Math-Net.Ru

Общероссийский математический портал

Вик. С. Куликов, Разложения на множители в конечных группах, *Матем. сб.*, 2013, том 204, номер 2, 87–116

DOI: <https://doi.org/10.4213/sm7919>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.164.48.24

26 апреля 2023 г., 13:30:39

УДК 512.53+512.544+512.772.5

Вик. С. Куликов

Разложения на множители в конечных группах

Дано необходимое условие для однозначности разложений на множители элементов конечной группы G с множителями, принадлежащими объединению некоторых классов сопряженности элементов группы G . Это условие является достаточным, если число множителей, принадлежащих каждому классу сопряженности, является достаточно большим. Этот результат затем применяется к проблеме о числе неприводимых компонент пространства Гурвица отмеченных накрытий степени d проективной прямой $\mathbb{P}^1$ с заданной группой Галуа G накрытий и фиксированным набором локальных монодромий.

Библиография: 9 названий.

Ключевые слова: полугруппы разложений на множители, неприводимые компоненты пространства Гурвица накрытий проективной прямой.

DOI: 10.4213/sm7919

Введение

Пусть $f: X \rightarrow \mathbb{P}^1$ – морфизм неособой неприводимой проективной кривой X (определенной над полем комплексных чисел $\mathbb{C}$) на проективную прямую $\mathbb{P}^1$. Обозначим через $\mathbb{C}(X)$ поле рациональных функций на кривой X . Морфизм f определяет конечное расширение $f^*: \mathbb{C}(z) \hookrightarrow \mathbb{C}(X)$ поля рациональных функций $\mathbb{C}(\mathbb{P}^1) \simeq \mathbb{C}(z)$. Обозначим через G группу Галуа этого расширения.

Выберем точку $z_0 \in \mathbb{P}^1$ такую, что z_0 не является точкой ветвления морфизма f , перенумеруем точки множества $f^{-1}(z_0) = \{w_1, \dots, w_d\}$, где $d = \deg f$, и будем называть морфизм f с фиксированной нумерацией точек из $f^{-1}(z_0)$ *отмеченным накрытием*.

Пусть $z_1, \dots, z_n \in \mathbb{P}^1$ – множество точек ветвления накрытия f . Нумерация точек из $f^{-1}(z_0)$ определяет гомоморфизм $f_*: \pi_1(\mathbb{P}^1 \setminus \{z_1, \dots, z_n\}, z_0) \rightarrow \Sigma_d$ из фундаментальной группы $\pi_1 = \pi_1(\mathbb{P}^1 \setminus \{z_1, \dots, z_n\}, z_0)$ в симметрическую группу Σ_d . Образ $\text{im } f_*$ действует транзитивно на $f^{-1}(z_0)$ и изоморфен группе G (поэтому мы отождествляем группы $\text{im } f_*$ и G). Пусть $\gamma_1, \dots, \gamma_n$ – простые петли вокруг соответственно точек $z_1, \dots, z_n$, начинающиеся и заканчивающиеся в точке z_0 , такие, что они порождают группу π_1 . Образ $g_j = f_*(\gamma_j) \in G$ называется *локальной монодромией накрытия f в точке z_j* . Отметим, что множество $\{g_1, \dots, g_n\}$ локальных монодромий порождает группу G . Каждая локальная монодромия g_j зависит от выбора петель γ_j , поэтому она определена однозначно с точностью до сопряжения в группе G . Обозначим через

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант № 11-01-00185) и Программы Президента РФ поддержки ведущих научных школ (грант № НШ-4713.2010.1), а также при поддержке лаборатории алгебраической геометрии ГУ-ВШЭ по гранту Правительства РФ (договор № 11.G34.31.0023).

$O = C_1 \sqcup \dots \sqcup C_m \subset G$ объединение классов сопряженности всех локальных монодромий и через τ_i число локальных монодромий накрытия f , принадлежащих классу сопряженности C_i . Пара (G, O) называется *оснащенной группой*, а набор $\tau = (\tau_1 C_1, \dots, \tau_m C_m)$ – *типом монодромии* накрытия f .

Пусть $\text{HUR}_{d,G,\tau}^m(\mathbb{P}^1)$ – пространство Гурвица (см. определение пространств Гурвица в [1]) отмеченных накрытий проективной прямой $\mathbb{P}^1$ степени d с группой Галуа G и типом монодромии τ . Знаменитая теорема Клебша–Гурвица (см. [2], [3]) гласит, что если $G = \Sigma_d$ и O – множество транспозиций, то пространство $\text{HUR}_{d,\Sigma_d,\tau}^m(\mathbb{P}^1)$ состоит из единственной неприводимой компоненты в случае $\tau = (nO)$ с четным $n \geq 2(d-1)$ и пусто во всех других случаях. Некоторые обобщения теоремы Клебша–Гурвица были получены в [4] и [5]. В частности, в [5] было доказано, что для оснащенной группы (Σ_d, O) с $O = C_1 \sqcup \dots \sqcup C_m$, где C_1 – это класс сопряженности нечетной перестановки, оставляющей неподвижными по крайней мере два элемента, пространство Гурвица $\text{HUR}_{d,\Sigma_d,\tau}^m(\mathbb{P}^1)$ неприводимо, если τ_1 является достаточно большим числом. С другой стороны, пример в [6] показывает, что $\text{HUR}_{8,\Sigma_8,\tau}^m(\mathbb{P}^1)$ состоит по крайней мере из двух неприводимых компонент, где $\tau = (1C_1, 1C_2, 1C_3)$ и C_1 – класс сопряженности перестановки $(1, 2)(3, 4, 5)$, C_2 – класс сопряженности перестановки $(1, 2, 3)(4, 5, 6, 7)$ и C_3 – класс сопряженности перестановки $(1, 2, 3, 4, 5, 6, 7)$. Поэтому мы не можем ожидать, что для фиксированной оснащенной группы (G, O) число неприводимых компонент пространства $\text{HUR}_{d,G,\tau}^m(\mathbb{P}^1)$ не зависит от типа монодромии τ . Однако можно ожидать, что это число не зависит от τ , если τ_i при некотором i является достаточно большим числом и таким, что элементы из класса сопряженности C_i порождают группу G .

В п. 2.5 для каждой оснащенной конечной группы (G, O) такой, что элементы из O порождают группу G , определяется *индекс неоднозначности* $a_{(G,O)}$, зависящий от G и O . Следующая теорема является прямым следствием из теорем 6, 7 (см. п. 4.2) и результатов статьи [4].

ТЕОРЕМА 1. *Для каждой оснащенной конечной группы (G, O) , $O = C_1 \sqcup \dots \sqcup C_m$, такой, что элементы из O порождают группу G , существует константа T такая, что число неприводимых компонент каждого непустого пространства Гурвица $\text{HUR}_{d,G,\tau}^m(\mathbb{P}^1)$ равно $a_{(G,O)}$, если $\tau_i \geq T$ для всех $i = 1, \dots, m$.*

Если элементы, принадлежащие множеству $O_1 = C_1 \sqcup \dots \sqcup C_k$ при некотором $k < m$, порождают группу G , то существует константа T_1 такая, что число неприводимых компонент пространства $\text{HUR}_{d,G,\tau}^m(\mathbb{P}^1)$ не превосходит $a_{(G,O_1)}$, если $\tau_i \geq T_1$ для $i = 1, \dots, k$.

Настоящая работа является продолжением статьи [4], в которой было начато исследование полугрупп разложений на множители в конечных группах. Для удобства читателей в § 1 напоминаются основные определения и полезные утверждения из статьи [4]. В § 2 каждой оснащенной группе (G, O) сопоставляется C -группа, чья полугруппа разложений на множители совпадает с полугруппой разложений на множители оснащенной группы (G, O) , и исследуется связь между этой C -группой и (G, O) . В § 3 мы доказываем стабильность полугрупп разложений на множители над C -конечными группами. Теорема 2, доказанная в этом параграфе, играет ключевую роль в доказательстве всех

основных результатов этой статьи (см. § 4). В § 5 решается проблема слов для C -конечных групп и приведен алгоритм вычисления индексов неоднозначности $a_{(G,O)}$ для оснащенных конечных групп (G, O) .

Автор благодарен О. В. Куликовой, обратившей внимание автора на важную роль леммы ван Кампена в геометрической теории групп, только благодаря этой лемме стало возможным доказать теорему 2.

§ 1. Полугруппы над группами

1.1. Полугруппы разложений на множители. Пусть $O \subset G$ – инвариантное относительно действия внутренними автоморфизмами подмножество группы G . Назовем пару (G, O) *оснащенной группой*. В дальнейшем мы будем предполагать, что $1 \notin O$, множество O состоит из конечного числа классов сопряженности C_i группы G , $O = C_1 \sqcup \dots \sqcup C_m$, и, кроме того, зафиксируем нумерацию этих классов сопряженности.

Гомоморфизм $f: G_1 \rightarrow G_2$ является *гомоморфизмом оснащенных групп* (G_1, O_1) и (G_2, O_2) , если $f(O_1) \subset O_2$.

Полугруппа $S(G, O)$, порожденная элементами алфавита $X = X_O = \{x_g \mid g \in O\}$, которые связаны следующим соотношением:

$$x_{g_1} \cdot x_{g_2} = x_{g_2} \cdot x_{g_2^{-1}g_1g_2} = x_{g_1g_2g_1^{-1}} \cdot x_{g_1}, \quad (1)$$

называется *полугруппой разложений на множители с множителями из O* (или *полугруппой разложений на множители над группой G*). Гомоморфизм

$$\alpha = \alpha_G: S(G, O) \rightarrow G,$$

заданный формулой $\alpha(x_g) = g$ для каждого $x_g \in X$, называется *гомоморфизмом произведения*. Обозначим через $g_1 \dots g_n$ образ $\alpha(x_{g_1} \dots x_{g_n})$ элемента $s = x_{g_1} \dots x_{g_n} \in S(G, O)$.

Действие ρ группы G на множестве X , заданное формулой

$$x_a \in X \mapsto \rho(g)(x_a) = x_{gag^{-1}} \in X,$$

определяет гомоморфизм $\rho: G \rightarrow \text{Aut}(S(G, O))$. Действие $\rho(g)$ на полугруппе $S(G, O)$ называется *сопряжением посредством элемента $g \in G$* . Положим $\lambda(g) = \rho(g^{-1})$ и $\lambda_S = \lambda \circ \alpha$, $\rho_S = \rho \circ \alpha$.

УТВЕРЖДЕНИЕ 1 (см. [4]). Для всех $s_1, s_2 \in S(G, O)$ имеем

$$s_1 \cdot s_2 = s_2 \cdot \lambda_S(s_2)(s_1) = \rho_S(s_1)(s_2) \cdot s_1.$$

Каждому элементу $s = x_{g_1} \dots x_{g_n} \in S(G, O)$ сопоставляется положительное целое число $\ln(s) = n$ – *длина* элемента s . Легко видеть, что $\ln: S(G, O) \rightarrow \mathbb{Z}_{\geq 0} = \{\mathbf{a} \in \mathbb{Z} \mid \mathbf{a} \geq 0\}$ является гомоморфизмом полугрупп.

Каждому элементу $s = x_{g_1} \dots x_{g_n} \in S(G, O)$ сопоставим подгруппу G_s группы G , порожденную образами $\alpha(x_{g_1}) = g_1, \dots, \alpha(x_{g_n}) = g_n$ множителей $x_{g_1}, \dots, x_{g_n}$, и обозначим через G_O подгруппу группы G , порожденную элементами из O .

УТВЕРЖДЕНИЕ 2 (см. [4]). Подгруппа G_s группы G корректно определена, т.е. она не зависит от представления элемента s в виде произведения порождающих элементов $x_{g_i} \in X_O$.

Для подгрупп H и Z группы G положим

$$S(G, O)^H = \{s \in S(G, O) \mid G_s = H\}, \quad S(G, O)_Z = \{s \in S(G, O) \mid \alpha(s) \in Z\}, \\ S(G, O)_Z^H = S(G, O)_Z \cap S(G, O)^H.$$

Легко видеть, что $S(G, O)^H$ (соответственно $S(G, O)_Z^H$) изоморфна полугруппе $S(H, H \cap O)^H$ (соответственно полугруппе $S(H, H \cap O)_Z^H$) и этот изоморфизм индуцирован вложением $(H, H \cap O) \hookrightarrow (G, O)$.

ПРЕДЛОЖЕНИЕ 1 (см. [4]). Пусть (G, O) – оснащенная группа и пусть $s \in S(G, O)$. Имеем:

- (1) $\ker \rho$ совпадает с централизатором C_O группы G_O в группе G ;
- (2) если $\alpha(s)$ принадлежит центру $Z(G_s)$ группы G_s , то для каждого $g \in G_s$ действие $\rho(g)$ оставляет неподвижным элемент $s \in S(G, O)$;
- (3) если $\alpha(s \cdot x_g)$ принадлежит центру $Z(G_{s \cdot x_g})$ группы $G_{s \cdot x_g}$, то $s \cdot x_g = x_g \cdot s$;
- (4) если $\alpha(s) = 1$, то $s \cdot s' = s' \cdot s$ для любого элемента $s' \in S(G, O)$.

УТВЕРЖДЕНИЕ 3 (см. [4]). Для оснащенной группы (G, O) полугруппа $S(G, O)_1$ содержится в центре полугруппы $S(G, O)$ и, в частности, является коммутативной полугруппой.

Легко видеть, что если порядок элемента $g \in O$ равен n , то $x_g^n \in S(G, O)_1$.

ЛЕММА 1 (см. [4]). Пусть $s \in S(G, O)_{Z(G_O)}$ и элемент $s_1 \in S(G, O)$ таков, что $G_{s_1} = G_O$, где $Z(G_O)$ – центр группы G_O . Тогда

$$s \cdot s_1 = \rho(g)(s) \cdot s_1 \quad (2)$$

для каждого $g \in G_O$.

В частности, если элемент $s \in S(G, O)$ таков, что $G_s = G$, и $C \subset O$ – класс сопряженности группы G , то для любых $g_1, g_2 \in C$ имеем

$$x_{g_1}^n \cdot s = x_{g_2}^n \cdot s, \quad (3)$$

если элемент g_1^n принадлежит центру $Z(G)$ группы G .

ПРЕДЛОЖЕНИЕ 2 (см. [4]). Элементы полугруппы $S(G, O)_1^G$ являются неподвижными при действии группы G сопряжениями.

