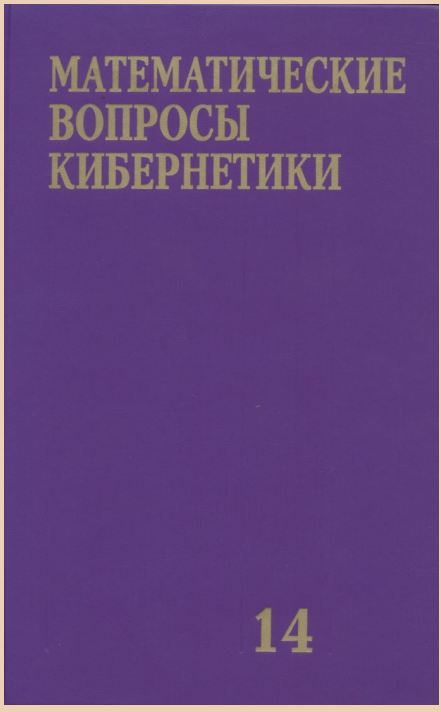
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 14



В. М. Фомичёв

Исследование признаков в конечных группах и группах подстановок

Рекомендуемая форма библиографической ссылки: Фомичёв В. М. Исследование признаков в конечных группах и группах подстановок // Математические вопросы кибернетики. Вып. 14. — М.: Физматлит, 2005. — С. 161–260. URL: http://library.keldysh.ru/mvk.asp?id=2005-161

ИССЛЕДОВАНИЕ ПРИЗНАКОВ В КОНЕЧНЫХ ГРУППАХ И В ГРУППАХ ПОДСТАНОВОК

В. М. ФОМИЧЁВ

(МОСКВА)

Оглавление

Основные обозначения

Обозначения величин и множеств

$[a]$ — целая часть действительного числа a;

N — множество натуральных чисел;

$N_0 = N \cup \{0\}$;

$N_n = \{1, \ldots, n\}$, где $n \in N$;

$D(n)$ — множество всех натуральных делителей числа n, где $n \in N$;

$НОК\{n_1, \ldots, n_m\}$ — наименьшее общее кратное натуральных чисел $n_1, \ldots, n_m$;

$НОД\{n_1, \ldots, n_m\}$ — наибольший общий делитель натуральных чисел $n_1, \ldots, n_m$;

(n, m) — наибольший общий делитель двух натуральных чисел n и m;

$|X|$ — порядок конечного множества X;

X^n — декартова n-я степень множества X, где $n \in N$;

2^X — булеан (множество всех подмножеств) множества X;

V_n — множество n-мерных двоичных векторов, где $n \in N$;

$F(Y', Y)$ — класс функций, определённых на множестве Y' и принимающих значения во множестве Y;

$\Gamma(V, U)$ — граф (или ориентированный граф) с множеством вершин V и множеством рёбер (дуг) U;

$\rho_\Gamma(i, j)$ — длина кратчайшего пути из вершины i в вершину j в графе Γ (или ориентированном графе Γ);

$\omega_i(\Gamma)$ — длина кратчайшего цикла в графе Γ, содержащего вершину i;

$\omega(\Gamma)$ — обхват (длина кратчайшего цикла) сильно связного орграфа Γ;

e — нейтральный элемент группы;

g^{-1} — элемент группы, обратный к элементу g;

ord g — порядок элемента g группы;
ord G — порядок конечной группы G;
$\langle g \rangle$ — циклическая группа, порождённая элементом g;
$|G\colon G'|$ — индекс подгруппы G' в конечной группе G.

Обозначения отношений и специальные значки

m/n — натуральное число m делит натуральное число n без остатка;
$x \leqslant y$ — бинарное отношение $\leqslant$ на некотором множестве;
$x \overset{\pi}{\cong} y$ — элементы x и y эквивалентны по отношению π;
$G' < G$ — группа G' есть подгруппа группы G;
$\square$ — завершение доказательства утверждения (леммы, теоремы);
$\diamondsuit$ — завершение формулировок определений, замечаний, примеров, а также утверждений и теорем, приведённых в работе без доказательства.

Введение

Теория групп, активно развиваясь уже третье столетие, нашла немало глубоких применений в различных естественных науках, прежде всего, в различных отраслях математики и физики [15]. В частности, в криптологии особый интерес к изучению групп объясняется тем, что шифрующие отображения являются, как правило, подстановками, и «качество» шифрования определяется многочисленными свойствами шифрующих подстановок.

Группы, как правило, неоднородны по составу, т. е. содержат особые элементы, свойства, которых отличаются от свойств остальных элементов. Например, группа может содержать элементы, порядки которых сильно различаются. Группа преобразований n-мерного векторного пространства над некоторым полем может содержать как нелинейные, так и аффинные преобразования, свойства которых существенно различаются с точки зрения некоторых прикладных задач. Многие методы исследований в теории групп основаны на дифференциации групп и их элементов по определённым признакам (свойствам) и использовании этой дифференциации при дальнейшем групповом анализе, классификации или в приложениях.

Данная работа посвящена разработке вопросов дифференциации конечных групп (элементов групп) по характеристикам их подмножеств с заданными признаками (по принадлежности элементов подмножеству группы с заданными признаками). Общность предлагаемого подхода позволяет рассматривать подмножество группы с произвольным заданным признаком.

Работа состоит из введения, трёх глав и заключения.

В первой главе разрабатывается общий подход к исследованию подмножества конечной группы G, обладающего определённым признаком H. Сформулированы задачи исследования признака H в группе G, направленные на описание соответствующего подмножества $G \cap H$ группы и определение различных характеристик этого подмножества. Развивается соответствующий математический аппарат для исследования признаков в конечной группе.

Особый интерес представляет изучение признаков в конечной группе $\langle S \rangle$, заданной системой образующих S. В этом случае в качестве меры сложности порождения элементов из определённого подмножества H рассматривается кратчайшая из длин элементов множества H в системе образующих S. Эта величина (обозначаемая $\mathrm{pok}_S H$ и названная показателем множества H в системе образующих S) совпадает с наименьшим номером слоя группы $\langle S \rangle$, содержащего элементы с признаком H.

При исследовании признаков использовано представление группы как квазиупорядоченного множества, где $g \leqslant g'$ для элементов g и g' группы, если $\langle g \rangle < \langle g' \rangle$. Такое представление позволяет рассматривать наследственное

подмножество $G \cap H$ группы G как наследственный признак H, который имеется в группе G тогда, когда свойства любого элемента $g \in H$ наследуются всеми элементами циклической группы $\langle g \rangle$. Исследован и важный частный случай наследственного признака — групповой признак H, имеющийся в группе G, когда подмножество $G \cap H$ образует группу.

Установлена и использована при исследованиях связь между классом наследственных признаков в конечной группе и классом монотонных и антимонотонных функций, заданных на группе.

Метод исследования ряда характеристик наследственного признака H в группе G основан на представлении группы G в виде несократимого объединения циклических подгрупп [7, гл. II, § 1]. Показано, что определение некоторых характеристик наследственного признака H в группе сводится к нескольким менее сложным задачам определения соответствующих характеристик признака H в циклических подгруппах группы G.

Исследован наследственный признак H в циклической группе $\langle g \rangle$ порядка n. Описание подмножества $\langle g \rangle \cap H$ равносильно описанию системы элементов $g^{t_1}, \ldots, g^{t_r}$ группы $\langle g \rangle$, которые порождают минимальную систему циклических подгрупп, покрывающих множество $\langle g \rangle \cap H$. Эта задача сводится к числовой задаче определения соответствующего подмножества $\{t_1, \ldots, t_r\}$ множества чисел $\{1, \ldots, n\}$.

Во второй главе исследован ряд наследственных признаков в группах подстановок множества X, которые описываются с помощью монотонных и антимонотонных функций, заданных на группе подстановок.

Выделены три класса функций, значения которых на подстановке g однозначно определены соответственно:

1) разбиением множества X на подмножества, образующие циклы подстановки g;

2) цикловой структурой подстановки g;

3) множеством всех различных длин циклов подстановки g.

Характеристики рассмотренных наследственных признаков в циклической группе подстановок $\langle g \rangle$ выражены в зависимости от подходящей функции соответственно либо через характеристики разбиения множества X на циклы подстановки g, либо через характеристики цикловой структурой подстановки g, либо через характеристики множества всех различных длин циклов подстановки g. Рассмотрены вопросы вычислительной сложности определения характеристик некоторых признаков в циклической группе подстановок.

Исследованы также некоторые наследственные признаки в группе подстановок множества X, когда X является аддитивной группой. Установлены теоретико-множественные связи между изученными наследственными признаками.

В главе III результаты предыдущей главы использованы для исследования группового линейного и группового аффинного признаков в группе G подстановок векторного пространства над конечным полем. Установлено, что линейная подгруппа группы G включена в пересечение четырёх наследственных подмножеств группы G, а аффинная подгруппа включена в пересечение двух наследственных подмножеств группы G, определяемых конкретными наследственными признаками. Описание этих признаков в группе G (или лишь некоторых из них) позволяет во многих случаях существенно сузить поиск линейной и аффинной подгрупп группы G, а в ряде случаев — доказать их тривиальность.

В заключительном разделе работы представлены основные результаты и сформулированы некоторые перспективные задачи исследования признаков в конечных группах.

Исследование признаков в конечных группах является новым направлением в теории групп. Вместе с тем, к этому направлению следует отнести некоторые ранее полученные результаты более частного характера. Ещё в начале 70-х годов В. А. Башев доказал, что показатель линейности любой подстановки g векторного пространства над конечным полем (т. е. наименьшее натуральное t, при котором подстановка g^t линейна) является делителем числа $\operatorname{ord} g$. Этот результат, инициировавший в определённой мере исследования автора, обобщен в теореме 1.2 для элемента g произвольной конечной группы G и произвольного группового признака в группе G.

В работе использована двойная нумерация определений, формул, теорем и пр., первый номер указывает на номер главы, второй является порядковым в главе. Для наглядности изложение материала сопровождается рядом примеров.

ГЛАВА I
ИССЛЕДОВАНИЕ ПРИЗНАКОВ В КОНЕЧНЫХ ГРУППАХ

§ 1.1. Основные понятия и определяющие свойства признаков в конечных группах

1.1.1. Основные понятия и исследовательские задачи, связанные с изучением признаков в конечных группах. Пусть Φ — конечная группа и $G = \langle S \rangle$ — её подгруппа, порожденная системой образующих $S = \{s_1, \ldots, s_p\}$, $S \subset \Phi$, $p = |S| > 0$. Как известно, группа G состоит из всех элементов g вида:

$$g = s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_t}, \tag{1.1}$$

где $i_1, \ldots, i_t \in \{1, \ldots, p\}$, t — натуральное число.

Представление элемента g словами в алфавите S в общем случае неоднозначно, и для многих приложений интересны представляющие слова возможно меньшей длины. Заметим, что длина t кратчайшего слова в алфавите S, используемого для представления любого элемента g группы G, не превосходит порядка группы G.

Дадим некоторые определения, связанные с порождением элементов группы Φ в системе образующих S.

Определение 1.1 [5]. *Длиной элемента* g конечной группы Φ в системе образующих S, обозначаемой $L(g, S)$, называется длина кратчайшего из слов в алфавите S, представляющих элемент g. Если $g \in \Phi \setminus G$, то положим $L(g, S) = \infty$. $\diamondsuit$

Таким образом, если правая часть равенства (1.1) есть слово кратчайшей длины в алфавите S, представляющее элемент g, то $L(g, S) = t$.

Определение 1.2 [5]. Для непустого подмножества $Q \subseteq \Phi$ его *длиной* (или *длиной покрытия*) *в системе образующих* S (обозначается $L(Q, S)$) называют наибольшую из длин всех элементов множества Q

$$L(Q, S) = \max_{g \in Q} L(g, S). \ \diamondsuit$$

Из определения 1.2 следует:

1) если $Q \setminus G \neq \varnothing$, то $L(Q, S) = \infty$;

2) если $Q' \subseteq Q$, то $L(Q', S) \leqslant L(Q, S)$.

Определение 1.3. Для непустого подмножества $Q \subseteq \Phi$ его *показателем в системе образующих* S (обозначается $\operatorname{pok}_S Q$) назовём

наименьшую из длин всех элементов множества Q в системе образующих S, т. е.

$$\operatorname{pok}_S Q = \min_{g \in Q} L(g, S). \diamondsuit$$

Для одноэлементной системы образующих $S = \{s\}$ показатель множества Q в системе $\{s\}$ (обозначается $\operatorname{pok}_s Q$) есть наименьшее натуральное t такое, что $s^t \in Q$. Если $Q \cap G = \varnothing$, то $\operatorname{pok}_S Q = \infty$.

Рассмотрим подмножества Q и H группы Ф, где H — множество элементов, обладающих определённым признаком (*attribute*), набором свойств.

Определение 1.4. Будем говорить, что *множество* Q (*элемент* g *множества* Q) *имеет* H*-признак* или *во множестве* Q *имеется* H*-признак*, если $Q \cap H \neq \varnothing$ ($g \in H$). Назовём H-признак *тривиальным* (*нетривиальным*), если $Q \cap H$ — одноэлементное множество (содержит более одного элемента). *Множество* Q *не имеет* H*-признака* или *множество* Q *имеет пустой* H*-признак*, если $Q \cap H = \varnothing$. $\diamondsuit$

В частности, если Q и H — подгруппы группы Ф, то группа Q имеет, по меньшей мере, тривиальный H-признак, так как группа $Q \cap H$ содержит единичный элемент e. В этом случае H-признак группы Q нетривиален (тривиален) тогда и только тогда, когда нетривиальна (тривиальна) группа $Q \cap H$.

Определение 1.5. Если множество Q имеет H-признак, то *показателем* H*-признака множества* Q (или H*-показателем множества* Q) *в системе образующих* S назовём показатель множества $Q \cap H$ в системе образующих S, т. е. $\operatorname{pok}_S(Q \cap H)$. $\diamondsuit$

Из определений 1.2 и 1.5 следует, что

$$\operatorname{pok}_S(Q \cap H) \leqslant L(Q \cap H, S).$$

Для одноэлементной системы образующих $S = \{s\}$ H-показатель множества Q в системе $\{s\}$ есть $\operatorname{pok}_s(Q \cap H)$.

Далее рассматриваются (за исключением особо оговорённых случаев) свойства группы G, порождённой системой образующих S, поэтому считаем, что $Q \subseteq G$. В этом случае длины всех элементов подмножества Q в системе образующих S конечны.

Кроме того, из определений 1.3–1.5 следует, что в случае $Q \subseteq G$ множество Q имеет H-признак тогда и только тогда, когда группа G имеет $Q \cap H$-признак. Поэтому достаточно рассматривать признаки лишь в группе G, пользуясь обозначением $\operatorname{pok}_S H$ или $\operatorname{pok}_s H$ для показателя H-признака.

В связи с данными определениями сформулируем несколько важных задач исследования строения группы G, связанных с распознаванием элементов заданного множества H в группе G, а также с оценкой сложности порождения элементов множества H в системе образующих S.

1. Для заданной системы образующих S и заданного множества H распознавание наличия H-признака в G и описание множества $G \cap H$. Определение условий тривиальности H-признака в группе G.

2. При наличии H-признака в группе G определение показателя H-признака в группе G и доли элементов множества $G \cap H$ в группе G и её подгруппах.

3. Для заданного множества H исследование зависимости величины $\operatorname{pok}_S H$ от выбора системы S образующих элементов (от свойств группы G).

Если H-признак в группе G тривиален, т. е. $G \cap H = \{g\}$, то задача определения показателя H-признака в группе G сводится к определению величины $L(g, S)$.

Подмножество S^r группы G (т. е. множество всех элементов группы G, представимых словами длины r в алфавите S,) называют её r-м слоем [5], $r = 1, 2, \ldots$ Для приложений представляет интерес изучение H-признака в r-м слое группы G.

Многие из представленных задач допускают более глубокую вероятностную формулировку, если определить вероятностную меру на множестве элементов группы G.

Многообразие данных задач определяется многообразием выбора группы G, а также множеств H и S.

1.1.2. Определяющие свойства признаков в конечной группе. Установим важные свойства и взаимосвязи характеристик признаков подмножеств конечной группы.

Утверждение 1.1. а) *Если $Q \subseteq G$ и множество Q имеет H-признак, то группа G имеет H-признак и*

$$\mathrm{pok}_S H \leqslant \mathrm{pok}_S(Q \cap H).$$

б) *Если $H' \subseteq H$ и группа G имеет H'-признак, то группа G имеет H-признак и*

$$\mathrm{pok}_S H \leqslant \mathrm{pok}_S H'.$$

в) *Если $S \subseteq S'$, то для любого непустого подмножества Q группы G*

$$\mathrm{pok}_{S'} Q \leqslant \mathrm{pok}_S Q.$$

Вследствие этого, если группа G имеет H-признак, то

$$\mathrm{pok}_{S'} H \leqslant \mathrm{pok}_S H.$$

Доказательство. а) Так как $Q \subseteq G$, то $Q \cap H \subseteq G \cap H$ и

$$\min_{g \in G \cap H} L(g, S) \leqslant \min_{g \in Q \cap H} L(g, S).$$

Отсюда по определению 1.5 получаем, что $\mathrm{pok}_S H \leqslant \mathrm{pok}_S(Q \cap H)$.

б) Так как $H' \subseteq H$, то $G \cap H' \subseteq G \cap H$ и

$$\min_{g \in G \cap H} L(g, S) \leqslant \min_{g \in G \cap H'} L(g, S).$$

Отсюда по определению 1.5 получаем, что $\mathrm{pok}_S H \leqslant \mathrm{pok}_S H'$.

в) Так как $G < \langle S' \rangle$, то всякий элемент g группы G представляется словом как в алфавите S, так и в алфавите S'. При этом кратчайшее слово в алфавите S, представляющее элемент g, в силу включения $S \subseteq S'$ есть одно из слов, представляющих g в алфавите S'. Значит, $L(g, S') \leqslant L(g, S)$ для любого $g \in G$. Следовательно, для любого непустого подмножества Q группы G

$$\min_{g \in Q} L(g, S') \leqslant \min_{g \in Q} L(g, S),$$

т. е. $\mathrm{pok}_{S'} Q \leqslant \mathrm{pok}_S Q$.

Отсюда следует, что если группа G имеет H-признак, т. е. $G \cap H \neq \varnothing$, то $\mathrm{pok}_{S'}(G \cap H) \leqslant \mathrm{pok}_S(G \cap H)$. Данное неравенство равносильно неравенству $\mathrm{pok}_{S'} H \leqslant \mathrm{pok}_S H$. □

Утверждение 1.2. *Пусть группа G и её циклические подгруппы $\langle s_1 \rangle, \ldots, \langle s_r \rangle$ имеют H-признак, $1 \leqslant r \leqslant p$. Тогда*

$$\mathrm{pok}_S H \leqslant \min\{\mathrm{pok}_{s_1} H, \ldots, \mathrm{pok}_{s_r} H\}.$$

Доказательство. Так как $s_i \in S$, то в данных условиях получаем по утверждению 1.1,в):

$$\mathrm{pok}_S(\langle s_i\rangle \cap H) \leqslant \mathrm{pok}_{s_i}(\langle s_i\rangle \cap H).$$

где $\mathrm{pok}_{s_i}(\langle s_i\rangle \cap H) = \mathrm{pok}_{s_i}(\langle s_i\rangle \cap H)$ и по утверждению 1.1,а)

$$\mathrm{pok}_S H \leqslant \mathrm{pok}_S(\langle s_i\rangle \cap H),\ i = 1, \ldots, r.$$

Значит, $\mathrm{pok}_S H \leqslant \mathrm{pok}_{s_i}(\langle s_i\rangle \cap H)$, $i = 1, \ldots, r$. Так как последнее неравенство верно для всех $i = 1, \ldots, r$, отсюда получаем требуемое неравенство. □

Следствие. *В условиях утверждения* 1.2

$$\mathrm{pok}_S H \leqslant \min\{\mathrm{ord}\, s_1, \ldots, \mathrm{ord}\, s_r\}.$$

Доказательство. По определению $\mathrm{pok}_{s_i}(\langle s_i\rangle \cap H)$ есть наименьшее натуральное число $t \in \{1, \ldots, \mathrm{ord}\, s_i\}$ такое, что $(s_i)^t \in H$. Значит, $\mathrm{pok}_{s_i}(\langle s_i\rangle \cap H) \leqslant \mathrm{ord}\, s_i$, $i = 1, \ldots, r$. Отсюда и из утверждения 1.2 следует требуемое неравенство. □

Утверждение 1.3. *Если* $\varphi\colon \Phi \to \Phi'$ *— гомоморфизм групп и группа* G *имеет* H*-признак, то группа* $\varphi(G)$ *имеет* $\varphi(H)$*-признак и*

$$\mathrm{pok}_S H \geqslant \mathrm{pok}_{\varphi(S)}\, \varphi(H).$$

Если φ *— изоморфизм, то* $\mathrm{pok}_S H = \mathrm{pok}_{\varphi(S)}\, \varphi(H)$.

Доказательство. Пусть $\mathrm{pok}_S H = t$. Тогда во множестве H найдётся элемент g такой, что $L(g, S) = t$, и не найдётся элементов меньшей длины. Значит, элемент g можно представить словом длины t в системе образующих S:

$$g = s_{i_1} \cdot \ldots \cdot s_{i_t},\ i_1, \ldots, i_t \in \{1, \ldots, p\}.$$

По свойствам гомоморфизма φ [6, теорема 1, глава X] множество $\varphi(G)$ есть группа, содержащая, в частности, элемент $\varphi(g)$, где $\varphi(g) \in \varphi(H)$ и

$$\varphi(g) = \varphi(s_{i_1}) \cdot \ldots \cdot \varphi(s_{i_t}).$$

Так как $\varphi(s_{i_j}) \in \varphi(S)$, $j = 1, \ldots, t$, последнее равенство означает, что $L(\varphi(g), \varphi(S)) \leqslant t$. Следовательно, $\mathrm{pok}_{\varphi(S)}\, \varphi(H) \leqslant t$.

Пусть φ — изоморфизм и $\mathrm{pok}_{\varphi(S)}\, \varphi(H) = l$, где $l \leqslant t$. Тогда во множестве $\varphi(H)$ найдётся элемент g' длины l в системе образующих $\varphi(S)$. Значит, элемент $\varphi^{-1}(g')$ множества H можно записать словом длины l в алфавите S. При $l < t$ имеем противоречие с определением числа t. Следовательно, $l = t$. □

1.1.3. О связи показателя H-признака в конечной группе с характеристиками некоторых графов и матриц. Показатель H-признака в конечной группе G можно изучать с помощью графа Кэли этой группы [8, 14] и матрицы смежности вершин этого графа.

Графом Кэли Γ_S группы $\langle S\rangle$, построенным по системе образующих S, называют ориентированный граф с множеством вершин G, в котором пара элементов (g, g') группы G образует дугу, помеченную элементом s, где $s \in S$, тогда и только тогда, когда $g \cdot s = g'$.

Следовательно, длина $L(g, S)$ (в системе образующих S) элемента g группы G есть длина кратчайшего пути в графе Γ_S из вершины e в вершину g.

Если группа G имеет H-признак, то $\mathrm{pok}_S H$ есть наименьшая из длин кратчайших путей в графе Γ_S из вершины e в вершины множества $G \cap H$. Отсюда следует, в частности, что показатель H-признака оценивается сверху диаметром графа Кэли:

$$\mathrm{pok}_S H \leqslant \mathrm{Diam}(\Gamma_S),$$

где $\mathrm{Diam}(\Gamma_S)$ — диаметр графа Γ_S.

Заметим, что для любого сильно связного n-вершинного орграфа Γ верна оценка диаметра [1, с. 139]

$$\mathrm{Diam}(\Gamma) \leqslant n,$$

и в случае графа Γ_S она улучшена для многих систем образующих S. Например, если $\mathrm{ord}\, G = n$, $1 < p \leqslant [n/3]$, и система S не содержит элемента e, инволюций и взаимно обратных элементов, то из оценки теоремы 3 [10] следует, что

$$\mathrm{Diam}(\Gamma_S) \leqslant \left[\frac{5}{2} \cdot \left[\frac{n}{p+1}\right] - \frac{1}{2}\right].$$

Теперь получим точное выражение величины $\mathrm{pok}_S H$ через характеристики матрицы M_S смежности вершин графа Γ_S.

Через M_S^t обозначим t-ю степень матрицы M_S, $t = 1, 2, \ldots$. Положим, что строки и столбцы матриц M_S^t «занумерованы» элементами группы G. Для непустых подмножеств Q и Q' группы G через $M_S^t(Q, Q')$ обозначим подматрицу матрицы M_S^t размера $|Q| \times |Q'|$, полученную удалением из M_S^t всех строк и столбцов с номерами из множеств $G \setminus Q$ и $G \setminus Q'$ соответственно.

Утверждение 1.4. *Если группа G имеет H-признак, то $\mathrm{pok}_S H$ есть наименьшее натуральное t, при котором матрица*

$$M_S^t(\{e\}, G \cap H)$$

отлична от нулевой.

Доказательство. Пусть $m_{h,g}^t$ есть элемент матрицы M_S^t, расположенный в g-й строке и h-м столбце, где $g, h \in G$. Известно, что $m_{h,g}^t$ есть число путей длины t в графе Γ_S из вершины h в вершину g. Поэтому матрица $M_S^t(\{e\}, G \cap H)$ отлична от нулевой тогда и только тогда, когда в графе Γ_S имеется путь длины t из вершины e в одну из вершин g множества H.

Следовательно, если t — наименьшее натуральное число, при котором матрица $M_S^t(\{e\}, G \cap H)$ отлична от нулевой, то в множестве $G \cap H$ имеется элемент g, для которого $L(g, S) = t$, и длина всех остальных элементов множества $G \cap H$ в системе образующих S не меньше t, т. е. не меньше длины элемента g в системе образующих S. □

Отметим, что определение величины $\mathrm{pok}_S H$ с помощью вычисления матриц M_S^t, $t = 1, 2, \ldots$, можно реализовать практически для групп G небольшого порядка.

§ 1.2. Свойства групповых и наследственных признаков в конечных группах

Исследуем зависимость характеристик H-признака в группе G от алгебраических свойств множества H. Рассмотрим характеристики H-признака в двух случаях: когда H — подгруппа группы Ф и когда H — объединение циклических подгрупп группы Ф.

1.2.1. Исследование свойств групповых признаков.

Определение 1.6. Если $G \cap H < G$, то H-признак в группе G назовём *групповым признаком.* ◇

Замечание 1. В группе G имеется групповой H-признак, если, в частности, $H < \Phi$.

Замечание 2. Если групповой H-признак тривиален в группе G, то $G \cap H = \{e\}$ и, следовательно, $\mathrm{pok}_S H = L(e, S)$.

Оценим в теоретико-графовых и групповых характеристиках величину $\mathrm{pok}_S H$ в случае, когда группа G имеет групповой H-признак.

Определение 1.7. *В графе* $\Gamma(V, U)$ с множеством вершин V и множеством дуг U *наименьшим разбросом подмножества* W множества V назовём число

$$\sigma_\Gamma(W) = \min_{i, j \in W} \rho_\Gamma(i, j),$$

где $\rho_\Gamma(i, j)$ — длина кратчайшего пути из вершины i в вершину j в графе $\Gamma(V, U)$. ◇

Теорема 1.1. *Если группа G имеет групповой H-признак, то:*

а) $\mathrm{pok}_S H = \sigma_{\Gamma_S}(G \cap H)$;

б) $\mathrm{pok}_S H \leqslant |G : (G \cap H)|$.

Доказательство. а) Пусть $\sigma_{\Gamma_S}(G \cap H) = t$. Тогда $\rho_{\Gamma_S}(h', h) \geqslant t$ для любых элементов h' и h группы $G \cap H$, и найдутся элементы $g', g \in G \cap H$, не обязательно различные, для которых $\rho_{\Gamma_S}(g', g) = t$. Отсюда по определению графа Γ_S следует, что в алфавите S имеется слово длины t, представляющее элемент g'', где $g'' = (g')^{-1} \cdot g$. Значит, $L(g'', S) \leqslant t$.

Так как $G \cap H$ — группа, то $g'' \in G \cap H$. Следовательно, неравенство $L(g'', S) \leqslant t$ означает, что $\mathrm{pok}_S H \leqslant t$.

Если $\mathrm{pok}_S H < t$, то в группе $G \cap H$ имеется элемент g, длина которого $L(g, S)$ меньше t. Возьмём элемент $g' \in G \cap H$, тогда $g' \cdot g \in G \cap H$ и $\rho_{\Gamma_S}(g', g' \cdot g) < t$ по определению графа Γ_S. Отсюда $\sigma_{\Gamma_S}(G \cap H) < t$, что противоречит исходному предположению.

б) Пусть $\mathrm{ord}\, G = n$, $\mathrm{ord}(G \cap H) = m$, где по теореме Лагранжа m/n.

Орграф Γ_S есть псевдосимметрический граф порядка p. Следовательно, граф Γ_S является эйлеровым, так как он сильно связен и все его вершины равновесны [9, теорема 3, раздел 4].

Эйлеров цикл C графа Γ_S имеет длину $n \cdot p$. Представим цикл C как последовательность $V = (v_0, v_1, \ldots, v_{n \cdot p - 1}, v_{n \cdot p})$ вершин графа Γ_S (элементов группы G), где $v_{n \cdot p} = v_0$. Последовательности V соответствует последовательность $\varphi(V) = (s_{i_1}, s_{i_2}, \ldots, s_{i_{n \cdot p}})$ дуг графа Γ_S (символов алфавита S), $i_1, i_2, \ldots, i_{n \cdot p} \in \{1, 2, \ldots, p\}$, образующая тот же цикл C и построенная для всех $t = 0, 1, \ldots, n \cdot p - 1$ по правилу:

$$\varphi(v_t, v_{t+1}) = s_{i_{t+1}}.$$

Распространим соответствие φ с множества пар соседних вершин последовательности V на множество всех различных неупорядоченных пар

вершин последовательности V. Пусть $j, k \in \{0, 1, \ldots, n \cdot p\}$, $j < k$, тогда

$$\varphi(v_j, v_k) = \prod_{i=j}^{k-1} \varphi(v_i, v_{i+1}) = s_{i_{j+1}} \cdot s_{i_{j+2}} \cdot \ldots \cdot s_{i_k}.$$

По определению графа Кэли Γ_S вершина v_j последовательности V связана с вершиной v_0 выражением $v_j = v_0 \cdot s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_j}$, $j = 1, 2, \ldots, n \cdot p$, поэтому из последнего равенства получаем, что

$$\varphi(v_j, v_k) = s_{i_{j+1}} \cdot s_{i_{j+2}} \cdot \ldots \cdot s_{i_k} = (v_j)^{-1} \cdot v_k.$$

Следовательно, если $v_j, v_k \in G \cap H$, то и $\varphi(v_j, v_k) \in G \cap H$, так как $G \cap H$ есть группа. Это означает, что между любыми двумя вершинами эйлерова цикла, соответствующими элементам группы $G \cap H$, содержится отрезок последовательности $\varphi(V)$, произведение элементов которого есть также элемент группы $G \cap H$.

