4.6. (1) *Each of the local subspaces $\mathbf{O}_p$ and $\mathbf{N}_p$ with $p|q$, as well as the global subspaces $\mathbf{O}$ and $\mathbf{N}$ are invariant under all of the Hecke operators corresponding to elements of the regular reducible ring $\mathcal{H}^n_{rr}(q)$ defined by* (2-3)*;*

(2) *Each of the listed subspaces is spanned by common eigenfunctions of all operators of the part* (1)*.*

Proof. By *Theorem 2.5*, it is sufficient to prove the theorem for a local ring $\mathcal{H}_{p'}(q)$ with $p' \nmid q$ instead of $\mathcal{H}^n_{rr}(q)$. It follows from *Lemma 4.5* and the definitions (4-6), (4-7) of subspaces of old forms, that every of $\mathbf{O}_p$ is invariant under $|T$ with $T \in \mathcal{H}_{p'}(q)$, and so does their sum (4-12). The invariance of $\mathbf{N}_p$ and $\mathbf{N}$ follows by (4-13), (4-14), (2-6), and *Theorem 1.9(2)*. The part (1) is proved.

By *Theorem 2.3* and *Theorem 1.9(2)*, the operators $|T$ with $T \in \mathcal{H}^n_{rr}(q)$ commute with each other and are selfadjoint. Since the space $\mathfrak{N}$ is finite–dimensional, the second part follows from the first one, by a well-known theorem of linear algebra.

□

Let us turn now to singular Hecke operators.

Proposition 4.7. *Let p be an unramified prime divisor of q. Then the relation*

$$F|\widetilde{T} = F|T \tag{4-18}$$

holds for every $F \in \mathfrak{N}(q/p)$ and every $T \in \mathcal{H}_p(q/p)$, where $T \to \widetilde{T}$ is the mapping (3-58). In particular, the space $\mathfrak{N}(q/p)$ is invariant under all of the Hecke operators correponding to elements of the unramified p–ring $\mathcal{H}_p(q)$.

Proof. It is sufficient to check the relations (4-18) for generators (3-69) of $\mathcal{H}_p(q)$. By the definition of elements $T^n(p)$ and $T_j^n(p^2)$ (see (2-20)), and *Proposition 2.11*, we have inclusions

$$\widehat{T}^n(p)\widehat{\Pi}(p), \quad \widehat{T}_j^n(p^2)\widehat{\Pi}(p)^2 \in \widehat{C}_p,$$

and so, by (3-56),

$$\widetilde{T}^n(p) = \Pi(p)^{-1} \cdot i\left(\widehat{T}^n(p)\widehat{\Pi}(p)\right), \quad \widetilde{T}_j^n(p^2) = \Pi(p)^{-2} \cdot \left(\widehat{T}_j^n(p^2)\widehat{\Pi}(p)^2\right).$$

Since Hecke operators on $\mathfrak{N}$ corresponding to elements $\widehat{T} \in \widehat{C}_p$ and $i(\widehat{T}) \in C_p$ clearly coincide, the relations (4-18) for the generators will follow from (2-49) and (2-50), if we can prove the formulas

$$F|\Pi(p)^{-1} = F|\Pi_+^{-1} \tag{4-19}$$

and

$$F|\Pi(p)^{-2} = F|\Pi_+^{-2} \tag{4-20}$$

for every $F \in \mathfrak{N}(q/p)$, where

$$\Pi_+^{-1}, \Pi_+^{-2} \in \mathcal{L}_p' = \mathcal{L}_p\left[[p]^{-1}\right]$$

are first "negative powers" of the Frobenius element $\Pi_+ = \widehat{\Pi}(p)$.

