Chapter 4
Automorphic Forms and Hecke Operators

4.1 Lattices and Class Sets of $\mathbb{Z}$-groups

Let P be the set of prime numbers. Set $\widehat{\mathbb{Z}} = \prod_{p\in \mathrm{P}} \mathbb{Z}_p$, and let $\mathbb{A}_f = \mathbb{Q}\otimes\widehat{\mathbb{Z}}$ be the set of finite adeles of $\mathbb{Q}$. Fix a $\mathbb{Z}$-group G, that is, an affine group scheme of finite type over $\mathbb{Z}$. The group $G(\mathbb{A}_f)$ can be canonically identified with the subgroup of $\prod_{p\in \mathrm{P}} G(\mathbb{Q}_p)$ whose elements (g_p) satisfy $g_p \in G(\mathbb{Z}_p)$ for *almost all* p, in other words, for all $p \in \mathrm{P}$ except possibly a finite number. The groups $G(\mathbb{Q})$ and $G(\widehat{\mathbb{Z}})$ embed naturally into $G(\mathbb{A}_f)$ and satisfy $G(\widehat{\mathbb{Z}}) = \prod_{p\in \mathrm{P}} G(\mathbb{Z}_p)$ and $G(\mathbb{Z}) = G(\mathbb{Q}) \cap G(\widehat{\mathbb{Z}})$. The $G(\mathbb{A}_f)$-set

$$\mathcal{R}(G) = G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$$

will play an important role in this chapter. We denote it by $\mathcal{R}$, for the French word for lattice, "réseau", because it can, in general, be identified with the set of lattices of a certain type in a $\mathbb{Q}$-vector space.

A classical result of Borel [32, Sect. 5] asserts that the *class set of* G:

$$\mathrm{Cl}(G) = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}}) = G(\mathbb{Q})\backslash\mathcal{R}(G)$$

is finite. Its cardinality $\mathrm{h}(G) = |\mathrm{Cl}(G)|$ is called the *class number* of G. In this section, we describe $\mathcal{R}(G)$ and $\mathrm{Cl}(G)$ in several standard cases we are interested in (see, for example, [32, Sect. 2]).

4.1.1 Linear Groups

Let us begin with the case of GL_n. If V is a vector space of finite dimension n over the field of fractions of a principal ideal domain A, we denote by $\mathcal{R}_A(V)$ the set of

G. Chenevier, J. Lannes, *Automorphic Forms and Even Unimodular Lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 69, https://doi.org/10.1007/978-3-319-95891-0_4

lattices in V with respect to A, that is, the set of free sub-A-modules of V of rank n (Sect. 2.1). It is endowed with a transitive action of $\mathrm{GL}(V)$; the stabilizer of L in $\mathcal{R}_A(V)$ is $\mathrm{GL}(L)$.

Let V be a $\mathbb{Q}$-vector space of dimension n. If p is prime and we set $V_p = V \otimes \mathbb{Q}_p$, then there is a natural map $\mathcal{R}_{\mathbb{Z}}(V) \to \mathcal{R}_{\mathbb{Z}_p}(V_p)$ defined by $M \mapsto M_p := M \otimes \mathbb{Z}_p$. We fix $L \in \mathcal{R}_{\mathbb{Z}}(V)$ and set $G = \mathrm{GL}_L$. We easily verify, following Eichler [78, Sect. 13], that the map

$$\mathcal{R}_{\mathbb{Z}}(V) \to \prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p) \ , \quad M \mapsto (M_p) \ , \tag{4.1.1}$$

is an injection from $\mathcal{R}_{\mathbb{Z}}(V)$ to the subset $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p) \subset \prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ consisting of the families (M_p) such that $M_p = L_p$ for almost all p (this subset does not depend on the choice of L). The natural action of $G(\mathbb{A}_f)$ on $\prod_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ preserves $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$, and it is transitive on the latter. Therefore, if we identify $\mathcal{R}_{\mathbb{Z}}(V)$ with $\prod'_{p \in \mathrm{P}} \mathcal{R}_{\mathbb{Z}_p}(V_p)$ using the map (4.1.1), which we will do systematically from now on, then by transport of structure, we obtain a transitive action of $G(\mathbb{A}_f)$ on $\mathcal{R}_{\mathbb{Z}}(V)$ that extends the obvious action of $G(\mathbb{Q}) = \mathrm{GL}(V)$. Since the stabilizer of the lattice L is $G(\widehat{\mathbb{Z}})$, this leads to an isomorphism of $G(\mathbb{A}_f)$-sets

$$\mathcal{R}(G) \xrightarrow{\sim} \mathcal{R}_{\mathbb{Z}}(V).$$

Since $G(\mathbb{Q})$ also acts transitively on $\mathcal{R}_{\mathbb{Z}}(V)$, it follows, in particular, that we have

$$\mathrm{h}(\mathrm{GL}_n) = 1 \ .$$

In the case $G = \mathrm{PGL}_L$ (resp. $G = \mathrm{SL}_L$), the set $\mathcal{R}(G)$ can also be viewed as the quotient of $\mathcal{R}_{\mathbb{Z}}(V)$ by $\mathbb{Q}^\times$ for the action by homotheties (resp. as the subset of $\mathcal{R}_{\mathbb{Z}}(V)$ consisting of the M that have a $\mathbb{Z}$-basis of determinant 1 with respect to a $\mathbb{Z}$-basis of L). We again have $\mathrm{h}(\mathrm{PGL}_n) = \mathrm{h}(\mathrm{SL}_n) = 1$.

4.1.2 Orthogonal and Symplectic Groups

We now assume that the $\mathbb{Q}$-vector space V is endowed with a nondegenerate bilinear form φ that is symmetric or alternating. Let $L \in \mathcal{R}_{\mathbb{Z}}(V)$. Recall that the *dual lattice* of L is the lattice $L^\sharp \in \mathcal{R}_{\mathbb{Z}}(V)$ defined by (Sect. 2.1)

$$L^\sharp = \{v \in V \, ; \, \varphi(v, x) \in \mathbb{Z} \ \ \forall x \in L\} \ .$$

We call L *homodual*, for "homothetic to its dual," if there exists a $\lambda \in \mathbb{Q}^\times$ such that we have $L^\sharp = \lambda L$; there then exists a unique strictly positive λ with this property; we denote it by λ_L. The lattice L is called *self-dual* if we have $L^\sharp = L$. If L is homodual and φ is symmetric (resp. alternating), then the bilinear form $\lambda_L \varphi$ gives L the structure of a b-module (resp. a-module) over $\mathbb{Z}$ in the sense of Sect. 2.1. We

then say that L is *even* if $\lambda_L\varphi(x,x) \in 2\mathbb{Z}$ for every $x \in L$. This is automatic if φ is alternating, and if φ is symmetric, this allows us to view L as a q-module over $\mathbb{Z}$ by setting $\mathrm{q}(x) = \lambda_L\ \varphi(x,x)/2$ for $x \in L$. We denote by

$$\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \subset \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$$

the subsets of $\mathcal{R}_{\mathbb{Z}}(V)$ consisting of the even self-dual (resp. homodual) lattices.

Set $n = \dim V$, and fix $L \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$. By reduction modulo 2, the existence of such an L induces the congruence $n \equiv 0 \bmod 2$. Consider the sub-$\mathbb{Z}$-group $G \subset \mathrm{GL}_L$ defined by

$$G = \begin{cases} \mathrm{Sp}_L & \text{if } \varphi \text{ is alternating,} \\ \mathrm{O}_L & \text{else.} \end{cases}$$

We denote by $\widetilde{G}$ the corresponding similitude $\mathbb{Z}$-group, so that we have $G \subset \widetilde{G} \subset \mathrm{GL}_L$, and by $\mathrm{P}\widetilde{G}$ the *projective similitude* $\mathbb{Z}$-group, which is the quotient of $\widetilde{G}$ by its central sub-$\mathbb{Z}$-group isomorphic to $\mathbb{G}_m$ consisting of the homotheties (Sect. 2.1).

Lemma 4.1.3. *The restriction of the action of* $\mathrm{GL}_L(\mathbb{A}_f)$ *on* $\mathcal{R}_{\mathbb{Z}}(V)$ *to* $\widetilde{G}(\mathbb{A}_f)$ *(resp.* $G(\mathbb{A}_f)$*) preserves* $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ *(resp.* $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$*).*

Before giving the proof, let us introduce the local analogs of the previous definitions. Let p be prime. For $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$, the dual lattice $M^\sharp \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$ (with respect to $\mathbb{Z}_p$; see Sect. 2.1) is well defined. We denote by $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) \subset \mathcal{R}_{\mathbb{Z}_p}(V_p)$ the subset of lattices M such that there exists $\lambda \in \mathbb{Q}_p^\times$ with $M^\sharp = \lambda M$ and $\lambda\varphi(x,x) \in 2\mathbb{Z}_p$ for every $x \in M$. Furthermore, we denote by $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p) \subset \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ the subset of lattices M such that we have $M^\sharp = M$. For $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$, there exists a unique $\lambda_M \in p^{\mathbb{Z}}$ with $M^\sharp = \lambda_M M$. If φ is symmetric (resp. alternating), the quadratic form $x \mapsto \lambda_M\,\varphi(x,x)/2$ (resp. the alternating form $\lambda_M\varphi$) then gives M the structure of a q-module (resp. a-module) over $\mathbb{Z}_p$.

Proof. Let $M \in \mathcal{R}_{\mathbb{Z}}(V)$. We begin by noting that M is in $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ if and only if M_p is in $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ for every prime p, in which case we, moreover, have $\lambda_M = \prod_p \lambda_{M_p}$ (of course, λ_{M_p} is 1 for almost all p). Indeed, this follows from the identity $\mathbb{A}_f^\times = \mathbb{Q}^\times \cdot \widehat{\mathbb{Z}}^\times$ (that is, $\mathrm{h}(\mathbb{G}_m) = 1$) and the immediate relation $(N^\sharp)_p = (N_p)^\sharp$, which holds for every prime p and every $N \in \mathcal{R}_{\mathbb{Z}}(V)$. In particular, we have $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ if and only if we have $M_p \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p)$ for every p.

To conclude the proof, it suffices to note that if $g \in \widetilde{G}(\mathbb{Q}_p)$ has similitude factor $\nu(g)$ (Sect. 2.1) and we have $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$, then we have the relation $g(M)^\sharp = \nu(g)^{-1} g(M^\sharp)$. □

Note that the action of the homotheties $\mathbb{Q}^\times$ on $\mathcal{R}_{\mathbb{Z}}(V)$ preserves $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$. By Lemma 4.1.3, the quotient set

$$\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) := \mathbb{Q}^\times \backslash \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$$

is therefore endowed with an action of $\mathrm{P}\widetilde{G}(\mathbb{A}_f)$ that extends the obvious action of $\mathrm{P}\widetilde{G}(\mathbb{Q})$. We denote the homothety class of $M \in \mathcal{R}_{\mathbb{Z}}(V)$ by $\underline{M}$. In summary, we have the following commutative diagram:

$$\begin{array}{ccccc}
\mathcal{R}(G) & \hookrightarrow & \mathcal{R}(\widetilde{G}) & \twoheadrightarrow & \mathcal{R}(\mathrm{P}\widetilde{G}) \\
\downarrow{\scriptstyle \omega_1} & & \downarrow{\scriptstyle \omega_2} & & \downarrow{\scriptstyle \omega_3} \\
\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) & \hookrightarrow & \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) & \twoheadrightarrow & \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V) \\
\downarrow & & \downarrow & & \downarrow \\
G(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) & \xrightarrow{\xi_1} & \widetilde{G}(\mathbb{Q})\backslash\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V) & \xrightarrow{\xi_2} & \mathrm{P}\widetilde{G}(\mathbb{Q})\backslash\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V)\ .
\end{array}$$

The ω_i, for $i = 1, 2, 3$, are, respectively, the "orbit" maps of L, L, and $\underline{L}$ under the actions of $G(\mathbb{A}_f)$, $\widetilde{G}(\mathbb{A}_f)$, and $\mathrm{P}\widetilde{G}(\mathbb{A}_f)$. All other arrows denote canonical maps.

Proposition 4.1.4. *The maps ω_i and ξ_j are bijective. In particular, the action of $G(\mathbb{A}_f)$ on $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ is transitive; the orbit of L defines an isomorphism of $G(\mathbb{A}_f)$-sets $\mathcal{R}(G) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$.*

Proof. The injectivity of the ω_i is obvious. Let us begin by verifying the last assertion, which is nothing more than the surjectivity of ω_1. If φ is symmetric, Scholium 2.2.5 asserts that for every $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, the q-module M_p over $\mathbb{Z}_p$ is hyperbolic. It is, in particular, isomorphic to L_p, which concludes the proof of the last assertion because every isometry $L_p \to M_p$ is necessarily induced by an element of $\mathrm{O}(V_p) = G(\mathbb{Q}_p)$. Let us therefore suppose that φ is alternating. It is well known that if A is a principal ideal domain, there exists, up to equivalence, a unique nondegenerate alternating bilinear form on the A-module A^n (n even). We conclude by considering the case $A = \mathbb{Z}_p$.

The surjectivity of ω_3 (resp. ω_2) follows from that of ω_2 (resp. from those of ω_1 and ξ_1). Let us show the surjectivity of ξ_1. For $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$ and $g \in \widetilde{G}(\mathbb{Q})$ with similitude factor $\nu(g)$, we have $\lambda_{g(M)} = \pm\,\nu(g)^{-1}\,\lambda_M$. It therefore suffices to see that $\nu(\widetilde{G}(\mathbb{Q}))$ contains the set $\mathbb{Q}_{>0}$ of strictly positive rational numbers. This is obvious in the alternating case and, more generally, when V is hyperbolic. In the symmetric case, we must show that for $\lambda \in \mathbb{Q}_{>0}$, the vector spaces V and $V \otimes \langle\lambda\rangle$ (obtained by multiplying the quadratic form on V by λ) are isomorphic as q-vector spaces over $\mathbb{Q}$. But they are so over $\mathbb{Q}_p$ for every prime p because the $V \otimes \mathbb{Q}_p$ are hyperbolic by Scholium 2.2.5, and they are so over $\mathbb{R}$ because we have $\lambda > 0$. We conclude using the Hasse–Minkowski theorem.

The map ξ_2 is bijective because of the equality $\mathrm{P}\widetilde{G}(\mathbb{Q}) = \widetilde{G}(\mathbb{Q})/\mathbb{Q}^{\times}$. Finally, let us verify the injectivity of ξ_1. We may assume that φ is symmetric because the argument given in the first paragraph shows that we have $h(G) = 1$ if φ is alternating. Let us therefore assume that there exist $M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ and $g \in \widetilde{G}(\mathbb{Q})$ such that $g(M) = L$. We then have $\nu(g) = \pm 1$. If $\nu(g) = 1$, then we have $g \in G(\mathbb{Q})$, and we are done. Otherwise, M is isometric to the q-module $L \otimes \langle -1\rangle$, which

has underlying space L but opposite quadratic form. This implies that $V \otimes \mathbb{R}$ is hyperbolic, and thus that L and M are isomorphic by Theorem 2.2.7. □

Corollary 4.1.5. *We have* $\mathrm{h}(G) = \mathrm{h}(\widetilde{G}) = \mathrm{h}(\mathrm{P}\widetilde{G})$.

When φ is alternating, the classification given above of the nondegenerate alternating forms applied to the ring $\mathbb{Z}$ implies[1] $\mathrm{h}(G) = 1$, and therefore $\mathrm{h}(\mathrm{Sp}_{2g}) = \mathrm{h}(\mathrm{GSp}_{2g}) = \mathrm{h}(\mathrm{PGSp}_{2g}) = 1$ for every $g \geq 1$.