Каждый элемент группы G соответствует p вершинам цикла C, поэтому все элементы группы G (группы $G \cap H$) соответствуют $n \cdot p$ вершинам ($m \cdot p$ вершинам) цикла C. Следовательно, $m \cdot p$ вершин эйлерова цикла, принадлежащие группе $G \cap H$, разбивают последовательность дуг $\varphi(V)$ на $m \cdot p$ отрезков, каждый из которых есть слово в алфавите S, представляющее некоторый элемент группы $G \cap H$. При этом суммарная длина всех слов данного разбиения равна $n \cdot p$. Отсюда получаем, что длина кратчайшего из указанных слов не превосходит $\frac{n}{m}$. □

Оценка теоремы 1.1,б) достигается на классе циклических групп.

Теорема 1.2. *Для группового H-признака в циклической группе $\langle g \rangle$*

$$\operatorname{pok}_g H = |\langle g \rangle : (\langle g \rangle \cap H)|.$$

Доказательство. Группа $\langle g \rangle$ состоит из элементов $g, g^2, \ldots, g^{n-1}, g^n = e$, где $n = \operatorname{ord} g$. По определению $\operatorname{pok}_g H$ есть наименьшее натуральное число t, $t \leqslant n$, при котором $g^t \in H$. Разделим n на t с остатком: $n = k \cdot t + r$, где $0 \leqslant r < t$. Отсюда получаем, что $e = g^n = (g^t)^k \cdot g^r$. Следовательно, $g^r = (g^t)^{-k}$. Так как $\langle g \rangle \cap H$ — группа, то отсюда и из включения $g^t \in \langle g \rangle \cap H$ следует включение $g^r \in \langle g \rangle \cap H$. При $r > 0$ имеем противоречие с определением числа t, т. е. t/n.

Так как $g^t \in \langle g \rangle \cap H$, то циклическая группа $\langle g^t \rangle$ есть подгруппа группы $\langle g \rangle \cap H$. Если $\langle g \rangle \cap H \neq \langle g^t \rangle$, то в $\langle g \rangle \cap H$ найдётся элемент g^m со свойством: $m = k \cdot t + r$, где $0 < r < t$. Значит, $g^m = (g^t)^k \cdot g^r$, откуда следует: $g^r = (g^t)^{-k} \cdot g^m$. Значит, $g^r \in \langle g \rangle \cap H$, так как элементы g^r и g^t принадлежат группе $\langle g \rangle \cap H$. Имеем противоречие с определением числа t. □

Следствие. *Циклическая группа $\langle g \rangle$ простого порядка имеет тривиальный групповой H-признак тогда и только тогда, когда $g \notin H$. В этом случае* $\operatorname{pok}_g H = \operatorname{ord} g$.

Доказательство. Так как $\operatorname{ord} g$ есть простое число q, то порядок подгруппы $\langle g \rangle \cap H$ равен либо 1, либо q. Первый вариант имеет место тогда и только тогда, когда $g \notin H$. При этом $\langle g \rangle \cap H = \{e\}$ и $\operatorname{pok}_g H = \operatorname{ord} g$. □

Нижние оценки величин $\operatorname{pok}_S H$ существенно зависят от свойств множеств S и H и могут достигать малых значений.

Например, если $S \cap H \neq \varnothing$, то $\operatorname{pok}_S H = 1$. В случае $S \cap H = \varnothing$, если множество H содержит единицу группы Ф и система S содержит инволюции или взаимно обратные элементы, то $\operatorname{pok}_S H = 2$. □

1.2.2. Свойства наследственных подмножеств конечной группы и их покрытий циклическими группами. Элементы в циклических группах «наследуют» некоторые свойства порождающего элемента, т. е., если элемент g обладает некоторым свойством, то и любой другой элемент группы $\langle g\rangle$ обладает этим свойством. Например, если $\operatorname{ord} g \leqslant n$, то и $\operatorname{ord} g' \leqslant n$ для любого $g' \in \langle g\rangle$.

В связи с этим представляет интерес изучение наследственных подмножеств группы [7, гл. II, § 1, определение 8] и наследственных признаков в группе.

Рассмотрим квазипорядок $\leqslant$ на группе Φ, где $g' \leqslant g$ для $g', g \in \Phi$ тогда и только тогда, когда $\langle g'\rangle \subseteq \langle g\rangle$.

Определение 1.8. Непустое подмножество Q группы Φ называется *наследственным* (*heritable*), если из включения $g \in Q$ следует, что $\langle g\rangle \subseteq Q$. $\diamondsuit$

Отметим, при групповом гомоморфизме $\varphi\colon \Phi \to \Phi'$ наследственное подмножество Q группы Φ отображается в наследственное подмножество $\varphi(Q)$ группы Φ'.

Обозначим через $HR(\Phi)$ множество всех наследственных подмножеств группы Φ, упорядоченное относительно теоретико-множественного включения. $HR(\Phi)$ совпадает с множеством всех наследственных подмножеств фактормножества $\Phi/\cong$, где $g \cong g'$ для $g, g' \in \Phi$ тогда и только тогда, когда $\langle g\rangle = \langle g'\rangle$. Так как $\Phi/\cong$ есть множество с частичным порядком, то $HR(\Phi)$ — дистрибутивная решётка [7, гл. II, § 1]. Отсюда и из определения 1.8 вытекают следующие свойства.

Утверждение 1.5. а) *Любое наследственное подмножество Q группы Φ содержит единицу e группы Φ.*

б) *Если $Q, Q' \in HR(\Phi)$, то $Q \cap Q', Q \cup Q' \in HR(\Phi)$.* $\diamondsuit$

Циклические подгруппы группы Φ являются неразложимыми (в сумму) элементами [7, гл. I, § 6] решётки $HR(\Phi)$.

Из определения 1.8 следует, что всякое наследственное подмножество Q конечной группы Φ, в частности, сама группа Φ, может быть представлено как объединение циклических подгрупп группы Φ (неразложимых элементов решётки $HR(\Phi)$). Например, представление

$$Q = \bigcup_{g \in R} \langle g\rangle, \tag{1.2}$$

при $R = Q$ является тривиальным представлением такого вида.

Определение 1.9. Представление (1.2) наследственного подмножества Q группы Φ, где $R \subseteq Q$, назовём *c-покрытием наследственного множества Q*, а множество R назовём *системой c-образующих наследственного множества Q*. $\diamondsuit$

Система c-образующих множества Q и, следовательно, c-покрытие наследственного множества Q могут определяться неоднозначно. Например, если R есть система c-образующих наследственного множества Q, где $Q \neq \{e\}$ и $e \in R$, то множество $R \setminus \{e\}$ — также система c-образующих наследственного множества Q.

Определение 1.10. Систему c-образующих наследственного множества Q назовём *c-базисом наследственного множества Q* (обозначается B_Q), если никакая её собственная подсистема не является системой c-образующих множества Q, при этом *c-покрытие наследственного множества Q*, соответствующее c-базису, назовём *каноническим*. $\diamondsuit$

Таким образом, каноническое c-покрытие наследственного множества Q является несократимым представлением [7, гл. II, § 1] наследственного множества Q в виде объединения неразложимых элементов решётки

$HR(\Phi)$ и имеет вид:

$$Q = \bigcup_{g \in B_Q} \langle g \rangle, \tag{1.3}$$

Определение 1.11. Если $\langle g \rangle \subseteq Q \subseteq \Phi$ и $\langle g \rangle$ не является собственной подгруппой циклической группы, содержащейся во множестве Q, то группа $\langle g \rangle$ называется *максимальной циклической группой множества* Q. ◇

Замечание. Из определений 1.10 и 1.11 следует что:

1) каждая циклическая подгруппа канонического c-покрытия наследственного множества Q максимальна в Q, в частности, поэтому c-базис нетривиального наследственного множества не содержит e;

2) каноническое c-покрытие наследственного множества Q состоит из попарно невложимых циклических подгрупп;

3) всякая система c-образующих наследственного множества содержит некоторый c-базис этого множества.

Определение 1.12. *c-базисы* $B = (g_1, \ldots, g_r)$ и $B' = (g_1, \ldots, g'_m)$ наследственного множества Q называются *эквивалентными* (обозначается $B \cong B'$), если наборы циклических групп $\{\langle g_1 \rangle, \ldots, \langle g_r \rangle\}$ и $\{\langle g'_1 \rangle, \ldots, \langle g'_m \rangle\}$ совпадают как множества. ◇

Определение 1.13. Число элементов c-базиса наследственного множества Q назовём *рангом c-базиса* или *c-шириной множества* Q. ◇

Корректность определения c-ширины наследственного множества Q (обозначим её через $h_c(Q)$) вытекает из [7, гл. II, § 1, следствие 13], согласно которому любой элемент Q решётки $HR(\Phi)$ имеет единственное несократимое представление в виде объединения неразложимых элементов.

В терминах определений 1.10–1.13 указанное следствие 13 имеет следующую формулировку.

Теорема 1.3. *Всякое наследственное подмножество Q группы имеет единственное каноническое c-покрытие, полученное с помощью объединения всех максимальных циклических подгрупп множества* Q. ◇

Замечание. Из теоремы 1.3 следует, что все c-базисы наследственного множества Q эквивалентны и имеют одинаковые ранги, c-ширина наследственного множества Q есть число максимальных циклических подгрупп множества Q. ◇

Утверждение 1.6. *Пусть B_i есть c-базис наследственного множества Q_i, $i = 0, 1, \ldots, r$, и $Q_0 = Q_1 \cup \ldots \cup Q_r$, тогда*

а) $B_0 \subseteq B_1 \cup \ldots \cup B_r$;

б) $h_c(Q_0) \leqslant h_c(Q_1) + \ldots + h_c(Q_r)$;

в) *Равенства $B_0 = B_1 \cup \ldots \cup B_r$ и $h_c(Q_0) = h_c(Q_1) + \ldots + h_c(Q_r)$ выполнены тогда и только тогда, когда для любого $i = 1, \ldots, r$ и любого $g \in B_i$ циклическая подгруппа $\langle g \rangle$ является максимальной во множестве Q_0.*

Доказательство. а) По условию из равенства (1.3) имеем:

$$Q_i = \bigcup_{g \in B_i} \langle g \rangle, \; i = 0, 1, \ldots, r.$$

Так как $Q_0 = Q_1 \cup \ldots \cup Q_r$, то отсюда получаем, что

$$Q_0 = \bigcup_{i=1}^{r} \bigcup_{g \in B_i} \langle g \rangle.$$

Следовательно, множество $B_1 \cup \ldots \cup B_r$ есть система c-образующих множества Q_0. Отсюда с учётом замечания 3) к определению 1.11 следует, что $B_0 \subseteq B_1 \cup \ldots \cup B_r$.

б) По определению 1.13 $h_c(Q_i)=|B_i|$, $i=0, 1, \ldots, r$, поэтому из утверждения 1.6,а) следует оценка ширины $h_c(Q_0)$ множества Q_0.

Утверждение в) следует из теоремы 1.3. □

Замечание. В общем случае c-ширина нетривиального наследственного множества Q оценивается неравенствами:

$$1 \leqslant h_c(Q) \leqslant |Q| - 1. \tag{1.4}$$

Нижняя оценка достигается в случае, когда Q — циклическая группа.

Верхняя оценка достигается, в частности, когда Q — прямая сумма нескольких циклических групп порядка 2. Если $Q = \Sigma_r$, где Σ_r — группа сдвигов пространства V_r двоичных r-мерных векторов, то

$$h_c(\Sigma_r) = 2^r - 1,$$

так как c-базис группы Σ_r образуют все ненулевые сдвиги векторного пространства V_r. ◇

1.2.3. Определяющие свойства наследственных признаков в группе.

Определение 1.14. *H-признак* в группе G назовём *наследственным*, если $G \cap H$ — наследственное множество. ◇

Замечание 1. Из замкнутости групповой операции следует, что всякая группа является наследственным множеством и, следовательно, групповой H-признак в любой группе является наследственным признаком. ◇

Замечание 2. Из утверждения 1.5,а) следует, что наследственное множество нетривиально, если оно отлично от $\{e\}$. Следовательно, наследственный H-признак в группе G тривиален тогда и только тогда, когда $G \cap H = \{e\}$. ◇

Установим некоторые свойства наследственных признаков в группе.

Утверждение 1.7. а) *Если H — наследственное подмножество группы Φ, то любая подгруппа G группы Φ имеет наследственный H-признак.*

б) *Если группа G имеет наследственный H-признак и наследственный F-признак, то группа G имеет наследственный $H \cap F$-признак и наследственный $H \cup F$-признак.*

Доказательство. а) По условию $\Phi \cap H \in HR(\Phi)$ и $G \in HR(\Phi)$. Тогда по утверждению 1.5,б)

$$G \cap (\Phi \cap H) \in HR(\Phi),$$

где $G \cap (\Phi \cap H) = G \cap H$.

б) По условию $G \cap H \in HR(\Phi)$ и $G \cap F \in HR(\Phi)$. Значит, по утверждению 1.5,б) множества $(G \cap H) \cap (G \cap F)$ и $(G \cap H) \cup (G \cap F)$ также наследственные. При этом

$$(G \cap H) \cap (G \cap F) = G \cap (H \cap F),$$
$$(G \cap H) \cup (G \cap F) = G \cap (H \cup F).$$

Следовательно, группа G имеет наследственный $H \cap F$-признак и наследственный $H \cup F$-признак. □

Утверждение 1.8. *Пусть c-покрытие группы G определено равенством* (1.2). *Тогда:*

а) *группа G имеет H-признак в том и только в том случае, если для некоторого $g \in R$ циклическая группа $\langle g \rangle$ имеет H-признак;*

б) *группа G имеет наследственный H-признак в том и только в том случае, если для любого $g \in R$ циклическая группа $\langle g \rangle$ имеет наследственный H-признак;*

в) *группа G имеет тривиальный наследственный H-признак в том и только в том случае, если для любого $g \in R$ циклическая группа $\langle g \rangle$ имеет тривиальный наследственный H-признак.*

Доказательство. а) Из равенства (1.2) следует:

$$G \cap H = \bigcup_{g \in R} (\langle g \rangle \cap H). \tag{1.5}$$

Значит, $G \cap H \neq \varnothing$ тогда и только тогда, когда найдётся $g \in R$ такой, что $\langle g \rangle \cap H \neq \varnothing$.

б) Если группа G имеет наследственный H-признак, то по утверждению 1.7,а) любая циклическая подгруппа группы G также имеет наследственный H-признак.

Докажем в обратную сторону. Если $g \in G \cap H$, то в силу равенства (1.5) $g \in \langle g' \rangle \cap H$ при некотором $g' \in R$. По условию множество $\langle g' \rangle \cap H$ является наследственным. Тогда из определения 1.8 следует, что $\langle g \rangle \subseteq \langle g' \rangle \cap H$ при указанном $g' \in R$. Отсюда и из равенства (1.5) получаем, что $\langle g \rangle \subseteq G \cap H$, т. е. множество $G \cap H$ является наследственным.

в) В силу утверждения 1.8,б) и замечания 2) к определению 1.14 достаточно доказать, что равенство $G \cap H = \{e\}$ выполнено тогда и только тогда, когда $\langle g \rangle \cap H = \{e\}$ для любого $g \in R$. Последнее утверждение верно в силу равенства (1.5). □

Применяя утверждение 1.6 к каноническому c-покрытию наследственного множества $G \cap H$, получаем следующую теорему.

Теорема 1.4. *Если группа G имеет наследственный H-признак, то*

а) $B_{G \cap H} \subseteq \bigcup_{g \in B_G} B_{\langle g \rangle \cap H}$;

б) $h_c(G \cap H) \leqslant \sum_{g \in B_G} h_c(\langle g \rangle \cap H)$;

в) *равенства* $B_{G \cap H} = \bigcup_{g \in B_G} B_{\langle g \rangle \cap H}$ *и* $h_c(G \cap H) = \sum_{g \in B_G} h_c(\langle g \rangle \cap H)$ *выполнены тогда и только тогда, когда для любого $g \in B_G$ и любого $g' \in B_{\langle g \rangle \cap H}$ циклическая подгруппа $\langle g' \rangle$ максимальна во множестве $G \cap H$.* ◇

Таким образом, изучение наследственного признака H в группе G можно свести к изучению наследственного признака H в циклических подгруппах, образующих каноническое c-покрытие группы G. Одной из характеристик сложности реализации такого подхода является c-ширина группы G.

1.2.4. Свойства наследственных признаков в циклической группе. Пусть группа G имеет наследственный H-признак и требуется описать наследственное множество $G \cap H$.

Естественным способом описания множества $G \cap H$ является (см. теорему 1.3) определение его канонического c-покрытия или, что равносильно, одного из эквивалентных c-базисов множества $G \cap H$. Согласно теореме 1.4 для решения этой задачи достаточно описать канонические c-покрытия наследственных множеств $\langle g \rangle \cap H$, где g пробегает все элементы c-базиса группы G.

Итак, пусть $g \in G$ и требуется описать множество $\langle g \rangle \cap H$. Произвольный элемент группы $\langle g \rangle$ имеет вид g^t, где $t \in \{1, \ldots, n\}$. Следовательно, если группа $\langle g \rangle$ имеет наследственный H-признак, то c-базис наследственного множества $\langle g \rangle \cap H$ (пусть его ранг равен r) есть подмножество

$\{g^{t_1}, \ldots, g^{t_r}\}$ элементов группы $\langle g\rangle$, где $\{t_1, \ldots, t_r\} \subseteq \{1, \ldots, n\}$. Поэтому множество $\langle g\rangle \cap H$ описывается набором чисел $t_1, \ldots, t_r$, соответствующим элементам c-базиса этого множества.

Для описания набора чисел $t_1, \ldots, t_r$ сделаем некоторые определения.

Определение 1.15. *c-базис* $\{g^{t_1}, \ldots, g^{t_r}\}$ наследственного множества $\langle g\rangle \cap H$ назовём *g-каноническим*, если $t_1, \ldots, t_r \in D(n)$. ◇

Существование g-канонического c-базиса множества $\langle g\rangle \cap H$ следует из того, что всякую подгруппу $\langle g'\rangle$, являющуюся элементом канонического c-покрытия множества $\langle g\rangle \cap H$, можно породить элементом g^t, где $t = \frac{n}{\operatorname{ord}\langle g'\rangle}$.

Определение 1.16. Натуральные числа $\{t_1, \ldots, t_r\}$, соответствующие g-каноническому c-базису $\{g^{t_1}, \ldots, g^{t_r}\}$ наследственного множества $\langle g\rangle \cap H$, назовём *(H, g)-пороговыми числами.* ◇

Множество $\{t_1, \ldots, t_r\}$ всех (H, g)-пороговых чисел обозначим $\Pi(H, g)$. Тогда из определения 1.16 имеем:

$$\langle g\rangle \cap H = \bigcup_{t \in \Pi(H, g)} \langle g^t\rangle. \tag{1.6}$$

Таким образом, строение множества $\langle g\rangle \cap H$ определяется множеством чисел $\Pi(H, g)$.

Множество подгрупп циклической группы $\langle g\rangle$ порядка n, рассматриваемое как частично упорядоченное множество, является решёткой, антиизоморфной (обратно изоморфной) решётке $D(n)$ всех натуральных делителей числа n. То есть для $g^\tau, g^t \in \langle g\rangle$ отношение $g^\tau \leqslant g^t$ выполнено тогда и только тогда, когда (t, n) делит (τ, n). При этом изоморфизме атомам решётки $\langle g\rangle$ соответствуют коатомы решётки $D(n)$ и наоборот. Поэтому изучение множества чисел $\Pi(H, g)$ связано с изучением определённых свойств решётки $D(n)$.

При исследовании частично упорядоченного множества M нередко используется диаграмма этого множества, представляющая собой орграф с множеством вершин M [2, гл. I, § 3].

Напомним, что в множестве M *элемент τ' покрывает элемент τ* или *элемент τ покрывается элементом τ'* (обозначается $\tau' \succ\!- \tau$), если $\tau' \neq \tau$, $\tau \leqslant \tau'$ и в M не найдётся отличного от τ и τ' числа τ'', такого, что $\tau \leqslant \tau''$ и $\tau'' \leqslant \tau'$. Пара элементов (τ', τ) образует дугу диаграммы множества M тогда и только тогда, когда $\tau' \succ\!- \tau$.

Если M — решётка, то в M имеется наименьший элемент (обозначим его $\mathbf{0}$) и наибольший элемент (обозначим его $\mathbf{1}$). Тогда *атомом решётки M* называют всякий элемент τ со свойством $\tau \succ\!- \mathbf{0}$ и *коатомом* решётки M называют всякий элемент τ со свойством $\mathbf{1} \succ\!- \tau$ [7, гл. I, § 6].

Заметим, что в решётке M каждый элемент или совпадает или сравним хотя бы с одним из атомов (коатомов) решётки.

Пример 1.1. Пусть каноническое разложение числа n есть

$$n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \tag{1.7}$$

где $p_1, \ldots, p_s$ — попарно различные простые числа и $k_1, \ldots, k_s$ — натуральные числа. Тогда атомами решётки $D(n)$ являются все числа $p_1, \ldots, p_s$. Коатомами решётки $D(n)$ являются все числа $\frac{n}{p_1}, \ldots, \frac{n}{p_s}$. ◇

В связи с изучением некоторых свойств натуральных чисел введём необходимые определения. Пусть M — множество натуральных чисел, т. е. $M \subset N$.

Определение 1.17. Натуральное число t из M назовём *простым во множестве M* (или *M-простым*), если t не делится ни на одно другое число множества M. ◇

Множество всех M-простых чисел обозначим $\operatorname{prm} M$. Таким образом, $\operatorname{prm} M$ есть подмножество всех минимальных элементов [2, гл. I, § 3] множества M по отношению делимости натуральных чисел.

Если $M=\{n_1, \ldots, n_m\}$, то из определения 1.17 следует, что множество $\operatorname{prm} M$ либо состоит из одного элемента, либо образует антицепь в решётке чисел $D(НОК(n_1, \ldots, n_m))$.

Пусть теперь M — набор натуральных чисел, не обязательно различных, т. е. $M \in N^m$.

Определение 1.18. *Редукцией набора* M натуральных чисел (обозначается M^*) назовём множество попарно различных элементов набора M. *Набор* M назовём *редуцированным*, если он не содержит одинаковых элементов. $\diamondsuit$

Символом $\operatorname{prm} M^*$, где M — набор натуральных чисел, обозначим множество $\operatorname{prm}(M^*)$.

Теорема 1.5. а) *Если* $\{g^{t_1}, \ldots, g^{t_r}\}$ *и* $\{g^{\tau_1}, \ldots, g^{\tau_r}\}$ *есть соответственно* g*-канонический и иной* (*т. е.* $(t_1, \ldots, t_r) \neq (\tau_1, \ldots, \tau_r)$) c*-базисы множества* $\langle g\rangle \cap H$, *где* $\langle g^{\tau_i}\rangle = \langle g^{t_i}\rangle$, $i=1, \ldots, r$, *то* $t_1=(\tau_1, n), \ldots, t_r = (\tau_r, n)$, *и* $\tau_i \notin D(n)$ *при некотором* $i \in \{1, \ldots, r\}$. *Вследствие этого наследственное множество* $\langle g\rangle \cap H$ *имеет единственный* g*-канонический* c*-базис.*

б) *Если* M *есть подмножество множества* $\{1, \ldots, n\}$ *такое, что* $g^t \in H$ *при любом натуральном* t *в том и только в том случае, если число* t *кратно хотя бы одному из чисел множества* M, *то* $\Pi(H, g) = \operatorname{prm} M$.

в) *Множество* (H, g)*-пороговых чисел описывается равенством:*

$$\Pi(H, g) = \operatorname{prm}\{t \in D(n): g^t \in H\}. \tag{1.8}$$

г) $h_c(\langle g\rangle \cap H) = |\Pi(H, g)|$.

Доказательство. а) По условию $\langle g^{\tau_i}\rangle = \langle g^{t_i}\rangle$, $i=1, \ldots, r$, отсюда, учитывая, что t_i/n, получаем по теореме 3.3.2 [18], что

$$(\tau_1, n) = (t_1, n) = t_1, \ldots, (\tau_r, n) = (t_r, n) = t_r.$$

Равенство $(\tau_i, n) = t_i$ выполняется для делителя τ_i числа n в том и только в том случае, если $\tau_i = t_i$, $i=1, \ldots, r$. Поэтому если $(t_1, \ldots, t_r) \neq \neq (\tau_1, \ldots, \tau_r)$, то хотя бы одно из чисел $\tau_1, \ldots, \tau_r$ не является делителем числа n.

Отсюда и из эквивалентности всех c-базисов наследственного множества (теорема 1.3) следует единственность g-канонического c-базиса множества $\langle g\rangle \cap H$. $\square$

Утверждение 1.9 (промежуточное). *Делитель* t *числа* n *является элементом множества* $\Pi(H, g)$ *тогда и только тогда, когда* $g^t \in H$ *и* $g^\tau \notin H$ *для любого собственного делителя* τ *числа* t.

Доказательство. Пусть $t \in \Pi(H, g)$, тогда из равенства (1.6) следует, что группа $\langle g^t\rangle$ есть элемент канонического c-покрытия наследственного множества $\langle g\rangle \cap H$. Докажем, что $g^\tau \notin H$.

Из теоремы 1.5,а) следует, что t/n, тогда τ/n и $\langle g^t\rangle$ есть собственная подгруппа группы $\langle g^\tau\rangle$. Значит, если $g^\tau \in H$, то $\langle g^\tau\rangle \subseteq H$ в силу наследственности множества $\langle g\rangle \cap H$. Следовательно, группа $\langle g^t\rangle$ не является максимальной во множестве $\langle g\rangle \cap H$. Отсюда по теореме 1.3 группа $\langle g^t\rangle$ не является элементом канонического c-покрытия наследственного множества $\langle g\rangle \cap H$. Имеем противоречие, значит, $g^\tau \notin H$.

Пусть теперь t/n, $g^t \in H$ и $g^\tau \notin H$ для любого собственного делителя τ числа t. Если g^t не является элементом g-канонического c-базиса множества $\langle g\rangle \cap H$, то по теореме 1.3 группа $\langle g^t\rangle$ не является максимальной во

множестве $\langle g\rangle \cap H$. Значит, она есть подгруппа циклической группы $\langle g^\tau\rangle$, где $\tau \neq t$ и τ / t. Имеем противоречие, следовательно, g^t — элемент g-канонического c-базиса множества $\langle g\rangle \cap H$.

Отсюда и из равенства (1.6) следует, что $t \in \Pi(H, g)$. □

Продолжим доказательство теоремы.

б) Из утверждения 1.9 имеем, что если $t \in \Pi(H, g)$, то $g^t \in H$ и $g^\tau \notin H$ для любого собственного делителя τ числа t. Кроме того, из равенства (1.6) следует, что $g^\mu \in H$ для любого μ, кратного t. По условию отсюда следует, что $t \in M$ и $\tau \notin M$. Значит, по определению 1.17 $t \in \operatorname{prm} M$. Следовательно, $\Pi(H, g) \subseteq \operatorname{prm} M$.

Если $t \in \operatorname{prm} M$, то по условию $g^t \in H$ и по определению 1.17 $\tau \notin M$, где τ — собственный делитель числа t. Значит, из условий имеем, что $g^\tau \notin H$ для любого собственного делителя τ числа t. Следовательно, по утверждению 1.9 $t \in \Pi(H, g)$, т. е. $\operatorname{prm} M \subseteq \Pi(H, g)$.

Таким образом, $\Pi(H, g) = \operatorname{prm} M$.

в) Из равенства (1.6) следует, что $g^t \in H$ при любом натуральном t в том и только в том случае, если число t кратно хотя бы одному из чисел множества $\Pi(H, g)$. Так как из теоремы 1.5,а) следует, что $\Pi(H, g) \subseteq D(n)$, то верно и следующее утверждение: $g^t \in H$ при любом натуральном t в том и только в том случае, если число t кратно хотя бы одному из чисел множества M, где $M = \{\mu \in D(n)\colon g^\mu \in H\}$. Отсюда по теореме 1.5,б) получаем равенство (1.8).

г) По определению 1.13 c-ширина наследственного множества $\langle g\rangle \cap \cap H$ совпадает с его рангом. Ранг множества $\langle g\rangle \cap H$ по определению 1.16 совпадает с порядком множества $\Pi(H, g)$. □

Следствие 1. *Если циклическая группа $\langle g\rangle$ имеет наследственный H-признак, то* $\operatorname{pok}_g H$ *есть наименьшее из (H, g)-пороговых чисел.*

Доказательство. По определению $\operatorname{pok}_g H$ есть наименьшее натуральное число t, при котором $g^t \in H$. Так как $g^t \in H$ для любого $t \in \Pi(H, g)$, то $\operatorname{pok}_g H \leqslant \min\{t_1, \ldots, t_r\}$, где $\Pi(H, g) = \{t_1, \ldots, t_r\}$.

С другой стороны, если $g^t \in H$, то в силу равенства (1.6) число t кратно одному из чисел $t_1, \ldots, t_r$. Значит, $\operatorname{pok}_g H$ кратен одному из чисел $t_1, \ldots, t_r$. Это совместимо с неравенством $\operatorname{pok}_g H \leqslant \min\{t_1, \ldots, t_r\}$ только в случае, если $\operatorname{pok}_g H = \min\{t_1, \ldots, t_r\}$. □

Следствие 2. *Наследственный H-признак в группе $\langle g\rangle$ является групповым тогда и только тогда, когда множество $\Pi(H, g)$ состоит из единственного числа t, равного $|\langle g\rangle\colon (\langle g\rangle \cap H)|$, при этом $\langle g\rangle \cap H = \langle g^t\rangle$.*

Вследствие этого наследственный H-признак в группе $\langle g\rangle$ тривиален тогда и только тогда, когда $\Pi(H, g) = \{n\}$.

Доказательство. Если множество $\Pi(H, g)$ состоит из единственного числа t, то равенство (1.6) принимает вид:

$$\langle g\rangle \cap H = \langle g^t\rangle,$$

т. е. $\langle g\rangle \cap H$ — группа порядка $\frac{n}{t}$.

По следствию 1 теоремы 1.5 $\operatorname{pok}_g H = t$. Вместе с тем, по теореме 1.2 $\operatorname{pok}_g H = |\langle g\rangle\colon (\langle g\rangle \cap H)|$. Значит, $t = |\langle g\rangle\colon (\langle g\rangle \cap H)|$.

Пусть $\Pi(H, g) = \{t_1, \ldots, t_r\}$, где $r > 1$ и $t_1 < \ldots < t_r$. Покажем, что множество $\langle g\rangle \cap H$ не является группой. Заметим, что число $t_2 - t_1$ не кратно ни одному из чисел $t_1, \ldots, t_r$. Действительно, число $t_2 - t_1$ меньше каждого из чисел $t_2, \ldots, t_r$ и не кратно числу t_1, иначе число t_2 было бы кратным числу t_1 и не являлось бы простым во множестве $\{t \in D(n)\colon g^t \in H\}$, что противоречило бы равенству (1.7). Так как число $t_2 - t_1$ не кратно ни одному из чисел $\{t_1, \ldots, t_r\}$, то из равенства (1.6) следует, что $g^{t_2 - t_1} \notin \langle g\rangle \cap H$.

