Решетки, алгоритмы и современные проблемы криптографии. Основные понятия и определения теории решеток

Шокуров

5 февраля 2025 г.

Абелевы группы

Определение

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. Этот элемент обозначается через $-g$.*

Примеры абелевы групп

Замечание. Обычно операция в абелевых группах имеет аддитивную запись. Но имеются, конечно, и мультипликативные абелевы группы.

- $\mathbb{Z}$ — группа целых чисел относительно сложения.
- $\mathbb{Z}^n$ — группа целочисленных векторов длины n относительно сложения векторов.
- $\mathbb{R}^n$ — группа вещественных векторов длины n относительно сложения векторов.
- $\mathbb{Q}^*$ — группа ненулевых рациональных чисел относительно операции умножения.
- $G = \{x \in \mathbb{Q} | x = a/2^n, a, n \in \mathbb{Z}, n \geq 0\}$ — группа относительно операции сложения.
- $\mathbb{Z}/n\mathbb{Z}$ — группа сравнений по модулю n.
- Группа алгебраических чисел относительно операции сложения.
- Группа целозначных матриц размера $n \times m$ относительно сложения.
- Группnпа целозначных матриц размера $n \times n$ с определителем 1 относительно операции умножения матриц (не является коммутативной).

Кольца

Определение

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

1. ***Ассоциативность**: Для любых $a, b, c \in A$ выполняется $(ab)c = a(bc)$.*
2. ***Дистрибутивность**: Для любых $a, b, c \in A$ выполняется $(a + b)c = ac + bc$ и $(a + b) = ca + cb$.*

Если также для любых a, inA 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.

Примеры.

1. Кольцо целых чисел $\mathbb{Z}$.
2. Кольцо рациональных чисел $\mathbb{Q}$.
3. Кольцо матриц размера $n \times n$.

Абелевы группы как $\mathbb{Z}$-модули

Определение

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

1. ***Ассоциативность**: Для любых $a, b \in A$, $g \in G$ выполняется $(ab)g = a(bg)$.*
2. ***Дистрибутивность**: Для любых $a, b \in A$, $g \in G$ выполняется $(a + b)g = ag + bg$.*
3. ***Дистрибутивность**: Для любых $a \in A$, $g_1 g_2 \in G$ выполняется $a(g_1 + g_2) = ag_1 + ag_2$.*

Образующие и базисы абелевых групп

Определение

Прямой суммой абелевых групп G и H называется группа $G \oplus H$, элементами которой являются пары $(g, h), g \in G, h \in H$. Сумма элементов определяется формулой
$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$.

Определение

Множество M элементов аддитивной абелевой группы G называется системой образующих этой группы, рассматриваемой как $\mathbb{Z}$-модуль, если любой ее элемент α можно представить в виде $\alpha = c_1\alpha_1 + \ \ldots + c_n\alpha_n$, где $c_i \in \mathbb{Z}$, $\alpha_i \in M$. Система образующих называется базисом, если такое представление единственно.

Определение

Элемент $a \neq 0$ аддитивной абелевой группы M называется элементом конечного порядка, если $ca = 0$ при некотором $c \in \mathbb{Z}$, $c \neq 0$. Элемент 0 также элемент конечного порядка.

Свойства базисов абелевых групп

Определение

Элементы $g_1, \ldots, g_n$ абелевой группы называются линейно независимыми, если из соотношения $a_1 g_1 + \ldots + a_n g_n = 0$ для целых $a_1, \ldots, a_n$ следует, что $a_1 = \ldots = a_n = 0$.

Лемма

Система образующих является базисом тогда и только тогда, когда эти образующие линейно независимы.

Доказательство.

Пусть имеется два представления некоторого элемента $a_1 g_1 + \ldots a_n g_n = b_1 g_1 + \ldots b_n g_n$. Это условие эквивалентно условию линейной зависимости $(a_1 - b_1) g_1 + \ldots (a_n - b_n) g_n = 0$. □

Теорема

Если абелева группа без элементов конечного порядка имеет конечную систему образующих, то она имеет и базис. Число элементов базиса является инвариантом группы.

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. Допустим теперь, что они линейно зависимы, т. е. выполняется соотношение

$$c_1\alpha_1 + \ldots + c_n\alpha_n = 0$$

при некоторых одновременно не равных нулю целых $c_1, \ldots, c_n$. Выберем среди ненулевых элементов коэффициент c_i с наименьшим абсолютным значением. Без ограничения общности можно считать, что это c_1. Пусть не все коэффициенты c_i делятся на c_1, например, $c_2 = c_1q + c'$, где $0 < c' < |c_1|$.

