Лекция 6

Определение 1. Система элементов S абелевой группы A называется *линейно независимой* (над $\mathbb{Z}$), если из того, что $k_1 s_1 + \ldots + k_n s_n = 0$ для некоторых $k_i \in \mathbb{Z}$, $s_i \in S$, следует что все k_i равны нулю.

Определение 2. *Базис* абелевой группы – это линейно независимая система порождающих этой группы.

Заметим, что не у всякой группы есть базис. Например, у группы $\mathbb{Z}_n$ базиса нет, так как для любой системы $\{s_1, \ldots, s_k\}$ выполнено $ns_1 = 0$, что противоречит линейной независимости этой системы.

Определение 3. Пусть в абелевой группе A есть базис $\{e_1, \ldots, e_n, \ldots\}$. Тогда группа A называется *свободной абелевой группой.* Будем обозначать эту группу

$$\mathcal{A}(e_1, \ldots, e_n, \ldots).$$

Если базис конечен и имеет мощность n, то будем говорить, что A – свободная абелева группа ранга n и обозначать $\operatorname{rk} A = n$.

Лемма 1. *Пусть в абелевой группе A есть базис $\{e_1, \ldots, e_n\}$. Тогда любой другой базис этой группы также состоит из n элементов. (То есть ранг свободной абелевой группы определен однозначно.)*

Доказательство. Пусть в группе A есть другой базис $\{e'_1, \ldots, e'_m, \ldots\}$ и количество элементов в нем не равно n. Без ограничения общности мы можем считать, что в нем больше, чем n элементов. Рассмотрим $e'_1, \ldots, e'_{n+1}$ Так как $\{e_1, \ldots, e_n\}$ – базис, каждый элемент e'_j выражается через $\{e_1, \ldots, e_n\}$ с целыми коэффициентами: $e'_j = c_{1j}e_1 + \ldots + c_{nj}e_n$. Можно собрать все коэффициенты c_{ij} в целочисленную матрицу C размера $n \times n+1$ такую, что

$$(e'_1, \ldots, e'_{n+1}) = (e_1, \ldots, e_n)C.$$

Интерпретируем столбцы $C^{(1)}, \ldots, C^{(n+1)}$ матрицы C как векторы из пространства $\mathbb{Q}^n$ строк с рациональными коэффициентами длины n. Тогда столбцы – это $n+1$ векторов в n-мерном векторном пространстве. По основной лемме о линейной зависимости столбцы C линейно зависимы, то есть есть рациональные числа $\frac{p_1}{q_1}, \ldots, \frac{p_{n+1}}{q_{n+1}}$ не все равные нулю такие, что

$$\frac{p_1}{q_1}C^{(1)} \ldots + \frac{p_{n+1}}{q_{n+1}}C^{(n+1)} = 0.$$

Домножим это равенство на произведение знаменателей и получим

$$k_1 C^{(1)} \ldots + k_{n+1}C^{(n+1)} = 0$$

для некоторых $k_i \in \mathbb{Z}$ не всех равных нулю. Но тогда $k_1 e'_1 + \ldots + k_{n+1}e'_{n+1} = 0$, что противоречит линейной независимости $\{e'_1, \ldots, e'_{n+1}, \ldots\}$. $\square$

Замечание 1. Пусть $F = \mathcal{A}(e_1, \ldots, e_n)$. Тогда $F = \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$. В самом деле, сопоставим элементу $k_1 e_1 + \ldots k_n e_n \in \mathcal{A}(e_1, \ldots, e_n)$ элемент $(k_1 e_1, \ldots, k_n e_n) \in \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle$. Легко проверить, что это изоморфизм.

Предложение 1. *Подгруппа L свободной абелевой группы F ранга n – это свободная абелева группа ранга $m \leq n$.*

Доказательство. Докажем это утверждение индукцией по n.

База индукции $n = 1$. $F \cong \mathbb{Z}$. Мы знаем, что подгруппа в $\mathbb{Z}$ имеет вид $k\mathbb{Z}$. При $k \neq 0$ это свободная абелева группа ранга 1. Если же $k = 0$ получаем свободную абелеву группу ранга ноль.

