

SL2Reps

**Constructs congruent representations of
 $SL(2, \mathbb{Z})$.**

0.1

12 November 2021

Siu-Hung Ng

Yilong Wang

Samuel Wilson

Siu-Hung Ng

Email: rng@math.lsu.edu

Homepage: <https://www.math.lsu.edu/~rng/>

Yilong Wang

Email: wyl@bimsa.cn

Homepage: <https://yilongwang11.github.io>

Samuel Wilson

Email: swil311@lsu.edu

Copyright

© 2021 by Siu-Hung Ng, Yilong Wang, and Samuel Wilson

This package is free software; you can redistribute it and/or modify it under the terms of the [GNU General Public License](#) as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

Acknowledgements

This project is partially supported by NSF grant DMS 1664418.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | Installation | 4 |
| 1.2 | Usage | 4 |
| 2 | Description | 5 |
| 2.1 | Construction | 5 |
| 2.2 | Weil representation types | 7 |
| 3 | Irreducible representations of prime-power level | 10 |
| 3.1 | Representations of type D | 10 |
| 3.2 | Representations of type N | 11 |
| 3.3 | Representations of type R | 11 |
| 4 | Lists of representations | 13 |
| 4.1 | Lists by degree | 13 |
| 4.2 | Lists by level | 14 |
| 4.3 | Lists of exceptional representations | 14 |
| 5 | Methods for testing | 15 |
| 5.1 | Testing | 15 |
| | References | 16 |
| | Index | 17 |

Chapter 1

Introduction

This package, `SL2Reps`, provides methods for constructing and testing matrix presentations of the representations of $SL_2(\mathbb{Z})$ whose kernels are congruence subgroups of $SL_2(\mathbb{Z})$.

Irreducible representations of prime-power level are constructed individually by using the Weil representations of quadratic modules, and from these a list of all representations of a given degree or level can be produced. The format is designed for the study of modular tensor categories in particular.

1.1 Installation

To install `SL2Reps`, first download it from <https://github.com/ontoclasml/sl2-reps>, then place it in the `pkg` subdirectory of your GAP installation (or in the `pkg` subdirectory of any other GAP root directory, for example one added with the `-l` argument).

`SL2Reps` is then loaded with the GAP command

```
gap> LoadPackage( "SL2Reps" );
```

1.2 Usage

Specific irreducible representations may be constructed via the methods in Chapter 3, while lists of irreducible representations with a given degree or level may be constructed with those in Chapter 4.

This package uses an `InfoClass`, `InfoSL2Reps`. It may be set to 0 (silent), 1 (info), or 2 (verbose). To change it, use

```
gap> SetInfoLevel( InfoSL2Reps, k );
```

Chapter 2

Description

The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by $\mathfrak{s} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $\mathfrak{t} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (which satisfy the relations $\mathfrak{s}^4 = (\mathfrak{st})^3 = \mathrm{id}$). Thus, any complex representation ρ of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{C}^n (where $n \in \mathbb{Z}^+$ is called the *degree* of ρ) is determined by the $n \times n$ matrices $S = \rho(\mathfrak{s})$ and $T = \rho(\mathfrak{t})$.

This package constructs irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ which factor through $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for some $\ell \in \mathbb{Z}^+$; the smallest such ℓ is called the *level* of the representation. One may equivalently say that the kernel of the representation is a congruence subgroup. It has been shown that any representation of $\mathrm{SL}_2(\mathbb{Z})$ arising from a modular tensor category has this property [DLN15].

We therefore present representations in the form of a record `rec(S, T, degree, level, name)`, where the name follows the conventions of [NW76].

Note that our definition of \mathfrak{s} follows that of [Nob76]; other authors prefer the inverse, i.e. $\mathfrak{s} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ (under which convention the relations are $\mathfrak{s}^4 = \mathrm{id}$, $(\mathfrak{st})^3 = \mathfrak{s}^2$). When working with that convention, one must invert the S matrices output by this package.

Throughout, we denote by \mathfrak{e} the map $k \mapsto e^{2\pi i k}$ (an isomorphism from \mathbb{Q}/\mathbb{Z} to the group of finite roots of unity in \mathbb{C}). For a group G , we denote by \widehat{G} the character group $\mathrm{Hom}(G, \mathbb{C}^\times)$.