Перейдем к новой системе образующих $\alpha'_1 = \alpha_1 + q\alpha_2, \ \ldots, \alpha_n$. Тогда будет выполняться соотношение

$$c_1\alpha'_1 + c'\alpha_2 + \ \ldots + c_n\alpha_n = 0,$$

причем $0 < c' < |c_1|$. Продолжим данную процедуру до тех пор пока через конечное число шагов (не более $|c_1|$) 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 коэффициентов, например, k_1 является делителем остальных. Сократив последнее выражение 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 $(n-1)$ -го элемента.

Теперь можем применить описанную здесь процедуру к новой системе образующих. В результате получим либо базис, либо новую систему образующих с меньшим количеством элементов. Повторив эту процедуру конечное число раз, получим базис группы.
Напомним, что $M \otimes \mathbb{Q} = M \times \mathbb{Q}/\sim$, где отношение $\sim$ задается формулой

$$(k\alpha, r) \sim (\alpha, kr),$$

где $k \in \mathbb{Z}, \alpha \in M, r \in \mathbb{Q}$. Имеется вложение групп

$$M \hookrightarrow M \otimes \mathbb{Q},$$

преобразующее линейно независимые элементы в линейно независимые. Инвариантность числа элементов базиса теперь следует из инвариантности размерности векторного пространства $M \otimes \mathbb{Q}$.

Следствие

Пусть $\omega_1, \ldots, \omega_m$ и $\omega'_1, \ldots, \omega'_m$ — два базиса модуля M. Тогда матрица перехода одного базиса в другой целочисленная матрица порядка m с определителем единица.

Ранг группы

Определение

Максимальное количество линейно независимых элементов абелевой группы называется ее рангом. Число элементов группы называется порядком этой группы.

Определение

Пусть $g \in G$. Минимальное положительное число k, такое, что $kg = 0$ называется порядком элемента g.

Предложение

Порядок элемента не превосходит числа элементов группы. Если порядок группы конечен, что порядок любого элемента этой группы делит порядок группы. В частности все элементы конечной группы имеют конечный порядок.

Ранг группы

Определение

Кручением абелевой группы называется множество всех ее элементов конечного порядка, т.е.

$$\operatorname{Tors} G = \{g \in G \mid \exists n \in \mathbb{Z} \mid n \neq 0, ng = 0\}.$$

Предложение

Tors G — *подгруппа группы* G.

Лемма

Подгруппа группы $\mathbb{Z}^n$ *конечно порождена и ее ранг не превосходит* n.

Следствие

Подгруппа в $\mathbb{Z}$ *имеет базис.*

Задача. Доказать лемму и вывести следствие.

Существование базисов

Теорема

В абелевой группе M без элементов конечного порядка и с конечной системой образующих всякая подгруппа N также имеет конечное число образующих и, следовательно, имеет базис. При этом для любого базиса $\omega_1, \ldots, \omega_m$ группы M для N существует базис вида

$$\begin{array}{lllllll} \eta_1 & = & c_{11}\omega'_1 + & c_{12}\omega'_2 + & \ldots + & c_{1k}\omega'_k + & \ldots + c_{1m}\omega'_m \\ \eta_2 & = & & c_{22}\omega'_2 + & \ldots + & c_{2k}\omega'_k + & \ldots + c_{1m}\omega'_m \\ \ldots & \ldots & \ldots\ldots & \ldots\ldots\ldots\ldots & & \ldots\ldots\ldots\ldots\ldots\ldots & \\ \eta_k & = & & & & c_{kk}\omega'_k + & \ldots + c_{km}\omega'_m \end{array},$$

где базис $\omega'_1, \ldots, \omega'_m$ отличается от базиса $\omega_1, \ldots, \omega_m$ только перестановкой элементов.