Теперь, полагая $g' = g^{t_1}$ и $g'' = g^{t_2}$, получаем, что $g', g'' \in \langle g\rangle \cap H$ и, в то же время, $g''\cdot(g')^{-1} \notin \langle g\rangle \cap H$. Значит, множество $\langle g\rangle \cap H$ — не группа. □

Обозначим через $H(\mathrm{ord} \leqslant r)$ множество всех элементов g из H порядка не выше r, где r — натуральное.

Следствие 3. *Если группа G имеет наследственный H-признак, то группа G имеет и наследственный $H(\mathrm{ord} \leqslant r)$-признак, r — натуральное. Если $g \in H$ и $\mathrm{ord}\, g = n$, то*

$$\Pi(H(\mathrm{ord} \leqslant r), g) = \mathrm{prm}\{t \in D(n):\ n \leqslant t \cdot r\}.$$

Доказательство. По теореме 7 [6, гл. XI, § 4] при любом натуральном t

$$\mathrm{ord}\, g^t = \frac{\mathrm{ord}\, g}{(\mathrm{ord}\, g,\ t)} \leqslant \mathrm{ord}\, g.$$

Поэтому если $g \in H$ и $\mathrm{ord}\, g \leqslant r$, то в силу наследственности H-признака $g^t \in H$ и $\mathrm{ord}\, g^t \leqslant r$. Следовательно, по определению 1.8 множество $H(\mathrm{ord} \leqslant \leqslant r)$ является наследственным.

Если $g \in H$ и $\mathrm{ord}\, g = n$, то по (1.8)

$$\Pi(H(\mathrm{ord} \leqslant r), g) = \mathrm{prm}\{t \in D(n):\ g^t \in H(\mathrm{ord} \leqslant r)\}.$$

Так как в силу наследственности H-признака $g^t \in H$, то

$$\{t \in D(n):\ g^t \in H(\mathrm{ord} \leqslant r)\} = \{t \in D(n):\ \mathrm{ord}\, g^t \leqslant r\} = \{t \in D(n):\ n \leqslant t \cdot r\}.$$

Отсюда получаем выражение для множества $\Pi(H(\mathrm{ord} \leqslant r), g)$. □

Следствие 4. *Если группа G, заданная системой образующих S, имеет наследственный H-признак, то* $\mathrm{pok}_S H$ *не превышает наименьшего из чисел множества* $\Pi(H, s_1) \cup \ldots \cup \Pi(H, s_p)$.

Доказательство. Рассмотрим c-покрытие группы G, определённое равенством (1.2) и такое, что $S \subseteq R$ (такое c-покрытие имеется, в частности, таково тривиальное c-покрытие).

По условию группа G имеет наследственный H-признак, отсюда по утверждению 1.8,б) циклические подгруппы $\langle s_1\rangle, \ldots, \langle s_p\rangle$ группы G также имеют наследственный H-признак. Тогда по утверждению 1.2

$$\mathrm{pok}_S H \leqslant \min\{\mathrm{pok}_{s_1} H, \ldots, \mathrm{pok}_{s_p} H\}.$$

По следствию 1 теоремы 1.5 $\mathrm{pok}_{s_i} H$ есть наименьшее из (H, s_i)-пороговых чисел. Значит, $\min\{\mathrm{pok}_{s_1} H, \ldots, \mathrm{pok}_{s_p} H\}$ — наименьшее число множества $\Pi(H, s_1) \cup \ldots \cup \Pi(H, s_p)$. □

Пример 1.2. Рассмотрим циклическую группу $\langle g\rangle$ порядка 24 и определим наследственное множество $H(m)$ как множество всех элементов группы, порядок которых не превышает m, где $m \leqslant 24$. При $m = 4$:

1) $H(4) = \{g^6, g^8, g^{12}, g^{16}, g^{18}, g^{24}\}$, где $g^{24} = e$;

2) $\Pi(H(4), g) = \mathrm{prm}\{t \in D(24):\ g^t \in H(4)\} = \mathrm{prm}\{6, 8, 12, 16, 18, 24\} = \{6, 8\}$, т. е. верно представление $H(4) = \langle g^6\rangle \cup \langle g^8\rangle$;

3) список всех эквивалентных c-базисов множества $H(4)$ имеет вид:

$$\{g^6, g^8\}, \{g^{18}, g^8\}, \{g^6, g^{16}\}, \{g^{18}, g^{16}\};$$

Первый в этом списке c-базис является g-каноническим;

4) c-ширина множества $H(4)$ равна 2;

5) $\mathrm{pok}_g H(4) = 6$.

При $m = 2$ ($H(2)$-признак является групповым):

1) $H(2) = \{g^{12}, g^{24}\} = \langle g^{12}\rangle$;

2) по формуле (1.8)

$$\Pi(H(2), g) = \mathrm{prm}\{t \in D(24)\colon g^t \in H(2)\} = \mathrm{prm}\{12, 24\} = \{12\};$$

3) единственный (g-канонический) c-базис множества $H(2)$ есть $\{g^{12}\}$;

4) c-ширина множества $H(2)$ равна 1;

5) $\mathrm{pok}_g H(2) = 12$. $\diamond$

1.2.5. Свойства наследственных признаков в прямом произведении групп. Для совместного рассмотрения нескольких признаков важна следующая теорема.

Теорема 1.6. *Пусть* $\Phi = \Phi_1 \dot{\times} \ldots \dot{\times} \Phi_r$ *и* $G = G_1 \dot{\times} \ldots \dot{\times} G_r$ *— прямые произведения конечных групп,* $H = H_1 \times \ldots \times H_r$ *и* $S = S_1 \times \ldots \times S_r$ *— декартовы произведения множеств, где* $\varnothing \neq H_i \subseteq \Phi_i$, $\varnothing \neq S_i \subset \Phi_i$, $\langle S_i\rangle = G_i$, $i = 1, \ldots, r$. *Тогда*

а) *группа* G *имеет* H*-признак в том и только в том случае, если при всех* $i = 1, \ldots, r$ *группа* G_i *имеет* H_i*-признак;*

б) *группа* G *имеет наследственный* H*-признак в том и только в том случае, если при всех* $i = 1, \ldots, r$ *группа* G_i *имеет наследственный* H_i*-признак;*

в) *если группа* G *имеет наследственный* H*-признак, то*

$$\mathrm{pok}_S H \leqslant HOK(\mathrm{pok}_{S_1} H_1, \ldots, \mathrm{pok}_{S_r} H_r).$$

Доказательство. а) По условиям $H \subseteq \Phi$, $S \subset \Phi$ и $G < \Phi$, тогда

$$G \cap H = (G_1 \cap H_1) \times \ldots \times (G_r \cap H_r).$$

Отсюда по определению декартова произведения множеств следует, что $G \cap H \neq \varnothing$ тогда и только тогда, когда $G_i \cap H_i \neq \varnothing$ для всех $i = 1, \ldots, r$.

б) Элемент g группы G имеет вид: $g = (g_1, \ldots, g_r)$, где $g_i \in G_i$, $i = 1, \ldots, r$. Поэтому если из включения $g \in G \cap H$ следует включение $\langle g\rangle \subseteq G \cap H$, то это равносильно тому, что при всех $i = 1, \ldots, r$ из включения $g_i \in G_i \cap H_i$ следует включение $\langle g_i\rangle \subseteq G_i \cap H_i$.

в) По условию множество $G \cap H$ и, следовательно (в силу теоремы 1.6,б)), множества $G_i \cap H_i$ являются наследственными, $i = 1, \ldots, r$.

Пусть $\mathrm{pok}_{S_1} H_i = t_i$, $i = 1, \ldots, r$, и g_i есть слово длины t_i в алфавите S_i такое, что $g_i \in G_i \cap H_i$. Так как множество $G_i \cap H_i$ является наследственным, то при любом натуральном m слово g_i^m, составленное из m-кратно повторенного слова g_i, соответствует m-й степени элемента g_i и поэтому также принадлежит $G_i \cap H_i$.

Рассмотрим набор слов $g = (g_1^{m_1}, \ldots, g_r^{m_r})$, где $m_i = HOK(t_1, \ldots, t_r)/t_i$. Заметим, что g есть слово длины $HOK(t_1, \ldots, t_r)$ в алфавите $S = S_1 \times \ldots \times S_r$. При этом $g \in G \cap H$, так как $g_i^{m_i} \in G_i \cap H_i$, $i = 1, \ldots, r$. Значит, $L(g, S) \leqslant HOK(t_1, \ldots, t_r)$ и, следовательно, $\mathrm{pok}_S H \leqslant HOK(t_1, \ldots, t_r)$. $\square$

Следствие 1. *Если в условиях теоремы* 1.6 $G_i = \langle g_i\rangle$ *— циклическая группа, имеющая наследственный* H_i*-признак,* $i = 1, \ldots, r$, *и* $g = (g_1, \ldots, g_r)$, *то*

$$\mathrm{pok}_g H = \min_{(\tau_1, \ldots, \tau_r)} \{HOK(\tau_1, \ldots, \tau_r)\},$$

где $\tau_i \in \Pi(H_i, g_i)$, $i = 1, \ldots, r$.

Если при этом $(\operatorname{ord} g_i, \operatorname{ord} g_j)=1$ *для* $i, j \in \{1, \ldots, r\}$ *и* $i \neq j$, *то*

$$\operatorname{pok}_g H = \operatorname{pok}_{g_1} H_1 \cdot \ldots \cdot \operatorname{pok}_{g_r} H_r.$$

Доказательство. Элемент $g^t \in H$ в том и только в том случае, если $g_i^t \in H_i$ для всех $i=1, \ldots, r$. Так как $G_i = \langle g_i \rangle$, то в силу равенства (1.6) $g_i^t \in H_i$ тогда и только тогда, когда t кратно одному из чисел множества $\Pi(H_i, g_i)$, $i=1, \ldots, r$. Значит, $g^t \in H$ тогда и только тогда, когда t кратно $HOK(\tau_1, \ldots, \tau_r)$, где $\tau_i \in \Pi(H_i, g_i)$, $i=1, \ldots, r$. Наименьшее из таких чисел по определению 1.3 совпадает с $\operatorname{pok}_g H$.

Если $(\operatorname{ord} g_i, \operatorname{ord} g_j) = 1$ для $i \neq j$, $i, j \in \{1, \ldots, r\}$, то в силу теоремы 1.5,а) любое (H_i, g_i)-пороговое число взаимно просто с любым (H_j, g_j)-пороговым числом. Значит, величина $HOK(\tau_1, \ldots, \tau_r)$ принимает наименьшее значение при $(\tau_1, \ldots, \tau_r) \in \Pi(H_1, g_1) \times \ldots \times \Pi(H_r, g_r)$ тогда и только тогда, когда τ_i — наименьшее из (H_i, g_i)-пороговых чисел, $i=1, \ldots, r$. Отсюда с учётом следствия 1 теоремы 1.5 получаем требуемое равенство. □

Следствие 2. *Если циклическая группа* $\langle g \rangle$ *имеет наследственный* H_i*-признак,* $i=1, \ldots, r$, *то группа* $\langle g \rangle$ *имеет наследственный* H*-признак, где* $H = H_1 \cap \ldots \cap H_r$. *При этом*

$$\Pi(H, g) = \operatorname{prm}\{HOK(\tau_1, \ldots, \tau_r)\}^*,$$
$$\operatorname{pok}_g H = \min_{(\tau_1, \ldots, \tau_r)} \{HOK(\tau_1, \ldots, \tau_r)\},$$

где $\tau_i \in \Pi(H_i, g)$, $i=1, \ldots, r$.

Доказательство. По утверждению 1.5,б) группа $\langle g \rangle$ имеет наследственный H-признак, где $H = H_1 \cap \ldots \cap H_r$.

Из формулы (1.6) в данных условиях следует, что $g^t \in H$ тогда и только тогда, когда при каждом $i=1, \ldots, r$ число t кратно хотя бы одному из чисел множества $\Pi(H_i, g)$. Это равносильно тому, что t кратно хотя бы одному из чисел $HOK(\tau_1, \ldots, \tau_r)$ при $\tau_i \in \Pi(H_i, g)$, $i=1, \ldots, r$. Применяя теперь теорему 1.5,б), получаем выражение для множества $\Pi(H, g)$.

Отсюда по следствию 1 теоремы 1.5 получаем выражение для величины $\operatorname{pok}_g H$. □

Следствие 3. *Если в условиях теоремы* 1.6 G_i *есть циклическая группа* $\langle g_i \rangle$, *имеющая групповой* H_i*-признак,* $i=1, \ldots, r$, *то*

$$\operatorname{pok}_g H = HOK(|\langle g_1 \rangle : (\langle g_1 \rangle \cap H_1)|, \ldots, |\langle g_r \rangle : (\langle g_r \rangle \cap H_r)|).$$

Доказательство. Так как циклическая группа $\langle g_i \rangle$ имеет групповой H_i-признак, то по следствию 2 теоремы 1.5 множество $\Pi(H_i, g_i)$ состоит из единственного числа t_i, где $t_i = |\langle g_i \rangle : (\langle g_i \rangle \cap H_i)|$, $i=1, \ldots, r$. Отсюда и из следствия 1 теоремы 1.6 получаем требуемое равенство. □

Следствие 4. *Если в условиях следствия* 3 *теоремы* 1.6 $g_i \notin H_i$ *и* $\operatorname{ord} g_i$ *— простое число,* $i=1, \ldots, r$, *то* H*-признак группы* $\langle g \rangle$ *является тривиальным и*

$$\operatorname{pok}_g H = HOK(\operatorname{ord} g_1, \ldots, \operatorname{ord} g_r).$$

Данное равенство вытекает из следствия 3 теоремы 1.6 и следствия теоремы 1.2. □

1.2.6. О распределении признака по циклическим подгруппам группы. Пусть группа G имеет H-признак и требуется описать H-признак в циклических подгруппах группы G.

Определение 1.19. Множество всех элементов g группы G, для которых циклическая группа $\langle g\rangle$ имеет тривиальный H-признак (обозначим его G_H^1), назовём *множеством H-тривиальности группы G*. ◇

Множество всех элементов g группы G, для которых циклическая подгруппа $\langle g\rangle$ не имеет H-признака, обозначим G_H^0.

Утверждение 1.10. а) *Непустое множество G_H^0 является наследственным.*

б) *Если группа G имеет наследственный H-признак, то $G_H^0=\varnothing$, множество G_H^1 является наследственным и*

$$G_H^1=\bigcup_{g\in B_G}\langle g\rangle_H^1.$$

в) *Если наследственный H-признак тривиален в группе G, то $G_H^1=G$.*

Доказательство. а) Пусть $g\in G_H^0$, тогда $\langle g\rangle\cap H=\varnothing$. Так как любой элемент g' группы $\langle g\rangle$ порождает подгруппу $\langle g'\rangle$ группы $\langle g\rangle$, то $\langle g'\rangle\cap H=\varnothing$. Следовательно, $\langle g\rangle\subseteq G_H^0$, и множество G_H^0 является наследственным.

б) При любом $g\in G$ циклическая подгруппа $\langle g\rangle$ имеет наследственный H-признак в силу утверждения 1.7,а) Значит, $G_H^0=\varnothing$.

Пусть $g\in G_H^1$, тогда $\langle g\rangle\cap H=\{e\}$ в силу наследственности H-признака в группе G. Так как любой элемент g' группы $\langle g\rangle$ порождает подгруппу $\langle g'\rangle$ группы $\langle g\rangle$, то с учётом утверждения 1.7,а) $\langle g'\rangle\cap H=\{e\}$. Следовательно, $\langle g\rangle\subseteq G_H^1$, и множество G_H^1 — наследственное.

По теореме 1.3 для любого $g'\in G$ циклическая группа $\langle g'\rangle$ есть подгруппа хотя бы одной из максимальных циклических подгрупп $\langle g\rangle$ группы G, образующих каноническое c-покрытие. Поэтому если $g'\in G_H^1$, то $g'\in\langle g\rangle_H^1$, где g — указанный элемент c-базиса B группы G. Следовательно,

$$G_H^1\subseteq\bigcup_{g\in B}\langle g\rangle_H^1.$$

С другой стороны, если $g'\notin G_H^1$, то $\langle g'\rangle\cap H\neq\{e\}$. Значит, $g'\notin\langle g\rangle_H^1$ при любом элементе g c-базиса B, для которого $g'\in\langle g\rangle$. При этом $g'\notin\langle g\rangle$ для остальных элементов g c-базиса, поэтому $g'\notin\bigcup\limits_{g\in B}\langle g\rangle_H^1$. Следовательно, выполнено и обратное включение, поэтому $G_H^1=\bigcup\limits_{g\in B}\langle g\rangle_H^1$.

в) Если группа G имеет тривиальный наследственный H-признак, то из утверждения 1.8,в) при $R=G$ следует, что любая циклическая подгруппа группы G также имеет тривиальный наследственный H-признак и, следовательно, $G_H^1=G$. □

Опишем теперь H-признак в подгруппах циклической группы $\langle g\rangle$.

Теорема 1.7. *Пусть циклическая группа $\langle g\rangle$ порядка n имеет наследственный H-признак, $\Pi(H,g)=\{t_1,\ldots,t_r\}$ и t/n. Тогда*

$$\langle g^t\rangle\cap H=\bigcup_{j\in\Pi}\langle g^j\rangle,$$

где $\Pi=\mathrm{prm}\{HOK(t_1,t),\ldots,HOK(t_r,t)\}^*$.

Доказательство. Так как $\langle g^t\rangle<\langle g\rangle$, из (1.6) следует, что

$$\langle g^t\rangle\cap H=\bigcup_{j\in\Pi(H,g)}(\langle g^j\rangle\cap\langle g^t\rangle).$$

Пересечение подгрупп $\langle g^j\rangle$ и $\langle g^t\rangle$, где j и t — делители числа n, есть подгруппа $\langle g^{HOK(j,t)}\rangle$, поэтому отсюда получаем:

$$\langle g^t\rangle \cap H = \bigcup_{j \in \Pi(H, g)} \langle g^{HOK(j,t)}\rangle.$$

Таким образом, получено c-покрытие наследственного множества $\langle g^t\rangle \cap H$. По теореме 1.3 каноническое c-покрытие множества $\langle g^t\rangle \cap H$ состоит из максимальных циклических подгрупп данного множества.

Следовательно, g-канонический c-базис наследственного множества $\langle g^t\rangle \cap H$ образует множество элементов $\{g^j\}$ где $j \in \mathrm{prm}\{HOK(t_1, t), \ldots, HOK(t_r, t)\}^*$. □

Прежде чем вывести важное следствие из этой теоремы введём некоторые определения.

Определение 1.20. Если число n имеет каноническое разложение (1.7), то число $p_j^{k_j}$ назовём *примарным делителем числа* n, $j = 1, \ldots, s$. ◇

Определение 1.21. Пусть t/n. *Мультипримарным дополнением числа* t *до числа* n (обозначается $\mathrm{mp}_n(t)$) назовём произведение всех тех примарных делителей числа n, которые не делят t. При $t = n$ полагаем $\mathrm{mp}_n(n) = 1$. ◇

Обозначим через MP_n множество мультипримарных дополнений всех делителей числа n до числа n. Несложно показать, что MP_n есть 2^s-элементная дистрибутивная подрешётка решётки $D(n)$, изоморфная решётке всех подмножеств s-элементного множества.

Замечание. Величина $\mathrm{mp}_n(t)$ является псевдодополнением [7, гл. I, § 6] элемента t решётки $D(n)$, т. е., делителем числа n, для которого $HOK(t, \mathrm{mp}_n(t)) = n$ и из равенства $HOK(t, t') = n$ для $t' \in D(n)$ следует, что t' кратен $mp_n(t)$. ◇

Следствие (теоремы 1.7). *Множество* $\langle g\rangle_H^1$ *есть циклическая группа, порождённая элементом* g^t, *где*

$$t = HOK(\mathrm{mp}_n(t_1), \ldots, \mathrm{mp}_n(t_r)).$$

Доказательство. По утверждению 1.10,б) множество $\langle g\rangle_H^1$ является наследственным.

Покажем, что $\Pi(\langle g\rangle_H^1, g) = \mathrm{prm}\, M$, где M — множество всех делителей t числа n, для которых выполнена система равенств:

$$HOK(t, t_i) = n,\ i = 1, \ldots, r. \tag{1.9}$$

Из теоремы 1.7 следует, что включение $g^t \in \langle g\rangle_H^1$ выполнено тогда и только тогда, когда t удовлетворяет системе равенств (1.9).

Заметим, что если делитель t числа n удовлетворяет системе равенств (1.9), то этой системе удовлетворяет любой делитель числа n, кратный t. Значит, включение $g^t \in \langle g\rangle_H^1$ выполнено тогда и только тогда, когда t кратно одному из делителей числа n, удовлетворяющих системе равенств (1.9). Отсюда получаем по теореме 1.5,б), что $\Pi(\langle g\rangle_H^1, g) = \mathrm{prm}\, M$.

В силу замечания к определению 1.21 всякий делитель t' числа n, при котором $HOK(t_i, t') = n$, кратен числу $\mathrm{mp}_n(t_i)$, $i = 1, \ldots, r$. Значит, всякий делитель t числа n, при котором выполнена система равенств (1.9), кратен числу $HOK(\mathrm{mp}_n(t_1), \ldots, \mathrm{mp}_n(t_r))$. Следовательно, множество $\Pi(\langle g\rangle_H^1, g)$ состоит из единственного числа, равного $HOK(\mathrm{mp}_n(t_1), \ldots, \mathrm{mp}_n(t_r))$.

Отсюда по следствию 2 теоремы 1.5 получаем, что множество $\langle g\rangle_H^1$ есть циклическая группа. □

Замечание. В силу доказанного следствия множество $\langle g\rangle^1_H$ будем называть подгруппой H-тривиальности группы $\langle g\rangle$.

Пример 1.3. Пусть $\langle g\rangle$ — циклическая группа порядка 24, $H(m)$ — наследственное множество всех элементов группы $\langle g\rangle$, порядок которых не превышает m, где $m \leqslant 24$ (см. пример 1.2).

Определим при $m \in \{2, 4\}$ распределение $H(m)$-признака по собственным подгруппам группы $\langle g\rangle$ и множество $H(m)$-тривиальности группы $\langle g\rangle$.

Список собственных подгрупп группы $\langle g\rangle$ имеет вид:

$$\langle g^2\rangle, \langle g^3\rangle, \langle g^4\rangle, \langle g^6\rangle, \langle g^8\rangle, \langle g^{12}\rangle.$$

В примере 1.1 указано, что $\Pi(H(4), g) = \{6, 8\}$ и $H(4) = \langle g^6\rangle \cup \langle g^8\rangle$. Поэтому по теореме 1.7:

1) $\mathrm{prm}\{HOK(6, 2), HOK(8, 2)\}^* = \{6, 8\}$ и $\langle g^2\rangle \cap H(4) = \langle g^6\rangle \cup \langle g^8\rangle$;
2) $\mathrm{prm}\{HOK(6, 3), HOK(8, 3)\}^* = \mathrm{prm}\{6, 24\} = \{6\}$ и $\langle g^3\rangle \cap H(4) = \langle g^6\rangle$;
3) $\mathrm{prm}\{HOK(6, 4), HOK(8, 4)\}^* = \{12, 8\}$ и $\langle g^4\rangle \cap H(4) = \langle g^8\rangle \cup \langle g^{12}\rangle$;
4) $\mathrm{prm}\{HOK(6, 6), HOK(8, 6)\}^* = \mathrm{prm}\{6, 24\} = \{6\}$ и $\langle g^6\rangle \cap H(4) = \langle g^6\rangle$;
5) $\mathrm{prm}\{HOK(6, 8), HOK(8, 8)\}^* = \mathrm{prm}\{24, 8\} = \{8\}$ и $\langle g^8\rangle \cap H(4) = \langle g^8\rangle$;
6) $\mathrm{prm}\{HOK(6, 12), HOK(8, 12)\}^* = \mathrm{prm}\{12, 24\} = \{12\}$ и $\langle g^{12}\rangle \cap H(4) = \langle g^{12}\rangle$.

Используя канонические разложения чисел $24 = 2^3 \cdot 3$, $6 = 2 \cdot 3$, $8 = 2^3$, получаем по следствию теоремы 1.7:

$$\Pi(\langle g\rangle^1_{H(4)}, g) = \{HOK(\mathrm{mp}_{24}(6), \mathrm{mp}_{24}(8))\} = \{HOK(2^3, 3)\} = \{24\},$$

т. е. подгруппа $H(4)$-тривиальности группы $\langle g\rangle$ тривиальна.

В примере 1.1 указано, что $\Pi(H(2), g) = \{12\}$ и $H(2) = \langle g^{12}\rangle$. Поэтому по теореме 1.7:

1) $HOK(12, 2) = \{12\}$ и $\langle g^2\rangle \cap H(2) = \langle g^{12}\rangle$;
2) $HOK(12, 3) = \{12\}$ и $\langle g^3\rangle \cap H(2) = \langle g^{12}\rangle$;
3) $HOK(12, 4) = \{12\}$ и $\langle g^4\rangle \cap H(2) = \langle g^{12}\rangle$;
4) $HOK(12, 6) = \{12\}$ и $\langle g^6\rangle \cap H(2) = \langle g^{12}\rangle$;
5) $HOK(12, 8) = \{24\}$ и $\langle g^8\rangle \cap H(2) = e$;
6) $HOK(12, 12) = \{12\}$ и $\langle g^{12}\rangle \cap H(2) = \langle g^{12}\rangle$.

Используя канонические разложения чисел $24 = 2^3 \cdot 3$, $12 = 2^2 \cdot 3$, получаем по следствию теоремы 1.7:

$$\Pi(\langle g\rangle^1_{H(4)}, g) = \{HOK(\mathrm{mp}_{24}(12)\} = \{HOK(8)\} = \{8\},$$

т. е. подгруппа $H(2)$-тривиальности группы $\langle g\rangle$ равна $\langle g^8\rangle$. ◇

Определение 1.22. *Наследственный H-признак в группе G* назовём *квазиполным*, если $B_G \cap H = \varnothing$ и $\langle g\rangle \subseteq H$, где B_G есть c-базис группы G и $\langle g\rangle$ — любая немаксимальная циклическая подгруппа группы G. ◇

Наличие квазиполного наследственного H-признака в циклической группе $\langle g\rangle$ можно рассматривать как ситуацию, в определённом смысле двойственную к наличию тривиального наследственного H-признака в $\langle g\rangle$ (все элементы группы $\langle g\rangle$, кроме порождающих элементов, принадлежат множеству H).

Утверждение 1.11. а) *Пусть каноническое c-покрытие группы G определено равенством* (1.3). *Тогда группа G имеет квазиполный наследственный H-признак в том и только в том случае, если для любого $g \in B_G$ циклическая группа $\langle g\rangle$ имеет квазиполный наследственный H-признак.*

б) *Циклическая группа* $\langle g\rangle$ *имеет квазиполный наследственный* H*-признак тогда и только тогда, когда множество* $\Pi(H, g)$ *совпадает с множеством всех атомов решётки* $D(n)$.

в) *Пусть* H, H' *— наследственные подмножества группы* Φ, *где* $H \subseteq H'$, *и* $B_G \cap H' = \varnothing$, *где* $G < \Phi$ *и* B_G *есть* c*-базис группы* G. *Тогда если* H*-признак в группе* G *является квазиполным, то и* H'*-признак в группе* G *является квазиполным.*

Доказательство. а) Утверждение вытекает непосредственно из определения 1.22.

б) Из определения 1.22 следует в силу обратного изоморфизма решёток $\langle g\rangle$ и $D(n)$, где $n = \operatorname{ord} g$, что группа $\langle g\rangle$ имеет квазиполный наследственный H-признак в том и только в том случае, если $g \notin H$ и $g^t \in H$ для любого атома t решётки $D(n)$. Отсюда по утверждению 1.9 получаем, что $\Pi(H, g)$ есть множество всех атомов решётки $D(n)$.

в) Пусть $B_G = (g_1, \ldots, g_r)$. По условию H-признак в группе G является квазиполным, тогда по определению 1.22 $B_G \cap H = \varnothing$ и все коатомы решётки $\langle g_i\rangle$ принадлежат множеству H, $i = 1, \ldots, r$.

По условию $H \subseteq H'$, поэтому все коатомы решётки $\langle g_i\rangle$ принадлежат множеству H', $i = 1, \ldots, r$. Так как $B_G \cap H' = \varnothing$, то по определению 1.22 получаем, что H'-признак в группе G является квазиполным. □

Следствие. *Групповой* H*-признак в циклической группе* $\langle g\rangle$ *является квазиполным тогда и только тогда, когда* n *есть степень простого числа* p *и* $\Pi(H, g) = \{p\}$.

Доказательство. Квазиполнота группового H-признака в циклической группе $\langle g\rangle$ по утверждению 1.11,б) равносильна тому, что решётка $D(n)$ имеет единственный атом p, совпадающий с (H, g)-пороговым числом группового H-признака. □

Пример 1.4. Пусть $\langle g\rangle$ — циклическая группа порядка n, где каноническое разложение числа определено равенством (1.7) и $p_1 < \ldots < p_s$. Рассмотрим наследственное множество $H(m)$ всех элементов группы $\langle g\rangle$, порядок которых не превышает m, где $m \leqslant n$.

Используя вид атомов решётки $D(n)$ (см. пример 1.1) и обратный изоморфизм решёток $\langle g\rangle$ и $D(n)$, получаем, что $H(m)$-признак в группе $\langle g\rangle$ является квазиполным тогда и только тогда, когда $\frac{n}{p_1} \leqslant m < n$. ◇

§ 1.3. Свойства некоторых классов функций, определённых на группах

Некоторые свойства групп можно описывать с помощью свойств функций, определённых на этих группах. Рассмотрим классы функций, важные для изучения признаков в группах.

1.3.1. Классы монотонных и нормальных функций, определённых на группах; подфункции функций; задание функций диаграммами. Пусть Y' — множество с квазипорядком, Y — линейно или частично упорядоченное множество, $F(Y', Y)$ — класс функций, определенных на множестве Y', принимающих значения во множестве Y и обладающих свойством: если $g \cong g'$ для $g, g' \in Y'$ (то есть $g \leqslant g'$ и $g' \leqslant g$), то $f(g) = f(g')$.

Определение 1.23. Функция f из $F(Y', Y)$ называется *монотонной* (*антимонотонной*), если из отношения $y' \leqslant y''$ для $y', y'' \in Y'$ следует, что $f(y') \leqslant f(y'')$ $(f(y') \geqslant f(y''))$. ◇

Для произвольного натурального числа p обозначим через $N^{[p]}$ множество всех натуральных чисел, являющимися неотрицательными степенями

числа p, следовательно,

$$N^{[p]} = \{1, p, p^2, \ldots\} \subset N.$$

Определение 1.24. Функцию из $F(Y', N)$ назовём *нормальной*, (*антинормальной, p-нормальной, p-антинормальной*), если из отношения $y' \leqslant y''$ для $y', y'' \in Y'$ следует, что

$$\frac{f(y'')}{f(y')} \in N \left(\frac{f(y')}{f(y'')} \in N, \frac{f(y'')}{f(y')} \in N^{[p]}, \frac{f(y')}{f(y'')} \in N^{[p]}\right). \diamondsuit$$

Класс всех монотонных (антимонотонных, нормальных, антинормальных, p-нормальных, p-антинормальных) функций из $F(Y', N)$ обозначим соответственно через $M(Y', N)$ ($\overline{M}(Y', N)$, $NR(Y', N)$, $\overline{NR}(Y', N)$, $NR^p(Y', N)$, $\overline{NR^p}(Y', N)$).

