Теория групп. Лекция 14

Штепин Вадим Владимирович

5 декабря 2019 г.

1 Свободные абелевы группы

Опр. Абелева группа $C_1 \times ... \times C_k$ — **конечнопорожденная**, если $\forall i$ C_i — циклическая (возможно, бесконечного порядка).

В дальнейшем будем считать операцию сложением.

Опр. Пусть G — конечнопорожденная абелева группа. Система элементов $A = \{a_1, ..., a_n\}$ **независима**, если из условия $\sum\limits_i \lambda_i a_i = 0$ следует, что все $\lambda_i = 0$.

Опр. Система элементов $A = \{a_1, ..., a_n\}$ — **базис** в G, если это независимая система и $G = \langle a_1, ..., a_n \rangle$.

Замечание

Если G — конечнопорожденная абелева группа и $e_1, ..., e_n$ — базис, то каждый элемент однозначно раскладывается по базису.

Замечание

Не во всякой конечнопорожденной абелевой группе есть базис.

Пример

$Z_n = Z/nZ$ — конечнопорождена элементом 1, но она не обладает базисом, так как $\forall a \in Z_n$ $na = 0$ и любая система зависима.

Опр. Группа A (абелева, конечнопорожденная) — **свободная абелева группа** ранга n, если в ней существует базис из n элементов.

Утв.

Всякая свободная абелева группа ранга n изоморфна Z^n.

Доказательство

Пусть $e_1, ..., e_n$ — базис A. Тогда каждому элементу $a \in A$ однозначно сопоставляется столбец его координат в базисе. Это соотвествие линейно, а значит это гомоморфизм групп. Биекция следует из однозначности разложения по базису.

Теорема

Любые два базиса свободной абелевой группы равномощны.

Доказательство

Пусть $e_1, ..., e_n$, $f_1, ..., f_k$ — базисы и $k > n$. Тогда $(f_1, ..., f_k) = (e_1, ..., e_n)S$, где S — матрица перехода между базисами (получена разложением f_i по базису $e_1, ..., e_n$). $S \in M_{n\times k}(Z) \subset M_{n\times k}(Q)$.

СЛУ $Sx = 0$ (над Q) из n уравнений с k неизвестными при $n < k$ обязательно имеет нетривиальное решение x_0. Умножая, при необходимости, на НОК всех знаменателей координат, можно считать, что решение целочисленно. Значит, $(f_1, ..., f_k)x_0 = (e_1, ..., e_n)Sx_0 = 0$ и $f_1, ..., f_k$ — не базис.

2 Строение конечнопорожденной абелевой группы

Теорема

Пусть G — конечнопорожденная свободная абелева группа с базисом $e = (e_1, ..., e_n)$. Тогда $f = (f_1, ..., f_n)$ — базис в $G \Leftrightarrow (f_1, ..., f_n) = (e_1, ..., e_n)S$, где S — матрица перехода и $det(S) \in \{1, -1\}$.

Доказательство

1. Необходимость.

   $(e_1, ..., e_n) = (f_1, ..., f_n)T$ — разложение e по базису f, где T — матрица перехода. Тогда $(e_1, ..., e_n) = (e_1, ..., e_n)ST$. В силу единственности разложения, $ST = E$, а все коэффициенты разложения целые. Значит, $S = T^{-1}$ и $det(S) = det(T) \in \{1, -1\}$, так как $det(S)det(T) = 1$ и значения определителей — целые числа.

2. Достаточность. Пусть $f = eS$ и $det(S) \in \{1, -1\}$. Покажем, что f — базис. Очевидно, что существует S^{-1} с целыми коэффициентами, так как $|det(S)| = 1$. Значит, $(e_1, ..., e_n) = (f_1, ..., f_n)S^{-1}$ и $f_1, ..., f_n$ так же порождают G. Покажем независимость $f_1, ..., f_n$. Пусть не так и $(f_1, ..., f_n)\begin{pmatrix}\alpha_1 \\ \cdot \\ \cdot \\ \alpha_n\end{pmatrix} = 0$. Тогда $(e_1, ..., e_n)S\begin{pmatrix}\alpha_1 \\ \cdot \\ \cdot \\ \alpha_n\end{pmatrix} = 0$ и $S\begin{pmatrix}\alpha_1 \\ \cdot \\ \cdot \\ \alpha_n\end{pmatrix} = 0$.