§ 2. C -группы и C -графы

2.1. C -графы C -групп. Напомним определение C -групп. По определению (см., например, [7]) C -группа G – это оснащенная группа (G, O) такая, что элементы из O являются порождающими элементами (так называемые, C -порождающие) группы G , которые связаны следующими соотношениями:

$$g_i^{-1} g_j g_i = g_k, \quad (g_i, g_j, g_k) \in M, \quad (4)$$

где M – некоторое подмножество множества O^3 . Гомоморфизм $f: G_1 \rightarrow G_2$ C -групп называется *C-гоморфизмом*, если он является гомоморфизмом оснащенных групп. В частности, две C -группы G_1 и G_2 *C-изоморфны*, если они изоморфны как оснащенные группы.

Сопоставим каждой C -группе направленный граф, называемый *C-графом*. Чтобы дать определение C -графов, рассмотрим направленный граф $\Gamma = (V, E)$, где V – множество вершин графа Γ и множество ребер E – это набор $\{e_{v_i, v_j} = (v_i, v_j)\}$ упорядоченных пар его вершин (некоторые из ребер могут быть петлями, т.е. допускается равенство $v_i = v_j$). Для каждой вершины $v \in V$ обозначим через $T_v = \{e_{v, v_i}\}$ (соответственно через $H_v = \{e_{v_i, v}\}$) множество ребер, чьи начала (соответственно концы) – это вершина v . Направленный граф Γ называется *C-графом*, если каждое ребро $e \in E$ помечено некоторым элементом из V (т.е. фиксировано отображение $f: E \rightarrow V$ такое, что метка ребра $e \in E$ – это $f(e) \in V$; в дальнейшем ребро e_{v_1, v_2} с меткой $f(e_{v_1, v_2}) = v$ будет обозначаться через $e_{v_1, v_2, v}$) и, кроме того, Γ удовлетворяет следующим пяти условиям.

- (i) Для каждой вершины $v \in V$ ограничения $f|_{T_v}, f|_{H_v}$ отображения f на T_v и H_v являются взаимно однозначными соответствиями с V .
- (ii) Для каждой вершины v конец v_1 ребра $e_{v, v_1, v}$ – это вершина v , т.е. ребро $e_{v, v_1, v}$ является петлей ($v_1 = v$).

Отметим, что согласно условию (i) начало (соответственно конец) v_1 и метка v_2 определяют однозначно ребро e , чье начало (соответственно конец) есть v_1 и чья метка есть v_2 . Поэтому последовательность $v_1, \dots, v_n$ и начало v_0 определяют однозначно путь $l(v_0; v_1, \dots, v_n)$ вдоль ребер с метками $v_1, \dots, v_n$ (в положительном направлении), начинающийся в вершине v_0 .

- (iii) Если для некоторых двух вершин v_1 и v_2 ребро e_{v_1, v_3, v_2} является петлей, т.е. $v_1 = v_3$, то ребро e_{v_2, v_4, v_1} также является петлей ($v_2 = v_4$).
- (iv) Для любого ребра e_{v_1, v_2, v_3} и для любой вершины v пути $l(v; v_1, v_3)$ и $l(v; v_3, v_2)$ имеют один и тот же конец.

Сопоставим каждому направленному графу Γ с метками двумерный комплекс K_Γ , чей одномерный остов – это Γ , а его двумерные клетки – четырехугольники $Q_{(v, e_{v_1, v_2, v_3})}$, находящиеся во взаимно однозначном соответствии с парами $(v, e_{v_1, v_2, v_3}) \in V \times E$, такие, что граница $\partial Q_{(v, e_{v_1, v_2, v_3})}$ четырехугольника $Q_{(v, e_{v_1, v_2, v_3})}$ – это петля $l(v; v_1, v_3) \cdot l(v; v_3, v_2)^{-1}$.

Пятое условие состоит в следующем:

- (v) если для некоторых двух ребер e_{v, v_1, v_2} и e_{v, v_1, v_3} петля $e_{v, v_1, v_2} \cdot e_{v, v_1, v_3}^{-1}$ представляет единицу фундаментальной группы $\pi_1(K_\Gamma, v)$, то $v_2 = v_3$.

Каждой C -группе (G, O) можно сопоставить C -граф. По определению C -граф $\Gamma = \Gamma_{(G, O)}$ C -группы (G, O) – это C -граф, чье множество вершин $V = \{v_{g_i} \mid g_i \in O\}$ находится во взаимно однозначном соответствии с множеством O . Две вершины v_{g_1} и v_{g_2} , $g_1, g_2 \in O$, соединены отмеченным ребром $e_{v_{g_1}, v_{g_2}, v_g}$ тогда и только тогда, когда в G имеет место соотношение $g^{-1}g_1g = g_2$ с некоторым элементом $g \in O$.

Обратно, каждому C -графу Γ можно сопоставить C -группу $G_\Gamma = (G, Y)$, множество $Y = \{y_{v_i} \mid v_i \in V\}$ C -порождающих элементов которой находится во взаимно однозначном соответствии с множеством V вершин графа Γ . В группе G_Γ имеет место соотношение $y_{v_3}^{-1}y_{v_1}y_{v_3} = y_{v_2}$ тогда и только тогда, когда в графе Γ имеется ребро e_{v_1, v_2, v_3} .

УТВЕРЖДЕНИЕ 4. Для каждого C -графа Γ C -группа G_Γ C -изоморфна C -группе G_{G_Γ} .

C -графы Γ_G и Γ_{G_Γ} изоморфны для каждой C -группы G .

Доказательство этого утверждения очевидно.

В дальнейшем для C -группы G_Γ порождающие элементы x_{y_v} , $v \in \Gamma$, полугруппы $S(G_\Gamma, Y)$ будем обозначать через x_v .

Скажем, что подграф Γ_1 C -графа Γ является C -подграфом, если Γ_1 также является C -графом.

Пусть Γ_1 является C -подграфом C -графа Γ . Рассмотрим C -группы $(G, Y) = G_\Gamma$ и $(G_1, Y_1) = G_{\Gamma_1}$ и их полугруппы разложений на множители $S(G, Y)$ и $S(G_1, Y_1)$. Вложение $i: \Gamma_1 \hookrightarrow \Gamma$ определяет естественный гомоморфизм C -групп $i_*: G_{\Gamma_1} \rightarrow G_\Gamma$ и гомоморфизм $i_*: S(G_1, Y_1) \rightarrow S(G, Y)$ их полугрупп разложений на множители, заданных соответственно формулами $i_*(y_{v_i}) = y_{v_i}$ и $i_*(x_{v_i}) = x_{v_i}$ для $v_i \in \Gamma_1 \hookrightarrow \Gamma$.

УТВЕРЖДЕНИЕ 5. Пусть Γ_1 является C -подграфом C -графа Γ . Тогда гомоморфизм $i_*: S(G_{\Gamma_1}, Y_1) \rightarrow S(G_\Gamma, Y)$ является вложением.

Доказательство этого утверждения очевидно.

Для каждого C -графа Γ определен гомоморфизм из C -группы G_Γ в группу автоморфизмов графа Γ : действие C -порождающего элемента $y_{v'}$ на вершине $v \in \Gamma$ задано следующим правилом: ее образ $y_{v'}(v)$ – это конец ребра с началом в вершине v и меткой v' , а для ребра e_{v_1, v_2, v_3} образ – это $y_{v'}(e_{v_1, v_2, v_3}) = e_{y_{v'}(v_1), y_{v'}(v_2), y_{v'}(v_3)}$. Из условий (i)–(v) в определении C -графов следует, что это действие корректно определено.

В дальнейшем мы будем рассматривать только конечно порожденные C -группы (как обычные группы без оснащения) и C -графы, состоящие из конечного числа компонент связности. Обозначим через m число связных компонент C -графа Γ . Легко видеть, что $G_\Gamma/[G_\Gamma, G_\Gamma] \simeq \mathbb{Z}^m$ и что любые два C -порождающих элемента y_{v_1} и y_{v_2} сопряжены в C -группе G_Γ тогда и только тогда, когда вершины v_1 и v_2 принадлежат одной и той же компоненте связности графа Γ , т.е. множество Y C -порождающих элементов C -группы G_Γ – это объединение m классов сопряженности группы G_Γ . Обозначим через $\text{ab}: G_\Gamma \rightarrow H_1(G_\Gamma, \mathbb{Z}) = G_\Gamma/[G_\Gamma, G_\Gamma]$ естественный эпиморфизм. Ниже будем предполагать, что фиксирована некоторая нумерация связных компонент графа Γ . В этом случае группа $H_1(G_\Gamma, \mathbb{Z}) \simeq \mathbb{Z}^m$ имеет естественный базис, состоящий из векторов $\text{ab}(y_v) = (0, \dots, 0, 1, 0, \dots, 0)$, где 1 стоит на i -м месте, если v принадлежит i -ой компоненте связности графа Γ . Обозначим композицию $\text{ab} \circ \alpha_{G_\Gamma}$ через τ .

Пусть $l = l(v_0; v_1, \dots, v_n)$ – путь в C -графе Γ . Число n называется длиной пути l . Наименьшее положительное целое число p_v (возможно, $p_v = \infty$) такое, что для любой вершины v_i графа Γ путь $l(v_i; v, \dots, v)$ длины p_v является петлей с началом и концом в вершине v_i , называется периодом вершины v . Легко видеть, что $p_v = \min\{p \in \mathbb{N} \mid y_v^p \in Z(G_\Gamma)\}$, где $Z(G_\Gamma)$ – центр группы G_Γ .

УТВЕРЖДЕНИЕ 6. Если вершины v_1 и v_2 принадлежат одной и той же компоненте связности C -графа Γ , то $p_{v_1} = p_{v_2}$.

ДОКАЗАТЕЛЬСТВО. Элементы y_{v_1} и y_{v_2} сопряжены в G_Γ . Следовательно, если $y_{v_1}^{p_{v_1}} \in Z(G_\Gamma)$, то $y_{v_2}^{p_{v_1}} = y_{v_1}^{p_{v_1}}$, и поэтому $y_{v_2}^{p_{v_1}} \in Z(G_\Gamma)$.

УТВЕРЖДЕНИЕ 7. Если вершина v_1 C -графа Γ такова, что ее период $p_{v_1} = 1$, то C -группа G_Γ естественным образом изоморфна прямому произведению $G_{\Gamma_1} \times \mathbb{F}_1$, где $\mathbb{F}_1$ – свободная группа, порожденная элементом y_{v_1} , а C -группа G_{Γ_1} порождена всеми C -порождающими элементами y_v , где $v \neq v_1$, и она связана с C -графом Γ_1 , полученным из Γ в результате удаления вершины v_1 и всех ребер с меткой v_1 .

Доказательство этого утверждения очевидно.

C -группа G_Γ называется C -конечной группой, если C -граф Γ является конечным графом.

Пусть $\Gamma = \Gamma_1 \sqcup \dots \sqcup \Gamma_m$ – разложение в несвязное объединение связных компонент конечного C -графа Γ и пусть p_i – период множества $V_i = \{v_{i,1}, \dots, v_{i,n_i}\}$ вершин связной компоненты Γ_i . Элемент

$$c = \prod_{i=1}^m \prod_{j=1}^{n_i} y_{v_{i,j}}^{p_i}$$

называется каноническим элементом C -группы G_Γ .

ПРЕДЛОЖЕНИЕ 3. Пусть G_Γ – C -конечная группа. Тогда коммутатор $[G_\Gamma, G_\Gamma]$ является конечной группой. Более того, каждый элемент $g \in [G_\Gamma, G_\Gamma]$ может быть записан в виде

$$g = c^{-1} \prod_{i=1}^m y_{i,1}^{k_i p_i} y_{i,1}^{a_{i,1}} y_{i,2}^{a_{i,2}} \dots y_{i,n_i}^{a_{i,n_i}}, \quad (5)$$

где c – канонический элемент группы G_Γ и целые числа k_i и $a_{i,j}$ удовлетворяют следующим соотношениям и неравенствам:

$$\sum_{j=1}^{n_i} a_{i,j} + k_i p_i = n_i p_i, \quad (6)$$

$$0 < a_{i,j} \leq p_i, \quad 0 \leq k_i < n_i. \quad (7)$$

ДОКАЗАТЕЛЬСТВО. Ввиду соотношений (4) и так как $y_{i,j}^{p_i} = y_{i,1}^{p_i}$, каждый элемент $g \in [G, G]$ может быть записан в виде

$$g = \prod_{i=1}^m y_{i,1}^{k_i p_i} y_{i,1}^{b_{i,1}} y_{i,2}^{b_{i,2}} \dots y_{i,n_i}^{b_{i,n_i}}, \quad (8)$$

где целые числа k_i и $b_{i,j}$ удовлетворяют следующим соотношениям и неравенствам:

$$\sum_{j=1}^{n_i} b_{i,j} + k_i p_i = 0, \quad (9)$$

$$|b_{i,j}| \leq p_i - 1, \quad |k_i| < n_i. \quad (10)$$

Для фиксированных целых чисел p_i и n_i множество целых решений уравнений (9) при ограничениях (10) является конечным. Следовательно, $[G_\Gamma, G_\Gamma]$ является конечной группой. Чтобы получить представление (5) из (8), достаточно умножить g в представлении (8) на $c^{-1}c$ и еще раз использовать соотношения $y_{i,j}^{p_i} = y_{i,1}^{p_i}$.

2.2. Канонические элементы полугрупп разложений на множители. В обозначениях, использованных выше, элемент

$$s_{\Gamma'} = \prod_{l=1}^k \prod_{j=1}^{n_{i_l}} x_{v_{i_l,j}}^{p_{i_l}} \in S(G, Y)$$

корректно определен и называется *каноническим элементом*, ассоциированным с подграфом $\Gamma' = \Gamma_{i_1} \sqcup \dots \sqcup \Gamma_{i_k}$ C -графа Γ . Если $\Gamma' = \Gamma$, то элемент s_{Γ} называется *каноническим элементом* полугруппы $S(G, Y)$. Очевидно, элемент $s_{\Gamma'}$ принадлежит центру полугруппы $S(G, Y)$, так как каждый его множитель $x_{v_{i_l,j}}^{p_{i_l}}$ принадлежит центру полугруппы $S(G, Y)$.

Скажем, что элемент $s_1 \in S(G, Y)$ является *делителем* элемента $s \in S(G, Y)$, если существует такой элемент $s_2 \in S(G, Y)$, что $s = s_1 \cdot s_2$.

