Modular Forms and Modular Symbols over Imaginary Quadratic Fields

J. S. Bygott

PhD 1998

Submitted by

Jeremy Stephen Bygott

to the University of Exeter

as a thesis for the degree of

Doctor of Philosophy in Mathematics

in the Faculty of Science

September 1998

I certify that all material in this thesis that is not my own work has been identified and that no material is included for which a degree has previously been conferred upon me.

Jeremy S. Bygott, September 1998

Abstract

The aim of this thesis is to contribute to the understanding of cusp forms over number fields, primarily over imaginary quadratic fields, from both a theoretical and a computational point of view.

There is already a deep theory of automorphic forms over general global fields k which arose out of trying to generalise the classical case $k = \mathbb{Q}$. The sophisticated approach (Jacquet-Langlands theory) is via the representations of the adele group $G_{\mathbb{A}}$ of GL(2); following instead Weil's "elementary" book [Wei71], we define cusp forms of weight two for $\Gamma_0(\mathfrak{n})$ as certain functions on $G_{\mathbb{A}}$. When k has r real embeddings, s pairs of complex embeddings and class number h, the upper half-plane of the classical theory must be replaced by h copies of the product of r upper half-planes and s upper half-spaces; when k is imaginary quadratic, we obtain an especially concrete description, which we work out in detail. In the general theory, Hecke operators are usually introduced via double cosets; in the special case, we can give a "classical" description in terms of lattices.

The main motivation for the work in this thesis comes from the theory of elliptic curves, in which an analogue of the Taniyama-Weil conjecture predicts that every elliptic curve of conductor $\mathfrak{n}$ defined over a number field k should (usually) be attached to a newform at level $\mathfrak{n}$. The existing theory in the classical case is especially rich; in particular, there are good computational techniques for finding newforms and their Hecke eigenvalues, and for determining the associated (strong Weil) curve [Cre97].

Cremona [Cre81] and his student Whitley [Whi90] began the programme of trying to extend these techniques to the case of imaginary quadratic fields, treating the case $h = 1$. This thesis describes an algorithm for determining the space of cusp forms and for computing the eigenforms and eigenvalues for the action of the Hecke algebra on this space in the case $h = 2$. The approach, using modular symbols, closely follows the work of Cremona and Whitley, but new features arise from the presence of a non-trivial class group. The methods presented here suffice for $h = 2$ and probably for an elementary abelian 2-group; the general case remains open but promising. Results from an implementation of the algorithm in the case $k = \mathbb{Q}(\sqrt{-5})$ form part of this thesis.

Contents

List of Figures

List of Tables

Introduction

The aim of this thesis is to contribute to the understanding of cusp forms over number fields, primarily over imaginary quadratic fields, from both a theoretical and a computational point of view.

There is already a deep theory of automorphic forms over general global fields k which arose out of trying to generalise the classical case $k = \mathbb{Q}$. The sophisticated approach (Jacquet-Langlands theory) is via the representations of the adele group $G_{\mathbb{A}}$ of GL(2); following instead Weil's "elementary" book [Wei71], we define cusp forms of weight two for $\Gamma_0(\mathfrak{n})$ as certain functions on $G_{\mathbb{A}}$. It turns out that if k has r real embeddings, s pairs of complex embeddings and class number h, then the upper half-plane of the classical theory should be replaced by h copies of the product of r upper half-planes and s upper half-spaces. When k is an imaginary quadratic field we obtain an especially concrete description, which we work out in much greater detail than [Cre81]. In the general theory, Hecke operators are usually introduced via double cosets; in the special case, we can give a "classical" description in terms of lattices, which is more suited to our purposes.

The main motivation for the work in this thesis comes from the theory of elliptic curves, in which an analogue of the Taniyama-Weil conjecture predicts that every isogeny class of elliptic curves of conductor $\mathfrak{n}$ defined over a number field k should (usually) be attached to a newform at level $\mathfrak{n}$.

The existing theory in the classical case $k = \mathbb{Q}$ is especially rich and by far the best understood; in particular, there are good computational techniques. Tingley [Tin75], Cremona [Cre97] and others have shown how to compute newforms of level N and their Hecke eigenvalues, and how to compute, given such a form f, a modular elliptic curve of conductor N whose L-function is the Mellin transform of f; the curve in a given isogeny class which arises in this way is known as the strong Weil curve, and it is known, by celebrated work of Wiles [Wil95], that every (semistable) elliptic curve is isogenous to a curve arising in this way.

Cremona [Cre81] and his student Whitley [Whi90] began the programme of trying to extend these computations to the case of imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-d})$. The geometrical input into the algorithms goes back to work of Bianchi [Bia92] and Swan [Swa71]; it becomes more complicated as the arithmetic of k becomes more complicated.

The five Euclidean fields, with $d \in \{1, 2, 3, 7, 11\}$, were studied by Cremona [Cre81]. The situation is already much less satisfactory. There are newforms which do not correspond to elliptic curves, but to certain abelian varieties with "extra twist" [Cre92]. Where an elliptic curve with the right conductor and L-series exists, there is no simple construction of it from the newform, although recent deep work of Richard Taylor on l-adic representations [HST93, Tay94] makes progress in this direction. Whitley [Whi90] studied the other fields of class number one, where $d \in \{19, 43, 67, 163\}$.

This thesis describes an algorithm for determining the space of cusp forms and for computing the eigenforms and eigenvalues for the action of the Hecke algebra on this space in the case $h = 2$. The approach, using modular symbols, closely follows the work of Cremona and Whitley, but new features arise from the presence of a non-trivial class group. Using a trick, it is still possible to obtain all the information from just one copy of upper half-space.

The methods presented here suffice for $h = 2$ and probably for an elementary abelian 2-group; the general case remains open, but is a promising area for further work. Results from an implementation of the algorithm in the case $k = \mathbb{Q}(\sqrt{-5})$ form part of this thesis.

Acknowledgement

I would like to thank my supervisor, John Cremona, for suggesting this topic, for all his help and encouragement, and for his patience.

J. S. B.

Chapter 1

Algebraic preliminaries

Roughly speaking, this chapter is about Dedekind domains. We summarise a few facts of module theory that we will need, and go on to discuss congruence subgroups, M-symbols, "normaliser groups" and cusps over Dedekind domains. The early parts are standard results of algebra, the later parts less so. We draw attention to our notation for congruence subgroups, which we find more logical than the many ad hoc conventions in the literature.

1.1 Dedekind domains

Throughout this section, $\mathfrak{O}$ is an arbitrary Dedekind domain with field of fractions k. We begin with two lemmas, which assert the existence of elements with certain properties. We then recall some facts from the theory of finitely generated modules over Dedekind domains; these facts may be found in [FT91, CR62, O'M63]. Lastly, we define lattices in k^r and prove some results about towers of lattices; these results will be needed in Chapter 7.

1.1.1 Two lemmas

The first, well-known lemma is recorded here for later reference.

Lemma 1. *Let $\mathfrak{a}$ be a fractional ideal and $\mathfrak{b}$ an integral ideal of $\mathfrak{O}$. Then there is an integral ideal in the same ideal class as $\mathfrak{a}$ and coprime to $\mathfrak{b}$.*

Proof. In other words, there exists an element $u \in k^\times$ such that $u\mathfrak{a} + \mathfrak{b} = \mathfrak{O}$. For a proof, see [Coh89, Cor.9.6.5]. □

The next lemma, due in this form largely to J. E. Cremona,[1] will be needed in Chapter 7.

Lemma 2. *Let $\mathfrak{n}$ be an integral ideal of $\mathfrak{O}$. For $\beta \in k$, the following are equivalent:*

(i) $\mathfrak{n}^{-1} = \mathfrak{O} + \mathfrak{O}\beta$;

(ii) $\mathfrak{n} = \{\, x \in \mathfrak{O} \mid x\beta \in \mathfrak{O} \,\}$;

(iii) *the map* $\mathfrak{O} \to \mathfrak{n}^{-1}/\mathfrak{O}$, $x \mapsto x\beta \bmod \mathfrak{O}$ *is surjective;*

(iv) *the map* $\mathfrak{O} \to \mathfrak{n}^{-1}/\mathfrak{O}$, $x \mapsto x\beta \bmod \mathfrak{O}$ *has kernel* $\mathfrak{n}$;

(v) *the map* $x \mapsto x\beta$ *induces an isomorphism* $\mathfrak{O}/\mathfrak{n} \to \mathfrak{n}^{-1}/\mathfrak{O}$.

Moreover, there does exist $\beta \in k$ satisfying the conditions; it is unique up to being replaced by $\alpha\beta + \gamma$, with $\alpha, \gamma \in \mathfrak{O}$ and α invertible modulo $\mathfrak{n}$.

Proof. The equivalence of (i) and (ii) follows from

$$(\mathfrak{O} + \mathfrak{O}\beta)^{-1} = \{\, x \in k \mid x(\mathfrak{O} + \mathfrak{O}\beta) \subseteq \mathfrak{O} \,\} = \{\, x \in \mathfrak{O} \mid x\beta \in \mathfrak{O} \,\}.$$

Note that statements (iii), (iv) and (v) implicitly assert that $\beta \in \mathfrak{n}^{-1}$. It is trivial that (i) $\iff$ (iii) and (ii) $\iff$ (iv). Statement (v) is trivially equivalent to (iii) and (iv) together, and hence also to either separately.

Existence of $\beta \in k$ satisfying (i) follows from the so-called "one-and-a-half generator theorem" applied to $1 \in \mathfrak{n}^{-1}$. Suppose that β' also qualifies, so that $\mathfrak{O} + \mathfrak{O}\beta = \mathfrak{O} + \mathfrak{O}\beta'$. Write $\beta' = \alpha\beta + \gamma$ and $\beta = \alpha'\beta' + \gamma'$ for some $\alpha, \alpha', \gamma, \gamma' \in \mathfrak{O}$. Then $(1 - \alpha\alpha')\beta = \alpha'\gamma + \gamma' \in \mathfrak{O}$. By (ii), $1 - \alpha\alpha' \in \mathfrak{n}$, so that α is invertible modulo $\mathfrak{n}$. Conversely, put $\beta' = \alpha\beta + \gamma$ with $\alpha, \gamma \in \mathfrak{O}$ and α invertible modulo $\mathfrak{n}$, say $1 - \alpha\alpha' \in \mathfrak{n}$ with $\alpha' \in \mathfrak{O}$. Clearly $\beta' \in \mathfrak{O} + \mathfrak{O}\beta$. By (ii), $\beta - \beta\alpha\alpha' \in \mathfrak{O}$, whence $\beta - \alpha'(\beta' - \gamma) \in \mathfrak{O}$, showing $\beta \in \mathfrak{O} + \mathfrak{O}\beta'$. □

1.1.2 Torsion modules

Let T be a finitely generated torsion module over $\mathfrak{O}$. Recall that there are proper integral ideals $\mathfrak{a}_i$ such that

$$T \cong \frac{\mathfrak{O}}{\mathfrak{a}_1} \oplus \cdots \oplus \frac{\mathfrak{O}}{\mathfrak{a}_r}. \tag{1.1}$$

[1] personal communication to the author

If we further assume that $\mathfrak{a}_i \supseteq \mathfrak{a}_{i+1}$, then this decomposition is unique up to isomorphism. We define

$$\mathrm{ord}_{\mathfrak{O}}(T) = \prod \mathfrak{a}_i, \tag{1.2}$$

for any decomposition (1.1); when $r = 0$ this is of course the empty product, equal to $\mathfrak{O}$.

Our definition is slightly different from the one given in [FT91], but equivalent. For the definition given there, one has $\mathrm{ord}_{\mathfrak{O}}(\mathfrak{O}/\mathfrak{a}) = \mathfrak{a}$. Together with Proposition 3 below, this implies (1.2). From our point of view, this argument shows that $\mathrm{ord}_{\mathfrak{O}}$ is well defined by (1.2), i.e. independent of the choice of decomposition (1.1). Since $\mathfrak{O}$ will be fixed we shall drop the subscript $\mathfrak{O}$ from the notation, and write simply $\mathrm{ord}(T)$.

Proposition 3. *For any exact sequence* $0 \to T_1 \to T \to T_2 \to 0$ *of finitely generated torsion* $\mathfrak{O}$*-modules,*

$$\mathrm{ord}(T) = \mathrm{ord}(T_1)\,\mathrm{ord}(T_2).$$

Proof. See [FT91, theorem 14]. □

Lemma 4. *Let* T *be a finitely generated torsion module, and let* $\mathfrak{a} = \mathrm{ord}(T)$*. Then* $\mathfrak{a}$ *annihilates* T*. For* $\mathfrak{b}$ *an integral ideal,* $T = \mathfrak{b}T$ *if and only if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime.*

Proof. We have a decomposition (1.1) with $\mathfrak{a} = \prod \mathfrak{a}_i$, so the first statement is obvious. Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. Then $T = (\mathfrak{a} + \mathfrak{b})T = \mathfrak{b}T$. Conversely, assume $T = \mathfrak{b}T$ and let $\mathfrak{p}$ be a prime dividing $\mathfrak{a} + \mathfrak{b}$. Then $T = \mathfrak{p}T$. But $\mathfrak{p}$ divides $\mathfrak{a}_1$, say, and $\mathfrak{p}(\mathfrak{O}/\mathfrak{a}_1) \subsetneq \mathfrak{O}/\mathfrak{a}_1$, a contradiction. So $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. □

1.1.3 Torsion-free modules

Let M be a non-zero finitely generated torsion-free $\mathfrak{O}$-module. By standard structure theory,

$$M \cong \mathfrak{O}^{r-1} \oplus \mathfrak{b} \tag{1.3}$$

where r is the rank of M, and the ideal class $cl(\mathfrak{b})$ of $\mathfrak{b}$ is uniquely determined, whilst $\mathfrak{b}$ may be any ideal in that class. We call $cl(\mathfrak{b})$ the *Steinitz class* of M, and write

$$cl(M) = cl(\mathfrak{b}).$$

A special case of (1.3), usually used in its proof, is that for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$,

$$\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{O} \oplus \mathfrak{a}\mathfrak{b}. \tag{1.4}$$

Theorem 5 (Invariant factor theorem). *Let $N \subseteq M$ be finitely generated torsion-free $\mathfrak{O}$-modules of the same rank r. Then there exist elements $m_1, \ldots, m_r \in M$, integral ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ and fractional ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ such that $\mathfrak{a}_i \supseteq \mathfrak{a}_{i+1}$ for $1 \leq i < r$ and*

$$M = \mathfrak{b}_1 m_1 \oplus \cdots \oplus \mathfrak{b}_r m_r, \qquad N = \mathfrak{a}_1\mathfrak{b}_1 m_1 \oplus \cdots \oplus \mathfrak{a}_r\mathfrak{b}_r m_r.$$

The ideals $\mathfrak{a}_i$ are uniquely determined by the inclusion $N \subseteq M$ and are called the invariant factors *of N in M.*

Proof. See [CR62, theorem 22.12] or [O'M63, theorem 81:11]. □

Corollary 6. *Let $N \subseteq M$ be finitely generated torsion-free $\mathfrak{O}$-modules of the same rank r. Then M/N is a finitely-generated torsion module and*

$$cl(N) = cl(M)cl\big(\mathrm{ord}(M/N)\big).$$

Proof. By (1.4) and with notation as in Theorem 5, $cl(M) = cl\big(\prod \mathfrak{b}_i\big)$ and $cl(N) = cl\big(\prod(\mathfrak{a}_i\mathfrak{b}_i)\big)$, whilst $M/N \cong \prod(\mathfrak{O}/\mathfrak{a}_i)$, so $\mathrm{ord}(M/N) = \prod \mathfrak{a}_i$. □

The last result in this section is due to Swan [Swa71, Proposition 3.10] and will be used in the proof of Lemma 39.

Proposition 7. *Let M be a finitely generated torsion-free $\mathfrak{O}$-module of rank r. Let $a_1, \ldots, a_s$ and $b_1, \ldots, b_s$ be generating sets for M with $s > r$. Then there is some $(c_{ij}) \in \mathrm{SL}(s, \mathfrak{O})$ with $a_i = \sum c_{ij} b_j$.*

Contrast the case $s = r$ (of course, generating sets with r elements exist if and only if M is free). In this case, there is a unique matrix $(c_{ij}) \in \mathrm{GL}(r, \mathfrak{O})$ satisfying $a_i = \sum c_{ij} b_j$. The matrix need not lie in $\mathrm{SL}(r, \mathfrak{O})$; indeed, every element of $\mathrm{GL}(r, \mathfrak{O})$ can arise.

Proof. We give an expanded version of Swan's proof.[2] The (a_i),(b_i) give maps $a, b \colon \mathfrak{O}^s \to M$ with respective kernels A and B, say. Consider the short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathfrak{O}^s & \xrightarrow{a} & M & \longrightarrow & 0 \\ 0 & \longrightarrow & B & \longrightarrow & \mathfrak{O}^s & \xrightarrow{b} & M & \longrightarrow & 0. \end{array} \tag{1.5}$$

[2] It is necessary to choose the various isomorphisms carefully, or diagram (1.8) need not commute.

We shall exhibit a family of isomorphisms $\theta_u : \mathfrak{O}^s \to \mathfrak{O}^s$ indexed by $u \in \mathfrak{O}^\times$ and satisfying (i) $a = b \circ \theta_u$ and (ii) $\det \theta_u = u \det \theta_1$. Being an isomorphism, each θ_u is given by a matrix in $\mathrm{GL}(s, \mathfrak{O})$, and by (ii) we can choose $u = (\det \theta_1)^{-1}$ such that $\det \theta_u = 1$. Then the matrix (c_{ij}) representing θ_u lies in $\mathrm{SL}(s, \mathfrak{O})$, and by (i), satisfies $a_i = \sum c_{ij} b_j$.

Since M is finitely generated and torsion-free, it is projective (see e.g. Prop. 9.6.6 of [Coh89]), so the sequences (1.5) split, and

$$\mathfrak{O}^s = A \oplus M' = B \oplus M'', \tag{1.6}$$

where M' and M'' are submodules of $\mathfrak{O}^s$ such that $a|_{M'} : M' \to M$ and $b|_{M''} : M'' \to M$ are isomorphisms. By structure theory there is an isomorphism $\mu : M \to \mathfrak{m} \oplus E$, where E is free (of rank $r-1$) and $\mathfrak{m}$ is a fractional ideal of $\mathfrak{O}$. By (1.4) and (1.6), there are isomorphisms

$$\alpha : A \to F \oplus \mathfrak{a}, \qquad \beta : B \to F \oplus \mathfrak{a},$$

where F is free (of rank $s-r-1$) and $\mathfrak{a} = \mathfrak{m}^{-1}$. The isomorphism $\theta_u : \mathfrak{O}^s \to \mathfrak{O}^s$ is defined to be the composite map $\big(\beta^{-1} \circ (1_F \oplus u) \circ \alpha\big) \oplus \big((b|_{M''})^{-1} \circ a|_{M'}\big)$, as shown in (1.7) below, where u denotes multiplication by the unit u.

$$\begin{array}{ccc}
A & \bigoplus & M' \\
\alpha \big\downarrow & & \big\downarrow \mu \circ (a|_{M'}) \\
F \oplus \mathfrak{a} & \bigoplus & \mathfrak{m} \oplus E \\
\big\| \quad \big\downarrow u & & \big\| \\
F \oplus \mathfrak{a} & \bigoplus & \mathfrak{m} \oplus E \\
\beta^{-1} \big\downarrow & & \big\downarrow (b|_{M''})^{-1} \circ \mu^{-1} \\
B & \bigoplus & M''
\end{array} \tag{1.7}$$

It is now clear that (i) holds, so there is a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & \mathfrak{O}^s & \xrightarrow{a} & M & \longrightarrow & 0 \\
 & & \big\downarrow \theta_u|_A & & \big\downarrow \theta_u & & \big\downarrow 1 & & \\
0 & \longrightarrow & B & \longrightarrow & \mathfrak{O}^s & \xrightarrow{b} & M & \longrightarrow & 0.
\end{array} \tag{1.8}$$

Let $\mathfrak{a} = \langle x_1, x_2 \rangle$, say. Since $\mathfrak{a}\mathfrak{m} = \mathfrak{O}$ there are $y_1, y_2 \in \mathfrak{m}$ such that $x_1 y_2 - x_2 y_1 = 1$, i.e. $\det P = 1$ where $P = \left(\begin{smallmatrix} x_1 & y_1 \\ x_2 & y_2 \end{smallmatrix}\right)$. The $\mathfrak{O}$-linear map $\psi : \mathfrak{O}^2 \to \mathfrak{a} \oplus \mathfrak{m}$ defined by $(1,0) \mapsto x_1 \oplus y_1$,

$(0,1) \mapsto x_2 \oplus y_2$ has inverse $x \oplus y \mapsto (xy_2 - yx_2, yx_1 - xy_1)$ and is therefore an isomorphism. Formally, ψ may be viewed as right-multiplication by the matrix P.

Let Θ be the matrix representing θ_u with respect to the standard basis of $\mathfrak{O}^s$. For every pair of $\mathfrak{O}$-bases for the free module $F \oplus \mathfrak{a} \oplus \mathfrak{m} \oplus E$, the factorisation of θ_u in (1.7) above leads to a corresponding expression of Θ as the product of three matrices representing the composed maps with respect to the bases involved. Thus $\det \Theta$ is the product of three determinants, of which only the middle one depends on u; we show it to be proportional to u, thereby proving (ii).

Take a basis for $F \oplus \mathfrak{a} \oplus \mathfrak{m} \oplus E$ built from a basis for F, the basis $x_1 \oplus y_1, x_2 \oplus y_2$ for $\mathfrak{a} \oplus \mathfrak{m}$ and a basis for E. With respect to this basis, the middle map has matrix

$$\Theta' = \begin{pmatrix} 1_{s-r-1} & 0 & 0 \\ 0 & T & 0 \\ 0 & 0 & 1_{r-1} \end{pmatrix},$$

where T represents the map

$$\begin{aligned} (1,0) &\overset{\psi}{\longmapsto} x_1 \oplus y_1 \longmapsto ux_1 \oplus y_1 \longmapsto \psi^{-1}(ux_1 \oplus y_1) \\ (0,1) &\overset{\psi}{\longmapsto} x_2 \oplus y_2 \longmapsto ux_2 \oplus y_2 \longmapsto \psi^{-1}(ux_2 \oplus y_2) \end{aligned}$$

and therefore $T = P\left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)P^{-1}$. Thus $\det \Theta' = \det T = u$, as required. □

1.1.4 Lattices in k^r

Again, let M be a non-zero, finitely generated torsion-free $\mathfrak{O}$-module. By [FT91, Chap.II (4.1)], we may view M as contained in a finite-dimensional k-vector space E, with M containing a basis of E. Moreover, there exist free $\mathfrak{O}$-modules F, F', both spanning E, with $F' \subseteq M \subseteq F$. Such a module M is called an $\mathfrak{O}$-*lattice* on E; following O'Meara [O'M63] we say "on E" rather than "in E" to emphasise that M has full rank.[3]

For the moment, we regard $E = k^r$ as fixed. By a *lattice of rank* r, or simply a *lattice*, we mean an $\mathfrak{O}$-lattice Λ on k^r, that is, a finitely generated $\mathfrak{O}$-submodule of k^r whose rank is r.

[3] A lattice "in E" is a lattice "on" some vector subspace of E; thus $\mathbb{R}$ is an $\mathbb{R}$-lattice in $\mathbb{C}$ but not on $\mathbb{C}$.

If $\Lambda \supseteq \Lambda'$ are lattices, then by Corollary 6,

$$cl(\Lambda') = cl(\Lambda)cl\big(\mathrm{ord}(\Lambda/\Lambda')\big). \tag{1.9}$$

In particular, if Λ is free then Λ' is also free if and only if $\mathrm{ord}(\Lambda/\Lambda')$ is a principal ideal. This will be important later.[4]

Lemma 8. *Let Λ be a lattice of rank r, and $\mathfrak{a}$ an integral ideal. Then*

$$\Lambda/\mathfrak{a}\Lambda \cong (\mathfrak{O}/\mathfrak{a})^r.$$

Proof. By (1.3) we have $\Lambda \cong \mathfrak{O}^{r-1} \oplus \mathfrak{b}$ for some integral ideal $\mathfrak{b}$. Since only the ideal class of $\mathfrak{b}$ is determined, we may choose $\mathfrak{b}$ to be prime to $\mathfrak{a}$. For any $\mathfrak{O}$-module M, $M/\mathfrak{a}M \cong M \otimes_{\mathfrak{O}} (\mathfrak{O}/\mathfrak{a})$. Therefore

$$\Lambda/\mathfrak{a}\Lambda \cong (\mathfrak{O}^{r-1} \oplus \mathfrak{b}) \otimes_{\mathfrak{O}} (\mathfrak{O}/\mathfrak{a}) \cong (\mathfrak{O}/\mathfrak{a})^{r-1} \oplus \mathfrak{b}/\mathfrak{a}\mathfrak{b}.$$

But $\mathfrak{b}/\mathfrak{a}\mathfrak{b} = \mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b}) \cong (\mathfrak{a} + \mathfrak{b})/\mathfrak{a} = \mathfrak{O}/\mathfrak{a}$. □

Corollary 9. $\mathrm{ord}(\Lambda/\mathfrak{a}\Lambda) = \mathfrak{a}^r$.

Lemma 10 ("Tower Law"). *Let $\Lambda \supseteq \Lambda' \supseteq \Lambda''$ be a tower of lattices. Then*

$$\mathrm{ord}(\Lambda/\Lambda'') = \mathrm{ord}(\Lambda/\Lambda')\,\mathrm{ord}(\Lambda'/\Lambda'').$$

Proof. Apply Proposition 3 to the exact sequence

$$0 \to \Lambda'/\Lambda'' \to \Lambda/\Lambda'' \to \Lambda/\Lambda' \to 0.$$

□

Lemma 11. *Let $\Lambda \supseteq \Lambda''$ be lattices with $\mathrm{ord}(\Lambda/\Lambda'') = \mathfrak{a}\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. Then there is a unique intermediate lattice Λ' for which $\mathrm{ord}(\Lambda'/\Lambda'') = \mathfrak{a}$. It is given by $\Lambda' = \Lambda'' + \mathfrak{b}\Lambda$.*

[4] It accounts for the special rôle of the Hecke operators $T_{\mathfrak{p}}$ for *principal* prime ideals $\mathfrak{p}$; see §7.5.

Proof. By (1.1) and the Chinese Remainder Theorem, we can write $\Lambda/\Lambda'' \cong M_1 \oplus M_2$, where $\mathrm{ord}(M_1) = \mathfrak{a}$ and $\mathrm{ord}(M_2) = \mathfrak{b}$. Then

$$(\Lambda'' + \mathfrak{b}\Lambda)/\Lambda'' = \mathfrak{b}(\Lambda/\Lambda'') \cong \mathfrak{b}(M_1 \oplus M_2) = \mathfrak{b}M_1 = M_1,$$

by Lemma 4, so that

$$\mathrm{ord}\big((\Lambda'' + \mathfrak{b}\Lambda)/\Lambda''\big) = \mathrm{ord}(M_1) = \mathfrak{a}. \tag{1.10}$$

To show uniqueness, suppose now that $\Lambda'' \subseteq \Lambda' \subseteq \Lambda$ with $\mathrm{ord}(\Lambda'/\Lambda'') = \mathfrak{a}$. By the tower law, $\mathrm{ord}(\Lambda/\Lambda') = \mathfrak{b}$, whence $\Lambda' \supseteq \Lambda'' + \mathfrak{b}\Lambda \supseteq \Lambda''$. Now from (1.10) and the tower law, we deduce $\Lambda' = \Lambda'' + \mathfrak{b}\Lambda$. □

We isolate the following useful fact as a lemma.

Lemma 12. *Let $\Lambda \supseteq \Lambda''$ be lattices, and $\mathfrak{p}$ an ideal with $\mathfrak{p} \mid \mathrm{ord}(\Lambda/\Lambda'')$. Then $\Lambda''+\mathfrak{p}\Lambda \subsetneqq \Lambda$.*

Proof. $(\Lambda'' + \mathfrak{p}\Lambda)/\Lambda'' = \mathfrak{p}(\Lambda/\Lambda'') \subsetneqq \Lambda/\Lambda''$ by Lemma 4 and the hypothesis on $\mathrm{ord}(\Lambda/\Lambda'')$. The conclusion follows. □

Our final result in this section applies only to lattices of rank 2. The general case is more complicated, but we shall not need it.

Lemma 13. *Let $\Lambda \supseteq \Lambda''$ be lattices of rank 2 with $\mathrm{ord}(\Lambda/\Lambda'') = \mathfrak{p}^n$, where $\mathfrak{p}$ is prime and $n \geq 2$. Assume that $\Lambda'' \nsubseteq \mathfrak{p}\Lambda$.*

Then there is a unique intermediate lattice Λ' for which $\mathrm{ord}(\Lambda/\Lambda') = \mathfrak{p}$. It is given by $\Lambda' = \Lambda'' + \mathfrak{p}\Lambda$.

Proof. We have $\mathfrak{p}\Lambda \subsetneqq \Lambda'' + \mathfrak{p}\Lambda \subsetneqq \Lambda$, where the second inequality follows from Lemma 12. But $\mathrm{ord}(\Lambda/\mathfrak{p}\Lambda) = \mathfrak{p}^2$, by Corollary 9. Using the tower law, we deduce

$$\mathrm{ord}\big(\Lambda/(\Lambda'' + \mathfrak{p}\Lambda)\big) = \mathrm{ord}\big((\Lambda'' + \mathfrak{p}\Lambda)/\mathfrak{p}\Lambda\big) = \mathfrak{p}.$$

So $\Lambda' = \Lambda'' + \mathfrak{p}\Lambda$ has the required properties. It really is intermediate between Λ'' and Λ because $n \geq 2$.

Now let Λ' be a lattice with the required properties, i.e. $\Lambda'' \subseteq \Lambda' \subseteq \Lambda$ and $\mathrm{ord}(\Lambda/\Lambda') = \mathfrak{p}$. Then $\mathfrak{p}\Lambda \subseteq \Lambda' \subseteq \Lambda$. Comparing towers, we find $\mathrm{ord}(\Lambda'/\mathfrak{p}\Lambda) = \mathrm{ord}\big((\Lambda'' + \mathfrak{p}\Lambda)/\mathfrak{p}\Lambda\big)$. But $\Lambda' \supseteq \Lambda'' + \mathfrak{p}\Lambda \supseteq \mathfrak{p}\Lambda$ is a tower. Therefore $\Lambda' = \Lambda'' + \mathfrak{p}\Lambda$, proving uniqueness. □

Remark. The hypothesis on the rank cannot be omitted. Consider the case of rank 3. Let $\Lambda = \mathfrak{O} \oplus \mathfrak{O} \oplus \mathfrak{O}$. Then $\mathfrak{p}\Lambda = \mathfrak{p} \oplus \mathfrak{p} \oplus \mathfrak{p}$. Let $\Lambda'' = \mathfrak{O} \oplus \mathfrak{p} \oplus \mathfrak{p}$, so $\operatorname{ord}(\Lambda/\Lambda'') = \mathfrak{p}^2$. Then there are several lattices Λ' with $\Lambda \supseteq \Lambda' \supseteq \Lambda''$ and $\operatorname{ord}(\Lambda/\Lambda') = \mathfrak{p}$, for example, $\mathfrak{O} \oplus \mathfrak{O} \oplus \mathfrak{p}$ and $\mathfrak{O} \oplus \mathfrak{p} \oplus \mathfrak{O}$. In fact, the set of such lattices Λ' is in bijection with $\mathbb{P}^1(\mathfrak{O}/\mathfrak{p})$, as is easily seen.

1.2 Congruence subgroups

In this section, we introduce notation for a number of groups. We need to distinguish clearly between subgroups of GL and subgroups of SL, and between a group and its projectivisation; we achieve this clarity by extending the use of the prefixes S and P to congruence subgroups.

Warning. The notation varies in the literature. For example, [Cre84] has $\tilde{\Gamma}$ and Γ where we write Γ and $\mathrm{S}\Gamma$; [Cre81] has $\Delta_0(\mathfrak{n})$ and $\overline{\Delta_0(\mathfrak{n})}$ where we write $\mathrm{S}\Gamma_0(\mathfrak{n})$ and $\mathrm{PS}\Gamma_0(\mathfrak{n})$, whilst [Fig95] writes $\Gamma_1(\mathfrak{n})$ for two different groups, one of which is our $\mathrm{P}\Gamma_1(\mathfrak{n})$. The group we denote by $\mathrm{PS}\Gamma_0(N)$ is $\overline{\Gamma_0(N)}$ in [Kob84, Swi92] but plain $\Gamma_0(N)$ in [Cre97].

1.2.1 Subgroups of $\mathrm{GL}(2, \mathfrak{O})$

Let $\mathfrak{O}$ be a commutative ring with identity and $\mathfrak{n}$ an ideal of $\mathfrak{O}$. We define a number of groups as follows.

$$\begin{aligned}
\Gamma &= \mathrm{GL}(2, \mathfrak{O}), \\
\Gamma_0(\mathfrak{n}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \in \mathfrak{n} \right\}, \\
\Gamma_1(\mathfrak{n}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{n}) \;\middle|\; d - 1 \in \mathfrak{n} \right\}, \\
\Gamma_1^1(\mathfrak{n}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(\mathfrak{n}) \;\middle|\; a - 1 \in \mathfrak{n} \right\}, \\
\Gamma(\mathfrak{n}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1^1(\mathfrak{n}) \;\middle|\; b \in \mathfrak{n} \right\}.
\end{aligned}$$

Subgroups of Γ containing $\Gamma(\mathfrak{n})$, for example those above, are called *congruence subgroups* of *level* $\mathfrak{n}$; the group $\Gamma(\mathfrak{n})$ itself is called the "principal congruence subgroup" of level $\mathfrak{n}$. In general, a *congruence subgroup* is one containing $\Gamma(\mathfrak{n})$ for some $\mathfrak{n} \neq 0$. Clearly $\Gamma = \Gamma(\mathfrak{O})$, and if $\mathfrak{n} \subseteq \mathfrak{n}'$, then

$$\Gamma(\mathfrak{n}) \subseteq \Gamma(\mathfrak{n}'), \qquad \Gamma_1^1(\mathfrak{n}) \subseteq \Gamma_1^1(\mathfrak{n}'), \qquad \Gamma_1(\mathfrak{n}) \subseteq \Gamma_1(\mathfrak{n}'), \qquad \Gamma_0(\mathfrak{n}) \subseteq \Gamma_0(\mathfrak{n}').$$

We shall have no cause to consider the groups

$$\Gamma^0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; b \in \mathfrak{n} \right\},$$
$$\Gamma^1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(\mathfrak{n}) \;\middle|\; a - 1 \in \mathfrak{n} \right\};$$

note that they are conjugate to $\Gamma_0(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$ respectively, since with $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$,

$$\Gamma^0(\mathfrak{n}) = S^{-1}\Gamma_0(\mathfrak{n})S, \qquad \Gamma^1(\mathfrak{n}) = S^{-1}\Gamma_1(\mathfrak{n})S.$$

For each of the groups above, we use the prefix S (in roman type) to denote the subgroup consisting of elements of determinant 1; thus

$$\mathrm{S}\Gamma = \mathrm{SL}(2, \mathfrak{O}),$$
$$\mathrm{S}\Gamma_0(\mathfrak{n}) = \Gamma_0(\mathfrak{n}) \cap \mathrm{S}\Gamma,$$
$$\mathrm{S}\Gamma_1(\mathfrak{n}) = \Gamma_1(\mathfrak{n}) \cap \mathrm{S}\Gamma,$$
$$\mathrm{S}\Gamma_1^1(\mathfrak{n}) = \Gamma_1^1(\mathfrak{n}) \cap \mathrm{S}\Gamma,$$
$$\mathrm{S}\Gamma(\mathfrak{n}) = \Gamma(\mathfrak{n}) \cap \mathrm{S}\Gamma.$$

Congruence subgroups of $\mathrm{S}\Gamma$ are subgroups containing $\mathrm{S}\Gamma(\mathfrak{n})$ for some $\mathfrak{n} \neq 0$. Clearly,

$$\mathrm{S}\Gamma_1^1(\mathfrak{n}) = \mathrm{S}\Gamma_1(\mathfrak{n}).$$

The relationships between the various groups introduced above are made clearer by the following lemma.

Lemma 14. *Let $\phi\colon \mathfrak{O}^\times \to (\mathfrak{O}/\mathfrak{n})^\times$ be the natural map. Then there is a commutative diagram*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{S}\Gamma & \longrightarrow & \Gamma & \xrightarrow{\det} & \mathfrak{O}^\times & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \Vert & & \\
1 & \longrightarrow & \mathrm{S}\Gamma_0(\mathfrak{n}) & \longrightarrow & \Gamma_0(\mathfrak{n}) & \xrightarrow{\det} & \mathfrak{O}^\times & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \Vert & & \\
1 & \longrightarrow & \mathrm{S}\Gamma_1(\mathfrak{n}) & \longrightarrow & \Gamma_1(\mathfrak{n}) & \xrightarrow{\det} & \mathfrak{O}^\times & \longrightarrow & 1 \\
 & & \Vert & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \mathrm{S}\Gamma_1^1(\mathfrak{n}) & \longrightarrow & \Gamma_1^1(\mathfrak{n}) & \xrightarrow{\det} & \ker\phi & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \Vert & & \\
1 & \longrightarrow & \mathrm{S}\Gamma(\mathfrak{n}) & \longrightarrow & \Gamma(\mathfrak{n}) & \xrightarrow{\det} & \ker\phi & \longrightarrow & 1
\end{array}$$

in which the rows are exact and the vertical arrows denote inclusions.

Proof. The kernel of det on each row is as shown, by definition. To see that det is surjective on each row, let $\epsilon \in \mathfrak{O}^\times$ and $\gamma = \left(\begin{smallmatrix}\epsilon & 0\\ 0 & 1\end{smallmatrix}\right)$. Clearly $\gamma \in \Gamma_1(\mathfrak{n})$; moreover, if $\epsilon \in \ker\phi$, i.e. $\epsilon \equiv 1 \pmod{\mathfrak{n}}$, then $\gamma \in \Gamma(\mathfrak{n})$. This completes the proof. □

Clearly $\Gamma(\mathfrak{n})$ is a normal subgroup of Γ, being the kernel of the natural homomorphism $\mathrm{GL}(2,\mathfrak{O}) \to \mathrm{GL}(2,\mathfrak{O}/\mathfrak{n})$ induced by the functor $\mathrm{GL}(2,-)$ from the map $\mathfrak{O} \to \mathfrak{O}/\mathfrak{n}$. Likewise, $\mathrm{S}\Gamma(\mathfrak{n})$ is normal in $\mathrm{S}\Gamma$. On the other hand, none of $\mathrm{S}\Gamma_1^1(\mathfrak{n}) = \mathrm{S}\Gamma_1(\mathfrak{n})$, $\mathrm{S}\Gamma_0(\mathfrak{n})$, $\Gamma_1^1(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$ and $\Gamma_0(\mathfrak{n})$ is normal in $\mathrm{S}\Gamma$ or Γ (except when $\mathfrak{n} = \mathfrak{O}$) since $S^{-1}TS \notin \Gamma_0(\mathfrak{n})$, where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{S}\Gamma, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{S}\Gamma_1^1(\mathfrak{n}).$$

Although these groups are not normal in Γ or $\mathrm{S}\Gamma$, lemmas 15–17 show that the vertical maps in the three lowest tiers of the diagram *are* inclusions of normal subgroups, with quotients that are easily described.

Lemma 15. *There is a commutative diagram of exact rows*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \Gamma_1(\mathfrak{n}) & \longrightarrow & \Gamma_0(\mathfrak{n}) & \xrightarrow{f} & (\mathfrak{O}/\mathfrak{n})^\times & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \Vert & & \\
1 & \longrightarrow & \mathrm{S}\Gamma_1(\mathfrak{n}) & \longrightarrow & \mathrm{S}\Gamma_0(\mathfrak{n}) & \xrightarrow{f} & (\mathfrak{O}/\mathfrak{n})^\times & \longrightarrow & 1.
\end{array}$$

Proof. The map f is defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \bmod \mathfrak{n}$. It is clearly a homomorphism, with kernels on each row as shown. If $ad \equiv 1 \pmod{\mathfrak{n}}$, for $a, d \in \mathfrak{O}$, then

$$\begin{pmatrix} a & 1 \\ ad-1 & d \end{pmatrix} \in \mathrm{S}\Gamma_0(\mathfrak{n}).$$

So f is surjective on each row, which completes the proof. □

Lemma 16. *With ϕ as above, there is an exact sequence*

$$1 \longrightarrow \Gamma_1^1(\mathfrak{n}) \longrightarrow \Gamma_1(\mathfrak{n}) \xrightarrow{g} \operatorname{im}\phi \longrightarrow 1.$$

Proof. The map g is defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto a \bmod \mathfrak{n} \in (\mathfrak{O}/\mathfrak{n})^\times$. It is clearly a homomorphism with kernel $\Gamma_1^1(\mathfrak{n})$, and its image is contained in $\operatorname{im}\phi$. Given $\bar{\epsilon} \in \operatorname{im}\phi$, write $\bar{\epsilon} = \phi(\epsilon)$ with $\epsilon \in \mathfrak{O}^\times$. Then

$$\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(\mathfrak{n}),$$

so $\operatorname{im} g = \operatorname{im}\phi$. □

Lemma 17. *There is a commutative diagram of exact rows*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma(\mathfrak{n}) & \longrightarrow & \Gamma_1^1(\mathfrak{n}) & \xrightarrow{h} & \mathfrak{O}/\mathfrak{n} & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & \mathrm{S}\Gamma(\mathfrak{n}) & \longrightarrow & \mathrm{S}\Gamma_1^1(\mathfrak{n}) & \xrightarrow{h} & \mathfrak{O}/\mathfrak{n} & \longrightarrow & 1. \end{array}$$

Proof. The map h is defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto b \bmod \mathfrak{n}$. It is clearly a homomorphism, with kernels on each row as shown. Surjectivity is clear, since $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{S}\Gamma_1^1(\mathfrak{n})$ for all $x \in \mathfrak{O}$. This completes the proof. □

1.2.2 Projective groups

For each of the groups above, it is natural to define a "projectivised" group by factoring out the subgroup of scalar matrices; in all the cases of interest, this amounts to factoring out the centre, as Lemma 21 below shows. For each group G, we denote the corresponding projectivised group by $\mathrm{P}G$ (with the prefix P in roman type). Congruence subgroups of $\mathrm{P}\Gamma$ and $\mathrm{PS}\Gamma$ are subgroups containing $\mathrm{P}\Gamma(\mathfrak{n})$ and $\mathrm{PS}\Gamma(\mathfrak{n})$ respectively, for some $\mathfrak{n} \neq 0$.

We will shortly see how various exact sequences of groups induce exact sequences of the corresponding projectivised groups; the general situation is described by the following lemma, which might be described as "abstract nonsense".

Lemma 18. *Let G_1 be a normal subgroup of a group G and write $g\colon G \to G/G_1$ for the natural quotient map. Let $f\colon H \to G$ be an injective group homomorphism such that $f(H)$ is normal in G, and let $H_1 = \{\, h \in H \mid f(h) \in G_1 \,\}$. Then there is a commutative diagram of exact rows and columns:*

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H_1 & \longrightarrow & H & \xrightarrow{gf} & f(H)G_1/G_1 & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle f|_{H_1}} & & \downarrow{\scriptstyle f} & & \downarrow & & \\
1 & \longrightarrow & G_1 & \longrightarrow & G & \xrightarrow{g} & G/G_1 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G_1/f(H_1) & \longrightarrow & G/f(H) & \longrightarrow & G/f(H)G_1 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1. & &
\end{array}
$$

Proof. The image of gf is clearly $f(H)G_1/G_1$, and the kernel of gf is H_1, by definition, so the first row is exact; exactness of the middle row and of the columns follows by the usual isomorphism theorems.

The maps in the bottom row are induced in the obvious way: since $f(H)$ is in the kernel of the composite $G \to G/G_1 \to G/f(H)G_1$, and $f(H_1)$ is in the kernel of the composite $G_1 \to G \to G/f(H)$, these composites factor uniquely through $G/f(H)$ and $G_1/f(H_1)$ respectively. It only remains to verify exactness of the bottom row. This is a pure "diagram chase" in the category of groups; compare [ML71, §VIII.4]. □

We give two examples here, and two more in §1.4; their relevance to modular forms will be seen later.

Lemma 19. *Write $(\mathfrak{O}^\times)^2$ for the subgroup of squares in $\mathfrak{O}^\times$. There is a commutative* *diagram of exact rows and columns:*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathfrak{O}^\times & \xrightarrow{a\mapsto a^2} & (\mathfrak{O}^\times)^2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{S}\Gamma_0(\mathfrak{n}) & \longrightarrow & \Gamma_0(\mathfrak{n}) & \xrightarrow{\det} & \mathfrak{O}^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{PS}\Gamma_0(\mathfrak{n}) & \longrightarrow & \mathrm{P}\Gamma_0(\mathfrak{n}) & \xrightarrow{\det} & \mathfrak{O}^\times/(\mathfrak{O}^\times)^2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1. & &
\end{array}$$

Proof. The scalars in $\Gamma_0(\mathfrak{n})$ are given by $\mathfrak{O}^\times$, diagonally embedded; the scalars in $\mathrm{S}\Gamma_0(\mathfrak{n})$ are clearly $\{\pm 1\}$. The result follows by Lemma 18. □

Lemma 20. *With ϕ as in Lemma 14 and f as in Lemma 15 there is a commutative diagram of exact rows and columns:*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \ker\phi & \longrightarrow & \mathfrak{O}^\times & \xrightarrow{\phi} & \operatorname{im}\phi & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma_1(\mathfrak{n}) & \longrightarrow & \Gamma_0(\mathfrak{n}) & \xrightarrow{f} & (\mathfrak{O}/\mathfrak{n})^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{P}\Gamma_1(\mathfrak{n}) & \longrightarrow & \mathrm{P}\Gamma_0(\mathfrak{n}) & \longrightarrow & (\mathfrak{O}/\mathfrak{n})^\times/\mathfrak{O}^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1. & &
\end{array}$$

Proof. Apply Lemma 18. We remark that exactness of the bottom row, in the case when $\mathfrak{O}$ is a principal ideal domain, occurs as Lemma 7 of [Fig95]. □

We end this section by verifying that, in all the cases considered, projectivising amounts to factoring out the centre.

Lemma 21. *Assume that $\mathfrak{O}$ is an integral domain and that $\mathfrak{n} \neq 0$. Then the centre of each of the groups Γ, $\Gamma_0(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$, $\Gamma_1^1(\mathfrak{n})$, $\Gamma(\mathfrak{n})$, $S\Gamma$, $S\Gamma_0(\mathfrak{n})$, $S\Gamma_1(\mathfrak{n})$ and $S\Gamma(\mathfrak{n})$ is the subgroup of scalar matrices.*

Proof. Let $n \in \mathfrak{n}$ with $n \neq 0$. A central element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ must commute with $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, implying $a = d$ and $c = 0$, and with $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, implying $b = 0$. □

For completeness, we briefly discuss the anomalous case $\mathfrak{n} = 0$, showing that the assumption $\mathfrak{n} \neq 0$ in Lemma 21 may not be dropped. Clearly $\Gamma(0) = S\Gamma(0)$ is just the trivial group. Next, note that $\Gamma_1^1(0) = S\Gamma_1^1(0) = S\Gamma_1(0)$; this group is isomorphic to the additive group of $\mathfrak{O}$ via $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto b$; in particular, the group is abelian, and the centre contains non-scalar matrices.

Next, consider the group $\Gamma_1(0) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathfrak{O}^\times,\ b \in \mathfrak{O} \right\}$. Assume that $\mathfrak{O}^\times$ is not trivial, for otherwise $\Gamma_1(0) = \Gamma_1^1(0)$. If $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ is central, it must commute with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, implying $a = 1$. One now checks that $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ is central if and only if $(a-1)b = 0$ for all $a \in \mathfrak{O}^\times$; since $\mathfrak{O}^\times$ is not trivial by assumption, it follows that the centre of $\Gamma_1(0)$ is trivial.

Next, consider the group $\Gamma_0(0) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, c \in \mathfrak{O}^\times,\ b \in \mathfrak{O} \right\}$. Again, assume that $\mathfrak{O}^\times$ is not trivial, for otherwise $\Gamma_0(0) = \Gamma_1^1(0)$. A central element of $\Gamma_0(0)$ must commute with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so must have the form $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$. It must also commute with $\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for all $\epsilon \in \mathfrak{O}^\times$, implying $(\epsilon - 1)b = 0$ for all $\epsilon \in \mathfrak{O}^\times$. Since $\mathfrak{O}^\times$ is not trivial by assumption, the centre of $\Gamma_0(0)$ consists of scalars.

Lastly, consider $S\Gamma_0(0)$. If $\mathfrak{O}^\times = \{\pm 1\}$, then $S\Gamma_0(0) = \{ \pm\gamma \mid \gamma \in S\Gamma_1(0) \}$; this group is abelian, and contains non-scalar matrices. Assume instead that there is $a \in \mathfrak{O}^\times$ with $a^2 \neq 1$. Since a central element of $S\Gamma_0(0)$ must commute with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$, it follows that the centre is just $\{\pm 1_2\}$, the subgroup of scalar matrices.

1.3 M-symbols

Throughout this section, $\mathfrak{O}$ will be a Dedekind domain and $\mathfrak{n}$ an ideal of $\mathfrak{O}$. M-symbols provide a convenient system of right coset representatives for $S\Gamma_0(\mathfrak{n})$ in $S\Gamma$. They were first introduced by Manin [Man72] in the case $\mathfrak{O} = \mathbb{Z}$, and were named by Cremona [Cre81] who generalised them to principal ideal domains; in this section, we generalise to arbitrary Dedekind domains, showing that all the main properties continue to hold.

Proposition 22. *There is an exact sequence*

$$1 \longrightarrow \mathrm{S}\Gamma(\mathfrak{n}) \longrightarrow \mathrm{SL}(2,\mathfrak{O}) \xrightarrow{f} \mathrm{SL}(2,\mathfrak{O}/\mathfrak{n}) \longrightarrow 1,$$

where f is the natural map reducing each matrix entry modulo $\mathfrak{n}$.

Proof. Our proof is based on the argument given for $\mathfrak{O} = \mathbb{Z}$ in [Swi92]. Trivially, we may assume $0 \neq \mathfrak{n} \neq \mathfrak{O}$. Clearly $\mathrm{S}\Gamma(\mathfrak{n}) = \ker f$, so we need only show that f is surjective. Let $\alpha, \beta, \gamma, \delta \in \mathfrak{O}$ satisfy $\alpha\delta - \beta\gamma \equiv 1 \pmod{\mathfrak{n}}$. We must find $a, b, c, d \in \mathfrak{O}$, congruent modulo $\mathfrak{n}$ to α, β, γ and δ respectively, such that $ad - bc = 1$.

Consider first the special case in which α is coprime to $\mathfrak{n}$, i.e. $\langle\alpha\rangle + \mathfrak{n} = \mathfrak{O}$. By the Chinese Remainder Theorem for pairwise comaximal ideals, we may find $b \in \mathfrak{O}$ such that $b \equiv \beta \pmod{\mathfrak{n}}$ and $b \equiv 1 \pmod{\alpha}$, and $c \in \mathfrak{O}$ such that $c \equiv \gamma \pmod{\mathfrak{n}}$ and $c \equiv -1 \pmod{\alpha}$. We let $a = \alpha$, and observe $1 + bc \equiv 0 \pmod{\alpha}$, i.e. $1 + bc = ad$ for some $d \in \mathfrak{O}$. Then $\alpha d \equiv 1 + \beta\gamma \equiv \alpha\delta \pmod{\mathfrak{n}}$, forcing $d \equiv \delta \pmod{\mathfrak{n}}$, since α is coprime to $\mathfrak{n}$.

We reduce to the special case by showing that we can find λ such that $\alpha + \lambda\gamma$ is coprime to $\mathfrak{n}$. For then the matrix

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha + \lambda\gamma & \beta + \lambda\delta \\ \gamma & \delta \end{pmatrix}$$

is congruent modulo $\mathfrak{n}$ to some $M \in \mathrm{SL}(2,\mathfrak{O})$, so that $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is congruent modulo $\mathfrak{n}$ to the matrix $\left(\begin{smallmatrix} 1 & -\lambda \\ 0 & 1 \end{smallmatrix}\right) M \in \mathrm{SL}(2,\mathfrak{O})$.

Let $\mathfrak{q} = \prod_{\mathfrak{p} \in S} \mathfrak{p}$, where S is the set of primes dividing $\mathfrak{n}$ but not dividing α. Let $\mathfrak{r}$ be an integral ideal coprime to α and in the ideal class inverse to the class of $\mathfrak{q}$; such an $\mathfrak{r}$ exists by Lemma 1. Thus, $\mathfrak{q}\mathfrak{r}$ is principal, equal to $\langle\lambda\rangle$, say. We show that $\alpha + \lambda\gamma$ is coprime to $\mathfrak{n}$ as required.

Let $\mathfrak{p}$ be prime and suppose $\mathfrak{p} \mid \mathfrak{n}$ and $\mathfrak{p} \mid \langle\alpha + \lambda\gamma\rangle$, i.e. $\alpha + \lambda\gamma \in \mathfrak{p}$. If $\mathfrak{p} \mid \mathfrak{q}$, then $\alpha \notin \mathfrak{p}$ but $\lambda \in \mathfrak{q}\mathfrak{r} \subseteq \mathfrak{p}$, a contradiction. So $\mathfrak{p} \nmid \mathfrak{q}$, i.e. $\alpha \in \mathfrak{p}$. But $\langle\alpha\rangle + \mathfrak{r} = \mathfrak{O}$, so $\mathfrak{p} \nmid \mathfrak{q}\mathfrak{r}$. So $\lambda \notin \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\gamma \in \mathfrak{p}$. But this contradicts $\alpha\delta - \beta\gamma - 1 \in \mathfrak{n} \subseteq \mathfrak{p}$. □

The analogous statement with SL(2) replaced by GL(2) is no longer true. Essentially, surjectivity fails because it already fails for GL(1), even when $\mathfrak{O} = \mathbb{Z}$.

Corollary 23. *Let* $\phi\colon \mathfrak{O}^\times \to (\mathfrak{O}/\mathfrak{n})^\times$ *and* $f\colon \mathrm{GL}(2,\mathfrak{O}) \to \mathrm{GL}(2,\mathfrak{O}/\mathfrak{n})$ *be the natural maps induced by* $\mathfrak{O} \to \mathfrak{O}/\mathfrak{n}$. *Then* $\operatorname{im} f = S$, *where*

$$S = \{\, \gamma \in \mathrm{GL}(2,\mathfrak{O}/\mathfrak{n}) \mid \det\gamma \in \operatorname{im}\phi \,\}.$$

Proof. Clearly $\operatorname{im} f \subseteq S$. Conversely, let $\gamma \in S$ be represented by $C \in \mathrm{M}_2(\mathfrak{O})$, say. There is $\epsilon \in \mathfrak{O}^\times$ with $\det C \equiv \epsilon \mod \mathfrak{n}$. Put $C' = C\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. Then $\det C' \equiv 1 \mod \mathfrak{n}$, so by Proposition 22, there is $A' \in \mathrm{SL}(2,\mathfrak{O})$ such that $A' \equiv C' \mod \mathfrak{n}$. Put $A = A'\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathfrak{O})$. Then $f(A) = \gamma$. □

The following lemma is really just a corollary of Proposition 22.

Lemma 24. *Let* $\lambda, \mu \in \mathfrak{O}$ *satisfy* $\langle \lambda, \mu \rangle + \mathfrak{n} = \mathfrak{O}$. *Then there exist* $\lambda', \mu' \in \mathfrak{O}$, *with* $\lambda' \equiv \lambda \pmod{\mathfrak{n}}$ *and* $\mu' \equiv \mu \pmod{\mathfrak{n}}$ *such that* $\langle \lambda', \mu' \rangle = \mathfrak{O}$.

Proof. Write $\alpha\mu - \beta\lambda \equiv 1 \pmod{\mathfrak{n}}$ for some $\alpha, \beta \in \mathfrak{O}$, and lift $\left(\begin{smallmatrix} \alpha & \beta \\ \lambda & \mu \end{smallmatrix}\right)$ to $\mathrm{SL}(2,\mathfrak{O})$ using Proposition 22. □

We record the following refinement: it is possible to take μ' as μ, provided that $\mu \neq 0$. This hypothesis is essential, as is shown by the example $\mathfrak{O} = \mathbb{Z}$, $\mathfrak{n} = \langle 8 \rangle$, $\lambda = 3$, $\mu = 0$.

Lemma 25. *Let* $\lambda, \mu \in \mathfrak{O}$ *satisfy* $\langle \lambda, \mu \rangle + \mathfrak{n} = \mathfrak{O}$. *Assume that* $\mu \neq 0$. *Then there exists* $\lambda' \in \mathfrak{O}$ *such that* $\lambda \equiv \lambda' \pmod{\mathfrak{n}}$ *and* $\langle \lambda', \mu \rangle = \mathfrak{O}$.

Proof. Let $\mathfrak{q} = \prod_{\mathfrak{p} \in S} \mathfrak{p}$ where S is the set of primes $\mathfrak{p}$ with $\mathfrak{p} \mid \mu$ and $\mathfrak{p} \nmid \lambda$; this step requires $\mu \neq 0$. By Lemma 1 there is an integral ideal $\mathfrak{r}$ coprime to λ and in the ideal class inverse to the class of $\mathfrak{n}\mathfrak{q}$. Thus $\mathfrak{r} + \langle \lambda \rangle = \mathfrak{O}$ and $\mathfrak{n}\mathfrak{q}\mathfrak{r} = \langle \beta \rangle$, say. We may take $\lambda' = \lambda + \beta$.

For suppose that $\mathfrak{p}$ is a prime satisfying $\mathfrak{p} \mid \lambda'$ and $\mathfrak{p} \mid \mu$. If $\mathfrak{p} \nmid \lambda$, then $\mathfrak{p} \mid \mathfrak{q}$ (by definition), so $\mathfrak{p} \mid \beta$, whence $\mathfrak{p} \mid \lambda$, a contradiction. On the other hand, if $\mathfrak{p} \mid \lambda$, then $\mathfrak{p} \nmid \mathfrak{q}$ (again by definition), and $\mathfrak{p} \nmid \mathfrak{r}$, but $\mathfrak{p} \mid \beta$. So $\mathfrak{p} \mid \mathfrak{n}$, contradicting the hypothesis. Therefore no such $\mathfrak{p}$ can exist, and so $\langle \lambda', \mu \rangle = \mathfrak{O}$, as required. □

The following lemma is based on [Cre97, Lemma 2.2.1].

Lemma 26. *For $i \in \{1,2\}$, let $\lambda_i, \mu_i \in \mathfrak{O}$ satisfy $\langle \lambda_i, \mu_i \rangle + \mathfrak{n} = \mathfrak{O}$. Then the following are equivalent:*

(a) $\lambda_1\mu_2 \equiv \lambda_2\mu_1 \pmod{\mathfrak{n}}$,

(b) *there exists $u \in \mathfrak{O}$ such that*

(i) $\langle u \rangle + \mathfrak{n} = \mathfrak{O}$ *and*

(ii) $\lambda_1 \equiv u\lambda_2,\ \mu_1 \equiv u\mu_2 \pmod{\mathfrak{n}}$,

(c) *there exists $\bar{u} \in (\mathfrak{O}/\mathfrak{n})^\times$ such that $(\bar{\lambda_1}, \bar{\mu_1}) = \bar{u}(\bar{\lambda_2}, \bar{\mu_2})$.*

Proof. Each of (a), (b) and (c) depends only on the residue classes of the λ_i and μ_i modulo $\mathfrak{n}$, so by Lemma 24, we may assume without loss of generality that $\langle \lambda_i, \mu_i \rangle = \mathfrak{O}$. Clearly (b) and (c) are equivalent.

Assume (a). There are $\alpha_i, \beta_i \in \mathfrak{O}$ such that $\alpha_i\mu_i - \beta_i\lambda_i = 1$. Let $M_i = \begin{pmatrix} \alpha_i & \beta_i \\ \lambda_i & \mu_i \end{pmatrix}$ and define $u, v \in \mathfrak{O}$ by $M_1{M_2}^{-1} = \begin{pmatrix} v & * \\ \lambda_1\mu_2 - \lambda_2\mu_1 & u \end{pmatrix}$. Taking determinants shows that $uv \equiv 1 \pmod{\mathfrak{n}}$, confirming (b)(i), whilst (b)(ii) follows from the bottom row of

$$M_1 = \left(M_1{M_2}^{-1}\right) M_2 \equiv \begin{pmatrix} * & * \\ u\lambda_2 & u\mu_2 \end{pmatrix} \pmod{\mathfrak{n}}.$$

Conversely, (b) implies $\lambda_1\mu_2 \equiv u\lambda_2\mu_2 \equiv \lambda_2\mu_1 \pmod{\mathfrak{n}}$; so (b) implies (a). ☐

On the set of ordered pairs $\lambda, \mu \in \mathfrak{O}^2$ such that $\langle \lambda, \mu \rangle + \mathfrak{n} = \mathfrak{O}$, we now define the relation $\sim$, where

$$(\lambda_1, \mu_1) \sim (\lambda_2, \mu_2) \iff \lambda_1\mu_2 \equiv \lambda_2\mu_1 \pmod{\mathfrak{n}}.$$

This is an equivalence relation, as one sees by an easy direct calculation or yet more simply by using Lemma 26(c), and we can identify the equivalence classes with the elements of $\mathbb{P}^1(\mathfrak{n})$, the projective line over $\mathfrak{O}/\mathfrak{n}$. The equivalence class of (λ, μ) will be denoted $(\lambda : \mu)$, and by tradition [Cre81, Whi90], such symbols will be called *M-symbols modulo* $\mathfrak{n}$, or *M-symbols of level* $\mathfrak{n}$. Notice that the components λ and μ of an M-symbol $(\lambda : \mu)$

are only determined modulo $\mathfrak{n}$, and that by Lemma 24 we can always choose them such that $\langle \lambda, \mu \rangle = \mathfrak{O}$. There is a map

$$\Gamma \to \mathbb{P}^1(\mathfrak{n}), \qquad \begin{pmatrix} \alpha & \beta \\ \lambda & \mu \end{pmatrix} \mapsto (\lambda : \mu);$$

it induces a well-defined map

$$\mathrm{P}\Gamma \to \mathbb{P}^1(\mathfrak{n}), \qquad \begin{pmatrix} \alpha & \beta \\ \lambda & \mu \end{pmatrix} \mathfrak{O}^\times \mapsto (\lambda : \mu).$$

By Lemma 24, each of these maps is surjective — indeed, their restrictions $\mathrm{S}\Gamma \to \mathbb{P}^1(\mathfrak{n})$ and $\mathrm{PS}\Gamma \to \mathbb{P}^1(\mathfrak{n})$ are surjective.

Proposition 27. *Two elements of* Γ, $\mathrm{S}\Gamma$, $\mathrm{P}\Gamma$ *or* $\mathrm{PS}\Gamma$ *have the same image in* $\mathbb{P}^1(\mathfrak{n})$ *if and only if they lie, respectively, in the same right coset of* $\Gamma_0(\mathfrak{n})$ *in* Γ, *of* $\mathrm{S}\Gamma_0(\mathfrak{n})$ *in* $\mathrm{S}\Gamma$, *of* $\mathrm{P}\Gamma_0(\mathfrak{n})$ *in* $\mathrm{P}\Gamma$, *or of* $\mathrm{PS}\Gamma_0(\mathfrak{n})$ *in* $\mathrm{PS}\Gamma$.

Proof. Consider the case of $\Gamma_0(\mathfrak{n})$. The matrices $M_i = \begin{pmatrix} \alpha_i & \beta_i \\ \lambda_i & \mu_i \end{pmatrix}$ for $i \in \{1, 2\}$ lie in the same right coset of $\Gamma_0(\mathfrak{n})$ in Γ if and only if

$$M_1 {M_2}^{-1} = \begin{pmatrix} * & * \\ \lambda_1\mu_2 - \lambda_2\mu_1 & * \end{pmatrix} \in \Gamma_0(\mathfrak{n}),$$

which is true if and only if $\lambda_1\mu_2 \equiv \lambda_2\mu_1 \pmod{\mathfrak{n}}$, that is, if and only if M_1 and M_2 map to the same M-symbol. The same argument applies *mutatis mutandis* to the other cases. $\square$

Remark. Thus, we may obtain a set of right coset representatives for $\Gamma_0(\mathfrak{n})$ in Γ, for $\mathrm{S}\Gamma_0(\mathfrak{n})$ in $\mathrm{S}\Gamma$, for $\mathrm{P}\Gamma_0(\mathfrak{n})$ in $\mathrm{P}\Gamma$, and for $\mathrm{PS}\Gamma_0(\mathfrak{n})$ in $\mathrm{PS}\Gamma$ by lifting each M-symbol arbitrarily to an element of $\mathrm{S}\Gamma$. This idea is at the heart of computer implementations of modular symbol calculations of homology spaces (see §6.2.4). Note that the natural action of Γ on the right cosets of $\Gamma_0(\mathfrak{n})$ induces a right action on M-symbols:

$$(\lambda : \mu) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (\lambda\alpha + \mu\gamma : \lambda\beta + \mu\delta).$$

This formula is used over and over again in modular symbol calculations. Typically, the matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ represents an edge of our tessellation (i.e. a 1-chain in homology) which forms part of some basic edge or face relation. To compute the homology of $\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$, one needs to include all the translates of the basic relation under Γ; for this it suffices to let $(\lambda : \mu)$ run through a set of coset representatives of $\Gamma_0(\mathfrak{n})$ in Γ.

1.4 Normaliser groups

Let $\mathfrak{O}$ be a Dedekind domain with field of fractions k. Fix $n \in \mathbb{N}$. Let $G = \mathrm{GL}(n, k)$ and $\Gamma = \mathrm{GL}(n, \mathfrak{O})$. Let $\Delta = N_G(\Gamma)$ be the normaliser of Γ in G. In this section, we recall a result of Cremona [Cre88] on the structure of Δ and develop some of its consequences. As motivation for this section we mention that the introduction of Δ leads to simplified geometry (see §1.5 and Chapter 3).

Let J be the group of fractional ideals, P the group of principal fractional ideals, and $C = J/P$ the ideal class group. Let

$$J(n) = \ker\bigl(J \xrightarrow{n} J \to C\bigr)$$

be the group of ideals whose n^{th} power is principal, and

$$C(n) = \ker\bigl(C \xrightarrow{n} C\bigr)$$

the n-torsion subgroup of C. Following [Cre88], we consider the function

$$G \to J, \qquad M \mapsto \langle M \rangle,$$

which assigns to a matrix M the fractional ideal $\langle M \rangle$ generated by the entries of M.

Proposition 28. *Let $M \in G$. Then*

$$M \in \Delta \iff \langle M \rangle^n = \langle \det M \rangle.$$

Proof. This is [Cre88, Theorem 1, part (1)]. □

Corollary 29. *The map $\diamondsuit\colon \Delta \to J(n)$ given by $M \mapsto \langle M \rangle$ is a surjective group homomorphism, and there is an exact sequence of groups*

$$1 \longrightarrow \Gamma \longrightarrow \Delta \xrightarrow{\diamondsuit} J(n) \longrightarrow 1.$$

Proof. That $\diamondsuit$ is a homomorphism follows at once from Proposition 28, using uniqueness of factorisation into ideals;[5] surjectivity follows from the proof of [Cre88, Theorem 1], although the assertion *loc. cit.* is merely that the composite $\Delta \to J(n) \to C(n)$ is surjective. Let $\gamma \in \Gamma$. Then $\mathfrak{O} \supseteq \langle\gamma\rangle \supseteq \langle\det\gamma\rangle = \mathfrak{O}$, so $\langle\gamma\rangle = \mathfrak{O}$, so $\gamma \in \ker\diamondsuit$. Conversely, let $\gamma \in \ker\diamondsuit$. Since $\langle\gamma\rangle = \mathfrak{O}$, certainly $\gamma \in \mathrm{M}_n(\mathfrak{O})$. By Proposition 28, $\langle\det\gamma\rangle = \langle\gamma\rangle^n = \mathfrak{O}$, so $\det\gamma \in \mathfrak{O}^\times$, as required. □

Corollary 30. *There is a commutative diagram of exact rows and columns,*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathfrak{O}^\times & \longrightarrow & k^\times & \longrightarrow & P & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma & \longrightarrow & \Delta & \xrightarrow{\diamondsuit} & J(n) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma/\mathfrak{O}^\times & \longrightarrow & \Delta/k^\times & \longrightarrow & C(n) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1, & &
\end{array}$$

and an exact sequence

$$1 \longrightarrow k^\times\Gamma \longrightarrow \Delta \longrightarrow C(n) \longrightarrow 1.$$

Proof. We may identify $k^\times$ with the centre $\{\,\alpha 1_n \mid \alpha \in k^\times\,\}$ of G; by definition, Δ contains $k^\times$, and clearly $k^\times \cap \Gamma = \mathfrak{O}^\times$. The middle row is exact by Corollary 29, and the rest of the diagram by Lemma 18. (Exactness of the first row also follows directly from Corollary 29, being the special case $n = 1$.) The last part follows trivially from Lemma 18. □

Lemma 31. *Let $M \in \Delta$ and $\mathfrak{a} = \langle M\rangle$. Then there is an $\mathfrak{O}$-module isomorphism*

$$\underbrace{\mathfrak{O} \oplus \cdots \oplus \mathfrak{O}}_{n} \to \underbrace{\mathfrak{a} \oplus \cdots \oplus \mathfrak{a}}_{n}, \qquad v \mapsto vM.$$

In particular, $\mathfrak{a}$ is already generated by the entries in any one row or column of M.

[5] [Cre88] gives a different proof.

Proof. The map is clearly a homomorphism, and $M^{-1} = (\det M)^{-1}\,\mathrm{adj}(M)$ defines the required inverse map into $\mathfrak{O}\oplus\cdots\oplus\mathfrak{O}$, since $\mathfrak{a}^n = \langle \det M\rangle$ and $\mathrm{adj}(M)$ has entries in $\mathfrak{a}^{n-1}$. Surjectivity implies that $\mathfrak{a}$ is generated by the entries in any one column of M; for rows, replace M by its transpose. □

We now restrict to the case $n = 2$, so Δ is the normaliser of $\Gamma = \mathrm{GL}(2,\mathfrak{O})$ in $G = \mathrm{GL}(2,k)$. For $M \in \Delta$ we define $S_{\mathfrak{n}}(M)$, the set of "admissible scaling factors" for M at level $\mathfrak{n}$, by

$$S_{\mathfrak{n}}(M) = \left\{ \alpha \in k^\times \;\middle|\; \alpha\langle M\rangle + \mathfrak{n} = \mathfrak{O} \right\}.$$

Clearly $S_{\mathfrak{n}}(M)$ is non-empty, by Lemma 1; in particular, if $M \in \Gamma$, then $1 \in S_{\mathfrak{n}}(M)$.

Lemma 32. *If $\alpha \in S_{\mathfrak{n}}(M)$, then $\alpha^{-1}\det(\alpha M) \in S_{\mathfrak{n}}(M^{-1})$. If moreover $\alpha' \in S_{\mathfrak{n}}(M')$, then $\alpha\alpha' \in S_{\mathfrak{n}}(MM')$.*

Proof. Clearly $\langle \alpha^{-1}\det(\alpha M)M^{-1}\rangle = \langle \alpha M\rangle^2\langle \alpha^{-1}M^{-1}\rangle = \langle \alpha M\rangle$. The integral ideals $\langle \alpha M\rangle$ and $\langle \alpha' M'\rangle$ are coprime to $\mathfrak{n}$, hence so is their product $\alpha\alpha'\langle MM'\rangle$. □

Consequently, we can define a subgroup of Δ as follows:

$$\Delta_0(\mathfrak{n}) = \left\{ M \in \Delta \;\middle|\; \exists \alpha \in S_{\mathfrak{n}}(M) \text{ such that } \alpha M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \mathfrak{n} \right\}.$$

The next proposition gives a more intrinsic definition.

Proposition 33. *The group $\Gamma(\mathfrak{n})$ is normal in Δ. The normaliser of each of $\Gamma_1^1(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$ in Δ is $\Delta_0(\mathfrak{n})$.*

Proof. Let $M \in \Delta$ and $\alpha \in S_{\mathfrak{n}}(M)$; write $\alpha M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Let $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ and $\gamma' = M^{-1}\gamma M$; thus $\gamma' \in \Gamma$, by definition of Δ. Explicitly,

$$\gamma' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{ad-bc}M' \tag{1.11}$$

where

$$M' = \begin{pmatrix} ad(A-1) - bc(D-1) - abC + cdB & bd(A-D) - b^2C + d^2B \\ ac(D-A) + a^2C - c^2B & ad(D-1) - bc(A-1) + abC - cdB \end{pmatrix}.$$

Since $\langle \alpha M \rangle$ is coprime to $\mathfrak{n}$, so is its square $\langle ad - bc \rangle$. The various congruence conditions for γ' therefore amount to conditions for the corresponding entries of M' to lie in $\mathfrak{n}$. It is now clear that $\gamma \in \Gamma(\mathfrak{n})$ implies $\gamma' \in \Gamma(\mathfrak{n})$; thus $\Gamma(\mathfrak{n}) \triangleleft \Delta$.

Now let $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1^1(\mathfrak{n})$ and assume $\gamma' \in \Gamma_1(\mathfrak{n})$. Then $c^2 \in \mathfrak{n}$ and $cd \in \mathfrak{n}$, so $c\langle c, d \rangle \subseteq \mathfrak{n}$. But $\langle c, d \rangle = \langle \alpha M \rangle$, by Lemma 31, so $\langle c, d \rangle$ is coprime to $\mathfrak{n}$, implying $c \in \mathfrak{n}$. Conversely, let $c \in \mathfrak{n}$; if $\gamma \in \Gamma_1(\mathfrak{n})$, then $\gamma' \in \Gamma_1(\mathfrak{n})$, and if $\gamma \in \Gamma_1^1(\mathfrak{n})$, then $\gamma' \in \Gamma_1^1(\mathfrak{n})$. □

The normaliser of $\Gamma_0(\mathfrak{n})$ in Δ can be strictly larger than $\Delta_0(\mathfrak{n})$. For example, let $\mathfrak{O} = \mathbb{Z}$ and

$$M = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \mathrm{S}\Gamma.$$

Then M normalises $\Gamma_0(4)$, even though $M \notin \Delta_0(4)$. The precise result is as follows.

Corollary 34. *Let $M \in \Delta$ and $\alpha \in S_{\mathfrak{n}}(M)$. Write $\alpha M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then M normalises $\Gamma_0(\mathfrak{n})$ if and only if both $c^2 \in \mathfrak{n}$ and $c(A - D) \in \mathfrak{n}$ for all $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$.*

Proof. Take $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$; then by (1.11), $c^2 \in \mathfrak{n}$, whence also $ac(A - D) \in \mathfrak{n}$ for all $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$. Since $\mathfrak{n} \mid c^2$ and $\mathfrak{n}$ is coprime to $\langle \alpha M \rangle = \langle a, c \rangle$, we find $c(A - D) \in \mathfrak{n}$ for all $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$. The converse is clear. □

Having given an intrinsic definition of $\Delta_0(\mathfrak{n})$, we now prove our main result concerning this group.

Proposition 35. *There is a commutative diagram of exact rows*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma & \longrightarrow & \Delta & \xrightarrow{\Diamond} & J(2) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & \Gamma_0(\mathfrak{n}) & \longrightarrow & \Delta_0(\mathfrak{n}) & \xrightarrow{\Diamond} & J(2) & \longrightarrow & 1. \end{array}$$

Proof. The inclusions are obvious, and the top row is exact by Corollary 30. On the second row, $\ker \Diamond = \Gamma \cap \Delta_0(\mathfrak{n})$; we claim this equals $\Gamma_0(\mathfrak{n})$. For let $M \in \Delta_0(\mathfrak{n})$ with $\langle M \rangle = \mathfrak{O}$. Then any $\alpha \in S_{\mathfrak{n}}(M)$ is invertible modulo $\mathfrak{n}$, and we deduce from $\alpha M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod \mathfrak{n}$ that $M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod \mathfrak{n}$, i.e. that $M \in \Gamma_0(\mathfrak{n})$. It only remains to show surjectivity of $\Diamond$ on the second row.

