Master's Thesis

Discriminant forms and Hecke operators

– by Fabian Werner –

TU Darmstadt

University:	Darmstadt University of Technology
Department:	Mathematics
Subject group:	Algebra, Geometry and Functional analysis
Supervisor:	Prof. Dr. Nils Scheithauer

Erklärung an Eides Statt

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt habe. Ich habe alle Stellen, die ich aus den Quellen wörtlich oder inhaltlich entnommen habe, als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 15. September 2011

The latest version of this document is available at

`http://happy-werner.de/mthesis.pdf`

If there are any questions, comments or mistakes then do not hesitate to contact me:

`fw@cccmz.de`

Contents

Notation

Name/Symbol	Description	Page
RRS	System of **r**ight **r**epresentatives	2
R	Mostly a principal ideal domain (PID)	
K	Generally a field, later $K = \mathrm{Quot}(R)$, the quotient field of R	
$x \operatorname{modd} N$	The unique representative x' of $x + N\mathbb{Z}$ with $0 \leq x' < N$	
$(x_1, ..., x_n)$	A vector in K^n (i.e. $x_1, ..., x_n \in K$)	
$[v_1, ..., v_n]$	An ordered touple consisting of vectors in K^n (i.e. $v_1, ..., v_n \in K^n$)	
V	$= Kv_1 \oplus ... \oplus Kv_n$	
$\mathbf{Q_p}$	The p-adic rationals	
$\mathbf{Z_p}$	The p-adic integers, i.e. $\mathbf{Z_p} = \{x \in \mathbf{Q_p} \mid \|x\|_p \leq 1\}$	
ν	Either $\nu \in \mathbb{Z}$ is an exponent or $\nu : \mathbb{Q} \mapsto \mathbf{Q_p}$ is the embedding of fields	
$\mathbb{Z}_N$	$= \mathbb{Z}/N\mathbb{Z}$	
$A \sim_R B$	$\iff \exists C \in R^{n\times n}$ such that $C^{-1} \in R^{n\times n}$ and $C^T AC = B$	5
$A \textcircled{+} B$	$= \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$	5
R_{p^m}	$\alpha \in \mathbf{Z_p}, \alpha = \alpha_0 p^0 + \alpha_1 p^1 + ... \Rightarrow R_{p^m}(\alpha) = \alpha_0 + ... + \alpha_{m-1} p^{m-1} \in \mathbb{Z}$	6
$\left(\frac{x}{y}\right)$	The extended Jacobi-Legendre symbol	6
oddity	The oddity of a matrix	7
$\mathrm{symbol}_p(G)$	The Jordan symbol of a matrix G	8
$p^{\mathbb{N}_0}$	$= \{p^\nu \mid \nu \in \mathbb{N}_0\}$	
δ_{ij}	$= 1$ if $i = j$ and 0 otherwise	
Θ	$\Theta = \Theta_{(v,e)}$. Later, Θ denotes a fixed vector in $\mathbb{C}[D]$.	16
$\widetilde{\cdot}$	Whenever given a vector $x \in V$, $\widetilde{x}$ simply denotes $\Theta(x)$. Also, $\widetilde{X} := \{\widetilde{x} \mid x \in X\}$ for sets $X \subset V$.	
L_p	$= \mathbf{Z_p} e_1 \oplus ... \oplus e_n = \Theta(L) =\subset \widetilde{V} = {\mathbf{Q_p}}^n$	16
L'_p	$= \mathbf{Z_p}\Theta(v_1^*) \oplus ... \oplus \Theta(v_n^*)$	18
G_p	For a finite abelian group G, G_p denotes the p-component of G	20
$\mathbb{Q}^{(p)}$	The set of elements $q \in \mathbb{Q}$ having a p-power as their denominator	20
ϑ_p	$\vartheta_p : \mathbb{Q}^{(p)}/\mathbb{Z} \mapsto \mathbf{Q_p}/\mathbf{Z_p}, \vartheta_p(q + \mathbb{Z}) = \nu(q) + \mathbf{Z_p}$	20

$G = \mathbb{Z}_{a_1} g_1 \oplus ... \oplus \mathbb{Z}_{a_n} g_n$	This means that the map $\eta : \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n} \mapsto G, \eta(\overline{1}, \overline{0}, ..., \overline{0}) = g_1, \eta(\overline{0}, \overline{1}, ..., \overline{0}) = g_2, ...$ is a well-defined isomorphism	21
y_i^*	$= c_i v_i^*$ for $c_i = r_i^{-1} \operatorname{modd} p^{s_i} r_i \in \mathbb{Z}$, i.e. a finite basis for D_p	22
v_i^*	A basis of L' that serves as finite basis for D	23
v_i	$= v_i^{**}$, a basis of L	23
$\langle \cdot, \cdot \rangle$	A non-degenerate K-bilinear form on $V = K^n$	
$\langle \cdot, \cdot \rangle_{\mathbf{Q_p}}$	If $[v_1, ..., v_n]$ is a K-basis of V, then $e_i = \Theta(v_i) = \widetilde{v_i}$ form a $\mathbf{Q_p}$-basis of ${\mathbf{Q_p}}^n$ and the form $\langle \cdot, \cdot \rangle_{\mathbf{Q_p}}$ is the $\mathbf{Q_p}$-bilinear continuation of $\langle \widetilde{v_i}, \widetilde{v_j} \rangle := \nu(\langle v_i, v_j \rangle)$	
$(\cdot, \cdot)$	The finite $\mathbb{Z}$-bilinear form on L'/L	15, 24
$(\cdot, \cdot)_{\mathbf{Q_p}}$	The finite $\mathbf{Z_p}$-bilinear form on L_p'/L_p	15, 24
$[\![s]\!], \langle\!\langle s \rangle\!\rangle$	$[\![s]\!] = R_{p^N}(s)$ for N sufficiently large and $\langle\!\langle s \rangle\!\rangle = s - [\![s]\!]$	24
g_i^*	A finite basis of D_p that simplifies the structure of $(\cdot, \cdot)$	31
Φ	$\Phi : D_p \mapsto L_p'/L_p$, $\Phi(\sum_i k_i y_i^*) = \sum_i k_i c_i \widetilde{v_i^*}$ is an isomorphism of $\mathbb{Z}$-modules	26
$D(q^{\epsilon_q, n_q})$	A subgroup of D that is spanned by the dual vectors to the vectors that cause the factor q^{ϵ_q, n_q} in the Jordan symbol	36
$L(D)$, $E(D)$	Level and exponent of D	47
φ_D, χ_D	Dirichlet characters modulo N	53
$\mathbb{C}[D]$	The group ring of D	54
ρ	The Weil representation of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C}[D]$	55
$\mathrm{MF}_k(\Gamma)$	The set of modular forms for the subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ of weight $k \in \mathbb{Z}$	58
$\mathrm{MF}_k(\Gamma, \chi)$	The set of modular forms for the subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ that transform with character χ of weight $k \in \mathbb{Z}$	59
VVMF_k	The set of vector-valued modular forms of weight k w.r.t. the Weil representation	61
Ω, Ω_n	$\Omega_n := \{\alpha \in \mathbb{Z}^{2\times 2} \mid \det(\alpha) = n\}$, $\Omega = \cup_{n \in \mathbb{N}} \Omega_n$	63
$\mathcal{L}_H$	A map that produces vector-valued modular forms from scalar-valued ones	62
$T_{\mathcal{A}}$	Hecke operator on scalar-valued modular forms	65
$\mathcal{G}(N)$, $\mathcal{Q}(N)$	Groups	66
$T_{\mathcal{A}}^{(x)}$	Hecke operator on vector-valued modular forms	66
$(x)_\Gamma, [x]_\Gamma, [\![x]\!]$	equivalence relations on Ω	72

1 Introduction

The purpose of this thesis is twofold: The first goal is to establish some structural results on discriminant forms. Discriminant forms are finite algebraic quotients $D = L'/L$ of a dual lattice modulo a lattice together with a $\mathbb{Z}$-bilinear form. Although probably known to the community, these results have not been published in a clean and structured way. If the lattice satisfies some properties, one can define the so-called Weil representation of $\mathrm{SL}_2(\mathbb{Z})$ on the group ring $\mathbb{C}[D]$ of the discriminant form. Vector-valued functions $F : \mathbb{H} \mapsto \mathbb{C}[D]$ that transform under this representation are called vector-valued modular forms. Recently, Bruinier [Br] has defined Hecke operators on these functions. Scheithauer [Sch II] has constructed a lift that yields vector-valued modular forms from scalar-valued forms for different subgroups of $\mathrm{SL}_2(\mathbb{Z})$ (i.e. $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(N)$). Hecke operators for scalar-valued modular forms have been studied for a long time, cf. [Mi], [Ko] and [Ra]. The second goal is to prove the commutativity of the Hecke operators on vector-valued modular forms and the lift. The thesis is organized as follows: In Section 2 we are going to provide some preliminary results and notations, for example on the p-adic numbers which we will use subsequently. In Section 3 we will cite and deduce some results on matrices (mainly over the p-adic integers) in general which we will use in Section 4 to formally prove a certain structural theorem on discriminant forms; we shall prove that every discriminant form possesses a Jordan decomposition. This result was mentioned in [Ni] as Proposition 1.8.1 without a proof. We prove both, Proposition 1.7.1 (cf. Lemma 4.27, Thm. 4.28 and Thm. 4.30) and Proposition 1.8.1 (cf. Thm. 4.35 and Thm. 4.36) from [Ni] together with some additional properties. This section also concludes the first part of the thesis. The second part starts with Section 5 in which we will define the Weil representation and derive some results on two characters that are intertwined into this representation on the group ring of the discriminant form. We are going to recall the definition of scalar-valued modular forms and Hecke operators on such in Section 6. Furthermore, we will define vector-valued modular forms and extend the Weil representation following Bruinier [Br] in order to define Hecke operators on vector-valued modular forms. The main part of the second half of the thesis will be Section 7 in which we shall prove that the lift and the Hecke operators on vector-valued modular forms commute in a general setting. Subsequently we will apply this result to $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(N)$ in Sections 8, 9 and 10. We conclude by drawing a corollary from these results in Section 11: We show that under certain conditions, vector-valued Eisenstein series are eigenforms of the

Hecke operators on vector-valued modular forms.

2 Preliminary results

2.1 Notation. *Let X be a set and G be a group that acts on X by $(g,x) \mapsto g.x \in X$. On X we define an equivalence relation $x_1 \sim x_2 \iff \exists g \in G\ x_2 = g.x_1$. A system of G-right representatives (G-RRS for short) is a system of representatives for this equivalence relation, i.e. if for example, $\{x_1, ..., x_n\}$ is such a finite G-RRS then $X = G.x_1 \dot\cup ... \dot\cup G.x_n$.*

2.2 Notation. *Let $x \in \mathbb{Z}, y \in \mathbb{N}$. We set $\overline{x} := x \mod y := x + y\mathbb{Z}$. No index is given at the bar because it will be clear from the context which number is the modulus. Whenever we write $x \operatorname{modd} y$ we mean an arbitrary but fixed representative of the equivalence class $x + y\mathbb{Z}$.*

2.3 Definition. *Let $\{0\} \neq R$ be a ring with unit 1. A pair $(M, .)$ consisting of an abelian group M and a map $. : R \times M \mapsto M$ is called an R-module if the map "." satisfies the conditions:*

- $(r+s).m = r.m + s.m \quad \forall\ r, s \in R, \quad m \in M$
- $r.(m+m') = r.m + r.m' \quad \forall\ r \in R \quad m, m' \in M$
- $(r \cdot s).m = r.s.m \quad \forall\ r, s \in R, \quad m \in M$
- $1.m = m \quad \forall\ m \in M$

We will often write rm in place for $r.m$ and $Rm = \{r.m \mid r \in R\}$.

An R-module M is called finitely generated if there are $m_1, ..., m_n \in M$ such that $M = Rm_1 + ... + Rm_n$. It is called free of rank n if there are $m_1, ..., m_n \in M$ such that $M = Rm_1 \oplus ... \oplus Rm_n$ meaning that for every $m \in M$ there are $r_1, ..., r_n \in R$ such that $m = r_1m_1 + ... + r_nm_n$ and the r_i are uniquely determined by this property. In this case, $m_1, ..., m_n$ is called an R-basis of M. In general, an R-module may possess up to infinitely many different ranks but if R is commutative, then the rank n is uniquely determined (see [JS], Example VII.4.2 and Thm. VII.4.3).

2.4 Definition. *Let M, N be R-modules. A map $\phi : M \mapsto N$ is called an R-module homomorphism if $\phi(rm + sm') = r\phi(m) + s\phi(m')$ for all $r, s \in R$ and $m, m' \in M$. An R-module homomorphism ϕ is called an R-module isomorphism if it is bijective.*

2.5 Definition. *Let M, N be R-modules. A map $b : M \times M \mapsto N$ is called a symmetric R-bilinear form if for all $x, y, z \in M$, $r, s \in R$,*

- *b(r x + s y, z) = r b(x,z) + s b(y,z)*
- *b(x,y) = b(y,x)*

We want to associate problems concerning bilinear forms to problems on matrices over R. For this reason we assume that M is free and that $m_1, ..., m_n$ is an R-basis. We define the Gram matrix of b with respect to the this basis:

$$G := (b(m_i, m_j))_{i,j=1,...,n} \in N^{n \times n}$$

b is called non-degenerate if the homomorphism of R-modules

$$\Phi : M \mapsto \{\phi : M \mapsto N \mid \phi \text{ is a homomorphism of } R\text{-modules } \},$$
$$x \mapsto b(x, \cdot)$$

is injective. It is called unimodular if Φ is bijective.

An ordered set of vectors (mostly bases) will also be denoted as $[v_1, ..., v_n]$. We do not write this as $(v_1, ..., v_n)$ in order not to confuse touples of numbers in K (round brackets) with touples of vectors (squared brackets).

2.6 Notation. *For a vector $a = (a_1, ..., a_n) \in K^n$ and an ordered set of vectors $[v_1, ..., v_n]$ where $v_i \in K^n$ for all $1 \leq i \leq n$, we define*

$$a * v := (a_1, ..., a_n) * [v_1, ..., v_n] := \sum_{i=1}^{n} a_i v_i$$

When given a matrix $M = (m_{ij})_{i,j=1,...,n} \in K^{n \times n}$, we set

$$(M, i.row) = (m_{i1}, ..., m_{in})$$

and

$$(M, i.col) = (m_{1i}, ..., m_{ni})$$

This is the vector consisting of the i-th row (column respectively).

In view of the "$*$" operator we do not distinguish between row vectors and column vectors, i.e. $a^T * v = a * v = \sum_{i=1}^{n} a_i v_i$. A direct computation gives

2.7 Proposition. *(a) Let* $v_1, ..., v_n \in K^n$, $\Lambda = (\lambda_{ij})_{i,j=1,...,n} \in K^{n\times n}$ *and* $a_1, ..., a_n \in K$. *Then*

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} * \begin{bmatrix} (\Lambda, 1.col) * \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \\ \vdots \\ (\Lambda, n.col) * \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \end{bmatrix} = \left(\Lambda \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right) * \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

i.e. matrices in double "" operations can be pulled to the front.*

(b) Let $\langle \cdot, \cdot \rangle$ *be a* K*-bilinear form and* $v_1, ..., v_n \in K^n$ *and* $A, B \in K^{n\times n}$ *then for all* $1 \leq c, d \leq n$ *we have*

$$\langle (A, c.row) * \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, (B, d.row) * \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \rangle = (AGB^T)_{cd}$$

where $G = (\langle v_i, v_j \rangle)_{i,j=1,...,n}$.

Let V be a K-vector space of dimension n. The K-vector space $V^* := \{\phi : V \mapsto K \mid \phi \text{ is } K\text{-linear}\}$ is called the dual space of V.
We recall some basic facts about $\mathbf{Q_p}$ and $\mathbf{Z_p}$, the p-adic integers:

2.8 Theorem. *Let* $\alpha \in \mathbf{Z_p}$ *then there exists a uniquely determined sequence of integers* $(\alpha_n)_{n\in\mathbb{N}_0}$ *with* $0 \leq \alpha_n \leq p-1$ *such that*

$$\alpha = \sum_{n=0}^{\infty} \alpha_n p^n$$

The sum on the right converges absolutely in the norm $|\cdot|_p$ *on* $\mathbf{Q_p}$. *Further, for any* $\beta \in \mathbf{Q_p}$ *there are uniquely determined integers* N *and* $(\beta_n)_{n\geq N}$ *such that* $0 \leq \beta_n \leq p-1$, $\beta_N \neq 0$ *and*

$$\beta = \sum_{n\geq N} \beta_n p^n$$

The sum on the right converges absolutely and $\sum_{n=0}^{\infty} \beta_n p^n \in \mathbf{Z_p}$. *Summarized, every p-adic integer may be written as a unique "power series" in p and every* $\beta \in \mathbf{Q_p}$ *may be written as a unique "Laurent series" in p. Further,* $\beta \in \mathbf{Z_p}^{\times} \iff |\beta|_p = 1 \iff N = 0$

2.9 Corollary. *In particular, it follows that either* $\beta \in \mathbf{Z_p}$ *(if* $N \geq 0$*) or if* $N = -M$ *then*

$$\beta = \frac{\beta - M}{p^M} + ... + \frac{\beta - 1}{p^1} + \underbrace{\beta'}_{\in \mathbf{Z_p}} \in \frac{\beta - M + p\beta_{-M+1} + ... + p^{M-1}\beta_{-1}}{p^M} + \mathbf{Z_p}$$

so that $\mathrm{Quot}(\mathbf{Z_p})$ *is given by an isomorphic copy of* $\mathbf{Q_p}$ *which will we identify with each other henceforth.*

2.10 Corollary. *For every* $\alpha \in \mathbf{Z_p}$ *there exist unique* $e \in \mathbb{N}_0, \gamma \in \mathbf{Z_p}^\times$ *such that*

$$\alpha = p^e \gamma$$

Furthermore, for every $n \in \mathbb{N}_0$ *there exist unique* $k \in \mathbb{N}_0, \beta \in \mathbf{Z_p}$ *such that*

$$\alpha = k + p^n \beta$$

If $\alpha = \alpha_0 p^0 + \alpha_1 p^1 + ...$ *then* $k = \alpha_0 p^0 + \alpha_1 p^1 + ... + \alpha_{n-1} p^{n-1}$.

3 Results on quadratic forms,bilinear forms,matrices

A matrix X over some field K is called non-degenerate if $\det(X) \neq 0$.

3.1 Definition. *Let* K *be a field and* $R \subset K$ *be a subring. Two symmetric matrices* $A \in K^{n \times n}, B \in K^{n \times n}$ *are called equivalent over* R*, written* $A \sim_R B$ *if there exists a matrix* $S \in R^{n \times n}$ *such that* $S^{-1} \in R^{n \times n}$ *(or equivalently,* $\det(S) \in R^\times$ *by Cramer's rule) and*

$$S^T A S = B$$

The equivalence class of X *over* R *will be denoted as* $[X]_R$.

3.2 Notation. *For two matrices* $A \in K^{n \times n}, B \in K^{m \times m}$ *we denote by* $A \boxplus B$ *the* $(n+m) \times (n+m)$ *matrix*

$$A \boxplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

3.3 Lemma (and notation)**.** *Let* $p \in \mathbb{P}$ *and let* $M \in \mathbf{Z_p}^{n \times n}$ *be an arbitrary symmetric non-degenerate matrix. If* $p > 2$ *then there is a matrix* $S \in \mathbf{Z_p}^{n \times n}$ *with* $\det(S) \in \mathbf{Z_p}^\times$ *such that* $S^T M S = \mathrm{diag}(\alpha_1, ..., \alpha_n)$ *for some* $\alpha_1, ..., \alpha_n \in \mathbf{Z_p}$ *(in other words,* M *is equivalent to a diagonal matrix over* $\mathbf{Z_p}$*). If* $p = 2$ *then* G *can be "almost" diagonalized meaning that there is an* $S \in \mathbf{Z_2}^{n \times n}$ *with*

$\det(S) \in \mathbf{Z_2}^\times$ *and there are* 2×2*-matrices* $B_1, ..., B_f$ *and* $\alpha_1, ..., \alpha_{f'} \in \mathbf{Z_2}$ *such that* $S^T G S = B_1 \perp ... \perp B_f \perp \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$*. The block* B_i *has the following structure:*

$$B_i = \begin{pmatrix} q_i\alpha_i & q_i\beta_i \\ q_i\beta_i & q_i\gamma_i \end{pmatrix} = q_i \underbrace{\begin{pmatrix} \alpha_i & \beta_i \\ \beta_i & \gamma_i \end{pmatrix}}_{:=B_i'}$$

where $q_i = 2^{e_i}$ *and* $2 \mid \alpha_i,\ 2 \mid \gamma_i,\ 2 \nmid \beta_i,\ 2 \nmid \alpha_i\gamma_i - {\beta_i}^2$*. We write* $\alpha_i = p^{d_i}\beta_i$*,* $\beta_i \in \mathbf{Z_2}^\times$ *as in Cor. 2.10 and the whole notation for the diagonalization process shall be valid here and henceforth. For all* p*, the entries of the matrices* S *are rational in those of* M*, i.e. if* M *actually is in* $\operatorname{Im}(\nu)$*,* $\nu : \mathbb{Q} \mapsto \mathbf{Q_p}$ *the embedding of fields, then so is* S*.*

Proof. See [CS], chapter 15, §4.4, Theorem 2, Page 369. □

Note that we use the symbol β twice here but it will be clear from the context whether it will be the unit part of a diagonal element α or an entry in a 2×2-block. We now want to introduce a so-called Jordan-symbol which characterizes the p-adic equivalence class (in a certain way) of some symmetric matrix in $\mathbb{Q}^{n \times n}$.

3.4 Definition. *Let* $m \in \mathbb{N}, s \in \mathbf{Z_p}$ *and*

$$s = s_0 + s_1 p + s_2 p^2 + ... + s_m p^m + \widetilde{s} p^{m+1}$$

be its unique p*-adic expansion with* $\widetilde{s} = s_{m+1} + p s_{m+1} + ... \in \mathbf{Z_p}$*. We define*

$$R_{p^m}(s) := s_0 + s_1 p + ... + s_m p^m \in \mathbb{Z}$$

Using some computations in $\mathbf{Z_p}$ one can show the following:

3.5 Lemma. R_{p^m} *is additive and multiplicative in the sense that for* $s, t \in \mathbf{Z_p}$*,*

(a) $R_{p^m}(s+t) \equiv R_{p^m}(s) + R_{p^m}(t) \mod p^m$

(b) $R_{p^m}(st) \equiv R_{p^m}(s) R_{p^m}(t) \mod p^m$

so that $R_{p^m} : \mathbf{Z_p} \mapsto \mathbb{Z}_{p^m}$ *is a homomorphism of rings.*

3.6 Definition (Legendre-Jacobi-symbol)**.** *Let* $m, n \in \mathbb{Z}$ *so that there are* $p_1, ..., p_r \in \mathbb{P}$*,* $\epsilon, \delta \in \{+1, -1\}$ *and* $n_1, ..., n_r, m_1, ..., m_r \in \mathbb{N} \cup \{0\}$ *such that*

$$n = \epsilon p_1^{n_1} \cdots p_r^{n_r}, \quad m = \delta p_1^{m_1} \cdots p_r^{m_r}$$

We define

$$\gcd(m,n) := (-1)^{\min(\epsilon,\delta)} p_1^{\min(n_1,m_1)} \cdots p_r^{\min(n_r,m_r)} = (-1)^{\min(\epsilon,\delta)} \gcd(|n|,|m|)$$

If $\gcd(n,m) = +1$ *we define the Legendre-Jacobi Symbol to be*

$$m = p \in \mathbb{P} \Rightarrow \left(\frac{n}{m}\right) := \begin{cases} +1 & \text{if } \exists r \in \mathbb{Z} \text{ with } r^2 \equiv n \mod p \\ -1 & \text{otherwise} \end{cases}$$

$$m = 2 \Rightarrow \left(\frac{n}{2}\right) := \begin{cases} +1 & \text{if } n \equiv \pm 1 \mod 8 \\ -1 & \text{otherwise} \end{cases}$$

$$m = -1 \Rightarrow \left(\frac{n}{-1}\right) := +1$$

$$m = \delta p_1^{m_1} \cdots p_r^{m_r} \Rightarrow \left(\frac{n}{m}\right) := \left(\frac{n}{-1}\right)^{\delta} \left(\frac{n}{p_1}\right)^{m_1} \cdots \left(\frac{n}{p_r}\right)^{m_r}$$

Further, for $s \in \mathbf{Z_p}$ *we set*

$$\left(\frac{s}{p}\right) := \begin{cases} \left(\frac{R_8(s)}{2}\right) & \text{if } p = 2 \\ \left(\frac{R_p(s)}{p}\right) & \text{otherwise} \end{cases}$$

3.7 Definition. *Let* $p \in \mathbb{P}$. *Every* $\alpha \in \mathbf{Q_p}$ *can be uniquely written as* $\alpha = p^\nu \beta$ *with* $|\beta|_p = 1$ *and* $\nu \in \mathbb{Z}$. *We say that* α *is a p-adic antisquare if*

(i) ν *is odd*

(ii) $\left(\frac{\beta}{p}\right) = -1$

3.8 Notation. *We extend the set of "primes" to* $\overline{\mathbb{P}} = \{-1\} \cup \mathbb{P}$ *and write* $\mathbf{Q}_{-1} := \mathbb{R}$ *and* $\mathbf{Z}_{-1} := \mathbb{Z}$.

Let $x = \frac{a}{b} \in \mathbb{Q}$ such that $(b,p) = 1$ then we always put $x \mod 8 := a \cdot b^{-1} \mod 8$. It is easily checked that this map does not depend on the representative of q, i.e. if $q = \frac{c}{d}$, then $cd^{-1} \equiv ab^{-1} \mod 8$. In this sense we define

3.9 Definition. *Let* $p \in \overline{\mathbb{P}}$, $X \in {\mathbf{Q_p}}^{n \times n}$ *be a symmetric non-degenerate matrix. From linear algebra (e.g. see [Fi], p.325) we know that we can find a matrix* $V \in {\mathbf{Q_p}}^{n \times n}$ *(not necessarily* $V \in {\mathbf{Z_p}}^{n \times n}$*!),* $\det(V) \neq 0$ *with* $V^T X V = \operatorname{diag}(\alpha_1, ..., \alpha_n)$ *for some* $\alpha_1, ..., \alpha_n \in \mathbf{Q_p}$. *Write* $\alpha_i = p^{\nu_i} \beta_i$ *with*

$\nu_i \in \mathbb{Z}, \beta_i \in \mathbf{Z_p}^\times$ then we define the p-signature of X (with respect to V) as follows:

$$\mathrm{sig}_p(X) := \begin{cases} p^{\nu_1} + ... + p^{\nu_n} + 4m \mod 8 & \text{if } p \neq 2 \\ R_8(\beta_1) + ... + R_8(\beta_n) + 4m \mod 8 & \text{if } p = 2 \end{cases}$$

where $m = |\{i \in \{1, ..., n\} : \alpha_i$ is a p-adic antisquare$\}|$. Furthermore we define

$$p\text{–excess}(X) := \begin{cases} \mathrm{sig}_p(X) - n \mod 8 & \text{if } p \neq 2 \\ n - \mathrm{sig}_2(X) \mod 8 & \text{if } p = 2 \end{cases}$$

3.10 Notation. *The 2-signature of X will also be called oddity of X and the (-1)-signature is usually just called the signature of X.*

3.11 Remark. *The p-signature is an invariant under different diagonalization matrices V and it is an invariant of the equivalence class $[X]_{\mathbf{Q_p}}$. In other words, if $V, W \in \mathbf{Q_p}^{n\times n}$ are such that $\det(V) \neq 0, \det(W) \neq 0$, $V^T XV$ and $W^T XW$ both are diagonal then the quantities defined above coincide modulo 8 and if there are two matrices X, Y such that $X \sim_{\mathbf{Q_p}} Y$ then the quantities do also coincide modulo 8. For $p = -1$, this is called Sylversters law of inertia, see for example [Fi] p. 323. In the case $p \neq -1$, a proof can be found in [CS], chapter 15, §6. 6.1. and the first half of 6.2. To understand the table in 6.1 one should take a look at [Ca], Lemma 1.6 and the subsequent corollary.*

We define a formal product for a symmetric non-degenerate matrix $M \in \mathbf{Z_p}^{n\times n}$.

3.12 Definition (Jordan symbol)**.** *Let $p \in \mathbb{P}, p \neq 2, M \in \mathbf{Z_p}^{n\times n}$ be a symmetric non-degenerate matrix so that by Lemma 3.3 there is a non-degenerate matrix $S \in \mathbf{Z_p}^{n\times n}$ such that after resorting the diagonal entries according to their p-exponents, $S^T MS = p^0 M_{p^0} \perp p^1 M_{p^1} \perp p^2 M_{p^2} \perp ...$ for some quadratic matrices M_{p^ν} of size* $\mathrm{dimension}(M_q)$ *consisting of diagonal entries which are units in $\mathbf{Z_p}$. For $q = p^\nu$ we define*

$$\epsilon_q := \left(\frac{\det(M_q)}{p}\right), \quad n_q := \mathrm{dimension}(M_q)$$

To M, we assign the following formal product, the p-adic Jordan symbol (with respect to S):

$$\mathrm{symbol}_p(M) := \prod_{q \in p^{\mathbb{N}_0}} q^{\epsilon_q n_q}$$

If $p = 2$ and the matrix almost diagonalizes as in Lemma 3.3, i.e. there is a non-degenerate $S \in \mathbf{Z_p}^{n\times n}$ such that $S^T M S = 2^0 M_{2^0} \perp 2^1 M_{2^1} \perp ...$ where every M_{p^ν} is given by a direct sum of the form

$$M_{p^\nu} = B'_1 \perp ... \perp B'_{f_\nu} \perp \operatorname{diag}(\beta_1, ..., \beta_{f'_\nu})$$

each $B_j^{(\nu)}$ being a 2×2 block such that for $q = 2^\nu$, $\operatorname{dimension}(M_q) = 2f_\nu + f'_\nu$. Note that in the notation of the lemma, $B_i = q \cdot B'_i$ i.e. in B'_i, the leading power of 2 has already been canceled and the same applies to the α_i (β_i respectively). We assign the following formal product, the 2-adic variant of the Jordan symbol (with respect to S):

$$\operatorname{symbol}_2(M) := \prod_{q\in p^{\mathbb{N}_0}} q_{t_q S_q}^{\epsilon_q n_q}$$

where

- $\epsilon_q := \left(\frac{det(M_q)}{2}\right)$
- $n_q = \operatorname{dimension}(M_q) = 2f_\nu + f'_\nu$
- $S_q := \begin{cases} I & \text{if } f'_\nu = 0 \\ II & \text{otherwise} \end{cases}$
- $t_q := \operatorname{sig}_2(M_q) \in \mathbb{Z}_8$

3.13 Remark (and notation)**.** *For $i = 1, ..., k$ let $B_i = 2^\nu \left(\begin{smallmatrix} a_i & b_i \\ b_i & d_i \end{smallmatrix}\right)$ be matrices to the same 2-power that occur in the 2-adic diagonalization process of M. As then by Lemma 3.3, $2 \mid a_i, 2 \mid c_i$, there are only even entries on the diagonal of each $B'_i := 2^{-\nu} B_i$ so that parts of M of the form $M_q = B'_1 \perp ... \perp B'_k \perp \operatorname{diag}(\beta_1, ..., \beta_l)$ where $l = 0$ (i.e. parts that produce terms like $q_{.II}^{\vdots}$ in the Symbol) are called even blocks. Parts that produce terms like $q_{.I}^{\vdots}$ in the Symbol are called odd blocks. It would be somehow more convenient to call these blocks "mixed" blocks as there are even and odd entries on the diagonal. We will see in 3.18 why these blocks are called odd.*

3.14 Remark. *We have $\operatorname{sig}_2(B'_i) \equiv 0 \mod 8$ so that $\operatorname{sig}_2(M_q) \equiv 0 \mod 8$ for every even block M_q. Consequently, we write $q_{II}^{\epsilon_q, n_q}$ in place of the term $q_{0,II}^{\epsilon_q, n_q}$. We will also write q^{ϵ_q, n_q} in place of terms $q_{t_q, I}^{\epsilon_q, n_q}$ whenever the value of t_q is unimportant to us.*

Proof. This is an elementary computation that can be done by the reader by just using the definition of the oddity. One could also use Remark 3.11 together with Corollary 3.16. Then, the only thing one has to do is to verify the claim for two special matrices $D_{(+1)}$ and $D_{(-1)}$ (cf. Cor. 3.16). □

3.15 Theorem. *Let $p \in \mathbb{P}$, let $X, Y \in \mathbf{Z_p}^{n\times n}$ be symmetric non-degenerate matrices and take $S_X, S_Y \in \mathbf{Z_p}^{n\times n}$ as in Lemma 3.3 such that*

$$S_X^T X S_X = 2^0 X_{2^0} \perp 2^1 X_{2^1} \perp ... = \perp_{\substack{n\in\mathbb{N},\\ q=p^n}} qX_q$$

and

$$S_Y^T Y S_Y = 2^0 Y_{2^0} \perp 2^1 Y_{2^1} \perp ... = \perp_{\substack{n\in\mathbb{N},\\ q=p^n}} qY_q$$

with associated Jordan symbols

$$\text{symbol}_p(X) := \begin{cases} \prod_{q\in p^{\mathbb{N}_0}} q^{\epsilon_q n_q} & , p \neq 2 \\ \prod_{q\in p^{\mathbb{N}_0}} q_{t_q S_q}^{\epsilon_q n_q} & , p = 2 \end{cases}$$

$$\text{symbol}_p(Y) := \begin{cases} \prod_{q\in p^{\mathbb{N}_0}} q^{\delta_q m_q} & , p \neq 2 \\ \prod_{q\in p^{\mathbb{N}_0}} q_{f_q G_q}^{\delta_q m_q} & , p = 2 \end{cases}$$

(a) If $p \neq 2$, then

$$X \sim_{\mathbf{Z_p}} Y \iff \forall q \in p^{\mathbb{N}_0}, n_q = m_q \text{ and } \epsilon_q = \delta_q$$

(b) If $p = 2$, then let $Q := \{q = p^{n''} \mid n'' \in \mathbb{N}_0, \epsilon_q \neq \delta_q\}$, then

$$X \sim_{\mathbf{Z_2}} Y \iff \forall q \in p^{\mathbb{N}_0}, n_q = m_q, S_q = G_q$$
$$\text{and for each } n \in N_0 \text{ for which } X_{2^n} \text{ has type } S_{2^n} = II,$$
$$\sum_{\substack{0\le k\le n,\\ q':=2^k}} t_{q'} - f_{q'} \equiv 4 \left(\sum_{q''=p^{n''}\in Q} \min(n'', n) \right) \mod 8$$

Proof. The author believes that this is what is meant in [CS], chapter 15, §7, Theorems 9 and 10. Unfortunately, the result is not written down completely precise in [CS]. The reader should check the references given at the beginning of §7 in [CS]. □

From this theorem we draw a few corollaries:

3.16 Corollary. *Fix $p = 2$ and let $B = 2^n \left(\begin{smallmatrix} \alpha & \beta \\ \beta & \gamma \end{smallmatrix}\right) \in {\mathbf{Z_2}}^{2\times 2}$ one single 2×2 block as it occurs in Lemma 3.3. Let $B' = \left(\begin{smallmatrix} \alpha & \beta \\ \beta & \gamma \end{smallmatrix}\right)$ and $\epsilon = (\frac{\det(B')}{2})$. Set*

$$D_{(\epsilon)} := \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & , \epsilon = +1 \\ \\ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} & , \epsilon = -1 \end{cases} \tag{3.1}$$

then $B' \sim_{\mathbf{Z_2}} D_{(\epsilon)}$.

In case the reader does not accept the correctness of Thm 3.15 we refer to a direct proof that does not use this theorem: see [Wer IV] but be warned: it is a rather long and tedious computation.