ЛЕММА 2. *Элемент $s \in S(G, Y)$ длины $\ln(s) \leq k$ является делителем элемента $s_{\Gamma'}^k$, если s может быть представлен словом, состоящим из порождающих элементов $x_{v_{i,j}}$, где $v_{i,j} \in \Gamma'$.*

Доказательство леммы 2 очевидно.

ЛЕММА 3. *Пусть $G_{\Gamma} = (G, Y)$ – C -конечная группа и пусть для элемента $s = s' \cdot s'' \in S(G, Y)^G$ i -я координата $\tau_i(s)$ элемента $\tau(s)$ не меньше чем $n_i p_i + 1$. Предположим, что $\tau_i(s'') = 0$. Тогда для $1 \leq j \leq n_i$ элемент s может быть записан в виде $s = x_{v_{i,j}}^{p_i} \cdot s_i \cdot s''$, где $s_i \cdot s'' \in S(G, Y)^G$.*

ДОКАЗАТЕЛЬСТВО. Так как $\tau_i(s) \geq n_i p_i + 1$, то для данного i найдется по крайней мере $p_i + 1$ множителей $x_{v_{i,j}}$ в разложении на множители элемента s' , $s' = x_{v_{i_1,j_1}} \dots x_{v_{i_k,j_k}}$, имеющих одинаковый индекс j . Применяя соотношения (1), мы можем передвинуть их влево и после этого получить новое разложение на множители: $s' = x_{v_{i,j}}^{p_i} \cdot (x_{v_{i,j}} \cdot s'_i)$. Очевидно, элемент $s_i \cdot s'' := (x_{v_{i,j}} \cdot s'_i) \cdot s''$ принадлежит полугруппе $S(G, Y)^G$, так как $s \in S(G, Y)^G$. Применение леммы 1 завершает доказательство леммы 3.

СЛЕДСТВИЕ 1. *Пусть $G_{\Gamma} = (G, Y)$ – C -конечная группа и пусть для элемента $s = s' \cdot s'' \in S(G, Y)^G$ i -я координата $\tau_i(s)$ не меньше чем $2n_i p_i + 1$. Предположим, что $\tau_i(s'') = 0$. Тогда элемент s может быть записан в виде $s = s_{\Gamma_i} \cdot s_i \cdot s''$, где $s_i \cdot s'' \in S(G, Y)^G$.*

2.3. Обильные подграфы C -графов. Пусть Γ' – объединение нескольких компонент связности C -графа Γ . Скажем, что Γ' является *обильным* подграфом, если любые две вершины, принадлежащие любой связной компоненте графа Γ , могут быть соединены путем вдоль ребер графа Γ с метками, принадлежащими подграфу Γ' . На языке C -групп это означает, что любые два сопряженных C -порождающих элементов группы G_{Γ} сопряжены с помощью некоторого элемента, принадлежащего подгруппе $G_{\Gamma'}$ группы G_{Γ} , порожденной C -порождающими элементами y_v , где $v \in \Gamma'$. Отметим, что группа $G_{\Gamma'}$ является образом C -группы $G_{\tilde{\Gamma}'}$ при C -гомоморфизме $i_*: G_{\tilde{\Gamma}'} \rightarrow G_{\Gamma}$, заданным вложением $i: \tilde{\Gamma}' \hookrightarrow \Gamma$, где $\tilde{\Gamma}'$ – это C -подграф графа Γ , полученный из Γ' в результате удаления всех ребер, помеченных вершинами $v \notin \Gamma'$.

C -группа G_{Γ} действует на графе Γ . Поэтому гомоморфизм i_* определяет действие группы $G_{\tilde{\Gamma}'}$ на графе Γ , оставляющее неподвижной каждую связную

компоненту графа Γ . Легко видеть, что если Γ' является обильным подграфом, то $G_{\Gamma'}$ действует транзитивно на множестве вершин каждой связной компоненты графа Γ .

ЛЕММА 4. Пусть объединение Γ' некоторых связных компонент C -конечного графа Γ является обильным подграфом и пусть v_o, v_e – две вершины, принадлежащие некоторой компоненте связности графа Γ , скажем Γ_1 . Тогда существует путь $l(v_o; v_1, \dots, v_n)$, связывающий вершины v_o и v_e и такой, что $v_1, \dots, v_n$ являются вершинами графа Γ' .

ДОКАЗАТЕЛЬСТВО. Пусть V_1 – множество вершин графа Γ_1 . Для $v \in V_1$ обозначим через $V_1(v)$ множество всех вершин $v' \in V_1$ таких, что для v' существует путь $l(v; v_1, \dots, v_n)$, соединяющий вершины v и v' и такой, что вершины $v_1, \dots, v_n$ принадлежат графу Γ' . Скажем, что $v \leq v'$, если $v' \in V_1(v)$. Легко видеть, что $V_1(v) \subset V_1(v')$, если $v' \leq v$. Следовательно, множество подмножеств $V_1(v) \subset V_1$, $v \in V_1$, является частично упорядоченным относительно включений и поэтому существует максимальное подмножество, скажем $V_1(\tilde{v})$, так как Γ является конечным графом.

Кроме того, легко видеть, что C -группа $G_{\Gamma'}$ действует на множестве подмножеств $V_1(v) \subset V_1$, $v \in V_1$, по правилу $y_{v_1}(V_1(v)) = V_1(y_{v_1}(v))$ для C -порождающих элементов $y_{v_1} \in G_{\Gamma'}$. Поэтому для максимального подмножества $V_1(\tilde{v})$ имеем $V_1(\tilde{v}) = V_1(v)$ для всех $v \in V_1(\tilde{v})$, так как $G_{\Gamma'}$ действует транзитивно на V_1 . Следовательно, V_1 может быть представлен в виде несвязного объединения $V_1(\tilde{v}_1) \sqcup \dots \sqcup V_1(\tilde{v}_m)$ максимальных подмножеств $V_1(\tilde{v}_i)$. Наконец, так как Γ' является обильным подграфом и Γ_1 связан, получаем, что $m = 1$.

Пусть объединение Γ' нескольких связных компонент C -конечного графа Γ является обильным подграфом и пусть Γ_1 – связная компонента графа Γ . По определению, расстоянием $d_{\Gamma'}(v_o, v_e)$ между двумя вершинами v_o, v_e графа Γ_1 относительно Γ' назовем наименьшее n такое, что существует путь $l(v_o; v_1, \dots, v_n)$, соединяющий вершины v_o и v_e и такой, что вершины $v_1, \dots, v_n$ принадлежат графу Γ' . Число $d_{\Gamma'}(\Gamma_1) = \max_{v_o, v_e \in V_1} d_{\Gamma'}(v_o, v_e)$ называется *диаметром* графа Γ_1 относительно графа Γ' .

ПРЕДЛОЖЕНИЕ 4. Пусть $G_\Gamma = (G, Y)$ – C -конечная группа, $\Gamma' = \Gamma_1 \sqcup \dots \sqcup \Gamma_k$ – обильный подграф графа Γ и $\Gamma \setminus \Gamma' = \Gamma_{k+1} \sqcup \dots \sqcup \Gamma_m$, где Γ_i , $i = 1, \dots, m$, – связные компоненты графа Γ . Обозначим через

$$d = d_{\Gamma'} = \max(d_{\Gamma'}(\Gamma_1), \dots, d_{\Gamma'}(\Gamma_m)),$$

и пусть элемент $s \in S(G, Y)^G$ является таким, что $\tau_i(s) \geq 2n_i p_i d + 1$ для всех $i \leq k$, где $\tau_i(s)$ – i -я координата элемента $\tau(s)$. Тогда элемент s может быть записан в виде $s = (x_{v_{k+1},1}^{a_{k+1}} \cdot \dots \cdot x_{v_{m,1}}^{a_m}) \cdot s_{\Gamma'}^d \cdot s_1$, где $a_i = \tau_i(s)$ при $i = k+1, \dots, m$ и элемент $s_1 \in S(G, Y)$ таков, что $\tau_i(s_1) = 0$ при $i = k+1, \dots, m$.

ДОКАЗАТЕЛЬСТВО. Запишем элемент s в виде $s = s' \cdot s''$, где s' и s'' таковы, что $\tau_i(s') = 0$ при $i \geq k+1$ и $\tau_i(s'') = 0$ при $i \leq k$. Тогда согласно следствию 1 элемент s может быть записан в виде $s = \tilde{s}' \cdot s_{\Gamma'}^d \cdot s''$.

Пусть для некоторого j буква $x_{v_{m,j}}$ входит в s'' . Соединим вершину $v_{m,1}$ с $v_{m,j}$ путем $l(v_{m,1}; v_1, \dots, v_r)$ длины $r \leq d$, где $v_1, \dots, v_r$ – некоторые вершины

графа Γ' (напомним, что Γ' является обильным подграфом и поэтому согласно лемме 4 вершины $v_{m,1}$ и $v_{m,j}$ могут быть соединены таким путем), и запишем s'' в виде $s'' = x_{v_{m,j}} \cdot \tilde{s}''$. Согласно лемме 2 имеем $s_{\Gamma'}^d = \tilde{s} \cdot (x_{v_1} \cdot \dots \cdot x_{v_r})$ при некотором $\tilde{s}$. Также имеем $\alpha(x_{v_1} \dots x_{v_r}) = y_{v_1} \dots y_{v_r}$ и согласно определению C -графов C -групп имеем $(y_{v_1} \dots y_{v_r}) y_{v_{m,j}} (y_{v_1} \dots y_{v_r})^{-1} = y_{v_{m,1}}$. Следовательно,

$$s_{\Gamma'}^d \cdot x_{v_{m,j}} = \tilde{s} \cdot (x_{v_1} \cdot \dots \cdot x_{v_r}) \cdot x_{v_{m,j}} = \tilde{s} \cdot x_{v_{m,1}} \cdot (x_{v_1} \cdot \dots \cdot x_{v_r}),$$

и поэтому (после сдвига $x_{v_{m,1}}$ направо)

$$s = s'_1 \cdot s_{\Gamma'}^d \cdot s'' = \tilde{s}' \cdot \tilde{s} \cdot x_{v_{m,1}} \cdot (x_{v_1} \cdot \dots \cdot x_{v_r}) \cdot \tilde{s}'' = s'_1 \cdot s''_1 \cdot x_{v_{m,1}},$$

где элемент s'_1 таков, что $\tau_i(s'_1) = 0$ при $i \geq k+1$ и $\tau_i(s'_1) \geq 2n_i p_i d + 1$ для всех $i \leq k$, а s''_1 таков, что $\tau_i(s''_1) = 0$ при $i \leq k$.

Применив следствие 1, утверждение 5 и лемму 2, мы можем повторить описанные выше преобразования $a_m - 1$ раз и получить разложение на множители $s = s'_{a_m} \cdot s''_{a_m} \cdot x_{v_{m,1}}^{a_m}$. После этого для $i = m-1, \dots, k+1$ мы можем повторить описанные выше преобразования и получить разложение на множители $s = s'_{a_m + a_{m-1}} \cdot s''_{a_m + a_{m-1}} \cdot x_{v_{m-1,1}}^{a_{m-1}} \cdot x_{v_{m,1}}^{a_m}$. Наконец, двигаем полученное произведение $(x_{v_{k+1,1}}^{a_{k+1}} \cdot \dots \cdot x_{v_{m,1}}^{a_m})$ налево и применяем следствие 1, чтобы завершить доказательство.

2.4. C -графы оснащенных групп. Каждой оснащенной группе (G, O) можно сопоставить C -граф. По определению, C -граф $\Gamma = \Gamma_{(G,O)}$ оснащенной группы (G, O) – это C -граф, множество вершин которого находится во взаимно однозначном соответствии с множеством O . Две вершины v_{g_1} и v_{g_2} , $g_1, g_2 \in O$, соединены ребром $e_{v_{g_1}, v_{g_2}, v_g}$ тогда и только тогда, когда $g^{-1}g_1g = g_2$ для некоторого $g \in O$.

ПРИМЕР 1. Чтобы описать C -граф $\Gamma_{(\Sigma_n, T_n)}$ оснащенной симметрической группы (Σ_n, T_n) , где T_n – множество транспозиций, рассмотрим $(n-1)$ -мерный симплекс Δ_{n-1} . Пусть $V_1, \dots, V_n$ – вершины симплекса Δ_{n-1} и $E_{i,j}$ – его ребра, соединяющие вершины V_i и V_j . Вершины $v_{i,j}$ графа $\Gamma_{(\Sigma_n, T_n)}$ – это середины ребер $E_{i,j}$. Если $E_{i,j}$ и $E_{k,l}$ – скрещивающиеся ребра, то ребро графа $\Gamma_{(\Sigma_n, T_n)}$ с началом $v_{i,j}$ и меткой $v_{k,l}$ является петлей. Конец ребра с началом $v_{i,j}$ и меткой $v_{j,k}$ – это $v_{i,k}$.

Сопоставим каждой оснащенной группе (G, O) C -группу $G_{\Gamma_{(G,O)}}$. Обозначим C -порождающие элементы $y_{v_{g_i}} \in Y$, $g_i \in O$, C -группы $G_{\Gamma_{(G,O)}}$ через y_{g_i} . Имеем естественный гомоморфизм оснащенных групп $\beta = \beta_{(G,O)}: G_{\Gamma_{(G,O)}} \rightarrow (G, O)$, заданный формулой $\beta(y_{g_i}) = g_i$ для всех $g_i \in O$. Очевидно, $\beta|_Y: Y \rightarrow O$ является взаимно однозначным соответствием.

УТВЕРЖДЕНИЕ 8. (i) Ядро $\ker \beta$ гомоморфизма β является подгруппой центра группы $G_{\Gamma_{(G,O)}}$.

(ii) Если (G, O) – оснащенная группа такая, что G порождается элементами из O , то β и $\beta|_{[G_{\Gamma_{(G,O)}}, G_{\Gamma_{(G,O)}}]}: [G_{\Gamma_{(G,O)}}, G_{\Gamma_{(G,O)}}] \rightarrow [G, G]$ являются эпиморфизмами.

Доказательство этого утверждения очевидно.

2.5. Эквивалентность оснащенных групп. Пусть (G_1, O_1) и (G_2, O_2) – две оснащенные группы такие, что G_1 и G_2 порождены соответственно элементами из O_1 и O_2 . Скажем, что (G_1, O_1) и (G_2, O_2) *эквивалентны*, если C -графы $\Gamma_{(G_1, O_1)}$ и $\Gamma_{(G_2, O_2)}$ изоморфны как C -графы.