Given $\mathfrak{a} \in J(2)$, choose $\alpha \in k^\times$ such that $\alpha\mathfrak{a} + \mathfrak{n} = \mathfrak{O}$. Choose $M \in \Delta$ with $\langle M \rangle = \alpha\mathfrak{a}$; in particular, the entries of M lie in $\mathfrak{O}$. We show how to "adjust" M by a matrix $A \in \mathrm{S}\Gamma$ such that $AM \in \Delta_0(\mathfrak{n})$. By Lemma 31, the first column of $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfies $\langle a, c \rangle = \alpha\mathfrak{a}$, hence $\langle a, c \rangle + \mathfrak{n} = \mathfrak{O}$, and so $(c : -a)$ is an M-symbol at level $\mathfrak{n}$. Using Lemma 24 on M-symbols, find

$$A = \begin{pmatrix} x & y \\ c' & -a' \end{pmatrix} \in \mathrm{S}\Gamma$$

with $a' \equiv a \pmod{\mathfrak{n}}$ and $c' \equiv c \pmod{\mathfrak{n}}$. Then $AM = \left(\begin{smallmatrix} * & * \\ \gamma & * \end{smallmatrix}\right) \in \Delta$ with $\gamma = c'a - a'c \in \mathfrak{n}$ and $\langle AM \rangle = \langle A \rangle \langle M \rangle = \alpha\mathfrak{a}$. Put $M' = \alpha^{-1}AM$. Then $\alpha \in S_{\mathfrak{n}}(M')$, showing that $M' \in \Delta_0(\mathfrak{n})$ with $\langle M' \rangle = \mathfrak{a}$. □

Clearly $\Delta_0(\mathfrak{n})$ contains the scalar matrices $k^\times$, so we may define the corresponding projectivised group $\mathrm{P}\Delta_0(\mathfrak{n})$. We obtain the following result, a generalisation of Corollary 30 in the case $n = 2$.

Corollary 36. *There is a commutative diagram of exact rows and columns,*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathfrak{O}^\times & \longrightarrow & k^\times & \longrightarrow & P & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \Gamma_0(\mathfrak{n}) & \longrightarrow & \Delta_0(\mathfrak{n}) & \xrightarrow{\diamond} & J(2) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{P}\Gamma_0(\mathfrak{n}) & \longrightarrow & \mathrm{P}\Delta_0(\mathfrak{n}) & \longrightarrow & C(2) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1, & &
\end{array}$$

and an exact sequence

$$1 \longrightarrow k^\times\Gamma_0(\mathfrak{n}) \longrightarrow \Delta_0(\mathfrak{n}) \longrightarrow C(2) \longrightarrow 1.$$

Proof. Apply Lemma 18. □

Regard the level $\mathfrak{n}$ as fixed, and choose ideals $\mathfrak{p}_i \in J(2)$ to represent the ideal classes in $C(2)$; by Lemma 1, we may assume that the $\mathfrak{p}_i$ are prime to $\mathfrak{n}$. (Indeed, when $\mathfrak{O}$ is the ring of integers of a number field, we may further assume that the $\mathfrak{p}_i$ are prime, using the well-known but deep theorem that every ideal class contains infinitely many prime ideals.) Lift the $\mathfrak{p}_i$ arbitrarily to matrices $A_i \in \Delta_0(\mathfrak{n})$. By Corollary 36, the images $A_i k^\times$ of the A_i in $\mathrm{P}\Delta_0(\mathfrak{n})$ form a system of (right) coset representatives for $\mathrm{P}\Gamma_0(\mathfrak{n})$ in $\mathrm{P}\Delta_0(\mathfrak{n})$, and *a fortiori* for $\mathrm{P}\Gamma$ in $\mathrm{P}\Delta$.

The "adjustment" step in the proof of Proposition 35 shows that Δ is generated by its subgroups $\mathrm{S}\Gamma$ and $\Delta_0(\mathfrak{n})$; consequently, $\mathrm{P}\Delta$ is generated by $\mathrm{PS}\Gamma$ and $\mathrm{P}\Delta_0(\mathfrak{n})$.

Corollary 37. *If $\{S_i\}_{i\in I}$ is a set of (right) coset representatives for $\Gamma_0(\mathfrak{n})$ in Γ, then it is also a set of (right) coset representatives for $\Delta_0(\mathfrak{n})$ in Δ. Similarly, if $\{S_i\}_{i\in I}$ is a set of (right) coset representatives for $\mathrm{P}\Gamma_0(\mathfrak{n})$ in $\mathrm{P}\Gamma$, then it is also a set of (right) coset representatives for $\mathrm{P}\Delta_0(\mathfrak{n})$ in $\mathrm{P}\Delta$.*

Proof. Since Γ is normal in Δ,

$$\Delta = \Delta_0(\mathfrak{n}) \cdot \Gamma = \Delta_0(\mathfrak{n}) \cdot \bigcup_{i\in I} \Gamma_0(\mathfrak{n}) S_i = \bigcup_{i\in I} \Delta_0(\mathfrak{n}) S_i.$$

Moreover, if $\Delta_0(\mathfrak{n})S_i = \Delta_0(\mathfrak{n})S_j$, then $S_i S_j^{-1} \in \Delta_0(\mathfrak{n}) \cap \Gamma = \Gamma_0(\mathfrak{n})$, whence $i = j$. The same proof applies *mutatis mutandis* in the projective case; note that $\mathrm{P}\Delta_0(\mathfrak{n}) \cap \mathrm{P}\Gamma = \mathrm{P}\Gamma_0(\mathfrak{n})$, as one sees from the bottom rows of the diagrams in Corollaries 30 and 36. □

Thus, in particular, the M-symbols at level $\mathfrak{n}$ provide a set of right coset representatives for $\Delta_0(\mathfrak{n})$ in Δ and for $\mathrm{P}\Delta_0(\mathfrak{n})$ in $\mathrm{P}\Delta$.

Aside. It is tempting to think of Proposition 35 as a partial analogue of Lemma 14, and to try to embed $\Gamma_1(\mathfrak{n})$, $\Gamma_1^1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$ in suitable groups $\Delta_1(\mathfrak{n})$, $\Delta_1^1(\mathfrak{n})$ and $\Delta(\mathfrak{n})$. The naïve approach fails, however. Thus we could put

$$\Delta_1(\mathfrak{n}) = \left\{ M \in \Delta \;\middle|\; \exists \alpha \in S_{\mathfrak{n}}(M) \text{ such that } \alpha M \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \bmod \mathfrak{n} \right\},$$

$$\Delta_1^1(\mathfrak{n}) = \left\{ M \in \Delta \;\middle|\; \exists \alpha \in S_{\mathfrak{n}}(M) \text{ such that } \alpha M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod \mathfrak{n} \right\},$$

$$\Delta(\mathfrak{n}) = \left\{ M \in \Delta \;\middle|\; \exists \alpha \in S_{\mathfrak{n}}(M) \text{ such that } \alpha M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \mathfrak{n} \right\},$$

but in fact $\Delta_1(\mathfrak{n}) = \Delta_0(\mathfrak{n})$. For suppose $\alpha M = \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right)$, where $M \in \Delta_0(\mathfrak{n})$ and $\alpha \in S_{\mathfrak{n}}(M)$. Then $\langle \alpha M \rangle + \mathfrak{n} = \mathfrak{O}$, whence $\langle \det(\alpha M) \rangle + \mathfrak{n} = \mathfrak{O}$. Since $c \in \mathfrak{n}$, this implies that d is invertible modulo $\mathfrak{n}$, with inverse β, say; clearly $\alpha\beta \in S_{\mathfrak{n}}(M)$ and $\alpha\beta M \equiv \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Thus $\Delta_1(\mathfrak{n}) = \Delta_0(\mathfrak{n})$, as claimed. The question of finding a natural choice of $\Delta_1(\mathfrak{n})$, i.e. a subgroup $\Delta_1(\mathfrak{n})$ of Δ with $\Gamma \cap \Delta_1(\mathfrak{n}) = \Gamma_1(\mathfrak{n})$ and $\operatorname{im} \diamondsuit$ as large as possible in the exact sequence

$$1 \longrightarrow \Gamma_1(\mathfrak{n}) \longrightarrow \Delta_1(\mathfrak{n}) \xrightarrow{\ \diamondsuit\ } J(2)$$

may be left for a rainy day, and will not concern us further.

1.5 Cusps

Let $\mathfrak{O}$ be a Dedekind domain with field of fractions k. The set $\mathbb{P}^1(k) = k \cup \{\infty\}$ is called the set of *cusps* over k. We usually represent cusps, including the cusp at infinity, as λ/μ, with $\lambda, \mu \in \mathfrak{O}$ not both zero. This expression is not unique, of course, but the ideal class $cl(\langle \lambda, \mu \rangle)$ is well-defined, for if $\lambda/\mu = \lambda'/\mu'$, then either $\mu = \mu' = 0$ or $cl(\langle \lambda, \mu \rangle) = cl(\langle \lambda, \mu \rangle \mu') = cl(\langle \lambda', \mu' \rangle \mu) = cl(\langle \lambda', \mu' \rangle)$.

Definition. The *class* of a cusp λ/μ, denoted $cl(\lambda/\mu)$, is the ideal class $cl(\langle \lambda, \mu \rangle)$. A cusp is *principal* if its class is the principal class.

Clearly any principal cusp λ/μ may be expressed "in lowest terms", i.e. with $\langle \lambda, \mu \rangle = \mathfrak{O}$. The following lemma shows that the general situation is as good as one could hope for: given fixed ideals $\{ \mathfrak{a}_i \mid i \in I \}$, one in each ideal class, one can write any cusp as λ/μ with $\langle \lambda, \mu \rangle = \mathfrak{a}_i$ for some $i \in I$.

Lemma 38. *Let $\mathfrak{a}$ be an integral ideal. Then every cusp with class $cl(\mathfrak{a})$ may be written in the form λ/μ with $\langle \lambda, \mu \rangle = \mathfrak{a}$.*

Proof. Let $\alpha = \lambda'/\mu'$ have class $cl(\mathfrak{a})$. Then there exists $u \in k^\times$ with $u\langle \lambda', \mu' \rangle = \mathfrak{a}$. Put $\lambda = u\lambda'$ and $\mu = u\mu'$. Then $\alpha = \lambda/\mu$, where $\lambda, \mu \in \mathfrak{O}$ and $\langle \lambda, \mu \rangle = \mathfrak{a}$. □

The group $\mathrm{GL}(2,k)$ acts on the left on the cusps (compare §3.1 below) by the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{\lambda}{\mu} = \frac{a\lambda + b\mu}{c\lambda + d\mu}.$$

This action is clearly transitive, for if $\alpha \in k$ then $\left(\begin{smallmatrix} \alpha & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \infty = \alpha$; slightly less trivially, the orbit of ∞ under $\mathrm{GL}(2,\mathfrak{O})$ is the set of principal cusps:

$$\left\{ \frac{\lambda}{\mu} \;\middle|\; \lambda, \mu \in \mathfrak{O},\; \langle \lambda, \mu \rangle = \mathfrak{O} \right\}.$$

So the action of $\mathrm{GL}(2,\mathfrak{O})$ is transitive on the cusps if and only if every ideal is principal.

Lemma 39. *The orbit of a cusp α under both $\mathrm{SL}(2,\mathfrak{O})$ and $\mathrm{GL}(2,\mathfrak{O})$ is the set of cusps with class $cl(\alpha)$.*

Proof. The action of $\mathrm{GL}(2,\mathfrak{O})$ preserves the class of a cusp, since if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathfrak{O})$, then $\langle a\lambda + b\mu, c\lambda + d\mu \rangle = \langle \lambda, \mu \rangle$. We now show that $\mathrm{SL}(2,\mathfrak{O})$ acts transitively on each class. Suppose $cl(\lambda/\mu) = cl(\lambda'/\mu')$, so there is $u \in k^\times$ with $\langle \lambda, \mu \rangle = u\langle \lambda', \mu' \rangle$. By Proposition 7 there exists $M \in \mathrm{SL}(2,\mathfrak{O})$ such that $M\left(\begin{smallmatrix} \lambda \\ \mu \end{smallmatrix}\right) = \left(\begin{smallmatrix} u\lambda' \\ u\mu' \end{smallmatrix}\right)$. Then $M \cdot \lambda/\mu = \lambda'/\mu'$. □

We now consider the orbits under the group Δ defined in §1.4; recall that Δ is the normaliser of $\Gamma = \mathrm{GL}(2,\mathfrak{O})$ in $\mathrm{GL}(2,k)$.

Lemma 40. *Let $M \in \Delta$ and let $\alpha \in k \cup \{\infty\}$. Then $cl(M \cdot \alpha) = cl\langle M \rangle cl(\alpha)$. More precisely, let $\lambda, \mu \in \mathfrak{O}$. Then $M\left(\begin{smallmatrix} \lambda \\ \mu \end{smallmatrix}\right) = \left(\begin{smallmatrix} \lambda' \\ \mu' \end{smallmatrix}\right)$, where*

$$\langle \lambda', \mu' \rangle = \langle M \rangle \langle \lambda, \mu \rangle. \tag{1.12}$$

Proof. The first part follows from the second by writing $\alpha = \lambda/\mu$ and taking ideal classes. We now prove the second part. Write $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and let $\mathfrak{a} = \langle M \rangle$. Clearly $\lambda', \mu' \in \mathfrak{a}\langle \lambda, \mu \rangle$. Also, with $\delta = \det M$,

$$\begin{pmatrix} \delta\lambda \\ \delta\mu \end{pmatrix} = \mathrm{adj}(M) \begin{pmatrix} \lambda' \\ \mu' \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \lambda' \\ \mu' \end{pmatrix},$$

whence $\delta\langle \lambda, \mu \rangle \subseteq \mathfrak{a}\langle \lambda', \mu' \rangle \subseteq \mathfrak{a}^2\langle \lambda, \mu \rangle$. Since $\langle \delta \rangle = \mathfrak{a}^2$ (because $M \in \Delta$), equality is forced throughout, implying (1.12). □

Corollary 41. *For two cusps α, α', the following are equivalent:*

(i) *there exists $M \in \Delta$ such that $\alpha' = M \cdot \alpha$;*

(ii) *there exists an integral ideal $\mathfrak{a}$, with $\mathfrak{a}^2$ principal, such that $cl(\alpha') = cl(\mathfrak{a})cl(\alpha)$.*

Proof. Assume (i). Then (ii) holds with $\mathfrak{a} = \langle M \rangle$, by Lemma 40. Conversely, assume (ii). By surjectivity of $\diamondsuit$ in Corollary 29, there exists $M' \in \Delta$ with $\langle M' \rangle = \mathfrak{a}$. Put $\alpha'' = M' \cdot \alpha$. By Lemma 40, $cl(\alpha'') = cl(\mathfrak{a})cl(\alpha) = cl(\alpha')$, whence by Lemma 39, there exists $M'' \in \Gamma$ such that $\alpha' = M'' \cdot \alpha''$. Then $M = M''M'$ has the required property. ☐

In particular, suppose that $\mathfrak{O}$ has finite class number h. Then there are h orbits of cusps under Γ (and $S\Gamma$), but only $|C/C(2)|$ orbits under Δ (in the notation of §1.4).

Chapter 2

The classical case

The purpose of this thesis is to generalise a small part of the classical theory of modular forms. It is therefore appropriate to record the basic definitions; the reader will recognise many analogous situations later in the thesis. By the "classical" theory, we mean specifically the case in which the underlying number field is $\mathbb{Q}$. There is, of course, a well-established theory over general global fields.

2.1 Classical modular forms

2.1.1 Definitions

Let $\mathfrak{H}_2$ denote the complex upper half plane $\{\, x + iy \mid x, y \in \mathbb{R},\ y > 0 \,\}$, and $\mathfrak{H}_2^*$ the *extended half plane*

$$\mathfrak{H}_2^* = \mathfrak{H}_2 \cup \mathbb{Q} \cup \{\infty\}\,,$$

obtained by adjoining the *cusps*. The group

$$\mathrm{GL}^+(2, \mathbb{R}) = \{\, \gamma \in \mathrm{GL}(2, \mathbb{R}) \mid \det \gamma > 0 \,\}$$

acts on $\mathfrak{H}_2^*$ by fractional linear transformations; explicitly, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}^+(2, \mathbb{R})$ and $z \in \mathfrak{H}_2^*$,

$$\gamma \cdot z = \frac{az + b}{cz + d}, \tag{2.1}$$

with the obvious conventions regarding infinity. Now define

$$\mu(\gamma, z) = \left(\frac{d}{dz}(\gamma \cdot z)\right)^{1/2} = (\det \gamma)^{1/2}(cz+d)^{-1}.$$

For $t \in \mathbb{N}$, define an action of $\mathrm{GL}^+(2, \mathbb{R})$ on meromorphic functions $f\colon \mathfrak{H}_2 \to \mathbb{C}$ via

$$(f\big|_t \gamma)(z) = f(\gamma \cdot z)\mu(\gamma, z)^t \qquad \big(\gamma \in \mathrm{GL}^+(2, \mathbb{R}),\ z \in \mathfrak{H}_2\big). \tag{2.2}$$

Let $N \in \mathbb{N}$ and let Γ' be a congruence subgroup of $\mathrm{SL}(2, \mathbb{Z})$ of level N, i.e. a subgroup containing $\mathrm{S}\Gamma(N)$ in the notation of §1.2.1. A meromorphic function $f\colon \mathfrak{H}_2 \to \mathbb{C}$ is said to be *weakly modular* of *weight* t for Γ' if

$$f\big|_t \gamma = f \qquad \forall \gamma \in \Gamma'. \tag{2.3}$$

Since $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma'$, weakly modular forms are invariant under $z \mapsto z + N$, and so have a Fourier expansion

$$f(z) = \sum_{n \in \mathbb{Z}} a_n \exp(2\pi i n z/N).$$

If f is weakly modular for Γ', and $\gamma \in \mathrm{SL}(2, \mathbb{Z})$, then $f\big|_t \gamma$ is weakly modular for $\gamma^{-1}\Gamma'\gamma$, which is again a congruence subgroup since $\mathrm{S}\Gamma(N)$ is normal in $\mathrm{SL}(2, \mathbb{Z})$. If f is holomorphic and the Fourier expansions of all the the functions $f\big|_t \gamma$ for $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ have $a_n = 0$ for $n < 0$ we say that f is a *modular form*; if moreover each $a_0 = 0$, we say that f is a *cuspform*. More generally, for a Dirichlet character χ mod N, one also has the notion of a modular form with *character* or *nebentypus* χ, for which (2.3) is replaced by

$$f\big|_t \gamma = \chi(d) f \qquad \forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma'.$$

The complex vector space of cuspforms of weight t for Γ' is denoted $S_t(\Gamma')$. It carries an Hermitian inner product, the *Petersson inner product*, defined by

$$\langle f, g \rangle = \int_{\Gamma' \backslash \mathfrak{H}_2^*} f(z)\overline{g(z)} y^{t-2}\, dx\, dy. \tag{2.4}$$

The quotient space $\Gamma' \backslash \mathfrak{H}_2^*$ carries the structure of a compact Riemann surface. By applying the Riemann-Roch theorem, one can deduce a formula for the dimension of $S_t(\Gamma')$. From our point of view, the interesting case is when $t = 2$; in this case, equations (2.2) and (2.3), together with the cusp condition, amount to saying that $f(z)\, dz$ is a holomorphic differential 1-form on $\Gamma' \backslash \mathfrak{H}_2^*$.

2.1.2 Modular points

Let f be a modular form of weight t for $\mathrm{SL}(2, \mathbb{Z})$. Then one can define

$$\tilde{F}(\omega_1, \omega_2) = \omega_2^{-t} f(\omega_1/\omega_2) \tag{2.5}$$

for all pairs (ω_1, ω_2) with $\omega_1/\omega_2 \in \mathfrak{H}_2$; by construction, $\tilde{F}$ is homogeneous of weight $-t$. The automorphy condition for f translates into the fact that $\tilde{F}$ depends only on the $\mathbb{Z}$-lattice spanned by ω_1, ω_2; therefore, $\tilde{F}$ corresponds in turn to a function F defined on $\mathbb{Z}$-lattices and having "weight" t in the sense that

$$F(\zeta\Lambda) = \zeta^{-t} F(\Lambda) \qquad \forall \zeta \in \mathbb{C}^{\times}.$$

Conversely, given such a lattice function, one can construct a modular form of weight t; indeed, the most basic of all constructions of modular forms, that of the Eisenstein series G_t, proceeds in this way:

$$\tilde{G}_t(\omega_1, \omega_2) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} (m\omega_1 + n\omega_2)^{-t}.$$

For details, the reader may consult any introduction to modular forms, for example [Swi92, Ser73, Kob84, Lan76].

Thus, classical modular forms for $\mathrm{SL}(2, \mathbb{Z})$ correspond to certain functions on $\mathbb{Z}$-lattices in $\mathbb{C}$. The idea generalises to forms for the main congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$; such forms correspond in a similar way to functions on "modular points", which are lattices equipped with extra structure [Kob84, Lan76]. Modular points provide one approach to the introduction of the Hecke operators, which are tremendously important in the theory. Roughly speaking, modular forms give rise to Dirichlet series with functional equation (for details, including Weil's converse result, see [Wei67b]), and simultaneous Hecke eigenforms to Dirichlet series with functional equation and an Euler product expansion.

2.1.3 Hecke operators and newforms

For concreteness, we now take $t = 2$ and $\Gamma' = \Gamma_0(N)$, and write $S_2(N)$ for the space $S_2(\Gamma_0(N))$. Since $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \in \Gamma_0(N)$, an element of $S_2(N)$ has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}. \tag{2.6}$$

For each prime p there is a linear operator T_p on $S_2(N)$, called a Hecke operator; when $p \mid N$, the operator T_p is sometimes denoted U_p, and there is a related involution operator W_p which yields slightly more information. All these operators commute pairwise. Moreover, the T_p for $p \nmid N$ are self-adjoint with respect to (2.4). Therefore, by an elementary theorem of algebra, $S_2(N)$ has a basis consisting of *eigenforms*, i.e. simultaneous eigenvectors for all the T_p with $p \nmid N$; moreover, the eigenspaces are preserved by the U_p.

However, the operators U_p are not in general self-adjoint, so $S_2(N)$ does *not* in general have a basis consisting of eigenforms for *all* the T_p. To make progress, one introduces the concepts of "oldforms" and "newforms" following Atkin and Lehner [AL70]. If $M \mid N$ and $f \in S_2(M)$, then both f itself and the function $z \mapsto f(Nz/M)$ lie in $S_2(N)$. The subspace of $S_2(N)$ spanned by all such forms as M ranges over the proper divisors of N is called the *oldspace* at level N; its orthogonal complement with respect to the Petersson inner product is called the *newspace*.

When the operators T_p with $p \nmid N$ are restricted to the newspace at level N, the simultaneous eigenspaces turn out to be one-dimensional. Since they are preserved by the U_p, they are automatically eigenspaces for those operators too. Hence the newspace at level N has a basis consisting of simultaneous eigenforms of the T_p for *all* primes p; such forms are called *newforms* at level N. (The language might cause confusion, so we emphasise that, in general, not every element of the newspace is a newform.)

A cuspform (2.6) gives rise, via Mellin transform, to a Dirichlet L-series $\sum a_n n^{-s}$ which has a functional equation and analytic continuation to $s \in \mathbb{C}$. If f is a newform, then $a_1 \neq 0$, and one always chooses to normalise f so that $a_1 = 1$. In that case, by [AL70, Theorem 3], one has $T_p f = a_p f$ for all primes p; furthermore, if $p \mid N$ then $W_p f = \epsilon_p f$

with $\epsilon_p \in \{\pm 1\}$ and

$$a_p = \begin{cases} -\epsilon_p & \text{if } p \mid N \text{ but } p^2 \nmid N, \\ 0 & \text{if } p^2 \mid N. \end{cases} \tag{2.7}$$

If f is a normalised newform for $\Gamma_0(N)$ with character χ, then it follows from relations among the Hecke operators that its L-series has the Euler product expansion

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{p \mid N} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid N} \left(1 - a_p p^{-s} + \chi(p) p^{1-2s}\right)^{-1}. \tag{2.8}$$

Various authors [Cre97, FM98] have made extensive computations of newforms for $\Gamma_0(N)$. The examples below are taken from Table 3 of [Cre97] and the extended version available electronically.[1]

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89
20A	−	−2	+	2	0	2	−6	−4	6	6	−4	2	6	−10	−6	−6	12	2	2	−12	2	8	6	−6
40A	+	0	−	−4	4	−2	2	4	4	−2	−8	6	−6	−8	4	6	−4	−2	8	0	−6	0	−16	−6
80A	+	0	−	4	−4	−2	2	−4	−4	−2	8	6	−6	8	−4	6	4	−2	−8	0	−6	0	16	−6
80B	−	2	+	−2	0	2	−6	4	−6	6	4	2	6	10	6	−6	−12	2	−2	12	2	−8	−6	−6

Each row represents a newform. The first column gives the label of the newform, consisting of the level N at which the form arises and a code letter to distinguish the newforms at that level. The other columns give, for $p \nmid N$ the eigenvalue of T_p, and for $p \mid N$ the sign of the involution W_p.

Notice that the eigenvalues $a(p)$ of 20A and $b(p)$ of 80B are the same up to sign; more precisely, $b(p) = \chi(p)a(p)$, where χ is the quadratic character

$$p \mapsto \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4) \\ -1 & \text{if } p \equiv -1 \pmod 4). \end{cases} \tag{2.9}$$

[1] The file `ftp://euclid.ex.ac.uk/pub/cremona/data/aplist.1-5300` lists all newforms for $N \leq 5300$.

2.1.4 Twists: new forms from old

Let $f \in S_2(N)$ be given by (2.6), and let χ be a quadratic Dirichlet character of conductor m, where $m^2 \mid N$. Then there is another cuspform $f\big|R_\chi$ in $S_2(N)$ given by

$$f\big|R_\chi(z) = \sum_{n=1}^{\infty} a_n \chi(n) e^{2\pi i n z}.$$

Even if f is a newform, $f\big|R_\chi$ need not be, but there is always an associated newform at some possibly different level N' with the same eigenvalues for all primes $p \nmid m$. We denote this newform by $f * \chi$ and call it the *twist* of f by χ. Of course, any quadratic character is built up from the basic characters χ_{-4} given by (2.9), χ_8 given by $p \mapsto (2/p)$, and χ_q given by $p \mapsto (p/q)$ for odd primes q, and we also write $f * -4$, $f * 5$, $f * -20 = f * -4 * 5$, and so on. Thus, in §2.1.3 above, 80B $=$ 20A $* -4$, and 80A $=$ 40A $* -4$.

For details of how the level changes under twisting, see Theorems 6 and 7 of [AL70]. For example, if f is a newform at level N, and $f * 5$ is a newform at level N', then $N' = 5^\alpha N$, where

$$\alpha = \begin{cases} 2 & \text{if } 5 \nmid N, \\ 1 & \text{if } 5 \mid N \text{ but } 5^2 \nmid N, \\ 0, -1 \text{ or } -2 & \text{if } 5^2 \mid N \text{ but } 5^3 \nmid N, \text{ and} \\ 0 & \text{if } 5^3 \mid N. \end{cases}$$

2.2 Towards a general theory

It is natural to search for an analogous theory when $\mathbb{Z}$ in $\mathrm{SL}(2,\mathbb{Z})$ is replaced by the ring of integers $\mathfrak{O}$ of a number field k. To make the right definitions, one must address a number of questions.

What should replace $\mathfrak{H}_2$ as the domain of definition of our forms? Should they still take values in the space $\mathbb{C}$? What should replace the weight t and the automorphy factor $\mu(\gamma, z)$? Finally, what analytic conditions should our forms satisfy? The requirement of holomorphy may have to be weakened or modified, necessarily so if the domain of definition does not have a complex structure.

Some of the first successes in this direction were achieved by Hilbert. For Hilbert modular forms, one retains the requirement of holomorphy; consequently, one has to restrict attention to totally real number fields, since otherwise the appropriate domain for the forms has no (obvious) complex structure. Even in this case, it was soon found that serious technical difficulties arose, due to the class group and the unit group. These difficulties largely disappeared with the adoption of the adelic viewpoint which had proved so successful in class field theory.

From the adele point of view, the theory of automorphic forms on GL(2) over k is the theory of various types of functions on the adele group $G_{\mathbb{A}}$ which are left-invariant under G_k. Our main source for this theory is the book of Weil [Wei71]. We mention briefly that there is a yet more general point of view; once we have agreed to study spaces of functions on $G_k\backslash G_{\mathbb{A}}$, we may consider the (right) regular representation of $G_{\mathbb{A}}$ on such a space:

$$\big(\rho(g)(f)\big)(h) = f(hg);$$

thus, the finite-dimensional spaces of various types of automorphic form may be regarded as various finite-dimensional representations of $G_k\backslash G_{\mathbb{A}}$. This is the viewpoint of Jacquet-Langlands theory, but we will be content with the "elementary" approach of Weil.

In the case of an imaginary quadratic field, we shall develop a theory of modular points entirely analogous to the classical one, allowing us to define Hecke operators and, in certain cases, to compute their action on the space of cuspforms.

Chapter 3

Geometry of upper half space

The *upper half-space* is the set

$$\mathfrak{H}_3 = \mathbb{C} \times \mathbb{R}_{>0} = \{ (z,t) \mid z \in \mathbb{C},\ t \in \mathbb{R}_{>0} \}.$$

The space carries a hyperbolic metric, and the group $\mathrm{GL}(2,\mathbb{C})$ acts on $\mathfrak{H}_3$ by isometries. There are two quite natural ways of introducing this action: (i) by expressing $\mathfrak{H}_3$ as the coset space $\mathrm{GL}(2,\mathbb{C})/\mathbb{C}^\times \cdot \mathrm{SU}(2)$ and acting on cosets (see §3.1); (ii) by identifying points of $\mathfrak{H}_3$ with Hermitian forms and acting by change of variable (see §3.2). Of these points of view, (i) is the more natural for the study of modular forms (see Chapters 4 and 6); we also give (ii) since it led to the geometrical methods that we use in this chapter.

Let k be an imaginary quadratic field with ring of integers $\mathfrak{O}$ and class number h. One of the main goals of this chapter is to obtain a tessellation of the extended half space $\mathfrak{H}_3^*$ by hyperbolic polyhedra, a tessellation on which the group $\Gamma = \mathrm{GL}(2,\mathfrak{O})$ acts. Our approach closely follows the work of Cremona and Whitley [Cre81, Whi90] for the nine fields with $h = 1$, the main innovation in this thesis being the introduction of the normaliser Δ of Γ in $\mathrm{GL}(2,k)$, which simplifies the geometry when $h = 2$ (and more generally, when $C = C(2)$ in the notation of §1.4), enabling such fields to be dealt with almost as easily as those with $h = 1$. We develop the theory for general k, and give all the geometrical details for $k = \mathbb{Q}(\sqrt{-5})$, which has $h = 2$. There are two stages.

First, we find fundamental regions D for the action of Γ and Δ on $\mathfrak{H}_3^*$. This involves studying the geometry of hemispheres, and leads to certain algorithms, akin to the Euclidean algorithm, which will be important for our computations later in this thesis.

Then, we glue together copies of D (translates of D under the stabilisers of its vertices) to form hyperbolic polyhedra, with vertices at the cusps, which tessellate $\mathfrak{H}_3^*$. We choose a "basic edge" e_i in each Γ-orbit of edges. Each edge of our tessellation has the form γe_i for some i and some $\gamma \in \Gamma$; thus the homology of $\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$ is generated by the $(c:d)e_i$, where $(c:d)$ runs through a set of coset representatives of $\Gamma_0(\mathfrak{n})$ in Γ, as in §1.3. There is some redundancy: the stabiliser of the (unordered) edge e_i, when non-trivial, gives rise to some "edge relations". From our polyhedra, we obtain one "face relation" for each orbit of faces. Note that a polyhedron with F faces gives rise to at most $F-1$ independent face relations.

The relations we obtain encode all the necessary geometric information about k in the form of algebraic symbols that are readily stored on a computer; the calculations in later chapters reduce to algebraic manipulations and linear algebra.

3.1 Action of $\mathrm{GL}(2,\mathbb{C})$ on half-space

Let $\mathbb{H}$ be the ring of quaternions. It is 4-dimensional algebra over $\mathbb{R}$, with the usual basis $1, i, j, k$. It may also be regarded as a left vector space over $\mathbb{C}$, with basis $1, j$; accordingly, we sometimes identify $\mathbb{H}$ with $\mathbb{C}^2$. Define an equivalence relation $\sim$ on $\mathbb{H}^2 \setminus \{(0,0)\}$ by

$$(q,r) \sim (q',r') \;\Leftrightarrow\; \exists\lambda \in \mathbb{H}^\times \text{ such that } (q\lambda, r\lambda) = (q',r').$$

The equivalence class of (q,r) is $\{\,(q\lambda, r\lambda) \mid \lambda \in \mathbb{H}^\times\,\}$, and will be denoted by $[q:r]$. The set $\mathbb{P}^1(\mathbb{H})$ of these classes is the *quaternionic projective line.* A set of representatives of $\mathbb{P}^1(\mathbb{H})$ is $\{\,(q,1) \mid q \in \mathbb{H}\,\} \cup \{(1,0)\}$. We may identify $\mathbb{P}^1(\mathbb{H})$ with $\mathbb{H} \cup \{\infty\}$ and $\mathbb{C}^2 \cup \{\infty\}$ via

$$\begin{array}{ccccc} [q:1] & \longleftrightarrow & q = z + tj & \longleftrightarrow & (z,t) \\ [1:0] & \longleftrightarrow & \infty & \longleftrightarrow & \infty. \end{array} \tag{3.1}$$

It is convenient to identify $\mathbb{C} \times \{0\}$ with $\mathbb{C}$ and write $(0,1)$ as j; this is consistent with (3.1).

Regard $\mathbb{H}^2 \setminus \{(0,0)\}$ as a set of column vectors. The group $G = \mathrm{GL}(2,\mathbb{C})$ acts on the left by matrix multiplication; since this action preserves equivalence classes, there is a well-defined left action of G on $\mathbb{P}^1(\mathbb{H})$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot [q : r] = [aq + br : cq + dr]. \tag{3.2}$$

Notice that real scalar matrices act trivially, because $\mathbb{R}^\times$ is contained in the centre of $\mathbb{H}^\times$, but that $i \cdot [j : 1] = [ij : i] = [-ji : i] = [-j : 1] \neq [j : 1]$. Hence there is an induced action of $G/\mathbb{R}^\times$ but not of $\mathrm{PGL}(2, \mathbb{C})$. More generally,

$$e^{i\theta} \cdot [z + tj : 1] = [z + e^{2i\theta} tj : 1]. \tag{3.3}$$

It follows immediately from (3.2) and the identification (3.1) that there is an action of G on $\mathbb{H} \cup \{\infty\}$, given for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ by

$$\begin{aligned} g \cdot \infty &= \begin{cases} \infty & \text{if } c = 0, \\ a/c & \text{otherwise,} \end{cases} \\ g \cdot q &= \begin{cases} \infty & \text{if } q = -d/c, \\ (aq + b)(cq + d)^{-1} & \text{otherwise,} \end{cases} \end{aligned} \tag{3.4}$$

and hence an action of G on $\mathbb{C}^2 \cup \{\infty\}$ given by

$$\begin{aligned} g \cdot \infty &= \begin{cases} \infty & \text{if } c = 0, \\ (a/c, 0) & \text{otherwise,} \end{cases} \\ g \cdot (z, t) &= \begin{cases} \infty & \text{if } z = -d/c \text{ and } t = 0, \\ (z', t') & \text{otherwise,} \end{cases} \end{aligned} \tag{3.5}$$

where

$$z' = \frac{(az + b)\overline{(cz + d)} + (at)\overline{(ct)}}{|cz + d|^2 + |ct|^2}, \qquad t' = \frac{(ad - bc)t}{|cz + d|^2 + |ct|^2}. \tag{3.6}$$

For convenience we record the following special case of (3.5):

$$\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \cdot j = z + tj. \tag{3.7}$$

Lemma 42. *The action* (3.5) *has two orbits:* $\mathbb{C} \cup \{\infty\}$ *and its complement* $\mathbb{C} \times \mathbb{C}^\times$. *The stabiliser of* j *is the group*

$$\mathbb{R}^\times \cdot \mathrm{SU}(2) = \left\{ \begin{pmatrix} \bar{d} & -\bar{c} \\ c & d \end{pmatrix} \;\middle|\; c, d \in \mathbb{C},\ (c,d) \neq (0,0) \right\}.$$

Proof. Clearly (3.5) restricted to $\mathbb{C} \cup \{\infty\}$ is just the usual action by Möbius transformations on the Riemann sphere; in particular, it is transitive. The action on $\mathbb{C} \times \mathbb{C}^\times$ is transitive by (3.7). If $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ fixes j, then $aj + b = j(cj + d)$, whence $b + \bar{c} = (\bar{d} - a)j = 0$, so g is as stated; conversely, $\mathbb{R}^\times \cdot \mathrm{SU}(2)$ fixes j. □

Corollary 43. *There is a decomposition* $G = ZBK$, *where*

$$Z = \left\{ \zeta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; \zeta \in \mathbb{C}^\times \right\},$$

$$B = \left\{ \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \;\middle|\; z \in \mathbb{C},\ t \in \mathbb{R}_{>0} \right\},$$

$$K = \mathrm{SU}(2) = \left\{ \begin{pmatrix} \bar{v} & -\bar{u} \\ u & v \end{pmatrix} \;\middle|\; u, v \in \mathbb{C},\ u\bar{u} + v\bar{v} = 1 \right\}.$$

Explicitly, for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \zeta \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{v} & -\bar{u} \\ u & v \end{pmatrix}, \tag{3.8}$$

where

$$\begin{aligned} z &= \left(a\bar{c} + b\bar{d}\right) / \left(|c|^2 + |d|^2\right), \\ t &= |ad - bc| \,/\, \left(|c|^2 + |d|^2\right), \\ \zeta &= \epsilon \left(|c|^2 + |d|^2\right)^{1/2}, \\ u &= c\zeta^{-1}, \\ v &= d\zeta^{-1}, \end{aligned}$$

and ϵ *is given by*

$$\epsilon = \left((ad - bc) \,/\, |ad - bc|\,\right)^{1/2}.$$

Moreover, in the decomposition (3.8), t *and* z *are uniquely determined, and* ζ, u *and* v *are unique up to choice of the sign of* ϵ.

Proof. By (3.6), $g \cdot j = z + \epsilon^2 tj$, where z, t and ϵ are as stated. Hence by (3.3), $\epsilon^{-1} g \cdot j = z + tj$. By (3.7) and Lemma 42,

$$\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}^{-1} \epsilon^{-1} g \in \mathbb{R}^{\times} \cdot \mathrm{SU}(2),$$

giving an equation of the form (3.8), for some ζ, u and v; taking determinants in (3.8) shows that ζ is as stated, and multiplying out the bottom row that u and v are as stated. The uniqueness follows from $B \cap ZK = \{1_2\}$ and $Z \cap K = \{\pm 1_2\}$. □

There is an obvious bijection $B \to \mathfrak{H}_3$ given by

$$\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \mapsto (z, t). \tag{3.9}$$

Since $B \cap ZK = \{1_2\}$, the group B may also be identified with the coset space G/ZK. Write $\pi\colon G \to \mathfrak{H}_3$ for the map $G \to G/ZK \to B \to \mathfrak{H}_3$; thus $\pi|_B$ is the map (3.9). The coset action of G on G/ZK induces a left action of G on $\mathfrak{H}_3$ by

$$g \cdot (z, t) = \pi \left(g \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \right). \tag{3.10}$$

Explicitly, for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$,

$$g \cdot (z, t) = (z', t'), \tag{3.11}$$

where

$$z' = \frac{(az + b)\overline{(cz + d)} + a\bar{c}t^2}{|cz + d|^2 + |ct|^2}, \qquad t' = \frac{|ad - bc| t}{|cz + d|^2 + |ct|^2}. \tag{3.12}$$

Notice that (3.6) and (3.12) are not quite the same: the t' of (3.6) has been replaced by its modulus.

The space $\mathfrak{H}_3$ may be equipped with the Riemannian metric

$$ds^2 = \frac{dz\, d\bar{z} + dt^2}{t^2},$$

and G acts by isometries. The induced topology is just the Euclidean topology, but the geometry is hyperbolic: the geodesic lines are vertical half-lines and vertical semi-circles with centre in the plane $t = 0$; the geodesic surfaces are vertical half-planes and hemispheres with centre in the plane $t = 0$. We prove below (see Proposition 44) that G acts transitively on these geodesic surfaces.

Definition. A *fundamental domain* or *fundamental region* for the action of a group G on a topological space X is an open set U such that each orbit of G meets U at most once and meets the closure $\bar{U}$ of U at least once.

This definition is rather too general to be of much use, since it does not ensure that U is at all well-behaved — for example, condition (iii) below may fail — so in practice one looks for "good" fundamental domains. For a detailed discussion in the case of Fuchsian groups acting on the hyperbolic plane, see [Bea83, Chapter 9]. We are concerned with the case of certain groups acting on the spaces $X = \mathbb{C}$ (with the Euclidean metric) and $X = \mathfrak{H}_3$ (with the hyperbolic metric). We shall avoid dwelling on the topological niceties, but the fundamental regions we construct do have the following, desirable properties:

(i) U is convex (i.e. U contains the geodesic line segment joining any two points of U);

(ii) U is "locally finite" (i.e. each compact subset of X meets $g\bar{U}$ for only finitely many $g \in G$);

(iii) the map $G\backslash\bar{U} \to G\backslash X$ induced by the inclusion $\bar{U} \to X$ is a homeomorphism;

(iv) the boundary of U is the union of finitely many geodesic line segments (and, in the case $X = \mathfrak{H}_3$, polygons).

3.2 Hermitian forms

It is well-known that the reduction theory for positive-definite binary quadratic forms over $\mathbb{Z}$ (due to C. F. Gauß) may be interpreted geometrically: a form corresponds to a point in the upper half plane $\mathfrak{H}_2$, the actions of $\mathrm{SL}(2, \mathbb{Z})$ on forms (by change of variable) and on $\mathfrak{H}_2$ (by formula (2.1)) are compatible, and "reduced" forms correspond to points in (the closure of) the usual fundamental domain for the action of $\mathrm{SL}(2,\mathbb{Z})$, namely

$$\left\{ z \in \mathfrak{H}_2 \;\middle|\; |\Re z| < \frac{1}{2},\ |z|^2 > 1 \right\}. \tag{3.13}$$

There is a similar reduction theory, due to Bianchi [Bia92] and Humbert [Hum15], for positive-definite binary Hermitian forms under the action of $\mathrm{SL}(2,\mathfrak{O})$, where $\mathfrak{O}$ is the ring of integers of an imaginary quadratic field k. Building on their work, Swan [Swa71] gave a method (which we shall use) for finding fundamental domains analogous to (3.13).

Let $F(u,v)$ be a binary Hermitian form; thus, writing $*$ for the Hermitian conjugate (i.e. the conjugate transpose), $F(u,v) = \mathbf{x}M\mathbf{x}^*$, where $\mathbf{x} = (u\ v)$ and $M = M^* = \left(\begin{smallmatrix} a & w \\ \bar{w} & d \end{smallmatrix}\right)$. Then F is positive-definite if and only if $a > 0$, $d > 0$ and $ad - w\bar{w} > 0$ (see, for example, [Coh82, §8.3, Thm 6]). Replacing F by $d^{-1}F$, we may write the matrix as

$$\begin{pmatrix} |z|^2 + t^2 & z \\ \bar{z} & 1 \end{pmatrix}$$

for $(z,t) \in \mathfrak{H}_3$, corresponding to the form $F(u,v) = |uz+v|^2 + |ut|^2$. Thus, each point of $\mathfrak{H}_3$ represents an equivalence class of positive-definite binary Hermitian forms modulo scaling by positive real numbers.

The group $\mathrm{GL}(2,\mathbb{C})$ acts on the left on forms by $(gF)\mathbf{x} = F(\mathbf{x}g)$. Suppose the form $F\mathbf{x} = \mathbf{x}M\mathbf{x}^*$ corresponds to (z,t) and let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{C})$. Then $(gF)\mathbf{x} = (\mathbf{x}g)M(\mathbf{x}g)^* = \mathbf{x}M'\mathbf{x}^*$, where

$$M' = gMg^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} |z|^2 + t^2 & z \\ \bar{z} & 1 \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} f(a,b) & w \\ \bar{w} & f(c,d) \end{pmatrix}$$

with $w = (az+b)(\overline{cz+d}) + a\bar{c}t^2$. Thus gF corresponds to (z',t'), where $z' = w/f(c,d)$ and $(t')^2 = \det M'/f(c,d)^2$. Since $\det M' = |ad-bc|^2 t^2$, one obtains (3.12). We remark that Swan's formula is slightly different (with both b and c negated) since he starts from the right-action $(gF)\mathbf{x} = F(g^{-1}\mathbf{x})$, where $\mathbf{x}$ is now a column vector.

Proposition 44. *Let A be the set consisting of all vertical (half) planes in $\mathfrak{H}_3$ and all hemispheres in $\mathfrak{H}_3$ with centre in the plane $t = 0$. Then* $\mathrm{GL}(2,\mathbb{C})$ *acts transitively on A.*

Proof. This is a strengthened version of Lemma 3.4(1) of [Swa71], which did not mention transitivity. Write $G = \mathrm{GL}(2,\mathbb{C})$. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, define

$$H(g) = \{\, F \in \mathfrak{H}_3 \mid F(a,b) = F(c,d) \,\}.$$

Let $A' = \{\, H(g) \mid g \in G \,\}$. For $g, h \in G$, a trivial calculation gives $h \cdot H(g) = H(gh^{-1})$. Hence G acts transitively on A'. We show that $A' = A$. First, note that

$$\begin{aligned} H(g) &= \left\{(z,t) : |az+b|^2 + t^2|a|^2 = |cz+d|^2 + t^2|c|^2\right\} \\ &= \left\{(z,t) : (|a|^2 - |c|^2)(|z|^2 + t^2) + (a\bar{b} - c\bar{d})z + (\bar{a}b - \bar{c}d)\bar{z} = |d|^2 - |b|^2\right\}. \end{aligned}$$

If $|a| = |c|$ then t is arbitrary and $wz + \overline{wz}$ is constant, where $w = a\bar{b} - c\bar{d}$; since $w \neq 0$ (else $(ad-bc)\bar{c} = 0$, implying $ad - bc = 0$, a contradiction), z lies on a straight line as required. If $|a| \neq |c|$, then completing the square and using

$$\frac{(|d|^2 - |b|^2)(|a|^2 - |c|^2) + (\bar{a}b - \bar{c}d)(a\bar{b} - c\bar{d})}{(|a|^2 - |c|^2)^2} = \left(\frac{|ad-bc|}{|a|^2 - |c|^2}\right)^2$$

gives

$$H(g) = \left\{(z,t) :\ t^2 + \left|z + \frac{(\bar{a}b - \bar{c}d)}{|a|^2 - |c|^2}\right|^2 = \left(\frac{|ad-bc|}{|a|^2-|c|^2}\right)^2\right\},$$

a hemisphere as required. Thus $A' \subseteq A$. Conversely, A' certainly contains the unit hemisphere centred at $(0,0)$, and the vertical plane above the imaginary axis, since

$$H(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \{\, (z,t) \bigm| |z|^2 + t^2 = 1 \,\}, \qquad H(\left(\begin{smallmatrix} 1 & -1/2 \\ 1 & 1/2 \end{smallmatrix}\right)) = \{\, (z,t) \mid t > 0,\ z + \bar{z} = 0 \,\}.$$

Since A' is closed under translations (given by $\left(\begin{smallmatrix} 1 & w \\ & 1 \end{smallmatrix}\right)$ for $w \in \mathbb{C}$), rotations about the axis $z = 0$ through an angle θ (given by $\left(\begin{smallmatrix} w & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where $w = \exp(i\theta)$) and enlargements (given by $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for $a \in \mathbb{R}_{>0}$), it contains all planes and hemispheres, i.e. $A' \supseteq A$. Hence $A' = A$. □

3.3 Some geometry of $\mathbb{Q}(\sqrt{-d})$

Notation. In the rest of this chapter, we let k be an imaginary quadratic field with ring of integers $\mathfrak{O}$, and write $k = \mathbb{Q}(\sqrt{-d})$, where $d \in \mathbb{N}$ is square-free. We let $\Gamma = \mathrm{GL}(2,\mathfrak{O})$, and let Δ be the normaliser of Γ in $\mathrm{GL}(2,k)$, as in §1.4. We call $\mathbb{P}^1(k) = k \cup \{\infty\}$ the set of *cusps* (as in §1.5). We identify k with $k \times \{0\} \subset \mathbb{C} \times \mathbb{R}$, and define the *extended upper half-space* $\mathfrak{H}_3^*$ by

$$\mathfrak{H}_3^* = \mathfrak{H}_3 \cup k \cup \{\infty\}.$$

We single out certain elements of Γ of special importance. Let ϵ be a generator of the unit group $\mathfrak{O}^\times$; it is natural to choose $\epsilon = e^{2\pi i/n}$, where n is the order of $\mathfrak{O}^\times$, i.e.

$$\epsilon = \begin{cases} \sqrt{-1} & \text{if } d = 1 \\ (1+\sqrt{-3})/2 & \text{if } d = 3 \\ -1 & \text{otherwise.} \end{cases}$$

We define

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}.$$

Clearly $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for $n \in \mathbb{Z}$. More generally, for $a \in \mathfrak{O}$, we *define*

$$T^a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

The map $a \mapsto T^a$ is an isomorphism of the additive group of $\mathfrak{O}$ onto the subgroup $\Gamma_1^1(0)$ of Γ. We refer to T^a as "a power of T". The action of T^a and U on $\mathbb{C}$ and $\mathfrak{H}_3$ is as follows; clearly T^a acts by translation and U by rotation.

$$T^a \cdot z = z + a, \qquad U \cdot z = \epsilon z,$$
$$T^a \cdot (z,t) = (z+a,t), \qquad U \cdot (z,t) = (\epsilon z, t).$$

A natural choice of fundamental region for $\mathbb{C}$ with respect to translations is the set

$$F_T = \left\{ z \in \mathbb{C} \;\middle|\; |z| < |z-a| \text{ for all non-zero } a \in \mathfrak{O} \right\}, \tag{3.14}$$

called the *Poincaré polygon* with centre 0 for the group of translations acting on $\mathbb{C}$. The translates of F_T tessellate $\mathbb{C}$, as shown in Figure 3.1; the region F_T is either a rectangle or a hexagon, according to the shape of the lattice of integers: recall that an integral basis for $\mathfrak{O}$ is $\{1, \omega\}$, where

$$\omega = \begin{cases} \sqrt{-d} & \text{if } d \equiv 1,2 \pmod 4, \\ (1+\sqrt{-d})/2 & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

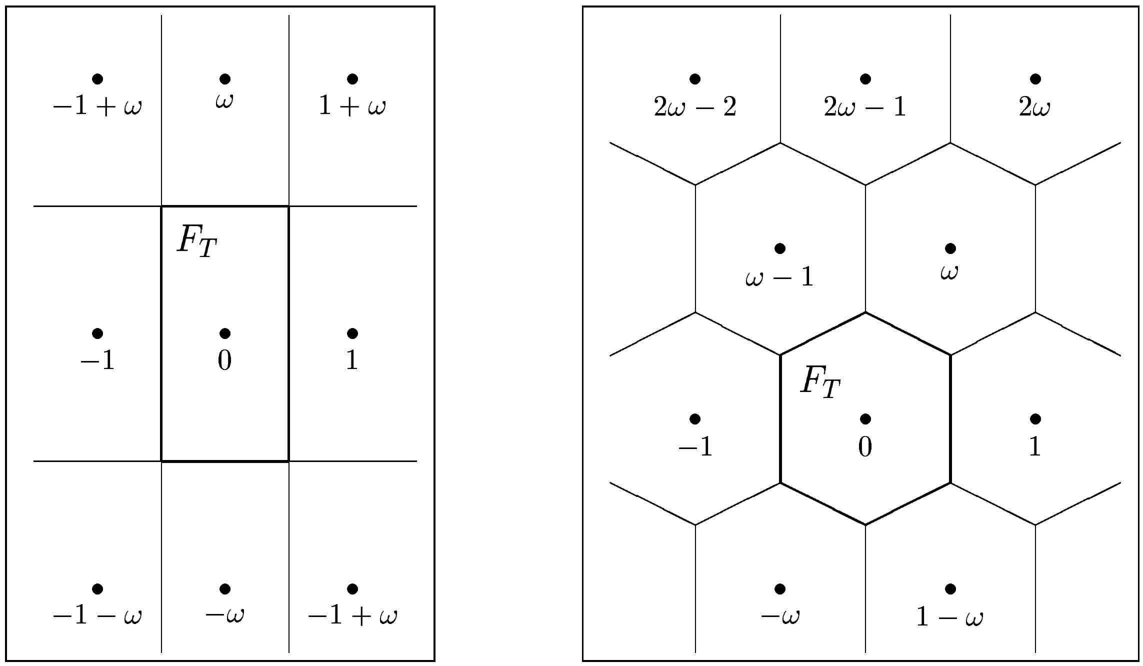

Figure 3.1: Fundamental regions F_T for translations for $d \equiv 1, 2$ and $d \equiv 3 \pmod 4$

Lemma 45. *The stabiliser of* ∞ *under the action of* Γ *is* $\mathfrak{O}^\times\Gamma_1(0)$ *and under the action of* Δ *is* $k^\times\Gamma_1(0)$, *where*

$$\Gamma_1(0) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \mathfrak{O}^\times,\ b \in \mathfrak{O} \right\}.$$

Proof. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta$ stabilise ∞. Then $c = 0$, so $\langle M \rangle = \langle a \rangle = \langle d \rangle$. Thus $a/d \in \mathfrak{O}^\times$ and $d^{-1}M \in \Gamma_1(0)$. □

Clearly $\Gamma_1(0)$ is generated by U and the powers of T. To obtain a fundamental region F for $\Gamma_1(0)$, we need to take account of the symmetries of F_T which lie in $\Gamma_1(0)$, i.e. of the rotations given by the powers of U. If $d \notin \{1, 3\}$, there is just two-fold symmetry, but if $d = 1$, the rectangle F_T is actually a square, with four-fold symmetry, and if $d = 3$ the hexagon F_T is regular and has six-fold symmetry. Thus F is obtained by cutting F_T into 2, 4 or 6 pieces. When $d \neq 3$, we can always obtain a rectangle (in the case $d \equiv 3$ this requires us to replace parts of the region $\{ z \in F_T \mid \Re z > 0 \}$ by equivalent parts). We obtain, for example

$$F = \left\{ x + y\sqrt{-d} \,\middle|\, 0 < x < 1/2,\ -1/2 < y < 1/2 \right\} \quad \text{if } d \neq 1 \text{ but } d \equiv 1, 2 \pmod 4,$$
$$F = \left\{ x + y\sqrt{-d} \,\middle|\, 0 < x < 1/2,\ -1/4 < y < 1/4 \right\} \quad \text{if } d \neq 3 \text{ but } d \equiv 3 \pmod 4,$$
$$F = \left\{ x + y\sqrt{-d} \,\middle|\, 0 < x < 1/2,\ 0 < y < 1/2 \right\} \quad \text{if } d = 1,$$
$$F = \{ z \in \mathbb{C} \mid 0 < \Re z < 1/2,\ |\arg z| < \pi/6 \} \quad \text{if } d = 3.$$

Later, we will make use of the symmetry $z \mapsto \bar{z}$; this is not in Γ, but allows us to obtain all the geometry from just half of the region F.

3.4 Theory of hemispheres

Recall that $\mathfrak{O}$ is called *norm-Euclidean* if and only if for every $\beta \in k$ there exists $a \in \mathfrak{O}$ with $|\beta - a| < 1$, i.e. if and only if the norm function $\mu \mapsto \mathbf{N}(\mu)$ is a Euclidean function for $\mathfrak{O}$ (engendering a Euclidean algorithm). It is clear from Figure 3.1 that this is so if and only if $d \in \{1, 2, 3, 7, 11\}$, and it is well-known that $\mathfrak{O}$ is a Euclidean domain for no other values of d [ST87, §4.7]. The Euclidean algorithm for $\lambda, \mu \in \mathfrak{O}$ may be interpreted geometrically as follows:

(1) Translation step: if $\mu = 0$ then stop, otherwise choose $a \in \mathfrak{O}$ such that $|\frac{\lambda}{\mu} - a| < 1$, and apply T^{-a} to $\binom{\lambda}{\mu}$, i.e. replace λ by $\lambda - a\mu$;

(2) Inversion step: apply the matrix $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to $\binom{\lambda}{\mu}$, i.e. replace λ/μ by $-\mu/\lambda$, and go to (1).

The two steps reduce $|\mu|$, the size of the denominator. Since $|\mu|^2 \in \mathbb{N}_0$, this can happen only finitely many times before μ becomes zero. Multiplying together the matrices that arise yields a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathfrak{O})$ such that $M\binom{\lambda}{\mu} = \binom{f}{0}$; here $f = a\lambda + b\mu$ is a greatest common divisor of λ and μ. (Notice that if $\lambda, \mu \in \mathbb{Z}$, then one may take $a \in \mathbb{Z}$ in step (1), and obtains $M \in \mathrm{SL}(2, \mathbb{Z})$; thus the algorithm as stated above subsumes the Euclidean algorithm for $\mathbb{Z}$.)

Let $M' \in \Gamma$. Applying the algorithm to $M' \cdot \infty$ yields a matrix $M \in \mathrm{S}\Gamma$, expressed as a word in the matrices T, T^{ω} and S (and their inverses), such that $MM' \cdot \infty = \infty$, i.e. $MM' \in \mathfrak{O}^{\times}\Gamma_1(0)$.

Corollary 46. *For $d \in \{1, 2, 3, 7, 11\}$, the group Γ is generated by T, T^ω, S, U and ϵI, and a similar result holds for* $\mathrm{S}\Gamma$.

The algorithm depends critically on the geometrical fact that (for these fields k) every $\beta \in k$ lies within one of the circles (or hemispheres) of radius 1 centred on the integers $a \in \mathfrak{O}$ (in fact, every $z \in \mathbb{C}$ does, but this fact is not needed). We say that these circles "cover the floor" of $\mathfrak{H}_3$.

Swan's paper [Swa71] generalises Corollary 46 to other values of d, by developing geometrical ideas of Bianchi [Bia92] and Humbert [Hum15]. The basic idea is to associate hemispheres to all principal cusps λ/μ, where the radii diminish as the size of the denominator μ grows. This wider class of hemispheres covers the floor if and only if $\mathfrak{O}$ is a principal ideal domain, i.e. precisely for the further values $d \in \{19, 43, 67, 163\}$. These were the fields studied by Whitley [Whi90], who describes an algorithm (for which she coins the phrase "pseudo-Euclidean") similar to the one above. For other values of d, there exist non-principal ideals in $\mathfrak{O}$; this is equivalent to the geometrical fact that there exist "singular points" which are still not covered by a hemisphere.

Below, we describe the relevant theory, with particular attention to pseudo-Euclidean algorithms. At the same time, we show that there is a theory for the group Δ, entirely parallel to Swan's, that makes use of a yet wider class of hemispheres (we term these "semi-principal"). The advantage of working with Δ is that it simplifies the geometry: in particular, it can reduce the number of singular points, even eliminating them when $C = C(2)$ in the notation of §1.4, such as when k has class number 2.

Definition. The *pseudo-Euclidean function* for k is the function $\psi\colon \mathbb{P}^1(k) \to \mathbb{N}_0$ given by

$$\frac{\lambda}{\mu} \mapsto \frac{\mathbf{N}\langle\mu\rangle}{\mathbf{N}\langle\lambda,\mu\rangle}.$$

This is well-defined for much the same reason as $cl(\lambda/\mu)$; see §1.5. Clearly $\psi(\alpha) = 0$ if and only if $\alpha = \infty$ (since $\mathbf{N}\langle 0\rangle = 0$, by definition), whilst k is mapped into $\mathbb{N}$, since $\langle\lambda,\mu\rangle \mid \langle\mu\rangle$ when $\mu \neq 0$. Note that $\psi(\alpha) = 1$ if and only if $\alpha \in \mathfrak{O}$. If $\alpha = \lambda/\mu$ is a principal cusp written in lowest terms, then $\psi(\alpha) = \mathbf{N}(\mu) = |\mu|^2$. Thus ψ generalises the notion of "size of the denominator".

Definition. For $\alpha \in k$, the *hemisphere attached to* α, denoted S_α, is the set

$$S_\alpha = \left\{ (z,t) \in \mathfrak{H}_3 \;\middle|\; |z-\alpha|^2 + t^2 = \frac{1}{\psi(\alpha)} \right\}.$$

In hyperbolic space, this is a geodesic surface; in Euclidean space, it is a hemisphere. Its complement has two components, the inside (where t is bounded) and the outside (where t is unbounded). Thus, we say that a point $(z,t) \in \mathfrak{H}_3$ *lies under* S_α, or that S_α *covers* (z,t), if (and only if)

$$|z-\alpha|^2 + t^2 < \frac{1}{\psi(\alpha)}.$$

Definition. For $\alpha \in k$, the *circle attached to* α, denoted C_α, is the set

$$C_\alpha = \left\{ z \in \mathbb{C} \;\middle|\; |z-\alpha|^2 = \frac{1}{\psi(\alpha)} \right\}.$$

Clearly, C_α is a circle in $\mathbb{C}$; in particular, it is a closed curve, whose complement has two components, the "inside" (which contains α) and the "outside" (which contains ∞). Moreover, C_α is the boundary of S_α regarded as a subset of $\mathfrak{H}_3 \cup \mathbb{P}^1(\mathbb{C})$, and $C_\alpha \cap k$ is the boundary of S_α regarded as a subset of $\mathfrak{H}_3^*$.

It is convenient to define $S_\infty = \mathfrak{H}_3$ and $C_\infty = \mathbb{P}^1(\mathbb{C})$. (As motivation for this convention, we mention that our set S_α is the set of points equidistant from ∞ and α as measured by Siegel's distance function, i.e. the set denoted $S(\infty, \alpha)$ in [Vog85, p402].)

Lemma 47. *Let $(z,t) \in \mathfrak{H}_3$. Then the set of cusps α such that S_α covers (z,t) is finite.*

Proof. By Lemma 38 and the remark preceding it, there exists a bound B such that every cusp may be written in the form λ/μ with $\mathbf{N}\langle \lambda, \mu \rangle \le B$. Suppose that S_α covers (z,t) and write $\alpha = \lambda/\mu$ in this way. Then

$$\frac{\mathbf{N}\langle \mu \rangle}{B} \le \psi(\alpha) < \frac{1}{t^2}.$$

So only finitely many values of μ can occur, and for each, since $|\mu z - \lambda|^2 + |\mu t|^2 < B$, only finitely many values of λ are possible. ∎

In practice, since k is imaginary quadratic, we may take for B the Minkowski bound $\frac{2}{\pi}\sqrt{|\delta|}$, or Kneser's stronger bound $\sqrt{|\delta|/3}$, where δ is the discriminant of k [Swa71, §7].

Definition. Let $\alpha \in \mathbb{P}^1(k)$ be a cusp; we say that α is *semi-principal* if $cl(\alpha)^2$ is trivial, i.e. if $cl(\alpha) \in C(2)$ in the notation of §1.4. A hemisphere S_α or a circle C_α is *principal* if α is principal, and *semi-principal* if α is semi-principal.

Lemma 48. *A cusp α is semi-principal if and only if $M \cdot \alpha = \infty$ for some $M \in \Delta$.*

Proof. Since ∞ is principal, this follows easily from Corollary 41: if M exists, then by (i) $\Longrightarrow$ (ii), there exists $\mathfrak{a}$ with both $\mathfrak{a}^2$ and $cl(\mathfrak{a})cl(\alpha)$ principal, whence α is semi-principal; conversely, if α is semi-principal, then any $\mathfrak{a}$ with $cl(\mathfrak{a}) = cl(\alpha)$ satisfies (ii). □

By attaching a hemisphere to every cusp, we introduced more hemispheres than we actually need: only semi-principal hemispheres occur in the sequel.

Lemma 49. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta$, let $\alpha = -d/c$, let $(z,t) \in \mathfrak{H}_3$, and let $(z',t') = M \cdot (z,t)$. Then*

$$\frac{t}{t'} = \begin{cases} 1 & \textit{if } \alpha = \infty, \\ \psi(\alpha)\big(|z-\alpha|^2 + t^2\big) & \textit{otherwise.} \end{cases}$$

Hence $t' > t$ if and only if (z,t) lies under the hemisphere S_α. Similarly, $t' = t$ if and only if $(z,t) \in S_\alpha$, and $t' < t$ if and only if (z,t) lies outside S_α.

Proof. Write $\mathfrak{a} = \langle M \rangle$. Since $\langle c, d \rangle = \mathfrak{a}$ (by Lemma 31) and $\mathfrak{a}^2 = \langle \det M \rangle$, we have $|\det M| = \mathbf{N}(\mathfrak{a}) = \mathbf{N}\langle c, d \rangle$. By (3.12), if $c \neq 0$ then

$$\frac{t}{t'} = \frac{|cz+d|^2 + |ct|^2}{|\det M|} = \frac{\mathbf{N}\langle c \rangle}{\mathbf{N}\langle c, d \rangle}\big(|z + \tfrac{d}{c}|^2 + t^2\big) = \psi(\alpha)\big(|z-\alpha|^2 + t^2\big).$$

If $c = 0$, then $\langle M \rangle = \langle a \rangle = \langle d \rangle$ by Lemma 31, so $d = \epsilon a$ for some $\epsilon \in \mathfrak{O}^\times$, whence $t/t' = |d/a| = |\epsilon| = 1$ (the last step needs k to be imaginary quadratic). The rest follows at once. □

In other words, if S_α covers (z,t), then applying M raises the "height" of (z,t) (but only finitely many greater heights can be attained, by Lemma 47). The points which cannot be raised, because they lie under no suitable hemisphere, are of special importance.

Definition. Let B_Γ (respectively, B_Δ) be the set of $(z,t) \in \mathfrak{H}_3$ that lie above all hemispheres S_α with $\alpha \in k$ principal (or semi-principal). The boundary of B_Γ (or B_Δ) will be called the *Bianchi diagram* for Γ (or Δ); see Figure 3.2 for an example.

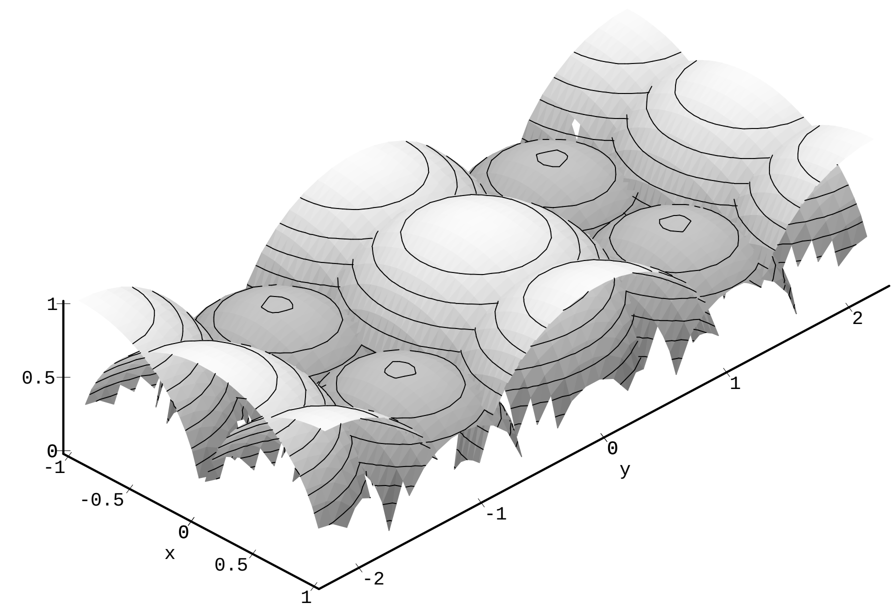

Figure 3.2: Bianchi diagram for Δ when $k = \mathbb{Q}(\sqrt{-5})$

The next result does for cusps what Lemma 49 did for interior points.

Lemma 50. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta$, let $\alpha = -d/c$, and let $\beta \in k \cup \{\infty\}$. Then*

$$\psi(M \cdot \beta) = \begin{cases} \psi(\beta) & \text{if } \alpha = \infty, \\ \psi(\alpha) & \text{if } \beta = \infty, \\ \psi(\alpha)\psi(\beta)|\beta - \alpha|^2 & \text{otherwise.} \end{cases} \tag{3.15}$$

Consequently, $\psi(M \cdot \beta) < \psi(\beta)$ if and only if β lies inside C_α, i.e. $|\beta - \alpha|^2 < 1/\psi(\alpha)$. Similarly, $\psi(M \cdot \beta) = \psi(\beta)$ if and only if $\beta \in C_\alpha$, and $\psi(M \cdot \beta) > \psi(\beta)$ if and only if β lies outside C_α.

Proof. Write $\beta = \lambda/\mu$, let $\lambda' = a\lambda + b\mu$ and $\mu' = c\lambda + d\mu$, so that $M \cdot \beta = \lambda'/\mu'$. By Lemma 40, $\langle \lambda', \mu' \rangle = \langle c, d \rangle \langle \lambda, \mu \rangle$. Thus,

$$\psi(M \cdot \beta) = \frac{\mathbf{N}\langle \mu' \rangle}{\mathbf{N}\langle \lambda', \mu' \rangle} = \frac{|c\lambda + d\mu|^2}{\mathbf{N}\langle c, d \rangle \, \mathbf{N}\langle \lambda, \mu \rangle}.$$

If $c = 0$, the right-hand side simplifies to $\psi(\beta)$, and if $\mu = 0$, to $\psi(\alpha)$. Hence (3.15) follows. When $\alpha = \infty$, the corollary holds vacuously (since C_∞ has neither an inside nor an outside), and otherwise, it follows from (3.15). □

In other words, if β lies inside C_α, then applying M reduces the "size" of β as measured by ψ. In view of this, the points (if any) that lie inside no C_α are of special importance.

Definition. A cusp $\beta \in \mathbb{P}^1(k)$ is *singular with respect to* Γ, or Γ*-singular*, if it lies inside no principal C_α. Similarly, β is *singular with respect to* Δ, or Δ*-singular*, if it lies inside no semi-principal C_α.

Clearly ∞ is singular, and if β is Δ-singular, then it is Γ-singular.

Corollary 51. *Let $\beta \in \mathbb{P}^1(k)$. Then β is Γ-singular if and only if $\psi(\beta)$ is minimal for points in the Γ-orbit of β. Similarly, β is Δ-singular if and only if $\psi(\beta)$ is minimal for points in the Δ-orbit of β.*

Proof. Assume that β lies inside some principal (respectively, semi-principal) C_α. By Lemma 48, there exists $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ (respectively, $M \in \Delta$) such that $\alpha = -d/c$; hence by Lemma 50, $\psi(M \cdot \beta) < \psi(\beta)$, so $\psi(\beta)$ is not minimal. Conversely, if $\psi(\beta)$ is not minimal, then by Lemma 50, β lies inside some suitable C_α. □

It follows at once from Lemma 39 that ∞ is the unique singular point if and only if $h = 1$, where h is the class number of k. A detailed discussion of singular points may be found in Swan's paper [Swa71]. In fact, he considers points $z \in \mathbb{C}$, defining z to be singular if and only if (in our notation) z lies inside no principal C_α, but goes on to show, by Diophantine approximation, that singular points necessarily lie in k. Thus our Γ-singular points are precisely Swan's singular points together with ∞.

Swan proves that there are only finitely many singular points modulo translations by elements of $\mathfrak{O}$; moreover, he gives an explicit construction for determining representative singular points $s_1, \ldots, s_n \in k$ such that for each singular point $s \neq \infty$ there exists i with $s - s_i \in \mathfrak{O}$. It is clear that that there is at least one s_i in each Γ-orbit of non-principal cusps, i.e. for each non-principal ideal class. In general, there may be more than one: two singular points lying in a fundamental region F (as in §3.3) may be Γ-equivalent (but obviously not $\Gamma_1(0)$-equivalent). This phenomenon does not arise for $k = \mathbb{Q}(\sqrt{-5})$, when $n = 1$, so it will not concern us further.

3.5 Fundamental regions for the action of Γ and Δ on $\mathfrak{H}_3$

Let F be a fundamental region for $\mathbb{C}$ with respect to $\Gamma_1(0)$, such as the one constructed above (any reasonable choice of F will do). Define

$$D_\Gamma = \{\, (z,t) \in B_\Gamma \mid z \in F \,\}, \qquad D_\Delta = \{\, (z,t) \in B_\Delta \mid z \in F \,\}.$$

Theorem 52. *The set D_Γ (respectively D_Δ) is a fundamental region for the action of Γ (respectively Δ) on $\mathfrak{H}_3$.*

Proof. We prove the result for Δ (the proof for Γ is similar, with Δ replaced throughout by Γ and "semi-principal" by "principal"). Let $(z,t) \in \mathfrak{H}_3$. If there is at least one semi-principal cusp α such that S_α covers (z,t), we may choose, from among the finitely many such cusps, one that minimises the quantity $\psi(\alpha)\big(|z-\alpha|^2+t^2\big)$; otherwise, put $\alpha = \infty$. Let $M \in \Delta$ be such that $M \cdot \alpha = \infty$, and put $(z',t') = M \cdot (z,t)$. Multiplying M on the left by an element of $\Gamma_1(0)$ if necessary, we may assume that $z' \in \bar{F}$. By Lemma 49, t' is maximal among t-coordinates of points in the Δ-orbit of (z,t), so no semi-principal hemisphere covers (z',t'). Consequently $M \cdot (z,t) \in \overline{D_\Delta}$.

Now let $(z,t), (z',t') \in D_\Delta$, and suppose $M \cdot (z,t) = (z',t')$ for some $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta$. Then $t \geq t'$, since $S_{-d/c}$ does not cover (z,t); by symmetry, $t = t'$. Hence (z,t) lies on $S_{-d/c}$, forcing $c = 0$, so (up to scalars) $M \in \Gamma_1(0)$. Since $z, z' \in F$, we deduce $z = z'$. □

Theorem 53. *The boundary ∂D_Γ (respectively ∂D_Δ) is defined by finitely many hemispheres S_{α_i} with α_i principal (respectively, semi-principal).*

Proof. For Γ, this was proved by Swan [Swa71]. The case of Δ is similar. □

Swan also gives an algorithm for finding the hemispheres on the boundary of D_Γ; for certain small values of d, the results are already in [Bia92]. The method is further discussed in [Whi90], and it is not necessary to give details here; however, we give several figures to help the reader to visualise the situation for $k = \mathbb{Q}(\sqrt{-5})$. Figure 3.6 shows that part of B_Δ lying above the region $\{\, x + y\omega \mid -1 \leq x \leq 1,\ -1 \leq y \leq 1 \,\}$, which consists of four copies of F_T; it is made up of 2-cells that are hyperbolic polygons. Figure 3.5 shows its 1-skeleton, and Figure 3.4 the projection into $\mathbb{C}$, which consists of Euclidean polygons. The correctness of these figures follows from the correctness of Figure 3.3, discussed below.

To find B_Δ for general k, one would need to modify Swan's algorithm suitably. But when $C = C(2)$ (so F contains no Δ-singular points) we can determine ∂D_Δ from ∂D_Γ with very little work. By adding the (semi-principal) hemispheres at the Γ-singular points, we obtain a "covering of the floor" whose lowest point is at (z, t), say, with $t > 0$. The only hemispheres which might improve this covering have $\psi(\alpha) < t^{-2}$, so only finitely many hemispheres come into consideration, and a finite refinement process yields ∂D_Δ.