According to *Proposition 3.9*, we obtain the relations

$$F|\xi_n(p) = p^{\langle n \rangle}F, \qquad (F \in \mathfrak{N}(q/p))$$

which imply the relations

$$F|\xi_n(p)^{-1} = p^{-\langle n \rangle}F. \qquad (F \in \mathfrak{N}(q/p)) \tag{4-21}$$

Then, by (3-53) and (3-43), we get

$$\begin{aligned} F|\Pi(p)^{-1} &= F|[p]^{-1}\xi_n(p)^{-1}\Omega(p) \\ &= F|(p^{\langle n\rangle}[p])^{-1}\begin{pmatrix} aE_n & bE_n \\ (q/p)E_n & pE_n \end{pmatrix}\begin{pmatrix} pE_n & 0 \\ 0 & E_n \end{pmatrix} \\ &= F|(p^{\langle n\rangle}[p])^{-1}\begin{pmatrix} pE_n & 0 \\ 0 & E_n \end{pmatrix}, \end{aligned}$$

which is equal to $F|\Pi_+^{-1}$ (see, for example, [An(87), Exercise 3.5.7(3)]. We have proved the relations (4-19), which, in particular imply the inclusion

$$\mathfrak{N}(q/p)|\Pi_+^{-1} \subset \mathfrak{N}.$$

Let us show also that

$$\mathfrak{N}(q/p)|\Pi_+^{-2} \subset \mathfrak{N}. \tag{4-22}$$

By the definition of "negative powers" (see [An(87), §3.5]), we have

$$\Pi_+^{-2} = -\widehat{q_m}^{\,-1}\left(\sum_{i=1}^{m}(-1)^i\widehat{q_{m-i}^n}(p)\Pi_+^{i-2}\right),$$

where $m = 2^n$, and $\widehat{q_j^n}(p)$ are images under parabolic embedding of corresponding coefficients of the polynomial (2-27) over the ring $\mathcal{H}_p(q/p)$. It follows that

$$\begin{aligned} \mathfrak{N}(q/p)|\Pi_+^{-2} &\subset \sum_{i=1}^{m}\mathfrak{N}(q/p)|\widehat{q_m^n}(p)^{-1}\widehat{q_{m-i}^n}(p)\Pi_+^{i-2} \\ &\subset \mathfrak{N}(q/p)|\Pi_+^{-1} + \mathfrak{N}(q/p) + \sum_{i=3}^{m}\mathfrak{N}(q/p)|\Pi_+^{i-2} \\ &\subset \mathfrak{N}, \end{aligned}$$

since, by definitions and *Theorem 3.3*,

$$\mathfrak{N}(q/p)|\Pi_+^{d} = \mathfrak{N}(q/p)|\Pi(p)^{d} \subset \mathfrak{N},$$

if $d \geq 1$. We can prove now the relation (4-20). Let $F \in \mathfrak{N}(q/p)$. Set

$$F_1 = F|\Pi(p)^{-2}, \quad F_2 = F|\Pi_+^{-2}.$$

Since the operator $|\Pi(p)^{-2}$ maps the space $\mathfrak{N}$ into itself, it follows that $F_1 \in \mathfrak{N}$. By (4-22), we have inclusions $F_2 \in \mathfrak{N}$. Also

$$F_1|\Pi(p)^2 = F|\Pi(p)^{-2}\Pi(p)^2 = F,$$

and

$$F_2|\Pi(p)^2 = F|\Pi_+^{-2}|\Pi_+^2 = F|\Pi_+^{-2}\Pi_+^2 = F,$$

by (2-38), (3-4), the definition of Hecke operators, and relation (2-50) with $d = 2$ and $X = [1]$. Since the operator $|\Pi(p)^2$ is invertible on $\mathfrak{N}$, we conclude that $F_1 = F_2$. $\square$

We can now prove the following theorem:

Theorem 4.8. *Suppose that $n = 1$ or $n = 2$. Then the following asserions holds:*

(1) *Each of the local subspaces $\mathbf{O}_p$ and $\mathbf{N}_p$ with prime p dividing q, as well as the global subspaces $\mathbf{O}$ and $\mathbf{N}$ are invariant under all of the Hecke operators corresponding to elements of the singular unramified ring $\mathcal{H}^n_{su}(q)$ defined by* (4-1)*;*

(2) *Each of the listed subspaces is spanned by common eigenfunctions of all of the operators.*

Proof. According to *Theorem 3.17(2)* and (4-1), it is sufficient to prove the theorem for a local singular unramified ring $\mathcal{H}_{p'}(q)$ instead of $\mathcal{H}_{su}(q)$.

