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

Operations

operator	explanation

Examples

```
\end{ex}%Don't indent!
\C
  \method
  \subsubsection{createElement -- create element}\linkedtwo{lattice}{Lattice}{create
  \func{createElement}{\param{self}, \ \hiki{compo}{list}}{\out{\linkingone{lattice}
  \spacing
  % document of basic document
  \quad Create the element which has coefficients with given \param{compo}. \\
  \spacing
  % add document
  %\spacing
  % input, output document
%
  \subsubsection{bilinearForm -- bilinear form}\linkedtwo{lattice}{Lattice}{bilinear
  \func{bilinearForm}{\param{self}, \ \param{v_1}{}, \, \param{v_2} }{\out{integer}}
  \spacing
  % document of basic document
  \quad Return the (polynomial) discriminant of the \param{self}.\linkingtwo{lattice
  \spacing
  % add document
  \quad \negok The output is not discriminant of the number field itself. \\
  %\spacing
  % input, output document
%
  \subsubsection{isCyclic -- Check whether cyclic lattice or not}\linkedtwo{lattice}
  \func{isCyclic}{\param{self}}{\out{bool}}}\\
  \spacing
  % document of basic document
  \quad Check whether \param{self} lattice is a cyclic lattice or not.
  \spacing
  % add document
  \quad
  %\spacing
  % input, output document
%
  \subsubsection{isIdeal -- Check whether ideal lattice or not}\linkedtwo{lattice}{I
  \func{signature}{\param{self}}{\out{bool}}\\
  \spacing
  % document of basic document
  \quad Check whether \param{self} lattice is a ideal lattice or not.
```

```
  \spacing
  % add document
  %\spacing
  % input, output document
%
\begin{ex}
```

1.1.2 LatticeElement – Lattice Element

Initialize (Constructor)

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

Attribute

lattice :

row :

column :

compo :

Operations

operator	explanation

Examples

```
\end{ex}%Don't indent!
\C
  \method
  \subsubsection{getLattice -- FInd lattice belongs to}\linkedtwo{lattice}{LatticeEl
  \func{getLattice}{\param{self}}{\out{\linkingone{lattice}{Lattice}}}\\
  \spacing
  % document of basic document
  \spacing
  % add document
  %\spacing
  % input, output document
%
\begin{ex}
```

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])
>>>
```