For example, let $k = \mathbb{Q}(\sqrt{-5})$, so that $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}\omega$ where $\omega = \sqrt{-5}$. Let F be a fundamental region for $\mathbb{C}$ with respect to $\Gamma_1(0)$, as in §3.3 above. Making use of the symmetry

$$(z, t) \mapsto (\bar{z}, t) \tag{3.16}$$

we need only consider half of this region, say the region

$$Q = \left\{ x + y\omega \;\middle|\; 0 < x < \frac{1}{2},\ 0 < y < \frac{1}{2} \right\}.$$

There is one singular point in Q, namely $(1 + \omega)/2$. The projection of ∂D_Γ and ∂D_Δ into the plane $\mathbb{C}$ consists of polygonal cells as shown in Figure 3.3 below. In the figure, (x, y) denotes the point $x + y\omega$, centres of covering hemispheres are denoted by small discs (i.e. •), thick lines indicate "true" edges formed where covering hemispheres intersect, and thin lines "spurious" edges (the terminology is from [Swa71]) which disappear when the symmetry (3.16) and elements of $\Gamma_1(0)$ are applied.

The left-hand diagram, for D_Γ, is taken from [Swa71]. Three hemispheres are required: (I) $S_{0/1}$, of radius 1, (II) $S_{\omega/2}$, of radius 1/2, and (III) S_α for $\alpha = (\omega - 4)/2\omega = (5 + 4\omega)/10$, of radius $\sqrt{5}/10$.

The corresponding diagram for D_Δ is simpler, requiring just two hemispheres: (I) $S_{0/1}$, of radius 1, and (II) $S_{(1+\omega)/2}$, of radius $\sqrt{2}/2$. It is easy to verify that this figure gives the best covering: its lowest point is at the vertex $2\omega/5$, where $t^2 = 1/5$, so only hemispheres with $\psi(\alpha) < 5$ might improve the covering, and in practice, they do not.

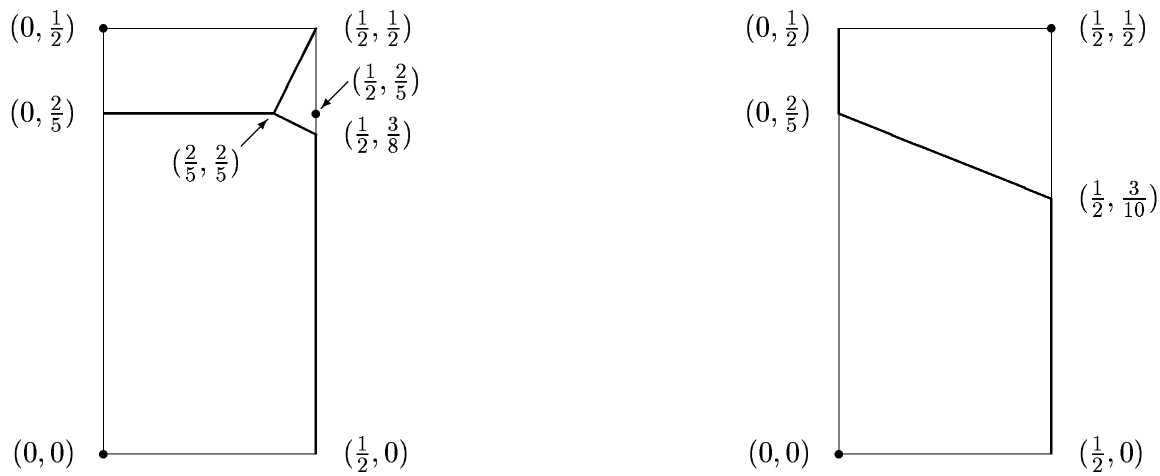

Figure 3.3: Cell decomposition of Q for Γ (left) and Δ (right) for $\mathbb{Q}(\sqrt{-5})$

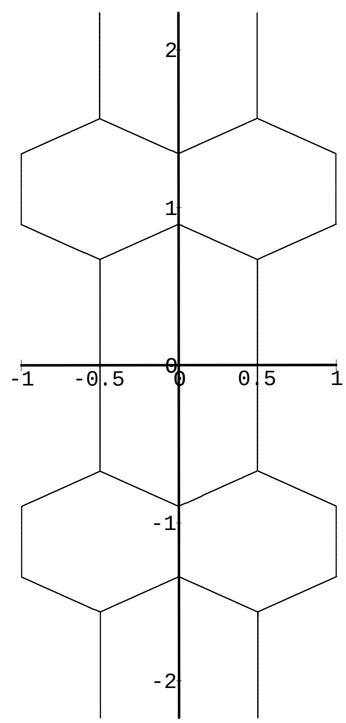

Figure 3.4: Projection of Figure 3.5 into $\mathbb{C}$

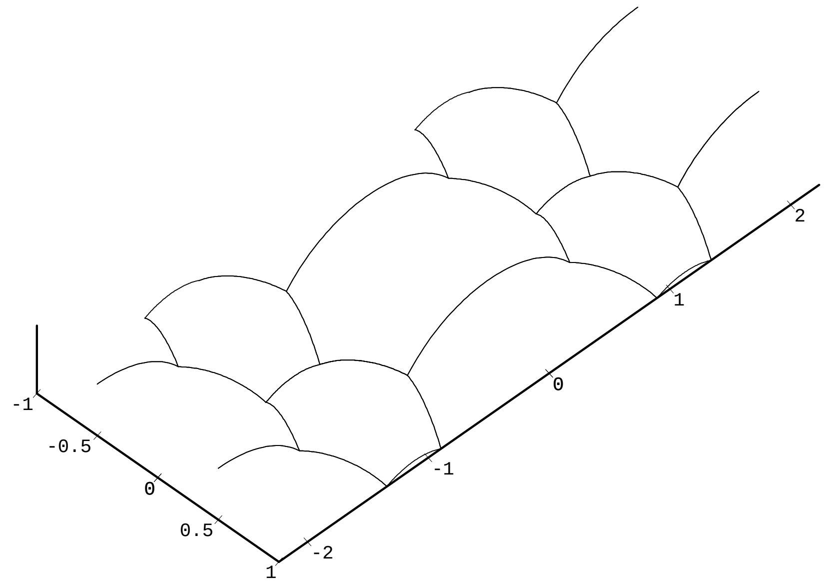

Figure 3.5: 1-skeleton of the Bianchi diagram for Δ when $k = \mathbb{Q}(\sqrt{-5})$

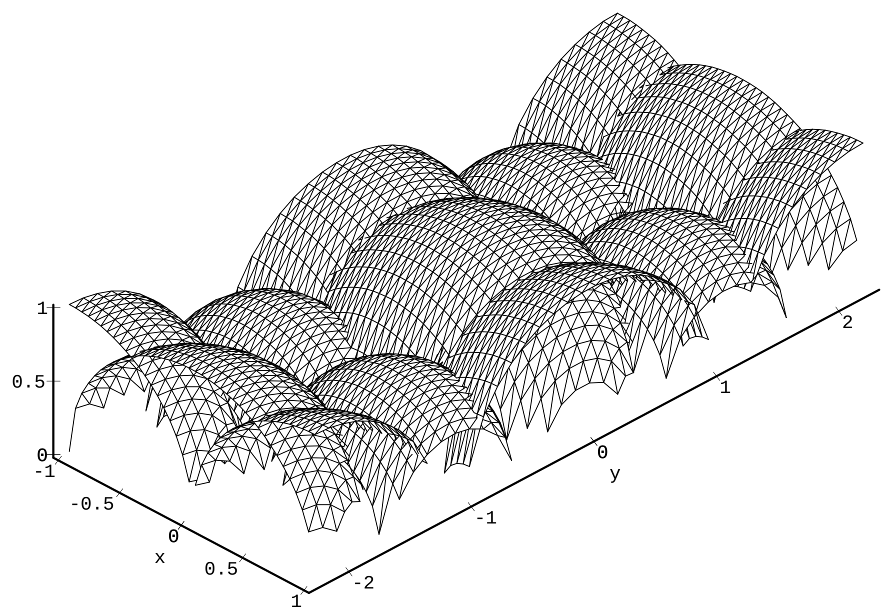

Figure 3.6: Bianchi diagram for Δ when $k = \mathbb{Q}(\sqrt{-5})$

3.6 Pseudo-Euclidean algorithms

Let $G = \Gamma$ or $G = \Delta$. Having determined the Bianchi diagram for G, we can give explicit "pseudo-Euclidean" algorithms. More precisely, we need to know:

(i) a fundamental domain F for $\mathbb{C}$ with respect to $\Gamma_1(0)$;

(ii) a sub-algorithm that returns, given $z \in \mathbb{C}$, a matrix $M \in \Gamma_1(0)$, expressed as a word in powers of T and U, such that $M \cdot z \in \bar{F}$;

(iii) a list $s_1, \dots, s_n$ of the G-singular points (if any) lying in $\bar{F}$, together with $s_0 = \infty$;

(iv) the decomposition of F into polygonal 2-cells, $P_1, \dots, P_m$, obtained by projecting ∂D_G into $\mathbb{C}$;

(v) for each $i \in \{1, \dots, m\}$, the cusp α_i such that P_i is the projection into $\mathbb{C}$ of the hyperbolic polygon $S_{\alpha_i} \cap \partial D_G$;

(vi) for each $i \in \{1, \dots, m\}$, an "inversion matrix" $S_i \in G$ such that $S_i \cdot \alpha_i = \infty$.

The sub-algorithm in (ii) is easiest if we take F_T given by (3.14) and obtain F by cutting F_T into pieces congruent under U. The "inversion matrices" in (vi) are constructed explicitly as follows. Write $\alpha_i = \lambda/\mu$. Put $\mathfrak{a} = \langle \lambda, \mu \rangle$. Then $\mathfrak{a}^2 = \langle \delta \rangle$, say, since α_i is semi-principal. Hence $\delta = -\lambda\lambda' - \mu\mu'$ for some $\lambda', \mu' \in \mathfrak{a}$. Put

$$M = \begin{pmatrix} \lambda' & \mu' \\ \mu & -\lambda \end{pmatrix} \in \mathrm{GL}(2, k).$$

Clearly $M \cdot \alpha_i = \infty$. Moreover, $\langle M \rangle = \langle \mu, -\lambda, \lambda', \mu' \rangle = \mathfrak{a}$, so by Proposition 28, $M \in \Delta$. When α_i is principal, one naturally chooses λ, μ so that $\mathfrak{a} = \mathfrak{O}$; in this case, $M \in \Gamma$. Of course, the matrix M constructed above is not unique: it may be replaced by AM for any A fixing ∞; there is no further freedom, since if $M \cdot \alpha = M' \cdot \alpha = \infty$, then $M^{-1} \cdot \infty = (M')^{-1} \cdot \infty$, so $M^{-1}M'$ fixes ∞. We always choose $A \in \Gamma_1(0)$ such that $AM \cdot \alpha_i \in \bar{F}$, and we let $S_i = AM$. For example, when $k = \mathbb{Q}(\sqrt{-5})$ and $G = \Delta$, we take

$$S_{0/1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad S_{(1+\omega)/2} = \begin{pmatrix} 1+\omega & 1-\omega \\ 2 & -1-\omega \end{pmatrix}.$$

Both matrices satisfy not only $M \cdot \alpha = \infty$, but also $M \cdot \infty = \alpha$. We should point out that for general k, it is not always possible to satisfy the last condition — see [Whi90] for examples. Also, there are examples when α_i does not lie in P_i.

3.6.1 Algorithm for interior points

Given $(z, t) \in \mathfrak{H}_3$, this algorithm returns a matrix M, expressed as a word in powers of T, U and the matrices S_i, such that $M \cdot (z, t) \in \overline{D_G}$.

(1) Apply a matrix in $\Gamma_1(0)$, found using the sub-algorithm under (ii) above, such that $z \in \bar{F}$.

(2) Find i such that $z \in \bar{P}_i$. If S_{α_i} covers (z, t), then apply the inversion matrix S_i and go to (1), otherwise stop.

This algorithm terminates because each inversion step increases t (by Lemma 49), which can happen only finitely many times (by Lemma 47); when it does so, clearly $(z, t) \in \overline{D_G}$. Multiplying together the matrices that arise gives the required M.

3.6.2 Algorithm for cusps

This algorithm maps any cusp to a G-singular point. More precisely, given $\beta \in \mathbb{P}^1(k)$, this algorithm returns a matrix M, expressed as a word in powers of T, U and the matrices S_i, such that $M \cdot \beta = s_j$ for some $j \in \{0, \ldots, n\}$.

(1) If $\beta = \infty$, then stop; otherwise, apply a matrix in $\Gamma_1(0)$, found using the sub-algorithm under (ii) above, such that $\beta \in \bar{F}$.

(2) If β is a singular point, then stop; otherwise, choose i such that β lies inside C_{α_i}, apply the inversion matrix S_i, and go to (1).

This algorithm terminates because each inversion step reduces the natural number $\psi(\beta)$ (by Lemma 50), which can happen only finitely many times; when it does so, β is clearly one of the singular points s_j. Multiplying together the matrices that arise gives the required M.

An immediate corollary is that G is finitely generated, namely by the matrices T, T^ω, U and the appropriate S_i; compare Corollary 46. Using these methods, one can also find the relations among these generators in order to give a presentation of G as an abstract group; for $G = \Gamma$, this was carried out by [Swa71].

Remark. These algorithms generalise those of Cremona [Cre81] and Whitley [Whi90]. Cremona considered the case when $\mathfrak{O}$ is Euclidean (so $G = \Gamma = \Delta$ and $n = 0$) and gave algorithm 3.6.1 for this case; there was no need to treat 3.6.2 explicitly, since it reduces to the ordinary Euclidean algorithm for $\mathfrak{O}$, as discussed in §3.4 above. Whitley considered the more general case $h = 1$ (so again $G = \Gamma = \Delta$ and $n = 0$); both algorithms are present in spirit, but the discussion blurs them together: in particular, the argument given to justify that 3.6.2 terminates was invalid (applying instead to 3.6.1) and the function ψ, which plays the vital rôle for us, had not been introduced.

3.7 Tessellations of $\mathfrak{H}_3^*$

In the following, we let $G = \Gamma$ or Δ; hemispheres will be understood to be principal or semi-principal accordingly. We write $B = B_G$.

We are interested in the vertices of the Bianchi diagram, i.e. the 0-cells of the cell decomposition of ∂B. They are the points above the "true vertices" (points where three or more "true edges" meet) of a figure such as Figure 3.3. They are clearly the points where the height of the covering of the floor has a local minimum ("where lakes form when it rains" [Sch92]), i.e. points $(z, t) \in \partial B$ for which there exists $\epsilon > 0$ such that $|z' - z| < \epsilon$ implies $(z', t) \notin \bar{B}$.

We consider the tessellation of $\mathbb{C}$ dual to the one shown in Figure 3.4, i.e. with vertices at the centres of the hemispheres making up the 2-cells of ∂B, and with two vertices joined by an edge if and only if the corresponding hemispheres meet at a 1-cell of ∂B. *We assume that each vertex of B lies above the polygon associated to it.*

Warning. This assumption is valid for $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 5\}$ but *not* for $d = 163$ [Whi90]. Indeed, this author is not convinced that Whitley's polyhedra are correct when $d = 163$, since her methods rely on "a simple geometrical argument" which she omits [p.93

op.cit.] and it is not clear what happens to that argument when the assumption fails. We should point out that for $d = 163$, Whitley gives ∂D, and claims to have 25 polyhedra, but does not actually list the polyhedra, and did not succeed in finding any newforms, although this may simply have been due to the relatively low bound on the level $\mathfrak{n}$ forced by the implementation [CW94]. It is a pity that Whitley did not tabulate "minusforms" (see §9.2), for one could have compared her result at level $\mathfrak{n} = \mathfrak{O}$ with that of Scheutzow, who gives $\dim V(\mathfrak{n}) = 6$ and $\dim V^+(\mathfrak{n}) = 0$ [Sch92]. It seems clear that more work is required on the case $d = 163$.

We choose our fundamental domain F to consist of some of these polygons, and define $D = D_G$ relative to this choice of F. Thus D is partitioned into a number of "spiky chimneys", one above each vertex. We shall obtain polyhedra which tessellate $\mathfrak{H}_3^*$ by gluing together copies of these chimneys. Note that the vertices of ∂D lie above interior points of F, so no two are $\Gamma_1(0)$-equivalent.

Example. Let $k = \mathbb{Q}(\sqrt{-5})$ and $G = \Delta$. We take for F the quadrilateral with vertices at 0, 1, $(1+\omega)/2$ and $(-1+\omega)/2$, consisting of two triangles, one on each side of the line from 0 to $(1+\omega)/2$. The vertices above $\bar{F}$ (their co-ordinates may be read off from Figure 3.3) are at

$$q = \left(\frac{2\omega}{5}, \frac{1}{\sqrt{5}}\right), \qquad r = \left(\frac{5+3\omega}{10}, \sqrt{\frac{3}{10}}\right).$$

Let v be a vertex above F. Our next task is to determine its stabiliser G_v in G, i.e. the set $G_v = \{\, M \in G \mid M \cdot v = v \,\}$. If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ fixes the vertex v, then so does M^{-1}; in particular, the height is unchanged by M and M^{-1}, so by Lemma 49, $v \in S_{-d/c}$ and $v \in S_{a/c}$; note that these two hemispheres (they need not be distinct, of course) have the same radius, since $\langle -d, c\rangle = \langle M \rangle = \langle a, c\rangle$. Thus, G_v is finite, and one could determine it as follows: write down the finite list of pairs λ, μ, with $\langle \lambda, \mu\rangle$ one of a fixed set of ideal class representatives, such that $v \in S_{\lambda/\mu}$; hence make a finite list of candidate matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$; test which of these fix v. But we can do better, since there is a converse result, as follows.

Given a vertex v and a hemisphere S_α through v, we can write down a unique inversion matrix $M_\alpha \in G$ (with $M_\alpha \cdot \alpha = \infty$) adjusted to that $M_\alpha \cdot v \in \bar{F}$. By Proposition 44, it maps hemispheres (and half-planes) through α to half-planes, and other hemispheres (and half-planes) to hemispheres; thus it maps S_α to another hemisphere.

In particular, suppose that $S_\alpha \cap \partial B$ is a polygonal 2-cell with a vertex at v. Then applying M_α maps each point of this 2-cell to another point at the same height; these image points lie on a hemisphere, but cannot lie under any other hemisphere (since they cannot be raised) hence form part of ∂B; in particular, v, being a local minimum, is mapped to a vertex, and this vertex lies above F.

Suppose for simplicity that v is the unique vertex above F of its height (this holds, for example, when $d = 19$, and when $d = 5$ and $G = \Delta$; it does not hold for $d \in \{43, 67, 163\}$ [Whi90], and in such cases one must consider several v together). Then $M_\alpha \in G_v$, and the above construction shows that each 2-cell having a vertex at v gives rise to a unique element of G_v.

Proposition 54. *The elements of G_v so constructed generate G_v, and the transforms of the (closed) "chimney" above v fill out a neighbourhood of v.*

Proof. Let p be close to v but below ∂B. Then p is below one of the hemispheres S_α making up the 2-cells meeting at v; inverting in the corresponding M_α gives a higher point which is still close to v. After finitely many such steps, p has been moved into $\bar{B}$. This shows that the transforms fill out a neighbourhood of v, as claimed. Given $M \in G_v$, take p' lying just above v and put $p = M \cdot p'$; applying the above process to p maps it to a point close to v lying in B, hence back to p', and this expresses M in terms of the generators claimed (compare algorithm 3.6.1). □

Corollary 55. *Let $k = \mathbb{Q}(\sqrt{-5})$, let $G = \Delta$, and let q and r be as above. Then the stabiliser of q (modulo scalars) is given by the matrices*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B^2 = \begin{pmatrix} \omega & 2 \\ 2 & -\omega \end{pmatrix}, \quad B^2S = \begin{pmatrix} -2 & \omega \\ \omega & 2 \end{pmatrix},$$

$$B = \begin{pmatrix} 1+\omega & 2 \\ 2 & 1-\omega \end{pmatrix}, \quad BS = \begin{pmatrix} -2 & 1+\omega \\ -1+\omega & 2 \end{pmatrix},$$

$$B^3 = \begin{pmatrix} -1+\omega & 2 \\ 2 & -1-\omega \end{pmatrix}, \quad B^3S = \begin{pmatrix} -2 & -1+\omega \\ 1+\omega & 2 \end{pmatrix},$$

and the stabiliser of r (modulo scalars) is given by the matrices

$$TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad (TS)^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad R = \begin{pmatrix} 1+\omega & 1-\omega \\ 2 & -1-\omega \end{pmatrix},$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad RTS = \begin{pmatrix} 2 & -1-\omega \\ 1-\omega & -2 \end{pmatrix}, \qquad R(TS)^2 = \begin{pmatrix} -1+\omega & 2 \\ 1+\omega & 1-\omega \end{pmatrix}.$$

It is now straightforward to glue together copies of the "spiky chimneys" above q and r. Note for example that S, which stabilises q, interchanges 0 and ∞; thus the geodesic half-line from ∞ to $(0,1)$, which forms part of the boundary of the "chimney" above q, is joined with the half-line from 0 to $(0,1)$ to form the complete geodesic from 0 to ∞. A similar thing happens for the other edges, and the result is a so-called "ideal" polyhedron, i.e. a polyhedron with vertices at the cusps.

First consider the polyhedron P_q around q. It has one vertex at ∞, with edges leading to 0, $(\omega-1)/2$ and $(1+\omega)/2$, as depicted in Figure 3.7; in all our figures, principal cusps are depicted as circles, and non-principal cusps as squares. Applying each matrix in G_q in turn to this figure allows us to deduce the shape of the full polyhedron. It is a square prism, as depicted in Figure 3.8, and G_q is its symmetry group in Δ. Note that B acts by rotation of the square faces through a quarter turn.

Similarly, we find that the polyhedron P_r around r is a triangular prism, as depicted in Figure 3.9, and that TS acts by rotation of the triangles.

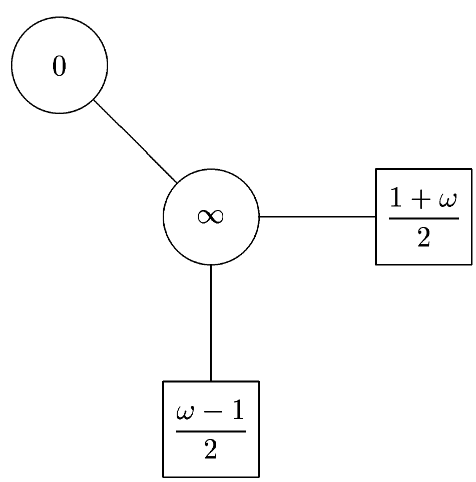

Figure 3.7: The infinite vertex of P_q

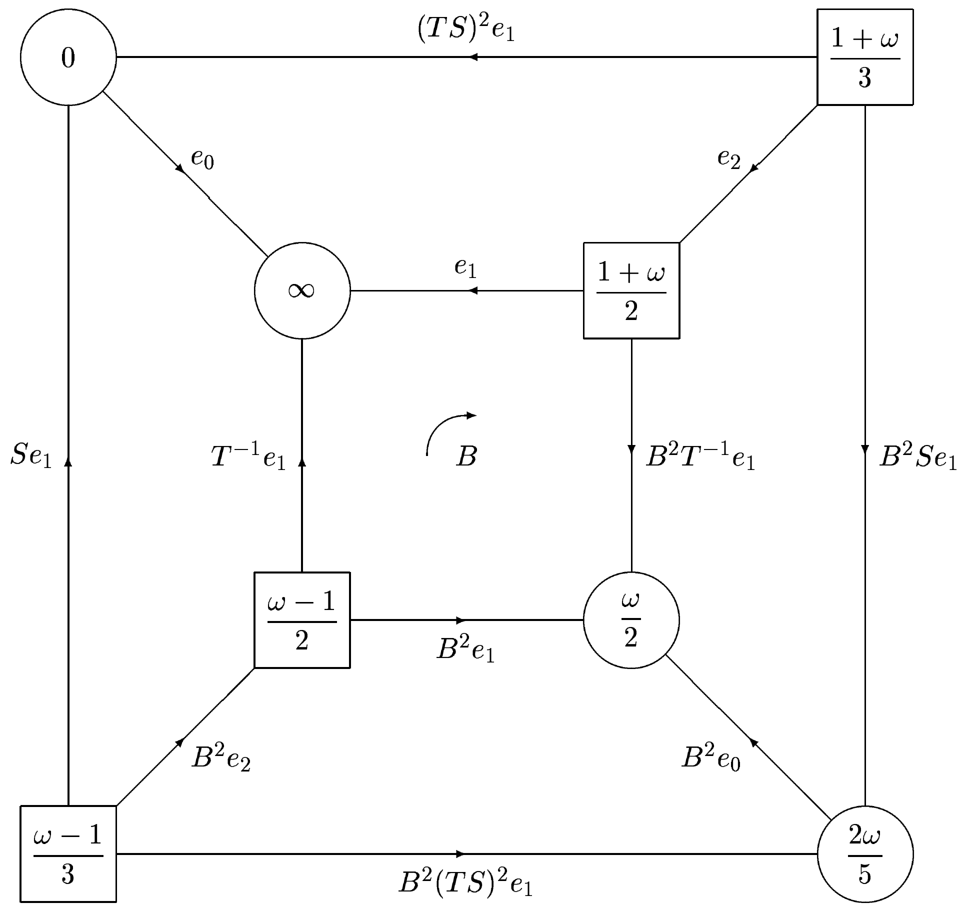

Figure 3.8: Polyhedron around q

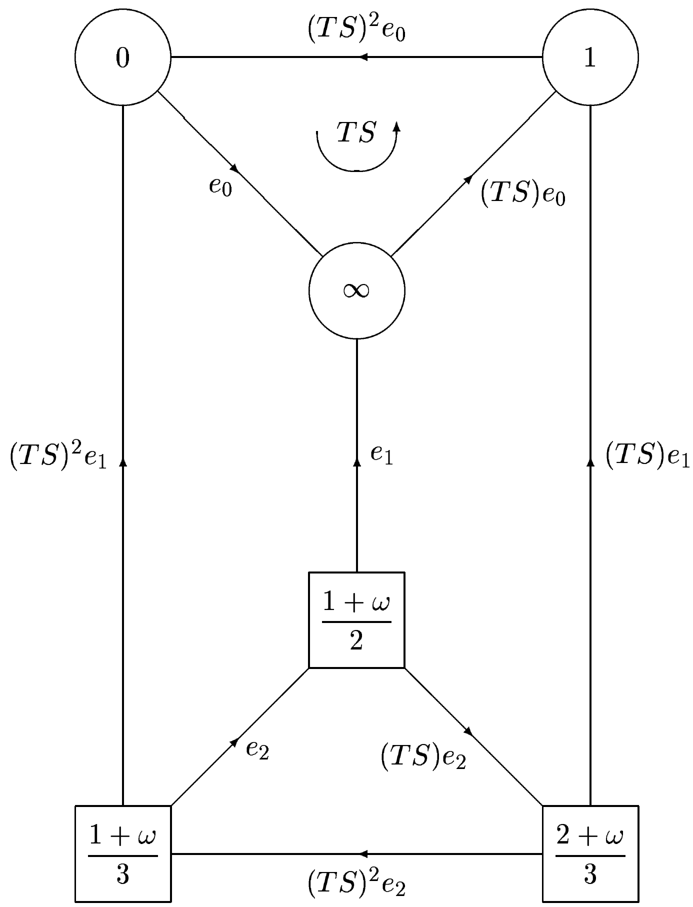

Figure 3.9: Polyhedron around r

3.8 Generators and relations for homology

It is clear that translates under Δ of our two "basic polyhedra" tessellate $\mathfrak{H}_3^*$, and that Δ acts on this tessellation. Exactly as in the work of Cremona and Whitley [Cre81, Whi90], we can read off generators and relations for computing the rational 1-homology of $\mathrm{P}\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$. There is a new feature, though: we can also work with $\mathrm{P}\Delta_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$. Recall from the remark at the end of §1.3, and from Corollary 37, that the M-symbols at level $\mathfrak{n}$ provide a set of right coset representatives for $\mathrm{P}\Gamma_0(\mathfrak{n})$ in $\mathrm{P}\Gamma$ and for $\mathrm{P}\Delta_0(\mathfrak{n})$ in $\mathrm{P}\Delta$.

3.8.1 Generators

The edges of our tessellation come in three "types": the number of end-points at non-principal vertices can be 0, 1 or 2, as for the edges e_0, e_1 and e_2 of Figure 3.8, respectively. Let $\gamma \in \Gamma$. Since γ preserves the class of each cusp, it preserves the "type" of an edge. Hence there are at least three Γ-orbits of edges; in fact, there are exactly three, represented by the edges e_0, e_1 and e_2. However, $e_2 = B \cdot e_0$, so there are just two Δ-orbits of edges.

With a view to the rôle of edges as modular symbols (c.f. §6.2.4), let us denote the directed edge from α to β by the symbol $\{\alpha, \beta\}$. Thus

$$e_0 = \{0, \infty\}, \qquad e_1 = \{\tfrac{1+\omega}{2}, \infty\}, \qquad e_2 = \{\tfrac{1+\omega}{3}, \tfrac{1+\omega}{2}\}.$$

Also, let us write, for each $\gamma \in \Delta$,

$$(\gamma) = \gamma \cdot e_0 = \{\gamma \cdot 0, \gamma \cdot \infty\}, \qquad [\gamma] = \gamma \cdot e_1 = \{\gamma \cdot \tfrac{1+\omega}{2}, \gamma \cdot \infty\}.$$

Thus $e_0 = (I)$, $e_1 = [I]$ and $e_2 = (B)$. Each edge of our tessellation has the form $\gamma \cdot e_i$ for some $i \in \{0, 1, 2\}$ and some $\gamma \in \Gamma$; thus the homology of $\mathrm{P}\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$ is generated by the $(c : d)e_i$, where $i \in \{0, 1, 2\}$ and $(c : d)$ runs through the set of M-symbols at level $\mathfrak{n}$. Similarly, the homology of $\mathrm{P}\Delta_0(\mathfrak{n})\backslash\mathfrak{H}_3^*$ is generated by the $(c : d)e_i$, where $i \in \{0, 1\}$ and $(c : d)$ runs through the set of M-symbols at level $\mathfrak{n}$.

3.8.2 "Edge relations"

There is some redundancy in our labelling of the generators: the stabiliser of the (un-ordered) edge e_i, when non-trivial, gives rise to "edge relations", which measure this redundancy. The stabiliser in Δ of the (undirected) edge e_0 is generated by U and S; note that U preserves the orientation, whilst S reverses it. Similarly, the stabiliser of the (undirected) edge e_1 is $\mathrm{gp}\langle A, R\rangle$, where $A = \left(\begin{smallmatrix} -1 & 1+\omega \\ 0 & 1 \end{smallmatrix}\right)$; here A preserves and R reverses the orientation. Thus, we obtain

$$(I) = (U) = -(S), \qquad [I] = [A] = -[R].$$

Working in Γ, we find that the stabilisers of e_0, e_1 and e_2 are, respectively,

$$\mathrm{gp}\langle U, S\rangle, \qquad \Gamma \cap \mathrm{gp}\langle A, R\rangle = \mathrm{gp}\langle A\rangle, \qquad \mathrm{gp}\langle BUB^{-1}, BSB^{-1}\rangle.$$

We obtain:

$$e_0 = Ue_0 = -Se_0, \qquad e_1 = Ae_1, \qquad e_2 = BUB^{-1}e_2 = -B^2Se_2.$$

Of course, these (and all subsequent) relations are really "relation schemes"; we need to use all their translates under the elements $(c : d)$.

3.8.3 "Face relations"

Recall that 1-homology is given by 1-cycles modulo 1-boundaries (see §4.1.2). Thus, we need to factor out by relations coming from the edges around each face of our tessellation. From Figures 3.8 and 3.9 we read off one "face relation" for each orbit of faces. Over Δ we obtain two orbits of quadrilaterals, from P_q, and one orbit of triangles, from P_r, giving

$$(I) + (TS) + \big((TS)^2\big) = 0,$$
$$[I] + [B] + [B^2] + [B^3] = 0,$$
$$(I) - [I] + (BS) - [BS] = 0.$$

Over Γ these become

$$e_0 + TSe_0 + (TS)^2e_0 = 0, \tag{3.17}$$
$$e_2 + TSe_2 + (TS)^2e_2 = 0, \tag{3.18}$$
$$e_1 - T^{-1}e_1 + B^2e_1 - B^2T^{-1}e_1 = 0, \tag{3.19}$$
$$e_0 - e_1 - e_2 + (TS)^2e_1 = 0. \tag{3.20}$$

Of these, (3.18) is redundant: for if P is a polyhedron with F faces, say, then the relations from any $F - 1$ of its faces imply the relation from the last face.

3.8.4 Homology

Let $G = \Gamma$ or Δ, and let $G' = \Gamma_0(\mathfrak{n})$ or $\Delta_0(\mathfrak{n})$ accordingly. The boundary homomorphism for G' is the map $\{\alpha, \beta\} \mapsto [\beta] - [\alpha]$, where $[\alpha]$ denotes the G'-orbit of the cusp α. We summarise the results of this section in the following theorem; compare [Cre81].

Theorem 56. *Form the $\mathbb{Q}$-vector space with basis the symbols (γ) and $[\gamma]$, for γ in a complete set of right coset representatives of $\mathrm{P}\Delta_0(\mathfrak{n})$ in $\mathrm{P}\Delta$, modulo all relations of the form*

$$(\gamma) = (\gamma U) = -(\gamma S),$$
$$[\gamma] = [\gamma A] = -[\gamma R],$$
$$(\gamma) + (\gamma TS) + \big(\gamma (TS)^2\big) = 0,$$
$$[\gamma] + [\gamma B] + [\gamma B^2] + [\gamma B^3] = 0,$$
$$(\gamma) - [\gamma] + (\gamma BS) - [\gamma BS] = 0,$$

and let H_Δ be its kernel under the boundary homomorphism. Then there is an isomorphism $H_\Delta \to H_1(\mathrm{P}\Delta_0(\mathfrak{n})\backslash\mathfrak{H}_3^*, \mathbb{Q})$ given by

$$(\gamma) \mapsto \gamma e_0, \qquad [\gamma] \mapsto \gamma e_1.$$

Similarly, form the $\mathbb{Q}$-vector space with basis the symbols $(\gamma)_i$, for $i \in \{0,1,2\}$ and γ in a complete set of right coset representatives of $\mathrm{P}\Gamma_0(\mathfrak{n})$ in $\mathrm{P}\Gamma$, modulo all relations of the form

$$(\gamma)_0 = (\gamma U)_0 = -(\gamma S)_0, \qquad (\gamma)_1 = (\gamma A)_1, \qquad (\gamma)_2 = (\gamma BUB^{-1})_2 = -(\gamma B^2 S)_2,$$
$$(\gamma)_0 + (\gamma TS)_0 + (\gamma (TS)^2)_0 = 0,$$
$$(\gamma)_1 - (\gamma T^{-1})_1 + (\gamma B^2)_1 - (\gamma B^2 T^{-1})_1 = 0,$$
$$(\gamma)_0 - (\gamma)_1 - (\gamma)_2 + (\gamma (TS)^2)_1 = 0.$$

and let H_Γ be its kernel under the boundary homomorphism. Then there is an isomorphism $H_\Gamma \to H_1(\mathrm{P}\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3^*, \mathbb{Q})$ given by

$$(\gamma)_i \mapsto \gamma e_i.$$

Chapter 4

Harmonic differential forms

The purpose of this chapter is threefold. In §4.1, we describe the background from differential geometry that is necessary for an understanding of the definition of harmonic differential forms and an appreciation of their significance. Roughly speaking, harmonic forms are important firstly because they are closed, so that they may be integrated in a path-independent manner, and secondly because each de Rham cohomology class is represented by a unique harmonic form.

In §4.2, we describe the harmonic forms that arise in this thesis. The results presented are not new,[1] and may all be found, at least implicitly, in [Wei71]. However, Weil's treatment is rather concise, and subsequent writers (such as [Cre81, Fig95]) have introduced some slight inaccuracies. We hope that a more leisurely account will be useful.

Let k be either $\mathbb{R}$ or $\mathbb{C}$, and let $G = \mathrm{GL}(2, k)$; much of the theory can be developed in parallel for the two cases. The real case is relevant for the real embeddings of a number field; in particular, it is the only case which arises in the study of classical modular forms over $\mathbb{Q}$. The complex case is relevant for the complex embeddings; it is thus the only case which is needed for the study of modular forms over an imaginary quadratic field. Ultimately, then, the latter case is the important one for this thesis.

The group G has centre Z and a maximal compact subgroup K, either $\mathrm{O}(2)$ or $\mathrm{U}(2)$. We are interested in differential forms on the coset space G/ZK and their inverse images on G. We choose suitable bases for the spaces of differential forms, so that forms on G

[1] except equation (4.30), perhaps

and G/ZK now correspond to functions on those spaces; these functions are related by means of a representation of ZK, which we compute explicitly. Harmonicity now imposes some partial differential equations, which reduce to the Cauchy-Riemann equations in the real case; thus harmonicity generalises holomorphy. By separation of variables, we find certain solutions of these partial differential equations which will be important later.

Finally, in §4.3, we develop detailed formulae for the complex case, going further than [Cre81]. The formalism is independent of the interpretation of the functions as differential forms and the action of G as defining the pullback of those differentials.

4.1 Background from differential geometry

We assume that the reader has some familiarity with the notions of differentiable manifold and differential form. An elementary introduction to differential forms is given in [Woo86], and a fuller treatment in [Car71]. For full definitions and proofs, see [Spi79, vols. I and IV], which was our principal source, or the standard reference [dR55]. Section §4.1.2 is based on the discussion in [Sha90, §21].

4.1.1 Basic concepts

Let V be a differentiable manifold of dimension m. To each point $p \in V$ one associates the tangent space at p, denoted V_p; it is an m-dimensional real vector space. Let TV be the tangent bundle of the manifold V; it is a vector bundle over the base space V, the fibre over p being V_p, and it inherits a natural structure as a manifold of dimension $2m$. A vector field is a (smooth) section of the tangent bundle, that is, a (smoothly varying) choice of vectors $v_p \in V_p$.

Differential forms are defined in a manner dual to vector fields. Thus, let $\Omega^r(V_p)$ be the space of alternating r-linear forms on V_p; by convention, $\Omega^0(V_p) = \mathbb{R}$. Let $\Omega^r(TV)$ be the vector bundle over V with fibres $\Omega^r(V_p)$, equipped with its natural manifold structure; in the case $r = 1$, it is called the cotangent bundle of V. A differential r-form is then a (smooth) section of the bundle $\Omega^r(TV)$, that is, a compatible choice of elements $\omega(p) \in \Omega^r(V_p)$. A 0-form is just a (smooth) real-valued function on V.

We denote the space of differential r-forms on V by $\Omega^r(V)$. Observe that it is not just a real vector space: it carries the structure of a module over the ring of 0-forms.

4.1.2 Duality

As above, let V be an m-manifold. Then on the one hand, if V is compact, it admits a triangulation, giving rise to a chain complex $\{C_n, \partial_n\}_{n\geq 0}$. Here C_n, the group of n-chains, is the free abelian group generated by the n-simplices in the triangulation, and $\partial_n \colon C_n \to C_{n-1}$ is the boundary map, satisfying $\partial^2 = 0$. Elements $x_n \in \ker \partial_n$ are called n-cycles, and $y_n \in \operatorname{im} \partial_{n+1}$ n-boundaries. The quotient group $H_n(V)$ of n-cycles modulo n-boundaries is called the n-th homology group of V. Although it is not at all obvious from this definition, the $H_n(V)$ are independent of the choice of triangulation and have nice functorial properties.

On the other hand, V is a differentiable manifold. For brevity, write Ω^r for $\Omega^r(V)$. The usual differentiation operators $d_r \colon \Omega^r \to \Omega^{r+1}$ satisfy $d^2 = 0$. Therefore, $\{\Omega^r, d_r\}_{r\geq 0}$ is a cochain complex. Its cohomology is called the *de Rham cohomology* of V and denoted $H^r_{DR}(V)$.

The connection between these two constructions is given by the operation of integrating a differential form along a chain, and one has the following far-reaching generalisation of the fundamental theorem of calculus.

Generalised Stokes' Theorem. *For a form $\phi \in \Omega^{r-1}$ and a chain $c \in C_r$,*

$$\int_{\partial c} \phi = \int_c d\phi.$$

Introducing the notation $(c, \phi) = \int_c \phi$ for $c \in C_r$ and $\phi \in \Omega^r$, and extending the pairing (c, ϕ) to $c \in C_r \otimes \mathbb{R}$ turns Stokes' theorem into the assertion that the two operators ∂ on $\oplus(C_r \otimes \mathbb{R})$ and d on $\oplus\Omega^r$ are dual maps. Suppose now that $\partial c = 0$, so that c represents a homology class in $H_r(V, \mathbb{R})$, and that $d\phi = 0$, so that ϕ represents a cohomology class in $H^r_{DR}(V)$. Then for arbitrary $c' \in C_{r+1}$ and $\phi' \in \Omega^{r-1}$,

$$\begin{aligned}(c + \partial c', \phi + d\phi') &= (c, \phi) + (c, d\phi') + (\partial c', \phi + d\phi')\\ &= (c, \phi) + (\partial c, \phi') + (c', d\phi + d^2\phi')\\ &= (c, \phi)\end{aligned}$$

by Stokes' theorem, showing that (c, ϕ) induces a pairing between $H_r(V, \mathbb{R})$ and $H^r_{DR}(V)$.

de Rham's Theorem. *The pairing thus constructed is a duality between* $H_r(V, \mathbb{R})$ *and* $H^r_{DR}(V)$.

Sometimes this theorem is used to provide an analytic method of computing the homology of a manifold. From our point of view, it will provide a combinatorial way of computing differential forms.

4.1.3 The Hodge star operator

A basic theme of differential geometry is that any construction on vector spaces can be extended to a construction on vector bundles, in particular, on the tangent bundle. For example, an orientation on a finite-dimensional real vector space is an equivalence class of ordered bases of the space, two bases being related if and only if the change of basis matrix has positive determinant. An orientation on V is then a compatible choice of orientations on the V_p, and V is orientable if it has an orientation.

Similarly, a Riemannian metric on V is a (smoothly varying) choice of inner products on the spaces V_p. It is a theorem that every m-manifold V can be equipped with a Riemannian metric; when this is done, we speak of a Riemannian manifold.

Now let V be an orientable Riemannian m-manifold. Then one can define an operator $*\colon \Omega^r(V) \to \Omega^{m-r}(V)$, called the (Hodge) star operator. We first recall the coordinate-free definition [Spi79, addendum IV.7.2]; as usual, the construction is given on each fibre. Recall that an r-form $\omega \in \Omega^r(V)$ is really a collection of elements $\omega(p) \in \Omega^r(V_p)$. We always have the "wedge" map of alternating multilinear forms:

$$\Omega^r(V_p) \times \Omega^{m-r}(V_p) \xrightarrow{\wedge} \Omega^m(V_p).$$

The orientation and inner product on V give us an orientation and inner product on each V_p, hence give isomorphisms $\Omega^m(V_p) \cong \mathbb{R}$. So we have bilinear maps

$$A'_p\colon \Omega^r(V_p) \times \Omega^{m-r}(V_p) \to \mathbb{R}$$

which induce maps $A_p\colon \Omega^r(V_p) \to \big(\Omega^{m-r}(V_p)\big)^*$ in the usual way:

$$A_p(\omega)(\eta) = A'_p(\omega, \eta) \qquad \big(\omega \in \Omega^r(V_p),\ \eta \in \Omega^{m-r}(V_p)\big).$$

On the other hand, the inner product on each V_p induces an isomorphism $\iota_p\colon V_p \to (V_p)^*$,

$$v \mapsto (w \mapsto \langle w, v \rangle), \tag{4.1}$$

which in turn induces an isomorphism $B_p\colon \big(\Omega^{m-r}(V_p)\big)^* \to \Omega^{m-r}(V_p)$ via

$$(B_p f)(v_1, \ldots, v_{m-r}) = f(\iota_p v_1 \wedge \cdots \wedge \iota_p v_{m-r}).$$

The Hodge $*$ operator is now defined on each fibre as the composition

$$\Omega^r(V_p) \xrightarrow{A_p} \big(\Omega^{m-r}(V_p)\big)^* \xrightarrow{B_p} \Omega^{m-r}(V_p),$$

i.e. we define $*\omega \in \Omega^{m-r}(V)$, for each $\omega \in \Omega^r(V)$, by

$$(*\omega)(p) = B_p A_p\big(\omega(p)\big).$$

It is clear from the fibre-wise definition that

$$*(\alpha + \beta) = *\alpha + *\beta, \qquad *(f\alpha) = f(*\alpha),$$

for all r-forms α, β and all 0-forms f. In other words, the star operator is not merely $\mathbb{R}$-linear; it is a morphism of modules over the ring of (smooth) real-valued functions.

In coordinates, the operator is easiest to express with respect to an orthonormal basis; if $ds^2 = \sum \eta_i^2$, and $\eta_1, \ldots, \eta_m$ is positively oriented, then

$$*(\eta_{i_1} \wedge \cdots \wedge \eta_{i_r}) = \epsilon \eta_{j_1} \wedge \cdots \wedge \eta_{j_{m-r}}, \tag{4.2}$$

where $(i_1, \ldots, i_r, j_1, \ldots, j_{m-r}) = (\sigma(1), \ldots, \sigma(m))$ for some permutation σ of $\{1, \ldots, m\}$, and $\epsilon = \operatorname{sign} \sigma$.

If α and β are r-forms, then

(i) $**\alpha = (-1)^{r(m-r)}\alpha$;

(ii) $\alpha \wedge *\beta = \beta \wedge *\alpha$;

(iii) $\alpha \wedge *\alpha = f(*1) = f\eta_1 \wedge \cdots \wedge \eta_m$, where $f \geq 0$ and f is zero at exactly the points of V where α is zero (i.e. f has the same support as α).

Therefore, if V is compact, there is an inner product on $\Omega^r(V)$ given by

$$(\alpha, \beta) = \int_V \alpha \wedge *\beta. \tag{4.3}$$

(Actually, compactness is a stronger condition than we really need; we could equally consider forms with compact support or subject to a suitable growth condition. We shall not keep pointing this out in the sequel.)

4.1.4 The star operator for complex differentials

For our application, we need to extend the definition of $*$ to the complexifications $\Omega^r(V)\otimes_{\mathbb{R}} \mathbb{C}$. Recall that $*$ is linear over real-valued functions. The extension of $*$ turns out to be $\mathbb{C}$-antilinear:

$$*(\alpha + \beta) = *\alpha + *\beta, \qquad *(f\alpha) = \bar{f}(*\alpha), \tag{4.4}$$

for all complex-valued r-forms α, β and all complex-valued 0-forms f. To see why, we go back to the coordinate-free definition. We use the same sequence of maps as in the real case. The Riemannian inner product extends to an Hermitian inner product. The wedge product of forms is $\mathbb{C}$-linear, hence so are the maps A_p, but the map (4.1) is $\mathbb{C}$-antilinear; consequently, so are the maps B_p and $*$, proving (4.4). We now have, for $\alpha, \beta \in \Omega^r(V) \otimes_{\mathbb{R}} \mathbb{C}$,

(i) $**\alpha = (-1)^{r(m-r)}\alpha$;

(ii) $\alpha \wedge *\beta = \overline{\beta \wedge *\alpha}$.

(iii) $\alpha \wedge *\alpha = f(*1)$, where f is real-valued, non-negative, and has the same support as α.

The first two follow easily from the corresponding facts for real differentials. To prove (iii) in both cases, we simply write $\alpha = \sum f_i\omega_i$, where i ranges over r-tuples with $i_1 \leq \cdots \leq i_r$

and $\omega_i = \eta_{i_1} \wedge \cdots \wedge \eta_{i_r}$, and compute

$$\begin{aligned}\alpha \wedge *\alpha &= \left(\sum f_i\omega_i\right) \wedge \left(\sum \bar{f}_j *\omega_j\right)\\ &= \sum_{i,j} f_i\bar{f}_j(\omega_i \wedge *\omega_j)\\ &= \sum_i |f_i|^2(\omega_i \wedge *\omega_i)\\ &= \sum_i |f_i|^2\eta_1 \wedge \cdots \wedge \eta_m.\end{aligned}$$

Hence, if V is compact, there is an Hermitian inner product on $\Omega^r(V) \otimes_{\mathbb{R}} \mathbb{C}$ given by

$$(\alpha, \beta) = \int_V \alpha \wedge *\beta. \tag{4.5}$$

4.1.5 Harmonicity

Since we have the map d, which raises the degree of a form, we can define a map $\delta\colon \Omega^r(V) \to \Omega^{r-1}(V)$, which lowers the degree of a form, by

$$\delta = (-1)^{m(r+1)+1} * d * .$$

We clearly have $\delta^2 = 0$, and $\delta = 0$ on functions (0-forms). On r-forms,

$$*\delta = (-1)^r d*,$$

so that for $\omega \in \Omega^{r-1}(V)$ and $\eta \in \Omega^r(V)$,

$$\begin{aligned}d(\omega \wedge *\eta) &= d\omega \wedge *\eta + (-1)^{r-1}\omega \wedge d*\eta\\ &= d\omega \wedge *\eta - \omega \wedge *\delta\eta.\end{aligned}$$

Since V has no boundary, Stokes' theorem now gives

$$(d\omega, \eta) = (\omega, \delta\eta). \tag{4.6}$$

Thus, δ is the (Hermitian) adjoint of d for the inner products (4.3), (4.5). Now define the "Laplacian", an operator preserving the degree of a form, by

$$\Delta = \delta d + d\delta.$$

Using (4.6) we see that Δ is self-adjoint:

$$(\Delta\omega, \eta) = (\omega, \Delta\eta). \tag{4.7}$$

An r-form ω is called *closed* if $d\omega = 0$, *co-closed* if $\delta\omega = 0$ (or equivalently, if $*\omega$ is closed), and *harmonic* if $\Delta\omega = 0$. Using (4.6) we have

$$(\Delta\omega, \omega) = (\delta\omega, \delta\omega) + (d\omega, d\omega),$$

showing that ω is harmonic if and only if it is both closed and co-closed:

$$\Delta\omega = 0 \iff (d\omega = 0 \text{ and } \delta\omega = 0). \tag{4.8}$$

If ω and η are r-forms, and $\Delta\omega = 0$, then (4.7) gives

$$(\Delta\eta, \omega) = (\eta, \Delta\omega) = 0,$$

so the vector space of all harmonic forms (the kernel of Δ) is orthogonal to the image of Δ. The fundamental result on harmonic forms is as follows.

Hodge Decomposition Theorem. *If V is a compact oriented Riemannian m-manifold, then for each r with $0 \le r \le m$, the vector space $H^r(V)$ of harmonic r-forms is finite-dimensional, and there is an orthogonal direct sum decomposition*

$$\Omega^r(V) = \Delta\big(\Omega^r(V)\big) \oplus H^r(V).$$

Write $H^r\colon \Omega^r(V) \to H^r(V)$ for the projection map onto the subspace of harmonic r-forms. For any $\alpha \in \Omega^r(V)$, the form $\alpha - H^r(\alpha)$ is equal to $\Delta\omega$ for a unique $\omega \in \Delta\big(\Omega^r(V)\big)$. Denote this ω by $G(\alpha)$. Thus

$$G = \big(\Delta|_{\Delta(\Omega^r(V))}\big)^{-1} \circ (\mathrm{id} - H^r).$$

It is now straightforward to check that if $T\colon \Omega^r(V) \to \Omega^s(V)$ is any linear map with $\Delta T = T\Delta$, then $GT = TG$. In particular, $Gd = dG$. Let α be any r-form. Then

$$\begin{aligned} \alpha &= \Delta G\alpha + H^r(\alpha) \\ &= d\delta G\alpha + \delta dG\alpha + H^r(\alpha) \\ &= d\delta G\alpha + \delta Gd\alpha + H^r(\alpha), \end{aligned}$$

so if $d\alpha = 0$, then

$$\alpha = d\delta G\alpha + H^r(\alpha).$$

Thus $H^r(\alpha)$ is a harmonic r-form in the same de Rham cohomology class as α. On the other hand, suppose α_1 and α_2 are two harmonic r-forms in the same de Rham cohomology class, so that $\alpha_1 - \alpha_2 = d\beta$ for some β. Then

$$\begin{aligned} (d\beta, d\beta) = (d\beta, \alpha_1 - \alpha_2) &= (\beta, \delta\alpha_1 - \delta\alpha_2) && \text{by (4.6)} \\ &= 0 && \text{by (4.8)}. \end{aligned}$$

So $d\beta = 0$, that is, $\alpha_1 = \alpha_2$. Thus there is indeed a *unique* harmonic form in each de Rham cohomology class, as asserted in the introduction to this chapter.

4.1.6 Pullbacks and left-invariance of differential forms

The construction of the tangent bundle TV of the manifold V is functorial; if $f\colon V \to W$ is a (smooth) map of manifolds, then there is an induced bundle map $f_*\colon TV \to TW$, consisting of linear maps $(f_*)_p\colon V_p \to W_{f(p)}$ for each $p \in V$. Essentially, $(f_*)_p$ is the derivative of f at the point p.

Our only use for the map f_* is in the definition of another induced map $f^*\colon \Omega^r(W) \to \Omega^r(V)$, which associates to a differential r-form ω on W an r-form $f^*\omega$ on V, called its *inverse image on V* or its *pullback along f to V*. It is defined for each $p \in V$ by

$$(f^*\omega)(p)\big((X_1)_p, \ldots, (X_r)_p\big) = \omega\big(f(p)\big)\big((f_*)_p(X_1)_p, \ldots, (f_*)_p(X_r)_p\big),$$

for all vector fields $X_1, \ldots, X_r$ on V.

Now let G be a Lie group, that is, a group with a compatible structure as a differentiable manifold. For fixed $a \in G$, we have two diffeomorphisms $G \to G$:

$$\begin{aligned} &L_a\colon g \mapsto ag && \text{left translation,} \\ &R_a\colon g \mapsto ga && \text{right translation.} \end{aligned}$$

A differential r-form ω on G is called *left-invariant under a* if it is invariant under pullback along L_a, that is, if $L_a^*\omega = \omega$. What this really means is

$$\omega(ag)\big(((L_a)_*)((X_1)_g), \ldots, ((L_a)_*)((X_r)_g)\big) = \omega(g)\big((X_1)_g, \ldots, (X_r)_g\big)$$

for all vector fields $X_1, \ldots, X_r$ on G and for all $g \in G$, but we shall abuse notation and write simply $\omega(ag) = \omega(g)$. If ω is left invariant under all $a \in G$, it is called *left-invariant under* G, or simply *left-invariant*. Right-invariance is defined similarly.

Let $\beta_1, \ldots, \beta_m$ be left-invariant real-valued differential 1-forms on G whose values $\beta_i(e)$ at the identity $e \in G$ span the fibre $(G_e)^*$ of the cotangent bundle of G at the identity. Let ω be any left-invariant 1-form. Then $\omega(e) = \sum a_i\beta_i(e)$ for some $a_i \in \mathbb{R}$. By left-invariance, it follows that $\omega = \sum a_i\beta_i$, and the essential point here is that the a_i are *constants*. We call the β_i a *basis* (over $\mathbb{R}$) for the left-invariant 1-forms on G. For details, see [Spi79, I.10]. Similarly, we have the notion of a basis (over $\mathbb{C}$) of the left-invariant complex-valued differentials.

4.2 Harmonic differential forms

4.2.1 Notation

Let k be $\mathbb{R}$ or $\mathbb{C}$, and let $G = \mathrm{GL}(2, k)$. Then G is a Lie group, and the notation of §4.1.6 applies to G and its Lie subgroups. Recall that there is a decomposition

$$G = BZK$$

in which K is a compact subgroup of G, usually[2] given by

$$K = \begin{cases} \mathrm{O}(2) & \text{when } k = \mathbb{R}, \\ \mathrm{U}(2) & \text{when } k = \mathbb{C}, \end{cases}$$

Z is the centre of G, and B is the subgroup of G given by

$$B = \left\{ \begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix} \;\middle|\; t > 0,\ u \in k \right\}.$$

Since $B \cap ZK = \{1_2\}$, B provides a complete set of right coset representatives for ZK in G. So B may be identified with the coset space G/ZK. It may also be identified in the

[2] With this, the usual choice, K is a maximal compact subgroup of G, but maximality is not essential in the sequel and one can replace $\mathrm{U}(2)$ by $\mathrm{SU}(2)$; see §4.2.4.

obvious manner with the space

$$\mathfrak{H} = \{(u,t)\} = k \times \mathbb{R}_{>0};$$

this is the complex upper half plane if $k = \mathbb{R}$ and "upper half space" if $k = \mathbb{C}$. Write $\pi\colon G \to \mathfrak{H}$ for the canonical mapping (the "projection") of G onto $\mathfrak{H}$; the restriction of π to B is the bijection identifying B with $\mathfrak{H}$.

The group G acts on $\mathfrak{H}$ on the left; this is just the coset action. Write $L_g\colon \mathfrak{H} \to \mathfrak{H}$ for the map $(u,t) \mapsto g \cdot (u,t)$. Thus, $L_g \circ \pi = \pi \circ L_g$. Explicitly,

$$g \cdot (u,t) = \pi\left(g\begin{pmatrix} t & u \\ 0 & 1\end{pmatrix}\right). \tag{4.9}$$

The space $\mathfrak{H}$ is a differentiable manifold of dimension m, where $m = 2$ if $k = \mathbb{R}$ and $m = 3$ if $k = \mathbb{C}$. It has a Riemannian metric, invariant under the action of G, given by

$$ds^2 = \frac{dt^2 + du\,d\bar{u}}{t^2}.$$

Remark. We should point out that [Wei71] actually works with the group

$$B_1 = \left\{ t^{-1/2}\begin{pmatrix} t & u \\ 0 & 1\end{pmatrix} \,\middle|\, t > 0,\ u \in k \right\},$$

in place of B. There is a bijection $B \to B_1$ given by $g \mapsto (\det g)^{-1/2} g$. Both subgroups appear to serve equally well; from our point of view, there does not appear to be a preferred choice.

4.2.2 Forms on $\mathfrak{H}$ and their pullbacks to G

We are interested in differential 1-forms on $\mathfrak{H}$ and their pullbacks to G. In this section, we describe the theory common to the cases $k = \mathbb{R}$ and $k = \mathbb{C}$; explicit formulae will be given in §4.2.3 and §4.2.4 respectively.

We start by choosing a basis $\beta_1, \ldots, \beta_m$ (over $\mathbb{C}$) for the left-invariant differential 1-forms on B; as we remarked in §4.1.6, it suffices to choose left-invariant 1-forms whose values $\beta_i(e)$ at the identity span the fibre $(B_e)^*$ of the cotangent bundle of B at the identity.

We observe that the pullbacks $\pi^*\beta_i$ are right-invariant under all $g \in ZK$. For, obviously, $\pi = \pi \circ R_g$ as maps $G \to \mathfrak{H}$, and applying what Cartan [Car71] calls the *transitivity of the change of variable* gives

$$\pi^* = (\pi \circ R_g)^* = R_g^* \circ \pi^*.$$

So the $\pi^*\beta_i$ really are right-invariant under ZK. But they need not be left-invariant under G. For each i, let ω_i be the left-invariant differential 1-form on G which agrees with $\pi^*\beta_i$ at the identity. This defines ω_i uniquely, of course; the values at the non-identity fibres are determined by left-translation. We shall determine the ω_i in terms of the β_i. Write ω (respectively β, $\pi^*\beta$) for the column vector of the ω_i (resp. β_i, $\pi^*\beta_i$.) We claim that

$$\omega(g) = \rho\big(\pi(g)^{-1}g\big)^{-1}(\pi^*\beta)(g) \tag{4.10}$$

for a certain m-dimensional representation ρ of ZK. To derive (4.10), and show how ρ should be defined, we proceed as follows.

First, as in [Cre81], we let $J(g;z)$ be the Jacobian matrix, with respect to the basis β, of the transformation $L_g\colon \mathfrak{H} \to \mathfrak{H}$ given by $z \mapsto g \cdot z$; thus

$$\beta(g \cdot z) = J(g;z)\beta(z) \qquad (g \in G,\ z \in \mathfrak{H}). \tag{4.11}$$

Note that the matrix $J(g;z)$ is invertible, because L_g is a diffeomorphism. The chain rule (really, transitivity again) implies the *cocycle identity*

$$J(g_1g_2;z) = J(g_1;g_2 \cdot z)J(g_2;z) \qquad (g_1, g_2 \in G,\ z \in \mathfrak{H}). \tag{4.12}$$

By assumption, the β_i are left-invariant under B. This just means

$$J(b;z) = 1 \qquad (b \in B,\ z \in \mathfrak{H}).$$

Together with (4.12), this implies, more generally,

$$J(bg;z) = J(g;z) \qquad (b \in B,\ g \in G,\ z \in \mathfrak{H}).$$

In particular, since we are identifying $\pi(g) \in \mathfrak{H}$ with the corresponding element of the group B, so that $\pi(g)^{-1}g \in ZK$ for all $g \in G$, we have

$$J(g;z) = J\big(\pi(g)^{-1}g;z\big) \qquad (g \in G,\ z \in \mathfrak{H}). \tag{4.13}$$

We also have the equation

$$(\pi^*\beta)(ag) = J\big(a;\pi(g)\big)(\pi^*\beta)(g) \qquad (a, g \in G), \tag{4.14}$$

which we obtain by pulling back β in two directions around the commutative square

$$\begin{array}{ccc} G & \xrightarrow{L_a} & G \\ {\scriptstyle\pi}\big\downarrow & & \big\downarrow{\scriptstyle\pi} \\ \mathfrak{H} & \xrightarrow[L_a]{} & \mathfrak{H} \end{array}$$

and using transitivity again to give

$$L_a^* \circ \pi^* = (\pi \circ L_a)^* = (L_a \circ \pi)^* = \pi^* \circ L_a^*.$$

The factor $J\big(a;\pi(g)\big)$ in (4.14) measures the extent to which the pullbacks $\pi^*\beta_i$ fail to be left-invariant. Since $\pi(g) = g \cdot \pi(1)$, we have, by (4.12),

$$J\big(a;\pi(g)\big) = J\big(ag;\pi(1)\big) \cdot J\big(g;\pi(1)\big)^{-1}.$$

Substituting from (4.13) gives

$$J\big(a;\pi(g)\big) = J\big(\pi(ag)^{-1}ag;\pi(1)\big) \cdot J\big(\pi(g)^{-1}g;\pi(1)\big)^{-1}, \tag{4.15}$$

where the right hand side depends only on the values of $J\big(-;\pi(1)\big)$ on ZK. Of course, by definition of $\mathfrak{H}$, every $z \in \mathfrak{H}$ has the form $z = \pi(g)$ for some $g \in G$. So J is determined by the values of $J\big(-;\pi(1)\big)$ on ZK. This motivates us to define a function $\rho\colon ZK \to \mathrm{GL}(m, \mathbb{C})$ by

$$\rho(g) = J\big(g;\pi(1)\big) \qquad (g \in ZK). \tag{4.16}$$

Using (4.12) and the fact that ZK stablilises $\pi(1)$, we see at once that

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2) \qquad (g_i \in ZK),$$

showing that ρ is an m-dimensional representation of ZK. In fact, ρ is trivial on Z, because the $\pi^*\beta_i$ are right-invariant under ZK and hence also left-invariant under the centre Z.

In this notation, (4.15) becomes

$$J\big(a;\pi(g)\big) = \rho\big(\pi(ag)^{-1}ag\big)\cdot\rho\big(\pi(g)^{-1}g\big)^{-1},$$

so that (4.14) may be written

$$\rho\big(\pi(ag)^{-1}ag\big)^{-1}(\pi^*\beta)(ag) = \rho\big(\pi(g)^{-1}g\big)^{-1}(\pi^*\beta)(g).$$

Observe that the left hand side of this equation is the result of applying L_a^* to the right hand side. So the right hand side is left-invariant and agrees with $\pi^*\beta$ at the identity $1 \in G$. This proves (4.10). Consequently,

$$\begin{aligned}\omega(g\kappa\zeta) &= \rho\big(\pi(g\kappa\zeta)^{-1}g\kappa\zeta\big)^{-1}(\pi^*\beta)(g\kappa\zeta)\\ &= \rho(\kappa\zeta)^{-1}\rho\big(\pi(g)^{-1}g\big)^{-1}(\pi^*\beta)(g)\\ &= \rho(\kappa\zeta)^{-1}\omega(g),\end{aligned}$$

as claimed by Weil [Wei71, p.106].

The following lemma summarises the relationship between differential 1-forms on $\mathfrak{H}$ and G. Of course, $\mathbb{C}^m$ is to be regarded as a space of row vectors.

Lemma 57. (i) *For each i, the differential ω_i on G induces β_i on $\mathfrak{H}$, by restriction to the subgroup B (identified with $\mathfrak{H}$). More generally, for $\phi\colon G \to \mathbb{C}^m$, the form $\phi\cdot\omega$ induces $f\cdot\beta$, where $f\colon \mathfrak{H} \to \mathbb{C}^m$ is given by*

$$f(u,t) = \phi\left(\begin{pmatrix} t & u \\ 0 & 1\end{pmatrix}\right). \tag{4.17}$$

(ii) *The pullback to G of a differential form $f\cdot\beta$ on $\mathfrak{H}$ is $\phi\cdot\omega$, where*

$$\phi(g) = f\big(\pi(g)\big)\rho\big(\pi(g)^{-1}g\big) \qquad (g \in G). \tag{4.18}$$

(iii) *A differential form on G is the pullback of one on $\mathfrak{H}$ if and only if it can be written as $\phi\cdot\omega$, where $\phi\colon G \to \mathbb{C}^m$ satisfies*

$$\phi(g\kappa\zeta) = \phi(g)\rho(\kappa\zeta) \qquad (g \in G,\ \kappa\zeta \in ZK). \tag{4.19}$$

(iv) *The constructions of* (i) *and* (ii) *define mutually inverse bijections between differential forms on* G *and* $\mathfrak{H}$.

(v) *Correspondingly,* (4.17) *and* (4.18) *define mutually inverse bijections between the set of functions* $\phi\colon G \to \mathbb{C}^m$ *that satisfy* (4.19)*, and the set of functions* $f\colon \mathfrak{H} \to \mathbb{C}^m$.

Proof. Part (i) is clear. For (ii), we pull back $f \cdot \beta$ and use (4.10) to give

$$\pi^*(f \cdot \beta)(g) = f\big(\pi(g)\big) \cdot (\pi^*\beta)(g) = f\big(\pi(g)\big)\rho\big(\pi(g)^{-1}g\big) \cdot \omega(g).$$

We now prove (iii). By (ii), the pullback of a form on $\mathfrak{H}$ may be written $\phi \cdot \omega$, where ϕ is given by (4.18); using $\pi(g\kappa\zeta) = \pi(g)$, it is easy to see that ϕ satisfies (4.19). Conversely, suppose that ϕ satisfies (4.19). Pulling back the differential form $\phi|_B \cdot \beta$ on B gives

$$\begin{aligned} \pi^*\big(\phi|_B \cdot \beta\big)(g) &= \phi\big(\pi(g)\big)\rho\big(\pi(g)^{-1}g\big) \cdot \omega(g) && \text{by (ii)} \\ &= \phi(g) \cdot \omega(g) && \text{by (4.19).} \end{aligned}$$

So $\phi \cdot \omega$ is the pullback of a differential form on B (namely, of $\phi|_B \cdot \beta$), as required for (iii).

Part (iv) follows at once, and (v) is a purely formal consequence. *Aliter*, part (v) can be proved by direct calculation, as in Lemma 64 below. □

Remark. This lemma, although straightforward, is actually quite important. In relating differential forms on $\mathfrak{H}$ to functions on G that transform in a certain way, it prepares the way for the general definition of modular forms in Chapter 6 as functions on GL(2) with certain transformation properties.

So far, we have not really used the fact that the ω_i are left-invariant; indeed, Lemma 57 holds *mutatis mutandis* if ω is replaced by $\pi^*\beta$. Weil [Wei71] provides little motivation for working with ω, and the distinction between $\pi^*\beta$ and ω has been partly or wholly overlooked in [Cre81, Fig95]. The advantage of working with ω and not merely $\pi^*\beta$ becomes apparent when we consider the action of G on differentials and on the corresponding functions.

The mapping $a \mapsto L_a^*$ defines an action of the group G on the set of differentials on G; explicitly, the action of $a \in G$ is $\eta \mapsto L_a^*(\eta)$. This is a right-action, for $L_a^* \circ L_b^* = (L_b \circ$

$L_a)^* = (L_{ba})^*$. Correspondingly, there is an induced right-action on functions $\phi\colon G \to \mathbb{C}^m$, written $\phi \mapsto \phi\big|a$ and defined by

$$(\phi\big|a) \cdot \omega = L_a^*(\phi \cdot \omega);$$

since ω is left-invariant, this action takes the especially simple form $\phi\big|a = \phi \circ L_a$. Clearly, this action preserves the set of those ϕ satisfying (4.19).

Similarly, G acts on the set of differentials on $\mathfrak{H}$ and correspondingly on the set of functions f on $\mathfrak{H}$. Explicitly, $(f\big|a) \cdot \beta = L_a^*(f \cdot \beta)$, so that $f\big|a = (f \circ L_a)J(a; -)$.

4.2.3 The real case

Consider the case $k = \mathbb{R}$. Out of tradition, we write (x, y) for (u, t). We have $G = ZBK$, where

$$\begin{aligned}
G &= \mathrm{GL}(2, \mathbb{R}), \\
Z &= \left\{ \zeta\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \;\middle|\; \zeta \in \mathbb{R}^\times \right\}, \\
B &= \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R},\ y \in \mathbb{R}_{>0} \right\}, \\
K &= \mathrm{O}(2) = \left\{ g \in G \mid g^t = g^{-1} \right\}.
\end{aligned}$$

Thus K is the orthogonal group $\mathrm{O}(2)$; it is generated by the matrices $r(\theta)$ and s, defined by

$$r(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \qquad s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

With $z = x + iy$, we choose the basis β as follows:

$$\beta_1 = \frac{dz}{y}, \qquad \beta_2 = -\frac{d\bar{z}}{y}. \tag{4.20}$$

Lemma 58. *With this choice of β, the representation ρ is given by*

$$\rho\big(r(\theta)\big) = \begin{pmatrix} e^{2i\theta} & 0 \\ 0 & e^{-2i\theta} \end{pmatrix}, \qquad \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.21}$$

Proof. Write $P = \operatorname{diag}(1, -1)$, so that

$$\beta(z) = \frac{1}{y} P \begin{pmatrix} dz \\ d\bar{z} \end{pmatrix}.$$

Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. By (4.16), we must calculate $\rho(g) = J\big(g; \pi(1)\big) = J(g; i)$, where $J(g; z)$ is defined by (4.11). First suppose that $\Delta > 0$, where $\Delta = \det g$. Then (4.9) becomes

$$z \longmapsto z' = x' + iy' = \frac{az + b}{cz + d}. \tag{4.22}$$

In particular,

$$\frac{y}{y'} = \frac{|cz + d|^2}{\Delta}. \tag{4.23}$$

Computing the Jacobian of (4.22) with respect to the variables $(z, \bar{z})$ gives

$$J = \frac{\partial(z', \bar{z'})}{\partial(z, \bar{z})} = \Delta \cdot \begin{pmatrix} (cz + d)^{-2} & 0 \\ 0 & (c\bar{z} + d)^{-2} \end{pmatrix}.$$

Using $PJP^{-1} = J$, we deduce

$$\beta(g \cdot z) = \frac{1}{y'} P \begin{pmatrix} dz' \\ d\bar{z'} \end{pmatrix} = \frac{1}{y'} PJ \begin{pmatrix} dz \\ d\bar{z} \end{pmatrix} = \frac{y}{y'} PJP^{-1} \beta(z) = \frac{y}{y'} J\beta(z).$$

From (4.23) we obtain

$$J(g; z) = \begin{pmatrix} \epsilon^{-2} & 0 \\ 0 & \epsilon^2 \end{pmatrix},$$

where $\epsilon = (cz + d)/|cz + d|$. Putting $g = r(\theta)$ and $z = i$ gives the first half of (4.21).

For $\Delta < 0$, equation (4.22) would have to be modified; indeed, it is clear from (4.23) that (4.22) no longer defines an action on the upper half plane. To determine ρ it suffices, of course, to take $g = s$. Since

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

we see that s acts via $z \mapsto -\bar{z}$. Consequently,

$$\frac{\partial(z', \bar{z'})}{\partial(z, \bar{z})} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \qquad J(s; z) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Evaluating at $z = i$ gives the second half of (4.21); in fact, $J(s; z)$ is actually independent of z. ◻

4.2.4 The complex case

Now consider the case $k = \mathbb{C}$. Out of tradition, we write (z,t) for (u,t). We have $G = ZBK$, where

$$\begin{aligned} G &= \mathrm{GL}(2,\mathbb{C}), \\ Z &= \left\{ \zeta\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \mid \zeta \in \mathbb{C}^\times \right\}, \\ B &= \left\{ \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \,\middle|\, z \in \mathbb{C},\ t \in \mathbb{R}_{>0} \right\}, \\ K = \mathrm{SU}(2) &= \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \,\middle|\, u, v \in \mathbb{C},\ u\bar{u} + v\bar{v} = 1 \right\}. \end{aligned}$$

Remark. The analogy with the real case would suggest taking for K the full unitary group $\mathrm{U}(2) = \{ g \in G \mid \bar{g}^t = g^{-1} \}$. However, $Z\cdot\mathrm{SU}(2) = Z\cdot\mathrm{U}(2)$, since $Z \cong \mathbb{C}^\times = \mathbb{R}^\times \cdot S^1$, where $S^1 = \{ e^{i\theta} \mid \theta \in \mathbb{R}\}$, and $\mathrm{U}(2) = S^1 \cdot \mathrm{SU}(2)$. Thus the choice of K makes no difference here; in §4.3, however, $K = \mathrm{SU}(2)$ is a convenient choice.

The coset action (4.9) of G on $\mathfrak{H}_3 = B = G/ZK$ is given explicitly by (3.11) and (3.12); as before, we write $L_g \colon \mathfrak{H}_3 \to \mathfrak{H}_3$ for the map $(z,t) \mapsto g\cdot(z,t)$. We choose the basis β of left-invariant differentials on $\mathfrak{H}_3$ as follows:

$$\beta_0 = -\frac{dz}{t}, \qquad \beta_1 = \frac{dt}{t}, \qquad \beta_2 = \frac{d\bar{z}}{t}. \tag{4.24}$$

Let $J\big(g;(z,t)\big)$ be the Jacobian matrix of $L_g \colon \mathfrak{H}_3 \to \mathfrak{H}_3$ in terms of our chosen basis β; thus

$$\beta\big(g\cdot(z,t)\big) = J\big(g;(z,t)\big)\beta\big((z,t)\big).$$

Lemma 59. *Let $g = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in G$. Write $\Delta = ad - bc$, $r = \overline{cz+d}$, and $s = \bar{c}t$. Then*

$$J\big(g;(z,t)\big) = \frac{1}{|\Delta|(r\bar{r}+s\bar{s})} \begin{pmatrix} \Delta & 0 & 0 \\ 0 & |\Delta| & 0 \\ 0 & 0 & \bar{\Delta} \end{pmatrix} \begin{pmatrix} r^2 & -2rs & s^2 \\ r\bar{s} & r\bar{r} - s\bar{s} & -\bar{r}s \\ \bar{s}^2 & 2\bar{r}\bar{s} & \bar{r}^2 \end{pmatrix}. \tag{4.25}$$

Proof. Calculating the Jacobian J of L_g in terms of the variables $(z, t, \bar{z})$, using (3.11) and (3.12), gives

$$J = \frac{\partial(z', t', \bar{z'})}{\partial(z, t, \bar{z})} = \frac{1}{(|r|^2 + |s|^2)^2} \begin{pmatrix} \Delta & 0 & 0 \\ 0 & |\Delta| & 0 \\ 0 & 0 & \bar{\Delta} \end{pmatrix} \begin{pmatrix} r^2 & 2rs & -s^2 \\ -r\bar{s} & r\bar{r} - s\bar{s} & -\bar{r}s \\ -\bar{s}^2 & 2\bar{r}\bar{s} & \bar{r}^2 \end{pmatrix}.$$

Since

$$\beta\big((z,t)\big) = \frac{1}{t} P \begin{pmatrix} dz \\ dt \\ d\bar{z} \end{pmatrix}$$

where $P = \operatorname{diag}(-1, 1, 1)$, we have

$$\beta\big(g \cdot (z,t)\big) = \frac{t}{t'} PJP^{-1} \beta\big((z,t)\big).$$

Substituting for t/t' from (3.12), we obtain (4.25). Note that conjugation with P changes some of the signs in the matrix. ☐

We know that $J\big(g; (0,1)\big)$ restricted to $g \in ZK$ affords a representation $\rho\colon ZK \to \mathrm{GL}(3, \mathbb{C})$; in fact

$$\rho\colon ZK \to \mathrm{SL}(3, \mathbb{C}). \tag{4.26}$$

Explicitly, we know that ρ is trivial on Z (of course, one can verify this directly from (4.25)); for $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \in K$ we find

$$\rho\left(\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}\right) = \begin{pmatrix} u^2 & 2uv & v^2 \\ -u\bar{v} & u\bar{u} - v\bar{v} & \bar{u}v \\ \bar{v}^2 & -2\bar{u}\bar{v} & \bar{u}^2 \end{pmatrix}. \tag{4.27}$$

Note that the restriction of ρ to $\mathrm{SU}(2)$ is precisely the well-known three-dimensional polynomial representation of $\mathrm{SU}(2)$; this would not have been so if the basis β had not been chosen suitably. Another choice would, however, yield an equivalent representation, since ρ is the unique irreducible representation of degree 3 up to equivalence, as is well known.