Let p be a singular prime number, and let $T \in \mathcal{H}_{p'}(q)$. Then $T^* = T$, by *Proposition 3.20*, and so, by *Theorem 3.17(2)*, we have $\Pi(p)T = T\Pi(p)$, and

$$T \cdot \Pi^*(p) = T^* \cdot \Pi^*(p) = (\Pi(p) \cdot T)^* = (T \cdot \Pi(p))^* = \Pi^*(p) \cdot T. \tag{4-23}$$

It follows from (4-23) and (4-6) or (4-7), that subspace $\mathbf{O}_p$ is invariant under operator $|T$, if the inclusions

$$\mathfrak{N}(q/p)|T \subset \mathfrak{N}(q/p) \qquad (T \in \mathcal{H}_{p'}(q)) \tag{4-24}$$

are valid. By *Proposition 4.7*, the inclusions are true,if $p' = p$. So we can assume that $p' \neq p$. By *Theorem 4.4*, for every singular prime number p we can write

$$\mathfrak{N}(q/p) = \mathfrak{N}|\tau(p), \tag{4-25}$$

where $\tau(p)$ is the trace–idempotent (4-9). On the other hand, every element $T \in \mathcal{H}_{p'}(q)$ has the form $T = \Pi(p')^{-d}T_1$ with $d \in \mathbb{N}$ and $T_1 \in C_{p'}$. By *Proposition 3.9(4)*, if p^2 does not divide q, and *Proposition 3.12(3)*, if p^2 divides q, we have

$$\tau(p)\Pi(p') = \Pi(p')\tau(p), \tag{4-26}$$

whence

$$\tau(p)\Pi(p')^{-1} = \Pi(p')^{-1}\tau(p). \tag{4-27}$$

It follows from (4-27) and (4-25) that

$$\mathfrak{N}(q/p)|\Pi(p')^{-d} = \mathfrak{N}|\tau(p)\Pi(p')^{-d} = \big(\mathfrak{N}|\Pi(p')^{-d}\big)|\tau(p) \subset \mathfrak{N}(q/p).$$

Since p' divides q/p, it follows from *Theorem 3.3* that every operator $|T_1$ with $T_1 \in C_{p'}$ maps the space $\mathfrak{N}(q/p)$ into itself. The inclusion (4-24) and the invariance of the subspace $\mathbf{O}_p$ follows. This implies the invariance of the subspace $\mathbf{O}$. The invariance of $\mathbf{N}_p$ and $\mathbf{N}$ follows by (4-13), (4-15), *Theorem 1.9(2)*, and *Proposition 3.20*. The part (1) is proved.

By *Theorem 3.17(2)*, the ring $\mathcal{H}^n_{su}$ is commutative. It follows then, by *Proposition 3-20*, that it consist of symmetric elements. The part (2) follows from *Theorem 1.9(2)*, by the same tautology, as end of the proof of *Theorem 4.6*.

□

Remark 4.9. *The same proof goes through without any changes for a given n, if one knows that all all of unramified local rings $\mathcal{H}^n_p(q)$ consist of symmetric elements.*

We turn now to Hecke operators corresponding to singular Frobenius elements (3-2).

Lemma 4.10. *Let p be an unramified prime divisor of q and $n = 1$ or $n = 2$. Then the subspaces $\mathbf{O}_p$ and $\mathbf{N}_p$ are both invariant under Hecke operators corresponding to elements $\Pi(p)^{\pm 1}$, $\Pi^*(p)^{\pm 1}$, $\xi_n(p)$, and $\Omega(p)$.*

Proof. By *Theorem 1.9(2)*, it is sufficient to consider only the case of subspace $\mathbf{O}_p$. By (4-6), we have

$$\mathbf{O}_p|\Pi^*(p) = \sum_{i=1}^{m} \mathfrak{N}(q/p)|\Pi^*(p)^i \subset \mathbf{O}_p + \mathfrak{N}(q/p)|\Pi^*(p)^m. \tag{4-28}$$