Доказательство. Пусть базис подгруппы $N \subset M$ выражается через базис $\omega_1, \ \ldots, \omega_m$ группы M соотношениями

$$\begin{array}{lllll} \beta_1 & = & a_{11}\omega_1 + & a_{12}\omega_2 + \ \ldots + & a_{1k}\omega_k + \ \ldots + a_{1m}\omega_m \\ \beta_2 & = & a_{21}\omega_1 + & a_{22}\omega_2 + \ \ldots + & a_{2k}\omega_k + \ \ldots + a_{2m}\omega_m \\ \ldots & \ldots & \ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_k & = & a_{k1}\omega_1 + & a_{k2}\omega_2 + \ \ldots + & a_{kk}\omega_k + \ \ldots + a_{km}\omega_m \end{array},$$

Пусть a — минимальная из ненулевых координат вектора $(|a_{11}|, |a_{21}|, \ \ldots, |a_{k,1}|)$. Если все координаты нулевые, то поменяем порядок базисных векторов группы M, поместив базисный вектор ω_1 в конец списка.

Без ограничения общности можно считать, что $|a_{11}| = a$ (в противном случае поменяем строки и перенумеруем элементы базиса группы N в другом порядке). Выполним деление с остатком $a_{21} = \alpha a + b_{21}, \ 0 \leq b_{21} < |a|$ и положим $\beta_2' = \beta_2 - \alpha\beta_1$. Тогда

$$\beta_2' = b_{21}\omega_1 + (a_{22} - \alpha a_{12})\omega_2 + \ \ldots + (a_{2m} - \alpha a_{1m})\omega_m.$$

Повторим эту процедуру со всеми оставшимися строками.

В результате получим новый базис подгруппы N

$$\begin{array}{lllll}
\beta'_1 &= b_{11}\omega_1 + & b_{12}\omega_2 + \ldots + & b_{1k}\omega_k + \ldots + & b_{1m}\omega_m \\
\beta'_2 &= b_{21}\omega_1 + & b_{22}\omega_2 + \ldots + & b_{2k}\omega_k + \ldots + & b_{2m}\omega_m \\
\ldots & \ldots & \ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\
\beta'_k &= b_{k1}\omega_1 + & b_{k2}\omega_2 + \ldots + & b_{kk}\omega_k + \ldots + & b_{km}\omega_m
\end{array},$$

для которого либо все, кроме первой координаты в векторе $(|b_{11}|, \ldots, |b_{k1}|)$ нулевые, либо минимальная величина из ненулевых элементов этого вектора меньше a. Будем повторять эту процедуру до тех пор, пока не добъемся выполнения первого условия: равенства нулю всех координат, кроме первой.
В итоге получим базис подгруппы, представимый в виде

$$\begin{array}{lllll}
\beta_1 &= a_{11}\omega_1 + & a_{12}\omega_2 + \ldots + & a_{1k}\omega_k + \ldots + & a_{1m}\omega_m \\
\beta_2 &= & a_{22}\omega_2 + \ldots + & a_{2k}\omega_k + \ldots + & a_{2m}\omega_m \\
\ldots & \ldots & \ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\
\beta_k &= & a_{k2}\omega_2 + \ldots + & a_{kk}\omega_k + \ldots + & a_{km}\omega_m
\end{array}.$$

Теперь повторим эту процедуру для строк со 2-й до k-й. В итоге получим второй вектор базиса и так далее, пока не исчерпаем все строки. Полученное представление базиса будет искомым.

Определение решетки

Определение

Решеткой называется подгруппа группы $\mathbb{R}^n$, порожденная системой линейно независимых над $\mathbb{R}$ векторов-столбцов $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$. Если $m = n$, то решетка называется полной, в противном случае — неполной. Базис группы называется в этом случае базисом решетки.Набор базисных векторов-столбцов задает матрицу

$$B = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m].$$

Матрица B называется матрицей соответствующей решетки.

Определение

Решетка называется целочисленной, если матрица B — целочисленная.

Инвариантность размерности решетки

Напомним, что целочисленная $m \times m$ матрица с определителем единица называется **унимодулярной**.

Лемма

Пусть имеются два набора линейно независимых векторов B и B', задающие одну и ту же решетку размерности n. Тогда ранги матриц B и B' равны и существует единственная унимодулярная $m \times m$ матрица A, такая что $BA = B'$.

Задача. Доказать лемму.

Замечание. В силу доказанных выше теорем число m из определения решетки задается однозначно и совпадает с рангом группы решетки.
Решетку, порожденную линейно независимыми векторами $\mathbf{b}_1, \ldots, \mathbf{b}_m$ будем обозначать так

$$\Lambda = L(\mathbf{b}_1, \ldots, \mathbf{b}_m).$$

Дискретные подгруппы

Определение

Подгруппа G группы $\mathbb{R}^n$ называется дискретной, если в шаре $U(r) = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\| < r\}$ радиуса r имеется только конечное число элементов группы G.