Proof (using Thm. 3.15): The forms B' and $D_{(\epsilon)}$ satisfy the conditions of Theorem 3.15: Both matrices are in ${\mathbf{Z_2}}^{2\times 2}$, non-degenerate and symmetric. Both matrices decompose into a single Jordan constituent having a leading 2-power of $2^0 = 1$. The Jordan symbols of B' and $D_{(\epsilon)}$ are given by $\text{symbol}_2(B') = 1^{\epsilon,2}_{t,S}$ and $\text{symbol}_2(D_{(\epsilon)}) =: 1^{\delta,2}_{f,G}$. According to remark 3.14, $t \equiv 0 \mod 8$. The matrices $D_{(\pm 1)}$ particularly occur as "B'"-matrices for special choices of α, β, γ. Hence, it also follows from remark 3.14 that $f \equiv 0 \mod 8$. $G = S = II$ as there are only even entries along the diagonal of both matrices. We compute $\det\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \equiv -1 \equiv \pm 1 \mod 8$ and $\det\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \equiv 3 \not\equiv \pm 1 \mod 8$ so that $\delta = (\frac{\det(D_{(\epsilon)})}{2}) = \epsilon$ and consequently, in the language of Thm. 3.15, $Q = \emptyset$ so that

$$\sum_{\substack{0\le k\le n, \\ q':=2^k}} t_{q'} - f_{q'} \equiv \sum_{q=2^0} t - f \equiv 0 - 0 \equiv 0 \equiv 4 \underbrace{\left(\sum_{q''=p^{n''} \in \emptyset} \min(n'', n) \right)}_{\equiv 0} \mod 8$$

is satisfied. □

3.17 Corollary. *Let $M \in {\mathbf{Z_2}}^{n\times n}$ be symmetric and non-degenerate, then there exists a matrix $S \in {\mathbf{Z_2}}^{n\times n}$ such that $\det(S) \in {\mathbf{Z_2}}^{\times}$ and $H := S^T M S$ is of the form*

$$H = q_1 D_1 \perp ... \perp q_f D_f \perp \text{diag}(\alpha_1, ..., \alpha_{f'})$$

and every D_j is one of the matrices $D_{(\pm 1)}$ from equation (3.1)*, the $\alpha_i \in \mathbf{Z_2}$ are the ones from Lemma 3.3 and $q_i \in 2^{\mathbb{N}_0}$.*

Proof. By Lemma 3.3, there is a matrix $S \in {\mathbf{Z_2}}^{n\times n}$ such that $\det(S) \in {\mathbf{Z_2}}^\times$ and $H := S^T M S$ is of the form

$$H = B_1 \boxplus ... \boxplus B_f \boxplus \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$$

where $B_i = 2^{\nu_i} B_i'$. Put $\epsilon_i := (\frac{\det(B_i')}{2})$, then by 3.16 we obtain a matrix $W \in {\mathbf{Z_2}}^{2\times 2}, \det(W) \in {\mathbf{Z_2}}^\times$ such that $W^T B_1' W = D_{(\epsilon_1)}$. If we set

$$S' := W \boxplus I, \quad I = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \boxplus ... \boxplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{f-1 \text{ times}}$$

then $SS' \in {\mathbf{Z_2}}^{n\times n}$ and $\det(SS') = \det(S)\det(W) \in {\mathbf{Z_2}}^\times$ and $(SS')^T M SS' = 2^{\nu_1} D_{(\epsilon_1)} \boxplus B_2 \boxplus ... \boxplus B_f \boxplus \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$. If we put $D_j := D_{(\epsilon_j)}$ and proceed with $B_2, ..., B_f$ as we did with B_1, we obtain the decomposition claimed. □

3.18 Corollary. *Let $M \in {\mathbf{Z_2}}^{n\times n}$ be a symmetric, non-degenerate matrix, then there exists a matrix $S \in {\mathbf{Z_2}}^{n\times n}$ such that $\det(S) \in {\mathbf{Z_2}}^\times$ and $H := S^T M S$ is of the form $H = 2^0 H_{2^0} \boxplus 2^1 H_{2^1} \boxplus ...$ where for every $q \in 2^{\mathbb{N}_0}$, qH_q is of the form*

$$qH_q = qD_1 \boxplus ... qD_{f_q} \boxplus \operatorname{diag}(\alpha_1, ..., \alpha_{f_q'})$$

such that either $f_q = 0$ or $f_q' = 0$. Phrased differently, M decomposes into Jordan constituents that are either purely odd or purely even (but no mixture of both) in the sense of 3.13 and the 2×2-blocks are the $D_{(\pm 1)}$ from equation (3.1).

Proof. By the preceding corollary, M is $\mathbf{Z_2}$-equivalent to a matrix H of the form $H = 2^0 H_{2^0} \boxplus 2^1 H_{2^1} \boxplus ...$ where every qH_q is of the structure

$$qH_q = qD_1 \boxplus ... \boxplus qD_f \boxplus \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$$

Fix a q such that $f_q > 0$ and $f_q' > 0$ (i.e. this odd block of M is of type I but it still contains even parts). Consider the matrix

$$qH_q' = qE \boxplus ... \boxplus qE \boxplus \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$$

where $E = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then qH_q and qH_q' obviously satisfy the conditions of Theorem 3.15 (the second condition in the theorem is trivial as both form qH_q and qH_q' are of odd type!) so that $qH_q \sim_{\mathbf{Z_2}} qH_q'$. Processing every q in this way yields the result claimed. □

4 Discriminant forms

Every abelian group can be viewed as a $\mathbb{Z}$-module. In particular, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{Q}/2\mathbb{Z}$ are $\mathbb{Z}$-modules. We define the function

$$\text{half} : {}^{\mathbb{Q}}\!/_{2\mathbb{Z}} \mapsto {}^{\mathbb{Q}}\!/_{\mathbb{Z}}, \quad \text{half}(q + 2\mathbb{Z}) := q/2 + \mathbb{Z}$$

It is easy to see that half is an isomorphism of $\mathbb{Z}$-modules.

4.1 Definition. *Let D be a finite abelian group. A function $b(\cdot,\cdot) : D \times D \mapsto \mathbb{Q}/\mathbb{Z}$ that is a symmetric $\mathbb{Z}$-bilinear form in the sense of definition 2.5 is called a finite bilinear form. A function $q : D \mapsto \mathbb{Q}/2\mathbb{Z}$ is called a finite quadratic form if*

- $q(nx) = n^2 q(x) \ \ \forall\ n \in \mathbb{Z},\ x \in D$
- $b_q(x, y) := \text{half}(q(x + y) - q(x) - q(y))$ *is a finite $\mathbb{Z}$-bilinear form*

In this situation, b_q is called the associated bilinear form (to q).

Some authors define the term "finite quadratic form" in a different way: they require a map $Q : D \mapsto \mathbb{Q}/\mathbb{Z}$ that possesses the properties

- $Q(nx) = n^2 Q(x) \ \ \forall\ n \in \mathbb{Z},\ x \in D$
- $B_Q(x, y) := Q(x + y) - Q(x) - Q(y)$ is a finite $\mathbb{Z}$-bilinear form

Both definitions are similar in the sense that every Q induces a q and vice versa, i.e. in principal, both definitions coincide and just vary by a factor of 2 in the calculations.

4.2 Definition. *A discriminant form is a pair $(D, (\cdot,\cdot))$ such that D is a finite abelian group and $(\cdot,\cdot)$ is a non-degenerate finite bilinear form on D. A discriminant-quadratic form is a discriminant form that is equipped with a finite bilinear form q (or Q) which has $(\cdot,\cdot)$ as its associated finite bilinear form.*

Essentially, there is only one way to construct discriminant forms. They occur as quotients of lattices modulo some sublattice so we need to define the term lattice in order to give examples for such groups.

4.3 Definition. *Let R be a ring which is a principal ideal domain and K be a field extension of its quotient field. Let V be an n-dimensional K-vector space and $v = [v_1, ..., v_n]$ a basis. We define $\mathcal{L}_R(v) := Rv_1 \oplus ... \oplus Rv_n \subset V$.*

(a) A subset $L \subset V$ is called an R-lattice set if there is a K-vector space basis $v = [v_1, ..., v_n]$ such that $L = \mathcal{L}_R(v)$.

(b) A pair (L, b) consisting of an R-lattice set $L \subset V$ and a non-degenerate K-bilinear form $b : V \times V \mapsto K$ is called an R-lattice.

We will drop the prefix "R-" if R is determined by the context. (L, b) is said to be R-integral if $b(x, y) \in R$ for all $x, y \in L$. (L, b) is said to be R-even if $b(x, x) \in 2R$ for all $x \in L$. In the case that $K = \mathbb{R}, \mathbb{C}$ or $\mathbb{Q}$ we will always set $R := \mathbb{Z}$ and we will just write integral and even in place for $\mathbb{Z}$-integral and $\mathbb{Z}$-even.

4.4 Remark. *(a) The reason we want R to be a principal ideal domain is that the term "lattice" indicates some known results which do not hold if R is not a principal ideal domain. See, for example, [Ge], chapter 6.*

(b) Let L be R-even and let K have a characteristic unequal to 2, then

$$\begin{aligned} b(x, y) &= \frac{1}{2}\big(b(x + y, x + y) - b(x, x) - b(y, y)\big) \\ &\in \frac{1}{2}\big(2R + 2R + 2R\big) \subset R \end{aligned}$$

which implies that L is R-integral (provided it is R-even).

4.5 Notation. *If we want to have access to the basis of the lattice set L we write (L, v, G) and mean the lattice (L, b) where b is the K-bilinear form having a Gram matrix G with respect to the basis v.*

4.6 Lemma (and definition)**.** *Let $(L, b) = (L, v, G)$ be an R-lattice then we define the set $(L, b)'$ as*

$$(L, b)' := \{y \in V \mid b(x, y) \in R\}$$

For the sake of readability we drop the reference to the bilinear form if it is clear from the context which bilinear form is meant, i.e. we then write L' in place of $(L, b)'$. One can show that – if the Gram matrix of b is invertible – then L' is a lattice set given by $L' = \mathcal{L}_R(v^*)$ for the uniquely determined basis $v^* = [v_1^*, ..., v_n^*]$ with $\langle v_i^*, v_j \rangle = \delta_{ij}$. The i-th vector in this basis v_i^* is given by $v_i^* = (G^{-1}, i.col) * [v_1, ..., v_n]$. Using proposition 2.7(b), one can furthermore show that the Gram matrix of b w.r.t. the basis v^* is G^{-1} so if we endow L' with the same bilinear form b then the pair (L', b) (the triple (L', v^*, G^{-1}) respectively) is called the dual R-lattice.

If b is non-degenerate, then by simple linear algebra, the Gram matrix is invertible. One verifies that then, the homomorphism of R-modules

$$\begin{aligned}\Phi : L' &\mapsto \{\phi : L \mapsto K \mid \phi \text{ is a homomorphism of } R\text{-modules }\},\\ x &\mapsto b(x,\cdot)\end{aligned}$$

is bijective. Hence, L' can be seen as an isomorphic copy of a generalization $\mathrm{Hom}_R(L,K)$ of the dual vector space $V^* = \mathrm{Hom}_K(V,K)$. This is the reason why L' is called the dual lattice.
We give examples for discriminant forms:

4.7 Theorem. *Let R be a PID, K its quotient field and V a n-dimensional K-vector space. Let $(L,\langle\cdot,\cdot\rangle)$ be an R-lattice in V.*

(a) If $(L,\langle\cdot,\cdot\rangle)$ is R-integral, then $L \subset L'$ and $D = L'/L$ makes sense as algebraic quotient. The map $(\cdot,\cdot) : D \times D \mapsto \mathrm{Quot}(R)/R$,

$$(x+L, y+L) := \langle x, y\rangle + R$$

is a well-defined R-bilinear form.

(b) If $(L,\langle\cdot,\cdot\rangle)$ is R-even, the map $q : D \mapsto \mathrm{Quot}(R)/2R$,

$$q(x+L) := \langle x, x\rangle + 2R$$

is a well-defined R-quadratic form having $(\cdot,\cdot)$ as its associated bilinear form. In view of the remark after the definition of R-quadratic forms, we also have that

$$Q(x+L) := \frac{\langle x, x\rangle}{2} + \mathbb{Z}$$

is a well-defined R-quadratic form having $(\cdot,\cdot)$ as its associated R-bilinear form.

(c) If $K = \mathbb{Q}$, $R = \mathbb{Z}$, and (L,b) is an integral lattice (in particular $L \subset L'$) then $D := L'/L$ is a finite abelian group of size $|L'/L| = |\det(G)|$. The map $(\cdot,\cdot)$ on D from (a) *is non-degenerate so that L'/L is a discriminant form. If additionally, L is even, then the maps q,Q from* (b) *are well-defined and the associated bilinear form is $(\cdot,\cdot)$ from* (a).

The proof is left to the reader.
Two discriminant forms $(D_1, b_1(\cdot,\cdot)), (D_2, b_2(\cdot,\cdot))$ are called isomorphic as discriminant forms if there exists an isomorphism of finite abelian groups

$\Phi : D_1 \mapsto D_2$ such that $b_2(\Phi(x), \Phi(y)) = b_1(x, y)$ for all $x, y \in D_1$. Whenever there exist finite quadratic forms q_1, q_2 such that the associated bilinear form of q_j is b_j then they are called isomorphic as discriminant forms with quadratic form if there exists an isomorphism Φ as above that satisfies $q_2(\Phi(x)) = q_1(x)$ for all $x \in D_1$. The examples given above are the only occurrences of discriminant forms:

4.8 Theorem. *Let D be a discriminant form, then there exists an integral lattice $(L, \langle \cdot, \cdot \rangle)$ such that $D \cong L'/L$ as a discriminant form. If additionally, there exists a finite quadratic form on D then there exists an even lattice $(L, \langle \cdot, \cdot \rangle)$ such that $D \cong L'/L$ as discriminant form with finite quadratic form.*

Proof. See [Wa]. □

4.9 Remark. *Let D be a given discriminant form. Choose a $\mathbb{Z}$-lattice L such that $L'/L \cong D$ as discriminant forms. By adding unimodular even lattices of dimension 8 and splitting off hyperbolic planes (bilinear forms of dimension 2 having a Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$) we obtain a new lattice M such that $M'/M \cong D$ still holds (adding unimodular even lattices and splitting off hyperbolic planes does not alter the discriminant form of a lattice) but now, M is positive definite meaning that its bilinear form satisfies $b_M(x, x) > 0$ or equivalently, its Gram matrix is equivalent to the matrix* diag *(1,1,...,1) over $\mathbb{R}$.*

In view of this theorem and the remark we may always assume $D = L'/L$ for a suitable positive definite $\mathbb{Z}$-lattice.

Now, we want to define a "$\mathbf{Z_p}$-version" of our lattice, i.e. we want to admit $\mathbf{Z_p}$-linear combinations of the v_i. The idea is to define the object $\mathbf{Q_p}v_1 \oplus ... \oplus \mathbf{Q_p}v_n$ but the question is how to understand the symbol v_i in this context, i.e. if $L = \mathbb{Q}v_1 \oplus \mathbb{Q}v_2 \subset \mathbb{R}^2$ and $v_1 = (\sqrt{2}, \pi)$ then we wonder how to understand v_1 as an Element of $\mathbf{Q_p}^2$? Consequently we have to render this object more carefully in order to obtain a precise semantic:

4.10 Definition. *Let V be an n-dimensional $\mathbb{Q}$-vector space. For any pair $(v, \widetilde{w})$ where $v = [v_1, ..., v_n]$ is any basis of V and $\widetilde{w} = [\widetilde{w_1}, ..., \widetilde{w_n}]$ is any $\mathbf{Q_p}$-basis of the $\mathbf{Q_p}$-vector space $\mathbf{Q_p}^n$, we define a $\mathbb{Q}$-linear embedding of $\mathbb{Q}$-vector spaces*

$$\Theta_{(v,\widetilde{w})} : \mathbb{Q}v_1 \oplus ... \oplus \mathbb{Q}v_n \mapsto \mathbf{Q_p}^n, \quad \Theta_{(v,\widetilde{w})}(\sum_{i=1}^{n} \lambda_i v_i) = \sum_{i=1}^{n} \nu(\lambda_i)\widetilde{w_i}$$

where $\nu : \mathbb{Q} \mapsto \mathbf{Q_p}$ is the embedding of fields. Let $(L, b) = (L, v, G)$ be a $\mathbb{Z}$-lattice in V. Let $e := [e_1, ..., e_n]$ be the usual standard basis of ${\mathbf{Q_p}}^n$, i.e. $e_1 = (1, 0, ..., 0), e_2 = (0, 1, 0, ..., 0)$ and so forth. Let $\Theta := \Theta_{(v,e)}$ be the $\mathbb{Q}$-linear embedding of $\mathbb{Q}$-vector spaces

$$\Theta : \mathbb{Q}v_1 \oplus ... \oplus \mathbb{Q}v_n \mapsto {\mathbf{Q_p}}^n, \quad \Theta(v_i) := e_i$$

In $\widetilde{V} := {\mathbf{Q_p}}^n$, we then define the $\mathbf{Z_p}$-latticeset

$$L_p := \mathbf{Z_p}e_1 \oplus ... \oplus \mathbf{Z_p}e_n$$

i.e. $L_p = \Theta(L)$. We endow ${\mathbf{Q_p}}^n$ with a $\mathbf{Q_p}$-bilinear form $\widetilde{b}$ induced by $\widetilde{b}(e_i, e_j) := \nu(G_{ij})$ therefore turning L_p into a $\mathbf{Z_p}$-lattice. For the sake of readability we rename e_i in ${\mathbf{Q_p}}^n$ to $\widetilde{v}_i$. We will also write b again in place of $\widetilde{b}$ and G_{ij} in place for $\nu(G_{ij})$.

4.11 Remark. *Let R be a PID, K its quotient field and V be an n-dimensional K-vector space. Let (L, v, G) be an R-lattice and let $w = [w_1, ..., w_n]$ be another basis of V. Then there exist $\lambda_{ij}, \sigma_{ij} \in K$ with the property that*

$$w_i = \sum_{j=1}^{n} \lambda_{ij} v_j \text{ and } v_i = \sum_{j=1}^{n} \sigma_{ij} w_j$$

Set $\Lambda := (\lambda_{ij})_{i,j=1,...,n}$ and $\Sigma := (\sigma_{ij})_{i,j=1,...,n}$. Then $\Lambda^{-1} = \Sigma$ and

$$\begin{aligned} w \text{ is another basis of } L &\iff \mathcal{L}_R(w) = L = \mathcal{L}_R(v) \\ &\iff \Lambda \in R^{n \times n} \text{ and } \Sigma \in R^{n \times n} \end{aligned}$$

Let w be such a second basis for L, then $\{\Theta(w_1), ..., \Theta(w_n)\}$ is another basis for L_p because for any $x = \sum_{i=1}^{n} \alpha_i e_i$ with $\alpha_i \in \mathbf{Z_p}$ we have

$$x = \sum_{i=1}^{n} \alpha_i e_i = \sum_{j=1}^{n} \sum_{i=1}^{n} \alpha_i \sigma_{ij} \Theta(w_j)$$

so that $L_p \subset \text{span}_{\mathbf{Z_p}}(\Theta(w_1), ..., \Theta(w_n))$ and the other direction is proven similar. Furthermore, the $\Theta(w_i)$ are $\mathbf{Q_p}$-linearly independent, because: From linear algebra over general fields K, one knows that vectors $\widetilde{w}_1, ..., \widetilde{w}_n$, where $\widetilde{w}_i = \sum_{j=1}^{n} k_{ij} e_j$ for some $k_{ij} \in K$, are linearly independent if and only if the matrix $\kappa := (k_{ij})_{i,j=1,...,n}$ is invertible. In our case, $\kappa = \nu(\Sigma)$ and $K = \mathbf{Q_p}$. Since $\Lambda\Sigma = Id$ holds in $\mathbb{Q}^{n \times n}$, we may apply the homomorphism (of fields!) ν to this equation and obtain that $\nu(\Sigma)\nu(\Lambda) = \nu(Id) = Id$ in ${\mathbf{Q_p}}^n$ where we identify $0, 1$ with $\nu(0)$ and $\nu(1)$.

4.12 Remark. *Let $(L, \langle\cdot,\cdot\rangle)$ be an R-lattice with $V \subset K^n$. Chose an arbitrary K-vector space basis $v_1, ..., v_n$ such that $L = Rv_1 \oplus ... \oplus Rv_n$ and put $G = (G_{ij})_{i,j=1,...,n} := (\langle v_i, v_j\rangle)_{i,j=1,...,n}$ to be the Gram matrix with respect to this basis. Let $x = \sum_i r_i v_i \in L$ then since*

$$\langle x, x\rangle = \sum_i r_i \langle v_i, v_i\rangle + \boxed{2} \sum_{i,j} r_i r_j \langle v_i, v_j\rangle$$

we see that L is even if and only if $G \in R^{n\times n}$ and $G_{ii} \in 2R$ for all i. For $R = \mathbb{Z}$ this implies in particular:

$$L \text{ even } \Rightarrow L_p \ \mathbf{Z_p}\text{-even}$$

Proof. Since L is even, $G \in \mathbb{Z}^{n\times n}$ and $G_{ii} \in 2\mathbb{Z}$ (i.e. $G_{ii} = 2h_{ii}$) so that "Gram-matrix of L_p " $= \nu(G) \in \mathbf{Z_p}^{n\times n}$ is such that $\nu(g_{ii}) = 2\nu(h_{ii}) \in 2\mathbf{Z_p}$. □

Let $(L, \langle\cdot,\cdot\rangle)$ be a $\mathbb{Z}$-lattice in the n-dimensional $\mathbb{Q}$-vector space V, then L' is a $\mathbb{Z}$-lattice too. Thus, we could use the above definition to obtain a $\mathbf{Z_p}$-version of L' too. For two reasons we do not proceed in this way: Firstly, if we proceeded in that way, the result would always be that $L_p = L'_p$ as sets but if this was not the case in V then this is an unwanted side effect. Secondly we want the $\mathbf{Z_p}$-version of L' to be the actual dual lattice of L_p in the sense of definition 4.6. We therefore put

4.13 Definition.

$$L'_p := \mathbf{Z_p}\Theta(v_1^*) \oplus ... \oplus \mathbf{Z_p}\Theta(v_n^*)$$

and endow this with the same bilinear form $\langle\cdot,\cdot\rangle_{\mathbf{Q_p}}$ (that computes everything with respect to the basis $\widetilde{v}_1, ..., \widetilde{v}_n$) that we used for L_p therefore turning L'_p into a $\mathbf{Z_p}$-lattice. Note that in contrast to definition 4.10, we do not use $\Theta_{(v^*,e)}$ here but rather the same $\Theta = \Theta_{(v,e)}$ that was used for the definition of L_p. Then we have the funny law

4.14 Lemma. $L'_p = (L_p)'$

Proof. As the assertions in 4.6 hold over general fields (in particular $\mathbf{Q_p}$), there exists a basis $\widetilde{w}_1, ..., \widetilde{w}_n$ which is dual to $\widetilde{v}_1, ..., \widetilde{v}_n$ with $(L_p)' = \mathbf{Z_p}\widetilde{w}_1 \oplus ... \oplus \widetilde{w}_n$. We claim that the $\widetilde{w}_i$ are given by the $\widetilde{v}_i^* := \Theta(v_i^*)$. Indeed, let $v_i^* =$

$\sum_{j=1}^n \lambda_{ij} v_j$ for some $\lambda_{ij} \in \mathbb{Q}$ and $\widetilde{v}_i := \Theta(v_i)$ then $\Theta(v_i^*) = \sum_{j=1}^n \nu(\lambda_{ij})\Theta(v_j)$ so that

$$\begin{aligned}
\widetilde{b}(\widetilde{v}_i^*, \widetilde{v}_k) &= \sum_{j=1}^n \nu(\lambda_{ij})\widetilde{b}(\widetilde{v}_i, \widetilde{v}_k) \\
&= \sum_{j=1}^n \nu(\lambda_{ij})\nu(b(v_i, v_k)) \qquad \text{(definition of } \widetilde{b}) \\
&= \nu\left(\sum_{j=1}^n \lambda_{ij} b(v_i, v_k)\right) \\
&= \nu(b(v_i^*, v_k)) = \nu(\delta_{ik}) = \delta_{ik}
\end{aligned}$$

Hence, the $\Theta(v_i^*)$ form some dual basis for the $\Theta(v_i)$ but this basis is unique due to Lemma 4.6 so that $\widetilde{w}_i = \Theta(v_i^*)$ (i.e. $\Theta(v_i)^* = \Theta(v_i^*)$) and

$$(L_p)' = \mathbf{Z_p}\widetilde{w}_1 \oplus ... \oplus \mathbf{Z_p}\widetilde{w}_n = \mathbf{Z_p}\widetilde{v}_1^* \oplus ... \oplus \mathbf{Z_p}\widetilde{v}_n^* = L_p'$$

□

4.15 Remark. *Let (L, v, G) be an integral $\mathbb{Z}$-lattice in an $\mathbb{Q}$-vector space V of dimension n and take $L_p, L_p' = (L_p)'$ as above, then $L_p \subset L_p'$ so that the quotient L_p'/L_p makes sense as an algebraic quotient of abelian groups. As L_p, L_p' are not only abelian groups but also $\mathbf{Z_p}$-modules, so is L_p'/L_p as a quotient of such so that we have found a "$\mathbf{Z_p}$-variant" of our discriminant form $D = L'/L$.*

Proof. By Lemma 4.6, G^{-1} is the matrix that switches from the v_i to the v_i^* in the sense that $v_i^* = (G^{-1}, \text{i.col}) * [v_1, ..., v_n]$. Applying proposition 2.7(a) tells us that $(G^{-1})^{-1} = G$ is the matrix that brings us from the v_i^* to the v_i in the sense that $v_i = ((G^{-1})^{-1}, \text{i.col}) * [v_1^*, ..., v_n^*] = (G, \text{i.col}) * [v_1^*, ..., v_n^*]$. As L is integral (i.e. $G \in \mathbb{Z}^{n \times n}$), $v_i \in \text{span}_{\mathbb{Z}}(v_1^*, ..., v_n^*)$ so that in particular, $\Theta(v_i) \in \text{span}_{\mathbf{Z_p}}(\Theta(v_1^*), ..., \Theta(v_n^*)) = L_p'$ where the last step is valid because of the definition of L_p'. □

We will give a result which allows to compute the structure and describes the bilinear form on L'/L for an even lattice L. The essential idea is to inspect the p-component of the finite abelian group L'/L via the extension of $\mathbb{Q}$ to the p-adic numbers $\mathbf{Q_p}$. The notable fact is that there is a strong relation between the p-component of D and its $\mathbf{Z_p}$-variant L_p'/L_p, namely they are isomorphic as abelian groups and even more, the bilinear forms are essentially the same. We will see that the structure of L_p'/L_p can be computed easily. We need some preparation.

4.16 Definition. *Let G be a group (multiplicatively written) with unit 1 and let p be a prime number.*

(a) The order of an element $x \in G$ is defined as

$$\operatorname{ord}(x) := \min\{n \in \mathbb{N} \mid x^n = 1\}$$

Note that if G is written additively then $\operatorname{ord}(x) = \min\{n \in \mathbb{N} \mid n \cdot x = 0\}$.

(b) The set $G_p := \{x \in G \mid \exists \nu \in \mathbb{N}_0 \ .\ \operatorname{ord}(x) = p^\nu\}$ is called the p-component of G.

One can show the following:

4.17 Theorem. *For every group G we have $G_p \leq G$ and if G is a finite abelian group then $G = \bigoplus_{p\in\mathbb{P}} G_p$ (i.e. for every $x \in G$ there is a unique representation $x = \sum_{p\in\mathbb{P}} x_p$ where $x_p \in G_p$ for all p) and if $G = D$ is a discriminant form with finite bilinear form then $D = \bigoplus_{p\in\mathbb{P}} D_p$*

Proof. Existence of the representation: apply Cor. II.1.3 and Thm. II.1.6 from [JS] to abelian groups. Uniqueness is proved by an induction over the length of the representation. In the induction step one multiplies the difference of two representations with a suitable p_1^ν to null the first summand. On the orthogonality: let $x \in D_p, y \in D_q$ with $p \neq q$ both prime numbers and $a, b \in \mathbb{Z}$ with $ap^\nu + bq^\mu = 1$ where $p^\nu = \operatorname{ord}(x), q^\mu = \operatorname{ord}(y)$ then

$$\begin{aligned}(x, y) &= (1 \cdot x, y) = ((ap^\nu + bq^\mu)x, y) \\ &= a(p^\nu x, y) + b(x, p^\mu y) = a(0, y) + b(x, 0) = 0\end{aligned}$$

□

The above theorem says that it suffices to study the structure and the behavior of $(\cdot,\cdot)$ on a p-component of a discriminant form D and this is what we will do next.

4.18 Definition. *For a prime number p we define the subring of all rational numbers with p-power denominators*

$$\mathbb{Q}^{(p)} := \left\{\frac{a}{b} \in \mathbb{Q} \mid a = 0 \text{ or } (a, b) = 1 \text{ and } b = p^\nu \text{ for some } \nu \in \mathbb{N}_0\right\}$$

4.19 Lemma. *Let L be an integral lattice, $D = L'/L$ its discriminant form and let $(\cdot,\cdot)$ be the finite bilinear form on D.*

(a) $(\cdot,\cdot)\Big|_{D_p\times D_p}$ *maps to* $\mathbb{Q}^{(p)}/\mathbb{Z}$

(b) $\vartheta_p : \mathbb{Q}^{(p)}/\mathbb{Z} \mapsto \mathbf{Q_p}/\mathbf{Z_p}, \quad (q+\mathbb{Z}) \mapsto (\nu(q)+\mathbf{Z_p})$ *– where* $\nu : \mathbb{Q} \mapsto \mathbf{Q_p}$ *is the embedding of fields – is an isomorphism of abelian groups and* $\mathbb{Z}$*-modules.*

Proof. We only show that ϑ_p is surjective as this reasoning already contains the crucial insight that is necessary for the proof of the theorem on the structure of D. Let $\alpha \in \mathbf{Q_p}$ so that by Thm. 2.8, α may be represented as

$$\alpha = \sum_{k=-N}^{\infty} \alpha_k p^k =: \underbrace{\sum_{k=-N}^{-1} \alpha_k p^k}_{=:\alpha'} + \underbrace{\sum_{k=0}^{\infty} \alpha_k p^k}_{=:\alpha''}, \quad -N > -\infty, \;\; \alpha_k \in \{0,...,p-1\}$$

If $N \leq 0$ then $\alpha \in \mathbf{Z_p}$ so that $\alpha + \mathbf{Z_p} = 0 + \mathbf{Z_p} = \vartheta_p(0+\mathbb{Z})$. Now let $N > 0$, then

$$\begin{aligned}
\alpha + \mathbf{Z_p} &= \alpha' + \mathbf{Z_p} && (\text{as } \alpha'' \in \mathbf{Z_p}) \\
&= \frac{\alpha_{-N}}{p^N} + \frac{p}{p}\frac{\alpha_{-N+1}}{p^{N-1}} + ... + \frac{p^{N-1}}{p^{N-1}}\frac{\alpha_{-1}}{p} + \mathbf{Z_p} \\
&= \overbrace{\frac{\alpha_{-N} + p\alpha_{-N+1} + ... + p^{N-1}\alpha_{-1}}{p^N}}^{=:k\in\mathbb{Z}} + \mathbf{Z_p} \\
&= \vartheta_p\left(\frac{k}{p^N} + \mathbb{Z}\right) \in \mathrm{Im}(\vartheta_p) && \left(\text{as } \frac{k}{p^N} \in \mathbb{Q}^{(p)}\right)
\end{aligned}$$

□

4.20 Definition. *Let* G *be a finite abelian group. By the fundamental theorem of finitely generated abelian groups there are natural numbers* $N, a_1, ..., a_N \in \mathbb{N}$ *such that there is an isomorphism of abelian groups*

$$\eta : \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_N} \mapsto G$$

The set $\{x_1, ..., x_N\}$ *where* $x_1 := \eta(\overline{1}, \overline{0}, ..., \overline{0}), ..., x_N := \eta(\overline{0}, \overline{0}, ..., \overline{1})$ *is called a finite basis . The bar should indicate that we speak about* $\mathbb{Z}$*-cosets (i.e.* $\overline{1} := 1 + a_i\mathbb{Z}$*), not actual numbers. In the following we will denote this fact by the sloppy notation*

$$G = \mathbb{Z}_{a_1}x_1 \oplus ... \oplus \mathbb{Z}_{a_N}x_N$$

the isomorphism will always be named η and will map from $\mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_N}$ to G.

4.21 Remark. *(a) N and the a_i are absolutely not unique. Quite the contrary is the case, if $a_i = p_1^{e_1} \cdots p_r^{e_r}$ then every $\mathbb{Z}_{a_i}$ can be split up into $\mathbb{Z}_{p_1^{e_1}} \times ... \times \mathbb{Z}_{p_r^{e_r}}$ by the Chinese remainder theorem. Nevertheless, in the following sense, this is the only equivocality that occurs: If every a_i is a power of the same fixed prime number p then N and the a_i are unique, i.e. assume that p is a fixed prime and $e_1, ..., e_r, d_1, ..., d_s \in \mathbb{N} \setminus \{0\}$ and that*

$$\mathbb{Z}_{p^{e_1}} \times ... \times \mathbb{Z}_{p^{e_r}} \cong G \cong \mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_s}}$$

holds, then $r = s$ and there exists a bijection $\pi : \{1, ..., r\} \mapsto \{1, ..., r\}$ such that $e_i = d_{\pi(i)}$ for all $1 \leq i \leq r$.

(b) By definition, a finite basis has the property that every $x \in G$ can be written as a sum of the form $x = \sum_{i=1}^{N} c_i x_i$, the c_i being in $\mathbb{Z}$. Furthermore, if we are given two different representations of this form, i.e. $\sum_{i=1}^{N} c_i x_i = x = \sum_{i=1}^{N} d_i x_i$ then we have $c_i \equiv d_i \mod a_i$.

(c) Let G be a finite abelian group, let $G = \mathbb{Z}_{a_1} x_1 \oplus ... \oplus \mathbb{Z}_{a_N} x_N$. Fix a prime p and let $a_i = p^{s_i} r_i$ with $(r_i, p) = 1$ then the p-component of G is given by

$$G_p \cong \mathbb{Z}_{p^{s_1}} \times ... \times \mathbb{Z}_{p^{s_N}}$$

A finite basis for the p-component is given by $y_1, ..., y_N$ where $y_i = c_i x_i$ with $c_i = (r_i^{-1} \operatorname{modd} p^{s_i}) r_i$ (meaning that $c_i = 0$ if $s_i = 0$).

Proof. (a): See [JS] Thm 5.16, (b) holds by definition and (c) is an easy exercise in algebra that uses the terms "order", divisibility and some computations mod a_i. The assertion on the finite basis uses the chinese remainder theorem. □

The following result is well known:

4.22 Theorem. *Let R be a principal ideal domain. Let M be a free R-module of rank n and N a submodule of M (i.e. it is a subset and closed under the operation "." of R). There exists a basis $v_1, ..., v_n \in M$ and $a_1, ..., a_n \in R$ such that $N = Ra_1 v_1 + ... + Ra_n v_n$ and $a_1 \mid a_2 \mid ... \mid a_n$.*

Proof. See [JS], thm. VII.8.4. □

4.23 Corollary. *Let $(L, \langle\cdot,\cdot\rangle)$ be an integral lattice in $V \cong \mathbb{Q}^n$. We may chose a specific basis $v_1, ..., v_n$ for L such that $v_1^* + L, ..., v_n^* + L$ is a finite basis for D in the sense that*

$$D = \mathbb{Z}_{a_1}(v_1^* + L) \oplus ... \oplus \mathbb{Z}_{a_n}(v_n^* + L)$$

for $a_i = \mathrm{ord}(v_i^* + L)$.