Из определений 1.23 и 1.24 вытекает утверждение.

Утверждение 1.12. а) *При любом натуральном p*

$$NR^p(Y', N) \subseteq NR(Y', N) \subseteq M(Y', N),$$
$$\overline{NR^p}(Y', N) \subseteq \overline{NR}(Y', N) \subseteq \overline{M}(Y', N).$$

б) *Если функция f из $F(Y', N)$ монотонна (антимонотонна, нормальна, антинормальна, p-нормальна, p-антинормальна), то ограничение функции f на любое подмножество множества Y' также есть монотонная (антимонотонная, нормальная, антинормальная, p-нормальная, p-антинормальная) функция.* $\diamondsuit$

Приведём примеры функций из класса $F(\Phi, N)$ с указанными свойствами.

Пример 1.5. Функция $f(g) = \operatorname{ord} g$ (функция $f(g) = \frac{\operatorname{ord}\Phi}{\operatorname{ord} g}$) является нормальной (антинормальной) и, в силу утверждения 1.12,а), монотонной (антимонотонной).

Если $g' \leqslant g$, то $\langle g' \rangle \subseteq \langle g \rangle$. Значит, $\langle g' \rangle$ есть подгруппа группы $\langle g \rangle$ и $\operatorname{ord} g'$ делит $\operatorname{ord} g$. Следовательно, $\operatorname{ord} g \in NR(\Phi, N)$. $\diamondsuit$

Пример 1.6. Если $\operatorname{ord}\Phi = p^r$, где p — простое, r — натуральное, то функция $f(g) = \operatorname{ord} g$ (функция $f(g) = \frac{\operatorname{ord}\Phi}{\operatorname{ord} g}$) p-нормальна (p-антинормальна).

Порядки элементов g и g' из Φ делят $\operatorname{ord}\Phi$, поэтому $\operatorname{ord} g$ и $\operatorname{ord} g'$ суть натуральные степени числа p. Отсюда и из нормальности функции $\operatorname{ord} g$ (см. пример 1.5) следует p-нормальность этой функции. $\diamondsuit$

Определение 1.25. Пусть $f \in F(\Phi, Y)$ и $g \in \Phi$. Ограничение функции f на циклическую подгруппу $\langle g \rangle$ группы Φ назовём *g-подфункцией функции f*. $\diamondsuit$

Замечание 1. Семейство g-подфункций однозначно задаёт функцию f, если g пробегает все элементы некоторой системы R c-образующих группы Φ (см. определение 1.9). Поэтому из утверждения 1.12,б) получаем следующее утверждение: функция f монотонна (антимонотонна, нормальна, антинормальна, p-нормальна, p-антинормальна) тогда и только тогда, когда при любом $g \in R$ монотонна (антимонотонна, нормальна, антинормальна, p-нормальна, p-антинормальна) g-подфункция функции f. $\diamondsuit$

Замечание 2. Любой элемент группы $\langle g \rangle$ порядка n имеет вид g^t, где $t \in N_n$, поэтому g-подфункцию функции f зададим как функцию $f_g(t)$ из $F(N_n, Y)$, где $f_g(t) = f(g^t)$. $\diamondsuit$

Утверждение 1.13. а) *Функция* $f_g(t)$ *монотонна (антимонотонна) тогда и только тогда, когда для любых* τ, $t \in D(n)$ *таких, что* t *делит* τ, *выполнено:*

$$f_g(t) \geqslant f_g(\tau)$$

$$(f_g(t) \leqslant f_g(\tau)).$$

б) *Функция* $f_g(t)$ *нормальна (антинормальна,* p*-нормальна,* p*-антинормальна) тогда и только тогда, когда для любых* τ, $t \in D(n)$ *таких, что* t *делит* τ, *выполнено:*

$$\frac{f_g(t)}{f_g(\tau)} \in N\left(\frac{f_g(\tau)}{f_g(t)} \in N, \frac{f_g(t)}{f_g(\tau)} \in N^{[p]}, \frac{f_g(\tau)}{f_g(t)} \in N^{[p]}\right).\diamondsuit$$

Стандартным заданием подфункции $f_g(t)$ является таблица: $\{(t, f_g(t))$; $t \in N\}$. Рассмотрим вопросы минимизации задания подфункции $f_g(t)$.

Монотонную (антимонотонную) g-подфункцию достаточно задать на всех элементах фактормножества $\langle g\rangle/\cong$. В силу антиизоморфизма решётки $D(n)$ и решётки всех подгрупп циклической группы $\langle g\rangle$ порядка n это равносильно заданию функции $f_g(t)$ на $D(n)$. Следовательно, её можно задать диаграммой решётки $D(n)$, на которой вершина t помечена величиной $f_g(t)$, $t \in D(n)$. Такое задание функции $f_g(t)$ назовём её *D-диаграммой.*

Для дальнейшей минимизации задания функции с использованием диаграммы с меньшим числом вершин рассмотрим эпиморфизм частично упорядоченных множеств $\mu(t)$: $D(n) \to M$, где $M \subseteq D(n)$. Для $\tau \in M$ обозначим через $f_\mu^\tau(t)$ ограничение функции $f(t)$ на множество тех t, для которых $\mu(t) = \tau$. Пусть Z_f^τ — таблица функции $f_\mu^\tau(t)$ и Y_f^τ — область её значений:

$$Z_f^\tau = \{(t, f(t))\colon\ t \in \{1, \ldots, n\}, \mu(t) = \tau\},$$

$$Y_f^\tau = \{\{f(t)\colon\ t \in \{1, \ldots, n\}, \mu(t) = \tau\}^*.$$

Эпиморфизм $\mu(t)$ индуцирует новое задание функции $f(t)$, связанное с диаграммой частично упорядоченного множества M. При новом задании элементу τ множества M ставится в соответствие множество Z_f^τ. То есть отображение $\mu(t)$ определяет разбиение таблицы функции $f(t)$ на систему наборов $\{Z_f^\tau\}$, $\tau \in M$. Набор Z_f^τ можно рассматривать как метку вершины τ на диаграмме множества M.

Определение 1.26. Диаграмму частично упорядоченного множества M, в которой каждая вершина τ помечена набором Z_f^τ, назовём *M-диаграммой* (при $M = D(n)$ назовём *D-диаграммой*) *функции* $f(t)$.$\diamondsuit$

Обозначим через $\Gamma_M(f)$ (через $\Gamma_D(f)$) ориентированный граф, соответствующий M-диаграмме (D-диаграмме) функции $f(t)$.

Утверждение 1.14. *Пусть* $\mu(t)$ *есть эпиморфизм* $D(n) \to M$, *где* $M \subseteq D(n)$. *Тогда:*

а) *функция* $f(t)$ *монотонна (антимонотонна) в том и только в том случае, когда для любого ориентированного пути* $(\tau_1, \ldots, \tau_k)$ *в графе* $\Gamma_M(f)$ *и любой последовательности* $(f(t_1), \ldots, f(t_k)) \in Y_f^{\tau_1} \times \ldots \times Y_f^{\tau_k}$:

$$f(t_1) \leqslant \ldots \leqslant f(t_k)$$

$$(f(t_1) \geqslant \ldots \geqslant f(t_k));$$

б) *функция* $f(t)$ *нормальна (антинормальна,* p*-нормальна,* p*-антинормальна) в том и только в том случае, когда для любого ориентированного пути* $(\tau_1, \ldots, \tau_k)$ *в графе* $\Gamma_M(f)$ *и любой последовательности*

$(f(t_1), \ldots, f(t_k)) \in Y_f^{\tau_1} \times \ldots \times Y_f^{\tau_k}$:

$$\frac{f(t_i)}{f(t_{i-1})} \in N\left(\frac{f(t_{i-1})}{f(t_i)} \in N,\ \frac{f(t_i)}{f_g(t_{i-1})} \in N^{[p]},\ \frac{f_g(t_{i-1})}{f(t_i)} \in N^{[p]}\right),\ i = 2, \ldots, k.\diamondsuit$$

Доказательство. а) Из монотонности (антимонотонности) функции f по утверждению 13,а) получаем, что каждой цепи решётки $D(n)$ соответствует цепь в частично упорядоченном множестве Y. Вместе с тем, полным прообразом любой цепи в M относительно эпиморфизма $\mu(t)$ является множество цепей в $D(n)$. Следовательно, для любой цепи $(\tau_1, \ldots, \tau_k)$ в M последовательность соответствующих меток $(Y_f^{\tau_1}, \ldots, Y_f^{\tau_k})$, на M-диаграмме такова, что любой элемент $(f_g(t_1), \ldots, f_g(t_k))$ из $Y_f^{\tau_1} \times \ldots \times Y_f^{\tau_k}$ есть цепь в Y.

б) Утверждение доказывается аналогично с использованием утверждения 1.13,б) и свойства нормальности (антинормальности, p-нормальности, p-антинормальности) функции f. □

Следствие. а) *Если функция $f(t)$ монотонна (антимонотонна), то*

$$f(1) \geqslant f(t) \geqslant f(n)$$

$$(f(1) \leqslant f(t) \leqslant f(n)),\ t = 1, \ldots, n.$$

б) *Если функция $f(t)$ нормальна (антинормальна, p-нормальна, p-антинормальна), то при $t = 1, \ldots, n$*

$$\frac{f(1)}{f(t)} \in N \text{ и } \frac{f(t)}{f(n)} \in N.$$

$$\left(\frac{f(t)}{f(1)} \in N \text{ и } \frac{f(n)}{f(t)} \in N,\ \frac{f(1)}{f(t)} \in N^{[p]} \text{ и } \frac{f(t)}{f(n)} \in N^{[p]},\ \frac{f(t)}{f(1)} \in N^{[p]} \text{ и } \frac{f(n)}{f(t)} \in N^{[p]}\right).$$

Доказательство. Рассмотрим D-диаграмму функции $f(t)$ (граф $\Gamma_D(f)$). Для любого $t \in \{1, \ldots, n\}$ в графе $\Gamma_D(f)$ имеется путь из вершины n в вершину 1, проходящий через вершину τ, где $\tau = (t, n)$, так как 1 делит (t, n) и (t, n) делит n. При этом $f(1) \in Y_f^1$, $f(n) \in Y_f^n$ и $f(\tau) \in Y_f^\tau$. Отсюда и из утверждения 1.14 получаем оба следствия. □

Определение 1.27. Если Y_f^τ — одноэлементное множество при любом τ из M (из $D(n)$), то *M-диаграмму (D-диаграмму) функции $f(t)$* назовём *простой*. $\diamondsuit$

Каждая вершина τ простой M-диаграммы функции f в силу определения 1.27 помечена единственным символом $f(t)$, где t таково, что $\mu(t) = \tau$. При этом считаем, что полный прообраз числа τ относительно отображения μ определён. Вершина τ простой D-диаграммы функции f помечена символом $f(\tau)$, так как $(\tau, n) = \tau$.

Одной из величин, характеризующих сложность изучения свойств функции f, определённой на циклической группе, является порядок наименьшего подмножества M решётки $D(n)$, для которого M-диаграмма функции f является простой.

1.3.2. Взаимосвязь наследственных признаков и заданных на конечных группах монотонных и антимонотонных функций. Установим некоторые связи между наследственными признаками конечной группы и заданными на ней монотонными и антимонотонными функциями.

Определение 1.28. Пусть $G < \Phi$. *Характеристической функцией H-признака* в группе G назовём функцию $\psi_H^G \in F(G, \{0, 1\})$, где

$$\psi_H^G(g) = \begin{cases} 1, & g \in G \cap H, \\ 0, & g \in G \setminus H. \end{cases} \diamondsuit$$

Обозначим через $\psi^G_{H,g}(t)$ g-подфункцию характеристической функции ψ^G_H.

Утверждение 1.15. *H-признак в группе G является наследственным тогда и только тогда, когда характеристическая функция ψ^G_H антимонотонна.*

Доказательство. Для $g \in G$ рассмотрим g-подфункцию $\psi^G_{H,g}(t)$.

Пусть $a=(\tau, n)$, $b=(t, n)$ и a/b, тогда по утверждению 1.13,а) антимонотонность функции $\psi^G_{H,g}(t)$ равносильна тому, что

$$\psi^G_{H,g}(a) \leqslant \psi^G_{H,g}(b). \tag{1.10}$$

Докажем, что неравенство (1.10) выполнено тогда и только тогда, когда H-признак в группе G является наследственным.

Неравенство (1.10) в силу определения 1.28 равносильно тому, что из равенства $\psi^G_{H,g}(a)=1$ следует равенство $\psi^G_{H,g}(b)=1$.

Пусть $\psi^G_{H,g}(a)=1$, по определению 1.28 это означает, что $g^a \in H$. Если H-признак в группе G является наследственным, то и $g^b \in H$, так как a/b. Следовательно, по определению 1.28 $\psi^G_{H,g}(b)=1$, т. е. неравенство (1.10) выполнено.

Если H-признак в группе G не является наследственным, то при некотором $g \in G$ выполнено $g \in H$ и $g^b \notin H$, где $b \in \{1, \ldots, \operatorname{ord} g\}$. Значит, при этом g выполнены равенства: $\psi^G_{H,g}(1)=1$, $\psi^G_{H,g}(b)=0$, т. е. неравенство (1.10) при указанном g и $a=1$ не выполнено. □

Для любой монотонной функции f из $F(\Phi, Y)$ можно определить «двойственную» ей антимонотонную функцию f' из $F(\Phi, Y)$, и наоборот. Например, «двойственной» к антимонотонной характеристической функции ψ^G_H можно считать монотонную инвертированную функцию $\psi^G_H \oplus 1$. В связи с этим некоторые утверждения для монотонных функций можно симметричным образом сформулировать и для антимонотонных функций.

Пусть $f \in F(\Phi, Y)$, $y \in Y$, $G < \Phi$. Множество всех элементов g группы G, удовлетворяющих при $y \in Y$ условию $f(g) \geqslant y$ ($f(g) \leqslant y$), обозначим $G(f \geqslant y)$ ($G(f \leqslant y)$). Без ущерба для общности считаем, что функция f сюръективна.

Теорема 1.8. а) *Если функция f монотонна (антимонотонна), то при любом $y \in Y$ множество $G(f \leqslant y)$ (множество $G(f \geqslant y)$) является наследственным. Вследствие этого группа G имеет наследственный $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак).*

б) *Если группа G имеет наследственный H-признак, то существует монотонная (антимонотонная) на группе G функция f такая, что $G \cap H = G(f \geqslant y)$ ($G \cap H = G(f \leqslant y)$) при некотором $y \in Y$.*

Доказательство. а) Пусть функция f монотонна (антимонотонна). Тогда по следствию а) утверждения 1.14 $f_g(1) \geqslant f_g(t)$ ($f_g(1) \leqslant f_g(t)$) при любом $g \in G$ и $t=1, \ldots, n$. Поэтому если $f_g(1) \leqslant y$ ($f_g(1) \geqslant y$), то и $f_g(t) \leqslant y$ ($f_g(t) \geqslant y$), где множество $G(f \geqslant y)$ (множество $G(f \leqslant y)$) не пусто при любом $y \in Y$.

Значит, для любого $g \in G$ имеем: если выполнено включение $g \in G(f \leqslant y)$ (включение $g \in G(f \geqslant y)$), то выполнено и включение $g^t \in G(f \leqslant y)$ (включение $g^t \in G(f \geqslant y)$), $t=1, \ldots, n$. Следовательно, множество $G(f \leqslant y)$ (множество $G(f \geqslant y)$) является наследственным. По определению 1.14 это означает, что группа G имеет наследственный $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак).

б) Если группа G имеет наследственный H-признак, то по утверждению 1.15 характеристическая функция ψ^G_H антимонотонна и из определе-

ния 1.28 следует, что $G \cap H = G(\psi_H^G \geqslant 1)$. При этом двойственная ей функция $\psi_H^G \oplus 1$ является монотонной и $G \cap H = G(\psi_H^G \oplus 1 \leqslant 0)$. □

Следствие 1. *Пусть функция f монотонна (антимонотонна) и $y \in Y$. Тогда $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) в группе G является тривиальным в том и только в том случае, когда для любого элемента g c-базиса группы G и любого коатома t решётки $D(n)$, где $n = \operatorname{ord} g$, выполнены неравенства:*

$$f_g(n) \leqslant y, f_g(t) > y$$

$$(f_g(n) \geqslant y, f_g(t) < y).$$

Доказательство. По теореме 1.8 $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) в группе G и, следовательно, в любой её подгруппе является наследственным. Отсюда по утверждению 1.8,в) $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) в группе G является тривиальным тогда и только тогда, когда этот признак тривиален в циклической группе $\langle g \rangle$ для любого элемента g c-базиса группы G.

В силу замечания 2 к определению 1.14 наследственный $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) в циклической группе $\langle g \rangle$ является тривиальным тогда и только тогда, когда $G(f \leqslant y) = \{e\}$ ($G(f \geqslant y) = \{e\}$). Это равносильно тому, что $f_g(n) \leqslant y$ и $f_g(t) > y$ ($f_g(n) \geqslant y$ и $f_g(t) < y$) для любого $t = 1, \ldots, n-1$.

Вместе с тем, так как функция $f_g(t)$ монотонна (антимонотонна), то по утверждению 1.13 $f_g(t) \geqslant f_g(\tau)$ ($f_g(t) \leqslant f_g(\tau)$) для любых τ, $t \in N_n$ таких, что $t \rho \tau$.

Следовательно, $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) является тривиальным в группе $\langle g \rangle$ тогда и только тогда, когда $f_g(n) \leqslant y$ и $f_g(t) > y$ ($f_g(n) \geqslant y$ и $f_g(t) < y$) для любого $t \in D(n) \setminus \{n\}$.

Пусть $t_1, \ldots, t_s$ суть все коатомы решётки $D(n)$ (см. пример 1.1). Тогда по свойству коатомов для любого элемента $t \in D(n) \setminus \{n\}$ найдётся номер $j \in \{1, \ldots, s\}$ такой, что $t \leqslant t_j$. Отсюда, неравенства $f_g(t) > y$ ($f_g(t) < y$) выполнены для любого $t \in D(n) \setminus \{n\}$ тогда и только тогда, когда они выполнены для всех коатомов $t_1, \ldots, t_s$ решётки $D(n)$.

Таким образом, $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) является тривиальным в группе $\langle g \rangle$ тогда и только тогда, когда $f_g(n) \leqslant y$ и $f_g(t) > y$ ($f_g(n) \geqslant y$ и $f_g(t) < y$) для любого коатома t решётки $D(n)$. □

Следствие 2. *Наследственный H-признак в группе $\langle g \rangle$ является тривиальным в том и только в том случае, когда $\psi_{H,g}^G(n) = 1$ и $\psi_{H,g}^G(t) = 0$ для любого коатома t решётки $D(n)$.*

Доказательство. По утверждению 1.15 характеристическая функция ψ_H^G наследственного H-признака является антимонотонной. Отсюда и из определения 1.28 получаем по следствию 1 теоремы 1.8, что H-признак тривиален в группе $\langle g \rangle$ тогда и только тогда, когда $\psi_{H,g}^G(n) = 1$ и $\psi_{H,g}^G(t) = 0$ для любого коатома t решётки $D(n)$. □

Следствие 3. *Пусть функция f монотонна (антимонотонна) и $y \in Y$. Тогда $G(f \leqslant y)$-признак ($G(f \geqslant y)$-признак) в группе G является квазиполным в том и только в том случае, когда для любого элемента g c-базиса группы G и любого атома t решётки $D(n)$, где $n = \operatorname{ord} g$, выполнены неравенства:*

$$f_g(1) > y, f_g(t) \leqslant y$$

$$(f_g(1) < y, f_g(t) \geqslant y).$$

Доказательство. Из определения множества $G(f \leqslant y)$ (множества $G(f \geqslant y)$) следует, что для $g \in \Phi$ неравенства $f_g(1) > y$ и $f_g(t) \leqslant y$ ($f_g(1) < y$ и $f_g(t) \geqslant y$) равносильны соответственно отношениям: $g \notin G(f \leqslant y)$ и $g^t \in G(f \leqslant y)$ ($g \notin G(f \geqslant y)$ и $g^t \in G(f \geqslant y)$). Поэтому по утверждению 1.9 выполнение этих неравенств для любого атома t решётки $D(n)$ равносильно тому, что множество $\Pi(G(f \leqslant y), g)$ (множество $\Pi(G(f \geqslant y), g)$) есть множество всех атомов решётки $D(n)$.

Отсюда по утверждению 1.11,б) получаем, что при выполнении данных неравенств для любого атома t решётки $D(n)$ циклическая группа $\langle g \rangle$ имеет квазиполный наследственный H-признак.

В силу произвольности рассмотренного неединичного элемента $g \in \Phi$ из утверждения 1.11,а) вытекает требуемое утверждение. □

Следствие 4. *Наследственный H-признак в группе $\langle g \rangle$ является квазиполным в том и только в том случае, когда $\psi^G_{H,g}(1) = 0$ и равенство $\psi^G_{H,g}(t) = 1$ выполнено для любого атома t решётки $D(n)$.*

Доказательство. По утверждению 1.15 характеристическая функция ψ^G_H наследственного H-признака является антимонотонной. Отсюда и из определения 1.28 получаем по следствию 3 теоремы 1.8, что H-признак в группе $\langle g \rangle$ является квазиполным тогда и только тогда, когда $\psi^G_{H,g}(1) = 0$ и равенство $\psi^G_{H,g}(t) = 1$ выполнено для любого атома t решётки $D(n)$. □

ГЛАВА II

ИССЛЕДОВАНИЕ НАСЛЕДСТВЕННЫХ ПРИЗНАКОВ В ГРУППАХ ПОДСТАНОВОК

Пусть $\Phi(X)$ — группа всех подстановок конечного множества X, $G < \Phi(X)$ и H — множество подстановок из группы $\Phi(X)$, графы которых обладают определённым свойством, например все циклы подстановок из H имеют нечетные длины. Соответствующий H-признак назовем структурным признаком в группе подстановок. Исследование ряда характеристик наследственного H-признака в группе подстановок g, как показано в пункте 1.2.3, можно свести к исследованию соответствующих характеристик H-признака в циклических подгруппах группы g, образующих каноническое c-покрытие группы g. Поэтому основное внимание в главе II уделено исследованию наследственных H-признаков в циклической группе подстановок.

Метод изучения основан на установленной в теореме 1.8 связи наследственных признаков с монотонными и антимонотонными функциями, определёнными на группе подстановок $\Phi(X)$. Выявление таких функций для некоторых приложений представляет собой самостоятельную задачу, для решения которой требуется, как представляется автору, определённая исследовательская интуиция.

Далее при изучении наследственного H-признака в циклической группе $\langle g \rangle$, где $g \in \Phi(X)$, считаем, что $\operatorname{ord} g = n$. При изучении некоторых признаков сделаны дополнительные предположения об алгебраических свойствах множества X.

§ 2.1. Некоторые свойства цикловых структур подстановок

2.1.1. Определяющие свойства цикловых структур подстановок. Напомним некоторые определения и утверждения, необходимые для последующего изложения.

Определение 2.1. *Графом преобразования* g множества X (обозначается Γ_g) называется орграф с множеством вершин X и множеством дуг $(x, g(x))$, где $x \in X$. $\diamondsuit$

Граф Γ_g подстановки g множества X состоит из k независимых циклов без подходов, $1 \leqslant k \leqslant |X|$ ([6, гл. XI, теорема 17]).

Определение 2.2. Если граф Γ_g состоит из k_i циклов длины l_i, $i = 1, \ldots, m$, где $k_1, \ldots, k_m$ — натуральные числа, и $\{l_1, \ldots, l_m\}$ — набор попарно различных натуральных чисел, то говорят, что подстановка g имеет *цикловую структуру* $C(g)$:

$$C(g) = (l_1^{k_1}, \ldots, l_m^{k_m}).$$

Набор $(l_1, \ldots, l_m)$ всех длин циклов подстановки g назовём *редукцией цикловой структуры* подстановки g, набор $(k_1, \ldots, k_m)$ назовём *набором кратностей длин циклов*. $\diamondsuit$

Обозначим: $L(g) = (l_1, \ldots, l_m)$, $K(g) = (k_1, \ldots, k_m)$. В этих обозначениях используем символическую запись: $C(g) = L^K$.

Если из контекста ясно, какая подстановка g рассматривается, используем краткие обозначения: $L = (l_1, \ldots, l_m)$, $K = (k_1, \ldots, k_m)$.

Из определения 2.2 следует, что наборы $L(g)$ и $K(g)$ связаны соотношениями:

$$\sum_{i=1}^{m} l_i \cdot k_i = |X|.$$

Определение 2.3. *Подстановку* g множества X назовём *равноцикловой*, если она состоит из циклов одинаковой длины. $\diamondsuit$

Цикловая структура равноцикловой подстановки g есть $C(g) = (l^k)$, где $l \cdot k = |X|$.

Пример 2.1. Тождественная подстановка e множества X имеет цикловую структуру $C(e) = (1^{|X|})$ и редукцию цикловой структуры $L(e) = (1)$. Следовательно, тождественная подстановка e является равноцикловой. Цикловая структура всех других подстановок множества X отличается от $C(e)$. $\diamondsuit$

По теореме 18 [6, гл. XI] $\operatorname{ord} g = НОК\{l_1, \ldots, l_m\}$. Значит, набор $L(g)$ можно рассматривать как подмножество решётки $D(n)$, где $n = \operatorname{ord} g$.

Отметим некоторые связи между элементами цикловых структур различных подстановок, в частности, подстановок циклической группы.

Определение 2.4 [11, гл. I, § 3]. Подстановки g и g' множества X называются *сопряжёнными* или *подобными*, если найдётся подстановка h того же множества, при которой $g' = h^{-1} \cdot g \cdot h$. $\diamondsuit$

Отношение подобия на множестве подстановок есть отношение эквивалентности.

Утверждение 2.1. *Следующие предложения равносильны:*

1) *подстановки* g *и* g' *подобны;*

2) *графы* Γ_g *и* Γ'_g *изоморфны;*

3) $C(g) = C(g')$. $\diamondsuit$

Пусть X' есть последовательность всех элементов цикла длины l подстановки g, где $X' \subseteq X$, $x \in X'$, $l \in \{l_1, \ldots, l_m\}$:

$$X' = (x, g(x), \ldots, g^{l-1}(x)).$$

Из правила возведения цикла в степень t, где t — натуральное число, вытекают следующие факты.

Утверждение 2.2. *Пусть* $(t, l) = d$. *Тогда цикл* X' *длины* l *при возведении в степень* t *(в степень* d*) разбивается на* d *независимых*

циклов $Y_0'(t), \ldots, Y_{d-1}'(t)$ *(на* d *независимых циклов* $Y_0'(d), \ldots, Y_{d-1}'(d)$*) длины* $\nu^t(l)$, *где*

$$\nu^t(l) = \frac{l}{(t, l)} \tag{2.1}$$

и множества $Y_i'(t)$ *и* $Y_i'(d)$ *состоят из элементов* $g^j(x), g^{j+d}(x), \ldots$ $\ldots, g^{j+i\cdot d}(x), \ldots$, *т. е. циклы совпадают с точностью до порядка следования элементов,* $i = 0, \ldots, d-1$. ◇

Обозначим через $\pi_t(X')$ разбиение множества элементов цикла X' на блоки $Y_0'(t), \ldots, Y_{d-1}'(t)$, образующиеся при возведении цикла в степень t.

Замечание. Из равенства (2.1) непосредственно следует:

1) $\nu^t(l)/l$;

2) для любых натуральных τ и t выполнено равенство $\nu^{\tau\cdot t}(l) = \nu^\tau(\nu^t(l))$;

3) $\nu^t(l) = \nu^d(l)$ тогда и только тогда, когда $(t, l) = d$;

4) $\pi_t(X') = \pi_d(X')$ тогда и только тогда, когда $(t, l) = d$. ◇

Занумеруем все циклы подстановки g числами от 1 до k, где $k = k_1 + \ldots$ $\ldots + k_m$, и пусть X_i есть множество элементов i-го цикла, $i = 1, \ldots, k$:

$$X_i = (x_i, g(x_i), \ldots, g^{r_i-1}(x_i)),$$

где x_i — элемент i-го цикла, r_i — длина i-го цикла, $r_i \in \{l_1, \ldots, l_m\}$.

Обозначим через $\pi(g)$ разбиение множества X на блоки X_i, $i = 1, \ldots, k$, образуемые циклами подстановки g. Из утверждения 2.2 и замечаний 3, 4 к этому утверждению вытекают следующие факты.

Утверждение 2.3. *Пусть* $(t, n) = d$. *Тогда между множествами циклов подстановок* g^t *и* g^d *имеется биекция, при которой соответствующие циклы совпадают с точностью до порядка следования элементов. Вследствие этого:*

1) $C(g^t) = C(g^d)$ *тогда и только тогда, когда* $(t, n) = d$;

2) *число различных цикловых структур подстановок циклической группы* $\langle g\rangle$ *равно* $|D(n)|$;

3) *разбиение* $\pi(g^t)$ *является продолжением разбиения* $\pi(g)$ *и* $\pi(g^t) = \pi(g^d)$ *тогда и только тогда, когда* $(t, n) = d$. ◇

Замечание. В соответствии с принятыми обозначениями N^m есть множество всех наборов из m натуральных чисел. Следовательно, множество цикловых структур (редукций цикловых структур) всех подстановок конечных множеств может быть задано как множество C'' (множество C'):

$$C'' = \bigcup_{m=1}^{\infty} N^{2m}; \quad C' = \bigcup_{m=1}^{\infty} N^m.$$

Следовательно, цикловую структуру $C(g)$ (редукцию цикловой структуры $L(g)$) подстановки g можно рассматривать как функцию, определённую на группе $\Phi(X)$, т. е. $C(g)\colon \Phi(X) \to C''$ ($L(g)\colon \Phi(X) \to C'$).

Из утверждения 2.3. следует, что имеется биекция между множеством цикловых структур подстановок циклической группы $\langle g\rangle$ и множеством делителей числа n, где $n = \operatorname{ord} g$. Отсюда получаем, что D-диаграмма подфункции $C_g(t)$ функции $C(g)$ является простой при любой подстановке $g \in \Phi(X)$ (см. определения 1.26 и 1.27). ◇

2.1.2. Соотношения между длинами циклов подстановок циклической группы. Пусть далее $g \in \Phi(X)$, $\operatorname{ord} g = n$, $C(g) = L^K$, где $L = (l_1, \ldots, l_m)$ и $K = (k_1, \ldots, k_m)$, и для определённости положим, что элементы набора L упорядочены: $l_1 < \ldots < l_m$.