УТВЕРЖДЕНИЕ 9. Пусть (G_1, O_1) и (G_2, O_2) – эквивалентные оснащенные группы. Тогда C -группы $G_{\Gamma_{(G_1, O_1)}}$ и $G_{\Gamma_{(G_2, O_2)}}$ C -изоморфны.

Доказательство следует из утверждения 4.

Из утверждений 8 и 4 следует, что в каждом классе эквивалентных оснащенных групп с C -графом Γ существует максимальная группа, а именно C -группа G_Γ , такая, что для любой оснащенной группы (G, O) , принадлежащей этому классу, существует эпиморфизм оснащенных групп, а именно $\beta_{(G, O)}: G_{\Gamma_{(G, O)}} \rightarrow (G, O)$, который определяется однозначно изоморфизмом $\Gamma \simeq \Gamma_{(G, O)}$ и следующим условием: для каждого C -порождающего элемента y группы G_Γ образ $\beta_{(G, O)}(y) = g \in O$, если y и g соответствуют одной и той же вершине v графа $\Gamma \simeq \Gamma_{(G, O)}$. Согласно утверждению 8 ядро $\ker \beta_{(G, O)}$ является подгруппой центра $Z(G_\Gamma)$ группы G_Γ . Обратное утверждение также верно, а именно оснащенная группа (G, O) , полученная как факторгруппа G_Γ/H C -группы G_Γ , эквивалентна группе G_Γ , если H является подгруппой центра $Z(G_\Gamma)$ и не содержит ни C -порождающих элементов группы G_Γ , ни частных $y_i y_j^{-1}$ C -порождающих элементов y_i и y_j , $y_i \neq y_j$.

Порядок $a_{(G, O)} = |H \cap [G_\Gamma, G_\Gamma]|$ группы $H \cap [G_\Gamma, G_\Gamma]$ называется *индексом неоднозначности* оснащенной группы $(G = G_\Gamma/H, O)$, эквивалентной C -группе G_Γ .

ПРЕДЛОЖЕНИЕ 5. Пусть оснащенная группа (G, O) эквивалентна C -группе G_Γ . Если G является совершенной группой, то группа G_Γ изоморфна прямому произведению $[G_\Gamma, G_\Gamma] \times (G_\Gamma/[G_\Gamma, G_\Gamma])$.

ДОКАЗАТЕЛЬСТВО. Выберем вершину $v_i \in \Gamma_i$ в каждой связной компоненте Γ_i графа Γ .

Ограничение гомоморфизма $\beta_{(G, O)}$ на $[G_\Gamma, G_\Gamma]$ является эпиморфизмом на группу G , так как $\beta_{(G, O)}$ является эпиморфизмом и G – совершенная группа. Следовательно, для каждого C -порождающего элемента y_{v_i} группы G_Γ найдется элемент $g_i \in [G_\Gamma, G_\Gamma]$ такой, что $\beta_{(G, O)}(g_i) = \beta_{(G, O)}(y_{v_i})$. Имеем $y_{v_i} g_i^{-1} \in \ker \beta_{(G, O)} \subset Z(G_\Gamma)$ и $\text{ab}(y_{v_i} g_i^{-1}) = (0, \dots, 0, 1, 0, \dots, 0)$, где 1 стоит на i -м месте. Следовательно, элементы $y_{v_i} g_i^{-1}$ порождают в $Z(G_\Gamma)$ свободную абелеву группу H такую, что $\text{ab}|_H: H \rightarrow G_\Gamma/[G_\Gamma, G_\Gamma]$ является изоморфизмом. Поэтому предложение 5 следует из короткой точной последовательности

$$1 \rightarrow [G_\Gamma, G_\Gamma] \rightarrow G_\Gamma \rightarrow G_\Gamma/[G_\Gamma, G_\Gamma] \rightarrow 1. \quad (11)$$

ПРЕДЛОЖЕНИЕ 6. Пусть оснащенная группа (G, O) эквивалентна C -группе G_Γ . Если O состоит из единственного класса сопряженности, то группа G_Γ изоморфна полупрямому произведению $[G_\Gamma, G_\Gamma] \rtimes Z$.

Доказательство следует из точной последовательности (11), так как факторгруппа $G_\Gamma/[G_\Gamma, G_\Gamma] \simeq \mathbb{Z}$, если O состоит из единственного класса сопряженности.

Отметим, что предложение 6 перестает быть верным, если O состоит из более чем одного класса сопряженности. Например, аналог предложения 6 не верен, если G_Γ является свободной группой $\mathbb{F}^n$, $n > 1$, в которой множество C -порождающих элементов – это объединение классов сопряженности множества свободных порождающих группы $\mathbb{F}^n$.

ЛЕММА 5. Пусть подгруппа H центра $Z(G_\Gamma)$ C -конечной группы G_Γ порождена элементами $y_{v_i}^{k_i p_i} \in Z(G_\Gamma)$, $i = 1, \dots, m$, где $k_i p_i \geq 2$, v_i – вершина, принадлежащая i -й связной компоненте C -графа Γ и p_i – ее период. Тогда $(G, O) = G_\Gamma/H$ является оснащенной группой, эквивалентной группе G_Γ , и $\beta_{(G,O)}: [G_{\Gamma(G,O)}, G_{\Gamma(G,O)}] \rightarrow [G, G]$ является изоморфизмом. В частности, $\alpha_{(G,O)} = 1$.

Доказательство леммы 5 очевидно.

2.6. Гомоморфизм типа. Пусть (G, O) – оснащенная группа, $\Gamma = \Gamma_{(G,O)}$ – ее C -граф и G_Γ – C -группа, эквивалентная группе (G, O) . Гомоморфизм $\beta = \beta_{(G,O)}: G_\Gamma \rightarrow (G, O)$ определяет гомоморфизм полугрупп

$$\beta_*: S(G_\Gamma, Y) \rightarrow S(G, O),$$

заданный формулой $\beta_*(x_{y_g}) = x_g$ для $g \in O$.

УТВЕРЖДЕНИЕ 10. Гомоморфизм β_* является изоморфизмом.

Доказательство этого утверждения очевидно.

В дальнейшем в согласии с утверждением 10 мы будем отождествлять полугруппы $S(G, O)$ и $S(G_{\Gamma(G,O)}, Y)$.

Гомоморфизм полугрупп

$$\tau: S(G, O) = S(G_{\Gamma(G,O)}, Y) \rightarrow \mathbb{Z}_{\geq 0}^m \subset \mathbb{Z}^m = G_{\Gamma(G,O)} / [G_{\Gamma(G,O)}, G_{\Gamma(G,O)}]$$

называется *гомоморфизмом типа*, а образ $\tau(s)$ элемента $s \in S(G, O)$ называется *типом* элемента s . Если O состоит из единственного класса сопряженности, то гомоморфизм τ может быть (и будет) отождествлен с гомоморфизмом $\ln: S(G, O) \rightarrow \mathbb{Z}_{\geq 0}$. В общем случае, если $\tau(s) = (\tau_1(s), \dots, \tau_m(s))$, то $\ln(s) = \sum_{i=1}^m \tau_i(s)$.

Элемент $g \in G_\Gamma$ называется *положительным*, если найдется элемент $s \in S(G_\Gamma, Y)$ такой, что $\alpha_{G_\Gamma}(s) = g$.

ЛЕММА 6. Любой элемент g C -группы G_Γ может быть представлен в виде

$$g = g_1 g_2^{-1}, \quad (12)$$

где g_1 и g_2 – положительные элементы. В частности, $g \in [G_\Gamma, G_\Gamma]$ тогда и только тогда, когда $\text{ab}(g_1) = \text{ab}(g_2)$ в представлении (12) элемента g в виде частного двух положительных элементов g_1 и g_2 .

Если G_Γ – C -конечная группа, то для каждого элемента $g \in G_\Gamma$ существует такое представление (12) элемента g в виде частного двух положительных элементов g_1 и g_2 , в котором $g_2 = \alpha_{G_\Gamma}(s_\Gamma^n)$ при некотором n и $g_1 = \alpha_{G_\Gamma}(s_1)$ для некоторого элемента $s_1 \in S(G_\Gamma, Y)^{G_\Gamma}$, где s_Γ – канонический элемент полугруппы $S(G_\Gamma, Y)$.

ДОКАЗАТЕЛЬСТВО. Первая часть леммы 6 очевидна. Вторая часть следует из леммы 2.

Пусть H – подгруппа центра C -конечной группы G_Γ . Обозначим через z_H минимальный показатель n такой, что каждый элемент $g \in H \cap [G_\Gamma, G_\Gamma]$ имеет представление (12), в котором $g_2 = \alpha_{G_\Gamma}(s_\Gamma^n)$.

ПРЕДЛОЖЕНИЕ 7. Пусть $G_\Gamma = (G, Y)$ – C -конечная группа, $\Gamma' = \Gamma_1 \sqcup \dots \sqcup \Gamma_k \subset \Gamma$ – обильный подграф графа Γ и $\tilde{\Gamma}'$ – C -граф, определяемый графом Γ' . Тогда $i_*|_{[G_{\tilde{\Gamma}'}, G_{\tilde{\Gamma}'}]}: [G_{\tilde{\Gamma}'}, G_{\tilde{\Gamma}'}] \rightarrow [G_\Gamma, G_\Gamma]$ является изоморфизмом.

Доказательство следует из предложения 4 и леммы 6.

СЛЕДСТВИЕ 2. Пусть G_Γ и $G_{\tilde{\Gamma}'}$ – C -конечные группы, эквивалентные соответственно оснащенным группам (G, O) и (G, O') , где $O' \subset O$ – оснащение группы G такое, что элементы из O' порождают группу G . Тогда $a_{(G, O)} \leq a_{(G, O')}$, в частности, если $a_{(G, O')} = 1$, то $a_{(G, O)} = 1$.

§ 3. Стабильность полугрупп разложений на множители

3.1. Эквивалентность элементов. Элементы s_1 и s_2 полугруппы S называются r -эквивалентными (соответственно l -эквивалентными), если найдется такой элемент $s_3 \in S$, что $s_1 \cdot s_3 = s_2 \cdot s_3$ (соответственно $s_3 \cdot s_1 = s_3 \cdot s_2$) и эти элементы называются эквивалентными, если найдутся такие два элемента $s_3, s_4 \in S$, что $s_3 \cdot s_1 \cdot s_4 = s_3 \cdot s_2 \cdot s_4$. Обозначение $s_1 \sim s_2$ (соответственно $s_1 \sim_r s_2$ и $s_1 \sim_l s_2$) означает, что элементы s_1 и s_2 эквивалентны (соответственно r -эквивалентны и l -эквивалентны). Легко видеть, что если $s_1 \sim s_2$, где $s_1, s_2 \in S(G, O)$, то $\tau(s_1) = \tau(s_2)$.

ЛЕММА 7. Пусть $s_1, s_2 \in S(G, O)$ – два элемента полугруппы разложений на множители над группой G . Тогда следующие утверждения эквивалентны:

- (i) $s_1 \sim_r s_2$;
- (ii) $s_1 \sim_l s_2$;
- (iii) $s_1 \sim s_2$.

ДОКАЗАТЕЛЬСТВО. Докажем только импликацию (i) $\implies$ (ii), так как доказательства всех остальных импликаций аналогичны.

Имеем $s_1 \cdot s_3 = \rho(\alpha_G(s_1))(s_3) \cdot s_1$ и $s_2 \cdot s_3 = \rho(\alpha_G(s_2))(s_3) \cdot s_2$. Так как α_G является гомоморфизмом, то легко видеть, что $\alpha_G(s_1) = \alpha_G(s_2)$, если s_1 и s_2 являются r -эквивалентными (соответственно l -эквивалентными или эквивалентными). Следовательно, если $s_1 \sim_r s_2$, т.е. $s_1 \cdot s_3 = s_2 \cdot s_3$ для некоторого $s_3 \in S(G, O)$, то $\rho(\alpha_G(s_1))(s_3) \cdot s_1 = \rho(\alpha_G(s_2))(s_3) \cdot s_2$, т.е. $s_1 \sim_l s_2$.

ЛЕММА 8. Пусть $S(G, O)$ – полугруппа разложений на множители над группой G . Тогда отношение $s_1 \sim s_2$ является отношением эквивалентности.

ДОКАЗАТЕЛЬСТВО. Пусть $s_1 \sim s_2$ и $s_2 \sim s_3$. Тогда согласно лемме 7 найдутся элементы s_4 и s_5 такие, что $s_4 \cdot s_1 = s_4 \cdot s_2$ и $s_2 \cdot s_5 = s_3 \cdot s_5$. Следовательно, $s_4 \cdot s_1 \cdot s_5 = s_4 \cdot s_2 \cdot s_5 = s_4 \cdot s_3 \cdot s_5$, т.е. $s_1 \sim s_3$.

ЛЕММА 9. Пусть $s_1, s_2, s_3, s_4 \in S(G, O)$ – четыре элемента полугруппы разложений на множители над группой G . Тогда $s_1 \cdot s_2 \sim s_3 \cdot s_4$, если $s_1 \sim s_3$ и $s_2 \sim s_4$. Если $s_1 \cdot s_3 \sim s_2 \cdot s_4$ и $s_1 \sim s_2$, то $s_3 \sim s_4$.

Доказательство аналогично доказательству леммы 8.

ТЕОРЕМА 2. Пусть G – C -группа и Y – множество ее C -порождающих элементов. Два элемента $s_1, s_2 \in S(G, Y)$ эквивалентны тогда и только тогда, когда $\alpha_G(s_1) = \alpha_G(s_2)$, где α_G – гомоморфизм произведения.

ДОКАЗАТЕЛЬСТВО. Очевидно, что если $s_1 \sim s_2$, то $\alpha_G(s_1) = \alpha_G(s_2)$.

Обозначим через $x_i = x_{y_i}$ порождающий элемент $S(G, Y)$, соответствующий C -порождающему элементу $y_i \in Y$. Пусть элементы $s_1 = x_{i_1} \cdot \dots \cdot x_{i_n}$ и $s_2 = x_{j_1} \cdot \dots \cdot x_{j_k}$ таковы, что $\alpha_G(s_1) = y_{i_1} \cdot \dots \cdot y_{i_n} = y_{j_1} \cdot \dots \cdot y_{j_m} = \alpha_G(s_2)$. Тогда легко видеть, что $\tau(s_1) = \tau(s_2)$ и, в частности, $n = k$. Кроме того, слово $w = y_{i_1} \cdot \dots \cdot y_{i_n} y_{j_n}^{-1} \cdot \dots \cdot y_{j_1}^{-1}$ представляет единицу группы G .