Proof. In the last theorem set $M = L'$ and $N = L \subset L'$. Let $v_1^*, ..., v_n^*$ be the basis from the last theorem for L', then we dualize once more and show that $v^{**} := [v_1^{**}, ..., v_n^{**}]$ forms a basis of L. Let $(\cdot,\cdot)$ be the finite bilinear form on D. The v_i^{**} are contained in L because $(v_i^{**} + L, v_j^* + L) = \delta_{ij} + \mathbb{Z} = 0 + \mathbb{Z}$ so that – as $(\cdot,\cdot)$ is non-degenerate – $v_i^{**} + L = 0 + L$. The v_i^{**} form an $\mathbb{Q}$-basis for the vector space V by 4.6. Let $v \in L$ so that there are $\lambda_j \in \mathbb{Q}$ with $v = \sum_{j=1}^n \lambda_j v_j^{**}$. Now $\lambda_j = \lambda_j \cdot \langle v_i^{**}, v_i^*\rangle + 0 = \langle \sum_{j=1}^n \lambda_j v_j^{**}, v_i^*\rangle \in \langle L, L'\rangle \subset \mathbb{Z}$ so that

$$L \subset \mathbb{Z}v_1^{**} \oplus ... \oplus \mathbb{Z}v_n^{**} \subset \mathbb{Z}L + ... + \mathbb{Z}L \subset L$$

and thus $L = \mathbb{Z}v_1^{**} \oplus ... \oplus \mathbb{Z}v_n^{**}$. One now shows that the map

$$\eta : \mathbb{Z}^n \mapsto D, \eta(x_1, ..., x_n) = \sum_{i=1}^n x_i v_i^* + L$$

is a surjective homomorphism of abelian groups and $\ker(\eta) = a_1\mathbb{Z} \times ... \times a_n\mathbb{Z}$. The arguments for these facts are similar to the ones we will see in the proof of Theorem 4.28 (see the proof for the kernel of Δ) so we skip them here. Using the isomorphism theorem, $\mathrm{Im}(\eta) \cong \mathbb{Z}^n/\ker(\eta)$ and furthermore $\mathbb{Z}^n/(a_1\mathbb{Z} \times ... \times a_n\mathbb{Z}) \cong \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n}$ (which is easily shown!), the first claim follows. We show that $a_i = \mathrm{ord}(v_i^* + L) = \min\{n \in \mathbb{N} \mid nv_i^* + L = 0 + L\}$. Let $m_i := \mathrm{ord}(v_i^* + L)$, then $a_1(v_i^* + L) = 0 + L$ be definition of the a_i so that $m_i \leq a_i$. Further, $0 + L = m_i(v_i^* + L) = \eta(\overline{0}, ..., \overline{0}, \overline{m_i}, \overline{0}, ..., \overline{0})$ and since η is injective, $m_i \equiv 0 \mod a_i$, in other words, $a_i \mid m_i$. The order of the element $v_i^* + L$ in D in turn is easily computed: We know that $L = \mathbb{Z}v_1 \oplus ... \oplus \mathbb{Z}v_n$. The v_i form an $\mathbb{Q}$-vector space basis and we may simply compute the (unique!) representation of av_i^* in terms of the v_i, by Lemma 4.6, it is given by

$$av_i^* = a(G^{-1}, \mathrm{i.col}) * [v_1, ..., v_n]$$

so that

$$av_i^* \in L \iff av_i^* \in \mathbb{Z}v_1 \oplus ...\mathbb{Z}v_n \iff a(G^{-1}, \mathrm{i.col}) \in \mathbb{Z}^n$$

Therefore, the order of $v_i^* + L$ is the minimal a satisfying the above equation, i.e. it is the least common multiple of all denominators in the i-th column of G^{-1} (provided that we have chosen a representation of all fractions that are maximally reduced). $\square$

Let us consider the lattice $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \subset V = \mathbb{Q}^2$ with the gram matrix $G = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ then $|D| = |\det(G)| = 3$. The dual basis is given by $v_1^* = (2/3 - 1/3), v_2^* = (-1/3, 2/3)$ (see 4.6). One can easily compute that $\mathrm{ord}(v_1^* + L) = \mathrm{ord}(v_2^* + L) = 3$. The above does *not* state that then $D \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ (this obviously contradicts $|D| = 3!$) but rather that there *exists* a basis w_1^*, w_2^* of L' that serves as a finite basis, i.e. $w_i^* \neq v_i^*$ in general.

4.24 Notation. *We will now inspect the algebraic structure L'_p/L_p very closely. We first note that we may also define a $\mathbf{Z_p}$-bilinear form on L'_p/L_p using Theorem 4.7*(a) *(set $R = \mathbf{Z_p}, K = \mathbf{Q_p}, V = \mathbf{Q_p}^n, L := L_p, \widetilde{L} := L'_p$). In order to distinguish between the $\mathbb{Q}$-bilinear form on L and the finite bilinear form on D (which will be denoted $\langle \cdot, \cdot \rangle : L \times L \mapsto \mathbb{Q}$ and $(\cdot, \cdot) : D \times D \mapsto \mathbb{Q}/\mathbb{Z}$ subsequently) and the $\mathbf{Q_p}$-variants of these, we will write $\langle \cdot, \cdot \rangle_{\mathbf{Q_p}}$ for the $\mathbf{Q_p}$-bilinear form on L_p and $(\cdot, \cdot)_{\mathbf{Q_p}}$ for the $\mathbf{Z_p}$-bilinear form on L'_p/L_p.*

4.25 Definition. *Let (L, v, G) be an integral lattice and let $D = L'/L$ be its discriminant form. Let*

$$D \cong \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n}$$

and

$$D_p \cong \mathbb{Z}_{p^{s_1}} \times ... \times \mathbb{Z}_{p^{s_n}}$$

Let $N := s_1 + ... + s_n$ then $|D_p| = p^N$. For $s \in \mathbf{Z_p}$ having a p-adic expansion

$$s = s_0 + ps_1 + ... + p^{N-1}s_{N-1} + p^N s_N + p^{N+1}s_{N+1} + ...$$

we define $[\![s]\!] := s_0 + ps_1 + ... + p^{N-1}s_{N-1} \in \mathbb{Z}$ and $\langle\!\langle s \rangle\!\rangle := s_N + ps_{N+1} + p^2 s_{N+2} + ...$ so that $s = [\![s]\!] + p^N \langle\!\langle s \rangle\!\rangle$. We extend this definition in a natural way to $\mathbf{Z_p}$-matrices, i.e. if $X \in \mathbf{Z_p}^{n \times n}$ then we set $[\![X]\!] := ([\![x_{ij}]\!])_{i,j=1,...,n}$ and so forth.

Why did we define this? The answer is coming up; the following lemma tells us that for every "$\mathbf{Z_p}$ action" we may execute on cosets in L'_p/L_p, we can repeat essentially the same step in L'/L using only "$\mathbb{Z}$ actions", i.e. only a finite part of the p-adic number is important.

4.26 Lemma. *Let $(L, \langle \cdot, \cdot \rangle)$ be an integral lattice and $p \in \mathbb{P}$. For $s, t \in \mathbf{Z_p}, x, y \in L'_p$ we have*

(a) $t[\![s]\!](x+L_p) = ts(x+L_p)$

(b) $t\langle[\![s]\!]x, y\rangle_{\mathbf{Q_p}} + \mathbf{Z_p} = t\langle sx, y\rangle_{\mathbf{Q_p}} + \mathbf{Z_p}$

Proof. (a): The difference of both expressions is $p^N t\langle\!\langle s\rangle\!\rangle x + L_p$ and we intend to show that this is equal to $0 + L_p$. By definition the $\widetilde{v}_i^*$ form a $\mathbf{Z_p}$-basis for L_p' so it suffices to show that $p^N\widetilde{v}_i^* + L_p = 0 + L_p$. Due to Corollary 4.23 we know that $a_1v_1^*, ..., a_nv_n^*$ is a basis for L. By remark 4.11 we know that $L_p = \mathbf{Z_p}a_1\widetilde{v}_1^* \oplus ... \oplus \mathbf{Z_p}a_n\widetilde{v}_n^*$. Let $a_i = r_ip^{s_i}$ with $(r_i, p) = 1$ then r_i is a unit in $\mathbf{Z_p}$ so that in particular

$$p^N\widetilde{v}_i^* = \underbrace{r_i^{-1}}_{\in\mathbf{Z_p}}\underbrace{p^{N-s_i}}_{\in\mathbb{Z}\subset\mathbf{Z_p}}\underbrace{r_ip^{s_i}\widetilde{v}_i^*}_{=a_i\widetilde{v}_i^*\in L_p} \in \mathbf{Z_p}\cdot L_p \subset L_p$$

(b) Let $(\cdot,\cdot)_{\mathbf{Q_p}}$ be the $\mathbf{Z_p}$-bilinear form on L_p'/L_p, then the difference of both sides is

$$\langle t\langle\!\langle s\rangle\!\rangle p^N x, y\rangle_{\mathbf{Q_p}} + \mathbf{Z_p} = (t\langle\!\langle s\rangle\!\rangle \underbrace{p^N x + L_p}_{=0+L_p}, y+L_p)_{\mathbf{Q_p}} = (0+L_p, y+L_p) = 0+\mathbf{Z_p}$$

□

Now we will link the structure of L_p'/L_p and the p-component of L'/L. The following result was already mentioned in [Ni], Prop. 1.7.1 but no proof can be found there.

4.27 Lemma. *Let $(L, \langle\cdot,\cdot\rangle) = (L, v, G)$ be an integral lattice in $V = \mathbb{Q}^n$. Let $L' = \mathbb{Z}v_1^* \oplus ... \oplus \mathbb{Z}v_n^*$ be its dual lattice and set $D := L'/L$ to be its discriminant form. Fix a prime $p \in \mathbb{P}$ and let D_p be the p-component of the finite abelian group D. Then,*

$$D_p \cong {L_p'}\big/{L_p}$$

as abelian groups.

Proof. Let η be the isomorphism of

$$D = \mathbb{Z}_{a_1}(v_1^* + L) \oplus ... \oplus \mathbb{Z}_{a_N}(v_n^* + L)$$

with $a_i = p^{s_i}r_i$ and $(r_i, p) = 1$ such that $v_1^* + L = \eta(\overline{1}, \overline{0}, ..., \overline{0}), ..., v_n^* + L = \eta(\overline{0}, ..., \overline{0}, \overline{1})$ form a finite basis with $a_1v_1^*, ..., a_nv_n^*$ being a basis of L as in Corollary 4.23 and therefore

$$L_p = \mathbf{Z_p}a_1\widetilde{v}_1^* \oplus ... \oplus \mathbf{Z_p}a_n\widetilde{v}_n^* \tag{4.1}$$

as in Remark 4.11. Consider the finite basis $y_i^* + L := c_i v_i^* + L, i = 1, ..., n$ of D_p as in 4.21(c). For $x + L \in D_p$ take numbers $k_i \in \mathbb{Z}$ uniquely determined modulo p^{s_i} such that $x + L = \sum_{i=1}^n k_i y_i^* + L$ then we define

$$\Phi : D_p \mapsto {L'_p}\Big/{L_p} \qquad \Phi(x + L) := \sum_{i=1}^n k_i c_i \widetilde{v_i^*} + L_p = \sum_{i=1}^n k_i \widetilde{y_i^*} + L_p$$

where we understand the symbol $\widetilde{v_i^*}$ as in definition 4.10. Observe that the definition is compatible with the case that $s_i = 0$ because if $s_i = 0$ then $a_i v_i^* + L = \eta(\overline{0}, ..., \overline{0}, \underbrace{\overline{a_i}}_{\equiv 0 \mod a_i}, \overline{0}, ..., \overline{0}) = 0 + L$ and $a_i = p^0 r_i$ is a unit in $\mathbf{Z_p}$ so that $\Phi(v_i^* + L) = a_i^{-1} \Phi(a_i v_i^* + L) \in \mathbf{Z_p} L_p \subset L_p$ i.e. we have defined $\Phi(0 + L) = 0 + L_p$. We claim that Φ is a well-defined isomorphism of abelian groups. Independence of the k_i: if $x + L = \sum_{i=1}^n k_i y_i^* + L = \sum_{i=1}^n k_i' y_i^* + L$ so that $k_i - k_i' = m_i p^{s_i}$ for some $m_i \in \mathbb{Z}$ then

$$\begin{aligned}
\sum_{i=1}^n (k_i - k_i') c_i \widetilde{v_i^*} + L_p &= \sum_{i=1}^n (m_i r_i^{-1} \operatorname{modd} p^{s_i}) \underbrace{p^{s_i} r_i}_{=a_i} \widetilde{v_i^*} + L_p \\
&\in \sum_{i=1}^n \underbrace{\mathbb{Z} \underbrace{a_i \widetilde{v_i^*}}_{\in L_p \text{ by (4.1)}} + L_p}_{=0 + L_p} \\
&= \{0\} + L_p
\end{aligned}$$

so that the value of Φ does not depend on the concrete representative of k_i modulo p^{s_i} and hence, Φ is a homomorphism. Injectivity: Let $k_i \in \mathbb{Z}$ so that

$$\sum_{i=1}^n k_i c_i \widetilde{v_i^*} + L_p = \Phi\left(\sum_{i=1}^n k_i y_i^* + L\right) = 0 + L_p$$

so that by (4.1) there are $\mu_i \in \mathbf{Z_p}$ with

$$\sum_{i=1}^n k_i c_i \widetilde{v_i^*} = \sum_{i=1}^n \mu_i a_i \widetilde{v_i^*}$$

As the $\widetilde{v_i^*} = e_i$ are $\mathbf{Q_p}$-linearly independent in ${\mathbf{Q_p}}^n$ by definition, this implies that $k_i c_i = \mu_i a_i$. Note that because of $(r_i, p) = 1$, c_i is a unit in $\mathbf{Z_p}$ and hence, applying the p-norm on both side yields

$$|k_i|_p \cdot 1 = |k_i c_i|_p = |\mu_i a_i|_p \leq 1 \, |a_i|_p = p^{-s_i}$$

so that $\mathrm{ord}_p(k_i) \geq s_i$ which means nothing else than $p^{s_i} \mid k_i$ and finally $k_i \equiv 0 \mod p^{s_i}$ which concludes the proof of the injectivity. Surjectivity: As Φ is linear, it suffices to show that for every $1 \leq i \leq n$, $\mathbf{Z_p}\widetilde{v}_i^* + L_p \subset \mathrm{Rg}(\Phi)$. Take $\alpha \in \mathbf{Z_p}$ and write

$$\alpha = [\![\alpha]\!] + p^N \langle\!\langle \alpha \rangle\!\rangle$$

then by Lemma 4.26

$$\alpha\widetilde{v}_i^* + L_p = \underbrace{[\![\alpha]\!]}_{\in\mathbb{Z}} \widetilde{v}_i^* + L_p = \Phi([\![\alpha]\!]\widetilde{v}_i^* + L) \in \mathrm{Rg}(\Phi)$$

□

We are now able to formulate and prove a first structural theorem on discriminant forms. The subsequent theorems will also describe the behavior of the finite bilinear form or (if existent) of the finite quadratic form.

4.28 Theorem. *Let $(L, \langle\cdot,\cdot\rangle) = (L, v, G)$ be an integral lattice in $V = \mathbb{Q}^n$. Let $L' = \mathbb{Z}v_1^* \oplus ... \oplus \mathbb{Z}v_n^*$ its dual lattice and set $D := L'/L$ to be its discriminant form. Fix a prime $p \in \mathbb{P}$ and let D_p be the p-component of the finite abelian group D. Consider $\widetilde{G} := \nu(G) \in \mathbf{Z_p}^{n\times n}$ (for brevity we just write G for $\nu(G)$ too) and take $S \in \mathbf{Z_p}^{n\times n}$ such that $H := S^TGS$ is (almost) diagonal in the sense of Lemma 3.3, then using the notation of Lemma 3.3 the following holds:*

(a) Let $p \in \mathbb{P}, p \neq 2$ and $H = \mathrm{diag}(\alpha_1, ..., \alpha_n)$ with $\alpha_i = p^{d_i}\beta_i$ then

$$D_p \cong \mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_n}}$$

The isomorphism is an isomorphism of abelian groups.

(b) Let $p = 2$ and $H = B_1 \dotplus ... \dotplus B_f \dotplus \mathrm{diag}(\alpha_f, ..., \alpha_{f'})$ where $B_i = 2^{e_i}B_i', \alpha_i = 2^{d_i}\beta_i$ then

$$D_2 \cong (\mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_1}}) \times ... \times (\mathbb{Z}_{2^{e_f}} \times \mathbb{Z}_{2^{e_f}}) \times \mathbb{Z}_{2^{d_1}} \times ... \times \mathbb{Z}_{2^{d_{f'}}}$$

The isomorphism is an isomorphism of abelian groups.

A finite basis with respect to this decomposition is given by $\widetilde{w}_i^* + L_p$ where $\widetilde{w}_i^*$ are the dualized vectors with respect to the basis $\widetilde{w}_i = (S, i.col) * [\widetilde{v}_1, ..., \widetilde{v}_n]$ (where $\widetilde{v}_i := \Theta(v_i)$) in $\widetilde{v} = \mathbf{Q_p}^n$.

Proof. The basic insight one needs to have is that

$$D_p \overset{(1)}{\cong} {L'_p}\Big/_{L_p} \overset{(2)}{\cong} G_p$$

where G_p is as claimed in the theorem and L'_p/L_p is to be interpreted as quotient of $\mathbf{Z_p}$ modules and the isomorphism is an isomorphism of $\mathbb{Z}$-modules. (1) is precisely the assertion of Lemma 4.27.
On (2): Let $p \neq 2$ so that $H = \mathrm{diag}(\alpha_1, ..., \alpha_n), \alpha_i = p^{d_i}\beta_i$ where $|\beta_i|_p = 1$. We define $\widetilde{w}_i := (S, \mathrm{i.col}) * [\widetilde{v}_1, ..., \widetilde{v}_n]$. Doing this means nothing else than actually executing the change of basis S, which simplifies the Gram matrix G. It was not possible to do so in the original lattice because $S \in \mathbb{Q}^{n\times n}$. As $S^{-1}, (S^{-T})^{-1} \in {\mathbf{Z_p}}^{n\times n}$, remark 4.11 tells us that $L_p = \mathbf{Z_p}\widetilde{w}_1 \oplus ... \oplus \mathbf{Z_p}\widetilde{w}_n$. Further, we know by Lemma 4.6 that $L'_p = \mathbf{Z_p}\widetilde{w}_1^* \oplus ... \oplus \mathbf{Z_p}\widetilde{w}_n^*$ where $\widetilde{w}_i^*$ is the dual basis to $\widetilde{w}$.
We define a homomorphism of abelian groups:

$$\Delta : \mathbb{Z} \times ... \times \mathbb{Z} = \mathbb{Z}^n \mapsto {L'_p}\Big/_{L_p},$$

$$\Delta(k_1, ..., k_n) := k_1\widetilde{w}_1^* + ... + k_n\widetilde{w}_n^* + L_p$$

and show that Δ is surjective and that

$$\ker(\Delta) = \mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_n}} \tag{4.2}$$

On the surjectivity of Δ: As the $\widetilde{w}_i^*$ span L'_p,

$${L'_p}\Big/_{L_p} = \mathbf{Z_p}(\widetilde{w}_1^* + L_p) + ... + \mathbf{Z_p}(\widetilde{w}_n^* + L_p)$$

This means that – using the linearity of Δ–, it suffices to show $\alpha\widetilde{w}_i^* + L_p \in \mathrm{Rg}(\Delta)$. Write

$$\alpha = [\![\alpha]\!] + p^N\langle\!\langle\alpha\rangle\!\rangle$$

then by Lemma 4.26

$$\alpha\widetilde{w}_i^* + L_p = \underbrace{[\![\alpha]\!]}_{\in\mathbb{Z}}\widetilde{w}_i^* + L_p = \Delta(0, ..., 0, [\![\alpha]\!], 0, ..., 0) \in \mathrm{Rg}(\Delta)$$

where $[\![\alpha]\!]$ is at the $i-th$ position of the vector in $\mathbb{Z}^n$. The surjectivity of Δ is therefore shown and we proceed to showing equation (4.2): "$\supset$": Proposition 2.7(b) tells us that the Gram matrix w.r.t. the basis $\widetilde{w}_i$ is given

by H. Using Lemma 4.6, we obtain an interesting representation of the $\widetilde{w}_i^*$ in terms of the $\widetilde{w}_i$, namely

$$\widetilde{w}_i^* = (H^{-1}, \text{i.col}) * [\widetilde{w}_1, ..., \widetilde{w}_n]$$

i.e. $\widetilde{w}_i^* = \alpha_i^{-1}\widetilde{w}_i$ so that $\alpha_i\widetilde{w}_i^* = \widetilde{w}_i \in L_p$. We have written $\alpha_i = p^{d_i}\beta_i$ where β_i is a unit in $\mathbf{Z_p}$, thus

$$p^{d_i}\widetilde{w}_i^* + L_p = \beta_i^{-1}\alpha_i\widetilde{w}_i^* + L_p = 0 + L_p$$

To see "$\subset$" let us assume $(k_1, ..., k_n) \in \ker(\Delta)$ so that $\sum_{i=1}^n k_i\widetilde{w}_i^* \in L_p$ and thus there are $\gamma_i \in \mathbf{Z_p}$ satisfying

$$\sum_{i=1}^n \gamma_i\widetilde{w}_i = \sum_{i=1}^n k_i\widetilde{w}_i^* = \sum_{i=1}^n \frac{k_i}{\alpha_i}\widetilde{w}_i = \sum_{i=1}^n \frac{k_i}{\beta_i}p^{-d_i}\widetilde{w}_i$$

Since the $\widetilde{w}_i$ are a $\mathbf{Q_p}$-linearly independent, it follows that $\gamma_i = (k_i/\beta_i)\cdot p^{-d_i}$ and thus

$$1 \overset{\gamma_i \in \mathbf{Z_p}}{\geq} |\gamma_i|_p = \left|\frac{k_i}{\beta_i}p^{-d_i}\right|_p = \frac{|k_i|_p}{1}p^{d_i}$$

This implies $p^{d_i} \leq p^{\text{ord}_p(k_i)}$ but this means nothing else than $p^{d_i} \mid k_i$, hence $(k_1, ..., k_n) \in p^{d_1}\mathbb{Z} \times ... \times p^{d_n}\mathbb{Z}$, so (4.2) is shown.
One easily shows that

$$\frac{\mathbb{Z} \times ... \times \mathbb{Z}}{p^{d_1}\mathbb{Z} \times ... \times p^{d_n}\mathbb{Z}} \cong \mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_n}}$$

Using the first isomorphism theorem finally yields (2), namely

$$L_p'\Big/L_p \overset{\text{surjectivity of } \Delta}{=} \text{Rg}(\Delta) \cong \frac{\mathbb{Z}^n}{\ker(\Delta)} \cong \mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_n}}$$

It follows that Δ may be regarded as an isomorphism

$$\mathbb{Z}_{p^{d_1}} \times ... \times \mathbb{Z}_{p^{d_n}} \mapsto L_p'/L_p$$

and since $\Delta(e_i) = \widetilde{w}_i^* + L_p$ (where we write $e_1 = (\overline{1}, \overline{0}, ..., \overline{0})$ and so forth) this also shows that $\widetilde{w}_i^* + L_p$ forms a finite basis for L_p'/L_p. $\Rightarrow$ (2) is shown for the case where $p \neq 2$ and the case $p = 2$ is proved very similar to the above. $\square$

4.29 Remark (and notation). *Let* $D \cong \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n}$ *with* $a_i = p^{s_i}\beta_i$ *for some* $p \in \mathbb{P}, p \neq 2$ *and* $H = \mathrm{diag}(\alpha_1, ..., \alpha_n)$ *with* $\alpha_i = p^{d_i}\beta_i$ *satisfying* $|\beta_i|_p = 1$. *Using 4.28 and 4.21(a) we have also shown that there is a bijection* $\pi : \{1, ..., n\} \mapsto \{1, ..., n\}$ *such that* $s_i = d_{\pi(i)}$. *Note that some of the* s_i *may be zero. For the sake of readability we will assume* $\pi = Id$ *in the sequel and* $s_1 \neq 0, ..., s_{n'} \neq 0, s_{n'+1} = ... = s_n = 0$. *This is reasonable: before we start the proof we switch the roles of the* v_i^* *so that the first* n' *exponents are non trivial. By substituting* S *with* $S \cdot X$ *where* X *switches the respective rows, we achieve that* $\pi = Id$. *We proceed analogously when* $p = 2$ *so that (in the notation of Lemma 3.3)* $s_1 = e_1, s_2 = e_1, s_3 = e_2, s_4 = e_2, ..., s_{2f} = e_f, s_{2f+1} = d_1, ..., s_n = d_{f'}$.

We want to rephrase the assertion of the last theorem. Let L be a $\mathbb{Z}$-lattice with Gram matrix G and $D = L'/L$ its discriminant form. The last theorem states that if one knows the diagonalization of G over the local rings $\mathbf{Z_p}$ for all p, then one also knows the structure of the p-components of D and since $D = \oplus_{p\in\mathbb{P}} D_p$, one knows the structure of D as an abelian group. Rephrased once again this means that the Jordan symbols of G uniquely determine the structure of D as an abelian group, namely if $\mathrm{symbol}_p(G) = \prod_{q\in p^{\mathbb{N}_0}} q^{\delta_q m_q}$ for $p \neq 2$ then $D_p \cong \oplus_{q\in p^{\mathbb{N}_0}} \mathbb{Z}_q^{m_q}$ and analogously for the case $p = 2$.

We will now see that the map Φ from Thm. 4.28 it is not only an isomorphism of abelian groups but rather of discriminant forms (up to an isomorphism of the ranges of the finite bilinear forms). This particular insight will help us to find a finite basis of D that significantly decreases the complexity of the finite bilinear form. We will start by finding a finite basis of the p-component of L'/L on which the behavior of the finite bilinear form is as simple as possible. The main idea is that since in the $\mathbf{Q_p}$-vector space, the form behaves almost diagonal with respect to the basis $\widetilde{w}_1^*, ..., \widetilde{w}_n^*$, the original finite bilinear form should behave almost diagonal with respect to the basis $\Phi^{-1}(\widetilde{w}_1^* + L_p), ..., \Phi^{-1}(\widetilde{w}_n^* + L_p)$. Even more is true: We can almost translate the behavior of the finite bilinear form on L_p'/L_p and the one on L'/L which is useful, because on L_p'/L_p, we achieve a very simple structure using Lemma 3.3 or (even better) using Corollary 3.18.

4.30 Theorem. *Fix* $p \in \mathbb{P}$. *Let* (L, v, G) *be an integral lattice in* $V = \mathbb{Q}^n$ *and* $D := L'/L$ *its discriminant form with finite bilinear form* $(\cdot, \cdot)$. *Let* $D = \mathbb{Z}_{a_1}(v_1^* + L) \oplus ... \oplus \mathbb{Z}_{a_n}(v_n^* + L)$ *with* $a_i = p^{s_i} \cdot r_i$ *satisfying* $(r_i, p) = 1$. *Put* $y_i^* = c_i \cdot v_i^*$ *such that the* $y_i^* + L$ *form a finite basis for* D_p *as in 4.21*(c).

(a) The isomorphism from 4.28,

$$\Phi : D_p \mapsto {L'_p}\Big/{L_p}, \quad \Phi(y_i^* + L) := c_i \widetilde{v}_i^* + L_p =: \widetilde{y_i}^* + L_p$$

is an isomorphism that respects the bilinear forms in the sense that for all $x + L, y + L \in D$ we have

$$(x + L, y + L) = \vartheta_p^{-1}((\Phi(x + L), \Phi(y + L))_{\mathbf{Q_p}})$$

where ϑ_p is the isomorphism from Lemma 4.19.

(b) Let $S \in {\mathbf{Z_p}}^{n \times n}$ such that $\det(S) \in {\mathbf{Z_p}}^{\times}$ and put $H := S^T G S$. Set $C := \mathrm{diag}(c_1, ..., c_n)$ and

$$g_i^* + L = ([\![S^{-1}C^{-1}]\!], i.row) * [y_1^*, ..., y_n^*] + L$$

then the $g_i^* + L$ are precisely the preimages of the vectors $(S^{-1}C^{-1}, i.row) * [\widetilde{y}_1^*, ..., \widetilde{y}_n^*] + L_p$ under the map Φ. The finite bilinear form is given by

$$((g_i^* + L, g_j^* + L))_{i,j=1,...,n} = \vartheta_p^{-1}(H^{-1})$$

Proof. (a): For $1 \leq a, b \leq n$

$$\begin{aligned}
\vartheta_p((y_a^* + L, y_b^* + L)) &= \vartheta_p(\langle c_a v_a^*, c_b v_b^* \rangle + \mathbb{Z}) \\
&= c_a c_b \ \vartheta_p(\langle v_a^*, v_b^* \rangle + \mathbb{Z}) && (\vartheta_p \text{ is } \mathbb{Z}\text{-linear}) \\
&= c_a c_b \langle v_a^*, v_b^* \rangle + \mathbf{Z_p} && (\text{def. of } \vartheta_p) \\
&= c_a c_b (G^{-1})_{ab} + \mathbf{Z_p} \\
&= c_a c_b \langle \widetilde{v}_a^*, \widetilde{v}_b^* \rangle_{\mathbf{Q_p}} + \mathbf{Z_p} \\
&\quad \text{(by definition of the bilinear form on } L_p\text{')} \\
&= (c_a \widetilde{v}_a^* + L_p, c_b \widetilde{v}_b^* + L_p)_{\mathbf{Q_p}} \\
&= (\Phi_p(y_a^* + L), \Phi_p(y_b^* + L))_{\mathbf{Q_p}}
\end{aligned}$$

Since all involved mappings are $\mathbb{Z}$-linear the assertion holds for the $\mathbb{Z}$-span of the $y_i^* + L$ too (which is exactly D_p as they form a finite basis for D_p).

(b) We show that the $g_i^* + L$ form a finite basis for D_p. Let $\widetilde{g}_i^* = (S^{-1}C^{-1}, \mathrm{i.row}) * [\widetilde{y}_1^*, ..., \widetilde{y}_n^*]$ in the $\mathbf{Q_p}$-vector space. We claim that $\widetilde{g}_i^* + L_p$ form a finite basis for L'_p/L_p. We want this to be true, because then it suffices to show that the $g_i^* + L$ really are the preimages of the $\widetilde{g}_i^* + L_p$ under the isomorphism Φ since isomorphisms transfer finite bases to finite bases again.

The $\widetilde{g}_i^* + L_p$ form a finite basis for L_p'/L_p: Put $\widetilde{w_i} := (S, \text{i.col}) * [\widetilde{v}_1, ..., \widetilde{v}_n]$ and $\widetilde{w}_i^* := (H^{-1}, \text{i.col}) * [\widetilde{w}_1, ..., \widetilde{w}_n]$ as in Theorem 4.28. Using Proposition 2.7(a) a few times we see that

$$\begin{aligned}
\widetilde{w}_i^* &= (H^{-1}, \text{i.col}) * [\widetilde{w}_1, ..., \widetilde{w}_n] \\
&= (S^{-1}G^{-1}S^{-T}, \text{i.col}) * \begin{bmatrix} (S, 1.\text{col}) * [\widetilde{v}_1, ..., \widetilde{v}_n] \\ \vdots \\ (S, \text{n.col}) * [\widetilde{v}_1, ..., \widetilde{v}_n] \end{bmatrix} \\
&= (G^{-1}S^{-T}, \text{i.col}) * \begin{bmatrix} (G, 1.\text{col}) * [\widetilde{v}_1^*, ..., \widetilde{v}_n^*] \\ \vdots \\ (G, \text{n.col}) * [\widetilde{v}_1^*, ..., \widetilde{v}_n^*] \end{bmatrix} \\
&= (CC^{-1}S^{-T}, \text{i.col}) * [\widetilde{v}_1^*, ..., \widetilde{v}_n^*] \\
&= (C^{-1}S^{-T}, \text{i.col}) * \begin{bmatrix} (C, 1.\text{row}) * [\widetilde{v}_1^*, ..., \widetilde{v}_n^*] \\ \vdots \\ (C, \text{n.row}) * [\widetilde{v}_1^*, ..., \widetilde{v}_n^*] \end{bmatrix} \\
&= (S^{-1}C^{-1}, \text{i.row}) * [\widetilde{y}_1^*, ..., \widetilde{y}_n^*] = \widetilde{g}_i^*
\end{aligned}$$

so that the $\widetilde{g}_i^* + L_p$ form a finite basis solely because the $\widetilde{w}_i^* + L_p$ do as shown in 4.28.
Furthermore, the $g_i^* + L$ are the preimages of the $\widetilde{g}_i^* + L_p$ as

$$\begin{aligned}
\Phi_p(g_i^* + L) &= ([\![S^{-1}C^{-1}]\!], \text{i.row}) * [\widetilde{y}_1^*, ..., \widetilde{v}_n^*] + L_p \\
&\overset{4.26(a)}{=} (S^{-1}C^{-1}, \text{i.row}) * [\widetilde{y}_1^*, ..., \widetilde{y}_n^*] + L_p = \widetilde{g}_i^* + L_p
\end{aligned}$$

Now we compute the Gram matrix of the bilinear form on L_p' w.r.t. the basis $\widetilde{g}_i^*$:

$$\begin{aligned}
\langle \widetilde{g}_i^*, \widetilde{g}_j^* \rangle_{\mathbf{Q_P}} &= \left\langle (C^{-1}S^{-T}, \text{i.col}) * \begin{bmatrix} \widetilde{y}_1^* \\ \vdots \\ \widetilde{y}_n^* \end{bmatrix}, (C^{-1}S^{-T}, \text{j.col}) * \begin{bmatrix} \widetilde{y}_1^* \\ \vdots \\ \widetilde{y}_n^* \end{bmatrix} \right\rangle \\
&= \left\langle (S^{-1}, \text{i.row}) * \begin{bmatrix} \widetilde{v}_1^* \\ \vdots \\ \widetilde{v}_n^* \end{bmatrix}, (S^{-1}, \text{j.row}) * \begin{bmatrix} \widetilde{v}_1^* \\ \vdots \\ \widetilde{v}_n^* \end{bmatrix} \right\rangle \qquad \text{(by 2.7(a))} \\
&= (S^{-1}(\text{Gram matrix w.r.t. the } \widetilde{v}^*)S^{-T})_{ij} \qquad \text{(by 2.7(b))} \\
&= (S^{-1}G^{-1}S^{-T})_{ij} = (H^{-1})_{ij}
\end{aligned}$$

so that

$$(\Phi(g_i^*+L),\Phi(g_j^*+L))_{\mathbf{Q_p}} = (\widetilde{g}_i^*+L_p,\widetilde{g}_j^*+L_p)_{\mathbf{Q_p}} = \langle \widetilde{g}_i^*,\widetilde{g}_j^*\rangle_{\mathbf{Q_p}}+\mathbf{Z_p} = H_{ij}^{-1}+\mathbf{Z_p} \tag{4.3}$$

and consequently,

$$(g_i^*+L,g_j^*+L) \overset{\text{(a)}}{=} \vartheta_p^{-1}(\Phi_p(g_i^*+L),\Phi_p(g_j^*+L))_{\mathbf{Q_p}} \overset{(4.3)}{=} \vartheta_p^{-1}(H_{ij}^{-1})$$

□

Now we want to deduce an equivalent version of Theorem 4.28 for finite quadratic forms q. We need a preparatory lemma to clarify the coherence of the finite quadratic form q and the finite bilinear form $(\cdot,\cdot)$ on D.

4.31 Lemma. *For $p \in \mathbb{P}$, $p \neq 2$ let*

$$\mathrm{half}_p : {2\mathbb{Q}^{(p)}}\Big/{2\mathbb{Z}} \mapsto {\mathbb{Q}^{(p)}}\Big/{\mathbb{Z}}, \quad 2\frac{x}{p^\nu}+2\mathbb{Z} \mapsto \frac{x}{p^\nu}+\mathbb{Z}$$

Define $w_p := \vartheta_p \circ \mathrm{half}_p$ and let

$$u_2 : {\mathbb{Q}^{(2)}}\Big/{2\mathbb{Z}} \mapsto {\mathbf{Q_2}}\Big/{2\mathbf{Z_2}}, \quad \frac{x}{2^\nu}+2\mathbb{Z} \mapsto \frac{x}{2^\nu}+2\mathbf{Z_2}$$

then for all $p \in \mathbb{P}$, half_p and w_p are isomorphisms of $\mathbb{Z}$-modules and u_2 is an isomorphism of $\mathbb{Z}$-modules too.