Шаг индукции. Пусть для $n < k$ утверждение доказано. Рассмотрим

$$P = \mathcal{A}(e_1, \dots, e_{n-1}) \subset F.$$

Обозначим $B = P \cap L$. Так как P – свободная группа ранга $n - 1$, по предположению индукции $B \subset P$ – свободная абелева группа ранга не более $n - 1$. Если $L \subset P$, то $L = B$ – свободная абелева группа ранга не более $n - 1$. Пусть $L \neq B$. Рассмотрим гомоморфизм $\pi \colon F \to \mathbb{Z}$, $\pi(k_1e_1 + \ldots + k_ne_n) = k_n$. Тогда образ π – циклическая группа и найдется $l \in L$ такой, что $\operatorname{Im} \pi = \langle \pi(l) \rangle$. Пусть $s = t_1e_1 + \ldots t_ne_n \in L$. Тогда $\pi(s) \in \langle \pi(s) \rangle$. То есть $\pi(s) = q\pi(s)$ для некоторого целого q. Получаем $\pi(s - ql) = 0$, то есть $s - ql \in B$. Значит, $s \in B \oplus \langle l \rangle$ (данные две подгруппы пересекаются только по нулю, так как $\pi(l) \neq 0$). Получаем $L = B \oplus \langle l \rangle$ – свободная абелева группа ранга $\operatorname{rk} B + 1 \leq n$. □

Теорема 1 (Универсальное свойство свободной абелевой группы)**.** *Пусть A – абелева группа с образующими $a_1, \dots, a_n$. Тогда существует сюрьективный гомоморфизм*

$$\varphi \colon \mathcal{A}(x_1, \dots, x_n) \to A,$$

причем $\varphi(x_i) = a_i$.

Доказательство. Подходит гомоморфизм определенный по правилу

$$\varphi(k_1x_1 + \ldots + k_nx_n) = k_1a_1 + \ldots + k_na_n.$$

□

Применяя теорему о гомоморфизме, получаем следствие.

Следствие 1. *Каждая конечно порожденная абелева группа изоморфна факторгруппе свободной абелевой группы по некоторой подгруппе (ядру гомоморфизму φ).*

Опишем все базисы данной свободной абелевой группы через один фиксированный базис.

Определение 4. Обозначим через $\mathrm{GL}_n(\mathbb{Z})$ множество целочисленных матриц $n \times n$, обратные к которым также являются целочисленными.

Замечание 2. Множество $\mathrm{GL}_n(\mathbb{Z})$ является группой по умножению матриц. В самом деле, умножение двух целочисленных матриц A и B дает целочисленную матрицу, обратная к которой равна $(AB)^{-1} = B^{-1}A^{-1}$, а значит, целочисленная. Таким образом, $\mathrm{GL}_n(\mathbb{Z})$ замкнуто относительно умножения. Замкнутость относительно взятия обратного элемента очевидна. Также $E \in \mathrm{GL}_n(\mathbb{Z})$. Мы проверили, что $\mathrm{GL}_n(\mathbb{Z})$ – подгруппа в $\mathrm{GL}_n(\mathbb{Q})$.

Лемма 2. *Группа $\mathrm{GL}_n(\mathbb{Z})$ состоит из целочисленных матриц с определителем* ± 1

Доказательство. У целочисленной матрицы целый определитель. Значит, если $A \in \mathrm{GL}_n(\mathbb{Z})$, то $\det A, \det A^{-1} \in \mathbb{Z}$. Но $(\det A)(\det A^{-1}) = 1$. Значит, $\det A = \pm 1$.

Напротив, если для целочисленной матрицы выполнено $\det A = \pm 1$, то применяя формулу через алгебраические дополнения, получаем, что обратная матрица A^{-1} также является целочисленной. □

Предложение 2. *Пусть* $\{e_1, \dots, e_n\}$ *базис свободной абелевой группы* F*. Тогда следующие условия эквивалентны:*

1) $\{e'_1, \dots, e'_n\}$ *– базис* F*;*

2) $(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$*, где* $C \in \mathrm{GL}_n(\mathbb{Z})$*.*

Доказательство. $1 \Rightarrow 2$. Поскольку $\{e_1, \dots, e_n\}$ – базис F, каждый вектор выражается через $\{e_1, \dots, e_n\}$. Значит, $(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C$, где C – некоторая целочисленная матрица $n \times n$. Аналогично $(e_1, \dots, e_n) = (e'_1, \dots, e'_n)D$ для некоторой целочисленной матрицы D. Тогда $(e_1, \dots, e_n) = (e_1, \dots, e_n)CD$. Так как $\{e_1, \dots, e_n\}$ – базис, получаем $CD = E$. Значит, $C \in \mathrm{GL}_n(\mathbb{Z})$.

