Make me a Module

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

October, 2025

$\boxed{IX}$

1 Introduction

Till now we have seen lattices as some periodic arrangements of vectors in a vector spaces. We are only allowed to add vectors but scaling is restricted to integers only. The same kind of structure is module which generalizes the idea of vector spaces. We will look at this algebraic structure in this article and also try to connect it with lattices.

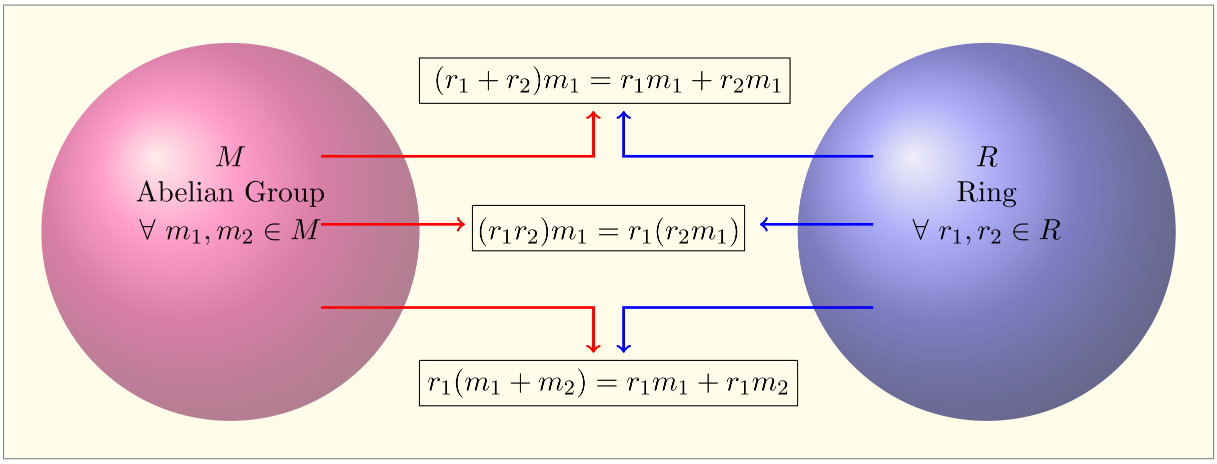
2 Modules

As a start we can think of a vector space V as a nonempty set over a field F. To generalize this we would replace V by an abelian group M and F by a Ring with unity R.
Note: we will purposefully use $v \in M$ instead of $\mathbf{v} \in M$ for elements in a module, because we are not treating them as vector in this article.

Definition 2.1. **(Module)** *Let $(R, \oplus, *)$ be a ring, a left R module is a set M with opeations defined as addition $+ : M \times M \to M$ and scalar multiplication $\circ : R \times M \to M$ such that*

- $(M, +)$ *is an abelian group*
  - ✓ $(x + y) + z = x + (y + z)$
  - ✓ $x + y = y + x$
  - ✓ $x + 0 = 0 + x$
  - ✓ $x + (-x) = (-x) + x = 0$
- *Scalar multiplication is distributive*
  - ✓ $(r_1 \oplus r_2) \circ m = r_1 \circ m + r_2 \circ m$
  - ✓ $r \circ (m_1 + m_2) = r \circ m_2 + r \circ m_2$
- *Scalar multiplication is an action on M*
  - ✓ $1 \circ x = x$
  - ✓ $(r_1 * r_2) \circ m = r_1 \circ (r_2 \circ m)$

We will not specify the operation as $*, \circ, \oplus, +$ as it would be visible what is being done by looking at elements, to distinguish addition.


$(r_1+r_2)m_1 = r_1m_1 + r_2m_1$
M
Abelian Group
$\forall\ m_1, m_2 \in M$
$(r_1r_2)m_1 = r_1(r_2m_1)$
R
Ring
$\forall\ r_1, r_2 \in R$
$r_1(m_1+m_2) = r_1m_1 + r_1m_2$

Definition 2.2. **(Module)** *For a commutative ring R an $R-$module M is an abelian group on which R acts by additive maps along with the group structure of R when these maps are added and composed. define a map $R \times M \to M$ denoted by $(r, m) \mapsto rm$ such that*