2.1 Construction

Any representation ρ of $\mathrm{SL}_2(\mathbb{Z})$ can be decomposed into a direct sum of irreducible representations (irreps). Further, if ρ has finite level, each irrep can be factorized into a tensor product of irreps whose levels are powers of distinct primes (using the Chinese remainder theorem). Therefore, to characterize all finite-dimensional representations of $\mathrm{SL}_2(\mathbb{Z})$ of finite level, it suffices to consider irreps of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ for primes p and positive integers λ .

2.1.1 Weil representations

Such representations may be constructed using Weil representations as described in [Nob76, Section 1]. We give a brief summary of the process here. First, if M is any additive abelian group, a *quadratic form* on M is a map $Q : M \rightarrow \mathbb{Q}/\mathbb{Z}$ such that

- $Q(-x) = Q(x)$ for all $x \in M$, and
- $B(x, y) = Q(x + y) - Q(x) - Q(y)$ defines a \mathbb{Z} -bilinear map $M \times M \rightarrow \mathbb{Q}/\mathbb{Z}$.

Now let p be a prime number and $\lambda \in \mathbb{Z}^+$. Choose a $\mathbb{Z}/p^\lambda\mathbb{Z}$ -module M and a quadratic form Q on M such that the pair (M, Q) is of one of the three types described in Section 2.2. Each such M

is a ring, and has at most 2 cyclic factors as an additive group. Those with 2 cyclic factors may be identified with a quotient of the quadratic integers, giving a norm on M . Then the *quadratic module* (M, Q) gives rise to a representation of $SL_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ on the vector space $V = \mathbb{C}^M$ of complex-valued functions on M . This representation is denoted $W(M, Q)$. Note that the *central charge* of (M, Q) is given by $S_Q(-1) = \frac{1}{\sqrt{|M|}} \sum_{x \in M} \mathbf{e}(Q(x))$.

We may construct subrepresentations $W(M, Q, \chi)$ of $W(M, Q)$ as follows. Denote

$$\text{Aut}(M, Q) = \{\varepsilon \in \text{Aut}(M) \mid Q(\varepsilon x) = Q(x) \text{ for all } x \in M\}.$$

We then associate to (M, Q) an abelian subgroup $\mathfrak{A} \leq \text{Aut}(M, Q)$; the structure of this group depends on (M, Q) and is described in Section 2.2. Note that \mathfrak{A} has at most two cyclic factors, whose generators we denote by α and β . Now, let $\chi \in \widehat{\mathfrak{A}}$ be a 1-dimensional representation (*character*) of \mathfrak{A} , and define

$$V_\chi = \{f \in V \mid f(\varepsilon x) = \chi(\varepsilon)f(x) \text{ for all } x \in M \text{ and } \varepsilon \in \mathfrak{A}\},$$

which is a $SL_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ -invariant subspace of V . We then denote by $W(M, Q, \chi)$ the subrepresentation of $W(M, Q)$ on V_χ . Note that $W(M, Q, \chi) \cong W(M, Q, \bar{\chi})$.

2.1.2 Primitive characters

For the abelian groups $\mathfrak{A} \leq \text{Aut}(M, Q)$, we will frequently refer to a character $\chi \in \widehat{\mathfrak{A}}$ as being *primitive*. With the exception of a single family of modules of type R (the *extremal* case, for which see Section 2.2.4), primitivity amounts to the following: there exists some $\varepsilon \in \mathfrak{A}$ such that $\chi(\varepsilon) \neq 1$ and ε fixes the submodule $pM \subset M$ pointwise. There exists a subgroup $\mathfrak{A}_0 \leq \mathfrak{A}$ such that a non-trivial $\chi \in \widehat{\mathfrak{A}}$ is primitive if and only if χ is injective on \mathfrak{A}_0 (or, equivalently, if $\mathfrak{A}_0 \cap \ker \chi$ is trivial).

Explicit descriptions of the group \mathfrak{A}_0 for each type are given in Section 2.2 and may be used to determine the primitive characters.

2.1.3 Irrep types

The prime-power irreps then fall into three cases.

- The overwhelming majority are of the form $W(M, Q, \chi)$ for χ primitive and $\chi^2 \neq 1$; we call these *standard*. This includes the primitive characters from the extremal case.
- A finite number, and a single infinite family arising from the extremal case (Section 2.2.4), are instead constructed by using non-primitive characters or primitive characters χ with $\chi^2 = 1$. We call these *non-standard*.
- Finally, 18 *exceptional* irreps are constructed as tensor products of two irreps from the other two cases.