$2 \Rightarrow 1$. Для любого $f \in F$ выполняется

$$f = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix} \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = \begin{pmatrix} e'_1 & \dots & e'_n \end{pmatrix} C^{-1} \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}.$$

Таким образом любой элемент f выражается через $\{e'_1, \dots, e'_n\}$. Так как матрица C невырожденная, система $\{e'_1, \dots, e'_n\}$ линейно независима над $\mathbb{Z}$. Значит, это базис F. $\square$

Примерами матриц из $\mathrm{GL}_n(\mathbb{Z})$ являются матрицы следующих элементарных преобразований:

1) прибавление одной строки к другой с целым коэффициентом,

2) смена двух строк местами

3) умножение строки на -1.

Таким образом, переходя от базиса $(e_1, \dots, e_n)$ к базису $(e_1, \dots, e_n)C$ мы можем делать данные элементарные преобразования с данным базисом. Назовем данные элементарные преобразования базиса *допустимыми.*

Рассмотрим пару состоящую из свободной абелевой группы $F = \mathcal{A}(x_1, \dots, x_n)$ и ее подгруппы $L = \mathcal{A}(y_1, \dots, y_m)$, $m \le n$. Тогда

$$(y_1, \dots, y_m) = (x_1, \dots, x_n)P,$$

где P – целочисленная матрица размера $n \times m$.

Теорема 2 (Теорема о согласованных базисах)**.** *Существует такой базис* $\{e_1, \dots, e_n\}$ *группы* F *и такие натуральные числа* $u_1, \dots u_m$*, что система* $\{u_1 e_1, \dots, u_m e_m\}$ *является базисом* L*.*

Доказательство. Будем делать элементарные преобразования с базисами группы F и подгруппы L. Пусть $(x'_1, \dots, x'_n) = (x_1, \dots, x_n)C$, $(y'_1, \dots, y'_m) = (y_1, \dots, y_m)D$, тогда равенство $(y_1, \dots, y_m) = (x_1, \dots, x_n)P$ дает $(y'_1, \dots, y'_m) = (x'_1, \dots, x'_n)C^{-1}PD$. При умножении P слева на матрицу C^{-1} и справа на матрицу D происходят допустимые элементарные преобразования со строками и столбцами P. Далее утверждение теоремы следует из следующей леммы.

Лемма 3. *Пусть P – целочисленная матрица $n \times m$. Делая допустимые элементарные преобразования со строками и столбцами P можно привести P к виду*

$$\begin{pmatrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & u_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & 0 & 0 & u_m \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Доказательство леммы. Если не все коэффициенты матрицы равны нулю, то перестановкой строк и столбцов можно поставить на место p_{11} ненулевой элемент с минимальным модулем. Далее будем уменьшать минимальный модуль ненулевого элемента пока это будет возможно.

Случай 1. В первой строке матрицы P есть элемент p_{1i} не делящийся на p_{11}. Поделим p_{1i} на p_{11} с остатком: $p_{1i} = qp_{11} + r$, $0 < |r| < |p_{11}|$. Прибавим первый столбец к i-му с коэффициентом $-q$. На месте p_{1i} получим r. Таким образом мы уменьшили модуль минимального по модулю ненулевого элемента.

Случай 2. В первом столбце матрицы P есть элемент p_{i1} не делящийся на p_{11}. Прибавляя 1-ю строку к i-ой с нужным коэффициентом получаем элемент с модулем меньше $|p_{11}|$ в первом столбце.

Случай 3. Все элементы первой строки и первого столбца делятся на p_{11}. Можно сделать все элементы первой строки и первого столбца нулевыми. Получим матрицу

$$\begin{pmatrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & p_{22} & p_{23} & \dots & p_{2m} \\ 0 & p_{32} & p_{33} & \dots & p_{3m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & p_{n2} & p_{n3} & \dots & p_{nm} \end{pmatrix}$$

Далее работаем аналогичным образом с матрицей без первой строки и первого столбца. При этом элементарные преобразования строк со 2 по n-ю и столбцов со 2-го по m-ый не меняют первые строку и столбец. В итоге получаем нужный вид матрицы. □

□