Чтобы доказать, что $s_1 \sim s_2$, мы будем использовать некоторые допустимые преобразования диаграмм ван Кампена, определенных над C -копредставлением группы G . Чтобы определить их, напомним, что согласно лемме ван Кампена (см., например, [8] или [9]), для слова w существует диаграмма ван Кампена, т.е. плоский конечный клеточный комплекс $D \subset \mathbb{R}^2$ со следующими дополнительными данными и имеющий следующие свойства:

- 1) комплекс D связан и односвязен;
- 2) каждое ребро (одномерная клетка) комплекса D имеет направление и метку – некоторый элемент $y \in Y$;
- 3) некоторая вершина (нульмерная клетка), принадлежащая топологической границе ∂D комплекса D , является выделенной в качестве базисной вершины A и называется *началом* диаграммы;
- 4) каждая двумерная клетка Q комплекса D является четырехугольником, соответствующим C -соотношению $y_i y_j = y_k y_l$, входящему в C -копредставление группы G (см. рис. 1; вершина v_1 будет называться *основанием* четырехугольника Q , а вершина v_2 – его *верхней точкой*);

Рис. 1

5) граничный цикл ∂D , т.е. путь вдоль ребер, принадлежащих границе, в направлении часовой стрелки, один раз обходящий границу неограниченного дополнительного к D региона, начинающийся и заканчивающийся в вершине A , имеет метку $w = y_{i_1} \cdot \dots \cdot y_{i_n} y_{j_n}^{-1} \cdot \dots \cdot y_{j_1}^{-1}$.

Так как в нашем случае слово w распадается на два подслова: первое состоит из букв с положительными экспонентами, а второе – с отрицательными, то диаграмма ван Кампена D имеет следующий вид: она является цепью дисков, соединенных простыми направленными путями (см. рис. 2).

Рис. 2

Обозначим конечную вершину этой цепи через B и назовем ее *концом* диаграммы D . Диаграммы, удовлетворяющие условиям 1–5, будем называть *допустимыми*.

Из лемм 8 и 9 следует, что достаточно рассматривать только диаграммы D , являющиеся дисками (см. рис. 3).

Рис. 3

Вершина v диаграммы ван Кампена D называется *локально максимальной* (соответственно *минимальной*), если не существует ребра диаграммы D , для которого вершина v является началом (соответственно концом). Путь l вдоль ребер $e_1, \dots, e_k$ диаграммы D называется *возрастающим*, если начало каждого ребра e_{i+1} является концом ребра e_i при $i = 1, \dots, k-1$. Метка возрастающего пути l является положительным словом $y_{l_1} \dots y_{l_k}$.

Начало A и конец B делят границу ∂D на две части. Возрастающий путь $\partial_l D$ (соответственно $\partial_r D$) вдоль границы ∂D , соединяющий A и B и имеющий метку $y_{i_1} \dots y_{i_n}$ (соответственно $y_{j_1} \dots y_{j_n}$) будем называть *левой* (соответственно *правой*) *частью* границы ∂D .

Если начало A не является локально минимальной вершиной диаграммы D , то найдется локально минимальная вершина C и простой возрастающий путь l , соединяющий вершины C и A . (Отметим, что вершина C не может принадлежать границе ∂D , так как положительное слово от C -порождающих элементов не может представлять единицу C -группы.) Тогда мы можем разрезать диск D вдоль пути l и в результате получить новую дисковую диаграмму D' (см. рис. 4), в которой C является началом и метка границы $\partial D'$ – это

$$y_{l_1} \dots y_{l_k} y_{i_1} \dots y_{i_n} y_{j_n}^{-1} \dots y_{j_1}^{-1} y_{l_k}^{-1} \dots y_{l_1}^{-1},$$

где $y_{l_1} \dots y_{l_k}$ – метка пути l .

Назовем описанное выше преобразование $D \rightsquigarrow D'$ *допустимым преобразованием* I. Отметим, что диаграмма D' , полученная из допустимой диаграммы

Рис. 4

после преобразования I, является допустимой и начало C диаграммы D' является локально минимальной вершиной.

Аналогично, если конец B не является локально максимальной вершиной диаграммы D , то найдется локально максимальная вершина C и простой возрастающий путь l , соединяющий B и C . Тогда мы можем разрезать диск D вдоль пути l и в результате получим новую допустимую диаграмму D' , в которой C является концом и метка границы $\partial D'$ – это

$$y_{i_1} \dots y_{i_n} y_{l_1} \dots y_{l_k} y_{l_k}^{-1} \dots y_{l_1}^{-1} y_{j_n}^{-1} \dots y_{j_1}^{-1},$$

где $y_{l_1} \dots y_{l_k}$ – метка пути l . Назовем это преобразование $D \rightsquigarrow D'$ *допустимым преобразованием II*. Отметим, что после преобразования II конец C диаграммы D' является локально максимальной вершиной.

Пусть $v \in \partial_l D$ – вершина допустимой дисковой диаграммы D такая, что v не совпадает ни с началом A , ни с концом B диаграммы D , и пусть существует ребро e диаграммы D , $e \not\subset \partial D$, для которого v является началом. Обозначим через y_0 метку этого ребра и пусть C – его конец, $C \notin \partial D$. Предположим для определенности, что $v \in \partial_l D$ (случай, когда $v \in \partial_r D$ аналогичен). Пусть y_{i_k} (соответственно $y_{i_{k+1}}$) – метка ребра, принадлежащего границе ∂D , для которого v является концом (соответственно началом). Разрежем диаграмму D вдоль e и после этого приклеим последовательно $n - k$ дополнительных четырехугольников так, как это изображено на рис. 5, при этом четырехугольник, подклеиваемый на l -м шаге к полученной дисковой диаграмме вдоль ребер с метками y_0 и $y_{i_{k+l}}$, соответствует соотношению $y_{i_{k+l}} y_0 = y_0 y'_{i_{k+l}}$, $l = k + 1, \dots, n - k$, в S -группе G .

После подклейки этих четырехугольников мы получим новую допустимую диаграмму D' , конец которой – это вершина B' и метка границы $\partial D'$ – это

$$y_{i_1} \dots y_{i_k} y_0 y'_{i_{k+1}} \dots y'_{i_n} y_0^{-1} y_{j_n}^{-1} \dots y_{j_1}^{-1}.$$

Назовем описанное выше преобразование $D \rightsquigarrow D'$ *допустимым преобразованием III, определенным ребром e* .

УТВЕРЖДЕНИЕ 11. Если элементы $x_{i_1} \dots x_{i_k} \cdot x_0 \cdot x'_{i_{k+1}} \dots x'_{i_n}$ и $x_{j_1} \dots x_{j_n} \cdot x_0$, полученные из $x_{i_1} \dots x_{i_k} \cdot x_{i_{k+1}} \dots x_{i_n}$ и $x_{j_1} \dots x_{j_n}$ в результате допустимого преобразования III, определенного ребром e , являются

Рис. 5

эквивалентными, то элементы $x_{i_1} \cdot \dots \cdot x_{i_k} \cdot x_{i_{k+1}} \cdot \dots \cdot x_{i_n}$ и $x_{j_1} \cdot \dots \cdot x_{j_n}$ также являются эквивалентными.

Доказательство этого утверждения очевидно.

Пусть D является допустимой дисковой диаграммой такой, что ее начало A является локально минимальной вершиной, а ее конец B – локально максимальной вершиной. Пусть C – локально максимальная вершина диаграммы D , $C \neq B$. Тогда $C \notin \partial D$, так как в этом случае существует только одна локально максимальная вершина, принадлежащая границе ∂D , а именно конец B . Скажем, что вершина C является *видимой*, если найдется вершина $v \in \partial D$, $v \neq A$, такая, что ее можно соединить с вершиной C с помощью возрастающего пути l вдоль ребер, принадлежащих $D \setminus \partial D$, и такого, что $l \cap \partial D = v$. Пусть путь l состоит из ребер $e_1, \dots, e_k$ с метками $y_1, \dots, y_k$. Осуществим последовательность допустимых преобразований III, определяемых ребрами $e_1, \dots, e_k$. В результате получим новую допустимую диаграмму D' , начало A которой является локально минимальной вершиной, конец B' – локально максимальной вершиной, имеющую строго меньше локально максимальных вершин по сравнению с числом локально максимальных вершин диаграммы D . Такую последовательность допустимых преобразований назовем *преобразованием, понижающим число локально максимальных вершин*.

Вернемся к доказательству того, что $s_1 \sim s_2$, если $\alpha_G(s_1) = \alpha_G(s_2)$, где $s_1 = x_{i_1} \cdot \dots \cdot x_{i_n}$ и $s_2 = x_{j_1} \cdot \dots \cdot x_{j_n}$ – два элемента полугруппы разложений на множители $S(G, Y)$ над C -группой (G, Y) . Так как $\alpha_G(s_1) = \alpha_G(s_2)$, слово $w = y_{i_1} \dots y_{i_n} y_{j_1}^{-1} \dots y_{j_n}^{-1}$ представляет единицу группы G . Поэтому согласно лемме ван Кампена существует плоская дисковая диаграмма D над C -копредставлением группы G с граничной меткой – словом w . Согласно

леммам 8 и 9, как было указано выше, мы можем предполагать, что D является диском. Обратно, допустимая дисковая диаграмма с граничной меткой $w = y_{i_1} \dots y_{i_n} y_{j_1}^{-1} \dots y_{j_n}^{-1}$ определяет два элемента $s_1(D) = x_{i_1} \dots x_{i_n}$ и $s_2(D) = x_{j_1} \dots x_{j_n}$ полугруппы $S(G, Y)$ такие, что $\alpha_G(s_1(D)) = \alpha_G(s_2(D))$. Отметим, что если $D \rightsquigarrow D'$ является допустимым преобразованием типа I, либо II, либо III, то согласно леммам 8, 10 и утверждению 11 $s_1(D) \sim s_2(D)$ тогда и только тогда, когда $s_1(D') \sim s_2(D')$. Поэтому, не ограничивая общности, мы можем предполагать, что D является допустимой дисковой диаграммой такой, что:

- (i) начало A диаграммы D является локально минимальной вершиной;
- (ii) конец B диаграммы D является локально максимальной вершиной;
- (iii) существует только одна видимая локально максимальная вершина диаграммы D , а именно ее конец B .

Покажем, что если допустимая дисковая диаграмма D удовлетворяет условиям (i)–(iii), то $s_1(D) \sim s_2(D)$. Действительно, если D состоит из единственного четырехугольника Q , то начало A является основанием четырехугольника Q , а ее конец B является верхней точкой четырехугольника Q . Очевидно, в этом случае имеем $s_1(D) = s_2(D)$ (см. рис. 1).

Теперь, пусть D удовлетворяет условиям (i)–(iii), имеет K невидимых локально максимальных вершин и состоит из k четырехугольников. Рассмотрим ребро $e_1 \subset \partial_l D$, начало которого – это A , и пусть v_1 – конец ребра e_1 и Q – четырехугольник такой, что $e_1 \subset \partial Q$. Тогда основанием четырехугольника Q является начало A , так как A – локально минимальная вершина. Пусть v_2 – верхняя точка четырехугольника Q и $e_2 \subset \partial Q$ – ребро, соединяющее вершины v_1 и v_2 .

Имеется две возможности: либо $e_2 \subset \partial_l D$, и поэтому $v_2 \in \partial_l D$, либо $e_2 \not\subset \partial_l D$. В первом случае, если $y_{i_1} y_{i_2} y_{l_2}^{-1} y_{l_1}^{-1}$ является меткой границы ∂Q , то

$$s_1(D) = x_{i_1} \cdot x_{i_2} \cdot (x_{i_3} \cdot \dots \cdot x_{i_n}) = x_{l_1} \cdot x_{l_2} \cdot (x_{i_3} \cdot \dots \cdot x_{i_n})$$

и если мы вырежем четырехугольник Q из D , то получим новую допустимую диаграмму $D'' = D \setminus Q$, имеющую только $k - 1$ четырехугольник, и такую, что $s_1(D'') = x_{l_1} \cdot x_{l_2} \cdot (x_{i_3} \cdot \dots \cdot x_{i_n})$ и $s_2(D'') = x_{j_1} \cdot \dots \cdot x_{j_n}$. Обозначим также четырехугольник Q через D' . Отметим, что не обязательно диаграмма D'' удовлетворяет условиям (i)–(iii). Действительно, если ребро e четырехугольника Q с меткой x_{l_1} принадлежит правой границе $\partial_r D$, то мы должны удалить его, чтобы получить допустимую дисковую диаграмму. Поэтому в этом случае метка границы $\partial D''$ – это $y_{l_2} (y_{i_3} \dots y_{i_n}) y_{j_n}^{-1} \dots y_{j_2}^{-1}$ (так как $y_{l_1} = y_{j_1}$), и если начало диаграммы D'' не является локально минимальной вершиной, то мы должны осуществить преобразование I, которое, однако, не увеличивает ни числа локально максимальных вершин, ни числа четырехугольников. Затем, возможно, что некоторая невидимая локально максимальная вершина диаграммы D становится видимой в D'' . (Это возможно только в случае $K > 0$.) Но в этом случае мы можем осуществить допустимое преобразование, уменьшающее число локально максимальных вершин и получить новую допустимую дисковую диаграмму, имеющую строго меньше чем K невидимых локально максимальных вершин.

Рис. 6

Если $v_2 \notin \partial D$, то найдется ребро e_3 диаграммы D , начало которого – это v_2 , так как по предположению вершина v_2 не может быть локально максимальной. Пусть v_3 – конец ребра e_3 . Если $v_3 \notin \partial D$, то найдется ребро e_4 , конец которого – это v_3 , и т.д. В результате мы можем найти возрастающий путь $l = (e_2, \dots, e_m)$, соединяющий вершину v_1 с некоторой вершиной v_m , принадлежащей границе ∂D . Имеется две возможности: либо $v_m \in \partial_l D$ (см. рис. 6, случай l), либо $v_m \in \partial_r D$ (см. рис. 6, случай r). В обоих случаях путь l делит диаграмму D на две дисковые диаграммы D' и D'' , каждая из которых состоит из не более чем $k - 1$ четырехугольников. Если $y_{l_2} \dots y_{l_m}$ – метка пути l , то

$$\begin{aligned} s_1(D') &= x_{i_2} \cdot \dots \cdot x_{i_m}, & s_2(D') &= x_{l_2} \cdot \dots \cdot x_{l_m}, \\ s_1(D'') &= x_{i_1} \cdot x_{l_2} \cdot \dots \cdot x_{l_m} \cdot x_{i_{m+1}} \cdot \dots \cdot x_{i_n}, & s_2(D'') &= x_{j_1} \cdot \dots \cdot x_{j_n} \end{aligned}$$

в случае $v_2 \in \partial_l D$ и

$$\begin{aligned} s_1(D') &= x_{i_2} \cdot \dots \cdot x_{i_n}, & s_2(D') &= x_{l_2} \cdot \dots \cdot x_{l_m} \cdot x_{j_{m+1}} \cdot \dots \cdot x_{j_n}, \\ s_1(D'') &= x_{i_1} \cdot x_{l_2} \cdot \dots \cdot x_{l_m}, & s_2(D'') &= x_{j_1} \cdot \dots \cdot x_{j_m} \end{aligned}$$

в случае $v_2 \in \partial_r D$. Если конец v_m диаграммы D' (соответственно D'') в случае l (соответственно в случае r) не является локально максимальной вершиной, то осуществим допустимое преобразование Π диаграммы D' (соответственно диаграммы D''), которое не увеличивает ни числа четырехугольников, ни числа

локально максимальных вершин. Аналогично, осуществим допустимое преобразование I в диаграмме D' , если ее начало v_1 не является локально минимальной вершиной.