There is a more elegant way of writing (4.25). It is convenient to define a function $\rho\colon \mathbb{C}^2 \setminus \{(0,0)\} \to \mathrm{SL}(3,\mathbb{C})$ by

$$\rho(u,v) = \frac{1}{u\bar{u}+v\bar{v}} \begin{pmatrix} u^2 & 2uv & v^2 \\ -u\bar{v} & u\bar{u}-v\bar{v} & \bar{u}v \\ \bar{v}^2 & -2\bar{u}\bar{v} & \bar{u}^2 \end{pmatrix}.$$

Thus the restriction of (4.26) to $\mathbb{R}^\times K$ is given by

$$\rho\left(\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}\right) = \rho(u,v).$$

As usual, let $\mathbb{H}^\times$ denote the multiplicative group of non-zero quaternions. There is an isomorphism $\sigma\colon \mathbb{H}^\times \to \mathbb{R}^\times K$ given by

$$\sigma(u+vj) = \begin{pmatrix} \bar{u} & -\bar{v} \\ v & u \end{pmatrix} \qquad \big(u,v\in\mathbb{C},\ (u,v)\neq(0,0)\big); \tag{4.28}$$

this choice of σ, not quite the traditional one, is made to ensure that

$$\begin{pmatrix} j \\ 1 \end{pmatrix}(u+vj) = \begin{pmatrix} \bar{u}j-\bar{v} \\ u+vj \end{pmatrix} = \sigma(u+vj)\begin{pmatrix} j \\ 1 \end{pmatrix}.$$

With this notation, (4.25) becomes

$$J\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right);(z,t)\right) = \frac{1}{|\Delta|}\operatorname{diag}(\Delta,|\Delta|,\bar{\Delta})\cdot\rho(r,-s) \tag{4.29}$$

$$= \frac{1}{|\Delta|}\operatorname{diag}(\Delta,|\Delta|,\bar{\Delta})\cdot\rho\sigma(cq+d), \tag{4.30}$$

where $q = z+tj$.

4.2.5 Harmonicity

We now express harmonicity in terms of partial differential equations. Recall that if $z = x+iy$, then $\partial/\partial z$ and $\partial/\partial\bar{z}$ are defined by

$$\frac{\partial}{\partial z} = \frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right), \qquad \frac{\partial}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right);$$

one sees immediately that if $h = u+iv$ for real-valued functions u and v, then $\partial h/\partial\bar{z} = 0$ if and only if u and v satisfy the Cauchy-Riemann equations.

Lemma 60. *Let $k = \mathbb{R}$. In terms of the basis* (4.20) *chosen above, the Hodge star operator is given by*

$$*(f_1\beta_1 + f_2\beta_2) = -i(\bar{f}_1\beta_2 - \bar{f}_2\beta_1). \tag{4.31}$$

Consequently, the form $f_1\beta_1 + f_2\beta_2$ is harmonic if and only if f_1/y and $\bar{f}_2/y$ are holomorphic functions of z.

Proof. We have $ds^2 = \eta_1^2 + \eta_2^2$, where $\eta_1 = dx/y$ and $\eta_2 = dy/y$. By (4.2), $*\eta_1 = \eta_2$ and $*\eta_2 = -\eta_1$. Using (4.4), we obtain $*\beta_1 = -i\beta_2$ and $*\beta_2 = i\beta_1$. By (4.4) again, (4.31) follows. Taking the complex conjugate, we see that $*(f_1\beta_1 + f_2\beta_2)$ is closed if and only if $f_1\beta_1 - f_2\beta_2$ is closed. So $f_1\beta_1 + f_2\beta_2$ is harmonic if and only if $f_1\beta_1$ and $f_2\beta_2$ are closed, which is if and only if $f_1 y^{-1}\,dz$ and $\bar{f}_2 y^{-1}\,dz$ are closed. But $h(z)\,dz$ is closed if and only if $\partial h/\partial \bar{z} = 0$, which is if and only if $h(z)$ is holomorphic, by the Cauchy-Riemann equations. ☐

Lemma 61. *Let $k = \mathbb{C}$. In terms of the basis* (4.24) *chosen above, the Hodge star operator is given by*

$$*(f_0\beta_0 + f_1\beta_1 + f_2\beta_2) = i\bar{f}_0\beta_1 \wedge \beta_2 + \frac{i}{2}\bar{f}_1\beta_2 \wedge \beta_0 + i\bar{f}_2\beta_0 \wedge \beta_1. \tag{4.32}$$

Consequently, the form $f_0\beta_0 + f_1\beta_1 + f_2\beta_2$ is harmonic if and only if

$$\frac{\partial f_0}{\partial \bar{z}} + \frac{\partial f_2}{\partial z} = 0, \tag{4.33a}$$

$$\frac{\partial f_1}{\partial z} + \frac{\partial f_0}{\partial t} - t^{-1} f_0 = 0, \tag{4.33b}$$

$$\frac{\partial f_1}{\partial \bar{z}} - \frac{\partial f_2}{\partial t} + t^{-1} f_2 = 0, \tag{4.33c}$$

$$\frac{t}{2}\frac{\partial f_1}{\partial t} - f_1 - 2t\frac{\partial f_0}{\partial \bar{z}} = 0. \tag{4.33d}$$

Proof. We have $ds^2 = \eta_1^2 + \eta_2^2 + \eta_3^2$, where

$$\eta_1 = \frac{dx}{t} = \frac{1}{2}(\beta_2 - \beta_0), \qquad \eta_2 = \frac{dy}{t} = \frac{i}{2}(\beta_2 + \beta_0), \qquad \eta_3 = \frac{dt}{t} = \beta_1.$$

Hence

$$*\eta_1 = \eta_2 \wedge \eta_3 = \frac{i}{2}(\beta_2 \wedge \beta_1 + \beta_0 \wedge \beta_1),$$

$$*\eta_2 = \eta_3 \wedge \eta_1 = \frac{1}{2}(\beta_1 \wedge \beta_2 - \beta_1 \wedge \beta_0),$$

$$*\eta_3 = \eta_1 \wedge \eta_2 = \frac{i}{2}\beta_2 \wedge \beta_0.$$

Using (4.4), we obtain

$$\begin{aligned}
*\beta_0 &= *(-\eta_1 - i\eta_2) = -*\eta_1 + i*\eta_2 = i\beta_1 \wedge \beta_2,\\
*\beta_1 &= \frac{i}{2}\beta_2 \wedge \beta_0,\\
*\beta_2 &= *(\eta_1 - i\eta_2) = *\eta_1 + i*\eta_2 = i\beta_0 \wedge \beta_1.
\end{aligned}$$

By (4.4) again, (4.32) follows. Since $d\beta_0 = \beta_0 \wedge \beta_1$, $d\beta_1 = 0$, and $d\beta_2 = \beta_2 \wedge \beta_1$, we find that $\sum f_j\beta_j$ is closed if and only if (4.33a)–(4.33c) hold, the three equations coming from the coefficients of $\beta_2 \wedge \beta_0$, $\beta_0 \wedge \beta_1$ and $\beta_1 \wedge \beta_2$ respectively. From (4.32), we find that $*(\sum f_j\beta_j)$ is closed if and only if one further equation holds, coming from the coefficient of $\beta_0 \wedge \beta_1 \wedge \beta_2$; this equation is

$$\frac{t}{2}\frac{\partial \bar{f}_1}{\partial t} - \bar{f}_1 - t\frac{\partial \bar{f}_0}{\partial z} + t\frac{\partial \bar{f}_2}{\partial \bar{z}} = 0.$$

Taking the complex conjugate and using (4.33a), we obtain (4.33d). □

4.2.6 Standard functions

Let ϕ and f be related as in Lemma 57. Write $f = (f_1, f_2)$ when $k = \mathbb{R}$ and $f = (f_0, f_1, f_2)$ when $k = \mathbb{C}$.

Definition. We say that f is *B-moderate* if (and only if) there is $N \geq 0$ such that, for every compact subset S of k,

$$\|f(u,t)\| = O(t^N + t^{-N}),$$

uniformly over $u \in S$, where $\| \ \|$ is any norm on $\mathbb{C}^m$; in other words such that, for every such S, there exists $C > 0$, depending on S, such that for each i,

$$|f_i(u,t)| \leq C \sup(t^N, t^{-N}). \tag{4.34}$$

Remark. Roughly speaking, the presence of the term t^N on the right hand side ensures that f is of moderate growth as its argument approaches the "cusp at infinity". Similarly, the term t^{-N} ensures that f is of moderate growth as its argument approaches the "floor" $t = 0$ of $\mathfrak{H}$, where there can also be cusps, even in level 1 when the class number is greater than 1.

Definition. We say that ϕ is *B-moderate* if (and only if) f is B-moderate.

Definition. The function ϕ is *admissible of type $\mathcal{H}_k$* if it is B-moderate and $f \cdot \beta$ is harmonic.

Now choose a "standard" character of the additive group k^+ as follows:

$$\psi(u) = \begin{cases} e^{-2\pi i u} & \text{if } k = \mathbb{R}, \\ e^{-2\pi i(u+\bar{u})} & \text{if } k = \mathbb{C}. \end{cases} \tag{4.35}$$

Definition. The function ϕ is *standard of type $\mathcal{H}_k$* if it is admissible of that type and satisfies

$$\phi\left(\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} g\right) = \psi(u)\phi(g) \qquad (u \in k,\ g \in G). \tag{4.36}$$

An easy calculation shows that for ϕ satisfying (4.19), condition (4.36) is equivalent to

$$f_i(u,t) = \psi(u) f_i(0,t) \qquad (u \in k,\ t \in \mathbb{R}_{>0}). \tag{4.37}$$

Standard functions will play a special rôle in the Fourier analysis of Chapter 6. In this section, we find a standard function for each k and prove its uniqueness up to scalar multiples.

Lemma 62. *Let $k = \mathbb{R}$ and let ϕ and f be related as in Lemma 57. Then ϕ is standard of type $\mathcal{H}_\mathbb{R}$ if and only if there exists $C \in \mathbb{C}$ such that*

$$f(x,y) = Ce^{-2\pi i\bar{z}}(0,y).$$

Proof. Assume that ϕ is standard. This means that f_1 and f_2 satisfy (4.37) and (4.34), and by Lemma 60, that f_1/y and $\bar{f}_2/y$ are holomorphic functions of z. Put $g(y) = y^{-1} f_1(0,y)$ and $h(y) = y^{-1}\bar{f}_2(0,y)$. Then f_1/y and $\bar{f}_2/y$ are holomorphic if and only if

$$\frac{\partial}{\partial \bar{z}}\left(e^{-2\pi i x} g(y)\right) = 0, \qquad \frac{\partial}{\partial \bar{z}}\left(e^{2\pi i x} h(y)\right) = 0,$$

which is if and only if $dg/dy = 2\pi g$ and $dh/dy = -2\pi h$, which is if and only if $f_1(x,y) = C_1 y e^{-2\pi i z}$ and $f_2(x,y) = C_2 y e^{-2\pi i \bar{z}}$ for some $C_1, C_2 \in \mathbb{C}$. The growth condition (4.34) forces $C_1 = 0$. So f is as stated. Conversely, the stated f certainly corresponds to a standard ϕ. □

Thus our standard differential form is $f \cdot \beta = e^{-2\pi i\bar{z}}\,d\bar{z}$. This is not quite what the classical theory of modular forms leads us to expect. The discrepancy is due to Weil's choice of standard character (4.35). Suppose we make a different choice:

$$\psi(x) = e^{2\pi i x}.$$

The same calculation as above now gives $f_1 = C_1 y e^{2\pi i z}$ and $f_2 = C_2 y e^{2\pi i \bar{z}}$. Now $C_2 = 0$ and we obtain $f \cdot \beta = e^{2\pi i z}\,dz$. In this way, then, we could recover classical q-series expansions in terms of $q = e^{2\pi i z}$.

We now turn to the complex case. In the course of the proof, we encounter the "modified Bessel equation of order 0":

$$sK''(s) + K'(s) - sK(s) = 0; \tag{4.38}$$

it is known [Wat52] that the only solution which does not increase exponentially as $s \to +\infty$ is Basset's function K_0. Another of Basset's functions is $K_1(s) = -K_0'(s)$. Bessel's equation has been extensively studied, and the solutions K_n carry many different names in the literature, such as Macdonald functions, Hankel functions, modified Bessel functions of the third kind, and so on; according to Watson [Wat52], however, they appear to have been introduced by Basset.

Lemma 63. *Let $k = \mathbb{C}$ and let ϕ and f be related as in Lemma 57. Then ϕ is standard of type $\mathcal{H}_\mathbb{C}$ if and only if*

$$f(z,t) = Ce^{-2\pi i(z+\bar{z})}H(t),$$

where $C \in \mathbb{C}$,

$$H(t) = \left(-\frac{i}{2}t^2K_1(4\pi t), t^2K_0(4\pi t), \frac{i}{2}t^2K_1(4\pi t)\right), \tag{4.39}$$

and K_0, K_1 are Basset's functions.

Proof. Assume that ϕ is standard. This means that f_0, f_1 and f_2 satisfy (4.37), (4.34), and (4.33). Put $g_j(t) = f_j(0,t)$. Now (4.33a) is equivalent to

$$g_2 = -g_0. \tag{4.40}$$

Given (4.40), each of (4.33b) and (4.33c) is equivalent to

$$\frac{d}{dt}\left(t^{-1}g_0\right) = 2\pi i t^{-1} g_1. \tag{4.41}$$

Finally, equation (4.33d) is equivalent to

$$\frac{d}{dt}\left(t^{-2}g_1\right) = -8\pi i t^{-2} g_0. \tag{4.42}$$

It just remains to solve (4.40), (4.41) and (4.42), as in [Wei71]. Let $s = 4\pi t$ and $K(s) = t^{-2}g_1(t)$. One obtains precisely equation (4.38). Since $f_1(z,t) = e^{-2\pi i(z+\bar{z})}g_1(t)$ is to satisfy (4.34), we must have $g_1(t) = t^2 K_0(4\pi t)$ up to some constant factor. By (4.40) and (4.42) we now have, up to the same constant factor,

$$g_0(t) = -g_2(t) = \frac{i}{2}t^2\frac{d}{ds}K_0(s) = -\frac{i}{2}t^2 K_1(4\pi t).$$

So f is as stated. Conversely, our calculations show that f as stated certainly corresponds to a standard ϕ. This completes the proof. □

4.3 The complex case (revisited)

Let $G = \mathrm{GL}(2,\mathbb{C})$, and let Z, B, K, S^1 and $\mathfrak{H}_3$ be as in §4.2.4. So far, we have followed Weil [Wei71], and expressed the theory in terms of differential forms on G and $\mathfrak{H}_3$ and the corresponding functions on those spaces. This is sufficient for many purposes, but sometimes another formulation is more convenient. For example, Cremona [Cre81] noticed, when working with functions f on $\mathfrak{H}_3 = \mathbb{C} \times \mathbb{R}_{>0}$, that "it is often convenient to allow arbitrary complex numbers as the second argument of functions." Thus, one can define

$$f(z, e^{i\theta}t) = f(z,t)\,\mathrm{diag}\left(e^{i\theta}, 1, e^{-i\theta}\right). \tag{4.43}$$

This idea arises almost by abuse of notation in [Cre81], but it actually rests on a perfectly sound foundation: as we explain below, it amounts to pulling our differentials on $\mathfrak{H}_3$ back, not all the way to G, but to the intermediate space $G/(\mathbb{R}^\times K)$.

There is a related formulation involving quaternions, based on the isomorphism between $\mathbb{R}^\times K$ and $\mathbb{H}^\times$. The parallel with the real case is often most striking in this setting, and the formulae most elegant: two such formulae are (4.30) above and (4.55) below.

The aim of this section is to clarify the relationship between the different points of view. We attempt to place (4.43) in its natural setting. We describe the quaternionic formulation, for its elegance if not for its utility. We also describe a related formulation, analogous to that given in §2.1.2 for the real case; it will form the basis for the theory of "modular points" in Chapter 7.

We begin by describing various spaces related to G and $\mathfrak{H}_3$. Then we consider the functions on those spaces corresponding to the functions ϕ on G and f on $\mathfrak{H}_3$. Finally, we consider the action of G on those functions that is induced by pullback of the corresponding differential forms.

4.3.1 Spaces related to G and $\mathfrak{H}_3$

The ring $\mathbb{H}$ of quaternions may be regarded as a left-vector space over $\mathbb{C}$, with basis $1, j$. There is an obvious bijection $\mathrm{M}_2(\mathbb{C}) \setminus \{0\} \longrightarrow \mathbb{H}^2 \setminus \{0\}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} j \\ 1 \end{pmatrix} = \begin{pmatrix} aj + b \\ cj + d \end{pmatrix}; \tag{4.44}$$

composing with the natural quotient map onto the projective line (obtained by factoring out on the right, as in §3.1) we obtain a map $\pi_1\colon \mathrm{M}_2(\mathbb{C}) \setminus \{0\} \to \mathbb{P}^1(\mathbb{H})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto [aj + b : cj + d].$$

Let $\sigma\colon \mathbb{H}^\times \to \mathbb{R}^\times K$ be the isomorphism (4.28); it satisfies

$$\begin{pmatrix} j \\ 1 \end{pmatrix} \lambda = \sigma(\lambda) \begin{pmatrix} j \\ 1 \end{pmatrix} \qquad (\lambda \in \mathbb{H}^\times).$$

For $M, M' \in \mathrm{M}_2(\mathbb{C}) \setminus \{0\}$, we readily deduce that $\pi_1(M) = \pi_1(M')$ if and only if $M = M'P$ for some $P \in \mathbb{R}^\times K$. We thus obtain an induced bijection

$$\big(\mathrm{M}_2(\mathbb{C}) \setminus \{0\}\big) \,/\, \big(\mathbb{R}^\times K\big) \longrightarrow \mathbb{P}^1(\mathbb{H}). \tag{4.45}$$

Using (3.1), we obtain the following commutative diagram, in which horizontal arrows are bijections and vertical arrows are quotient maps:

$$\begin{array}{ccccccc}
\mathrm{M}_2(\mathbb{C}) \setminus \{0\} & \xrightarrow{(4.44)} & \mathbb{H}^2 \setminus \{0\} & & & & \\
\downarrow & & \downarrow & & & & \\
\big(\mathrm{M}_2(\mathbb{C}) \setminus \{0\}\big) \;/\; (\mathbb{R}^\times K) & \xrightarrow{(4.45)} & \mathbb{P}^1(\mathbb{H}) & \xrightarrow{(3.1)} & \mathbb{H} \cup \{\infty\} & \xrightarrow{(3.1)} & \mathbb{C}^2 \cup \{\infty\}\,.
\end{array}$$

Recall that G acts on the left on each of our spaces; explicit formulae are given in §3.1. In particular, real scalars act trivially on the second row, and the action of S^1 on $\mathbb{P}^1(\mathbb{H})$ is given by (3.3), whence

$$e^{i\theta} \cdot (z + tj) = z + e^{2i\theta} tj, \qquad e^{i\theta} \cdot (z, t) = (z, e^{2i\theta} t).$$

We can now do two things. Firstly, we can add a third row to the diagram, by factoring out on the left under the action of Z. Secondly, we can replace the set $\mathrm{M}_2(\mathbb{C}) \setminus \{0\}$ of non-zero matrices by its subset G of invertible matrices. The bijection (4.44) restricts to $G \longrightarrow \mathbb{H}^2 \setminus \mathcal{C}$, where $\mathcal{C}$ is the set of $\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right)$ such that q_1, q_2 are linearly dependent (on the left) over $\mathbb{C}$, in other words,

$$\mathcal{C} = \left\{ \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \;\middle|\; q_2 = 0 \text{ or } q_1 q_2^{-1} \in \mathbb{C} \right\}.$$

Thus $\mathcal{C}$ consists of the zero vector and the pre-image under the quotient map $\mathbb{H}^2 \setminus \{0\} \to \mathbb{P}^1(\mathbb{H})$ of $\mathbb{P}^1(\mathbb{C})$ (regarded as a subset of $\mathbb{P}^1(\mathbb{H})$ in the obvious way). Combining these ideas, we arrive at the commutative diagram

$$\begin{array}{ccccccc}
G & \xrightarrow{(4.44)} & \mathbb{H}^2 \setminus \mathcal{C} & & & & \\
\downarrow & & \downarrow & & & & \\
G/(\mathbb{R}^\times K) & \xrightarrow{(4.45)} & \mathbb{P}^1(\mathbb{H}) \setminus \mathbb{P}^1(\mathbb{C}) & \xrightarrow{(3.1)} & \mathbb{H} \setminus \mathbb{C} & \xrightarrow{(3.1)} & \mathbb{C} \times \mathbb{C}^\times \\
\downarrow & & & & \downarrow & & \downarrow \\
G/ZK & \longrightarrow & \left\{ \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} \;\middle|\; t > 0 \right\} & \longrightarrow & \{z + tj \mid t > 0\} & \longrightarrow & \mathbb{C} \times \mathbb{R}_{>0};
\end{array}$$

as before, the horizontal arrows are bijections and the vertical arrows (where present) are quotient maps. Hitherto, we have usually identified all the sets on the bottom row with $\mathfrak{H}_3$; strictly speaking, the second from the left is B, and the fourth $\mathfrak{H}_3$.

4.3.2 Functions on upper half space and related spaces

In Lemma 57, we considered functions ϕ on G and f on $\mathfrak{H}_3$ related by means of a certain representation ρ of ZK, trivial on Z; this ρ was chosen so that $\phi \cdot \omega$ was the pullback of the differential $f \cdot \beta$. We now generalise this set-up, taking an arbitrary ρ; there will no longer be an obvious interpretation in terms of differential forms. We also discuss the corresponding functions on $\mathbb{H}^2 \setminus \mathcal{C}$ and $\mathbb{H} \setminus \mathbb{C}$.

Let V be a finite-dimensional vector space over $\mathbb{C}$, and let $\rho\colon ZK \to \mathrm{GL}(V)$ be a representation, not necessarily trivial on Z. We refer to ρ as the *weight*, for reasons which will become apparent. Consider the following two sets of functions:

$$\mathcal{S}_1 = \{f : \mathfrak{H}_3 \to V\}$$
$$\mathcal{S}_2 = \{\, \phi\colon G \to V \mid \phi(\zeta g \kappa) = \phi(g)\rho(\zeta\kappa) \quad \forall \zeta \in Z,\ g \in G,\ \kappa \in K \,\}.$$

There is an obvious map $\dagger\colon \mathcal{S}_2 \to \mathcal{S}_1$, given essentially by restriction to B; explicitly,

$$\phi^\dagger\big(\pi(b)\big) = \phi(b) \qquad (b \in B). \tag{4.46}$$

In the other direction, given $f \in \mathcal{S}_1$, define $f^*\colon G \to V$ by

$$f^*(\zeta b \kappa) = f\big(\pi(b)\big)\rho(\zeta\kappa) \qquad (\zeta \in Z,\ b \in B,\ \kappa \in K). \tag{4.47}$$

Lemma 64. *The map $\dagger\colon \mathcal{S}_2 \to \mathcal{S}_1$ is a bijection, with inverse $*\colon \mathcal{S}_1 \to \mathcal{S}_2$.*

Proof. This is essentially part (v) of Lemma 57; (4.46), (4.47) and the condition for ϕ to lie in $\mathcal{S}_2$ generalise (4.17), (4.18) and (4.19) respectively. The function f^* is well-defined by (4.47), since $G = ZBK$ and $B \cap ZK = \{1\}$. It is easy to verify that $f^* \in \mathcal{S}_2$, that $f^{*\dagger} = f$, and that $\phi^{\dagger *} = \phi$. □

Next, we pass from functions on G to functions on pairs of quaternions. The bijection between G and $\mathbb{H}^2 \setminus \mathcal{C}$ given by (4.44) induces a bijection between V-valued functions on those two spaces in the obvious way, i.e. by means of the contravariant functor $\mathrm{Hom}(-, V)$ in the category of sets; explicitly, given $\phi\colon G \to V$, we define $\phi^*\colon \mathbb{H}^2 \setminus \mathcal{C} \to V$ by

$$\phi^*\left(g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\right) = \phi\,(g) \qquad (g \in G), \tag{4.48}$$

whilst given $\tilde{F}\colon \mathbb{H}^2 \setminus \mathcal{C} \to V$, we define $\tilde{F}^\dagger\colon G \to V$ by

$$\tilde{F}^\dagger(g) = \tilde{F}\left(g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\right) \qquad (g \in G). \tag{4.49}$$

Our next lemma states that, under these bijections, $\mathcal{S}_2$ corresponds to the set

$$\mathcal{S}_3 = \Big\{\tilde{F}\colon \mathbb{H}^2 \setminus \mathcal{C} \to V \mid \tilde{F}\big(\zeta\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right)\lambda\big) = \tilde{F}\big(\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right)\big)\rho(\zeta)\rho\sigma(\lambda) \\ \forall\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right) \in \mathbb{H}^2 \setminus \mathcal{C},\ \zeta \in \mathbb{C}^\times,\ \lambda \in \mathbb{H}^\times\Big\}.$$

Lemma 65. *The maps given by* (4.48) *and* (4.49) *restrict to mutually inverse bijections* $*\colon \mathcal{S}_2 \to \mathcal{S}_3$ *and* $\dagger\colon \mathcal{S}_3 \to \mathcal{S}_2$*.*

Proof. Let $\phi \in \mathcal{S}_2$. Then for all $\zeta \in Z$, $g \in G$ and $\lambda \in \mathbb{H}^\times$,

$$\phi^*\left(\zeta g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\lambda\right) = \phi\big(\zeta g\sigma(\lambda)\big) = \phi(g)\,\rho(\zeta)\rho\sigma(\lambda) = \phi^*\left(g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\right)\rho(\zeta)\rho\sigma(\lambda),$$

proving that $\phi^* \in \mathcal{S}_3$. Conversely, let $\tilde{F} \in \mathcal{S}_3$. Given $\kappa \in K$, write $\kappa = \sigma(\lambda)$ for some $\lambda \in \mathbb{H}^\times$. Then for all $\zeta \in Z$ and $g \in G$,

$$\tilde{F}^\dagger(\zeta g\kappa) = \tilde{F}\big(\zeta g\sigma(\lambda)\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\big) = \tilde{F}\big(\zeta g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\lambda\big) = \tilde{F}\big(g\left(\begin{smallmatrix} j \\ 1 \end{smallmatrix}\right)\big)\rho(\zeta)\rho\sigma(\lambda) = \tilde{F}^\dagger(g)\rho(\zeta\kappa),$$

proving that $\tilde{F}^\dagger \in \mathcal{S}_2$. The constructions (4.48) and (4.49) are obviously mutually inverse.

□

We now pass from functions on $\mathbb{H}^2 \setminus \mathcal{C}$ to functions on $\mathbb{H} \setminus \mathbb{C}$, and show that $\mathcal{S}_3$ corresponds to

$$\mathcal{S}_4 = \left\{f\colon \mathbb{H} \setminus \mathbb{C} \to V \;\middle|\; f(\zeta q\zeta^{-1}) = f(q)\rho(\zeta)\rho\sigma(\zeta^{-1}) \quad \forall q \in \mathbb{H} \setminus \mathbb{C},\ \zeta \in \mathbb{C}^\times\right\}.$$

Lemma 66. *Let* $\tau\colon \mathbb{H}^\times \to \mathrm{GL}(V)$ *be any representation. Consider the sets*

$$\mathcal{S}_3' = \Big\{\tilde{F}\colon \mathbb{H}^2 \setminus \mathcal{C} \to V \mid \tilde{F}\big(\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right)\lambda\big) = \tilde{F}\big(\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right)\big)\tau(\lambda) \quad \forall\left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right) \in \mathbb{H}^2 \setminus \mathcal{C},\ \lambda \in \mathbb{H}^\times\Big\}$$
$$\mathcal{S}_4' = \{f\colon \mathbb{H} \setminus \mathbb{C} \to V\}.$$

Given $\tilde{F} \in \mathcal{S}_3'$*, define* $\tilde{F}^* \in \mathcal{S}_4'$ *by*

$$\tilde{F}^*(q) = \tilde{F}\big(\left(\begin{smallmatrix} q \\ 1 \end{smallmatrix}\right)\big). \tag{4.50}$$

Conversely, given $f \in \mathcal{S}_4'$*, define* $f^\dagger \colon \mathbb{H}^2 \setminus \mathcal{C} \to V$ *by*

$$f^\dagger\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big) = f(q_1 q_2^{-1})\tau(q_2). \tag{4.51}$$

Then the maps $* \colon \mathcal{S}_3' \to \mathcal{S}_4'$ *and* $\dagger \colon \mathcal{S}_4' \to \mathcal{S}_3'$ *given by* (4.50) *and* (4.51) *are mutually inverse bijections.*

Proof. Given $f \in \mathcal{S}_4'$, we have

$$f^\dagger\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\lambda\big) = f\big((q_1\lambda)(q_2\lambda)^{-1}\big)\tau(q_2\lambda) = f(q_1 q_2^{-1})\tau(q_2)\tau(\lambda) = f^\dagger\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big)\tau(\lambda),$$

proving $f^\dagger \in \mathcal{S}_3'$. Moreover,

$$f^{\dagger *}(q) = f^\dagger\big(\big(\begin{smallmatrix} q \\ 1 \end{smallmatrix}\big)\big) = f(q)\tau(1) = f(q),$$

i.e. $f^{\dagger *} = f$, and

$$\tilde{F}^{*\dagger}\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big) = \tilde{F}^*(q_1 q_2^{-1})\tau(q_2) = \tilde{F}\big(\big(\begin{smallmatrix} q_1 q_2^{-1} \\ 1 \end{smallmatrix}\big)\big)\tau(q_2) = \tilde{F}\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big),$$

showing $\tilde{F}^{*\dagger} = \tilde{F}$. □

Corollary 67. *The maps given by* (4.50) *and* (4.51) *restrict to mutually inverse bijections* $* \colon \mathcal{S}_3 \to \mathcal{S}_4$ *and* $\dagger \colon \mathcal{S}_4 \to \mathcal{S}_3$.

Proof. Let $\tau = \rho\sigma$ in Lemma 66 and note that $\mathcal{S}_3 \subseteq \mathcal{S}_3'$ and $\mathcal{S}_4 \subseteq \mathcal{S}_4'$. Given $\tilde{F} \in \mathcal{S}_3$, we certainly have $\tilde{F}^* \in \mathcal{S}_4'$; moreover,

$$\tilde{F}^*(\zeta q \zeta^{-1}) = \tilde{F}\big(\zeta\big(\begin{smallmatrix} q \\ 1 \end{smallmatrix}\big)\zeta^{-1}\big) = \tilde{F}\big(\big(\begin{smallmatrix} q \\ 1 \end{smallmatrix}\big)\big)\rho(\zeta)\rho\sigma(\zeta^{-1}) = \tilde{F}^*(q)\rho(\zeta)\rho\sigma(\zeta^{-1}),$$

so that (4.50) maps $\mathcal{S}_3$ into $\mathcal{S}_4$. Conversely, given $f \in \mathcal{S}_4$, we have $f^\dagger \in \mathcal{S}_3'$ by Lemma 66; moreover,

$$\begin{aligned} f^\dagger\big(\zeta\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big) &= f\big((\zeta q_1)(\zeta q_2)^{-1}\big)\rho\sigma(\zeta q_2) = f(\zeta q_1 q_2^{-1}\zeta^{-1})\rho\sigma(\zeta q_2) \\ &= f(q_1 q_2^{-1})\rho(\zeta)\rho\sigma(\zeta^{-1})\rho\sigma(\zeta q_2) = f(q_1 q_2^{-1})\rho\sigma(q_2)\rho(\zeta) = f^\dagger\big(\big(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\big)\big)\rho(\zeta), \end{aligned}$$

where we have used that $\rho(\zeta)$ lies in the centre of $\operatorname{im}\rho$. Thus $f^\dagger \in \mathcal{S}_3$, which completes the proof. □

Now let us return to the case of greatest interest, when $V = \mathbb{C}^3$ and ρ is trivial on Z and given by (4.27) on K, as in §4.2.4. In the definition of $\mathcal{S}_4$, we need only consider $\zeta \in S^1$. Let $\zeta = e^{i\theta/2}$ for some $\theta \in \mathbb{R}$. Then $\zeta(z+tj)\zeta^{-1} = z + e^{i\theta}tj$ and $\rho\sigma(\zeta^{-1}) = \operatorname{diag}\bigl(e^{i\theta}, 1, e^{-i\theta}\bigr)$. It follows that $\mathcal{S}_4$ is the set of functions $f\colon \mathbb{H}\setminus\mathbb{C} \to V$ satisfying

$$f(z + e^{i\theta}tj) = f(z+tj)\operatorname{diag}\bigl(e^{i\theta}, 1, e^{-i\theta}\bigr). \tag{4.52}$$

We see, therefore, that the justification for extending functions f on $\mathfrak{H}_3$ to functions on $\mathbb{C}\times\mathbb{C}^\times$ by means of (4.43), as in [Cre81], is that this corresponds to pulling back the differentials $f\cdot\beta$ to $G/(\mathbb{R}^\times K)$ rather than all the way to G.

Finally, it is instructive to compare (4.51) with the exactly analogous formula (2.5) in the classical case; the representation $\tau = \rho\sigma$ of $\mathbb{H}^\times$ replaces the representation $\omega_2 \mapsto \omega_2^{-t}$ of $\mathbb{C}^\times$. This justifies the terminology of "weight" for the representation ρ.

4.3.3 Action of G

We saw at the end of §4.2.2 that it is natural to consider the right-action of G on the set $\{\phi\colon G \to V\}$ given by $\phi \mapsto \phi\big|\gamma$, where

$$(\phi\big|\gamma)(\delta) = \phi(\gamma\delta) \qquad (\gamma, \delta \in G). \tag{4.53}$$

It is clear that this action preserves the set $\mathcal{S}_2$; thus (4.53) defines a right-action of G on $\mathcal{S}_2$. Using the bijections of Lemma 64, Lemma 65 and Corollary 67, we transfer this action to the sets $\mathcal{S}_1$, $\mathcal{S}_3$ and $\mathcal{S}_4$. Thus, for $f \in \mathcal{S}_1$ and $\gamma \in G$, we define $f\big|\gamma = \bigl((f^*)\big|\gamma\bigr)^\dagger$. Explicitly,

$$(f\big|\gamma)\bigl(\pi(b)\bigr) = f\bigl(\gamma\cdot\pi(b)\bigr)\rho\bigl(\pi(\gamma b)^{-1}\gamma b\bigr) \qquad (b \in B);$$

in the special case when ρ is given by (4.27), this simplifies to

$$(f\big|\gamma)(p) = f(\gamma\cdot p)J(\gamma; p) \qquad (p \in \mathfrak{H}_3), \tag{4.54}$$

which we already obtained at the end of §4.2.2 by pulling back differentials. Similarly, for $\tilde{F} \in \mathcal{S}_3$, we define $\tilde{F}\big|\gamma = \bigl((\tilde{F}^\dagger)\big|\gamma\bigr)^*$. Explicitly,

$$(\tilde{F}\big|\gamma)\bigl(\bigl(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\bigr)\bigr) = \tilde{F}\bigl(\gamma\bigl(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\bigr)\bigr).$$

Finally, for $f \in \mathcal{S}_4$, we define $f\big|\gamma = \big((f^\dagger)\big|\gamma\big)^*$. Explicitly,

$$\big(f\big|\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\big)(q) = f\big((aq+b)(cq+d)^{-1}\big)\rho\sigma(cq+d), \tag{4.55}$$

or more briefly, recalling (3.4),

$$(f\big|\gamma)(q) = f(\gamma \cdot q)\rho\sigma(cq+d). \tag{4.56}$$

Notice the similarity to (2.2), the corresponding formula in the theory of classical modular forms!

Remark. We can recover (4.30) from a comparison of (4.54) and (4.56), by applying (4.52) with $e^{i\theta}$ equal to $\Delta/|\Delta|$, the factor which expresses the difference between the actions (3.12) on $\mathfrak{H}_3$ and (3.6) on $\mathbb{H} \setminus \mathbb{C}$.

It will be useful later to have an explicit formula for the special case of (4.54) when $\gamma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. We find

$$\begin{aligned}
(f\big|\gamma)(z,t) &= f\big(\gamma \cdot (z,t)\big)J\big(\gamma;(z,t)\big) && \text{by (4.54)} \\
&= f\left(\frac{az+b}{d}, \frac{|a|t}{|d|}\right) \cdot \operatorname{diag}\left(\frac{a\bar{d}}{|ad|}, 1, \frac{\bar{a}d}{|ad|}\right) && \text{by (3.12) and (4.25).}
\end{aligned}$$

By (4.43), we may therefore write

$$\big(f\big|\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\big)(z,t) = f\left(\frac{az+b}{d}, \frac{at}{d}\right). \tag{4.57}$$

Chapter 5

Adeles and algebraic groups

The purpose of this chapter[1] is to develop the basic theory of adeles, in order to provide the necessary background for the definition of automorphic forms in Chapter 6.

We begin the chapter by recalling the definitions of the adele ring $k_{\mathbb{A}}$ and idele group $k_{\mathbb{A}}^{\times}$ of an algebraic number field k. Next we discuss quasicharacters of the idele class group, which occur again in Chapter 6. Their relation to Dirichlet characters is best understood using class field theory.

The passage from k to $k_{\mathbb{A}}$ and $k_{\mathbb{A}}^{\times}$ provides the two simplest examples of the process of adelisation of an algebraic group over k, in this case, of the "additive group" G_a and the "multiplicative group" G_m. In §5.2, we discuss the adelised group $G_{\mathbb{A}}$ of GL(2) in some detail. We use its action on lattices in k^2 to derive some results on the structure of $G_{\mathbb{A}}$. Our treatment is self-contained; in particular, we prove all the "strong approximation" results that we need. Finally, we use our results on the structure of $G_{\mathbb{A}}$ to discuss functions on $G_{\mathbb{A}}$ that have certain transformation properties. §5.2.7 will be needed in in Chapter 6, where automorphic forms will be introduced as functions on $G_{\mathbb{A}}$ with similar properties.

Notation. Throughout this chapter, we let k be an algebraic number field and $\mathfrak{O}$ its ring of integers; we write v for a place of k, that is, an equivalence class of non-trivial valuations, and k_v for the completion of k with respect to v. We say that v is *real* if $k_v \cong \mathbb{R}$, *complex* if $k_v \cong \mathbb{C}$, *infinite* if it is real or complex and *finite* if it is not infinite; we write $v \mid \infty$ or $v \nmid \infty$ accordingly. If v is finite, that is, non-Archimedean, we write $\mathfrak{O}_v$ for the ring of

[1] The title is a conscious echo of a book title of Weil.

valuation integers in k_v, P_v for the maximal ideal of $\mathfrak{O}_v$, π_v for a prime element, and $\mathfrak{p}_v$ for the prime ideal $P_v \cap \mathfrak{O}$ of $\mathfrak{O}$ corresponding to the place v. For each v, finite or infinite, we write $|\ |_v$ for the normalised valuation at v, so that $\prod_v |x|_v = 1$ for all $x \in k^\times$. Finally, we write h for the class number of k, that is, for the order of its ideal class group.

By a homomorphism of topological groups we mean a continuous map that is algebraically a homomorphism; following modern usage, we do not require the map to be open, so in particular, the first isomorphism theorem need not hold.

5.1 GL(1)

The main sources for this section were [Neu86, Chap.IV], [Wei67a], and the articles by Cassels, Tate and Heilbronn in [CF67].

5.1.1 The adele ring

An *adele* of k is a family $x = (x_v)$ of elements $x_v \in k_v$, where v runs over all the places of k, and for which x_v is integral in k_v for almost all[2] v. The adeles form a topological ring, denoted by $k_{\mathbb{A}}$; addition and multiplication are defined component-wise. Thus

$$k_{\mathbb{A}} = \{\, (x_v) \mid x_v \in k_v \text{ for all } v;\ x_v \in \mathfrak{O}_v \text{ for almost all } v \,\}.$$

The topology on $k_{\mathbb{A}}$ may be described as the coarsest one for which, whenever S is a finite set of places of k containing the infinite places, the ring

$$A_k^S = \prod_{v \in S} k_v \times \prod_{v \notin S} \mathfrak{O}_v$$

is an open subring of $k_{\mathbb{A}}$, where A_k^S carries the product topology. More precisely, $k_{\mathbb{A}}$ is the inductive limit of the rings A_k^S as S ranges over the direct system of finite sets of places of k containing the infinite places.

[2]The phrase "for almost all" means "for all but finitely many". In a context like this one, a purist might prefer to say "for almost all finite v", but there is never any ambiguity, since almost all places *are* finite.

5.1.2 The idele group

The idele group $k_{\mathbb{A}}^{\times}$ of k is the group of units of the adele ring $k_{\mathbb{A}}$; explicitly,

$$k_{\mathbb{A}}^{\times} = \left\{ (x_v) \in k_{\mathbb{A}} \mid x_v \in k_v^{\times} \text{ for all } v;\ x_v \in \mathfrak{O}_v^{\times} \text{ for almost all } v \right\}.$$

The idele group is a topological group in a natural way. The topology is *finer* than the subspace topology induced by the inclusion $k_{\mathbb{A}}^{\times} \to k_{\mathbb{A}}$, for which the inversion map $x \mapsto x^{-1}$ need not be continuous; rather, it is the subspace topology coming from the map $k_{\mathbb{A}}^{\times} \to k_{\mathbb{A}}^2$, $x \mapsto (x, x^{-1})$, where $k_{\mathbb{A}}^2$ carries the product topology.

Remark. This is the natural way to topologise $k_{\mathbb{A}}^{\times} = \mathrm{GL}(1, k_{\mathbb{A}})$; the construction generalises at once to the case of $\mathrm{GL}(n, k_{\mathbb{A}})$ regarded as the set of $(x_{ij}, y) \in k_{\mathbb{A}}^{n^2+1}$ defined by the equation $\det(x_{ij}) \cdot y = 1$.

A basis for the open neighbourhoods of $1 \in k_{\mathbb{A}}^{\times}$ is given by the subgroups

$$\prod_{v \in S} W_v \times \prod_{v \notin S} \mathfrak{O}_v^{\times},$$

where S runs over the finite sets of places of k containing the infinite places, and $W_v \subseteq k_v^{\times}$ runs over a basis of open neighbourhoods of $1 \in k_v^{\times}$. In other words, $k_{\mathbb{A}}^{\times}$ is the restricted topological product of the $k_v^{\times}$ with respect to the $\mathfrak{O}_v^{\times}$, that is, the inductive limit of the open subgroups

$$I_k^S = \prod_{v \in S} k_v^{\times} \times \prod_{v \notin S} \mathfrak{O}_v^{\times},$$

each carrying the product topology, as S ranges over the direct system of finite sets of places of k containing the infinite places. The group I_k^S is called the group of S-ideles of k. Let S_∞ be the set of infinite places and put $k_\infty^{\times} = \prod_{v \mid \infty} k_v^{\times}$, so that

$$I_k^{S_\infty} = k_\infty^{\times} \times \prod_{v \nmid \infty} \mathfrak{O}_v^{\times}.$$

Given $x = (x_v) \in k_{\mathbb{A}}^{\times}$, define a fractional ideal $il(x)$ of k by $il(x)_v = x_v \mathfrak{O}_v$ for all finite places v. Explicitly,

$$il(x) = \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}.$$

Lemma 68. *Let* $r_1, \ldots, r_h \in k_{\mathbb{A}}^{\times}$ *be chosen such that the* $il(r_i)$ *represent the* h *distinct ideal classes of* k*. Then there is a disjoint union*

$$k_{\mathbb{A}}^{\times} = \bigcup_{i=1}^{h} r_i \cdot k^{\times} \cdot I_k^{S_\infty}.$$

Proof. Let $x \in k_{\mathbb{A}}^{\times}$. There is a unique i such that the fractional ideal $il(r_i^{-1}x)$ is principal; write $x' = r_i^{-1}x$, so that $il(x') = \langle c \rangle$ for some $c \in k^{\times}$. Then $x'' = c^{-1}x'$ satisfies $x''_v \in \mathfrak{O}_v^{\times}$ for all finite v. Hence $x'' \in I_k^{S_\infty}$. □

In other words, if J_k and P_k denote the groups of fractional ideals and of principal fractional ideals, then $il\colon k_{\mathbb{A}}^{\times} \to J_k$ is a surjective homomorphism with kernel $I_k^{S_\infty}$, and the composite $k_{\mathbb{A}}^{\times} \to J_k \to J_k/P_k$ is surjective with kernel $k^{\times} \cdot I_k^{S_\infty}$.

Remark. It is tempting here, and later also for $\mathrm{GL}(2, k_{\mathbb{A}})$, to refer to the image of an idele in J_k/P_k as its class, and to those ideles with principal class as "principal"; we shall not do this, however, since it would conflict with the established usage of "principal" to mean "coming from a global object via the diagonal embedding $k \to k_{\mathbb{A}}$".

There is a continuous (and clearly surjective) homomorphism

$$|\ |_{\mathbb{A}}\colon k_{\mathbb{A}}^{\times} \to \mathbb{R}_{+}^{\times}, \qquad x = (x_v) \mapsto \prod_v |x_v|_v,$$

with kernel $k_{\mathbb{A}}^{1}$, say. Since $|x|_{\mathbb{A}} = 1$ for a principal idele $x \in k^{\times}$, there is an induced exact sequence

$$1 \to k_{\mathbb{A}}^{1}/k^{\times} \to k_{\mathbb{A}}^{\times}/k^{\times} \to \mathbb{R}_{+}^{\times} \to 1.$$

Moreover, this sequence splits; to see this, fix an infinite place v and map $\mathbb{R}_{+}^{\times} \to k_{\mathbb{A}}^{\times}/k^{\times}$ by mapping $t \in \mathbb{R}_{+}^{\times}$ to the class of the idele that has t in the v-component and 1 in every other component. Therefore,

$$k_{\mathbb{A}}^{\times}/k^{\times} \cong k_{\mathbb{A}}^{1}/k^{\times} \times \mathbb{R}_{+}^{\times}.$$

The group $k_{\mathbb{A}}^{\times}/k^{\times}$ is called the *idele class group*; its study forms part of class field theory.

5.1.3 Class field theory

A *modulus* of k is a formal product $\mathfrak{m} = \prod_v \mathfrak{p}_v^{n_v}$ of prime powers, with $n_v \geq 0$ for all places v, with $n_v = 0$ for almost all v, and with $n_v \in \{0, 1\}$ for the infinite places v. We set

$$U_v^{n_v} = \begin{cases} \mathfrak{O}_v^\times & \text{if } v \nmid \infty \text{ and } n_v = 0, \\ 1 + P_v^{n_v} & \text{if } v \nmid \infty \text{ and } n_v > 0, \\ \mathbb{R}^\times = k_v^\times & \text{if } v \text{ is real and } n_v = 0, \\ \mathbb{R}_+^\times \subset k_v^\times & \text{if } v \text{ is real and } n_v = 1, \\ \mathbb{C}^\times = k_v^\times & \text{if } v \text{ is complex.} \end{cases}$$

For $a_v \in k_v^\times$, we set

$$a_v \equiv 1 \pmod{\mathfrak{p}_v^{n_v}} \quad \Longleftrightarrow \quad a_v \in U_v^{n_v}.$$

For every idele $a = (a_v) \in k_\mathbb{A}^\times$, we set

$$a \equiv 1 \pmod{\mathfrak{m}} \quad \Longleftrightarrow \quad a_v \equiv 1 \pmod{\mathfrak{p}_v^{n_v}} \text{ for all } v,$$

and consider the groups

$$I_k^\mathfrak{m} = \left\{ \alpha \in k_\mathbb{A}^\times \;\middle|\; \alpha \equiv 1 \pmod{\mathfrak{m}} \right\}.$$

Let C_k denote the idele class group $k_\mathbb{A}^\times / k^\times$. The subgroup $C_k^\mathfrak{m} = I_k^\mathfrak{m} \cdot k^\times / k^\times$ is called the *congruence subgroup* mod $\mathfrak{m}$ of C_k. The factor group $C_k / C_k^\mathfrak{m}$ is called the *ray class group* mod $\mathfrak{m}$. When $\mathfrak{m} = 1$, we have

$$I_k^\mathfrak{m} = \prod_{v \mid \infty} k_v^\times \times \prod_{v \nmid \infty} \mathfrak{O}_v^\times = I_k^{S_\infty},$$

where S_∞ is the set of infinite places, so by the remarks after Lemma 68, we have $C_k / C_k^1 = k_\mathbb{A}^\times / I_k^{S_\infty} \cdot k^\times = J_k / P_k$. So the ray class group mod 1 is canonically isomorphic to the ideal class group.

There is also an ideal-theoretic description of the ray class group mod $\mathfrak{m}$ for general $\mathfrak{m}$. Let $J_k^\mathfrak{m}$ be the group of all fractional ideals prime to $\mathfrak{m}$, and $P_k^\mathfrak{m}$ the group of all principal fractional ideals $\langle a \rangle$ with $a \equiv 1 \pmod{\mathfrak{p}_v^{n_v}}$ for all $\mathfrak{p} \mid \mathfrak{m}$. Using the strong approximation theorem, it is easy to show [Neu86, Ch.IV (8.1)] that the homomorphism $il\colon k_{\mathbb{A}}^{\times} \to J_k$ induces an isomorphism

$$C_k/C_k^{\mathfrak{m}} \cong J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}. \tag{5.1}$$

The "existence theorem" of (abelian) global class field theory [Neu86, Ch.IV (7.1)] establishes a bijection between the finite abelian extensions $L|k$ and the closed subgroups of finite index in C_k; if $L|k$ is associated to the group $\mathcal{N}_L$, then L is called the *class field* of $\mathcal{N}_L$, and $\mathcal{N}_L$ is called the *norm group* of L. The correspondence is order-reversing: $L' \supseteq L \iff \mathcal{N}_{L'} \subseteq \mathcal{N}_L$. By "Artin's global reciprocity law", the Galois group of $L|k$ is canonically isomorphic to the quotient of C_k modulo the norm group $\mathcal{N}_L$:

$$\mathrm{Gal}(L|k) \cong C_k/\mathcal{N}_L.$$

The class field $k^{\mathfrak{m}}$ of the congruence subgroup $C_k^{\mathfrak{m}}$ is called the *ray class field* modulo $\mathfrak{m}$. In particular, then, the Galois group of $k^{\mathfrak{m}}|k$ is canonically isomorphic to the ray class group:

$$\mathrm{Gal}(k^{\mathfrak{m}}|k) \cong C_k/C_k^{\mathfrak{m}}. \tag{5.2}$$

It is not hard to show that every norm group $\mathcal{N}_L$ contains a congruence subgroup $C_k^{\mathfrak{m}}$; thus every finite abelian extension of $L|k$ lies in some ray class field $k^{\mathfrak{m}}|k$. The least $\mathfrak{m}$ for which this is possible (i.e. the g.c.d. of all such $\mathfrak{m}$) is called the *conductor* of $L|k$ and denoted $\mathfrak{f}(L|k)$. A prime $\mathfrak{p}$ of k ramifies in L if and only if it divides the conductor.[3]

The ray class field mod 1 is called the *Hilbert class field* of k, and $k^1|k$ is the maximal unramified abelian extension of k; its Galois group is isomorphic to the ideal class group, so in particular, the degree $[k^1 : k]$ is equal to the class number h of k.

Example. Let $k = \mathbb{Q}$ and $\mathfrak{m} = m \cdot \mathfrak{p}_\infty$, where $m \in \mathbb{N}$. Canonically,

$$J_{\mathbb{Q}}^{\mathfrak{m}}/P_{\mathbb{Q}}^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^{\times}. \tag{5.3}$$

[3]It is worth commenting on the interpretation of ramification at an infinite prime $\mathfrak{p}$. Recall that $\mathfrak{p}$ is really an embedding $\sigma\colon k \to \mathbb{C}$ that fixes $\mathbb{Q}$. If $L|k$ is Galois and $\tau\colon L \to \mathbb{C}$ extends σ, we say that $\mathfrak{p}$ ramifies in L if and only if $\sigma k \subseteq \mathbb{R}$ but $\tau L \nsubseteq \mathbb{R}$; this is clearly independent of the choice of τ, because any other choice differs from τ by an element of $\mathrm{Gal}(L|k)$. See [Gar81, p.211].

Namely, each ideal $\langle a \rangle$ in $J_{\mathbb{Q}}^{\mathfrak{m}}$ has two generators, a and $-a$. Mapping the positive generator to its residue class modulo m (defined in the obvious way for $a \in \mathbb{Q}$) we obtain a surjective homomorphism $J_{\mathbb{Q}}^{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^\times$, the kernel of which consists of all ideals $\langle a_1/a_2 \rangle$, with coprime $a_i \in \mathbb{N}$, such that $a_1 \equiv a_2 \pmod{m}$, and these are precisely the ideals $P_{\mathbb{Q}}^{\mathfrak{m}}$. Trivially,

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}_m|\mathbb{Q}),$$

where $\mathbb{Q}_m$ denotes the cyclotomic field obtained by adjoining the m-th roots of unity to $\mathbb{Q}$. This is no coincidence, of course, for $\mathbb{Q}_m$ is the ray class field mod $\mathfrak{m}$. The classical Kronecker-Weber theorem states that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, and this result is generalised by class field theory.

5.1.4 Quasicharacters

The group $k_{\mathbb{A}}^1/k^\times$ is compact [Neu86, Ch.IV (2.8)], so $k_{\mathbb{A}}^\times/k^\times$ is what Weil [Wei67a] calls *quasicompact*, that is, the product of a compact group and one isomorphic to either $\mathbb{R}$ or $\mathbb{Z}$. Other, more elementary examples are the multiplicative groups of local fields, in particular, the groups $k_v^\times$. A *quasicharacter* of a quasicompact group is, by definition, a homomorphism into $\mathbb{C}^\times$. By a *character* of any group we mean a homomorphism into $\{ z \in \mathbb{C}^\times : |z| = 1 \}$.

Lemma 69. *A character of a group G is trivial if its image is contained in the right-hand half-plane $\{z \in \mathbb{C} \mid \Re z > 0\}$.*

Proof. Clear. A 4-line proof may be found in [Wei67a, VII-3, Lemma 2]. □

We shall shortly define the *conductor* of a quasicharacter of the idele class group. Since our treatment follows [Wei67a, Chap.VII, §§3–4], we first give a result about topological groups, part of which is implicitly assumed *loc.cit.*.

Proposition 70. *Let G be a locally compact group with identity e. Then the following are equivalent:*

(i) *G is totally disconnected, i.e. the connected component of e is $\{e\}$;*

(ii) *G is Hausdorff and has a basis of open neighbourhoods of e consisting of compact open subgroups;*

(iii) *G is Hausdorff and has a basis of open neighbourhoods of e consisting of open subgroups.*

Proof. The implication (ii) $\Longrightarrow$ (iii) is trivial, and (iii) $\Longrightarrow$ (i) is clear. The content of the lemma is (i) $\Longrightarrow$ (ii), which is theorem 7.7 in [HR63]. □

For example, $k_{\mathbb{A}}^{\times}$ has the compact, totally disconnected subgroup

$$H = \prod_{v \nmid \infty} \mathfrak{O}_v^{\times}.$$

Let ψ be a quasicharacter of $k_{\mathbb{A}}^{\times}/k^{\times}$; we may regard it as a homomorphism of $k_{\mathbb{A}}^{\times}$ into $\mathbb{C}^{\times}$, trivial on $k^{\times}$. The map $g \mapsto |\psi(g)|$ maps H onto a compact subgroup of $\mathbb{R}_{+}^{\times}$, i.e. onto $\{1\}$, so $\psi|_H$ is a character of H. The pre-image under $\psi|_H$ of $\{z \in \mathbb{C} \mid \Re z > 0\}$ is open, hence by Proposition 70 contains an open subgroup H' of H. By Lemma 69, $H' \subseteq \ker \psi|_H$, so that $\ker \psi|_H$ is an open subgroup of H. This means that $\ker \psi|_H$ contains a subgroup of the form

$$\prod_{v \nmid \infty} U_v^{e(v)}$$

for non-negative integers $e(v)$ almost all of which are zero. For each finite place v, we may therefore define $f(v)$ to be the smallest non-negative integer such that ψ_v is trivial on the subgroup $U_v^{f(v)}$ of $\mathfrak{O}_v^{\times}$. By the above, $f(v) = 0$ for almost all v, so that the ideal

$$\mathfrak{f}_{\psi} = \prod_{v \nmid \infty} \mathfrak{p}_v^{f(v)}$$

exists; $\mathfrak{f}_{\psi}$ is called the *conductor* of ψ.

Remark. Of course, we could have applied property (iii) without calling it total disconnectedness; that approach is taken in Tate's thesis [Tat67, lemma 3.2.1]. So Proposition 70 was not essential in the above.

For every place v of k, we write ψ_v for the *local component* of ψ at v, i.e. for the quasicharacter of $k_v^{\times}$ induced by ψ. For every finite place v, the extended ideal $\mathfrak{f}_{\psi}\mathfrak{O}_v$ is called the *conductor* of ψ_v. The existence of $\mathfrak{f}_\psi$ implies that ψ is the product of its local components: more precisely, for each $x = (x_v) \in k_{\mathbb{A}}^\times$, we can write

$$\psi(x) = \prod_v \psi_v(x_v), \tag{5.4}$$

because almost all the factors in the product are equal to 1. This equation may be abbreviated as $\psi = \prod_v \psi_v$. For later reference, we record the following lemma.

Lemma 71. *Let $\mathfrak{n}$ be an ideal of $\mathfrak{O}$ and let ψ be a quasicharacter of $k_{\mathbb{A}}^\times/k^\times$ whose conductor divides $\mathfrak{n}$. Then ψ induces a character χ of $(\mathfrak{O}/\mathfrak{n})^\times$, given by*

$$\chi(x) = \prod_{v|\mathfrak{n}} \psi_v(x). \tag{5.5}$$

If ψ_v is trivial for the infinite places v, then χ is trivial on $\mathfrak{O}^\times$.

Proof. Let M be the multiplicative monoid $\{\, x \in \mathfrak{O} \mid \langle x \rangle + \mathfrak{n} = \mathfrak{O} \,\}$; certainly (5.5) defines a homomorphism $M \to \mathbb{C}^\times$. For $x, y \in M$ with $xy \equiv 1 \pmod{\mathfrak{n}}$, the assumption on the conductor of ψ implies that $\psi_v(xy) = 1$ for all $v \mid \mathfrak{n}$, so that $\chi(xy) = 1$. Thus χ maps M into the unit circle. Let $x, x' \in M$ satisfy $x \equiv x' \pmod{\mathfrak{n}}$. Let $y \in M$ be an inverse of $x \pmod{\mathfrak{n}}$. Then $\chi(xy) = 1 = \chi(x'y)$, whence $\chi(x) = \chi(x')$. Thus (5.5) induces a character of $(\mathfrak{O}/\mathfrak{n})^\times$. Finally, assume that ψ_v is trivial for the infinite places v and let $\epsilon \in \mathfrak{O}^\times$. Certainly $\psi(\epsilon) = 1$, since $\epsilon \in k^\times$. By the assumption on the conductor, $\psi_v(\epsilon) = 1$ for all finite places v not dividing $\mathfrak{n}$, so applying (5.4) gives $\chi(\epsilon) = 1$, as claimed. ☐

5.1.5 Dirichlet characters

Now let ψ be a character of the idele class group. We say that ψ has *discrete infinite components* if the image of ψ_v for each infinite place v is a discrete subgroup of the unit circle. If v is complex, this means that ψ_v is trivial, and if v is real, that ψ_v is either trivial or of the form $x_v \mapsto \operatorname{sign}(x_v)$. Thus if ψ has discrete infinite components, then it is trivial on $I_k^{\mathfrak{m}}$, where

$$\mathfrak{m} = \mathfrak{f}_\psi \prod_{\substack{v|\infty \\ \psi_v \neq 1}} \mathfrak{p}_v. \tag{5.6}$$

Definition. A *Dirichlet character* is a character ψ of the idele class group having discrete infinite components. The *defining modulus* of ψ is the modulus $\mathfrak{m}$ defined by (5.6). If v is a place dividing $\mathfrak{m}$, we say that ψ is *ramified* at v.

Definition. Let $\mathfrak{m}$ be a modulus of k. A *Dirichlet character* mod $\mathfrak{m}$ is one whose defining modulus divides $\mathfrak{m}$.

Clearly, the Dirichlet characters mod $\mathfrak{m}$ form a group under multiplication. Let ψ be a Dirichlet character mod $\mathfrak{m}$. Then ψ is a character of C_k which is trivial on $C_k^{\mathfrak{m}} = I_k^{\mathfrak{m}} \cdot k^\times / k^\times$, and may be viewed as a character of the ray class group $C_k/C_k^{\mathfrak{m}}$; by (5.1), this is also the same as a character of $J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}$. Conversely, a character of $J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}$ and $C_k/C_k^{\mathfrak{m}}$ gives rise to a Dirichlet character mod $\mathfrak{m}$, because the image of a finite group is automatically discrete. Of course, the definition closest to Dirichlet's is as a character of $J_k^{\mathfrak{m}}/P_k^{\mathfrak{m}}$.

The *Dirichlet L-series* of ψ is defined by

$$L_{\mathfrak{m}}(s, \psi) = \sum_{0 \neq \mathfrak{a} \lhd \mathfrak{O}} \frac{\psi(\mathfrak{a})}{\mathbf{N}(\mathfrak{a})^s},$$

where we have set $\psi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{m}) \neq 1$.

Example. For $k = \mathbb{Q}$ and $\mathfrak{m} = m \cdot \mathfrak{p}_\infty$, we see from (5.3) that ψ is a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. We obtain the classical Dirichlet L-series

$$L(s, \psi) = \sum_{n=1}^{\infty} \frac{\psi(n)}{n^s}.$$

5.1.6 Galois characters

Let $L|k$ be a Galois extension, and let w be a place of L lying above some place v of k. Attached to w is the *inertia group* of w, defined by

$$\{\, \gamma \in \mathrm{Gal}(L|k) \;:\; |a^\gamma - a|_w < 1 \text{ for all } a \in \mathfrak{O}_L \,\},$$

where $\mathfrak{O}_L$ is the ring of integers of L and $|\;|_w$ is any absolute value associated with w. The inertia group of w need not be normal in $\mathrm{Gal}(L|k)$; rather, its conjugates are the inertia groups of all the places of L lying above v. When $L|k$ is abelian, these groups coincide, and we speak of the inertia group of v in $L|k$, denoted by $G_T(v)$. Let k^v be the fixed field of $G_T(v)$; it is the maximal subextension of $L|k$ which is unramified at v.

A *Galois character* of an abelian extension $L|k$ is a character χ of $\mathrm{Gal}(L|k)$. We say that χ is *unramified* at a place v if $\ker\chi$ contains $G_T(v)$ [FT91, p.218]. Since χ is trivial on $\mathrm{Gal}(L|k^v)$, it is determined by the character it induces on $\mathrm{Gal}(k^v|k)$.

We say that χ is *unramified* if it is unramified at all v. This means that $\ker\chi$ contains the subgroup generated by all the inertia groups; its fixed field $k^0|k$ is the maximal unramified subextension of $L|k$. Thus χ is determined by the character it induces on $\mathrm{Gal}(k^0|k)$, which in turn may always be extended to $\mathrm{Gal}(k^1|k)$, since $k^0|k$ is a subextension of the Hilbert class field extension $k^1|k$. Thus unramified Galois characters are really Galois characters of $k^1|k$.

Let $\mathfrak{m}$ be a modulus of k, and let ψ be a Dirichlet character mod $\mathfrak{m}$. By (5.2), we may also regard ψ as a Galois character χ of $k^{\mathfrak{m}}|k$. Conversely, a Galois character of $k^{\mathfrak{m}}|k$ corresponds to a Dirichlet character mod $\mathfrak{m}$. The two notions of ramification are obviously compatible; in particular, ψ is unramified if and only if χ is unramified.

A character χ is *quadratic* if $\chi^2 = 1$. Our interest in unramified quadratic characters stems from their use in defining certain "twists" of modular forms; see [Cre81] for a full discussion in the case when k is an imaginary quadratic field of class number 1.

Example. Let $k = \mathbb{Q}(\sqrt{d_k})$ be the imaginary quadratic field of discriminant $d_k < 0$. Write d_k uniquely as a product of "prime discriminants" [FT91, Ch.III (3.7)], say $d_k = q_1 \cdots q_t$, where t is the number of primes which ramify in $k|\mathbb{Q}$. Put $L = k(\sqrt{q_1}, \ldots, \sqrt{q_t})$. Clearly $[L : \mathbb{Q}] = 2^t$. Moreover, $[C_k : (C_k)^2] = 2^{t-1} = [L : k]$, by "genus theory" [FT91, Ch.VII (2.27)]. On the other hand, $L|\mathbb{Q}$ is abelian [FT91, Ch.III, (3.6)], hence so is $L|k$. Moreover, $L|k$ is unramified [FT91, Ch.III, (3.8)], so by class field theory, there is a tower of fields $k^1 \supseteq L \supseteq k$. By (5.2), we have $C_k \cong \mathrm{Gal}(k^1|k)$, and the subgroup $(C_k)^2$ of squares in C_k clearly fixes L. Comparing degrees, we see that L is the fixed field of $(C_k)^2$; it is called the *genus field* of k, and its Galois group $C_k/(C_k)^2$ the *genus group*.

If χ is a quadratic character of $\mathrm{Gal}(k^1|k)$, then it is certainly trivial on $(C_k)^2$. Moreover, if χ is non-trivial, its image is precisely $\{\pm 1\}$, and its kernel has index 2 in $\mathrm{Gal}(k^1|k)$, so χ corresponds to a quadratic subfield of $L|k$.

5.2 GL(2)

The passage from k to $k_{\mathbb{A}}$ and $k_{\mathbb{A}}^{\times}$ provides two examples of the process of adelisation of an algebraic group, in this case, of the "additive group" G_a and the "multiplicative group" G_m. In §5.2.1, we briefly discuss a general algebraic group G. Thereafter, we always take $G = \mathrm{GL}(2)$. We discuss the adele group $G_{\mathbb{A}}$ in some detail, showing how it acts on lattices in k^2, and deducing some results on the structure of $G_{\mathbb{A}}$. Our treatment is largely self-contained; in particular, we prove all the "strong approximation" results that we need. Finally, we use our results on the structure of $G_{\mathbb{A}}$ to discuss certain functions on $G_{\mathbb{A}}$.

5.2.1 Algebraic groups and strong approximation

A *linear algebraic group* defined over k is an affine variety G defined over k and equipped with group operations which are morphisms of the variety. The basic example is $\mathrm{GL}(n, k)$, which can be represented as the set of points (x_{ij}, y) in k^{n^2+1} that satisfy the equation

$$\det(x_{ij}) \cdot y = 1.$$

According to [Kne67], one can show that the linear algebraic groups are precisely the closed subgroups of $\mathrm{GL}(n, k)$ as n varies.

Let G be a linear algebraic group defined over k. We fix a coordinate system for G; the coordinates of products and inverses are then given by certain polynomials in the coordinates of the operands. If R is a ring containing all the coefficients of these polynomials, we define G_R to be the group of elements of G with coordinates in R. In particular, $G_{\mathbb{A}}$ denotes the adele group of G, and G_k the group of k-rational elements of G, identified with the principal adeles of $G_{\mathbb{A}}$ by means of the embedding of k in $k_{\mathbb{A}}$. For any finite set S of places of k, we put

$$G_S = \prod_{v \in S} G_{k_v},$$

and identify the elements of this group with those adeles of $G_{\mathbb{A}}$ whose v-components are 1 for $v \notin S$.

If $G_k G_S$ is dense in $G_{\mathbb{A}}$, we say that G admits strong approximation with respect to S. For this to happen, it is necessary that G_S not be compact [Kne65]. If this condition on S

is also sufficient, we say that the strong approximation theorem holds for G. It is known to hold for many groups G (see [Kne65]), but we shall only need one result of this type, the case when $G = \mathrm{SL}(2)$ and S is the set of infinite places. This is our Proposition 78 below, for which we give an elementary proof. Our proposition is stated in a slightly different form; the following lemma relates the two formulations.

Lemma 72. *If $G_k G_S$ is dense in $G_{\mathbb{A}}$, then $G_{\mathbb{A}} = G_k \cdot U$ for every open subgroup U of $G_{\mathbb{A}}$ containing G_S. If S contains the infinite places, then the converse is also true.*

Proof. Assume that $G_k G_S$ is dense, and let U be an open subgroup containing G_S. Let $c \in G_{\mathbb{A}}$. Then $G_k G_S$ meets the open set cU, so $cu = \gamma u'$ for some $u \in U$, $\gamma \in G_k$ and $u' \in G_S \subseteq U$. Therefore $c \in G_k \cdot U$.

Conversely, we first note that G_S is a "quasifactor" of $G_{\mathbb{A}}$, that is, $G_{\mathbb{A}} = G_S \times G_1$, where G_1 is an inductive limit over finite sets S' of places disjoint from S. Moreover, if we assume that S contains the infinite places, then G_1 is totally disconnected. Let $c \in G_{\mathbb{A}}$; we must show that $G_k G_S$ meets every open neighbourhood U of c. Writing $c = c_0 c_1$ with $c_0 \in G_S$ and $c_1 \in G_1$, we can find an open neighbourhood U_0 of 1 in G_S and an open *subgroup* U_1 in G_1 with $c_0 U_0 \times c_1 U_1 \subseteq U$. Now $G_S U_1$ is an open subgroup of $G_{\mathbb{A}}$ containing G_S, so by assumption, we can write $c = \gamma \delta u$ with $\gamma \in G_k$, $\delta \in G_S$ and $u \in U_1$. Therefore $\gamma\delta = c_0 \cdot c_1 u^{-1} \in G_k G_S \cap (c_0 U_0 \times c_1 U_1) \subseteq G_k G_S \cap U$. □

5.2.2 The adeles $G_{\mathbb{A}}$ of $\mathrm{GL}(2)$

Let $G = \mathrm{GL}(2)$ be the general linear group in 2 variables considered as an algebraic group defined over k. For each place v of k, write G_v for $\mathrm{GL}(2, k_v)$. Let $G_{\mathbb{A}}$ be the adelisation of G; as we remarked in §5.1.2, we may regard $G_{\mathbb{A}}$ as $\mathrm{GL}(2, k_{\mathbb{A}})$, topologised as a subset of $k_{\mathbb{A}}^5$. Equivalently, we may regard it as the inductive limit of the open subgroups

$$\prod_{v \in S} G_v \times \prod_{v \notin S} \mathrm{GL}(2, \mathfrak{O}_v)$$

where S ranges, as usual, over the finite sets of places of k containing the infinite places. Explicitly,

$$G_{\mathbb{A}} = \{\, (x_v) \mid x_v \in G_v \text{ for all } v;\ x_v \in \mathrm{GL}(2, \mathfrak{O}_v) \text{ for almost all } v \,\}.$$

For finite v, the groups G_v and $\mathrm{GL}(2,\mathfrak{O}_v)$ are totally disconnected (see Proposition 70), a basis of open neighbourhoods of 1 being given by

$$\{\, x_v \in \mathrm{GL}(2,\mathfrak{O}_v) \mid x_v \equiv 1_2 \pmod{\pi_v^n} \,\}, \qquad (n = 0, 1, 2, \dots),$$

where 1_2 is the 2×2 identity matrix; of course, a congruence of matrices is to be understood element-wise. Also put

$$G_\infty = \prod_{v|\infty} G_v.$$

Let G_∞^+ be the connected component of 1 in G_∞, in other words, the subgroup determined by $\det(x_v) > 0$ for all real places v.

5.2.3 Action of $G_{\mathbb{A}}$ on lattices

Let v be a finite place of k, and E_v a finite-dimensional k_v-vector space. A *lattice* L_v in E_v is a compact and open $\mathfrak{O}_v$-submodule ([Wei67a, II-2, defn. 2]). Equivalently ([prop. 5 *loc. cit.*]) it is a finitely generated $\mathfrak{O}_v$-submodule of E_v whose k_v-span is all of E_v. Since $\mathfrak{O}_v$ is a principal ideal domain, L_v is a free $\mathfrak{O}_v$-module and any $\mathfrak{O}_v$-basis of L_v is also a k_v-basis of E_v.

Let E be a finite-dimensional k-vector space. Recall from §1.1.4 that a lattice L in E is a finitely generated $\mathfrak{O}$-submodule of E whose k-span is E. Write $E_v = E \otimes_k k_v$ and take E to be "naturally" embedded in E_v by the injection $e \mapsto e \otimes 1_{k_v}$. Let L_v be the $\mathfrak{O}_v$-submodule generated by L in E_v, in other words, $L_v = L \otimes_{\mathfrak{O}} \mathfrak{O}_v$. Then L_v is a lattice in E_v, and in fact L_v is the closure of L in E_v.

It is now natural to ask, firstly, whether L is uniquely determined by the L_v, and secondly, under what conditions a given set of L_v does come from a global lattice L. The answer is given by the following theorem.

Theorem 73. *Let M be a k-lattice in E. For each finite place v of k, let M_v be the closure of M in E_v and L_v any k_v-lattice in E_v. Then there is a k-lattice L in E whose closure in E_v is L_v for every v if and only if $L_v = M_v$ for almost all v; when that is so, there is only one such k-lattice, and it is given by $L = \cap_v (E \cap L_v)$.*

Proof. [Wei67a, V-3, theorem 2]. □

Using this theorem, one can define an action of the adelisation of $\mathrm{GL}(n)$ on the set of lattices in the n-dimensional space E. We shall only need the case $n = 2$. After choosing a basis, we may identify E with k^2 (regarded as a space of column vectors) and choose for M the *standard lattice* $\mathfrak{O}^2$.

For $c = (c_v) \in G_{\mathbb{A}}$ and a lattice L, we define cL to be the unique lattice in k^2 satisfying $(cL)_v = c_v L_v$ for all finite places v. This works because $L_v = \mathfrak{O}_v^2$ for almost all v (by the theorem) and $c_v \in \mathrm{GL}(2, \mathfrak{O}_v)$ for almost all v (by definition) so that $c_v L_v = \mathfrak{O}_v^2$ for almost all v.

Notice that when $c \in G_k$, this definition agrees with the usual action of a matrix on a set of column vectors. So the action of $G_{\mathbb{A}}$ extends the action of G_k, and there is no confusion when we write cL with $c \in G_k$.

Remark. Because we regarded E as a space of column vectors, we have described a left-action of $G_{\mathbb{A}}$ on "column lattices". Similarly, of course, one obtains a right-action on "row lattices"; the two actions are related by transposition: $Lc = (c^t L^t)^t$.