- $1m_1 = m_1$ *for all* $m_1 \in M$
- $r_1(m_1+m_2) = r_1m_1 + r_1m_2$ *for all* $r_1 \in R$ *and* $m_1, m_2 \in M$
- $(r_1+r_2)m_1 = r_1m_1 + r_2m_1$ *and* $(r_1r_2)m_1 = r_1(r_2m)$ *for all* $r_1, r_2 \in R$ *and* $m \in M$

Example 2.3. ($\mathbb{Z}-$*module*) *$R = \mathbb{Z}$ and $(M, +)$ is an abelian group, with* $r \cdot m = \underbrace{m + m + \cdots + m}_{r-times}$

$$\begin{aligned} r \cdot (m_1+m_2) &= \underbrace{(m_1+m_2) + (m_1+m_2) + \cdots + (m_1+m_2)}_{r-times} \\ &= \underbrace{m_1 + m_1 + \cdots + m_1}_{r-times} + \underbrace{m_2 + m_2 + \cdots + m_2}_{r-times} \\ &= r \cdot m_1 + r \cdot m_2 \end{aligned}$$

✓ $r \cdot (m_1+m_2) = r \cdot m_1 + r \cdot m_2$

$$\begin{aligned} (r_1+r_2) \cdot m &= \underbrace{m + m \cdots + m}_{(r_1+r_2)-times} \\ &= \underbrace{m + m + \cdots + m}_{r_1-times} + \underbrace{m + m + \cdots + m}_{r_2-times} \\ &= r_1 \cdot m + r_2 \cdot m \end{aligned}$$

✓ $(r_1+r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

$$\begin{aligned} (r_1r_2) \cdot m &= \underbrace{m + m \cdots + m}_{r_1r_2-times} \\ &= \underbrace{\underbrace{m + m + \cdots + m}_{r_2-times} + \underbrace{m + m + \cdots + m}_{r_2-times} + \cdots + \underbrace{m + m + \cdots + m}_{r_2-times}}_{r_1-times} \\ &= \underbrace{r_2m + r_2m + \cdots + r_2m}_{r_1-times} \\ &= r_1 \cdot (r_2m) \end{aligned}$$

✓ $(r_1 r_2) \cdot m = r_1 \cdot (r_2 m)$

Example 2.4. *$M = R$ and scalar multiplication is same as the ring multiplication*

✓ $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
✓ $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
✓ $(r_1 r_2) \cdot m = r_1 \cdot (r_2 m)$

Example 2.5. *R be a ring and M, N be modules, consider $M \times N$ with scalar multiplication $R \times (M \times N) \to M \times N$ as $(r, (m, n)) \mapsto (rm, rn)$*

$$\begin{aligned} r \cdot ((m_1, n_1) + (m_2, n_2)) &= r \cdot (m_1 + m_2, n_1 + n_2) \\ &= (r(m_1 + m_2), r(n_1 + n_2)) \\ &= (r \cdot m_1 + r \cdot m_2, r \cdot n_1 + r \cdot n_2) \\ &= (r \cdot m_1, r \cdot n_1) + (r \cdot m_2, r \cdot n_2) \\ &= r \cdot (m_1, n_1) + r \cdot (m_2, n_2) \end{aligned}$$

✓ $r \cdot ((m_1, n_1) + (m_2, n_2)) = r \cdot (m_1, n_1) + r \cdot (m_2, n_2)$

$$\begin{aligned} (r_1 + r_2) \cdot (m, n) &= ((r_1 + r_2) \cdot m, (r_1 + r_2) \cdot n) \\ &= ((r_1 \cdot m + r_2 \cdot m), (r_1 \cdot n + r_2 \cdot n)) \\ &= r_1 \cdot (m, n) + r_2 \cdot (m, n) \end{aligned}$$

✓ $(r_1 + r_2) \cdot (m, n) = r_1 \cdot (m, n) + r_2 \cdot (m, n)$

$$\begin{aligned} (r_1 r_2) \cdot (m, n) &= ((r_1 r_2) \cdot m, (r_1 r_2) \cdot n) \\ &= (r_1 \cdot (r_2 m), r_1 \cdot (r_2 n)) \\ &= r_1 \cdot (r_2 m, r_2 n) \\ &= r_1 \cdot (r_2 (m, n)) \end{aligned}$$