Чтобы завершить доказательство теоремы 2, используем две индукции: первая – по числу K невидимых локально максимальных вершин допустимых дисковых диаграмм, удовлетворяющих условиям (i)–(iii), а вторая – по числу k четырехугольников, содержащихся в таких диаграммах. Как было показано выше, на каждом шаге индукций можно найти путь l , делящий допустимую дисковую диаграмму D , удовлетворяющую условиям (i)–(iii), на две поддиаграммы D' и D'' такие, что либо (после некоторого допустимого преобразования) D' и D'' имеют не более чем K невидимых локально максимальных вершин и имеют строго меньше чем k четырехугольников, либо D' и D'' имеют строго меньше чем K невидимых локально максимальных вершин (в случае $K > 0$). По индуктивным предположениям имеем $s_1(D') \sim s_2(D')$ и $s_1(D'') \sim s_2(D'')$. Поэтому согласно леммам 8 и 9 имеем $s_1(D) \sim s_2(D)$.

3.2. Стабильность полугрупп разложений на множители над C -конечными группами. Напомним, что полугруппа разложений на множители $S(G, O)$ над оснащенной группой (G, O) называется *стабильной*, если существует элемент $s \in S(G, O)$ такой, что $s_1 \cdot s = s_2 \cdot s$ для любых двух элементов $s_1, s_2 \in S(G, O)$ таких, что $\alpha_G(s_1) = \alpha_G(s_2)$ и $\tau(s_1) = \tau(s_2)$. Элемент $s \in S(G, O)$, участвующий в определении стабильной полугруппы, называется *стабилизирующим* элементом этой полугруппы над оснащенной группой.

Пусть s_1, s_2 – два эквивалентных элемента полугруппы разложений на множители $S(G, Y)$ над C -группой (G, Y) . Обозначим через $e(s_1, s_2)$ наименьшее число k такое, что существует элемент $s \in S(G, Y)$ длины k и такой, что $s_1 \cdot s = s_2 \cdot s$.

Как и выше, пусть $\Gamma = \Gamma_1 \sqcup \dots \sqcup \Gamma_m$ – представление конечного C -графа C -группы $(G, Y) = G_\Gamma$ в виде объединения его связных компонент, $V_i = \{v_{i,1}, \dots, v_{i,n_i}\}$ – множество вершин компоненты Γ_i и p_i – период вершин $v_{i,j}$.

Любой элемент $s \in S(G, Y)$ может быть записан в виде $s = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j}}$. Рассмотрим множество

$$R = \left\{ s = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j}} \in S(G, Y) \mid \sum_{j=1}^{n_i} k_{i,j} \leq p_i n_i, i = 1, \dots, m \right\},$$

и пусть

$$E = \{(s_1, s_2) \in R^2 \mid s_1 \sim s_2\}.$$

Положим

$$e_\Gamma = \max_{(s_1, s_2) \in E} e(s_1, s_2).$$

ЛЕММА 10. *Имеем $s_1 \cdot s_\Gamma^{e_\Gamma} = s_2 \cdot s_\Gamma^{e_\Gamma}$ для всех $(s_1, s_2) \in E$, где s_Γ – канонический элемент полугруппы $S(G, Y)$.*

ДОКАЗАТЕЛЬСТВО. Для любой пары $(s_1, s_2) \in E$ найдется элемент $s_{1,2}$ длины $\ln(s_{1,2}) \leq e_\Gamma$ и такой, что $s_1 \cdot s_{1,2} = s_2 \cdot s_{1,2}$. Согласно лемме 2 существует элемент $s'_{1,2}$ такой, что $s_{1,2} \cdot s'_{1,2} = s_\Gamma^{e_\Gamma}$. Поэтому

$$s_1 \cdot s_\Gamma^{e_\Gamma} = s_1 \cdot s_{1,2} \cdot s'_{1,2} = s_2 \cdot s_{1,2} \cdot s'_{1,2} = s_2 \cdot s_\Gamma^{e_\Gamma}.$$

ТЕОРЕМА 3. Пусть $(G, Y) = G_\Gamma$ является C -конечной группой. Тогда полугруппа $S(G, Y)$ стабильна и s_Γ^e является стабилизирующим элементом.

ДОКАЗАТЕЛЬСТВО. Пусть s_1, s_2 — два элемента полугруппы $S(G, Y)$ такие, что $\alpha_G(s_1) = \alpha_G(s_2)$ и $\tau(s_1) = \tau(s_2)$. Запишем их в виде

$$s_1 = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j,1}}, \quad s_2 = \prod_{v_{i,j} \in \Gamma} x_{v_{i,j}}^{k_{i,j,2}}.$$

Так как $\tau(s_1) = \tau(s_2)$, имеем

$$\sum_{j=1}^{n_i} k_{i,j,1} = \sum_{j=1}^{n_i} k_{i,j,2}, \quad i = 1, \dots, m.$$

Если $\sum_{j=1}^{n_i} k_{i,j,1} \geq p_i n_i$ для некоторого i , то существует j_1 (соответственно j_2) такое, что $k_{i,j_1,1} \geq p_i$ (соответственно $k_{i,j_2,2} \geq p_i$). Если снова

$$k_{i,j_1,1} - p_i + \sum_{j=1, j \neq j_1}^{n_i} k_{i,j,1} \geq p_i n_i$$

$$\left(\text{соответственно } k_{i,j_2,2} - p_i + \sum_{j=1, j \neq j_2}^{n_i} k_{i,j,2} \geq p_i n_i \right),$$

то либо существует j'_1 (соответственно j'_2) такое, что $k_{i,j'_1,1} \geq p_i$ (соответственно $k_{i,j'_2,2} \geq p_i$), либо $k_{i,j_1,1} - p_i \geq p_i$ (соответственно $k_{i,j_2,2} - p_i \geq p_i$). Продолжая этот процесс, в результате получим, что элементы s_1 и s_2 могут быть записаны в следующем виде:

$$s_1 = \prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,1} + r_{i,j,1}} = \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,1}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right),$$

$$s_2 = \prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,2} + r_{i,j,2}} = \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_i c_{i,j,2}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right),$$

где

$$\sum_{j=1}^{n_i} r_{i,j,1} = \sum_{j=1}^{n_i} r_{i,j,2} < n_i p_i, \quad i = 1, \dots, m,$$

$$\sum_{j=1}^{n_i} c_{i,j,1} = \sum_{j=1}^{n_i} c_{i,j,2}, \quad i = 1, \dots, m.$$

Так как $\alpha_G(x_{v_{i,j_1}}^{p_i}) = \alpha_G(x_{v_{i,j_2}}^{p_i}) = y_{v_{i,1}}^{p_i}$ для $1 \leq j_1 \leq j_2 \leq n_i$ и для всех i и так как $\alpha_G(s_1) = \alpha_G(s_2)$, то имеем

$$\alpha_G \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) = \alpha_G \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right).$$

Тогда согласно теореме 2 имеем

$$\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \sim \prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}}$$

и согласно лемме 10

$$\left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_\Gamma^{e_\Gamma} = \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_\Gamma^{e_\Gamma}.$$

Отметим, что элемент $s_1 \cdot s_\Gamma^{e_\Gamma}$ (соответственно $s_2 \cdot s_\Gamma^{e_\Gamma}$) принадлежит полугруппе $S(G, Y)^G$. Следовательно, согласно лемме 1

$$\begin{aligned} s_1 \cdot s_\Gamma^{e_\Gamma} &= \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_{i,j,1}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_\Gamma^{e_\Gamma} \\ &= \left(\prod_{i=1}^m x_{v_{i,1}}^{p_{i,1}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,1}} \right) \cdot s_\Gamma^{e_\Gamma}, \\ s_2 \cdot s_\Gamma^{e_\Gamma} &= \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{p_{i,j,2}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_\Gamma^{e_\Gamma} \\ &= \left(\prod_{i=1}^m x_{v_{i,1}}^{p_{i,1}} \right) \cdot \left(\prod_{i=1}^m \prod_{j=1}^{n_i} x_{v_{i,j}}^{r_{i,j,2}} \right) \cdot s_\Gamma^{e_\Gamma}, \end{aligned}$$

где $c_i = \sum_{j=1}^{n_i} c_{i,j,1} = \sum_{j=1}^{n_i} c_{i,j,2}$, и поэтому $s_1 \cdot s_\Gamma^{e_\Gamma} = s_2 \cdot s_\Gamma^{e_\Gamma}$.

ТЕОРЕМА 4. Пусть (G, O) – оснащенная конечная группа. Полугруппа $S(G, O)$ (соответственно $S(G, O)^G$, $S(G, O)_1$ и $S(G, O)_1^G$) над группой G является стабильной тогда и только тогда, когда индекс неоднозначности $a_{(G, O)} = 1$.

ДОКАЗАТЕЛЬСТВО. Оснащенная группа (G, O) эквивалентна C -конечной группе (G_Γ, Y) , где $\Gamma = \Gamma_{(G, O)}$, и существует эпиморфизм $\beta_{(G, O)}: G_\Gamma \rightarrow G$ такой, что $H = \ker \beta \subset Z(G_\Gamma)$. Согласно утверждению 9 полугруппы $S(G, O)$ и $S(G_\Gamma, Y)$ естественным образом изоморфны. Пусть α_{G_Γ} и α_G – соответственно гомоморфизмы произведения из полугруппы $S(G, O)$ в группы G_Γ и G . Заметим, что согласно теореме 3 для любого натурального числа c элемент $s_\Gamma^{ce_\Gamma}$ является стабилизирующим элементом полугруппы $S(G_\Gamma, Y)$ над группой G_Γ и существует натуральное число c_0 такое, что $\alpha_G(s_\Gamma^{c_0 e_\Gamma}) = 1 \in G$, так как G является конечной группой.

Если $a_{(G, O)} = |H \cap [G_\Gamma, G_\Gamma]| = 1$, то для $s_1, s_2 \in S(G, O)$ таких, что $\tau(s_1) = \tau(s_2)$, имеем $\alpha_G(s_1) = \alpha_G(s_2)$ тогда и только тогда, когда $\alpha_{G_\Gamma}(s_1) = \alpha_{G_\Gamma}(s_2)$. Поэтому если $a_{(G, O)} = 1$, то полугруппы $S(G, O)$, $S(G, O)^G$, $S(G, O)_1$ и $S(G, O)_1^G$ над группой G являются стабильными и $s_\Gamma^{c_0 e_\Gamma}$ является одним из их стабилизирующих элементов.

Если $a_{(G, O)} > 1$, то существует элемент $g \in H \cap [G_\Gamma, G_\Gamma]$ такой, что $g \neq 1$. Согласно лемме 6 существуют два элемента $s_1, s_2 \in S(G_\Gamma, Y)$ такие, что $g = \alpha_{G_\Gamma}(s_1)\alpha_{G_\Gamma}(s_2)^{-1}$. Следовательно, $s_1 \not\sim s_2$, но $\alpha_G(s_1) = \alpha_G(s_2)$ и $\tau(s_1) = \tau(s_2)$,

т.е. полугруппы $S(G, O)$, $S(G, O)^G$, $S(G, O)_1$ и $S(G, O)_1^G$ над группой G не являются стабильными (умножая s_1 и s_2 на некоторый элемент s , мы можем предполагать, что $s_1, s_2 \in S(G, O)_1^G$).

§ 4. Однозначность разложения на множители в случае достаточно большого числа множителей

4.1. Случай C -конечных групп. Пусть $G_\Gamma = (G, Y)$ – C -конечная группа и m – число связных компонент C -графа Γ .

ТЕОРЕМА 5. *Для C -конечной группы $G_\Gamma = (G, Y)$ существует константа $T \in \mathbb{N}$ такая, что если элементы $s_1, s_2 \in S(G, Y)^G$ удовлетворяют следующим условиям:*

- (i) $\tau_i(s_1) \geq T$ для $i = 1, \dots, m$;
- (ii) $\alpha_G(s_1) = \alpha_G(s_2)$,

то $s_1 = s_2$.

ДОКАЗАТЕЛЬСТВО. Положим $\alpha = \alpha_G$ и прежде всего заметим, что если $\alpha(s_1) = \alpha(s_2)$, то $\tau_i(s_1) = \tau_i(s_2)$ для $i = 1, \dots, m$, так как $\tau_i(s_j) = \text{ab}_i(\alpha(s_j))$.

Обозначим через d_Γ диаметр графа Γ и, используя обозначения из п. 3.2, положим

$$T_1 = (d_\Gamma + 1) \max_{1 \leq i \leq m} n_i p_i + 1.$$

Покажем, что любое целое число $T \geq T_1$ удовлетворяет условиям теоремы 5. Действительно, пусть $\tau_i(s_1) \geq T_1$ для $i = 1, \dots, m$. Тогда согласно следствию 1 элементы s_1 и s_2 могут быть записаны в виде $s_1 = s_\Gamma^{d_\Gamma} \cdot s'_1$ и $s_2 = s_\Gamma^{d_\Gamma} \cdot s'_2$. Имеем

$$\alpha(s'_1) = \alpha(s_1)\alpha(s_\Gamma^{d_\Gamma})^{-1} = \alpha(s_2)\alpha(s_\Gamma^{d_\Gamma})^{-1} = \alpha(s'_2).$$

Следовательно, $s'_1 \sim s'_2$ согласно теореме 2, и поэтому $s_1 = s_2$ согласно теореме 3.