Let us assume that φ is symmetric. If the q-vector space $L \otimes \mathbb{R}$ is indefinite, then Theorem 2.2.7 implies $\mathrm{h}(\mathrm{O}_L) = 1$. The situation is quite different if $L \otimes \mathbb{R}$ is positive definite, which we will assume from now on. Recall that L can then be viewed as an even unimodular lattice in the Euclidean space $V \otimes \mathbb{R}$ of dimension n. In particular, we have $n \equiv 0 \bmod 8$. In this case, $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ is, by definition, the set of even unimodular lattices in $V \otimes \mathbb{R}$ that are contained in $L \otimes \mathbb{Q}$. Recall that X_n denotes the set of isometry classes of even unimodular lattices in the Euclidean space $V \otimes \mathbb{R}$. By Scholium 2.2.1, the natural inclusion $\mathrm{O}(V)\backslash\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \to \mathrm{X}_n$ is bijective and therefore induces an isomorphism $\mathrm{Cl}(\mathrm{O}_L) \xrightarrow{\sim} \mathrm{X}_n$. In particular, if O_n denotes the orthogonal $\mathbb{Z}$-group of the lattice $L = \mathrm{E}_n$ (Sect. 1.3), we obtain the equality

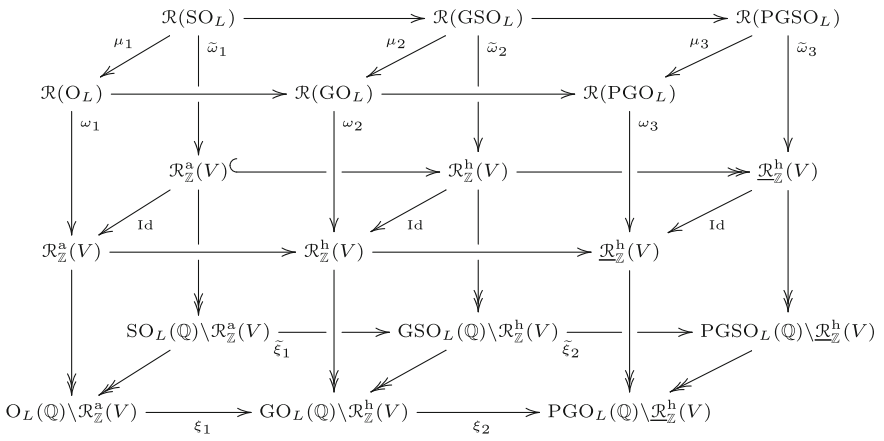
$$\mathrm{h}(\mathrm{O}_n) = |\mathrm{X}_n| \,,$$

which shows that $\mathrm{h}(\mathrm{O}_n)$ is a quite interesting number.

4.1.6 SO_L *Versus* O_L

We continue the analysis of the previous subsection by assuming that φ is symmetric, so that G, $\widetilde{G}$, and $\mathrm{P}\widetilde{G}$ are, respectively, O_L, GO_L, and PGO_L. We are interested in their respective sub-$\mathbb{Z}$-groups SO_L, GSO_L, and PGSO_L (Sect. 2.1). The groups $\mathrm{SO}_L(\mathbb{A}_f)$, $\mathrm{GSO}_L(\mathbb{A}_f)$, and $\mathrm{PGSO}_L(\mathbb{A}_f)$ act on, respectively, $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$, and $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V)$ (Proposition 4.1.3). Let us consider the following commutative diagram, which extends that of Sect. 4.1.2:

[1] The assertions $\mathrm{h}(\mathrm{SL}_n) = \mathrm{h}(\mathrm{Sp}_{2g}) = 1$ recalled above are also very particular cases of Kneser's strong approximation theorem (see [123], [162, Theorem 7.12]). It asserts that we have $\mathrm{h}(G) = 1$ whenever the $\mathbb{C}$-group $G_{\mathbb{C}}$ is semisimple and simply connected and the topological group $G(\mathbb{R})$ does not have a nontrivial connected, compact, normal subgroup.



The vertical maps $\widetilde{\omega}_i$ are again the "orbit" maps of L (resp. L, resp. $\underline{L}$), and the other arrows are the canonical maps.

Proposition 4.1.7. *The maps $\widetilde{\omega}_i$, μ_i, and $\widetilde{\xi}_j$ are bijective. In particular, the action of $\mathrm{SO}_L(\mathbb{A}_f)$ on $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ is again transitive; the orbit of L defines an isomorphism $\mathcal{R}(\mathrm{SO}_L) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$.*

Proof. We have already seen that the natural action of $\mathrm{O}_L(\mathbb{A}_f)$ on $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ is transitive (Proposition 4.1.4). The same holds for the restriction of this action to its subgroup $\mathrm{SO}_L(\mathbb{A}_f)$ because the orthogonal group of a nontrivial hyperbolic q-module over $\mathbb{Z}_p$ always has an element of determinant -1. The same reasoning shows that the μ_i are bijective because $\mathrm{O}_L(\mathbb{Z}_p)/\mathrm{SO}_L(\mathbb{Z}_p) \to \mathrm{GO}_L(\mathbb{Q}_p)/\mathrm{GSO}_L(\mathbb{Q}_p)$ is bijective for every prime p (Sect. 2.1). Since the ω_i are bijective, the bijectivity of the $\widetilde{\omega}_i$ follows.

The bijectivity of $\widetilde{\xi}_2$ is obvious. The surjectivity of $\widetilde{\xi}_1$ follows from that of ξ_1 and from the fact that we have $-1 \in \det(\mathrm{O}(V))$. Finally, the injectivity of $\widetilde{\xi}_1$ can be shown similarly to that of ξ_1 (Proposition 4.1.4), using that we have $-1 \in \det(\mathrm{O}(\mathrm{H}(\mathbb{Z}^{n/2})))$. □

Corollary 4.1.8. *If L is a* q*-module over $\mathbb{Z}$, we have $\mathrm{h}(\mathrm{SO}_L) = \mathrm{h}(\mathrm{GSO}_L) = \mathrm{h}(\mathrm{PGSO}_L)$. If, moreover, $L \otimes \mathbb{R}$ is indefinite, then these integers are equal to* 1.

Proof. The first assertion follows from the bijectivity of the maps ξ_i (Proposition 4.1.7). When $L \otimes \mathbb{R}$ is indefinite, we already explained the equality $\mathrm{h}(\mathrm{O}_L) = 1$ in Sect. 4.1.2. It remains to show that there exists an $s \in \mathrm{O}(L)$ with $\det s = -1$. The assumption on L and Theorem 2.2.7 show that there exists a q-module L' over $\mathbb{Z}$ such that $L \simeq L' \oplus \mathrm{H}(\mathbb{Z})$ (orthogonal sum). This concludes the proof because $\mathrm{H}(\mathbb{Z})$ contains an automorphism of determinant -1. □

Finally, let us assume that L is positive definite. As before, we then have a canonical bijection $\mathrm{Cl}(\mathrm{SO}_L) \xrightarrow{\sim} \widetilde{\mathrm{X}}_n$, where $\widetilde{\mathrm{X}}_n$ denotes the set of *direct* isometry classes of even unimodular lattices in $V \otimes \mathbb{R}$ (in other words, the set of orbits of the action of $\mathrm{SO}(V \otimes \mathbb{R})$ on the latter). The isometry class of an even unimodular

lattice $M \subset V \otimes \mathbb{R}$ admits exactly one or two inverse images under the canonical projection

$$\widetilde{\mathrm{X}}_n \to \mathrm{X}_n\,,$$

depending on whether $\mathrm{O}(M)$ has an element of determinant -1 or not. It has one if, for example, M has at least one root, that is, an $\alpha \in M$ such that $\alpha \cdot \alpha = 2$, because the associated orthogonal reflection is in $\mathrm{O}(M)$ (Sect. 2.3). On the other hand, if M is the Leech lattice, then we have $\mathrm{O}(M) = \mathrm{SO}(M)$ by Conway [65]. The results recalled in Sect. 2.3 imply the following corollary. For $n \equiv 0 \bmod 8$, we set $\mathrm{SO}_n = \mathrm{SO}_{\mathrm{E}_n}$.

Corollary 4.1.9. *We have* $\mathrm{h}(\mathrm{SO}_8) = 1$, $\mathrm{h}(\mathrm{SO}_{16}) = 2$, *and* $\mathrm{h}(\mathrm{SO}_{24}) = 25$.

4.1.10 Orthogonal Groups in Odd Dimensions

We return to the setting of Sect. 4.1.2, where we assume that φ is symmetric. We now consider the set

$$\mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V) \subset \mathcal{R}_{\mathbb{Z}}(V)$$

consisting of the $L \in \mathcal{R}_{\mathbb{Z}}(V)$ with $\varphi(x,x) \in 2\mathbb{Z}$ for every $x \in L$ and $L^\sharp/L \simeq \mathbb{Z}/2\mathbb{Z}$. This last condition is equivalent to requiring that $\varphi_{|L\times L}$ have determinant ± 2. We refer to Appendix B for an analysis of these lattices.

We fix $L \in \mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$, which requires the dimension n of V to be odd. Then $\mathrm{SO}_L(\mathbb{A}_f)$ acts transitively on $\mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$ by Proposition B.2.5, and the stabilizer of L is $\mathrm{SO}_L(\widehat{\mathbb{Z}})$. If $L \otimes \mathbb{R}$ is indefinite, the number of classes of SO_L is 1; this is a classical result that would not be difficult to deduce from Proposition B.2.5 (iii) and Theorem 2.2.7. The situation is more interesting when $L \otimes \mathbb{R}$ is definite, say positive definite to fix the ideas; we will assume that this is the case from now on.

In this case, we have the congruence $n \equiv \pm 1 \bmod 8$ and $\mathrm{Cl}(\mathrm{SO}_L)$ can be identified with the set of isometry classes of even lattices of determinant 2 in $\mathbb{R}^n$ (Sect. B.2). Here, we do not need to distinguish between direct and indirect isometries because $x \mapsto -x$ is in $\mathrm{O}(M)$ and has determinant -1 for every $M \in \mathcal{R}^{\mathrm{b}}_{\mathbb{Z}}(V)$. If $n \equiv 1 \bmod 8$, we set $\mathrm{L}_n = \mathrm{E}_{n-1} \oplus \mathrm{A}_1$. If $n \equiv -1 \bmod 8$, we denote by L_n the orthogonal complement of an arbitrary root of E_{n+1}; since these roots are permuted transitively by the orthogonal group of E_{n+1}, the isometry class of such a lattice does not depend on any choice we make. If $n \equiv \pm 1 \bmod 8$, the lattice L_n is therefore even of determinant 2 (Sect. B.2), and we set $\mathrm{SO}_n = \mathrm{SO}_{\mathrm{L}_n}$ (Sect. B.1).

The known values of $\mathrm{h}(\mathrm{SO}_n)$ with n odd are gathered in the following corollary (see also [68]). The cases $n \le 23$ are treated, for example, in Appendix B, Sect. B.2; the case $n = 25$ is due to Borcherds [29, Table -2].

Corollary 4.1.11. *We have* $\mathrm{h}(\mathrm{SO}_1) = \mathrm{h}(\mathrm{SO}_7) = \mathrm{h}(\mathrm{SO}_9) = 1$, $\mathrm{h}(\mathrm{SO}_{15}) = 2$, $\mathrm{h}(\mathrm{SO}_{17}) = 4$, $\mathrm{h}(\mathrm{SO}_{23}) = 32$, *and* $\mathrm{h}(\mathrm{SO}_{25}) = 121$.

4.2 Hecke Correspondences

4.2.1 General Formalism

Let Γ be an (abstract) group, and let X be a transitive Γ-set. The ring of *Hecke correspondences* (*or operators*) of X is the ring

$$\mathrm{H}(X) = \mathrm{End}_{\mathbb{Z}[\Gamma]}(\mathbb{Z}[X]) \ .$$

With each $T \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$ is associated a matrix $(T_{x,y})_{(x,y)\in X\times X}$ that determines it uniquely; the matrix is defined by the formula

$$\forall y \in X \ , \quad T(y) = \sum_{x\in X} T_{x,y}\ x \ .$$

By definition, such an element T is in the ring $\mathrm{H}(X)$ if and only if the function $X \times X \to \mathbb{Z}$ given by $(x, y) \mapsto T_{x,y}$ is constant on the orbits of the group Γ acting diagonally on $X \times X$. The resulting function $\Gamma\backslash(X \times X) \to \mathbb{Z}$ then has finite support, by the finiteness of $\{x \in X\,;\, T_{x,y} \neq 0\}$ for $y \in X$ and by the transitivity of X. We therefore have an injective map

$$\mathrm{H}(X) \to \mathrm{Hom}_{\mathrm{fs}}(\Gamma\backslash(X \times X), \mathbb{Z}) \ , \quad T \mapsto ((x, y) \mapsto T_{x,y}) \ , \tag{4.2.1}$$

where $\mathrm{Hom}_{\mathrm{fs}}(Y, \mathbb{Z})$ denotes the abelian group of functions with finite support on the set Y and values in $\mathbb{Z}$.

For $x \in X$, we denote the stabilizer of x by $\Gamma_x \subset \Gamma$. We assume that the following properties hold:

(i) For every orbit Ω of Γ in $X \times X$ and every $x \in X$, the intersection $\Omega \cap (X \times \{x\})$ is finite.
(ii) For every $x \in X$, the orbits of Γ_x on X are finite. In other words, for every $x, y \in X$, the intersection $\Gamma_x \cap \Gamma_y$ has finite index in Γ_x.

These conditions ensure that the map (4.2.1) is bijective. In particular, $\mathrm{H}(X)$ is a free $\mathbb{Z}$-module with natural basis the characteristic functions of the orbits of Γ on $X \times X$.

Fix $x \in X$. The transitivity of X ensures that the map $\Gamma \to X \times X$ given by $\gamma \mapsto (\gamma(x), x)$ induces bijections

$$\Gamma_x\backslash\Gamma/\Gamma_x \xrightarrow{\sim} \Gamma_x\backslash(X \times \{x\}) \xrightarrow{\sim} \Gamma\backslash(X \times X) \ . \tag{4.2.2}$$

In particular, this identifies $\mathrm{H}(X)$ with $\mathrm{Hom}_{\mathrm{fs}}(\Gamma_x\backslash\Gamma/\Gamma_x, \mathbb{Z})$. By transport of structure, the latter inherits a ring structure from $\mathrm{H}(X)$: we recover the more standard presentations of the Hecke rings, such as those in [174], [188, Sect. 3], [48], [88, Kap. IV], or [97]. Note that depending on the reference, the ring structure considered on $\mathrm{Hom}_{\mathrm{fs}}(\Gamma_x\backslash\Gamma/\Gamma_x, \mathbb{Z})$ (defined, in general, by an explicit convolution product) may differ slightly from ours; this is, in particular, the case in the articles of Cartier and

Gross, to which we refer in Sect. 6.2, in which the ring $\mathrm{H}(X)$ is exactly the opposite of ours.

Since the second formulation of condition (ii) is symmetric in x, y, condition (i) is also equivalent to requiring that for every orbit Ω of Γ in $X \times X$ and every $x \in X$, the intersection $\Omega \cap (\{x\} \times X)$ be finite. Thus, if we have $T \in \mathrm{H}(X)$, there exists a unique $T^{\mathrm{t}} \in \mathrm{H}(X)$ such that $T^{\mathrm{t}}_{x,y} = T_{y,x}$ for every $x, y \in X$. The endomorphism

$$T \mapsto T^{\mathrm{t}}$$

of $\mathrm{H}(X)$ is an anti-involution, that is, satisfies $(ST)^{\mathrm{t}} = T^{\mathrm{t}} S^{\mathrm{t}}$ and $(T^{\mathrm{t}})^{\mathrm{t}} = T$ for every $S, T \in \mathrm{H}(X)$; this endomorphism simply corresponds to taking the transpose of the associated matrices. This anti-involution is the identity if and only if the Γ-orbits of $X \times X$ are invariant under $(x, y) \mapsto (y, x)$, in which case $\mathrm{H}(X)$ is commutative; this is a special case of Gelfand's criterion.

4.2.2 A Functor from Γ-Modules to $\mathrm{H}(X)^{\mathrm{opp}}$-Modules

Let X be a transitive Γ-set that satisfies conditions (i) and (ii) of Sect. 4.2.1. The ring $\mathrm{H}(X)$ appears as follows in the representation theory of Γ. If M is a $\mathbb{Z}[\Gamma]$-module, then the abelian group

$$M_X = \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathbb{Z}[X], M)$$

inherits a right action of $\mathrm{H}(X)$ by composition at the source. It is obvious that $M \mapsto M_X$ is a functor from Γ-modules (on the left) to $\mathrm{H}(X)$-modules on the right.