Заметим, что обобщённое каноническое разложение любого делителя числа n есть произведение неотрицательных степеней тех же простых чисел, которые образуют каноническое разложение числа n (равенство (1.7)).

Исследуем, как изменяются соотношения между длинами циклов подстановки g при возведении её в степень.

Утверждение 2.4. *Для натуральных чисел l, l', l'' и t выполнено:*

а) *если l'/l, то $\nu^t(l')$ делит $\nu^t(l)$, при этом $\nu^t(l') = \nu^t(l)$ тогда и только тогда, когда t кратно $\mathrm{mp}_l(l')$;*

б) *пусть l' не делит l и $n = НОК(l, l')$, тогда $\nu^t(l')$ делит $\nu^t(l)$ в том и только в том случае, когда t кратно $\mathrm{mp}_n(l)$, при этом $\nu^t(l') = \nu^t(l)$ тогда и только тогда, когда t кратно $\mathrm{mp}_n(l)\cdot\mathrm{mp}_n(l')$;*

в) *если $l = НОК(l', l'')$, то $\nu^t(l) = НОК(\nu^t(l'), \nu^t(l''))$;*

г) *пусть $l \neq НОК(l', l'')$, $n = НОК(l', l'')$ и $w = НОК(l, l', l'')$, тогда $\nu^t(l) = НОК(\nu^t(l'), \nu^t(l''))$ в том и только в том случае, когда число t кратно числу $\mathrm{mp}_w(l)\cdot\mathrm{mp}_w(n)$.*

Доказательство. а) Пусть каноническое разложение числа l есть

$$l = p_1^{t_1}\cdot\ldots\cdot p_s^{t_s}, \tag{2.2}$$

где $p_1, \ldots, p_s$ — попарно различные простые числа и $t_1, \ldots, t_s$ — натуральные числа. Тогда справедливо разложение:

$$l' = p_1^{\tau_1}\cdot\ldots\cdot p_s^{\tau_s}, \tag{2.3}$$

где $\tau_1, \ldots, \tau_s$ — целые неотрицательные числа, в силу условий удовлетворяющие неравенствам $\tau_i \leqslant t_i$, $i = 1, \ldots, s$.

Любое натуральное число t можно представить в виде:

$$t = p_1^{\theta_1}\cdot\ldots\cdot p_s^{\theta_s}\cdot r, \tag{2.4}$$

где $\theta_1, \ldots, \theta_s$ — целые неотрицательные числа и $НОД(p_1^{\theta_1}\cdot\ldots\cdot p_s^{\theta_s}, r) = 1$. Отсюда по формуле 2.1 получаем, что

$$\nu^t(l) = p_1^{\max(t_1-\theta_1,0)}\cdot\ldots\cdot p_s^{\max(t_s-\theta_s,0)},\ \nu^t(l') = p_1^{\max(\tau_1-\theta_1,0)}\cdot\ldots\cdot p_s^{\max(\tau_s-\theta_s,0)}.$$

В силу неравенств $\tau_i \leqslant t_i$ выполнены и неравенства

$$\max\{\tau_i-\theta_i, 0\} \leqslant \max\{t_i-\theta_i, 0\},\ i = 1, \ldots, s,$$

поэтому $\nu^t(l')$ делит $\nu^t(l)$.

Множество номеров $\{1, \ldots, s\}$ можно разбить на 2 блока $\{i_1, \ldots, i_\nu\}$ и $\{j_1, \ldots, j_{s-\nu}\}$ по следующему правилу: $i \in \{i_1, \ldots, i_\nu\}$, если $t_i > \tau_i$, и $i \in \{j_1, \ldots, j_{s-\nu}\}$, если $t_i = \tau_i$. Без ущерба для общности можно считать, что

$$\{i_1, \ldots, i_\nu\} = \{1, \ldots, \nu\},\ \{j_1, \ldots, j_{s-\nu}\} = \{\nu+1, \ldots, s\}.$$

В этих условиях $\mathrm{mp}_l(l') = p_1^{t_1}\cdot\ldots\cdot p_\nu^{t_\nu}$, и по формуле (2.1) получаем для $t = \mathrm{mp}_l(l')$:

$$\nu^t(l) = p_{\nu+1}^{t_{\nu+1}}\cdot\ldots\cdot p_s^{t_s} = p_{\nu+1}^{\tau_{\nu+1}}\cdot\ldots\cdot p_s^{\tau_s} = \nu^t(l').$$

Отсюда по утверждению 2.2 $\nu^t(l) = \nu^t(l')$ и при любом t, кратном числу $\mathrm{mp}_l(l')$.

Пусть теперь число t не кратно $\mathrm{mp}_l(l')$. Это равносильно тому, что число t имеет вид (2.4), где $\theta_i < t_i$ для некоторого $i \in \{1, \ldots, \nu\}$. Без ущерба для общности можно считать, что $\theta_1 < t_1$. Тогда, используя формулу (2.1), получаем, что $\nu^t(l)$ делится на $p_1^{t_1-\theta_1}$, где $t_1 - \theta_1 > 0$, и $\nu^t(l')$ не делится на $p_1^{t_1-\theta_1}$. Значит, $\nu^t(l) \neq \nu^t(l')$ при t, не кратном числу $\mathrm{mp}_l(l')$.

б) Пусть каноническое разложение числа n определено равенством (1.7). Тогда для чисел l и l' справедливы разложения (2.2) и (2.3) соответственно, где $t_1, \ldots, t_s, \tau_1, \ldots, \tau_s$ — целые неотрицательные числа, связанные равенствами $k_i = \max\{t_i, \tau_i\}$, $i = 1, \ldots, s$.

Множество номеров $\{1, \ldots, s\}$ можно разбить на 3 подмножества:

$$\{1, \ldots, s\} = \{i_1, \ldots, i_\nu\} \cup \{j_1, \ldots, j_u\} \cup \{r_1, \ldots, r_{s-\nu-u}\}$$

по следующему правилу: $i \in \{i_1, \ldots, i_\nu\}$, если $t_i < \tau_i$, $i \in \{j_1, \ldots, j_u\}$, если $t_i > \tau_i$ и $i \in \{r_1, \ldots, r_{s-\nu-u}\}$, если $t_i = \tau_i$. Так как l' не делит l, то $\{i_1, \ldots, i_\nu\} \neq \neq \varnothing$. Без ущерба для общности можно считать, что $\{i_1, \ldots, i_\nu\} = \{1, \ldots, \nu\}$ и $\{j_1, \ldots, j_u\} = \{\nu+1, \ldots, \nu+u\}$. В этих условиях

$$\mathrm{mp}_n(l) = p_1^{k_1} \cdot \ldots \cdot p_\nu^{k_\nu} = p_1^{\tau_1} \cdot \ldots \cdot p_\nu^{\tau_\nu}.$$

При оговоренных условиях получаем по формуле (2.1) для $t = \mathrm{mp}_n(l)$:

$$\nu^t(l) = p_{\nu+1}^{t_{\nu+1}} \cdot \ldots \cdot p_s^{t_s},$$
$$\nu^t(l') = p_{\nu+1}^{\tau_{\nu+1}} \cdot \ldots \cdot p_s^{\tau_s}.$$

Отсюда следует, что при $t = \mathrm{mp}_n(l)$ число $\nu^t(l')$ делит число $\nu^t(l)$. Следовательно, по утверждению 2.4,а) $\nu^t(l')$ делит $\nu^t(l)$ и при любом t, кратном числу $\mathrm{mp}_n(l)$.

Пусть теперь число t не кратно $\mathrm{mp}_n(l)$. Это равносильно тому, что число t имеет вид (2.4), где $\theta_i < \tau_i$ для некоторого $i \in \{1, \ldots, \nu\}$. Без ущерба для общности можно считать, что $\theta_1 < \tau_1$. Тогда, используя формулу (2.1), получаем, что $\nu^t(l')$ делится на $p_1^{\tau_1-\theta_1}$, где $\tau_1 - \theta_1 > 0$, и $\nu^t(l)$ не делится на $p_1^{\tau_1-\theta_1}$. Значит, число $\nu^t(l')$ не делит $\nu^t(l)$ при t, не кратном числу $\mathrm{mp}_l(l')$.

Так как $\nu^t(l')$ делит $\nu^t(l)$ при $t = \mathrm{mp}_n(l)$, то из утверждения 2.4,а) следует, что $\nu^\tau(\nu^t(l')) = \nu^\tau(\nu^t(l))$ тогда и только тогда, когда τ кратно $\mathrm{mp}_q(\nu^t(l'))$, где $q = HOK(\nu^t(l), \nu^t(l'))$.

В данных условиях $q = \nu^t(l)$ и

$$\mathrm{mp}_q(\nu^t(l')) = p_{\nu+1}^{\tau_{\nu+1}} \cdot \ldots \cdot p_{\nu+u}^{\tau_{\nu+u}} = \mathrm{mp}_n(l').$$

Следовательно, равенство $\nu^t(l') = \nu^t(l)$ выполнено тогда и только тогда, когда число t кратно $\mathrm{mp}_n(l) \cdot \mathrm{mp}_n(l')$.

в) Пусть $l' = d \cdot a$, $l'' = d \cdot b$, где $d = (l', l'')$ и $(a, b) = 1$. Тогда $l = = d \cdot a \cdot b$. Отсюда при любом натуральном t число (l, t) можно однозначно представить в виде:

$$(l, t) = d_t \cdot a_\tau \cdot b_\tau,$$

где сомножители в правой части обозначают следующие величины:

$$d_t = (d, t), \tau = \frac{t}{d_t}, a_\tau = (a, \tau), b_\tau = (b, \tau),$$

при этом однозначность величин a_τ и b_τ следует из однозначности величины d_t и взаимной простоты чисел a и b. Следовательно, по формуле (2.1) получаем:

$$\nu^t(l) = \frac{d}{d_t} \cdot \frac{a}{a_\tau} \cdot \frac{b}{b_\tau},$$

где $(\frac{a}{a_\tau}, \frac{b}{b_\tau}) = 1$ в силу того, что $(a, b) = 1$. В данных обозначениях $\nu^t(l') = \frac{d}{d_t}, \frac{a}{a_\tau}$, $\nu^t(l'') = \frac{d}{d_t} \cdot \frac{b}{b_\tau}$. Учитывая, что $(\frac{a}{a_\tau} \cdot \frac{b}{b_\tau}) = 1$, получаем отсюда утверждение 2.4,в).

г) По утверждению 2.4,в) $\nu^t(n) = HOK(\nu^t(l'), \nu^t(l''))$. Следовательно, $\nu^t(l) = HOK(\nu^t(l'), \nu^t(l''))$ в том и только в том случае, когда $\nu^t(l) = \nu^t(n)$.

Так как $HOK(l, n) = w$, то из утверждений 2.4,а) и 2.4,б) следует, что равенство $\nu^t(l) = \nu^t(n)$ выполнено в том и только в том случае, когда t кратно числу $\mathrm{mp}_w(l) \cdot \mathrm{mp}_w(n)$. □

2.1.3. Свойства доминирования в редукциях цикловых структур подстановок циклической группы. Исследуем некоторые свойства цикловых структур и их редукций как свойства числовых наборов, отвлекаясь от понятия подстановки.

Рассмотрим множество натуральных чисел $L = \{l_1, \ldots, l_m\}$.

Определение 2.5. Число l_i, где $i \in \{1, \ldots, m\}$, назовём *доминирующим во множестве* L (или L*-доминирующим*), если l_i не делит никакого другого числа из множества L.

Множество всех L-доминирующих чисел (обозначается $\mathrm{dom}\, L$) назовём *доминантой множества* L. ◇

Таким образом, $\mathrm{dom}\, L$ есть подмножество всех максимальных элементов [2, гл. I, § 3] множества M по отношению делимости натуральных чисел.

Если M — набор не обязательно различных натуральных чисел, то символом $\mathrm{dom}\, M^*$ обозначим множество $\mathrm{dom}(M^*)$, где M^* — редукция набора M (см. определение 1.18).

Множество L можно рассматривать как подмножество решётки $D(n)$ натуральных делителей числа n, где $n = HOK\{l_1, \ldots, l_m\}$. Поэтому из определения 2.5 следует, что множество $\mathrm{dom}\, L$ либо состоит из одного элемента, либо образует антицепь в $D(n)$.

Утверждение 2.5. а) *Множество* L *при* $m > 1$ *является антицепью в решётке* $D(n)$ *тогда и только тогда, когда* $L = \mathrm{dom}\, L = \mathrm{prm}\, L$.

б) *Если* L *— цепь в* $D(n)$, *то* $|\mathrm{dom}\, L| = |\mathrm{prm}\, L| = 1$.

Доказательство. а) Множество L является антицепью в $D(n)$, если любые два элемента из L попарно несравнимы. Это равносильно тому, что каждое число из L является одновременно и L-доминирующим, и L-простым.

б) Если L — цепь в $D(n)$, то по определениям 2.5 и 1.17 соответственно $\mathrm{dom}\, L = \{\max\{l_1, \ldots, l_m\}\}$ и $\mathrm{prm}\, L = \{\min\{l_1, \ldots, l_m\}\}$. □

Пусть далее $\mathrm{dom}\, L(g) = \{l_1, \ldots, l_d\}$, где $1 \leqslant d \leqslant m$. Исследуем, как изменяются порядки множеств $L(g)$ и $\mathrm{dom}\, L(g)$ при возведении подстановки g в натуральную степень.

Множество $\mathrm{dom}\, L(g)$ является важной характеристикой подстановки g. Например, из определения 2.5 следует, что порядок подстановки g вполне определяется множеством $\mathrm{dom}\, L(g)$. Теорему 18 [6, гл. XI] можно уточнить, а именно: $\mathrm{ord}\, g = HOK(l_1, \ldots, l_d)$.

Определение 2.6. *Подстановку* g назовём d*-доминантной*, d — натуральное, если $|\mathrm{dom}\, L(g)| = d$, в частности, *унидоминантной*, если $|\mathrm{dom}\, L(g)| = 1$. ◇

Если g — унидоминантная подстановка и число l доминирует в наборе $L(g)$, то $\mathrm{ord}\, g = l$.

Пример 2.2. Унидоминантной подстановкой является:

а) равноцикловая подстановка g с циклами длины l, так как $L(g) = \{l\}$ (в частности, тождественная подстановка e);

б) подстановка g, у которой редукция цикловой структуры $L(g)$ образует цепь в решётке $D(n)$. ◇

Утверждение 2.6. *При любом натуральном* t:

а) $|L(g^t)| \leqslant m$ *и набор чисел* $L(g^t)$ *содержит ровно* r *различных чисел, где* $r \leqslant m$, *тогда и только тогда, когда редуцированный набор чисел* $\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*$ *содержит ровно* r *различных чисел;*

б) $|\operatorname{dom} L(g^t)| \leqslant d$ *и подстановка* g^t *является* r*-доминантной, где* $r \leqslant d$, *тогда и только тогда, когда редуцированный набор чисел* $\{\nu^t(l_1), \ldots, \nu^t(l_d)\}^*$ *содержит ровно* r *доминирующих чисел.*

Доказательство. Из равенства (2.1) следует, что все различные длины циклов подстановки g^t есть все различные элементы множества чисел $\{\nu^t(l_1), \ldots, \nu^t(l_m)\}$, т. е.

$$L(g^t) = \{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*.$$

Отсюда следует утверждение 2.6,а), а также следует равенство:

$$\operatorname{dom} L(g^t) = \operatorname{dom}\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*.$$

Вместе с тем, так как $l_i \notin \operatorname{dom} L(g)$ для $i = d+1, \ldots, m$, то найдётся число $j \in \{1, \ldots, d\}$ такое, что $l_j \in \operatorname{dom} L(g)$ и l_i / l_j. Тогда по утверждению 2.4,а) $\nu^t(l_i)/\nu^t(l_j)$. Значит, либо $\nu^t(l_i) = \nu^t(l_j)$, либо $\nu^t(l_i)/\nu^t(l_j)$ и $\nu^t(l_i) \neq \nu^t(l_j)$.

Отсюда следует, что для любого из чисел $\nu^t(l_{d+1}), \ldots, \nu^t(l_m)$ найдётся кратное ему число в наборе $\{\nu^t(l_1), \ldots, \nu^t(l_d)\}$, поэтому по определению 2.5

$$\operatorname{dom}\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^* = \operatorname{dom}\{\nu^t(l_1), \ldots, \nu^t(l_d)\}^*.$$

Следовательно, при любом натуральном t:

$$\operatorname{dom} L(g^t) = \operatorname{dom}\{\nu^t(l_1), \ldots, \nu^t(l_d)\}^*.$$

Отсюда непосредственно следует утверждение 2.6,б). □

Следствие. *Подстановка* g^t *является унидоминантной тогда и только тогда, когда множество чисел* $\{\nu^t(l_1), \ldots, \nu^t(l_d)\}^*$ *содержит единственное доминирующее число.* ◇

2.1.4. Свойства замкнутости сверху в редукциях цикловых структур подстановок. Рассмотрим множество натуральных чисел $L = \{l_1, \ldots, l_m\}$.

Определение 2.7. *Верхним замыканием множества* L (обозначается $\lceil L \rceil$) назовём верхнюю подполурешётку [7, гл. I, § 1] решётки $D(n)$, порождённую множеством L. ◇

Множество $\lceil L \rceil$ состоит из всех чисел вида $HOK(l_{i_1}, \ldots, l_{i_s})$, где $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, m\}$, $1 \leqslant s \leqslant m$.

Определение 2.8. Множество L назовём *замкнутым сверху*, если $\lceil L \rceil = L$. ◇

Определение 2.9. Пусть $\varnothing \neq M \subseteq L$. Подмножество M назовём *замкнутым сверху во множестве* L, если $\lceil M \rceil \subseteq L$. ◇

Замечание. Из определения 2.9 следует, что:

1) число l_i замкнуто сверху во множестве L, $i = 1, \ldots, m$;

2) пара чисел (l_i, l_j), где $l_i, l_j \in L$, замкнута сверху во множестве L тогда и только тогда, когда $HOK(l_i, l_j) \in L$. ◇

Утверждение 2.7. *Множество* L *замкнуто сверху тогда и только тогда, когда любая пара чисел из* L *замкнута сверху во множестве* L.

Доказательство. Если множество L замкнуто сверху, то из определений 2.7 и 2.8 следует, что для любой пары (l_i, l_j) чисел из L число $HOK(l_i, l_j) \in L$. Следовательно, любая пара чисел из L замкнута сверху во множестве L.

Пусть любая пара (l_i, l_j) чисел из L замкнута сверху во множестве L. Требуется доказать, что $HOK(l_{i_1}, \ldots, l_{i_s}) \in L$, где $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, m\}$, $1 \leqslant s \leqslant m$.

Для $1 \leqslant s \leqslant 2$ включение $HOK(l_{i_1}, \ldots, l_{i_s}) \in L$ выполнено по условию. Предположим, что оно выполнено для $s < r$, где $r > 2$.

Любое подмножество $\{i_1, \ldots, i_r\}$ множества $\{1, \ldots, m\}$ можно представить при $r > 2$ в виде объединения непустых подмножеств:

$$\{i_1, \ldots, i_r\} = \{i_1, \ldots, i_{r-1}\} \cup \{i_2, \ldots, i_r\}.$$

Пусть $l_i = HOK(l_{i_1}, \ldots, l_{i_{r-1}})$ и $l_j = HOK(l_{i_2}, \ldots, l_{i_r})$. По предположению индукции $l_i, l_j \in L$. Значит, по условию $HOK(l_i, l_j) \in L$, при этом $HOK(l_i, l_j) = HOK(l_{i_1}, \ldots, l_{i_r})$. Следовательно, $HOK(l_{i_1}, \ldots, l_{i_r}) \in L$ и множество L замкнуто сверху. □

Определение 2.10. *Подстановку g* назовём *L-замкнутой сверху*, если замкнуто сверху множество $L(g)$. ◇

Определение 2.11. *Подстановку g* назовём *L-цепной*, если множество $L(g)$ образует цепь в решётке $D(n)$. ◇

Замечание 1. Всякая L-замкнутая сверху подстановка является унидоминантной, так как если число $HOK(l_1, \ldots, l_m) \in L(g)$, то это значит, что множество $L(g)$ содержит число, кратное любому числу множества $L(g)$.

Замечание 2. Всякая цепная подстановка по утверждению 2.7 является L-замкнутой сверху, так как в цепи любая пара чисел замкнута сверху.

Замечание 3. Если $L(g) = \{l_1, l_2\}$, то подстановка g одновременно является или не является унидоминантной, L-замкнутой сверху и L-цепной. Она является таковой тогда и только тогда, когда числа l_1 и l_2 сравнимы.

Пример 2.3. L-цепными подстановками являются:

а) равноцикловые подстановки — в силу замечания 1 к определению 2.9;

б) инволюции;

в) подстановки g, у которых множество $L(g)$ имеет вид $\{1, l\}$, где $l > 1$.

L-замкнутой сверху, но не L-цепной подстановкой является, например, подстановка g, у которой множество $L(g)$ имеет вид:

$$L(g) = \{1, l-1, l, (l-1) \cdot l\}, \text{ где } l > 2.$$

Унидоминантной, но не L-замкнутой сверху подстановкой является, например, подстановка g, у которой множество $L(g)$ имеет вид:

$$\{1, l-1, l, (l-1) \cdot l^2\}, \text{ где } l > 2. \diamond$$

2.1.5. Свойства характеристик цикловых структур подстановок. Обозначим через $F(\Phi(X), Y)$ класс функций, определённых на группе подстановок $\Phi(X)$ и принимающих значения во множестве Y, где Y — линейно или частично упорядоченное множество. Среди функций f из $F(\Phi(X), Y)$ выделим классы функций, обладающих свойствами:

а) если $C(g)=C(g')$ для $g, g'\in\Phi(X)$, то $f(g)=f(g')$;
б) если $L(g)=L(g')$ для $g, g'\in\Phi(X)$, то $f(g)=f(g')$.

Определение 2.12. Функции со свойством а) назовём *характеристиками цикловых структур*, и функции со свойством б) назовём *характеристиками редукций цикловых структур*. ◇

Такие функции определены, по существу, в случае а) — на множестве C'' цикловых структур подстановок и в случае б) — на множестве C' редукций цикловых структур подстановок. Поэтому характеристики цикловых структур и характеристики редукций цикловых структур могут быть представлены соответственно в виде: $f(g)=\psi(C(g))$ и $f(g)=\varphi(L(g))$.

Цикловая структура $C(g)$ всякой подстановки g задаётся парой наборов $(L, K)\in C''$, а редукция цикловой структуры $L(g)$ преобразования g задаётся набором $L\in C'$. В связи с этим для обозначения характеристик цикловых структур и характеристик редукций цикловых структур используем и соответственно символы $\psi(L, K)$ и $\varphi(L)$.

Функцию $\varphi(L)$ можно рассматривать как характеристику цикловых структур, зависящую несущественно от элементов набора K. Следовательно, всякое утверждение, верное для некоторого класса характеристик цикловых структур, выполнено и для соответствующего класса характеристик редукций цикловых структур.

Пример 2.4. Функция $\pi(g)$ из $F(\Phi(X), Y)$, определённая в п. 2.1.1 (в этом случае Y есть множество разбиений множества X), не является характеристикой цикловых структур, так как её значения зависят от состава циклов подстановки g. ◇

Пример 2.5. Пусть t — натуральное, $g\in\Phi(X)$. Зададим функцию $f_t(g)$ из $F(\Phi(X), Y)$, где $Y=\{0, 1, \ldots, |X|\}$, как число элементов множества X, удовлетворяющих равенству $g^t(x)=x$. Несложно определить, что

$$f_t(g)=\sum_{i:\ l_i/t} l_i\cdot k_i.$$

Значение функции $f_t(g)$ однозначно определяется числом t и элементами наборов L, K. Следовательно, функция $f_t(g)$ есть характеристика цикловых структур. ◇

Пример 2.6. Функция f из $F(\Phi(X), N)$, определённая равенством $f(g)=\operatorname{ord} g$, является характеристикой редукций цикловых структур, её соответствующее задание через элементы набора L имеет вид: $\varphi(L)=НОК\{l_1, \ldots, l_m\}$.

В примере 1.5 показана нормальность этой функции. ◇

Для подстановки $g\in\Phi(X)$ через $\psi_g(t)$ (через $\varphi_g(t)$) обозначим g-подфункцию функции $\psi(L, K)$ (функции $\varphi(L)$). Такое обозначение корректно, так как в силу утверждения 2.3 цикловая структура элемента g^t циклической группы $\langle g\rangle$ вполне определена цикловой структурой преобразования g и показателем t.

Как и любая функция, заданная на группе подстановок g, характеристика цикловых структур $\psi(L, K)$ однозначно задаётся семейством своих g-подфункций, если g пробегает все элементы некоторой системы R c-образующих группы g (см. определение 1.9). Поэтому свойства функции $\psi(L, K)$ можно изучать с помощью изучения свойств указанных g-подфункций.

Утверждение 2.8. *Пусть $\psi(L, K)$ есть характеристика цикловых структур. Тогда:*

а) *для любой подстановки $g\in\Phi(X)$ D-диаграмма g-подфункции $\psi_g(t)$ функции $\psi(L, K)$ является простой;*

б) *функция* $\psi(L, K)$ *монотонна (антимонотонна) тогда и только тогда, когда для любой подстановки* $g \in \Phi(X)$ *и любого* $\tau \in D(\operatorname{ord} g)$:

$$\psi_g(1) \geqslant \psi_g(\tau)$$

$$(\psi_g(1) \leqslant \psi_g(\tau));$$

в) *функция* $\psi(L, K)$, *принимающая натуральные значения, нормальна (антинормальна,* p*-нормальна,* p*-антинормальна) тогда и только тогда, когда для любой подстановки* $g \in \Phi(X)$ *и любого* $\tau \in D(\operatorname{ord} g)$:

$$\frac{\psi_g(1)}{\psi_g(\tau)} \in N \left(\frac{\psi_g(\tau)}{\psi_g(1)} \in N, \frac{\psi_g(1)}{\psi_g(\tau)} \in N^{[p]}, \frac{\psi_g(\tau)}{\psi_g(1)} \in N^{[p]}\right).$$

Доказательство. а) Утверждение вытекает непосредственно из замечания к утверждению 2.3.

Необходимость утверждений б), в) вытекает из замечания 1) к определению 1.25 и соответственно следствий а), б) утверждения 1.14.

В силу имеющейся аналогии докажем достаточность лишь для утверждения б).

Пусть $g \in \Phi(X)$ и $\operatorname{ord} g = n$. По утверждению 1.13,а) для доказательства монотонности (антимонотонности) функции $\psi_g(t)$ достаточно показать, что если (t, n) делит (τ, n) для $t, \tau \in N_n$, то $\psi_g(t) \geqslant \psi_g(\tau)$ $(\psi_g(t) \leqslant \psi_g(\tau))$.

Из утверждения 2.8,а) следует, что для подстановки g при любых τ, $t \in N_n$ выполнено:

$$\psi_g(t) = \psi_g(a), \psi_g(\tau) = \psi_g(b),$$

где $a = (t, n)$ и $b = (\tau, n)$.

Если (t, n) делит (τ, n), то $b = a \cdot r$, где $r \in D(n)$, так как $b \in D(n)$ и r/b. В этих обозначениях для подстановки $h = g^a$ верны равенства:

$$\psi_g(a) = \psi_h(1), \psi_g(b) = \psi_h(r).$$

По условию $\psi_h(1) \geqslant \psi_h(r)$ $(\psi_h(1) \leqslant \psi_h(r))$ при $r \in D(n)$. Значит,

$$\psi_g(a) \geqslant \psi_g(b) \quad (\psi_g(a) \leqslant \psi_g(b)).$$

Следовательно, $\psi_g(t) \geqslant \psi_g(\tau)$ $(\psi_g(t) \leqslant \psi_g(\tau))$, т. е. функция $\psi_g(t)$ монотонна (антимонотонна). □

Следствие (критерий наследственности H-признака). *Если группа подстановок* G *имеет* H*-признак и характеристическая функция* H*-признака* ψ_H^G *есть характеристика цикловых структур, то* H*-признак является наследственным тогда и только тогда, когда для любого* $g \in G \cap H$ *и любого* $\tau \in D(n)$ *выполнено* $g^\tau \in G \cap H$.

Доказательство. По утверждению 1.15 H-признак в группе G является наследственным тогда и только тогда, когда функция ψ_H^G антимонотонна. В силу того, что функция ψ_H^G есть характеристика цикловых структур, из утверждения 2.8,б) получаем, что H-признак является наследственным тогда и только тогда, когда для любой подстановки $g \in G$ и любого $\tau \in D(n)$ выполнено неравенство $\psi_{H,g}^G(1) \leqslant \psi_{H,g}^G(\tau)$, где $\psi_{H,g}^G(t)$ есть g-подфункция характеристической функции ψ_H^G.

Вместе с тем, из определения 1.28 следует, что неравенство $\psi_{H,g}^G(1) \leqslant \psi_{H,g}^G(\tau)$ равносильно тому, что из включения $g \in G \cap H$ следует включение $g^\tau \in G \cap H$, где $\tau \in D(n)$.

Следовательно, критерий наследственности H-признака доказан. □

§ 2.2. Исследование в группах подстановок наследственных признаков, определяемых свойствами редукций цикловых структур подстановок

Пусть $g \in \Phi(X)$ и редукция цикловой структуры $L(g) = (l_1, \ldots, l_m)$. Обозначим для $i, j, r \in \{1, \ldots, m\}$: $n(i, j) = HOK(l_i, l_j)$, $n(i, j, r) = HOK(l_i, l_j, l_r)$.

2.2.1. Наследственные признаки, определяемые количеством длин циклов подстановок. На группе подстановок $\Phi(X)$ определим функцию $\mu(g)$, принимающую натуральные значения: $\mu(g)$ — число различных длин циклов в цикловой структуре $C(g)$ подстановки g порядка n. Таким образом, если $L(g) = (l_1, \ldots, l_m)$, то $\mu(g) = m$.

Обозначим через $\Phi(\mu \leqslant r)$, где r — натуральное, множество подстановок g из группы $\Phi(X)$, для которых $\mu(g) \leqslant r$. Заметим, что $\Phi(\mu \leqslant 1)$ есть множество равноцикловых подстановок группы $\Phi(X)$, соответствующий признак назовём признаком равноцикловости.