By *Theorem 3.17(2),(3)* and *Proposition 3.20*, we get the relation

$$\begin{aligned}\left(\sum_{j=0}^{m}(-1)^j\widetilde{q^n_j}(p)\Pi(p)^{m-j}\right)^* &= \left(\sum_{j=0}^{m}(-1)^j\Pi(p)^{m-j}\widetilde{q^n_j}(p)^*\right)^* \\ &= \sum_{j=0}^{m}\widetilde{q^n_j}(p)\Pi^*(p)^{m-j} = 0,\end{aligned} \tag{4-29}$$

where the coefficients $\widetilde{q_j^m}(p)$ belong to $\mathcal{H}_p(q)$. It follows then, by (3-61), that

$$\Pi^*(p)^m = -\sum_{j=1}^{m}(-1)^j\widetilde{q_j^n}(p)\Pi^*(p)^{m-j},$$

whence, by *Proposition 4.7*, we get

$$\begin{aligned}\mathfrak{N}(q/p)|\Pi^*(p)^m &\subset \sum_{j=1}^{m}\mathfrak{N}(q/p)|\widetilde{q_j^n}(p)\Pi^*(p)^{m-j}\\ &\subset \sum_{j=1}^{m}\mathfrak{N}(q/p)|\Pi^*(p)^{m-j} = \mathbf{O}_p,\end{aligned}$$

which together with (4-28) proves the invariance of $\mathbf{O}_p$ under $\Pi^*(p)$.

Since, by (3-50), (3-49), and (3-34), we have

$$\Pi^*(p) = (\Omega(p)\xi_n(p))^* = \xi_n(p)\Omega(p), \tag{4-30}$$

it follows from *Lemma 3.11* and (3-48) that the element $\Pi^*(p)$ is invertible and

$$\Pi^*(p)^{-1} = [p]^{-1}\Omega(p)\xi_n(p)^{-1}. \tag{4-31}$$

In particular, the inclusion $\mathbf{O}_p|\Pi^*(p) \subset \mathbf{O}_p$ implies the equalities

$$\mathbf{O}_p|\Pi^*(p) = \mathbf{O}_p, \qquad \mathbf{O}_p|\Pi^*(p)^{-1} = \mathbf{O}_p, \tag{4-32}$$

since we are only dealing with finite-dimensional spaces.

By (3-53), (3-39), and (3-40), we obtain the relations

$$p[p]\Pi(p)^{-1} = ((1-p)(\xi_0(p)+\xi_1(p)) + p\xi_1(p))\,\Omega(p), \tag{4-33}$$

if $n=1$, and the relation

$$p^3[p]\Pi(p)^{-1} = \big((1-p)(\xi_0(p)+\xi_1(p)+\xi_2(p)) + p\xi_2(p)\big)\Omega(p), \tag{4-34}$$

if $n=2$. By *Proposition 3.9*, we have the relation

$$\xi_0(p)+\xi_1(p)+\cdots+\xi_n(p) = \nu(p)\tau(p), \tag{4-35}$$

where $\nu(p) = \left[\Gamma_0^n(q/p) : \Gamma_0^n(q)\right]$ and $\tau(p)$ is the trace–idempotent (4-9). Then, by (4-33), (4-34), (4-35), (4-30), and (4-4), we get the relation

$$\begin{aligned}p^{\langle n\rangle}[p]\Pi(p)^{-1} &= (1-p)\nu(p)\tau(p)\Omega(p) + p\Pi^*(p)\\ &= c(p)\tau(p)\xi_n(p)\Omega(p) + p\Pi^*(p)\\ &= c(p)\tau(p)\Pi^*(p) + p\Pi^*(p)\end{aligned} \tag{4-36}$$

with a nonzero constant $c(p)$, valid for $n=1$ and $n=2$. (Unfortunately, it is not valid, if $n \geq 3$.) It follows from (4-36), (4-32), and (4-25), that

$$\begin{aligned}\mathbf{O}_p|\Pi(p)^{-1} &\subset \mathbf{O}|\tau(p)\Pi^*(p) + \mathbf{O}_p|\Pi^*(p)\\ &\subset \mathfrak{N}(q/p)|\Pi^*(p) + \mathbf{O}_p \subset \mathbf{O}_p,\end{aligned}$$

whence

$$\mathbf{O}_p|\Pi(p)^{-1} = \mathbf{O}_p, \qquad \mathbf{O}_p|\Pi(p) = \mathbf{O}_p. \tag{4-37}$$