For a $\mathbb{Z}[\Gamma]$-module M and $x \in X$, the map $\varphi \mapsto \varphi(x)$ identifies M_X with the subgroup of invariants $M^{\Gamma_x} \subset M$, which also endows this subgroup with the structure of an $\mathrm{H}(X)$-module. Suppose that the matrix of $T \in \mathrm{H}(X)$ is the characteristic function of the double coset $\Gamma_x \gamma \Gamma_x$ through the identification $\Gamma_x \backslash \Gamma / \Gamma_x \xrightarrow{\sim} \Gamma \backslash (X \times X)$ chosen in Sect. 4.2.1. We have the classical formula

$$T(m) = \sum_i \gamma_i(m) \quad \forall m \in M^{\Gamma_x} \tag{4.2.3}$$

for every decomposition $\Gamma_x \gamma \Gamma_x = \coprod_i \gamma_i \Gamma_x$ (this is a finite union).

In this context, the anti-involution $T \mapsto T^{\mathrm{t}}$ defined in Sect. 4.2.1 takes on the following meaning. Let M and M' be two $\mathbb{Z}[\Gamma]$-modules, N an abelian group, and $(-|-)\colon M \times M' \to N$ a bilinear map with $(\gamma m | \gamma m') = (m|m')$ for every $\gamma \in \Gamma$ and every $(m, m') \in M \times M'$. For $(\varphi, \varphi') \in M_X \times M'_X$, $(\varphi(x)|\varphi'(x))$ does not depend on the choice of $x \in X$ hence

$$(\varphi|\varphi') := (\varphi(x)|\varphi'(x))$$

defines a bilinear form from $M_X \times M'_X$ to N. If we identify M_X with M^{Γ_x} as before, this bilinear map is nothing more than the restriction of $(-|-)$ to $M^{\Gamma_x} \times M'^{\Gamma_x}$.

We will say that X is *symmetric* if, in addition to verifying conditions (i) and (ii) of Sect. 4.2.1, it has the following equivalent properties[2]:

(iii) For every orbit Ω of Γ in $X \times X$ and every $x \in X$, we have the equality $|\Omega \cap (X \times \{x\})| = |\Omega \cap (\{x\} \times X)|$.
(iv) For every $x, y \in X$, the intersection $\Gamma_x \cap \Gamma_y$ has the same index in Γ_x and Γ_y.

Lemma 4.2.3. *Suppose that X is symmetric. For $T \in \mathrm{H}(X)$ and $(\varphi, \varphi') \in M_X \times M'_X$, we have $(T(\varphi)|\varphi') = (\varphi|T^{\mathrm{t}}(\varphi'))$.*

Proof. Let $\psi\colon X \times X \to N$ be a map that is constant on every Γ-orbit in $X \times X$ and zero outside a finite number of them. The symmetry of X implies, for every $x \in X$, the relation $\sum_{y \in X} \psi(y, x) = \sum_{y \in X} \psi(x, y)$. We apply this to the function $(x, y) \mapsto T_{x,y} \cdot (\varphi(x)|\varphi'(y))$. □

Remark 4.2.4. Suppose that V is a right $\mathrm{H}(X)$-module. The map $\mathrm{H}(X) \times V \to V$ given by $(T, v) \mapsto T^{\mathrm{t}}\, v$ defines the structure of a (left) $\mathrm{H}(X)$-module on V, which we denote by V^{t}.

4.2.5 The Hecke Ring of a $\mathbb{Z}$-group

Let G be a $\mathbb{Z}$-group. We will apply the definitions given above to $\Gamma = G(\mathbb{A}_f)$ and $X = \mathcal{R}(G)$. The *Hecke ring of* G is the ring

$$\mathrm{H}(G) := \mathrm{H}(\mathcal{R}(G)) \ .$$

Recall that for every prime p, the group $G(\mathbb{Q}_p)$ inherits from $\mathbb{Q}_p$ the structure of a locally compact topological group (that is, moreover, separated and the union of a countable number of compact groups). The subgroup $G(\mathbb{Z}_p)$ is both compact and open. The group $G(\mathbb{A}_f)$ is also a locally compact topological group for the topology whose base of open neighborhoods of the identity consists of the open sets of the form $\prod_{p \in \mathrm{P}} U_p$, where U_p for p prime is an open neighborhood of the identity in $G(\mathbb{Q}_p)$ and we have $U_p = G(\mathbb{Z}_p)$ for almost all p. In particular, $G(\widehat{\mathbb{Z}})$ is a compact open subgroup of $G(\mathbb{A}_f)$. Consequently, $\mathcal{R}(G)$ has property (ii) of Sect. 4.2.1, as do the $G(\mathbb{Q}_p)$-sets

$$\mathcal{R}_p(G) := G(\mathbb{Q}_p)/G(\mathbb{Z}_p) \ .$$

The $G(\mathbb{A}_f)$-set $\mathcal{R}(G)$ and the $\mathcal{R}_p(G)$ are symmetric in the sense of Sect. 4.2.2 if $G(\mathbb{A}_f)$ is unimodular, which is, in particular, the case if the neutral component of $G(\mathbb{C})$ is reductive [32, Sect. 5.5].

[2] This property is not automatic if X is infinite. Consider, for example, the group $\Gamma = \mathbb{Q} \rtimes \mathbb{Q}^\times$ of affine transformations of $\mathbb{Q}$ and the Γ-set X consisting of the subsets of $\mathbb{Q}$ of the form $a\mathbb{Z} + b$ with $a \in \mathbb{Q}^\times$ and $b \in \mathbb{Q}$.

For p prime, we also define $\mathrm{H}_p(G)$ as the Hecke ring of the $G(\mathbb{Q}_p)$-set $\mathcal{R}_p(G)$. The $G(\mathbb{A}_f)$-set $\mathcal{R}(G)$ can be canonically identified with the subset of $\prod_{p\in \mathrm{P}} \mathcal{R}_p(G)$ consisting of the (x_p) with $x_p = G(\mathbb{Z}_p)$ for almost all p. We have already seen a manifestation of this fact in the Eichler embedding (4.1.1). In particular, for every prime p, we have a canonical injective ring homomorphism

$$\mathrm{H}_p(G) \to \mathrm{H}(G)$$

that takes $T \in \mathrm{H}_p(G)$ to the endomorphism of $\mathbb{Z}[\mathcal{R}(G)]$ that sends $y = (y_\ell)_{\ell\in \mathrm{P}}$ to $\sum_x T_{x_p,y_p}\, x$, where the sum is taken over the elements x of $\mathcal{R}(G)$ with $x_\ell = y_\ell$ in $\mathcal{R}_\ell(G)$ for every $\ell \neq p$. We will simply write

$$\mathrm{H}_p(G) \subset \mathrm{H}(G)\ .$$

If $p \neq q$, then for $S \in \mathrm{H}_p(G)$ and $T \in \mathrm{H}_q(G)$, we have $TS = ST$.

If for every prime p, we take a $G(\mathbb{Q}_p)$-orbit $\Omega_p \subset \mathcal{R}_p(G) \times \mathcal{R}_p(G)$ and if, moreover, Ω_p is the orbit of $G(\mathbb{Z}_p) \times G(\mathbb{Z}_p)$ for almost all p, then the subset of elements (ω_p) of $\prod_p \Omega_p$ with $\omega_p = G(\mathbb{Z}_p) \times G(\mathbb{Z}_p)$ for almost all p can be naturally identified with a $G(\mathbb{A}_f)$-orbit in $\mathcal{R}(G) \times \mathcal{R}(G)$. Conversely, every $G(\mathbb{A}_f)$-orbit $\Omega \subset \mathcal{R}(G) \times \mathcal{R}(G)$ is of this form for a unique family (Ω_p), where the $G(\mathbb{Q}_p)$-orbit Ω_p is the image of Ω by the canonical projection $\mathcal{R}(G) \times \mathcal{R}(G) \to \mathcal{R}_p(G) \times \mathcal{R}_p(G)$. From these observations and the surjectivity of the map (4.2.1) it follows that $\mathrm{H}(G)$ is isomorphic to the tensor product of its subrings $\mathrm{H}_p(G)$:

$$\bigotimes_{p\in \mathrm{P}} \mathrm{H}_p(G) \xrightarrow{\sim} \mathrm{H}(G)\ .$$

Understanding $\mathrm{H}(G)$ therefore completely reduces to understanding the $\mathrm{H}_p(G)$.

The ring $\mathrm{H}_p(G)$ depends only on the $\mathbb{Z}_p$-group $G_{\mathbb{Z}_p} = G \times_{\mathbb{Z}} \mathbb{Z}_p$. When $G_{\mathbb{Z}_p}$ is reductive, general results of Satake and Bruhat–Tits imply that $\mathrm{H}_p(G)$ is commutative; we will come back to this in Sect. 6.2. As a consequence, the same holds for $\mathrm{H}(G)$ if G is reductive over $\mathbb{Z}$. However, this property is elementary in the most classical cases, which we recall below.

4.2.6 Some Classical Hecke Rings

First, suppose $G = \mathrm{PGL}_n$. We have seen that $\mathcal{R}(G)$ can be identified with

$$\underline{\mathcal{R}}_{\mathbb{Z}}(V) := \mathbb{Q}^\times \backslash \mathcal{R}_{\mathbb{Z}}(V)\ ,$$

where $V = \mathbb{Q}^n$. Recall that $\underline{M} \in \underline{\mathcal{R}}_{\mathbb{Z}}(V)$ denotes the homothety class of a lattice $M \in \mathcal{R}_{\mathbb{Z}}(V)$.

For $M, N \in \mathcal{R}_{\mathbb{Z}}(V)$, there exists a least integer $d \geq 1$ with $dN \subset M$. The isomorphism class of the abelian group M/dN depends only on the $G(\mathbb{A}_f)$-orbit of

$(\underline{N}, \underline{M})$ in $\underline{\mathcal{R}}_{\mathbb{Z}}(V) \times \underline{\mathcal{R}}_{\mathbb{Z}}(V)$. The theory of elementary divisors then shows that the resulting map

$$G(\mathbb{A}_f)\backslash(\underline{\mathcal{R}}_{\mathbb{Z}}(V) \times \underline{\mathcal{R}}_{\mathbb{Z}}(V)) \to \mathrm{AF}\ ,$$

where AF is the set of isomorphism classes of finite abelian groups, is an injection whose image consists of the groups generated by $n-1$ elements. If A is such a group, the associated Hecke operator $\mathrm{T}_A \in \mathrm{H}(G)$ satisfies, by definition,

$$\mathrm{T}_A(\underline{M}) = \sum_N \underline{N}\ ,$$

where the sum is taken over the subgroups N of M with $M/N \simeq A$. When A runs through the finite abelian groups generated by $n-1$ elements, these operators T_A therefore form a $\mathbb{Z}$-basis of $\mathrm{H}(G)$. It is clear that we have $\mathrm{T}_{A\times B} = \mathrm{T}_A\mathrm{T}_B$ if $|A|$ and $|B|$ are relatively prime and that we have $\mathrm{T}_A \in \mathrm{H}_p(G)$ if and only if A is a p-group.

If $n = 2$, we easily verify that $\mathrm{T}_A^{\mathrm{t}} = \mathrm{T}_A$ for every A; in particular, $\mathrm{H}(G)$ is commutative (the notation T^{t} is defined in Sect. 4.2.1). The first statement no longer holds for $n > 2$, but $\mathrm{H}(G)$ remains commutative. We can see this simply by endowing V with a nondegenerate symmetric bilinear form. The map $\underline{M} \mapsto \underline{M^\sharp}$ is an involution of $\underline{\mathcal{R}}_{\mathbb{Z}}(V)$. It induces a linear involution of $\mathbb{Z}[\,\underline{\mathcal{R}}_{\mathbb{Z}}(V)\,]$ and then, by conjugation, an involution ι of $\mathrm{H}(G)$, which is nothing more than $(T_{\underline{N},\underline{M}}) \mapsto (T_{\underline{N^\sharp},\underline{M^\sharp}})$ on the associated matrices. But for $N \subset M$, the quotient $N^\sharp/M^\sharp$ is in perfect duality with M/N and therefore ι coincides with the canonical anti-involution of $\mathrm{H}(G)$: $\iota(T) = T^{\mathrm{t}}$ for every $T \in \mathrm{H}(G)$ (see also [188, Sect. 3]).

Let us now discuss the case of orthogonal and symplectic $\mathbb{Z}$-groups, which is particularly important for this book [174, 88, 5]. We use the notation of Sect. 4.1.2; in particular, $V = L \otimes \mathbb{Q}$ has even dimension n, φ is a bilinear form on V that is symmetric (resp. alternating), for which L is self-dual and even, and $G \subset \mathrm{GL}_L$ is the group O_L (resp. Sp_L).

In this case, we have seen that $\mathcal{R}(G)$ can be identified with the $G(\mathbb{A}_f)$-set $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ of self-dual lattices in V (Proposition 4.1.4). For (N, M) in the product $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, the isomorphism class of the abelian group $M/(N \cap M)$ depends only on the $G(\mathbb{A}_f)$-orbit of (N, M). We have thus defined a natural map

$$G(\mathbb{A}_f)\backslash(\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)) \to \mathrm{AF}\ , \quad (N, M) \mapsto M/(N \cap M)\ . \tag{4.2.4}$$

Proposition 4.2.7. *The map* (4.2.4) *is an injection whose image consists of the groups generated by* $n/2$ *elements.*

This proposition is well known; we will recall a proof at the end of this subsection for the sake of the reader. Let A be a finite abelian group generated by at most $n/2$ elements. To this group corresponds a Hecke operator

$$\mathrm{T}_A \in \mathrm{H}(G)$$

defined by $\mathrm{T}_A(M) = \sum_N N$, where the sum is taken over the N such that $M/(N \cap M) \simeq A$ or, equivalently, over the A-neighbors of M in the sense of Scholium-Definition 3.1.2 in the quadratic case. These operators T_A therefore form a $\mathbb{Z}$-basis of $\mathrm{H}(G)$. We, of course, still have $\mathrm{T}_{A\times B} = \mathrm{T}_A\mathrm{T}_B$ if $|A|$ and $|B|$ are relatively prime, and $\mathrm{T}_A \in \mathrm{H}_p(G)$ if and only if A is a p-group. From the point of view of Chap. 3, an operator that is particularly important for us is $\mathrm{T}_{\mathbb{Z}/d\mathbb{Z}}$ for $d \geq 1$, which we also denote simply by T_d.

Proposition 4.2.8. *Let A be a finite abelian group generated by $n/2$ elements. Then we have $\mathrm{T}^{\mathrm{t}}_A = \mathrm{T}_{A^\vee} = \mathrm{T}_A$. In particular, the ring $\mathrm{H}(G)$ is commutative.*

Proof. The first assertion follows from Scholium-Definition 3.1.2 when φ is symmetric, and from a similar argument in the alternating case. The second assertion follows from the first by the end of Sect. 4.2.1. See also [174, Chap. III], [88, Kap. IV], and Sect. 6.2.8. □

Finally, let us discuss the group of projective similitudes $\mathrm{P}\widetilde{G}$. Let p be a prime and $\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ the set of even homodual lattices in V_p, introduced after Lemma 4.1.3. Recall that if φ is symmetric (resp. alternating), a lattice $M \in \mathcal{R}_{\mathbb{Z}_p}(V_p)$ is homodual if and only if there exists a $\lambda_M \in p^{\mathbb{Z}}$, necessarily unique, such that $x \mapsto \lambda_M\, \varphi(x,x)/2$ (resp. $\lambda_M\varphi$) endows M with the structure of a q-module (resp. a-module) over $\mathbb{Z}_p$. Since the q-vector space V_p is hyperbolic by Scholium 2.2.5, the same holds for $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ as a q-module over $\mathbb{Z}_p$, by Proposition 2.1.2. This shows that the map $g \mapsto g(L)$ induces isomorphisms $\mathcal{R}_p(\widetilde{G}) \xrightarrow{\sim} \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ and $\mathcal{R}_p(G) \xrightarrow{\sim} \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}_p}(V_p)$. In particular, the set $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) := \mathbb{Q}_p^\times\backslash\mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ can be naturally identified with $\mathcal{R}_p(\mathrm{P}\widetilde{G})$.