Определим для подстановки g множество E_L делителей числа n:

$$E_L = \{\mathrm{mp}_{n(i,j)}(l_i) \cdot \mathrm{mp}_{n(i,j)}(l_j),\ i, j \in \{1, \ldots, m\},\ i < j\}^*.$$

Теорема 2.1. а) *Любая группа подстановок G имеет наследственный $\Phi(\mu \leqslant r)$-признак, r — натуральное, и для любой подстановки $g \in \Phi(X)$*

$$\Pi(\Phi(\mu \leqslant r), g) = \mathrm{prm}\{t \in D(n):\ |\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*| \leqslant r\}.$$

б) *Если $\mu(g) = m$, то*

$$\Pi(\Phi(\mu \leqslant m-1), g) = \mathrm{prm}\, E_L.$$

в) *Любая циклическая группа $\langle g \rangle$ подстановок имеет групповой признак равноцикловости и*

$$\mathrm{pok}_g\, \Phi(\mu \leqslant 1) = HOK\{t \in E_L\}.$$

Доказательство. а) По утверждению 2.2 при возведении подстановки g в степень t, где t — натуральное, цикл длины l подстановки g либо преобразуется в цикл длины l, если $(l, t) = 1$, либо разлагается на (l, t) циклов одинаковой длины $\nu^t(l_i)$ (см. формулу (2.1)). Отсюда получаем, что для g-подфункции $\mu_g(t)$ функции $\mu(g)$ выполнено: $\mu_g(t) \leqslant \mu_g(1)$, где

$$\mu_g(t) = |\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*|. \tag{2.5}$$

Так как функция $\mu(g)$ является характеристикой редукций цикловых структур, то по утверждению 2.8,б) из неравенства $\mu_g(t) \leqslant \mu_g(1)$ следует, что функция $\mu_g(t)$ монотонна. В силу произвольности рассмотренной подстановки g из замечания 1 к определению 1.25 следует, что монотонной является и функция $\mu(g)$. Отсюда по теореме 1.8,а) получаем, что $\Phi(\mu \leqslant r)$-признак является наследственным.

Из равенства (2.5) следует, что подстановка $g^t \in \Phi(\mu \leqslant r)$ тогда и только тогда, когда $|\{\nu^t(l_1), \ldots, \nu^t(l_m)\}^*| \leqslant r$. Отсюда по теореме 1.5,в) получаем выражение для множества $\Pi(\Phi(\mu \leqslant r), g)$.

б) Если $\mu(g) = m$, то подстановка $g^t \in \Phi(\mu \leqslant m-1)$ тогда и только тогда, когда $\nu^t(l_i) = \nu^t(l_j)$ для некоторой пары различных номеров $i, j \in \{1, \ldots, m\}$. По утверждению 2.4,б) это условие равносильно тому, что t

кратно хотя бы одному из чисел множества E_L. Отсюда по теореме 1.5,б) получаем выражение для множества $\Pi(\Phi(\mu \leqslant m-1), g)$.

в) Если $L(g) = (l_1, \ldots, l_m)$, то подстановка $g^t \in \Phi(\mu \leqslant 1)$ тогда и только тогда, когда $\nu^t(l_i) = \nu^t(l_j)$ для любой пары различных номеров $i, j \in \{1, \ldots, m\}$. По утверждению 2.4,б) это условие равносильно тому, что t кратно каждому из чисел множества E_L, т. е. t кратно $HOK\{t \in E_L\}$. Отсюда по теореме 1.5,б) получаем, что множество $\Pi(\Phi(\mu \leqslant 1), g)$ состоит из единственного числа, равного $HOK\{t \in E_L\}$. Значит, по следствию 1 теоремы 1.5 это число и есть $\mathrm{pok}_g \Phi(\mu \leqslant 1)$, и по следствию 2 теоремы 1.5 $\Phi(\mu \leqslant 1)$-признак является групповым. □

Проиллюстрируем на примере некоторые свойства этих признаков.

Пример 2.7. Рассмотрим $\Phi(\mu \leqslant 1)$-признак в циклической группе $\langle g \rangle$ в случае $L = (1, n)$, где n — натуральное число, отличное от 1.

Так как функция $\mu_g(t)$ монотонна, то:

1) по следствию 1 теоремы 1.8 $\Phi(\mu \leqslant 1)$-признак в циклической группе $\langle g \rangle$ является тривиальным в том и только в том случае, когда $\nu^t(n) > 1$ для любого коатома t решётки $D(n)$; это условие выполнено при любом натуральном $n > 1$;

2) по следствию 3 теоремы 1.8 $\Phi(\mu \leqslant 1)$-признак в циклической группе $\langle g \rangle$ является квазиполным в том и только в том случае, когда $\nu^t(n) = 1$ для любого атома t решётки $D(n)$; это условие выполнено только при простых числах n. ◇

2.2.2. Наследственные признаки, связанные с доминированием чисел в редукции цикловой структуры подстановок. Пусть $\mathrm{dom}\, L(g) = \{l_1, \ldots, l_d\}$. Рассмотрим $|\mathrm{dom}\, L(g)|$ как функцию, определённую на группе $\Phi(X)$. Через $d_g(t)$, где $t \in N_n$, обозначим g-подфункцию функции $|\mathrm{dom}\, L(g)|$, т. е. $d_g(t) = |\mathrm{dom}\, L(g^t)|$. Из определений 2.5 и 2.6 следует, что функция $|\mathrm{dom}\, L(g)|$ является характеристикой редукций цикловых структур подстановок.

Обозначим через $\Phi(\mathrm{dom} \leqslant r)$, где r — натуральное, множество подстановок g из группы $\Phi(X)$, для которых $|\mathrm{dom}\, L(g)| \leqslant r$.

Теорема 2.2. *Любая группа подстановок G имеет наследственный $\Phi(\mathrm{dom} \leqslant r)$-признак, r — натуральное, при этом*

$$\Pi(\Phi(\mathrm{dom} \leqslant r), g) = \mathrm{prm}\{t \in D(n): |\mathrm{dom}\{v^t(l_1), \ldots, v^t(l_d)\}^*| \leqslant r\}.$$

Доказательство. Из утверждения 2.6,б) следует, что для g-подфункции $d_g(t)$ функции $|\mathrm{dom}\, L(g)|$ при любом натуральном t выполнено: $d_g(t) \leqslant d_g(1)$, где

$$d_g(t) = |\mathrm{dom}\{v^t(l_1), \ldots, v^t(l_d)\}^*|. \tag{2.6}$$

Так как функция $|\mathrm{dom}\, L(g)|$ является характеристикой цикловых структур, то по утверждению 2.8,б) из неравенства $d_g(t) \leqslant d_g(1)$ следует, что функция $d_g(t)$ монотонна. В силу произвольности рассмотренной подстановки g монотонной является и функция $|\mathrm{dom}\, L(g)|$. Отсюда по теореме 1.8,а) получаем, что любая группа подстановок G имеет наследственный $\Phi(\mathrm{dom} \leqslant r)$-признак.

Из равенства (2.6) следует, что подстановка $g^t \in \Phi(\mathrm{dom} \leqslant r)$ тогда и только тогда, когда $|\mathrm{dom}\{v^t(l_1), \ldots, v^t(l_d)\}^*| \leqslant r$. Отсюда по теореме 1.5,в) получаем требуемое равенство для множества $\Pi(\Phi(\mathrm{dom} \leqslant r), g)$. □

Множество всех унидоминантных подстановок множества X обозначим $U(X)$ или кратко U.

Следствие 1. *Всякая группа G подстановок множества X имеет наследственный U-признак.*

Доказательство. По теореме 2.2 группа G имеет наследственный $G(\mathrm{dom} \leqslant 1)$-признак, где в соответствии с принятыми обозначениями $G(\mathrm{dom} \leqslant 1)$ — множество всех унидоминантных подстановок группы G, т. е. $G(\mathrm{dom} \leqslant 1) = G \cap U$. □

Следствие 2. *$\Phi(\mathrm{dom} \leqslant r)$-признак в циклической группе $\langle g \rangle$ является тривиальным (квазиполным) в том и только в том случае, когда $|\mathrm{dom}\{v^t(l_1), \ldots, v^t(l_d)\}^*| > r$ ($|\mathrm{dom}\, L(g)| > r$ и $|\mathrm{dom}\{v^t(l_1), \ldots, v^t(l_d)\}^*| \leqslant r$) для любого коатома (атома) t решётки $D(n)$, $r = 1, 2, \ldots$*

Доказательство. Так как функция $d_g(t)$ монотонна и $d_g(n) = d_e(1) = 1$ (см. пример 2.2,а), то по следствию 1 теоремы 1.8 $\Phi(\mathrm{dom} \leqslant r)$-признак в циклической группе $\langle g \rangle$ является тривиальным в том и только в том случае, когда $|\mathrm{dom}\, L(g^t)| > r$ для любого коатома t решётки $D(n)$. Отсюда по утверждению 2.6,б) получаем требуемое утверждение.

Критерий квазиполноты $\Phi(\mathrm{dom} \leqslant r)$-признака доказывается аналогично с использованием следствия 3 теоремы 1.8. □

Определим множество W_L делителей числа n:

$$W_L = \{\mathrm{mp}_{n(i,j)}(l_i), \mathrm{mp}_{n(i,j)}(l_j)\colon\ i, j \in \{1, \ldots, d\},\ i \neq j\}^*.$$

Следствие 3. *Пусть $|\mathrm{dom}\, L(g)| = d > 1$ и каноническое разложение числа n определено равенством* (1.7). *Тогда*

$$\Pi(\Phi(\mathrm{dom} \leqslant d - 1), g) = \mathrm{prm}\, W_L.$$

Вследствие этого $\Phi(\mathrm{dom} \leqslant d - 1)$-признак в циклической группе $\langle g \rangle$ является квазиполным в том и только в том случае, когда

$$\mathrm{prm}\, W_L = \{p_1, \ldots, p_s\}.$$

Доказательство. Множество $\mathrm{dom}\, L(g)$ образует антицепь порядка d, где $d > 1$. Поэтому $\mathrm{dom}\, L(g^t)$ содержит не более $d - 1$ доминирующих чисел в том и только в том случае, когда $v^t(l_i)$ делит $v^t(l_j)$ для некоторых $i, j \in \{1, \ldots, d\}$, где $i \neq j$. По утверждению 2.4,б) это условие равносильно тому, что t кратно хотя бы одному из чисел множества W_L. Отсюда по теореме 1.5,б) получаем равенство для множества $\Pi(\Phi(\mathrm{dom} \leqslant d - 1), g)$. Из этого равенства по утверждению 1.11,б) следует критерий квазиполноты $\Phi(\mathrm{dom} \leqslant d - 1)$-признака в циклической группе $\langle g \rangle$. □

2.2.3. Свойства наследственного U-признака в группах подстановок. Рассмотрим циклическую группу $\langle g \rangle$ подстановок множества X, и опишем наследственное множество $\langle g \rangle \cap U$. В соответствии с равенством (1.6) для этого достаточно определить множество (U, g)-пороговых чисел.

Установим связь между цикловой структурой преобразования g и множеством (U, g)-пороговых чисел.

Теорема 2.3. *Пусть $\mathrm{dom}\, L(g) = \{l_1, \ldots, l_d\}$, где $d > 1$, и каноническое разложение числа n определено равенством* (1.7). *Тогда*

$$\Pi(U, g) = \mathrm{prm}\{\mathrm{mp}_n(l_1), \ldots, \mathrm{mp}_n(l_d)\}^*.$$

Доказательство. По следствию утверждения 2.6 подстановка g^t является унидоминантной тогда и только тогда, когда редуцированный набор чисел $\{v^t(l_1), \ldots, v^t(l_d)\}^*$ содержит единственное доминирующее число.

Это выполнено тогда и только тогда, когда при некотором $i \in \{1, \ldots, d\}$ число $v^t(l_i)$ кратно каждому из чисел $v^t(l_1), \ldots, v^t(l_d)$.

По условию $d > 1$, поэтому по утверждению 2.5,а) множество $\{l_1, \ldots, l_d\}$ образует антицепь в решётке $D(n)$. Отсюда по утверждению 2.4,б) следует, что $v^t(l_i)$ кратно $v^t(l_j)$, где $i, j \in \{1, \ldots, d\}$ и $i \neq j$, в том и только в том случае, когда t кратно $\mathrm{mp}_{n(i,j)}(l_i)$, где $n(i, j) = HOK(l_i, l_j)$. Значит, $v^t(l_i)$ кратно каждому из чисел $v^t(l_1), \ldots, v^t(l_d)$ в том и только в том случае, когда t кратно числу u_i, где для $i = 1, \ldots, d$

$$u_i = HOK(\mathrm{mp}_{n(i,j)}(l_i)\colon\ j \in \{1, \ldots, d\} \setminus \{i\}).$$

Докажем, что u_i совпадает с произведением всех тех примарных делителей числа n, которые не делят l_i, т. е. $u_i = \mathrm{mp}_n(l_i)$.

Пусть разложения доминирующих чисел множества $L(g)$ имеют вид:

$$l_i = p_1^{k_{i1}} \cdot \ldots \cdot p_s^{k_{is}},$$

где $k_{i1}, \ldots, k_{is}$ — целые неотрицательные числа, связанные соотношениями $k_j = \max\{k_{1j}, \ldots, k_{dj}\}$, $i = 1, \ldots, d$, $j = 1, \ldots, s$.

В силу замечания к определению 1.21 u_i / n, поэтому справедливо разложение:

$$u_i = p_1^{\tau_{i1}} \cdot \ldots \cdot p_s^{\tau_{is}},$$

где $\tau_{i1}, \ldots, \tau_{is}$ — целые неотрицательные числа, не превышающие соответственно чисел $k_1, \ldots, k_s$, $i = 1, \ldots, d$.

Из определения 1.20 следует, что равенство $u_i = \mathrm{mp}_n(l_i)$ выполнено, если совпадают все соответственные примарные делители чисел u_i и $\mathrm{mp}_n(l_i)$. Без ущерба для общности рассмотрим один из примарных делителей числа u_i, например, $p_1^{\tau_{i1}}$.

Из определения числа u_i следует, что $p_1^{\tau_{i1}}$ есть наибольший из примарных делителей чисел $\mathrm{mp}_{n(i,j)}(l_i)$, где $j \in \{1, \ldots, d\} \setminus \{i\}$, являющихся степенями числа p_1. Значит, $p_1^{\tau_{i1}}$ совпадает с наибольшим из примарных делителей $p_1^{k_{j1}}$ (чисел l_j соответственно) таких, что $p_1^{k_{j1}}$ не делит l_i, где $j \in \{1, \ldots, d\} \setminus \{i\}$. Следовательно, $k_{i1} < \tau_{i1} = k_1$, т. е. $p_1^{\tau_{i1}}$ есть примарный делитель числа n, который не делит l_i. Отсюда следует по определению 1.21, что $p_1^{\tau_{i1}}$ есть примарный делитель числа $\mathrm{mp}_n(l_i)$.

Таким образом, подстановка g^t является унидоминантной тогда и только тогда, когда t кратно одному из чисел $\mathrm{mp}_n(l_i)$, $i = 1, \ldots, d$. Отсюда, применяя теорему 1.5,б), получаем выражение для множества $\Pi(U, g)$. □

Следствие 1. *Нетривиальная группа подстановок G имеет нетривиальный наследственный U-признак, который не является групповым, если хотя бы один из элементов с-базиса группы G не является унидоминантной подстановкой.*

Вследствие этого множество U-тривиальности группы подстановок G тривиально.

Доказательство. Так как $\mathrm{ord}\, G > 1$, то в группе G имеется подстановка g, порядок которой больше 1.

Если $g \in U$, то в силу наследственности U-признака $\langle g \rangle \subseteq U$. Значит, в этом случае U-признак в группе подстановок G нетривиален.

Если $|\Pi(U, g)| > 1$, то по следствию 2 теоремы 1.5 наследственный U-признак в циклической подгруппе $\langle g \rangle$ не является групповым и, следовательно, нетривиален как в группе $\langle g \rangle$, так и в группе G.

Докажем, что $|\Pi(U, g)| > 1$, если $g \notin U$ или, что равносильно, если $d > 1$.

Пусть $u_i \in \Pi(U, g)$ при некотором $i \in \{1, \ldots, d\}$, где $u_i = \mathrm{mp}_n(l_i)$. Для данного номера i найдётся номер $j \in \{1, \ldots, s\}$ такой, что $k_{ij} < k_j$. Действительно, если выполнена система равенств $k_{ij} = k_j$, $j = 1, \ldots, s$, то $l_i = n$

и, следовательно, число l_i доминирует во множестве $\operatorname{dom} L(g)$, что невозможно, так как по утверждению 2.5,а) множество $\operatorname{dom} L(g)$ при $d>1$ есть антицепь в решётке $D(n)$. Значит, $k_{ij}<k_j$, и по определению 1.21 получаем, что число u_i делится на число $p_j^{k_j}$.

С другой стороны, так как $n=HOK(l_1,\ldots,l_d)$, то для указанного j имеется некоторое $r\in\{1,\ldots,d\}$ такое, что $k_{rj}=k_j$. Отсюда следует, что $r\neq i$, при этом $u_r\neq u_i$, так как число u_r не делится на число $p_j^{k_j}$. Если $u_r\in\Pi(U,g)$, то неравенство $|\Pi(U,g)|>1$ выполнено.

Если $u_r\notin\Pi(U,g)$, то по теореме 2.3 $u_r\notin \operatorname{prm}\{u_1,\ldots,u_d\}^*$. Значит, среди чисел множества $\{u_1,\ldots,u_d\}$ найдётся число u_q, простое во множестве $\{u_1,\ldots,u_d\}$ и такое, что $q\in\{1,\ldots,d\}\setminus\{r\}$ и u_q/u_r. Следовательно, число u_q не делится на число $p_j^{k_j}$. Значит, $u_q\neq u_i$ и верны включения $u_i,\ u_q\in\Pi(U,g)$, т. е. в любом случае $|\Pi(U,g)|>1$.

Так как U-признак в циклической подгруппе $\langle g\rangle$ не является групповым, он не является групповым и в группе G.

Рассмотрим множество U-тривиальности группы G. Если множество G_U^1 нетривиально, то найдётся нетождественная подстановка $g\in G$ такая, что $\langle g\rangle\cap U=\{e\}$. Значит, нетривиальная группа $\langle g\rangle$ имеет тривиальный наследственный U-признак, что противоречит доказанному выше. □

Оценим некоторые характеристики наследственного U-признака в группах подстановок.

Следствие 2. *Пусть* $\operatorname{dom} L(g)=\{l_1,\ldots,l_d\}$, *где* $d>1$. *Тогда*

$$\operatorname{pok}_g U=\min\{\operatorname{mp}_n(l_1),\ldots,\operatorname{mp}_n(l_d)\},$$
$$h_c(\langle g\rangle\cap U)\leqslant d.$$

Доказательство. По следствию 1 теоремы 1.5 $\operatorname{pok}_g U$ совпадает с наименьшим числом из множества $\Pi(U,g)$. В то же время, по теореме 2.3 $\Pi(U,g)=\operatorname{prm}\{u_1,\ldots,u_d\}^*$, где $u_i=\operatorname{mp}_n(l_i)$, $i=1,\ldots,d$. Из определений 1.17 и 1.18 следует, что наименьшие числа множеств $\operatorname{prm}\{u_1,\ldots,u_d\}^*$ и $\{u_1,\ldots,u_d\}$ совпадают.

По теореме 1.5,г) $h_c(\langle g\rangle\cap U)=|\Pi(U,g)|$, при этом из теоремы 2.2 следует, что $|\Pi(U,g)|\leqslant d$. □

Следствие 3. *Пусть* $\operatorname{dom} L(g)=\{l_1,\ldots,l_d\}$, *где* $d>1$, *и каноническое разложение числа* n *определено равенством* (1.7). *Тогда* U*-признак в циклической группе* $\langle g\rangle$ *является квазиполным тогда и только тогда, когда число* n *свободно от квадратов,* $s=d$ *и* $\operatorname{dom} L(g)$ *есть множество всех коатомов решётки* $D(n)$.

Доказательство. Предположим, что циклическая группа $\langle g\rangle$ имеет квазиполный U-признак. Тогда по утверждению 1.11,б) множество $\Pi(U,g)$ совпадает с множеством всех атомов решётки $D(n)$, значит, по теореме 2.3:

$$\operatorname{prm}\{\operatorname{mp}_n(l_1),\ldots,\operatorname{mp}_n(l_d)\}^*=\{p_1,\ldots,p_s\}.$$

С другой стороны, по определению 1.21 каждое число вида $\operatorname{mp}_n(l_i)$ есть примарный делитель числа n или произведение нескольких примарных делителей числа n. Значит, $\{p_1,\ldots,p_s\}$ есть множество примарных делителей числа n, т. е. число n свободно от квадратов.

Без ущерба для общности можно считать, что $\operatorname{mp}_n(l_i)=p_i$, тогда $l_i=\frac{n}{p_i}$, $i=1,\ldots,s$. Отсюда следует, что антицепь $\operatorname{dom} L(g)$ решётки $D(n)$ исчерпывается числами $l_1,\ldots,l_s$, так как $\{l_1,\ldots,l_s\}$ есть насыщенная антицепь,

состоящая из всех коатомов решётки $D(n)$. Действительно, при добавлении к множеству $\{l_1, \ldots, l_s\}$ любого делителя t числа n образуется множество, не являющееся антицепью, так как число t сравнимо хотя бы с одним из коатомов решётки $D(n)$. Следовательно, $s = d$.

Докажем в обратную сторону. Пусть $n = p_1 \cdot \ldots \cdot p_s$ и $\operatorname{dom} L(g) = (\frac{n}{p_1}, \ldots, \frac{n}{p_s})$. Тогда по теореме 2.3

$$\Pi(U, g) = \operatorname{prm}\{\operatorname{mp}_n(l_1), \ldots, \operatorname{mp}_n(l_s)\}^* = \{p_1, \ldots, p_s\}.$$

Отсюда по утверждению 1.11,б) циклическая группа $\langle g \rangle$ имеет квазиполный U-признак. □

Замечание. Для группы подстановок G, порождённой системой образующих S, где $S = \{s_1, \ldots, s_p\}$, можно оценить величину $\operatorname{pok}_S U$ с использованием неравенства следствия 4 теоремы 1.5:

$$\operatorname{pok}_S U \leqslant \min\{\Pi(U, s_1) \cup \ldots \cup \Pi(U, s_p)\}.$$

Пример 2.8. Определим характеристики U-признака в циклической группе, порождаемой подстановкой g степени 84 с цикловой структурой $C(g) = (1^7, 6, 15, 21, 35)$.

1) Характеристики цикловой структуры этой подстановки есть набор

$$L = (1, 6, 15, 21, 35), \operatorname{dom} L = (6, 15, 21, 35), \operatorname{ord} g = HOK(6, 15, 21, 35) = 210.$$

2) Используя канонические разложения чисел $210 = 2 \cdot 3 \cdot 5 \cdot 7$, $6 = 2 \cdot 3$, $15 = 3 \cdot 5$, $21 = 3 \cdot 7$, $35 = 5 \cdot 7$, получаем по теореме 2.3:

$$\Pi(U, g) = \operatorname{prm}\{\operatorname{mp}_{210}(6), \operatorname{mp}_{210}(15), \operatorname{mp}_{210}(21), \operatorname{mp}_{210}(35)\}^* = \operatorname{prm}\{35, 14, 10, 6\} = \{35, 14, 10, 6\}.$$

Следовательно, каноническое c-покрытие множества $\langle g \rangle \cap U$ имеет вид:

$$\langle g \rangle \cap U = \langle g^6 \rangle \cup \langle g^{10} \rangle \cup \langle g^{14} \rangle \cup \langle g^{35} \rangle.$$

3) c-ширина множества $\langle g \rangle \cap U$ равна 4.

4) $\operatorname{pok}_g U = \min\{35, 14, 10, 6\} = 6$.

Укажем, используя теорему 1.7, распределение U-признака по собственным подгруппам группы $\langle g \rangle$, не являющимся подмножествами множества $\langle g \rangle \cap U$:

$$\langle g^2 \rangle \cap U = \langle g^6 \rangle \cup \langle g^{10} \rangle \cup \langle g^{14} \rangle;$$
$$\langle g^3 \rangle \cap U = \langle g^6 \rangle \cup \langle g^{105} \rangle;$$
$$\langle g^5 \rangle \cap U = \langle g^{10} \rangle \cup \langle g^{35} \rangle;$$
$$\langle g^7 \rangle \cap U = \langle g^{14} \rangle \cup \langle g^{35} \rangle;$$
$$\langle g^{15} \rangle \cap U = \langle g^{30} \rangle \cup \langle g^{105} \rangle;$$
$$\langle g^{21} \rangle \cap U = \langle g^{42} \rangle \cup \langle g^{105} \rangle. \diamondsuit$$

2.2.4. Наследственные признаки в группах подстановок, связанные с замкнутостью сверху элементов редукций цикловых структур. Обозначим:

1) для подстановки g из $\Phi(X)$ через $\operatorname{opn} L^2(g)$ (или кратко $\operatorname{opn} L^2$) — множество всех пар чисел множества $L(g)$, не являющихся замкнутыми сверху в $L(g)$;

2) для натурального r через $\Phi(\operatorname{opn} \leqslant r)$ — множество подстановок g из группы $\Phi(X)$, для которых $|\operatorname{opn} L^2(g)| \leqslant r$;

3) через $\bar{C}(X)$ (кратко $\bar{C}$) множество всех L-замкнутых сверху подстановок из группы $\Phi(X)$;

4) через $\psi_{\bar{C}}^G$ — характеристическую функцию $\bar{C}$-признака в группе подстановок G.

Из утверждения 2.7 следует, что подстановка $g \in \bar{C}$ тогда и только тогда, когда $\operatorname{opn} L^2 = \varnothing$. Исследуем свойства $\Phi(\operatorname{opn} \leqslant r)$-признаков и $\bar{C}$-признака в группах подстановок.

Пусть $g \notin \bar{C}$. Поставим в соответствие каждой паре чисел (l_i, l_j) из множества $\operatorname{opn} L^2$ набор чисел T_L^{ij} и множеству $\operatorname{opn} L^2$ в целом — множество T_L, где T_L — декартово произведение множеств, связанных с наборами T_L^{ij}:

$$T_L^{ij} = \{\operatorname{mp}_{n(i,j)}(l_i), \operatorname{mp}_{n(i,j)}(l_j), \operatorname{mp}_{n(i,j,r)}(l_r) \cdot \operatorname{mp}_{n(i,j,r)}(n(i,j))\}^*,$$
$$r \in \{1, \ldots, m\} \setminus \{i, j\},$$
$$T_L = \prod_{(i,j):\ (l_i, l_j) \in \operatorname{opn} L^2(g)} \operatorname{prm} T_L^{ij}.$$

Рассмотрим $|\operatorname{opn} L^2|$ как функцию, определённую на группе $\Phi(X)$. Через $\mathrm{o}_g(t)$, где $t \in N_n$, обозначим g-подфункцию функции $|\operatorname{opn} L^2(g)|$, т. е. $\mathrm{o}_g(t) = |\operatorname{opn} L^2(g^t)|$.

Теорема 2.4. *Любая группа подстановок G имеет наследственный $\Phi(\operatorname{opn} \leqslant r)$-признак, r — натуральное, при этом если $|\operatorname{opn} L^2(g)| = r+1$, то*

$$\Pi(\Phi(\operatorname{opn} \leqslant r), g) = \operatorname{prm}\{\bigcup_{(i,j):\ (l_i, l_j) \in \operatorname{opn} L^2(g)} T_L^{ij}\}^*.$$

Доказательство. Из утверждения 2.4,в) следует, что для g-подфункции $\mathrm{o}_g(t)$ функции $|\operatorname{opn} L^2(g)|$ при любом натуральном t выполнено: $\mathrm{o}_g(t) \leqslant \mathrm{o}_g(1)$. Так как функция $|\operatorname{opn} L^2(g)|$ является характеристикой редукций цикловых структур подстановок, то по утверждению 2.8,б) из неравенства $\mathrm{o}_g(t) \leqslant \mathrm{o}_g(1)$ следует, что функция $\mathrm{o}_g(t)$ монотонна. В силу произвольности рассмотренной подстановки g монотонной является и функция $|\operatorname{opn} L^2|$. Отсюда по теореме 1.8,а) получаем, что любая группа подстановок G имеет наследственный $\Phi(\operatorname{opn} \leqslant r)$-признак.

Пусть $|\operatorname{opn} L^2(g)| = r+1$, тогда подстановка $g^t \in \Phi(\operatorname{opn} \leqslant r)$ в том и только в том случае, когда хотя бы для одной из пар чисел $(l_i, l_j) \in \operatorname{opn} L^2(g)$ соответствующая пара чисел $(v^t(l_i), v^t(l_j))$ замкнута сверху во множестве $L(g^t)$. Иначе говоря, либо числа $v^t(l_i)$ и $v^t(l_j)$ сравнимы, либо во множестве $L(g)$ имеется число l_r такое, что $v^t(l_r) = HOK(v^t(l_i), v^t(l_j))$. По утверждениям 2.4,б) и 2.4,г) это условие равносильно тому, что число t кратно одному из чисел множества $\bigcup_{(i,j):\ (l_i, l_j) \in \operatorname{opn} L^2(g)} T_L^{ij}$. Отсюда, применяя теорему 1.5,б), получаем выражение для множества $\Pi(\Phi(\operatorname{opn} \leqslant r), g)$. □

Теорема 2.5. *Нетривиальная группа подстановок G имеет нетривиальный наследственный $\bar{C}$-признак, при этом:*

1) *если $L(g) = \{l_1, l_2\}$ и $g \notin \bar{C}$, то*

$$\Pi(\bar{C}, g) = \{\operatorname{mp}_n(l_1), \operatorname{mp}_n(l_2)\};$$

2) *если* $L(g)=\{l_1, \ldots, l_m\}$, *где* $m>2$, *и* $g \notin \bar{C}$, *то*

$$\Pi(\bar{C}, g)=\operatorname{prm}\{HOK\{t_1, t_2, \ldots\}: (t_1, t_2, \ldots) \in T_L\}^*.$$

Доказательство. Цикловая структура подстановки g однозначно определяет наличие или отсутствие у подстановки g свойства L-замкнутости сверху, поэтому функция $\psi_{\bar{C}}^G$ является характеристикой цикловых структур подстановок группы $\Phi(X)$. Отсюда по следствию утверждения 2.8 $\bar{C}$-признак является наследственным в группе G тогда и только тогда, когда для любого $g \in G \cap \bar{C}$ и любого $t \in D(\operatorname{ord} g)$ выполнено включение $g^t \in G \cap \bar{C}$.

Из утверждения 2.4,в) следует, что если пара чисел (l_i, l_j) набора $L(g)$ замкнута сверху в наборе $L(g)$, то при любом натуральном t пара чисел $(v^t(l_i), v^t(l_j))$ набора $L(g^t)$ также замкнута сверху в наборе $L(g^t)$. Следовательно, если L-замкнута сверху подстановка g, то и подстановка g^t также L-замкнута сверху. Отсюда $\bar{C}$-признак в группе G является наследственным.

Пусть $g \notin \bar{C}$, тогда множество $L(g)$ состоит из двух или более чисел. Определим множество $\Pi(\bar{C}, g)$ и покажем нетривиальность $\bar{C}$-признака.

Пусть $L(g)=\{l_1, l_2\}$, тогда числа l_1 и l_2 несравнимы, если $g \notin \bar{C}$. В этом случае L-замкнутость сверху подстановки g^t в силу утверждения 2.7 равносильна сравнимости чисел $v^t(l_1)$ и $v^t(l_2)$.