Lemma 74. *Let L and L' be lattices in k^2 which are isomorphic as $\mathfrak{O}$-modules. Then there exists $\gamma \in G_k$ such that $\gamma L = L'$.*

Proof. Let $f \colon L \to L'$ be an $\mathfrak{O}$-module isomorphism. Localising with respect to the prime ideal $\mathfrak{p} = \langle 0 \rangle$ of $\mathfrak{O}$ (equivalently, tensoring up with k) we obtain a k-module isomorphism $f_{\mathfrak{p}}$ of the vector space k^2 with itself; thus $f_{\mathfrak{p}}$ is given by some matrix $\gamma \in G_k$, and by restriction, the map f is also given by γ. Thus, $\gamma L = L'$. □

In §1.1.3, we defined the Steinitz class $cl(M)$ of a non-zero finitely generated torsion-free $\mathfrak{O}$-module M. Recall that two such modules are isomorphic if and only if they have the same rank and the same Steinitz class. In particular, this theory applies to lattices in k^2; moreover, since these all have the same rank, two such lattices are isomorphic as $\mathfrak{O}$-modules if and only if they have the same Steinitz class. This fact will be used repeatedly below.

It is natural to consider the following open subgroup of $G_{\mathbb{A}}$:

$$\Omega_1 = G_\infty \times \prod_{v\nmid\infty} \mathrm{GL}(2, \mathfrak{O}_v). \tag{5.7}$$

Observe that Ω_1 is the stabiliser of $\mathfrak{O}^2$ under the action of $G_{\mathbb{A}}$:

$$\Omega_1 = \left\{ c \in G_{\mathbb{A}} \mid c\mathfrak{O}^2 = \mathfrak{O}^2 \right\}.$$

Proposition 75. *Let L be a lattice in k^2 and let $c \in G_{\mathbb{A}}$. Then*

$$cl(cL) = cl(il(\det c)) \cdot cl(L).$$

Proof. Choose ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ representing the h ideal classes of k. For each i, let $r_i \in k_{\mathbb{A}}^\times$ be such that $il(r_i) = \mathfrak{a}_i$, and let $a_i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & r_i \end{smallmatrix}\right) \in G_{\mathbb{A}}$. Clearly $a_i\mathfrak{O}^2 = \mathfrak{O} \oplus \mathfrak{a}_i$.

By the structure theory of $\mathfrak{O}$-modules, $L \cong \mathfrak{O} \oplus \mathfrak{a}_i$ for some unique i and $cL \cong \mathfrak{O} \oplus \mathfrak{a}_j$ for some unique j. By the lemma, it follows that $\gamma L = a_i\mathfrak{O}^2$ for some $\gamma \in G_k$ and $\gamma' cL = a_j\mathfrak{O}^2$ for some $\gamma' \in G_k$. Therefore,

$$a_j^{-1}\gamma' c\gamma^{-1}a_i\mathfrak{O}^2 = \mathfrak{O}^2,$$

whence $a_j^{-1}\gamma' c\gamma^{-1}a_i \in \Omega_1$ and so $il(\det(a_j^{-1}\gamma' c\gamma^{-1}a_i)) = \langle 1 \rangle$. Hence

$$il(\det c) \cdot il(\det a_i) \cong il(\det a_j),$$

as required. □

With just these tools at our disposal, we can derive the following coset decompositions of $G_{\mathbb{A}}$. The result will be refined in propositions 81 and 83.

Lemma 76. *Let $a_1, \dots, a_h \in G_{\mathbb{A}}$ be chosen such that the ideals $il(\det a_i)$ represent the h ideal classes of k. Let L be a lattice in k^2 and U the subgroup of $G_{\mathbb{A}}$ stabilising L. Then $G_{\mathbb{A}}$ decomposes as a disjoint union in the following two ways:*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} a_i \cdot G_k \cdot U \qquad \textit{and} \qquad G_{\mathbb{A}} = \bigcup_{i=1}^{h} G_k \cdot a_i \cdot U.$$

Proof. Let $c \in G_{\mathbb{A}}$ and choose i such that $il(\det c) \cong il(\det a_i)$. Then by Proposition 75, $a_i^{-1}cL \cong L$, so by Lemma 74, $\gamma a_i^{-1}cL = L$ for some $\gamma \in G_k$, whence $\gamma a_i^{-1}c \in U$ and so $c \in a_i \cdot G_k \cdot U$.

On the other hand, $cL \cong a_iL$, so $\gamma' cL = a_iL$ for some $\gamma' \in G_k$, whence $a_i^{-1}\gamma' c \in U$ and so $c \in G_k \cdot a_i \cdot U$, as required. □

For any linear algebraic group G, the orbit of a lattice L under $G_{\mathbb{A}}$ is called the *genus* of L, and the orbit under G_k is called the *class* of L. In other words, the genus of L consists of all lattices that are locally isomorphic to L at all finite primes, and the class of L of all lattices that are globally isomorphic to L. We refer to [Kne67] for more information. For $G = \mathrm{GL}(2)$, it is clear from the proof of Proposition 75 that $G_{\mathbb{A}}$ acts transitively on lattices. Thus in our case, there is one genus of h classes.

5.2.4 The group $\Omega_0(\mathfrak{n})$ and the subgroups K_v

Recall that Ω_1 is the stabiliser of $\mathfrak{O}^2$ under the action of $G_{\mathbb{A}}$. More generally, for each integral ideal $\mathfrak{n}$, we consider the stabiliser of $\mathfrak{O} \oplus \mathfrak{n}$:

$$\Omega_{\mathfrak{n}} = \{\, c \in G_{\mathbb{A}} \mid c(\mathfrak{O} \oplus \mathfrak{n}) = \mathfrak{O} \oplus \mathfrak{n} \,\}.$$

Since $G_{\mathbb{A}}$ acts transitively on lattices, the groups $\Omega_{\mathfrak{n}}$ are all conjugate. Explicitly, if n is an idele with $il(n) = \mathfrak{n}$, then by the proof of Proposition 75,

$$\Omega_{\mathfrak{n}} = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Omega_1 \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}^{-1}. \tag{5.8}$$

From our point of view, the interesting group is

$$\Omega_0(\mathfrak{n}) = \Omega_1 \cap \Omega_{\mathfrak{n}},$$

which turns out to be an adelic analogue of the congruence subgroup $\Gamma_0(\mathfrak{n})$, in a manner to be explained below. Indeed, part of our motivation for studying the action of $G_{\mathbb{A}}$ on lattices is to prove Proposition 83 below concerning the group $\Omega_0(\mathfrak{n})$.

Let $\mathfrak{n}$ be an integral ideal, which we shall call the *level*. Choose an idele $n = (n_v) \in k_{\mathbb{A}}^{\times}$ with $il(n) = \mathfrak{n}$. For each finite place v of k, define a compact open subgroup K_v of

$\mathrm{GL}(2, k_v)$ by

$$K_v = \left\{ \begin{pmatrix} a & b \\ n_v c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathfrak{O}_v, \; ad - n_v bc \in \mathfrak{O}_v^\times \right\}.$$

Clearly K_v depends only on the ideal $\mathfrak{n}$; it is a maximal compact subgroup of $\mathrm{GL}(2, k_v)$ if (and only if) $|n|_v = 1$, i.e. if the place v does not occur in $\mathfrak{n}$; when that is so, of course, $K_v = \mathrm{GL}(2, \mathfrak{O}_v)$. By (5.7) and (5.8),

$$\Omega_\mathfrak{n} = G_\infty \times \prod_{v \nmid \infty} K'_v,$$

where

$$K'_v = \left\{ \begin{pmatrix} a & n_v^{-1} b \\ n_v c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathfrak{O}_v, \; ad - bc \in \mathfrak{O}_v^\times \right\}.$$

Taking the intersection $\Omega_0(\mathfrak{n}) = \Omega_1 \cap \Omega_\mathfrak{n}$ now gives

$$\Omega_0(\mathfrak{n}) = G_\infty \times \prod_{v \nmid \infty} K_v. \tag{5.9}$$

It is clear from (5.9) that

$$G_k \cap \Omega_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, d \in \mathfrak{O}, \; c \in \mathfrak{n}, \; ad - bc \in \mathfrak{O}^\times \right\},$$

so that the group of "principal" adeles in $\Omega_0(\mathfrak{n})$ is nothing other than the usual congruence subgroup $\Gamma_0(\mathfrak{n})$ of $\mathrm{GL}(2, \mathfrak{O})$.

5.2.5 Strong approximation for SL(2)

In addition to Ω_1, we consider the following open subgroups of $G_\mathbb{A}$:

$$\Omega_1^+ = G_\infty^+ \times \prod_{v \nmid \infty} \mathrm{GL}(2, \mathfrak{O}_v),$$

and for any integral ideal $\mathfrak{n}$,

$$U_\mathfrak{n} = \{ \, x = (x_v) \in \Omega_1 \mid x_v \equiv 1_2 \pmod{\mathfrak{n}\mathfrak{O}_v} \text{ for all finite } v \, \},$$

$$U_\mathfrak{n}^+ = U_\mathfrak{n} \cap \Omega_1^+.$$

Lemma 77. *Every open subgroup of $G_{\mathbb{A}}$ contains $U_{\mathfrak{n}}^{+}$ for some $\mathfrak{n}$, and every open subgroup of $G_{\mathbb{A}}$ containing G_∞ contains $U_{\mathfrak{n}}$ for some $\mathfrak{n}$.*

Proof. Clear from the definition of the topology on $G_{\mathbb{A}}$. □

As we remarked just before Lemma 72, the next result is a special case of strong approximation for SL(2).

Proposition 78. *Let U be an open subgroup of $G_{\mathbb{A}}$ containing G_∞. Then*

$$\mathrm{SL}(2, k_{\mathbb{A}}) = \mathrm{SL}(2, k) \cdot \big(U \cap \mathrm{SL}(2, k_{\mathbb{A}})\big) = \big(U \cap \mathrm{SL}(2, k_{\mathbb{A}})\big) \cdot \mathrm{SL}(2, k).$$

Proof. Our proof is based on [Shi71, lemma 6.15], which deals with the case $k = \mathbb{Q}$. The first equality will imply the second, since we can take transposes and note that U^t is open and contains G_∞.

Let $L = \mathfrak{O}^2$ and let $c \in \mathrm{SL}(2, k_{\mathbb{A}})$. Then $il(\det c) = \langle 1 \rangle$, so by Proposition 75, $cL \cong L$ as $\mathfrak{O}$-modules. By Lemma 74, $\gamma c L = L$ for some $\gamma \in G_k$. That is, $\gamma c \in \Omega_1$ for some $\gamma \in G_k$.

Therefore $\det\gamma \in \det(\Omega_1) \cap k^\times = \mathfrak{O}^\times$. Let $\epsilon = \begin{pmatrix} \det\gamma & 0 \\ 0 & 1 \end{pmatrix}^{-1} \in G_k$. Then $\det(\epsilon\gamma) = 1$ and $\gamma c L = L = \epsilon^{-1} L$, whence $(\epsilon\gamma)c \in \Omega_1 \cap \mathrm{SL}(2, k_{\mathbb{A}})$. This proves

$$\mathrm{SL}(2, k_{\mathbb{A}}) = \mathrm{SL}(2, k) \cdot \big(\Omega_1 \cap \mathrm{SL}(2, k_{\mathbb{A}})\big). \tag{5.10}$$

In view of Lemma 77, it is sufficient to prove the proposition in the case $U = U_{\mathfrak{n}}$. By virtue of (5.10), the question is reduced to showing that

$$\Omega_1 \cap \mathrm{SL}(2, k_{\mathbb{A}}) \subseteq \mathrm{SL}(2, \mathfrak{O}) \cdot \big(U_{\mathfrak{n}} \cap \mathrm{SL}(2, k_{\mathbb{A}})\big). \tag{5.11}$$

Let $u = (u_v) \in \Omega_1 \cap \mathrm{SL}(2, k_{\mathbb{A}})$. By the Chinese Remainder Theorem for $\mathfrak{O}$ applied to each matrix entry, there exists $\beta \in \mathrm{M}_2(\mathfrak{O})$ such that

$$\beta \equiv u_v^{-1} \mod \mathfrak{n}\mathfrak{O}_v \tag{5.12}$$

for each finite v. (Notice that for almost all v, namely unless $v \mid \mathfrak{n}$, condition (5.12) just says that the entries of β must lie in $\mathfrak{O}_v$; as this holds automatically for elements of $\mathfrak{O}$, it is indeed enough to use the Chinese Remainder Theorem for $\mathfrak{O}$, rather than the strong approximation theorem for k.) Then $\det \beta \equiv 1 \pmod{\mathfrak{n}}$. By surjectivity of $\mathrm{SL}(2, \mathfrak{O}) \to \mathrm{SL}(2, \mathfrak{O}/\mathfrak{n})$ in Proposition 22, there exists an element α of $\mathrm{SL}(2, \mathfrak{O})$ such that $\alpha \equiv \beta \pmod{\mathfrak{n}}$. Then $\alpha u \in U_{\mathfrak{n}} \cap \mathrm{SL}(2, k_{\mathbb{A}})$, proving (5.11). □

5.2.6 Decomposition of $G_{\mathbb{A}}$

Let v be a finite place of k and let $\pi = \pi_v$. Let L_v be a sublattice of $\mathfrak{O}_v^2$. Since $\mathfrak{O}_v$ is a principal ideal domain, L_v is free, and we may write the elements of a basis as the columns of a matrix M, so that $L_v = M\mathfrak{O}_v^2$. We shall say that L_v is *spanned by* M. Write $M \sim M'$ if M and M' span the same lattice, that is, if they are right-associate by an element of $\mathrm{GL}(2, \mathfrak{O}_v)$. The index of L_v in $\mathfrak{O}_v^2$ is just the ideal $\langle \det M \rangle$. Every L_v of index $\langle \pi^n \rangle$ is spanned by some M of the form $\begin{pmatrix} \pi^l & 0 \\ * & \pi^{n-l} \end{pmatrix}$. This is just the Hermite normal form, which exists over any principal ideal domain, so *a fortiori* over the discrete valuation ring $\mathfrak{O}_v$.

Lemma 79. *Let L_v be a lattice in $\mathfrak{O}_v^2$ of index $\langle \pi^n \rangle$. Let $u_v, u_v' \in \mathrm{GL}(2, \mathfrak{O}_v)$ satisfy $u_v \equiv u_v' \pmod{\pi^n}$. Then $u_v L_v = u_v' L_v$.*

Proof. We may write $L_v = M\mathfrak{O}_v^2$ with $M = \begin{pmatrix} \pi^l & 0 \\ z & \pi^{n-l} \end{pmatrix}$. We must show that $u_v M \sim u_v' M$, in other words, that $N \in \mathrm{GL}(2, \mathfrak{O}_v)$, where $N = M^{-1} u_v^{-1} u_v' M$. Clearly $\det N = 1$, so we need only show that the entries of

$$\begin{pmatrix} \pi^{n-l} & 0 \\ -z & \pi^l \end{pmatrix} u_v^{-1} u_v' \begin{pmatrix} \pi^l & 0 \\ z & \pi^{n-l} \end{pmatrix}$$

are divisible by $\det M = \pi^n$. But working modulo π^n we have $u_v^{-1} u_v' = 1_2$, so the result is obvious. □

Proposition 80. *With notation as above,*

$$\Omega_1 = \mathrm{SL}(2, \mathfrak{O}) \cdot \Omega_0(\mathfrak{n}).$$

Proof. Recalling that $\Omega_0(\mathfrak{n}) = \Omega_1 \cap \Omega_{\mathfrak{n}}$, we see that one inclusion is trivial, since Ω_1 contains $\mathrm{SL}(2,\mathfrak{O})$. Conversely, let $u = (u_v) \in \Omega_1$ be given and let $L = \mathfrak{O} \oplus \mathfrak{n}$. For each finite v, let $\pi = \pi_v$ and define n (depending on v) by $\mathfrak{n}\mathfrak{O}_v = \pi^n \mathfrak{O}_v$. Thus L_v is spanned by $\begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix}$ and has index $\langle \pi^n \rangle$ in $\mathfrak{O}_v^2$. For $v \mid \mathfrak{n}$, put $u_v' = u_v \begin{pmatrix} \det u_v^{-1} & 0 \\ 0 & 1 \end{pmatrix}$. Then $\det u_v' = 1$, and since

$$\begin{pmatrix} \det u_v^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix},$$

it follows that $u_v' L_v = u_v L_v$.

By the Chinese Remainder Theorem, there is $\gamma' \in \mathrm{M}_2(\mathfrak{O})$ such that $\gamma' \equiv u_v' \pmod{\pi^n}$ for each finite v. Then $\det \gamma' \equiv \det u_v' \equiv 1 \pmod{\pi^n}$, whence by the Chinese Remainder Theorem again, $\det \gamma' \equiv 1 \pmod{\mathfrak{n}}$. Now by surjectivity of $\mathrm{SL}(2,\mathfrak{O}) \to \mathrm{SL}(2,\mathfrak{O}/\mathfrak{n})$ in Proposition 22, there is $\gamma \in \mathrm{SL}(2,\mathfrak{O})$ satisfying $\gamma \equiv \gamma' \pmod{\mathfrak{n}}$.

Clearly $\gamma \mathfrak{O}^2 = \mathfrak{O}^2$, so $\gamma \in \Omega_1$ and therefore $\gamma^{-1} u \in \Omega_1$. We claim that $\gamma^{-1} u \in \Omega_{\mathfrak{n}}$ also, which will complete the proof. For finite $v \nmid \mathfrak{n}$, $L_v = \mathfrak{O}_v^2$ and so

$$\gamma L_v = \gamma \mathfrak{O}_v^2 = \mathfrak{O}_v^2 = u_v \mathfrak{O}_v^2 = u_v L_v.$$

For $v \mid \mathfrak{n}$, using Lemma 79,

$$\gamma L_v = u_v' L_v = u_v L_v.$$

Thus $(\gamma L)_v = \gamma L_v = u_v L_v = (uL)_v$ for all finite v, whence by Theorem 73, $\gamma L = uL$. Therefore $\gamma^{-1} u \in \Omega_{\mathfrak{n}}$, as required. □

Note the resemblance of this proof to that of Proposition 78. The next result is an easy corollary.

Proposition 81. *Let $a_1, \ldots, a_h \in G_{\mathbb{A}}$ be such that the ideals $il(\det a_i)$ represent the h ideal classes of k. Then $G_{\mathbb{A}}$ decomposes as a disjoint union*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} a_i \cdot G_k \cdot \Omega_0(\mathfrak{n}).$$

Proof. Let $c \in G_{\mathbb{A}}$. By Lemma 76 with $U = \Omega_1$, there is a unique i such that $\gamma a_i^{-1} c \in \Omega_1$ for some $\gamma \in G_k$. By Proposition 80 there exists $\gamma' \in \mathrm{SL}(2, \mathfrak{O})$ such that $\gamma a_i^{-1} c \in \gamma' \Omega_0(\mathfrak{n})$. Therefore $c \in a_i \cdot G_k \cdot \Omega_0(\mathfrak{n})$. □

The advantage of this proof is that it works directly with the characterisation of $\Omega_0(\mathfrak{n}) = \Omega_1 \cap \Omega_{\mathfrak{n}}$ in terms of the action of $G_{\mathbb{A}}$ on lattices. Using Proposition 78, we can give another, somewhat less direct proof, along the lines of the one in [Wei71, §3] for the case $k = \mathbb{Q}$; see also the notes at the end of §3 of [Gel75]. This allows us to replace $\Omega_0(\mathfrak{n})$ by a somewhat more general subgroup U. We give this result here, although we shall not need to use it.

Proposition 82. *Let $a_1, \ldots, a_h \in G_{\mathbb{A}}$ be such that the ideals $il(\det a_i)$ represent the h ideal classes of k, and let U be an open subgroup of $G_{\mathbb{A}}$ containing G_∞ and all $\left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for $u \in I_k^{S_\infty}$. Then $G_{\mathbb{A}}$ decomposes as a disjoint union*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} a_i \cdot G_k \cdot U.$$

Proof. The map $g \mapsto \det(g)$ is a morphism of $G_{\mathbb{A}}$ onto $k_{\mathbb{A}}^\times$, and by Lemma 68,

$$k_{\mathbb{A}}^\times = \bigcup r_i \cdot k^\times \cdot I_k^{S_\infty},$$

where $r_i = \det(a_i)$. For any $g \in G_{\mathbb{A}}$, write $\det(g) = r_i \cdot r \cdot u$ with $r \in k^\times$ and $u \in I_k^{S_\infty}$. Put

$$g' = \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix} a_i^{-1} g \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\det g' = 1$, i.e. $g' \in \mathrm{SL}(2, k_{\mathbb{A}})$. By Proposition 78, we can find $\gamma_1 \in \mathrm{SL}(2, k)$ such that $\gamma_1^{-1} g' \in U \cap \mathrm{SL}(2, k_{\mathbb{A}})$. Put $\gamma = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \gamma_1$. Then $\gamma \in G_k$ and

$$\gamma^{-1} a_i^{-1} g = \gamma_1^{-1} g' \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$$

The right hand side is in U, by assumption, so $\gamma^{-1} a_i^{-1} g \in U$, proving $g \in a_i \cdot G_k \cdot U$. □

The next result is similar to Proposition 81, but the factors occur in a different order, necessitating an extra step in the proof. It is this result which will be of central importance for us in §5.2.7.

Proposition 83. *Let $a_1, \ldots, a_h \in G_{\mathbb{A}}$ be such that the ideals $il(\det a_i)$ represent the h ideal classes of k. Then $G_{\mathbb{A}}$ decomposes as a disjoint union*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} G_k \cdot a_i \cdot \Omega_0(\mathfrak{n}).$$

Proof. Let $c \in G_{\mathbb{A}}$. By Lemma 76 with $U = \Omega_1$, there is a unique i such that $a_i^{-1}\gamma c \in \Omega_1$ for some $\gamma \in G_k$. Therefore, $\gamma c a_i^{-1} \in a_i \Omega_1 a_i^{-1}$. By Proposition 80,

$$\begin{aligned} a_i \Omega_1 a_i^{-1} &= a_i \, \mathrm{SL}(2, \mathfrak{O}) a_i^{-1} \cdot a_i \Omega_0(\mathfrak{n}) a_i^{-1} \\ &\subseteq \mathrm{SL}(2, k_{\mathbb{A}}) \cdot a_i \Omega_0(\mathfrak{n}) a_i^{-1}; \end{aligned}$$

hence we can write $\gamma c a_i^{-1} = c'(a_i \omega a_i^{-1})$, where $c' \in \mathrm{SL}(2, k_{\mathbb{A}})$ and $\omega \in \Omega_0(\mathfrak{n})$. Since $a_i \Omega_0(\mathfrak{n}) a_i^{-1}$ is an open subgroup of $G_{\mathbb{A}}$ containing G_∞, Proposition 78 implies that $c' = \gamma' a_i \omega' a_i^{-1}$ for some $\gamma' \in \mathrm{SL}(2, k)$ and $\omega' \in \Omega_0(\mathfrak{n})$. Consequently, $\gamma c a_i^{-1} = \gamma' a_i \omega' \omega a_i^{-1}$, so that $a_i^{-1}(\gamma')^{-1}\gamma c = \omega'\omega \in \Omega_0(\mathfrak{n})$. Therefore $c \in G_k \cdot a_i \cdot \Omega_0(\mathfrak{n})$. □

5.2.7 Functions on $G_{\mathbb{A}}$

The automorphic forms of interest to us will be introduced as certain functions from $G_{\mathbb{A}}$ into a complex vector space V. For the moment, we regard V as any topological space.

We fix a level $\mathfrak{n}$ and a choice of the a_i as in Proposition 83, so that

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} G_k \cdot a_i \cdot \Omega_0(\mathfrak{n}).$$

Any function Φ on $G_k \backslash G_{\mathbb{A}}$ (i.e. on $G_{\mathbb{A}}$, left-invariant by G_k) thus determines a collection of h functions $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$, via

$$\Phi^{(i)}(\omega) = \Phi(a_i \omega) \qquad \big(\omega \in \Omega_0(\mathfrak{n})\big). \tag{5.13}$$

It turns out that each $\Phi^{(i)}$ is left-invariant under the group $\Gamma^{(i)}$ defined by

$$\Gamma^{(i)} = \Omega_0(\mathfrak{n}) \cap a_i^{-1} G_k a_i.$$

For let $\omega = a_i^{-1}\gamma a_i \in \Gamma^{(i)}$ and $\omega' \in \Omega_0(\mathfrak{n})$. Then $a_i \omega\omega' = \gamma a_i \omega'$, so

$$\Phi^{(i)}(\omega\omega') = \Phi(a_i\omega\omega') = \Phi(\gamma a_i \omega') = \Phi(a_i\omega') = \Phi^{(i)}(\omega').$$

Conversely, suppose we are given functions $\Phi^{(i)}$ left-invariant under $\Gamma^{(i)}$. Then we can define Φ on $G_{\mathbb{A}}$, left-invariant by G_k, via

$$\Phi(\gamma a_i \omega) = \Phi^{(i)}(\omega) \qquad \big(\gamma \in G_k,\ \omega \in \Omega_0(\mathfrak{n})\big). \tag{5.14}$$

If this Φ is well-defined, it is certainly left-invariant under G_k. To show that it is well-defined, we need only show that two ways of writing an element of $G_{\mathbb{A}}$ in the form $\gamma a_i \omega$ give the same value of Φ. Since i is uniquely determined, we just need to check that

$$\gamma a_i \omega = \gamma' a_i \omega' \implies \Phi^{(i)}(\omega) = \Phi^{(i)}(\omega').$$

But this is clear, since $a_i^{-1}(\gamma')^{-1}\gamma a_i = \omega'\omega^{-1} \in \Gamma^{(i)}$, so $\Phi^{(i)}(\omega) = \Phi^{(i)}(\omega'\omega^{-1}\cdot\omega) = \Phi^{(i)}(\omega')$.

Proposition 84. *With notation as above, there is a bijection, given by* (5.13) *and* (5.14)*, between the set of functions Φ on $G_{\mathbb{A}}$ that are left-invariant under G_k, and the set of h-tuples of functions $\Phi^{(i)}$ on $\Omega_0(\mathfrak{n})$ such that for $1 \le i \le h$, $\Phi^{(i)}$ is left-invariant under $\Gamma^{(i)}$. Moreover, Φ is continuous if and only if the corresponding $\Phi^{(i)}$ are continuous.*

Proof. It is clear that the constructions (5.13) and (5.14) are mutually inverse, so we need only prove the last sentence. Assume that Φ is continuous, and let $U \subseteq V$ be open. Then $\big(\Phi^{(i)}\big)^{-1}(U) = \Omega_0(\mathfrak{n}) \cap a_i^{-1}\cdot\Phi^{-1}(U)$ is open, so $\Phi^{(i)}$ is continuous. Conversely, assume that each $\Phi^{(i)}$ is continuous, and let $U \subseteq V$ be open. Then $\Phi^{-1}(U) = \cup G_k \cdot a_i \cdot \big(\Phi^{(i)}\big)^{-1}(U)$. Since $\big(\Phi^{(i)}\big)^{-1}(U)$ is open in $\Omega_0(\mathfrak{n})$ which is open in $G_{\mathbb{A}}$, it follows that $\Phi^{-1}(U)$ is open, so Φ is continuous. $\square$

In §5.2.4 we defined the subgroups K_v of $\Omega_0(\mathfrak{n})$ for the finite places v. Below, $\prod K_v$ denotes the product over the finite places.

Corollary 85. *The bijection given by* (5.13) *and* (5.14) *restricts to a bijection between, on the one hand, the set of functions Φ on $G_{\mathbb{A}}$ that are left-invariant under G_k and right-invariant under $\prod K_v$, and, on the other hand, the set of h-tuples of functions $\Phi^{(i)}$ on $\Omega_0(\mathfrak{n})$ such that for $1 \le i \le h$, $\Phi^{(i)}$ is left-invariant under $\Gamma^{(i)}$ and right-invariant under $\prod K_v$.*

Proof. Clearly Φ is right-invariant under $\prod K_v$ if and only if the same is true of each $\Phi^{(i)}$. The corollary is thus immediate. $\square$

Notation. For $a = (a_v) \in G_{\mathbb{A}}$, we write a_∞ for the projection of a onto the quasifactor[4] G_∞, and a_0 for the projection onto the complementary factor; in other words, $a_\infty = (a_w)$, where w ranges over the infinite places, and $a_0 = (a_v)$, where v now ranges only over the finite places. Thus, we may write $a = (a_\infty, a_0)$.

With this notation, if $a \in \Omega_0(\mathfrak{n})$, then $a_0 \in \prod K_v$. Of course, the last sentence relies on (5.9) of §5.2.4, viz on the equation

$$\Omega_0(\mathfrak{n}) = G_\infty \times \prod_{v \nmid \infty} K_v.$$

In view of this decomposition, functions on $\Omega_0(\mathfrak{n})$ which are right-invariant under $\prod K_v$ correspond naturally to functions on G_∞. We will apply this to the functions $\Phi^{(i)}$ in Corollary 85; in order to formulate the transformation property of the resulting functions, we introduce the groups

$$\Gamma^{[i]} = G_k \cap a_i \Omega_0(\mathfrak{n}) a_i^{-1}. \tag{5.15}$$

so that

$$\Gamma^{(i)} = a_i^{-1} \Gamma^{[i]} a_i.$$

Given $\Phi^{(i)}$ as in Corollary 85, we define $\phi^{(i)} \colon G_\infty \to V$ by

$$\phi^{(i)}(\delta) = \Phi^{(i)}\left((a_i^{-1}\delta a_i)_\infty, 1\right). \tag{5.16}$$

Conversely, given $\phi^{(i)} \colon G_\infty \to V$, left-invariant under $\Gamma^{[i]}$, we define $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$ by

$$\Phi^{(i)}(x) = \phi^{(i)}\left((a_i x a_i^{-1})_\infty\right). \tag{5.17}$$

Lemma 86. *For $1 \leq i \leq h$, there is a bijection, given by* (5.16) *and* (5.17), *between, on the one hand, the set of functions $\Phi^{(i)}$ on $\Omega_0(\mathfrak{n})$ that are left-invariant under $\Gamma^{(i)}$ and right-invariant under $\prod K_v$, and, on the other hand, the set of functions $\phi^{(i)}$ on G_∞ that are left-invariant under $\Gamma^{[i]}$.*

[4] see p.121

Proof. Let $\Phi^{(i)}$ be given and define $\phi^{(i)}$ by (5.16). Then for $\gamma \in \Gamma^{[i]}$,

$$\begin{aligned} \phi^{(i)}(\gamma\delta) &= \Phi^{(i)}\left((a_i^{-1}\gamma\delta a_i)_\infty, 1\right) \\ &= \Phi^{(i)}\left((a_i^{-1}\delta a_i)_\infty, (a_i^{-1}\gamma^{-1}a_i)_0\right) && \text{since } a_i^{-1}\gamma a_i \in \Gamma^{(i)} \\ &= \Phi^{(i)}\left((a_i^{-1}\delta a_i)_\infty, 1\right) && \text{since } (a_i^{-1}\gamma^{-1}a_i)_0 \in \prod K_v \\ &= \phi^{(i)}(\delta). \end{aligned}$$

Thus $\phi^{(i)}$ is left-invariant under $\Gamma^{[i]}$, as required. Conversely, let $\phi^{(i)}$ be given and define $\Phi^{(i)}$ by (5.17). Right-invariance of $\Phi^{(i)}$ under $\prod K_v$ is obvious. Moreover, for $\gamma \in \Gamma^{[i]}$,

$$\begin{aligned} \Phi^{(i)}(a_i^{-1}\gamma a_i x) &= \phi^{(i)}\left((a_i a_i^{-1}\gamma a_i x a_i^{-1})_\infty\right) \\ &= \phi^{(i)}\left(\gamma(a_i x a_i^{-1})_\infty\right) \\ &= \phi^{(i)}\left((a_i x a_i^{-1})_\infty\right) && \text{by left-invariance under } \Gamma^{[i]} \\ &= \Phi^{(i)}(x). \end{aligned}$$

Thus $\Phi^{(i)}$ is left-invariant under $\Gamma^{(i)}$, as required. □

The following result is an immediate corollary; in view of its importance in Chapter 6, we designate this result a theorem.

Theorem 87. *There is a bijection between, on the one hand, the set of functions Φ on $G_{\mathbb{A}}$ that are left-invariant under G_k and right-invariant under $\prod K_v$, and, on the other hand, the set of h-tuples of functions $\phi^{(i)}$ on G_∞ such that for $1 \leq i \leq h$, $\phi^{(i)}$ is left-invariant under $\Gamma^{[i]}$.*

Proof. Compose the bijections of Corollary 85 and Lemma 86. □

Of course, the correspondence between the functions $\Phi^{(i)}$ and $\phi^{(i)}$ is especially simple when the a_i are chosen such that $(a_i)_\infty = 1$. In that case, equations (5.16) and (5.17) simplify to

$$\phi^{(i)}(\delta) = \Phi^{(i)}(\delta, 1) \qquad (\delta \in G_\infty)$$

and

$$\Phi^{(i)}(x) = \phi^{(i)}(x_\infty) \qquad \left(x \in \Omega_0(\mathfrak{n})\right).$$

Notation. Let $\mathcal{Z}$ denote the centre of $G = \mathrm{GL}(2)$ as an algebraic group defined over k; it consists of scalar multiples of the 2×2 identity matrix 1_2 and can thus be identified with the multiplicative group $G_m = \mathrm{GL}(1)$. Write $\mathcal{Z}_{\mathbb{A}}$ for the corresponding adelised group; $\mathcal{Z}_{\mathbb{A}}$ can be identified with the idele group $k_{\mathbb{A}}^{\times}$ of k.

We now consider what happens when Φ in Proposition 84 is invariant under the centre, i.e. when

$$\Phi(zx) = \Phi(x) \qquad (z \in \mathcal{Z}_{\mathbb{A}},\ x \in G_{\mathbb{A}}).$$

Clearly, the corresponding functions $\Phi^{(i)}$ will not now be arbitrary.

Definition. Functions $\Phi^{(i)}$ as in Proposition 84 are *$\mathcal{Z}$-compatible* if the corresponding function Φ is invariant under $\mathcal{Z}_{\mathbb{A}}$.

Let $\Phi\colon G_{\mathbb{A}} \to V$ be left-invariant under G_k and invariant under $\mathcal{Z}_{\mathbb{A}}$. Let $z \in \mathcal{Z}_{\mathbb{A}}$ and suppose that $il(\det z)$ is principal. Thus $za_i = \delta a_i w$ for some $\delta \in G_k$, $w \in \Omega_0(\mathfrak{n})$. Then

$$\Phi^{(i)}(x) = \Phi(a_i x) = \Phi(z a_i x) = \Phi(\delta a_i w x) = \Phi^{(i)}(wx),$$

so that $\Phi^{(i)}$ is left-invariant under all the $w \in \Omega_0(\mathfrak{n})$ that arise in this way; the set of all such w is easily seen to be equal to the group

$$\widetilde{\Gamma}^{(i)} = \Omega_0(\mathfrak{n}) \cap a_i^{-1} G_k \mathcal{Z}_{\mathbb{A}} a_i,$$

since if $a_i^{-1}\delta z a_i \in \Omega_0(\mathfrak{n})$, where $\delta \in G_k$ and $z \in \mathcal{Z}_{\mathbb{A}}$, then $il(\det z)$ is automatically principal.

Thus, for functions $\Phi^{(i)}$ to be $\mathcal{Z}$-compatible, it is necessary that each $\Phi^{(i)}$ be left-invariant under $\widetilde{\Gamma}^{(i)}$. This is not sufficient, of course, since (in general) there are elements z in $\mathcal{Z}_{\mathbb{A}}$ with $il(\det z)$ non-principal. Suppose that i, j are such that $il(\det(a_i^{-1}a_j))$ is a square, say equal to $\mathfrak{a}^2$. Let $a \in k_{\mathbb{A}}^{\times}$ be an idele with $il(a) = \mathfrak{a}$. Let $z = a \cdot 1_2 \in \mathcal{Z}_{\mathbb{A}}$. Then multiplication by z (on the left, say) defines a homeomorphism

$$G_k \cdot a_i \cdot \Omega_0(\mathfrak{n}) \longrightarrow G_k \cdot a_j \cdot \Omega_0(\mathfrak{n}).$$

So if the $\Phi^{(i)}$ are $\mathcal{Z}$-compatible, the function $\Phi^{(j)}$ is determined by $\Phi^{(i)}$. Thus, all the information about Φ is contained in just some of the functions $\Phi^{(i)}$: we only need one for each ideal class modulo squares. The next proposition shows that there is no further redundancy.

Proposition 88. *Let S be a set of indices such that the $il(\det a_i)$, for $i \in S$, represent the ideal classes modulo squares. For $i \in S$, let $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$ be left-invariant under $\widetilde{\Gamma}^{(i)}$. Then there are unique functions $\Phi^{(j)} \colon \Omega_0(\mathfrak{n}) \to V$ for $j \notin S$ such that the $\Phi^{(i)}$ for $1 \le i \le h$ are $\mathcal{Z}$-compatible.*

Proof. Suppose that such functions (for $j \notin S$) exist, and that the $\Phi^{(i)}$ for $1 \le i \le h$ correspond to Φ, say. Let j be an index not in S. There is a unique $i \in S$ for which there exists $z \in \mathcal{Z}_{\mathbb{A}}$ with $za_j \in G_k \cdot a_i \cdot \Omega_0(\mathfrak{n})$. (In fact, i must be chosen such that $il(\det(a_j^{-1}a_i))$ is a square, say equal to $\mathfrak{a}^2$. A possible choice of z is then $z = a \cdot 1_2$, where $a \in k_{\mathbb{A}}^{\times}$ is an idele with $il(a) = \mathfrak{a}$.) Write $za_j = \delta a_i w$ with $\delta \in G_k$ and $w \in \Omega_0(\mathfrak{n})$. Then for all $x \in \Omega_0(\mathfrak{n})$,

$$\Phi^{(j)}(x) = \Phi(a_j x) = \Phi(za_j x) = \Phi(\delta a_i w x) = \Phi^{(i)}(wx).$$

So if such functions (for $j \notin S$) exist, they are uniquely determined by the given functions (for $i \in S$).

We now define functions $\Phi^{(j)}$, for $j \notin S$, by

$$\Phi^{(j)}(x) = \Phi^{(i)}(wx) \qquad \big(x \in \Omega_0(\mathfrak{n})\big), \tag{5.18}$$

where i and w are as above. We first check that $\Phi^{(j)}$ is well-defined by (5.18). Suppose we also have $z'a_j = \delta' a_i w'$ with $z' \in \mathcal{Z}_{\mathbb{A}}$, $\delta' \in G_k$ and $w' \in \Omega_0(\mathfrak{n})$. Then $w'w^{-1} = a_i^{-1}(\delta')^{-1}\delta z' z^{-1} a_i \in \widetilde{\Gamma}^{(i)}$. Therefore $\Phi^{(i)}(w'x) = \Phi^{(i)}(w'w^{-1} \cdot wx) = \Phi^{(i)}(wx)$.

Next, we see that $\Phi^{(j)}$ is left-invariant under $\widetilde{\Gamma}^{(j)}$. For let $y \in \widetilde{\Gamma}^{(j)}$, say $y = a_j^{-1}\gamma z' a_j$ with $\gamma \in G_k$ and $z' \in \mathcal{Z}_{\mathbb{A}}$. Then $wy = y'w$, where $y' = a_i^{-1}\delta^{-1}\gamma\delta z' a_i \in \widetilde{\Gamma}^{(i)}$. Therefore, for all $x \in \Omega_0(\mathfrak{n})$,

$$\Phi^{(j)}(yx) = \Phi^{(i)}(wyx) = \Phi^{(i)}(y'wx) = \Phi^{(i)}(wx) = \Phi^{(j)}(x).$$

Since the $\Phi^{(i)}$ are left-invariant under $\widetilde{\Gamma}^{(i)}$, *a fortiori* under $\Gamma^{(i)}$, they correspond as in Proposition 84 to a function Φ which is left-invariant under G_k. It only remains to show that Φ is invariant under $\mathcal{Z}_{\mathbb{A}}$. Let $a \in G_{\mathbb{A}}$ and $z \in \mathcal{Z}_{\mathbb{A}}$. Write $a = \gamma a_i w_0$ and $za_i = \delta a_j w_1$

with $\gamma, \delta \in G_k$ and $w_0, w_1 \in \Omega_0(\mathfrak{n})$. (Of course, $i = j$ if and only if $il(\det z)$ is principal.) Then $a_i^{-1} a_j w_1 = a_i^{-1} \delta^{-1} z a_i \in \widetilde{\Gamma}^{(i)}$, so

$$\Phi(za) = \Phi(a_j w_1 w_0) = \Phi^{(i)}(a_i^{-1} a_j w_1 \cdot w_0) = \Phi^{(i)}(w_0) = \Phi(a).$$

This completes the proof. □

Corollary 89. *Let S be as in Proposition 88. The constructions above give bijections between*

(i) *the set of functions $\Phi \colon G_{\mathbb{A}} \to V$ that are left-invariant under G_k and invariant under $\mathcal{Z}_{\mathbb{A}}$,*

(ii) *the set of $\mathcal{Z}$-compatible h-tuples of functions $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$ such that, for $1 \leq i \leq h$, $\Phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{(i)}$, and*

(iii) *the set of families of functions $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$, indexed by $i \in S$, such that for each $i \in S$, $\Phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{(i)}$.*

Proof. The bijection between (i) and (ii) follows from the definition of $\mathcal{Z}$-compatibility and the remarks that followed it, and that between (ii) and (iii) from Proposition 88. □

Corollary 90. *Let S be as in Proposition 88. The constructions above give bijections between*

(i) *the set of functions $\Phi \colon G_{\mathbb{A}} \to V$ that are left-invariant under G_k, invariant under $\mathcal{Z}_{\mathbb{A}}$, and right-invariant under $\prod K_v$, and*

(ii) *the set of families of functions $\Phi^{(i)} \colon \Omega_0(\mathfrak{n}) \to V$, indexed by $i \in S$, such that for each $i \in S$, $\Phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{(i)}$ and right-invariant under $\prod K_v$.*

Proof. Immediate, just as Corollary 85 is immediate from Proposition 84. □

Next, we need a version of Lemma 86 in which the functions $\Phi^{(i)}$ are left-invariant not just under $\Gamma^{(i)}$ but under the larger groups $\widetilde{\Gamma}^{(i)}$. For convenience, we define the related groups

$$\widetilde{\Gamma}^{[i]} = G_k \cap a_i \Omega_0(\mathfrak{n}) \mathcal{Z}_{\mathbb{A}} a_i^{-1}.$$

We denote the centre of G_∞ by $\mathcal{Z}_\infty$.

Lemma 91. *For $1 \leq i \leq h$, the bijection of Lemma 86 restricts to one between*

(i) *the set of functions $\Phi^{(i)}\colon \Omega_0(\mathfrak{n}) \to V$ that are left-invariant under $\widetilde{\Gamma}^{(i)}$ and right-invariant under $\prod K_v$, and*

(ii) *the set of functions $\phi^{(i)}\colon G_\infty \to V$ that are left-invariant under $\widetilde{\Gamma}^{[i]}$ and invariant under $\mathcal{Z}_\infty$.*

Proof. Let $\Phi^{(i)}$ be given and define $\phi^{(i)}$ by (5.16). Then $\phi^{(i)}$ is invariant under $\mathcal{Z}_\infty$, for if $\zeta \in \mathcal{Z}_\infty$, then $(\zeta, 1) \in \widetilde{\Gamma}^{(i)}$, so

$$\phi^{(i)}(\zeta\delta) = \Phi^{(i)}((a_i^{-1}\zeta\delta a_i)_\infty, 1) = \Phi^{(i)}((a_i^{-1}\delta a_i)_\infty, 1) = \phi^{(i)}(\delta).$$

Now let $\gamma \in \widetilde{\Gamma}^{[i]}$. Choose $z \in \mathcal{Z}_\mathbb{A}$ with $a_i^{-1}\gamma z a_i \in \Omega_0(\mathfrak{n})$. Then

$$\begin{aligned}
\phi^{(i)}(\gamma\delta) &= \Phi^{(i)}\left((a_i^{-1}\gamma\delta a_i)_\infty, 1\right) \\
&= \Phi^{(i)}\left((a_i^{-1}\gamma z a_i)_\infty (a_i^{-1}\delta a_i)_\infty, 1\right) && \text{since } (z_\infty, 1) \in \widetilde{\Gamma}^{(i)} \\
&= \Phi^{(i)}\left((a_i^{-1}\delta a_i)_\infty, (a_i^{-1}\gamma z a_i)_0^{-1}\right) && \text{since } a_i^{-1}\gamma z a_i \in \widetilde{\Gamma}^{(i)} \\
&= \Phi^{(i)}\left((a_i^{-1}\delta a_i)_\infty, 1\right) && \text{since } (a_i^{-1}\gamma z a_i)_0 \in \prod K_v \\
&= \phi^{(i)}(\delta).
\end{aligned}$$

Thus $\phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{[i]}$, as required.

Conversely, let $\phi^{(i)}$ be given and define $\Phi^{(i)}$ by (5.17). Right-invariance of $\Phi^{(i)}$ under $\prod K_v$ is obvious. Moreover, let $w = a_i^{-1}\gamma z a_i \in \widetilde{\Gamma}^{(i)}$, where $\gamma \in G_k$ and $z \in \mathcal{Z}_\mathbb{A}$. Then $\gamma \in \widetilde{\Gamma}^{[i]}$, so

$$\begin{aligned}
\Phi^{(i)}(wx) &= \phi^{(i)}\left((a_i a_i^{-1}\gamma z a_i x a_i^{-1})_\infty\right) \\
&= \phi^{(i)}\left(\gamma z_\infty (a_i x a_i^{-1})_\infty\right) \\
&= \phi^{(i)}\left(z_\infty (a_i x a_i^{-1})_\infty\right) && \text{by left-invariance under } \widetilde{\Gamma}^{[i]} \\
&= \phi^{(i)}\left((a_i x a_i^{-1})_\infty\right) && \text{by invariance under } \mathcal{Z}_\infty \\
&= \Phi^{(i)}(x).
\end{aligned}$$

Thus $\Phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{(i)}$, as required. □

We finally obtain the following analogue of Theorem 87.

Theorem 92. *Let S be as in Proposition 88. The constructions above give a bijection between*

(i) *the set of functions $\Phi\colon G_{\mathbb{A}} \to V$ that are left-invariant under G_k, invariant under $\mathcal{Z}_{\mathbb{A}}$, and right-invariant under $\prod K_v$, and*

(ii) *the set of families of functions $\phi^{(i)}\colon G_\infty \to V$, indexed by $i \in S$, such that for each $i \in S$, $\phi^{(i)}$ is left-invariant under $\widetilde{\Gamma}^{[i]}$ and invariant under $\mathcal{Z}_\infty$.*

Proof. Compose the bijections of Corollary 90 and Lemma 91. □

It is instructive to compare this result with Theorem 87. In the next chapter, we work with functions invariant under

$$\mathcal{Z}_\infty \Gamma^{[i]},$$

but Theorem 92 suggests imposing invariance under the (possibly) larger group

$$\mathcal{Z}_\infty \widetilde{\Gamma}^{[i]}.$$

Of course, the distinction would not exist if we had the equality

$$\mathcal{Z}_\infty \widetilde{\Gamma}^{[i]} = \mathcal{Z}_\infty \Gamma^{[i]}.$$

Chapter 6

Automorphic forms

In this chapter, we define the automorphic forms and cuspforms of interest to us; roughly speaking, these are the harmonic modular forms for the group $\Gamma_0(\mathfrak{n})$. The necessary background was developed in chapters 4 and 5.

For a description of modular forms over $\mathbb{Q}$ from the adelic viewpoint, the reader is referred to [Wei71, §§3–5], which would serve as a suitable introduction to this chapter.

In §6.1, we describe the theory for a general number field k. In passing from $\mathbb{Q}$ to k one encounters complications arising from the embeddings of k and from its unit group and ideal class group; this is the case, for example, in the classical treatment of Hilbert modular forms, when k is totally real. These difficulties largely disappear with the adoption of the adelic viewpoint. Our account is based on Weil's book [Wei71].

In §6.2, we specialise to the case of an imaginary quadratic field of arbitrary class number h. The case $h = 1$ was treated by Cremona [Cre81]; an automorphic form is then a function $f \colon \mathfrak{H}_3 \to \mathbb{C}^3$ invariant under $\Gamma_0(\mathfrak{n})$. In the general case, we obtain a family of functions $f^{(i)}$ invariant under various "twists" of $\Gamma_0(\mathfrak{n})$. This formulation is clearly more cumbersome than the adelic one, and would not seem persuasive without the adelic derivation; its merit lies in its concreteness. Thus, we can apply results of Kurcănov [Kur78] to express the space of cuspforms as a homology group which we can calculate.

6.1 The general case

As in §5.2.2, let k be an arbitrary algebraic number field, let G equal GL(2) as an algebraic group over k, let $\mathcal{Z}$ denote its centre, and write $G_{\mathbb{A}}$ and $\mathcal{Z}_{\mathbb{A}}$ for the corresponding adelised groups.

Automorphic forms will be introduced as functions on $G_{\mathbb{A}}$ satisfying a number of conditions. First we state their symmetry properties. Then we derive their Fourier expansions and state the cusp condition. Finally, we state the remaining conditions and define automorphic forms and cuspforms.

6.1.1 Symmetry properties

We choose an ideal $\mathfrak{n}$ (the *level*) and a corresponding idele n, and define the groups K_v (for finite places v) as in §5.2.4. We also define groups K_w for the infinite places w, as follows. Recall that

$$G_w = \begin{cases} \mathrm{GL}(2,\mathbb{R}) & \text{if } w \text{ is real,} \\ \mathrm{GL}(2,\mathbb{C}) & \text{if } w \text{ is complex.} \end{cases}$$

Accordingly, we choose a maximal compact subgroup K_w of each G_w as in §4.2; explicitly,

$$K_w = \begin{cases} \mathrm{O}(2) & \text{if } w \text{ is real,} \\ \mathrm{U}(2) & \text{if } w \text{ is complex.} \end{cases}$$

We put

$$\mathcal{K} = \prod_{\text{all } v} K_v, \qquad K_\infty = \prod_{w\mid\infty} K_w.$$

Let $\psi\colon k_{\mathbb{A}}^\times/k^\times \to \mathbb{C}^\times$ be a quasicharacter of the idele class group, of conductor dividing $\mathfrak{n}$. Write ψ_v, ψ_∞ for the quasicharacters induced by ψ on $k_v^\times$ and $k_\infty^\times$.

Let V be a finite-dimensional complex vector space, and let $\rho\colon K_\infty \to \mathrm{GL}(V)$ be an irreducible representation of K_∞ which agrees with ψ on the centre of K_∞. Since ρ is irreducible, it can be written as the tensor product $\rho = \otimes\rho_w$ of irreducible representations $\rho_w\colon K_w \to \mathrm{GL}(V_w)$, taken over the infinite places w [Wei71, §14, Remark 1]. The representation space V then equals $\otimes V_w$.

Let $\Phi\colon G_{\mathbb{A}} \to V$ be a function. We may consider the following conditions on Φ:

(A) $\Phi(\gamma g) = \Phi(g)$ for all $\gamma \in G_k$ and $g \in G_{\mathbb{A}}$;

(B) $\Phi(g\zeta) = \Phi(g)\psi(\zeta)$ for all $g \in G_{\mathbb{A}}$ and $\zeta \in \mathcal{Z}_{\mathbb{A}}$;

(C) $\Phi(g\kappa) = \Phi(g)$ for all $g \in G_{\mathbb{A}}$ and $\kappa \in \prod' K_v$ (the product being over all finite places not dividing $\mathfrak{n}$);

(D) for $v \mid \mathfrak{n}$ and for all $g \in G_{\mathbb{A}}$ and $\kappa = \begin{pmatrix} a & b \\ n_v c & d \end{pmatrix} \in K_v$,

$$\Phi(g\kappa) = \Phi(g)\psi_v(d);$$

(E) $\Phi(g\kappa) = \Phi(g)\rho(\kappa)$ for all $g \in G_{\mathbb{A}}$ and $\kappa \in K_\infty$.

Note that conditions (B) and (E) are compatible because of the assumption that ρ and ψ agree on the centre of K_∞.

Lemma 93. (i) *In* (D), *the map $\kappa \mapsto \psi_v(d)$ is a character of K_v. The kernel K_v' of this character is an open subgroup of K_v.*

(ii) *For finite v not dividing $\mathfrak{n}$, put $K_v' = K_v$. Put $K' = \prod K_v'$, the product being over all finite places v. Assume that Φ satisfies* (C) *and* (D). *Then Φ is constant on cosets gK' with respect to K'.*

Proof. This is [Wei71, §12, Remark 1]. The first part follows from our assumption on the conductor of ψ. Explicitly, ψ_v is trivial on $1 + \pi_v^{f(v)}\mathfrak{O}_v$ where $\pi_v^{f(v)}\mathfrak{O}_v$ is the conductor of ψ_v. Now let

$$\kappa = \begin{pmatrix} a & b \\ n_v c & d \end{pmatrix} \in K_v, \qquad \kappa' = \begin{pmatrix} a' & b' \\ n_v c' & d' \end{pmatrix} \in K_v.$$

Then $dd' \in \mathfrak{O}_v^\times$, so

$$\kappa\kappa' \mapsto \psi_v(n_v c b' + dd') = \psi_v(d)\psi_v(d')\psi_v\big(1 + n_v c b'(dd')^{-1}\big);$$

here the last factor is 1, since $\pi_v^{f(v)} \mid n_v$. So $\kappa \mapsto \psi_v(d)$ is algebraically a homomorphism; since it is clearly continuous, it is a homomorphism. Since K_v is compact, the map is a character.

To show that K'_v is open, we use the fact that K_v is totally disconnected, and argue as in §5.1.4, with $H = K_v$. This proves (i). Part (ii) is clear. □

Now write $\mathcal{B}$ for the subgroup of G consisting of all elements of the form $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)$, and $\mathcal{B}_{\mathbb{A}}$ for the corresponding adelised group; explicitly,

$$\mathcal{B}_{\mathbb{A}} = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \,\middle|\, x \in k_{\mathbb{A}},\ y \in k_{\mathbb{A}}^{\times} \right\}.$$

The motivation for considering $\mathcal{B}_{\mathbb{A}}$ is twofold. Firstly, according to Weil, if Φ is continuous and satisfies at least conditions (A) and (B), then it is uniquely determined by its restriction to $\mathcal{B}_{\mathbb{A}}$. Secondly, Weil [Wei71, §15] gives the decomposition

$$G_{\mathbb{A}} = G_k \mathcal{B}_{\mathbb{A}} \mathcal{K} \mathcal{Z}_{\mathbb{A}}; \tag{6.1}$$

it clearly follows that any (not necessarily continuous) function $\Phi\colon G_{\mathbb{A}} \to V$ satisfying conditions (A)–(E) is uniquely determined by its restriction to $\mathcal{B}_{\mathbb{A}}$. Thus, given $\Phi\colon G_{\mathbb{A}} \to V$, we define $F\colon k_{\mathbb{A}} \times k_{\mathbb{A}}^{\times} \to V$ by

$$F(x, y) = \Phi\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right). \tag{6.2}$$

Lemma 94. *Let Φ satisfy conditions* (A), (C), *and* (D), *and define F by* (6.2). *Then F has the following properties:*

(a) $F(x + \eta, y) = F(x, y)$ *for all* $\eta \in k$*;*

(b) $F(\eta x, \eta y) = F(x, y)$ *for all* $\eta \in k^{\times}$*;*

(c) $F(x + yz, y) = F(x, y)$ *for each finite place* v *and all* $z \in \mathfrak{O}_v$*;*

(d) $F(x, uy) = F(x, y)$ *for all* $u \in \prod_{v \nmid \infty} \mathfrak{O}_v^{\times}$.

Proof. Part (a) follows from (A) with $\gamma = \left(\begin{smallmatrix} 1 & \eta \\ 0 & 1 \end{smallmatrix}\right)$, part (b) from (A) with $\gamma = \left(\begin{smallmatrix} \eta & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For (c) use (C) and (D) with $\kappa = \left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$, and for (d) use (C) and (D) with $\kappa = \left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Note that (a) and (b) are given by Weil [Wei71, §13], that (c) is the corrected version of Weil's (a′), misprinted *loc. cit.*, and that (d) is stronger than Weil's (b′). □

Remark. Actually, our condition (C) above is stronger than the condition given by Weil [Wei71, §12]:

(C′) For v a finite place not dividing $\mathfrak{n}$ and for all $g \in G_{\mathbb{A}}$ and $\kappa \in K_v$, $\Phi(g\kappa) = \Phi(g)$.

There are two reasons why we give (C) in place of (C′). Firstly, it is not clear that Lemma 93 (ii) holds with (C′) in place of (C), since (C′) only allows one to adjust finitely many places at a time. Secondly, we will need the strong version of Lemma 94 (d) in the proof of Proposition 95, for the same reason.

6.1.2 Fourier series and the cusp condition

At this point, the theory of harmonic analysis on topological groups is brought to bear, in order to express F as a Fourier series. We follow the approach of [Wei71, §13]; where necessary, it will be assumed implicitly that F is well enough behaved (square-integrable, say) for Fourier theory to apply.

Once and for all, choose a non-trivial additive character ψ of $k_{\mathbb{A}}$, trivial on k. Every character ψ' with the same property can be written as $\psi'(x) = \psi(\xi x)$ with $\xi \in k^\times$. For each place v, write ψ_v for the character of k_v induced by ψ on k_v. For v finite, we say that ψ_v is of *order* δ, or that ψ is of *order* δ at v, if ψ_v is trivial on $\pi_v^{-\delta}\mathfrak{O}_v$ but not on $\pi_v^{-\delta-1}\mathfrak{O}_v$; one can show that δ equals 0 for almost all v. For each finite v, let $\delta(v)$ be the order of ψ at v. Let $d = (d_v)$ be the idele given by $d_v = \pi_v^{\delta(v)}$ for finite v and $d_w = 1$ for infinite w. The idele d is called a *differental idele* belonging to ψ; it depends upon the choice of the prime elements π_v, but the ideal $il(d)$ does not. We may assume ψ chosen so that

$$\psi_w(x) = e^{-2\pi i x} \qquad \text{when } k_w = \mathbb{R},$$

$$\psi_w(x) = e^{-2\pi i(x+\bar{x})} \qquad \text{when } k_w = \mathbb{C};$$

this determines ψ uniquely, and $il(d)$ is then the *different* of the number field k in the usual sense. Note that ψ is compatible with (4.35).

Proposition 95. *Let* $\Phi\colon G_{\mathbb{A}} \to V$ *satisfy conditions* (A)–(D). *Define* F *by* (6.2). *Then* F *has a Fourier expansion*

$$F(x, y) = c_0(y) + \sum_{\xi \in k^\times} c(\xi d y)\psi(\xi x), \tag{6.3}$$

with $c_0(\eta y) = c_0(y)$ for all $\eta \in k^\times$, with $c_0(uy) = c_0(y)$ for all $u \in \prod \mathfrak{O}_v^\times$, with $c(y)$ depending only on y_∞ and $il(y)$, and with $c(y) = 0$ unless the ideal $il(y)$ is integral.

Proof. In fact, it is sufficient to assume that F satisfies the conclusions of Lemma 94. Because of (a), F has a Fourier expansion

$$F(x,y) = c_0(y) + \sum_{\xi \in k^\times} c(\xi, y)\psi(\xi x).$$

By (b) we have, for $\eta \in k^\times$,

$$\begin{aligned} F(x,y) &= c_0(\eta y) + \sum c(\xi, \eta y)\psi(\xi\eta x) \\ &= c_0(\eta y) + \sum c(\xi\eta^{-1}, \eta y)\psi(\xi x); \end{aligned}$$

Therefore $c_0(y) = c_0(\eta y)$ and $c(\xi, y) = c(\xi\eta^{-1}, \eta y)$; in particular, for $\eta = \xi$ we get $c(\xi, y) = c(1, \xi y)$. Now put

$$c(y) = c(1, d^{-1}y),$$

where d is a differental idele belonging to ψ. Then the Fourier series for F has the form (6.3). By (c), we must have, for all $z \in \mathfrak{O}_v$,

$$c(\xi dy) = c(\xi dy)\psi_v(\xi yz).$$

By the definition of d this means that $c(\xi dy) = 0$ unless $\mathrm{ord}_v(\xi dy) \geq 0$. Putting $\xi = 1$ and replacing y by $d^{-1}y$, we see that $c(y) = 0$ unless $\mathfrak{m} = il(y)$ is an integral ideal; taking (d) into account, we see that $c(y)$ depends only upon $\mathfrak{m}$ and y_∞ and may thus be written as $c(y_\infty, \mathfrak{m})$ with $c(y_\infty, \mathfrak{m}) = 0$ unless $\mathfrak{m}$ is an integral ideal. Finally, (d) also implies that $c_0(uy) = c_0(y)$ for all $u \in \prod \mathfrak{O}_v^\times$. This completes the proof. □

The coefficients c_0, c in (6.3) are given by the usual Fourier formulae:

$$c_0(y) = \int_{k_\mathbb{A}/k} F(x,y)\,dx, \tag{6.4}$$

$$c(y) = c(y_\infty, il(y)) = \int_{k_\mathbb{A}/k} F(x, d^{-1}y)\psi(-x)\,dx. \tag{6.5}$$

Definition. Let Φ be as in Proposition 95. We say that Φ is *cuspidal* if and only if $c_0(y) = 0$ for all $y \in k_\mathbb{A}^\times$.

Cuspidality can be defined for a more general class of functions Φ; below, we sketch the approach of Garrett [Gar90, §2.5]. For $x \in k_{\mathbb{A}}$, put

$$u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G_{\mathbb{A}}.$$

Let Φ satisfy (A). For $\xi \in k$ and $g \in G_{\mathbb{A}}$, put

$$W_\xi(g) = \int_{k_{\mathbb{A}}/k} \bar{\psi}(\xi x)\Phi\big(u(x)g\big)\,dx.$$

Proposition 96. *There is a Fourier expansion*

$$\Phi(g) = \sum_{\xi \in k} W_\xi(g), \tag{6.6}$$

and for $p = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G_k$, the Fourier coefficients satisfy

$$W_\xi(g) = W_{a^{-1}d\xi}(pg). \tag{6.7}$$

Proof. Put $\phi(x) = \Phi\big(u(x)g\big)$. Then ϕ is k-invariant, so by Fourier theory there is an L^2-equality

$$\phi(x) = \sum_{\xi \in k} \psi(\xi x) \int_{k_{\mathbb{A}}/k} \bar{\psi}(\xi x')\phi(x')\,dx'.$$

Putting $x = 0$ yields (6.6). Since $pu(x) = u(ad^{-1}x)p$ and Φ is left-invariant under p, we have

$$\sum_{\xi \in k} \psi(\xi x) W_\xi(g) = \Phi\big(u(x)g\big) = \Phi\big(u(ad^{-1}x)pg\big) = \sum_{\xi \in k} \psi(ad^{-1}\xi x) W_\xi(pg),$$

from which (6.7) follows by uniqueness of Fourier expansions.[1] □

In [Gar90], Φ is said to be cuspidal if and only if $W_0(g) = 0$ for (almost) all $g \in G_{\mathbb{A}}$.

Corollary 97. *Let Φ be as in Proposition 95. Then Φ is cuspidal (in our sense) if and only if $W_0(g) = 0$ for all $g \in G'_k \mathcal{B}_{\mathbb{A}} \mathcal{K} \mathcal{Z}_{\mathbb{A}}$, where*

$$G'_k = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G_k \right\}.$$

[1] Our (6.7) differs slightly from the formula in [Gar90], which appears to be misprinted.

Proof. The function W_0 inherits properties (B)–(D) from Φ and is left-invariant under G'_k by (6.7). Thus W_0 vanishes on $G'_k\mathcal{B}_{\mathbb{A}}\mathcal{K}\mathcal{Z}_{\mathbb{A}}$ if and only if it vanishes on $\mathcal{B}_{\mathbb{A}}$, which is if and only if

$$\int_{k_{\mathbb{A}}/k} \Phi\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}y & z\\ 0 & 1\end{pmatrix}\right) dx = 0 \qquad \text{for all } (z,y) \in k_{\mathbb{A}} \times k_{\mathbb{A}}^{\times}.$$

By (6.2), the integrand may be written $F(z+x,y)$. By a change of variables in the integral, and (6.4), we deduce that W_0 vanishes if and only if c_0 vanishes, as required. □

Thus, if Φ is cuspidal in the sense of Garrett, then it is cuspidal in our sense. In the other direction, it suffices to assume that F is left-invariant under $S = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, in view of (6.1) and the well-known Bruhat decomposition $G_k = G'_k \cup G'_k S G'_k$; see [Wei71, §15].

6.1.3 Automorphic forms and cuspforms

Let $\Phi\colon G_{\mathbb{A}} \to V$ be a function satisfying conditions (A)–(E), as in §6.1.1.

Definition. The function Φ is *B-moderate* if there exist constants $C > 0$ and $\lambda \geq 0$ such that, for all $x \in k_{\mathbb{A}}$ and $y \in k_{\mathbb{A}}^{\times}$,

$$\left\|\Phi\left(\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix}\right)\right\| \leq C \sup(|y|^{\lambda}, |y|^{-\lambda}),$$

where $\| \, \|$ denotes any (fixed) norm on V.

If Φ is B-moderate in this sense, then for each infinite place w, the induced function $\Phi_w\colon G_w \to V$ is B-moderate in the sense of §4.2.6; see [Wei71, §55].

From now on, assume that for each infinite place w, the differentials β_w and ω_w, and the representation $\rho_w\colon K_w \to \mathrm{GL}(V_w)$ are chosen as in §4.2, so that ρ_w relates differential 1-forms $\Phi_w \cdot \omega_w$ on G_w and $f_w \cdot \beta_w$ on $\mathfrak{H}_w = G_w/Z_w K_w$, in the manner of Lemma 57. Let $\mathfrak{H}_\infty = \prod \mathfrak{H}_w$ carry the natural Riemannian structure; if k has r real places and s complex places, then $\mathfrak{H}_\infty$ has dimension $2r + 3s$. We may regard $\otimes\beta_w$ and $\otimes\omega_w$ as V-valued differential $(r+s)$-forms on $\mathfrak{H}_\infty$ and G_∞, respectively.

Definition. The function Φ is *admissible of type $\mathcal{H}_\infty$* if it is B-moderate on each G_w and the differential $(r+s)$-form $\Phi_\infty \cdot (\otimes\omega_v)$ on G_∞ is the pullback to G_∞ of a harmonic form

Ω on $\mathfrak{H}_\infty$; note that $*\Omega$ is then a form of degree $[k:\mathbb{Q}]$, since $\dim \mathfrak{H}_\infty - (r+s) = r+2s = [k:\mathbb{Q}]$.

Note that this definition becomes greatly simplified when k has only one infinite place, since there is then no need for tensor products (there being only one factor in each).

Definition (Imaginary quadratic case). The function Φ is *admissible of type* $\mathcal{H}_\infty$ if the induced function $\Phi_\infty\colon G_\infty \to \mathbb{C}^3$ is admissible of type $\mathcal{H}_\mathbb{C}$ in the sense of §4.2.6.

We are (at last!) ready to state the adelic definition of automorphic forms and cuspforms.

Definition. An *automorphic form of weight* ρ*, character* ψ *and type* $\mathcal{H}_\infty$ *for* $\Gamma_0(\mathfrak{n})$, or, more briefly, an *automorphic form of type* $(\mathfrak{n}, \rho, \psi, \mathcal{H}_\infty)$ is a function $\Phi\colon G_\mathbb{A} \to V$ that satisfies conditions (A)–(E) and is B-moderate and admissible of type $\mathcal{H}_\infty$. A *cuspform* is a cuspidal automorphic form.

Remark. The analytic condition on Φ, that it be admissible of type $\mathcal{H}_\infty$, is the natural analogue of the requirement that a classical modular form be holomorphic. In order to state the condition, we had to make a special choice of ρ. The general theory of automorphic forms allows a general ρ, and replaces the type $\mathcal{H}_\infty$ by something more complicated. We briefly sketch how this is done; for details, see [Wei71, §52]. The generalisation encompasses Maass wave-forms, for example.

For functions f on $\mathfrak{H}_2$ and ϕ on $\mathrm{GL}(2,\mathbb{R})$, related in the usual way, holomorphy of f amounts to real-analyticity and the Cauchy-Riemann equations; in terms of ϕ, these may be written as $W\phi = 0$, where W is the left-invariant differential operator on $\mathrm{GL}(2,\mathbb{R})$ defined by the element $\left(\begin{smallmatrix} 1 & -i \\ -i & -1 \end{smallmatrix}\right)$ of its complexified Lie algebra. One can show that this is equivalent to $D\phi = 0$, where the element D of the Lie algebra is a "Casimir operator".

The generalisation is then as follows. For each real place, one specifies a (possibly non-zero) eigenvalue δ, and requires

$$D\phi = \delta\phi.$$

Similarly, for a complex place, one specifies the eigenvalues δ' and δ'' of two "Casimir operators" D' and D'', and requires

$$D'\phi = \delta'\phi, \qquad D''\phi = \delta''\phi;$$

the case $\delta' = \delta'' = 0$ is then more or less equivalent to the condition that $\phi\cdot\omega$ be harmonic. Given ρ, only certain choices of eigenvalues δ, δ' and δ'' are possible.

6.2 The imaginary quadratic case

In this section, we specialise to the case in which the number field k is imaginary quadratic. Let $\Phi\colon G_{\mathbb{A}} \to \mathbb{C}^3$ be a function satisfying conditions (A)–(E). The analysis of Φ in §6.1 was based on the decomposition $G_{\mathbb{A}} = G_k \mathcal{B}_{\mathbb{A}} \mathcal{K} \mathcal{Z}_{\mathbb{A}}$. We now analyse Φ in the manner suggested by §5.2.7, based on the decomposition $G_{\mathbb{A}} = \cup G_k \cdot a_i \cdot (G_\infty \times \prod K_v)$.

6.2.1 Symmetry properties

First, suppose that the quasicharacter ψ is trivial. By Theorem 87, the function Φ corresponds to an h-tuple of functions $\phi^{(i)}\colon G_\infty \to \mathbb{C}^3$, with $\phi^{(i)}$ left-invariant under the group $\Gamma^{[i]}$.

Since k is imaginary quadratic, $G_\infty = \mathrm{GL}(2,\mathbb{C}) = ZBK$ in the notation of §4.2.4. By (B), $\phi^{(i)}$ is invariant under Z. Extend ρ by triviality on Z to a representation of ZK; then (B) and (E) imply

$$\phi^{(i)}(g\kappa\zeta) = \phi^{(i)}(g)\rho(\kappa\zeta) \qquad (g \in G,\ \kappa \in K,\ \zeta \in Z),$$

so that $\phi^{(i)} \in \mathcal{S}_2$ in the notation of §4.3.2. Hence $\phi^{(i)}$ corresponds to a function $f^{(i)}\colon \mathfrak{H}_3 \to \mathbb{C}^3$ as in Lemma 64; explicitly,

$$f^{(i)}(z,t) = \phi^{(i)}\left(\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}\right).$$

Now consider the case of general ψ. We must modify Theorem 87. Recall from Lemma 71 that ψ, whose conductor divides $\mathfrak{n}$, induces a character χ of $(\mathfrak{O}/\mathfrak{n})^\times$ given by

$$\chi(d) = \prod_{v|\mathfrak{n}} \psi_v(d).$$

Similarly, by Lemma 93 (i), the map

$$\prod_{v\nmid\infty} K_v \to \mathbb{C}^\times, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \prod_{v|\mathfrak{n}} \psi_v(d)$$

is a character of $\prod K_v$; we denote this character by $\hat{\psi}$. Thus (C) and (D) may be written

$$\Phi(g\kappa) = \Phi(g)\hat{\psi}(\kappa) \qquad \text{for all } g \in G_{\mathbb{A}} \text{ and } \kappa \in \prod K_v,$$

and this condition replaces right-invariance under $\prod K_v$ in Corollary 85. Equation (5.16) is unchanged, but (5.17) must be replaced by

$$\Phi^{(i)}(x) = \phi^{(i)}\left((a_i x a_i^{-1})_\infty\right)\hat{\psi}(x_0). \tag{6.8}$$

Finally, it is necessary to assume that the a_i are chosen in a special way, viz

$$a_i = \begin{pmatrix} r_i & 0 \\ 0 & 1 \end{pmatrix},$$

where $r_i \in k_{\mathbb{A}}^\times$ are ideles whose ideals $il(r_i)$ represent the distinct ideal classes. This choice ensures that conjugation with a_i does not affect the diagonal:

$$a_i^{-1}\begin{pmatrix} a & * \\ * & d \end{pmatrix} a_i = \begin{pmatrix} a & * \\ * & d \end{pmatrix}. \tag{6.9}$$

Theorem 98. *There is a bijection, given by* (5.13), (5.14), (5.16) *and* (6.8), *between, on the one hand, the set of functions* Φ *satisfying* (A), (C) *and* (D), *and, on the other hand, the set of h-tuples of functions* $\phi^{(i)}$ *on* G_∞ *such that for* $1 \le i \le h$, *for all* $\gamma = \left(\begin{smallmatrix} * & * \\ * & d \end{smallmatrix}\right) \in \Gamma^{[i]}$ *and* $\delta \in G_\infty$,

$$\phi^{(i)}(\gamma\delta) = \phi^{(i)}(\delta) \cdot \chi^{-1}(d). \tag{6.10}$$

Proof. This is Lemma 86, *mutatis mutandis.* The point of interest is that

$$\hat{\psi}\left((a_i^{-1}\gamma^{-1}a_i)_0\right) = \chi^{-1}(d),$$

using (6.9). □

With ρ extended to ZK by means of ψ_∞, the passage between $\phi^{(i)}$ and $f^{(i)}$ is just as before.

Remark. In the case of trivial ψ, we used only (A), (C) and (D) when we applied Theorem 87. Using (B) as well, we could apply Theorem 92 instead, to show that Φ corresponds to a collection of functions $\phi^{(i)}\colon G_\infty \to \mathbb{C}^3$, with $\phi^{(i)}$ left-invariant under the group $\widetilde{\Gamma}^{[i]}$; moreover, we could assume that the index i ranges only over a set S as in Proposition 88. Again, for general ψ, we could generalise $\mathcal{Z}$-compatibility, and replace Theorem 98 with an analogue of Theorem 92. However, we shall not pursue this line here.

6.2.2 Fourier series and the cusp condition

We now develop $f^{(i)}$ as a Fourier series, using ideas from [Cre81, §3.2] and [Gar90]. We assume that $\phi^{(i)}$ is left-invariant under $\Gamma^{[i]}$. For fixed t, we may regard $f^{(i)}$ as a function of z alone, and expand it in terms of the characters of $\mathbb{C}^+$, the additive group of $\mathbb{C}$. These characters all have the form $z \mapsto \psi(wz)$, for some $w \in \mathbb{C}$, where ψ is any non-trivial character (c.f. Tate's thesis, [Tat67, §2.2]). Of course, we choose ψ as in (4.35), that is

$$\psi(z) = \exp(-2\pi i \operatorname{Tr}(z)) \qquad (z \in \mathbb{C}).$$

Define

$$W^{(i)} = \left\{ w \in \mathfrak{O} \;\middle|\; \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \in \Gamma^{[i]} \right\}.$$

This set is clearly a $\mathbb{Z}$-module, but need not be an ideal of $\mathfrak{O}$, not even in the Euclidean case (*pace* [Cre81, p.34]). In some sense, $W^{(i)}$ may be thought of as the "width" of the cusp at infinity. For $w \in W^{(i)}$,

$$f^{(i)}(z+w,t) = \phi^{(i)}\left(\begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix}\right) = f^{(i)}(z,t). \tag{6.11}$$

From here on, we fix the index i and write $f = f^{(i)}$ and $W = W^{(i)}$. From (6.11), it follows that f has a Fourier expansion in terms of the characters of $\mathbb{C}^+$ that are trivial on W. The character $z \mapsto \psi(wz)$ is trivial on W if and only if $w \in W^*$, where W^* is the dual $\mathbb{Z}$-module of W, viz

$$W^* = \{\, w \in k \mid \operatorname{Tr}(wW) \subseteq \mathbb{Z} \,\}.$$

Thus the expansion of f takes the form

$$f(z,t) = c_0(t) + \sum_{\xi \in W^*} c_\xi(t)\psi(\xi z). \tag{6.12}$$

The coefficients c_ξ are given by the usual Fourier formulae:

$$c_0(t) = \int_{\mathbb{C}/W} f(z,t)dz, \qquad c_\xi(t) = \int_{\mathbb{C}/W} f(z,t)\psi(-\xi z)dz.$$

Equation (6.12) may be thought of as the expansion of f at the cusp at infinity. As usual, we must consider Fourier expansions at all the "k-rational" cusps $\mathbb{P}^1(k) = k \cup \{\infty\}$. If $\sigma \in \mathrm{GL}(2,k)$ sends ∞ to the cusp s, and f is invariant under a subgroup Γ of $\mathrm{GL}(2,k)$, then $f\big|\sigma$ is invariant under $\sigma^{-1}\Gamma\sigma$, since for $\gamma \in \Gamma$,

$$(f\big|\sigma)\big|(\sigma^{-1}\gamma\sigma) = f\big|(\gamma\sigma) = (f\big|\gamma)\big|\sigma = f\big|\sigma.$$

Let

$$W_s = \left\{ w \in \mathfrak{O} \;\middle|\; \begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix} \in \sigma^{-1}\Gamma\sigma \right\}.$$

(Since the $\left(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right)$ for $w \in W_s$ fix ∞, they even lie in $\sigma^{-1}\Gamma_s\sigma$ for $\Gamma_s = \{\, \gamma \in \Gamma \mid \gamma s = s \,\}$, but we shall not need to use this fact.) As before, $f\big|\sigma$ has a Fourier expansion of the form

$$(f\big|\sigma)(z,t) = c_0(t) + \sum_{\xi \in W_s^*} c_\xi(t)\psi(\xi z). \tag{6.13}$$

Definition. We say that f *vanishes at the cusp* s if $c_0(t)$ vanishes in (6.13); note that, in general, this does not mean that $f(s,t) \to 0$ as $t \to 0$, but rather that $(f\big|\sigma)(z,t) \to 0$ as $t \to \infty$.