All the finite-dimensional irreducible representations of $SL_2(\mathbb{Z})$ of finite level can now be constructed by taking tensor products of these prime-power irreps. Note that, if two representations are determined by pairs $[S1, T1]$ and $[S2, T2]$, then the pair for their tensor product may be calculated via the GAP command `KroneckerProduct`, namely as `[KroneckerProduct(S1, S2), KroneckerProduct(T1, T2)]`.

2.2 Weil representation types

2.2.1 Type D

Let p be prime. If $p = 2$ or $p = 3$, let $\lambda \geq 2$; otherwise, let $\lambda \geq 1$. Then the Weil representation arising from the quadratic module with

$$M = \mathbb{Z}/p^\lambda \mathbb{Z} \oplus \mathbb{Z}/p^\lambda \mathbb{Z} \quad \text{and} \quad Q(x, y) = \frac{xy}{p^\lambda}$$

is said to be of type D and denoted $D(p, \lambda)$. Information on type D quadratic modules may be obtained via `SL2ModuleD` (3.1.1), and subrepresentations of $D(p, \lambda)$ with level p^λ may be constructed via `SL2IrrepD` (3.1.2).

The group

$$\mathfrak{A} \cong (\mathbb{Z}/p^\lambda \mathbb{Z})^\times$$

acts on M by $a(x, y) = (a^{-1}x, ay)$ and is thus identified with a subgroup of $\text{Aut}(M, Q)$; see [NW76, Section 2.1]. The group \mathfrak{A} has order $p^{\lambda-1}(p-1)$ and $\mathfrak{A} = \langle \alpha \rangle \times \langle \beta \rangle$. The relevant information for type D quadratic modules is as follows:

| p | λ | α | β | \mathfrak{A}_0 |
|-------|-----------|---|-----------------|--------------------------|
| > 2 | 1 | 1 | $ \beta = p-1$ | $\langle 1 \rangle$ |
| > 2 | > 1 | $ \alpha = p^{\lambda-1}$ (e.g. $\alpha = 1+p$) | $ \beta = p-1$ | $\langle \alpha \rangle$ |
| 2 | 2 | 1 | -1 | $\langle 1 \rangle$ |
| 2 | > 2 | $ \alpha = 2^{\lambda-2}$ (e.g. $\alpha = 5$) | -1 | $\langle \alpha \rangle$ |

When \mathfrak{A}_0 is trivial, every non-trivial character $\chi \in \widehat{\mathfrak{A}}$ is primitive.

2.2.2 Type N

Let p be prime and $\lambda \geq 1$. If $p \neq 2$, let u be a positive integer so that $u \equiv 3 \pmod{4}$ with $-u$ a quadratic non-residue mod p ; if $p = 2$, let $u = 3$. Then the Weil representation arising from the quadratic module with

$$M = \mathbb{Z}/p^\lambda \mathbb{Z} \oplus \mathbb{Z}/p^\lambda \mathbb{Z} \quad \text{and} \quad Q(x, y) = \frac{x^2 + xy + \frac{1+u}{4}y^2}{p^\lambda}$$

is said to be of type N and denoted $N(p, \lambda)$. Information on type N quadratic modules may be obtained via `SL2ModuleN` (3.2.1), and subrepresentations of $N(p, \lambda)$ with level p^λ may be constructed via `SL2IrrepN` (3.2.2).

The additive group M is a ring with multiplication given by

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - \frac{1+u}{4}y_1y_2, x_1y_2 + x_2y_1 + y_1y_2)$$

and identity element $(1, 0)$. We define a norm $\text{Nm}(x, y) = x^2 + xy + \frac{1+u}{4}y^2$ on M ; then the multiplicative subgroup

$$\mathfrak{A} = \{\varepsilon \in M^\times \mid \text{Nm}(\varepsilon) = 1\}$$

of M^\times acts on M by multiplication and is identified with a subgroup of $\text{Aut}(M, Q)$; see [NW76, Section 2.2].