Из утверждения 2.4,б) следует, что числа $v^t(l_1)$ и $v^t(l_2)$ сравнимы тогда и только тогда, когда t кратно либо $\operatorname{mp}_n(l_1)$, либо $\operatorname{mp}_n(l_2)$. При этом числа $\operatorname{mp}_n(l_1)$ и $\operatorname{mp}_n(l_2)$ несравнимы, так как они взаимно просты и отличны от 1 в силу несравнимости чисел l_1 и l_2. Отсюда, применяя теорему 1.5,б), получаем выражение для множества $\Pi(\bar{C}, g)$ в первом случае.

Пусть $L(g)=\{l_1, \ldots, l_m\}$, где $m>2$, и $g \notin \bar{C}$. Тогда по утверждению 2.7 $\operatorname{opn} L^2 \neq \varnothing$. Для любой пары $(l_i, l_j) \in \operatorname{opn} L^2$ числа l_i и l_j несравнимы и $HOK(l_i, l_j) \notin L(g)$.

Из замечания 2 к определению 2.9 следует, что пара чисел $(v^t(l_i), v^t(l_j))$ набора $L(g^t)$ замкнута сверху в наборе $L(g^t)$ тогда и только тогда, когда либо числа $v^t(l_i)$ и $v^t(l_j)$ сравнимы, либо они несравнимы и при некотором $r \in \{1, \ldots, m\} \setminus \{i, j\}$ выполнено равенство:

$$v^t(l_r)=HOK(v^t(l_i), v^t(l_j)).$$

Отсюда и из утверждений 2.4,б) и 2.4,г) получаем, что пара чисел $(v^t(l_i), v^t(l_j))$ набора $L(g^t)$ замкнута сверху в наборе $L(g^t)$ тогда и только тогда, когда число t кратно одному из чисел множества T_L^{ij}. В силу определений 1.17 и 1.18 это равносильно тому, что t кратно одному из чисел множества $\operatorname{prm} T_L^{ij}$.

Из утверждения 2.7 следует, что подстановка $g^t \in \bar{C}$ тогда и только тогда, когда для любой пары $(l_i, l_j) \in \operatorname{opn} L^2$ соответствующая пара чисел $(v^t(l_i), v^t(l_j))$ множества $L(g^t)$ замкнута сверху во множестве $L(g^t)$. Следовательно, подстановка $g^t \in \bar{C}$ тогда и только тогда, когда число t кратно одному из чисел набора $\{HOK\{t_1, t_2, \ldots\}: (t_1, t_2, \ldots) \in T_L\}$.

Применяя теперь теорему 1.5,б), получаем требуемое равенство для множества $\Pi(\bar{C}, g)$ во втором случае.

Покажем нетривиальность $\bar{C}$-признака в нетривиальной группе G. Так как $\operatorname{ord} G > 1$, то в группе G имеется подстановка g, порядок которой больше 1.

Если $g \in \bar{C}$, то в силу наследственности $\bar{C}$-признака $\langle g \rangle \subseteq \bar{C}$. Значит, в этом случае $\bar{C}$-признак в группе подстановок G нетривиален.

Пусть $g \notin \bar{C}$ и $L(g) = \{l_1, l_2\}$, тогда числа $\mathrm{mp}_n(l_1)$ и $\mathrm{mp}_n(l_2)$, составляющие множество $\Pi(\bar{C}, g)$, суть взаимно простые делители числа n, отличные от 1. Значит, $\Pi(\bar{C}, g) \neq \{n\}$, и по следствию 2 теоремы 1.5 наследственный $\bar{C}$-признак в группе $\langle g \rangle$ нетривиален.

Пусть $g \notin \bar{C}$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 2$. Заметим, что числа $\mathrm{mp}_{n(i,j)}(l_i)$ и $\mathrm{mp}_{n(i,j)}(l_j)$ суть отличные от 1 взаимно простые делители числа n при любой паре (i, j) такой, что $(l_i, l_j) \in \mathrm{opn}\, L^2$. Значит, хотя бы одно из этих чисел не делится на p, где p — произвольный простой делитель числа n. Следовательно, хотя бы одно из чисел множества $\mathrm{prm}\, T_L^{ij}$ не делится на p. Поэтому найдётся набор чисел $(t_1, t_2, \ldots) \in T_L$ такой, что $HOK\{t_1, t_2, \ldots\}$ не делится на p. Значит, множество $\Pi(\bar{C}, g)$ содержит число, которое не делится на p. Отсюда по следствию 2 теоремы 1.5 наследственный $\bar{C}$-признак в группе $\langle g \rangle$ нетривиален.

Таким образом, любая нетривиальная циклическая группа подстановок, а значит, и нетривиальная группа G имеет нетривиальный наследственный $\bar{C}$-признак. □

Следствие. *Пусть* $g \notin \bar{C}(X)$ *и* $L(g) = \{l_1, \ldots, l_m\}$, *где* $m > 2$ *и каноническое разложение числа* n *определено равенством* (1.7).

Тогда $\bar{C}$*-признак в циклической группе* $\langle g \rangle$ *является квазиполным в том и только в том случае, когда* $s \leqslant m$ *и для любой пары* (i, j) *такой, что* $(l_i, l_j) \in \mathrm{opn}\, L^2$, *выполнено включение* $\{p_1, \ldots, p_s\} \subseteq T_L^{ij}$.

Доказательство. Пусть циклическая группа $\langle g \rangle$ имеет квазиполный $\bar{C}$-признак. Тогда по утверждению 1.11,б) и теореме 2.4 имеем:

$$\mathrm{prm}\{HOK\{t_1, t_2, \ldots\} \colon (t_1, t_2, \ldots) \in T_L\}^* = \{p_1, \ldots, p_s\}.$$

Отсюда и из определений 1.17 и 1.18 следует, что

$$\{p_1, \ldots, p_s\} \subseteq \{HOK\{t_1, t_2, \ldots\} \colon (t_1, t_2, \ldots) \in T_L\}.$$

Следовательно, если множества чисел T_L^{ij} не содержат 1 при любой паре (i, j) такой, что $(l_i, l_j) \in \mathrm{opn}\, L^2$, то данное включение равносильно тому, что $\{p_1, \ldots, p_s\} \subseteq T_L^{ij}$ при любой паре (i, j) такой, что $(l_i, l_j) \in \mathrm{opn}\, L^2$.

Докажем, что множества чисел T_L^{ij} не содержат 1 при указанных парах (i, j). Для любой пары (i, j) такой, что $(l_i, l_j) \in \mathrm{opn}\, L^2$, числа l_i и l_j несравнимы, поэтому $\mathrm{mp}_{n(i,j)}(l_i) > 1$ и $\mathrm{mp}_{n(i,j)}(l_j) > 1$. Кроме того, если $(l_i, l_j) \in \mathrm{opn}\, L^2$, то $l_r \neq n(i, j)$ для любого $r \in \{1, \ldots, m\} \setminus \{i, j\}$, поэтому $\mathrm{mp}_{n(i,j,r)}(l_r) \cdot \mathrm{mp}_{n(i,j,r)}(n(i, j)) > 1$. Значит, множество T_L^{ij} состоит из делителей числа n, отличных от 1.

Так как $|T_L^{ij}| = m$, то отсюда следует, что $s \leqslant m$. □

Замечание. Если $g \notin \bar{C}(X)$ и $L(g) = \{l_1, l_2\}$, то в силу замечания 3 к определению 2.11 условия квазиполноты $\bar{C}$-признака в циклической группе $\langle g \rangle$ совпадают с условиями квазиполноты U-признака в циклической группе $\langle g \rangle$.

Пример 2.9. Определим характеристики $\bar{C}$-признака в циклической группе, порождаемой подстановкой g степени 84, у которой редукция цикловой есть набор чисел $L = (1, 6, 15, 21, 35)$.

Каноническое разложение числа $\mathrm{ord}\, g$ следующее: $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Множество $\mathrm{opn}\, L^2$ всех пар чисел набора $L(g)$, не являющихся замкнутыми

сверху в наборе $L(g)$, имеет вид:

$$\operatorname{opn} L^2 = \{(6, 15), (6, 21), (6, 35), (15, 21), (15, 35), (21, 35)\}.$$

Вычисления дают следующие результаты:

$$T_L^{6,15} = \{\mathrm{mp}_{30}(6), \mathrm{mp}_{30}(15), \mathrm{mp}_{30}(1)\cdot\mathrm{mp}_{30}(30), \mathrm{mp}_{210}(21)\cdot\mathrm{mp}_{210}(30),$$
$$\mathrm{mp}_{210}(35)\cdot\mathrm{mp}_{210}(30)\} = \{5, 2, 30\cdot 1, 10\cdot 7, 6\cdot 7\} = \{5, 2, 30, 70, 42\};$$
$$T_L^{6,21} = \{\mathrm{mp}_{42}(6), \mathrm{mp}_{42}(21), \mathrm{mp}_{42}(1)\cdot\mathrm{mp}_{42}(42), \mathrm{mp}_{210}(15)\cdot\mathrm{mp}_{210}(42),$$
$$\mathrm{mp}_{210}(35)\cdot\mathrm{mp}_{210}(42)\} = \{7, 2, 42\cdot 1, 14\cdot 5, 6\cdot 5\} = \{7, 2, 42, 70, 30\};$$
$$T_L^{6,35} = \{\mathrm{mp}_{210}(6), \mathrm{mp}_{210}(35), \mathrm{mp}_{210}(1)\cdot\mathrm{mp}_{210}(210), \mathrm{mp}_{210}(15)\cdot\mathrm{mp}_{210}(210),$$
$$\mathrm{mp}_{210}(21)\cdot\mathrm{mp}_{210}(210)\} = \{35, 6, 210\cdot 1, 14\cdot 1, 10\cdot 1\} = \{35, 6, 210, 14, 10\};$$
$$T_L^{15,21} = \{\mathrm{mp}_{105}(15), \mathrm{mp}_{105}(21), \mathrm{mp}_{105}(1)\cdot\mathrm{mp}_{105}(105), \mathrm{mp}_{210}(6)\cdot\mathrm{mp}_{210}(105),$$
$$\mathrm{mp}_{105}(35)\cdot\mathrm{mp}_{105}(105)\} = \{7, 5, 105\cdot 1, 35\cdot 2, 3\cdot 1\} = \{7, 5, 105, 70, 3\};$$
$$T_L^{15,35} = \{\mathrm{mp}_{105}(15), \mathrm{mp}_{105}(35), \mathrm{mp}_{105}(1)\cdot\mathrm{mp}_{105}(105), \mathrm{mp}_{210}(6)\cdot\mathrm{mp}_{210}(105),$$
$$\mathrm{mp}_{105}(21)\cdot\mathrm{mp}_{105}(105)\} = \{7, 3, 105\cdot 1, 35\cdot 2, 5\cdot 1\} = \{7, 3, 105, 70, 5\};$$
$$T_L^{21,35} = \{\mathrm{mp}_{105}(21), \mathrm{mp}_{105}(35), \mathrm{mp}_{105}(1)\cdot\mathrm{mp}_{105}(105), \mathrm{mp}_{210}(6)\cdot\mathrm{mp}_{210}(105),$$
$$\mathrm{mp}_{105}(15)\cdot\mathrm{mp}_{105}(105)\} = \{5, 3, 105\cdot 1, 35\cdot 2, 7\cdot 1\} = \{5, 3, 105, 70, 7\}.$$

Отсюда получаем, что

$$\operatorname{prm} T_L^{6,15*} = \{2, 5\};\ \operatorname{prm} T_L^{6,21*} = \{2, 7\};$$
$$\operatorname{prm} T_L^{6,35*} = \{6, 10, 14, 35\};\ \operatorname{prm} T_L^{15,21*} = \{3, 5, 7\};$$
$$\operatorname{prm} T_L^{15,35*} = \{3, 5, 7\};\ \operatorname{prm} T_L^{21,35*} = \{3, 5, 7\}.$$

Таким образом,

$$T_L = (\operatorname{prm} T_L^{6,15*}) \times (\operatorname{prm} T_L^{6,21*}) \times (\operatorname{prm} T_L^{6,35*}) \times (\operatorname{prm} T_L^{15,21*}) \times$$
$$\times (\operatorname{prm} T_L^{15,35*}) \times (\operatorname{prm} T_L^{21,35*}),$$
$$\{HOK\{t_1, t_2, \ldots\}\colon (t_1, t_2, \ldots) \in T_L\}^* = \{6, 30, 35, 42, 70, 105, 210\}.$$

Следовательно, по теореме 2.4

$$\Pi(\bar{C}, g) = \operatorname{prm}\{6, 30, 35, 42, 70, 105, 210\} = \{6, 35\}.$$

По множеству $\Pi(\bar{C}, g)$ определяем (следствие 1 теоремы 1.5,в)):

$$\operatorname{pok}_g \bar{C} = \min\{6, 35\} = 6.$$

Также по множеству $\Pi(\bar{C}, g)$ определяем (следствие 2 теоремы 1.5,в)), что $\bar{C}$-признак в циклической группе $\langle g\rangle$ не является тривиальным.

По следствию теоремы 2.5 $\bar{C}$-признак в группе $\langle g\rangle$ не является квазиполным, так как, в частности, множество $T_L^{6,15}$ не содержит все атомы (числа 2, 3, 5, 7) решётки $D(210)$. ◇

2.2.5. Наследственные цепные признаки в группах подстановок. Введём обозначения:

– $CH(X)$ (кратко CH) — множество всех L-цепных подстановок из группы $\Phi(X)$;

– $CH(r, X)$ (кратко $CH(r)$) — множество цепных подстановок g из группы $\Phi(X)$, у которых множество $L(g)$ образует L-цепь длины не более r;

– ψ_{CH}^{G} и $\psi_{CH(r)}^{G}$ — характеристические функции соответственно CH-признака и $CH(r)$-признака в группе подстановок G.

Цепными признаками назовём CH-признак и $CH(r)$-признаки в подгруппах группы $\Phi(X)$, $r = 1, 2, \ldots$ Исследуем свойства цепных признаков в группах подстановок.

Пусть $\overline{\mathrm{cmp}}L^2$ — множество всех несравнимых пар чисел из множества $L(g)$ и Z_L — декартово произведение двухэлементных множеств:

$$Z_L = \prod_{(i,j):\ (l_i, l_j) \in \overline{\mathrm{cmp}}L^2} (\mathrm{mp}_{n(i,j)}(l_i), \mathrm{mp}_{n(i,j)}(l_j)).$$

Теорема 2.6. а) *Любая группа подстановок G имеет наследственный CH-признак и наследственный $CH(r)$-признак при любом натуральном r.*

б) *Если $g \notin CH$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 1$, то*

$$\Pi(CH, g) = \mathrm{prm}\{HOK\{t_1, t_2, \ldots\}: (t_1, t_2, \ldots) \in Z_L\}^*.$$

в) *Если $g \in CH$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 1$, то*

$$\Pi(CH(m-2), g) = \mathrm{prm}\{\mathrm{mp}_{l_2}(l_1), \ldots, \mathrm{mp}_{l_m}(l_{m-1})\}^*.$$

Доказательство. а) Множество $L(g)$ однозначно определяет принадлежность подстановки g классу CH (классу $CH(r)$), поэтому функция ψ_{CH}^{G} (функция $\psi_{CH(r)}^{G}$) есть характеристика редукций цикловых структур подстановок группы $\Phi(X)$. Отсюда по следствию утверждения 2.8 CH-признак ($CH(r)$-признак) является наследственным в группе G тогда и только тогда, когда для любого $g \in G \cap CH$ (любого $g \in G \cap CH(r)$) и любого $t \in D(\mathrm{ord}\, g)$ выполнено включение $g^t \in G \cap CH$ (включение $g^t \in G \cap CH(r)$).

Из утверждения 2.4,а) следует, что если числа l_i и l_j из множества $L(g)$ сравнимы, то при любом натуральном t числа $v^t(l_i)$ и $v^t(l_j)$ из множества $L(g^t)$ также сравнимы. Следовательно, если подстановка g является L-цепной и длина цепи $L(g)$ равна r, то подстановка g^t также является L-цепной и длина цепи $L(g^t)$ не превышает r в силу того, что $\Phi(\mu \leqslant r)$-признак является наследственным (теорема 2.1). Отсюда CH-признак ($CH(r)$-признак при любом натуральном r) в группе G является наследственным признаком.

б) Если $g \notin CH$, то $\overline{\mathrm{cmp}}L^2 \neq \varnothing$. Подстановка g^t является L-цепной тогда и только тогда, когда сравнима любая пара чисел из множества $L(g^t)$. В силу утверждения 2.4,а) это условие равносильно тому, что для любой пары $(l_i, l_j) \in \overline{\mathrm{cmp}}L^2$ сравнимы числа $v^t(l_i)$ и $v^t(l_j)$ из множества $L(g^t)$.

По утверждению 2.4,б) числа $v^t(l_i)$ и $v^t(l_j)$ из множества $L(g^t)$ сравнимы, если t кратно либо $\mathrm{mp}_{n(i,j)}(l_i)$, либо $\mathrm{mp}_{n(i,j)}(l_j)$. Поэтому подстановка g^t является L-цепной тогда и только тогда, когда t кратно одному из чисел набора $\{HOK\{t_1, t_2, \ldots\}: (t_1, t_2, \ldots) \in Z_L\}$.

Отсюда по теореме 1.5,б) получаем выражение для $\Pi(CH, g)$.

в) Пусть $L(g) = \{l_1, \ldots, l_m\}$, где $\{l_1, \ldots, l_m\}$ есть цепь длины $m-1$. Подстановка $g^t \in CH(m-2)$ тогда и только тогда, когда $v^t(l_i) = v^t(l_{i+1})$ при некотором $i \in \{1, \ldots, m-1\}$. Так как l_i / l_{i+1}, то по утверждению 2.4,а) $v^t(l_i) = v^t(l_{i+1})$ тогда и только тогда, когда t кратно $\mathrm{mp}_{l_{i+1}}(l_i)$, $i = 1, \ldots, m-1$. Поэтому подстановка $g^t \in CH(m-2)$ тогда и только тогда,

когда t кратно одному из чисел $\mathrm{mp}_{l_2}(l_1), \ldots, \mathrm{mp}_{l_m}(l_{m-1})$. Отсюда, применяя теорему 1.5,б), получаем выражение для множества $\Pi(CH(m-2), g)$. □

Следствие 1. *Любая нетривиальная группа подстановок G имеет нетривиальный CH-признак. Если $g \in CH$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 1$, то $CH(m-2)$-признак в циклической группе $\langle g \rangle$ тривиален тогда и только тогда, когда $m = 2$ и $l_1 = 1$.*

Доказательство. Так как $\mathrm{ord}\, G > 1$, то в группе G имеется подстановка g, порядок которой больше 1.

Если $g \in CH$, то в силу наследственности CH-признака $\langle g \rangle \subseteq CH$. Значит, в этом случае CH-признак в группе подстановок G нетривиален.

Пусть $g \notin CH$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 1$. Заметим, что числа $\mathrm{mp}_{n(i,j)}(l_i)$ и $\mathrm{mp}_{n(i,j)}(l_j)$ суть отличные от 1 взаимно простые делители числа n при любой паре (i, j) такой, что $(l_i, l_j) \in \overline{\mathrm{cmp}} L^2$. Значит, хотя бы одно из этих двух чисел не делится на p, где p — произвольный простой делитель числа n. Следовательно, найдётся набор чисел $(t_1, t_2, \ldots) \in Z_L$ такой, что $HOK\{t_1, t_2, \ldots\}$ не делится на p. Значит, множество $\Pi(CH, g)$ (см. теорему 2.6,б)) содержит число, которое не делится на p. Отсюда по следствию 2 теоремы 1.5 наследственный CH-признак в группе $\langle g \rangle$ и, следовательно, в группе G нетривиален.

Пусть $g \in CH$ и $L(g) = \{l_1, \ldots, l_m\}$, где $m > 1$. По следствию 2 теоремы 1.5 $CH(m-2)$-признак в группе $\langle g \rangle$ тривиален тогда и только тогда, когда $\Pi(CH(m-2), g) = \{n\}$. В данных условиях $n = l_m$ и из теоремы 2.6,в) с учётом определения 1.21 следует, что $\Pi(CH(m-2), g) = \{n\}$ тогда и только тогда, когда $m = 2$ и $l_1 = 1$. □

Следствие 2. *Пусть $g \notin CH$, тогда CH-признак в циклической группе $\langle g \rangle$ является квазиполным в том и только в том случае, когда $n = p_1 \cdot p_2$ и $L(g)$ есть подмножество решётки $D(n)$, содержащее оба её атома.*

Доказательство. Пусть каноническое разложение числа n определено равенством (1.7), где $s > 1$, иначе $g \in CH$.

Предположим, что циклическая группа $\langle g \rangle$ имеет квазиполный CH-признак. Тогда по утверждению 1.11,б) множество $\Pi(CH, g)$ совпадает с множеством всех атомов решётки $D(n)$. Отсюда по теореме 2.5,б) получаем:

$$\mathrm{prm}\{HOK\{t_1, t_2, \ldots\} : (t_1, t_2, \ldots) \in Z_L\}^* = \{p_1, \ldots, p_s\}.$$

Отсюда следует, что во множестве Z_L имеется набор чисел $\{p_i, \ldots, p_i\}$, $i = 1, \ldots, s$. С другой стороны, множество Z_L есть декартово произведение двухэлементных множеств $\{\mathrm{mp}_{n(i,j)}(l_i), \mathrm{mp}_{n(i,j)}(l_j)\}$, состоящих из делителей числа n. Причём оба делителя отличны от 1 и взаимно несравнимы, так как несравнимы числа l_i и l_j. Поэтому во множестве Z_L имеется не более двух наборов чисел вида $\{p_i, \ldots, p_i\}$, $i \in \{1, \ldots, s\}$. Следовательно, из условия квазиполноты CH-признака вытекает, что для любой пары (i, j) такой, что $(l_i, l_j) \in \overline{\mathrm{cmp}} L^2$,

$$\{\mathrm{mp}_{n(i,j)}(l_i), \mathrm{mp}_{n(i,j)}(l_j)\} = \{p_1, p_2\}.$$

Отсюда получаем, что $n(i, j) = p_1 \cdot p_2$ и $\{l_i, l_j\} = \{p_1, p_2\}$ для любой пары $(l_i, l_j) \in \overline{\mathrm{cmp}} L^2$. Значит, $n = p_1 \cdot p_2$ и множество $\overline{\mathrm{cmp}} L^2$ состоит из единственной пары, иначе во множестве $L(g)$ содержатся одинаковые числа. Следовательно, множество $L(g)$ содержит числа p_1, p_2 и, возможно, другие делители числа n, т. е. числа 1, $p_1 \cdot p_2$.

Докажем в обратную сторону.

Пусть $n = p_1 \cdot p_2$ и $p_1, p_2 \in L(g)$. Тогда $\overline{\text{cmp}}L^2 = \{(p_1, p_2)\}$ и по теореме 2.6,б)

$$\Pi(CH, g) = \text{prm}\{\text{mp}_n(p_1), \text{mp}_n(p_2)\}^* = \{p_1, p_2\}.$$

Отсюда по утверждению 1.11,б) циклическая группа $\langle g\rangle$ имеет квазиполный CH-признак. □

Следствие 3. *Пусть множество $L(g)$ — цепь длины $m-1$, где $m>1$, и каноническое разложение числа n определено равенством* (1.7).

Тогда $CH(m-2)$-признак в циклической группе $\langle g\rangle$ является квазиполным в том и только в том случае, когда $s \leqslant m-1$, $l_1 = 1$ и для некоторых номеров $i_1, \ldots, i_s$, где $2 = i_1 < \ldots < i_s \leqslant m$, и некоторой перестановки $j_1 < \ldots < j_s$ чисел $1, \ldots, s$ выполнены равенства:

$$l_{i_1} = p_{j_1} \cdot l_{i_1 - 1}, \ldots, l_{i_s} = p_{j_s} \cdot l_{i_s - 1},$$

где числа $l_1, \ldots, l_{i_r - 1}$ не делятся на p_{j_1}, $r = 1, \ldots, s$.

Доказательство. Пусть циклическая группа $\langle g\rangle$ имеет квазиполный $CH(m-2)$-признак. Тогда по утверждению 1.11,б) и теореме 2.5,в) имеем:

$$\text{prm}\{n_2, \ldots, n_m\}^* = \{p_1, \ldots, p_s\},$$

где $n_i = \text{mp}_{l_i}(l_{i-1})$, $i = 2, \ldots, m$. Отсюда $\{p_1, \ldots, p_s\} \subseteq \{n_2, \ldots, n_m\}$ и, следовательно, $s \leqslant m-1$.

Вместе с тем, из определения 1.21 следует, что если n_i есть простое число p, $i \in \{2, \ldots, m\}$, то $l_i = p \cdot l_{i-1}$ и число l_{i-1} не делится на p. Так как числа $l_1, \ldots, l_{i-1}$ по условию образуют цепь, то каждое из них не делится на p.

Следовательно, для некоторых номеров $i_1, \ldots, i_s$, где $2 \leqslant i_1 < \ldots < i_s \leqslant m$, и некоторой перестановки $j_1 < \ldots < j_s$ чисел $1, \ldots, s$ выполнены равенства:

$$l_{i_1} = p_{j_1} \cdot l_{i_1 - 1}, \ldots, l_{i_s} = p_{j_s} \cdot l_{i_s - 1},$$

При этом числа $l_1, \ldots, l_{i_r - 1}$ не делятся на p_{j_r}, $r = 1, \ldots, s$.

Следовательно, числа $l_1, \ldots, l_{i_1 - 1}$ не делятся ни на одно из простых чисел $p_1, \ldots, p_s$, т. е. , каждое из чисел $l_1, \ldots, l_{i_r - 1}$ равно 1. Так как $l_1, \ldots, l_{i_r - 1}$ есть цепь, не содержащая одинаковых чисел, то это возможно лишь при условиях: $i_1 = 2$, $l_1 = 1$, $l_2 \in \{p_1, \ldots, p_s\}$. □

Пример 2.10. Определим характеристики CH-признака в циклической группе, порождаемой подстановкой g степени 84 с редукцией цикловой структуры $L = (1, 6, 15, 21, 35)$. Каноническое разложение числа $\text{ord}\, g$ следующее: $210 = 2 \cdot 3 \cdot 5 \cdot 7$.

Определим множество $\overline{\text{cmp}}L^2$ всех несравнимых пар чисел из $L(g)$:

$$\overline{\text{cmp}}L^2 = \{(6, 15), (6, 21), (6, 35), (15, 21), (15, 35), (21, 35)\}.$$

Вычислим множество Z_L:

$$Z_L = \{\text{mp}_{30}(6), \text{mp}_{30}(15)\} \times \{\text{mp}_{42}(6), \text{mp}_{42}(21)\} \times \{\text{mp}_{210}(6), \text{mp}_{210}(35)\} \times$$
$$\times \{\text{mp}_{105}(15), \text{mp}_{105}(21)\} \times \{\text{mp}_{105}(15), \text{mp}_{105}(35)\} \times \{\text{mp}_{105}(21), \text{mp}_{105}(35)\} =$$
$$= \{5, 2\} \times \{7, 2\} \times \{35, 6\} \times \{7, 5\} \times \{7, 3\} \times \{5, 3\}.$$

Отсюда получаем, что

$$\{HOK\{t_1, t_2, \ldots\}: (t_1, t_2, \ldots) \in Z_L\}^* = \{30, 35, 42, 70, 105, 210\}.$$

Следовательно, по теореме 2.5,б)

$$\Pi(CH, g) = \mathrm{prm}\{30, 35, 42, 70, 105, 210\} = \{30, 35, 42\}.$$

По множеству $\Pi(CH, g)$ определяем:
1) $\mathrm{pok}_g\, CH = \min\{30, 35, 42\} = 30$;
2) CH-признак в группе $\langle g\rangle$ не является ни тривиальным, ни квазиполным. $\diamondsuit$

§ 2.3. Исследование в группах подстановок наследственных признаков, определяемых свойствами цикловых структур подстановок

2.3.1. Наследственные признаки, определяемые количеством всех циклов и количеством циклов заданной длины подстановки. На группе подстановок $\Phi(X)$ определим функции, принимающие натуральные значения: $\varkappa(g)$ — число всех циклов подстановки g, $\varkappa^l(g)$ — число циклов подстановки g длины не более l, $\xi^l(g)$ — число элементов множества X, принадлежащих циклам подстановки g длины не более l; g-подфункции этих функций обозначим соответственно $\varkappa_g(t)$, $\varkappa_g^l(t)$ и $\xi_g^l(t)$.

Обозначим через $\Phi(\varkappa \geqslant r)$ (через $\Phi(\varkappa^l \geqslant r)$, через $\Phi(\xi^l \geqslant r)$), где r — натуральное, множество подстановок g из группы $\Phi(X)$, для которых $\varkappa(g) \geqslant r$ ($\varkappa^l(g) \geqslant r$, $\xi^l(g) \geqslant r$).

Теорема 2.7. *Любая группа подстановок G имеет при любых натуральных r, l наследственный $\Phi(\varkappa \geqslant r)$-признак ($\Phi(\varkappa^l \geqslant r)$-признак, $\Phi(\xi^l \geqslant r)$-признак), и для $g \in \Phi(X)$*

$$\Pi(\Phi(\varkappa \geqslant r), g) = \mathrm{prm}\{t \in D(n): \sum_{i=1}^{m} k_i \cdot (l_i, t) \geqslant r\}, \tag{2.7а}$$

$$\Pi(\Phi(\varkappa^l \geqslant r), g) = \mathrm{prm}\{t \in D(n): \sum_{i=1}^{m} k_i \cdot (l_i, t) \cdot \delta(l_i, (l_i, t) \cdot l) \geqslant r\}, \tag{2.7б}$$

$$\Pi(\Phi(\xi^l \geqslant r), g) = \mathrm{prm}\{t \in D(n): \sum_{i=1}^{m} k_i \cdot l_i \cdot \delta(l_i, (l_i, t) \cdot l) \geqslant r\}, \tag{2.7в}$$

где $\delta(x, y) = 1$, если $x \leqslant y$, и $\delta(x, y) = 0$, если $x > y$, для действительных чисел x, y.

Доказательство. Если $C(g) = L^K$, где $L = (l_1, \ldots, l_m)$ и $K = (k_1, \ldots, k_m)$, то

$$\varkappa_g(1) = k_1 + \ldots + k_m, \tag{2.8а}$$

$$\varkappa_g^l(1) = k_1 \cdot \delta(l_1, l) + \ldots + k_m \cdot \delta(l_m, l), \tag{2.8б}$$

$$\xi_g^l(1) = k_1 \cdot l_1 \cdot \delta(l_1, l) + \ldots + k_m \cdot l_m \cdot \delta(l_m, l). \tag{2.8в}$$

По утверждению 2.2 при возведении подстановки g в степень t, где t — натуральное, цикл длины l подстановки g либо преобразуется в цикл длины l, если $(l, t) = 1$, либо разлагается на (l, t) циклов длины $v^t(l_i)$ (см. фор-

мулу (2.1)). Отсюда и из формул (2.8а), (2.8б) и (2.8в) получаем, что

$$\varkappa_g(t) = \sum_{i=1}^{m} k_i \cdot (l_i, t), \tag{2.9а}$$

$$\varkappa_g^l(t) = \sum_{i=1}^{m} k_i \cdot (l_i, t) \cdot \delta(l_i, (l_i, t) \cdot l), \tag{2.9б}$$

$$\xi_g^l(t) = \sum_{i=1}^{m} k_i \cdot l_i \cdot \delta(l_i, (l_i, t) \cdot l). \tag{2.9в}$$

При любом натуральном t выполнено неравенство $(l_i, t) \geqslant 1$, поэтому из равенств (2.8а) и (2.9а) следует неравенство $\varkappa_g(t) \geqslant \varkappa_g(1)$.