✓ $(r_1 r_2) \cdot (m, n) = r_1 \cdot (r_2 (m, n))$

Example 2.6. *R be a ring and define $M = R^n = \underbrace{R \times R \times \cdots \times R}_{n-times}$ with scalar multiplication $R \times R^n \to R^n$ as $(r, (m_1, m_2, \cdots, m_n)) \mapsto (rm_1, rm_2, \cdots, rm_n)$ is again a module.*

3 Sum of Modules

Definition 3.1. **(Submodule)**
Let M be a module then $N \neq \phi$ is a submodules of M iff

(i) N is an additive subgroup i.e $\forall\ n_1, n_2 \in N$ we have $n_1 - n_2 \in N$

(ii) N is closed under scalar multiplication i.e $\forall\ n \in N, r \in R$ we have $r \cdot n \in N$

Definition 3.2. **(Sum Of Submodules)**
Let M be a module and P, Q be submodules of M, then the sum of submodules P, Q is defined as

$$P + Q = \{p + q | p \in P, q \in Q\}$$

It is the smallest submodule of M containig P and Q.

3.1 Direct Sum

Definition 3.3. **(Direct Sum)**
Let M and N be R modules, consider $P = M \times N$ which is again an R module.
M and N can again be seen as subsets of P as

$$M = \{(m, 0)|m \in M\} \subseteq P$$

$$N = \{(0, n)|n \in N\} \subseteq P$$

Now consider the sum of M and N in P which is called the direct sum

$$M \oplus N = \{(m, 0) + (0, n)|m \in M, n \in N\} = \{(m, n)|m \in M, n \in N\}$$

- *$P = M + N$ with $M \cup N = (0)$*
- *Every element of P can be written uniquely as a sum of elements in M and N.*

4 Free Modules

Definition 4.1. **(Span)**
Let M be a R module and $X \subseteq M$ be a subset, then the submodule generated/spanned by X is defined as the smallest submodule of M contiaining X.
or,
It is the intersection of all the submodules of M that contains X.

Example 4.2. *The submodule generated by empty set ϕ is (0).*

Example 4.3. *The submodule generated by X is $N = \{ax|a \in R\}$.*

Definition 4.4. **(Finitely Generated Module)** *A module M is finitely generated if there exist a finite subset $X = \{x_1, x_2, \cdots, x_n\}$ of M which generates M*

$$M = \left\{ \sum_i a_i x_i | a_i \in R \right\}$$

Definition 4.5. **(Linear Independence)** *For a module M, a finite subset B is said to be linearly independent over R if for any finite subset $\{b_1, b_2, \cdots, b_k\} \subseteq B$*

$$r_1 b_1 + r_2 b_2 + \cdots r_k b_k = 0 \qquad \textit{with } r_i \in R$$

then $r_i = 0 \ \forall \ i$

Definition 4.6. **(Free Modules)**
R module M is called a free module if it has a basis B i.e a linearly independent subset B of M such that M is spanned by B over R.

Example 4.7.

(i) *$\mathbb{R}^n$ as $\mathbb{R}$ module. $B = \{(1, 0, \cdots, 0), (0, 1, \cdots, 0), \cdots, (0, 0, \cdots, 1)\}$ is called the standard basis.*

(ii) *$\mathbb{R}^n$ as $\mathbb{Z}$ module doesnot have a finite basis set, however we have a generating set $X = \{(x, 0, \cdots, 0)|x \in (0, 1]\} \cup \{(0, x, \cdots, 0)|x \in (0, 1]\} \cup \cdots \cup \{(0, 0, \cdots, x)|x \in (0, 1]\}$. First we see this as an infinite set, and secondly it is linearly dependent, so it is not a basis.*

(iii) $B = \{(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,0,\cdots,1)\}$ *called the standard basis when generated over $\mathbb{Z}$ gives $\mathbb{Z}^n$*

(iv) *Now if we consider any other basis $B = \{(\sqrt{2},0,0),(0,1.57,0),(0,0,\pi)\}$ and we would generate a $\mathbb{Z}$ module which is nothing but a module*

$$M = \{x = a(\sqrt{2},0,0) + b(0,1.57,0) + c(0,0,\pi) | a,b,c \in \mathbb{Z}\}$$

$$M = \left\{ \begin{bmatrix} \sqrt{2} & 0 & 0 \\ 0 & 1.57 & 0 \\ 0 & 0 & \pi \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \middle| a,b,c \in \mathbb{Z} \right\} = \mathcal{L}(B)$$