The group \mathfrak{A} has order $p^{\lambda-1}(p+1)$ and $\mathfrak{A} = \langle \alpha \rangle \times \langle \beta \rangle$. The relevant information for type N quadratic modules is as follows:

| p | λ | α | β | \mathfrak{A}_0 |
|-------|-----------|----------------------------|-------------------|---------------------------|
| > 2 | 1 | $(1, 0)$ | $ \beta = p + 1$ | $\langle (1, 0) \rangle$ |
| > 2 | > 1 | $ \alpha = p^{\lambda-1}$ | $ \beta = p + 1$ | $\langle \alpha \rangle$ |
| 2 | 1 | $(1, 0)$ | $ \beta = 3$ | $\langle (1, 0) \rangle$ |
| 2 | 2 | $(1, 0)$ | $ \beta = 6$ | $\langle (-1, 0) \rangle$ |
| 2 | > 2 | $ \alpha = p^{\lambda-2}$ | $ \beta = 6$ | $\langle \alpha \rangle$ |

When \mathfrak{A}_0 is trivial, every non-trivial character $\chi \in \widehat{\mathfrak{A}}$ is primitive.

2.2.3 Type R, generic cases

The structure of the quadratic module (M, Q) of type R depends upon three additional parameters: σ , r , and t . Details are as follows:

- If p is odd, let $\lambda \geq 2$, $\sigma \in \{1, \dots, \lambda\}$, and $r, t \in \{1, u\}$ with u a quadratic non-residue mod p . Then define

$$M = \mathbb{Z}/p^\lambda \mathbb{Z} \oplus \mathbb{Z}/p^{\lambda-\sigma} \mathbb{Z} \quad \text{and} \quad Q(x, y) = \frac{r(x^2 + p^\sigma t y^2)}{p^\lambda}.$$

When $\sigma = \lambda$, the second factor of M is trivial, and (M, Q) is said to be in the *unary* family; otherwise, it is called *generic*.

- If $p = 2$, let $\lambda \geq 2$, $\sigma \in \{0, \dots, \lambda - 2\}$ and $r, t \in \{1, 3, 5, 7\}$. Then define

$$M = \mathbb{Z}/2^{\lambda-1} \mathbb{Z} \oplus \mathbb{Z}/2^{\lambda-\sigma-1} \mathbb{Z} \quad \text{and} \quad Q(x, y) = \frac{r(x^2 + 2^\sigma t y^2)}{2^\lambda}.$$

When $\sigma = \lambda - 2$, the second factor of M is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and (M, Q) is said to be in the *extremal* family; otherwise, it is called *generic*.

In all cases, the resulting representation is said to be of type R and denoted $R(p, \lambda, \sigma, r, t)$. The additive group M admits a ring structure with multiplication

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - p^\sigma t y_1 y_2, x_1 y_2 + x_2 y_1)$$

and identity element $(1, 0)$. We define a norm $\text{Nm}(x, y) = x^2 + xy + p^\sigma t y^2$ on M .

In this section, we detail generic type R quadratic module. Information on the unary and extremal cases is covered in Section 2.2.4.

Let (M, Q) be a generic type R quadratic modules. Information on (M, Q) can be obtained via `SL2ModuleR` (3.3.1), and subrepresentations of $R(p, \lambda, \sigma, r, t)$ with level p^λ may be constructed via `SL2IrrepR` (3.3.2).

The multiplicative subgroup

$$\mathfrak{A} = \{\varepsilon \in M^\times \mid \text{Nm}(\varepsilon) = 1\}$$

of M^\times acts on M by multiplication and is identified with a subgroup of $\text{Aut}(M, Q)$; see [NW76, Section 2.3 - 2.4]. The relevant information is as follows:

- If p is odd, $\mathfrak{A} = \langle \alpha \rangle \times \langle \beta \rangle$ with order $2p^{\lambda-\sigma}$. In this case, for fixed p, λ, σ , each pair (r, t) gives rise to a distinct quadratic module [Nob76, Satz 4]. The following table covers a complete list of representatives of equivalence classes of such modules.

| p | λ | σ | (r, t) | α | β | \mathfrak{A}_0 |
|----------|-----------|-------------------------|-------------------------|-----------------------------------|---------------|--------------------------|
| 3 | 2 | 1 | $r, t \in \{1, 2\}$ | $ \alpha = 3$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| 3 | ≥ 3 | 1 | $t = 1, r \in \{1, 2\}$ | $ \alpha = 3^{\lambda-\sigma-1}$ | $ \beta = 6$ | $\langle \alpha \rangle$ |
| 3 | ≥ 3 | 1 | $t = 2, r \in \{1, 2\}$ | $ \alpha = 3^{\lambda-\sigma}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| 3 | ≥ 3 | $2, \dots, \lambda - 1$ | $r, t \in \{1, 2\}$ | $ \alpha = 3^{\lambda-\sigma}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| ≥ 5 | ≥ 2 | $1, \dots, \lambda - 1$ | $r, t \in \{1, u\}$ | $ \alpha = p^{\lambda-\sigma}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |

- If $p = 2$, then the generic case occurs when $\lambda \geq 3$ and $\sigma \in \{0, \dots, \lambda - 3\}$. Again, $\mathfrak{A} = \langle \alpha \rangle \times \langle \beta \rangle$; the order is $2^{\lambda-\sigma-k}$ with $k \in \{0, 1, 2\}$ (as specified below). In this case, for fixed p, λ, σ , two pairs (r_1, t_1) and (r_2, t_2) may give rise to equivalent quadratic modules [Nob76, Satz 4]. The following table covers a complete list of representatives of equivalence classes of such modules.

| λ | σ | r | t | $\alpha = (x, y)$ | β | \mathfrak{A}_0 |
|-----------|----------|------------|------------|---|----------------------|-----------------------------|
| 3 | 0 | 1, 3 | 1, 5 | $(1, 0)$ | $(\frac{t-1}{2}, 1)$ | $\langle (-1, 0) \rangle$ |
| 3 | 0 | 1 | 3, 7 | $(1, 0)$ | $(-1, 0)$ | $\langle (-1, 0) \rangle$ |
| 4 | 0 | 1, 3 | 5 | $x = 2, y \equiv 3 \pmod{4}, \alpha = 2^{\lambda-2}$ | $(-1, 0)$ | $\langle -\alpha^2 \rangle$ |
| ≥ 4 | 0 | 1, 3 | 1 | $x \equiv 1 \pmod{4}, y = 4, \alpha = 2^{\lambda-3}$ | $(0, 1)$ | $\langle \alpha \rangle$ |
| ≥ 4 | 0 | 1 | 3, 7 | $x \equiv 1 \pmod{4}, y = 4, \alpha = 2^{\lambda-3}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| ≥ 5 | 0 | 1, 3 | 5 | $x = 2, y \equiv 3 \pmod{4}, \alpha = 2^{\lambda-2}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| ≥ 3 | 1, 2 | 1, 3, 5, 7 | 1, 3, 5, 7 | $x \equiv 1 \pmod{4}, y = 2, \alpha = 2^{\lambda-\sigma-2}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |
| ≥ 3 | ≥ 3 | 1, 3, 5, 7 | 1, 3, 5, 7 | $x \equiv 1 \pmod{4}, y = 1, \alpha = 2^{\lambda-\sigma-1}$ | $(-1, 0)$ | $\langle \alpha \rangle$ |

2.2.4 Type R, unary and extremal cases

This section covers the unary and extremal cases of type R.

First, in the unary family, we have p odd and $\sigma = \lambda$. Then the second factor of M is trivial (and hence t is irrelevant). We then denote $R_{p^\lambda}(r) = R(p, \lambda, \lambda, r, t)$. In this case, we do not decompose $W(M, Q)$ using characters: instead, if $\lambda \leq 2$, then $W(M, Q)$ contains two distinct irreducible subrepresentations of level p^λ , denoted $R_{p^\lambda}(r)_\pm$; otherwise, it contains a single such subrepresentation, denoted $R_{p^\lambda}(r)_1$. The unary family is handled by SL2IrrepRUnary (3.3.3) (which is called by SL2IrrepR (3.3.2) when appropriate).

Second, in the extremal family, we have $p = 2$, $\lambda \geq 2$, and $\sigma = \lambda - 2$. Then the second factor of M is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and collapses in $2M$. Here, $\text{Aut}(M, Q)$ is itself abelian, so we let $\mathfrak{A} = \text{Aut}(M, Q)$. This group has order 1, 2, or 4, with the following structure:

- For $\lambda = 2$ and $t = 1$, $\mathfrak{A} = \langle \tau \rangle$ where $\tau: (x, y) \mapsto (y, x)$, and $\mathfrak{A}_0 = \mathfrak{A} = \langle \tau \rangle$.
- For $\lambda = 2$ and $t = 3$, \mathfrak{A} is trivial; there are no primitive characters.
- For $\lambda = 3$ or 4 , $\mathfrak{A} = \{\pm 1\}$ acting on M by multiplication; there are no primitive characters.
- Finally, for $\lambda \geq 5$, $\mathfrak{A} = \text{Aut}(M, Q) = \langle \alpha \rangle \times \langle -1 \rangle$ with α of order 2, and $\mathfrak{A}_0 = \langle \alpha \rangle$. Note that, for this special case, the usual test for primitivity (described in Section 2.1) fails, as there are no elements of \mathfrak{A} fixing $2M$ pointwise.