By (4-6) and (4-5), we get

$$\mathbf{O}_p = \sum_{i=0}^{m-1} \mathfrak{N}(q/p)|(\Pi^*)^i = \sum_{i=0}^{m-1} \mathfrak{N}|\tau(\Pi^*)^i,$$

where $\tau = \tau(p)$ and $\Pi^* = \Pi^*(p)$, whence, by (4-32), we obtain

$$\begin{aligned}\mathbf{O}_p &= \mathfrak{N}|\tau(\Pi^*)^{-1} + \sum_{i=1}^{m-1} \mathfrak{N}|\tau(\Pi^*)^{i-1}\\ &= \mathfrak{N}|\tau\Omega\xi^{-1} + \mathfrak{N}|\tau = \mathfrak{N}|\tau\xi\Omega\xi^{-1} + \mathfrak{N}|\tau,\end{aligned}$$

if $n=1$, and

$$\begin{aligned}\mathbf{O}_p &= \mathfrak{N}|\tau\Omega\xi^{-1} + \mathfrak{N}|\tau + \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\xi\Omega\xi\Omega\\ &= \mathfrak{N}|\tau\xi\Omega\xi^{-1} + \mathfrak{N}|\tau + \mathfrak{N}|\tau\Omega + \mathfrak{N}|\tau\Omega\xi\Omega,\end{aligned}$$

if $n=2$, where $\xi = \xi_n(p)$, $\Omega = \Omega(p)$ and where we have used several times the relation (4-4). It follows, by (4-25), (4-31), and (3-50), that

$$\mathbf{O}_p|\xi = \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\xi = \mathfrak{N}(q/p)|\Pi^* + \mathfrak{N}(q/p),$$

if $n=1$, and

$$\begin{aligned}\mathbf{O}_p|\xi &= \mathfrak{N}|\tau\xi\Omega + \mathfrak{N}|\tau\xi + \mathfrak{N}|\tau\Omega\xi + \mathfrak{N}|\tau\Omega\xi\Omega\xi\\ &= \mathfrak{N}(q/p)|\Pi^* + \mathfrak{N}(q/p) + \mathfrak{N}(q/p)|\Pi + \mathfrak{N}(q/p)|\Pi^2,\end{aligned}$$

if $n=2$, where $\Pi = \Pi(p)$. In both cases these relations together with the relations (4-32) and (4-37) imply the inclusion $\mathbf{O}_p|\xi \subset \mathbf{O}_p$, and so the relations

$$\mathbf{O}_p|\xi = \mathbf{O}_p|\xi_n(p) = \mathbf{O}_p|\xi_n(p)^{-1} = \mathbf{O}_p, \tag{4-38}$$

since element $\xi = \xi_n(p)$ is invertible. Finally, by (4-32) and (4-38), we have

$$\mathbf{O}_p|\Omega(p) = \mathbf{O}_p|\xi_n(p)^{-1}\xi_n(p)\Omega = \mathbf{O}_p|\Pi^*(p) = \mathbf{O}_p. \tag{4-39}$$

The corresponding equalities for $\mathbf{N}_p$ follows by *Theorem 1.9(2).*

$\square$

Lemma 4.11. *Let p be an uramified prime number and $n = 1$ or $n = 2$. Then the Hecke operators $|\Pi(p)$ and $|\Pi^*(p)$ on the space $\mathbf{N}_p$ of p–new forms satisfy the following relations:*

$$F|\Pi(p) = F|\Pi^*(p) = -F|\Omega(p), \qquad (F \in \mathbf{N}_p) \tag{4-40}$$

if $n = 1$, and

$$F|\Pi(p)\Pi^*(p) = F|\Pi^*(p)\Pi(p) = p^2 F|[p], \qquad (F \in \mathbf{N}_p) \tag{4-41}$$

if $n = 2$.