Лемма

Решетка является дискретной группой.

Доказательство.

Выберем базис $\mathbf{b}_1, \ldots, \mathbf{b}_k$ в решетке. Дополним этот набор линейно независимых векторов в $\mathbb{R}^n$ до базиса $\mathbf{b}_1, \ldots, \mathbf{b}_n$ векторного пространства $\mathbb{R}^n$, содержащего решетку. Выберем ненулевой элемент $\mathbf{x} \in \mathbb{R}^n$, ортогональный векторам $\mathbf{b}_2, \ldots, \mathbf{b}_n$. Положим $\mathbf{f}_1 = \frac{\mathbf{x}}{(\mathbf{x}, \mathbf{b}_1)}$. Заметим, что согласно определению элемента x знаменатель не равен нулю и $(\mathbf{f}_1, \mathbf{b}_j) = \delta_{1j}$. Аналогично определяются элементы $\mathbf{f}_i$, причем выполняются равенства $(\mathbf{f}_i, \mathbf{b}_j) = \delta_{ij}$.

Пусть элемент решетки $\mathbf{z}$ имеет длину меньше r. Выразим его через базис

$$\mathbf{z} = a_1\mathbf{b}_1 + \ldots + a_k\mathbf{b}_k$$

где $a_1, \ldots, a_k \in \mathbb{Z}$, причем $a_i = (\mathbf{z}, \mathbf{f}_i)$ по определению векторов $\mathbf{f}_i$. Тогда согласно неравенству Коши

$$|a_i| = |(\mathbf{z}, \mathbf{f}_i)| \leq \|\mathbf{z}\|\|\mathbf{f}_i\| < r\|\mathbf{f}_i\|.$$

Следовательно, ввиду целочисленности коэффициентов a_i, в шаре радиуса r лежит конечное число элементов решетки. □

Решетки

Определение

Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ — базис решетки Λ в $\mathbb{Z}^n$. Основным параллелепипедом этой решетки называется множество

$$T = T(\Lambda) = \{x \in \mathbb{R}^n | x = \alpha_1 \boldsymbol{b}_1 + \ldots + \alpha_m \boldsymbol{b}_m \mid 0 \leq \alpha_i < 1\}.$$

Детерминантом решетки Λ называется m-мерный объем этого множества и обозначается через $\det(\Lambda)$.

Отметим, что параллелепипед решетки зависит от выбранного базиса. Тем не менее детерминант решетки не зависит от выбранного базиса.

Лемма

Детерминант решетки не зависит от выбранного базиса.

Доказательство. Дополним базис решетки до базиса векторного пространства $\mathbb{R}^n$ взаимно ортогональными векторами единичной длины $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$, ортогональными подпространству, порожденному векторами $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Тогда объем основного параллелепипеда на базисе $\mathbf{b}_1, \ldots, \mathbf{b}_k$ равен объему основного параллелепипеда на базисе $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Пусть $\mathbf{f}_1, \ldots, \mathbf{f}_k$ — другой базис решетки. Тогда его можно пополнить теми же векторами $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ до базиса в $\mathbb{R}^n$. Преобразование базиса $\mathbf{b}_1, \ldots, \mathbf{b}_k$ в базис $\mathbf{f}_1, \ldots, \mathbf{f}_k$ продолжается до унимодулярного преобразования базиса $\mathbf{b}_1, \ldots, \mathbf{b}_n$ в базис $\mathbf{f}_1, \ldots, \mathbf{f}_k, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$.
Объем основного параллелепипеда равен абсолютной величине определителя, строками которого являются координаты базисных векторов,

$$\begin{vmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{vmatrix}.$$

Поскольку базисы связаны унимодулярными преобразованиями, соответствующие объемы равны.

Лемма

Если T — основной параллелепипед полной решетки M, то имеется разбиение

$$\mathbb{R}^n = \bigcup_{z \in M} z + T,$$

причем $z + T \cap w + T = \emptyset$ при $z \neq w$.

Упражнение. Доказать лемму.

Решетки и дискретные группы

Лемма

Пусть M — решетка. Для любого $r > 0$ множество $N = \{z \in M \mid z + T \cap U(r) \neq \emptyset\}$ конечно.

Доказательство.