The property of vanishing at s is well-defined, i.e. independent of the choice of σ, as we now show. Any other choice has the form $\sigma' = \sigma\tau$, where $\tau \in \mathrm{GL}(2,k)$ fixes ∞ and may thus be written $\tau = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Therefore,

$$\begin{aligned}
(f\big|\sigma')(z,t) &= (f\big|\sigma)\big((az+b)/d, at/d\big) && \text{by (4.57)} \\
&= c_0(at/d) + \sum_{\xi \in W_s^*} c_\xi(at/d)\psi\big(\xi(az+b)/d\big) && \text{by (6.13).}
\end{aligned}$$

Since $c_0(at/d) = 0$ for all t if and only if $c_0(t) = 0$ for all t, we see that vanishing at the cusp s is indeed well-defined.

Lemma 99. *Let $f\colon \mathfrak{H}_3 \to \mathbb{C}^3$ be invariant under the group Γ. If f vanishes at the cusp s, then it also vanishes at each cusp γs for $\gamma \in \Gamma$.*

Proof. If $\sigma \in \mathrm{GL}(2,k)$ maps ∞ to s, then $\gamma\sigma$ maps ∞ to γs. We must compare the c_0 terms in the Fourier expansions of $f\big|\sigma$ and $f\big|(\gamma\sigma)$ — but these are the same, since $f\big|(\gamma\sigma) = (f\big|\gamma)\big|\sigma = f\big|\sigma$. □

Definition. We say that f is *cuspidal* if it vanishes at all the cusps.

Remark. In view of Lemma 99, we see that this is really a set of conditions, one for each cusp of Γ; recall that "cusp of Γ" means "Γ-equivalence class of cusps". This closely resembles the situation in the classical theory of cuspforms over $\mathbb{Q}$, as in [Kob84, §III.3].

The expansion (6.12) takes a special form if $f \cdot \beta$ is harmonic, as our next proposition shows. The same is true of (6.13) if $(f\big|\sigma) \cdot \beta$ is harmonic; in fact, Cremona [Cre81] implicitly assumes that harmonicity of $f \cdot \beta$ ensures harmonicity of $L^*_\sigma(f \cdot \beta) = (f\big|\sigma) \cdot \beta$, but we will not need this here.

Proposition 100. *Let $f\colon \mathfrak{H}_3 \to \mathbb{C}^3$ be given by the Fourier series*

$$f(z,t) = c_0(t) + \sum_{\xi \in \mathbb{C}^\times} c_\xi(t)\psi(\xi z).$$

Suppose that $f \cdot \beta$ is harmonic and f is B-moderate. Then

$$c_0(t) = (c_{0,0}t, c_{0,1}t^2, c_{0,2}t) \tag{6.14}$$

for constants $c_{0,0}$, $c_{0,1}$ and $c_{0,2}$, and

$$c_\xi(t) = c(\xi)H\big(t|\xi|\big) \cdot \mathrm{diag}(\xi/|\xi|, 1, \bar{\xi}/|\xi|) \tag{6.15}$$

for each $\xi \in \mathbb{C}^\times$, where $c(\xi)$ is a constant depending on ξ and where $H(t)$ is given by (4.39).

Proof. We give two proofs. The first is a calculation generalising the proof of Lemma 63; the second uses a trick to enable Lemma 63 to be applied directly. Write $f = (f_0, f_1, f_2)$ and $c_\xi(t) = \big(c^0(\xi,t), c^1(\xi,t), c^2(\xi,t)\big)$. Note that

$$\frac{\partial}{\partial z}\psi(\xi z) = -2\pi i\xi\psi(\xi z), \qquad \frac{\partial}{\partial \bar{z}}\psi(\xi z) = -2\pi i\bar{\xi}\psi(\xi z).$$

By (4.33a),

$$0 = \sum_{\xi \in \mathbb{C}^\times} \Big(-2\pi i \bar{\xi} c^0(\xi, t) - 2\pi i \xi c^2(\xi, t) \Big) \psi(\xi z)$$

whence

$$\bar{\xi} c^0(\xi, t) = -\xi c^2(\xi, t) \tag{6.16}$$

for all $\xi \in \mathbb{C}^\times$. By (4.33b),

$$0 = \frac{d}{dt} c^0(0, t) - t^{-1} c^0(0, t) + \sum_{\xi \in \mathbb{C}^\times} \left(-2\pi i \xi c^1(\xi, t) + \frac{d}{dt} c^0(\xi, t) - t^{-1} c^0(\xi, t) \right) \psi(\xi z),$$

whence

$$\frac{d}{dt} c^0(0, t) = t^{-1} c^0(0, t), \tag{6.17}$$

and

$$-2\pi i \xi c^1(\xi, t) + \frac{d}{dt} c^0(\xi, t) - t^{-1} c^0(\xi, t) = 0 \tag{6.18}$$

for all $\xi \in \mathbb{C}^\times$. Similarly, (4.33c) gives

$$\frac{d}{dt} c^2(0, t) = t^{-1} c^2(0, t), \tag{6.19}$$

and

$$-2\pi i \bar{\xi} c^1(\xi, t) - \frac{d}{dt} c^2(\xi, t) + t^{-1} c^2(\xi, t) = 0 \tag{6.20}$$

for all $\xi \in \mathbb{C}^\times$. Note that given (6.16), equations (6.18) and (6.20) are equivalent and may be simplified to

$$\frac{d}{dt} \big(t^{-1} c^0(\xi, t) \big) = 2\pi i \xi t^{-1} c^1(\xi, t). \tag{6.21}$$

Lastly, by (4.33d),

$$0 = \frac{t}{2} \frac{d}{dt} c^1(0, t) - c^1(0, t) + \sum_{\xi \in \mathbb{C}^\times} \left(\frac{t}{2} \frac{d}{dt} c^1(\xi, t) - c^1(\xi, t) + 4\pi i \bar{\xi} t c^0(\xi, t) \right) \psi(\xi z),$$

whence

$$\frac{t}{2}\frac{d}{dt}c^1(0,t) = c^1(0,t), \tag{6.22}$$

and

$$\frac{t}{2}\frac{d}{dt}c^1(\xi,t) - c^1(\xi,t) + 4\pi i\bar{\xi}tc^0(\xi,t) = 0 \tag{6.23}$$

for all $\xi \in \mathbb{C}^\times$; this simplifies to

$$\frac{d}{dt}\big(t^{-2}c^1(\xi,t)\big) = -8\pi i\bar{\xi}t^{-2}c^0(\xi,t). \tag{6.24}$$

Solving (6.17), (6.22) and (6.19) clearly gives (6.14), whilst (6.21) and (6.24) give

$$t\frac{d^2}{dt^2}\big(t^{-2}c^1\big) + \frac{d}{dt}\big(t^{-2}c^1\big) - 16\pi^2|\xi|^2t^{-1}c^1 = 0.$$

This is the same equation as in the proof of Lemma 63, but with $\pi|\xi|$ substituted for π. Hence, up to a constant multiple, the only solution which does not increase exponentially for $t \to +\infty$ is

$$c^1(\xi,t) = t^2K_0\big(4\pi|\xi|t\big).$$

Hence

$$c^0(\xi,t) = -\frac{i}{2}\frac{\xi}{|\xi|}t^2K_1\big(4\pi|\xi|t\big), \qquad c^2(\xi,t) = \frac{i}{2}\frac{\bar{\xi}}{|\xi|}t^2K_1\big(4\pi|\xi|t\big).$$

Thus, up to a constant multiple, $c_\xi(t)$ is given by (6.15).

We now give the second proof, which is based on the argument in [Cre81]. Define $c_\xi(z,t) = c_\xi(t)\psi(\xi z)$. If $f\cdot\beta$ is harmonic, then so is $c_0(t)\cdot\beta$ and each $c_\xi(z,t)\cdot\beta$. This fact is stated without proof in [Cre81], but may be obtained as a by-product of the calculation above. Thus, (6.17), (6.19) and (6.22) show that $c_0(t)$ satisfies (4.33), i.e. that $c_0(t)\cdot\beta$ is harmonic. Similarly, equations (6.16), (6.18), (6.20) and (6.23) respectively show that $c_\xi(z,t)$ satisfies (4.33a)–(4.33d), i.e. that $c_\xi(z,t)\cdot\beta$ is harmonic.

We cannot apply Lemma 63 to $c_\xi(z,t)$, because the z-dependence is via $\psi(\xi z)$, not $\psi(z)$. The idea now is to put $c'_\xi(z,t) = c_\xi(z\xi^{-1}, t\xi^{-1})$; for this to make sense for non-real

ξ, we extend f, and hence each c_ξ, by means of formula (4.43), to a function on $\mathbb{C} \times \mathbb{C}^\times$, not just on $\mathfrak{H}_3$. Hence we define

$$c'_\xi(t) = c_\xi(t|\xi|^{-1}) \cdot \operatorname{diag}(\bar{\xi}/|\xi|, 1, \xi/|\xi|)$$

and put

$$c'_\xi(z,t) = c'_\xi(t)\psi(z);$$

equivalently, we could define

$$c'_\xi(z,t) = c_\xi(z\xi^{-1}, t|\xi|^{-1}) \cdot \operatorname{diag}(\bar{\xi}/|\xi|, 1, \xi/|\xi|)$$

and put

$$c'_\xi(t) = c'_\xi(0,t).$$

We now claim that the harmonicity of $c_\xi(z,t) \cdot \beta$ implies that of $c'_\xi(z,t) \cdot \beta$, a fact which is implicitly assumed in [Cre81]. There are two ways of seeing this. One is to evaluate (4.33a)–(4.33d) for $c_\xi(z,t)$ at $(z\xi^{-1}, t|\xi|^{-1})$, to verify the corresponding equations for $c'_\xi(z,t)$. The other is to verify that $c'_\xi(t) = \big(g_0(t), g_1(t), g_2(t)\big)$ satisfies (4.40)–(4.42), using the formula

$$g_i(t) = \int_{\mathbb{C}/W} f_i(w, t\xi^{-1})\psi(-\xi w)\,dw$$

together with (4.33a)–(4.33d), integration by parts, and (6.11).

Since $c'_\xi(z,t) = c'_\xi(0,t)\psi(z)$, we may apply Lemma 63 to $c'_\xi(z,t)$, giving $c'_\xi(t) = c(\xi)H(t)$. Consequently,

$$c_\xi(t) = c'_\xi(t|\xi|) \cdot \operatorname{diag}(\xi/|\xi|, 1, \bar{\xi}/|\xi|),$$

giving (6.15). This completes the proof. □

6.2.3 Automorphic forms and cuspforms

We can now give a concrete definition of automorphic forms and cuspforms over an imaginary quadratic field. For convenience, we summarise the relevant notation.

Let k be an imaginary quadratic field of class number h and ring of integers $\mathfrak{O}$. Let $\mathfrak{n}$ be an integral ideal (the *level*), and let $\psi\colon J^{\mathfrak{n}}/P^{\mathfrak{n}} \to \mathbb{C}^\times$ be a character, inducing a character $\chi\colon (\mathfrak{O}/\mathfrak{n})^\times \to \mathbb{C}^\times$ in the manner of Lemma 71. Choose ideles $r_i \in k_{\mathbb{A}}^\times$, with $(r_i)_\infty = 1$, such that the fractional ideals $il(r_i)$ represent the h ideal classes of k; by convention, we usually take $r_1 = 1$ to represent the principal class. Put $R = (r_1, \dots, r_h)$. Let $a_i = \left(\begin{smallmatrix} r_i & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and

$$\Gamma^{[i]} = \left\{ \gamma \in \mathrm{GL}(2,k) \;\middle|\; a_i^{-1}\gamma a_i \in \Omega_0(\mathfrak{n}) \right\}.$$

Definition. An *automorphic form* of weight 2 for $\big(\Gamma_0(\mathfrak{n}), R\big)$, with character ψ, is an h-tuple $F = (f^{(1)}, \dots, f^{(h)})$ of functions $f^{(i)}\colon \mathfrak{H}_3 \to \mathbb{C}^3$, such that each $f^{(i)}$ is admissible of type $\mathcal{H}_{\mathbb{C}}$, and such that for $1 \le i \le h$,

$$f^{(i)}\big|\gamma = \chi^{-1}(d) \cdot f^{(i)} \quad \text{for all} \quad \gamma = \left(\begin{smallmatrix} * & * \\ * & d \end{smallmatrix}\right) \in \Gamma^{[i]}. \tag{6.25}$$

Moreover, F is a *cuspform* if each $f^{(i)}$ is cuspidal.

The qualification "of weight 2", to be omitted henceforth, refers to the representation ρ of SU(2) which is implicit in the definition of the action $f^{(i)}\big|\gamma$. Also, the h-tuple of ideal class representatives R is usually regarded as fixed,[2] and we often speak simply of forms for $\Gamma_0(\mathfrak{n})$, rather than for $\big(\Gamma_0(\mathfrak{n}), R\big)$.

Notation. The complex vector space of cusp forms for $\Gamma_0(\mathfrak{n})$ with character ψ will be denoted $S_0(\mathfrak{n}, \psi)$. In particular, the space of cuspforms with trivial character will be denoted $S_0(\mathfrak{n})$.

Note that the only part of the definition of automorphic forms to depend on $\mathfrak{n}$ is the transformation condition (6.25). So if $\mathfrak{n} \mid \mathfrak{n}'$, then an automorphic form for $\big(\Gamma_0(\mathfrak{n}), R\big)$ is automatically an automorphic form for $\big(\Gamma_0(\mathfrak{n}'), R\big)$, since in this case, $\Omega_0(\mathfrak{n}) \supseteq \Omega_0(\mathfrak{n}')$. More succinctly,

$$\mathfrak{n} \mid \mathfrak{n}' \implies S_0(\mathfrak{n}, \psi) \subseteq S_0(\mathfrak{n}', \psi).$$

[2]In fact, thanks to the adelic viewpoint, we know that the apparent dependence on R is a mirage.

6.2.4 Homology

We briefly discuss how we can use results of Kurcănov [Kur78] to express $S_0(\mathfrak{n})$ as a homology group. It is this which we then calculate elsewhere in this thesis.

We adopt the notation of Kurcănov, and put $\Gamma_0^i(\mathfrak{n}) = \Gamma^{[i]}$. We write $\mathfrak{H}_3^* = \mathfrak{H}_3 \cup k \cup \{\infty\}$, and equip it with the usual topology. For an arbitrary discrete subgroup Γ of $\mathrm{GL}(2,k)$, we denote by $\bar{X}_\Gamma$ the topological space $\Gamma\backslash\mathfrak{H}_3^*$, and by X_Γ its subspace $\Gamma\backslash\mathfrak{H}_3$. In the case when Γ is torsion-free, i.e. has no elements of finite order, X_Γ is a real analytic Riemannian manifold, with compactification $\bar{X}_\Gamma$. We now form the disjoint union

$$\bar{X}_0(\mathfrak{n}) = \bigcup_{i=1}^{h} \bar{X}_{\Gamma_0^i(\mathfrak{n})}.$$

The object of central interest is the first cohomology with coefficients in $\mathbb{C}$,

$$H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) = \bigoplus_{i=1}^{h} H^1(\bar{X}_{\Gamma_0^i(\mathfrak{n})}, \mathbb{C}). \tag{6.26}$$

We now sketch how this is to be interpreted when (some of) the groups $\Gamma_0^i(\mathfrak{n})$ have elements of finite order, referring to [Kur78] for details. Namely, for each i, we choose a torsion-free normal subgroup Γ_i of finite index in $\Gamma_0^i(\mathfrak{n})$; such a subgroup exists by a general theorem of Selberg [Cas86, Ch.5, Theorem 4.1], since $\Gamma_0^i(\mathfrak{n})$ is finitely generated. We put

$$\bar{X} = \bigcup_{i=1}^{h} \bar{X}_{\Gamma_i}.$$

Clearly,

$$H^1(\bar{X}, \mathbb{C}) = \bigoplus_{i=1}^{h} H^1(\bar{X}_{\Gamma_i}, \mathbb{C}). \tag{6.27}$$

For each i, the quotient group $\Gamma_0^i(\mathfrak{n})/\Gamma_i$ acts on the manifold $\bar{X}_{\Gamma_i}$ and on its cohomology; (6.26) refers to the invariant subspace of (6.27) under these actions.

Kurcănov now defines certain spaces $P(\mathfrak{n}, \psi)$, similar to our spaces $S_0(\mathfrak{n}, \psi)$, and puts

$$P(\mathfrak{n}) = \sum_{\psi} P(\mathfrak{n}, \psi),$$

where the sum runs over all the unramified Dirichlet characters of k. The main theorem of [Kur78], which may be thought of as a version of the Hodge decomposition theorem,[3]

[3]see Chapter 4

is

$$P(\mathfrak{n}) \cong H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}),$$

where the isomorphism is induced by

$$\left(f^{(1)}, \ldots, f^{(h)}\right) \mapsto \left(f^{(1)} \cdot \beta, \ldots, f^{(h)} \cdot \beta\right);$$

we say "induced" rather than "given" because a differential form $f^{(i)} \cdot \beta$ may have to be replaced by a cohomologous form that is fixed by the action of $\Gamma_0^i(\mathfrak{n})/\Gamma_i$.

There is an exact duality

$$H_1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) \times H^1(\bar{X}_0(\mathfrak{n}), \mathbb{C}) \to \mathbb{C},$$

given by integrating a differential form along a chain; this is essentially de Rham's theorem. Remarkably, the duality works at the level of the rational (Hecke) structure [Kur78], so it suffices to work out

$$H_1(\bar{X}_0(\mathfrak{n}), \mathbb{Q}) \tag{6.28}$$

and the Hecke action on this space. The rational homology is generated by paths between cusps, and conversely, any path between cusps is rational. (The corresponding situation in the case of classical modular forms over $\mathbb{Q}$ is described by the Manin-Drinfeld theorem; see [Cre97] for details.) We can therefore calculate (6.28) using *modular symbols*; basically, the modular symbol $\{A, B\}_\Gamma$ is the (complex) homology class identified by duality with the functional

$$\omega \mapsto \int_A^B \phi^* \omega,$$

where ω denotes a differential on $\bar{X}_\Gamma$, and $\phi\colon \mathfrak{H}_3^* \to \bar{X}_\Gamma$ denotes the natural map. In fact, we will only compute

$$V(\mathfrak{n}) = H_1(\bar{X}_{\Gamma_0(\mathfrak{n})}, \mathbb{Q}); \tag{6.29}$$

this is equivalent to finding only the $f^{(1)}$ component of a cuspform.

Remark. It may appear inelegant that the $P(\mathfrak{n},\psi)$ are not the same as our $S_0(\mathfrak{n},\psi)$. The space $P(\mathfrak{n},\psi)$ is defined adelically, much like our functions $\Phi\colon G_{\mathbb{A}} \to \mathbb{C}^3$; the difference is that (D) is replaced by right-invariance under K_v. The result is that (6.25) is replaced by invariance of $f^{(i)}$ under $\Gamma^{[i]}$, which means that $f^{(i)} \cdot \beta$ may be viewed as a differential form on the quotient space $\bar{X}_{\Gamma^{[i]}}$. This is obviously very convenient in [Kur78], because it makes the main theorem work, but it does mean that the main theorem does not compute the space of greatest interest to us. Fortunately, $P(\mathfrak{n},\psi)$ and $S_0(\mathfrak{n},\psi)$ do coincide when $\psi = 1$.

Chapter 7

Modular points and Hecke theory

It is well known that classical modular forms for $\mathrm{SL}(2,\mathbb{Z})$ correspond to certain functions on $\mathbb{Z}$-lattices in $\mathbb{C}$. This idea, briefly described in §2.1.2, extends to forms for the main congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$; such forms correspond to functions on "modular points" defined over $\mathbb{Z}$, which are $\mathbb{Z}$-lattices in $\mathbb{C}$ equipped with some extra structure. Modular points may be used to introduce Hecke operators; the theory is described in [Kob84].

In fact, $\mathbb{C}$ is playing the rôle of $\mathbb{R}^2$, and the theory works because $\mathbb{Q}$ has a unique infinite place, which is real. The purpose of this chapter is to develop an analogous theory when $\mathbb{Q}$ is replaced by an imaginary quadratic field k, and $\mathbb{R}^2$ by $\mathbb{C}^2$. For much of the chapter, we allow k to be an arbitrary number field embedded in $\mathbb{C}$ (even a totally real field). However, the application to bear in mind is when $k \to \mathbb{C}$ is the unique archimedean embedding. We consider the most important congruence subgroups of $\Gamma = \mathrm{GL}(2,\mathfrak{O})$, namely Γ itself, $\Gamma_0(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$; we write Γ' in the generic case.[1]

We begin in §7.1 by defining lattices in $\mathbb{C}^r$. We then introduce the set $\mathcal{M} = \mathcal{M}(\Gamma')$ of modular points for Γ' as a set of lattices in $\mathbb{C}^2$ equipped with certain extra $\mathfrak{n}$-torsion data. In §7.2, we use modular points to develop a theory of "formal" Hecke operators; they form a certain ring of endomorphisms of the free abelian group on $\mathcal{M}$.

In §7.3, we introduce the rather *ad hoc* notion of an admissible basis of a modular point, and prove some technical lemmas. The case of $\Gamma(\mathfrak{n})$ turns out to be unsatisfactory,

[1] We shall not need to consider the derived subgroup (commutator subgroup) of Γ, so the notation Γ' should not cause confusion.

which may reflect the non-existence of a Hecke theory for $\Gamma(\mathfrak{n})$. (In the classical case, that problem is overcome by "twisting" forms for $\Gamma(N)$ into forms for $\Gamma_1(N)$; in the imaginary quadratic case, a proper theory of twists has yet to be worked out.)

The purpose of §7.3 becomes clear in §7.4, where we show that modular forms for $\Gamma_0(\mathfrak{n})$ over an imaginary quadratic field may be viewed as functions on modular points. This viewpoint allows us to use the "formal" Hecke operators of §7.2 as "actual" operators on the space of modular forms.

7.1 Modular points

7.1.1 Lattices in $\mathbb{C}^r$

Let k be a number field with ring of integers $\mathfrak{O}$. Fix an embedding $k \to \mathbb{C}$; this makes $\mathbb{C}^r$ into a k-module and hence an $\mathfrak{O}$-module. We shall be interested in certain $\mathfrak{O}$-submodules. There is clearly an induced embedding $k^r \to \mathbb{C}^r$, so that lattices in k^r (as discussed in §1.1.4) become lattices in $\mathbb{C}^r$; the purpose of this section is to describe a broader class of lattices in $\mathbb{C}^r$.

If $k \subseteq L \subseteq \mathbb{C}$ is a tower of fields, and Λ is an $\mathfrak{O}$-submodule of $\mathbb{C}^r$, then the L-subspace of $\mathbb{C}^r$ spanned by Λ is just

$$L\Lambda = \left\{ \sum a_i \omega_i \;\middle|\; a_i \in L,\ \omega_i \in \Lambda \right\}.$$

Definition. An $\mathfrak{O}$-*lattice* in $\mathbb{C}^r$ is an $\mathfrak{O}$-submodule Λ of $\mathbb{C}^r$ satisfying

(i) $\mathbb{C}\Lambda = \mathbb{C}^r$, i.e. Λ generates $\mathbb{C}^r$ over $\mathbb{C}$;

(ii) there are $\mathfrak{O}$-modules $F, F' \subset \mathbb{C}^r$, free of rank r over $\mathfrak{O}$, such that $F' \subseteq \Lambda \subseteq F$;

(iii) Λ is finitely generated over $\mathfrak{O}$, and $\dim(k\Lambda) = r$.

We abbreviate "$\mathfrak{O}$-lattice" to *lattice* when the intended $\mathfrak{O}$ is clear from the context. Condition (i) excludes submodules which are not "discrete" in the appropriate sense. For example, $\Lambda = \mathfrak{O}(1,0) \oplus \mathfrak{O}(x,0)$, with $x \notin k$, is not a lattice in $\mathbb{C}^2$, even though (ii) holds with $F = F' = \Lambda$. Conditions (ii) and (iii) are equivalent, as we now show; in practice, (ii) is often the easier to verify.

Proof of equivalence. Assume (iii). Since Λ is obviously torsion-free, Λ is a (rank r) $\mathfrak{O}$-lattice in $k\Lambda$. By our remarks at the start of §1.1.4, this implies (ii).

Conversely, assume (ii). Since F/F' is torsion, it is finite of order equal to the norm of the ideal $\operatorname{ord}(F/F')$. So Λ is finitely generated, *viz* by the r generators of F' together with coset representatives of F' in Λ. Obviously $\dim(k\Lambda) = r$, proving (iii). □

Essentially, where in §1.1.4 we considered lattices on the fixed (abstract) vector space k^r, we now consider lattices on all the r-dimensional k-vector spaces $E \subset \mathbb{C}^r$ satisfying $\mathbb{C}E = \mathbb{C}^r$; for a given lattice $\Lambda \subset \mathbb{C}^r$, the space E is just $k\Lambda$. All our earlier results on lattices may be applied to lattices in $\mathbb{C}^r$, for the constructions are all taking place inside the appropriate E. Thus, if $\Lambda' \supseteq \Lambda$ are lattices and $\mathfrak{a}$ is a fractional ideal, then $\mathfrak{a}\Lambda$ is a lattice, and Λ, Λ' and $\mathfrak{a}\Lambda$ all embed in the same E.

Finally, note that if $\Lambda'' \supseteq \Lambda$ are lattices, then any $\mathfrak{O}$-module Λ' satisfying $\Lambda'' \supseteq \Lambda' \supseteq \Lambda$ is automatically a lattice, by (ii) above; this fact will often be used implicitly.

7.1.2 Modular points

Let $\Gamma = \mathrm{GL}(2, \mathfrak{O})$, let $\mathfrak{n}$ be an integral ideal of $\mathfrak{O}$, and let Γ' be one of the congruence subgroups Γ, $\Gamma_0(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$. Of course, $\Gamma = \Gamma_0(\mathfrak{O}) = \Gamma_1(\mathfrak{O}) = \Gamma(\mathfrak{O})$, so everything we say about the cases $\Gamma_0(\mathfrak{n})$, $\Gamma_1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$ will apply to Γ if we set $\mathfrak{n} = \mathfrak{O}$.

Definition. By a *modular point* for Γ' we mean:

(i) for $\Gamma' = \Gamma$: a lattice $\Lambda \subset \mathbb{C}^2$;

(ii) for $\Gamma' = \Gamma_0(\mathfrak{n})$: a pair (Λ, S), where Λ is a lattice in $\mathbb{C}^2$ and $S \subset \mathbb{C}^2/\Lambda$ is a (cyclic) $\mathfrak{O}$-submodule isomorphic to $\mathfrak{O}/\mathfrak{n}$;

(iii) for $\Gamma' = \Gamma_1(\mathfrak{n})$: a pair (Λ, t), where Λ is a lattice in $\mathbb{C}^2$ and $t \in \mathbb{C}^2/\Lambda$ is an element with annihilator $\mathfrak{n}$;

(iv) for $\Gamma' = \Gamma(\mathfrak{n})$: a pair $\big(\Lambda, (t_1, t_2)\big)$, where Λ is a lattice in $\mathbb{C}^2$ and $t_1, t_2 \in \mathbb{C}^2/\Lambda$ are generators over $\mathfrak{O}$ of the total $\mathfrak{n}$-torsion submodule $\mathfrak{n}^{-1}\Lambda/\Lambda$ of $\mathbb{C}^2/\Lambda$.

In each case, Λ is called the *underlying lattice* of the modular point.

We make some remarks about these definitions. In (iv) above, pairs (t_1, t_2) always exist, for by Lemma 8, $\mathfrak{n}^{-1}\Lambda/\Lambda \cong (\mathfrak{O}/\mathfrak{n})^2$, so we may take as t_1, t_2 the pullbacks of generators of the two summands $\mathfrak{O}/\mathfrak{n}$.

Thus also, in (iii), a suitable t always exists, for example $t = t_1$. Finally, in (ii), a suitable S always exists, for example $S = \mathfrak{O}t$. The number of different t giving rise to the same S is of course $\phi(\mathfrak{n}) = |(\mathfrak{O}/\mathfrak{n})^\times|$. In other words, in (ii), the isomorphism $\mathfrak{O}/\mathfrak{n} \cong S$ is only determined up to automorphism of S, whilst in (iii), we fix an isomorphism $\bar{1} \mapsto t$.

Given a lattice Λ, there will in general be several modular points of the form (Λ, S), (Λ, t) and $\big(\Lambda, (t_1, t_2)\big)$. However, when $\mathfrak{n} = \mathfrak{O}$ there is only one modular point corresponding to each Λ, and we identify it with the modular point Λ for Γ.

Various concepts associated with lattices will be extended to modular points without further comment; for example, the *Steinitz class* of a modular point is the Steinitz class of its underlying lattice, and a modular point is *free* if its Steinitz class is trivial.

Notation. The set of modular points for Γ' is denoted $\mathcal{M}(\Gamma')$. The subset of free modular points is denoted $\mathcal{M}_1(\Gamma')$.

It will be convenient to adopt the following notational convention regarding towers of lattices.

Notation. Let $\Lambda' \supseteq \Lambda$ be lattices. If (Λ, S) is a modular point for $\Gamma_0(\mathfrak{n})$, we write S' for the image of S modulo the larger lattice Λ'. Similarly, if (Λ, t) is a modular point for $\Gamma_1(\mathfrak{n})$, we write t' for the image of t in $\mathbb{C}^2/\Lambda'$. Again, if $\big(\Lambda, (t_1, t_2)\big)$ is a modular point for $\Gamma(\mathfrak{n})$, we write t'_1 and t'_2 for the images of t_1 and t_2 in $\mathbb{C}^2/\Lambda'$.

In general, (Λ', S') need not be a modular point for $\Gamma_0(\mathfrak{n})$. It will be one, however, if $\operatorname{ord}(\Lambda'/\Lambda)$ is prime to $\mathfrak{n}$, as we now show.

Lemma 101. *Let $\mathcal{M} = \mathcal{M}\big(\Gamma_0(\mathfrak{n})\big)$, and let $\Lambda' \supseteq \Lambda$ be lattices with $\operatorname{ord}(\Lambda'/\Lambda)$ prime to $\mathfrak{n}$. Then $(\Lambda, S) \in \mathcal{M} \implies (\Lambda', S') \in \mathcal{M}$.*

Proof. Let $T = \Lambda'/\Lambda$. Then $\mathfrak{n}$ annihilates S and $\operatorname{ord}(T)$ annihilates T, so $\mathfrak{O} = \mathfrak{n} + \operatorname{ord}(T)$ annihilates $S \cap T$. Therefore, $S \cap T = 0$. But $T = \ker(\mathbb{C}^2/\Lambda \to \mathbb{C}^2/\Lambda')$. So $S' \cong S \cong \mathfrak{O}/\mathfrak{n}$. So $(\Lambda', S') \in \mathcal{M}$, as required. □

Corollary 102. *The analogous result holds for $\Gamma_1(\mathfrak{n})$ and $\Gamma(\mathfrak{n})$.*

Proof. Let (Λ, t) be a modular point for $\Gamma_1(\mathfrak{n})$. By Lemma 101, $\mathfrak{O}t' \cong \mathfrak{O}t \cong \mathfrak{O}/\mathfrak{n}$, so t' has annihilator $\mathfrak{n}$, and (Λ', t') is modular. For $\big(\Lambda, (t_1, t_2)\big)$ we argue as in the proof of Lemma 101, with $\mathfrak{O}t_1 + \mathfrak{O}t_2$ in place of S. □

7.2 Formal Hecke theory

Let Γ' be one of the congruence subgroups considered above, let $\mathcal{M} = \mathcal{M}\big(\Gamma'\big)$, and let $\mathbb{Z}\mathcal{M}$ be the free abelian group generated by $\mathcal{M}$. We shall define formal Hecke operators as certain endomorphisms of $\mathbb{Z}\mathcal{M}$. For concreteness, we shall work with $\Gamma_0(\mathfrak{n})$, but the formalism applies, *mutatis mutandis*, to the other congruence subgroups.

For each integral ideal $\mathfrak{a}$ of $\mathfrak{O}$, define a $\mathbb{Z}$-linear map $T_{\mathfrak{a}} \colon \mathbb{Z}\mathcal{M} \to \mathbb{Z}\mathcal{M}$ by

$$T_{\mathfrak{a}}(\Lambda, S) = \sum_{\substack{\Lambda' \supseteq \Lambda \\ \operatorname{ord}(\Lambda'/\Lambda) = \mathfrak{a} \\ (\Lambda', S') \in \mathcal{M}}} (\Lambda', S').$$

This sum is over all those superlattices Λ' of Λ with $\operatorname{ord}(\Lambda'/\Lambda) = \mathfrak{a}$ and $(\Lambda', S') \in \mathcal{M}$; the sum is finite because any such Λ' satisfies $\Lambda \subseteq \Lambda' \subseteq \mathfrak{a}^{-1}\Lambda$, and $\mathfrak{a}^{-1}\Lambda/\Lambda \cong (\mathfrak{O}/\mathfrak{a})^2$ is finite.

Also, for each integral ideal $\mathfrak{a}$ of $\mathfrak{O}$ prime to $\mathfrak{n}$, define an endomorphism $T_{\mathfrak{a},\mathfrak{a}} \colon \mathbb{Z}\mathcal{M} \to \mathbb{Z}\mathcal{M}$ by

$$T_{\mathfrak{a},\mathfrak{a}}(\Lambda, S) = (\mathfrak{a}^{-1}\Lambda, S'), \tag{7.1}$$

where, as usual, S' denotes the image of S modulo the larger lattice. By Lemma 101, this definition makes sense, that is to say, $(\mathfrak{a}^{-1}\Lambda, S') \in \mathcal{M}$.

We shall shortly derive some identities between these operators and prove that they commute pairwise. Our first proposition records some almost obvious facts.

Proposition 103. *The operators $\mathbb{Z}\mathcal{M} \to \mathbb{Z}\mathcal{M}$ introduced above satisfy the following identities:*

(i) $T_{<1>} = T_{<1>,<1>} = 1 =$ identity map.

(ii) *For $\mathfrak{a}$ and $\mathfrak{b}$ both prime to $\mathfrak{n}$,*

$$T_{\mathfrak{a},\mathfrak{a}} T_{\mathfrak{b},\mathfrak{b}} = T_{\mathfrak{ab},\mathfrak{ab}} = T_{\mathfrak{b},\mathfrak{b}} T_{\mathfrak{a},\mathfrak{a}}.$$

(iii) *For* $\mathfrak{a}$ *prime to* $\mathfrak{n}$ *and any* $\mathfrak{b}$,

$$T_{\mathfrak{a},\mathfrak{a}}T_{\mathfrak{b}} = T_{\mathfrak{b}}T_{\mathfrak{a},\mathfrak{a}}.$$

Proof. Clear. □

Proposition 104. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime, then* $T_{\mathfrak{a}}$ *and* $T_{\mathfrak{b}}$ *commute. In fact,*

$$T_{\mathfrak{a}}T_{\mathfrak{b}} = T_{\mathfrak{a}\mathfrak{b}}. \tag{7.2}$$

Proof. We compute the action of both sides on generators (Λ, S) of $\mathbb{Z}\mathcal{M}$.

$$T_{\mathfrak{a}\mathfrak{b}}(\Lambda, S) = \sum_{\substack{\Lambda''\supseteq\Lambda \\ \mathrm{ord}(\Lambda''/\Lambda)=\mathfrak{a}\mathfrak{b} \\ (\Lambda'',S'')\in\mathcal{M}}} (\Lambda'', S'') \tag{7.3}$$

$$T_{\mathfrak{a}}T_{\mathfrak{b}}(\Lambda, S) = \sum_{\substack{\Lambda'\supseteq\Lambda \\ \mathrm{ord}(\Lambda'/\Lambda)=\mathfrak{b} \\ (\Lambda',S')\in\mathcal{M}}} \sum_{\substack{\Lambda''\supseteq\Lambda' \\ \mathrm{ord}(\Lambda''/\Lambda')=\mathfrak{a} \\ (\Lambda'',S'')\in\mathcal{M}}} (\Lambda'', S'') \tag{7.4}$$

First note that, by the tower law, every (Λ'', S'') arising in (7.4) arises in (7.3). We must show that, conversely, every (Λ'', S'') arising in (7.3) arises in (7.4) for one and only one Λ'.

Given (Λ'', S'') arising in (7.3), by Lemma 11 there is a unique lattice Λ' such that $\Lambda'' \supseteq \Lambda' \supseteq \Lambda$, $\mathrm{ord}(\Lambda''/\Lambda') = \mathfrak{a}$ and $\mathrm{ord}(\Lambda'/\Lambda) = \mathfrak{b}$. Moreover, since $(\Lambda'', S'') \in \mathcal{M}$, it is clear that $(\Lambda', S') \in \mathcal{M}$, completing the proof. □

We now consider $T_{\mathfrak{a}}$ for $\mathfrak{a}$ a power of a prime ideal $\mathfrak{p}$. The situation is simpler when $\mathfrak{p}$ divides the level.

Proposition 105. *Let* $\mathfrak{p}$ *be a prime ideal dividing* $\mathfrak{n}$. *Then for* $n \geq 1$,

$$T_{\mathfrak{p}^n} = (T_{\mathfrak{p}})^n. \tag{7.5}$$

Proof. By induction on n, it suffices to show that $T_{\mathfrak{p}^{n+1}} = T_{\mathfrak{p}}T_{\mathfrak{p}^n}$ for $n \geq 1$. Let $(\Lambda, S) \in \mathcal{M}$.

$$T_{\mathfrak{p}^{n+1}}(\Lambda, S) = \sum_{\substack{\Lambda''\supseteq\Lambda \\ \mathrm{ord}(\Lambda''/\Lambda)=\mathfrak{p}^{n+1} \\ (\Lambda'',S'')\in\mathcal{M}}} (\Lambda'', S'') \tag{7.6}$$

$$T_{\mathfrak{p}}T_{\mathfrak{p}^n}(\Lambda, S) = \sum_{\substack{\Lambda' \supseteq \Lambda \\ \operatorname{ord}(\Lambda'/\Lambda)=\mathfrak{p}^n \\ (\Lambda',S') \in \mathcal{M}}} \sum_{\substack{\Lambda'' \supseteq \Lambda' \\ \operatorname{ord}(\Lambda''/\Lambda')=\mathfrak{p} \\ (\Lambda'',S'') \in \mathcal{M}}} (\Lambda'', S'') \tag{7.7}$$

By the tower law, every (Λ'', S'') arising in (7.7) certainly arises in (7.6). We must show that, conversely, every (Λ'', S'') arising in (7.6) arises in (7.7) for one and only one Λ'.

It suffices to show that given $\Lambda'' \supseteq \Lambda$ with $\operatorname{ord}(\Lambda''/\Lambda) = \mathfrak{p}^{n+1}$ and (Λ'', S'') modular, there exists a unique lattice Λ' with $\Lambda'' \supseteq \Lambda' \supseteq \Lambda$ and $\operatorname{ord}(\Lambda''/\Lambda') = \mathfrak{p}$, since for such Λ' it is automatic that $\operatorname{ord}(\Lambda'/\Lambda) = \mathfrak{p}^n$ and that (Λ', S') is modular.

The key step is to observe that $\Lambda \not\subseteq \mathfrak{p}\Lambda''$. Otherwise, writing $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$, we would have $\mathfrak{p}\mathfrak{n}'S \subseteq \Lambda \subseteq \mathfrak{p}\Lambda''$, whence $\mathfrak{n}'S \subseteq \Lambda''$, contradicting $S'' \cong \mathfrak{O}/\mathfrak{n}$, i.e. (Λ'', S'') modular. Hence Lemma 13 applies, completing the proof. □

In the case when $\mathfrak{p}$ does not divide the level, we need the operator $T_{\mathfrak{a},\mathfrak{a}}$ introduced earlier.

Proposition 106. *Let $\mathfrak{p}$ be a prime ideal not dividing $\mathfrak{n}$. Then for $n \geq 1$,*

$$T_{\mathfrak{p}^n}T_{\mathfrak{p}} = T_{\mathfrak{p}^{n+1}} + \mathbf{N}(\mathfrak{p})T_{\mathfrak{p}^{n-1}}T_{\mathfrak{p},\mathfrak{p}}. \tag{7.8}$$

Proof. Let $(\Lambda, S) \in \mathcal{M}$. We apply the various operators in (7.8) to (Λ, S). Because of Lemma 101 and the assumption $\mathfrak{p} \nmid \mathfrak{n}$, the condition on S is automatically fulfilled for all lattices Λ', Λ'' considered below.

By Corollary 9, $\operatorname{ord}(\mathfrak{p}^{-1}\Lambda/\Lambda) = \mathfrak{p}^2$. So by the tower law, $T_{\mathfrak{p}^n}T_{\mathfrak{p}}(\Lambda, S)$, $T_{\mathfrak{p}^{n+1}}(\Lambda, S)$ and $T_{\mathfrak{p}^{n-1}}T_{\mathfrak{p},\mathfrak{p}}(\Lambda, S)$ are linear combinations of modular points (Λ'', S''), where $\Lambda'' \supseteq \Lambda$ and $\operatorname{ord}(\Lambda''/\Lambda) = \mathfrak{p}^{n+1}$.

Let Λ'' be a lattice with $\Lambda'' \supseteq \Lambda$ and $\operatorname{ord}(\Lambda''/\Lambda) = \mathfrak{p}^{n+1}$. In the above linear combinations (Λ'', S'') appears with respective coefficients a, b and c, say. We have to show that $a = b + \mathbf{N}(\mathfrak{p})c$. Clearly $b = 1$, so we must show that $a = 1 + \mathbf{N}(\mathfrak{p})c$.

We have two cases. First, assume that $\Lambda'' \not\supseteq \mathfrak{p}^{-1}\Lambda$. Then $c = 0$, and a is the number of lattices Λ' satisfying $\Lambda'' \supseteq \Lambda' \supseteq \Lambda$ and $\operatorname{ord}(\Lambda'/\Lambda) = \mathfrak{p}$. The assumption $\Lambda \not\subseteq \mathfrak{p}\Lambda''$ allows us to apply Lemma 13, giving $a = 1$ as required.

Now assume instead that $\Lambda'' \supseteq \mathfrak{p}^{-1}\Lambda$. Then $c = 1$. Any lattice Λ' having $\operatorname{ord}(\Lambda'/\Lambda) = \mathfrak{p}$ satisfies $\mathfrak{p}\Lambda' \subseteq \Lambda \subseteq \mathfrak{p}\Lambda''$, so satisfies $\Lambda' \subseteq \Lambda''$. So a is the number of such lattices Λ'. Since such a Λ' satisfies $\Lambda' \subseteq \mathfrak{p}^{-1}\Lambda$, the number of such Λ' is just the number of non-trivial proper submodules of $\mathfrak{p}^{-1}\Lambda/\Lambda \cong \mathfrak{O}/\mathfrak{p} \oplus \mathfrak{O}/\mathfrak{p}$. Because $\mathfrak{p}$ is maximal, $\mathfrak{O}/\mathfrak{p}$ is a field with $\mathbf{N}(\mathfrak{p})$ elements, and a is just the number of one-dimensional vector subspaces. So $a = \mathbf{N}(\mathfrak{p}) + 1$. This concludes the proof. □

If $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ is the prime factorisation of the integral ideal $\mathfrak{a}$, then (7.2) shows that $T_{\mathfrak{a}} = T_{\mathfrak{p}_1^{e_1}} \cdots T_{\mathfrak{p}_r^{e_r}}$. Then (7.5) and (7.8) show that each $T_{\mathfrak{p}_i^{e_i}}$ is a polynomial in $T_{\mathfrak{p}_i}$ and $T_{\mathfrak{p}_i,\mathfrak{p}_i}$. It is easy to see from this and Proposition 103 that all of the operators $T_{\mathfrak{a}}$ (for $\mathfrak{a}$ any integral ideal) and $T_{\mathfrak{a},\mathfrak{a}}$ (for $\mathfrak{a}$ prime to $\mathfrak{n}$) commute with each other. Thus, these operators generate a commutative algebra $\mathcal{H}$ of $\mathbb{Z}$-linear maps $\mathbb{Z}\mathcal{M} \to \mathbb{Z}\mathcal{M}$. Of course, $\mathcal{H}$ is already generated by the $T_{\mathfrak{p},\mathfrak{p}}$ (for $\mathfrak{p} \nmid \mathfrak{n}$ prime) and the $T_{\mathfrak{p}}$ (for $\mathfrak{p}$ any prime).

There is an elegant way to summarise equations (7.2), (7.5) and (7.8) as formal power series identities, where the coefficients of the power series are elements of $\mathcal{H}$. First, for $\mathfrak{p} \mid \mathfrak{n}$, we can restate (7.5) as follows:

$$\sum_{l=0}^{\infty} T_{\mathfrak{p}^l} X^l = \frac{1}{1 - T_{\mathfrak{p}} X}, \qquad \mathfrak{p} \mid \mathfrak{n}, \tag{7.9}$$

that is, $(\sum T_{\mathfrak{p}^l} X^l)(1 - T_{\mathfrak{p}} X) = 1$ in $\mathcal{H}[[X]]$. This follows from (7.5) by equating coefficients, because the coefficient of X^l for $l > 0$ is $T_{\mathfrak{p}^l} - T_{\mathfrak{p}^{l-1}} T_{\mathfrak{p}}$. Similarly, for $\mathfrak{p} \nmid \mathfrak{n}$, (7.8) is equivalent to the identity

$$\sum_{l=0}^{\infty} T_{\mathfrak{p}^l} X^l = \frac{1}{1 - T_{\mathfrak{p}} X + \mathbf{N}(\mathfrak{p}) T_{\mathfrak{p},\mathfrak{p}} X^2}, \qquad \mathfrak{p} \nmid \mathfrak{n}. \tag{7.10}$$

For by equating coefficients of X^l in $(\sum T_{\mathfrak{p}^l} X^l)\big(1 - T_{\mathfrak{p}} X + \mathbf{N}(\mathfrak{p}) T_{\mathfrak{p},\mathfrak{p}} X^2\big) = 1$ we see that (7.10) is equivalent to the equalities

$$T_{<1>} = 1,$$
$$T_{\mathfrak{p}} - T_{\mathfrak{p}} = 0,$$
$$T_{\mathfrak{p}^l} - T_{\mathfrak{p}^{l-1}} T_{\mathfrak{p}} + \mathbf{N}(\mathfrak{p}) T_{\mathfrak{p}^{l-2}} T_{\mathfrak{p},\mathfrak{p}} = 0 \qquad \text{for } l \geq 2.$$

To incorporate Proposition 104, we introduce a new variable $s \in \mathbb{C}$ by putting $X = \mathbf{N}(\mathfrak{p})^{-s}$ for each $\mathfrak{p}$ in (7.9) or (7.10). We then take the product of (7.9) over all $\mathfrak{p}$ with

$\mathfrak{p} \mid \mathfrak{n}$ and of (7.10) over all $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{n}$:

$$\prod_{\mathfrak{p}} \sum_{l=0}^{\infty} T_{\mathfrak{p}^l} \, \mathbf{N}(\mathfrak{p}^l)^{-s} = \prod_{\mathfrak{p}|\mathfrak{n}} \frac{1}{1 - T_{\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{-s}} \prod_{\mathfrak{p}\nmid\mathfrak{n}} \frac{1}{1 - T_{\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{-s} + T_{\mathfrak{p},\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{1-2s}}.$$

Using Proposition 104, uniqueness of the prime factorisation $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, and the relation $\mathbf{N}(\mathfrak{a})^{-s} = \mathbf{N}(\mathfrak{p}_1^{e_1})^{-s} \cdots \mathbf{N}(\mathfrak{p}_r^{e_r})^{-s}$, we can multiply out the left hand side, much as in the proof of the Euler product expansion for the Riemann zeta-function. We conclude that

$$\sum_{\mathfrak{a} \triangleleft \mathfrak{O}} T_{\mathfrak{a}} \, \mathbf{N}(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}|\mathfrak{n}} \frac{1}{1 - T_{\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{-s}} \prod_{\mathfrak{p}\nmid\mathfrak{n}} \frac{1}{1 - T_{\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{-s} + T_{\mathfrak{p},\mathfrak{p}} \, \mathbf{N}(\mathfrak{p})^{1-2s}}. \tag{7.11}$$

Remark. One could consider an analogous theory based on lattices of rank r and a suitable definition of modular points. The proof of $T_{\mathfrak{a}} T_{\mathfrak{b}} = T_{\mathfrak{a}\mathfrak{b}}$ would be unchanged. However, the analogues of (7.5) and (7.8) would be more complicated, because of the failure of uniqueness in Lemma 13 when $r > 2$. The appropriate Euler factors would be correspondingly more complicated.

7.3 Admissible bases

This purpose of this somewhat technical section will become clear in §7.4. Once and for all, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ be integral ideals of $\mathfrak{O}$ representing the h ideal classes; as usual, we take $\mathfrak{p}_1 = \mathfrak{O}$ to represent the principal class. When necessary, we will further assume (as we may by Lemma 1) that the $\mathfrak{p}_i$ are chosen so that

$$\mathfrak{p}_i + \mathfrak{n} = \mathfrak{O}. \tag{7.12}$$

7.3.1 Bases of arbitrary lattices

By structure theory (§1.1.3), every lattice $\Lambda \subset \mathbb{C}^2$ is isomorphic to $\mathfrak{p}_i \oplus \mathfrak{O}$ for some i, called the *class* of Λ. Hence Λ has the form $\mathfrak{p}_i\omega_1 \oplus \mathfrak{O}\omega_2$ for vectors $\omega_1, \omega_2 \in \mathbb{C}^2$ which are linearly independent over $\mathbb{C}$. By abuse of language, we call ω_1, ω_2 a *basis* for Λ, even when Λ is not free.[2] In the free case, of course, a basis is unique up to transformation by an

[2] A purist might say "quasibasis", but no confusion will arise.

element of $\Gamma = \mathrm{GL}(2, \mathfrak{O})$; for the general case, we need the "generalised Bianchi groups" $\mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$ of Chapman [Cha94], defined by

$$\mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, d \in \mathfrak{O},\ b \in \mathfrak{p}_i^{-1},\ c \in \mathfrak{p}_i,\ ad - bc \in \mathfrak{O}^\times \right\}.$$

Lemma 107. *The bases of a lattice $\Lambda = \mathfrak{p}_i\omega_1 \oplus \mathfrak{O}\omega_2$ are precisely those $\omega_1', \omega_2' \in \mathbb{C}^2$ satisfying*

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \tag{7.13}$$

for some $\gamma \in \mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$.

Proof. Let ω_1', ω_2' be a basis. Certainly (7.13) holds for for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, k)$. In fact, as $\omega_2' \in \Lambda$, we have $c \in \mathfrak{p}_i$ and $d \in \mathfrak{O}$; as $\mathfrak{p}_i\omega_1' \subseteq \Lambda$, we have $\mathfrak{p}_i a \subseteq \mathfrak{p}_i$ and $\mathfrak{p}_i b \subseteq \mathfrak{O}$, i.e. $a \in \mathfrak{O}$ and $b \in \mathfrak{p}_i^{-1}$. It follows that $\det\gamma \in \mathfrak{O}$. By symmetry, $(\det\gamma)^{-1} \in \mathfrak{O}$, whence $\det\gamma \in \mathfrak{O}^\times$. Thus $\gamma \in \mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$.

Conversely, let $\gamma \in \mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$ and define ω_1', ω_2' by (7.13). Then

$$\mathfrak{p}_i\omega_1' + \mathfrak{O}\omega_2' = \mathfrak{p}_i(a\omega_1 + b\omega_2) + \mathfrak{O}(c\omega_1 + d\omega_2) \subseteq \mathfrak{p}_i\omega_1 + \mathfrak{O}\omega_2 = \Lambda,$$

and

$$\Lambda = \mathfrak{p}_i\omega_1 + \mathfrak{O}\omega_2 = \mathfrak{p}_i(d\omega_1' - b\omega_2') + \mathfrak{O}(a\omega_2' - c\omega_1') \subseteq \mathfrak{p}_i\omega_1' + \mathfrak{O}\omega_2',$$

proving $\Lambda = \mathfrak{p}_i\omega_1' \oplus \mathfrak{O}\omega_2'$, as required. □

Notation. Let $\omega_1, \omega_2 \in \mathbb{C}^2$ be linearly independent over $\mathbb{C}$. We may regard the row vectors ω_1, ω_2 as the rows of a matrix

$$\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C}),$$

and define

$$\Lambda_\omega^{(i)} = \mathfrak{p}_i\omega_1 \oplus \mathfrak{O}\omega_2.$$

The sum is direct because the ω_i are even independent over $\mathbb{C}$. Thus $\omega \mapsto \Lambda_\omega^{(i)}$ is a surjection from $\mathrm{GL}(2, \mathbb{C})$ to the set of lattices of class i.

Notation. The set of modular points of class i for Γ' is denoted $\mathcal{M}_i(\Gamma')$. Thus, there is a disjoint union

$$\mathcal{M}(\Gamma') = \bigcup_{i=1}^{h} \mathcal{M}_i(\Gamma'). \tag{7.14}$$

Our first task is to construct a modular point for Γ' with underlying lattice $\Lambda_\omega^{(i)}$; this gives rise to functions $\mathrm{GL}(2, \mathbb{C}) \to \mathcal{M}_i(\Gamma')$, which we denote by $\omega \mapsto P_\omega^{(i)}$. A basis ω of a modular point P of class i will be called *admissible* if $P = P_\omega^{(i)}$. We will then discuss the existence of admissible bases and to what extent they are unique.

It is instructive to begin with the special case of free lattices, firstly, because it is simpler to deal with, and secondly, because it is sufficient for some applications. In the special case, we can omit the superscripts, writing $\omega \mapsto \Lambda_\omega$ and so on.

7.3.2 Special case: free modular points

Once and for all, choose $\beta \in \mathfrak{n}^{-1}$ as in Lemma 2; recall that it satisfies

$$\mathfrak{n}^{-1} = \mathfrak{O} + \mathfrak{O}\beta, \qquad \mathfrak{n} = \{\, x \in \mathfrak{O} \mid x\beta \in \mathfrak{O} \,\}.$$

Given a free lattice Λ, we may use β to write down an element of each $\mathcal{M}_1(\Gamma')$; this is accomplished by our next lemma. The case $\mathfrak{O} = \mathbb{Z}$, $\mathfrak{n} = \langle N \rangle$ occurs in [Kob84]; in the general case, the rôle of $1/N$ is played by β.

Lemma 108. *Let $\omega_1, \omega_2 \in \mathbb{C}^2$ be linearly independent over $\mathbb{C}$. Define a lattice Λ in $\mathbb{C}^2$ by $\Lambda = \Lambda_\omega = \mathfrak{O}\omega_1 \oplus \mathfrak{O}\omega_2$. Then*

(i) $\Lambda \in \mathcal{M}_1(\Gamma)$,

(ii) $\bigl(\Lambda, (\mathfrak{O}\beta\omega_2 + \Lambda)/\Lambda\bigr) = \bigl(\Lambda, (\mathfrak{n}^{-1}\omega_2 + \Lambda)/\Lambda\bigr) \in \mathcal{M}_1\bigl(\Gamma_0(\mathfrak{n})\bigr)$,

(iii) $(\Lambda, \beta\omega_2 \bmod \Lambda) \in \mathcal{M}_1\bigl(\Gamma_1(\mathfrak{n})\bigr)$,

(iv) $\bigl(\Lambda, (\beta\omega_1 \bmod \Lambda, \beta\omega_2 \bmod \Lambda)\bigr) \in \mathcal{M}_1\bigl(\Gamma(\mathfrak{n})\bigr)$.

Proof. Case (i) holds by definition. For (ii), define a map $\mathfrak{O} \to (\mathfrak{O}\beta\omega_2 + \Lambda)/\Lambda$ by $x \mapsto x\beta\omega_2 \bmod \Lambda$. This is clearly surjective, with kernel

$$\{ x \in \mathfrak{O} \mid x\beta\omega_2 \in \Lambda \} = \{ x \in \mathfrak{O} \mid x\beta \in \mathfrak{O} \} = \mathfrak{n}. \tag{7.15}$$

So $(\mathfrak{O}\beta\omega_2+\Lambda)/\Lambda = (\mathfrak{n}^{-1}\omega_2+\Lambda)/\Lambda \cong \mathfrak{O}/\mathfrak{n}$, as required for (ii). Equation (7.15) also shows that the annihilator of $\beta\omega_2 \bmod \Lambda$ equals $\mathfrak{n}$, proving (iii). To verify (iv), we observe

$$\mathfrak{O}\beta\omega_1 + \mathfrak{O}\beta\omega_2 + \Lambda = \mathfrak{n}^{-1}\omega_1 + \mathfrak{n}^{-1}\omega_2 + \Lambda = \mathfrak{n}^{-1}\Lambda$$

showing that the $\beta\omega_i \bmod \Lambda$ do generate $\mathfrak{n}^{-1}\Lambda/\Lambda$, as required. □

We remark that the modular points in (i) and (ii) do not depend on the choice of β, although of course those in (iii) and (iv) do.

Notation. The function $\mathrm{GL}(2,\mathbb{C}) \to \mathcal{M}_1(\Gamma')$ constructed in the lemma will be denoted

$$\omega \mapsto P_\omega.$$

Definition. An *admissible basis* of a free modular point is

(i) for $\Lambda \in \mathcal{M}_1(\Gamma)$, any basis of Λ;

(ii) for $(\Lambda, S) \in \mathcal{M}_1\big(\Gamma_0(\mathfrak{n})\big)$, a basis ω_1, ω_2 of Λ such that $S = (\Lambda + \mathfrak{O}\beta\omega_2)/\Lambda$;

(iii) for $(\Lambda, t) \in \mathcal{M}_1\big(\Gamma_1(\mathfrak{n})\big)$, a basis ω_1, ω_2 of Λ such that $t = \beta\omega_2 \bmod \Lambda$;

(iv) for $\big(\Lambda, (t_1, t_2)\big) \in \mathcal{M}_1\big(\Gamma(\mathfrak{n})\big)$, a basis ω_1, ω_2 of Λ such that $t_i = \beta\omega_i \bmod \Lambda$ for $i = 1, 2$.

Thus, ω_1, ω_2 is an admissible basis of a free modular point P if and only if the construction of Lemma 108 applied to ω_1, ω_2 yields P, i.e. if and only if $P_\omega = P$. Of course, in cases (iii) and (iv) we should really say "β-admissible"; however, it does no harm to suppress the dependence on β, since β is assumed fixed once and for all.

We postpone the question of existence for the moment. First we show that if an admissible basis exists, then the set of admissible bases is the orbit under the corresponding congruence subgroup Γ' of any one such basis.

Lemma 109 (Uniqueness up to Γ'-equivalence). *Let $P \in \mathcal{M}_1(\Gamma')$, let $\omega = (\omega_1\ \omega_2)^t$ and $\omega' = (\omega_1'\ \omega_2')^t$ be bases of P, and assume that ω is admissible. Then ω' is admissible if and only if $\omega' = \gamma\omega$ for some $\gamma \in \Gamma'$.*

Proof. There are four cases: (i) $P = \Lambda \in \mathcal{M}_1(\Gamma)$, (ii) $P = (\Lambda, S) \in \mathcal{M}_1\big(\Gamma_0(\mathfrak{n})\big)$, (iii) $P = (\Lambda, t) \in \mathcal{M}_1\big(\Gamma_1(\mathfrak{n})\big)$, and (iv) $P = \big(\Lambda, (t_1, t_2)\big) \in \mathcal{M}_1\big(\Gamma(\mathfrak{n})\big)$. Certainly

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathfrak{O})$. In case (i) the result is obvious. In case (ii) we have

$$\begin{aligned}
\mathfrak{O}\beta\omega_2 + \Lambda \supseteq \mathfrak{O}\beta\omega_2' + \Lambda &\iff \beta\omega_2' - \beta\alpha\omega_2 \in \Lambda \text{ for some } \alpha \in \mathfrak{O} \\
&\iff \beta c\omega_1 + \beta(d-\alpha)\omega_2 \in \Lambda \text{ for some } \alpha \in \mathfrak{O} \\
&\iff \beta c \in \mathfrak{O},\ \beta(d-\alpha) \in \mathfrak{O} \text{ for some } \alpha \in \mathfrak{O} \\
&\iff c \in \mathfrak{n},\ d - \alpha \in \mathfrak{n} \text{ for some } \alpha \in \mathfrak{O} \\
&\iff \gamma \in \Gamma_0(\mathfrak{n}).
\end{aligned}$$

By symmetry, we also have

$$\mathfrak{O}\beta\omega_2 + \Lambda \subseteq \mathfrak{O}\beta\omega_2' + \Lambda \iff \gamma^{-1} \in \Gamma_0(\mathfrak{n}),$$

and therefore

$$\begin{aligned}
\omega' \text{ is admissible} &\iff \mathfrak{O}\beta\omega_2 + \Lambda = \mathfrak{O}\beta\omega_2' + \Lambda \\
&\iff \gamma \in \Gamma_0(\mathfrak{n}).
\end{aligned}$$

In case (iii), we argue as in case (ii) but with $\alpha = 1$; thus

$$\begin{aligned}
\omega' \text{ is admissible} &\iff t = \beta\omega_2' \bmod \Lambda \\
&\iff \beta(\omega_2' - \omega_2) \in \Lambda \\
&\iff c, d - 1 \in \mathfrak{n} \\
&\iff \gamma \in \Gamma_1(\mathfrak{n}).
\end{aligned}$$

The argument in case (iv) is similar. $\square$

We now turn to the question of existence. First, we report the good news.

Lemma 110 (Existence of admissible bases). *Let Γ' equal Γ, $\Gamma_0(\mathfrak{n})$ or $\Gamma_1(\mathfrak{n})$, and let $P \in \mathcal{M}_1(\Gamma')$. Then P has an admissible basis.*

Proof. We number the cases as before; the result holds vacuously in case (i). We prove cases (ii) and (iii); consider first case (iii). Let e_1, e_2 be an $\mathfrak{O}$-basis for Λ. Since $t \in \mathfrak{n}^{-1}\Lambda/\Lambda = (\Lambda + \beta\Lambda)/\Lambda$, there is $\omega_0 \in \Lambda$ such that $t = \beta\omega_0 \bmod \Lambda$. Write $\omega_0 = a_1 e_1 + a_2 e_2$ with $a_i \in \mathfrak{O}$. We claim that

$$\langle a_1, a_2 \rangle + \mathfrak{n} = \mathfrak{O}. \tag{7.16}$$

For let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{n}$. Since the annihilator of t is precisely $\mathfrak{n}$, we have $\mathfrak{p}^{-1}\mathfrak{n}\beta\omega_0 \nsubseteq \Lambda$. Therefore $\mathfrak{p}^{-1}\mathfrak{n}\beta\langle a_1, a_2\rangle \nsubseteq \mathfrak{O}$, whence $\langle a_1, a_2 \rangle \nsubseteq \mathfrak{p}$. This proves (7.16). By Lemma 24 on M-symbols, there exists $(A_{ij}) \in \mathrm{SL}(2, \mathfrak{O})$ such that $A_{21} \equiv a_1 \pmod{\mathfrak{n}}$, $A_{22} \equiv a_2 \pmod{\mathfrak{n}}$. Put

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = (A_{ij}) \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Then ω_1, ω_2 is a basis for Λ, and $\omega_2 = A_{21}e_1 + A_{22}e_2 \equiv \omega_0 \pmod{\mathfrak{n}\Lambda}$, whence $\beta(\omega_0 - \omega_2) \in \beta\mathfrak{n}\Lambda \subseteq \Lambda$, and so $\beta\omega_2 \bmod \Lambda = t$. Thus ω_1, ω_2 is an admissible basis.

We now turn to case (ii). Since $S \cong \mathfrak{O}/\mathfrak{n}$ is cyclic, we may choose a generator $t \in S$. Clearly $\mathrm{ann}(t) = \mathfrak{n}$, in other words, $(\Lambda, t) \in \mathcal{M}_1\big(\Gamma_1(\mathfrak{n})\big)$. By (iii), Λ has a basis ω_1, ω_2 such that $t = \beta\omega_2 \bmod \Lambda$. Then clearly $S = \mathfrak{O}t = (\Lambda + \mathfrak{O}\beta\omega_2)/\Lambda$. $\square$

In case (iv), the news is not so good: there are modular points with no admissible basis. This is made more precise in the following proposition; for convenience, its statement and proof employ the summation convention.

Proposition 111. *Let $\Lambda \subset \mathbb{C}^2$ be a lattice with basis e_1, e_2. Let $(C_{ij}) \in \mathrm{M}_2(\mathfrak{O})$ be invertible modulo $\mathfrak{n}$. For $i \in \{1, 2\}$, put $x_i = C_{ij}e_j$ and $t_i = \beta x_i \bmod \Lambda \in \mathfrak{n}^{-1}\Lambda/\Lambda$. Then $P = \big(\Lambda, (t_1, t_2)\big) \in \mathcal{M}_1\big(\Gamma(\mathfrak{n})\big)$. Moreover, P has an admissible basis if and only if there exists $(A_{ij}) \in \Gamma$ such that $A_{ij} \equiv C_{ij} \bmod \mathfrak{n}$, and when that is so, $A_{1j}e_j, A_{2j}e_j$ is admissible.*

Proof. Let $(D_{ki}) \in \mathrm{M}_2(\mathfrak{O})$ be an inverse of (C_{ij}) modulo $\mathfrak{n}$. Let $s \in \mathfrak{n}^{-1}\Lambda/\Lambda$. We may write $s = \beta x \bmod \Lambda$ for some $x = b_k e_k \in \Lambda$, where $b_k \in \mathfrak{O}$. Since $D_{ki}x_i \equiv e_k \mod \mathfrak{n}\Lambda$, we have $\beta(D_{ki}x_i - e_k) \in \beta\mathfrak{n}\Lambda \subseteq \Lambda$. Therefore $\beta(b_k D_{ki} x_i - x) \in \Lambda$, whence $s = b_k D_{ki} t_i \bmod \Lambda$, showing that s lies in the span of the t_i. Thus P is a modular point.

Assume that P has an admissible basis y_1, y_2, say. Certainly $y_i = A_{ij}e_j$ for some $(A_{ij}) \in \Gamma$, and admissibility implies $\beta(y_i - x_i) \in \Lambda$, whence $\beta(A_{ij} - C_{ij})e_j \in \Lambda$, whence $\beta(A_{ij} - C_{ij}) \in \mathfrak{O}$, whence finally $A_{ij} \equiv C_{ij} \mod \mathfrak{n}$. Conversely, assume that $(A_{ij}) \in \Gamma$ congruent to (C_{ij}) exists, and put $y_i = A_{ij}e_j$. Then clearly $\beta(y_i - x_i) \in \Lambda$, proving admissibility. □

Thus, the obstruction to admissibility in all cases is the failure of surjectivity of the natural homomorphism $\mathrm{GL}(2, \mathfrak{O}) \to \mathrm{GL}(2, \mathfrak{O}/\mathfrak{n})$; see Corollary 23.

Example. Let $\mathfrak{O} = \mathbb{Z}$, $\mathfrak{n} = 5\mathbb{Z}$ and $\beta = 1/5$. Let $\Lambda = \mathbb{Z}^2$, with basis $e_1 = (1,0)$, $e_2 = (0,1)$. Put $x_1 = (2,0)$ and $x_2 = (0,1)$; thus $(C_{ij}) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which is invertible mod 5. Then $P = \big(\Lambda, ((2/5, 0) \bmod \Lambda, (0, 1/5) \bmod \Lambda)\big)$ is a modular point with no admissible basis.

This is a counterexample to case (iv) of a proposition of Koblitz [Kob84, p. 154, Prop. 31], the proof of which had been left to the reader.[3] It implies that modular points, at least as we have defined them, are not a successful approach to $\Gamma(\mathfrak{n})$.

Of course, we may have the wrong definition of modular point in this case, *pace* Koblitz [Kob84]. For $\mathfrak{O} = \mathbb{Z}$, the moduli problem associated to $\Gamma(N)$ is discussed in [Sil86, Appendix C, §13]. The N-torsion points of an elliptic curve come equipped with the Weil pairing e_N, and the pair $(1/N, \tau/N)$ satisfies

$$e_N(1/N, \tau/N) = e^{2\pi i/N}.$$

So a better notion of modular point for $\Gamma(N)$ would be a pair as defined in (iv) above (but over $\mathbb{Z}$, of course) that maps under the Weil pairing to a specific (fixed) primitive N^{th} root of unity. Presumably a suitable analogue exists in the case of an imaginary quadratic field, with the Weil pairing on elliptic curves replaced by a 2-dimensional analogue and with roots of unity replaced by $\mathfrak{n}$-division points in $\mathbb{C}/\mathfrak{O}$.

[3] p. 174 *op. cit.*, Problem 1

7.3.3 General case

We now repeat much of §7.3.2 for general lattices. In view of Proposition 111, we no longer consider case (iv), so Γ' will be one of Γ, $\Gamma_0(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$.

Lemma 112. *Let $\omega_1, \omega_2 \in \mathbb{C}^2$ be linearly independent over $\mathbb{C}$, and put $\Lambda = \Lambda_\omega^{(i)} = \mathfrak{p}_i\omega_1 \oplus \mathfrak{O}\omega_2$. Then*

(i) $\Lambda \in \mathcal{M}_i(\Gamma)$,

(ii) $\big(\Lambda, (\mathfrak{O}\beta\omega_2 + \Lambda)/\Lambda\big) = \big(\Lambda, (\mathfrak{n}^{-1}\omega_2 + \Lambda)/\Lambda\big) \in \mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big)$,

(iii) $(\Lambda, \beta\omega_2 \bmod \Lambda) \in \mathcal{M}_i\big(\Gamma_1(\mathfrak{n})\big)$.

Proof. The proof is word for word the same as for (i)–(iii) of Lemma 108. □

Notation. As indicated earlier, the function $\mathrm{GL}(2, \mathbb{C}) \to \mathcal{M}_i(\Gamma')$ constructed in the lemma will be denoted

$$\omega \mapsto P_\omega^{(i)}.$$

Definition. Let $P \in \mathcal{M}_i(\Gamma')$. Then ω_1, ω_2 is an admissible basis for P if and only if $P = P_\omega^{(i)}$. Explicitly, an admissible basis is

(i) for $\Lambda \in \mathcal{M}_i(\Gamma)$, any basis of Λ;

(ii) for $(\Lambda, S) \in \mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big)$, a basis ω_1, ω_2 of Λ such that $S = (\Lambda + \mathfrak{O}\beta\omega_2)/\Lambda$;

(iii) for $(\Lambda, t) \in \mathcal{M}_i\big(\Gamma_1(\mathfrak{n})\big)$, a basis ω_1, ω_2 of Λ such that $t = \beta\omega_2 \bmod \Lambda$.

Our next lemma generalises Lemma 110; in place of Lemma 24 on M-symbols, we shall use its refinement Lemma 25.

Lemma 113 (Existence of admissible bases). *Let Γ' equal Γ, $\Gamma_0(\mathfrak{n})$ or $\Gamma_1(\mathfrak{n})$, and let $P \in \mathcal{M}_i(\Gamma')$. Then P has an admissible basis.*

Proof. We number the cases as before. In case (i), the result holds by the remarks at the start of §7.3.1. We prove cases (ii) and (iii); consider first case (iii). Let e_1, e_2 be a basis for Λ, so $\Lambda = \mathfrak{p}_i e_1 \oplus \mathfrak{O} e_2$. Since $t \in \mathfrak{n}^{-1}\Lambda/\Lambda = (\Lambda + \beta\Lambda)/\Lambda$, there is $\omega_0 \in \Lambda$ such that

$t = \beta\omega_0 \bmod \Lambda$. Write $\omega_0 = a_1 e_1 + a_2 e_2$ with $a_1 \in \mathfrak{p}_i$ and $a_2 \in \mathfrak{O}$. For the first time, we assume (7.12). We claim that

$$\langle a_1, a_2 \rangle + \mathfrak{n} = \mathfrak{O}. \tag{7.17}$$

For let $\mathfrak{p}$ be a prime ideal dividing $\mathfrak{n}$. We must show $\langle a_1, a_2 \rangle \not\subseteq \mathfrak{p}$. If $a_1 \notin \mathfrak{p}$, we are done, so assume $a_1 \in \mathfrak{p}$, whence by (7.12), we have $a_1 \in \mathfrak{p}\mathfrak{p}_i$. Thus $\mathfrak{p}^{-1}\mathfrak{n}\beta a_1 \subseteq \mathfrak{p}_i$. Since the annihilator of t is precisely $\mathfrak{n}$, we have $\mathfrak{p}^{-1}\mathfrak{n}\beta\omega_0 \not\subseteq \Lambda$. Therefore $\mathfrak{p}^{-1}\mathfrak{n}\beta a_2 \not\subseteq \mathfrak{O}$, whence $a_2 \notin \mathfrak{p}$. This proves (7.17).

As we may assume without loss of generality that $a_1 \neq 0$, we may apply Lemma 25 on M-symbols, giving $(A_{ij}) \in \mathrm{SL}(2, \mathfrak{O})$ such that $A_{21} = a_1 \in \mathfrak{p}_i$ and $A_{22} \equiv a_2 \pmod{\mathfrak{n}}$. Put

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = (A_{ij}) \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}.$$

Then ω_1, ω_2 is a basis for Λ, by Lemma 107. Now $\omega_2 = A_{21}e_1 + A_{22}e_2 \equiv \omega_0 \pmod{\mathfrak{n}\Lambda}$, whence $\beta(\omega_0 - \omega_2) \in \beta\mathfrak{n}\Lambda \subseteq \Lambda$, and so $\beta\omega_2 \bmod \Lambda = t$. Thus ω_1, ω_2 is an admissible basis.