Proof. If $n = 1$ and $F \in \mathbf{N}_p$, then, by (4-16), (4-35), and (3-50), we get the relations

$$F|\tau(p) = \nu(p)^{-1}F|(\xi_0(p) + \xi_1(p)) = 0,$$

and

$$F|\Pi(p)\tau(p) = F|\Omega(p)\xi_1\tau(p) = F|\Omega(p)p(\xi_0(p) + \xi_1(p)) = 0,$$

whence

$$F|\xi_1(p) = -F, \quad \text{and} \quad F|\Pi(p) = -F|\Omega(p).$$

On the other hand, by (4-30), we have

$$F|\Pi^*(p) = F|\xi_1(p)\Omega(p) = -F|\Omega(p).$$

But if $n = 2$, then, by (3-36) and (4-35), we can write

$$\xi_2(p)^2 = p^2(p-1)(\xi_0(p) + \xi_1(p) + \xi_2(p)) + p^2\xi_0(p) = p^2(p-1)\nu(p)^{-1}\tau(p) + p^2\xi_0(p),$$

whence, by (3-50), (4-30), and (3-38), we get

$$\begin{aligned} F|\Pi(p)\Pi^*(p) &= F|\Omega(p)\xi_2(p)^2\Omega(p) = F_1|\xi_2(p)^2\Omega(p) \\ &= p^2F_1|\Omega(p) = p^2F|\Omega(p)^2 = p^2F|[p], \end{aligned}$$

since $F_1 = F|\Omega(p) \in \mathbf{N}_p$, by previous lemma. Similarly,

$$F|\Pi^*(p)\Pi(p) = F|\xi_2(p)\Omega(p)^2\xi_2(p) = F|\xi_2(p)^2[p] = p^2F|[p].$$

$\square$

Lemma 4.12. *Let $n \in \mathbb{N}$ and let p, p' be two different prime divisors of q, where p^2 does not divide q. Then the following assertions hold:*

(1) *The Frobenius element $\Pi(p)$ and its dual $\Pi^*(p)$ commute both with $\Pi(p')$ and $\Pi^*(p)$;*

(2) *The subspaces $\mathbf{O}_{p'}$ and $\mathbf{N}_{p'}$ are invariant under operators $|\Pi(p)$ and $|\Pi^*(p)$.*

Proof. The elements $\Pi(p)$ and $\Pi(p')$ both belong to the commutative ring C_q and so commute. Hence, by duality, $\Pi^*(p)$ commutes with $\Pi^*(p')$. By (3-50) and (3-52), we obtain

$$\Omega(p)\xi_n(p)\Pi(p') = \Pi(p')\Omega(p)\xi_n(p) = \Omega(p)\Pi(p')\xi_n(p).$$

Since the element $\Omega(p)$ is invertible, it implies the relation

$$\xi_n(p)\Pi(p') = \Pi(p')\xi_n(p),$$

whence, by (4-30),

$$\Pi^*(p)\Pi(p') = \xi_n(p)\Omega(p)\Pi(p') = \xi_n(p)\Pi(p')\Omega(p) = \Pi(p')\Pi^*(p).$$

Element $\Pi(p)$ commutes with $\Pi^*(p')$ by duality. The first part is proved.

In order to prove the second part, it is sufficient, by (4-16), (4-17), and the above, to check that $\Pi(p)$ and $\Pi^*(p)$ both commute with the trace–idempotent $\tau(p')$, which is true, by *Proposition 3.9(4)*, if p^2 does not divide q, and by *Proposition 3.12(3)*, if p^2 divides q.

□

Lemma 4.13. *Let p, p' be two prime divisors of q and p^2 divides q. Then for every genus n the subspaces $BN_{p'}$ and $\mathbf{N}$ are invariant under the operator $|\Pi(p)$, and*

$$\mathbf{N}_p|\Pi(p) = \mathbf{N}|\Pi(p) = \{0\}. \tag{4-42}$$

Proof. Let us suppose first that $p' \neq p$. Then, since $\Pi(p)$ and $\Pi(p')$ commute, the invariance of $\mathbf{N}_{p'}$ follows from (4-16) and *Proposition 3.9(4)*, if p' is unramified, and from (4-17) and *Proposition 3.12(3)*, if p' is ramified.

It remains to prove (4-42). If $F \in \mathbf{N}_p$, then $F|\Pi(p)\tau(p) = 0$, by (4-17). On the other hand, $\Pi(p)\tau(p) = \Pi(p)$, by *Proposition 3.12(2)*. The relation (4-42) follows.