   Но в силу невырожденности S получаем, что $\begin{pmatrix}\alpha_1 \\ \cdot \\ \cdot \\ \alpha_n\end{pmatrix} = 0$.

   Значит, система $f_1, ..., f_n$ независима.

Замечание

Множество целочисленных матриц с определителем из множества $\{1, -1\}$ образуют группу $GL_n(Z)$. В частности, в $GL_n(Z)$ содержатся элементарные матрицы:

1. $E + tE_{i,j},\ i \neq j, t \in Z$ — матрицы, в которых на главной диагонали стоят единицы, и некоторое число вне главной диагонали равно t.

2. $diag(\pm 1, ..., \pm 1)$

3. Единичная матрица, получаемая из диагональной перестановкой двух строк (столбцов, что эквивалентно).

Опр. Рассмотренные матрицы — **целочисленные элементарные матрицы**, а соответствующие им преобразования — **целочисленные элементарные преобразования**.

Теорема (о подгруппах свободной абелевой группы

Пусть G — САГ, $rk(G) = n$, $H \le G$. Тогда H — САГ и $rk(H) \le n$.

В качестве свободных абелевых групп ранга ноль будем рассматривать группы, состоящие только из нейтрального элемента.

Доказательство

Индукция по n.

1. База: если $n = 0$, то $G = H = \{e\}$

2. Переход: пусть для всех групп G, что $rk(G) < n$ верно и $rk(G) = n$, $e_1, ..., e_n$ — базис в G, $H \le G$

   Пусть $G_1 = \langle e_1, ..., e_{n-1} \rangle$. Тогда $rk(G_1) = n-1$ и $H_1 = H \cap G_1$. Очевидно, что $H_1 \le G_1$, и, по предположению индукции, $rk(H_1) \le n-1$. Пусть $h_1, ..., h_k$ — базис в H_1 ($k \le n-1$). Если $H_1 = H$, то утверждение верно.

   Иначе $\exists h \in H \setminus H_1$. Тогда $h = \sum\limits_i e_i\alpha_i$, причем $\alpha_n \neq 0$, так как иначе $h \in H_1$.

   Положим $h_{k+1} \in H \setminus H_1$, такой, что α_n минимально возможно (> 0). Покажем, что $h_1, ..., h_k, h_{k+1}$ — базис H.

   Пусть $x \in H \setminus H_1$ — произвольный. Тогда $x = \sum\limits_i e_i\beta_i$. $\beta_n = q\alpha_n + r$ — деление с остатком.

   Если $r \neq 0$, то $x - qh_{k+1} \in H \setminus H_1$ и его последняя координата в разложении по базису $e_1, ..., e_n$ равна $r > 0$ и $r < \alpha_n$ — получаем противоречие с выбором h_{k+1}. Значит $r = 0$ и $\beta_n = q\alpha_n$. Тогда $x - qh_{k+1} \in H_1$ (так как $r = 0$). Тогда имеет место представление $x = \sum\limits_i \alpha_i h_i + qh_{k+1}$ и $H = \langle h_1, ..., h_{k+1} \rangle$, так как все $x \in H_1$ разлагаются по $h_1, ..., h_k$.

   Покажем независимость $h_1, ..., h_{k+1}$.

   Пусть $\sum_{i=1}^k \gamma_i h_i + \gamma_{k+1}h_{k+1} = 0$. Если $\alpha_{k+1} = 0$, то в силу независимости $h_1, ..., h_k$ получаем, что $\forall i \ \alpha_i = 0$. Если $\alpha_{k+1} \neq 0$, тогда $\sum_{i=1}^{k+1} \gamma_i h_i$ имеет ненулевую последнюю координату в разложении по базису $e_1, ..., e_n$ и не может равняться нулю. Значит, $h_1, ..., h_{k+1}$ — базис H и $k + 1 \le n$.