The extremal family is handled by SL2ModuleR (3.3.1) and SL2IrrepR (3.3.2), just like the generic case.

Chapter 3

Irreducible representations of prime-power level

Methods for generating individual irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ for a given level p^λ .

In each case (except the unary type R , for which see `SL2IrrepRUnary` (3.3.3)), the underlying module M is of rank 2, so its elements have the form (x, y) and are thus represented by lists $[x, y]$.

Characters of the abelian group $\mathfrak{A} = \langle \alpha \rangle \times \langle \beta \rangle$ have the form $\chi_{i,j}$, given by

$$\chi_{i,j}(\alpha^v \beta^w) \mapsto \mathbf{e}\left(\frac{vi}{|\alpha|}\right) \mathbf{e}\left(\frac{wj}{|\beta|}\right),$$

where i and j are integers. We therefore represent each character by a list $[i, j]$. Note that in some cases α or β is trivial, and the corresponding index i or j is therefore irrelevant.

We write $p=p$, $\text{lambda}=\lambda$, $\text{sigma}=\sigma$, and $\text{chi}=\chi$.

3.1 Representations of type D

See Section 2.2.1.

3.1.1 SL2ModuleD

▷ `SL2ModuleD(p, lambda)` (function)

Returns: a record `rec(Agrp, Bp, Char, IsPrim)` describing (M, Q) .

Constructs information about the underlying quadratic module (M, Q) of type D , for p a prime and $\lambda \geq 1$.

`Agrp` is a list describing the elements of \mathfrak{A} . Each element $a \in \mathfrak{A}$ is represented in `Agrp` by a list $[v, a, a_inv]$, where v is a list defined by $a = \alpha^{v[1]} \beta^{v[2]}$. Note that β is trivial, and hence $v[2]$ is irrelevant, when \mathfrak{A} is cyclic.

`Bp` is a list of representatives for the \mathfrak{A} -orbits on M^\times , which correspond to a basis for the $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ -invariant subspace associated to any primitive character $\chi \in \widehat{\mathfrak{A}}$ with $\chi^2 \neq 1$. For other characters, we must use different bases which are particular to each case.

`Char(i, j)` converts two integers i, j to a function representing the character $\chi_{i,j} \in \widehat{\mathfrak{A}}$.

`IsPrim(chi)` tests whether the output of `Char(i, j)` represents a primitive character.

3.1.2 SL2IrrepD

▷ SL2IrrepD(p , λ , χ) (function)

Returns: a list of lists of the form $[S, T]$.

Constructs the modular data for the irreducible representation(s) of type D with level p^λ , for p a prime and $\lambda \geq 1$, corresponding to the character χ indexed by $\chi_index = [i, j]$ (see the discussion of $\text{Char}(i, j)$ in SL2ModuleD (3.1.1)).

Depending on the parameters, $W(M, Q)$ will contain either 1 or 2 such irreps.

3.2 Representations of type N

See Section 2.2.2.

3.2.1 SL2ModuleN

▷ SL2ModuleN(p , λ) (function)

Returns: a record $\text{rec}(\text{Agrp}, \text{Bp}, \text{Char}, \text{IsPrim}, \text{Nm}, \text{Prod})$ describing (M, Q) .

Constructs information about the underlying quadratic module (M, Q) of type N , for p a prime and $\lambda \geq 1$.

Agrp is a list describing the elements of \mathfrak{A} . Each element $a \in \mathfrak{A}$ is represented in Agrp by a list $[v, a]$, where v is a list defined by $a = \alpha^{v[1]} \beta^{v[2]}$. Note that α is trivial, and hence $v[1]$ is irrelevant, when \mathfrak{A} is cyclic.

Bp is a list of representatives for the \mathfrak{A} -orbits on M^\times , which correspond to a basis for the $\text{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ -invariant subspace associated to any primitive character $\chi \in \widehat{\mathfrak{A}}$ with $\chi^2 \neq 1$. For other characters, we must use different bases which are particular to each case.

$\text{Char}(i, j)$ converts two integers i, j to a function representing the character $\chi_{i,j} \in \widehat{\mathfrak{A}}$.