Proof. The proof that half_p is an isomorphism is a straightforward computation. Since ϑ_p is an isomorphism by Lemma 4.19, so is w_p. We show that u_2 is an isomorphism. It is clear that u_2 is well-defined and the surjectivity of u_2 follows precisely as in Lemma 4.19. On the injectivity: Let $k/2^\nu + 2\mathbf{Z_2} = 0 + 2\mathbf{Z_2}$ so that $k/2^\nu = 2\alpha$ for some $\alpha \in \mathbf{Z_2}$. Comparing the 2-norms yields

$$2^{-(\mathrm{ord}_2(k)-\nu)} = \left|\frac{k}{2^\nu}\right|_2 = |2|_2\,|\alpha|_2 \leq 1/2 \cdot 1 = 2^{-1}$$

hence, $\mathrm{ord}_2(k)-\nu \geq 1$ and thus $k = 2^{\nu+1}\cdot k'$ for some $k' \in \mathbb{Z}$ so that

$$\frac{k}{2^\nu} = 2k' \in 2\mathbb{Z}$$

Therefore, $k/2^\nu$ is the zero element in $\mathbb{Q}^{(2)}/2\mathbb{Z}$. □

4.32 Theorem. *Let $(L, \langle\cdot,\cdot\rangle) = (L, v, G)$ be an even lattice in $V \cong \mathbb{Q}^n$ and $D = L'/L$ its discriminant form with finite bilinear form $(\cdot,\cdot)$ and finite quadratic form $q : L'/L \mapsto \mathbb{Q}/2\mathbb{Z}$. Fix a prime p, let $x + L \in D_p$ and chose a fixed but arbitrary representative $x' \in L'_p$ of $\Phi_p(x + L)$ then*

(a) For all $p \neq 2$,

$$q(x + L) = \langle x, x\rangle + 2\mathbb{Z} = w_p^{-1}\left(\frac{\langle x', x'\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p}\right)$$

(b) For $p = 2$ we obtain

$$q(x + L) = \langle x, x\rangle + 2\mathbb{Z} = u_2^{-1}\left(\langle x', x'\rangle_{\mathbf{Q_2}} + 2\mathbf{Z_2}\right)$$

(c) For all $p \in \mathbb{P}$ we obtain for the map Q

$$Q(x + L) = \frac{\langle x, x\rangle}{2} + \mathbb{Z} = \vartheta_p^{-1}\left(\frac{\langle x', x'\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p}\right)$$

Proof. If we consider fixed representatives $y_i^* = c_i v_i^*$ (note that by definition, c_i is a fixed number in $\mathbb{Z}$ and not an element in some $\mathbb{Z}_{p^e}$!) then we obtain

$$\langle y_l^*, y_k^*\rangle = c_l c_k \langle v_l^*, v_k^*\rangle = c_l c_k (G^{-1})_{lk} = c_l c_k \langle \widetilde{v_l^*}, \widetilde{v_k^*}\rangle_{\mathbf{Q_p}} = \langle \widetilde{y_l^*}, \widetilde{y_k^*}\rangle_{\mathbf{Q_p}} \quad (4.4)$$

without a "$+\mathbf{Z_p}$". Since the $y_i^* + L$ are a finite basis for D_p, any $x + L \in D_p$ may be expressed as

$$x + L = \sum_{i=1}^{n} \mu_i y_i^* + L$$

for some suitable $\lambda_i \in \mathbb{Z}_{p^{d_i}}$. We select a fixed representative $x = \sum_{i=1}^n \lambda_i y_i^*$ for $\lambda_i := \mu_i \bmod p^{d_i}$. As a fixed representative of $\Phi(x+L) = \sum_{i=1}^n \lambda_i \widetilde{y_i^*} + L$ we select $x'' = \sum_{i=1}^n \lambda_i \widetilde{y_i^*}$ so that $x'' + L_p = x' + L_p$. As all operations in (4.4) are $\mathbb{Z}$-linear, it follows that

$$\langle x, x\rangle = \langle x'', x''\rangle_{\mathbf{Q_p}} \quad (4.5)$$

Notice that these expressions are really equal (up to identification of $\langle x, x\rangle$ with $\nu(\langle x, x\rangle)$ and not equivalent modulo $\mathbf{Z_p}$!). Observe that $\langle x'', x''\rangle_{\mathbf{Q_p}}$ and $\langle x', x'\rangle_{\mathbf{Q_p}}$ are not equal in general, the only thing we know right now is that $\langle x', x'\rangle_{\mathbf{Q_p}} + \mathbf{Z_p} = \langle x'', x''\rangle_{\mathbf{Q_p}} + \mathbf{Z_p}$ as the finite $\mathbf{Z_p}$-bilinear form on L'_p/L_p is well-defined. But we can achieve more: We also know that

$$\langle x', x'\rangle_{\mathbf{Q_p}} + 2\mathbf{Z_p} = \langle x'', x''\rangle_{\mathbf{Q_p}} + 2\mathbf{Z_p} \text{ and } \frac{\langle x', x'\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p} = \frac{\langle x'', x''\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p} \quad (4.6)$$

This is due to the following: By assumption, L is even. By Remark 4.12, L_p is $\mathbf{Z_p}$-even so that the above equations follow from the fact that the finite quadratic $\mathbf{Z_p}$-forms on L_p'/L_p are well-defined by Theorem 4.7(b).

(a): Let $p \neq 2$ and $|D_p| = p^N$ then $p^N(x+L) = 0 + L$ so let $p^N x = x_0$ for some $x_0 \in L$, hence

$$p^{2N}\langle x, x\rangle = \langle p^N x, p^N x\rangle = \langle x_0, x_0\rangle = 2k$$

for some $k \in \mathbb{Z}$ as the lattice is even. Consequently $\langle x, x\rangle = 2k/p^{2N}$. Let $k = p^\nu \cdot r$ with $(r, p) = 1$ then, since $p \neq 2$

$$\langle x, x\rangle = 2\frac{r}{p^{2N-\nu}} \in 2\mathbb{Q}^{(p)}$$

as the leading 2 cannot be canceled because $p \geq 3$ and p is prime. We have shown that $q(x+L) = \langle x, x\rangle + 2\mathbb{Z}$ lies in the domain of half_p. Consequently,

$$\begin{aligned} w_p(\langle x, x\rangle + 2\mathbb{Z}) = \vartheta_p\Big(\frac{\langle x, x\rangle}{2} + \mathbb{Z}\Big) &= \frac{\langle x, x\rangle}{2} + \mathbf{Z_p} \\ &\overset{(4.5)}{=} \frac{\langle x'', x''\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p} \overset{(4.6)}{=} \frac{\langle x', x'\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p} \end{aligned}$$

(b): Let $p = 2$. As in the case above,

$$\langle x, x\rangle = 2\frac{r}{2^{2N-\nu}} \in \mathbb{Q}^{(2)}$$

No matter whether the leading 2 gets canceled or not, $\langle x, x\rangle + 2\mathbb{Z}$ lies in the domain of u_2. Now

$$u_2(\langle x, x\rangle + 2\mathbb{Z}) = \langle x, x\rangle + 2\mathbf{Z_2} \overset{(4.5)}{=} \langle x'', x''\rangle_{\mathbf{Q_2}} + 2\mathbf{Z_2} \overset{(4.6)}{=} \langle x', x'\rangle_{\mathbf{Q_2}} + 2\mathbf{Z_2}$$

(c) is shown analogously to (a):

$$\vartheta_p\left(\frac{\langle x, x\rangle}{2} + \mathbb{Z}\right) \overset{(4.5)}{=} \frac{\langle x'', x''\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p} \overset{(4.6)}{=} \frac{\langle x', x'\rangle_{\mathbf{Q_p}}}{2} + \mathbf{Z_p}$$

□

4.33 Remark. *(a) In particular, the quadratic form behaves as expected on the $g_i^* + L$ from 4.30*(b)*: Using $\Phi(g_i^* + L) = \widetilde{g}_i^* + L_p$ where $\widetilde{g}_i^* = (S^{-1}C^{-1}, i.row) * [\widetilde{y}_1^*, ..., \widetilde{y}_n^*]$ we see that we may select $\widetilde{g}_i^*$ as x' for $\Phi(g_i^* + L)$. By the above theorem,*

$$Q(g_i^* + L) = \vartheta_p^{-1}\left(\frac{\langle \widetilde{g}_i^*, \widetilde{g}_i^*\rangle}{2} + \mathbf{Z_p}\right) = \vartheta_p\left(\frac{H_{ii}^{-1}}{2} + \mathbf{Z_p}\right)$$

where $H = S^T G S$ is intended to be the simplified Gram-matrix over $\mathbf{Z_p}$ as in 4.30(b).

(b) *Here we can see the advantage of the usage of Q instead of q as we obtain a relation that holds for all p. When using q, we have to distinguish whether $p = 2$ or $p \neq 2$.*

(c) *Another remark on the special relation in the case $p = 2$: We could call a Lattice $(L, \langle \cdot, \cdot \rangle)$ "p-even" for $p \neq 2$ if $\langle x, x \rangle \in p\mathbb{Z}$ for all $x \in L$, then $\langle x + L, x + L \rangle$ is well-defined modulo $p\mathbb{Z}$ instead of $2\mathbb{Z}$. If we set*

$$u_p : {}^{\mathbb{Q}^{(p)}}\Big/_{p\mathbb{Z}} \mapsto {}^{\mathbf{Q_p}}\Big/_{p\mathbf{Z_p}}, \quad u_p\left(\frac{k}{p^\nu}\right) + p\mathbb{Z} := \frac{k}{p^\nu} + p\mathbf{Z_p}$$

then we can show that u_p is an isomorphism of abelian groups and $\mathbb{Z}$-modules and obtain an analogous relation for $\mathbf{Z_p}$ with u_p instead of $\mathbf{Z_2}$ with u_2. The alternative relation is therefore not caused by the "oddness" of the number 2, it is caused by us as we want the lattice to be "2-even" and not "p-even".

Now we finalize both results achieved above to construct a finite basis of the discriminant form on which the finite bilinear form behaves very simple. We formalize this structure in the Jordan decomposition:

4.34 Definition. *Let (L, v, G) be an integral (even respectively) $\mathbb{Z}$-lattice and $D = L'/L$ its discriminant form (including a finite quadratic form if L is even). A Jordan-decomposition for D is defined to be a set of matrices $S_p \in {\mathbf{Z_p}}^{n \times n}, (p \in \mathbb{P})$ such that*

1. $S_p \in \mathbf{Z_p}, \det(S_p) \in {\mathbf{Z_p}}^\times$.
2. $H_p := S_p^T G S_p \in (\mathbb{Q} \cap \mathbf{Z_p})^{n \times n}$
3. *H_p is diagonal if $p \neq 2$ and if $p = 2$, it has the structure $H_2 = S_2^T G S_2 = X_1 \perp ... \perp X_f \perp \operatorname{diag}(\alpha_1, ..., \alpha_{f'})$ for some (2×2)-matrices X_j.*

Now the question arises why we should call a set of matrices a Jordan decomposition for D. Let us fix $p \in \mathbb{P}, p \neq 2$, let $H := H_p = p^0 H_{p^0} \perp p^1 H_{p^1} \perp ...$, so that $\operatorname{symbol}_p(G) := \prod_{q \in p^{\mathbb{N}_0}} q^{\epsilon_q n_q}$ as in Definition 3.12. Fix $n \in \mathbb{N}$ and put $q = p^n$. Let $qH_q = \operatorname{diag}(\alpha_1, ..., \alpha_{n_q})$ and $\alpha_j = q\beta_j$ with $\beta_j \in {\mathbf{Z_p}}^\times$. Set $N_q = n_{p^0} + ... + n_{p^{n-1}}$ and set $\widetilde{g}_i^* + L_p, g_i^* + L$ to be as in Theorem 4.30(b). Put $\widetilde{g}_i := (S, \text{i.row}) * [\widetilde{v}_1, ..., \widetilde{v}_n]$ in the $\mathbf{Q_p}$-vector space (not $\widetilde{g}_i := ([\![S]\!], \text{i.row}) * ...!$) so that the Gram-matrix w.r.t. the $\widetilde{g}_i$ is precisely H. We write $D(q^{\epsilon_q, n_q})$ for the subgroup of D generated by the $g_i^* + L$, $N_q + 1 \leq i \leq N_q + n_q$ and we lazily write q^{ϵ_q, n_q} not only for the factor in the Jordan symbol but also for the part of H_p induced by the $\widetilde{g}_i, N_q + 1 \leq i \leq N_q + n_q$,

i.e. $q^{\epsilon_q,n_q} := (\langle \widetilde{g}_i, \widetilde{g}_j \rangle_{\mathbf{Q_p}})_{i,j=N_q+1,\ldots,N_q+n_q} \in \mathbb{Q}^{n_q \times n_q}$. We define the p-excess for this subgroup to be

$$p\text{–excess}(D(q^{\epsilon_q,n_q})) := p\text{–excess}(q^{\epsilon_q,n_q})$$

where the right hand term is to be read as in definition 3.9. Analogously we define the oddity and so on for $p = 2$. Let $g_i^{*,(p)} + L, 1 \leq i \leq n$ be the finite basis of D_p then rename the vectors $g_1^{*,(2)} + L, ..., g_n^{*,(2)} + L, g_1^{*,(3)} + L, ...$ to $x_1^* + L, x_2^* + L, ...$, then this is a finite basis of whole D due to Theorem 4.17 and the fact that the $g_i^{*,(p)} + L$ form a finite basis of D_p. As this theorem states that the decomposition is orthogonal, the "Gram-matrix" $X = ((x_i^* + L, x_j^* + L))_{i,j}$ of the finite bilinear form $(\cdot,\cdot)$ on D (which is a matrix over $\mathbb{Q}/\mathbb{Z}$) has the structure

$$X = \begin{pmatrix} * & * & & & & & & & & & & \\ * & * & & & & & & & & & & \\ & & * & * & & & & & & & & \\ & & * & * & & & & & & & & \\ & & & & \ddots & & \ddots & & & & & \\ & & & & & & & * & * & & & \\ & & & & & & & * & * & & & \\ & & & & & & & & & * & & \\ & & & & & & & & & & * & \\ & & & & & & & & & & & \ddots \\ & & & & & & & & & & & & * \end{pmatrix} + \mathbb{Z}$$

where any missing entry is to be read as $0 + \mathbb{Z}$, i.e. the matrix has a shape which looks similar to the usual Jordan decomposition of a matrix over $\mathbb{C}$.

In current papers that deal with discriminant forms one mostly finds a short introduction and a certain claim on the structure of the discriminant form – cf. [Sch], lower half of Page 5 or [Bo], Page 5-6 –, namely that one can find a Jordan decomposition for which the finite bilinear form has a very simple structure. We will now present and formally prove this assertion.

For a subset $S \subset D$ of a discriminant form D we define the level of S

$$L(S) := \min\{n \in \mathbb{N} \mid n \cdot Q(\gamma) = 0 + \mathbb{Z} \text{ for all } \gamma \in S\}$$

4.35 Theorem. *Let $(L, \langle \cdot,\cdot \rangle)$ be an even lattice with fixed basis v and Gram matrix G (with respect to that basis) and let $D = L'/L$ be its discriminant*

form. Fix $p \in \mathbb{P}, p \neq 2$ then the p-component of D decomposes into a direct orthogonal sum of Jordan components $D(q^{\epsilon_q n_q})$ for $q = p^\nu \in p^{\mathbb{N}}$. The p-excess is given by $p\text{–excess}(D(q^{\epsilon_q n_q})) = n_q(q-1) + 4k \mod 8$ where

$$k = \begin{cases} 1 & \text{if } \nu \text{ is odd and } \epsilon_q = -1 \\ 0 & \text{otherwise, i.e. if } \nu \text{ is even or } \epsilon_q = +1 \end{cases}$$

and the level is precisely q. The so-called indecomposable Jordan constituents $D(q^{\epsilon_q \cdot 1})$ are generated by a single element $x + L \in D_p$ with $\operatorname{ord}(x+L) = q$, $Q(x) = \langle x, x\rangle/2 + \mathbb{Z} = a/q + \mathbb{Z}$ where $a \in \mathbb{Z}$ satisfies $(\frac{2a}{p}) = \epsilon$.
The finite basis of D_p that satisfies all these properties is exactly the one generated in Theorem 4.30 (b) *when using $S_p = S$ from Lemma 3.3.*

Proof. Choose a basis v for L and let G be the gram matrix w.r.t. the basis v. Using Lemma 3.3, we find a matrix $S \in \mathbf{Z_p}^{n\times n}$ such that $H := S^T G S = \operatorname{diag}(\alpha_1, ..., \alpha_n)$. Resort the $\alpha_1, ..., \alpha_n$ so that for fixed $q = p^\nu, \alpha_1 = p^\nu\beta_1, ..., \alpha_{n_q} = p^\nu\beta_{n_q}$ with $|\beta_j|_p = 1$ and $\alpha_k = p^{\mu_k}\beta_k$ with $\mu_k \neq \nu$ for all $k > n_q$. The matrix H has the form $H = \operatorname{diag}(\alpha_1, ..., \alpha_{n_q}) \perp ...$ causing the Jordan symbol to look like $\operatorname{symbol}_p(G) = q^{\epsilon_q n_q} \cdot (\text{ other } q\text{-factors })$.
Applying Theorem 4.30 (b) yields a finite basis $g_1^* + L, ..., g_{n_q}^* + L, g_{n_q+1}^* + L, ..., g_n^* + L$ of D_p satisfying

$$((g_i^* + L, g_j^* + L))_{i,j=1,...,n} = \vartheta_p^{-1}(H^{-1})$$

This is precisely the claim on the orthogonality as H^{-1} is a diagonal matrix. On the p-excess:

$$\begin{aligned} p\text{–excess}(q^{\epsilon_q n_q}) &= p\text{-excess of the corresponding part in the} \\ &\qquad \text{original bilinear form } H \\ &= p\text{–excess}(\operatorname{diag}(\alpha_1, ..., \alpha_{n_q})) \\ &= \operatorname{sig}_p(\operatorname{diag}(\alpha_1, ..., \alpha_{n_q})) - n_q \mod 8 \\ &= \operatorname{sig}_p(\operatorname{diag}(q\beta_1, ..., q\beta_{n_q})) + 4k - n_q \mod 8 \\ &= \underbrace{q + ... + q}_{n_q \text{ times}} + 4k - n_q \mod 8 \\ &= n_q(q - 1 + 1) + 4k - n_q \end{aligned}$$

where k is the amount of antisquares among $\{\alpha_1, ..., \alpha_{n_q}\}$. We have to show that we can choose k to be

$$k = \begin{cases} +1 & \text{if } \nu \text{ is odd and } \epsilon_q = -1 \\ 0 & \text{otherwise} \end{cases}$$

Let ν be even. Then, $k = 0$ actually, because non of the $\alpha_i = q\beta_i = p^\nu \beta_i$ is an antisquare. Let ν be odd but $\epsilon_q = +1$. Then,

$$+1 = \left(\frac{\det(\beta_1, ..., \beta_{n_q})}{p}\right) = \left(\frac{\beta_1}{p}\right) \cdot ... \cdot \left(\frac{\beta_{n_q}}{p}\right)$$

so that the amount of β_i producing $(\frac{\beta_i}{p})$ = -1 must be even, let those β_i be $\beta_1, ..., \beta_{2r}$. Since ν is odd, $\alpha_1, ..., \alpha_{2r}$ are antisquares, $\alpha_{2r+1}, ..., \alpha_n$ are not. Hence, $k = 2r$ so that $4k \equiv 4 \cdot 2 \cdot r \equiv 0 \mod 8$.

Let ν be odd and $\epsilon_q = -1$, then (by the same reason as above) the amount of antisquares must be $2r + 1$ so that

$$4k \equiv 4 \cdot 2 \cdot r + 4 \equiv 4 \cdot 1 \mod 8$$

The level of $D(q^{\epsilon_q n_q})$ is precisely q because: In the $\mathbf{Q_p}$-vector space, $q\widetilde{g}_i^* = q\widetilde{w}_i^* \in L_p$ (see the proofs of the Theorems 4.30 – in particular equation (4.2)– and 4.32) so that $\Phi(qg_i^* + L) = q\widetilde{g}_i^* + L_p = 0 + L_p$ and thus $qg_i^* + L = 0 + L$ as Φ is injective. Conversely, let $n \in \mathbb{N}$ such that $n(x + L) = 0 + L$ for all $x + L \in D(q^{\epsilon_q n_q})$. Then in particular $ng_i^* + L = 0 + L$ and hence applying Φ yields

$$\frac{n}{q}\beta_i^{-1}\widetilde{g}_i = n\widetilde{g}_i^* = \sum_{j=1}^{n} \gamma_j \widetilde{g}_j$$

for some $\gamma_j \in \mathbf{Z_p}$. As the $\widetilde{g}_i$ are $\mathbf{Q_p}$-linearly independent, $n/q \in \mathbf{Z_p}$, i.e. $|n/q|_p \leq 1$ which means nothing else than $q \mid n$. Summarized, q is the smallest natural number that nulls all $Q(\gamma), \gamma \in D(q^{\epsilon_q n_q})$.

On the indecomposable Jordan blocks: What is meant by $D(q^{\epsilon_q \cdot 1})$ is a single summand $\mathbb{Z}_q g_i^* + L$ of $D(q^{\epsilon_q n_q})$. It is generated (as a subgroup) by the single element $g_i^* + L$. Set $g^* := g_i^*, \beta := \beta_i$ and $\alpha := \alpha_i$ so that $\alpha = q\beta$ and β is a unit in $\mathbf{Z_p}$. By Remark 4.33(a) we have

$$Q(g^* + L) = \frac{\langle g^*, g^* \rangle}{2} + \mathbb{Z} = \vartheta_p^{-1}\left(\frac{\alpha^{-1}}{2} + \mathbf{Z_p}\right) \tag{4.7}$$

Let $(2\beta)^{-1} = x_0 + x_1 p + x_2 p^2 + ... + x_{\nu-1} p^{\nu-1} + p^\nu \gamma$, $\gamma \in \mathbf{Z_p}$, be the p-adic expansion. Put $a := x_0 + x_1 p^{\nu-2} + ... + x_{\nu-1} p^{\nu-\nu}$ (i.e. $a = R_{p^\nu}(1/2\beta)$) then

$$
\begin{aligned}
Q(g^* + L) &= \vartheta_p^{-1}[\frac{(q\beta)^{-1}}{2} + \mathbf{Z_p}] && \text{(by (4.7))} \\
&= \vartheta_p^{-1}[\frac{1}{q}(x_0 + x_1 p + ... + x_{\nu-1}p^{\nu-1}) + \underbrace{\frac{\not{q}}{2\not{q}}\gamma}_{\in \mathbf{Z_p}} + \mathbf{Z_p}] \\
&= \vartheta_p^{-1}[\frac{1}{q}(x_0 + x_1 p + ... + x_{\nu-1}p^{\nu-1}) + \mathbf{Z_p}] \\
&= \frac{a}{q} + \mathbb{Z}
\end{aligned}
$$

Since $1 = |1/(2\beta)|_p$, $x_0 \neq 0$ so that $(2a, p) = 1$ and therefore, the expression $(\frac{2a}{p})$ makes sense. According to Lemma 3.5, we have

$$
2a = 2R_{p^\nu}(\frac{1}{2\beta}) = R_{p^\nu}\left(2\frac{1}{2\beta}\right) + dp^\nu = R_{p^\nu}\left(\frac{1}{\beta}\right) + dp^\nu \tag{4.8}
$$

for some $d \in \mathbb{Z}$. Hence, $(\frac{2a}{p}) = (\frac{1/\beta}{p})$ as the extended Legendre symbol is only defined modulo p in the numerator. Further,

$$
R_q(\beta)R_q(\beta^{-1}) \equiv R_q(\beta\beta^{-1}) \equiv 1 \mod q
$$

so that

$$
1 = \left(\frac{1}{p}\right) = \left(\frac{R_q(\beta)R_q(\beta^{-1})}{p}\right) = \left(\frac{R_q(\beta)}{p}\right)\left(\frac{R_q(\beta^{-1})}{p}\right)
$$

which means nothing else than

$$
\left(\frac{R_q(\beta)}{p}\right) = \left(\frac{R_q(\beta^{-1})}{p}\right)^{-1} = \left(\frac{R_q(\beta^{-1})}{p}\right) \tag{4.9}
$$

as the Legendre symbol only produces values in $\{\pm 1\}$. Consequently,

$$\begin{aligned}
\epsilon &= \left(\frac{\det(\substack{\text{the part of the } 1\times 1 \text{ matrix}\\ (\alpha) \text{ without the } p\text{-power}})}{p}\right) \\
&= \left(\frac{\beta}{p}\right) \\
&= \left(\frac{R_p(\beta)}{p}\right) && \text{(def. of the Symbol on } \mathbf{Z_p}\text{-numbers)} \\
&= \left(\frac{R_{p^\nu}(\beta)}{p}\right) && \text{(as the numerators coincide modulo } p) \\
&= \left(\frac{R_q(\beta^{-1})}{p}\right) && \text{(by (4.9))} \\
&= \left(\frac{2a}{p}\right) && \text{(by (4.8))}
\end{aligned}$$

□

4.36 Theorem. *Let $(L, \langle\cdot,\cdot\rangle)$ be an even lattice with fixed basis v and Gram matrix G (with respect to that basis), let $D = L'/L$ be its discriminant form and let $p = 2$. There is a finite basis of D_2 such that D_2 decomposes into a direct orthogonal sum of Jordan components $D(q_{t_q,S_q}^{\epsilon_q n_q})$ for $q \in p^{\mathbb{N}_0}$. A finite basis producing such blocks is given in Theorem 4.30* (b) *when selecting $S_2 = S$ as in Corollary 3.18. This matrix has the property that $H = S^T G S = 2^0 H_{2^0} \perp 2^1 H_{2^1} \perp \ldots$ is almost diagonal in the sense that for a summand H_q, we have $qH_q = qD_1 \perp \ldots \perp qD_f \perp \operatorname{diag}(\alpha_1, \ldots, \alpha_{f'})$ where either $f = 0$ or $f' = 0$, i.e. the blocks of H are either purely even or purely odd but no mixture of both. Further, this finite basis of D_2 possesses the properties that*

(a) The (purely) even blocks $D(q_{0,II}^{\epsilon_q,n_q})$ for $q = 2^\nu$ are of level q and their oddity is given by $4k \mod 8$ where

$$k = \begin{cases} 1 & \text{if } \nu \text{ is odd and } \epsilon_q = -1 \\ 0 & \text{otherwise} \end{cases}$$

The so-called indecomposable even Jordan blocks $q_{0,II}^{\epsilon,2}$ are generated by two elements $x + L, y + L$ such that

- $\operatorname{ord}(x + L) = \operatorname{ord}(y + L) = q$
- $(x + L, y + L) = 1/q + \mathbb{Z}$

- $Q(x+L) = Q(y+L) = 0+\mathbb{Z}$ *if* $\epsilon = +1$ *and* $Q(x+L) = Q(y+L) = 1/q + \mathbb{Z}$ *otherwise*

(b) The (purely) odd blocks $D(q^{\epsilon_q,n_q}_{t_q,I})$ *for* $q = 2^\nu$ *are of level* $2q$ *and their oddity is given by* $t_q + 4k \mod 8$ *where*

$$k = \begin{cases} 1 & \text{if } \nu \text{ is odd and } \epsilon_q = -1 \\ 0 & \text{otherwise} \end{cases}$$

The so-called indecomposable odd Jordan blocks $D(q^{\epsilon,1}_{t,I})$ *are generated by a single element* $x + L$ *such that*

- $\mathrm{ord}(x + L) = q$
- $Q(x + L) = t/2q + \mathbb{Z}$
- $\left(\frac{t}{2}\right) = \epsilon$

Proof. The assertion on the oddity is proven by a relatively long but straightforward computation, hence it is left to the reader. The orthogonal decomposition is proved exactly as in the case $p \neq 2$ (cf. Thm. 4.35). On the level of the even blocks: Fix q such that $qH_q = qD_1 \perp ... \perp qD_f$ (i.e. $f' = 0$). For $q = 2^\nu$ set $N_q := n_{2^0} + ... + n_{2^{\nu-1}}$. Let $x_1^* + L, y_1^* + L, ..., x_{n_q}^* + L, y_{n_q}^* + L$ be the vectors forming a finite basis of $D(q^{\epsilon_q,n_q})$ as in 4.30 (b) (we have renamed $g^*_{N_q+1}$ to x_1^*, $g^*_{N_q+2}$ to y_1^*, $g^*_{N_q+3}$ to x_2^* and so forth). In the language of this theorem, $H = qH_q$ and $H^{-1} =$ Gram matrix with respect to the vectors $\widetilde{g}_i^* = q^{-1}(D_1^{-1} \perp ... D_f^{-1})$ so that for some arbitrary $x + L = \lambda_1 x_1^* + \mu_1 y_1^* + ... + \lambda_f x_f^* + \mu_f y_f^* + L \in D(q^{\epsilon_q,n_q})$ with $\lambda_i, \mu_i \in \mathbb{Z}$, we have by Theorem 4.32 $qQ(x+L) = q\vartheta_2^{-1}(\langle x', x'\rangle_{\mathbf{Q_p}}/2 + \mathbf{Z_2})$ for $x' = \lambda_1 \widetilde{x}_1^* + \mu_1 \widetilde{y}_1^* + ... + \lambda_f \widetilde{x}_f^* + \mu_f \widetilde{y}_f^*$ (where we have renamed $\widetilde{g}^*_{N_q+1}$ to $\widetilde{x}_1^*$, $\widetilde{g}^*_{N_q+2}$ to $\widetilde{y}_2^*$ and so forth analogously to the renaming process above). Now

$$\begin{aligned} &q\vartheta_2^{-1}(\langle x', x'\rangle_{\mathbf{Q_p}}/2 + \mathbf{Z_2}) \\ &\quad = q\vartheta_2^{-1}(\sum_{i=1}^{f} \underbrace{\langle \widetilde{x}_i^*, \widetilde{x}_i^*\rangle/2 + \langle \widetilde{y}_i^*, \widetilde{y}_i^*\rangle/2 + \langle \widetilde{x}_i^*, \widetilde{y}_i^*\rangle}_{:=a_i} + \mathbf{Z_2}) \end{aligned}$$

If $D_i = D_{(+1)}$ then $(qD_i)^{-1} = \left(\begin{smallmatrix} 0 & 1/q \\ 1/q & 0 \end{smallmatrix}\right)$ so that

$$\langle \widetilde{x}_i^*, \widetilde{x}_i^*\rangle_{\mathbf{Q_2}}/2 = 0, \quad \langle \widetilde{y}_i^*, \widetilde{y}_i^*\rangle_{\mathbf{Q_2}}/2 = 0, \quad \langle \widetilde{x}_i^*, \widetilde{y}_i^*\rangle_{\mathbf{Q_2}} = 1/q \tag{4.10}$$

and hence

$$q\vartheta_2^{-1}(a_i) = q(0 + 0 + 1/q) + \mathbb{Z} = 1 + \mathbb{Z} = 0 + \mathbb{Z}$$

If $D_i = D_{(-1)}$ then $(qD_i)^{-1} = \left(\begin{smallmatrix} 2/q & 1/q \\ 1/q & 2/q \end{smallmatrix}\right)$ so that

$$\frac{\langle \widetilde{x}_i^*, \widetilde{x}_i^* \rangle_{\mathbf{Q_2}}}{2} = \frac{2/q}{2} = \frac{1}{q}, \quad \frac{\langle \widetilde{y}_i^*, \widetilde{y}_i^* \rangle_{\mathbf{Q_2}}}{2} = \frac{2/q}{2} = \frac{1}{q}, \quad \langle \widetilde{x}_i^*, \widetilde{y}_i^* \rangle_{\mathbf{Q_2}} = \frac{1}{q} \tag{4.11}$$

and hence

$$q\vartheta_2^{-1}(a_i) = q(1/q + 1/q + 1/q) + \mathbb{Z} = 3 + \mathbb{Z} = 0 + \mathbb{Z}$$

Let $d = L(D(q^{\epsilon_q, n_q}))$, then we have shown that $qQ(x + L) = 0 + \mathbb{Z}$ for all $x + L \in D(q^{\epsilon_q, n_q})$ and hence, $d \leq q$. Since in particular

$$0 + \mathbb{Z} = dQ(y_1^* + L) = d(1/q + \mathbb{Z})$$

as computed above, $d/q \in \mathbb{Z}$ and therefore $q \mid d$ and finally $d \leq q$ so that $q = d$. On the indecomposable even components: What is meant is a subgroup generated by two fixed elements $x_i^* + L, y_i^* + L$ for some q, x_i^*, y_i^* as above. The values of the finite bilinear and quadratic form on those vectors have been computed in (4.10) and (4.11). With the help of (4.10) and (4.11), the orders of $x_i^* + L$ and $y_i^* + L$ are easily computed to be q. For example, let $D_i = D_{(+1)}$. Let $\widetilde{x}_i, \widetilde{y}_i$ be the original vectors in $L_p \subset \widetilde{V}$ (which are actually $\widetilde{g}_{N_q+2i}$, $\widetilde{g}_{N_q+2i+1}$) that produce $\widetilde{x}_i^*, \widetilde{y}_i^*$ as dual vectors, then $\widetilde{x}_i^* = (H^{-1}, \text{i.col}) * [\widetilde{g}_1, ..., \widetilde{g}_n] = (D_{(+1)}, 1.\text{col}) * [\widetilde{x}_i, \widetilde{y}_i] = \frac{1}{q}\widetilde{y}_i$ because of the almost diagonal structure of H^{-1}. This means that $n \cdot \widetilde{x}_i^* \in L_p \iff \frac{a}{q}\widetilde{y}_i \in L_p \iff a/q \in \mathbf{Z_p} \iff q \mid a$ as $L_p = \mathbf{Z_p}\widetilde{x}_i \oplus \mathbf{Z_p}\widetilde{y}_i \oplus ....$ Using the injectivity of Φ as in the case $p \neq 2$ we also obtain that $ax_i^* + L = 0 + L \iff a\widetilde{x}_i^* \in L_p$ and finally $q \mid \text{ord}(x_i^* + L)$, i.e. $q \leq \text{ord}(x_i^* + L)$ and, using the equations above again, the other direction is clear as $q\widetilde{x}_i^* + L_p = \widetilde{y}_i + L_p = 0 + L_p$.

On the level of the odd blocks: We fix q such that $qH_q = \text{diag}(\alpha_1, ..., \alpha_{f'})$ (i.e. it is a purely odd block, $f_q = 0$) and write $\alpha_i = q\beta_i$ with $\beta_i \in (\mathbb{Q} \cap \mathbf{Z_2})^\times$. Let $x_1^* + L, ..., x_{f'}^* + L$ form a finite basis of $D(q_{t_q,\text{I}}^{\epsilon_q, n_q})$ as in 4.30 (b) (we have renamed $g_{N_q+1}^*$ to x_1^*, $g_{N_q+2}^*$ to x_2^* and so forth). Now any $x + L \in D(q_{t_q,\text{I}}^{\epsilon_q, n_q})$ may be written as $x + L = \sum_{i=1}^{f'} \lambda_i x_i^* + L$ for some $\lambda_i \in \mathbb{Z}$. If we set $x' = \sum_{i=1}^{f'} \lambda_i \widetilde{x}_i^* + L$ (where we have renamed $\widetilde{g}_{N_q+1}^*$ to $\widetilde{x}_1^*$, $\widetilde{g}_{N_q+2}^*$ to $\widetilde{x}_2^*$ and

so forth) then by Theorem 4.32,

$$\begin{aligned} 2qQ(x+L) &= 2q\vartheta_2^{-1}(\langle x', x'\rangle/2 + \mathbf{Z_2}) \\ &= \sum_{i=1}^{f'} \lambda_i 2q\vartheta_2^{-1}(\langle \widetilde{x}_i^*, \widetilde{x}_i^*\rangle/2 + \mathbf{Z_2}) \\ &= \sum_{i=1}^{f'} \lambda_i 2q\vartheta_2^{-1}(\alpha_i^{-1}/2 + \mathbf{Z_2}) \\ &= \sum_{i=1}^{f'} \lambda_i 2q\vartheta_2^{-1}(\beta_i^{-1}/2q + \mathbf{Z_2}) \end{aligned}$$

Let $q = 2^\nu$, $\beta_i^{-1} = s_i + 2q(\beta_i')^{-1}$ as in 2.10 with $s_i = s_{i,0} + s_{i,1}2^1 + ... + s_{i,\nu}2^\nu$ and $s_{i,0} \neq 0$ as $\beta_i \in \mathbf{Z_2}^\times$ (cf. 2.8), i.e. s_i is an odd integer. Then

$$\lambda_i 2q\vartheta_2^{-1}(\beta_i^{-1}/2q + \mathbf{Z_2}) = \lambda_i 2q\frac{s_i}{2q} + \mathbb{Z} = \lambda_i s_i + \mathbb{Z} = 0 + \mathbb{Z}$$

Set $l := L(D(q_{t_q,\mathrm{I}}^{\epsilon_q,n_q}))$, then we have shown $l \leq 2q$. Since in particular

$$0 + \mathbb{Z} = lQ(x_1 + L) = l(s_1/2q) + \mathbb{Z}$$

we have $ls_1/2q \in \mathbb{Z}$, i.e. $2q \mid ls_1$ but as s_1 is odd, $2q \mid l$ and thus $2q \leq l$ and finally $l = 2q$. On the assertions of the indecomposable odd blocks: What is meant is $D(q_{t,\mathrm{I}}^{\epsilon,1}) = \langle x^* + L\rangle$ (the subgroup of D generated by $x^* + L$) for x^* being one of the x_i^* as above. Put $\alpha := \alpha_i, \beta = \beta_i$. The order of $x^* + L$ is computed exactly as in the case $p \neq 2$. We have

$$t_q = \mathrm{sig}_2(\substack{\text{the } 1\times 1 \text{ matrix } (\alpha_i) \\ \text{without the leading 2-power}}) = \mathrm{sig}_2((\beta_i)) \equiv R_8(\beta_i) + 4\cdot 0 \mod 8$$

because $\beta_i = 2^0\beta_i$ and therefore it is not an antisquare. Further,

$$\epsilon = \left(\frac{\det\left(\substack{\text{the } 1\times 1 \text{ matrix } (\alpha_i) \\ \text{without the leading 2-power}}\right)}{2}\right) = \left(\frac{\beta_i}{2}\right) = \left(\frac{t}{2}\right)$$

(the extended Legendre symbol $(\frac{\cdot}{2})$ only depends on $\cdot \mod 8$). The last line of the assertions of the theorem is in particular interesting because stated like this, it is utterly senseless: t is (by definition!) a class modulo 8 but the expression $t/2q + \mathbb{Z}$ is not even well-defined if t is only determined modulo 8 and $q = 16, 32, ...$! What is meant is the following: Chose an arbitrary

representative t' of the class $t \mod 8$, then we find another generator of $D(q_{t,\mathrm{I}}^{\epsilon,1})$ (those are precisely given by $y^* + L = ax^* + L$ where $a \in \mathbb{Z}$ is prime to the size of $\langle x^* + L\rangle = q$, i.e. it is odd) such that $Q(y^* + L) = t'/2q \mod \mathbb{Z}$. Proof of this statement:

Let $\alpha = q\beta$ and $\beta \in \mathbf{Z_2}^\times, \beta^{-1} = s + 2q'\gamma$ for some $\gamma \in \mathbf{Z_p}$ with s being an odd integer (cf. 2.8, 2.10) and $q' = q$ if $\nu \geq 2$ and $q' = 4$ otherwise. Let $q = 2^\nu$. If $\nu \leq 2$ then there is nothing to do as the expression $t/2q$ is well-defined modulo $\mathbb{Z}$, so let $\nu > 2$, i.e. $2q > 8$ and $q = q'$. In $\mathbb{Z}_8$, every square of a unit is congruent to 1. Since R_8 is multiplicative, it follows that $R_8(\beta) \equiv R_8(\beta^{-1}) \mod 8$. By Theorem 4.32 we have $Q(x^*+L) = \vartheta_2^{-1}(\beta^{-1}/2q+\mathbf{Z_2}) = s/2q'+\mathbb{Z}$ and as $2q' \geq 8$, $R_8(s) \equiv R_8(\beta) \equiv R_8(\beta^{-1}) \equiv t \mod 8$. We have shown that there exists $k \in \mathbb{Z}$ such that $t = s + 8k$. Since s is odd, it is a unit in $\mathbb{Z}_{2q}$. Chose an arbitrary representative $u \in \mathbb{Z}$ such that $u \equiv s^{-1} \mod 2q$, then

$$\begin{aligned} Q(ax^* + L) = t/2q + \mathbb{Z} &\iff a^2 Q(x^* + L) = t/2q + \mathbb{Z} \\ &\iff a^2 s/2q = t/2q + \mathbb{Z} = (s + 8k)/2q \\ &\iff a^2 s \equiv s + 8k \mod 2q \\ &\iff a^2 \equiv 1 + 8ku \mod 2q \end{aligned} \tag{4.12}$$

i.e. we have to find a square root of the odd integer $1 + 8ku \in \mathbb{Z}$ modulo $2q$. The following lemma was originally deduced by Gauss:

4.37 Lemma. *Let $N = 2^\mu$ for $\mu > 3$, then an odd integer $x \in \mathbb{Z}$ is a square in $\mathbb{Z}_N$ (meaning that there exists an odd integer $a \in \mathbb{Z}$ such that $a^2 \equiv x \mod N$) if and only if $x \equiv 1 \mod 8$.*

Proof. See [Ga]. □

Since $1 + 8ku \equiv 1 \mod 8$ we always find an odd a that satisfies (4.12) and therefore, $y^* + L := ax^* + L$ is the new generator satisfying $Q(y^* + L) = t/2q + \mathbb{Z}$. This completes the proof. □

In the rest of this section we are going to define some invariants of discriminant forms. Let $(L, v, G), (M, w, H)$ be two R-lattices with $L \subset K^n, m \subset K^m$ then we define the R-lattice set $L \oplus M := R(v_1 \times 0) \oplus ... \oplus R(v_n \times 0) \oplus R(0 \times w_1) \oplus ... \oplus R(0 \times w_m) \subset K^n \times K^m = K^{n+m}$ and embed this vector space with the K-bilinear form having Gram matrix $G \obot H$. The resulting lattice will be denoted by $L \obot M$ for short.