Consider $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$. We denote by $\mathrm{v}_M \in \mathbb{Z}$ the unique integer such that $\lambda_M = p^{-\mathrm{v}_M}$. For $g \in \widetilde{G}(\mathbb{Q}_p)$, we have $\mathrm{v}_{g(M)} = \mathrm{v}_M + v$, where v is the p-adic valuation of $\nu(g)$. Let $(\underline{N}, \underline{M})$ be an ordered pair of elements of $\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$. After changing the representative N if necessary, we may assume $\mathrm{v}_M - \mathrm{v}_N \in \{0,1\}$. The pair $(M/N \cap M, \mathrm{v}_M - \mathrm{v}_N)$ then depends only on the $\mathrm{P}\widetilde{G}(\mathbb{Q}_p)$-orbit of $(\underline{N}, \underline{M})$, which defines a map

$$\mathrm{P}\widetilde{G}(\mathbb{Q}_p)\backslash(\underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p) \times \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)) \to \mathrm{AF} \times \{0,1\}\,. \tag{4.2.5}$$

Proposition 4.2.9. *The map (4.2.5) is an injection whose image is the set of pairs $(A,-)$ with A an abelian p-group generated by $n/2$ elements.*

We push back the proof of this proposition to Sect. 6.2.8. Consider $(A,i) \in \mathrm{AF} \times \{0,1\}$, where A is a p-group generated by at most $n/2$ elements. We say that $\underline{N} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ is an A-neighbor of type i of $\underline{M} \in \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}_p}(V_p)$ if the image of $(\underline{N}, \underline{M})$ by the map (4.2.5) is (A,i). The corresponding Hecke operator is denoted by

$$\mathrm{T}_{(A,i)} \in \mathrm{H}_p(\mathrm{P}\widetilde{G})\,;$$

these operators form a $\mathbb{Z}$-basis of $\mathrm{H}_p(\mathrm{P}\widetilde{G})$. If we have $M^\sharp = M$, then $\underline{N}$ is an A-neighbor of type 0 of $\underline{M}$ if and only if $\underline{N}$ has a self-dual representative, which is then unique, and if the latter is an A-neighbor of M in the previous sense. The notion of an A-neighbor of type 1 of $\underline{M}$ is, on the other hand, "new." The following example will be particularly important in this book.

Consider $M, N \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$. Following Koch and Venkov in the quadratic case [127], we say that N is a *perestroika* of M with respect to p if we have

$$pM \subsetneq N \subsetneq M \ .$$

We easily verify that N is a perestroika of M with respect to p if and only if we have $\mathrm{v}_M - \mathrm{v}_{p^{-1}N} = 1$ and $\underline{N}$ is a 0-neighbor of $\underline{M}$ of type 1. Moreover, the following proposition is immediate.

Proposition 4.2.10. *Consider $M \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$, and let p be a prime number. The map $N \mapsto N/pM$ defines a bijection from the set of perestroikas of M with respect to p onto the set of Lagrangians of $M \otimes \mathbb{F}_p$.*

The perestroika operator with respect to p is the operator

$$\mathrm{K}_p := \mathrm{T}_{(0,1)} \in \mathrm{H}_p(\mathrm{P}\widetilde{G}) \ .$$

For $(N, M) \in \mathcal{R}^{\mathrm{h}}_{\mathbb{Z}}(V)$, N is a perestroika of M with respect to p if and only if pM is a perestroika of N with respect to p. In particular, we have $\mathrm{K}_p^{\mathrm{t}} = \mathrm{K}_p$. In fact, we have $T^{\mathrm{t}} = T$ for every $T \in \mathrm{H}(\mathrm{P}\widetilde{G})$, as we will see in Sect. 6.2.8.

Let us conclude this subsection, as announced, with a proof of Proposition 4.2.7.

Proof of Proposition 4.2.7. We place ourselves in the quadratic setting, that is, φ symmetric and $\mathrm{q}(x) = \varphi(x, x)/2$, in which case L is a q-module over $\mathbb{Z}$. The proof in the alternating setting is similar (and even simpler).

We must show that if U is a hyperbolic q-vector space over $\mathbb{Q}_p$ and (L_1, L_2) and (L'_1, L'_2) are two ordered pairs of self-dual lattices in U such that $L_1/(L_1 \cap L_2) \simeq L'_1/(L'_1 \cap L'_2)$, then there exists an $\alpha \in \mathrm{O}(U)$ with $\alpha(L_i) = L'_i$ for $i = 1, 2$. We use induction on $\dim(U)$.

The cases $U = 0$ and $L_1 = L_2$ are trivial. We assume $L_1 \neq L_2$; the annihilator of the quotient $L_1/(L_1 \cap L_2)$ is therefore of the form $p^\nu \mathbb{Z}_p$ with $\nu \geq 1$. Moreover, there exist an element e_1 of L_1 and an element e_2 of L_2 such that we have

$$\mathrm{q}(e_1) = 0 \ , \quad \mathrm{q}(e_2) = 0 \ , \quad e_1.e_2 = p^{-\nu} \ .$$

Indeed, it is first of all easy to see that there exist an element ϵ_1 of L_1 and an element ϵ_2 of L_2 with $\epsilon_1.\epsilon_2 = p^{-\nu}$. Hensel's lemma then shows that there exists a matrix

$$P = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$$

with coefficients in $\mathbb{Z}_p$, with $P \equiv \mathrm{I} \bmod p^\nu$, such that we have

$$ {}^{\mathrm{t}}P \begin{bmatrix} 2\mathrm{q}(\epsilon_1) & p^{-\nu} \\ p^{-\nu} & 2\mathrm{q}(\epsilon_2) \end{bmatrix} P \;=\; \begin{bmatrix} 0 & p^{-\nu} \\ p^{-\nu} & 0 \end{bmatrix} . $$

We take $e_1 = a_{1,1}\epsilon_1 + a_{2,1}\epsilon_2$ and $e_2 = a_{1,2}\epsilon_1 + a_{2,2}\epsilon_2 \in L_2$ (the congruence $P \equiv \mathrm{I} \bmod p^\nu$ implies $e_1 \in L_1$ and $e_2 \in L_2$). This concludes the proof of the statement.

Let us now finish the induction. We denote by H, H_1, and H_2, respectively, the linear subspace of U generated by e_1 and e_2, the submodule of L_1 generated by e_1 and $p^\nu e_2$, and the submodule of L_2 generated by $p^\nu e_1$ and e_2. We endow H, H_1, and H_2 with the quadratic forms induced by those on U. By construction, we have $H \approx \mathrm{H}(\mathbb{Q}_p)$ and $H_i \approx \mathrm{H}(\mathbb{Z}_p)$ for $i = 1, 2$. We denote by W, M_1, and M_2, respectively, the orthogonal complement of H in U, the orthogonal complement of H_1 in L_1, and the orthogonal complement of H_2 in L_2. We have decompositions into orthogonal sums

$$ U = H \oplus W \;, \quad L_1 = H_1 \oplus M_1 \;, \quad L_2 = H_2 \oplus M_2 $$

and isomorphisms

$$ L_1/(L_1 \cap L_2) \cong H_1/(H_1 \cap H_2) \oplus M_1/(M_1 \cap M_2) \;, \quad H_1/(H_1 \cap H_2) \cong \mathbb{Z}_p/p^\nu\mathbb{Z}_p \;. $$

We replace the ordered pair (L_1, L_2) by the ordered pair (L_1', L_2') and introduce the q-vector spaces H' and W' and the q-modules H_1', H_2', M_1', and M_2' analogously. We obtain the desired automorphism $\alpha \colon U \to U$ as the orthogonal sum of suitable isomorphisms of q-vector spaces $H \to H'$ and $W \to W'$; the existence of the second is ensured by the induction hypothesis. □

4.2.11 $\mathrm{H}(\mathrm{SO}_L)$ *Versus* $\mathrm{H}(\mathrm{O}_L)$

Let L be a q-module over $\mathbb{Z}$. Let us briefly discuss the link between $\mathrm{H}(\mathrm{SO}_L)$ and $\mathrm{H}(\mathrm{O}_L)$. The cases PGSO_L and PGO_L can be treated similarly.

By Proposition 4.1.7, the inclusion $\mathrm{SO}_L \to \mathrm{O}_L$ induces an $\mathrm{SO}_L(\mathbb{A}_f)$-equivariant bijection $\mathcal{R}(\mathrm{SO}_L) \xrightarrow{\sim} \mathcal{R}(\mathrm{O}_L)$. It follows that $\mathrm{H}(\mathrm{O}_L)$ can be canonically identified with a subring of $\mathrm{H}(\mathrm{SO}_L)$: these are the subrings of $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[\mathcal{R}_{\mathbb{Z}}^{\mathrm{a}}(V)])$ consisting of the $\mathrm{O}_L(\mathbb{A}_f)$-equivariant and $\mathrm{SO}_L(\mathbb{A}_f)$-equivariant endomorphisms, respectively. The quotient group

$$ \mathrm{O}_L(\mathbb{A}_f)/\mathrm{SO}_L(\mathbb{A}_f) \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathrm{P}} $$

acts naturally by conjugation on $\mathrm{H}(\mathrm{SO}_L)$, with ring of invariants $\mathrm{H}(\mathrm{O}_L)$. This action respects the decomposition of $\mathrm{H}(G)$ as a tensor product of the $\mathrm{H}_p(G)$ over the $p \in \mathrm{P}$ and also identifies $\mathrm{H}_p(\mathrm{O}_L)$ with $\mathrm{H}_p(\mathrm{SO}_L)^{\mathbb{Z}/2\mathbb{Z}}$.

Let us give an example of an element of $\mathrm{H}_p(\mathrm{SO}_L)$ that is not in $\mathrm{H}_p(\mathrm{O}_L)$. Consider $A = (\mathbb{Z}/p\mathbb{Z})^{n/2}$, where n is the rank of L. Let Ω be the set of pairs (N, M) of elements of $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$ such that N is an A-neighbor of M. Proposition 4.2.7 asserts that Ω is an $\mathrm{O}_L(\mathbb{Q}_p)$-orbit. However, it is the disjoint union of two orbits under the action of $\mathrm{SO}_L(\mathbb{Q}_p)$. To see this, we begin by verifying, using arguments similar to those in Sect. 3.1, that the map

$$N \mapsto (M \cap N)/pM$$

induces a surjection (that is not bijective in general) between the A-neighbors of M and the Lagrangians of the hyperbolic q-vector space $M \otimes \mathbb{F}_p$. But it is well known that for every field k and every hyperbolic q-vector space V over k, there are exactly two orbits of Lagrangians of V under the action of $\mathrm{SO}(V)$ (and only one under $\mathrm{O}(V)$, by Witt's theorem). By the smoothness of SO_M over $\mathbb{Z}_p$, each of these two orbits therefore defines an $\mathrm{SO}(M)$-orbit of A-neighbors of M and, consequently, two distinct Hecke operators $\mathrm{T}^{\pm}_A \in \mathrm{H}(\mathrm{SO}_L)$ with sum T_A, which are interchanged under the action of $\mathrm{O}_L(\mathbb{Q}_p)/\mathrm{SO}_L(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$.

4.2.12 Isogenies

We will now discuss the isogenies between transitive Γ-sets, by presenting a variant of the considerations in [174, Chap. II, Sect. 7].

Let X be a Γ-set and X' a Γ'-set. Recall that a morphism $X \to X'$ is a pair (f, g), where $g\colon X \to X'$ is a map and $f\colon \Gamma \to \Gamma'$ is a group morphism such that we have $g(\gamma x) = f(\gamma)g(x)$ for every $x \in X$ and every $\gamma \in \Gamma$. In what follows, we conveniently assume that a transitive set is nonempty.

Lemma 4.2.13. *Let X be a transitive Γ-set, X' a Γ'-set, and (f, g) a morphism $X \to X'$ such that $f(\Gamma)$ is normal in Γ'. Let S be the stabilizer of $g(X)$ in Γ', that is, $S = \{\gamma \in \Gamma' \,;\, \gamma g(X) \subset g(X)\}$.*

(i) *For every $x \in g(X)$, we have $S = f(\Gamma)\Gamma'_x$.*
(ii) *We have $S = \{\gamma \in \Gamma' \,;\, \gamma g(X) \cap g(X) \neq \emptyset\}$.*

Proof. Take $x \in g(X)$. Since the subgroup $f(\Gamma)$ is normal in Γ', the subset $E_x := f(\Gamma)\Gamma'_x \subset \Gamma'$ is a subgroup. The transitivity of X then shows that

- E_x does not depend on the choice of $x \in g(X)$;
- E_x is the set of $\gamma \in \Gamma'$ with $\gamma(x) \in g(X)$.

We consequently have the identities $S = \bigcap_{x \in g(X)} E_x = \bigcup_{x \in g(X)} E_x = \{\gamma \in \Gamma' \,;\, \gamma g(X) \cap g(X) \neq \emptyset\}$. □

Let X be a transitive Γ-set, X' a Γ'-set, and (f, g) a morphism $X \to X'$. We assume, as in the lemma above, that $f(\Gamma)$ is normal in Γ' and, moreover that the map

g is injective.[3] Let S be the stabilizer of $g(X)$ in Γ'. The map $(s, x) \mapsto g^{-1}(s(g(x))$, which is well defined by the injectivity of g, defines an action of S on X whose restriction to $f\colon \Gamma \to S$ is the Γ-set X. It therefore induces an action of $S/f(\Gamma)$ on $\mathrm{H}(X)$ by ring automorphisms; we denote by $\mathrm{H}(X)^{\mathrm{inv}} \subset \mathrm{H}(X)$ the subring of invariants, which is also $\mathrm{End}_{\mathbb{Z}[S]}(\mathbb{Z}[X])$.

Proposition-Definition 4.2.14. *Let $u = (f, g)\colon X \to X'$ be a morphism between the transitive Γ-set X and the transitive Γ'-set X'. We assume that $f(\Gamma)$ is normal in Γ' and that g is injective.*

(i) *For $T \in \mathrm{H}(X)^{\mathrm{inv}}$, there exists a unique $T' \in \mathrm{H}(X')$ that vanishes on $(X' - g(X)) \times g(X)$ and satisfies $T'_{g(x),g(y)} = T_{x,y}$ for every $x, y \in X$.*

(ii) *The resulting map $\mathrm{H}(u)\colon \mathrm{H}(X)^{\mathrm{inv}} \to \mathrm{H}(X')$ defined by $T \mapsto T'$ is an injective ring homomorphism.*

Proof. The uniqueness assertion in part (i) follows from the injectivity of g and the transitivity of X'. Assertion (ii) immediately follows from part (i). We are therefore left with justifying the existence of T' in part (i). But part (ii) of Lemma 4.2.13 shows that the injection $g\colon X \to X'$ induces a bijection $\mathrm{Ind}_S^{\Gamma'} X \xrightarrow{\sim} X'$ and therefore an isomorphism $\mathbb{Z}[\Gamma'] \otimes_{\mathbb{Z}[S]} \mathbb{Z}[X] \xrightarrow{\sim} \mathbb{Z}[X']$. Thus, when composed with $g\colon \mathbb{Z}[X] \to \mathbb{Z}[X']$, every S-equivariant linear map $T\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ extends uniquely to a Γ'-equivariant map $T'\colon \mathbb{Z}[X'] \to \mathbb{Z}[X']$; this has the desired properties. □

In all the examples we consider, it turns out that the group S preserves every Γ-orbit of $X \times X$, so that we have $\mathrm{H}(X)^{\mathrm{inv}} = \mathrm{H}(X)$. A particularly simple case is that where we have $\Gamma' = \Gamma$ and $X' = X$ and f and g are bijective. In this case, we have $S = f(\Gamma)$ and $\mathrm{H}(u)$ is, by definition, the automorphism of $\mathrm{H}(X)$ whose matrix is given by $(T_{x,y}) \mapsto (T_{g^{-1}x,g^{-1}y})$.

Let us assume that the hypotheses of Proposition-Definition 4.2.14 hold. For a Γ'-module M, we denote by $M_{|\Gamma}$ the Γ-module obtained by restricting M via $f\colon \Gamma \to \Gamma'$. We then have a canonical injective map

$$M_{X'} \to (M_{|\Gamma})_X\ , \quad \varphi \mapsto \varphi_{|X} := \varphi \circ g\ .$$

The following lemma is immediate.

Lemma 4.2.15. *Under the assumptions of Proposition-Definition 4.2.14, let M be a Γ'-module, and take $T \in \mathrm{H}(X)^{\mathrm{inv}}$ and $\varphi \in M_{X'}$. Then we have $T(\varphi_{|X}) = \mathrm{H}(u)(T)(\varphi)$.*

Example 4.2.16. By way of example, we return to the context of the similitude groups (Sect. 4.1.2) and consider the natural $\mathbb{Z}$-morphism $\mu\colon G \to \mathrm{P}\widetilde{G}$. The results of this

[3] We refer to the article of Satake for a variant without the injectivity assumption on g. The reader will not miss much in the current discussion by assuming $\Gamma \subset \Gamma'$ and $X \subset X'$, with f and g the corresponding inclusions.

section apply and define a ring morphism

$$\mathrm{H}(\mu)\colon \mathrm{H}(G) \to \mathrm{H}(\mathrm{P}\widetilde{G})$$

with $\mathrm{H}(\mu)(\mathrm{T}_A) = \mathrm{T}_{(A,0)}$ for every finite abelian group A generated by at most $n/2$ elements.