Пусть $\mathbf{b}_1, \ldots, \mathbf{b}_n$ — базис решетки M. Положим

$$d = \|\mathbf{b}_1\| + \ldots + \|\mathbf{b}_n\|.$$

Пусть $\mathbf{x} = \mathbf{z} + \mathbf{t} \in U(r)$, где $\mathbf{z} \in M$ и $\mathbf{t} \in T$. Тогда

$$\|\mathbf{t}\| = \|\alpha_1\mathbf{b}_1 + \ldots + \alpha_n\mathbf{b}_n\| \leq \alpha_1\|\mathbf{b}_1\| + \ldots + \alpha_n\|\mathbf{b}_n\| < d$$

и

$$\|\mathbf{z}\| = \|\mathbf{x} - \mathbf{t}\| \leq \|\mathbf{x}\| + \|\mathbf{t}\| < r + d,$$

т. е. множество N лежит в шаре радиуса $r + d$ и, следовательно, согласно лемме о дискретности решетки это множество конечно. □

Решетки и дискретные группы

Лемма

Дискретная группа является решеткой.

Следствие

Подгруппа $M \subset \mathbb{R}^n$ является решеткой тогда и только тогда, когда она дискретна.

Доказательство леммы. Пусть $L \subset \mathbb{R}^n$ — минимальное линейное пространство, содержащее группу M. Выберем в L базис $\mathbf{b}_1, \ldots, \mathbf{b}_m$ из элементов группы M и построим решетку M_0 с этим базисом. Тогда M_0 — подгруппа в M. Покажем, что индекс этой группы конечен. Для этого достаточно проверить, что факторгруппа M/M_0 состоит из конечного числа элементов. Согласно лемме о разбиении линейной оболочки решетки сдвигами основного параллелипипеда на элементы решетки получим, что элементы факторгруппы однозначно представляются элементами группы M, находящимися в основном параллелепипеде решетки M_0, содержащемся в шаре конечного радиуса. Поскольку группа M дискретна, число таких элементов конечно. Поэтому группа M конечно порождена и, следовательно, является решеткой.

Детерминант решетки

Лемма

Пусть $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ базис решетки M. Тогда ее детерминант равен квадратному корню из определителя

$$\begin{vmatrix} (\boldsymbol{b}_1, \boldsymbol{b}_1) & \cdots & (\boldsymbol{b}_1, \boldsymbol{b}_m) \\ \cdots & \cdots & \cdots \\ (\boldsymbol{b}_m, \boldsymbol{b}_1) & \cdots & (\boldsymbol{b}_m, \boldsymbol{b}_m) \end{vmatrix}.$$

Доказательство. Детерминант решетки, согласно определению, равен абсолютной величине определителя матрицы

$$D = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix},$$

где $\mathbf{b}_1, \ \ldots, \mathbf{b}_m$, а $\mathbf{b}_{m+1}, \ \ldots, \mathbf{b}_n$ — его ортогональное продолжение. Поэтому, он равен квадратному корню из квадрата определителя матрицы D и, следовательно, равен квадратному корню из определителя матрицы DD', где $'$ — операция транспонирования.

Имеем

$$
\begin{aligned}
DD' &= \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ \cdots & \cdots & \cdots \\ b_{1n} & \cdots & b_{nn} \end{pmatrix} \\
&= \begin{pmatrix} (\mathbf{b}_1, \mathbf{b}_1) & \cdots & (\mathbf{b}_1, \mathbf{b}_n) \\ \cdots & \cdots & \cdots \\ (\mathbf{b}_n, \mathbf{b}_1) & \cdots & (\mathbf{b}_n, \mathbf{b}_n) \end{pmatrix} \\
&= \begin{pmatrix} (\mathbf{b}_1, \mathbf{b}_1) & \cdots & (\mathbf{b}_1, \mathbf{b}_m) & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (\mathbf{b}_m, \mathbf{b}_1) & \cdots & (\mathbf{b}_m, \mathbf{b}_m) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{pmatrix} \\
&= \begin{pmatrix} (\mathbf{b}_1, \mathbf{b}_1) & \cdots & (\mathbf{b}_1, \mathbf{b}_m) \\ \cdots & \cdots & \cdots \\ (\mathbf{b}_m, \mathbf{b}_1) & \cdots & (\mathbf{b}_m, \mathbf{b}_m) \end{pmatrix}.
\end{aligned}
$$

Критерий полноты решетки

Теорема

Решетка 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 все пространство L.

