SL2Reps

Constructs representations of SL2(Z).

0.1

24 September 2021

Siu-Hung Ng

Yilong Wang

Samuel Wilson

Siu-Hung Ng
Email: rng@math.lsu.edu

Yilong Wang
Email: wyl@bimsa.cn

Samuel Wilson
Email: swil311@lsu.edu

Contents

1 Introduction **3**
- 1.1 Installation . . . 3
- 1.2 Usage . . . 3

2 Description **4**
- 2.1 Construction . . . 4
- 2.2 Weil representation types . . . 5

3 Lists of representations **8**
- 3.1 Lists by degree . . . 8
- 3.2 Lists by level . . . 8
- 3.3 Lists of exceptional representations . . . 9

4 Methods for testing **10**
- 4.1 Testing . . . 10

5 Irreducible representations of prime-power level **11**
- 5.1 Representations of type D . . . 11
- 5.2 Representations of type N . . . 12
- 5.3 Representations of type R . . . 12

References **14**

Index **15**

Chapter 1

Introduction

This package, SL2Reps, provides methods for constructing and testing matrix presentations of the representations of $\mathrm{SL}_2(\mathbb{Z})$ whose kernels are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

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 TODO, 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 5, while lists of irreducible representations with a given degree or level may be constructed with those in Chapter 3.

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 $\mathfrak{s}$ = `[[0,1],[-1,0]]` and $\mathfrak{t}$ = `[[1,1],[0,1]]` (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 defined by the $n \times n$ matrices $S = \rho(\mathfrak{s})$ and $T = \rho(\mathfrak{t})$.

This package constructs representations 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 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. $\mathfrak{s}$ = `[[0,-1],[1,0]]` (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 $\mathbf{e}$ 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 $\mathbb{C}$).

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 representations of $\mathrm{SL}_2(\mathbb{Z})$, it suffices to consider irreps of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ for primes p and positive integers λ.

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 $Q : M \to \mathbb{Q}/\mathbb{Z}$ 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 $M \times M \to \mathbb{Q}/\mathbb{Z}$.

Now let p be a prime number and $\lambda \in \mathbb{Z}^+$. Choose a $\mathbb{Z}/p^\lambda\mathbb{Z}$-module M of rank 1 or 2 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. Then the *quadratic module* (M,Q) gives rise to a representation of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ on the vector space $V = \mathbb{C}^M$ of complex-valued functions on M. This representation is denoted $W(M,Q)$.

With a finite number of exceptions, every representation of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ may be found as a subrepresentation of $W(M,Q)$ for an appropriate choice of (M,Q) [NW76, Hauptsatz 2] (the 18 *exceptional* *representations* can be constructed as the tensor product of two such subrepresentations; these can be generated with `SL2ExceptionalIrreps` (3.3.1)).

The subrepresentations in question are often of the form $W(M,Q,\chi)$, defined as follows. Let $\mathfrak{A}$ be an abelian subgroup of

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

and let $\chi \in \widehat{\mathfrak{A}}$ be a 1-dimensional character of $\mathfrak{A}$. 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.

In this context, we will frequently refer to a character χ as being *primitive*, which means, roughly speaking, that χ does not factor through a quadratic module of lower level. With the exception of a single family of modules of type R (the *extremal* case, for which see Section 2.2.3) primitivity amounts to the following: there exists some $\varepsilon \in \mathfrak{A}$ such that $\chi(\varepsilon) \neq 1$ and ε fixes the submodule pM pointwise. Explicit descriptions of the primitive characters are given in Section 2.2.

The prime-power irreps then fall into three cases. The overwhelming majority are of the form $W(M,Q,\chi)$ for χ primitive. A finite number, and a single infinite family arising from the extremal case (Section 2.2.3), are instead constructed by using non-primitive characters. Finally, the 18 exceptional irreps are constructed as tensor products of two irreps from the other two cases.