We now turn to case (ii). Since $S \cong \mathfrak{O}/\mathfrak{n}$ is cyclic, we may choose a generator $t \in S$. Clearly $\mathrm{ann}(t) = \mathfrak{n}$, in other words, $(\Lambda, t) \in \mathcal{M}_i(\Gamma_1(\mathfrak{n}))$. By (iii), Λ has a basis ω_1, ω_2 such that $t = \beta\omega_2 \bmod \Lambda$. Then clearly $S = \mathfrak{O}t = (\Lambda + \mathfrak{O}\beta\omega_2)/\Lambda$. □

It will not surprise the reader to learn that admissible bases are unique up to an element of a suitable "twist" of Γ'. For concreteness, we treat the case $\Gamma' = \Gamma_0(\mathfrak{n})$. The twisted groups arising will be precisely the groups $\Gamma^{[i]}$ of (5.15), provided that the ideles are chosen correctly. Thus, let $r_i \in k_{\mathbb{A}}^{\times}$ be ideles with $il(r_i) = \mathfrak{p}_i^{-1}$; as before, put

$$a_i = \begin{pmatrix} r_i & 0 \\ 0 & 1 \end{pmatrix} \in G_{\mathbb{A}}.$$

Assuming (7.12), a simple calculation gives

$$\Gamma^{[i]} = G_k \cap a_i \Omega_0(\mathfrak{n}) a_i^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, d \in \mathfrak{O},\ b \in \mathfrak{p}_i^{-1},\ c \in \mathfrak{n}\mathfrak{p}_i,\ ad - bc \in \mathfrak{O}^{\times} \right\};$$

when $\mathfrak{n} = \mathfrak{O}$, these groups are just the generalised Bianchi groups $\mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$, so here we have "generalised Bianchi groups of level $\mathfrak{n}$".

Lemma 114 (Uniqueness up to $\Gamma^{[i]}$-equivalence). *Let $P \in \mathcal{M}_i(\Gamma_0(\mathfrak{n}))$ and let $\omega = (\omega_1\ \omega_2)^t$ and $\omega' = (\omega_1'\ \omega_2')^t$ be bases of P. Assume that ω is admissible. Then ω' is admissible if and only if $\omega' = \gamma\omega$ for some $\gamma \in \Gamma^{[i]}$.*

Proof. Write $P = (\Lambda, S) \in \mathcal{M}_i(\Gamma_0(\mathfrak{n}))$. By Lemma 107,

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_{\mathfrak{p}_i}(2, \mathfrak{O})$. The proof will be complete when we have shown that ω' is admissible if and only if $c \in \mathfrak{n}\mathfrak{p}_i$. We have

$$\begin{aligned} \mathfrak{O}\beta\omega_2 + \Lambda \supseteq \mathfrak{O}\beta\omega_2' + \Lambda &\iff \beta\omega_2' - \beta\alpha\omega_2 \in \Lambda \text{ for some } \alpha \in \mathfrak{O} \\ &\iff \beta c\omega_1 + \beta(d-\alpha)\omega_2 \in \Lambda \text{ for some } \alpha \in \mathfrak{O} \\ &\iff \beta c \in \mathfrak{p}_i,\ \beta(d-\alpha) \in \mathfrak{O} \text{ for some } \alpha \in \mathfrak{O} \\ &\iff \beta c \in \mathfrak{p}_i, \\ &\iff c \in \mathfrak{n}\mathfrak{p}_i, \end{aligned}$$

where the last step uses $c \in \mathfrak{p}_i$. By symmetry, we also have

$$\mathfrak{O}\beta\omega_2 + \Lambda \subseteq \mathfrak{O}\beta\omega_2' + \Lambda \iff c \in \mathfrak{n}\mathfrak{p}_i.$$

This completes the proof. □

7.4 Modular forms as functions on modular points

We show how modular forms can be interpreted as functions on lattices. Our treatment parallels the treatment of $k = \mathbb{Q}$ in [Kob84].

It is well known that classical modular forms for $\mathrm{SL}(2, \mathbb{Z})$ correspond to certain functions on $\mathbb{Z}$-lattices in $\mathbb{C}$. The idea extends to forms for the main congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$; such forms correspond to functions on modular points defined over $\mathbb{Z}$. The main features of the classical case were described in §2.1.2.

The purpose of this section is to develop an entirely analogous theory over imaginary quadratic fields. After our preparatory work above, we can treat simultaneously the cases

$\Gamma' = \Gamma$, $\Gamma_0(\mathfrak{n})$ and $\Gamma_1(\mathfrak{n})$. The failure of Lemma 110 for $\Gamma' = \Gamma(\mathfrak{n})$ means that we cannot proceed further with that case. This may reflect the non-existence of a Hecke theory for $\Gamma(\mathfrak{n})$.

We use the notation of §4.3; thus $G = \mathrm{GL}(2,\mathbb{C})$, with centre Z and subgroup $K = \mathrm{SU}(2)$, and $\rho\colon ZK \to \mathbb{C}^3$ is a representation. Recall the definition of $\mathcal{S}_2$:

$$\mathcal{S}_2 = \left\{ \phi\colon G \to \mathbb{C}^3 \;\middle|\; \phi(\zeta g \kappa) = \phi(g)\rho(\zeta\kappa) \quad \forall \zeta \in Z,\ g \in G,\ \kappa \in K \right\}.$$

Let P be a modular point, i.e. of the form Λ, (Λ, S), (Λ, t) or $\big(\Lambda, (t_1, t_2)\big)$. Let $\zeta \in Z$ and $\kappa \in K$. It is clear how to interpret $\zeta P \kappa$, and that it is a modular point — for Z acts on the left by scalar multiplication and K on the right by matrix multiplication, the effect being to change merely the copy of k^2 in which the point lies, in the sense of §7.1.1.

Definition. A function $F\colon \mathcal{M}(\Gamma') \to \mathbb{C}^3$ is of *weight* ρ if

$$F(\zeta P \kappa) = F(P)\rho(\zeta\kappa) \qquad \forall P \in \mathcal{M}(\Gamma'),\ \zeta \in \mathbb{C}^\times,\ \kappa \in K.$$

Our aim is to show that modular forms correspond to certain weight-ρ functions on modular points. Again, it is instructive to begin with the "principal" part of modular forms, which corresponds to functions on free modular points.

7.4.1 Functions on modular points: special case

Thus, define sets $\mathcal{S}_5$ and $\mathcal{S}_6$ as follows:

$$\mathcal{S}_5 = \left\{ \phi \in \mathcal{S}_2 \;\middle|\; \phi\big|\gamma = \phi \text{ for all } \gamma \in \Gamma' \right\},$$
$$\mathcal{S}_6 = \left\{ F\colon \mathcal{M}_1(\Gamma') \to \mathbb{C}^3 \;\middle|\; F \text{ is of weight } \rho \right\}.$$

Given $\phi \in \mathcal{S}_5$, we define $\phi^\sharp\colon \mathcal{M}_1(\Gamma') \to \mathbb{C}^3$ by

$$\phi^\sharp(P) = \phi(\omega), \tag{7.18}$$

where ω is any admissible basis of $P \in \mathcal{M}_1(\Gamma')$. Conversely, given $F \in \mathcal{S}_6$, we define $F^\flat\colon G \to \mathbb{C}^3$ by

$$F^\flat(\omega) = F(P_\omega). \tag{7.19}$$

Our next result is exactly analogous to Proposition 31 of Koblitz [Kob84].[4]

Proposition 115. *The maps* (7.18) *and* (7.19) *define mutually inverse bijections* $\sharp\colon \mathcal{S}_5 \to \mathcal{S}_6$ *and* $\flat\colon \mathcal{S}_6 \to \mathcal{S}_5$.

Proof. The map (7.18) is possible by Lemma 110 and well-defined by Lemma 109 and Γ'-invariance of ϕ. If ω_1, ω_2 is an admissible basis of P, then $\zeta\omega_1\kappa, \zeta\omega_2\kappa$ is obviously an admissible basis of $\zeta P\kappa$, and so

$$\phi^\sharp(\zeta P\kappa) = \phi(\zeta\omega\kappa) = \phi(\omega)\rho(\zeta\kappa) = \phi^\sharp(P)\rho(\zeta\kappa),$$

proving that $\phi^\sharp$ is of weight ρ. Thus (7.18) does define a map $\mathcal{S}_5 \to \mathcal{S}_6$.

In the other direction, we must check that $F^\flat$ lies in $\mathcal{S}_2$ and is invariant under Γ'. The first part is formal, since $P_{\zeta\omega\kappa} = \zeta P_\omega\kappa$, and therefore

$$F^\flat(\zeta\omega\kappa) = F(P_{\zeta\omega\kappa}) = F(\zeta P_\omega\kappa) = F(P_\omega)\rho(\zeta\kappa) = F^\flat(\omega)\rho(\zeta\kappa).$$

To prove the second part, let $\gamma \in \Gamma'$. By Lemma 107, $\Lambda_{\gamma\omega} = \Lambda_\omega$, so by Lemma 109, $\gamma\omega$ is admissible for P_ω, i.e. $P_{\gamma\omega} = P_\omega$. Thus

$$\left(F^\flat\middle|\gamma\right)(\omega) = F^\flat(\gamma\omega) = F(P_{\gamma\omega}) = F(P_\omega) = F^\flat(\omega),$$

i.e. $F^\flat\big|\gamma = F^\flat$. Thus (7.19) does define a map $\mathcal{S}_6 \to \mathcal{S}_5$.

Finally, we check that the constructions are mutually inverse. Let $\phi \in \mathcal{S}_5$ and $\omega \in G$. Since ω is an admissible basis for P_ω, we have

$$\phi^{\sharp\flat}(\omega) = \phi^\sharp(P_\omega) = \phi(\omega).$$

Thus $\phi^{\sharp\flat} = \phi$. Conversely, let $F \in \mathcal{S}_6$ and $P \in \mathcal{M}_1(\Gamma')$. Choose an admissible basis ω, so that $P = P_\omega$. Then

$$F^{\flat\sharp}(P) = F^\flat(\omega) = F(P_\omega).$$

This shows that $F^{\flat\sharp} = F$, thereby completing the proof. $\square$

[4] As an aside, we remark that Koblitz [Kob84] denotes the analogue of the composite $F \mapsto F^\flat \mapsto F^{\flat *}$ of (7.19) and (4.48) by $F \mapsto \tilde{F}$; therein lies the origin of our notation for generic elements of $\mathcal{S}_3$.

7.4.2 Functions on modular points: general case

We now give the obvious generalisation of Proposition 115 for lattices of class i, restricting to $\Gamma' = \Gamma_0(\mathfrak{n})$ since we have not defined groups $\Gamma^{[i]}$ for $\Gamma_1(\mathfrak{n})$. Thus, define sets $\mathcal{S}_5^{(i)}$ and $\mathcal{S}_6^{(i)}$ as follows:

$$\mathcal{S}_5^{(i)} = \left\{ \phi \in \mathcal{S}_2 \;\middle|\; \phi\middle|\gamma = \phi \text{ for all } \gamma \in \Gamma^{[i]} \right\},$$
$$\mathcal{S}_6^{(i)} = \left\{ F\colon \mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big) \to \mathbb{C}^3 \;\middle|\; F \text{ is of weight } \rho \right\}.$$

Given $\phi \in \mathcal{S}_5^{(i)}$, we define $\phi^\sharp\colon \mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big) \to \mathbb{C}^3$ by

$$\phi^\sharp(P) = \phi(\omega), \tag{7.20}$$

where ω is any admissible basis of $P \in \mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big)$. Conversely, given $F \in \mathcal{S}_6^{(i)}$, we define $F^\flat\colon G \to \mathbb{C}^3$ by

$$F^\flat(\omega) = F(P_\omega). \tag{7.21}$$

Proposition 116. *Maps* (7.20) *and* (7.21) *give mutually inverse bijections* $\sharp\colon \mathcal{S}_5^{(i)} \to \mathcal{S}_6^{(i)}$ *and* $\flat\colon \mathcal{S}_6^{(i)} \to \mathcal{S}_5^{(i)}$.

Proof. As for Proposition 115, replacing the special cases of existence and uniqueness by the general, i.e. replacing Lemma 110 by Lemma 113 and Lemma 109 by Lemma 114. □

We can now sketch the following theorem which relates modular points to modular forms; it seems unnecessary to write out all the details.

Theorem 117. *Let* $\mathcal{M} = \mathcal{M}\big(\Gamma_0(\mathfrak{n})\big)$. *Modular forms for* $\Gamma_0(\mathfrak{n})$ *with trivial character correspond to certain weight-*ρ *functions on* $\mathcal{M}$.

Proof. Here "certain" functions means those consistent with "admissibility of type $\mathcal{H}_\mathbb{C}$" in the language of Chapter 6. In §6.2.3, we defined modular forms as h-tuples $F = (f^{(1)}, \ldots, f^{(h)})$, for functions $f^{(i)}\colon \mathfrak{H}_3 \to \mathbb{C}^3$ invariant under $\Gamma^{[i]}$. By Lemma 64, they may be viewed as h-tuples $\Phi = (\phi^{(1)}, \ldots, \phi^{(h)})$ with $\phi^{(i)} \in \mathcal{S}_5^{(i)}$. In view of (7.14), we can combine (7.20) and (7.21) for all i; thus, given a modular form Φ, define $\Phi^\sharp\colon \mathcal{M} \to \mathbb{C}^3$ by

$$\Phi^\sharp(P_\omega^{(i)}) = \phi^{(i)}(\omega),$$

and given a suitable $F\colon \mathcal{M} \to \mathbb{C}^3$, define a modular form $F^\flat = \big((F^\flat)^{(1)}, \ldots, (F^\flat)^{(h)}\big)$ by

$$(F^\flat)^{(i)}(\omega) = F(P^{(i)}_\omega).$$

Obviously (by Proposition 116) these constructions give the required correspondence. □

7.5 Hecke operators for modular forms

7.5.1 Action of Hecke operators

It is now a simple matter to turn the formal Hecke operators of §7.2 into actual Hecke operators for modular forms. Let $\mathcal{M} = \mathcal{M}\big(\Gamma_0(\mathfrak{n})\big)$. Extend functions $F\colon \mathcal{M} \to \mathbb{C}^3$ to functions $\hat{F}\colon \mathbb{Z}\mathcal{M} \to \mathbb{C}^3$ by $\mathbb{Z}$-linearity. We can then define

$$F\big|T_\mathfrak{a} = \hat{F} \circ T_\mathfrak{a}, \qquad F\big|T_{\mathfrak{a},\mathfrak{a}} = \hat{F} \circ T_{\mathfrak{a},\mathfrak{a}};$$

some authors write $T_\mathfrak{a}F$ and $T_{\mathfrak{a},\mathfrak{a}}F$ instead of $F\big|T_\mathfrak{a}$ and $F\big|T_{\mathfrak{a},\mathfrak{a}}$. Explicitly,

$$(F\big|T_\mathfrak{a})\big((\Lambda, S)\big) = \sum_{\substack{\Lambda'\supseteq\Lambda \\ \mathrm{ord}(\Lambda'/\Lambda)=\mathfrak{a} \\ (\Lambda',S')\in\mathcal{M}}} F\big((\Lambda', S')\big),$$

and

$$(F\big|T_{\mathfrak{a},\mathfrak{a}})\big((\Lambda, S)\big) = F\big((\mathfrak{a}^{-1}\Lambda, S')\big),$$

where, as usual, S' denotes the image of S modulo the larger lattice. Clearly these operators preserve the property of being of weight ρ; using Theorem 117, we at once obtain an action on modular forms, by defining

$$\Phi\big|T_\mathfrak{a} = (\Phi^\sharp\big|T_\mathfrak{a})^\flat, \qquad \Phi\big|T_{\mathfrak{a},\mathfrak{a}} = (\Phi^\sharp\big|T_{\mathfrak{a},\mathfrak{a}})^\flat.$$

There is an underlying representation $\mathfrak{a} \mapsto \sigma_\mathfrak{a}$ of the ideal class group by means of permutations of $\{1, \ldots, h\}$. Thus, given $\mathfrak{a}$ and i, define $j = \sigma_\mathfrak{a}(i)$ by

$$cl(\mathfrak{p}_i) = cl(\mathfrak{p}_j)cl(\mathfrak{a}).$$

In view of (1.9), the values of $F\big|T_{\mathfrak{a}}$ and $F\big|T_{\mathfrak{a},\mathfrak{a}}$ on $\mathcal{M}_i\big(\Gamma_0(\mathfrak{n})\big)$ depend only on the values of F on $\mathcal{M}_j\big(\Gamma_0(\mathfrak{n})\big)$. Correspondingly, $(\Phi\big|T_{\mathfrak{a}})^{(i)}$ and $(\Phi\big|T_{\mathfrak{a},\mathfrak{a}})^{(i)}$ depend only on $\phi^{(j)}$. Explicitly,

$$(\Phi\big|T_{\mathfrak{a}})^{(i)} = \sum_M \phi^{(j)}\big|M,$$

where M runs through the (finite) set of matrices for which $P^{(j)}_{M\omega}$ contains $P^{(i)}_{\omega}$ with index $\mathfrak{a}$; the number of these matrices is equal to $\mathbf{N}(\mathfrak{a})+1$ when $\mathfrak{a}$ is a prime ideal with $\mathfrak{a}\nmid\mathfrak{n}$. Of course, the action of matrices is by (4.53). We discuss how to find such matrices in §8.1 below.

By the usual correspondences, we finally obtain an action on modular forms $F = (f^{(1)},\dots,f^{(h)})$ on upper half-space, given by

$$(F\big|T_{\mathfrak{a}})^{(i)} = \sum_M f^{(j)}\big|M,$$

where M runs through the same set as above and matrices act according to (4.54), that is, by pullback of the corresponding differential forms.

7.5.2 Eigenforms and newforms

One might now develop a theory of eigenforms, oldforms and newforms, as achieved by Atkin and Lehner in the classical case $k=\mathbb{Q}$ [AL70]. In fact, it would only be necessary to verify that our definition of Hecke operators is equivalent to that found in a treatment of general global fields, such as that of Miyake [Miy71]. For a brief discussion in the case of an imaginary quadratic field of class number one, we refer to [Cre81, §3.3]. We shall be content with a few sketchy remarks.

A modular form F is an *eigenform* for $T_{\mathfrak{a}}$ with eigenvalue $a(\mathfrak{a})$ if and only if $F\big|T_{\mathfrak{a}} = a(\mathfrak{a})F$. We are interested in computing *newforms* at level $\mathfrak{n}$, that is, those simultaneous eigenforms in $S_0(\mathfrak{n})$ which do not arise from forms in $S_0(\mathfrak{n}')$ for some $\mathfrak{n}'\mid\mathfrak{n}$. To do this, we transfer the action to the homology spaces of §6.2.4 and perform all our computations there. In fact, we work only with the space $V(\mathfrak{n})$ of (6.29); by §7.5.1, the only Hecke operators whose action is even defined for this space alone are the $T_{\mathfrak{a}}$ and $T_{\mathfrak{a},\mathfrak{a}}$ for $\mathfrak{a}$ a principal ideal. Nevertheless, we can determine *all* eigenvalues from this one space, as we explain below.

To "find" newforms, one calculates $V(\mathfrak{n})$ and the action of enough Hecke operators on it to split off the 1-dimensional eigenspaces. In view of the result from the general theory that two forms whose eigenvalues agree at almost all primes are equal up to scalar multiple [Miy71, Theorem B], we confidently expect finitely many primes (more precisely, an initial segment of any enumeration of the primes) to suffice for this splitting off, so that an algorithm which steps through all primes will terminate; in practice, the operators $T_\mathfrak{p}$ for $\mathfrak{p} \nmid \mathfrak{n}$ a principal prime seem likely to suffice. Preferably, one splits off the eigenspaces in a way which allows arbitrarily many eigenvalues to be computed, such as would be needed to compute with the forms' Fourier series to high precision.

In fact, by the multiplicative relations of §7.2, it suffices to compute the $T_\mathfrak{p}$ (and $T_{\mathfrak{p},\mathfrak{p}}$) for $\mathfrak{p}$ prime. When $\mathfrak{p}$ is principal, this is relatively straightforward, since $T_\mathfrak{p}$ does act on $V(\mathfrak{n})$. We now sketch a trick for computing $a(\mathfrak{p})$ when $\mathfrak{p}^2$ is principal but $\mathfrak{p}$ is not. This method is sufficient to determine all Hecke eigenvalues for those imaginary quadratic fields with $C = C(2)$ in the notation of §1.4.

For simplicity, consider first the case of class number $h = 2$. Choose one non-principal prime $\mathfrak{q}$. Compute $T_{\mathfrak{q}^2}$ and $T_{\mathfrak{q},\mathfrak{q}}$; by (7.8), this yields the eigenvalue for $(T_\mathfrak{q})^2$, which determines $a(\mathfrak{q})$ up to choice of sign. Now, for each non-principal prime $\mathfrak{p} \nmid \mathfrak{n}$, we can compute $a(\mathfrak{p}\mathfrak{q})$, since $\mathfrak{p}\mathfrak{q}$ is principal, and deduce the eigenvalue for $a(\mathfrak{p})$ using $T_{\mathfrak{p}\mathfrak{q}} = T_\mathfrak{p} T_\mathfrak{q}$. Both choices of sign for $a(\mathfrak{q})$ are correct: the two forms thus obtained are "twists" of each other by the non-trivial unramified quadratic character attached to k; see §5.1.6.

In general, $C = C(2)$ implies that the genus field is equal to the Hilbert class field and that $C \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$, in the language and notation of §5.1.6. We now need to fix $t-1$ (independent) non-principal primes $\mathfrak{q}_i$ and make a choice of sign for each. For any other non-principal prime $\mathfrak{p}$, the ideal $\mathfrak{p} \prod \mathfrak{q}_i^{e_i}$ is principal for a unique choice of exponents, allowing the unique consistent value of $a(\mathfrak{p})$ to be deduced. The possible choices of sign give rise to all the twists of our form by the 2^{t-1} unramified quadratic characters attached to k.

Chapter 8

Computations

We make some remarks about explicit computations. (See also §7.5.2.) Our techniques closely follow the work of Cremona and Whitley [Cre81, Whi90] for the fields of class number one. The differences stem from the existence of non-principal ideals. The results of our computations are in Chapter 9.

8.1 Explicit Hecke matrices

Let k be an imaginary quadratic field with ring of integers $\mathfrak{O}$ and class number $h = 2$.

Proposition 118. *Let $\mathfrak{p}$ be a principal prime, with $\mathfrak{p} = \langle\beta\rangle$, say. Write down matrices as follows:*

(i) $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$;

(ii) $\begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}$, *for α running through a set of residues modulo β;*

Then the sum of these matrices (as an element of the group algebra over $\mathbb{Q}$) defines the Hecke operator $T_{\mathfrak{p}}$ at level $\mathfrak{n}$.

Proof. Exactly as for the classical theory (Hermite normal form). □

Now for the more interesting case of non-principal primes.

Proposition 119. *Let $\mathfrak{p}$ be a non-principal prime, with $\mathfrak{p}^2 = \langle\beta\rangle$, say. Solve $u\beta + v = 1$ for $u \in \mathfrak{O}$ and $v \in \mathfrak{n}$. Write down matrices as follows:*

(i) $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$;

(ii) $\begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}$, *for α running through a set of residues modulo $\mathfrak{p}^2$;*

(iii) $\begin{pmatrix} \beta & 0 \\ v\alpha & 1 \end{pmatrix}$, *for α running through a set of residues modulo $\mathfrak{p}^2$ and $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$;*

(iv) one "special" matrix giving an $\mathfrak{O}$-isomorphism $\mathfrak{O} \oplus \mathfrak{O} \to \mathfrak{p} \oplus \mathfrak{p}$, adjusted to lie in $\Delta_0(\mathfrak{n})$ as in the proof of Proposition 35.

Then the sum of these matrices (as an element of the group algebra over $\mathbb{Q}$) defines the Hecke operator $T_{\mathfrak{p}^2}$ at level $\mathfrak{n}$.

Proof. We do not need to exhibit our means of deriving this list of matrices (by looking at modules locally), as an *a posteriori* argument will suffice. The number of these matrices is $1 + \mathbf{N}\,\mathfrak{p} + \mathbf{N}\,\mathfrak{p}^2$, as required. One verifies that any two, say M_1 and M_2, give distinct sublattices, since $M_1 M_2^{-1} \notin \Gamma$. □

Proposition 120. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct non-principal primes, with $\mathfrak{pq} = \langle\beta\rangle$, say. Solve $u\beta + v = 1$ for $u \in \mathfrak{O}$ and $v \in \mathfrak{n}$. Write down matrices as follows:*

(i) $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$;

(ii) $\begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}$, *for α running through a set of residues modulo β;*

(iii) $\begin{pmatrix} \beta & 0 \\ v\alpha & 1 \end{pmatrix}$, *for α running through a set of residues modulo β and $\alpha \in \mathfrak{p} \setminus \mathfrak{q}$;*

(iv) $\begin{pmatrix} \beta & 0 \\ v\alpha & 1 \end{pmatrix}$, *for α running through a set of residues modulo β and $\alpha \in \mathfrak{q} \setminus \mathfrak{p}$;*

(v) two "special" matrices giving a $\mathfrak{O}$-isomorphisms $\mathfrak{O} \oplus \mathfrak{O} \to \mathfrak{p} \oplus \mathfrak{q}$ and $\mathfrak{O} \oplus \mathfrak{O} \to \mathfrak{q} \oplus \mathfrak{p}$, adjusted to lie in $\Delta_0(\mathfrak{n})$ as in the proof of Proposition 35.

Then the sum of these matrices (as an element of the group algebra over $\mathbb{Q}$) defines the Hecke operator $T_{\mathfrak{pq}}$ at level $\mathfrak{n}$.

Proof. Similar. □

8.2 Computations

We now step through the integral ideals $\mathfrak{n}$ in order of increasing norm; this ensures that all the proper divisors of $\mathfrak{n}$ will have been treated before $\mathfrak{n}$ itself. For each $\mathfrak{n}$, we use the relations obtained in §3.8 to determine the space $V(\mathfrak{n})$, in the manner sketched at the end of §1.3; by far the most expensive step here is the linear algebra involved in finding the kernel of the boundary map. At this stage, one can read off the dimension of $V(\mathfrak{n})$.

Having stored $V(\mathfrak{n})$ as a space generated by M-symbols in the computer's memory, we compute Hecke eigenvalues as indicated in §7.5.2. To do this, we convert M-symbols to modular symbols, a trivial step, and act on modular symbols with the Hecke operators. The modular symbols obtained must then be converted back into M-symbols; the pseudo-Euclidean algorithm of §3.6 is an essential tool here, exactly as in [Cre81, Whi90].

8.3 Some directions for further work

We comment briefly on some future directions of this research. We would like to have a more robust computer implementation of the algorithms than presently exists. Once enough eigenvalues become available, one could integrate the Fourier series to determine approximate periods of the forms. Secondly, one should treat other fields with $C = C(2)$.

In the spirit of Cremona's programme, one ought to search for elliptic curves over k of the right conductor having traces of Frobenius agreeing with the computed Hecke eigenvalues. In another direction, one should bring $\Gamma_1(\mathfrak{n})$ and forms for $\Gamma_0(\mathfrak{n})$ with arbitrary character into the picture, as was done in [Fig95] for $h = 1$. Perhaps more problematic is the question of fields with $C \neq C(2)$, clearly an interesting open problem.

Chapter 9

Results

Much of the theory we have developed in this thesis has been valid for an arbitrary imaginary quadratic field k. In this chapter, we tabulate results of our computations for the field $k = \mathbb{Q}(\sqrt{-5})$, of class number 2, and use them to illustrate various aspects of the theory. We begin by summarising some facts about ideals of k. We discuss the rôle of characters, since we compute forms with trivial and non-trivial unramified character. We discuss the action of complex conjugation, which allows us to infer all the information for level $\bar{\mathfrak{n}}$ from level $\mathfrak{n}$ and to identify forms which are self-conjugate and hence come from forms over $\mathbb{Q}$ by base change lift. We identify the oldforms and newforms at all levels $\mathfrak{n}$ with $\mathbf{N}(\mathfrak{n}) \leq 135$ and comment on the dimension of the oldspace, which can be lower than expected. Lastly, we tabulate Hecke eigenvalues for the newforms we find, and compute various characters which twist our newforms into others.

9.1 Ideals of k

Let $k = \mathbb{Q}(\sqrt{-5})$. The ring of integers $\mathfrak{O}$ of k is $[1, \sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. (We use square brackets to denote the $\mathbb{Z}$-span of elements of $\mathfrak{O}$, and angle brackets to denote the $\mathfrak{O}$-span.) The discriminant of k is $\Delta = -20$.

We use the notation of "reduced" ideals. Every ideal $\mathfrak{a}$ has the form $c\mathfrak{a}'$, where $c \in \mathbb{Z}$ and $\mathfrak{a}'$ is "reduced", i.e. $\mathfrak{a}' = [a, b + \sqrt{-5}]$ with $a, b \in \mathbb{Z}$. (It is natural to choose $a > 0$ and

$0 \le b < a$.) Thus, every ideal has the form

$$\texttt{Qideal}(a,b,c) = c[a, b+\sqrt{-5}].$$

Let p be a rational prime. If $p \mid \Delta$, i.e. $p \in \{2,5\}$, then p ramifies. Explicitly, $\langle 2\rangle = [2, 1+\sqrt{-5}]^2$ and $\langle 5\rangle = [5, \sqrt{-5}]^2 = \langle\sqrt{-5}\rangle^2$. For other primes p we find, using quadratic reciprocity, that

$$\left(\frac{\Delta}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1,3,7,9 \pmod{20}, \\ -1 & \text{if } p \equiv 11,13,17,19 \pmod{20}. \end{cases}$$

Therefore,

$$p \begin{cases} \text{splits} & \text{if } p \equiv 1,3,7,9 \pmod{20}, \\ \text{is inert} & \text{if } p \equiv 11,13,17,19 \pmod{20}. \end{cases}$$

If p is split, it may split as a product of principal primes or of non-principal primes. The first case occurs when p also splits in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{5})$ (those being the other two quadratic subfields of the Hilbert class field) and the second when p is inert in those two fields. To sum up:

$$p \begin{cases} \text{is ramified} & \text{if } p \in \{2,5\}, \\ \text{splits into principal primes} & \text{if } p \equiv 1,9 \pmod{20}, \\ \text{splits into non-principal primes} & \text{if } p \equiv 3,7 \pmod{20}, \\ \text{is inert} & \text{if } p \equiv 11,13,17,19 \pmod{20}. \end{cases}$$

Notation. When p is inert or ramified, we write $\mathfrak{p}_p$ for the prime of $\mathfrak{O}$ above p. When p is split, we write $\langle p\rangle = \mathfrak{p}_{p,a}\mathfrak{p}_{p,b}$, where $\mathfrak{p}_{p,a}$ is the conjugate with the lower value of "b" when written in standard form. For example, $\mathfrak{p}_{3a} = [3, 1+\sqrt{-5}]$ and $\mathfrak{p}_{3b} = [3, 2+\sqrt{-5}]$.

For convenience, we record some information about small primes in k in Tables 9.1 and 9.2 below. Table 9.1 gives, for each prime $p < 400$ which splits into principal primes, both a $\mathbb{Z}$-basis and a principal generator of $\mathfrak{p}_{p,a}$. Table 9.2 gives, for each prime $p < 180$ which splits into non-principal primes, a $\mathbb{Z}$-basis of $\mathfrak{p}_{p,a}$ and principal generators of $\mathfrak{p}_2\mathfrak{p}_{p,a}$ and $\mathfrak{p}_{3a}\mathfrak{p}_{p,a}$.

The last two columns of Table 9.2 will be useful in §9.7; an efficient way of obtaining them is via the theory of positive-definite binary quadratic forms due to C. F. Gauß, as follows. The two reduced forms of discriminant -20 are $f_1(x, y) = x^2 + 5y^2$ (the norm form) and $f_2(x, y) = 2x^2 + 2xy + 3y^2$, with composition law

$$\begin{aligned} f_2(x,y)f_2(u,v) &= f_1(2xu + xv + yu + 3yv, xv - yu) \\ &= f_1(2xu + xv + yu - 2yv, xv + yu + yv). \end{aligned}$$

A prime splits (or ramifies) into principal primes if it is represented by f_1 and into non-principal primes if it is represented by f_2. In the latter case, we find $u, v \in \mathbb{Z}$ (as shown in Table 9.2) such that $p = f_2(u, v)$. Since $2 = f_2(1, 0)$, we have $2p = f_1(2u + v, v)$. Exactly one of $2uv + v \pm v\sqrt{-5}$ lies in $\mathfrak{p}_{p,a}$ and is therefore a principal generator of $\mathfrak{p}_2\mathfrak{p}_{p,a}$. Similarly, $3 = f_2(0, 1)$, so $3p = f_1(u+3v, u) = f_1(u-2v, u+v)$ and the four elements $u+3v \pm u\sqrt{-5}$ and $u - 2v \pm (u + v)\sqrt{-5}$, in some order, are generators of $\mathfrak{p}_{3a}\mathfrak{p}_{p,a}$, $\mathfrak{p}_{3a}\mathfrak{p}_{p,b}$, $\mathfrak{p}_{3b}\mathfrak{p}_{p,a}$ and $\mathfrak{p}_{3b}\mathfrak{p}_{p,b}$. Of these four, only $u + 3v + u\sqrt{-5}$ and $u - 2v + (u + v)\sqrt{-5}$ lie in $\mathfrak{p}_{3a}$, so of those two, that one lying in $\mathfrak{p}_{p,a}$ is the desired generator of $\mathfrak{p}_{3a}\mathfrak{p}_{p,a}$.

p	$\mathfrak{p}_{p,a}$	generator
5	$[5, w]$	w
29	$[29, 13+w]$	$3-2w$
41	$[41, 6+w]$	$6+w$
61	$[61, 19+w]$	$4-3w$
89	$[89, 23+w]$	$3+4w$
101	$[101, 46+w]$	$9-2w$
109	$[109, 39+w]$	$8+3w$
149	$[149, 12+w]$	$12+w$
181	$[181, 30+w]$	$1-6w$
229	$[229, 37+w]$	$7-6w$
241	$[241, 85+w]$	$14+3w$
269	$[269, 110+w]$	$12+5w$
281	$[281, 41+w]$	$6+7w$
349	$[349, 56+w]$	$13-6w$
389	$[389, 165+w]$	$12-7w$
$w=\sqrt{-5}$		

Table 9.1: Split principal primes of $\mathbb{Q}(\sqrt{-5})$

p	$\mathfrak{p}_{p,a}$	(u,v)	$\mathfrak{p}_2\mathfrak{p}_{p,a}$	$\mathfrak{p}_{3a}\mathfrak{p}_{p,a}$
2	$[2, 1+w]$	$1, 0$	2	$1+w$
3	$[3, 1+w]$	$0, 1$	$1+w$	$2-w$
7	$[7, 3+w]$	$1, 1$	$3+w$	$1-2w$
23	$[23, 8+w]$	$-1, 3$	$1+3w$	$7-2w$
43	$[43, 9+w]$	$4, 1$	$9+w$	$2+5w$
47	$[47, 18+w]$	$2, 3$	$7+3w$	$4-5w$
67	$[67, 14+w]$	$-1, 5$	$3+5w$	$11-4w$
83	$[83, 24+w]$	$4, 3$	$11-3w$	$13+4w$
103	$[103, 43+w]$	$2, 5$	$9+5w$	$8-7w$
107	$[107, 40+w]$	$5, 3$	$13+3w$	$1-8w$
127	$[127, 54+w]$	$-2, 7$	$3-7w$	$19-2w$
163	$[163, 22+w]$	$1, 7$	$9-7w$	$22+w$
167	$[167, 50+w]$	$7, 3$	$17-3w$	$16+7w$
$w=\sqrt{-5}$				

Table 9.2: Non-principal primes of $\mathbb{Q}(\sqrt{-5})$

9.2 Characters

In the theory of modular forms for $\Gamma_0(N)$ over $\mathbb{Q}$, an important rôle is played by Dirichlet characters modulo N, i.e. by characters of $(\mathbb{Z}/N\mathbb{Z})^\times$; thus, one may have modular forms with character, and one may twist forms by such characters (see §2.1). In the general adelic theory, this rôle is taken by quasicharacters of the idele class group; for our purposes, these are best thought of as characters of ray class groups (see §5.1.5). Thus, we may have forms with such a character, and we may twist forms by such characters. As in the classical case, the twist of a form f by a character χ will be denoted $f * \chi$ (see §2.1.4). Twisting will be discussed further in §9.7.

9.2.1 Plusforms and minusforms

The modular forms we compute in this thesis are precisely those whose character is unramified (see §6.2.4 and [Kur78]). For fields k of class number 2 there are just two unramified characters (see Example 1 of §9.7 below), namely the trivial character and the character ν given on primes by

$$\mathfrak{p} \mapsto \begin{cases} +1 & \text{if } \mathfrak{p} \text{ is principal, and} \\ -1 & \text{otherwise.} \end{cases} \tag{9.1}$$

When $h(k) = 2$, a form with trivial character will be called a "plusform" and a form with character ν a "minusform".

Warning. The words "plusform" and "minusform" also occur in the theses of Cremona and Whitley [Cre81, Whi90], but with quite a different meaning, discussed in §9.2.2 below. All the forms in this thesis are "plusforms" in their sense, so we use the same language to make a different distinction.

9.2.2 GL(2) versus SL(2)

In their doctoral theses [Cre81, Whi90], Cremona and Whitley take as the starting point of the theory of modular forms the group SL(2), rather than GL(2), and set out to compute forms for $PS\Gamma_0(\mathfrak{n})$. The choice of SL(2) has certain technical disadvantages. Firstly, it then unclear how to bring characters into the theory, since, as Gelbart writes, "the existence of a non-trivial centre in GL(2) makes it the natural habitat for forms with non-trivial character" [Gel75, Remark 3.8]. Secondly, Cremona was able to define Hecke operators T_π for prime elements π, but found it "impossible, in general, to define an operator $T_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$, since the definition depends on the choice of generator for $\mathfrak{p}$" [Cre81, p.38]. To make progress, Cremona introduced the so-called "main involution" J given by $f \mapsto f\big|\left(\begin{smallmatrix}\epsilon & 0\\ 0 & 1\end{smallmatrix}\right)$, where ϵ generates $\mathfrak{O}^\times$; in Cremona's language, a "plusform" is a form for $\mathrm{PS}\Gamma_0(\mathfrak{n})$ such that $Jf = f$, whilst a "minusform" has $Jf = -f$. An easy calculation gives $T_{\epsilon\pi} = JT_\pi$, so that for plusforms the Hecke operators *are* independent of the choice of generator. It was only the plusforms that corresponded to elliptic curves, and minusforms could always be obtained from plusforms by twisting (specifically, by twisting by a character χ of $(\mathfrak{O}/\mathfrak{m})^\times$ satisfying $\chi(\epsilon) = -1$; to preserve plusforms, one needs $\chi(\epsilon) = 1$, which is precisely why it is characters of $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ which occur in this thesis).

It clarifies matters to adopt a slightly different viewpoint. In the classical theory, it is well-known that the space of forms for $\Gamma_1(N)$ decomposes as the sum over the characters ψ of the quotient $\Gamma_0(N)/\Gamma_1(N)$ of the spaces of forms for $\Gamma_0(N)$ with character ψ [Kob84, Prop.28]. Cremona's plus- and minusforms are another example of this rather general phenomenon. Thus, the space of forms for $\mathrm{PS}\Gamma_0(\mathfrak{n})$ is the sum of the spaces of forms for $\mathrm{P}\Gamma_0(\mathfrak{n})$ over the characters of the quotient $\mathrm{P}\Gamma_0(\mathfrak{n})/\mathrm{PS}\Gamma_0(\mathfrak{n})$; this quotient is isomorphic to $\mathfrak{O}^\times/(\mathfrak{O}^\times)^2$, by Lemma 19, and always has order 2 for imaginary quadratic fields. A (Cremona) plusform is just a form for $\mathrm{P}\Gamma_0(\mathfrak{n})$ with trivial character, whilst a minusform is a form for $\mathrm{P}\Gamma_0(\mathfrak{n})$ with non-trivial character.

9.2.3 The rôle of $T_{\mathfrak{p},\mathfrak{p}}$

Let k be an algebraic number field with ring of integers $\mathfrak{O}$, and let $\mathfrak{n}$ be an integral ideal of $\mathfrak{O}$. Let $J^\mathfrak{n}$ be the group of fractional ideals coprime to $\mathfrak{n}$, and let $P^\mathfrak{n}$ be the group of principal fractional ideals having a generator a such that $a \equiv 1 \pmod{\mathfrak{n}}$. Thus $J^\mathfrak{n}/P^\mathfrak{n}$ is the ray class group modulo $\mathfrak{n}$. Let ψ be a character of $J^\mathfrak{n}/P^\mathfrak{n}$ (or more generally, in view of the last part of Proposition 122 below, a character of $J^\mathfrak{m}/P^\mathfrak{m}$ where $\mathfrak{m} \mid \mathfrak{n}$), and let χ be the character of $(\mathfrak{O}/\mathfrak{n})^\times/\mathfrak{O}^\times$ induced in the manner of Lemma 71. Finally, let $S = S_0(\mathfrak{n}, \psi)$ be the space of cuspforms of level $\mathfrak{n}$ and character ψ. We shall use the operators $T_{\mathfrak{a},\mathfrak{a}}$ for $\mathfrak{a}$ coprime to $\mathfrak{n}$ to construct a representation of $J^\mathfrak{n}/P^\mathfrak{n}$ on S, and we claim that $J^\mathfrak{n}/P^\mathfrak{n}$ acts on S via the character ψ; this is the analogue of the result that $T_{n,n}f = \chi(n)f$ when $k = \mathbb{Q}$ [Kob84, Prop. 35].

Given $\mathfrak{a}$, coprime to $\mathfrak{n}$, there is $d \in \mathbb{N}$ such that $\mathfrak{a}^d$ is principal, say $\mathfrak{a}^d = \langle a \rangle$; raising to a further power if necessary, we may assume that $a \equiv 1 \pmod{\mathfrak{n}}$. By Proposition 103(ii), $(T_{\mathfrak{a},\mathfrak{a}})^d = T_{\langle a\rangle,\langle a\rangle}$; by (7.1), this operator maps each lattice Λ to $a^{-1}\Lambda$. Thus, for $F \in S$,

$$\begin{aligned} F\big|(T_{\mathfrak{a},\mathfrak{a}})^d &= F\big|\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)^{-1} \\ &= \chi(a)F && \text{by (6.10)} \\ &= F && \text{since } a \equiv 1 \pmod{\mathfrak{n}}. \end{aligned}$$

It follows that $F \mapsto F\big|T_{\mathfrak{a},\mathfrak{a}}$ defines an automorphism of S, which we denote by $\tau(\mathfrak{a})$. By Proposition 103(ii) again, $\tau(\mathfrak{a}\mathfrak{b}) = \tau(\mathfrak{a})\tau(\mathfrak{b})$, and by the calculation above, $\tau(\mathfrak{a}) = 1$ for $\mathfrak{a} \in P^\mathfrak{n}$. Thus τ is a representation of $J^\mathfrak{n}/P^\mathfrak{n}$ on S. Since $J^\mathfrak{n}/P^\mathfrak{n}$ is abelian, its irreducible characters are one-dimensional and the operators $T_{\mathfrak{a},\mathfrak{a}}$ on S are diagonalisable. Since the $T_\mathfrak{a}$ and $T_{\mathfrak{a},\mathfrak{a}}$ for $\mathfrak{a}$ coprime to $\mathfrak{n}$ commute pairwise, they are simultaneously diagonalisable, and S has a basis of simultaneous eigenforms.

If F is such a form, then certainly $F\big|T_{\langle a\rangle,\langle a\rangle} = \chi(a)F$, by the calculation above. In this formulation, proving that $F\big|T_{\mathfrak{a},\mathfrak{a}} = \psi(\mathfrak{a})F$ in general is slightly tricky, since the operator permutes the components of F; note that $T_{\mathfrak{a},\mathfrak{a}}$ takes $\mathfrak{p}_i \oplus \mathfrak{O}$ to $\mathfrak{a}^{-1}\mathfrak{p}_i \oplus \mathfrak{a}^{-1}$, which is isomorphic to $\mathfrak{p}_j \oplus \mathfrak{O}$, where j is defined by $cl(\mathfrak{p}_j) = cl(\mathfrak{a}^{-2}\mathfrak{p}_i)$; on the other hand, it is almost immediate in the adelic formulation, since $T_{\mathfrak{a},\mathfrak{a}}$ is then given by a matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, where $a \in k_\mathbb{A}$ is an adele with $il(a) = \mathfrak{a}$, and condition (B) of §6.1 gives what we want. We omit the details.

Of course, if $\mathfrak{a}^2$ is principal, then $i = j$. This means that $T_{\mathfrak{a},\mathfrak{a}}$ can be computed on each component separately. In particular, on the principal component one merely needs a matrix giving an isomorphism $\mathfrak{O} \oplus \mathfrak{O} \to \mathfrak{a} \oplus \mathfrak{a}$; such a matrix is easily computed. When $h(k) = 2$, moreover, since we are restricting to the case $\psi \in \{1, \nu\}$, we only need to compute $T_{\mathfrak{p},\mathfrak{p}}$ for one (good) non-principal prime to determine the character of our newforms.

9.3 Complex conjugation

Let $g \in \mathrm{GL}(2,\mathbb{C})$ and $(z,t) \in \mathfrak{H}_3$, so $g \cdot (z,t) = (z',t')$ as given by (3.12). Writing $\bar{g}$ for the complex conjugate of g, we see at once that $\bar{g} \cdot (\bar{z},t) = (\bar{z'},t')$. It follows that the conjugation action $(z,t) \mapsto (\bar{z},t)$ on $\mathfrak{H}_3$ induces a homeomorphism

$$c\colon \Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3 \to \Gamma_0(\bar{\mathfrak{n}})\backslash\mathfrak{H}_3. \tag{9.2}$$

By functoriality, there is an induced A-linear isomorphism

$$c\colon H_n\bigl(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3, A\bigr) \to H_n\bigl(\Gamma_0(\bar{\mathfrak{n}})\backslash\mathfrak{H}_3, A\bigr) \tag{9.3}$$

of homology, for any coefficient ring A. To make this more explicit, write $C = (C_n, \partial)$ and $C' = (C'_n, \partial')$ for the homology chain complexes attached to $\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3$ and $\Gamma_0(\bar{\mathfrak{n}})\backslash\mathfrak{H}_3$. The map (9.2) induces isomorphisms $c_n\colon C_n \to C'_n$ which respect the boundary maps, i.e. satisfy $\partial' \circ c_n = c_{n-1} \circ \partial$; thus we have a chain isomorphism from C to C', inducing (9.3). For $n = 1$ we can give the map explicitly in terms of modular symbols:

$$\{\alpha,\beta\}_{\Gamma_0(\mathfrak{n})} \mapsto \{\bar{\alpha},\bar{\beta}\}_{\Gamma_0(\bar{\mathfrak{n}})}. \tag{9.4}$$

The conjugation map is useful because it behaves well with respect to Hecke operators, in the following sense. Write $T(\mathfrak{a},\mathfrak{n})$ for the Hecke operator $T_\mathfrak{a}$ at level $\mathfrak{n}$, and $\overline{T(\mathfrak{a},\mathfrak{n})}$ for its "conjugate", i.e. for the formal linear combination of matrices obtained by conjugating each matrix in $T(\mathfrak{a},\mathfrak{n})$. Inspection of the matrices making up $T(\mathfrak{a},\mathfrak{n})$ shows that (formally) $\overline{T(\mathfrak{a},\mathfrak{n})} = T(\bar{\mathfrak{a}},\bar{\mathfrak{n}})$, because complex conjugation turns a list of residues modulo $\mathfrak{a}$ into one modulo $\bar{\mathfrak{a}}$ and turns a congruence condition modulo $\mathfrak{n}$ into one modulo $\bar{\mathfrak{n}}$. Thus, if $v \in H_1\bigl(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3, \mathbb{C}\bigr)$ is an eigenvector with $T(\mathfrak{a},\mathfrak{n})v = \lambda v$, then

$$T(\bar{\mathfrak{a}},\bar{\mathfrak{n}})c(v) = c\bigl(T(\mathfrak{a},\mathfrak{n})v\bigr) = \lambda c(v).$$

Thus, to every eigenspace in $H_1\bigl(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3\bigr)$ there corresponds one in $H_1\bigl(\Gamma_0(\bar{\mathfrak{n}})\backslash\mathfrak{H}_3\bigr)$ with the eigenvalues for $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ interchanged. By duality,[1] to every modular form f at level $\mathfrak{n}$ there corresponds a form at level $\bar{\mathfrak{n}}$ with the eigenvalues for $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ interchanged; we denote this "conjugate" form by $\bar{f}$.

[1] A more detailed argument, taking account of all h homology pieces, can be given. Note that c takes a form for $(\Gamma_0(\mathfrak{n}), R)$, in the notation of §6.2.3, to one for $(\Gamma_0(\bar{\mathfrak{n}}), R')$ for some R' different from R in general.

As an illustration, we give two examples taken from our tables of newforms in §9.6 below.

Example 1. At level $\mathfrak{n} = \mathfrak{p}_2\mathfrak{p}_{3b}\mathfrak{p}_{7b}$ there is a newform we denote f_8; consequently, $\bar{f}_8$ is a newform at level $\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{7a}$. The first few eigenvalues of f_8 and $\bar{f}_8$ are shown in Table 9.3 below. This is a typical example; the eigenvalues at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ appear to be quite unrelated.

Example 2. A more interesting example is provided by the newform f_5 at level $(\mathfrak{p}_{3a})^2\mathfrak{p}_{3b}$ and its conjugate $\bar{f}_5$ at level $\mathfrak{p}_{3a}(\mathfrak{p}_{3b})^2$; see Table 9.3. The eigenvalues at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ agree up to sign. The explanation is that both forms recur as oldforms at level $(\mathfrak{p}_{3a})^2(\mathfrak{p}_{3b})^2$, where they are related by twisting. See §9.7 for further details.

	5	29a	29b	41a	41b	61a	61b	89a	89b	101a	101b	109a	109b
f_8	1	0	−5	7	12	−8	−8	10	−15	−8	12	5	10
$\bar{f}_8$	1	−5	0	12	7	−8	−8	−15	10	12	−8	10	5
f_5	0	8	−8	2	−2	−6	−6	−6	6	−4	4	−2	−2
$\bar{f}_5$	0	−8	8	−2	2	−6	−6	6	−6	4	−4	−2	−2

Table 9.3: Two newforms and their conjugates

Now assume that $\mathfrak{n} = \bar{\mathfrak{n}}$. In this case, the complex conjugation map c defines an involution on $H_1(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3)$, which we can compute explicitly (using (9.4) and the same procedures used for Hecke operators).

Warning. In general, c does *not* commute with all the Hecke operators; in particular, it cannot be used to split off eigenspaces in the way that the Atkin-Lehner W-involutions and the "complex conjugation" involution (induced by the map $z \mapsto -\bar{z}$ on the upper half plane) are used in [Cre97].

If f is a newform at a self-conjugate level $\mathfrak{n}$, then so is $\bar{f}$; the effect of conjugation on all such newforms within the range of our tables is shown in Table 9.4. In most cases $\bar{f} = f$, but occasionally $\bar{f} = f * \nu$ (the two cases cannot be distinguished by computing c on $H_1(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3)$ alone, of course). Other behaviour is also possible. Thus, at level $\mathfrak{n} = \langle 11 \rangle$, the newforms h_2, $\bar{h}_2$, $h_2 * \nu$ and $\bar{h}_2 * \nu$ are all distinct; in fact, $\bar{h}_2 = h_2^{\sigma}$, where

σ is the automorphism of $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$ given by $\sqrt{-2} \mapsto \sqrt{-2}$ and $\sqrt{-3} \mapsto -\sqrt{-3}$. At level $\mathfrak{n} = (\mathfrak{p}_2)^9$, the newforms h_6, $\bar{h_6}$, $h_6 * \nu$ and $\bar{h_6} * \nu$ are all distinct; in fact, $\bar{h_6} = h_6 * \xi$, where ξ is the character given by (9.8).

	plusforms	minusforms
$\bar{f} = f$	$f_4, f_7, f_9, f_{11}, f_{16}, f_{18}, f_{22}, f_{25}, f_{30}$	$f_1, f_3, f_6, f_{10}, f_{12}, f_{15}, f_{19}, g_2, h_1, f_{26}, h_3$
$\bar{f} = f * \nu$	f_2	f_{20}, f_{21}
other	h_6	h_2

Table 9.4: Effect of conjugation on newforms at levels $\mathfrak{n} = \bar{\mathfrak{n}}$ with $\mathbf{N}(\mathfrak{n}) \leq 135$

9.4 Decomposition of $V(\mathfrak{n})$

The following result is very important, in view of the well-known facts from linear algebra that Hermitian operators are diagonalisable, and that pairwise commuting diagonalisable operators are simultaneously diagonalisable.

Proposition 121. *Let χ be an unramified character, let $f, g \in S(\mathfrak{n}, \chi)$, let $\mathfrak{p}$ be a prime with $\mathfrak{p} \nmid \mathfrak{n}$ and let $\langle\,,\,\rangle$ denote the natural Hermitian inner product* (4.5) *on $S(\mathfrak{n}, \chi)$. Then*

$$\langle T_\mathfrak{p} f, g\rangle = \chi(\mathfrak{p})\langle f, T_\mathfrak{p} g\rangle. \tag{9.5}$$

Let $c_\mathfrak{p}$ denote either square root of $\overline{\chi(\mathfrak{p})}$. Then $c_\mathfrak{p} T_\mathfrak{p}$ is a Hermitian operator on the complex vector space $S(\mathfrak{n}, \chi)$. If $f \neq 0$ and $T_\mathfrak{p} f = a_\mathfrak{p} f$, then $a_\mathfrak{p} \in \mathbb{R}$ if $\chi(\mathfrak{p}) = 1$ and $a_\mathfrak{p} \in i\mathbb{R}$ if $\chi(\mathfrak{p}) = -1$.

Proof. We omit to prove (9.5), which is the analogue of the result for $k = \mathbb{Q}$ [Kob84, Prop. 48]. Since $c_\mathfrak{p}\chi(\mathfrak{p}) = c_\mathfrak{p}\bar{c_\mathfrak{p}}^2 = \bar{c_\mathfrak{p}}$, it follows, as in [Kob84, Prop. 50], that $\langle c_\mathfrak{p} T_\mathfrak{p} f, g\rangle = c_\mathfrak{p}\langle T_\mathfrak{p} f, g\rangle = c_\mathfrak{p}\chi(\mathfrak{p})\langle f, T_\mathfrak{p} g\rangle = \bar{c_\mathfrak{p}}\langle f, T_\mathfrak{p} g\rangle = \langle f, c_\mathfrak{p} T_\mathfrak{p} g\rangle$, showing that $c_\mathfrak{p} T_\mathfrak{p}$ is Hermitian. Finally, if $T_\mathfrak{p} f = a_\mathfrak{p} f$, then a similar calculation using (9.5) gives $a_\mathfrak{p}\langle f, f\rangle = \chi(\mathfrak{p})\bar{a_\mathfrak{p}}\langle f, f\rangle$. For $f \neq 0$ this implies $a_\mathfrak{p} = \chi(\mathfrak{p})\bar{a_\mathfrak{p}}$, and the result follows. □

Hence $S(\mathfrak{n}, \chi)$, as a vector space over $\mathbb{C}$, has a basis whose elements are eigenforms for all the $T_\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{n}$. By duality, the same is true for each summand of $H_1(\bar{X}_0(\mathfrak{n}), \mathbb{C})$

when decomposed according to the characters (rather than the ideal classes; recall that $H_1(\bar{X}_0(\mathfrak{n}), \mathbb{C})$ was defined (in §6.2.4) as a sum over ideal classes).

Let $V_i(\mathfrak{n}) = H_1(\bar{X}_{\Gamma_0^i(\mathfrak{n})}, \mathbb{Q})$ (in the notation of §6.2.4). For simplicity, assume that $h = 2$, so by duality, there is an isomorphism

$$S(\mathfrak{n}, 1) \oplus S(\mathfrak{n}, \nu) \cong V_1(\mathfrak{n}) \oplus V_2(\mathfrak{n}),$$

where the V_i are viewed as $\mathbb{C}$-vector spaces by extension of scalars. It will be enough to work with the piece $V(\mathfrak{n}) = V_1(\mathfrak{n})$ corresponding to the principal class; it decomposes as a direct sum

$$V(\mathfrak{n}) = V^+(\mathfrak{n}) \oplus V^-(\mathfrak{n}),$$

where $V^+(\mathfrak{n})$ corresponds to forms with trivial character ("plusforms", elements of $S(\mathfrak{n}, 1)$) and $V^-(\mathfrak{n})$ corresponds to forms with non-trivial unramified character ("minusforms", elements of $S(\mathfrak{n}, \nu)$); see §9.2.

Each of $V^\pm(\mathfrak{n})$ is a module for the algebra, $\mathbb{T}$, say, of Hecke operators $T_\mathfrak{a}$ with $\mathfrak{a}$ principal and coprime to $\mathfrak{n}$, and by the remarks above, it has a basis of simultaneous eigenvectors for the elements of $\mathbb{T}$ (with eigenvalues and eigenvectors defined over the algebraic closure of $\mathbb{Q}$). We have computed the spaces $V^\pm(\mathfrak{n})$ in terms of a particular basis consisting of $\mathbb{Z}$-linear combinations of modular symbols with endpoints at the cusps; that this basis is the natural one to use is related to the appropriate analogue of the Manin-Drinfeld theorem, see [Kur78, Lemmas 6 and 8] (in particular, with respect to this basis the Hecke operators are given by matrices with entries in $\mathbb{Z}$). The eigenvalues of the $T_\mathfrak{p}$ are certainly algebraic integers, but they need not be rational integers, and the change of basis to a basis of eigenvectors need not be defined over $\mathbb{Q}$. As far as the rational structure is concerned, then, several kinds of behaviour are possible, as we now explain.

Decompose $V^\pm(\mathfrak{n}) = \oplus V^{(i)}$, say, where each $V^{(i)}$ is $\mathbb{T}$-invariant and irreducible. As we remarked elsewhere, finitely many Hecke operators suffice to effect this splitting. Each $V^{(i)}$ is characterised by its sequence of eigenvalues. If the sequence already occurs at a level dividing $\mathfrak{n}$, the component $V^{(i)}$ is called "old", and otherwise, "new".

Let v generate a 1-dimensional $V^{(i)}$. Then the eigenvalues for v of $T_\mathfrak{p}$ (for $\mathfrak{p}$ principal) and of $(T_\mathfrak{p})^2$ and $T_{\mathfrak{pq}}$ (for $\mathfrak{p}$ and $\mathfrak{q}$ non-principal) are necessarily rational. There are two possibilities:

(i) The eigenvalues for non-principal primes also lie in $\mathbb{Q}$; we say that such a factor is "of type f".

(ii) The eigenvalues for non-principal primes lie not in $\mathbb{Q}$, but in a quadratic extension of $\mathbb{Q}$; such a factor called "of type g".

Two-dimensional factors will all be called "of type h" (although there is a similar distinction, see §9.6).

Table 9.5 below lists $d(\mathfrak{n}) = \dim V(\mathfrak{n})$ for all levels $\mathfrak{n}$ of norm up to 135; levels with $\dim V(\mathfrak{n}) = 0$ are omitted, and in view of §9.3, only one level is listed from each pair of conjugate levels. For each level, both its prime factorisation and the coefficients (a, b, c) of its "standard form" $[a, b + \sqrt{-5}]c$ are given.

Notice that if $\mathfrak{m} \mid \mathfrak{n}$, then $d(\mathfrak{m}) \leq d(\mathfrak{n})$, because newforms at level $\mathfrak{m}$ give rise to spaces of oldforms at level $\mathfrak{m}$; for more precise statements, see §9.5.

The table also shows the decomposition of $V(\mathfrak{n})$ into eigenspaces for the Hecke algebra. For the levels $\mathfrak{n}$ in the range of the tables, the irreducible components have dimension 1 or 2, so they are all of "types" f, g or h. When a space is "new", its multiplicity is one, and it is denoted by a boldface letter according to "type" ($\mathbf{f}_1$, $\mathbf{f}_2$, $\mathbf{g}_1$, and so forth) together with a superscript to indicate the character (either plus or minus). When the same sequence of eigenvalues recurs in the oldspace, it is written in ordinary "maths italic" (f_1, f_2, g_1 and so on) and the table indicates the multiplicity with which it occurs; thus the oldspace at level $\mathfrak{n} = (\mathfrak{p}_2)^4$ with eigenvalues f_1 has dimension two. (When verifying that $d(\mathfrak{n})$ is fully accounted for, the reader should recall that an h needs to be counted with weight two!)

level			homology	
$\mathfrak{n}$	a, b, c	$\mathbf{N}(\mathfrak{n})$	$d(\mathfrak{n})$	$V(\mathfrak{n})$
$\mathfrak{p}_2^3$	$2, 1, 2$	8	1	$\mathbf{f}_1^-$
$\mathfrak{p}_2^4$	$1, 0, 4$	16	3	$2f_1 + \mathbf{f}_2^+$
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	$2, 1, 3$	18	1	$\mathbf{f}_3^-$
$\mathfrak{p}_2^2\mathfrak{p}_5$	$5, 0, 2$	20	1	$\mathbf{f}_4^+$
$\mathfrak{p}_2^3\mathfrak{p}_{3a}$	$6, 1, 2$	24	2	$2f_1$
$\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$	$3, 1, 3$	27	1	$\mathbf{f}_5^-$
$\mathfrak{p}_2^5$	$2, 1, 4$	32	5	$3f_1 + 2f_2$
$\mathfrak{p}_2^2\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	$1, 0, 6$	36	3	$2f_3 + \mathbf{f}_6^-$
$\mathfrak{p}_2^3\mathfrak{p}_5$	$10, 5, 2$	40	5	$2f_1 + 2f_4 + \mathbf{f}_7^+$
$\mathfrak{p}_2\mathfrak{p}_{3b}\mathfrak{p}_{7b}$	$42, 11, 1$	42	1	$\mathbf{f}_8^-$
$\mathfrak{p}_{3b}^2\mathfrak{p}_5$	$45, 20, 1$	45	1	$\mathbf{g}_1^-$
$\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	$5, 0, 3$	45	1	$\mathbf{f}_9^+$
$\mathfrak{p}_2^4\mathfrak{p}_{3a}$	$3, 1, 4$	48	6	$4f_1 + 2f_2$
$\mathfrak{p}_{7a}\mathfrak{p}_{7b}$	$1, 0, 7$	49	1	$\mathbf{f}_{10}^-$
$\mathfrak{p}_2\mathfrak{p}_5^2$	$2, 1, 5$	50	2	$\mathbf{f}_{11}^+ + \mathbf{f}_{12}^-$
$\mathfrak{p}_2\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$	$6, 1, 3$	54	4	$2f_3 + 2f_5$
$\mathfrak{p}_2^3\mathfrak{p}_{7a}$	$14, 3, 2$	56	3	$2f_1 + \mathbf{f}_{13}^-$
$\mathfrak{p}_2^2\mathfrak{p}_{3b}\mathfrak{p}_5$	$15, 5, 2$	60	3	$2f_4 + \mathbf{f}_{14}^-$
$\mathfrak{p}_2^6$	$1, 0, 8$	64	9	$4f_1 + 3f_2 + \mathbf{f}_{15}^- + \mathbf{f}_{16}^+$
$\mathfrak{p}_{3b}\mathfrak{p}_{23a}$	$69, 8, 1$	69	1	$\mathbf{f}_{17}^+$
$\mathfrak{p}_2^3\mathfrak{p}_{3a}^2$	$18, 7, 2$	72	3	$3f_1$
$\mathfrak{p}_2^3\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	$2, 1, 6$	72	11	$4f_1 + 3f_3 + 2f_6 + \mathbf{f}_{18}^+ + \mathbf{f}_{19}^-$
$\mathfrak{p}_2^4\mathfrak{p}_5$	$5, 0, 4$	80	13	$4f_1 + 2f_2 + 3f_4 + \mathbf{f}_{20}^- + 2f_7 + \mathbf{f}_{21}^-$
$\mathfrak{p}_{3a}\mathfrak{p}_{3b}^3$	$9, 2, 3$	81	2	$2\bar{f}_5$

Table 9.5: Decomposition of $V(\mathfrak{n})$ — part 1 of 2

level			homology	
$\mathfrak{n}$	a, b, c	$\mathbf{N}(\mathfrak{n})$	$d(\mathfrak{n})$	$V(\mathfrak{n})$
$\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}^2$	$1, 0, 9$	81	5	$2f_5 + 2\bar{f}_5 + \mathbf{g}_2^-$
$\mathfrak{p}_2^2\mathfrak{p}_{3a}\mathfrak{p}_{7a}$	$21, 10, 2$	84	2	$2\bar{f}_8$
$\mathfrak{p}_{89a}$	$89, 23, 1$	89	1	$\mathbf{g}_3^+$
$\mathfrak{p}_2\mathfrak{p}_{3a}^2\mathfrak{p}_5$	$90, 25, 1$	90	2	$2\bar{g}_1$
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	$10, 5, 3$	90	5	$2f_3 + 2f_9 + \mathbf{f}_{22}^+$
$\mathfrak{p}_2^5\mathfrak{p}_{3a}$	$6, 1, 4$	96	10	$6f_1 + 4f_2$
$\mathfrak{p}_2\mathfrak{p}_{7a}^2$	$98, 17, 1$	98	2	$\mathbf{f}_{23}^+ + \mathbf{f}_{24}^-$
$\mathfrak{p}_2\mathfrak{p}_{7a}\mathfrak{p}_{7b}$	$2, 1, 7$	98	5	$2f_{10} + \mathbf{f}_{25}^+ + \mathbf{h}_1^-$
$\mathfrak{p}_2^2\mathfrak{p}_5^2$	$1, 0, 10$	100	7	$2f_{11} + 2f_{12} + 2f_4 + \mathbf{f}_{26}^-$
$\mathfrak{p}_{101b}$	$101, 55, 1$	101	2	$\mathbf{g}_4^+ + \mathbf{g}_5^-$
$\mathfrak{p}_2^2\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$	$3, 1, 6$	108	10	$4f_3 + 3f_5 + 2f_6 + \mathbf{f}_{27}^+$
$\mathfrak{p}_2^4\mathfrak{p}_{7a}$	$7, 3, 4$	112	9	$4f_1 + 2f_2 + 2f_{13} + \mathbf{f}_{28}^+$
$\mathfrak{p}_2^2\mathfrak{p}_{29a}$	$29, 13, 2$	116	1	$\mathbf{f}_{29}^+$
$\mathfrak{p}_2^3\mathfrak{p}_{3b}\mathfrak{p}_5$	$30, 5, 2$	120	12	$4f_1 + 4f_4 + 2f_7 + 2f_{14}$
$\mathfrak{p}_{11}$	$1, 0, 11$	121	5	$\mathbf{f}_{30}^+ + \mathbf{h}_2^- + \mathbf{h}_3^-$
$\mathfrak{p}_{3b}\mathfrak{p}_{41a}$	$123, 47, 1$	123	2	$\mathbf{h}_4^+$
$\mathfrak{p}_2\mathfrak{p}_{3b}^2\mathfrak{p}_{7b}$	$126, 11, 1$	126	4	$2f_8 + \mathbf{f}_{31}^+ + \mathbf{f}_{32}^+$
$\mathfrak{p}_2\mathfrak{p}_{3a}^2\mathfrak{p}_{7b}$	$126, 25, 1$	126	1	$\mathbf{f}_{33}^+$
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_{7a}$	$14, 3, 3$	126	4	$2f_3 + 2\bar{f}_8$
$\mathfrak{p}_2^7$	$2, 1, 8$	128	11	$5f_1 + 4f_2 + f_{15} + f_{16}$
$\mathfrak{p}_{3b}^3\mathfrak{p}_5$	$135, 20, 1$	135	4	$2g_1 + \mathbf{h}_5^-$
$\mathfrak{p}_{3a}\mathfrak{p}_{3b}^2\mathfrak{p}_5$	$15, 5, 3$	135	6	$2\bar{f}_5 + 2g_1 + 2f_9$
$\mathfrak{p}_2^8$	$1, 0, 16$	256	19	see §9.7, Example 3
$\mathfrak{p}_2^9$	$2, 1, 16$	512	31	see §9.7, Example 3

Table 9.5 — part 2 of 2

9.5 Dimension of the oldspace

It would be interesting to develop Atkin-Lehner theory for modular forms over imaginary quadratic fields, and it should be possible to do so using modular points, as is done for the case $k = \mathbb{Q}$ in [Lan76, Chapter VIII], for example. Such a treatment would have to take account of the fact that the dimension of the oldspace is not always as high as one would expect: in particular, an oldform can occur with multiplicity one!

Recall that in the classical case, if $M \mid N$, then a newform f at level M gives rise at level N to an oldspace of dimension $\phi(N/M)$, where ϕ is the "divisor function" (i.e. $\phi(a)$ equals the number of natural numbers dividing a); to see this, one notes that for each t dividing N/M, the function $z \mapsto f(tz)$ is a modular form at level tM, hence at level N *a fortiori*, and that these functions are linearly independent.

In the case of an imaginary quadratic field, for ideals $\mathfrak{m}$ and $\mathfrak{n}$ with $\mathfrak{m} \mid \mathfrak{n}$, one might therefore expect a newform at level $\mathfrak{m}$ to give rise to an oldspace of dimension $\phi(\mathfrak{n}/\mathfrak{m})$, where $\phi(\mathfrak{a})$ now denotes the number of ideals dividing $\mathfrak{a}$.

Now consider Table 9.5. In nearly all cases, the dimension of the oldspace is as expected. For example, let $\mathfrak{m} = (\mathfrak{p}_2)^3$ and $\mathfrak{n} = (\mathfrak{p}_2)^5$. Then $\mathfrak{n}/\mathfrak{m}$ has the three factors 1, $\mathfrak{p}_2$ and $(\mathfrak{p}_2)^2$, and as expected the newform f_1 at level $\mathfrak{m}$ occurs with multiplicity three at level $\mathfrak{n}$.

However, there are exceptions; in the range of our table these are all caused by the newforms f_{15} and f_{16} at level $\mathfrak{m} = (\mathfrak{p}_2)^6$, which satisfy $f = f * \nu$. The induced oldspaces at levels $(\mathfrak{p}_2)^7$, $(\mathfrak{p}_2)^8$ and $(\mathfrak{p}_2)^9$ have dimensions 1, 2 and 2 respectively, rather than 2, 3 and 4. The oldspaces appear to grow at half the normal rate; for further details, see §9.7 (Example 3). Presumably, linear independence of some of the oldforms fails because all the eigenvalues at non-principal primes are zero, so that forms which "ought to be independent" are dependent after all.

9.6 Tables of newforms

In Table 9.5 we showed how $H_1(\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_3, \mathbb{Q})$ decomposes into modules for the Hecke algebra that are irreducible over $\mathbb{Q}$. One-dimensional modules were denoted by f or g, two-dimensional ones by h. We now pass to the corresponding newforms; to avoid needless repetition, we shall choose "representative" newforms as follows.

In general, a new eigenvector of type f corresponds to two newforms, which are twists of each other by the unramified character ν. We choose one arbitrarily, and denote it by the same symbol f; the other is then $f * \nu$. (Of course, if $f = f * \nu$, as happens for f_{15} and f_{16}, there is no choice to be made.) We only need to tabulate the eigenvalues of the representative form f, since those of $f * \nu$ are easily deduced (one simply negates the eigenvalues at non-principal primes).

Eigenvectors of type g are dealt with in the same way. For a module of type h, we make a choice v of eigenvector (defined over a real quadratic extension $F|\mathbb{Q}$) and then a choice of ν-twist. Let σ be the non-trivial Galois automorphism of $F|\mathbb{Q}$. The forms h and $h * \nu$ correspond to the eigenvector v, and there are two forms h^σ and $h^\sigma * \nu$ corresponding to the conjugate eigenvector v^σ. Note that F is real quadratic, by the Hermitian property of Hecke operators at principal primes. The eigenvalues at principal primes lie in F, and the eigenvalues at non-principal primes either in F (as for the plusforms h_4 and h_6) or in a quadratic extension F' of F (as for the minusforms h_1, h_2, h_3 and h_5). In our examples, $F'|\mathbb{Q}$ is always biquadratic (we do not know if this is so in general). The eigenvalues of h^σ are obtained from those of h by applying the automorphism σ (extended to $F'|\mathbb{Q}$ where necessary, one extension yielding h^σ and the other $h^\sigma * \nu$).

We now tabulate Hecke eigenvalues for the representative newforms chosen as described above. For each form, we list the eigenvalues of $T_\mathfrak{p}$ for the good principal primes with $\mathbf{N}(\mathfrak{p}) < 400$ and for the good non-principal primes with $\mathbf{N}(\mathfrak{p}) < 180$; an entry of "$*$" denotes a bad prime, and an entry of "?" a value we have not computed.

In Table 9.6 we give the plusforms of types f and g, and in Table 9.7 the minusforms of those types. In Table 9.8 we give the forms of type h (both plus and minus); we can always specify their eigenvalues in terms of a $\mathbb{Q}$-basis of two elements: for example, the eigenvalue of h_2 for $\mathfrak{p}_{23b}$ is $\sqrt{-2} - 3\sqrt{-3}$.

As predicted by Proposition 121, plusforms have real eigenvalues, whilst minusforms have real eigenvalues at principal primes and pure imaginary eigenvalues at non-principal primes.

