Contents

Chapter 1

Classes

1.1 lattice – Lattice

- **Classes**
  - **Lattice**
  - **LatticeElement**
- **Functions**
  - **LLL**

1.1.1 Lattice – lattice

Initialize (Constructor)

Lattice(`basis`: Matrix, `quadraticForm`: Matrix)
→ ***Lattice***

Create Lattice object.

Attribute

basis : The basis of `self` lattice.

quadraticForm : The quadratic form of

Methods

1.1.1.1 createElement – create element

createElement(`self`, `compo`: *list*) → **LatticeElement**

Create the element which has coefficients with given `compo`.

1.1.1.2 bilinearForm – bilinear form

bilinearForm(`self`, `v_1`, `v_2`) → *integer*

Return the (polynomial) discriminant of the `self`.**polynomial**.

†The output is not discriminant of the number field itself.

1.1.1.3 isCyclic – Check whether cyclic lattice or not

isCyclic(`self`) → *bool*

Check whether `self` lattice is a cyclic lattice or not.

1.1.1.4 isIdeal – Check whether ideal lattice or not

signature(`self`) → *bool*

Check whether `self` lattice is a ideal lattice or not.

1.1.2 LatticeElement – Lattice Element

Initialize (Constructor)

Lattice(`lattice`: *list*, `compo`: *list*,) → ***LatticeElement***

Attribute

lattice :

row :

column :

compo :

Methods

1.1.2.1 getLattice – FInd lattice belongs to

getLattice(`self`) → Lattice

1.1.3 LLL(function) – LLL reduction

LLL(M: Matrix) → *Matrix*, *Matrix*

Return

Examples

```
>>> M=mat.Matrix(3,3,[1,0,12,0,1,26,0,0,13]);
>>> lat.LLL(M);
([1, 0, 0]+[0, 1, 0]+[0, 0, 13], [1L, 0L, -12L]+[0L, 1L, -26L]+[0L, 0L, 1L])
>>>
```