All the irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ of finite level can now be constructed by taking tensor products of these prime-power irreps. Note that, if two representations are defined by pairs `[S1,T1]` and `[S2,T2]`, then 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 and $\lambda \geq 1$. Then the Weil representation arising from the quadratic module with $M = \mathbb{Z}/p^\lambda\mathbb{Z} \oplus \mathbb{Z}/p^\lambda\mathbb{Z}$ and $Q(x,y) = \frac{xy}{p^\lambda}$ is said to be of type D and denoted $D(p,\lambda)$. Information on (M,Q) may be obtained via `SL2ModuleD` (5.1.1), and subrepresentations of $D(p,\lambda)$ with level p^λ may be constructed via `SL2IrrepD` (5.1.2).

Here we define

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

acting on M by multiplication; see [NW76, Section 2.1]. This group has the following structure. When $p = 2$ and $\lambda \geq 3$, it is generated by $\alpha = -1$ and $\zeta = 5$. Otherwise, it is cyclic; in this case, we choose a generator α and (for simplicity) say $\zeta = 1$.

A character of $\mathfrak{A}$ is primitive if and only if it is injective on the subgroup $\langle \mathrm{o} \rangle \leq \mathfrak{A}$, where o is chosen as follows. If $p = 2$ and $\lambda \geq 3$, $\mathrm{o} = 5$. If $\lambda = 1$, $\mathrm{o} = \alpha$. In all other cases, $\mathrm{o} = 1 + p$.

2.2.2 Type N

Let p be prime and $\lambda \geq 1$. Then the Weil representation arising from the quadratic module with $M = \mathbb{Z}/p^\lambda\mathbb{Z} \oplus \mathbb{Z}/p^\lambda\mathbb{Z}$ and $Q(x,y) = \frac{x^2+xy+\frac{1+u}{4}y^2}{p^\lambda}$ (where, for $p \neq 2$, u is chosen so that $u \equiv 3 \bmod 4$

with $\left(\frac{-u}{p}\right) = -1$, and for $p = 2$, $u = 3$) is said to be of type N and denoted $N(p,\lambda)$. Information on (M,Q) may be obtained via `SL2ModuleN` (5.2.1), and subrepresentations of $D(p,\lambda)$ with level p^λ may be constructed via `SL2IrrepN` (5.2.2).

Here we define

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

acting on M by multiplication; see [NW76, Section 2.2]. This group has the following structure. When $\lambda \geq 2$, it is generated by α and ζ: for $p = 2$, $|\alpha| = 2^{\lambda-2}$ and $|\zeta| = 6$, while for $p \neq 2$, $|\alpha| = p^{\lambda-1}$ and $|\zeta| = p+1$. On the other hand, when $\lambda = 1$, $\mathfrak{A}$ is cyclic; in this case, we choose a generator ζ with $|\zeta| = p+1$ and (for simplicity) say $\alpha = 1$.

For $p = 2$, $\lambda = 2$, a character of $\mathfrak{A}$ is primitive if and only if $\chi(-1) = -1$. For all other cases, a character of $\mathfrak{A}$ is primitive if and only if it is injective on the subgroup $\langle \mathrm{o} \rangle \leq \mathfrak{A}$, where o is chosen as follows. If $\lambda = 1$, $\mathrm{o} = \zeta$; otherwise $\mathrm{o} = \alpha$.

2.2.3 Type R

The structure of (M,Q) of type R depends upon three additional parameters: σ, r, and t. The relevant values thereof depend on whether $p = 2$, as follows.

First, if p is an odd prime, let $\lambda \geq 2$, $\sigma \in \{1,\ldots,\lambda\}$, and $r,t \in \{1,u\}$ with u a quadratic non-residue mod p. Then define $M = \mathbb{Z}/p^\lambda\mathbb{Z} \oplus \mathbb{Z}/p^{\lambda-\sigma}\mathbb{Z}$ and $Q(x,y) = \frac{r(x^2+p^\sigma ty^2)}{p^\lambda}$.

On the other hand, if $p = 2$, let $\lambda \geq 2$, $\sigma \in \{0,\ldots,\lambda-2\}$ and $r,t \in \{1,3,5,7\}$. Then define $M = \mathbb{Z}/2^{\lambda-1}\mathbb{Z} \oplus \mathbb{Z}/2^{\lambda-\sigma-1}\mathbb{Z}$ and $Q(x,y) = \frac{r(x^2+2^\sigma ty^2)}{2^\lambda}$.