The elements of this module are the elements of the lattice generated by B

Result 4.8. *Direct sum of free modules is a free module.*

Result 4.9. *Any finite abelian group is not free as a module over $\mathbb{Z}$.*

5 Linear Maps

Definition 5.1. *An $R-$linear map between two $R-$modules M and N is a map $f : M \to N$ such that*

$$(i) \quad f(m_1 + m_2) = f(m_1) + f(m_2) \quad \forall\ m_1, m_2 \in M$$
$$(ii) \quad f(r \cdot m) = r \cdot f(m) \quad \forall\ m \in M,\ r \in R$$

Definition 5.2. **(Isomorphism)** *Let M and N be two $R-$modules then an isomorphism is a $R-$linear map between the two $R-$modules M and N, $f : M \to N$ such that f^{-1} exists and is also $R-$linear. Equivalently it is a bijective $R-$linear map.*

6 Lattice as $\mathbb{Z}$ Modules

Now we will shift the idea of Modules to its specific case where we will use the ideas from modules to define lattices instead of looking it as a subset of some vector space.

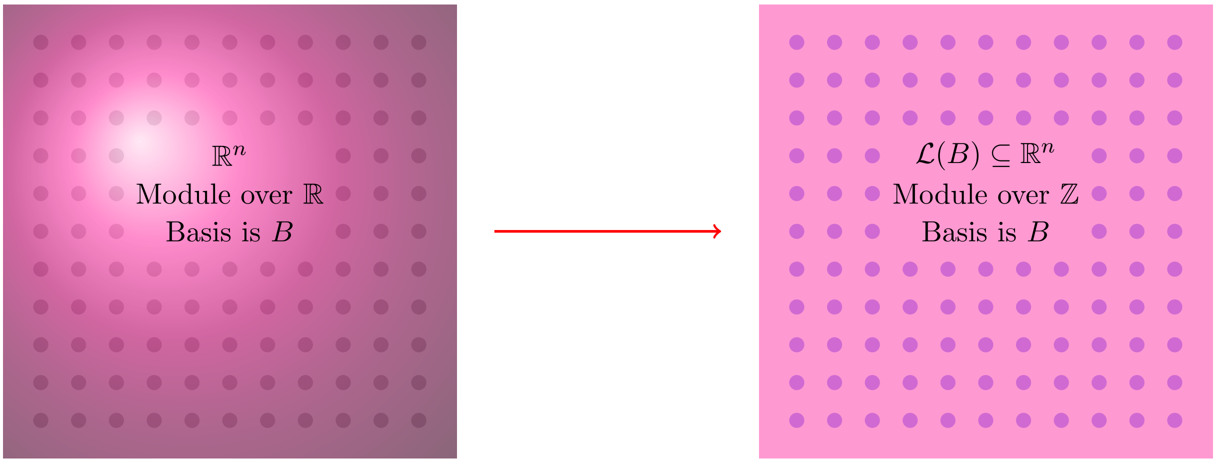
Consider a specific case of module where $M \subseteq \mathbb{R}^n$ is a subgroup of $(\mathbb{R}^n, +)$ and $R = \mathbb{Z}$, which is the ring of integers with usual addition and multiplication. when a multiplication with an integer and an element of M is done it is the component wise multiplication. It is easy to show that M is a $\mathbb{Z}$ Module.

Now consider a basis $B = \{b_1, b_2, \cdots, b_n\}$ of $\mathbb{R}^n$ for the $\mathbb{R}$ module and we will try to generate a $\mathbb{Z}$ module with that basis B,

$$M = \left\{ \begin{bmatrix} | & | & | \\ b_1 & b_2 & b_3 \\ | & | & | \end{bmatrix} \begin{bmatrix} | \\ z \\ | \end{bmatrix} \middle| z \in \mathbb{Z}^n \right\} = \{Bz | z \in \mathbb{Z}\}$$