Indeed, consider $\Gamma = G(\mathbb{A}_f)$, $X = \mathcal{R}(G)$, $\Gamma' = \mathrm{P}\widetilde{G}(\mathbb{A}_f)$, and $X' = \mathcal{R}(\mathrm{P}\widetilde{G})$, and for f and g, take the natural maps deduced from μ. The group Γ is a normal subgroup of $\widetilde{G}(\mathbb{A}_f)$; likewise, $f(\Gamma)$ is a normal subgroup of Γ'. Moreover, g can be identified with the natural injection $\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \to \underline{\mathcal{R}}^{\mathrm{h}}_{\mathbb{Z}}(V)$ defined by $M \mapsto \underline{M}$, by Proposition 4.1.4. The group S is the subgroup of elements $g \in \widetilde{G}(\mathbb{A}_f)$ such that $\nu(g)$ is of the form $a^2 b$ with $a \in \mathbb{A}_f^{\times}$ and $b \in \widehat{\mathbb{Z}}^{\times}$. It acts trivially on $\Gamma\backslash(\mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V) \times \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V))$. Indeed, given $N, M \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(V)$, $g \in \widetilde{G}(\mathbb{A}_f)$, and a prime p, the map g induces an isomorphism $M_p/(N_p \cap M_p) \simeq g(M)_p/(g(N)_p \cap g(M)_p)$, which allows us to conclude using Proposition 4.2.7. The assertion on T_A follows from the discussion following Proposition 4.2.9.

4.3 Automorpic Forms of a $\mathbb{Z}$-group

The ring of adeles of $\mathbb{Q}$ is the ring $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$. Let G be a $\mathbb{Z}$-group. The group $G(\mathbb{R})$ is naturally a Lie group, and the group

$$G(\mathbb{A}) = G(\mathbb{R}) \times G(\mathbb{A}_f)$$

is locally compact and separated for the product topology; we already recalled the topology on $G(\mathbb{A}_f)$ in Sect. 4.2.5. There is a natural diagonal embedding of the group $G(\mathbb{Q})$ in $G(\mathbb{A})$; the image is a discrete closed subgroup (see [92, Chap. II, Sect. 3] for the basics on these constructions).

4.3.1 Square-Integrable Automorphic Forms

Let us recall some classical results due to Borel and Harish-Chandra, for which we refer to [32, Sect. 5]. We assume that the neutral component of $G(\mathbb{C})$ is semisimple [103, 34]. The locally compact group $G(\mathbb{A})$ is then unimodular. By Weil, the homogeneous space

$$G(\mathbb{Q})\backslash G(\mathbb{A})$$

inherits a positive (nonzero) Radon measure μ invariant under the action of $G(\mathbb{A})$ by right translations [211, Chap. II], [172, Chap. 2]. It has finite measure.

The space of *square-integrable automorphic forms for* G is the subspace

$$\mathcal{A}^2(G) \subset \mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$$

of elements that are invariant under $G(\widehat{\mathbb{Z}})$ for right translations [92, Chap. 3], [36, Sect. 4]. It is a Hilbert space for the Hermitian inner product

$$\langle f, f' \rangle_{\mathrm{Pe}} := \int \overline{f} f' \ \mathrm{d}\mu \ ,$$

also called the *Petersson inner product*. Alternatively, $\mathcal{A}^2(G)$ can be viewed as the space of square-integrable functions on $G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$ endowed with the Radon measure that is the image of μ by the canonical (proper) map $G(\mathbb{Q})\backslash G(\mathbb{A}) \to G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})$. The space $\mathcal{A}^2(G)$ is endowed with two important additional structures that we will now describe.

On the one hand, since the space $\mathcal{A}^2(G)$ is the space of $G(\widehat{\mathbb{Z}})$-invariants of the $G(\mathbb{A}_f)$-module $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$ for the right translations, it is endowed with a right action of the Hecke ring $\mathrm{H}(G)$ (Sects. 4.2.2, 4.2.5). This action is a $\star$-*action* for the Petersson inner product. By this, we mean that the adjoint of $T \in \mathrm{H}(G)$ is the operator T^{t} defined in Sect. 4.2.1: for $f, f' \in \mathcal{A}^2(G)$ and $T \in \mathrm{H}(G)$, we have

$$\langle T(f), f' \rangle_{\mathrm{Pe}} = \langle f, T^{\mathrm{t}}(f') \rangle_{\mathrm{Pe}} \ . \tag{4.3.1}$$

Indeed, this is a consequence of Lemma 4.2.3 and the unimodularity of $G(\mathbb{A}_f)$.

On the other hand, $\mathcal{A}^2(G)$ is stable under the action of $G(\mathbb{R})$ by right translations, and this action commutes with that of $\mathrm{H}(G)$. It turns $\mathcal{A}^2(G)$ into a unitary representation of the Lie group $G(\mathbb{R})$ (we refer to [119] as a general reference on unitary representations). A more classical description of this representation is obtained by writing

$$G(\mathbb{A}_f) = \coprod_{i=1}^{\mathrm{h}(G)} G(\mathbb{Q}) g_i G(\widehat{\mathbb{Z}}) \tag{4.3.2}$$

for certain elements $g_i \in G(\mathbb{A}_f)$, by the finiteness of the class set of G. For every i, the double coset $G(\mathbb{Q})g_iG(\widehat{\mathbb{Z}})$ is an open subset of $G(\mathbb{A}_f)$ and the *congruence subgroup*

$$\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$$

is a discrete subgroup of $G(\mathbb{R})$ that is commensurable with $G(\mathbb{Z})$. The map $f \mapsto (f_{|G(\mathbb{R})\times g_i})_i$ induces a $G(\mathbb{R})$-equivariant isomorphism

$$\mathcal{A}^2(G) \xrightarrow{\sim} \prod_{i=1}^{\mathrm{h}(G)} \mathrm{L}^2(\Gamma_i\backslash G(\mathbb{R})) \ , \tag{4.3.3}$$

where each $\Gamma_i\backslash G(\mathbb{R})$ naturally inherits a strictly positive Radon measure that is right invariant for $G(\mathbb{R})$, has finite mass, and is uniquely determined by μ. This representation of $G(\mathbb{R})$ in general has a "discrete" part that is notoriously difficult to describe, as well as a "continuous" part whose study was reduced by Langlands to that of discrete subsets for auxiliary groups G' [138].

4.3.2 The Set $\Pi_{\mathrm{disc}}(G)$

Here, we are interested only in the discrete part of $\mathcal{A}^2(G)$, that is, in the subspace

$$\mathcal{A}_{\mathrm{disc}}(G) \subset \mathcal{A}^2(G)$$

defined as the closure of the sum of the closed and topologically irreducible sub-$G(\mathbb{R})$-representations of $\mathcal{A}^2(G)$. It is a representation of $G(\mathbb{R})$ that is, by construction, an orthogonal sum of irreducible representations,[4] where each component has a finite multiplicity by a fundamental result due to Harish-Chandra (see the introduction of [101], as well as Theorem 1 of Chap. 1 of the same reference; see also [36]). In other words, if U is a unitary irreducible representation of $G(\mathbb{R})$, then the space

$$\mathcal{A}_U(G) := \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}_{\mathrm{disc}}(G)) = \mathrm{Hom}_{G(\mathbb{R})}(U, \mathcal{A}^2(G))$$

has finite dimension over $\mathbb{C}$. We have, of course, a canonical isomorphism

$$\widehat{\bigoplus_{U \in \mathrm{Irr}(G(\mathbb{R}))}} U \otimes \mathcal{A}_U(G) \xrightarrow{\sim} \mathcal{A}_{\mathrm{disc}}(G)\ , \tag{4.3.4}$$

where $\mathrm{Irr}(H)$ is the set of isomorphism classes of topologically irreducible unitary representations of the locally compact group H.

The right $\mathrm{H}(G)$-module structure on $\mathcal{A}^2(G)$ naturally induces the structure of a right $\mathrm{H}(G)$-module on $\mathcal{A}_U(G)$. The latter also inherits a Hermitian inner product for which the action of $\mathrm{H}(G)$ is again a $\star$-action. For example, for a fixed nonzero $e \in U$ and $\varphi, \varphi' \in \mathcal{A}_U(G)$, we can set $\langle \varphi, \varphi' \rangle = \langle \varphi(e), \varphi'(e) \rangle_{\mathrm{Pe}}$. But it is well known that a sub-$\mathbb{C}$-algebra of $\mathrm{M}_n(\mathbb{C})$ that is stable under $M \mapsto {}^{\mathrm{t}}\overline{M}$ is semisimple: if X is in its Jacobson radical, then the Hermitian matrix $X\,{}^{\mathrm{t}}\overline{X}$ is nilpotent, hence zero, which implies that X is zero. In particular, $\mathcal{A}_U(G)$ is semisimple when viewed as a representation of the $\mathbb{C}$-algebra $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$.

We define a *representation of* $(G(\mathbb{R}), \mathrm{H}(G))$ to be a Hilbert space endowed with a unitary representation of $G(\mathbb{R})$, together with the structure of a right $\mathrm{H}(G)$-module, such that the action of any element of $G(\mathbb{R})$ commutes with that of any element of $\mathrm{H}(G)$. These representations naturally form a $\mathbb{C}$-linear category: a morphism $E \to F$ is a continuous $\mathbb{C}$-linear map $E \to F$ that commutes with the actions of $G(\mathbb{R})$ and $\mathrm{H}(G)$. For a unitary representation U of $G(\mathbb{R})$ and a $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module V of finite dimension as a $\mathbb{C}$-vector space, $U \otimes V$ is naturally a representation of $(G(\mathbb{R}), \mathrm{H}(G))$ (where the tensor product is taken over $\mathbb{C}$). We denote by $\Pi(G)$ the set of isomorphism classes of representations of $(G(\mathbb{R}), \mathrm{H}(G))$ of this form

[4] At this point, it is useful to recall the following version of Schur's lemma. Let U and V be Hilbert spaces endowed with unitary representations of a group Γ. We assume that U is topologically irreducible and that $u\colon U \to V$ is a nonzero, Γ-equivariant, continuous linear map. Then the adjoint $u^*\colon V \to U$ (which is Γ-equivariant) satisfies $u^* \circ u = \lambda \mathrm{Id}_U$ for some $\lambda \in \mathbb{R}^\times$. Indeed, $u^* \circ u \in \mathrm{End}(U)$ is Hermitian and nonzero and commutes with Γ; by the spectral theorem, its spectrum is therefore reduced to a point $\{\lambda\}$. It follows that V is the orthogonal sum of $\mathrm{Im}(u)$ (which is closed) and $\mathrm{Ker}(u^*)$.

such that, moreover, U is topologically irreducible and V is simple. The restriction to $G(\mathbb{R})$ of such a unitary representation π is isomorphic to $U^{\dim V}$, so that the isomorphism class π_∞ of the unitary representation U is fully determined by the unitary representation of $G(\mathbb{R})$ underlying π. Likewise, the $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module underlying π is semisimple and V-isotypical, so that the isomorphism class π_f of the $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module V is uniquely determined by that of π. In particular, we have $\pi \simeq \pi_\infty \otimes \pi_f$ for every $\pi \in \Pi(G)$. Finally, Schur's lemma implies that every $\pi \in \Pi(G)$ is topologically irreducible as a representation of $(G(\mathbb{R}), \mathrm{H}(G))$.

By the discussion above, for $U \in \mathrm{Irr}(G(\mathbb{R}))$, the space $U \otimes \mathcal{A}_U(G)$ is naturally a representation of $(G(\mathbb{R}), \mathrm{H}(G))$, as is $\mathcal{A}_{\mathrm{disc}}(G)$, where the isomorphism (4.3.4) trivially commutes with the actions of $G(\mathbb{R})$ and $\mathrm{H}(G)$. It follows that we have a decomposition into a Hilbert sum of elements of $\Pi(G)$ that refines the decomposition (4.3.4):

$$\mathcal{A}_{\mathrm{disc}}(G) \simeq \widehat{\bigoplus_{\pi \in \Pi(G)}} m(\pi)\, \pi \ , \tag{4.3.5}$$

where $m(\pi) \geq 0$ is an integer that is called the *multiplicity of* π. By definition, if $\pi \in \Pi(G)$ and $U \simeq \pi_\infty$, then $\mathrm{m}(\pi)$ is the multiplicity of π_f in the $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module $\mathcal{A}_U(G)$, which is semisimple and of finite dimension. We denote by

$$\Pi_{\mathrm{disc}}(G) \subset \Pi(G)$$

the subsets consisting of the π with $m(\pi) \neq 0$.

The elements of $\Pi_{\mathrm{disc}}(G)$ are called the *discrete automorphic representations*[5] of G. The only truly obvious example of such a representation is the *trivial representation*, denoted 1_G, realized as the subspace (of dimension 1) of constant functions in $\mathcal{A}^2(G)$ (note that μ has finite mass). The action of $G(\mathbb{R})$ in 1_G is, of course, the trivial action, while that of $\mathrm{H}(G)$ is the multiplication by the "degree" (see Example 6.2.3). In general, the set $\Pi_{\mathrm{disc}}(G)$ is countably infinite, which is not the case for $\Pi(G)$. We will give a few concrete examples in the following chapters.

An element $F \in \mathcal{A}_U(G)$ is called an *eigenform* if it is nonzero and generates an irreducible $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module. When $\mathrm{H}(G)$ is commutative, this is equivalent to requiring that $F \neq 0$ be an eigenvector of all Hecke operators in $\mathrm{H}(G)$. If F is an eigenform and $V \subset \mathcal{A}_U(G)$ denotes the $\mathrm{H}(G)^{\mathrm{opp}} \otimes \mathbb{C}$-module generated by F, the image of $U \otimes V$ in $\mathcal{A}_{\mathrm{disc}}(G)$ by the canonical map (4.3.4) is a topologically irreducible subrepresentation of $(G(\mathbb{R}), \mathrm{H}(G))$, which we denote by π_F; it is the (*automorphic, discrete*) *representation generated by* F. We often also denote its isomorphism class by π_F; this is an element of $\Pi_{\mathrm{disc}}(G)$.

[5] The reader should be aware that the definition we use here depends not only on $G_{\mathbb{Q}}$ but also on G as a $\mathbb{Z}$-group. In the literature, our discrete automorphic representations are more commonly called "discrete automorphic representations of $G(\mathbb{A})$ that are spherical (or unramified) with respect to $G(\widehat{\mathbb{Z}})$." The apparent loss of generality in our presentation is, however, at this point illusory, because every open compact subgroup of $G(\mathbb{A}_f)$ is of the form $G'(\widehat{\mathbb{Z}})$ for a well-chosen $\mathbb{Z}$-group G' with $G'_{\mathbb{Q}} \simeq G_{\mathbb{Q}}$.

Finally, following Gelfand, Graev, and Piatetski-Shapiro in [92, Chap. 3, Sect. 7], we consider the subspace $\mathcal{A}_{\mathrm{cusp}}(G) \subset \mathcal{A}^2(G)$ consisting of the *cusp forms* (the definition of a cusp form is recalled below). This is a closed subspace that is stable under the actions of $G(\mathbb{R})$ and $\mathrm{H}(G)$. Gelfand, Graev, and Piatetski-Shapiro show the inclusion

$$\mathcal{A}_{\mathrm{cusp}}(G) \subset \mathcal{A}_{\mathrm{disc}}(G) \tag{4.3.6}$$

(see also [35, Theorem 16.2]). We denote by

$$\Pi_{\mathrm{cusp}}(G) \subset \Pi_{\mathrm{disc}}(G)$$

the set of $\pi \in \Pi(G)$ that occur in the subspace $\mathcal{A}_{\mathrm{cusp}}(G)$; these representations are called the *cuspidal automorphic representations* of G.

When $G_{\mathbb{Q}}$ does not admit a strict parabolic sub-$\mathbb{Q}$-group, which is equivalent to saying that $G(\mathbb{Q})$ does not have any nontrivial unipotent elements, we have the obvious equality $\mathcal{A}_{\mathrm{cusp}}(G) = \mathcal{A}^2(G)$. In this case,[6] the inclusion (4.3.6) implies $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$.