□

Theorem 4.14. *Let p be a prime divisor of q. Suppose that $n = 1$ or $n = 2$. Then the following assertions hold:*

(1) *Each of the local subspaces $\mathbf{N}_p$, as well as the global subspace $\mathbf{N}$ are invariant under all of the Hecke operators $|\Pi(p')$ for prime divisors p' of q and operators*

$|\Pi^*(p')$ for prime divisors p' of q not dividing q/p'. The operators on $\mathbf{N}$ commute with each other.

(2) *The operators $|\Pi(p)$ on $\mathbf{N}$ are selfadjoint, if $n = 1$, are normal, if $p^2 \nmid q$ and $n = 2$, and are equal to the zero operator, if $p^2|q$.*

(3) *The subspace $\mathbf{N}$ has a basis of common eigenfunctions of all Frobenius operators $|\Pi(p)$ with primes p dividing q and all dual operators $|\Pi^*(p)$ for prime divisors p of q not dividing q/p.*

Proof. The invariance of $\mathbf{N}_p$ under $|\Pi(p')$ and $|\Pi^*(p')$ for unramified p' was proved in *Lemma 4.10* and *Lemma 4.12*. The invariance of $\mathbf{N}_p$ under $|\Pi(p')$ for ramified p' was proved in *Lemma 4.13*. Since all of the Frobenius elements $\Pi(p')$ commute with each other, the rest of part (1) follows from *Lemma 4.11* and *Lemma 4.12(1)*.

The part (2) follows from *Lemma 4.11* and *Lemma 4.13*.

The part (3) is a consequence of parts (1) and (2) and well-known theorems of linear algebra.

□

Now we can join together all groups of operators considered in *Theorems 4.6, 4.8*, and *4.14* in order to obtain the following final theorem on eigenfunctions of Hecke operators on the subspace $\mathbf{N}$ of new forms of $\mathfrak{N}$.

Theorem 4.15. *The subspace*

$$\mathbf{N} = \mathbf{N}_k^n(q) \subset \mathfrak{N} = \mathfrak{N}_k(K)$$

of all new cusp forms of an integral weight k for the group $K = \Gamma_0^n(q)$, where $n = 1$ or $n = 2$, is invariant under all of the Hecke operators corresponding to elements of the regular reducible ring $\mathcal{H}_{rr}^n(q)$, of the singular unramified ring $\mathcal{H}_{su}^n(q)$, to all of the singular Frobenius elements $\Pi(p)$ with primes p dividing q, and all duals $\Pi^*(p)$ for prime divisors p of q not dividing q/p. The subspace is spanned by common eigenfunctions of the operators.

Proof. All of the operators are generated by local operators which can be divided into the following four groups of operators corresponding, respectively, to the elements

(i) $T \in \mathcal{H}_p(q)$ for primes p not dividing q;

(ii) $T \in \mathcal{H}_p(q)$ for primes p dividing q, but not dividing q/p;

(iii) $\Pi(p)$ for primes p dividing q;

(iv) $\Pi^*(p)$ for primes p dividing q, but not dividing q/p.

The invariance of the space $\mathbf{N}$ and the existence of basises of common eigenfunctions for all of the operators of each of the four groups is true by *Theorems 4.6, 4.8, 4.15*. So according to linear algebra, the only thing we have to check in order to conclude the proof is that the operators of different groups commute with each other. We have: elements of the groups (i) and (ii) commute, by *Theorem 3.17(1)*; elements of the groups (i) and (iii) commute, by *Proposition 2.12, Theorem 2.8*, and *Theorem 3.3*; it implies, by duality and *Theorem 2.3*, that elements of the groups (i) and (iv) commute; elements of the group (ii) and (iii) commute by *Theorem 3.17(2)*; it implies, by duality and *Proposition 3.20*, that elements of the groups (ii) and (iv) commute; finally, by *Theorem 4.14(1)*, the operators on $\mathbf{N}$ correspondig to elements of the groups (iii) and (iv) commute.

$\square$

Conclusion

Speaking on possible extension of the results on eigenfunctions, I should like to note that in order to extend *Theorem 4.8* to a genus $n > 2$, it would be sufficient to prove that rings $\mathcal{H}_p^n(q)$ consist of symmetric elements for all q–singular unramified prime numbers p. On the other hand, it is doubtful that the part of *Theorem 4.14* related to unramified primes can be generalized to a genus $n > 2$. The reason is that the relations (4-36) and (4-41) are not valid, if $n \geq 3$.