Замечание

Если $H \le G$ и G, H — САГ одного ранга, то не обязательно $H = G$. Пример: $G = Z$, $H = 2Z$ (обе группы ранга 1).

Замечание

Из того, что элементы независимы не следует, что один из них выражается через остальные. Пример: $2a + 5b + 7c = 0$, но ни один из a, b, c невыразим через другие, так как нельзя делить.

Лемма (о смитовой нормальной форме)

Пусть $M \in M_{n\times k}(Z)$ и ненулевая. Тогда $\exists P, D, Q :\ M = PDQ$ и $P \in GL_n(Z)$, $Q \in GL_k(Z)$, а $D \in M_{n\times k}(Z)$ такая диагональная матрица, что $D_{1,1} \ge 0$, $D_{i,i} | D_{i+1,i+1}$ и, начиная с некоторого i все $D_{i,i} = 0$.

Доказательство

Индукция по n

1. База: $(a, b) \to$ (НОД$(a, b), 0)$ можно привести алгоритмом Эвклида. Аналогично, $(a_1, ..., a_k) \to$ (НОД$(a_1, ..., a_k), 0, ..., 0)$ можно привести применением $k-1$ раз алгоритма Эвклида, так как НОД$(a_1, ..., a_k)$ =НОД(НОД$(a_1, ..., a_{k-1}), a_k)$

2. Переход: пусть утверджение верно для всех матриц M, имеющих меньше n строк. С помощью целочисленных преобразований приведем матрицу к виду, в котором элемент $M_{1,1}$ =НОД$(M_{i,j})$, а остальные элементы первой строки и первого столбца равны нулю.

   Это можно сделать следующим алгоритмом.

   Перенесем минимальный по модулю элемент матрицы в левый верхний угол и начнем зануляnть первую строку и первый столбец. Если в процессе появится элемент, меньший по модулю, то перенесем его в угол и продолжим.

   Если после этого в матрице есть элемент, не делящийся на $M_{1,1}$, то прибавим строку, в которой он находится к первой и продолжим процесс, тем самым получив в углу НОД$(M_{1,1}, *, ..., *)$ — НОД элемента в углу и i-той строки, меньший, чем $M_{1,1}$. В итоге получим, что все элементы матрицы, получаемой вычеркиванием первой строки и первого столбца делятся на $M_{1,1}$. Приведем ее к смитовой нормальной форме по индукции.

   Так как мы делали элементарные преобразования строк и столбцов, то $D = P_1 M Q_1$, $P_1 \in GL_n(Z),\ Q \in GL_k(Z)$ и $M = P_1^{-1} D Q_1^{-1}$

Замечание

Смитова нормальная форма определена однозначно. Матрицы P, Q определены неоднозначно.

Упражнение

$u_1 ... u_t$ =НОД$(M_1, ..., M_t)$ — однозначно определены, где M_i — миноры. В частности, u_1 =НОД(M_1) =НОД$(M$

Теорема (о существовании согласованных базисов в САГ G и $H \le G$)

Пусть G — САГ ранга n, $H \le G$ ранга $k \le n$. Тогда в G и H существуют базисы $g_1, ..., g_n$ и $h_1, ..., h_k$, что $h_i = u_i g_i$, где $u_i \in N$ и $u_1 | u_2 | ... | u_k$

Доказательство

Пусть $e_1, ... e_n$ — базис в G, $f_1, ..., f_k$ — базис в H и оба базиса произвольны. Тогда $(f_1, ..., f_k) = (e_1, ..., e_n)M$, $M \in M_{n \times k}(Z)$. По лемме, $M = PDQ$, где D — матрица в смитовой нормальной форме.