4.38 Theorem. *Let $(L, v, G), (\widetilde{L}, \widetilde{v}, \widetilde{G})$ be two even $\mathbb{Z}$-lattices. L and $\widetilde{L}$ have the same discriminant form D as their discriminant form, i.e. $D \cong L'/L \cong \widetilde{L}'/\widetilde{L}$ as discriminant forms (including the finite quadratic form), if and only if there exist even unimodular $\mathbb{Z}$-lattices $(M, b, A), (\widetilde{M}, \widetilde{b}, \widetilde{A})$ such that $L \oplus M \cong_{\mathbb{Z}} \widetilde{L} \oplus \widetilde{M}$ (meaning that $(G \oplus A) \sim_{\mathbb{Z}} (\widetilde{G} \oplus \widetilde{A})$ in the sense of Definition 3.1).*

Proof. See the references in [Ni], Thm 1.3.1. □

Now let D be a discriminant form including a finite quadratic form, $(L, v, G), (\widetilde{L}, \widetilde{v}, \widetilde{G})$ even $\mathbb{Z}$-lattices and $(M, b, A), (\widetilde{M}, \widetilde{b}, \widetilde{A})$ even unimodular $\mathbb{Z}$-lattices such that $D \cong L'/L \cong \widetilde{L}'/\widetilde{L}$ and $L \oplus M \cong_{\mathbb{Z}} \widetilde{L} \oplus \widetilde{M}$ as in the theorem above. Let $M \subset \mathbb{Q}^n$ and $2 \neq p \in \mathbb{P}$. Since M is univariate, $M' = M$ which means that the discriminant form of M is trivial, $M'/M \cong \{1\}$. If we diagonalize A to some matrix $A \sim_{\mathbf{Z_p}} A' = p^0 A_{p^0} \oplus ... \oplus p^N A_{p^N}$ over $\mathbf{Z_p}$ as in Lemma 3.3 then Thm. 4.28 tells us that the p-component of D is given by $\mathbb{Z}_{p^0}^{\dim(A_{p^0})} \times ... \times \mathbb{Z}_{p^N}^{\dim(A_{p^N})} \cong \{1\}$ and this can only be true if $N = 0$ and $A' = A_{p^0}$. Hence, $A \sim_{\mathbf{Z_p}} \operatorname{diag}(p^0\epsilon_1, ..., p^0\epsilon_n)$ for some $\epsilon_i \in \mathbf{Z_p}^\times$. We compute the p-signature of M to be $\operatorname{sig}_p(M) = p^0 + ... + p^0 + 4 \cdot 0 \equiv n \mod 8$, hence, $p\text{–excess}(M) \equiv 0 \mod 8$. Analogously, $p\text{–excess}(\widetilde{M}) \equiv 0 \mod 8$ so that $p\text{–excess}(L) \equiv p\text{–excess}(L \oplus M) \equiv p\text{–excess}(\widetilde{L} \oplus \widetilde{M}) \equiv p\text{–excess}(\widetilde{L})$ and finally,

$$p\text{–excess}(D) := p\text{–excess}(L) \text{ for any arbitrary even lattice } L \text{ with } L'/L \cong D$$

is well-defined. Using Milgrams formula (see [Mil], Appendix 4, the first theorem) one can show that in the situation above, $\operatorname{sig}_{-1}(L) \equiv \operatorname{sig}_{-1}(\widetilde{L}) \mod 8$ so that we may define $\operatorname{sig}(D) := \operatorname{sig}_{-1}(L)$ to be the signature of D. This number does not depend on the chosen lattice L.
The following relation is called the oddity formula. The formula itself and a rough sketch of the proof can be found in [CS] Chapter 15, Section 5.1.

4.39 Theorem (oddity formula)**.** *Let (L, b, G) be a $\mathbb{Z}$-lattice. Then*

$$\operatorname{sig}_{-1}(L) + \sum_{p \geq 3} p\text{–excess}(L) \equiv \operatorname{oddity}(L) \mod 8$$

where $p\text{–excess}(L) := p\text{–excess}(G)$, $\operatorname{sig}_{-1}(L) := \operatorname{sig}_{-1}(G)$ and $\operatorname{oddity}(L) := \operatorname{oddity}(G)$.

Proof. See [Wer III]. □

Since $\mathrm{sig}_{-1}(D), p\text{–excess}(D)$ do not depend on the actual choice of the lattice, so does the oddity (by the above formula) so that $\mathrm{oddity}(D) := \mathrm{oddity}(L)$ is independent of the lattice L. Remark that the quantities $\mathrm{sig}_p(D)$ for $p \notin \{-1, 2\}$ are not independent of the lattice: Take any $p \in \mathbb{P} \setminus \{2\}$, an arbitrary even lattice L and the even unimodular lattice H given in terms of the Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ then the discriminant forms of L and $L \oplus H$ do coincide but $\mathrm{sig}_p(L \oplus H) \equiv \mathrm{sig}_p(L) + \mathrm{sig}_p(H) \equiv \mathrm{sig}_p(L) + 2 \not\equiv \mathrm{sig}_p(L) \mod 8$ because H diagonalizes to $\left(\begin{smallmatrix} 2 & 3 \\ 0 & 1 \end{smallmatrix}\right) H \left(\begin{smallmatrix} 2 & 0 \\ 3 & 1 \end{smallmatrix}\right) = \begin{pmatrix} p^0 \cdot 2 & 0 \\ 0 & p^{0 \cdot -1/2} \end{pmatrix}$.

This concludes the first part of the thesis on discriminant forms. Now we will inspect certain functions which map $\mathbb{H}$ to the group ring of such discriminant forms.

5 Characters and the Weil representation

In this section we will construct certain algebraic structures on which the modular forms will operate. In order to work with these structures we need to understand the role of two characters, χ_D and φ_D which will be defined later. The formal definition of a character will be given later. We need some preparation to inspect these characters.

5.1 Definition. *Let A be a finite abelian group (additively written) with neutral element 0. We define the set*

$$\mathcal{E}(A) := \{n \in \mathbb{N} \mid n \cdot a = 0 \text{ for all } a \in A\}$$

The exponent of A is defined as $E(A) := \min\{n \mid n \in \mathcal{E}(A)\}$ Let D be a discriminant-quadratic form with finite quadratic form Q. We define the set

$$\mathcal{L}(D) := \{n \in \mathbb{N} \mid n \cdot Q(x) = 0 + \mathbb{Z} \text{ for all } x \in D\}$$

and the level of D to be $L(D) := \min\{n \mid n \in \mathcal{L}(D)\}$. Note that due to Fermat, $|D| \in \mathcal{L}(D) \cap \mathcal{E}(D)$ so that $E(D), L(D) < \infty$. Similarly to the order of some element in a group, we define for a fixed element $x \in D$

$$L(x) := \min\{n \in \mathbb{N} \mid nQ(x) = 0 + \mathbb{Z}\}$$

5.2 Theorem. *Let A be a finite abelian group and let D be a discriminant form, then*

(a) $\mathrm{ord}(a) \mid E(A)$ *for all* $a \in A$, $E(B) \mid E(A)$ *for every subgroup* $B \subset A$ *and* $\mathcal{E}(A) = \mathbb{N} \cdot E(A)$

(b) *$L(x+L) \mid L(D)$ for all $x+L \in D$, $L(D') \mid L(D)$ for every subgroup $D' \subset D$ and $\mathcal{L}(D) = \mathbb{N} \cdot L(D)$*

(c) *Let $|A| = p_1^{a_1} \cdot ... p_r^{a_r}$ then by Remark 4.21*(a) *there are uniquely determined $e_{i,j} \in \mathbb{N}$ with*

$$A \cong \underbrace{\mathbb{Z}_{p_1^{e_{1,1}}} \times ... \times \mathbb{Z}_{p_1^{e_{1,s_1}}}}_{\cong A_{p_1}} \times ... \times \underbrace{\mathbb{Z}_{p_r^{e_{r,1}}} \times ... \times \mathbb{Z}_{p_r^{e_{r,s_r}}}}_{\cong A_{p_r}}$$

Set $m_j := \max e_{j,1}, ..., e_{j,s_j}$ then

$$E(A) = p_1^{m_1} \cdot ... \cdot p_r^{m_r}$$

Proof. (a),(b): As one shows that every subgroup of $\mathbb{Z}$ is generated by its minimal nonzero element. (c): Elementary computation □

5.3 Notation. *Let $(L, \langle \cdot, \cdot \rangle)$ be an even lattice and D its discriminant-quadratic form. For every $p \in \mathbb{P}$ choose a finite basis of D_p that satisfies the relations given in the Theorems 4.35 and 4.36. We then obtain an isomorphism*

$$\eta : D \leftarrow A := \mathbb{Z}_{p_1^{e_{1,1}}} \times ... \times \mathbb{Z}_{p_1^{e_{1,s_1}}} \times ..... \times \mathbb{Z}_{p_r^{e_{r,1}}} \times ... \times \mathbb{Z}_{p_r^{e_{r,s_r}}} \times \underbrace{(\mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_1}}) \times ... \times (\mathbb{Z}_{2^{e_f}} \times \mathbb{Z}_{2^{e_f}})}_{\text{purely even 2-dimensional blocks}} \times \underbrace{\mathbb{Z}_{2^{d_1}} \times ... \times \mathbb{Z}_{2^{d_{f'}}}}_{\text{purely odd 1-dimensional blocks}}$$

such that $\mu_{i,j}, \gamma_i, \delta_i$ and λ_i form a finite basis (e.g. set $s := s_1 + ... + s_r$ then $\mu_{1,1} = \eta(1,0,...,0), \mu_{1,2} = \eta(0,1,0,...,0)$ and so on till $x_{r,s_r} = \eta(\underbrace{0,...,0}_{s \text{ zeroes}},1,0,...,0)$ and so forth).

The following relation of the level and the exponent will be of importance for the analysis of the characters later on:

5.4 Theorem. *Let D be a discriminant-quadratic form that decomposes as described above, then*

$$L(D) = \begin{cases} E(D) & \text{if } d_j + 1 \leq \max\{e_1, ..., e_f\} \text{ for all } 1 \leq j \leq f' \\ 2E(D) & \text{otherwise} \end{cases}$$

Proof. We compute the exponent of D. Set

$$m_1 := \max\{e_{1,1}, ..., e_{1,s_1}\} \ , \ ... \ , \ m_r := \max\{e_{r,1}, ..., e_{r,s_r}\}$$

and

$$m^{(2)}_{\text{even}} := \max\{e_1, ..., e_f\} \quad m^{(2)}_{\text{odd}} := \max\{d_1, ..., d_{f'}\}$$
$$m^{(2)} := \max\{m^{(2)}_{\text{even}}, m^{(2)}_{\text{odd}}\}$$

According to 5.2(c) the exponent is given by

$$E(D) = p_1^{m_1} \cdot ... \cdot p_r^{m_r} \cdot 2^{m^{(2)}}$$

As we have choosen the finite basis such that the relations in Theorems 4.35 and 4.36 are satisfied, we know the level of the summands, it is

$$L(\mathbb{Z}_{p_i^{e_{i,j}}}) = p_i^{e_{i,j}} \ , \ L(\mathbb{Z}_{2^{e_l}} \times \mathbb{Z}_{2^{e_l}}) = 2^{e_l} \text{ and } L(\mathbb{Z}_{2^{d_l}}) = 2 \cdot 2^{d_l} = 2^{d_l+1}$$

By Theorem 5.2(b), all these levels have to divide $L(D)$ so that for $M^{(2)} := \max\{e_1, ..., e_f, d_1 + 1, ..., d_{f'} + 1\}$ and $N := p_1^{m_1} \cdot ... \cdot p_r^{m_r} \cdot 2^{M^{(2)}}$,

$$N \mid L(D)$$

must hold so that in particular $L(D) \geq N$. On the other hand we know $N \in \mathcal{L}(D)$: For $\gamma \in D$ let $\widetilde{\gamma}$ denote one fixed representative of $\gamma = \widetilde{\gamma} + L$. First note that by definition, $E(D) \mid N$ so that $N\gamma = 0 + L$ for all $\gamma \in D$. Let $\gamma, \delta \in D$ then

$$2N\frac{\langle\widetilde{\gamma}, \widetilde{\delta}\rangle}{2} + \mathbb{Z} = N\langle\widetilde{\gamma}, \widetilde{\delta}\rangle + \mathbb{Z} = (\underbrace{N\gamma}_{=0+L}, \delta) = 0 + \mathbb{Z} \tag{5.1}$$

We examine the evaluation $NQ(x+L)$ for some $x+L \in D_{p_i}$. As $x+L \in D_{p_i}$ there are $k_1, ..., k_{s_i} \in \mathbb{Z}$ such that

$$x + L = \sum_{j=1}^{s_i} k_j \mu_{ij}$$

Now

$$\begin{aligned} NQ(x+L) &= N\frac{\langle x,x\rangle}{2} + \mathbb{Z} \\ &= \frac{N}{2}\sum_{j=1}^{s_i}\langle k_j\widetilde{\mu_{ij}}, k_i\widetilde{\mu_{ij}}\rangle + \mathbb{Z} + \cancel{2}\frac{1}{\cancel{2}}\sum_{j,l} k_j k_l \underbrace{N\langle\widetilde{\mu_{ij}},\widetilde{\mu_{il}}\rangle + \mathbb{Z}}_{=0+\mathbb{Z} \text{ by (5.1)}} \\ &= \sum_{j=1}^{s_i} NQ(k_j\mu_{ij}) \\ &= 0+\mathbb{Z} \end{aligned} \tag{5.2}$$

where last step is valid since $L(\mathbb{Z}_{p_i^{e_{i,j}}}) = L(\langle\mu_{ij}\rangle) = p_i^{e_{i,j}}$ by Thm. 4.35 and $p_i^{e_{ij}} \mid N$ for all i,j by definition so that $NQ(k_j\mu_{ij}) = 0+\mathbb{Z}$ for all i,j as $k_j\mu_{ij} \in \langle\mu_{ij}\rangle$.

Let us now inspect the 2-component: Fix $x+L = \sum_i b_i\gamma_i + b_i'\delta_i + \sum_i c_i\lambda_i \in D_2$ for some $b_i, b_i', c_i \in \mathbb{Z}$, then as in (5.2),

$$\begin{aligned} NQ(x+L) &= \sum_i NQ(b_i\gamma_i + b_i'\delta_i) + \sum_i NQ(c_i\lambda_i) \\ &\qquad + \underbrace{2N(\text{bilinear mix terms})}_{=0+\mathbb{Z} \text{by (5.1)}} \\ &= \sum_i NQ(b_i\gamma_i + b_i'\delta_i) + \sum_i NQ(c_i\lambda_i) \\ &= 0+\mathbb{Z} \end{aligned} \tag{5.3}$$

where the last step is valid as $L(\mathbb{Z}_{2^{e_i}} \times \mathbb{Z}_{2^{e_i}}) = L(\langle\gamma_i,\delta_i\rangle) = 2^{e_i}$ by Thm. 4.36 and $2^{e_i} \mid N$ by definition so that $NQ(b_i\gamma_i + b_i'\delta_i) = 0+\mathbb{Z}$ because $b_i\gamma_i + b_i'\delta_i \in \langle\gamma_i,\delta_i\rangle$. We proceed analogously with the terms $c_i\lambda_i$ (this is in fact the reason why we let $2\cdot 2^{d_i} = 2^{d_i+1}$ divide N!).

Let $x+L \in D$ then because of the $\mu_{i,j}, \gamma_i, \delta_i, \lambda_i$ forming a finite basis for D we know that there are $a_{ij}, b_i, b_i', c_i \in \mathbb{Z}$ such that

$$x+L = \sum_{i,j} a_{ij}\mu_{i,j} + \sum_i b_i\gamma_i + b_i'\delta_i + \sum_i c_i\lambda_i$$

Put $x_{p_i} := \sum_{j=1}^{s_i} a_{ij}\mu_{ij} \in D_{p_i}$ and $x_2 := \sum_i b_i\gamma_i + b_i'\delta_i + \sum_i c_i\lambda_i \in D_2$. We now compute

$$\begin{aligned} NQ(x+L) &= NQ(x_{p_1} + ... + x_{p_r} + x_2) \\ &= NQ(x_{p_1}) + ... + NQ(x_{p_r}) + NQ(x_2) \quad \text{(by Thm. 4.17)} \\ &= NQ(x_2) \quad \text{(by (5.2))} \\ &= 0 + \mathbb{Z} \quad \text{(by (5.3))} \end{aligned}$$

Hence, $N \in \mathcal{L}(D)$ and thus $L(D) \leq N$ so that $L(D) = N$ but this is precisely the assertion claimed. □

This particular coherency between level and exponent will not be as useful as the consequences we can draw from it:

5.5 Corollary. *Let D be a discriminant-quadratic form. Let $N \in \mathbb{N}$ be a multiple of $L(D)$ then $N\gamma = 0 + L$ for all $\gamma \in D$.*

Proof. According to Theorem 5.4 we have $N = kL(D) = k\epsilon E(D)$ for some $\epsilon \in \{1, 2\}, k \in \mathbb{Z}$, therefore

$$N\gamma = k\epsilon E(D)\gamma = k\epsilon(0 + L) = 0 + L$$

□

5.6 Corollary. *Let D be a discriminant-quadratic form and $N \in \mathbb{N}$ be a multiple of $L(D)$. For every $a \in \mathbb{Z}$ we have*

$$(a, N) = 1 \Rightarrow (a, |D|) = 1$$

Proof. By the fundamental theorem of abelian groups,

$$D \cong A := \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_{i,1}}} \times ... \times \mathbb{Z}_{p_i^{e_{i,s_i}}}$$

the $e_{i,j}$ being in $\mathbb{N}$ and the p_i being primes not necessarily different from 2. Set $e_i := e_{i,1} + ... + e_{i,s_i}$ then $|D| = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$. By Fermat's little theorem $|D| \in \mathcal{E}(D)$ so that $E(D) \mid |D|$ by 5.2(a). Hence, $E(D)$ consists only of the primes $p_1, ..., p_r$, let $E(D) = p_1^{\nu_1} \cdot ... \cdot p_r^{\nu_r}$. We show that $\nu_i \neq 0$. Let γ be the first basis vector that belong to the finite basis induced by the decomposition of D, i.e. γ corresponds to $(\overline{1}, \overline{0}, ..., \overline{0}) \in A$. The leading "one" is an element

in $\mathbb{Z}_{p_1^{e_{1,1}}}$ so that $\mathrm{ord}(\gamma) = p_1^{e_{1,1}}$. By 5.2(a), $p_1^{e_{1,1}} \mid E(D)$ so that $\nu_1 \geq e_{1,1} \geq 1$. We proceed analogously with $\nu_2, ..., \nu_r$. Consequently:

$$\begin{aligned}(a,N) = 1 &\Rightarrow (a, L(D)) = 1 \\ &\Rightarrow (a, \epsilon E(D)) = 1 \\ &\qquad \text{(by Theorem 5.4)} \\ &\Rightarrow (a, E(D)) = 1 \\ &\Rightarrow a \text{ only consists of primes disjoint from those in E(D)} \\ &\Rightarrow a \text{ only consists of primes disjoint from } p_1, ..., p_r \\ &\qquad (\text{as } \nu_j \geq 1 \text{ for all } j) \\ &\Rightarrow a \text{ only consists of primes disjoint from those in } |\mathrm{D}|\end{aligned}$$

□

5.7 Corollary. *Let D be a discriminant-quadratic form, S a subgroup and N be a multiple of $L(D)$, then for every $a \in \mathbb{Z}$*

$$(a,N) = 1 \Longrightarrow (a, |S|) = 1$$

Proof. Lagrange: $|S| \mid |D|$ so that $(a,N) = 1 \overset{5.6}{\Rightarrow} (a,|D|) = 1 \Rightarrow (a,|S|) = 1$ □

Before we proceed to the definition and analysis of the characters we need one last preparation:

5.8 Lemma. *Let D be a discriminant-quadratic form. Let N be a multiple of $L(D)$ then*

$$N \textit{is odd} \Longrightarrow \mathrm{oddity}(D) \equiv 0 \mod 8$$

Proof. $L(D) \mid N$, so $L(D)$ is odd too. Choose an even lattice (L, v, G) with $L'/L \cong D$. Choose a matrix $S \in (\mathbf{Z_2} \cap \mathbb{Q})^{n \times n}$ as in Lemma 3.3 so that

$$S^T G S = B_1 \oplus ... \oplus B_f \oplus \mathrm{diag}(\alpha_1, ..., \alpha_{f'})$$

Let $B_i = 2^{e_i} B_i'$ and $\alpha_i = 2^{d_i}\beta_i$ as in the lemma. Choose a finite basis of D_2, $\gamma_1 = (g_1^* + L), \delta_1 = (g_2^* + L), ..., \gamma_f = (g_{2f-1}^* + L), \delta_f = (g_{2f}^* + L), \lambda_1 = (g_{2f+1}^* + L), ..., \lambda_{f'} = (g_{2f+f'}^* + L)$ according to Theorem 4.30(b). Assume that there exists an i with $e_i > 0$. The members γ_i, δ_i of the finite basis span a summand $\mathbb{Z}_{2^{e_i}} \times \mathbb{Z}_{2^{e_i}}$ which has a level 2^{e_i} due to Theorem 4.36. Due to Theorem 5.2(b), $2^{e_i} \mid L(D)$ so that $L(D)$ is even. Contradiction. Hence, $e_i = 0$ and $B_i = B_i'$. The same argument also shows that $d_i = 0$ as otherwise

the level $2 \cdot 2^{d_i}$ of the constituent $\mathbb{Z}_{2^{d_i}}$ causes $L(D)$ to be even again. Hence, $\alpha_i = 2^0 \beta_i$ is a unit in $\mathbf{Z_2}$. We claim that $f' = 0$, in particular we claim that the dimension n has to be even in the case where L is an even lattice and N is odd. Since L is even, L_p is $\mathbf{Z_p}$-even. By Remark 4.12, $S^T G S$ (which is a Gram matrix with respect to a different basis of L) has to have diagonal entires lying in $2\mathbf{Z_2}$. If $f' > 0$ then there would be a diagonal entry $\alpha_1 = \beta_1$ which lies in ${\mathbf{Z_2}}^\times$ which is disjoint from $2\mathbf{Z_2}$. Contradiction. Now

$$\begin{aligned}
\text{oddity}(D) &= \text{oddity}(L) = \text{oddity}(G) = \text{sig}_2(G) \\
&= \text{sig}_2(B_1 \oplus ... \oplus B_f) && (\text{as } f' = 0) \\
&= \text{sig}_2(B'_1 \oplus ... \oplus B'_f) && (\text{as } e_i = 0) \\
&= \sum_{j=1}^{f} \text{sig}_2(B'_j) \equiv 0 \mod 8 && (\text{by Rmk. } 3.14)
\end{aligned}$$

□

We will now formally define the term character and subsequently we will construct two special instances of them.

5.9 Definition. *Let G be a group (multiplicatively written). A homomorphism of groups $\chi : G \mapsto \mathbb{C}^\times$ is called a character of G. Characters of the group $\mathbb{Z}_N$ are called Dirichlet characters modulo N. They can also be viewed as multiplicative functions from $\mathbb{Z}$ to $\mathbb{C}$ by the definition*

$$\chi(k) := \begin{cases} \chi(k) & \text{if } (k, N) = 1 \\ 0 & \text{otherwise} \end{cases}$$

A character $\chi : G \mapsto \mathbb{C}^\times$ is said to be of finite order if there exists an $n \in \mathbb{N}$ such that $\chi(g)^n = 1$ for all $g \in G$. A character $\chi : G \mapsto \mathbb{C}^\times$ is said to be quadratic if $\chi(g) \in \{\pm 1\}$ for all $g \in G$.

5.10 Proposition. *Let Γ be a group and $\chi : \Gamma \mapsto \mathbb{C}^\times$ a character of finite order then $\chi(\Gamma) \subset \delta B_1(0)$ so that in particular $\overline{\chi(x)} = \chi(x)^{-1}$.*

5.11 Definition. *Let D be a discriminant-quadratic form of even signature. Let N be a multiple of $L(D)$. We define*

$$\chi_D : \mathbb{Z}_N^\times \mapsto \mathbb{C}^\times, \quad \chi_D(m) := \left(\frac{m}{|D|}\right) e\left((m-1)\frac{\text{oddity}(D)}{8}\right)$$

and

$$\varphi_D : \mathbb{Z}_N^\times \mapsto \mathbb{C}^\times, \quad \varphi_D(m) := \frac{g(D)}{g_m(D)}$$

where $e(x) := e^{2\pi i x}$, $g_x(D) := \sum_{\gamma \in D} e(x \cdot Q(\gamma))$ *and* $g(D) := g_1(D)$. *Note that* $e(x + \mathbb{Z}) = e(x)$ *is well defined, therefore we may view* $g_x(D) \in \mathbb{C}$.

Note that the Legendre symbol (and therefore χ_D) is well-defined because of Corollary 5.6. We will see that these functions are Dirichlet characters of finite order and actually they coincide. We will now define the Weil representation and the algebraic structure on which we want the modular forms to operate. We will make use of the Weil representation not only for the proof of the above assertion.

5.12 Definition. *Let* $A = \{a_1, ..., a_{|A|}\}$ *be a finite group and let* K *be a field. We define the* $|A|$*-dimensional* K *vector space* $K[A]$ *to be* $K^{|A|}$. *In* $K[A]$ *we rename the standard basis* $e_1, ..., e_{|A|}$ *to* $\mathbf{e}_{a_1}, ..., \mathbf{e}_{a_{|A|}}$ *and we declare a multiplication on* $K[A]$ *by*

$$\mathbf{e}_a \cdot \mathbf{e}_b := \mathbf{e}_{a \cdot b}$$

therefore turning $K[A]$ *into a* K*-algebra, the group ring of* A.

We want to define a representation of the group $\mathrm{SL}_2(\mathbb{Z})$ which (along with some interesting subgroups) is defined as follows:

5.13 Definition. *For any commutative ring* R *with unit* 1 *we put*

$$\mathrm{SL}_2(R) := \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2\times 2} \;\middle|\; \det(M) = ad - bc = 1 \right\}$$

We define the sets

$$\Gamma(N) := \left\{ M \in SL_2(\mathbb{Z}) \;\middle|\; M \equiv Id \mod N \right\}$$

$$\Gamma_1(N) := \left\{ M \in SL_2(\mathbb{Z}) \;\middle|\; M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

$$\Gamma_0(N) := \left\{ M \in SL_2(\mathbb{Z}) \;\middle|\; M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

It is easy to see that $SL_2(\mathbb{Z})$ *is a group and that* $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$ *are subgroups.*

We now define the Weil representation, a representation of $\mathrm{SL}_2(\mathbb{Z})$ on the $\mathbb{C}$-vector space $\mathbb{C}[D]$. Of course the following definition does not appear from nowhere. It is a special instance of a general construction given by Weil in [We]. However, we will prove the correctness of the special instance more direct; see below.

5.14 Definition. *Let D be a discriminant-quadratic form of even signature. For $\gamma \in D$ we define*

$$\rho(T).\mathbf{e}_\gamma = e\left(-Q(\gamma)\right)\mathbf{e}_\gamma$$
$$\rho(S).\mathbf{e}_\gamma = \frac{e\left(\mathrm{sig}(D)/8\right)}{\sqrt{|D|}} \sum_{\beta \in D} e\left((\gamma,\beta)\right)\mathbf{e}_\beta$$

5.15 Theorem. *Let D be a discriminant form of even signature, then the multiplicative continuation (i.e. $\rho(S^{x_1}T^{y_1}\cdot\ldots\cdot S^{x_n}T^{y_n}) := \rho(S)^{x_1}\circ\rho(T)^{y_1}\circ\ldots\circ\rho(S)^{x_n}\rho(T)^{y_n}$) defines a representation of $SL_2(\mathbb{Z})$ on $\mathbb{C}[D]$*

Proof. See [Wer II]. □

One can show the following about this representation:

5.16 Theorem. *Let D be a discriminant form of even signature and $N \in \mathbb{N}$ such that $L(D) \mid N$, then*

(a) Let $M \in \Gamma(N)$ then $\rho(M) = id$, i.e. ρ acts trivial on $\Gamma(N)$.

(b) Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ be such that $b \equiv c \equiv 0 \mod N$ then

$$\rho(M).\mathbf{e}_\gamma = \chi_D(d)\mathbf{e}_{d\gamma}$$

(c) Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ then

$$\rho(M).\mathbf{e}_\gamma = \chi_D(d)e\left(-bdQ(\gamma)\right)\mathbf{e}_{d\gamma}$$

(d) Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ be such that $b \equiv c \equiv 0 \mod N$ then

$$\rho(M).\mathbf{e}_\gamma = \varphi_D(d)^{-1}\mathbf{e}_{d\gamma}$$

Proof. (a) See [We]. (b) See [Sch], Prop. 4.4. (c) See [Sch], Prop. 4.5. (d) See [McG], Lemma 4.6. □

The main result of this section is the following:

5.17 Theorem. *Let D be a discriminant-quadratic form of even signature and $N \in \mathbb{N}$ such that $L(D) \mid N$, then for the function χ_D, φ_D as defined in 5.11, the following assertions hold:*

(a) χ_D and φ_D are multiplicative so that they are Dirichlet characters modulo N.

(b) χ_D is quadratic, i.e. $\chi_D(m)^2 = 1$ so that $\chi_D(m) \in \{\pm 1\}$ for all m (in particular, χ_D is of finite order).

(c) χ_D and φ_D coincide, i.e. $\chi_D(d) = \varphi_D(m)$ for all $m \in \mathbb{Z}_N^\times$ (in particular, φ_D is of finite order too).

Proof. (a) Assume that N is odd. By Lemma 5.8, $\operatorname{oddity}(D) \equiv 0 \mod 8$ so that $e\left(m \operatorname{oddity}(D)/8\right) = 1$ and $\chi_D(\cdot) = \left(\frac{\cdot}{|D|}\right)$. As the Legendre symbol is multiplicative, so is χ_D in this case. Now let N be even. Choose an even lattice (L, v, G) with $D \cong L'/L$. Observe that $p\text{–}\operatorname{excess}(D) = p\text{–}\operatorname{excess}(G)$ is even for $p \geq 3$, because: Choose a matrix S as in Lemma 3.3, then G diagonalizes to $H = S^T G S = \operatorname{diag}(\alpha_1, ..., \alpha_n)$ where $\alpha_i = p^{d_i}\beta_i$. By definition

$$\begin{aligned} p\text{–}\operatorname{excess}(G) &= \operatorname{sig}_p(G) - \operatorname{dimension} = p^{d_1} + ... + p^{d_n} + 4k - n \\ &\equiv 1 + ... + 1 + 0 - n \equiv n - n \equiv 0 \mod 2 \end{aligned}$$

because $p > 2$ implies that $p^d \equiv 1 \mod 2$ for all $d \in \mathbb{N}_0$. By assumption, the signature of D is even too so that by the oddity formula (cf. Theorem 4.39), so is the oddity of D. From this we derive

$$x \equiv y \mod 4 \Longrightarrow e\left(x\frac{\operatorname{oddity}(D)}{8}\right) = e\left(y\frac{\operatorname{oddity}(D)}{8}\right) \tag{5.4}$$

Now let $a, b \in \mathbb{Z}_N^\times$. Since a, b are units modulo N, $(a, N) = (b, N) = 1$. In particular, a, b are odd as N is even so that a, b are congruent to either 1 or 3 modulo 4. A direct case distinction shows that then

$$ab - 1 \equiv (a - 1) + (b - 1) \mod 4$$

so that

$$\begin{aligned}\chi_D(ab) &= \left(\frac{ab}{|D|}\right) e\left((ab-1)\frac{\text{oddity}(D)}{8}\right)\\ &= \left(\frac{a}{|D|}\right)\left(\frac{b}{|D|}\right) e\left([(a-1)+(b-1)]\frac{\text{oddity}(D)}{8}\right)\\ &\quad \text{(by (5.4) and the above)}\\ &= \left(\frac{a}{|D|}\right) e\left((a-1)\frac{\text{oddity}(D)}{8}\right)\left(\frac{b}{|D|}\right) e\left((b-1)\frac{\text{oddity}(D)}{8}\right)\\ &= \chi_D(a)\chi_D(b)\end{aligned}$$

We show that φ_D is multiplicative: For any $x \in \mathbb{Z}_N^\times$, let R_x be an arbitrary but fixed representative in $\mathrm{SL}_2(\mathbb{Z})$ of $\left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & x \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_N)$. By Theorem 5.16(d), $\rho(R_x)\mathbf{e}_\gamma = \varphi_D(x)^{-1}\mathbf{e}_{x\gamma}$. Let y be another unit in $\mathbb{Z}_N$, then R_xR_y is obviously a representative of R_{xy} so that

$$\varphi_D(xy)^{-1}\mathbf{e}_{xy\gamma} = \rho(R_{xy})\mathbf{e}_\gamma = \rho(R_x)\rho(R_y)\mathbf{e}_\gamma = \varphi_D(x)^{-1}\varphi_D(y)^{-1}\mathbf{e}_{xy\gamma}$$

because ρ is a representation. Consequently, $\varphi_D(xy)^{-1} = \varphi_D(x)^{-1}\varphi_D(y)^{-1}$. Inverting this equation yields the assertion.

