Содержание

ИСП Решётки

1. О сложности

2. О решётках

Определение 2.1 (Абелева группа)

Множество G вместе с отображением

$$G \times G \to G$$

называемым **операцией** на группе G и записываемым $g_1 + g_2 = g$, называется **абелевой группой**, если выполнены соотношения:

- $g_1 + g_2 = g_2 + g_1$ – **коммутативность**
- $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$ – **ассоциативность**
- Существует такой элемент $0 \in G$, что для всех $g \in G$ выполняется равенство $g + 0 = g$ – **существование нейтрального элемента**
- Для любого $g \in G$ существует $-g \in G$, для которого выполнено соотношение $g + (-g) = 0$ – **существование обратного элемента**

♣

Определение 2.2. Абелева группа

Определение 2.2 (Кольцо)

Множество A с двумя операциями $+ : A \times A \to A$ и $\times : A \times A \to A$ называется **кольцом**, если A абелева группа относительно операции $+$ и выполняются следующие условия

- **Ассоциативность**:

$$\forall a, b, c \in A : (ab)c = a(bc)$$

- **Дистрибутивность**:

$$\forall a, b, c \in A : (a + b)c = ac + bc; c(a + b) = ca + cb$$

Также, если $\forall a, b \in A$ выполняется $ab = ba$, то такое кольцо называется **коммутативным**.

Если существует элемент 1, такой, что $1 \cdot a = a \cdot 1$, то такое кольцо называется **кольцом с единицей**.

♣

Определение 2.3. Кольцо

Определение 2.3 (A-модуль)

Пусть A – кольцо. Абелева группа G называется **A-модулем**, если определена операция умножения $A \times G \to G$, для которой выполняются условия:

- **Ассоциативность**:

$$\forall a, b \in A : \forall g \in G : (ab)g = a(bg)$$

- **Дистрибутивность**:

$$\forall a, b \in A : \forall g \in G : (a + b)g = ag + bg$$

$$\forall a \in A : \forall g_1, g_2 \in G : a(g_1 + g_2) = ag_1 + ag_2$$

♣

Определение 2.4. А-модуль

Определение 2.4 (Система образующих)

Множество M элементов аддитивной абелевой группы G называется **системой образующих** этой группы, рассматриваемой как $\mathbb{Z}$-модуль, если любой её элемент α можно представить в виде

$$\alpha = c_1\alpha_1 + \ldots + c_n\alpha_n \quad c_i \in \mathbb{Z}, \alpha_i \in M$$

Система образующих называется **базисом**, если такое представление единственно

♣

Определение 2.5. Система образующих

Определение 2.5 (Элемент конечного порядка)

Элемент $a \neq 0$ аддитивной абелевой группы M называется **элементом конечного порядка**, если при некотором $c \in \mathbb{Z}, c \neq 0$:

$$\underbrace{a + \ldots + a}_{c} = 0$$

Принято считать, что 0 также элемент конечного порядка

♣

Определение 2.6. Элемент конечного порядка

Теорема 2.6

Если абелева группа без элементов конечного порядка имеет конечную систему образующих, то она имеет и базис.

Число элементов базиса является инвариантом группы.

♡

Теорема 2.7.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ – некоторая конечная система образующих.

Заметим, что при замене одной из образующих на новую, полученную добавлением к ней другой образующей, умноженной на произвольное целое число, снова получится система образующих.

Действительно, пусть $\alpha_1' = \alpha_1 + k\alpha_2$. Тогда для любого $\alpha \in M$ имеем

$$\alpha = c_1\alpha_1 + \ldots + c_n\alpha_n = c_1\alpha_1' + (c_2 - kc_1)\alpha_2 + \ldots + c_n\alpha_n$$

Если элементы $\alpha_1, \ldots\alpha_n$ линейно независимы, то они образуют базис M. Пусть они линейно зависимы, тогда существует ненулевая последовательность коэффициентов $c_1, \ldots, c_n$ разложения нуля.

Выберем среди ненулевых элементов коэффициент c_i с наименьшим абсолютным значением. БОО, можно считать, что это c_1.

Пусть не все коэффициенты c_i делятся на c_1, тогда $c_2 = c_1 q + c'$, где $0 < c' < |c_1|$.