Тогда $(f_1, ..., f_k) = (e_1, ..., e_n)PDQ$ и $(f_1, ..., f_k)Q^{-1} = (e_1, ..., e_n)PD$. Обозначим $(h_1, ..., h_k) = (f_1, ..., f_k)Q^{-1}$ и $(g_1, ..., g_n) = (e_1, ..., e_n)P$ и получим требуемое.

Следствие (о существовании разложения конечнопорожденной абелевой группы в прямую сумму циклических

Пусть A — конечнопорожденная абелева группа. Тогда $A \simeq Z_{u_1} \oplus Z_{u_2} \oplus ... \oplus Z_{u_k} \oplus Z^l$, где $u_1 | u_2 | ... | u_k$, $u_1 > 1$, $l \in N$ (возможно нулевое).

Доказательство

Пусть $a_1, ..., a_n$ — порождает A, G — САГ порядка n с базисом $e_1, ..., e_n$. Тогда существует сюръективный гомоморфизм $\phi : G \to A,\ \phi(e_i) = a_i$. Пусть $H = ker(\phi) \le G$.

Выберем в G и H согласованные базисы $g_1, ..., g_n$ и $h_1, ..., h_k$, что $h_i = u_i g_i$. По теореме о гомоморфизме и в силу сюръективности $A \simeq G/H$.

$G = \langle g_1 \rangle \oplus ... \oplus \langle g_n \rangle$ по определению базиса. Тогда $H = \langle u_1 g_1 \rangle \oplus ... \oplus \langle u_k g_k \rangle$.

$A \simeq G/H \simeq \langle g_1\rangle/\langle u_1 g_1\rangle \oplus ... \oplus \langle g_k\rangle/\langle u_k g_k\rangle \oplus Z^{n-k} \simeq Z_{u_1} \oplus Z_{u_2} \oplus ... \oplus Z_{u_k} \oplus Z^l$. Заметим, что все $u_i = 1$ можно не учитывать, так как $Z_1 = \{e\}$

Опр. **Примарная циклическая группа (соответсвующая простому числу p)** — Z_{p^k}, где p — простое.

Утв. (о разложении конечной циклической группы в прямую сумму примарных циклических

Любая конечная группа раскладывается в прямую сумму примарных циклических

Пусть $n = p_1^{\alpha_1}...p_s^{\alpha_s}$ — каноническое разложение на простые множители. Тогда $Z_n = Z_{p_1^{\alpha_1}} \oplus ... \oplus Z_{p_s^{\alpha_s}}$.

Доказательство

Пусть $\phi : Z_n \to \oplus Z_{p_i^{\alpha_i}}$ — гомоморфизм в прямую сумму примарных циклических групп (действующий на смежные классы $Z/nZ \simeq Z_n$).

$\phi(a + nZ) = (a + p_1^{\alpha_1} Z, ..., a + p_s^{\alpha_s} Z)$.

$a + nZ \in ker(\phi) \Leftrightarrow a \vdots p_1^{\alpha_1}...p_s^{\alpha_s} \Leftrightarrow a + nZ = nZ \Leftrightarrow a = 0$.

Значит, ядро тривиально и гомоморфизм инъективен, но $|Z_n| = n = |\oplus Z_{p_i^{\alpha_i}}|$ и гомоморфизм сюръективен, а значит это изоморфизм.

Замечание

Группы Z_{p^k} и Z неразложимы.

Доказательство

В Z_{p^k} есть единственная подгруппа H порядка p и она циклическая. Любая другая подгруппа в Z_{p^k} примарна и так же содержит H, а значит разложения быть не может.

Пусть $Z = H_1 \oplus H_2$ — разложение в циклические группы, то есть $H_1 = \langle n\rangle,\ H_2 = \langle m\rangle$. Тогда $\langle nm\rangle \subset H_1 \cap H_2$ и пересечение нетривиально

Замечание

Доказанные теоремы дополняет теорема о единственности разложения: конечные группы в разложении определены однозначно, степень l так же определена однозначно.

Разложение конечной конечнопорожденной абелевой группы единственно с точностью до порядка примарных групп в разложении.