In either case, the resulting representation is said to be of type R and denoted $R(p,\lambda,\sigma,r,t)$. Information on (M,Q) may be obtained via `SL2ModuleR` (5.3.1), and subrepresentations of $R(p,\lambda,\sigma,r,t)$ with level p^λ may be constructed via `SL2IrrepR` (5.3.2).

There are two special cases to consider. First, if $\sigma = \lambda$ for $p \neq 2$, then the second factor of M is trivial (and hence t is irrelevant); this special case is handled by `SL2IrrepRUnary` (5.3.3) (which is called by `SL2IrrepR` (5.3.2) when appropriate).

Second, if $\sigma = \lambda - 2$ for $p = 2$, $\lambda \geq 2$, then the second factor of M is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and collapses in $2M$; we call this case the *extremal* family. Here, $\mathrm{Aut}(M,Q)$ is itself abelian, so we let $\mathfrak{A} = \mathrm{Aut}(M,Q)$. This group has the following structure:

- For $\lambda = 2$, $t = 1$, $\mathfrak{A} = \langle \tau \rangle$ where $\tau : (x,y) \mapsto (y,x)$; a character χ is primitive if $\chi(\tau) = -1$.
- For $\lambda = 2$, $t = 3$, $\mathfrak{A}$ is trivial; there are no primitive characters.
- For $\lambda = 3$ or 4, $\mathfrak{A} = \{\pm 1\}$; there are no primitive characters.
- Finally, for $\lambda \geq 5$, $\mathfrak{A} = \langle -1 \rangle \times \langle \alpha \rangle$ with $\alpha \neq -1$ of order 2, and a character $\chi \in \widehat{\mathfrak{A}}$ is primitive if $\chi(\alpha) = -1$. Note that the reason for this special case is that the usual test for primitivity (described in Section 2.1) fails here, as there are no elements of $\mathfrak{A}$ fixing $2M$ pointwise.

Outside of these special cases, we define

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

acting on M by multiplication; see [NW76, Section 2.3 - 2.4]. The structure of $\mathfrak{A}$ is as follows, and a character is primitive if it is injective on $\langle \mathrm{o} \rangle \leq \mathfrak{A}$, with $\mathrm{o} = \alpha$ except when specified:

- Suppose $p \neq 2$, $\lambda \geq 2$, $\sigma \in \{1, \ldots, \lambda - 1\}$. If $\lambda \geq 3$ and $\sigma = t = 1$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle \zeta \rangle$ with α of order $3^{\lambda-2}$ and ζ of order 6. Otherwise, $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with α of order $p^{\lambda-\sigma}$.

- Suppose $p = 2$, $\lambda \geq 3$, $\sigma \in \{0, \ldots, \lambda - 3\}$. Then the structure of $(M, Q))$ depends on r, t, but only up to an equivalence class described in [Nob76, Satz 4]; we assume without loss of generality that r, t are minimal positive representatives thereunder. Then:

  - If $\sigma = 0$, $r \in \{1, 3\}$, $t = 1$, and $\lambda = 3$, then $\mathfrak{A} = \langle \zeta \rangle$ with $\zeta = (0, 1)$ of order 4. Here $\mathrm{o} = -1 = \zeta^2$.
  - If $\sigma = 0$, $r \in \{1, 3\}$, $t = 1$, and $\lambda \geq 4$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle \zeta \rangle$ with $\alpha = (1 \mod 4, 4)$ of order $2^{\lambda-3}$ and $\zeta = (0, 1)$ of order 4.
  - If $\sigma = 0$, $r \in \{1, 3\}$, $t = 5$, and $\lambda = 3$, then $\mathfrak{A} = \langle \zeta \rangle$ with $\zeta = (2, 1)$ of order 4. Here $\mathrm{o} = -1$.
  - If $\sigma = 0$, $r \in \{1, 3\}$, $t = 5$, and $\lambda \geq 4$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with $\alpha = (2, 3 \mod 4)$ of order $2^{\lambda-2}$. Here $\mathrm{o} = -\alpha^2$ when $\lambda = 4$ and $\mathrm{o} = \alpha$ otherwise.
  - If $\sigma = 0$, $r = 1$, $t \in \{3, 7\}$, and $\lambda = 3$, then $\mathfrak{A} = \langle -1 \rangle$. Here $\mathrm{o} = -1$.
  - If $\sigma = 0$, $r = 1$, $t \in \{3, 7\}$, and $\lambda \geq 4$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with $\alpha = (1 \mod 4, 4)$ of order $2^{\lambda-3}$.
  - If $\sigma = 1$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with $\alpha = (1 \mod 4, 2)$ of order $2^{\lambda-3}$.
  - If $\sigma = 2$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with $\alpha = (1 \mod 4, 2)$ of order $2^{\lambda-4}$.
  - If $\sigma \geq 3$, then $\mathfrak{A} = \langle \alpha \rangle \times \langle -1 \rangle$ with $\alpha = (1 \mod 4, 1)$ of order $2^{\lambda-\sigma-1}$.

Chapter 3

Lists of representations

3.1 Lists by degree

3.1.1 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 $\mathrm{SL}_2(\mathbb{Z})$ that are exactly the given degree and have prime power level.

3.1.2 SL2PrimePowerIrrepsOfDegreeAtMost

▷ `SL2PrimePowerIrrepsOfDegreeAtMost(max_degree)` (function)

Returns: a list of records of the form `rec(S, T, degree, level, name)`

Constructs a list of all irreps of $\mathrm{SL}_2(\mathbb{Z})$ that are at most the given degree and have prime power level.

3.1.3 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 $\mathrm{SL}_2(\mathbb{Z})$ that are exactly the given degree.

3.1.4 SL2IrrepsOfDegreeAtMost

▷ `SL2IrrepsOfDegreeAtMost(degree)` (function)

Returns: a list of records of the form `rec(S, T, degree, level, name)`

Constructs a list of all irreps of $\mathrm{SL}_2(\mathbb{Z})$ that are at most the given degree.

3.2 Lists by level

3.2.1 SL2PrimePowerIrrepsOfLevel

▷ `SL2PrimePowerIrrepsOfLevel(p, lambda)` (function)

Returns: a list of records of the form `rec(S, T, degree, level, name)`

Constructs a list of all irreps of $\mathrm{SL}_2(\mathbb{Z})$ with level exactly p^λ.

3.3 Lists of exceptional representations

3.3.1 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 $\mathrm{SL}_2(\mathbb{Z})$.

Chapter 4

Methods for testing

4.1 Testing

4.1.1 SL2WithConjClasses

▷ `SL2WithConjClasses(p, ld)` (function)

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

4.1.2 SL2ChiST

▷ `SL2ChiST(S, T, p, ld)` (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`.

4.1.3 SL2IrrepPositionTest

▷ `SL2IrrepPositionTest(p, lambda)` (function)

Returns: a boolean

Constructs and tests all irreps of level dividing p^λ by checking their positions in `Irr(G)`.

Chapter 5

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` (5.3.3)), the underlying module M is of rank 2, so its elements have the form (x,y) and are thus represented by lists $[x,y]$.

5.1 Representations of type D

See Section 2.2.1.

5.1.1 SL2ModuleD

▷ `SL2ModuleD(p, ld)` (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 $a = \alpha^{\mathrm{v}[1]}\zeta^{\mathrm{v}[2]}$. Note that ζ 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 $\chi^2 \not\equiv 1$. 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 a character of $\mathfrak{A}$. Each character in $\hat{\mathfrak{A}}$ is of the form $\chi_{i,j}$, given by \[\chi_{i,j}(\alpha^{v}\zeta^{w}) \mapsto \mathbf{e}\left(\frac{vi}{|\alpha|}\right) \mathbf{e}\left(\frac{wj}{|\zeta|}\right)~.\] Note that j is irrelevant when $\mathfrak{A}$ is cyclic.