This would form a discrete set in $\mathbb{R}^n$. This is what we would call a lattice, a discrete subgroup of $\mathbb{R}^n$.
It is now clear that

$$\mathcal{L}(B) = \left\{ \begin{bmatrix} | & | & | \\ b_1 & b_2 & b_3 \\ | & | & | \end{bmatrix} \begin{bmatrix} | \\ z \\ | \end{bmatrix} \middle| z \in \mathbb{Z}^n \right\} = \{Bz | z \in \mathbb{Z}\}$$



Definition 6.1. **(Lattice)** *Let B be a basis of $\mathbb{R}^n$ over $\mathbb{R}$, then a lattice is a submodule of $\mathbb{R}^n$ over $\mathbb{Z}$ which is generated by B over $\mathbb{Z}$.*

Result 6.2. *All properties of free modules are applicable to lattices.*

7 Duality in Modules

Consider the collection of all R linear maps from a module M to another module N, denoted as $Hom(M, N)$

$$Hom(M, N) = \{f | f : M \to N, R - \text{Linear Map}\}$$

consider the special case when $N = R$ which is a set of all $R-$linear maps that takes input as M and outputs a ring element. Such maps are called functionals, and such a set again forms a module which we would call the **dual module** of M and would represent it as M^V. It is also called the dual space or $R-$ dual of M.

Definition 7.1. **(Dual Module)** *Let M be a $R-$ module then the dual of M is defined as*

$$M^V = Hom(M, R) = \{f | f : M \to R, R - \textit{Linear Map}\}$$

Example 7.2. *Let R be a ring with unit then we have R^n as a R module, we will construct its dual*

Let R^n has a basis $b_1, b_2, \cdots, b_n$ then any element of R^n can be represented as a $\mathbb{Z}$ linear combination $r_1b_1 + r_2b_2 + \cdots r_nb_n$. Now any linear map f does the following

$$f(r_1b_1 + r_2b_2 + \cdots r_nb_n) = r_1f(b_1) + r_2f(b_2) + \cdots + r_nf(b_n)$$

Here, we have $r_i \in R$ and $f(b_i) \in R$ and we should recall that the operation is valid here.
In a R module on M we are equipped with the following operations

- $+ : M \times M \to M$
- $\oplus : R \times R \to R$
- $\circ : R \times M \to R$
- $* : R \times R \to R$ is what we use here.

consider dot product on R^n defined for all $v = (v_1, v_2, \cdots, v_n)$ and $w = (w_1, w_2, \cdots, w_n)$ in R^n as

$$v.w = (v_1, v_2, \cdots, v_n) \cdot (w_1, w_2, \cdots, w_n) = v_1 * w_1 + v_2 * w_2 + \cdots + v_n * w_n$$

we already have this as

$$f(r_1 b_1 + r_2 b_2 + \cdots r_n b_n) = r_1 f(b_1) + r_2 f(b_2) + \cdots + r_n f(b_n) = (r_1, r_2, \cdots, r_n) \cdot (f(b_1), f(b_2), \cdots, f(b_n))$$

Now if we fix this tuple $(f(b_1), f(b_2), \cdots, f(b_n))$ we will get functionals as f_w for $w \in R^n$ which is defined as $f_w(x) = x \cdot w$
We now claim that the set of functionals $M^V = \{f_w | f_w : R^n \to R, \ \forall w \in R\}$ is closed under the ring operations.

(Addition) $f_{r_1+r_2}(x) = x \cdot (r_1 + r_2) = x \cdot r_1 + x \cdot r_2 = f_{r_1}(x) + f_{r_2}(x) = (f_{r_1} + f_{r_2})(x)$
Thus, $f_{r_1} + f_{r_2} = f_{r_1+r_2} \in M^V$

(Multiplication) $f_{r_1 r_2}(x) = x \cdot r_1 r_2 = \begin{cases} x \cdot r_1 r_2 = f_{r_1}(x) r_2 \\ x \cdot r_2 r_1 = f_{r_2}(x) r_1 \end{cases}$
Thus, $r_1 f_{r_2} = r_2 f_{r_1} = f_{r_1 r_2} \in M^V$

A thing to observe here is that the functionals $f_w \in M^V$ are characterized by basis elements of M.