Let us recall the definition of a cusp form. Let $P \subset G_{\mathbb{Q}}$ be a *strict parabolic* sub-$\mathbb{Q}$-group, that is, such that $P(\mathbb{C})$ is connected, contains a Borel subgroup of the neutral component of $G(\mathbb{C})$, and is not equal to that component [103, 34]. If N denotes the unipotent radical of P, then the locally compact group $N(\mathbb{A})$ is unimodular and its subgroup $N(\mathbb{Q})$ is discrete and cocompact. We denote by $\mathrm{d}n$ a strictly positive $\mathrm{N}(\mathbb{A})$-invariant Radion measure on $N(\mathbb{Q})\backslash N(\mathbb{A})$. Let $f\colon G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$ be a Borel function that is square-integrable and take $g \in G(\mathbb{A})$. The function $n \mapsto f(ng)$, $N(\mathbb{Q})\backslash N(\mathbb{A}) \to \mathbb{C}$, is then a square-integrable Borel function for almost all $g \in G(\mathbb{A})$. We say that f is a cusp form if for every strict parabolic sub-$\mathbb{Q}$-group P of $G_{\mathbb{Q}}$, we have $\int_{N(\mathbb{Q})\backslash N(\mathbb{A})} f(ng)\ \mathrm{d}n = 0$ for almost all $g \in N(\mathbb{A})\backslash G(\mathbb{A})$. We can show that the subset of $\mathrm{L}^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mu)$ consisting of the classes of cusp forms is a closed linear subspace (see, for example, [35, Proposition 8.2]). It is trivially stable under right translations by the elements of $G(\mathbb{A})$.

4.4 Automorphic Forms for O_n

4.4.1 Automorphic Forms for the $\mathbb{Z}$-groups G with $G(\mathbb{R})$ Compact

We return to the setting of Sect. 4.3.1. Suppose that the $\mathbb{Z}$-group G has the property that $G(\mathbb{R})$ is compact. Then, the groups $\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$ of formula (4.3.2) are finite subgroups of $G(\mathbb{R})$ because they are discrete subgroups of a compact group. Moreover, the quotient $G(\mathbb{Q})\backslash G(\mathbb{A})$ is compact because it is homeomorphic to the disjoint union of the $\Gamma_i\backslash G(\mathbb{R})$. Formula (4.3.3) then implies $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$,

[6] In fact, a famous result of Godement shows that under this same hypothesis on G, the group $G(\mathbb{Q})$ is cocompact in $G(\mathbb{A})$, which implies the equality $\mathcal{A}_{\mathrm{disc}}(G) = \mathcal{A}^2(G)$ more directly in this specific case (see, for example, [35, Lemma 16.1]).

by the Peter–Weyl theorem. We will give another description of the $\mathrm{H}(G)$-modules $\mathcal{A}_U(G)$.

For a $\mathbb{Z}[G(\mathbb{Q})]$-module U, we denote by $\mathrm{M}_U(G)$ the space of functions

$$F\colon \mathcal{R}(G) \longrightarrow U$$

such that we have $F(\gamma x) = \gamma \cdot F(x)$ for all $\gamma \in G(\mathbb{Q})$ and $x \in \mathcal{R}(G)$. It can be canonically identified with $\mathrm{Hom}_{\mathbb{Z}[G(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(G)], U)$, which endows it with a right action of the ring $\mathrm{H}(G)$. Even better, $U \mapsto \mathrm{M}_U(G)$ defines a functor from the $G(\mathbb{Q})$-modules to the $\mathrm{H}(G)^{\mathrm{opp}}$-modules. Its additive structure is very simple because $F \mapsto (F(g_i))$ induces an isomorphism

$$\mathrm{M}_U(G) \longrightarrow \prod_{i=1}^{\mathrm{h}(G)} U^{\Gamma_i}\ . \tag{4.4.1}$$

In particular, we have $\mathrm{M}_{U\oplus V}(G) \simeq \mathrm{M}_U(G) \oplus \mathrm{M}_V(G)$. Observe, incidentally, that the construction so far makes sense for an arbitrary $\mathbb{Z}$-group G.

Next, assume that U is a finite-dimensional, continuous, complex representation of $G(\mathbb{R})$, and denote its dual by U^*. For $F \in \mathrm{M}_U(G)$ and $u \in U^*$, we denote by $\varphi_F(u)$ the function $G(\mathbb{R}) \times \mathcal{R}(G) \to \mathbb{C}$ defined by $(h, x) \mapsto \langle u, h^{-1}F(x)\rangle$. This function is invariant under the diagonal action of $G(\mathbb{Q})$. This is a continuous function of its first variable; it is therefore in $\mathcal{A}^2(G)$ because $G(\mathbb{Q})\backslash(G(\mathbb{R}) \times \mathcal{R}(G))$ is compact by (4.3.3). The obvious relation $\varphi_F(gu) = g \cdot (\varphi_F(u))$, which holds for $u \in U^*$ and $g \in G(\mathbb{R})$, shows that the function φ_F defined by $u \mapsto \varphi_F(u)$ is an element of $\mathcal{A}_{U^*}(G)$. The proof of the following lemma is immediate and is left to the reader.

Lemma 4.4.2. *Let U be an irreducible representation of $G(\mathbb{R})$. Then $F \mapsto \varphi_F$ is an $\mathrm{H}(G)$-equivariant isomorphism $\mathrm{M}_U(G) \xrightarrow{\sim} \mathcal{A}_{U^*}(G)$.*

Since the article of Gross [98], the elements of $\mathrm{M}_U(G)$ are sometimes called *algebraic modular forms* of weight U for the $\mathbb{Z}$-group G; we will not use this terminology, which conflicts with the notion of algebraicity introduced in Sect. 8.2.6. For example, if $U = \mathbb{C}$ is the trivial representation, then the $\mathrm{H}(G)^{\mathrm{opp}}$-module $\mathrm{M}_{\mathbb{C}}(G)$ can be canonically identified with the space of functions $\mathrm{Cl}(G) \to \mathbb{C}$ or, equivalently, with the dual of the $\mathrm{H}(G)$-module $\mathbb{C}[\mathrm{Cl}(G)]$.

Let us conclude these basic results with an assertion of compatibility with certain morphisms of $\mathbb{Z}$-groups. Let $\mu\colon G \to G'$ be a morphism of $\mathbb{Z}$-groups. It induces, in an obvious way, a morphism (f_μ, g_μ) from the $G(\mathbb{A}_f)$-set $\mathcal{R}(G)$ to the $G'(\mathbb{A}_f)$-set $\mathcal{R}(G')$, in the sense of Sect. 4.2.12. We assume that $f_\mu(G(\mathbb{A}_f))$ is a normal subgroup of $G'(\mathbb{A}_f)$, that g_μ is injective, and, moreover, that the action of the group S defined loc. cit. on $\mathcal{R}(G)$ is trivial. This is, for example, trivially the case if μ is an isomorphism. We then have an injective ring homomorphism $\mathrm{H}(\mu)\colon \mathrm{H}(G) \to \mathrm{H}(G')$ defined loc. cit. Let U' be a $G'(\mathbb{Q})$-module, and let U be its restriction to $G(\mathbb{Q})$. The following lemma paraphrases Lemma 4.2.15.

Lemma 4.4.3. *The morphism* $\mu^* \colon \mathrm{M}_{U'}(G') \longrightarrow \mathrm{M}_U(G)$ *defined by* $\varphi \mapsto (x \mapsto \varphi(g_\mu(x)))$ *satisfies* $T \circ \mu^* = \mu^* \circ \mathrm{H}(\mu)(T)$ *for every* $T \in \mathrm{H}(G)$.

4.4.4 The Case of the Groups O_n and SO_n

Let us now specify this construction for the orthogonal $\mathbb{Z}$-group O_n of the even unimodular lattice $\mathrm{E}_n \subset \mathbb{R}^n$, for $n \equiv 0 \bmod 8$ (Sect. 2.3, choosing another lattice would lead to a theory equivalent to the one we now present).

In this case, we saw in Sect. 4.1.2 that the $\mathrm{O}_n(\mathbb{A}_f)$-set $\mathcal{R}(\mathrm{O}_n)$ can be canonically identified with the set of even unimodular lattices in $\mathbb{R}^n$ contained in $\mathrm{E}_n \otimes \mathbb{Q}$ and that we have $\mathrm{Cl}(\mathrm{O}_n) \xrightarrow{\sim} \mathrm{X}_n$. In particular, we have

$$\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n) = \mathbb{C}[\mathrm{X}_n]^* \ .$$

The right action of $\mathrm{H}(\mathrm{O}_n)$ on $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ defines by transposition a left action of $\mathrm{H}(\mathrm{O}_n)$ on $\mathbb{C}[\mathrm{X}_n]$. In particular, the operator $\mathrm{T}_{\mathbb{Z}/d\mathbb{Z}} \in \mathrm{H}(\mathrm{O}_n)$ defined in Sect. 4.2.6, viewed as an endomorphism of $\mathbb{C}[\mathrm{X}_n]$, is the operator T_d of Sect. 3.2. The description of the structure of the $\mathrm{H}(\mathrm{O}_n)^{\mathrm{opp}}$-module $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ when $n \leq 24$ is therefore the main theme of this book.

The ring $\mathrm{H}(\mathrm{O}_n)$ is commutative by Proposition 4.2.8. Let us fix a (finite-dimensional, continuous, complex) representation U of $\mathrm{O}_n(\mathbb{R})$. By Lemma 4.4.2 and the general results recalled in Sect. 4.3.1, the action of $\mathrm{H}(\mathrm{O}_n)$ is therefore codiagonalizable on each $\mathrm{M}_U(\mathrm{O}_n)$. The eigenvalues of these operators have an important arithmetic meaning. In Corollary 8.2.20, we will see that they are linked, in an a priori rather surprising manner, to the representations of the absolute Galois group of $\mathbb{Q}$. The line of constant functions in $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$ is, for example, trivially stable under T_A for every A, where the eigenvalue of T_p on this line is, of course, $\mathrm{c}_n(p)$ (Proposition-Definition 3.2.1). We will give markedly more interesting examples in the next chapters.

Remark 4.4.5. Let $\mathcal{L}_n$ be the set of all even unimodular lattices in $\mathbb{R}^n$, which we already considered in the introduction (Chap. 1). It contains $\mathcal{R}(\mathrm{O}_n)$ and the natural action of $\mathrm{O}_n(\mathbb{R})$ on $\mathcal{L}_n$ extends the natural action of $\mathrm{O}_n(\mathbb{Q})$ on $\mathcal{R}(\mathrm{O}_n)$. The map $\mathrm{O}_n(\mathbb{R}) \times \mathrm{O}_n(\mathbb{A}_f) \to \mathcal{L}_n$ defined by $(g_\infty, g_f) \mapsto g_\infty^{-1}(g_f(\mathrm{E}_n))$ therefore factors through a map

$$\mathrm{O}_n(\mathbb{Q}) \backslash \mathrm{O}_n(\mathbb{A}) / \mathrm{O}_n(\widehat{\mathbb{Z}}) \to \mathcal{L}_n \ .$$

This is a bijection: the surjectivity follows from Scholium 2.2.1 and the injectivity is immediate.

Let us turn to the case of SO_n. By Proposition 4.1.7 and Sect. 4.2.11, the inclusion $\mathrm{SO}_n \to \mathrm{O}_n$ induces a bijection $\mathcal{R}(\mathrm{SO}_n) \xrightarrow{\sim} \mathcal{R}(\mathrm{O}_n)$ and $\mathrm{H}(\mathrm{O}_n)$ is naturally a subring of $\mathrm{H}(\mathrm{SO}_n)$. Let U be an $\mathrm{SO}_n(\mathbb{Q})$-module, and consider

$$U' = \mathrm{Ind}_{\mathrm{SO}_n(\mathbb{Q})}^{\mathrm{O}_n(\mathbb{Q})} U \ .$$

The universal property of induced modules provides a canonical isomorphism $\mathrm{ind}\colon \mathrm{Hom}_{\mathbb{Z}[\mathrm{SO}_n(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)]_{|\mathrm{SO}_n(\mathbb{Q})}, U) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[\mathrm{O}_n(\mathbb{Q})]}(\mathbb{Z}[\mathcal{R}(\mathrm{O}_n)], U')$, which can also be written as

$$\mathrm{ind}\colon \mathrm{M}_U(\mathrm{SO}_n) \xrightarrow{\sim} \mathrm{M}_{U'}(\mathrm{O}_n)\ .$$

This isomorphism is trivially $\mathrm{H}(\mathrm{O}_n)$-equivariant, so that studying the $\mathrm{H}(\mathrm{O}_n)$-modules $\mathrm{M}_U(\mathrm{SO}_n)$ reduces to studying $\mathrm{M}_W(\mathrm{O}_n)$, where W is an $\mathrm{O}_n(\mathbb{Q})$-module. Let us add that if U is the restriction to $\mathrm{SO}_n(\mathbb{Q})$ of an $\mathrm{SO}_n(\mathbb{R})$-module V and V' denotes the $\mathrm{O}_n(\mathbb{R})$-module induced by V, then we have $V'_{|\mathrm{O}_n(\mathbb{Q})} = \mathrm{Ind}_{\mathrm{SO}_n(\mathbb{Q})}^{\mathrm{O}_n(\mathbb{Q})} U$.

Finally, let W be an $\mathrm{O}_n(\mathbb{Q})$-module, and let W' denote its restriction to $\mathrm{SO}_n(\mathbb{Q})$. The group $\mathrm{O}_n(\mathbb{Q})$ has a natural action on $\mathrm{M}_{W'}(\mathrm{SO}_n)$, by $(\gamma, f) \mapsto (x \mapsto \gamma(f(\gamma^{-1}(x))))$, where the subgroup $\mathrm{SO}_n(\mathbb{Q})$ acts trivially. Let $s \in \mathrm{End}(\mathrm{M}_{W'}(\mathrm{SO}_n))$ be the operator induced by the nontrivial element of the quotient $\mathrm{O}_n(\mathbb{Q})/\mathrm{SO}_n(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. The restriction of the functions via the bijective map $\mathcal{R}(\mathrm{SO}_n) \to \mathcal{R}(\mathrm{O}_n)$ then defines an $\mathrm{H}(\mathrm{O}_n)$-equivariant injection

$$\mathrm{res}\colon \mathrm{M}_W(\mathrm{O}_n) \to \mathrm{M}_{W'}(\mathrm{SO}_n)$$

whose image is $\mathrm{M}_{W'}(\mathrm{SO}_n)^{s=\mathrm{id}}$.

Example 4.4.6. The isomorphism ind induces a canonical decomposition

$$\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_n) \simeq \mathrm{M}_{\mathbb{C}}(\mathrm{O}_n) \oplus \mathrm{M}_{\det}(\mathrm{O}_n)\ ,$$

where $\det$ is the representation of dimension 1 given by the determinant. If we, moreover, view $\mathbb{C}$ as the restriction to $\mathrm{SO}_n(\mathbb{R})$ of the trivial representation of $\mathrm{O}_n(\mathbb{R})$, this endows $\mathrm{M}_{\mathbb{C}}(\mathrm{SO}_n)$ with a symmetry s that preserves the decomposition given above, with fixed points $\mathrm{M}_{\mathbb{C}}(\mathrm{O}_n)$.

We refer to [55, Sect. 2] for a discussion of the spaces $\mathrm{M}_U(\mathrm{SO}_8)$, and in particular their dimension, in terms of the representation U; see also Sect. 7.4 for examples.

4.4.7 An Invariant Hermitian Inner Product

Let us consider the case of a general $\mathbb{Z}$-group G with $G(\mathbb{R})$ compact. Let U be a finite-dimensional, continuous, complex representation of $G(\mathbb{R})$. By transport of structure, the isomorphism $\mathrm{M}_U(G) \xrightarrow{\sim} \mathcal{A}_{U^*}(G)$ endows $\mathrm{M}_U(G)$ with a natural Hermitian inner product, for which the action of $\mathrm{H}(G)$ is a $\star$-action, by Sect. 4.3.1, which we now only need to make explicit. For this, fix a $G(\mathbb{R})$-invariant Hermitian inner product $\langle -, - \rangle_U$ on U. Also choose elements $g_i \in G(\mathbb{A}_f)$ satisfying equality (4.3.2); recall that $\Gamma_i = G(\mathbb{Q}) \cap g_i G(\widehat{\mathbb{Z}}) g_i^{-1}$ is a finite group.