Перейдём к новой системе образующих, где $\alpha_1' = \alpha_1 + q\alpha_2$. Тогда

$$c_1\alpha_1' + c'\alpha_2 + \ldots + c_n\alpha_n = 0$$

Продолжим данную процедуру до тех пор пока через конечное число шагов не получим соотношение

$$k_1\beta_1 + k_2\beta_2 + \ldots + k_n\beta_n = 0$$

с целыми коэффициентами k_i, в котором один из коэффициентом, БОО k_1, является делителем остальных. Сократив на k_1, получим

$$\beta_1 + l_2\beta_2 + \ldots + l_n\beta_n = 0$$

с целыми $l_2, \ldots, l_n$. Следовательно, $\beta_2, \ldots, \beta_n$ – система образующих группы M, состоящая из $n-1$ элемента.

Теперь мы может применять этот алгоритм снова и получим либо базис, либо новую систему образующих с меньшим количеством элементов. Повторив эту процедуру конечное число раз, получим базис группы.

Инвариантость числа элементов базиса M следует из инвариантности размерности векторного пространства $M \otimes \mathbb{Q}$, в которое M вложено. □

Следствие 2.6.1 (Свойства базисов абелевых групп)

Пусть $\omega_1, \ldots, \omega_m$ и $\omega_1', \ldots, \omega_m'$ – два базиса модуля M. Тогда матрица перехода одного базиса в другой – целочисленна, порядка m с определителем единица. ♡

Следствие 2.6.2. Свойства базисов абелевых групп

Определение 2.7 (Ранг абелевой группы)

Максимальное количество линейно независимых элементов абелевой группы называется её **рангом** ♣

Определение 2.8. Ранг абелевой группы

Определение 2.8 (Решётка)

Решёткой называется подгруппа группы $\mathbb{R}^n$, порождённая системой линейно независимых над $\mathbb{R}$ векторов-столбцов

$$b_1, \ldots, b_n \in \mathbb{R}^n$$

Если $m = n$, то решётка называется **полной**, в противном случае – **неполной**. Базис группы в этом случае называется базисом решётки.

Набор базисных векторов-столбцов задаёт матрицу

$$B = [b_1 \mid \ldots \mid b_m]$$

Матрица B называется матрицей, **соответствующей** решетки.

Определение 2.9. Решётка

Определение 2.9

Пусть $b_1, \ldots, b_m$ – базис решётки Λ в $\mathbb{Z}^n$.

Основным паралелепипедом этой решётки называется множество

$$T = T(\Lambda) = \{x \in \mathbb{R}^n \mid x = \alpha_1 b_1 + \ldots + \alpha_m b_m \mid 0 \leq \alpha_i < 1\}$$

Детерминантном решётки Λ называется m-мерный объём этого множества и обозначается через $\det(\Lambda)$.

Определение 2.10.

Теорема 2.10 (Критерий полноты решётки)

Решётка M в линейном пространстве L полна тогда и только тогда, когда в L существует ограниченное множество U, сдвиги которого на векторы из M полностью заполняют всё пространство L.

Теорема 2.11. Критерий полноты решётки

Доказательство. Если решётка Λ полная, то в качестве U можно взять любой её основной паралелепипед.

Пусть теперь решётка Λ неполная, и пусть U – произвольное ограниченное подмножество в $\mathbb{R}^n$.

Тогда существует такое $r > 0$, что

$$\forall x \in U : \|x\| < r$$

Пусть $L_0 \subset \mathbb{R}^n$ – подпространство, порождённое решёткой Λ. Поскольку решётка неполная, то L_0 – собственное подпространство и, следовательно, существует вектор $y \in \mathbb{R}^n$, имеющий длину больше r и ортогональный подпространству L_0.

Покажем, что y не покрывается сдвигами множества U.

Пусть это не так, тогда при некоторых $u \in U, z \in \Lambda$ выполняется равенство $y = u + z$. Тогда, согласно неравенству Коши-Буняковского

$$\|y\|^2 = (y, y) = (y, u) \leq \|y\| \|u\| < r\|y\|$$

откуда $\|y\| < r$ – противоречие. □