$\text{IsPrim}(\chi)$ tests whether the output of $\text{Char}(i, j)$ represents a primitive character.

$\text{Nm}(a)$ and $\text{Prod}(a, b)$ are the norm and product functions on M , respectively.

3.2.2 SL2IrrepN

▷ SL2IrrepN(p , λ , χ) (function)

Returns: a list of lists of the form $[S, T]$.

Constructs the modular data for the irreducible representation(s) of type N with level p^λ , for p a prime and $\lambda \geq 1$, corresponding to the character χ indexed by $\chi_index = [i, j]$ (see the discussion of $\text{Char}(i, j)$ in SL2ModuleN (3.2.1)).

Depending on the parameters, $W(M, Q)$ will contain either 1 or 2 such irreps.

3.3 Representations of type R

See Section 2.2.3.

3.3.1 SL2ModuleR

▷ SL2ModuleR(p , λ , σ , r , t) (function)

Returns: a record $\text{rec}(\text{Agrp}, \text{Bp}, \text{Char}, \text{IsPrim}, \text{Nm}, \text{Ord}, \text{Prod}, c, tM)$ describing (M, Q) .

Constructs information about the underlying quadratic module (M, Q) of type R , for p a prime. The additional parameters λ , σ , r , and t should be integers chosen as follows.

If p is an odd prime, let $\lambda \geq 2$, $\sigma \in \{1, \dots, \lambda - 1\}$, and $r, t \in \{1, u\}$ with u a quadratic non-residue mod p . Note that $\sigma = \lambda$ is a valid choice for type R , however, this gives the unary case, and so is not handled by this function, as it is decomposed in a different way; for this case, use `SL2IrrepUnary` (3.3.3) instead.

If $p = 2$, let $\lambda \geq 2$, $\sigma \in \{0, \dots, \lambda - 2\}$ and $r, t \in \{1, 3, 5, 7\}$.

`Agrp` is a list describing the elements of \mathfrak{A} . Each element a of \mathfrak{A} is represented in `Agrp` by a list $[v, a]$, where v is a list defined by $a = \alpha^{v[1]} \beta^{v[2]}$.

`Bp` is a list of representatives for the \mathfrak{A} -orbits on M^\times , which correspond to a basis for the $SL_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ -invariant subspace associated to any primitive character $\chi \in \widehat{\mathfrak{A}}$ with $\chi^2 \neq 1$. For other characters, we must use different bases which are particular to each case.

`Char(i, j)` converts two integers i, j to a function representing the character $\chi_{i,j} \in \widehat{\mathfrak{A}}$.

`IsPrim(chi)` tests whether the output of `Char(i, j)` represents a primitive character.

`Nm(a)`, `Ord(a)`, and `Prod(a, b)` are the norm, order, and product functions on M , respectively.

c is a scalar used in calculating the S -matrix; namely $c = \frac{1}{|M|} \sum_{x \in M} \mathbf{e}(Q(x))$. Note that this is equal to $S_Q(-1)/\sqrt{|M|}$, where $S_Q(-1)$ is the central charge (see Section 2.1.1).

`tM` is a list describing the elements of the group $M - pM$.

3.3.2 SL2IrrepR

▷ `SL2IrrepR(p, lambda, sigma, r, t, chi_index)` (function)

Returns: a list of lists of the form $[S, T]$.

Constructs the modular data for the irreducible representation(s) of type R with parameters p , λ , σ , r , and t , corresponding to the character χ indexed by `chi_index = [i, j]` (see the discussions of σ , r , t , and `Char(i, j)` in `SL2ModuleN` (3.2.1)).

Depending on the parameters, $W(M, Q)$ will contain either 1 or 2 such irreps.

If $\sigma = \lambda$ for $p \neq 2$, then the second factor of M is trivial (and hence t is irrelevant), so this falls through to `SL2IrrepUnary` (3.3.3).

3.3.3 SL2IrrepUnary

▷ `SL2IrrepUnary(p, lambda, r)` (function)

Returns: a list of lists of the form $[S, T]$.

Constructs the modular data for the irreducible representation(s) of unary type R (that is, the special case where $\sigma = \lambda$) with p an odd prime, λ a positive integer, and $r \in \{1, u\}$ with u a quadratic non-residue mod p .

In this case, $W(M, Q)$ always contains exactly 2 such irreps.