Proposition 4.4.8. *For $F, F' \in \mathrm{M}_U(G)$, the formula*

$$(F|F') = \sum_{i=1}^{\mathrm{h}(G)} \frac{1}{|\Gamma_i|} \langle F(g_i), F'(g_i) \rangle_U$$

defines a Hermitian inner product on $\mathrm{M}_U(G)$ that does not depend on the choice of the g_i and for which the action of $\mathrm{H}(G)$ is a $\star$-action.

We include a proof because we could not find any adequate reference for this result.

Proof. Fix a nonzero $e \in U^*$. By the isomorphism (4.4.2) and Sect. 4.3,

$$(F|F') := \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \overline{\varphi_F(e)} \varphi_{F'}(e) \, \mathrm{d}m$$

is a Hermitian inner product on $\mathrm{M}_U(G)$ for which the action of $\mathrm{H}(G)$ is a $\star$-action. We will verify that it is proportional to the inner product of Proposition 4.4.8.

Let $\Omega_i \subset G(\mathbb{A})$ be the compact open set $g_i(G(\mathbb{R}) \times G(\widehat{\mathbb{Z}}))$, let $\pi \colon G(\mathbb{A}) \to G(\mathbb{Q})\backslash G(\mathbb{A})$ be the canonical projection, and set $\overline{\Omega_i} = \pi(\Omega_i)$. By definition, $G(\mathbb{Q})\backslash G(\mathbb{A})$ is the (finite) disjoint union of the $\overline{\Omega_i}$. Let us first verify that there exists a Haar measure m on $G(\mathbb{A})$ such that for every continuous function ψ on (the compact set) $G(\mathbb{Q})\backslash G(\mathbb{A})$, we have

$$\int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \psi \, \mathrm{d}\mu = \sum_{i=1}^{\mathrm{h}(G)} \frac{1}{|\Gamma_i|} \int_{\Omega_i} \psi \circ \pi \, \mathrm{d}m \, . \tag{4.4.2}$$

Indeed, recall that if f is continuous with compact support on $G(\mathbb{A})$, then $\tilde{f}(g) := \sum_{\gamma \in G(\mathbb{Q})} f(\gamma g)$ is continuous with compact support on $G(\mathbb{Q})\backslash G(\mathbb{A})$. Moreover, by the characteristic property of the quotient measure μ, there exists a unique Haar measure m on $G(\mathbb{A})$ such that for every continuous function f on $G(\mathbb{A})$ with compact support, we have $\int_{G(\mathbb{A})} f \, \mathrm{d}m = \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \tilde{f} \, \mathrm{d}\mu$ (see [211, Chap. II]).

For $g \in G(\mathbb{A})$, set $n_i(g) = |G(\mathbb{Q})g \cap \Omega_i|$. We clearly have $n_i(\gamma g k) = n_i(g)$ for every $\gamma \in G(\mathbb{Q})$ and every $k \in 1 \times G(\widehat{\mathbb{Z}})$. By definition, we also have $n_i(g_j) = |\Gamma_i| \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta. Let ψ be a continuous function on $G(\mathbb{Q})\backslash G(\mathbb{A})$. The function $G(\mathbb{A}) \to \mathbb{C}$ defined by $f_i = 1_{\Omega_i} \times \psi \circ \pi$ is continuous with support in Ω_i and satisfies $\tilde{f}_i(g) = \psi(\pi(g)) \, n_i(g)$ for every $g \in G(\mathbb{A})$ (we denote the characteristic function of the set A by 1_A). In other words, we have $\psi \times 1_{\overline{\Omega_i}} = (1/|\Gamma_i|) \tilde{f}_i$. This proves formula (4.4.2).

Let us apply this formula to the function $\psi = \overline{\varphi_F(e)} \, \varphi_{F'}(e)$. Note that if $U = \mathbb{C}$, so that ψ is constant, equal to $|e(1)|^2 \overline{F(g_i)} F'(g_i)$ on Ω_i, the proposition follows from the fact that $m(\Omega_i) = m(G(\mathbb{R}) \times G(\mathbb{Z}))$ is independent of i. In general, we introduce the Haar measure $\mathrm{d}g$ on $G(\mathbb{R})$ of total mass 1 and the Haar measure m_f on $G(\mathbb{A}_f)$ such that $\mathrm{d}m = \mathrm{d}g \times \mathrm{d}m_f$. The right invariance of ψ under $1 \times G(\widehat{\mathbb{Z}})$

and Fubini's theorem imply

$$\int_{\Omega_i} \psi \circ \pi \, \mathrm{d}m = m_f(G(\widehat{\mathbb{Z}})) \int_{G(\mathbb{R})} \overline{\langle e, g^{-1}F(g_i)\rangle} \langle e, g^{-1}F'(g_i)\rangle \, \mathrm{d}g \ .$$

Let $E \in U$ be such that we have $\langle E, x\rangle_U = \langle e, x\rangle$ for every $x \in U$. The orthogonality relations of the matrix entries for the irreducible representations of the compact groups imply that we have

$$\int_{G(\mathbb{R})} \overline{\langle e, g^{-1}F(g_i)\rangle} \, \langle e, g^{-1}F'(g_i)\rangle \, \mathrm{d}m_\infty = \frac{1}{\dim U} \langle E, E\rangle_U \langle F(g_i), F'(g_i)\rangle_U \ ,$$

which concludes the proof of the proposition. □

Assume, for example, that we have $G = \mathrm{O}_n$ and $U = \mathbb{C}$. If $L_i \in \mathcal{R}^{\mathrm{a}}_{\mathbb{Z}}(\mathrm{E}_n \otimes \mathbb{Q})$ denotes the lattice $g_i(L)$, we have $\Gamma_i = \mathrm{O}(L_i) \subset \mathrm{O}_n(\mathbb{Q})$. The relation $\mathrm{T}_A = \mathrm{T}^{\mathrm{t}}_A$ of Proposition 4.2.8 and Proposition 4.4.8 can then be written as

$$\mathrm{N}_A(L, M)|\mathrm{O}(M)| = \mathrm{N}_A(M, L)|\mathrm{O}(L)| \ ,$$

where $\mathrm{N}_A(L, M)$ denotes the number of A-neighbors of L isometric to M (with $L, M \in \mathcal{R}(\mathrm{O}_n)$). This is the generalization of Proposition 3.2.3 we announced earlier.

Corollary 4.4.9. *The bilinear form on* $\mathrm{M}_{U^*}(G) \times \mathrm{M}_U(G)$ *defined by*

$$(F|F') = \sum_i \frac{1}{|\Gamma_i|} \langle F(g_i), F'(g_i)\rangle$$

is independent of the choice of the g_i *and is nondegenerate. It satisfies the identity* $(T(F)|F') = (F|T^{\mathrm{t}}(F'))$ *for all* $T \in \mathrm{H}(G)$, $F \in \mathrm{M}_{U^*}(G)$, *and* $F' \in \mathrm{M}_U(G)$. *In particular, it defines a canonical isomorphism between the* $\mathrm{H}(G)$*-module* $\mathrm{M}_{U^*}(G)^*$ *and the* $\mathrm{H}(G)$*-module* $\mathrm{M}_U(G)^{\mathrm{t}}$ (*see Remark* 4.2.4).

Proof. For a $\mathbb{C}$-vector space V, we denote by $\overline{V}$ the conjugate $\mathbb{C}$-vector space (that is, the abelian group V endowed with the action $\mathbb{C} \times V \to V$ of $\mathbb{C}$ defined by $(\lambda, v) \mapsto \overline{\lambda}v$). For U as in the corollary, $\overline{U}$ is naturally a representation of $G(\mathbb{R})$ and the map $v \mapsto (u \mapsto \langle v, u\rangle_U)$ induces an isomorphism of representations $\overline{U} \xrightarrow{\sim} U^*$. We therefore have a natural isomorphism $\mathrm{M}_{U^*}(G) \xrightarrow{\sim} \mathrm{M}_{\overline{U}}(G) = \overline{\mathrm{M}_U(G)}$. Via this isomorphism, the bilinear form of the corollary coincides with the form $\overline{\mathrm{M}_U(G)} \times \mathrm{M}_U(G) \to \mathbb{C}$ defined by $(F, F') \mapsto \sum_i (1/|\Gamma_i|)\langle F(g_i), F'(g_i)\rangle_U$, which is none other than the Hermitian form on $\mathrm{M}_U(G)$ given by Proposition 4.4.8. The first two assertions follow; the last is obvious. □

Let us conclude with one last observation. For $L \in \mathcal{R}(G)$ and $u \in U$, the map $F \mapsto \langle F(L), u\rangle$ is a linear form on $\mathrm{M}_{U^*}(G)$, which we denote by $\mathrm{ev}_{L,u}$. We have a unique linear map

$$\mathbb{Z}[\mathcal{R}(G)] \otimes U \to \mathrm{M}_{U^*}(G)^*$$

that sends $[L] \otimes u$ to $\mathrm{ev}_{L,u}$ for every $L \in \mathcal{R}(G)$ and every $u \in U$. The $\mathbb{C}$-vector space $\mathbb{Z}[\mathcal{R}(G)] \otimes U$ is endowed with a diagonal action of $G(\mathbb{Q})$, and the map above is constant on the orbits of this action. It therefore factors through a linear map

$$(\mathbb{Z}[\mathcal{R}(G)] \otimes U)_{G(\mathbb{Q})} \to \mathrm{M}_{U^*}(G)^* \ , \tag{4.4.3}$$

where V_Γ denotes the coinvariants of the Γ-module V. This is an isomorphism: this follows simply from the finiteness of $G(\mathbb{Q})\backslash\mathcal{R}(G)$ and of the natural isomorphism $(U^*)^\Gamma \xrightarrow{\sim} (U_\Gamma)^*$, which holds for every finite subgroup Γ of $G(\mathbb{R})$. The isomorphism (4.4.3) trivially commutes with the natural (left) actions of $\mathrm{H}(G)$. If we compose it with the isomorphism $\mathrm{M}_{U^*}(G)^* \longrightarrow \mathrm{M}_U(G)^{\mathrm{t}}$ given by Corollary 4.4.9, we obtain a canonical isomorphism of $\mathrm{H}(G)$-modules

$$(\mathbb{Z}[\mathcal{R}(G)] \otimes U)_{G(\mathbb{Q})} \xrightarrow{\sim} \mathrm{M}_U(G)^{\mathrm{t}} \ . \tag{4.4.4}$$

It sends (the class of) the element $[L] \otimes u$ to an element of $\mathrm{M}_U(G)$ that we denote by $[L, u]$. Concretely, $[L, u]$ is the unique function $F \in \mathrm{M}_U(G)$ that is zero outside of $G(\mathbb{Q}) \cdot L$ that satisfies $F(L) = \sum_{\gamma\in\Gamma} \gamma(u)$, where $\Gamma = G(\mathbb{Q})_L$ is the stabilizer of L in $G(\mathbb{Q})$. The isomorphism (4.4.4) will play a (small) role in our discussion of the theta series in Sect. 5.4.1 and Chap. 7.

4.5 Siegel Modular Forms

Let us begin by recalling some results on Siegel modular forms (see [5, 45, 46, 88]). We will closely follow the exposition of Van der Geer [89], to which we refer, in particular, for a history of the subject.

4.5.1 The Classical Point of View

Let $g \geq 1$ be an integer. For a ring R, we denote by $\mathrm{Mat}_g(R)$ the set of $g \times g$ matrices with coefficients in R and by $\mathrm{Sym}_g(R) \subset \mathrm{Mat}_g(R)$ the subset of symmetric matrices. We denote by 1_g the identity matrix in $\mathrm{Mat}_g(R)$ and by $\mathrm{J}_{2g} \in \mathrm{Mat}_{2g}(R)$ the element

$$\mathrm{J}_{2g} = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix} \ .$$

The Siegel half-space of genus g is the open subset

$$\mathbb{H}_g \subset \mathrm{Sym}_g(\mathbb{C})$$

of matrices with positive definite imaginary part. We view the $\mathbb{Z}$-group GSp_{2g} as the sub-group scheme of GL_{2g} consisting of the γ with $\gamma\, \mathrm{J}_{2g}\, {}^{\mathrm{t}}\gamma = \nu(\gamma)\mathrm{J}_{2g}$, where

the morphism $\nu\colon \mathrm{GSp}_{2g} \to \mathbb{G}_m$ is the similitude factor. Its elements are of the form

$$\gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}$$

with $a_\gamma, b_\gamma, c_\gamma, d_\gamma \in \mathrm{Mat}_g$ satisfying the relations $a_\gamma\, {}^{\mathrm{t}}b_\gamma = b_\gamma\, {}^{\mathrm{t}}a_\gamma$, $c_\gamma\, {}^{\mathrm{t}}d_\gamma = d_\gamma\, {}^{\mathrm{t}}c_\gamma$, and $a_\gamma\, {}^{\mathrm{t}}d_\gamma - b_\gamma\, {}^{\mathrm{t}}c_\gamma = \nu(\gamma)1_g$.

Let $\mathrm{GSp}_{2g}(\mathbb{R})^+$ be the subgroup of $\mathrm{GSp}_{2g}(\mathbb{R})$ consisting of the elements with strictly positive similitude factor. For $\gamma \in \mathrm{GSp}_{2g}(\mathbb{R})^+$ and $\tau \in \mathbb{H}_g$, we can show that the element $\mathrm{j}(\gamma,\tau) := c_\gamma\tau + d_\gamma$ is in $\mathrm{GL}_g(\mathbb{C})$ and that

$$(\gamma,\tau) \mapsto \gamma\tau = (a_\gamma\tau + b_\gamma)(c_\gamma\tau + d_\gamma)^{-1}$$

defines a transitive action of $\mathrm{GSp}_{2g}(\mathbb{R})^+$ on $\mathbb{H}_g$ by biholomorphic transformations. Moreover, we easily verify the 1-cocyle relation $\mathrm{j}(\gamma\gamma',\tau) = \mathrm{j}(\gamma,\gamma'\tau)\mathrm{j}(\gamma',\tau)$ for all $\gamma,\gamma' \in \mathrm{GSp}_{2g}(\mathbb{R})^+$ and every $\tau \in \mathbb{H}_g$.

Let W be a finite-dimensional $\mathbb{C}$-vector space endowed with a $\mathbb{C}$-representation $\rho\colon \mathrm{GL}_g \to \mathrm{GL}_W$. A *Siegel modular form of weight W and genus $g \geq 1$* is a holomorphic function $f\colon \mathbb{H}_g \to W$ with

$$f(\gamma\tau) = \rho(\,\mathrm{j}(\gamma,\tau)\,)\cdot f(\tau) \quad \forall\tau \in \mathbb{H}_g\ ,\ \forall\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})\ .$$

For $g = 1$, we add the assumption that f is bounded on $\{\tau \in \mathbb{H}_1\,;\, \Im(\tau) > 1\}$. These functions form a $\mathbb{C}$-vector space that we denote by

$$\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))\ ,$$

whose dimension is finite, as shown by Siegel.

When we have $(\rho, W) = (\det^k, \mathbb{C})$ for $k \in \mathbb{Z}$, we speak of *classical*, or scalar-valued *Siegel forms* of weight k; we speak of vector-valued forms otherwise. In the former case, we also denote the space $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ by $\mathrm{M}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$. When $g = 1$, we recover, as a special case, the usual modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$, which are, for example, treated in detail in Serre's book [177]. Finally, note that the presence of the element $-1_{2\mathrm{g}} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ and the relation $\mathrm{j}(-1_{2g},\tau) = -1_g$ imply $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) = 0$ if $\rho(-1_g) = -\mathrm{id}_W$.

Let us conclude this subsection with a reformulation of the notion of a Siegel modular form. Assume that the representation (ρ, W) is irreducible or, more generally, that there exists an element $\mathrm{m}_W \in \mathbb{Z}$, necessarily unique, such that $\rho(z1_g) = z^{\mathrm{m}_W}\,\mathrm{id}_W$ for every $z \in \mathbb{C}^\times$. For a map $f\colon \mathbb{H}_g \to W$, we set

$$f_{|_W}\gamma\colon \mathbb{H}_g \to W\ ,\quad \tau \mapsto\ \nu(\gamma)^{\mathrm{m}_W/2}\ \rho(\mathrm{j}(\gamma,\tau))^{-1}\ f(\gamma\tau)\ .$$

The map $(\gamma, f) \mapsto f_{|_W}\gamma$ defines a right action of the group $\mathrm{GSp}_{2g}(\mathbb{R})^+$ on the space of holomorphic functions $\mathbb{H}_g \to W$; by construction, this action is trivial on the subgroup of homotheties with strictly positive factor in $\mathrm{GSp}_{2g}(\mathbb{R})^+$. A *Siegel modular form of weight W and genus $g \geq 2$* is, by definition, an $\mathrm{Sp}_{2g}(\mathbb{Z})$-invariant element for this action.