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

5.1.2 SL2IrrepD

▷ `SL2IrrepD(p, ld, chi_index)` (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 `Char(i,j)` in `SL2ModuleD` (5.1.1)).

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

5.2 Representations of type N

See Section 2.2.2.

5.2.1 SL2ModuleN

▷ `SL2ModuleN(p, ld)` (function)

Returns: a record `rec(Agrp, Bp, Char, IsPrim, Nm, 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 $a = \alpha^{\mathrm{v}[1]}\zeta^{\mathrm{v}[2]}$. 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 $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$-invariant subspace associated to any primitive character $\chi \in \widehat{\mathfrak{A}}$ with $\chi^2 \not\equiv 1$. 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 a character of $\mathfrak{A}$. Each character in $\hat{\mathfrak{A}}$ is of the form $\chi_{i,j}$, given by \[\chi_{i,j}(\alpha^{v}\zeta^{w}) \mapsto \mathbf{e}\left(\frac{vi}{|\alpha|}\right) \mathbf{e}\left(\frac{wj}{|\zeta|}\right)~.\] Note that i is irrelevant in the cases where $\mathfrak{A}$ is cyclic.

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

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

5.2.2 SL2IrrepN

▷ `SL2IrrepN(p, ld, chi_index)` (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 `Char(i,j)` in `SL2ModuleN` (5.2.1)).

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

5.3 Representations of type R

See Section 2.2.3.

5.3.1 SL2ModuleR

▷ `SL2ModuleR(p, ld, sigma, r, t)` (function)

Returns: a record `rec(Agrp, Bp, Char, IsPrim, Nm, Ord, 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 `SL2IrrepRUnary` (5.3.3) 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 $a = \alpha^{\mathtt{v}[1]}\zeta^{\mathtt{v}[2]}$.

`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 $\chi^2 \not\equiv 1$. 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 a character of $\mathfrak{A}$. Each character in $\hat{\mathfrak{A}}$ is of the form $\chi_{i,j}$, given by \[\chi_{i,j}(\alpha^{v}\zeta^{w}) \mapsto \mathbf{e}\left(\frac{vi}{|\alpha|}\right) \mathbf{e}\left(\frac{wj}{|\zeta|}\right)~.\]

`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 $S_Q(-1) = \frac{1}{\sqrt{|M|}}\sum_{x\in M}\mathbf{e}(Q(x))$ is also known as the central charge.

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

5.3.2 SL2IrrepR

▷ `SL2IrrepR(p, ld, 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` (5.2.1)).

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 `SL2IrrepRUnary` (5.3.3).

5.3.3 SL2IrrepRUnary

▷ `SL2IrrepRUnary(p, ld, 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.

References

[DLN15] Chongying Dong, Xingjun Lin, and Siu-Hung Ng. Congruence property in conformal field theory. *Algebra Number Theory*, 9(9):2121–2166, 2015. 4

[Nob76] Alexandre Nobs. Die irreduziblen Darstellungen der Gruppen $SL_2(Z_p)$, insbesondere $SL_2(Z_2)$. I. *Comment. Math. Helv.*, 51(4):465–489, 1976. 4, 7

[NW76] Alexandre Nobs and Jürgen Wolfart. Die irreduziblen Darstellungen der Gruppen $SL_2(Z_p)$, insbesondere $SL_2(Z_p)$. II. *Comment. Math. Helv.*, 51(4):491–526, 1976. 4, 5, 6

Index

SL2ChiST, 10
SL2ExceptionalIrreps, 9
SL2IrrepD, 11
SL2IrrepN, 12
SL2IrrepPositionTest, 10
SL2IrrepR, 13
SL2IrrepRUnary, 13
SL2IrrepsOfDegree, 8
SL2IrrepsOfDegreeAtMost, 8
SL2ModuleD, 11
SL2ModuleN, 12
SL2ModuleR, 12
SL2PrimePowerIrrepsOfDegree, 8
SL2PrimePowerIrrepsOfDegreeAtMost, 8
SL2PrimePowerIrrepsOfLevel, 8
SL2WithConjClasses, 10