Chapter 4

Lists of representations

The *degree* of a representation is also known as the *dimension*. The *level* of the congruent representation determined by the pair (S, T) is equal to the order of T .

We assign to each representation a *name* according to the conventions of [NW76].

4.1 Lists by degree

4.1.1 SL2PrimePowerIrrepsOfDegree

- ▷ `SL2PrimePowerIrrepsOfDegree(degree)` (function)
Returns: a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of all irreps of $SL_2(\mathbb{Z})$ that have the given degree and prime power level.

4.1.2 SL2PrimePowerIrrepsOfDegreeAtMost

- ▷ `SL2PrimePowerIrrepsOfDegreeAtMost(maximum_degree)` (function)
Returns: a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of all irreps of $SL_2(\mathbb{Z})$ that have at most the given maximum degree and prime power level.

4.1.3 SL2IrrepsOfDegree

- ▷ `SL2IrrepsOfDegree(degree)` (function)
Returns: a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of all irreps of $SL_2(\mathbb{Z})$ that have the given degree.

4.1.4 SL2IrrepsOfDegreeAtMost

- ▷ `SL2IrrepsOfDegreeAtMost(maximum_degree)` (function)
Returns: a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of all irreps of $SL_2(\mathbb{Z})$ that have at most the given maximum degree.

4.2 Lists by level

4.2.1 SL2PrimePowerIrrepsOfLevel

- ▷ `SL2PrimePowerIrrepsOfLevel(p , λ)` (function)
- Returns:** a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of all irreps of $SL_2(\mathbb{Z})$ with level exactly p^λ .

4.3 Lists of exceptional representations

4.3.1 SL2ExceptionalIrreps

- ▷ `SL2ExceptionalIrreps(arg)` (function)
- Returns:** a list of records of the form `rec(S, T, degree, level, name)`.
Constructs a list of the 18 exceptional irreps of $SL_2(\mathbb{Z})$.

Chapter 5

Methods for testing

5.1 Testing

5.1.1 SL2WithConjClasses

- ▷ `SL2WithConjClasses(p, lambda)` (function)
Returns: the group $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ with conjugacy classes set to the format we use.

5.1.2 SL2ChiST

- ▷ `SL2ChiST(S, T, p, lambda)` (function)
Returns: a list representing a character of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$.
Converts the modular data (S, T) , which must have level dividing p^λ , into a character of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$, presented in a form matching the conjugacy classes used in `SL2WithConjClasses`.

5.1.3 SL2IrrepPositionTest

- ▷ `SL2IrrepPositionTest(p, lambda)` (function)
Returns: a boolean.
Constructs and tests all irreps of level dividing p^λ by checking their positions in $\mathrm{Irr}(G)$ (see [Section 71.8-2 of the GAP Manual](#)).

References

- [DLN15] Chongying Dong, Xingjun Lin, and Siu-Hung Ng. Congruence property in conformal field theory. *Algebra Number Theory*, 9(9):2121–2166, 2015. [5](#)
- [Nob76] Alexandre Nobs. Die irreduziblen Darstellungen der Gruppen $SL_2(\mathbb{Z}_p)$, insbesondere $SL_2(\mathbb{Z}_2)$. I. *Comment. Math. Helv.*, 51(4):465–489, 1976. [5](#), [8](#), [9](#)
- [NW76] Alexandre Nobs and Jürgen Wolfart. Die irreduziblen Darstellungen der Gruppen $SL_2(\mathbb{Z}_p)$, insbesondere $SL_2(\mathbb{Z}_p)$. II. *Comment. Math. Helv.*, 51(4):491–526, 1976. [5](#), [7](#), [8](#), [13](#)

Index

License, [2](#)

SL2ChiST, [15](#)

SL2ExceptionalIrreps, [14](#)

SL2IrrepD, [11](#)

SL2IrrepN, [11](#)

SL2IrrepPositionTest, [15](#)

SL2IrrepR, [12](#)

SL2IrrepRUnary, [12](#)

SL2IrrepsOfDegree, [13](#)

SL2IrrepsOfDegreeAtMost, [13](#)

SL2ModuleD, [10](#)

SL2ModuleN, [11](#)

SL2ModuleR, [11](#)

SL2PrimePowerIrrepsOfDegree, [13](#)

SL2PrimePowerIrrepsOfDegreeAtMost, [13](#)

SL2PrimePowerIrrepsOfLevel, [14](#)

SL2WithConjClasses, [15](#)