Доказательство. Если решетка Λ полная, то в качестве U можно взять любой ее основной параллелепипед.
Пусть теперь решетка Λ неполная, и пусть U — произвольное ограниченное подмножество в $\mathbb{R}^n$. Тогда существует такое $r > 0$, что $\|\mathbf{x}\| < r$ для любого $\mathbf{x} \in U$. Пусть $L_0 \subset \mathbb{R}^n$ — подпространство, порожденное решеткой Λ. Поскольку решетка неполная, то L_0 — собственное подпространство и, следовательно, существует вектор $\mathbf{y} \in \mathbb{R}^n$, имеющий длину больше r и ортогональный подпространству L_0. Покажем, что $\mathbf{y}$ не покрывается сдвигами множества U. Пусть это не так, тогда при некоторых $\mathbf{u} \in U$, $\mathbf{z} \in \Lambda$ выполняется равенство $\mathbf{y} = \mathbf{u} + \mathbf{z}$. Тогда согласно неравенству Коши-Буняковского

$$\|\mathbf{y}\|^2 = (\mathbf{y}, \mathbf{y}) = (\mathbf{y}, \mathbf{u}) \leq \|\mathbf{y}\| \cdot \|\mathbf{u}\| < r\|\mathbf{y}\|,$$

откуда $\|\mathbf{y}\| < r$.

Лемма Минковского

Теорема

(Лемма Минковского о выпуклом теле). *Пусть в n -мерном пространстве $\mathbb{R}^n$ заданы полная решетка M, объем основного параллелепипеда которой равен Δ, и ограниченное центрально симметричное выпуклое множество X с объемом $v(X)$. Если $v(X) > 2^n\Delta$, то множество X содержит по крайней мере одну отличную от нуля точку решетки M.*

Доказательство. Докажем вначале, что если множество $Y \subset \mathbb{R}^n$ таково, что все его сдвиги $Y_{\mathbf{z}} = Y + \mathbf{z}$ на векторы $\mathbf{z}$ из решетки M не пересекаются, то $v(Y) \leq \Delta$. Рассмотрим основной параллелепипед T решетки M и рассмотрим пересечения $Y \cap T_{-\mathbf{z}}$. Тогда по лемме о разбиении пространства на сдвиги основного параллелепипеда на элементы решетки

$$v(Y) = \sum_{\mathbf{z} \in M} v(Y \cap T_{-\mathbf{z}}),$$

причем по лемме о конечности множества элементов решетки, сдвиги на котороые основного параллелипипеда имеют непустое пересечение с шаром, с в этой сумме только конечное число слагаемых не равно нулю. Сдвиг множества $Y \cap T_{-\mathbf{z}}$ на вектор $\mathbf{z}$ равен $Y_{\mathbf{z}} \cap T$, поэтому $v(Y \cap T_{-\mathbf{z}}) = v(Y_{\mathbf{z}} \cap T)$. Следовательно,

$$v(Y) = \sum_{\mathbf{z} \in M} v(Y_{\mathbf{z}} \cap T).$$

Поскольку все $Y_{\mathbf{z}}$ попарно не пересекаются, то сумма правой части не больше $v(T)$. Следовательно, $v(Y) \leq v(T) = \Delta$.

Рассмотрим теперь множество $\frac{1}{2}X$, получающееся из X преобразованием сжатия с коэффициентом $1/2$. Тогда из условия теоремы следует, что $v\left(\frac{1}{2}X\right) = \frac{1}{2^n}v(X) > \Delta$. Если все сдвиги множества $\frac{1}{2}X$ на элементы решетки попарно не пересекаются, то по доказанному выше должно выполняться неравенство $v\left(\frac{1}{2}X\right) \leq \Delta$, что противоречит условию теоремы. Следовательно, существуют $\mathbf{z}_1, \mathbf{z}_2 \in M$, для которых множества $\frac{1}{2}X + \mathbf{z}_1$ и $\frac{1}{2}X + \mathbf{z}_2$ имеют непустое пересечение. Поэтому

$$\frac{1}{2}\mathbf{x}' + \mathbf{z}_1 = \frac{1}{2}\mathbf{x}'' + \mathbf{z}_2, \quad \mathbf{x}', \mathbf{x}'' \in X.$$

Тогда

$$\mathbf{z}_1 - \mathbf{z}_2 = \frac{1}{2}\mathbf{x}'' - \frac{1}{2}\mathbf{x}' = \frac{1}{2}\mathbf{x}'' + \frac{1}{2}(-\mathbf{x}').$$

Поскольку множество X центрально симметрично и выпукло, то разность $\mathbf{z}_1 - \mathbf{z}_2 \in M$ лежит также и в X.