4.2. Случай оснащенных конечных групп. Пусть (G, O) – оснащенная группа, эквивалентная C -конечной группе G_Γ , $\beta_{(G, O)}: G_\Gamma \rightarrow (G, O)$ – естественный эпиморфизм оснащенных групп, $H = \ker \beta_{(G, O)}$, $a_{(G, O)} = |H \cap [G_\Gamma, G_\Gamma]|$ – индекс неоднозначности группы (G, O) и m – число связных компонент графа Γ .

ТЕОРЕМА 6. *Для каждой оснащенной конечной группы (G, O) существует константа $T = T_{(G, O)}$ такая, что если для элемента $s_1 \in S(G, O)^G$ его i -й тип $\tau_i(s_1) \geq T$ для всех $i = 1, \dots, m$, то существует $a_{(G, O)}$ элементов $s_1, \dots, s_{a_{(G, O)}} \in S(G, O)^G$ таких, что:*

- (i) $s_i \neq s_j$ при $1 \leq i < j \leq a_{(G, O)}$;
- (ii) $\tau(s_i) = \tau(s_1)$ при $1 \leq i \leq a_{(G, O)}$;
- (iii) $\alpha_G(s_i) = \alpha_G(s_1)$ при $1 \leq i \leq a_{(G, O)}$;
- (iv) если $s \in S(G, O)^G$ – такой элемент, что $\tau(s) = \tau(s_1)$ и $\alpha_G(s) = \alpha_G(s_1)$, то $s = s_i$ при некотором i , $1 \leq i \leq a_{(G, O)}$.

ДОКАЗАТЕЛЬСТВО. Согласно лемме 6 для $n \geq z_H$ каждый элемент $g_i \in H \cap [G_\Gamma, G_\Gamma]$ (где $g_1 = 1$) может быть представлен в виде $g_i = \alpha_{G_\Gamma}(s_{i,n})\alpha_{G_\Gamma}(s_\Gamma^n)^{-1}$, где $s_{i,n} \in S(G_\Gamma, Y) = S(G, O)$ (в частности, $s_{1,n} = s_\Gamma^n$). Имеем $s_{i,n} \neq s_{j,n}$ для $1 \leq i < j \leq a_{(G,O)}$, $\tau(s_{i,n}) = \tau(s_{1,n})$ и $\alpha_G(s_{i,n}) = \alpha_G(s_{1,n})$ для $1 \leq i \leq a_{(G,O)}$.

Положим $T_2 = (\max(d_\Gamma, z_H) + 1) \max_{1 \leq i \leq m} n_i p_i + 1$. Согласно следствию 1, если $T \geq T_2$, то элемент s_1 может быть записан в виде $s_1 = s_\Gamma^{z_H} \cdot s'_1$. Обозначим $s_i := s_{i,z_H}^{z_H} \cdot s'_1$. Легко видеть, что элементы $s_1, \dots, s_{a_{(G,O)}} \in S(G, O)^G$ удовлетворяют условиям (i)–(iii), и если $s \in S(G, O)^G$ – такой элемент, что $\tau(s) = \tau(s_1)$ и $\alpha_G(s) = \alpha_G(s_1)$, то $\alpha_\Gamma(s)\alpha_G(s_1)^{-1} \in H \cap [G_\Gamma, G_\Gamma]$, и поэтому согласно теореме 5 имеем равенство $s = s_i$ при некотором i , $1 \leq i \leq a_{(G,O)}$.

Пусть (G, O) – оснащенная группа, $O = C_1 \sqcup \dots \sqcup C_m$, где C_i – классы сопряженности группы G . Пусть при некотором $k < m$ элементы множества $O' = C_1 \sqcup \dots \sqcup C_k$ порождают группу G . Вложение $i: O' \hookrightarrow O$ определяет подграфы $\tilde{\Gamma}' \subset \Gamma' = \Gamma_1 \sqcup \dots \sqcup \Gamma_k$ C -графа $\Gamma_{(G,O)} = \Gamma$, где $\tilde{\Gamma}'$ – C -граф оснащенной группы (G, O') . Подграф Γ' является обильным, так как элементы из O' порождают группу G .

Пусть G_Γ и $G_{\tilde{\Gamma}'}$ – C -группы, эквивалентные соответственно оснащенным группам (G, O) и (G, O') , и пусть $S(G_\Gamma, Y)$ и $S(G_{\tilde{\Gamma}'}, Y')$ – их полугруппы разложений на множители. Вложение $i: O' \hookrightarrow O$ определяет гомоморфизм $i_*: G_{\tilde{\Gamma}'} \rightarrow G_\Gamma$ C -групп и вложение

$$i_*: S(G, O') \simeq S(G_{\tilde{\Gamma}'}, Y') \hookrightarrow S(G_\Gamma, Y) \simeq S(G, O)$$

полугрупп такие, что $i_*(\alpha_{G_{\tilde{\Gamma}'}}(s)) = \alpha_{G_\Gamma}(i_*(s))$ для всех $s \in S(G_{\tilde{\Gamma}'}, Y')$.

ТЕОРЕМА 7. Пусть G – конечная группа и $O' \subset O$ – два ее оснащения такие, что элементы из O' порождают группу G . Тогда в использованных выше обозначениях существует такая константа $T = T_{(O,O')}$, что если для элемента $s_1 \in S(G, O)^G$ его i -й тип $\tau_i(s_1) \geq T$ для всех $i = 1, \dots, k$, тогда существует не более чем $a_{(G,O')}$ элементов $s_1, \dots, s_n \in S(G, O)^G$ таких, что:

- (i) $s_i \neq s_j$ при $1 \leq i < j \leq n$;
- (ii) $\tau(s_i) = \tau(s_1)$ при $1 \leq i \leq n$;
- (iii) $\alpha_G(s_i) = \alpha_G(s_1)$ при $1 \leq i \leq n$,

где $a_{(G,O')}$ – индекс неоднозначности группы (G, O') .

ДОКАЗАТЕЛЬСТВО. Пусть $T_1 = 2d_{\Gamma'} \max_{1 \leq i \leq k} n_i p_i$, где $d_{\Gamma'}$ – диаметр графа Γ относительно обильного подграфа Γ' , p_i и n_i – соответственно период и число вершин связной компоненты Γ_i графа Γ и T_2 – константа, существование которой для оснащенной группы (G, O') утверждается в теореме 6. Положим $T = \max(T_1, T_2)$. Согласно предложению 4, если для $s \in S(G, Y)^G$ его i -й тип $\tau_i(s) \geq T$ для всех $i \leq k$, то s может быть записан в виде $s = (x_{v_{k+1,1}}^{a_{k+1}} \cdot \dots \cdot x_{v_{m,1}}^{a_m}) \cdot s_{\Gamma'}^d \cdot s_1$, где $a_i = \tau_i(s)$ при $i = k+1, \dots, m$ и $s_1 \in S(G, O')$. Теперь теорема 7 следует из теоремы 6, примененной к элементу $s_{\Gamma'}^d \cdot s_1 \in S(G, O')^G$.

4.3. Производящие функции. Для каждого $\bar{k} = (k_1, \dots, k_m) \in \mathbb{Z}_{\geq 0}^m$ обозначим через $h_{\bar{k}}$ число элементов $s \in S(G, O)_1^G$ с $\tau(s) = \bar{k}$ и сопоставим оснащенной группе (G, O) степенной ряд

$$\chi_{(G, O)}(t_1, \dots, t_m) := \sum_{\bar{k} \in \mathbb{Z}_{\geq 0}^m} h_{\bar{k}} t_1^{k_1} \dots t_m^{k_m}.$$

ПРЕДЛОЖЕНИЕ 8. Пусть G – конечная группа и C – ее класс сопряженности такой, что элементы из C порождают группу G . Тогда $\chi_{(G, C)}(t)$ является рациональной функцией.

ДОКАЗАТЕЛЬСТВО. Пусть p – период и n – число вершин графа $\Gamma_{(G, C)}$ и пусть $a = a_{(G, C)}$ – индекс неоднозначности группы (G, C) . Рассмотрим множество целых чисел

$$R = \{r \mid 0 \leq r \leq pn - 1 \text{ и } \exists i \equiv r \pmod{np} \text{ такой, что } h_i > 0\},$$

и пусть i_r – это наименьшее i , для которого $i \equiv r \pmod{np}$ и $h_i > 0$. Для каждого $r \in R$ выберем представитель $s_r \in S(G, C)_1^G$ длины $\ln(s_r) = i_r$ и выберем константу M такую, что $T = 2pnM > \max_{r \in R} i_r$ – это константа, существование которой доказано в теореме 6.

Запишем $\chi_{(G, C)}(t)$ в виде $\chi_{(G, C)}(t) = \chi_{<T}(t) + \chi_{\geq T}(t)$, где $\chi_{<T}(t) = \sum_{i=1}^{T-1} h_i t^i$. Заметим, что $\chi_{<T}(t)$ является многочленом. Ряд $\chi_{\geq T}(t)$ может быть записан в виде

$$\chi_{\geq T}(t) = \sum_{r \in R} \sum_{j=0}^{\infty} h_{r+T+jpn} t^{r+T+jpn}.$$

Согласно теореме 6 имеем $h_{r+T+jpn} = a$ для каждого $r \in R$ и каждого $j \geq 0$, следовательно,

$$\chi_{\geq T}(t) = at^T \sum_{r \in R} t^r \sum_{j=0}^{\infty} t^{jpn} = \frac{at^T}{1 - t^{pn}} \sum_{r \in R} t^r.$$

ПРИМЕР 2. Если $G = \Sigma_n$ – симметрическая группа и O – множество транспозиций, то согласно теореме Клебша–Гурвица $\chi_{(G, O)} = t^{2(n-1)}/(1 - t^2)$.

Обобщением предложения 8 является

ТЕОРЕМА 8. Пусть G – конечная группа и $O = C_1 \sqcup \dots \sqcup C_m$ – несвязное объединение ее классов сопряженности такое, что элементы каждого класса C_i порождают группу G . Тогда $\chi_{(G, O)}(t_1, \dots, t_m)$ является рациональной функцией.

ДОКАЗАТЕЛЬСТВО. Аналогично доказательству предложения 8. Надо заметить только, что если k_i является достаточно большим числом, то из леммы 3 и теоремы 7 следует, что

$$0 \leq h_{(k_1, \dots, k_{i-1}, k_i + p_i n_i, k_{i+1}, \dots, k_m)} \leq h_{(k_1, \dots, k_{i-1}, k_i, k_{i+1}, \dots, k_m)}.$$

ВОПРОС. Является ли $\chi_{(G, O)}(\bar{t})$ рациональной функцией для всякой оснащенной конечной группы (G, O) ?

§ 5. Вычисление индекса неоднозначности

5.1. Проблема слов для C -конечной группы. В этом пункте будет доказана

ТЕОРЕМА 9. *Проблема слов для C -конечных групп разрешима.*

ДОКАЗАТЕЛЬСТВО. Пусть $\Gamma = \Gamma_1 \sqcup \dots \sqcup \Gamma_m$ – C -граф C -конечной группы (G_Γ, Y) . Согласно утверждению 7, не ограничивая общности, мы можем предполагать, что для каждой связной компоненты Γ_i графа Γ период p_i ее вершин больше единицы.

Согласно предложению 3 применением соотношений C -группы, заданных C -графом Γ , любое слово, состоящее из элементов, принадлежащих множеству Y , может быть преобразовано в слово следующего вида:

$$w = c^{-1} y_{1,1}^{t_1} y_{2,1}^{t_2} \dots y_{m,1}^{t_m} \prod_{i=1}^m y_{i,1}^{k_i p_i} y_{i,1}^{a_{i,1}} y_{i,2}^{a_{i,2}} \dots y_{i,n_i}^{a_{i,n_i}}, \quad (13)$$

где c – канонический элемент группы G_Γ , n_i – число вершин графа Γ_i и целые числа k_i и $a_{i,j}$ удовлетворяют следующим соотношениям и неравенствам:

$$\sum_{j=1}^{n_i} a_{i,j} + k_i p_i = n_i p_i, \quad (14)$$

$$0 < a_{i,j} \leq p_i - 1, \quad 0 \leq k_i < n_i. \quad (15)$$

Если два слова w_1 и w_2 представляют один и тот же элемент $g \in G_\Gamma$, то $\text{ab}(w_1) = \text{ab}(w_2) = (t_1, \dots, t_m)$. Следовательно, чтобы доказать теорему, достаточно показать, что существует конечный алгоритм, разрешающий следующую проблему:

узнать, когда два слова

$$w_l = \prod_{i=1}^m y_{i,1}^{k_{i,l} p_i} y_{i,1}^{a_{i,1,l}} y_{i,2}^{a_{i,2,l}} \dots y_{i,n_i}^{a_{i,n_i,l}}, \quad l = 1, 2, \quad (16)$$

в которых целые числа $k_{i,l}$ и $a_{i,j,l}$ при фиксированном $l = 1, 2$ удовлетворяют соотношениям (14) и неравенствам (15), представляют один и тот же элемент группы G_Γ .

Отметим также, что слова

$$w_l c^{-1}, \quad l = 1, 2, \quad (17)$$

где w_l – слова вида (16) – представляют элементы, принадлежащие коммутатору $[G_\Gamma, G_\Gamma]$ группы G_Γ .