Perhaps, on considering not only Frobenius elements, one could tell more on ramified primes, than I did. It would be interesting for consideration of standard zeta functions for the groups $\Gamma_0^n(q)$ in ramified cases.

The first and foremost application of the results on eigenfunctions of Frobenius operators will be to extend my results obtained nearly 25 years ago in [An(74)] on spinor zeta functions of the group $\Gamma^2 = Sp_2(\mathbb{Z})$ to the case of the groups $\Gamma_0^2(q)$, which is our next task.

References

[An(69)]
Andrianov,A.N.: Rationality theorems for Hecke series and zeta–functions of the groups GL_n and Sp_n over local fields, Izvestia AN SSSR, ser. matem. 33 (1969), N 3, 466-505 (in Russian). English transl. in Math. USSR Izv. 3 (1969), 439-476.

[An(70)]
Andrianov,A.N.: Spherical functions for GL_n over local fields and summation of Hecke series, Matem. Sbornik, 83 (1970), N 3, 429-451 (in Russian). English transl. in Math. USSR Sbornik 12 (1970), N 3, 429-452.

[An(74)]
Andrianov,A.N.: Euler products that correspond to Siegel modular forms of genus 2, Uspekhi Matem. Nauk, 29 (1974), N 3(177), 43-110, (in Russian). English transl. in Russian Math. Surveys, 29 (1974), 45-116.

[An(87)]
Andrianov,A.N.: Quadratic forms and Hecke operators, Springer-Verlag, Berlin, Heidelberg, ..., 1987, 374 p. (Grundlehren Math. Wiss., Bd. 286).

[An-Z(90)]
Andrianov,A.N.; Zhuravlev,V.G.: Modular forms and Hecke operators, Nauka, Moskow, 1990, 447 p. (in Russian). The English edition: AMS, Providence, Rhode Island, Transl. of Math. Monographs, vol.145, 1995, 334 p..

[Ar(57)]
Artin,E.: Geometric algebra, Interscience Tracts vol.3, Interscience Publ., New York–London, 1957.

[A-L(70)]
Atkin,A.O.L.; Lehner,J.: Hecke Operators on $\Gamma_0(m)$, Math. Ann. 185 (1970), 134-160.

[He(37)]
Hecke,E.: Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Productentwicklung I,II, Math. Ann. 114 (1937), 1-28, 316-351.

[Li(75)]
Li,Wen-Ch'ing Winnie: New Forms and Functional Equations, Math. Ann. 212 (1975), 285-315.

[Ma(51)]
Maass,H.: Die Primzahlen in der Theorie der Siegelschen Modulfunktionen, Math. Ann. 124 (1951), 87-122.

[Mo(17)]
Mordell,L.J.: On Mr Ramanujan's empirical expansions of modular functions, Proc. Cambridge Phil. Soc. 19 (1917), 117-124.

[Pet(39)]
Petersson,H.: Konstruction der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichletreichen mit Eulerscher Produktentwicklung, I, II, III, Math. Ann. 116 (1939), 401-412, 117 (1939), 39-64, 117 (1940/41), 277-300.

[SM-T(93)]
Salvati Manni,R.; Top,J.: Cusp forms of weight 2 for the group $\Gamma_0(4, 8)$, Amer. J. of Math. 115 (1993), N 2, 455-486.

[Sa(63)]
Satake,I.: Theory of spherical functions on reductive algebraic groups over $\wp$–adic fields, Publ. Math. IHES, N 18 (1963).

[Sh(63)]
Shimura,G.: On modular correspondences for $Sp(n, \mathbb{Z})$ and their congruence relations, Proc. Nat. Acad. Sci. USA, 49:6 (1963), 824-828.

[Si(63)]
Siegel,C.L.: Lectures on analytical theory of quadratic forms, Buchhandlung Robert Peppmüller, Göttingen, 1963.

[Zha(75)]
Zharkovskaya,N.A.: On the connection between eigenvalues of Hecke operators and Fourier coefficients of eigenfunctions for Siegel's modular forms of genus n, Matem. Sbornik 96(138) (1975), 584-593. English transl. in Math. USSR Sbornik 25 (1975).