(b) Either N is odd, then χ_D is the Legendre symbol which is quadratic by definition. If N is odd, then – as above – $\text{oddity}(D) = 2k$ for some $k \in \mathbb{Z}$ and $a \in \mathbb{Z}_N^\times \Rightarrow (a-1) = 2v$ for some $v \in \mathbb{Z}$ so that

$$\begin{aligned}\chi_D(a)^2 &= \underbrace{\left(\frac{a}{|D|}\right)^2}_{=1} e\left((a-1)\frac{\text{oddity}(D)}{8}\right)^2\\ &= e\left(2(a-1)\frac{\text{oddity}(D)}{8}\right)\\ &= e\left(2\cancel{2}v\frac{2k}{\cancel{8}}\right)\\ &\in e(\mathbb{Z}) = \{1\}\end{aligned}$$

(c) For $m \in \mathbb{Z}_N^\times$ set $R_m := ST^mS^{-1}T^xST^m$ where $x = m^{-1} \bmod N$. A direct calculation shows that $R_m \equiv \left(\begin{smallmatrix} x & 0 \\ 0 & m \end{smallmatrix}\right) \mod N$. For $\gamma := 0 + L$,

$$\begin{aligned}\frac{1}{\varphi_D(m)}\mathbf{e}_{0+L} = \frac{1}{\varphi_D(m)}\mathbf{e}_{m\gamma} &\overset{5.16(d)}{=} \rho(R_m).\mathbf{e}_\gamma\\ &\overset{5.16(b)}{=} \chi_D(m)\mathbf{e}_{m(0+L)} = \chi_D(m)\mathbf{e}_{0+L}\end{aligned}$$

As the $(\mathbf{e}_\delta)_{\delta\in D}$ form a $\mathbb{C}$-basis, $\varphi_D(m) = \chi_D(m)^{-1}$ and the last expression is precisely $\chi_D(m)$ as χ_D is quadratic. □

6 Modular forms

In this section we will briefly recall the definition of modular forms and Hecke operators. We will furthermore define modular forms for the Weil representation and Hecke operators for such following Bruinier [Br]. We will generate modular forms for the Weil representation out of usual modular forms using a lift as done in [Sch II].

6.1 Definition. *For a matrix* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = M \in \mathbb{R}^{2\times 2}$ *and* $\tau \in \mathbb{C}$ *we define* $(M:\tau) := c\tau + d$. *Let* $f : \mathbb{H} \mapsto \mathbb{C}$ *be a function and* $k \in \mathbb{Z}$ *then we define*

$$f|_M(\tau) := \det(M)^{k/2}(M:\tau)^{-k} f(M.\tau) \ ,$$

the Petersson "slash" operator. Observe that the slash operator depends on k *but we will not mention this index as it will be clear from the context. Let* $\Gamma \subset SL_2(\mathbb{Z})$ *be a subgroup having a finite index.* f *is called a modular form of weight* $k \in \mathbb{Z}$ *for the subgroup* Γ *if*

(I) f *is holomorphic on* $\mathbb{H}$

(II) $f\,(M.\tau) = (M:\tau)^k f(\tau)$ *for all* $M \in \Gamma, \tau \in \mathbb{H}$

(III) For every $M \in SL_2(\mathbb{Z})$, *there exists an* $N = N(M,\Gamma)$ *such that* $f|_M$ *has a Fourier expansion of the form*

$$f|_M(\tau) = \sum_{n=0}^{\infty} a_f(n) e^{2\pi i n\tau/N}$$

for all $\tau \in \mathbb{H}$, *the coefficients* $a_f(n)$ *being in* $\mathbb{C}$ *such that the series converges absolutely on* $\mathbb{H}$.

The set of all modular forms for Γ *of weight* k *will be denoted as* $\mathrm{MF}_k(\Gamma)$.

6.2 Remark. *Condition (III) does not consist of the existence of the Fourier expansion as one can show that there always exist* $N = N(L,\Gamma)$ *and* $a_f(n) \in \mathbb{C}$ *such that*

$$f|_L(\tau) = \sum_{n\in\mathbb{Z}} a_f(n) e^{2\pi i n\tau/N}$$

see for example [Wer], Thm 2.4.4. The reason is that all N*-periodic holomorphic functions on* $\mathbb{H}$ *possess an expansion* $\sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/N}$. *Because of the finite index there exists an* $n_{L,\Gamma} \in \mathbb{N}$ *such that* $LT^{n_{L,\Gamma}}L^{-1} \in \Gamma$ *which means that (use condition (II))* $f|_L$ *is* $n_{L,\Gamma}$*-periodic. Therefore, condition (III) rather states that this series starts with a positive index than the existence of a series.*

6.3 Remark. *Let* $SL_2(\mathbb{Z}).\infty := \{M.\infty \mid M \in SL_2(\mathbb{Z})\}$ *and* $\mathrm{cusps}(\Gamma) := SL_2(\mathbb{Z}).\infty/\sim$ *where two points* $\tau_1, \tau_2 \in SL_2(\mathbb{Z}).\infty$ *are equivalent if and only if there exists a* $\gamma \in \Gamma$ *with* $\gamma.\tau_1 = \tau_2$. *The name of the set comes from the geometrical reason that the representatives of these classes mark the ends of fundamental domains of the operation of* Γ *on* $\mathbb{H}$ *and look like cusps.*

Let f *be a function that satisfies conditions (I) and (II).*

(i) Let $\tau_1 = M_1.\infty, ..., \tau_r = M_r.\infty$ *be a system of representatives for* $\mathrm{cusps}(\Gamma)$, *then* f *satisfies condition (III) for all* $M \in SL_2(\mathbb{Z})$ *if and only if* f *satisfies (III) for* $M_1, ..., M_r$ *(i.e. we only have to check condition (III) for finitely many matrices).*

(ii) The existence of a Fourier expansion starting with a positive coefficient does not depend on N, *i.e. if*

$$f_M(\tau) = \sum_{n\in\mathbb{Z}} a_f(n) e^{2\pi i n\tau/N} = \sum_{n\in\mathbb{Z}} b_f(n) e^{2\pi i n\tau/M}$$

for some M, N *in* $\mathbb{N}$ *then*

$$a_f(n) = 0 \text{ for all } n < 0 \iff b_f(n) = 0 \text{ for all } n < 0$$

(iii) $f|_M M$ *possesses a Fourier expansion as in condition (III) if and only if* $\lim_{z\to i\infty} f|_M(z)$ *exists (this means that there exists a* $c \in \mathbb{C}$ *such that for all sequences* $(z_n)_{n\in\mathbb{N}}$ *with* $\mathrm{Im}(z_n) \overset{n\to\infty}{\longrightarrow} \infty$ *we have* $f|_M(z_n) \overset{n\to\infty}{\longrightarrow} c$*).*

Proof. (i): See for example [Wer], Thm. 2.4.10. (ii) is proved by comparison of the coefficients. This is allowed as the "pushed" functions $t \mapsto f(\frac{N \mathrm{Log}_{\mathbb{C}}(t)}{2\pi i})$ and $t \mapsto f(\frac{M \mathrm{Log}_{\mathbb{C}}(t)}{2\pi i})$ on the punctured unit disc $B_1(0)\setminus\{0\}$ are both Laurent series having the coefficients $a_f(n)$ and $b_f(n)$. One can now compare these as Laurent series are unique. (iii): See for example [Wer], Thm 2.4.7. □

There are various generalizations of this definition of being a modular form. Sometimes it is useful to relax condition (II) in the following sense:

6.4 Definition. *Let* $\Gamma \subset SL_2(\mathbb{Z})$ *be a subgroup of finite index,* $f : \mathbb{H} \mapsto \mathbb{C}$ *a function and let* $\chi : \Gamma \mapsto \mathbb{C}^\times$ *be a character of finite order. Put* $\ker(\chi) := \{\gamma \in \Gamma \mid \chi(\gamma) = 1\}$. *$f$ is called a modular form for* Γ *of weight* $k \in \mathbb{Z}$ *that transforms with respect to the character* χ *if*

(I)' *f is a modular form for the group* $\ker(\chi)$ *of weight k in the sense of definition 6.1.*

(II)' $f(M.\tau) = \chi(M)(M:\tau)^k f(\tau)$ *for all* $M \in \Gamma, \tau \in \mathbb{H}$

The set of modular forms transferring under the character χ *of weight* k *will be denoted by* $\mathrm{MF}_k(\Gamma, \chi)$.

One can show since χ is of finite order and Γ has a finite index, so has $\ker(\chi)$ so that the above definition makes sense.

6.5 Remark. *Let* Γ *be a subgroup possessing a finite index in* $SL_2(\mathbb{Z})$ *and* χ *a character for* Γ. *Put* $\Omega(\Gamma, \chi) := \{f : \mathbb{H} \mapsto \mathbb{C} \mid f|_\gamma = \chi(\gamma) f \ \forall \gamma \in \Gamma\}$ *to be the set of all functions that transform under the character* χ. *In this notation we have defined* $\mathrm{MF}_k(\Gamma, \chi) = \mathrm{MF}_k(\ker(\chi)) \cap \Omega(\Gamma, \chi)$. *Let* $\widetilde{\Gamma}$ *be another subgroup satisfying* $[SL_2(\mathbb{Z}) : \widetilde{\Gamma}] < \infty$ *and* $\widetilde{\Gamma} \subset \ker(\chi)$, *then*

$$\mathrm{MF}_k(\widetilde{\Gamma}) \cap \Omega(\Gamma, \chi) = \mathrm{MF}_k(\Gamma, \chi) = \mathrm{MF}_k(\ker(\chi)) \cap \Omega(\Gamma, \chi)$$

i.e. condition (III) does not depend so much on the concrete subgroup. Furthermore the following is true: Some authors do not want the denominator N *in condition (III) to be some arbitrary* N *but to be the specific natural* $n_{L,\ker(\chi)}$ *as in 6.2. The claim here is that both definitions coincide.*

Proof. Actually we have nothing to show but it is not obvious why this is the case: On the equality of sets: only condition (III) is interesting here, the other conditions are clearly covered. Let $f \in \mathrm{MF}_k(\ker(\chi))$. Then there exists a Fourier expansion $f|_L(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/N}$ where N depends on $\ker(\chi)$ and L. In our definition of condition (III) for the group $\widetilde{\Gamma}$ we could reuse the same N as above and condition (III) is satisfied. The other directions are shown in the same way by interchanging the roles of $\widetilde{\Gamma}$ and $\ker(\chi)$. Now the question arises why we allow any natural number M as denominator instead of $n_{L,\widetilde{\Gamma}}$: Assume we did not do so and we want the denominator to be $M = n_{L,\widetilde{\Gamma}}$. Since $\widetilde{\Gamma} \subset \ker(\chi)$ and $\widetilde{\Gamma}$ possesses a finite index in $\mathrm{SL}_2(\mathbb{Z})$, by Remark (6.2), for every L, there exists a Fourier expansion $f|_L(\tau) = \sum_{n=-\infty}^{\infty} b_n e^{2\pi i n\tau/M}$ where $M = n_{L,\widetilde{\Gamma}}$. By 6.3(ii), $b_n = 0$ for all $n < 0$ so that the abstract Fourier series is actually a Fourier series that contains only positive indices. □

We do not want condition (II) to be relaxed completely in the sense that we just require f to transform as in (II)' in the definition above because one still wants to guarantee the existence of a Fourier series and therefore $T^N \in \Gamma$ should somehow imply that f is N-periodical which is not guaranteed if $\chi(T^N) \neq 1$.
Now we will define the functions of interest: vector-valued modular forms on $\mathbb{H}$ transforming under the Weil representation:

6.6 Definition. *Let D be a discriminant-quadratic form of even signature and $N \in \mathbb{N}$ such that $L(D) \mid N$. A function $F : \mathbb{H} \mapsto \mathbb{C}[D]$ is called a modular form for $SL_2(\mathbb{Z})$ that acts under the Weil representation if*

(I) F is holomorphic.

(II) $F(M.\tau) = (M : \tau)^k \rho(M) F(\tau)$ for all $M \in SL_2(\mathbb{Z}), \tau \in \mathbb{H}$.

(III) F has a Fourier expansion of the form

$$F(\tau) = \sum_{n=0}^{\infty} a_F(n) e^{2\pi i n \tau / N}$$

for some $N \in \mathbb{N}$ with $a_F(n) \in \mathbb{C}[D]$ such that the series converges locally uniformly in $\mathbb{H}$.

The set of all these functions of weight k will be denoted by VVMF_k

6.7 Remark. *A map $F : \mathbb{C} \supset \Omega \mapsto V$ for a $\mathbb{C}$-vector spaces V is called holomorphic if the limit*

$$\lim_{h \to 0} \frac{F(z_0 + h) - F(z_0)}{h}$$

exists in V for every $z_0 \in \Omega$. Let $\pi_\gamma : \mathbb{C}[D] \mapsto \mathbb{C}$ be the projection on the $\mathbf{e}_\gamma$-th coordinate, then every function $F : \mathbb{H} \mapsto \mathbb{C}[D]$ may be written as $F = \sum_{\gamma \in D} F_\gamma \mathbf{e}_\gamma$ where $F_\gamma = \pi_\gamma \circ F$. Since all norms on finite dimensional $\mathbb{R}$-vector spaces are equivalent, a sequence $(v_n)_{n \in \mathbb{N}}$ converges in $\mathbb{C}[D]$ iff. every coordinate sequence $\pi_\gamma(v_n)$ converges in $\mathbb{C}$. This means that F is holomorphic if and only if every F_γ is in the usual sense. Let F be a function that satisfies conditions (I) and (II). Since $\rho(\Gamma(N)) = \{Id|_{\mathbb{C}[D]}\}$ and the $\mathbf{e}_\gamma$ are linearly independent, every component F_γ satisfies conditions (I) and (II) for a modular form for $\Gamma(N)$, i.e. by Remark 6.2 there exists a Fourier series (possibly containing an infinity number of terms with a negative index) in a certain denominator M_γ for every component F_γ. Therefore, F possesses such a Fourier series in the denominator $N = \mathrm{lcm}(\{M_\gamma \mid \gamma \in D\})$, i.e. as in the scalar-valued case: condition (III) does not state that there exists *a Fourier series but rather that it starts with a term having a positive index.*

We will now see that vector-valued modular forms exist and many of them arise in a certain way from scalar-valued modular forms.
For some $\gamma \in D$, we define a character

$$\chi_\gamma : \Gamma_1(N) \mapsto \mathbb{C}^\times : \quad \chi \begin{pmatrix} a & b \\ c & d \end{pmatrix} := e(-bQ(\gamma))$$

An element $\gamma = x + L \in D$ is called isotropic if $Q(\gamma) = \frac{\langle x,x\rangle}{2} + \mathbb{Z} = 0 + \mathbb{Z}$. A subset $S \subset D$ is called isotropic if every element $\gamma \in S$ is.

6.8 Theorem. *Let D be a discriminant-quadratic form of even signature and $L(D) \mid N$. Let $\Gamma \in \{\Gamma(N), \Gamma_1(N), \Gamma_0(N)\}$, $f \in \mathrm{MF}_k(\Gamma, \chi)$. Choose a system of right representatives $\mathcal{M}$ of $\Gamma\backslash SL_2(\mathbb{Z})$. If either*

(a) $\Gamma = \Gamma_0(N), \chi = \chi_D$, S_0 an isotropic subgroup of D and $\Theta = \sum_{\gamma \in S_0} \mathbf{e}_\gamma$

(b) $\Gamma = \Gamma_1(N), \chi = \chi_\gamma$ for some fixed $\gamma \in D$ and $\Theta = \mathbf{e}_\gamma$

(c) $\Gamma = \Gamma(N), \chi = 1$ (the trivial character) and $\Theta = \mathbf{e}_\gamma$ for some $\gamma \in D$

then the map

$$\mathcal{L}(f) := \sum_{M \in \mathcal{M}} \rho(M)^{-1} f|_M \Theta$$

is a vector-valued modular form for the Weil representation on $\mathbb{C}[D]$. The definition does not depend on the concrete choice of the system of right representatives $\mathcal{M}$. Such a map is called a well-defined lift of scalar-valued modular forms.

Proof. See [Sch II], Thm. 3.1. (note that in the first case, S_0 is invariant under $\gamma \mapsto x\gamma$ for every $x \in \mathbb{Z}_N^\times$, because $(x, N) = 1$ implies $(x, |S_0|) = 1$ by Corollary 5.7). □

6.9 Remark. *Let L, D, Γ be as above and fix a subgroup H of D. Put $\Theta := \sum_{\gamma \in H} \mathbf{e}_\gamma$. If either $\Gamma = \Gamma_0(N), \chi = \chi_D$ and H is isotropic or $\Gamma = \Gamma_1(N)$ and H is isotropic (then χ_γ is trivial for every γ) or $\Gamma = \Gamma(N)$ and χ is trivial then the map*

$$\mathcal{L}_H(f) := \sum_{M \in \mathcal{M}} \rho(M)^{-1} f|_M \Theta$$

is also a well-defined lift as a sum of the above ones.

6.10 Remark. *Select Γ to be $\Gamma_1(N)$ and $S_0 \subset D$ an isotropic subgroup, then $\chi_\gamma \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = e(-bQ(\gamma)) = e(0 + \mathbb{Z}) = 1$ so that the map*

$$f \mapsto \mathcal{L}_{S_0}(f) := \sum_{M \in \mathcal{M}} \rho(M)^{-1} f|_M \Theta$$

is a well-defined lift taking scalar-valued modular forms in $\mathrm{MF}_k(\Gamma_1(N))$ (without a character) as input.

We will now define a set of linear operators on modular forms, the Hecke operators. Subsequently we will define these Operators on vector-valued modular forms too (as far as possible).

6.11 Definition. *For $n \in \mathbb{N}$ we define*

$$\Omega_n := \left\{\alpha \in \mathbb{Z}^{2\times 2} \mid \det(\alpha) = n\right\}$$

and put

$$\Omega := \bigcup_{n\in\mathbb{N}} \Omega_n$$

Let $\Gamma \subset SL_2(\mathbb{Z})$ be a subgroup such that $\Gamma(N) \subset \Gamma$ (in particular, the index of Γ in $SL_2(\mathbb{Z})$ is finite). For any $\alpha, \beta \in \mathrm{GL}_2^+(\mathbb{R}) := \{X \in \mathbb{R}^{2\times 2} \mid \det(X) > 0\}$ we put

$$\alpha \approx_\Gamma \beta \iff \exists \gamma_1, \gamma_2 \in \Gamma \,.\, \alpha = \gamma_1\beta\gamma_2$$

The equivalence class of α is given by the double coset $\Gamma\alpha\Gamma$.

The key tool for defining Hecke operators is to find finitely many right representatives in α, i.e. to find finitely many $\alpha_1, ..., \alpha_r \in \Gamma\alpha\Gamma$ such that

$$\Gamma\alpha\Gamma = \Gamma\alpha_1 \,\dot\cup\, ... \,\dot\cup\, \Gamma\alpha_r$$

We say that α (or $\Gamma\alpha\Gamma$) permits a finite Γ-coset decomposition in this case. The next theorem shows that this is the case very often whenever the subgroup Γ is large enough (in the sense that $\Gamma(N) \subset \Gamma$):

6.12 Theorem. *Let $\Gamma(N) \subseteq \Gamma \subseteq SL_2(\mathbb{Z})$. Set $\widetilde{\Gamma} := \mathbb{R}^\times \cdot \mathrm{GL}_2^+(\mathbb{Q})$ then for every $\alpha \in \widetilde{\Gamma}$, we find finitely many $\alpha_1, ..., \alpha_r$ such that*

$$\Gamma\alpha\Gamma = \Gamma\alpha_1 \,\dot\cup\, ... \,\dot\cup\, \Gamma\alpha_r$$

Proof. Set $\Gamma' := \Gamma$ then apply [Mi], Lemma 4.5.1 to see that $\widetilde{\Gamma} = \{g \in \mathrm{GL}_2^+(\mathbb{R}) \mid g\Gamma g^{-1} \approx \Gamma\}$ where for two subgroups Δ, Δ' of $G := \mathrm{GL}_2^+(\mathbb{R})$,

$$\Delta_1 \approx \Delta_2 \iff [\Delta_1 : \Delta_1 \cup \Delta_2] < \infty \text{ and } [\Delta_2 : \Delta_1 \cup \Delta_2] < \infty$$

Since $\Gamma \approx \Gamma'$ (as in our case we have set Γ' to be nothing else but Γ) we may apply [Mi], Lemma 2.7.1(4) to obtain the finite coset decomposition for all $\alpha \in \widetilde{\Gamma}$. □

Observe that in particular $\Omega \subset \{1\}\,\mathrm{GL}_2^+(\mathbb{Q})$ so that the above implies

6.13 Corollary. *For every subgroup $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$, all $\alpha \in \Omega$ permit a finite Γ-coset decomposition.*

6.14 Definition. *Let $\{\alpha_1, ..., \alpha_r\} = \mathcal{A} \subset \Omega_n$ and let Γ be an arbitrary subgroup of $SL_2(\mathbb{Z})$. We say that $\mathcal{A}$ is Γ-inequivalent if the α_i are pairwise inequivalent modulo Γ, i.e. if $\Gamma\alpha_i = \Gamma\alpha_j$ then $i = j$ follows. We say that $\mathcal{A}$ commutes with Γ up to permutation and write $\mathcal{A} \sim \Gamma$ in this case, if for every $\gamma \in \Gamma$ there exists a permutation $\pi(\gamma, \cdot) : \{1, ..., r\} \mapsto \{1, ..., r\}$ and matrices $\delta(\gamma, i) \in \Gamma$ with $1 \leq i \leq r$ such that*

$$\alpha_i\gamma = \delta(\gamma, i)\alpha_{\pi(\gamma,i)}$$

If $\mathcal{A}$ is Γ-inequivalent and $\mathcal{A} \sim \Gamma$ then a direct computation shows that the $\delta(\gamma, i)$ are uniquely determined.
The following is the main reason why Hecke operators applied to modular forms yield functions that transform under Γ again:

6.15 Lemma. *Let $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$ be a subgroup of $SL_2(\mathbb{Z})$ such that every $A \in \Omega$ permits a finite Γ-coset decomposition by Thm. 6.12. Let $A_1, ..., A_t \in \Omega_n$ such that $\Gamma A_i\Gamma \neq \Gamma A_j\Gamma$ for $i \neq j$ and take $\mathcal{A}_i = \{\alpha_{i,1}, ..., \alpha_{i,r_i}\}$ such that $\Gamma A_i\Gamma = \Gamma\alpha_{i,1} \dot\cup ... \dot\cup \Gamma\alpha_{i,r_i}$ for all $1 \leq i \leq t$. The set $\omega := \Gamma A_1\Gamma \cup ... \cup \Gamma A_t\Gamma$ decomposes into a finite set of right representatives modulo Γ, namely $\mathcal{A} = \dot\bigcup_{i=1}^{t} \mathcal{A}_i$ so that $\mathcal{A}$ is Γ inequivalent and $\mathcal{A} \sim \Gamma$.*

Proof. Since every $\Gamma A_i\Gamma$ decomposes into its $\Gamma\alpha_{i,j}$ we have

$$\begin{aligned}\omega &= \Gamma A_1\Gamma \dot\cup ... \dot\cup \Gamma A_t\Gamma \\ &= \Gamma\alpha_{1,1} \dot\cup ... \dot\cup \Gamma\alpha_{1,r_1} \dot\cup ..... \dot\cup \Gamma\alpha_{t,1} \dot\cup ... \dot\cup \Gamma\alpha_{t,r_t}\end{aligned}$$

Since this union is disjoint, $\mathcal{A}$ is inequivalent modulo Γ. For the sake of readability we will show $\mathcal{A} \sim \Gamma$ for $t = 1$ (the case $t > 1$ works out completely the same). Set $r := r_1, A := A_1$ and $\alpha_i := \alpha_{1,i}$ and take $\gamma \in \Gamma$ and $1 \leq i \leq r$ then

$$\alpha_i\gamma \in \Gamma\alpha_i\Gamma = \Gamma A\Gamma = \Gamma\alpha_1 \dot\cup ... \dot\cup \Gamma\alpha_r$$

so that there exists a matrix $\delta =: \delta(\gamma, i)$ and an index $x =: \pi(\gamma, i)$ such that

$$\alpha_i\gamma = \delta\alpha_x$$

Using the Γ-inequivalence of $\mathcal{A}$, one can now easily show that $\pi(\gamma, \cdot)$ is a bijection. □

6.16 Corollary. *Let $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$ be a subgroup of $SL_2(\mathbb{Z})$. For all finite amount of members $A_1, ..., A_t$ of Ω_n, the set $\Gamma A_1 \Gamma \cup ... \cup \Gamma A_t \Gamma$ permits a finite Γ-coset decomposition and for the set of right representatives $\mathcal{A}$ we have $\mathcal{A} \sim \Gamma$.*

Proof. Remove matrices A_i as long as there exist $j \neq i$ with $(A_i) = (A_j)$ and apply the above Lemma afterwards. □

We will now define Hecke operators.

6.17 Definition. *Let $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$ and let χ be a character on Γ of finite order. Let Δ be a semigroup satisfying $\Gamma \subset \Delta \subset \mathbb{R}^\times \mathrm{GL}_2^+(\mathbb{Q})$. Assume that χ can be continued to a character on Δ such that the following condition holds:*

$$\text{if } \alpha\gamma\alpha^{-1} \in \Gamma \text{ for some } \gamma \in \Gamma, \alpha \in \Delta \text{ then } \chi(\alpha\gamma\alpha^{-1}) = \chi(\gamma)$$

Given $\alpha \in \Delta$ such that $\Gamma\alpha\Gamma = \Gamma\alpha_1 \dot\cup ... \dot\cup \alpha_r$ we put $\mathcal{A} := \{\alpha_1, ..., \alpha_r\}$ and define a $\mathbb{C}$-linear map, the Hecke operator with respect to the set $\mathcal{A}$ to be

$$T_{\mathcal{A}} : \mathrm{MF}_k(\Gamma, \chi) \mapsto \mathrm{MF}_k(\Gamma, \chi), \quad T_{\mathcal{A}}(f) := \det(\alpha)^{k/2-1} \sum_{i=1}^{r} \chi(\alpha_i)^{-1} f|_{\alpha_i}$$

For a finite union of double cosets ω as in Lemma 6.15 we put

$$T_{\mathcal{A}}(f) := \sum_{i=1}^{t} T_{\mathcal{A}_i}(f) = n^{k/2-1} \sum_{\alpha \in \mathcal{A}} \chi(\alpha)^{-1} f|_\alpha$$

i.e. $T_{\mathcal{A}_i}$ is to be understood as in the definition above.

6.18 Remark. *(a) Observe that because of Prop. 5.10, the above definition coincides with the one in [Mi], formula (2.8.2).*

(b) One can show that this is a well-defined map which is independent of the concrete choice of the system of right-representatives, cf. [Mi], Thm 2.8.1.

(c) The reason for placing a factor $\det(\alpha)^{k/2-1}$ in front is of cosmetic nature: it makes $T_{\mathcal{A}}$ self-adjoint with respect to the Petersson scalar product, see [Mi], Thm 4.5.4.

Now we want to define Hecke operators on the space VVMF_k too. As vector-valued modular forms transform with another multiplicative symbol ρ it is natural to try to set

$$T_{\mathcal{A}}(F) := \det(\alpha)^{k/2-1} \sum_{i=1}^{r} \rho(\alpha_i)^{-1} F|_{\alpha_i}$$

where we set $F|_\alpha(\tau) := \det(\alpha)^{k/2}(\alpha : \tau)^{-k} F(\alpha.\tau)$ as in the scalar-valued case (note that some authors define the slash operator so that it includes the Weil representation but we will not do so). The difficulty one is confronted with is not the definition of the actual Hecke operator, it is the question how the symbol $\rho(\alpha)$ is to be defined. This is non-trivial as ρ is a map that accepts members from $\mathrm{SL}_2(\mathbb{Z})$ but $\alpha \in \Omega \supsetneq \mathrm{SL}_2(\mathbb{Z})$ and we will show now how to do this following Bruinier [Br]. The main observation is that ρ is a representation of $\mathrm{SL}(\mathbb{Z}_N)$ too if $L(D) \mid N$. This comes from the fact that $\mathrm{SL}(\mathbb{Z}_N) \cong \mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$ and $\Psi_N : \Gamma(N)M \mapsto M \mod N$ is the isomorphism (see for example [Mi], Thm. 4.2.1), i.e. if we want to compute $\rho(M)$ for some $M \in \mathrm{SL}(\mathbb{Z}_N)$ then we select an arbitrary preimage $M_0 \in \mathrm{SL}_2(\mathbb{Z})$ and set $\rho(M) := \rho(M_0)$. It does not matter which preimage we choose: if M_0' is another preimage then a direct computation shows that $M_0 = \gamma M_0'$ for some $\gamma \in \Gamma(N)$ so that

$$\rho(M_0) = \rho(\gamma M_0') = \underbrace{\rho(\gamma)}_{=id} \rho(M_0') = \rho(M_0')$$

see Thm 5.16(c). The question now is how to construct an element in $\mathrm{SL}(\mathbb{Z}_N)$ from $\alpha \in \Omega$. We set $\alpha' := (\sqrt{\det(\alpha)})^{-1} \cdot \alpha \mod N \in \mathrm{SL}(\mathbb{Z}_N)$ whenever this is possible.

In the following, $\alpha \mod N$ for some matrix $\alpha \in \mathbb{Q}^{2\times 2}$ means the following: If there is an $n \in \mathbb{N}$ such that $(n, N) = 1$ and $n\alpha \in \mathbb{Z}$ then the denominators of the entries in α are given by n, a unit in $\mathbb{Z}_N$. We set $a/n \mod N := a \cdot n^{-1} \mod N$ and reduce α component wise in this sense then. Remark that Bruinier uses the character φ_D while we use χ_D but this makes no difference as both characters coincide by Thm. 5.17(c).

6.19 Definition. *Let D be a discriminant-quadratic form of even signature and $L(D) \mid N$. Put*

$$\mathcal{G}(N) := \{\alpha \in \mathrm{GL}_2^+(\mathbb{Q}) \mid \exists n \in \mathbb{Z} \,.\, (n, N) = 1 \,,\; n\alpha \in \mathbb{Z}^{2\times 2} \\ (\det(n\alpha), N) = 1\}$$

$$\mathcal{Q}(N) := \{(\alpha, x) \in \mathcal{G}(N) \times \mathbb{Z}_N^\times \mid \det(\alpha) \equiv x^2 \mod N\}$$

where χ_D is the character defined in 5.11. It is clear that $\mathcal{G}(N)$, $\mathcal{Q}(N)$ are groups. Let $\Psi : \Gamma(N)\backslash SL_2(\mathbb{Z}) \mapsto \mathrm{SL}(\mathbb{Z}_N)$, $\Psi(\Gamma(N)\alpha) = \alpha \mod N$, then Ψ is an isomorphism of groups. For each $(\alpha, x) \in \mathcal{Q}(N)$ we define the action on $\mathbf{e}_\gamma$ to be

$$\rho((\alpha, x)).\mathbf{e}_\gamma := \chi_D(x) \cdot \rho(\Psi^{-1}(x^{-1}\alpha \mod N)).\mathbf{e}_\gamma$$

then ρ is a representation on $\mathcal{Q}(N)$ that continues the original Weil representation in the sense that

$$\rho(M, 1) = \rho(M) \text{ for all } M \in SL_2(\mathbb{Z})$$

For some function $F : \mathbb{H} \mapsto \mathbb{C}[D]$ we set

$$F|_{(\alpha,x)} := \det(\alpha)^{k/2}(\alpha : \tau)^{-k} F(\alpha.\tau)$$

Let $A \in \Omega_n$ such that $(n, N) = 1$ and $n \equiv x^2 \mod N$ for some $x \in \mathbb{Z}_N^\times$. Let $SL_2(\mathbb{Z})ASL_2(\mathbb{Z}) = SL_2(\mathbb{Z})\alpha_1 \dot\cup ... \dot\cup SL_2(\mathbb{Z})\alpha_r$ and $\mathcal{A} = \{\alpha_1, ..., \alpha_r\}$, then we define the Hecke operator

$$T_{\mathcal{A}}^{(x)} : \mathrm{VVMF}_k \mapsto \mathrm{VVMF}_k, T_{\mathcal{A}}^{(x)}(F) := n^{k/2-1} \sum_{i=1}^{r} \rho(\alpha_i, x)^{-1} F|_{(\alpha_i,x)}$$

For a finite union of double cosets ω as in Lemma 6.15 we set

$$T_{\mathcal{A}}^{(x)}(F) := \sum_{i=1}^{t} T_{\mathcal{A}_i}^{(x)}(F) = n^{k/2-1} \sum_{\alpha \in \mathcal{A}} \rho(\alpha, x)^{-1} F|_{(\alpha,x)}$$

6.20 Remark. *Observe that the extended Weil representation is* not *a representation of $\mathcal{G}(N)$ but rather of a subset of $\mathcal{G}(N) \times \mathbb{Z}_N^\times$, for if the determinant of some α has two different roots, the representations $\rho(\alpha, root_1)$ and $\rho(\alpha, root_2)$ do not necessarily coincide, i.e. for the principal result, it is of importance which root has been chosen. That is the reason why we pass an extra index (x) to the Hecke operator in order to specify which root is to be taken.*

A rough motivation to put the factor $\chi_D(x)$ in front of the extended Weil representation is given by the "calculation"

$$\rho(\alpha) = \rho\left(\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} x^{-1} & 0 \\ 0 & x^{-1} \end{pmatrix}\alpha\right) = \rho\left(\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\right)\rho(x^{-1}\alpha)$$

as the definition for the right term is in some way naturally given by the above, it remains to define $\rho\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$. From the observations on the original Weil representation modulo N (cf. Thm 5.16) this diagonal matrix should somehow operate using a multiplication of $\chi_D(x)$. Note that although the original Weil representation sends $\mathbf{e}_\gamma$ to $\chi_D(d) \cdot \mathbf{e}_{d\gamma}$ for a matrix $M \equiv \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \bmod N$ we avoid doing this permutation $\gamma \mapsto d\gamma$ here. The reason for this is how $\mathrm{SL}_2(\mathbb{Z})$ is embedded into $\mathcal{Q}(N)$: A matrix $M \in \mathrm{SL}_2(\mathbb{Z})$ can be regarded as element in $\mathcal{Q}(N)$ via $M \mapsto (M, 1)$. If for example $x^{-1} \equiv x \mod N$ then $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \in \mathrm{SL}(\mathbb{Z}_N)$ so let $M \in \mathrm{SL}_2(\mathbb{Z})$ be a preimage of $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \mod N$. By Thm. 5.16(d),

$$\rho(M).\mathbf{e}_\gamma = \chi_D(x) \cdot \mathbf{e}_{x\gamma}$$

and

$$\rho\left(\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, 1\right).\mathbf{e}_\gamma = \chi_D(1)\rho\left(\Psi^{-1}\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\right).\mathbf{e}_\gamma = \rho(M).\mathbf{e}_\gamma = \chi_D(x) \cdot \mathbf{e}_{x\gamma}$$

so by avoiding the permutation we ensure that the extended Weil representation continues the original one.
Note that due to $F|_{(\alpha,x)}(\tau) = \boxed{\det(\alpha)^{k/2}}\rho(\alpha, x)^{-1}(\alpha : \tau)^{-k}F(\alpha\tau)$, we have

$$\begin{aligned} T_{\mathcal{A}}^{(x)}(F)(\tau) &= n^{k/2-1}\sum_{\alpha\in\mathcal{A}} \rho(\alpha, x)^{-1}F|_{(\alpha,x)}(\tau) \\ &= n^{\boxed{k-1}}\sum_{\alpha\in\mathcal{A}} \rho(\alpha, x)^{-1}(\alpha : \tau)^{-k}F(\alpha\tau) \end{aligned}$$

7 Lifts and Hecke Operators (general setting)

In this section we prove the "commutativity" (e.g. see the theorem below) of the Hecke operators and lifts in a general setting.