В дальнейшем, чтобы упростить обозначения, мы рассмотрим только случай, когда $m = 1$, так как общий случай аналогичен. Будем использовать следующие обозначения: $\Gamma = \Gamma_1$, $n := n_1$, $p := p_1$, $\{v_1, \dots, v_n\}$ – множество вершин графа Γ и y_i – C -порождающий элемент группы G_Γ , соответствующий вершине v_i . Обозначим через $\mathcal{R}_\Gamma$ множество соотношений в G_Γ , определяемых C -графом Γ (см. п. 2.1). Напомним, что для каждой упорядоченной пары

(l_1, l_2) такой, что $1 \leq l_1, l_2 \leq n$, существует единственный индекс l_3 (зависящий от (l_1, l_2)), $1 \leq l_3 \leq n$, такой, что

$$y_{l_1} y_{l_2} y_{l_1}^{-1} y_{l_3}^{-1} \in \mathcal{R}_\Gamma. \quad (18)$$

Рассмотрим оснащенную группу $(\bar{G} = G_\Gamma/H, O)$, где H – это подгруппа центра $Z(G_\Gamma)$ группы G_Γ , порожденная элементом $y_1^p = y_i^p, i = 1, \dots, n$. Обозначим через $f = f_{(G, O)}: G_\Gamma \rightarrow \bar{G}$ естественный эпиморфизм и через $f' = f|_{[G_\Gamma, G_\Gamma]}$ его ограничение на $[G_\Gamma, G_\Gamma]$. Группа $\bar{G}$ имеет следующее копредставление:

$$\bar{G} = \langle y_1, \dots, y_n \mid R(\bar{y}) = 1 \text{ для } R \in \mathcal{R}_\Gamma \text{ и } y_1^p = \dots = y_n^p = 1 \rangle.$$

Согласно лемме 5 имеем следующую коммутативную диаграмму, в которой f' является изоморфизмом, а f и f'' – эпиморфизмы:

$$\begin{array}{ccccccc} 1 & \longrightarrow & [G_\Gamma, G_\Gamma] & \longrightarrow & G & \xrightarrow{ab} & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow f' \simeq & & \downarrow f & & \downarrow f'' \\ 1 & \longrightarrow & [\bar{G}, \bar{G}] & \longrightarrow & \bar{G} & \xrightarrow{ab} & \mathbb{Z}/p\mathbb{Z} \longrightarrow 0 \end{array} \quad (*)$$

Из вышеизложенного и диаграммы $(*)$ следует, что каждый элемент $g \in \bar{G}$ может быть представлен словом вида

$$w = y_1^{a_1} y_2^{a_2} \dots y_n^{a_n}, \quad (19)$$

в котором каждое целое число a_j удовлетворяет неравенству

$$0 \leq a_j \leq p-1, \quad (20)$$

и поэтому

$$\sum_{j=1}^n a_j \leq n(p-1). \quad (21)$$

Обозначим через W_i множество положительных слов w , состоящих из элементов, принадлежащих множеству Y , длины которых $\ln(w)$ равны i (в частности, W_0 состоит из пустого слова), $W_{\leq k} = \bigcup_{i=0}^k W_i$, и пусть

$$\widetilde{W}_{\leq k} = \{w \in W_{\leq k} \mid \text{каждый элемент } y_j \in Y \text{ входит в } w \text{ меньше чем } p \text{ раз}\}.$$

Покажем, что существует конечный алгоритм распознавания, когда два слова $w_1, w_2 \in \widetilde{W}_{\leq n(p-1)}$ представляют один и тот же элемент группы $\bar{G}$. Прежде чем описать такой алгоритм, дадим несколько определений. Слово w называется *приведенным*, если не существует элементов $y_j \in Y$, входящих в w последовательно p раз. Если в слово w некоторый элемент $y_j \in Y$ входит последовательно p раз, т.е. $w = w' y_j^p w''$, то переход от слова w к слову $w_1 = w' w''$ называется *редукцией* слова w . Для каждого положительного слова w обозначим через $\bar{w}$ приведенное слово, которое получается из w с помощью редукций, и для каждого подмножества $V \subset W_{\leq 2n(p-1)}$ определим множество

$$\bar{V} = \{\tilde{w} \in \widetilde{W}_{\leq n(p-1)} \mid \exists w \in V \text{ такое, что } \tilde{w} = \bar{w}\}.$$

Пусть $\sigma_1, \dots, \sigma_{k-1}$ – множество артиновых порождающих элементов группы кос B_k . Определим действие группы B_k на множестве W_i следующим образом: если $i \neq k$, то это действие тривиально; если $i = k$, то для слова

$$w = y_{i_1} \dots y_{i_{j-1}} y_{i_j} y_{i_{j+1}} y_{i_{j+2}} \dots y_{i_k}$$

его образ $\sigma_j(w) = y_{i_1} \dots y_{i_{j-1}} y_{i'} y_{i_j} y_{i_{j+2}} \dots y_{i_k}$, где i' зависит от пары (i_j, i_{j+1}) и определяется соотношением (18), если положить $l_1 = i_j$, $l_2 = i_{j+1}$ и $i' = l_3$. Введем обозначение

$$B = B_0 \times B_1 \times \dots \times B_{2n(p-1)},$$

где B_0 и B_1 – тривиальные группы. Определенное выше действие групп B_k позволяет определить естественное действие группы B на множестве $W_{\leq 2n(p-1)} = \bigcup_{i=0}^{2n(p-1)} W_i$. Для каждого подмножества V множества $W_{\leq 2n(p-1)}$ обозначим через BV объединение орбит элементов из V при действии группы B .

Пусть N_1 – число слов в $\widetilde{W}_{\leq n(p-1)}$. Перенумеруем их, $w_1, \dots, w_{N_1}$, и рассмотрим каждое из них как подмножество множества $\widetilde{W}_{\leq n(p-1)}$ (обозначим эти подмножества через $\widetilde{V}_{j,1} = \{w_j\}$). Алгоритм, о котором идет речь, имеет следующее описание. Пусть в конце $(k-1)$ -го шага алгоритма мы получили представление множества $\widetilde{W}_{\leq n(p-1)}$ в виде объединения его подмножеств,

$$\widetilde{W}_{\leq n(p-1)} = \widetilde{V}_{1,k} \sqcup \dots \sqcup \widetilde{V}_{N_k,k}.$$

На k -м шаге алгоритма для каждой пары $(i, j) \in \{1, \dots, N_k\}^2$ строим подмножества

$$\widetilde{V}_{i,k} \widetilde{V}_{j,k} = \{w = w' w'' \mid w' \in \widetilde{V}_{i,k}, w'' \in \widetilde{V}_{j,k}\} \subset W_{\leq 2n(p-1)}$$

и строим множество их орбит $\{B(\widetilde{V}_{i,k} \widetilde{V}_{j,k})\}$. Определим отношение эквивалентности следующим образом: две орбиты $B(\widetilde{V}_{i_1,k} \widetilde{V}_{j_1,k})$ и $B(\widetilde{V}_{i_2,k} \widetilde{V}_{j_2,k})$ (соответственно $B(\widetilde{V}_{i_1,k} \widetilde{V}_{j_1,k})$ и $B(\widetilde{V}_{i_2,k} \widetilde{V}_{j_2,k})$) эквивалентны, если существует индекс j_0 (соответственно i_0) такой, что

$$B(\widetilde{V}_{i_1,k} \widetilde{V}_{j_0,k}) \cap B(\widetilde{V}_{i_2,k} \widetilde{V}_{j_0,k}) \neq \emptyset$$

(соответственно $B(\widetilde{V}_{i_0,k} \widetilde{V}_{j_1,k}) \cap B(\widetilde{V}_{i_0,k} \widetilde{V}_{j_2,k}) \neq \emptyset$), и для каждого класса эквивалентности мы объединяем подмножества $B(\widetilde{V}_{i,k} \widetilde{V}_{j,k})$, принадлежащие этому классу. Обозначим полученные подмножества через $V_{1,k}, \dots, V_{N_{k+1},k}$ и положим $\widetilde{V}_{i,k+1} := \overline{V}_{i,k}$.

Легко видеть, что $N_{k+1} \leq N_k$ и $\widetilde{V}_{1,k+1} \sqcup \dots \sqcup \widetilde{V}_{N_{k+1},k+1} = \widetilde{W}_{\leq n(p-1)}$. Алгоритм останавливается, если $N_{k+1} = N_k$. В этом случае два слова $w_l = y_1^{a_{1,l}} y_2^{a_{2,l}} \dots y_n^{a_{n,l}}$, $l = 1, 2$, удовлетворяющие неравенству (20) (в случае $m = 1$) представляют один и тот же элемент в группе $\overline{G}$ тогда и только тогда, когда w_1 и w_2 принадлежат одному и тому же подмножеству $\widetilde{V}_i := \widetilde{V}_{i,k+1}$ при некотором i . Чтобы показать это, введем структуру группы на множестве $\widetilde{G} = \{\widetilde{V}_i\}$. По определению произведением элементов V_i и V_j является

$$\widetilde{V}_i \widetilde{V}_j = \overline{B(\widetilde{V}_i \widetilde{V}_j)}.$$

Корректность этого произведения следует из построения подмножеств $\tilde{V}_i$, так как $N_{k+1} = N_k$. Единицей в $\tilde{G}$ является подмножество $\tilde{V}_{i_0}$, содержащее пустое слово, обратным элементом элемента $\tilde{V}_i$, содержащего слово $w = y_1^{a_1} y_2^{a_2} \dots y_n^{a_n}$, является подмножество $\tilde{V}_j$, содержащее редукцию слова $w = y_n^{p-a_n} y_{n-1}^{p-a_{n-1}} \dots y_1^{p-a_1}$. Перенумеруем подмножества $\tilde{V}_j$ так, что для $i = 1, \dots, n$ подмножество $\tilde{V}_i$ содержит слово y_i , и положим $\tilde{O} = \{\tilde{V}_1, \dots, \tilde{V}_n\}$. Тогда легко видеть, что множество $\tilde{O}$ инвариантно относительно внутренних автоморфизмов группы $\tilde{G}$ и C -граф оснащенной группы $(\tilde{G}, \tilde{O})$ совпадает с Γ . Более того, так как при построении элементов группы $\tilde{G}$ были использованы только соотношения из $\mathcal{R}_\Gamma$ и соотношения $y_1^p = \dots = y_n^p = 1$, то, очевидно, оснащенная группа $(\tilde{G}, \tilde{O})$ изоморфна оснащенной группе $(\bar{G}, \bar{O})$. Поэтому эпиморфизм $f_{(\tilde{G}, \tilde{O})}: [G_\Gamma, G_\Gamma] \rightarrow [\tilde{G}, \tilde{G}]$ совпадает с изоморфизмом $f': [G_\Gamma, G_\Gamma] \rightarrow [\bar{G}, \bar{G}]$, если мы отождествим оснащенные группы $(\tilde{G}, \tilde{O})$ и $(\bar{G}, \bar{O})$.

Окончательно, согласно предложению 3 и ввиду того, что слова вида (17) представляют элементы из $[G_\Gamma, G_\Gamma]$, два слова вида (16), удовлетворяющие соотношениям (14) и неравенствам (15), представляют один и тот же элемент в группе G_Γ , тогда и только тогда, когда редукции этих слов представляют один и тот же элемент группы $\tilde{G}$.

5.2. Вычисление индекса неоднозначности. Скажем, что оснащенная конечная группа (G, O) *эффективно задана*, если существует конечный алгоритм перечисления всех элементов группы G (например, если G задана своим графом Кэли или порождающие элементы группы G заданы как перестановки некоторой симметрической группы) и также задан представитель каждого класса сопряженности $C_i \subset O$.

ПРЕДЛОЖЕНИЕ 9. Для каждой эффективно определенной оснащенной конечной группы (G, O) существует конечный алгоритм вычисления ее индекса неоднозначности $a_{(G, O)}$.

ДОКАЗАТЕЛЬСТВО. Так как оснащенная группа (G, O) задана эффективно, то, очевидно, существует конечный алгоритм, полностью определяющий C -граф $\Gamma = \Gamma_{(G, O)}$.

Используя описание графа Γ , как и в доказательстве теоремы 9 перенумеруем подмножества $\tilde{V}_i$, содержащие редукции слов вида

$$w = \prod_{i=1}^m y_{i,1}^{k_i p_i} y_{i,1}^{a_{i,1}} y_{i,2}^{a_{i,2}} \dots y_{i,n_i}^{a_{i,n_i}}, \quad (22)$$

где целые числа k_i и $a_{i,j}$ удовлетворяют следующим соотношениям и неравенствам:

$$\sum_{j=1}^{n_i} a_{i,j} + k_i p_i = n_i p_i, \quad (23)$$

$$0 < a_{i,j} \leq p_i - 1, \quad 0 \leq k_i < n_i. \quad (24)$$

После этого для каждого i выберем слово w_i вида (22), редукция которого принадлежит множеству $\tilde{V}_i$, и проверим: представляет ли слово $c^{-1}w_i$ единицу в группе G , где c – канонический элемент группы G_Γ . Согласно предложению 3 число множеств $\tilde{V}_i$, для которых соответствующие элементы $c^{-1}w_i$ представляют единицу в G , равно индексу неоднозначности $a_{(G,O)}$.

Список литературы

- [1] W. Fulton, “Hurwitz schemes and irreducibility of moduli of algebraic curves”, *Ann. of Math.* (2), **90**:3 (1969), 542–575.
- [2] A. Clebsch, “Zur Theorie der Riemann’schen Fläche”, *Math. Ann.*, **6**:2 (1873), 216–230.
- [3] A. Hurwitz, “Ueber Riemann’sche Flächen mit gegebenen Verzweigungspunkten”, *Math. Ann.*, **39**:1 (1981), 1–60.
- [4] Вик. С. Куликов, “Полугруппы разложений на множители и неприводимые компоненты пространства Гурвица”, *Изв. РАН. Сер. матем.*, **75**:4 (2011), 49–90; англ. пер.: Vik. S. Kulikov, “Factorization semigroups and irreducible components of the Hurwitz space”, *Izv. Math.*, **75**:4 (2011), 711–748.
- [5] Вик. С. Куликов, “Полугруппы разложений на множители и неприводимые компоненты пространства Гурвица. II”, *Изв. РАН. Сер. матем.*, **76**:2 (2012), 151–160; англ. пер.: Vik. S. Kulikov, “Factorization semigroups and irreducible components of the Hurwitz space. II”, *Izv. Math.*, **76**:2 (2012), 356–364.
- [6] B. Wajnryb, “Orbits of Hurwitz action for coverings of a sphere with two special fibers”, *Indag. Math. (N.S.)*, **7**:4 (1996), 549–558.
- [7] Вик. С. Куликов, “Кривые Гурвица”, *УМН*, **62**:6 (2007), 3–86; англ. пер.: Vik. S. Kulikov, “Hurwitz curves”, *Russian Math. Surveys*, **62**:6 (2007), 1043–1119.
- [8] Р. Линдон, П. Шупп, *Комбинаторная теория групп*, Мир, М., 1980; пер. с англ.: R. C. Lyndon, P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin–Heidelberg–New York, 1977.
- [9] А. Ю. Ольшанский, *Геометрия определяющих соотношений в группах*, Мир, М., 1989; англ. пер.: A. Yu. Ol’shanskii, *Geometry of defining relations in groups*, Math. Appl. (Soviet Ser.), **70**, Kluwer Acad. Publ., Dordrecht, 1991.

Вик. С. Куликов (Vik. S. Kulikov)

Математический институт им. В. А. Стеклова РАН

E-mail: kulikov@mi.ras.ru

Поступила в редакцию

04.08.2011 и 30.10.2012