4.5.2 Fourier Series Expansions and Cusp Forms

For $n \in \mathrm{Sym}_g(\mathbb{C})$, we set

$$q^n = e^{2i\pi\,\mathrm{tr}(n\,\tau)} = \prod_{1\le i,j\le g} e^{2i\pi\, n_{i,j}\,\tau_{i,j}}\ ;$$

this is a holomorphic function on $\mathbb{H}_g$. If n is *semi-integral*, that is, if $n \in \frac{1}{2}\mathrm{Sym}_g(\mathbb{Z})$, and if $n_{i,i} \in \mathbb{Z}$ for every $i = 1, \ldots, g$, then q^n is invariant under translations by $\mathrm{Sym}_g(\mathbb{Z})$. It can be shown that every $f \in \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ admits a Fourier series expansion, which normally converges on every compact subset of $\mathbb{H}_g$, of the form

$$f = \sum_{n\ge 0} a_n q^n\ ,$$

where the sum is taken over the positive semi-integral elements $n \in \frac{1}{2}\mathrm{Sym}_g(\mathbb{Z})$ (in the sense of real symmetric matrices) and where the a_n are in W [89, Sect. 4]. For $g \ge 2$, the Siegel operator is the map

$$\Phi_g\colon \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \longrightarrow \mathrm{M}_{W'}(\mathrm{Sp}_{2g-2}(\mathbb{Z}))$$

defined by $\Phi_g(\sum_n a_n q^n) = \sum_{n'} a_{n'} q^{n'}$, where we view $\mathrm{Sym}_{g-1}(-)$ as a subset of $\mathrm{Sym}_g(-)$ with last line and column consisting of zeros, and we have $W' = W_{|\mathrm{GL}_{g-1}\times 1}$ [89, Sect. 5]. The subspace of cusp forms is

$$\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) := \mathrm{Ker}(\Phi_g) \subset \mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))\ .$$

A Siegel form is therefore cuspidal if its Fourier series expansion $\sum_n a_n q^n$ satisfies $a_n = 0$ for every n with $\det(n) = 0$. When we have $(W, \rho) = (\mathbb{C}, \det^k)$ for $k \in \mathbb{Z}$, we write $\mathrm{S}_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ for $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$.

4.5.3 The Relation Between $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ and $\mathcal{A}^2(\mathrm{PGSp}_{2g})$

We will now recall the classical link between $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ and the space $\mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$. A nice recent reference on this subject is the article [14], to which we will refer as soon as we can formulate the statement (see also [195, Sect. 5]).

Set $G = \mathrm{PGSp}_{2g}$. The similitude factor $\nu\colon \mathrm{GSp}_{2g} \to \mathbb{G}_m$ induces a homomorphism $\nu_\infty\colon G(\mathbb{R}) \to \mathbb{R}^\times/\mathbb{R}^\times_{>0}$ whose kernel we denote by $G(\mathbb{R})^+$. The canonical morphism $\mathrm{Sp}_{2g}(\mathbb{R}) \to G(\mathbb{R})$ induces an isomorphism

$$\mathrm{Sp}_{2g}(\mathbb{R})/\{\pm 1\} \xrightarrow{\sim} G(\mathbb{R})^+\ .$$

We also set $G(A)^+ = G(A) \cap G(\mathbb{R})^+$ when A is a subring of $\mathbb{R}$.

By Sect. 4.1.2, we have $\mathrm{h}(G) = 1$. Since we have $\nu_\infty(G(\mathbb{Z})) = \{\pm 1\}$, we obtain the equality

$$G(\mathbb{A}) = G(\mathbb{Q})(G(\mathbb{R})^+ \times G(\widehat{\mathbb{Z}})) \tag{4.5.1}$$

and, from (4.3.3), it follows that the restriction $f \mapsto f_{|G^+(\mathbb{R})\times 1}$ induces a $G(\mathbb{R})^+$-equivariant isomorphism

$$\mathcal{A}^2(\mathrm{PGSp}_{2g}) \xrightarrow{\sim} \mathrm{L}^2(G(\mathbb{Z})^+\backslash G(\mathbb{R})^+) \ . \tag{4.5.2}$$

The action of $\mathrm{GSp}_{2g}(\mathbb{R})^+$ on $\mathbb{H}_g$ recalled in Sect. 4.5.1 factors through an action of $G(\mathbb{R})^+$. The latter is faithful and transitive, and its stabilizers are the maximal compact subgroups of $G(\mathbb{R})^+$. If K denotes the stabilizer in $\mathrm{Sp}_{2g}(\mathbb{R})$ of the element $i1_g \in \mathbb{H}_g$ and K^+ denotes its image in $G(\mathbb{R})^+$, we therefore have a natural identification

$$G(\mathbb{R})^+/K^+ \xrightarrow{\sim} \mathbb{H}_g \ .$$

Let (ρ, W) be a $\mathbb{C}$-representation of GL_g as in Sect. 4.5.1, which we now assume to be irreducible and satisfy $\mathrm{m}_W \equiv 0 \bmod 2$. Fix $w \in W^*$ and $f \in \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$; we will associate a function $\varphi_{w,f} \in \mathcal{A}^2(G)$ with w and f. Consider the function $\varphi\colon G(\mathbb{R})^+ \longrightarrow \mathbb{C}$ defined by

$$\varphi(\gamma) = \langle w, (f_{|_W}\gamma)(i1_g)\rangle \ .$$

By construction, φ is continuous and left invariant under $G(\mathbb{Z})^+$. By formula (4.5.1), it is therefore the restriction to $G(\mathbb{R})^+ \times 1$ of a unique continuous function $\varphi'\colon G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$ that is invariant under right translations by $G(\widehat{\mathbb{Z}})$. Set

$$\varphi_{w,f} := \varphi' \ .$$

By Asgari and Schmidt [14, Lemma 5], we have $\varphi_{w,f} \in \mathcal{A}_{\mathrm{cusp}}(G)$.

Before stating the final proposition, we still need to define the notion of a holomorphic element of $\mathcal{A}^2(G)$. Let $\mathfrak{g}$ and $\mathfrak{k}$ be the Lie algebras of $G(\mathbb{R})^+$ and K, respectively, and let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ be the associated Cartan decomposition. Let $d\colon \mathfrak{g} \to \mathrm{T}_{i1_g}$ be the differential in the identity of the map $G(\mathbb{R})^+ \to \mathbb{H}_g$ defined by $h \mapsto h(i1_g)$. It induces an $\mathbb{R}$-linear isomorphism

$$\mathfrak{p} \xrightarrow{\sim} \mathrm{T}_{i1_g} = \mathrm{Sym}_g(\mathbb{C}) \ .$$

The $\mathbb{C}$-vector space structure of $\mathrm{Sym}_g(\mathbb{C})$ therefore endows $\mathfrak{p}$ with the structure of a $\mathbb{C}$-vector space that decomposes $\mathfrak{p} \otimes_{\mathbb{R}} \mathbb{C}$ into $\mathfrak{p}^+ \oplus \mathfrak{p}^-$, so that d induces a $\mathbb{C}$-linear isomorphism $\mathfrak{p}^+ \xrightarrow{\sim} \mathrm{T}_{i1_g}$. An element $f \in \mathcal{A}^2(G)$ is called *holomorphic* if it is continuous and if for every $g \in G(\mathbb{A})$, the function $G(\mathbb{R}) \to \mathbb{C}$ defined by $h \mapsto f(gh)$ is infinitely differentiable and annihilated by $\mathfrak{p}^-$.

Proposition 4.5.4. *The map $(w, f) \mapsto \varphi_{w,f}$ defines a $\mathbb{C}[K]$-linear injection*

$$W^* \otimes \mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z})) \longrightarrow \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$$

whose image is the set of $f \in \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})$ *that are holomorphic and* W^**-isotypical under the action of* K.

Let us make this statement more precise. The map $h \mapsto \mathrm{j}(h, i1_g)$ is a group morphism $K \to \mathrm{GL}_g(\mathbb{C})$ that realizes $\mathrm{GL}_g(\mathbb{C})$ as the complexification of the compact unitary group K. This, in particular, allows us to view W as a representation of K by restriction; it is irreducible because W is so as a representation of GL_g. We refer to [14, Sect. 4.5, Theorem 1] for a proof of this proposition, up to the assertion of surjectivity, which is verified in [195, Sect. 5.2].

4.5.5 The Action of Hecke Operators

It follows from Proposition 4.5.4 that the image of the map in that statement is stable under the action of $\mathrm{H}(\mathrm{PGSp}_{2g})$, so that the space $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$ inherits an action of $\mathrm{H}(\mathrm{PGSp}_{2g})$ from $\mathcal{A}^2(\mathrm{PGSp}_{2g})$. Up to normalization constants sometimes introduced by different authors for integrality reasons, this action coincides with the action traditionally defined on $\mathrm{S}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, and even on $\mathrm{M}_W(\mathrm{Sp}_{2g}(\mathbb{Z}))$, which we recall below (see also [88, Kap. IV], [89, Sect. 16], and [14, Sect. 4.3]). Without going into details, let us mention that is it particularly natural when we view $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ as the space of complex abelian varieties of dimension g endowed with a principal polarization[7] [89, Sect. 10].

Let (W, ρ) be an irreducible $\mathbb{C}$-representation of GL_g, p a prime, and G the $\mathbb{Z}$-group PGSp_{2g}. The natural map

$$a\colon G(\mathbb{Z}[\frac{1}{p}])^+/G(\mathbb{Z})^+ \to G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$$

is bijective because we have $\mathrm{h}(G) = 1$ (Corollary 4.1.5) and $\nu_\infty(G(\mathbb{Z})) = \{\pm 1\}$ (Sect. 4.5.3). It therefore induces, in an obvious way, an injective homomorphism between the ring $\mathrm{H}_p(G)$ and the Hecke ring of the $G(\mathbb{Z}[1/p])^+$-set $G(\mathbb{Z}[1/p])^+/G(\mathbb{Z})^+$. This homomorphism is an isomorphism; this follows from the isomorphism (4.2.1) and the fact that a also induces a bijection

$$G(\mathbb{Z})^+\backslash G(\mathbb{Z}[1/p])^+/G(\mathbb{Z})^+ \to G(\mathbb{Z}_p)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p)\ , \tag{4.5.3}$$

as shown by the theory of elementary divisors (Propositions 4.2.7 and 4.2.9, see also Sect. 6.2.5).

Suppose that the matrix of the element $T \in \mathrm{H}_p(G)$ is the characteristic function of the class set $G(\mathbb{Z}_p)\gamma G(\mathbb{Z}_p)$ with $\gamma \in G(\mathbb{Z}[1/p])^+$, in the sense of the identifica-

[7] A principal polarization on a lattice $L \subset \mathbb{C}^g$ consists of a nondegenerate alternating bilinear form $\eta\colon L \times L \to \mathbb{Z}$ whose extension of scalars $\eta_{\mathbb{R}}$ to $L \otimes \mathbb{R} = \mathbb{C}^g$ satisfies $\eta_{\mathbb{R}}(ix, iy) = \eta_{\mathbb{R}}(x, y)$ for every $x, y \in \mathbb{C}^g$ and whose associated Hermitian form $(x, y) \mapsto \eta_{\mathbb{R}}(ix, y) + i\eta_{\mathbb{R}}(x, y)$ on $\mathbb{C}^g$ is positive definite. Riemann's theory allows us to naturally identify $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathbb{H}_g$ with the set of $\mathrm{GL}_g(\mathbb{C})$-orbits of pairs (L, η), where $L \subset \mathbb{C}^g$ is a lattice and η is a principal polarization on L.

tion (4.2.2). If we write

$$G(\mathbb{Z})^+ \gamma G(\mathbb{Z})^+ = \coprod_i \gamma_i G(\mathbb{Z})^+ ,$$

we immediately see, using formula (4.2.3), that the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{S}_W(\mathrm{Sp}_{2g}) & \longrightarrow & \mathrm{Hom}_K(W, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})) \\ {\scriptstyle f \mapsto \sum_i f_{|_W} \gamma_i^{-1}} \downarrow & & \downarrow {\scriptstyle T} \\ \mathrm{S}_W(\mathrm{Sp}_{2g}) & \longrightarrow & \mathrm{Hom}_K(W, \mathcal{A}_{\mathrm{cusp}}(\mathrm{PGSp}_{2g})) , \end{array} \tag{4.5.4}$$

where the vertical maps are those defined by Proposition 4.5.4 (see [14, Lemma 9] for the details of the argument). Given the equality $T = T^{\mathrm{t}}$ for every $T \in \mathrm{H}(G)$, we will not need to remember the inversion of the γ_i in (4.5.4).

Formula (4.5.4) allows us to determine the link between the Hecke operators considered here and different definitions given in the literature. We will just give the translation of the definitions of Serre [177, Chap. VII, Sects. 2, 5] in the case $g = 1$. We will consider specific cases in genus $g = 2$ in Chap. 9.

Let $k \geq 0$ be an even integer. In [177, Chap. VII, Sect. 5.3], Serre defines, for every integer $n \geq 1$, an endomorphism of $\mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ that he denotes by $\mathrm{T}(n)$ and whose effect on the q-expansions he determines. We also have another endomorphism, given by the action defined above of the operator $\mathrm{T}_A \in \mathrm{H}(\mathrm{PGL}_2)$ introduced in Sect. 4.2.6, where A is a cyclic group. The translation is then as follows:

$$n^{-(k-1)/2} \mathrm{T}(n) = n^{-1/2} \sum_{d^2 | n} \mathrm{T}_{\mathbb{Z}/(n/d^2)\mathbb{Z}} . \tag{4.5.5}$$

This comes, in particular, from the fact that in Serre's book, the correspondence $\mathrm{T}(n)$ sends a lattice to the set of its subgroups of index n rather than the set of those with quotient $\mathbb{Z}/n\mathbb{Z}$.

4.5.6 $\mathcal{A}_{\mathrm{disc}}(\mathrm{Sp}_{2g})$ May Be Deduced from $\mathcal{A}_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$

By restriction of the functions, the morphism $\mathrm{Sp}_{2g}(\mathbb{A}) \to \mathrm{PGSp}_{2g}(\mathbb{A})$ induces an isomorphism

$$\mathrm{Res} \colon \mathcal{A}^2(\mathrm{PGSp}_{2g}) \xrightarrow{\sim} \mathcal{A}^2(\mathrm{Sp}_{2g}) .$$

This follows from formula (4.3.3), taking into account that we have

$$\mathrm{h}(\mathrm{Sp}_{2g}) = \mathrm{h}(\mathrm{PGSp}_{2g}) = 1$$

and that the natural homomorphism $\mathrm{Sp}_{2g}(\mathbb{R}) \to \mathrm{PGSp}_{2g}(\mathbb{R})$ induces a homeomorphism $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathrm{Sp}_{2g}(\mathbb{R}) \xrightarrow{\sim} \mathrm{PGSp}_{2g}(\mathbb{Z})\backslash\mathrm{PGSp}_{2g}(\mathbb{R})$.

Recall that in Sect. 4.2.6, we defined an injective ring homomorphism $\mathrm{H}(\mathrm{Sp}_{2g}) \to \mathrm{H}(\mathrm{PGSp}_{2g})$, which we will from now on view as an inclusion, by a slight abuse of language. The source and target of the morphism Res are therefore both $\mathrm{H}(\mathrm{Sp}_{2g})$-modules.

Proposition 4.5.7. *The map* Res *commutes with the action of* $\mathrm{Sp}_{2g}(\mathbb{R})$ *and that of* $\mathrm{H}(\mathrm{Sp}_{2g})$. *It sends* $\mathcal{A}^2_{\mathrm{disc}}(\mathrm{PGSp}_{2g})$ *onto* $\mathcal{A}^2_{\mathrm{disc}}(\mathrm{Sp}_{2g})$.

Proof. The first assertion is obvious; the second follows from Lemma 4.2.15. The last is a consequence of the first and the fact that the image of $\mathrm{Sp}_{2g}(\mathbb{R})$ in $\mathrm{PGSp}_{2g}(\mathbb{R})$ has finite index (equal to 2). □