7.1 Theorem. *Let D be a discriminant-quadratic form of even signature, $L(D) \mid N$. Let $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$ and chose a system of right representatives $M_1, ..., M_s \in SL_2(\mathbb{Z})$ such that*

$$SL_2(\mathbb{Z}) = \Gamma M_1 \dot\cup ... \dot\cup \Gamma M_s$$

Then, the map $\Psi : \{1, ..., s\} \mapsto \Gamma\backslash SL_2(\mathbb{Z}), \Psi(i) = \Gamma M_i$ is a bijection. Let H be a subset of D and set $\Theta := \sum_{\gamma\in H} \mathbf{e}_\gamma$. Let $\chi : \Gamma \mapsto \mathbb{C}^\times$ be a character of finite order. Assume that $\mathcal{A} \subset \Omega_n$ satisfies the following conditions:

(i) Lift and Hecke operators are well-defined, i.e. $\mathcal{L}_H$ *is well-defined (i.e. it results in vector-valued modular forms and is independent of the concrete choice of the right representatives) and* $(n, N) = 1$ *is such that* $n \equiv x^2 \mod N$ *for some* $x \in \mathbb{Z}_N^\times$ *and the character can be extended as mentioned in 6.17.*

(ii) $\mathcal{A}$ *is* $SL_2(\mathbb{Z})$ *inequivalent (and thus it is in particular* Γ *inequivalent).*

(iii) $\mathcal{A} \sim SL_2(\mathbb{Z})$ *(cf. Def. 6.14).*

(iv) The map $\Phi : \{1, ..., r\} \times \{1, ..., s\} \mapsto \{1, ..., r\} \times \{1, ..., s\}, \Phi(i, j) = (\pi(M_j, i), \Psi^{-1}\Gamma\delta(M_j, i))$ *is a bijection. Note that since* Φ *maps a finite set into the same set, the bijectivity of* Φ *already follows from one of both: injectivity or surjectivity.*

(v) $\rho(\alpha_i, x)^{-1}.\Theta = \chi(\alpha_i)^{-1} \cdot \Theta$*, i.e.* Θ *is an eigenvector for the automorphism* $\rho(\alpha_i, x)^{-1}$ *with eigenvalue* $\chi(\alpha_i)^{-1}$*.*

Then for all $f \in \mathrm{MF}_k(\Gamma, \chi)$*, Lift and Hecke operator commute, i.e.*

$$\boxed{T_{\mathcal{A}}^{(x)} \circ \mathcal{L}_H(f) = \mathcal{L}_H \circ T_{\mathcal{A}}(f)}$$

where $T_{\mathcal{A}}^{(x)}$ *on the left denotes the Hecke operator on vector-valued modular functions as in definition 6.19 while the latter one means the Hecke operator on scalar-valued modular forms as in definition 6.17.*

Proof. Let $\mathcal{I} := \{1,...,r\} \times \{1,...,s\}$.

$$
\begin{aligned}
&\frac{1}{n^{k-1}}\mathcal{L}_H(T_{\mathcal{A}}(f))(\tau) \\
&\quad = \mathcal{L}_H(\sum_{i=1}^{r} \chi(\alpha_i)^{-1}(\alpha_i:*)^{-k} f(\alpha_i.*))(\tau) \\
&\quad = \sum_{j=1}^{s} \rho(M_j)^{-1}. \sum_{i=1}^{r} \underbrace{(\alpha_i : M_j.\tau)^{-k}(M_j:\tau)^{-k}}_{=(\alpha_i M_j:\tau)^{-k}} f((\alpha_i M_j).\tau) \quad \underbrace{\chi(\alpha_i)^{-1}\Theta}_{\substack{=\rho(\alpha_i,x)^{-1}.\Theta \\ \text{by assumption (v)}}} \\
&\quad = \sum_{(i,j)\in\mathcal{I}} \rho\left((M_j,1)^{-1}(\alpha_i,x)^{-1}\right)(\alpha_i M_j:\tau)^{-k} f(\alpha_i M_j \tau)\Theta \\
&\quad = \sum_{(i,j)\in\mathcal{I}} \rho\big((\alpha_i M_j,x)^{-1}\big)(\alpha_i M_j:\tau)^{-k} f(\alpha_i M_j\tau)\Theta \\
&\quad = \sum_{(i,j)\in\mathcal{I}} \rho\big((\delta(M_j,i)\alpha_{\pi(M_j,i)},x)^{-1}\big)(\delta(M_j,i)\alpha_{\pi(M_j,i)}:\tau)^{-k} \\
&\qquad\qquad f(\delta(M_j,i)\alpha_{\pi(M_j,i)}\tau)\Theta \qquad \text{(by ass. (iii))}
\end{aligned}
$$

Fix $v \in \{1,...,r\}$. Since Φ is a bijection (by assumption (iv)), there are precisely s pairs $(i_1,j_1),...,(i_s,j_s)$ such that $\Phi(i_l,j_l) = (v,z_l)$ with

$$z_l = \Psi^{-1}(\Gamma\delta(M_{j_l},i_l)) \tag{7.1}$$

Note that

$$l_1 \neq l_2 \Rightarrow z_{l_1} \neq z_{l_2} \tag{7.2}$$

as otherwise $\Phi(i_{l_1},j_{l_1}) = (v,z_{l_1}) = (v,z_{l_2}) = \Phi(i_{l_2},j_{l_2})$ so that because of the injectivity of Φ, $l_1 = l_2$ must hold in contradiction to the assumption. Hence, by resorting the above sum we obtain (by construction, $\pi(M_{j_l},i_l) = v$

for all l):

$$
\begin{aligned}
&= \sum_{v=1}^{r} \sum_{l=1}^{s} \rho(\alpha_v, x)^{-1}\ \rho(\delta(M_{j_l}, i_l))^{-1}\ (\delta(M_{j_l}, i_l) : \alpha_v)^{-k} \\
&\qquad\qquad (\alpha_v : \tau)^{-k}\ f(\delta(M_{j_l}, i_l)\alpha_v\tau)\Theta \\
&= \sum_{v=1}^{r} \rho(\alpha_v, x)^{-1}(\alpha_v : \tau)^{-k} \\
&\qquad\qquad \left(\sum_{l=1}^{s} \rho(\delta(M_{j_l}, i_l)^{-1})(\delta(M_{j_l}, i_l) : *)^{-k} f(\delta(M_{j_l}, i_l)*)\Theta \right) (\alpha_v\tau) \\
&= \sum_{v=1}^{r} \rho(\alpha_v, x)^{-1}(\alpha_v : \tau)^{-k} \left(\sum_{l=1}^{s} \rho(\delta(M_{j_l}, i_l))^{-1} f|_{\delta(M_{j_l}, i_l)}\Theta \right) (\alpha_v\tau)
\end{aligned}
$$

We claim that $\delta(M_{j_l}, i_l),\ 1 \leq l \leq s$ is a system of right representatives for $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. They are Γ-inequivalent as $\Gamma\delta(M_{j_l}, i_l) = \Gamma\delta(M_{j_{l'}}, i_{l'})$ means nothing else than

$$\Psi(z_l) \overset{(7.1)}{=} \Gamma\delta(M_{j_l}, i_l) = \Gamma\delta(M_{j_{l'}}, i_{l'}) \overset{(7.1)}{=} \Psi(z_{l'})$$

then by the injectivity of Ψ and (7.2), $l = l'$. They generate $\mathrm{SL}_2(\mathbb{Z})$, as $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = s$ and by the Γ inequivalence of the $\delta(M_{j_l}, i_l)$, they already generate s different Γ coset classes. We have shown that $\delta(M_{j_l}, i_l),\ 1 \leq l \leq s$ forms a system of right representatives for $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. Since the lift is independent of the concrete choice of the system of right representatives, for every v we have

$$
\begin{aligned}
&\sum_{l=1}^{s} \rho(\delta(M_{j_l}, i_l))^{-1} f|_{\delta(M_{j_l}, i_l)}\Theta \\
&\qquad = \text{lift of } f \text{ w.r.t. } H \text{ and the RRS } \delta(M_{j_l}, i_l), 1 \leq l \leq n \\
&\qquad = \text{lift of } f \text{ w.r.t. } H \text{ and the RRS } M_j, 1 \leq j \leq n \qquad \text{(by ass. (i))} \\
&\qquad = \mathcal{L}_H(f)
\end{aligned}
$$

so that we finally arrive at

$$\begin{aligned}
&\frac{1}{n^{k-1}}\mathcal{L}_H(T_{\mathcal{A}}(f))(\tau)\\
&\quad=\sum_{v=1}^{r}\rho(\alpha_v,x)^{-1}(\alpha_v:\tau)^{-k}\left(\sum_{l=1}^{s}\rho(\delta(M_{j_l},i_l))^{-1}f|_{\delta(M_{j_l},i_l)}\Theta\right)(\alpha_v\tau)\\
&\quad=\sum_{v=1}^{r}\rho(\alpha_v,x)^{-1}(\alpha_v:\tau)^{-k}\mathcal{L}_H(f)(\alpha_v\tau)\\
&\quad=\frac{n^{k-1}}{n^{k-1}}n^{-k/2}\sum_{v=1}^{r}\rho(\alpha_v,x)^{-1}\mathcal{L}_H(f)|_{(\alpha_v,x)}(\tau)\\
&\quad=\frac{1}{n^{k-1}}n^{k/2-1}\sum_{v=1}^{r}\rho(\alpha_v,x)^{-1}\mathcal{L}_H(f)|_{(\alpha_v,x)}(\tau)\\
&\quad=\frac{1}{n^{k-1}}T_{\mathcal{A}}^{(x)}(\mathcal{L}_H(f))(\tau)
\end{aligned}$$

Thus, multiplying both sides by n^{k-1} yields the assertion. □

Observe that we also have shown that the image under Hecke Operator $T_{\mathcal{A}}^{(x)}$ of a lift of a scalar-valued modular form is independent of the chosen root x whenever the conditions mentioned above hold.
Now we want to apply the above general theorem on three specific subgroups, $\Gamma(N), \Gamma_1(N)$ and $\Gamma_0(N)$ and two kinds of Hecke operators. First we analyze the usual n-th Hecke operator as it is defined in current literature. This Hecke operator usually slashes the function with an RRS of a certain subset of $\bigcup_{\alpha\in\Omega_n}\Gamma\alpha\Gamma$. Secondly, we examine another Hecke operator that just slashes with an RRS of $\Gamma\left(\begin{smallmatrix}1&0\\0&n\end{smallmatrix}\right)\Gamma$. In order to do so, we first need to know how concrete systems of representatives look like for these sets.

8 The case $\Gamma(N)$

In this section we mainly follow the notation from [Ra] since all the results on Hecke operators with $\Gamma(N)$ can be found in this book.

8.1 Definition. *For some $n\in\mathbb{N}$ set $J_n:=\left(\begin{smallmatrix}1&0\\0&n\end{smallmatrix}\right)$. Let $\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathbb{Z}^{2\times 2}$ then we set* $\operatorname{div}(\alpha)=\gcd(a,b,c,d)$. *If* $\operatorname{div}(\alpha)=1$ *we say that α is primitive. Set $\Omega^*:=\{\alpha\in\Omega\mid\alpha$ is primitive$\}$. On Ω, we define some equivalence relations*

$$\alpha\sim_{()}\beta\iff\Gamma(N)\alpha\Gamma(N)=\Gamma(N)\beta\Gamma(N)$$

The equivalence class of some α will be denoted as $(\alpha) := \Gamma(N)\alpha\Gamma(N)$.

$$\alpha \sim_{[]} \beta \iff \alpha \equiv \beta \mod N, \mathrm{div}(\alpha) = \mathrm{div}(\beta) \text{ and } \det(\alpha) = \det(\beta)$$

the equivalence class of α will be denoted by $[\alpha]$.

$$\alpha \sim_{[[]]} \beta \iff \alpha \equiv \beta \mod N \text{ and } \det(\alpha) = \det(\beta)$$

the equivalence class of α will be denoted by $[\![\alpha]\!]$.
Notice that by definition,

$$(\alpha) \subseteq [\alpha] \subseteq [\![\alpha]\!]$$

When we want to play around with N, we emphasis the group $\Gamma(N)$ as a subindex, i.e. $(\alpha)_{\Gamma(N)}, [\alpha]_{\Gamma(N)}$ *and* $[\![\alpha]\!]_{\Gamma(N)}$.

8.2 Theorem. *(a) For $\gamma, \delta \in SL_2(\mathbb{Z})$ and $\alpha \in \Omega$, we have* $\mathrm{div}(\gamma\alpha\delta) = \mathrm{div}(\alpha)$

(b) For every primitive matrix α, there are $\gamma, \gamma' \in \Gamma(N)$ such that $\gamma\alpha\gamma' = J_{\det(\alpha)}$.

(c) For every primitive matrix α, we have $[\alpha] = (\alpha)$.

Proof. See [Ra], (a) is the lemma on Page 274, (b) is Thm. 4.3.6. while (c) is denoted as Thm. 9.1.3. □

8.3 Theorem. *Let $N \in \mathbb{N}, a \in \mathbb{Z}$ such that $(a, N) = 1$. Let* $\overline{R_a} := \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_N)$ *and let R_a be a arbitrary but fixed preimage of this matrix in $SL_2(\mathbb{Z})$. Let $n \in \mathbb{N}$ such that $(n, N) = 1$ then a concrete system of right representatives modulo $\Gamma(N)$ for the set $[\![J_n]\!]$ is given by*

$$\mathcal{A}_{\Gamma(N)}(n) = \big\{\alpha \mid \alpha = R_a\beta \text{ with } \beta = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \text{ such that } a, d \in \mathbb{N}, ad = n, b = \nu N \text{ where } \nu = 0, 1, ..., d-1\big\}$$

Further, $(J_n) = \dot{\cup}_{\alpha \in \mathcal{B}_{\Gamma(N)}(n)} \Gamma(N)\alpha$ *where*

$$\mathcal{B}_{\Gamma(N)}(n) = \{\alpha \in \mathcal{A}_{\Gamma(N)}(n) \mid \alpha \text{ is primitive}\}$$

Proof. See [Ra], formula (9.1.42), p.284 for the definition of T_L^+ and formula (9.1.51), p. 286 for the assertion on $\mathcal{A}_{\Gamma(N)}(n)$ with $(n, N) = 1$. On $\mathcal{B}_{\Gamma(N)}(n)$: Since $(J_n) \subseteq [\![J_n]\!]$ the matrices in $\mathcal{A}_{\Gamma(N)}(n)$ form a system of representatives (but they are not necessarily inequivalent modulo $\Gamma(N)$ and they are not necessarily contained in (J_n)!). Let $\lambda = \gamma J_n \gamma' \in (J_n)$ so that there is an $\alpha \in \mathcal{A}_{\Gamma(N)}(n)$ such that $\lambda = \gamma''\alpha$ for some $\gamma'' \in \Gamma(N)$. By 8.2(a), $\mathrm{div}(\alpha) =$

$\operatorname{div}(\lambda) = \operatorname{div}(J_n) = 1$ so that even the primitive matrices in $\mathcal{A}_{\Gamma(N)}(n)$ form a system of representatives and since the matrices in $\mathcal{A}_{\Gamma(N)}(n)$ were pairwise inequivalent modulo $\Gamma(N)$ so are the primitive ones. So far we have shown

$$(J_n) \subseteq \dot{\cup}_{\substack{\alpha \in \mathcal{A}_{\Gamma(N)}(n) \\ \alpha \text{ primitive}}} \Gamma(N)\alpha$$

the other direction, "$\supseteq$" is clear as $(J_n) = [J_n]$ by Thm. 8.2(c) so that every primitive α in $\mathcal{A}_{\Gamma(N)}(n)$ satisfies the conditions to be in $[J_n] = (J_n)$. $\square$

8.4 Theorem. *Let D be a discriminant-quadratic form of even signature, $L(D) \mid N$ and let H be a subgroup of D. Let $n \in \mathbb{N}$ with $(n, N) = 1$ and $n \equiv x^2 \mod N$ for some $x \in \mathbb{Z}$ then the sets $\mathcal{A} := \mathcal{A}_{\Gamma(N)}(n)$ and $\mathcal{B} := \mathcal{B}_{\Gamma(N)}(n)$ from the last theorem satisfy all conditions of Theorem 7.1 for χ being the trivial character and for every chosen root x. By Theorem 7.1 we obtain*

$$T^{(x)}_{\mathcal{A}_{\Gamma(N)}(n)} \circ \mathcal{L}_H(f) = \mathcal{L}_H \circ T_{\mathcal{A}_{\Gamma(N)}(n)}(f)$$

and

$$T^{(x)}_{\mathcal{B}_{\Gamma(N)}(n)} \circ \mathcal{L}_H(f) = \mathcal{L}_H \circ T_{\mathcal{B}_{\Gamma(N)}(n)}(f)$$

for every $f \in \mathrm{MF}_k(\Gamma(N))$, for every root x of n modulo N and every $k \in \mathbb{Z}$.

Remarks: Although it is not necessary for the lift to use a complete subgroup of D (a single element suffices) we need the subgroup for the commutativity, see equation (8.3) in the subsequent proof. The Hecke operator $T_{\mathcal{A}_{\Gamma(N)}(n)}$ is the usual n-th Hecke operator on $\Gamma(N)$ while $T^{(x)}_{\mathcal{B}_{\Gamma(N)}(n)}$ is the Hecke operator proposed by Bruinier (cf. [Br], §4.3, p.19).

Proof. Concerning the set $\mathcal{A}_{\Gamma(N)}(n)$. We verify the conditions. (i) The lift is well-defined by Remark 6.9. The Hecke operator on $\Gamma(N)$ is well-defined as the set $\mathcal{A}_{\Gamma(N)}(n)$ was explicitly chosen with respect to that operator. Note that the character is trivial so it can be continued trivially to the semigroup $\Delta = \Omega$ (cf. Def. 6.17). It remains to show that the Hecke operator on $\mathrm{SL}_2(\mathbb{Z})$ makes sense. By Thm. 8.3 (set $N = 1$, then $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$!), a system of representatives for the n-th Hecke operator is given by

$$[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})} = \dot{\cup}_{\alpha \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha$$

where (note that Id serves as R_a modulo 1)

$$\mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) = \big\{\alpha \mid \alpha = \beta \text{ with } \beta = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \text{ such that } a, b, d \in \mathbb{N}, ad = n, 0 \le b \le d-1\big\}$$

Set

$$\mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n) = \big\{\alpha \mid \alpha = \beta \text{ with } \beta = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \text{ such that } a, b, d \in \mathbb{N}, ad = n, b = \nu N,\ 0 \leq \nu \leq d-1\big\}$$

then we claim that

$$[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})} = \dot{\cup}_{\alpha' \in \mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha'$$

Consider some $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)$. The map $\{0, ..., (d-1)\} \mapsto \mathbb{Z}_d : x \mapsto x \mod d$ is a bijection but as $(d, N) \mid (n, N) = 1$, so is $\{0, ..., (d-1)\} \mapsto \mathbb{Z}_d : x \mapsto xN \mod d$, i.e. for every $b \in \{0, ..., (d-1)\}$ there is exactly one $x(b) \in \{0, ..., (d-1)\}$ such that $b \equiv x(b) \cdot N \mod d$, i.e. $d \mid b - x(b)N$ so that $n = ad \mid a(b - x(b)N)$. Set $\alpha' = \left(\begin{smallmatrix} a & x(b)N \\ 0 & d \end{smallmatrix}\right)$ then

$$\alpha\alpha'^{-1} = \frac{1}{n}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} d & -x(b)N \\ 0 & a \end{pmatrix} = \frac{1}{n}\begin{pmatrix} n & a(b - x(b)N) \\ 0 & n \end{pmatrix} \in \mathbb{Z}^{2\times 2}$$

but as $\det(\alpha) = \det(\alpha')$, the above matrix is contained in $\mathrm{SL}_2(\mathbb{Z})$ so that $\alpha \sim_{\mathrm{SL}_2(\mathbb{Z})} \alpha'$. Set $\sigma : \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) \mapsto \mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n) : \alpha \mapsto \alpha'$ then σ is injective: $\alpha = \sigma(\alpha_1) = \sigma(\alpha_2)$ then $\alpha_1 \sim_{\mathrm{SL}_2(\mathbb{Z})} \sigma(\alpha_1) = \alpha' = \sigma(\alpha_2) \sim_{\mathrm{SL}_2(\mathbb{Z})} \alpha_2$ so that $\alpha_1 = \alpha_2$ as the α form an $\mathrm{SL}_2(\mathbb{Z})$-RRS. As $|\mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)| = |\mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)|$, σ is bijective so that

$$\begin{aligned} \beta \in [\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})} &\iff \exists \alpha \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) : \mathrm{SL}_2(\mathbb{Z})\beta = \mathrm{SL}_2(\mathbb{Z})\alpha \\ &\iff \exists \alpha' \in \mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n) : \mathrm{SL}_2(\mathbb{Z})\beta = \mathrm{SL}_2(\mathbb{Z})\alpha' \\ &\iff \beta \in \bigcup_{\alpha' \in \mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha' \end{aligned}$$

The disjointness is due to the fact that the α' are left-$\mathrm{SL}_2(\mathbb{Z})$ products of the α and the α are $\mathrm{SL}_2(\mathbb{Z})$-inequivalent and thus, so are the α'.
Since the $\alpha' \in \mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$ are a $\mathrm{SL}_2(\mathbb{Z})$-RRS, we may as well multiply every α from the left side with a matrix $M_{\alpha'} \in \mathrm{SL}_2(\mathbb{Z})$ without changing the RRS property (neither the inequivalence nor the set they generate). For each $\alpha' = \left(\begin{smallmatrix} a & \nu N \\ 0 & d \end{smallmatrix}\right)$ select $M_{\alpha'} = R_a$ where $R_a \in \mathrm{SL}_2(\mathbb{Z})$ is the preimage of $\left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)$ mod N that was used in $\mathcal{A}_{\Gamma(N)}(n)$. Consequently, we have shown that

$$[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})} = \dot{\cup}_{\alpha \in \mathcal{A}_{\Gamma(N)}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha \tag{8.1}$$

Since the Hecke operator on the vector-valued modular forms with respect to $\mathrm{SL}_2(\mathbb{Z})$ is independent of the concrete choice of the RRS for $[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})}$,

we may as well select $\mathcal{A}_{\Gamma(N)}(n)$ for its definition. Hence, the Hecke operators $T_{\mathcal{A}}$ and $T_{\mathcal{A}}^{(x)}$ on the scalar-valued modular forms and on the vector-valued modular forms, which both esentially slash the function with the very same set $\mathcal{A} = \mathcal{A}_{\Gamma(N)}(n)$, are well-defined.

(ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{A}$ is exactly the disjointness of the union in (8.1).

(iii) $\mathcal{A} \sim \mathrm{SL}_2(\mathbb{Z})$ follows from the fact that $[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})}$ decomposes into a finite set of double $\mathrm{SL}_2(\mathbb{Z})$ cosets ($[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})}$ decomposes into a finite union of right $\mathrm{SL}_2(\mathbb{Z})$ cosets $\mathrm{SL}_2(\mathbb{Z})\alpha, \alpha \in \mathcal{A}_{\Gamma(N)}(n)$ then of course, $[\![J_n]\!]_{\mathrm{SL}_2(\mathbb{Z})} = \cup_{\alpha\in\mathcal{A}_{\Gamma(N)}(n)}\mathrm{SL}_2(\mathbb{Z})\alpha\mathrm{SL}_2(\mathbb{Z})$) and Corollary 6.16.

(iv) In the notation of Theorem 7.1, we show that the map $\Phi : \mathcal{I} \mapsto \mathcal{I}, (i,j) \mapsto (\pi(M_j, i), \Psi^{-1}(\Gamma(N)\delta(M_j, i)))$ is injective: Let $\Phi(i,j) = \Phi(i',j')$, then $x := \pi(M_j, \alpha_i) = \pi(M_{j'}, \alpha_{i'})$ and $\delta(M_j, i) = \gamma\delta(M_{j'}, \alpha_{i'})$ for some $\gamma \in \Gamma(N)$. Using these facts yields

$$\alpha_i M_j = \delta(M_j, i)\alpha_{\pi(M_j,i)} = \gamma\delta(M_{j'}, i')\alpha_x = \gamma\alpha_{i'}M_{j'} \tag{8.2}$$

As $\alpha_i, \alpha_{i'} \in \mathcal{A}_{\Gamma(N)}(n)$, they are of the structure

$$R_a \begin{pmatrix} a & \nu N \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} a & \nu N \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \mod N$$

Let $M_j = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right), M_{j'} = \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}$ then by taking equation (8.2) modulo N we obtain:

$$\begin{pmatrix} x & y \\ nz & nw \end{pmatrix} \equiv \alpha_i M_j \equiv \gamma\alpha_{i'}M_{j'} \equiv \begin{pmatrix} x' & y' \\ nz' & nw' \end{pmatrix}$$

From the first row we see that $x \equiv x' \mod N$ and $y \equiv y' \mod N$. As $(n, N) = 1$, n is a unit in $\mathbb{Z}_N$ and thus it follows from the second row that $z \equiv z' \mod N$ and $w \equiv w' \mod N$ and from this we directly compute $M_j(M_{j'})^{-1}$ to be in $\Gamma(N)$, hence $M_j \sim_{\Gamma(N)} M_{j'}$. As the M_j form a $\Gamma(N)$-RRS, $j = j'$. After we multiplied equation (8.2) from the right by $M_j^{-1} = M_{j'}^{-1}$, we deduce that $\alpha_i \sim_{\Gamma(N)} \alpha_{i'}$. Since the α_i form a $\Gamma(N)$-RRS, it follows that $i = i'$ and consequently the injectivity of Φ.

(v) Let

$$\alpha = R_a \left(\begin{smallmatrix} a & \nu N \\ 0 & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & a^{-1}\nu N \\ 0 & d \end{smallmatrix}\right) \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \mod N$$

Let $X \in \mathrm{SL}_2(\mathbb{Z})$ so that

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \equiv x\alpha^{-1} \equiv x\begin{pmatrix} 1 & 0 \\ 0 & n^{-1} \end{pmatrix} \equiv \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mod N$$

Put $y := x^{-1} \bmod N$, then by the definition of the extended Weil representation,

$$\begin{aligned}\rho(\alpha, x)^{-1}\mathbf{e}_\gamma &= \rho(\alpha^{-1}, x^{-1})\mathbf{e}_\gamma \\ &= \chi_D(x^{-1})\rho(X)\mathbf{e}_\gamma \\ &= \chi_D(x^{-1})\chi_D(x_4)\mathbf{e}_{x_4\gamma} \qquad \text{(by 5.16 (b))} \\ &= \cancel{\chi_D(x)^{-1}}\cancel{\chi_D(x)}\mathbf{e}_{y\gamma}\end{aligned}$$

where the last step is valid as $x_4 \equiv y \mod N$ and χ_D is a character modulo N. Furthermore, let $x_4 = y + vN$ then $x_4\gamma = y\gamma + vN\gamma$ and $N\gamma = 0$ in D according to Corollary 5.5.
For $\Theta = \sum_{\gamma\in H} \mathbf{e}_\gamma$ we therefore obtain

$$\rho(\alpha, x)^{-1}\Theta = \sum_{\gamma\in H} \mathbf{e}_{y\gamma} = \sum_{\gamma\in H} \mathbf{e}_\gamma = \chi(\alpha)^{-1} \cdot \Theta \tag{8.3}$$

because $\gamma \mapsto y\gamma$ is a bijection on H (as $(y, |H|) \mid (y, |D|) = 1$ by Corollary 5.6) and χ is the trivial character.

Concerning the set $\mathcal{B}_{\Gamma(N)}(n)$: (i) Lift and Hecke operator on scalar-valued modular forms of $\Gamma(N)$ are well defined: as above. Using Theorem 8.3 for $N = 1$, i.e. $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, we obtain that

$$\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n) = \{\alpha \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) \mid \alpha \text{ is primitive}\}$$

i.e.

$$(J_n)_{\mathrm{SL}_2(\mathbb{Z})} = \dot\cup_{\alpha\in\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha$$

Set

$$\begin{aligned}\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n) = \big\{\alpha \mid \alpha = \beta \text{ with } \beta = \left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) \text{ such that} \\ a, b, d \in \mathbb{N}, ad = n, b = \nu N, 0 \le \nu \le d-1 \text{ and } \beta \text{ is primitive}\big\}\end{aligned}$$

then we claim that

$$(J_n)_{\mathrm{SL}_2(\mathbb{Z})} = \dot\cup_{\alpha'\in\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha'$$

The function

$$\sigma : \alpha = \begin{pmatrix} a & b \\ 0 & d\end{pmatrix} \mapsto \begin{pmatrix} a & x(b)N \\ 0 & d\end{pmatrix} =: \alpha'$$

from the first part of the proof maps $\mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)$ bijectively to $\mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$ but it also maps $\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)$ bijectively to $\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$: Let $b \equiv x(b)N \mod d$, say $b = x(b)N + kd$ then

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \text{ primitive } \iff \alpha' = \begin{pmatrix} a & x(b)N \\ 0 & d \end{pmatrix} \text{ primitive}$$

"$\Rightarrow$": Assume that for some $s \neq 1$ we have $s \mid a, s \mid b, s \mid x(b) \cdot N$ then s also divides $x(b)N + kd = b$ so that α is not primitive. Contradiction. "$\Leftarrow$": Completely analogous. Consequently, for an $\alpha' \in \mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$, select the preimage α under the map σ on the whole set $\mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)$, then, by the above, $\alpha \in \mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)$ so that $\alpha' = \sigma(\alpha) \in \mathrm{Im}(\sigma|_{\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)})$ and $\sigma|_{\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)}$ is surjective. As σ is injective, so is $\sigma|_{\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)}$.

Consequently

$$\begin{aligned} \beta \in (J_n)_{\mathrm{SL}_2(\mathbb{Z})} &\iff \exists \alpha \in \mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n) : \mathrm{SL}_2(\mathbb{Z})\beta = \mathrm{SL}_2(\mathbb{Z})\alpha \\ &\iff \exists \alpha' \in \mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n) : \mathrm{SL}_2(\mathbb{Z})\beta = \mathrm{SL}_2(\mathbb{Z})\alpha' \\ &\iff \beta \in \bigcup_{\alpha' \in \mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha' \end{aligned}$$

the disjointness is clear as the elements in $\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$ are a subset of an $\mathrm{SL}_2(\mathbb{Z})$-RRS. Now we proceed as we did with $\mathcal{A}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$: we multiply every $\alpha' \in \mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$ by R_a that was used in $\mathcal{A}_{\Gamma(N)}(n)$ and do not change the RRS property of the elements in $\mathcal{B}'_{\mathrm{SL}_2(\mathbb{Z})}(n)$. Summarized, the Hecke operators on the scalar-valued modular forms and on the vector-valued modular forms with the very same set $\mathcal{B} = \mathcal{B}_{\Gamma(N)}(n)$ are well-defined.

(ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{B}$ as they are a subset of an $\mathrm{SL}_2(\mathbb{Z})$-RRS.

(iii) $\mathcal{B} \sim \mathrm{SL}_2(\mathbb{Z})$ follows directly from Lemma 6.15 as they form an $\mathrm{SL}_2(\mathbb{Z})$-RRS for a single double coset $(J_n)_{\mathrm{SL}_2(\mathbb{Z})}$.

(iv) Here the argument is the same as in the case for $\mathcal{A} = \mathcal{A}_{\Gamma(N)}(n)$: the only thing we really used was the fact that $\alpha \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & n \end{smallmatrix}\right)$ which is still true for all $\mathcal{B}$ as $\mathcal{B} \subset \mathcal{A}$.

(v) directly follows from $\mathcal{B} \subset \mathcal{A}$. □

9 The case $\Gamma_1(N)$

9.1 Theorem. *Let $N \in \mathbb{N}, a \in \mathbb{Z}$ such that $(a, N) = 1$. Let $\overline{R_a} := \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_N)$ and let R_a be a arbitrary but fixed preimage of this matrix in $SL_2(\mathbb{Z})$.*

Set

$$\Delta^n(N) := \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; c \equiv 0 \mod N, a \equiv 1 \mod N, \det(\alpha) = n \right\}$$

Let $n \in \mathbb{N}$ such that $(n, N) = 1$ then a concrete system of right representatives modulo $\Gamma_1(N)$ for the set $\Delta^n(N)$ is given by

$$\mathcal{A}_{\Gamma_1(N)}(n) = \{\alpha \mid \alpha = R_a\beta \text{ with } \beta = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \text{ such that } a, d \in \mathbb{N}, ad = n, b = 0, 1, ..., d-1\}$$

Further, $\Gamma_1(N)J_n\Gamma_1(N) = \dot{\cup}_{\alpha \in \mathcal{B}_{\Gamma_1(N)}(n)} \Gamma_1(N)\alpha$ where

$$\mathcal{B}_{\Gamma_1(N)}(n) = \{\alpha \in \mathcal{A}_{\Gamma_1(N)}(n) \mid \alpha \text{ is primitive}\}$$

Proof. See [Ko], formula (5.28) on Page 167. Concerning $\mathcal{B}_{\Gamma_1(N)}(n)$: Since $\Gamma_1(N)J_n\Gamma_1(N) \subseteq \Delta^n(N)$ the matrices in $\mathcal{A}_{\Gamma_1(N)}(n)$ form a system of representatives (but they are not necessarily inequivalent modulo $\Gamma_1(N)$ and they are not necessarily contained in $\Gamma_1(N)J_n\Gamma_1(N)$!). As it was the case with $\Gamma(N)$, even the primitive matrices in $\mathcal{A}_{\Gamma_1(N)}(n)$ form a system of representatives and are inequivalent modulo $\Gamma_1(N)$. So far we have shown

$$\Gamma_1(N)J_n\Gamma_1(N) \subseteq \dot{\cup}_{\substack{\alpha \in \mathcal{A}_{\Gamma_1(N)}(n) \\ \alpha \text{ primitive}}} \Gamma_1(N)\alpha$$

For the other direction, we use results from $\Gamma(N)$ although we are actually working with $\Gamma_1(N)$. Let $\alpha = R_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{A}_{\Gamma_1(N)}(n)$ be primitive. Put $y := a^{-1}b \bmod d\, N$ (remark: $ad = n$ and $(n, N) = 1$ so that a is a unit in $\mathbb{Z}_N$!) and $\gamma := \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, then

$$J_n\gamma = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & a^{-1}b \\ 0 & n \end{pmatrix} \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \alpha$$

Now $J_n\gamma$ and α are primitive, have the same determinant and are congruent modulo N, hence $\alpha \in [J_n]_{\Gamma(N)} = (J_n)_{\Gamma(N)}$ by Thm. 8.2(c). This means that there exists $\gamma_1, \gamma_2 \in \Gamma(N)$ such that $\gamma_1 J_n \gamma \gamma_2 = \alpha$, i.e. $\alpha \in \Gamma_1(N)J_n\Gamma_1(N)$. The disjointness of the union is clear as the $\alpha \in \mathcal{A}_{\Gamma_1(N)}(n)$ already form a $\Gamma_1(N)$-RRS. □

9.2 Theorem. *Let D be a discriminant-quadratic form of even signature, $L(D) \mid N$ and let S_0 be an isotropic subgroup of D. Let $n \in \mathbb{N}$ with $(n, N) = 1$ and $n \equiv x^2 \mod N$ for some $x \in \mathbb{Z}$ then the sets $\mathcal{A} := \mathcal{A}_{\Gamma_1(N)}(n)$ and $\mathcal{B} := \mathcal{B}_{\Gamma_1(N)}(n)$ from the last theorem satisfy all conditions of Theorem 7.1*

for χ being the trivial character and for every chosen root x. By Theorem 7.1 we obtain

$$T^{(x)}_{\mathcal{A}_{\Gamma_1(N)}(n)} \circ \mathcal{L}_{S_0}(f) = \mathcal{L}_{S_0} \circ T_{\mathcal{A}_{\Gamma_1(N)}(n)}(f)$$

and

$$T^{(x)}_{\mathcal{B}_{\Gamma_1(N)}(n)} \circ \mathcal{L}_{S_0}(f) = \mathcal{L}_{S_0} \circ T_{\mathcal{B}_{\Gamma_1(N)}(n)}(f)$$

for every $f \in \mathrm{MF}_k(\Gamma_1(N))$, for every root x of n modulo N and every $k \in \mathbb{Z}$.

Remarks: Although it is not necessary for the lift to use an isotropic subgroup of D (a single element suffices) we need the isotropy and the subgroup property for the commutativity, see equation (9.3) in the subsequent proof. The Hecke operator $T_{\mathcal{A}_{\Gamma_1(N)}(n)}$ is the usual n-th Hecke operator on $\Gamma_1(N)$ while $T^{(x)}_{\mathcal{B}_{\Gamma_1(N)}(n)}$ is the Hecke operator proposed by Bruinier (cf. [Br], §4.3, p.19).