$$f_{b_i}(\underbrace{r_1 \mathbf{b_1} + r_2 \mathbf{b_2} + \cdots + r_n \mathbf{b_n}}_{r_i \in R}) = r_i, \qquad i = 1, 2, \cdots, n$$

$$\begin{aligned} b_1 &\mapsto f_{b_1} \rightsquigarrow f_{d_1} \rightsquigarrow d_1 \\ b_2 &\mapsto f_{b_2} \rightsquigarrow f_{d_2} \rightsquigarrow d_1 \\ &\vdots \qquad\qquad \vdots \\ b_n &\mapsto f_{b_n} \rightsquigarrow f_{d_1} \rightsquigarrow d_1 \end{aligned}$$

So, for a basis $B = \{b_1, b_2, \cdots, b_n\}$ of a $R-$module M, the basis of its dual module also known as dual basis $D = \{d_1, d_2, \cdots, d_n\}$ is the set of linearly independent module elements that satisfy

$$d_i \cdot b_j = \begin{cases} 0; & i \neq j \\ 1; & i = j \end{cases}$$

7.1 Looking into Lattice Duals

$\mathbb{R}^n$ over ring $\mathbb{R}$ is a module, let B be a basis of this module and now we have span$(B) = \mathbb{R}^n$, and let $\mathcal{L}$ is a module generated by B over $\mathbb{Z}$.
We now want to define dual of lattice as $\mathcal{L}^V = \{f | f : \mathcal{L} \xrightarrow{\mathbb{Z}-\text{linear}} \mathbb{Z}\}$ and it fails,

Consider the lattice $\mathcal{L}(\sqrt{2}) = \{\sqrt{2}z | z \in \mathbb{Z}\}$. Now we define $\mathcal{L}^V = \{f | f : \mathcal{L} \xrightarrow{\mathbb{Z}-\text{linear}} \mathbb{Z}\}$
Any $\mathbb{Z}$ linear map would take the an input from lattice and scale it with an integer which would be a desired output.
In our case,
$f(\sqrt{2}) = n\sqrt{2}$, for some $n \in \mathbb{Z}$
Next thing is, for any such f in $\mathcal{L}^V$ our output have to be an integer.
$n\sqrt{2} = m$ such that $m \in \mathbb{Z}$.

Now,

$$n\sqrt{2} = m \implies \sqrt{2} = \frac{m}{n}$$

This is a contradiction.

Our next attempt of defining it as $\mathcal{L}^V = \{f | f : \mathcal{L} \xrightarrow{\mathbb{R}-\text{linear}} \mathbb{Z}\}$ however works.
In words we are having the flexibility to choose $\mathbb{R}-$linear maps that take a lattice element as input and bring out an integer as output.

$$\begin{aligned} f(\mathcal{L}) &\subseteq \mathbb{Z} \\ f_r(c_1b_1 + c_2b_2 + \cdots + c_nb_n) &= c_1f_r(b_1) + c_2f_r(b_2) + \cdots + c_nf_r(b_n) \\ &= (f_r(b_1), f_r(b_2), \cdots, f_r(b_n)) \cdot (c_1, c_2, \cdots, c_n) \end{aligned}$$

Moreover for a basis B of a lattice when looked as a module, we will have a dual basis D, i.e the basis of dual lattice such that,

$$D^TB = I$$

and for a square matrix we will always have $D^{-T} = B$

8 Bonus Remark

Modules will come handy with calculations when we would define the hard lattice problems such as Learning With Errors (LWE) and Short Integer Solution (SIS). These algebraic structure equipped with lattices helps to do fast computaions and reduce space. We will soon look into this in subsequent articles.

9 Conclusion

Our attention towards lattice as modules is to get an idea of what duals are in the abstract mathematical sense. However, to do computations we need ingredients such as directions, norms, etc. which is readily available in a Hilbert space. Our discussion on duals will continue with vector spaces in the next article.

References

[Con07] Keith Conrad. *Dual Modules.* 2007. URL: `https://kconrad.math.uconn.edu/blurbs/linmultialg/dualmod.pdf`.

[Mic14] Daniel Micciancio. *Lecture Notes on Lattices Algorithms and Applications.* 2014. URL: `https://cseweb.ucsd.edu/classes/sp14/cse206A-a/`.

[Mus01] C Musili. *Introduction to Rings and Modules.* en. 2nd ed. New Delhi, India: Narosa Publishing House, Jan. 2001.