$\mathfrak{n}$	$\mathbf{N}(\mathfrak{n})$		5	$29a$	$29b$	$41a$	$41b$	$61a$	$61b$	$89a$	$89b$
$\mathfrak{p}_2^4$	16	f_2	2	-2	-2	-2	-2	10	10	-6	-6
$\mathfrak{p}_2^2\mathfrak{p}_5$	20	f_4	$*$	6	6	6	6	2	2	-6	-6
$\mathfrak{p}_2^3\mathfrak{p}_5$	40	f_7	$*$	-2	-2	-6	-6	-2	-2	-6	-6
$\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	45	f_9	$*$	-2	-2	10	10	-2	-2	-6	-6
$\mathfrak{p}_2\mathfrak{p}_5^2$	50	f_{11}	$*$	0	0	-3	-3	2	2	15	15
$\mathfrak{p}_2^6$	64	f_{16}	-2	-10	-10	10	10	-10	-10	10	10
$\mathfrak{p}_{3b}\mathfrak{p}_{23a}$	69	f_{17}	-4	1	-6	9	-6	-8	-1	6	-10
$\mathfrak{p}_2^3\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	72	f_{18}	-2	6	6	-6	-6	-2	-2	-6	-6
$\mathfrak{p}_{89a}$	89	g_3	-2	-8	2	-10	-6	6	-2	$*$	-6
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	90	f_{22}	$*$	-6	-6	-6	-6	-10	-10	18	18
$\mathfrak{p}_2\mathfrak{p}_{7a}^2$	98	f_{23}	1	-1	-8	-2	-5	-8	0	-7	-8
$\mathfrak{p}_2\mathfrak{p}_{7a}\mathfrak{p}_{7b}$	98	f_{25}	0	-6	-6	6	6	8	8	-6	-6
$\mathfrak{p}_{101b}$	101	g_4	0	-10	0	2	-6	-10	14	-14	0
$\mathfrak{p}_2^2\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$	108	f_{27}	0	0	0	6	-6	-10	-10	18	-18
$\mathfrak{p}_2^4\mathfrak{p}_{7a}$	112	f_{28}	-3	3	-2	-2	3	10	-10	-11	4
$\mathfrak{p}_2^2\mathfrak{p}_{29a}$	116	f_{29}	-2	$*$	-6	-6	-10	-2	14	6	-6
$\mathfrak{p}_{11}$	121	f_{30}	1	0	0	-8	-8	12	12	15	15
$\mathfrak{p}_2\mathfrak{p}_{3b}^2\mathfrak{p}_{7b}$	126	f_{31}	3	0	9	-9	0	8	8	6	9
$\mathfrak{p}_2\mathfrak{p}_{3b}^2\mathfrak{p}_{7b}$	126	f_{32}	-3	-6	-3	-3	-6	-10	-10	-12	-3
$\mathfrak{p}_2\mathfrak{p}_{3a}^2\mathfrak{p}_{7b}$	126	f_{33}	3	6	3	3	6	-10	-10	12	3

Table 9.6: Plusforms of types f and g for $\mathbb{Q}(\sqrt{-5})$ — part 1 of 5

	101a	101b	109a	109b	11	149a	149b	13	181a	181b	229a	229b
f_2	6	6	−6	−6	−6	18	18	10	22	22	6	6
f_4	6	6	2	2	−22	−6	−6	−22	−10	−10	14	14
f_7	6	6	14	14	−6	−10	−10	−22	−10	−10	−26	−26
f_9	6	6	14	14	−6	22	22	−22	−10	−10	6	6
f_{11}	−18	−18	−10	−10	−13	0	0	−10	2	2	20	20
f_{16}	−2	−2	6	6	−22	14	14	10	−18	−18	30	30
f_{17}	0	−2	−11	−10	7	−7	−6	−19	4	−7	−6	−9
f_{18}	−18	−18	−2	−2	−6	14	14	−22	6	6	22	22
g_3	0	2	6	10	8	−20	−10	6	−10	−26	−2	26
f_{22}	18	18	−10	−10	−22	−6	−6	−22	14	14	−10	−10
f_{23}	−10	14	−2	11	3	8	17	9	2	12	−27	−13
f_{25}	0	0	2	2	−22	−18	−18	−10	20	20	−4	−4
g_4	−10	$*$	−2	10	6	6	−10	22	−14	−6	18	−26
f_{27}	12	−12	2	2	−10	−12	12	14	2	2	2	2
f_{28}	−4	−14	14	−1	19	18	−7	−15	−18	−8	21	11
f_{29}	−6	−2	−14	−6	−6	−10	6	−2	−18	−10	14	26
f_{30}	2	2	10	10	$*$	−10	−10	−10	7	7	15	15
f_{31}	12	0	−7	2	−13	−21	−18	−19	2	20	5	−13
f_{32}	6	0	−7	2	5	15	6	−1	−16	2	5	5
f_{33}	−6	0	−7	2	5	−15	−6	−1	−16	2	5	5

Table 9.6 — part 2 of 5

	$241a$	$241b$	$269a$	$269b$	$281a$	$281b$	17	$349a$	$349b$	19	$389a$	$389b$
f_2	22	22	−6	−6	−18	−18	34	−2	−2	−22	−30	−30
f_4	14	14	18	18	6	6	2	−10	−10	−22	−6	−6
f_7	2	2	14	14	10	10	−30	30	30	−22	6	6
f_9	−14	−14	14	14	−6	−6	−30	−2	−2	−22	6	6
f_{11}	17	17	0	0	−18	−18	−25	−10	−10	−13	30	30
f_{16}	−30	−30	−26	−26	10	10	−30	−10	−10	−38	−34	−34
f_{17}	−23	0	−4	−15	−22	31	23	1	−1	−20	23	−9
f_{18}	18	18	−10	−10	26	26	−30	30	30	−22	−2	−2
g_3	4	18	−10	−6	−18	16	−4	−10	−24	2	−6	30
f_{22}	2	2	−6	−6	18	18	2	−10	−10	−22	−6	−6
f_{23}	17	24	7	−10	2	16	−18	−30	−26	12	−2	−16
f_{25}	−10	−10	−12	−12	−6	−6	2	−28	−28	−34	18	18
g_4	0	10	2	−2	−14	22	20	−14	2	−12	8	−10
f_{27}	2	2	0	0	−6	6	14	−34	−34	26	24	−24
f_{28}	−23	−8	−21	14	12	−28	−16	18	−2	−2	30	0
f_{29}	10	−22	6	14	−22	−6	18	−2	−14	2	−2	6
f_{30}	−8	−8	10	10	−18	−18	−30	30	30	−38	−15	−15
f_{31}	−10	17	−6	9	30	6	−16	26	−10	20	−18	−6
f_{32}	8	−1	−6	21	12	24	20	−10	−10	−34	24	−18
f_{33}	8	−1	6	−21	−12	−24	20	−10	−10	−34	−24	18

Table 9.6 — part 3 of 5

	2	$3a$	$3b$	$7a$	$7b$	$23a$	$23b$	$43a$	$43b$	$47a$	$47b$	$67a$	$67b$
f_2	$*$	2	-2	2	-2	2	-2	-6	6	6	-6	14	-14
f_4	$*$	2	2	-2	-2	-6	-6	10	10	6	6	-2	-2
f_7	$*$	0	0	4	4	-4	-4	8	8	-4	-4	-8	-8
f_9	1	$*$	$*$	0	0	0	0	-4	-4	-8	-8	-12	-12
f_{11}	$*$	1	1	2	2	6	6	-4	-4	12	12	-13	-13
f_{16}	$*$	0	0	0	0	0	0	0	0	0	0	0	0
f_{17}	1	1	$*$	-2	-1	$*$	-7	-2	-5	11	4	10	-11
f_{18}	$*$	$*$	$*$	0	0	8	8	-4	-4	0	0	4	4
g_3	0	$2t$	$-t$	0	$-t$	$-4t$	$-5t$	$3t$	$-2t$	$9t$	$5t$	$-t$	$-5t$
f_{22}	$*$	$*$	$*$	4	4	0	0	4	4	0	0	4	4
f_{23}	$*$	0	3	$*$	3	6	-3	-6	-6	6	6	3	-12
f_{25}	$*$	2	2	$*$	$*$	0	0	-8	-8	12	12	4	4
g_4	t	$-t$	0	$2t$	$-t$	t	$-3t$	$6t$	$2t$	$-8t$	$-4t$	$2t$	$3t$
f_{27}	$*$	$*$	$*$	2	2	0	0	8	8	-12	12	-4	-4
f_{28}	$*$	2	3	$*$	3	2	-7	4	-4	-4	-6	-1	-4
f_{29}	$*$	2	0	0	-4	6	-2	-12	-2	-2	8	-10	10
f_{30}	2	1	1	2	2	1	1	6	6	-8	-8	7	7
f_{31}	$*$	1	$*$	-1	$*$	-3	0	-10	8	0	-12	-4	5
f_{32}	$*$	1	$*$	-1	$*$	-3	6	8	8	-6	0	-4	-13
f_{33}	$*$	$*$	2	1	$*$	-3	6	-8	-8	-6	0	4	13

$t = \sqrt{2}$

Table 9.6 — part 4 of 5

	$83a$	$83b$	$103a$	$103b$	$107a$	$107b$	$127a$	$127b$	$163a$	$163b$	$167a$	$167b$
f_2	-2	2	14	-14	-10	10	-6	6	2	-2	-18	18
f_4	-6	-6	-14	-14	6	6	-2	-2	10	10	-18	-18
f_7	16	16	-4	-4	0	0	12	12	-16	-16	-12	-12
f_9	-12	-12	16	16	12	12	8	8	4	4	0	0
f_{11}	-9	-9	-4	-4	-3	-3	2	2	11	11	12	12
f_{16}	0	0	0	0	0	0	0	0	0	0	0	0
f_{17}	14	0	0	-4	7	17	-15	0	16	-22	-14	9
f_{18}	4	4	-16	-16	12	12	8	8	-12	-12	-24	-24
g_3	$-8t$	$7t$	$8t$	$-3t$	t	$-5t$	$9t$	$8t$	$-2t$	$-5t$	$17t$	$-11t$
f_{22}	-12	-12	4	4	12	12	-20	-20	4	4	0	0
f_{23}	12	9	0	-6	18	6	12	-9	-3	-3	-12	-9
f_{25}	6	6	4	4	-12	-12	16	16	16	16	12	12
g_4	$-3t$	$-4t$	$-5t$	$4t$	$13t$	$-5t$	$6t$	$15t$	0	$3t$	$7t$	$-14t$
f_{27}	12	-12	14	14	12	-12	-10	-10	-16	-16	0	0
f_{28}	18	-3	4	16	10	-10	-6	11	17	-7	-8	3
f_{29}	12	16	14	6	8	-12	2	8	24	-2	-6	-18
f_{30}	6	6	16	16	-18	-18	-8	-8	-4	-4	12	12
f_{31}	-9	-18	14	-4	12	-6	11	2	?	11	3	?
f_{32}	-15	6	-4	-4	18	-6	-7	2	11	11	9	0
f_{33}	-15	6	4	4	18	-6	7	-2	-11	-11	9	0

$t = \sqrt{2}$

Table 9.6 — part 5 of 5

$\mathfrak{n}$	$\mathbf{N}(\mathfrak{n})$	name	5	$29a$	$29b$	$41a$	$41b$	$61a$	$61b$	$89a$	$89b$
$\mathfrak{p}_2^3$	8	f_1	-2	-2	-2	2	2	-10	-10	-6	-6
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	18	f_3	-4	0	0	2	2	2	2	10	10
$\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$	27	f_5	0	8	-8	2	-2	-6	-6	-6	6
$\mathfrak{p}_2^2\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	36	f_6	2	6	6	-10	-10	2	2	10	10
$\mathfrak{p}_2\mathfrak{p}_{3b}\mathfrak{p}_{7b}$	42	f_8	1	0	-5	7	12	-8	-8	10	-15
$\mathfrak{p}_{3b}^2\mathfrak{p}_5$	45	g_1	$*$	6	6	-6	-6	-10	2	6	-6
$\mathfrak{p}_{7a}\mathfrak{p}_{7b}$	49	f_{10}	-4	5	5	2	2	-8	-8	0	0
$\mathfrak{p}_2\mathfrak{p}_5^2$	50	f_{12}	$*$	0	0	-3	-3	2	2	-15	-15
$\mathfrak{p}_2^3\mathfrak{p}_{7a}$	56	f_{13}	3	3	-2	2	-3	-10	10	-11	4
$\mathfrak{p}_2^2\mathfrak{p}_{3b}\mathfrak{p}_5$	60	f_{14}	$*$	-2	-2	6	-10	2	2	-6	10
$\mathfrak{p}_2^6$	64	f_{15}	2	-10	-10	-10	-10	10	10	10	10
$\mathfrak{p}_2^3\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	72	f_{19}	4	-8	-8	2	2	2	2	-6	-6
$\mathfrak{p}_2^4\mathfrak{p}_5$	80	f_{20}	$*$	6	6	-6	-6	-2	-2	-6	-6
$\mathfrak{p}_2^4\mathfrak{p}_5$	80	f_{21}	$*$	-2	-2	6	6	2	2	-6	-6
$\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}^2$	81	g_2	0	0	0	0	0	2	2	0	0
$\mathfrak{p}_2\mathfrak{p}_{7a}^2$	98	f_{24}	3	3	-6	-6	-3	10	-10	-3	-12
$\mathfrak{p}_2^2\mathfrak{p}_5^2$	100	f_{26}	$*$	-6	-6	6	6	2	2	6	6
$\mathfrak{p}_{101b}$	101	g_5	0	6	0	-6	6	14	2	-6	0

Table 9.7: Minusforms of types f and g for $\mathbb{Q}(\sqrt{-5})$ — part 1 of 5

	101a	101b	109a	109b	11	149a	149b	13	181a	181b	229a	229b
f_1	6	6	6	6	−6	−18	−18	10	22	22	6	6
f_3	−8	−8	−10	−10	−18	20	20	−10	2	2	10	10
f_5	−4	4	−2	−2	6	4	−4	−2	2	2	−14	−14
f_6	−2	−2	2	2	−6	2	2	26	−10	−10	−26	−26
f_8	−8	12	5	10	−3	15	−10	−5	−18	−8	15	−25
g_1	−6	0	−10	8	−4	−12	0	−10	−4	20	26	−22
f_{10}	12	12	−5	−5	−13	−10	−10	25	−18	−18	10	10
f_{12}	−18	−18	10	10	−13	0	0	10	2	2	−20	−20
f_{13}	−4	−14	−14	1	19	−18	7	−15	−18	−8	21	11
f_{14}	−10	6	18	2	10	−6	−6	−6	−10	22	6	6
f_{15}	−2	−2	−6	−6	−22	−14	−14	10	−18	−18	30	30
f_{19}	0	0	6	6	−18	12	12	22	−14	−14	−6	−6
f_{20}	6	6	−2	−2	−22	6	6	−22	−10	−10	14	14
f_{21}	6	6	−14	−14	−6	10	10	−22	−10	−10	−26	−26
g_2	0	0	14	14	−22	0	0	26	−22	−22	26	26
f_{24}	0	−6	2	−7	−5	−6	15	1	−2	−16	5	−5
f_{26}	6	6	−2	−2	−22	6	6	22	−10	−10	−14	−14
g_5	−18	*	14	14	14	−18	−6	−10	−22	2	−22	−10

Table 9.7 — part 2 of 5

	241a	241b	269a	269b	281a	281b	17	349a	349b	19	389a	389b
f_1	−22	−22	6	6	18	18	34	−2	−2	−22	30	30
f_3	22	22	0	0	−18	−18	30	−10	−10	−38	−20	−20
f_5	14	14	24	−24	−26	26	−34	−2	−2	10	24	−24
f_6	−2	−2	−6	−6	6	6	18	14	14	−38	34	34
f_8	22	17	10	5	−18	−18	−20	−30	10	12	10	30
g_1	2	−10	−18	18	−18	−6	26	14	14	8	12	0
f_{10}	22	22	−10	−10	7	7	−15	20	20	−38	−5	−5
f_{12}	17	17	0	0	−18	−18	25	10	10	−13	−30	−30
f_{13}	23	8	21	−14	−12	28	−16	18	−2	−2	−30	0
f_{14}	−18	14	18	18	6	−10	−14	−34	−2	10	−22	10
f_{15}	30	30	26	26	−10	−10	−30	−10	−10	−38	34	34
f_{19}	−10	−10	−24	−24	−18	−18	−2	22	22	26	−12	−12
f_{20}	−14	−14	−18	−18	−6	−6	2	−10	−10	−22	6	6
f_{21}	−2	−2	−14	−14	−10	−10	−30	30	30	−22	−6	−6
g_2	2	2	0	0	0	0	14	−34	−34	−22	0	0
f_{24}	−1	−8	21	−6	24	−12	20	10	−10	34	18	24
f_{26}	14	14	−18	−18	6	6	−2	10	10	−22	6	6
g_5	8	−22	30	30	−6	6	20	2	2	20	24	30

Table 9.7 — part 3 of 5

	2	3a	3b	7a	7b	23a	23b	43a	43b	47a	47b	67a	67b
f_1	$*$	$2i$	$2i$	$-2i$	$-2i$	$-2i$	$-2i$	$-6i$	$-6i$	$6i$	$6i$	$-14i$	$-14i$
f_3	$*$	$*$	$*$	$2i$	$2i$	$4i$	$4i$	$4i$	$4i$	$-8i$	$-8i$	$-8i$	$-8i$
f_5	i	$*$	$*$	$-2i$	$2i$	$-4i$	$-4i$	$8i$	$-8i$	0	0	$-12i$	$12i$
f_6	$*$	$*$	$*$	$4i$	$4i$	$-4i$	$-4i$	$-4i$	$-4i$	$-4i$	$-4i$	$-4i$	$-4i$
f_8	$*$	i	$*$	$3i$	$*$	i	$-4i$	$6i$	$-4i$	$-12i$	$8i$	$-12i$	$3i$
g_1	t	$-t$	$*$	$-3t$	0	$-2t$	t	$3t$	$-6t$	$-2t$	$7t$	$9t$	$-6t$
f_{10}	$2i$	$-i$	$-i$	$*$	$*$	$-6i$	$-6i$	$4i$	$4i$	$-3i$	$-3i$	$2i$	$2i$
f_{12}	$*$	i	i	$-2i$	$-2i$	$6i$	$6i$	$-4i$	$-4i$	$-12i$	$-12i$	$13i$	$13i$
f_{13}	$*$	$2i$	$-3i$	$*$	$3i$	$-2i$	$-7i$	$4i$	$4i$	$-4i$	$6i$	i	$-4i$
f_{14}	$*$	0	$*$	0	$4i$	$-4i$	$8i$	$-8i$	$-4i$	$12i$	$8i$	$-8i$	$12i$
f_{15}	$*$	0	0	0	0	0	0	0	0	0	0	0	0
f_{19}	$*$	$*$	$*$	$2i$	$2i$	$-4i$	$-4i$	$-12i$	$-12i$	0	0	$8i$	$8i$
f_{20}	$*$	$2i$	$-2i$	$2i$	$-2i$	$6i$	$-6i$	$10i$	$-10i$	$6i$	$-6i$	$2i$	$-2i$
f_{21}	$*$	0	0	$4i$	$-4i$	$-4i$	$4i$	$-8i$	$8i$	$4i$	$-4i$	$-8i$	$8i$
g_2	u	$*$	$*$	0	0	$4u$	$4u$	0	0	$4u$	$4u$	0	0
f_{24}	$*$	$2i$	$-i$	$*$	i	$-6i$	$3i$	$8i$	$-8i$	0	$-6i$	$-13i$	$4i$
f_{26}	$*$	$2i$	$2i$	$2i$	$2i$	$-6i$	$-6i$	$10i$	$10i$	$-6i$	$-6i$	$2i$	$2i$
g_5	t	$-t$	$2t$	0	$3t$	$-5t$	t	0	0	$-2t$	$-2t$	0	$-9t$

$i = \sqrt{-1}, \qquad t = \sqrt{-2}, \qquad u = \sqrt{-5}$

Table 9.7 — part 4 of 5

	$83a$	$83b$	$103a$	$103b$	$107a$	$107b$	$127a$	$127b$	$163a$	$163b$	$167a$	$167b$
f_1	$2i$	$2i$	$14i$	$14i$	$10i$	$10i$	$6i$	$6i$	$2i$	$2i$	$-18i$	$-18i$
f_3	$4i$	$4i$	$14i$	$14i$	$12i$	$12i$	$2i$	$2i$	$-16i$	$-16i$	$12i$	$12i$
f_5	$-12i$	$-12i$	$6i$	$-6i$	$4i$	$4i$	$2i$	$-2i$	$-8i$	$8i$	$12i$	$12i$
f_6	$-4i$	$-4i$	$4i$	$4i$	$12i$	$12i$	$4i$	$4i$	$-20i$	$-20i$	$12i$	$12i$
f_8	$-9i$	$6i$	$-14i$	$-4i$	$8i$	$-2i$	$-7i$	$-2i$	$11i$	$-19i$	$-17i$	$-12i$
g_1	$10t$	t	$3t$	0	$13t$	$4t$	$9t$	0	$15t$	$-6t$	$-8t$	$7t$
f_{10}	$4i$	$4i$	$19i$	$19i$	$-8i$	$-8i$	$2i$	$2i$	$14i$	$14i$	$-3i$	$-3i$
f_{12}	$-9i$	$-9i$	$-4i$	$-4i$	$3i$	$3i$	$-2i$	$-2i$	$11i$	$11i$	$-12i$	$-12i$
f_{13}	$-18i$	$-3i$	$4i$	$-16i$	$-10i$	$-10i$	$6i$	$11i$	$17i$	$7i$	$-8i$	$-3i$
f_{14}	$-4i$	$-8i$	$-16i$	$-12i$	0	$4i$	$-16i$	$4i$	$8i$	$-4i$	$-12i$	0
f_{15}	0	0	0	0	0	0	0	0	0	0	0	0
f_{19}	$4i$	$4i$	$-2i$	$-2i$	$-4i$	$-4i$	$18i$	$18i$	$16i$	$16i$	$-12i$	$-12i$
f_{20}	$6i$	$-6i$	$-14i$	$14i$	$-6i$	$6i$	$2i$	$-2i$	$10i$	$-10i$	$-18i$	$18i$
f_{21}	$16i$	$-16i$	$4i$	$-4i$	0	0	$12i$	$-12i$	$16i$	$-16i$	$12i$	$-12i$
g_2	$-8u$	$-8u$	0	0	$-8u$	$-8u$	0	0	0	0	$4u$	$4u$
f_{24}	$6i$	$15i$	$-4i$	$-4i$	$-6i$	$18i$	$-2i$	$-7i$	$11i$	$-11i$	0	$-9i$
f_{26}	$-6i$	$-6i$	$-14i$	$-14i$	$-6i$	$-6i$	$2i$	$2i$	$10i$	$10i$	$18i$	$18i$
g_5	$7t$	$10t$	$3t$	$-6t$	$-5t$	$-5t$	$12t$	$-9t$	$6t$	$9t$	$7t$	$4t$

$i = \sqrt{-1}, \qquad t = \sqrt{-2}, \qquad u = \sqrt{-5}$

Table 9.7 — part 5 of 5

	basis		5		$29a$		$29b$		$41a$		$41b$		$61a$		$61b$	
h_1	1	$\sqrt{6}$	2	1	-2	-2	-2	-2	-6	2	-6	2	6	-1	6	-1
h_2	1	$\sqrt{6}$	3	0	0	0	0	0	0	2	0	-2	-4	0	-4	0
h_3	1	$\sqrt{33}$	$-\frac{3}{2}$	$\frac{1}{2}$	-3	-1	-3	-1	3	1	3	1	5	-1	5	-1
h_4	1	$\sqrt{2}$	0	2	0	-2	2	-4	$*$		2	-4	-4	-2	-12	2
h_5	1	$\sqrt{5}$	$*$		0	3	$-\frac{3}{2}$	$\frac{3}{2}$	$\frac{9}{2}$	$\frac{3}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$	-1	0	$\frac{7}{2}$	$\frac{3}{2}$
h_6	1	$\sqrt{3}$	0	0	-2	4	2	-4	2	-2	2	-2	4	-4	-4	4
$\bar{h}_6$	1	$\sqrt{3}$	0	0	2	-4	-2	4	2	-2	2	-2	-4	4	4	-4

	basis		$89a$		$89b$		$101a$		$101b$		$109a$		$109b$		11	
h_1	1	$\sqrt{6}$	10	0	10	0	6	-1	6	-1	-2	-2	-2	-2	2	0
h_2	1	$\sqrt{6}$	3	-2	3	2	-6	2	-6	-2	-10	0	-10	0	$*$	
h_3	1	$\sqrt{33}$	$\frac{3}{2}$	$-\frac{1}{2}$	$\frac{3}{2}$	$-\frac{1}{2}$	6	0	6	0	-10	0	-10	0	$*$	
h_4	1	$\sqrt{2}$	-14	0	6	8	10	0	0	-6	-10	4	-4	2	-2	12
h_5	1	$\sqrt{5}$	12	-3	6	3	$\frac{3}{2}$	$-\frac{3}{2}$	-3	6	-7	3	$\frac{13}{2}$	$-\frac{3}{2}$	5	0
h_6	1	$\sqrt{3}$	-2	0	-2	0	6	4	-6	-4	0	-8	0	8	10	0
$\bar{h}_6$	1	$\sqrt{3}$	-2	0	-2	0	-6	-4	6	4	0	8	0	-8	10	0

	basis		$149a$		$149b$		13		$181a$		$181b$		$229a$		$229b$	
h_1	1	$\sqrt{6}$	-6	4	-6	4	16	-4	2	-5	2	-5	2	7	2	7
h_2	1	$\sqrt{6}$	-6	2	-6	-2	-10	0	-1	-6	-1	6	11	0	11	0
h_3	1	$\sqrt{33}$	0	2	0	2	26	0	$\frac{31}{2}$	$\frac{3}{2}$	$\frac{31}{2}$	$\frac{3}{2}$	$-\frac{35}{2}$	$\frac{1}{2}$	$-\frac{35}{2}$	$\frac{1}{2}$
h_4	1	$\sqrt{2}$	0	6	6	-8	-2	-8	14	-4	-4	-10	18	0	8	10
h_5	1	$\sqrt{5}$	-3	0	9	0	$\frac{7}{2}$	$-\frac{9}{2}$	20	-3	$-\frac{23}{2}$	$-\frac{9}{2}$	-13	-3	$-\frac{35}{2}$	$-\frac{9}{2}$
h_6	1	$\sqrt{3}$	12	-4	-12	4	-10	-8	-14	-4	14	4	6	4	-6	-4
$\bar{h}_6$	1	$\sqrt{3}$	-12	4	12	-4	-10	-8	14	4	-14	-4	-6	-4	6	4

Table 9.8: Newforms of type h for $\mathbb{Q}(\sqrt{-5})$

	basis		241a		241b		269a		269b		281a		281b	
h_1	1	$\sqrt{6}$	6	-6	6	-6	-2	-7	-2	-7	-18	0	-18	0
h_2	1	$\sqrt{6}$	-16	0	-16	0	6	-8	6	8	18	0	18	0
h_3	1	$\sqrt{33}$	11	1	11	1	0	2	0	2	-12	2	-12	2
h_4	1	$\sqrt{2}$	6	16	-6	-8	-2	16	14	4	-6	-8	-22	0
h_5	1	$\sqrt{5}$	8	-3	-10	0	$-\frac{15}{2}$	$-\frac{15}{2}$	12	3	3	3	$-\frac{9}{2}$	$\frac{3}{2}$
h_6	1	$\sqrt{3}$	2	10	2	10	-4	4	4	-4	6	-2	6	-2
$\bar{h}_6$	1	$\sqrt{3}$	2	10	2	10	4	-4	-4	4	6	-2	6	-2

	basis		17		349a		349b		19		389a		389b	
h_1	1	$\sqrt{6}$	30	0	6	1	6	1	-16	-8	-18	2	-18	2
h_2	1	$\sqrt{6}$	2	0	14	6	14	-6	2	0	-9	2	-9	-2
h_3	1	$\sqrt{33}$	20	2	-4	-2	-4	-2	-22	0	$-\frac{9}{2}$	$-\frac{5}{2}$	$-\frac{9}{2}$	$-\frac{5}{2}$
h_4	1	$\sqrt{2}$	18	-4	-14	4	6	-4	14	8	-12	14	20	-6
h_5	1	$\sqrt{5}$	$-\frac{5}{2}$	$\frac{15}{2}$	-10	-6	-1	3	$-\frac{23}{2}$	$-\frac{21}{2}$	$-\frac{39}{2}$	$-\frac{9}{2}$	18	0
h_6	1	$\sqrt{3}$	18	-8	-10	4	10	-4	10	16	-20	-4	20	4
$\bar{h}_6$	1	$\sqrt{3}$	18	-8	10	-4	-10	4	10	16	20	4	-20	-4

	basis		2		3a		3b		7a		7b		23a		23b	
h_1	$\sqrt{-1}$	$\sqrt{-6}$	$*$		0	1	0	1	$*$		$*$		2	-2	2	-2
h_2	$\sqrt{-2}$	$\sqrt{-3}$	1	0	-1	1	-1	-1	0	2	0	-2	1	3	1	-3
h_3	$\sqrt{-11}$	$\sqrt{-3}$	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	-2	0	-2	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$
h_4	1	$\sqrt{2}$	1	-1	2	0	$*$		2	0	2	0	2	0	-2	4
h_5	$\sqrt{-1}$	$\sqrt{-5}$	$\frac{3}{2}$	$\frac{1}{2}$	$-\frac{3}{2}$	$-\frac{1}{2}$	$*$		3	0	$\frac{3}{2}$	$-\frac{3}{2}$	3	2	0	2
h_6	1	$\sqrt{3}$	$*$		1	-1	1	-1	-1	-1	1	1	-3	1	3	-1
$\bar{h}_6$	1	$\sqrt{3}$	$*$		1	-1	1	-1	1	1	-1	-1	3	-1	-3	1

Table 9.8 — part 2 of 3

	basis		$43a$		$43b$		$47a$		$47b$		$67a$		$67b$	
h_1	$\sqrt{-1}$	$\sqrt{-6}$	-4	2	-4	2	4	2	4	2	-8	0	-8	0
h_2	$\sqrt{-2}$	$\sqrt{-3}$	-6	-2	-6	2	-2	0	-2	0	9	1	9	-1
h_3	$\sqrt{-11}$	$\sqrt{-3}$	0	2	0	2	2	0	2	0	$-\frac{3}{2}$	$-\frac{5}{2}$	$-\frac{3}{2}$	$-\frac{5}{2}$
h_4	1	$\sqrt{2}$	-4	4	4	4	2	-4	2	0	0	-4	2	-4
h_5	$\sqrt{-1}$	$\sqrt{-5}$	0	-3	$-\frac{9}{2}$	$\frac{3}{2}$	$-\frac{9}{2}$	$\frac{1}{2}$	$-\frac{9}{2}$	$\frac{1}{2}$	$\frac{9}{2}$	$\frac{9}{2}$	$\frac{9}{2}$	$\frac{3}{2}$
h_6	1	$\sqrt{3}$	-3	-1	-3	-1	7	-1	-7	1	11	1	11	1
$\bar{h}_6$	1	$\sqrt{3}$	-3	-1	-3	-1	-7	1	7	-1	11	1	11	1

	basis		$83a$		$83b$		$103a$		$103b$		$107a$		$107b$	
h_1	$\sqrt{-1}$	$\sqrt{-6}$	0	1	0	1	-8	-2	-8	-2	-8	0	-8	0
h_2	$\sqrt{-2}$	$\sqrt{-3}$	-2	-6	-2	6	-6	0	-6	0	4	6	4	-6
h_3	$\sqrt{-11}$	$\sqrt{-3}$	2	0	2	0	0	-6	0	-6	2	0	2	0
h_4	1	$\sqrt{2}$	4	4	0	0	6	8	-6	0	10	0	-2	-4
h_5	$\sqrt{-1}$	$\sqrt{-5}$	6	-4	6	5	-6	3	-3	-6	9	-1	$-\frac{9}{2}$	$\frac{7}{2}$
h_6	1	$\sqrt{3}$	7	5	7	5	-1	-5	1	5	-9	1	-9	1
$\bar{h}_6$	1	$\sqrt{3}$	7	5	7	5	1	5	-1	-5	-9	1	-9	1

	basis		$127a$		$127b$		$163a$		$163b$		$167a$		$167b$	
h_1	$\sqrt{-1}$	$\sqrt{-6}$	-10	-2	-10	-2	12	-2	12	-2	0	-2	0	-2
h_2	$\sqrt{-2}$	$\sqrt{-3}$	6	4	6	-4	-6	4	-6	-4	-2	0	-2	0
h_3	$\sqrt{-11}$	$\sqrt{-3}$	3	-1	3	-1	0	-2	0	-2	-1	11	-1	11
h_4	1	$\sqrt{2}$	-2	8	-2	-8	-2	-12	10	4	-2	-8	-2	0
h_5	$\sqrt{-1}$	$\sqrt{-5}$	3	-3	-3	3	-6	0	$\frac{3}{2}$	$\frac{9}{2}$	9	2	-6	-7
h_6	1	$\sqrt{3}$	-9	-5	9	5	1	7	1	7	-1	-13	1	13
$\bar{h}_6$	1	$\sqrt{3}$	9	5	-9	-5	1	7	1	7	1	13	-1	-13

Table 9.8 — part 3 of 3

9.7 Ray class groups and twists

In this section, we compute those ray class groups whose characters occur as twisting characters in our tables of modular forms. It will be useful to have one general result.

Let k be an algebraic number field with ring of integers $\mathfrak{O}$, and let $\mathfrak{m}$ be an integral ideal of $\mathfrak{O}$. Let $J^{\mathfrak{m}}$ be the group of fractional ideals coprime to $\mathfrak{m}$, and let $P^{\mathfrak{m}}$ be the group of principal fractional ideals having a generator a such that $a \equiv 1 \pmod{\mathfrak{m}}$. Thus $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ is the ray class group modulo $\mathfrak{m}$, and J^1/P^1 is the ideal class group of k. Finally, let $P^{(\mathfrak{m})}$ be the group of principal fractional ideals coprime to $\mathfrak{m}$; thus $P^{(\mathfrak{m})} = J^{\mathfrak{m}} \cap P^1$.

Proposition 122. *There is an exact sequence of abelian groups*

$$1 \longrightarrow P^{(\mathfrak{m})}/P^{\mathfrak{m}} \longrightarrow J^{\mathfrak{m}}/P^{\mathfrak{m}} \longrightarrow J^{\mathfrak{m}}/P^{(\mathfrak{m})} \longrightarrow 1, \tag{9.6}$$

and there are isomorphisms $J^{\mathfrak{m}}/P^{(\mathfrak{m})} \cong J^1/P^1$ *and* $P^{(\mathfrak{m})}/P^{\mathfrak{m}} \cong (\mathfrak{O}/\mathfrak{m})^{\times}/\mathfrak{O}^{\times}$. *If* $\mathfrak{m}' \mid \mathfrak{m}$, *then there is a canonical surjection* $J^{\mathfrak{m}}/P^{\mathfrak{m}} \to J^{\mathfrak{m}'}/P^{\mathfrak{m}'}$ *and hence a canonical injection* $(J^{\mathfrak{m}'}/P^{\mathfrak{m}'})^* \to (J^{\mathfrak{m}}/P^{\mathfrak{m}})^*$ *of the corresponding character groups.*

Thus the ray class group is an extension of the group $(\mathfrak{O}/\mathfrak{m})^{\times}/\mathfrak{O}^{\times}$ by the ideal class group. We stress that $\mathfrak{m}$ in this proposition is an integral ideal, not a general modulus (which might be divisible by real infinite primes).

Proof. Exactness of (9.6) is trivial. The map $J^{\mathfrak{m}} \to J^1 \to J^1/P^1$ is surjective (since, by Lemma 1, every ideal class contains an ideal coprime to $\mathfrak{m}$) with kernel $J^{\mathfrak{m}} \cap P^1 = P^{(\mathfrak{m})}$, giving the first isomorphism. A similar argument gives the last sentence.

To define the map $P^{(\mathfrak{m})}/P^{\mathfrak{m}} \to (\mathfrak{O}/\mathfrak{m})^{\times}/\mathfrak{O}^{\times}$, begin by noting that every element of $P^{(\mathfrak{m})}$ has the form $\frac{a}{b}\mathfrak{O}$ for non-zero $a, b \in \mathfrak{O}$. By Lemma 38, we may assume that $\langle a, b\rangle$ is coprime to $\mathfrak{m}$, from which it follows (since a/b is coprime to $\mathfrak{m}$) that each of a and b is coprime to $\mathfrak{m}$; multiplying both a and b by an inverse of b modulo $\mathfrak{m}$ if necessary, we may further assume that $b \equiv 1 \pmod{\mathfrak{m}}$. Thus every element of $P^{(\mathfrak{m})}/P^{\mathfrak{m}}$ is represented by some $a \in \mathfrak{O}$ coprime to $\mathfrak{m}$, which we map to $(\mathfrak{O}/\mathfrak{m})^{\times}/\mathfrak{O}^{\times}$. The image of a is well-defined, for if $aP^{\mathfrak{m}} = a'P^{\mathfrak{m}}$, then $(a\mathfrak{O})b = (a'\mathfrak{O})b'$ for some $b, b' \equiv 1 \pmod{\mathfrak{m}}$, so there exists $\epsilon \in \mathfrak{O}^{\times}$ such that $ab = \epsilon a'b'$, whence $a \equiv \epsilon a' \pmod{\mathfrak{m}}$. The map thus defined is clearly a surjective homomorphism. If $aP^{\mathfrak{m}}$ is in the kernel, then $a \equiv \epsilon \pmod{\mathfrak{m}}$ for some $\epsilon \in \mathfrak{O}^{\times}$, whence $a\mathfrak{O} \in P^{\mathfrak{m}}$. This completes the proof. □

As in the case $k = \mathbb{Q}$, the twist of a form with character ψ by a character χ has character $\psi\chi^2$; thus, twisting by a quadratic character χ preserves the character, whilst twisting by a quartic character χ that satisfies $\chi^2 = \nu$ changes plusforms into minusforms and vice versa.

In the case $k = \mathbb{Q}$, the Chinese Remainder Theorem applied to $(\mathbb{Z}/M\mathbb{Z})^{\times}$ implies that it suffices to consider characters to prime-power moduli. To find all quadratic characters, it then suffices to consider $M = 4$, $M = 8$ and M an odd prime (thus only such characters are treated in [AL70], for example) whilst to find all quartic characters, one only needs the further modulus $M = 16$. A similar simplification is not possible in the case $h(k) > 1$, as we see below (Example 5).

From now on, let $k = \mathbb{Q}(\sqrt{-5})$, so that $\mathfrak{O} = \mathbb{Z} + \mathbb{Z}w$, where $w = \sqrt{-5}$. For each ideal $\mathfrak{m}$ such that $\mathfrak{m}^2$ divides one of the levels in our tables of newforms, we now determine all characters χ of $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ with $\chi^2 \in \{1, \nu\}$. The values of $\mathfrak{m}$ to be considered are $\mathfrak{O}$, $\mathfrak{p}_2$, $(\mathfrak{p}_2)^2$, $(\mathfrak{p}_2)^3$, $(\mathfrak{p}_2)^4$, $\mathfrak{p}_{3a}$, $(\mathfrak{p}_{3a})^2$, $\mathfrak{p}_{3a}\mathfrak{p}_{3b}$, $\mathfrak{p}_5$, $\mathfrak{p}_{7a}$, $\mathfrak{p}_2\mathfrak{p}_{3a}$ and $\mathfrak{p}_2\mathfrak{p}_5$ (and their conjugates).

Example 1. Let $\mathfrak{m} = 1$. Clearly $P^{(\mathfrak{m})} = P^{\mathfrak{m}}$ and the ray class group is just the ideal class group, cyclic of order 2. The non-trivial character ν is given by (9.1) above. (The same is true for any k with $h(k) = 2$.) Notice that $f_{15} * \nu = f_{15}$ and $f_{16} * \nu = f_{16}$, so the eigenvalues of f_{15} and f_{16} at all non-principal primes are zero.

For $\mathfrak{m} = \mathfrak{p}_2$ the group $(\mathfrak{O}/\mathfrak{m})^{\times}$ is again trivial, so $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong J^1/P^1$ and there are no new characters.

Example 2. Let $\mathfrak{m} = (\mathfrak{p}_2)^2 = \langle 2 \rangle$. A set of invertible residues modulo $\mathfrak{m}$ is $\{1, w\}$, so $(\mathfrak{O}/\mathfrak{m})^{\times}/\mathfrak{O}^{\times}$ has order 2 and $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ has order 4. Since $(\mathfrak{p}_{3a})^2 = \langle 2 - w \rangle \notin P^{\mathfrak{m}}$, the group $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ is cyclic of order 4, and any non-principal prime (other than $\mathfrak{p}_2$) serves as a generator. Note that for p a split prime, $\mathfrak{p}_{p,a}\mathfrak{p}_{p,b} = \langle p \rangle \in P^{\mathfrak{m}}$; hence inversion in $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ is given by conjugation. By inspection of the principal generators of $\mathfrak{p}$ (for principal primes $\mathfrak{p}$) and of $\mathfrak{p}_{3a}\mathfrak{p}$ (for non-principal $\mathfrak{p}$) in Tables 9.1 and 9.2, we obtain, with a slight abuse of notation (writing, for example, $29ab$ for $\mathfrak{p}_{29a}, \mathfrak{p}_{29b}$),

$$\begin{aligned} P^{\mathfrak{m}} &\supset \{29ab, 89ab, 101ab, 181ab, 229ab, 349ab, \dots, 11, 13, 17, 19, \dots\}, \\ \mathfrak{p}_5 P^{\mathfrak{m}} &\supset \{5, 41ab, 61ab, 109ab, 149ab, 241ab, 269ab, 281ab, 389ab, \dots\}, \\ \mathfrak{p}_{3a} P^{\mathfrak{m}} &\supset \{3a, 7b, 23b, 43a, 47a, 67b, 83b, 103a, 107b, 127b, 163a, 167a, \dots\}, \\ \mathfrak{p}_{3b} P^{\mathfrak{m}} &\supset \{3b, 7a, 23a, 43b, 47b, 67a, 83a, 103b, 107a, 127a, 163b, 167b, \dots\}, \end{aligned} \tag{9.7}$$

and the character group is generated by the quartic character, χ say, defined by

$$\mathfrak{p} \mapsto \begin{cases} i & \text{for } \mathfrak{p} \in \mathfrak{p}_{3a} P^{\mathfrak{m}}, \\ -1 & \text{for } \mathfrak{p} \in \mathfrak{p}_5 P^{\mathfrak{m}}, \\ -i & \text{for } \mathfrak{p} \in \mathfrak{p}_{3b} P^{\mathfrak{m}}, \\ 1 & \text{for } \mathfrak{p} \in P^{\mathfrak{m}}. \end{cases}$$

Forms at level $\mathfrak{n}$ may be twisted by χ whenever $(\mathfrak{p}_2)^4 \mid \mathfrak{n}$; in the range of our tables, this means at levels $(\mathfrak{p}_2)^4$, $(\mathfrak{p}_2)^5$, $(\mathfrak{p}_2)^4\mathfrak{p}_{3a}$, $(\mathfrak{p}_2)^6$, $(\mathfrak{p}_2)^4\mathfrak{p}_5$, $(\mathfrak{p}_2)^5\mathfrak{p}_{3a}$, $(\mathfrak{p}_2)^4\mathfrak{p}_{7a}$ and $(\mathfrak{p}_2)^7$. Since $\chi^2 = \nu$, twisting by χ interchanges "plusforms" and "minusforms" (at the expense of possibly changing the power of $\mathfrak{p}_2$ in the level). Sure enough, inspection of our tables of eigenvalues shows $f_1 = f_2 * \chi$ $\big($at level $(\mathfrak{p}_2)^4\big)$, $f_{15} = f_{16} * \chi$ $\big($at level $(\mathfrak{p}_2)^6\big)$, $f_{20} = f_4 * \chi$ and $f_{21} = f_7 * \chi^3$ $\big($both at level $(\mathfrak{p}_2)^4\mathfrak{p}_5\big)$, and $f_{13} = f_{28} * \chi$ $\big($at level $(\mathfrak{p}_2)^4\mathfrak{p}_{7a}\big)$.

For $\mathfrak{m} = (\mathfrak{p}_2)^3$ the invertible residues are $\{\pm 1, \pm w\}$, so $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ is the same as for $\mathfrak{m} = (\mathfrak{p}_2)^2$, and there are no new characters.

Example 3. Let $\mathfrak{m} = (\mathfrak{p}_2)^4$. The invertible residues are $\{\pm 1,\ \pm 1 + 2w,\ \pm w,\ 2 \pm w\}$, so $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times \cong C_2 \times C_2$. Since $(\mathfrak{p}_{3a})^2 = \langle 2 - w \rangle \mapsto 2 \pm w$, we see that $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong C_4 \times C_2$.

Each coset in (9.7) is partitioned into two, giving

$$\begin{aligned}
P^{\mathfrak{m}} &\supset \{89ab, \dots, 11, 13, 17, 19, \dots\}, \\
\mathfrak{p}_{29a}P^{\mathfrak{m}} &\supset \{29ab, 101ab, 181ab, 229ab, 349ab, \dots\}, \\
\mathfrak{p}_{5}P^{\mathfrak{m}} &\supset \{5, 61ab, 109ab, 149ab, 269ab, 389ab, \dots\}, \\
\mathfrak{p}_{41a}P^{\mathfrak{m}} &\supset \{41ab, 241ab, 281ab, \dots\}, \\
\mathfrak{p}_{3a}P^{\mathfrak{m}} &\supset \{3a, 43a, 67b, 83b, 107b, 163a, \dots\}, \\
\mathfrak{p}_{7b}P^{\mathfrak{m}} &\supset \{7b, 23b, 47a, 103a, 127b, 167a, \dots\}, \\
\mathfrak{p}_{3b}P^{\mathfrak{m}} &\supset \{3b, 43b, 67a, 83a, 107a, 163b, \dots\}, \\
\mathfrak{p}_{7a}P^{\mathfrak{m}} &\supset \{7a, 23a, 47b, 103b, 127a, 167b, \dots\}.
\end{aligned}$$

There is a new quadratic character, ξ say, given by

$$\mathfrak{p} \mapsto \begin{cases} +1 & \text{if } \mathfrak{p} \in P^{\mathfrak{m}} \cup (\mathfrak{p}_{41a}P^{\mathfrak{m}}) \cup (\mathfrak{p}_{3a}P^{\mathfrak{m}}) \cup (\mathfrak{p}_{3b}P^{\mathfrak{m}}), \\ -1 & \text{if } \mathfrak{p} \in (\mathfrak{p}_{5}P^{\mathfrak{m}}) \cup (\mathfrak{p}_{29a}P^{\mathfrak{m}}) \cup (\mathfrak{p}_{7a}P^{\mathfrak{m}}) \cup (\mathfrak{p}_{7b}P^{\mathfrak{m}}). \end{cases} \tag{9.8}$$

The full character group, generated by ξ and the character χ induced from the lower modulus $\mathfrak{m}' = (\mathfrak{p}_2)^2$, is as follows:

	1	χ	ν	χ^3	ξ	$\xi\chi$	$\xi\nu$	$\xi\chi^3$
$P^{\mathfrak{m}}$	1	1	1	1	1	1	1	1
$\mathfrak{p}_{29a}P^{\mathfrak{m}}$	1	1	1	1	-1	-1	-1	-1
$\mathfrak{p}_{5}P^{\mathfrak{m}}$	1	-1	1	-1	-1	1	-1	1
$\mathfrak{p}_{41a}P^{\mathfrak{m}}$	1	-1	1	-1	1	-1	1	-1
$\mathfrak{p}_{3a}P^{\mathfrak{m}}$	1	i	-1	$-i$	1	i	-1	$-i$
$\mathfrak{p}_{7b}P^{\mathfrak{m}}$	1	i	-1	$-i$	-1	$-i$	1	i
$\mathfrak{p}_{3b}P^{\mathfrak{m}}$	1	$-i$	-1	i	1	$-i$	-1	i
$\mathfrak{p}_{7a}P^{\mathfrak{m}}$	1	$-i$	-1	i	-1	i	1	$-i$

All the newforms at level $\mathfrak{n} = (\mathfrak{p}_2)^8$ are accounted for by twisting oldforms by the new characters: we find $\dim V(\mathfrak{n}) = 19$, where the oldspace may be written $6f_1 + 5f_2 + 2f_{15} + 2f_{16}$, and four representative newforms are $f_1 * \xi$, $f_2 * \xi$, $f_{15} * \xi$ and $f_{16} * \xi$.

At level $\mathfrak{n} = (\mathfrak{p}_2)^9$ we find $\dim V(\mathfrak{n}) = 31$. The oldspace may be written $7f_1 + 6f_2 + 2f_1 * \xi + 2f_2 * \xi + 2f_{15} + 2f_{16} + f_{15} * \xi + f_{16} * \xi$ (as in §9.5, note that the dimensions of oldspaces with $f = f * \nu$, such as $f_{15} * \xi$, grow at half the usual rate). The newspace consists of four modules of type h, these being twists of any one of them by 1, χ, ξ and $\xi\chi$. Representative newforms are h_6 and $\bar{h}_6$, as shown in Table 9.8, and the reader can verify that $\bar{h}_6 = h_6 * \chi$, as mentioned in §9.3.

Example 4. Let $\mathfrak{m} = \mathfrak{p}_5 = [5, w]$. The invertible residues are $\{\pm 1, \pm 2\}$, so $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ has order 2. Since $(\mathfrak{p}_2)^2 = \langle 2 \rangle \mapsto \pm 2$, the ray class group is cyclic of order 4, generated by any non-principal prime. Inspection of Tables 9.1 and 9.2 gives

$$\begin{aligned}
P^{\mathfrak{m}} &\supset \{41ab, 61ab, 101ab, 181ab, 241ab, 281ab, \dots, 11, 19, \dots\}, \\
\mathfrak{p}_{29a}P^{\mathfrak{m}} &\supset \{29ab, 89ab, 109ab, 149ab, 229ab, 269ab, 349ab, 389ab, \dots, 13, 17, \dots\}, \\
\mathfrak{p}_2P^{\mathfrak{m}} &\supset \{2, 7ab, 47ab, 67ab, 107ab, 127ab, 167ab, \dots\}, \\
\mathfrak{p}_{3a}P^{\mathfrak{m}} &\supset \{3ab, 23ab, 43ab, 83ab, 103ab, 163ab, \dots\},
\end{aligned}$$

and the character group is generated by the quartic character, χ say, given by

$$\mathfrak{p} \mapsto \begin{cases} i & \text{for } \mathfrak{p} \in \mathfrak{p}_{3a}P^{\mathfrak{m}}, \\ -1 & \text{for } \mathfrak{p} \in \mathfrak{p}_{29a}P^{\mathfrak{m}}, \\ -i & \text{for } \mathfrak{p} \in \mathfrak{p}_2P^{\mathfrak{m}}, \\ 1 & \text{for } \mathfrak{p} \in P^{\mathfrak{m}}. \end{cases} \tag{9.9}$$

Since $\chi^2 = \nu$, twisting by χ interchanges plusforms and minusforms. At level $\mathfrak{n} = \mathfrak{p}_2(\mathfrak{p}_5)^2$, we find $f_{12} = f_{11} * \chi$, and at level $\mathfrak{n} = (\mathfrak{p}_2)^2(\mathfrak{p}_5)^2$, we find $f_{26} = f_4 * \chi$.

If $\mathfrak{m} = \mathfrak{p}_{3a}$ or $\mathfrak{m} = \mathfrak{p}_{3b}$, then $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ is trivial. If $\mathfrak{m} = (\mathfrak{p}_{3a})^2 = [9, 7 + w]$, then $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times = \{\pm 1, \pm 2, \pm 4\}$ has order 3, and the corresponding *cubic* twist will not be visible in our tables; similarly, we do not see any twists with $\mathfrak{m} = \mathfrak{p}_{3b}^2$.

Example 5. Let $\mathfrak{m} = \mathfrak{p}_{3a}\mathfrak{p}_{3b} = \langle 3 \rangle$. The invertible residues are $\{\pm 1, \pm w\}$, so $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ has order 2. Since $(\mathfrak{p}_2)^2 = \langle 2 \rangle \mapsto \pm 1$, the ray class group has structure $C_2 \times C_2$. The four cosets of $P^{\mathfrak{m}}$ are

$$
\begin{aligned}
P^{\mathfrak{m}} &\supset \{61ab, 109ab, 181ab, 229ab, 241ab, 349ab, \dots, 11, 13, 17, 19, \dots\}, \\
\mathfrak{p}_5 P^{\mathfrak{m}} &\supset \{5, 29ab, 41ab, 89ab, 101ab, 149ab, 269ab, 281ab, 389ab, \dots\}, \\
\mathfrak{p}_2 P^{\mathfrak{m}} &\supset \{2, 23ab, 47ab, 83ab, 107ab, 167ab, \dots\}, \\
\mathfrak{p}_{7a} P^{\mathfrak{m}} &\supset \{7ab, 43ab, 67ab, 103ab, 127ab, 163ab, \dots\}.
\end{aligned}
$$

The character group is as follows, generated by the unramified character ν and a new character χ.

coset	1	ν	χ	$\nu\chi$
$P^{\mathfrak{m}}$	$+1$	$+1$	$+1$	$+1$
$\mathfrak{p}_5 P^{\mathfrak{m}}$	$+1$	$+1$	-1	-1
$\mathfrak{p}_2 P^{\mathfrak{m}}$	$+1$	-1	$+1$	-1
$\mathfrak{p}_{7a} P^{\mathfrak{m}}$	$+1$	-1	-1	$+1$

The character χ may be seen at level $\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}^2$. Firstly, there is a newform g_2 with $g_2 = g_2 * \chi$, a fact reflected in the high proportion of its Hecke eigenvalues that are zero. Secondly, the oldforms f_5 and $\bar{f}_5$ satisfy $\bar{f}_5 = f_5 * \chi$, but the χ-twist cannot be obtained by composing a $\mathfrak{p}_{3a}$-twist and a $\mathfrak{p}_{3b}$-twist (there being no such twists). This example demonstrates that unlike in Atkin-Lehner theory for $k = \mathbb{Q}$, or indeed for k imaginary quadratic of class number one, it is no longer sufficient to consider twists modulo prime powers only.

Another example is provided by the newforms f_{27} at level $\mathfrak{p}_2^2\mathfrak{p}_{3a}^2\mathfrak{p}_{3b}$ and $\bar{f}_{27}$ at level $\mathfrak{p}_2^2\mathfrak{p}_{3a}\mathfrak{p}_{3b}^2$, which are related by $\bar{f}_{27} = f_{27} * \nu\chi$.

For the remaining candidate moduli, nothing new is found. Thus, for $\mathfrak{m} = \mathfrak{p}_2\mathfrak{p}_{3a} = [2, 1+w][3, 1+w] = [6, 1+w]$, the invertible residues are $\{\pm 1\}$, so $(\mathfrak{O}/\mathfrak{m})^\times/\mathfrak{O}^\times$ is trivial. For $\mathfrak{m} = \mathfrak{p}_2\mathfrak{p}_5 = [2, 1+w][5, w] = [10, 5+w]$, the invertible residues are $\{\pm 1, \pm 3\}$; since all the generators to be considered are coprime to $\mathfrak{p}_2$, their residues modulo $\mathfrak{m}$ are determined by their residues modulo $\mathfrak{p}_5$ (by the Chinese Remainder Theorem) and we get nothing new, merely the characters modulo $\mathfrak{p}_5$ found above. Finally, for $\mathfrak{m} = \mathfrak{p}_{7a}$ or $\mathfrak{p}_{7b}$, the invertible residues are $\{\pm 1, \pm 2, \pm 3\}$, so the only new characters are cubic.

9.8 Base change lift of forms over $\mathbb{Q}$

Let $f = \sum a(n)e^{2\pi inz}$ be a weight 2 cuspform (over $\mathbb{Q}$) for $\Gamma_0(N)$ with character χ, and let $k \mid \mathbb{Q}$ be a quadratic field extension. There is a well-known process of "base change lift" from $\mathbb{Q}$ to k which constructs from f a weight 2 modular form F for $\Gamma_0(\mathfrak{n})$ for suitable $\mathfrak{n}$. Lifting may be described in the language of automorphic representations, or (as below) in the more classical language of automorphic forms.

Historically, real quadratic fields were treated first. The early paper of Doi and Naganuma [DN69] dealt with the special case $h(k) = 1$, $N = 1$ and $\chi = 1$. Those authors defined the lifted Dirichlet series $L(F, s)$ directly (by defining its coefficients in terms of the $a(n)$, as in (9.11) below) and derived its functional equation by exhibiting it as the integral of f against a certain Maass wave form.

Later, Asai [Asa78] considered the "Doi-Naganuma lifting" in the context of imaginary quadratic fields, restricting to the case of $\mathbb{Q}(\sqrt{-D})$ for $D \in \{7, 11, 19, 43, 67, 163\}$, to $N = 1$ and $\chi = \left(\frac{-D}{*}\right)$; here, the lift was defined by integrating f against a certain theta function. Asai's results were generalised to general class number, to arbitrary congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$, and to general χ by Friedberg [Fri83].

For a concise summary of relevant facts regarding base change lift from $\mathbb{Q}$ to an imaginary quadratic field of discriminant Δ (at least for $h(k) = 1$), see [Cre92]. In particular,

(i) Every cusp form f of weight 2 for $\Gamma_0(N)$ lifts to a form of weight 2 for $\Gamma_0(\mathfrak{n})$, where $\mathfrak{n}$ is an ideal of k divisible only by primes dividing $N\Delta$.

(ii) A cusp form F of weight 2 for $\Gamma_0(\mathfrak{n})$ is the lift of a form f on some $\Gamma_0(N)$ if and only if the Fourier coefficients of F satisfy $a(\mathfrak{p}) = a(\bar{\mathfrak{p}})$ for all $\mathfrak{p}$.

By this result, our plusforms satisfying $F = \bar{F}$ (see §9.3) are lifts of cuspforms defined over $\mathbb{Q}$; below, we aim to identify these cuspforms.

Proposition 123. *Let k be an imaginary quadratic field of discriminant Δ, and let χ_k be the associated quadratic Dirichlet character $x \mapsto \left(\frac{\Delta}{x}\right)$. Let $f = \sum a_n e^{2\pi inz}$ be a normalised newform for $\Gamma_0(N)$ with Dirichlet character χ. Let $\mathfrak{n}$ be an ideal of k and let F be a normalised newform for $\Gamma_0(\mathfrak{n})$ with unramified character ψ, and write $T_\mathfrak{p}F = C(\mathfrak{p})F$ for all primes $\mathfrak{p}$. Assume that F is a lift of f. Then*

(i) *if* $\mathfrak{p}$ *lies above* p*, then* $\mathfrak{p} \mid \mathfrak{n} \iff p \mid N$*;*

(ii) *if* $\chi_k(p) = 1$*, so* $\langle p \rangle = \mathfrak{p}\bar{\mathfrak{p}}$*, then* $C(\mathfrak{p}) = C(\bar{\mathfrak{p}}) = a(p)$*; if further* $p \nmid N$ *then* $\chi(p) = \psi(\mathfrak{p}) = \psi(\bar{\mathfrak{p}})$*;*

(iii) *if* $\chi_k(p) = -1$*, so* $\langle p \rangle = \mathfrak{p}$ *is prime, then* $C(\mathfrak{p}) = a(p)^2 - 2p\chi(p)$ *and* $\chi(p)^2 = 1$*.*

The case $\chi_k(p) = 0$ is treated in Corollary 124. Note that $\chi(p) = 0$ if $p \mid N$, even if χ is the trivial character, so that at bad inert primes, our formula for $C(\mathfrak{p})$ is not in agreement with the formula on p413 of [Cre92].

Sketch proof. Let $L(f, s) = \sum a_n n^{-s}$ be the L-series of f, let $L(f, \chi_k, s) = \sum a_n \chi_k(n) n^{-s}$ be its twist by χ_k, and let $L(F, s) = \sum C(\mathfrak{a}) \, \mathbf{N}(\mathfrak{a})^{-s}$ be the L-series attached to F. Then formula (3.5.2) in [Fri83] gives

$$L(f, s) \cdot L(f, \chi_k, s) = L(F, s).$$

We wish to express both sides as Euler products in order to equate Euler factors locally, i.e. for p on the left and the primes $\mathfrak{p}$ above p on the right. To obtain Euler products, we need newforms. Since $f \big| R_{\chi_k}$ need not be new (see §2.1.4) we replace it by the newform $f * \chi_k$ at level N' and replace $L(f, \chi_k, s)$ by $L(f * \chi_k, s) = \sum b(n) e^{2\pi i n z}$. By (2.8),

$$L(f, s)^{-1} = \prod_{p \mid N} \bigl(1 - a(p) p^{-s}\bigr) \prod_{p \nmid N} \bigl(1 - a(p) p^{-s} + \chi(p) p^{1-2s}\bigr),$$

and similarly for $L(f * \chi_k, s)$ with $a(p)$ replaced by $b(p)$. On the other hand, by (7.11),

$$L(F, s)^{-1} = \prod_{\mathfrak{p} \mid \mathfrak{n}} \bigl(1 - C(\mathfrak{p}) \, \mathbf{N}(\mathfrak{p})^{-s}\bigr) \prod_{\mathfrak{p} \nmid \mathfrak{n}} \bigl(1 - C(\mathfrak{p}) \, \mathbf{N}(\mathfrak{p})^{-s} + \psi(\mathfrak{p}) \, \mathbf{N}(\mathfrak{p})^{1-2s}\bigr).$$

Part (i) follows at once from the need to equate the right number of Euler factors of the right shape. Now let p be a prime with $p \nmid \Delta$, so p does not ramify. By Theorems 6 and 7 of [AL70], $b(p) = \chi_k(p) a(p)$, and p occurs to the same power in N and N'. First, suppose that $\chi_k(p) = 1$, so that p splits; write $\langle p \rangle = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathbf{N}(\mathfrak{p}) = \mathbf{N}(\bar{\mathfrak{p}}) = p$. If $p \nmid N$, then neither $\mathfrak{p}$ nor $\bar{\mathfrak{p}}$ divides $\mathfrak{n}$, and equating Euler factors gives

$$\bigl(1 - a(p) p^{-s} + \chi(p) p^{1-2s}\bigr)^2 = \bigl(1 - C(\mathfrak{p}) p^{-s} + \psi(\mathfrak{p}) p^{1-2s}\bigr)\bigl(1 - C(\bar{\mathfrak{p}}) p^{-s} + \psi(\bar{\mathfrak{p}}) p^{1-2s}\bigr),$$

implying that $C(\mathfrak{p}) = C(\bar{\mathfrak{p}}) = a(p)$ and $\chi(p) = \psi(\mathfrak{p}) = \psi(\bar{\mathfrak{p}})$, as claimed. If $p \mid N$, then $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ divide $\mathfrak{n}$, and we obtain

$$\left(1 - a(p)p^{-s}\right)^2 = \left(1 - C(\mathfrak{p})p^{-s}\right)\left(1 - C(\bar{\mathfrak{p}})p^{-s}\right),$$

and again $C(\mathfrak{p}) = C(\bar{\mathfrak{p}}) = a(p)$. Now suppose that $\chi_k(p) = -1$, so that p is inert, $\langle p \rangle = \mathfrak{p}$ say, where $\mathbf{N}(\mathfrak{p}) = p^2$. Note that $\psi(\mathfrak{p}) = 1$, since $\mathfrak{p}$ is principal and ψ is unramified (by assumption). If $p \nmid N$, then $\mathfrak{p} \nmid \mathfrak{n}$, and equating Euler factors gives

$$\left(1 - a(p)p^{-s} + \chi(p)p^{1-2s}\right)\left(1 + a(p)p^{-s} + \chi(p)p^{1-2s}\right) = 1 - C(\mathfrak{p})p^{-2s} + \psi(\mathfrak{p})p^{2(1-2s)},$$

implying $C(\mathfrak{p}) = a(p)^2 - 2p\chi(p)$ and $\chi(p)^2 = 1$. If $p \mid N$, then $\mathfrak{p} \mid \mathfrak{n}$, and we obtain

$$\left(1 - a(p)p^{-s}\right)\left(1 + a(p)p^{-s}\right) = 1 - C(\mathfrak{p})p^{-2s},$$

implying $C(\mathfrak{p}) = a(p)^2$. We may write this as $C(\mathfrak{p}) = a(p)^2 - 2p\chi(p)$ since χ is a Dirichlet character modulo N, so $\chi(p) = 0$ for $p \mid N$. □

Corollary 124. *With notation as above, assume that $\chi_k(p) = 0$, i.e. that p is ramified. Write $\langle p \rangle = \mathfrak{p}^2$. Then $C(\mathfrak{p}) = a(p) + b(p)$, and if $\mathfrak{p} \nmid \mathfrak{n}$, then $\chi(p) = \psi(\mathfrak{p})$.*

Sketch proof. Note that $\mathbf{N}(\mathfrak{p}) = p$. There are several cases. If $p \nmid N$, then $p^2 \mid N'$ by Theorems 6 and 7 of [AL70], so that $b(p) = 0$ by (2.7). Equating Euler factors gives

$$1 - a(p)p^{-s} + \chi(p)p^{1-2s} = 1 - C(\mathfrak{p})p^{-s} + \psi(\mathfrak{p})p^{1-2s},$$

whence $C(\mathfrak{p}) = a(p)$ and $\chi(p) = \psi(\mathfrak{p})$. Next, suppose $p \mid N$ but $p^2 \nmid N$. Again $p^2 \mid N'$ and $b(p) = 0$. We equate

$$1 - a(p)p^{-s} = 1 - C(\mathfrak{p})p^{-s},$$

giving $C(\mathfrak{p}) = a(p)$. In both cases above, it is more symmetrical to write $C(\mathfrak{p}) = a(p)+b(p)$; this covers also the cases in which $p^2 \nmid N'$. Finally, if p^2 divides both N and N', then $a(p) = b(p) = 0$, and equating Euler factors gives $C(\mathfrak{p}) = 0 = a(p) + b(p)$. □

Corollary 125. *Let $k = \mathbb{Q}(\sqrt{-5})$. Let F be a newform for $\Gamma_0(\mathfrak{n})$ with unramified character ψ. Assume that F is the lift of a newform f for $\Gamma_0(N)$ with character χ. If F is a plusform, then $\chi = 1$, whilst if F is a minusform, then χ is given by*

$$\chi(p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases} \tag{9.10}$$

For p not ramified and $\mathfrak{p} \mid p$ the Fourier coefficients of F and f are related by

$$C(\mathfrak{p}) = \begin{cases} a(p) & \text{if } p \text{ splits, and} \\ a(p)^2 - 2p\chi(p) & \text{if } p \text{ is inert.} \end{cases} \tag{9.11}$$

Proof. Note that $\chi(-1) = 1$, since $f = f|\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = \chi(-1)f$. (See [Kob84, p138], for example.) We have

$$\chi_k(p) = \begin{cases} 1 & \text{if } p \equiv 1,3,7,9 \pmod{20}, \\ -1 & \text{if } p \equiv 11,13,17,19 \pmod{20}. \end{cases}$$

If $\psi = 1$, then $\chi(p) = 1$ for $p \equiv 1,3,7,9 \pmod{20}$. Since $\chi(-1) = 1$, this implies $\chi = 1$. If $\psi = \nu$, then $\chi(p) = 1$ for $p \equiv 1,9 \pmod{20}$ and $\chi(p) = -1$ for $p \equiv 3,7 \pmod{20}$. Using $\chi(-1) = 1$, we deduce (9.10). □

Example. At level $\mathfrak{n} = (\mathfrak{p}_2)^2(\mathfrak{p}_5)$, there is the new plusform f_4 and its unramified twist $f_4 * \nu$. From Table 9.4, we know that both satisfy $C(\mathfrak{p}) = C(\bar{\mathfrak{p}})$ for all $\mathfrak{p}$. So they must be lifts of forms over $\mathbb{Q}$ with eigenvalues

	split/ramified														inert				
p	2	3	5	7	23	29	41	43	47	61	67	83	89	…	11	13	17	19	…
f_4	$*$	2	$*$	−2	−6	6	6	10	6	2	−2	−6	−6	…	0	±2	±6	±4	…
$f_4 * \nu$	$*$	−2	$*$	2	6	6	6	−10	−6	2	2	6	−6	…	0	±2	±6	±4	…

Cremona's tables contain four forms with matching eigenvalues:

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89
20A	–	−2	+	2	0	2	−6	−4	6	6	−4	2	6	−10	−6	−6	12	2	2	−12	2	8	6	−6
80B	–	2	+	−2	0	2	−6	4	−6	6	4	2	6	10	6	−6	−12	2	−2	12	2	−8	−6	−6
100A	–	2	+	−2	0	−2	6	−4	−6	6	−4	−2	6	10	6	6	12	2	−2	−12	−2	8	−6	−6
400E	–	−2	+	2	0	−2	6	4	6	6	4	−2	6	−10	−6	6	−12	2	2	12	−2	−8	6	−6

The forms listed above are all twists of 20A; thus 100A = 20A $*$ 5, 80B = 20A $*$ -4 and 400E = 20A $*$ -20. The forms 80B and 100A lift to f_4, whilst the forms 20A and 400E lift to $f_4 * \nu$. The situation is entirely typical, and may be illustrated with the following figure:

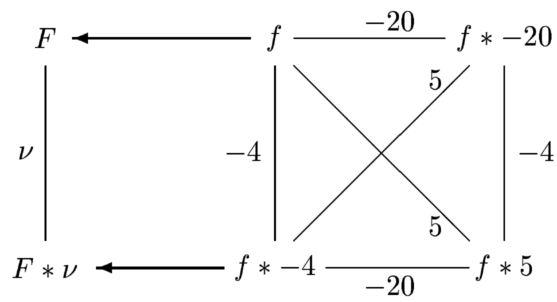

Table 9.9 below lists, for each plusform in our tables with $C(\mathfrak{p}) = C(\bar{\mathfrak{p}})$, the forms over $\mathbb{Q}$ of which it is a base change lift. We do not have a similar table for minusforms, since we have not had access to tables of forms for $\Gamma_0(N)$ with character (9.10).

Remark. The process of lifting has an obvious counterpart in the theory of elliptic curves: every elliptic curve $E/\mathbb{Q}$ may be viewed as a curve E/k. It is thought (and in most cases, known [Wil95]) that $E/\mathbb{Q}$ corresponds to a newform f (with trivial character) for $\Gamma_0(N)$ (where N is the conductor); naturally, we expect E/k to correspond to the lift of f. In general, it is our plusforms which should correspond to elliptic curves over k (or to abelian varieties over $\mathbb{Q}$ with "extra twist" by χ_k [Cre92]); our minusforms do not (as is clear from the presence of ν in the Euler factors).

New plusforms F for $\Gamma_0(\mathfrak{n})$			Corresponding new-forms for $\Gamma_0(N)$
$\mathfrak{n}$	$\mathbf{N}(\mathfrak{n})$	F	
$(\mathfrak{p}_2)^2\mathfrak{p}_5$	20	f_4	80B, 100A
		$f_4 * \nu$	20A, 400E
$(\mathfrak{p}_2)^3\mathfrak{p}_5$	40	f_7	80A, 200C
		$f_7 * \nu$	40A, 400A
$\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	45	f_9	75B, 240D
		$f_9 * \nu$	15A, 1200J
$\mathfrak{p}_2(\mathfrak{p}_5)^2$	50	f_{11}	50A, 400B
		$f_{11} * \nu$	50B, 400C
$(\mathfrak{p}_2)^6$	64	f_{16}	32A, 800A
$(\mathfrak{p}_2)^3\mathfrak{p}_{3a}\mathfrak{p}_{3b}$	72	f_{18}	48A, 600D
		$f_{18} * \nu$	24A, 1200A
$\mathfrak{p}_2\mathfrak{p}_{3a}\mathfrak{p}_{3b}\mathfrak{p}_5$	90	f_{22}	150C, 240B
		$f_{22} * \nu$	30A, 1200P
$\mathfrak{p}_2\mathfrak{p}_{7a}\mathfrak{p}_{7b}$	98	f_{25}	112C, 350D
		$f_{25} * \nu$	14A, 2800V
$\mathfrak{p}_{11}$	121	f_{30}	176B, 275B
		$f_{30} * \nu$	11A, 4400M

Table 9.9: Plusforms obtained by lifting from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{-5})$

Bibliography

[AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[Asa78] Tetsuya Asai. On the Doi-Naganuma lifting associated with imaginary quadratic fields. *Nagoya Math. J.*, 71:149–167, 1978.

[Bea83] Alan F. Beardon. *The Geometry of Discrete Groups*, volume 91 of *Graduate Texts in Mathematics*. Springer-Verlag, 1983.

[Bia92] Luigi Bianchi. Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari. *Math. Ann.*, 40:332–412, 1892.

[Car71] Henri Cartan. *Differential Forms*. Kershaw, London, 1971. Translated from the original French text *Formes différentielles*, first published by Hermann, Paris, 1967.

[Cas86] J. W. S. Cassels. *Local Fields*, volume 3 of *LMS Student Texts*. CUP, 1986.

[CF67] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. Academic Press, 1967.

[Cha94] Robin J. Chapman. Generalized Bianchi groups. Mathematics Department Preprint Series M94/45, University of Exeter, 1994.

[Coh82] Paul M. Cohn. *Algebra*, volume 1. John Wiley & Sons, 2nd edition, 1982.

[Coh89] Paul M. Cohn. *Algebra*, volume 2. John Wiley & Sons, 2nd edition, 1989.

[CR62] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Wiley (Interscience), New York, 1962.

[Cre81] John E. Cremona. *Modular Symbols.* D.Phil. thesis, Oxford University, 1981.

[Cre84] John E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Mathematica*, 51:275–323, 1984.

[Cre88] John E. Cremona. On GL(n) of a Dedekind domain. *Quart. J. Math. Oxford (2)*, 39:423–426, 1988.

[Cre92] John E. Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc.*, 45(2):404–416, 1992.

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves.* CUP, 2nd edition, 1997. (Extended data tables at `ftp://euclid.ex.ac.uk/pub/cremona/data`).

[CW94] John E. Cremona and Elise Whitley. Periods of cusp forms and elliptic curves over imaginary quadratic fields. *Mathematics of Computation*, 62(205):407–429, January 1994.

[DN69] Koji Doi and Hidehisa Naganuma. On the functional equation of certain Dirichlet series. *Inventiones Math.*, 9:1–14, 1969.

[dR55] G. de Rham. *Variétés Différentiables. Formes courants, formes harmoniques.* Number 1222 in Actualités Sci. Indust. Hermann, Paris, 1955.

[Fig95] Luiz Figueiredo. *Serre's Conjecture over Imaginary Quadratic Fields.* PhD thesis, Cambridge University, 1995.

[FM98] Gerhard Frey and Michael Müller. Arithmetic of modular curves and applications. Preprint, Institut für Experimentelle Mathematik, Essen, 1998.

[Fri83] Solomon Friedberg. On the imaginary quadratic Doi-Naganuma lifting of modular forms of arbitrary level. *Nagoya Math. J.*, 92:1–20, 1983.

[FT91] A. Fröhlich and M. J. Taylor. *Algebraic number theory.* CUP, 1991.

[Gar81] Dennis Garbanati. Class field theory summarized. *Rocky Mountain J. Math.*, 11(2):195–295, 1981.

[Gar90] Paul B. Garrett. *Holomorphic Hilbert Modular Forms.* Wadsworth& Brooks/Cole, 1990.

[Gel75] Stephen S. Gelbart. *Automorphic Forms on Adele Groups.* Number 83 in Annals of Mathematics Studies. Princeton University Press, 1975.

[HR63] Edwin Hewitt and Kenneth A. Ross. *Abstract Harmonic Anaylsis, volume I*, volume 115 of *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, 1963.

[HST93] Michael Harris, David Soudry, and Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields I: lifting to $GSp_4(\mathbb{Q})$. *Inventiones Math.*, 112:377–411, 1993.

[Hum15] G. Humbert. Sur la réduction des formes d'Hermite dans un corps quadratique imaginaire. *Compt. Rend. Acad. Sci. Paris*, 161:189–196, 1915.

[Kne65] Martin Kneser. Starke Approximation in algebraischen Gruppen. I. *J. reine angew. Math.*, 218:190–203, 1965.

[Kne67] Martin Kneser. Semi-simple algebraic groups. In Cassels and Fröhlich [CF67], pages 250–265.

[Kob84] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Graduate Texts in Mathematics.* Springer-Verlag, 1984.

[Kur78] P. F. Kurcǎnov. Cohomology of discrete groups and Dirichlet series connected with Jacquet-Langlands cusp forms. *Math. USSR Izvestija*, 12(3):543–555, 1978.

[Lan76] Serge Lang. *Introduction to Modular Forms*, volume 222 of *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, 1976.

[Man72] J. I. Manin. Parabolic points and zeta functions of modular curves. *Math. USSR Izv.*, 6(1), 1972.

[Miy71] Toshitsune Miyake. On automorphic forms on GL_2 and Hecke operators. *Ann. Math.*, 94:174–189, 1971.

[ML71] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, 1971.

[Neu86] Jürgen Neukirch. *Class Field Theory*, volume 280 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1986.

[O'M63] O. T. O'Meara. *Introduction to Quadratic Forms*, volume 117 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1963.

[Sch92] Alexander Scheutzow. Computing rational cohomology and Hecke eigenvalues for Bianchi groups. *Journal of Number Theory*, 40:317–328, 1992.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, 1973.

[Sha90] I. R. Shafarevich. *Algebra I. Basic Notions of Algebra*, volume 11 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, 1990.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Iwanami Shoten and Princeton University Press, 1971.

[Sil86] Joseph A. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[Spi79] Michael Spivak. *A Comprehensive Introduction to Differential Geometry.* Publish or Perish, Berkeley, 2nd edition, 1979. Five volumes.

[ST87] I. N. Stewart and D. O. Tall. *Algebraic Number Theory.* Chapman and Hall, 2nd edition, 1987.

[Swa71] Richard G. Swan. Generators and relations for certain special linear groups. *Adv. Math.*, 6:1–71, 1971.

[Swi92] H. P. F. Swinnerton-Dyer. Elliptic modular functions. Lecture notes accompanying Part III lecture course, Cambridge University, Lent Term 1992.

[Tat67] J. T. Tate. Fourier Analysis in Number Fields and Hecke's Zeta-Functions. In Cassels and Fröhlich [CF67], pages 305–347.

[Tay94] Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields II. *Inventiones Math.*, 116:619–643, 1994.

[Tin75] D. J. Tingley. *Elliptic Curves Uniformized by Modular Functions.* D.Phil. thesis, Oxford University, 1975.

[Vog85] Karen Vogtmann. Rational homology of Bianchi groups. *Math. Ann.*, 272:399–419, 1985.

[Wat52] G. N. Watson. *A Treatise on the Theory of Bessel Functions.* CUP, 2nd edition, 1952.

[Wei67a] André Weil. *Basic Number Theory*, volume 144 of *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, 1967.

[Wei67b] André Weil. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Mathematische Annalen*, 168:149–156, 1967.

[Wei71] André Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture Notes in Mathematics.* Springer-Verlag, 1971.

[Whi90] Elise Whitley. *Modular Forms and Elliptic Curves over Imaginary Quadratic Number Fields.* PhD thesis, Exeter University, 1990.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.*, 141:443–551, 1995.

[Woo86] L. M. Woodward. Elementary exposition of differential forms. In J. A. Gregory, editor, *The Mathematics of Surfaces*, IMA Conference Series, No. 6, pages 73–93, Clarendon Press, Oxford, 1986.