Proof. Concerning the set $\mathcal{A}_{\Gamma_1(N)}(n)$. We verify the conditions. (i) The lift is well-defined because of remark 6.10. The Hecke operator for $\Gamma_1(N)$ is well-defined as the set $\mathcal{A}_{\Gamma_1(N)}(n)$ was explicitly chosen with respect to that operator. The character is trivial and can be continued trivially to the semigroup $\Delta = \Omega$ (cf. Def. 6.17). It remains to show that the Hecke operator for $\mathrm{SL}_2(\mathbb{Z})$ makes sense. This is easier as it was the case with $\Gamma(N)$ because we do not need to manipuly the upper right entry. We just multiply every $\alpha \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)$ from the left by R_a that was used in $\mathcal{A}_{\Gamma_1(N)}(n)$ whithout changing the RRS-property or the $\mathrm{SL}_2(\mathbb{Z})$-span of the α to obtain

$$\Delta^n(1) = \dot{\bigcup}_{\alpha \in \mathcal{A}_{\Gamma_1(N)}(n)} \mathrm{SL}_2(\mathbb{Z})\alpha \tag{9.1}$$

and

$$\Delta^n(N) = \dot{\bigcup}_{\alpha \in \mathcal{A}_{\Gamma_1(N)}(n)} \Gamma_1(N)\alpha$$

Since the Hecke operator on the vector-valued modular forms with respect to $\mathrm{SL}_2(\mathbb{Z})$ is independent of the concrete choice of the RRS for $\Delta^n(N)$, we may as well select $\mathcal{A}_{\Gamma_1(N)}(n)$ for its definition. Hence, the Hecke operators $T_{\mathcal{A}}$ and $T^{(x)}_{\mathcal{A}}$ on the scalar-valued modular forms and on the vector-valued modular forms, which both esentially slash the function with the very same set $\mathcal{A} = \mathcal{A}_{\Gamma_1(N)}(n)$, are well-defined. (ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{A}$ is exactly the disjointness of the union in (9.1).

(iii) $\mathcal{A} \sim \mathrm{SL}_2(\mathbb{Z})$ follows from the fact that $\Delta^n(1)$ decomposes into a finite set of double $\mathrm{SL}_2(\mathbb{Z})$ cosets ($\Delta^n(1)$ decomposes into a finite union

of right $\mathrm{SL}_2(\mathbb{Z})$ cosets $\mathrm{SL}_2(\mathbb{Z})\alpha, \alpha \in \mathcal{A}$ then, as $\Delta^n(1)$ is closed under multiplication from both sides with matrices lying in $\mathrm{SL}_2(\mathbb{Z})$, $\Delta^n(1) = \cup_{\alpha\in\mathcal{A}}\mathrm{SL}_2(\mathbb{Z})\alpha\mathrm{SL}_2(\mathbb{Z}))$ and Corollary 6.16.

(iv) In the notation of Theorem 7.1, we show that the map $\Phi : \mathcal{I} \mapsto \mathcal{I}, (i,j) \mapsto (\pi(M_j, i), \Psi^{-1}(\Gamma_1(N)\delta(M_j, i)))$ is injective: Let $\Phi(i,j) = \Phi(i',j')$, then $x := \pi(M_j, \alpha_i) = \pi(M_{j'}, \alpha_{i'})$ and $\delta(M_j, i) = \gamma\delta(M_{j'}, \alpha_{i'})$ for some $\gamma \in \Gamma_1(N)$. Using these facts yields

$$\alpha_i M_j = \delta(M_j, i)\alpha_{\pi(M_j,i)} = \gamma\delta(M_{j'}, i')\alpha_x = \gamma\alpha_{i'}M_{j'} \tag{9.2}$$

As $\alpha_i, \alpha_{i'} \in \mathcal{A}_{\Gamma_1(N)}(n)$, they are of the structure

$$R_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \mod N$$

Let $M_j = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right), M_{j'} = \left(\begin{smallmatrix} x' & y' \\ z' & w' \end{smallmatrix}\right)$ then by taking equation (9.2) modulo N we obtain:

$$\begin{pmatrix} * & * \\ nz & nw \end{pmatrix} \equiv \alpha_i M_j \equiv \gamma\alpha_{i'}M_{j'} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\begin{pmatrix} * & * \\ nz' & nw' \end{pmatrix} \equiv \begin{pmatrix} * & * \\ nz' & nw' \end{pmatrix}$$

As $(n, N) = 1$, n is a unit in $\mathbb{Z}_N$ and thus it follows that $z \equiv z' \mod N$ and $w \equiv w' \mod N$ and from this we directly compute $M_j(M_{j'})^{-1}$ to be in $\Gamma_1(N)$, hence $M_j \sim_{\Gamma_1(N)} M_{j'}$. As the M_j form a $\Gamma_1(N)$-RRS, $j = j'$. After we multiplied equation (9.2) from the right by $M_j^{-1} = M_{j'}^{-1}$, we deduce that $\alpha_i \sim_{\Gamma_1(N)} \alpha_{i'}$. Since the α_i form a $\Gamma_1(N)$-RRS, it follows that $i = i'$ and consequently the injectivity of Φ.

(v) Let

$$\alpha = R_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} 1 & a^{-1}b \\ 0 & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \mod N$$

Let $X \in \mathrm{SL}_2(\mathbb{Z})$ so that

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \equiv x\alpha^{-1} \equiv x\begin{pmatrix} 1 & -a^{-1}b \\ 0 & n^{-1} \end{pmatrix} \equiv \begin{pmatrix} x & -xa^{-1}b \\ 0 & x^{-1} \end{pmatrix} \mod N$$

Put $y := x^{-1} \operatorname{mod} N$, then by the definition of the extended Weil representation, for every $\gamma \in S_0$,

$$\begin{aligned} \rho(\alpha, x)^{-1}\mathbf{e}_\gamma &= \rho(\alpha^{-1}, x^{-1})\mathbf{e}_\gamma \\ &= \chi_D(x^{-1})\rho(X)\mathbf{e}_\gamma \\ &= \chi_D(x^{-1})e(-x_2x_4Q(\gamma))\chi_D(x_4)\mathbf{e}_{x_4\gamma} \qquad \text{(by 5.16 (c))} \\ &= \cancel{\chi_D(x)^{-1}}\cancel{\chi_D(x)}\mathbf{e}_{y\gamma} \end{aligned}$$

where the last step is valid as $x_4 \equiv y \mod N$ and χ_D is a character modulo N. Furthermore, let $x_4 = y + vN$ then $x_4\gamma = y\gamma + vN\gamma$ and $N\gamma = 0$ in D according to Corollary 5.5. Finally, $e(-x_2x_4Q(\gamma)) = 1$ because $\gamma \in S_0$ and S_0 was isotropic so that $Q(\gamma) = 0 + \mathbb{Z}$.
For $\Theta = \sum_{\gamma \in S_0} \mathbf{e}_\gamma$ we therefore obtain

$$\rho(\alpha, x)^{-1}\Theta = \sum_{\gamma \in S_0} \mathbf{e}_{y\gamma} = \sum_{\gamma \in S_0} \mathbf{e}_\gamma = \Theta = \chi(\alpha)^{-1} \cdot \Theta \tag{9.3}$$

because $\gamma \mapsto y\gamma$ is a bijection on S_0 (as $(y, |S_0|) \mid (y, |D|) = 1$ by Corollary 5.6) and χ is the trivial character.

Concerning the set $\mathcal{B}_{\Gamma_1(N)}(n)$: (i) Lift and Hecke operator on scalar-valued modular forms of $\Gamma_1(N)$ are well defined: as above. Using Theorem 9.1 we obtain

$$\mathcal{B}_{\Gamma_1(N)}(n) = \{\alpha \in \mathcal{A}_{\Gamma_1(N)}(n) \mid \alpha \text{ is primitive}\}$$

Furthermore, by using 9.1 for $N = 1$, i.e. $\Gamma_1(1) = \mathrm{SL}_2(\mathbb{Z})$, we obtain that

$$\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n) = \{\alpha \in \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) \mid \alpha \text{ is primitive}\}$$

i.e.

$$\mathrm{SL}_2(\mathbb{Z})J_n\mathrm{SL}_2(\mathbb{Z}) = \dot{\cup}_{\alpha \in \mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)}\mathrm{SL}_2(\mathbb{Z})\alpha$$

Set $\sigma : \mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n) \mapsto \mathcal{B}_{\Gamma_1(N)}(n) : \alpha \mapsto R_a\alpha$ where R_a is the matrix that was used for α in $\mathcal{B}_{\Gamma_1(N)}(n)$. Since $\sigma(\alpha)$ is primitive iff. α is (by 8.2(a)), this procedure obviously maps bijectively from $\mathcal{B}_{\mathrm{SL}_2(\mathbb{Z})}(n)$ to $\mathcal{B}_{\Gamma_1(N)}(n)$ and, as usual, this does not affect the RRS-property nor the $\mathrm{SL}_2(\mathbb{Z})$-span of the α so that

$$\mathrm{SL}_2(\mathbb{Z})J_n\mathrm{SL}_2(\mathbb{Z}) = \dot{\cup}_{\alpha \in \mathcal{B}_{\Gamma_1(N)}(n)}\mathrm{SL}_2(\mathbb{Z})\alpha$$

and we may take this set of right representatives for the definition of the Hecke operator on $\mathrm{SL}_2(\mathbb{Z})$. Summarized, the Hecke operators on scalar-valued modular forms and on vector-valued modular forms with the very same set $\mathcal{B} = \mathcal{B}_{\Gamma(N)}(n)$ are well-defined.

(ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{B}$ follows as they are a subset of an $\mathrm{SL}_2(\mathbb{Z})$-RRS.

(iii) $\mathcal{B} \sim \mathrm{SL}_2(\mathbb{Z})$ follows directly from Lemma 6.15 as they form an $\mathrm{SL}_2(\mathbb{Z})$-RRS for a single double coset $\Gamma_1(N)J_n\Gamma_1(N)$.

(iv) Here the argument is the same as in the case for $\mathcal{A} = \mathcal{A}_{\Gamma(N)}(n)$: the only thing we really used was the fact that $\alpha \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & n \end{smallmatrix}\right)$ which is still true for all $\mathcal{B}$ as $\mathcal{B} \subset \mathcal{A}$.

(v) directly follows from $\mathcal{B} \subset \mathcal{A}$. □

10 The case $\Gamma_0(N)$

10.1 Theorem. *Let $N \in \mathbb{N}$ and set*

$$\Delta_0(N) := \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Omega \;\middle|\; N \mid c, (a, N) = 1 \right\}$$

Let $n \in \mathbb{N}$ such that $(n, N) = 1$ then a concrete system of right representatives modulo $\Gamma_1(N)$ for the set

$$\mathcal{T}_{\Gamma_0(N)}(n) := \bigcup_{\alpha \in \Delta_0(N) \cap \Omega_n} \Gamma_0(N) \alpha \Gamma_0(N)$$

is given by

$$\mathcal{A}_{\Gamma_0(N)}(n) = \{\alpha \mid \alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \text{ with } a, d \in \mathbb{N}, ad = n, b = 0, 1, ..., d-1\}$$

Further, $\Gamma_0(N) J_n \Gamma_0(N) = \dot{\cup}_{\alpha \in \mathcal{B}_{\Gamma_0(N)}(n)} \Gamma_0(N) \alpha$ where

$$\mathcal{B}_{\Gamma_0(N)}(n) = \{\alpha \in \mathcal{A}_{\Gamma_0(N)}(n) \mid \alpha \text{ is primitive}\}$$

Proof. Concerning the set $\mathcal{A}_{\Gamma_0(N)}(n)$: See [Mi], formula (4.5.25), Page 142. Concerning $\mathcal{B}_{\Gamma_0(N)}(n)$: Either we copy the proof from the case $\Gamma_1(N)$ and substitute $\Gamma_1(N)$ by $\Gamma_0(N)$ or we use [Mi], formula (4.5.24) where in his notation, $T(l, m) = \Gamma_0(N) \left(\begin{smallmatrix} l & 0 \\ 0 & m \end{smallmatrix}\right) \Gamma_0(N)$ so that we set $l = 1, m = n$. □

For the bijection we need a preparatory lemma that is normally used to compute the index of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$:

10.2 Lemma. *Let R be a commutative ring with 1, then we set*

$$G^1(R) := \{(a, b) \in R^2 \mid \exists x, y \in R \; xa + yb = 1\}$$

On $G^1(R)$ we define an equivalence relation $(a, b) \sim (a', b') \iff \exists \epsilon \in R^\times (\epsilon a, \epsilon b) = (a', b')$ and denote the equivalence class of (a, b) by $[(a, b)]$. We put $P^1(R) := G^1(R)/\sim$, then the map

$$\xi : \Gamma_0(N) \backslash SL_2(\mathbb{Z}) \mapsto P^1(\mathbb{Z}_N), \; \Gamma_0(N) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto [(c, d)]$$

is a bijection.

Proof. This is a direct computation that is left to the reader. □

10.3 Theorem. *Let D be a discriminant-quadratic form of even signature, $L(D) \mid N$ and let S_0 be an isotropic subgroup of D. Let $n \in \mathbb{N}$ with $(n,N)=1$ and $n \equiv x^2 \mod N$ for some $x \in \mathbb{Z}$ then the sets $\mathcal{A} := \mathcal{A}_{\Gamma_0(N)}(n)$ and $\mathcal{B} := \mathcal{B}_{\Gamma_0(N)}(n)$ from the last theorem satisfy all conditions of Theorem 7.1 for χ being the character χ_D and for every chosen root x. By Theorem 7.1 we obtain*

$$T^{(x)}_{\mathcal{A}_{\Gamma_0(N)}(n)} \circ \mathcal{L}_{S_0}(f) = \mathcal{L}_{S_0} \circ T_{\mathcal{A}_{\Gamma_0(N)}(n)}(f)$$

and

$$T^{(x)}_{\mathcal{B}_{\Gamma_0(N)}(n)} \circ \mathcal{L}_{S_0}(f) = \mathcal{L}_{S_0} \circ T_{\mathcal{B}_{\Gamma_0(N)}(n)}(f)$$

for every $f \in \mathrm{MF}_k(\Gamma_0(N), \chi_D)$, for every root x of n modulo N and every $k \in \mathbb{Z}$.

Proof. Concerning the set $\mathcal{A}_{\Gamma_0(N)}(n)$. We verify the conditions. (i) The lift is well defined by Thm. 6.8(a). The character on $\Gamma_0(N)$ is not trivial, it is defined by

$$\chi \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \chi_D(d)$$

The character on $\Gamma_0(N)$ will also be called χ_D from now on. By [Mi], formula (4.5.8) on Page 134,

$$\chi_D \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \overline{\chi_D(a)}$$

is a continuation of the character χ_D to the semigroup $\Delta = \Delta_0(N)$ that satisfies the condition in definition 6.17. By theorem 10.1, the system of representatives for the Hecke operator on $\Gamma_0(N)$ and $\mathrm{SL}_2(\mathbb{Z})$ coincide by construction, i.e. $\mathcal{A} = \mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n) = \mathcal{A}_{\Gamma_0(N)}(n)$ so that we have nothing left to do here and the Hecke operators $T_{\mathcal{A}}$ and $T^{(x)}_{\mathcal{A}}$ on the scalar-valued modular forms and on the vector-valued modular forms, which both esentially slash the function with the very same set $\mathcal{A} = \mathcal{A}_{\Gamma_0(N)}(n)$, are well-defined.

(ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{A}$ is given by definition.

(iii) Completely analogous to the case of $\Gamma_1(N)$.

(iv) In the notation of Theorem 7.1, we show that the map $\Phi : \mathcal{I} \mapsto \mathcal{I}, (i,j) \mapsto (\pi(M_j, i), \Psi^{-1}(\Gamma_0(N)\delta(M_j, i)))$ is injective: Let $\Phi(i,j) = \Phi(i',j')$, then $x := \pi(M_j, \alpha_i) = \pi(M_{j'}, \alpha_{i'})$ and $\delta(M_j, i) = \gamma\delta(M_{j'}, \alpha_{i'})$ for some $\gamma \in \Gamma_0(N)$. Using these facts yields

$$\alpha_i M_j = \delta(M_j, i)\alpha_{\pi(M_j,i)} = \gamma\delta(M_{j'}, i')\alpha_x = \gamma\alpha_{i'}M_{j'} \tag{10.1}$$

As $\alpha_i, \alpha_{i'} \in \mathcal{A}_{\Gamma_0(N)}(n)$, they are of the structure $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mod N$. Let $M_j = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right), M_{j'} = \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}$ and $\gamma = \left(\begin{smallmatrix} \delta & * \\ 0 & \epsilon \end{smallmatrix}\right)$ then by taking equation (10.1) modulo N we obtain:

$$\begin{pmatrix} * & * \\ dz & dw \end{pmatrix} \equiv \alpha_i M_j \equiv \gamma \alpha_{i'} M_{j'} \equiv \begin{pmatrix} * & * \\ 0 & \epsilon \end{pmatrix} \begin{pmatrix} * & * \\ d'z' & d'w' \end{pmatrix} \equiv \begin{pmatrix} * & * \\ \epsilon d'z' & \epsilon d'w' \end{pmatrix}$$

As $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $1 \equiv \delta\epsilon \mod N$ so that ϵ is a unit in $\mathbb{Z}_N$. As $(n, N) = 1$, n is a unit in $\mathbb{Z}_N$ and thus it follows solely from the second row that $(z, w) = \epsilon d'(z', w')$ so that in the language of Lemma 10.2 we have

$$\xi(\Gamma_0(N) M_j) = [(z, w)] = \left[(z', w')\right] = \xi(\gamma_0(N) M_{j'})$$

Since ξ is injective, $\Gamma_0(N) M_j = \Gamma_0(N) M_{j'}$ and as the M_j form a $\Gamma_0(N)$-RRS, $j = j'$. After we multiplied equation (10.1) from the right by $M_j^{-1} = M_{j'}^{-1}$, we deduce that $\alpha_i \sim_{\Gamma_0(N)} \alpha_{i'}$. Since the α_i form a $\Gamma_0(N)$-RRS, it follows that $i = i'$ and consequently the injectivity of Φ.

(v) Let $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{A}$. Let $X \in \mathrm{SL}_2(\mathbb{Z})$ so that

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \equiv x\alpha^{-1} \equiv x \begin{pmatrix} a^{-1} & -b/n \\ 0 & d^{-1} \end{pmatrix} \equiv \begin{pmatrix} xa^{-1} & -xb/n \\ 0 & xd^{-1} \end{pmatrix} \mod N$$

Put $y := xd^{-1} \operatorname{modd} N$, then by the definition of the extended Weil representation, for every $\gamma \in S_0$,

$$\begin{aligned} \rho(\alpha, x)^{-1} \mathbf{e}_\gamma &= \rho(\alpha^{-1}, x^{-1}) \mathbf{e}_\gamma \\ &= \chi_D(x^{-1}) \rho(X) \mathbf{e}_\gamma \\ &= \chi_D(x^{-1}) e(-x_2 x_4 Q(\gamma)) \chi_D(x_4) \mathbf{e}_{x_4\gamma} \qquad \text{(by 5.16 (c))} \\ &= \cancel{\chi_D(x)^{-1}} \cancel{\chi_D(x)} \chi_D(d^{-1}) \mathbf{e}_{y\gamma} \end{aligned}$$

where the last step is valid as $x_4 \equiv y \mod N$ and χ_D is a character modulo N. Furthermore, let $x_4 = y + vN$ then $x_4\gamma = y\gamma + vN\gamma$ and $N\gamma = 0 + L$ in D according to Corollary 5.5. Finally, $e(-x_2 x_4 Q(\gamma)) = 1$ because $\gamma \in S_0$ and S_0 was isotropic so that $Q(\gamma) = 0 + \mathbb{Z}$. We compute $\chi_D(d^{-1})$ to be $\overline{\chi_D(a)}$, because [note that $\chi_D(\cdot) = \chi_D(\cdot^{-1}) = \overline{\chi_D(\cdot)}$ as χ_D is quadratic and that $1 \equiv \det(x\alpha^{-1}) \equiv (xa^{-1}) \cdot (xd^{-1})$]:

$$\begin{aligned} \chi_D(d^{-1}) &= \chi_D(x^{-1}) \chi_D(xd^{-1}) = \chi_D(x^{-1}) \chi_D((xd^{-1})^{-1}) \\ &= \chi_D(x^{-1}) \chi_D(xa^{-1}) = \chi_D(a^{-1}) = \chi_D(a)^{-1} = \overline{\chi_D(a)}^{-1} = \chi_D(\alpha)^{-1} \end{aligned}$$

by the definition of the continuation of the character χ_D on $\Delta_0(N)$.

For $\Theta = \sum_{\gamma \in S_0} \mathbf{e}_\gamma$ we therefore obtain

$$\rho(\alpha, x)^{-1}\Theta = \sum_{\gamma \in S_0} \chi_D(\alpha)^{-1}\mathbf{e}_{y\gamma} = \chi_D(\alpha)^{-1} \sum_{\gamma \in H} \mathbf{e}_\gamma = \chi_D(\alpha)^{-1} \cdot \Theta$$

because $\gamma \mapsto y\gamma$ is a bijection on S_0 (as $(y, |S_0|) \mid (y, |D|) = 1$ by Corollary 5.6).

Concerning the set $\mathcal{B}_{\Gamma(N)}(n)$: (i) Lift and Hecke operator on $\Gamma_0(N)$ is well defined: as above. Using Theorem 10.1 we directly obtain that the Hecke operators on the scalar-valued modular forms and on the vector-valued modular forms with the very same set $\mathcal{B} := \mathcal{B}_{\Gamma_0(N)}(n)$ are well-defined.

(ii) The $\mathrm{SL}_2(\mathbb{Z})$-inequivalence of the members of $\mathcal{B}$ as they are a subset of an $\mathrm{SL}_2(\mathbb{Z})$-RRS $\mathcal{A}_{\mathrm{SL}_2(\mathbb{Z})}(n)$.

(iii) $\mathcal{B} \sim \mathrm{SL}_2(\mathbb{Z})$ follows directly from Lemma 6.15 as they form an $\mathrm{SL}_2(\mathbb{Z})$-RRS for a single double coset $\Gamma_0(N)J_n\Gamma_0(N)$.

(iv) Completely analogous to the proof of the injectivity in the case of $\mathcal{A}$.

(v) directly follows from $\mathcal{B} \subset \mathcal{A}$. □

11 Vector-valued eigenforms for the Hecke operators

Using the theorems above we may transform some known results on scalar-valued modular forms to the vector-valued case. We will show here that we find nontrivial eigenforms of the Hecke operator $T^{(x)}_{\mathcal{A}_{\Gamma_1(N)}(n)}$ whenever $(n, N) = 1$ and there exists an $x \in \mathbb{Z}$ with $x^2 \equiv n \mod N$. Let $N \in \mathbb{N}$, $d \mid N$ and χ a Dirichlet character modulo N. By $\pi_{N,d}$ we denote the well-defined map $\mathbb{Z}_N \mapsto \mathbb{Z}_d$, $x \mod N \mapsto x \mod d$. If χ_d is a Dirchlet character modulo d, then it induces a Dirichlet character modulo N by setting $\chi := \chi_d \circ \pi_{N,d}$. The conductor of χ is defined to be the minimal $d \in \mathbb{N}$ with $d \mid N$ such that there exists a Dirichlet character χ_d modulo d with $\chi = \chi_d \circ \pi_{N,d}$. χ is called primitive if its conductor is N.

11.1 Notation. *Since we will study Hecke operators in this section it is convenient to rename $T_{\mathcal{A}_{\Gamma_1(N)}(n)}$, the n-th Hecke operators on $\mathrm{MF}_k(\Gamma_1(N))$ as in definition 6.17, to T_n.*

11.2 Theorem. *Let $u, v, N \in \mathbb{N}$ with $uv = N$, ψ a Dirichlet character modulo u, ϕ a primitive Dirichlet character modulo v such that either $k \neq 2$*

or $\psi \neq 1$ *or* $\phi \neq 1$. *Put* $\chi := (\psi \circ \pi_{N,u}) \cdot (\phi \circ \pi_{N,v})$ *then* χ *is a Dirichlet character modulo* N. *For* $\overline{(x,y)} \in \mathbb{Z}_N^2$ *put*

$$G_k^{\overline{(x,y)}}(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ (c,d)\equiv(x,y) \mod N}} \frac{1}{(c\tau+d)^k}$$

then the function

$$\tau \mapsto G_k^{\psi,\phi}(\tau) = \sum_{c=0}^{u-1}\sum_{d=0}^{v-1}\sum_{e=0}^{u-1} \psi(c)\overline{\phi}(d) G_k^{\overline{(cv,d+ev)}}(\tau)$$

is contained in the set $\mathrm{MF}_k(\Gamma_1(N)) \cap \Omega(\Gamma_0(N), \chi)$ *which is nothing else than* $\mathrm{MF}_k(\Gamma, \chi)$ *due to remark 6.5.*

Proof. See [Di], Section 4.5, Page 127. □

In the above theorem, χ evaluated at some matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ is to be read as $\chi(M) := \chi(d)$.

11.3 Theorem. *For* N, ψ, ϕ, χ *as above, put*

$$E_k^{\psi,\phi}(\tau) = \delta(\psi) L(1-k, \phi) + 2\sum_{n=1}^{\infty} \sigma_{k-1}^{\psi,\phi}(n) q^n$$

where $q = e^{2\pi i \tau}$ *and*

$$\sigma_{k-1}^{\psi,\phi}(n) = \sum_{\substack{m\in\mathbb{N} \\ m|n}} \psi(n/m)\phi(m) m^{k-1}$$

is the generalized divisor sum, $\delta(\psi) = 1$ *if* ψ *is the trivial character* $\mathbf{1}$*sending everything to* $1 \in \mathbb{C}$ *and* $\delta(\psi) = 0$ *otherwise and* $L(\cdot, \phi)$ *is the Dirichlet L-function (see [Di], Section 4.4, Page 121). Then, there exists a constant* $c(k, \phi) \in \mathbb{C}$ *such that* $E_k^{\psi,\phi} = c(k,\phi) \cdot G_k^{\psi,\phi}$. *In particular* $E_k^{\psi,\phi} \in \mathrm{MF}_k(\Gamma_0(N), \chi)$ *due to the last theorem.*

Proof. See [Di], Thm. 4.5.1, Page 129. □

For any $t \in \mathbb{N}$ with $tuv \mid N$ and ψ, ϕ as above set $E_k^{\psi,\phi,t}(\tau) = E_k^{\psi,\phi}(t\tau)$. In particular, $E_k^{\psi,\phi,1} = E_k^{\psi,\phi}$, then

11.4 Theorem. *Let $N, \psi, \phi, \chi, u, v, t$ be as above so that χ satisfies the condition of definition 6.17. Let $p \in \mathbb{P}$ with $(p, N) = 1$ then*

$$T_p(E_k^{\psi,\phi,t}) = \underbrace{(\psi(p) + \phi(p)p^{k-1})}_{=:c_{k,\psi,\phi}} E_k^{\psi,\phi,t}$$

in other words: the function $E_k^{\psi,\phi,t}$ is an eigenform for the p-th Hecke operator.

Proof. See [Di], Prop. 5.2.3, Page 173. □

We need one more observation concerning eigenforms of Hecke operators:

11.5 Theorem. *Let $N, \psi, \phi, \chi, u, v, t$ be as above so that χ satisfies the condition of definition 6.17. Let $p \in \mathbb{P}$ with $(p, N) = 1$, $r \in \mathbb{N}, r \geq 2$ and $n, m \in \mathbb{N}$ such that $(n, m) = 1$. The relations*

$$T_{mn} = T_m \circ T_n = T_n \circ T_m \tag{11.1}$$

and

$$T_{p^r} = T_{p^{r-1}} T_p - p T_{p^{r-2}} T_{p,p} \tag{11.2}$$

hold for some operator $T_{p,p} : \mathrm{MF}_k(\Gamma_0(N), \chi) \mapsto \mathrm{MF}_k(\Gamma_0(N), \chi)$ that satisfies $T_{p,p}(f) = p^{k-2}\chi(p)f$ (i.e. it operates as a multiplication with a constant).

Proof. See [Ko], Prop. 32 on Page 156 and Prop. 35 on Page 160. □

11.6 Corollary. *Let $N, \psi, \phi, \chi, u, v, t$ be as above so that χ satisfies the condition of definition 6.17, then for all Hecke operators $T_n := T_{\mathcal{A}_{\Gamma_1(N)}(n)}$ satisfying $(n, N) = 1$ there exists a $\lambda_n \in \mathbb{C}$ such that $T_n(E_k^{\psi,\phi,t}) = \lambda_n E_k^{\psi,\phi,t}$.*

Proof. Write $n = p_1^{e_1} \cdots p_r^{e_r}$. By a simple induction using equation (11.2), Theorem 11.4 and $E_k^{\psi,\phi,t} \in \mathrm{MF}_k(\Gamma_0(N), \chi)$, one shows that $E_k^{\psi,\phi,t}$ is an eigenform for every $T_{p_j^{e_j}}$, i.e. there are $\lambda_j \in \mathbb{C}$ with $T_{p_j^{e_j}}(E_k^{\psi,\phi,t}) = \lambda_j E_k^{\psi,\phi,t}$. Further, by (11.1),

$$T_n(E_k^{\psi,\phi,t}) = T_{p_1^{e_1}} \circ \ldots \circ T_{p_r^{e_r}}(E_k^{\psi,\phi,t}) = \lambda_1 \cdot \ldots \cdot \lambda_r E_k^{\psi,\phi,t}$$

□

Let D be a discriminant-quadratic form of even signature and $L(D) \mid N$. Consider the character χ_D. Assume for a moment that

- N is squarefree (i.e. $N = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$ for primes $p_1, ..., p_r$ and $e_i = 1$ for all i).
- χ_D is primitive.
- $k \in \mathbb{Z}$ is an arbitrary integer such that $\chi_D(-1) = (-1)^k$.

We put $\psi := \mathbf{1}$ which is a character modulo $u = 1$ and $\phi = \chi_D$ which is a (primitive!) character modulo $v = N$. Therefore we obtain an Eisenstein series $E_k := E_k^{\mathbf{1},\chi_D,1} \in \mathrm{MF}_k(\Gamma_0(N), \chi_D) \subset \mathrm{MF}_k(\Gamma_1(N))$, i.e. we want to view E_k as modular form for $\Gamma_1(N)$ without a character. Let $S_0 := \{\mathbf{e}_{0+L}\}$ then S_0 is an isotropic subgroup of D so that the lift $\mathcal{L}_{S_0}$ as in Theorem 6.8(b) is senseful. Let $n \in \mathbb{N}$ be such that $(n, N) = 1$ and $x^2 \equiv n \mod N$ for some $x \in \mathbb{Z}$. By Corollary 11.6, we obtain $\lambda_n \in \mathbb{C}$ such that $T_n(E_k) = \lambda_n E_k$. Let $T_n^{(x)} := T^{(x)}_{\mathcal{A}_{\Gamma_1(N)}(n)}$ denote the n-th Hecke operator on vector-valued modular forms for the Weil representation as in definition 6.19. By Theorem 9.2 it follows that

$$T_n^{(x)} \circ \mathcal{L}_{S_0}(E_k) = \mathcal{L}_{S_0} \circ T_n(E_k) = \lambda_n \mathcal{L}_{S_0}(E_k)$$

in other words, the lifted Eisenstein series $\mathcal{L}_{S_0}(E_k)$ is either an eigenform for all the above Hecke operators or it is the zero function. Of course we want to see that $\mathcal{L}_{S_0}(E_k)$ is not the zero function. For a Dirichlet character χ modulo N put $E_{k,\chi} := 1/L(k,\chi) \sum_{d \mod N} \chi(d) G_k^{\overline{(0,d)}}$ where $d \mod N$ means that d runs through an arbitrary set of representatives modulo N (we could write $d \in \{0, 1, ..., N-1\}$ for example) and $L(\cdot,\cdot)$ is the L-series $L(k,\chi) = \sum_{n \in \mathbb{N}} \chi(n)/n^k$. Scheithauer has computed the Fourier expansion of $\mathcal{L}_{\{\mathbf{e}_0\}}(E_{k,\chi}) = \mathcal{L}_{S_0}(E_{k,\chi})$ to be unequal to zero in this case (cf. [Sch III], Thm. 7.2), in particular, it is not the zero function on $\mathbb{C}[D]$! We compute

$$\begin{aligned} E_k = E_k^{\mathbf{1},\chi_D,1} &= \sum_{c=0}^{u-1} \sum_{d=0}^{v-1} \sum_{e=0}^{u-1} \mathbf{1}(c) \overline{\chi_D}(d) G_k^{\overline{(cv, d+ev)}} \\ &= \sum_{d=0}^{N-1} \chi_D(d) G_k^{\overline{(0v, d+0v)}} = E_{k,\chi_D} \end{aligned}$$

and finally obtain that $\mathcal{L}_{S_0}(E_{k,\chi}) = \mathcal{L}_{S_0}(E_k)$ transforms as an eigenform under all Hecke operators $T_n^{(x)}$ as above and is unequal to zero, hence, it is an eigenform for all those Hecke operators. One can show that χ_D is primitive if, for example, $|D|$ is composed of primes that occur only with odd exponent, i.e. $|D| = p_1^{e_1} \cdot ... \cdot p_r^{e_r}$ for some primes p_i such that e_i is odd

for all i (cf. [Sch III], the remark on the conductor of χ on p. 11, note that since N is squarefree, χ_D reduces to $(\frac{\cdot}{|D|})$ and all the primes dividing $|D|$ do also divide N). The last two assertions can be shown with the results in Section 5.

References

[Al] $\mathrm{SL}_2(\mathbb{Z}) = \langle s, u \mid s^4 = id, s^2 = u^3 \rangle$
http://happy-werner.de/uni/sonstiges/sl2Z.pdf

[Bo] Richard Borcherds Reflection groups of Lorentzian lattices, Duke Math. J. 104 (2000) no. 2, 319 - 366. See http://math.berkeley.edu/ reb/papers/reflor/reflor.pdf

[Br] Jan Bruinier, Oliver Stein, The Weil representation and Hecke operators for vector-valued modular forms, Mathematische Zeitschrift 264 (2010), 249 - 270.
http://www.mathematik.tu-darmstadt.de/fbereiche
/AlgGeoFA/staff/bruinier/publications/weil5.pdf

[Ca] John Cassels Rational Quadratic Forms, Dover Publications, 2008.

[CS] John Conway, Neil Sloane, Sphere packings, lattices and groups. Springer, 1988.

[Di] Fred Diamond, Jerry Shurman, A first course in modular forms, Springer, 2007.

[Fi] Gerd Fischer, Lineare Algebra, Vieweg, 2005.

[Ga] Carl Gauss Disquisitiones Arithmeticae, Art. 103, see http://happy-werner.de/uni/sonstiges/GaussArt103.pdf

[Ge] Larry Gerstein, Basic Quadratic Forms

[JS] Jens Jantzen, Joachim Schwermer, Algebra, Springer.

[Ko] Neal Koblitz, Introduction to Elliptic Curves and Modular Forms. Springer.

[McG] William McGraw, The rationality of vector-valued modular forms associated with the Weil representation, Math. Ann. 326 (2003), 105 - 122.

[Mi] Toshitsune Miyake, Modular Forms, Springer, 2006.

[Mil] John Milnor, Symmetric bilinear forms, Springer, 1973.

[Ni] Viacheslav Nikulin, Integral symmetric bilinear forms and some of their applications, Math. USSR Izv. 14 (1979), 103...167.

[Ra] Robert Rankin, Modular forms and functions Cambridge University Press, 1977.

[Sch] Nils Scheithauer, The Weil representation of $SL_2(\mathbb{Z})$ and some applications, Int. Math. Res. Not. 2009, no. 8, 1488-1545. http://www.mathematik.tu-darmstadt.de/∼scheithauer/papers/weil.pdf

[Sch II] Nils Scheithauer, Some constructions of modular forms for the Weil representation of $SL_2(\mathbb{Z})$, preprint. http://www3.mathematik.tu-darmstadt.de/fileadmin/home/users/174/modularforms.pdf

[Sch III] Nils Scheithauer, On the classification of automorphic products and generalized Kac-Moody algebras, Invent. Math. 164 (2006), 641 - 678. http://www.mathematik.tu-darmstadt.de/∼scheithauer/papers/classification.pdf

[Str] Fredrik Stroemberg, On the Weil representation for finite quadratic modules, http://www3.mathematik.tu-darmstadt.de/fileadmin/home/users/149/fqm_weil_representation_02.pdf

[Wa] Charles Wall, Quadratic forms on finite groups and related topics, Topology 2 (1963), 281 - 298.

[We] André Weil, Sur certains groupes d opérateurs unitaires, Acta Math. 111 (1964), 143 Ű 211

[Wer] Fabian Werner, Rings of modular forms. Bachelor thesis, 2010, http://happy-werner.de/uni/Mathe_BSc/MainDocument.pdf.

[Wer II] Fabian Werner, The Weil representation is a representation, http://happy-werner.de/uni/sonstiges/WeilIsRepr.pdf

[Wer III] Fabian Werner, A PROOF FOR THE ODDITY FORMULA, http://happy-werner.de/uni/sonstiges/oddityFormula.pdf

[Wer IV] http://happy-werner.de/uni/sonstiges/miniConway_complete.pdf