При любом фиксированном x функция $\delta(x, y)$ монотонна по переменной y, поэтому из равенств (2.8б) и (2.9б) ((2.8в) и (2.9в)) следует неравенство $\varkappa_g^l(t) \geqslant \varkappa_g^l(1)$ (неравенство $\xi_g^l(t) \geqslant \xi_g^l(1)$).

Из формул (2.8а), (2.8б) и (2.8в) следует, что функции $\varkappa(g)$, $\varkappa^l(g)$ и $\xi^l(g)$ являются характеристиками цикловых структур подстановок, поэтому по утверждению 2.8,б) из полученных неравенств $\varkappa_g(t) \geqslant \varkappa_g(1)$, $\varkappa_g^l(t) \geqslant \varkappa_g^l(1)$ и $\xi_g^l(t) \geqslant \xi_g^l(1)$ следует, что функции $\varkappa_g(t)$, $\varkappa_g^l(t)$ и $\xi_g^l(t)$ антимонотонны.

В силу произвольности рассмотренной подстановки g из замечания 1 к определению 1.25 следует, что антимонотонными являются и функция $\varkappa(g)$, $\varkappa^l(g)$ и $\xi^l(g)$. Отсюда по теореме 1.8,а) получаем, что $\Phi(\varkappa \geqslant r)$-признак, $\Phi(\varkappa^l \geqslant r)$-признак и $\Phi(\xi^l \geqslant r)$-признак являются наследственными признаками.

Из равенств (2.9а), (2.9б) и (2.9в) и теоремы 1.5,в) получаем выражения (2.7а), (2.7б) и (2.7в) соответственно для множеств $\Pi(\Phi(\varkappa \geqslant r), g)$, $\Pi(\Phi(\varkappa^l \geqslant r), g)$ и $\Pi(\Phi(\xi^l \geqslant r), g)$. □

Проиллюстрируем на примерах некоторые свойства этих признаков.

Пример 2.11. Рассмотрим $\Phi(\varkappa \geqslant 3)$-признак в циклической группе $\langle g \rangle$ в случае, когда $L = (1, n)$, $K = (1, 1)$, n — натуральное число, отличное от 1.

Так как функция $\varkappa_g(t)$ антимонотонна, то:

1) по следствию 1 теоремы 1.8 $\Phi(\varkappa \geqslant 3)$-признак в циклической группе $\langle g \rangle$ является тривиальным в том и только в том случае, когда $(n, t) = 1$ для любого коатома t решётки $D(n)$; это равносильно тому, что число n — простое;

2) по следствию 3 теоремы 1.8 $\Phi(\varkappa \geqslant 3)$-признак в циклической группе $\langle g \rangle$ является квазиполным в том и только в том случае, когда $(n, t) > 1$ для любого атома t решётки $D(n)$; это условие выполнено для любого натурального $n > 1$. ◇

Пример 2.12. Рассмотрим $\Phi(\varkappa^2 \geqslant p)$-признак и $\Phi(\xi^2 \geqslant p)$-признак в циклической группе $\langle g \rangle$ в случае, когда $L = (1, 2p)$, $K = (1, 1)$, p — простое число, отличное от 2. В этом случае $n = 2p$, и числа 2 и p являются как коатомами, так и атомами решётки $D(n)$, при этом

$$\varkappa_g^2(2) = 1,\ \varkappa_g^2(p) = p + 1,\ \xi_g^2(2) = 1,\ \xi_g^2(p) = 2p + 1.$$

Так как функции $\varkappa_g^2(t)$ и $\xi_g^2(t)$ являются антимонотонными, то:

1) по следствию 1 теоремы 1.8 $\Phi(\varkappa^2 \geqslant p)$-признак и $\Phi(\xi^2 \geqslant p)$-признак в циклической группе $\langle g \rangle$ не являются тривиальными в силу того, что соответственно $\varkappa_g^2(p) \geqslant p$ и $\xi_g^2(p) \geqslant p$;

2) по следствию 3 теоремы 1.8 $\Phi(\boldsymbol{\varkappa}^2 \geqslant p)$-признак и $\Phi(\xi^2 \geqslant p)$-признак в группе $\langle g \rangle$ не являются квазиполными в силу того, что соответственно $\boldsymbol{\varkappa}_g^2(2) < p$ и $\xi_g^2(2) < p$. ◇

2.3.2. Определяющие свойства неподвижных подмножеств подстановок циклической группы. Одной из важных характеристик подстановки является множество элементов области определения, неподвижных относительно подстановки. В связи с этим напомним некоторые определения [6, гл. XI, § 7], полезные при рассмотрении неподвижных подмножеств подстановок.

Пусть $G < \Phi(X)$ и $g \in G$.

Определение 2.13. *Графом группы G подстановок множества X* называется орграф $\Gamma_{G(X)}$ с помеченными дугами, полученный объединением графов всех элементов группы G:

$$\Gamma_{G(X)} = \bigcup_{g \in G} \Gamma_g.$$

Множеством вершин графа $\Gamma_{G(X)}$ является X и пара элементов (x, y) множества X есть дуга графа $\Gamma_{G(X)}$, помеченная подмножеством $G_{x,y}$ группы G, тогда и только тогда, когда $y = g(x)$ для каждого $g \in G_{x,y}$.

Определение 2.14. Если $\{s_1, \ldots, s_p\} = S \subseteq \Phi(X)$ и $G = \langle S \rangle$, то *графом группы G подстановок множества X, построенным по системе образующих S* (обозначим его $\Gamma_{S(X)}$), называется орграф с помеченными дугами, полученный объединением графов всех подстановок системы S:

$$\Gamma_{S(X)} = \Gamma_{s_1} \cup \ldots \cup \Gamma_{s_p}. \diamond$$

Множеством вершин графа $\Gamma_{S(X)}$ является также X и пара элементов (x, y) множества X есть дуга графа $\Gamma_{S(X)}$, помеченная символом s_i, тогда и только тогда, когда $y = s_i(x)$, $i = 1, \ldots, p$. Таким образом, граф $\Gamma_{S(X)}$, также как и граф Кэли Γ_S группы G, является псевдосимметрическим порядка p, но в отличие от него может иметь параллельные дуги и быть несвязным.

Определение 2.15. Элемент $x \in X$ (подмножество $Y \subseteq X$) называется *неподвижным относительно преобразования g* множества X, если $g(x) = x$ ($g(x) = x$ для любого $x \in Y$). ◇

Подмножество всех неподвижных относительно преобразования g элементов множества X обозначим $I(g)$.

Пример 2.13. а) $I(e) = x$, при этом $I(g) \subset X$ для любой постановки $g \neq e$.

б) Если θ — нулевой элемент кольца X, то $\theta \in I(g)$ для любой линейной подстановки g кольца X. ◇

Рассмотрим множество $I(g)$ и его порядок $|I(g)|$ как функции из классов $F(\Phi(X), 2^X)$ и $F(\Phi(X), N)$, т. е. как функции, определённые на группе подстановок $\Phi(X)$ и принимающие значения соответственно в булеане 2^X множества X и в N. Заметим, что на области значений функции $I(g)$ определён частичный порядок, так как булеан 2^X является решёткой относительно теоретико-множественного включения.

Величина $|I(g)|$ (в отличие от множества $I(g)$) однозначно определяется цикловой структурой подстановки g. Следовательно, $|I(g)|$ есть характеристика цикловых структур подстановок, принимающая натуральные значения.

Пусть $\operatorname{ord} g = n$, $C(g) = L^K$, где $L = (l_1, \ldots, l_m)$ и $K = (k_1, \ldots, k_m)$, и для определённости положим, что элементы набора L упорядочены: $l_1 < \ldots < l_m$. Неподвижный относительно преобразования g элемент x образует цикл

длины 1 в графе Γ_g преобразования g. Следовательно, величина $|I(g)|$ есть число циклов длины 1 в подстановке g. Отсюда

$$|I(g)| = \begin{cases} k_1, & l_1 = 1 \\ 0, & l_1 > 1. \end{cases} \tag{2.10}$$

Подстановке g поставим в соответствие функцию $\lambda(\alpha, L, K)$, отображающую $V_m \times N^{2m}$ в N_0:

$$\lambda(\alpha, L, K) = \sum_{i=1}^{m} \alpha_i \cdot l_i \cdot k_i, \tag{2.11}$$

где $\alpha = (\alpha_1, \ldots, \alpha_m) \in V_m$, $L \in N^m$, $K \in N^m$. Функцию $\lambda(\alpha, L, K)$ можно рассматривать, с одной стороны, как семейство отображений $N^{2m} \to N_0$, состоящее из 2^m характеристик его цикловой структуры. С другой стороны, при фиксированных наборах L и K функция $\lambda(\alpha, L, K)$ есть монотонное отображение решётки V_m во множество N_0.

Для всякого вектора $\alpha = (\alpha_1, \ldots, \alpha_m)$ из V_m обозначим через $E(\alpha)$ множество номеров его единичных координат, $E(\alpha) \subseteq \{1, \ldots, m\}$. Если $E(\alpha) = \{i_1, \ldots, i_s\} \neq \varnothing$, то $\lambda(\alpha, L, K)$ есть число элементов множества X, принадлежащих всем циклам длины $l_{i_1}, \ldots, l_{i_s}$ графа Γ_g подстановки g. В частности, $\lambda(\alpha, L, K) = |X|$, если $E(\alpha) = \{1, \ldots, m\}$.

Введём операцию умножения булевой константы β на подмножество Y множества X:

$$\beta \cdot Y = \begin{cases} Y, & \beta = 1 \\ \varnothing, & \beta = 0. \end{cases}$$

Правила возведения подстановки в степень (утверждение 2.2) позволяют получить формулы (2.12)–(2.15), выражающие аналитически:

1) $I(g^t)$ — через множества элементов циклов подстановки g;

2) величину $|I(g^t)|$ — через элементы наборов L и K, $t = 1, \ldots, \operatorname{ord} g$.

Приведём эти формулы. Пусть подстановка g состоит из k независимых циклов, и X_i есть множество элементов i-го цикла, $i = 1, \ldots, k$. Тогда для $t = 1, \ldots, n$ выполнены равенства:

$$I(g^t) = \beta_1^t \cdot X_1 \cup \ldots \cup \beta_k^t \cdot X_k, \tag{2.12}$$

где

$$\beta_i^t = \begin{cases} 1, & \text{если } |X_i|/t, \\ 0, & \text{в противном случае;} \end{cases} \tag{2.13}$$

$$|I(g^t)| = \lambda(\alpha^t, L, K), \tag{2.14}$$

где $\alpha^t = (\alpha_1^t, \ldots, \alpha_m^t)$ и для каждого $j = 1, \ldots, m$

$$\alpha_j^t = \begin{cases} 1, & \text{если } l_i/t, \\ 0, & \text{в противном случае.} \end{cases} \tag{2.15}$$

Обозначим через $I_g(t)$ и $|I_g|(t)$ g-подфункции функций $I(g)$ и $|I(g)|$ соответственно.

Утверждение 2.9. *Функция $I(g)$ и характеристика цикловых структур $|I(g)|$ являются антимонотонными функциями.*

D-диаграмма g-подфункции $I_g(t)$ функции $I(g)$ является простой для любой подстановки $g \in \Phi(X)$.

Доказательство. Пусть $g \in \Phi(X)$, $t \in \{1, \ldots, n\}$ и $(t, n) = d$.

Из утверждения 2.3 следует, в частности, что между множествами неподвижных элементов (циклов длины 1) подстановок g^t и g^d, имеется биекция, при которой соответствующие неподвижные элементы совпадают, т. е. $I_g(t) = I_g(d)$. Значит, для любой фиксированной подстановки g множество $I_g(t)$ однозначно определено делителем d числа n. Следовательно, D-диаграмма функции $I_g(t)$ является простой.

Пусть теперь μ, $t \in \{1, \ldots, n\}$ и выполнено: $(\tau, n) = a$, $(t, n) = b$ и a/b, т. е. $b = a \cdot r$, где r делит n, так как b/n и r/b. По утверждению 1.13,а) g-подфункция функции $I(g)$ антимонотонна, если $I_g(\tau) \subseteq I_g(t)$.

Пусть $h = g^a$. Из определения 2.15 следует, что $I_h(1) \subseteq I_h(r)$ при любом натуральном r. Следовательно, $I_g(a) \subseteq I_g(b)$, что в силу равенств $I_g(t) = I_g(b)$ и $I_g(\tau) = I_g(a)$, вытекающих из простоты D-диаграммы функции $I_g(t)$, равносильно включению $I_g(\tau) \subseteq I_g(t)$. Следовательно, в силу произвольности рассмотренной подстановки g функция $I(g)$ антимонотонна.

Заметим, что $|I_g|(t) = \xi_g^1(t)$ (см. п. 2.3.1), $t = 1, 2, \ldots$, где при доказательстве теоремы 2.7 показано, что функция $\xi_g^1(t)$ антимонотонна. Значит, характеристика цикловых структур $|I(g)|$ антимонотонна. □

2.3.3. Свойства семейства неподвижных подмножеств подстановок циклической группы. Рассмотрим семейство неподвижных подмножеств $\{I_g(t)\colon t = 1, \ldots, n\}$, соответствующих всем подстановкам циклической группы $\langle g \rangle$. Обозначим через $N_{I(g)}$ множество порядков различных значений g-подфункции $|I_g|(t)$ функции $|I(g)|$, т. е.

$$N_{I(g)} = \{|I_g|(1), \ldots, |I_g|(n)\}^*. \tag{2.16}$$

Исследуем состав и порядок множества $N_{I(g)}$. В наборе $\{|I_g|(1), \ldots, |I_g|(n)\}$ могут содержаться одинаковые числа, поэтому для менее трудоёмкого вычисления множества $N_{I(g)}$ важно решить задачу определения наименьшего или близкого к нему подмножества T_g множества N_n со свойством: $N_{I(g)} = \{|I_g|(t), t \in T_g\}^*$.

Для $t \in N_n$ обозначим через $D(t, L)$ множество всех чисел $l_{i_1}, \ldots, l_{i_s}$ из набора L, которые делят число t, где $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, m\}$ и $1 \leqslant s \leqslant m$, если такие числа имеются. Если таких чисел в наборе L нет, то полагаем: $D(t, L) = \varnothing$.

Из формул (2.12) и (2.13) следует, что $I(g^t) \neq \varnothing$ тогда и только тогда, когда $D(t, L) \neq \varnothing$, $t = 1, \ldots, n$. Пусть $\lceil L \rceil$ — верхнее замыкание множества L (см. определение 2.7). Обозначим:

$$\lceil L \rceil_1 = \begin{cases} \lceil L \rceil, & 1 \in L, \\ \lceil L \rceil \cup \{1\}, & 1 \notin L. \end{cases} \tag{2.17}$$

Замечание. Множество $\lceil L \rceil_1$ содержит минимальный элемент (единицу) по отношению делимости чисел, поэтому подмножество $\lceil L \rceil_1$ решётки $D(n)$ является решёткой (решётка $\lceil L \rceil_1$ является подрешёткой решётки $D(n)$, если функция $\inf\{x, y\}$ определена одинаково на одинаковых парах элементов решеток $D(n)$ и $\lceil L \rceil_1$).

Множество атомов решётки $\lceil L \rceil_1$ есть $\{l_{i_1}, \ldots, l_{i_s}\}$, где

$$\{l_{i_1}, \ldots, l_{i_s}\} = \begin{cases} \operatorname{prm}\{l_1, l_2, \ldots, l_m\}, & l_1 > 1, \\ \operatorname{prm}\{l_2, \ldots, l_m\}, & l_1 = 1. \end{cases}$$

Собственный делитель t числа n является коатомом решётки $\lceil L \rceil_1$ тогда и только тогда, когда для некоторого $s < m$ найдётся непустое подмножество $\{i_1, \ldots, i_s\}$ множества $\{1, \ldots, m\}$ такое, что $HOK\{l_{i_1}, \ldots, l_{i_s}\} = t$ и в то же время $HOK\{l_{i_1}, \ldots, l_{i_s}, l_j\} = n$ при любом $j \in \{1, \ldots, m\}$, $j \neq \{i_1, \ldots, i_s\}$. $\diamondsuit$

Для подстановки g с редукцией цикловой структуры L определим функцию $v(t, L)$ из класса $F(N_n, \lceil L \rceil_1)$, где:

$$v(t, L) = \begin{cases} HOK\{l_{i_1}, \ldots, l_{i_s}\}, & D(t, L) = \{l_{i_1}, \ldots, l_{i_s}\} \neq \varnothing \\ 1, & D(t, L) = \varnothing. \end{cases} \tag{2.18}$$

Утверждение 2.10. *Функция $v(t, L)$: $N_n \to \lceil L \rceil_1$ есть нормальный эпиморфизм множества $(N_n, /)$ с частичным порядком относительно делимости чисел на решётку $\lceil L \rceil_1$. Ограничение $v'(t, L)$ функции $v(t, L)$ на решётку $D(n)$ есть нормальный эпиморфизм решёток. Для $t = 1, \ldots, n$ выполнено:*

а) *$v(t, L)$ делит t;*

б) *$v(t, L) = t$ тогда и только тогда, когда $t \in \lceil L \rceil_1$;*

в) *$I_g(t) = I_g(v(t, L))$.*

Доказательство. Если τ делит t для $\tau, t \in N_n$, то $D(\tau, L) \subseteq D(t, L)$, отсюда и из равенства (2.18) следует, что $v(\tau, L)$ делит $v(t, L)$. Следовательно, по утверждению 1.13,б) функции $v'(t, L)$ и $v(t, L)$ суть нормальные эпиморфизмы.

а) Пусть $D(t, L) \neq \varnothing$ и $D(t, L) = \{l_{i_1}, \ldots, l_{i_s}\}$. Тогда каждое из чисел $l_{i_1}, \ldots, l_{i_s}$ делит t, значит, $HOK(l_{i_1}, \ldots, l_{i_s})$ также делит t. Следовательно, $v(t, L)$ делит t.

Если $D(t, L) = \varnothing$, то $v(t, L) = 1$. Значит, и в этом случае $v(t, L)$ делит t.

б) По утверждению 2.10,а) справедливо выражение:

$$t = r \cdot v(t, L),\ t = 1, \ldots, n,$$

где в силу определения чисел $l_{i_1}, \ldots, l_{i_s}$ натуральное число r не делится ни на одно из чисел набора L, отличных от $l_{i_1}, \ldots, l_{i_s}$. Значит, если $r = 1$, то $v(t, L) = t$, поэтому $t \in \lceil L \rceil_1$. Если $r > 1$, то $v(t, L) \neq t$ и $t \notin \lceil L \rceil_1$.

в) Пусть $D(t, L) \neq \varnothing$ и $D(t, L) = \{l_{i_1}, \ldots, l_{i_s}\}$, тогда из определения множества $D(t, L)$ и равенств (2.15) следует, что $E(\alpha^t) = \{i_1, \ldots, i_s\}$.

С другой стороны, из равенств (2.18) и (2.15) получаем, что $E(\alpha^{v(t, L)}) = \{i_1, \ldots, i_s\}$. Значит, $E(\alpha^t) = E(\alpha^{v(t, L)})$ и, следовательно, $\alpha^t = \alpha^{v(t, L)}$. Отсюда по формуле (2.14) получаем: $|I_g|(t) = |I_g|(v(t, L))$.

По утверждению 2.10,а) $v(t, L)$ делит t, тогда из утверждения 2.9 следует, что $I_g(v(t, L)) \subseteq I_g(t)$. Так как порядки этих множеств равны, то равны и множества.

Если $D(t, L) = \varnothing$, то $I(g^t) = \varnothing$. Значит, из утверждения 2.9 следует, что $I(g) = \varnothing$. Следовательно, $I(g^{v(t, L)}) = \varnothing$, так как в этом случае из равенства (2.18) имеем: $v(t, L) = 1$. $\square$

Следствие 1. *Пусть $\bar{L} = (l_2, \ldots, l_m)$, тогда:*

а) $\lceil L \rceil_1 = \begin{cases} \lceil L \rceil \cup \{1\}, & I(g) = \varnothing, \\ \lceil \bar{L} \rceil \cup \{1\}, & I(g) \neq \varnothing. \end{cases}$

б) $N_{I(g)} = \begin{cases} \{0\} \cup \{|I_g|(t)\colon\ t \in \lceil L \rceil\}^*, & I(g) = \varnothing, \\ \{k_1\} \cup \{|I_g|(t)\colon\ t \in \lceil \bar{L} \rceil\}^*, & I(g) \neq \varnothing. \end{cases}$

Доказательство. а) В случае $I(g) = \varnothing$ равенство вытекает из равенств (2.17) и (2.10).

Если $I(g)\neq\varnothing$, то из равенства (2.10) следует, что $l_1=1$. Следовательно, из равенства (2.17) получаем, что $\lceil L\rceil_1=\lceil L\rceil$, где в силу равенства $l_1=1$ $\lceil L\rceil=\lceil\bar{L}\rceil_1$ и по формуле (2.17) $\lceil\bar{L}\rceil_1=\lceil\bar{L}\rceil\cup\{1\}$, так как $1\notin\bar{L}$.

б) Пусть $I(g)=\varnothing$, тогда $I(g^t)=\varnothing$ и $\upsilon(t,L)=1$ для тех t, которые не делятся ни на одно из чисел набора L, и для остальных $t\in\{1,\ldots,n\}$ в силу равенств (2.18) значения функции $\upsilon(t,L)$ пробегают все элементы множества $\lceil L\rceil$. Отсюда по утверждению 2.10,в) получаем:

$$\{|I_g|(1),\ldots,|I_g|(n)\}^*=\{0\}\cup\{|I_g|(t),\ t\in\lceil L\rceil\}^*.$$

Пусть $I(g)\neq\varnothing$, тогда из равенства (2.10) следует, что $l_1=1$, т. е. $L=(1,l_2,\ldots,l_m)$, где $1<l_2<\ldots<l_m$. В данном случае в силу равенств (2.18) $\upsilon(t,L)=1$ для тех $t\in N_n$, которые не делятся ни на одно из чисел множества $\bar{L}$, и $\upsilon(t,L)>1$ для остальных $t\in N_n$.

Значит, по утверждению 2.10,в) получаем:

$$\{|I_g|(1),\ldots,|I_g|(n)\}^*=\{|I_g|(1)\}\cup\{|I_g|(t),\ t\in\lceil\bar{L}\rceil\}^*,$$

где из равенства (2.10) следует, что $|I_g|(1)=k_1$.

В завершение заметим, что $|I_g|(\upsilon(t,L))>k_1$ для тех $t\in\{1,\ldots,n\}$, которые делятся хотя бы на одно из чисел множества $\bar{L}$.

Действительно, из равенств (2.14) имеем, что $|I_g|(\upsilon(t,L))=\lambda(\alpha^{\upsilon(t,L)},L,K)$, где вектор $\alpha^{\upsilon(t,L)}$ (см. равенства (2.15)) отличен от нулевого и имеет кроме первой единичной координаты по меньшей мере ещё одну единичную координату. □

Следствие 2. $|N_{I(g)}|\leqslant|\lceil L\rceil_1|\leqslant\begin{cases}2^m, & I(g)=\varnothing,\\ 2^{m-1}, & I(g)\neq\varnothing.\end{cases}$

Доказательство. Из определения множества $\lceil L\rceil$ следует: $|\lceil L\rceil|\leqslant 2^m-1$ и $|\lceil\bar{L}\rceil|\leqslant 2^{m-1}-1$. Отсюда и из следствия 1 утверждения 2.10 вытекают оценки порядков множеств. □

Установим важное свойство $\lceil L\rceil_1$-диаграммы функции $|I_g|(t)$ (см. определение 1.26).

Следствие 3. *$\lceil L\rceil_1$-диаграмма функции $|I_g|(t)$ является простой.*

Доказательство. По утверждению 2.10 функция $\upsilon(t,L)$ при фиксированном множестве L есть эпиморфизм решётки N_n на решётку $\lceil L\rceil_1$, где $\lceil L\rceil_1\subseteq D(n)$. Эпиморфизм $\upsilon(t,L)$ отображает простую (по утверждению 2.8,а)) D-диаграмму функции $|I_g|(t)$ на $\lceil L\rceil_1$-диаграмму этой функции, которая является также простой в силу утверждения 2.10,в). □

Граф с помеченными вершинами, соответствующий $\lceil L\rceil_1$-диаграмме функции $|I_g|(t)$, обозначим для краткости $\Gamma_L(|I_g|)$.

Пример 2.14. Определим множества $\lceil L\rceil_1$ и $N_{I(g)}$ для циклической группы, порождаемой подстановкой g степени 84 (такие подстановки рассмотрены в примерах 2.8–2.10), у которой цикловая структура $C(g)=(1^7,6,15,21,35)$.

Для этой подстановки

$$K=(7,1,1,1,1),\ L=(1,6,15,21,35),\ \bar{L}=(6,15,21,35).$$

Отсюда, по следствию 1,а) утверждения 2.10, используя формулу (2.18), получаем:

$$\lceil L\rceil_1=\{1\}\cup\lceil\bar{L}\rceil=\{1,6,15,21,35,30,42,105,210\}.$$

По формулам (2.11), (2.14) и (2.15) вычисляем множество чисел $\{|I_g|(t),\ t\in\{1\}\cup\lceil\bar{L}\rceil\}$.

Таблица 2.1

Метки вершин $\lceil L\rceil_1$-диаграммы функции $|I_g|(t)$

$t\in\lceil L\rceil_1$	1	6	15	21	35	30	42	105	210
$\|I_g\|(t)$	7	13	22	28	42	28	34	78	84

По следствию 1,б) утверждения 2.10

$$N_{I(g)}=\{k_1\}\cup\{|I_g|(t),\ t\in\lceil\bar{L}\rceil\}^*=\{7,13,22,28,42,28,34,78,84\}^*=$$
$$\{7,13,22,28,42,34,78,84\}.\diamond$$

2.3.4. Наследственные признаки, определяемые числом неподвижных элементов относительно подстановок. Обозначим через $\Phi(|I|\geqslant r)$ множество подстановок g из группы $\Phi(X)$, имеющих не менее r неподвижных элементов, $1\leqslant r\leqslant|X|$. Исследуем свойства $\Phi(|I|\geqslant r)$-признака в подгруппах группы $\Phi(X)$, в частности, в циклической группе $\langle g\rangle$.

Теорема 2.8. *При $r=1,\ldots,|X|$:*

а) *всякая группа подстановок G имеет наследственный $\Phi(|I|\geqslant r)$-признак и для любой подстановки $g\in\Phi(X)$*

$$\Pi(\Phi(|I|\geqslant r),g)=\mathrm{prm}\{t\in\lceil L\rceil:\ |I_g|(t)\geqslant r\};$$

б) *$\Phi(|I|\geqslant r)$-признак в группе $\langle g\rangle$ является тривиальным тогда и только тогда, когда $|I_g|(t)<r$ для любого коатома t решётки $\lceil L\rceil_1$.*

Доказательство. а) По утверждению 2.9 характеристика цикловых структур $|I(g)|$ антимонотонна. Отсюда по теореме 1.8,а) всякая группа G подстановок множества X, в частности, циклическая группа $\langle g\rangle$, имеет наследственный $\Phi(|I|\geqslant r)$-признак, $r=1,\ldots,|X|$.

По определению $\lceil L\rceil_1\subseteq D(n)$, поэтому для любой подстановки $g\in\Phi(X)$

$$\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}\subseteq\{t\in D(n):\ |I_g|(t)\geqslant r\}.$$

Поэтому каждое минимальное число решётки $\lceil L\rceil_1$ такое, что $|I_g|(t)\geqslant r$, делится на один из минимальных делителей t числа n с тем же свойством. С учётом утверждения 1.9 это равносильно тому, что любое число $\tau\in\mathrm{prm}\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}$ делится на одно из чисел множества $\mathrm{prm}\{t\in D(n):\ |I_g|(t)\geqslant r\}$.

С другой стороны, если $\tau\in\mathrm{prm}\{t\in D(n):\ |I_g|(t)\geqslant r\}$, то по утверждению 1.9 $|I_g|(\tau)\geqslant r$ и $|I_g|(\tau')<r$ для любого собственного делителя τ' числа τ. При этом по утверждению 2.10,в) $|I_g|(\tau)=|I_g|(\upsilon(\tau,L))$, где по утверждению 2.10,а) число $\upsilon(\tau,L)$ делит τ. Значит, $\upsilon(\tau,L)=\tau$ и по утверждению 2.10,б) $\tau\in\lceil L\rceil_1$. Следовательно,

$$\mathrm{prm}\{t\in D(n):\ |I_g|(t)\geqslant r\}\subseteq\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}.$$

Отсюда получаем, что каждое число множества $\mathrm{prm}\{t\in D(n):\ |I_g|(t)\geqslant r\}$ делится на одно из чисел множества $\mathrm{prm}\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}$.

Таким образом, доказано, что если число $\tau\in\mathrm{prm}\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}$, то имеется число $\tau'\in\mathrm{prm}\{t\in D(n):\ |I_g|(t)\geqslant r\}$ такое, что τ' делит τ, и имеется число $\tau''\in\mathrm{prm}\{t\in\lceil L\rceil_1:\ |I_g|(t)\geqslant r\}$ такое, что τ'' делит τ'. Так как

множество $\mathrm{prm}\{t \in \lceil L \rceil_1 \colon |I_g|(t) \geqslant r\}$ либо состоит из одного элемента, либо образует антицепь в решётке чисел $D(n)$, то $\tau = \tau' = \tau''$. Значит,

$$\mathrm{prm}\{t \in \lceil L \rceil_1 \colon |I_g|(t) \geqslant r\} = \mathrm{prm}\{t \in D(n) \colon |I_g|(t) \geqslant r\}.$$

Отсюда получаем по теореме 1.5,в) выражение для множества $\Pi(\Phi(|I| \geqslant r), g)$.

б) По утверждению 2.10 функция $\upsilon(t, L)$ является нормальным эпиморфизмом решётки $D(n)$ на решётку $\lceil L \rceil_1$. Поэтому если τ — коатом решётки $\lceil L \rceil_1$, то имеется коатом t' решётки $D(n)$ такой, что $\upsilon(t', L) = \tau$.

Действительно, если $\upsilon(t, L) = \tau$ и t — не коатом решётки $D(n)$, то в $D(n)$ имеется коатом t' такой, что t делит t', откуда по свойству нормального эпиморфизма следует, что $\upsilon(t, L)$ делит $\upsilon(t', L)$. Значит, коатом τ решётки $\lceil L \rceil_1$ делит $\upsilon(t', L)$, где $\upsilon(t', L) \neq n$. Отсюда $\upsilon(t', L) = \tau$, т. е. искомый коатом t' в решётке $D(n)$ имеется. Следовательно, если неравенство $|I_g|(t) < r$ выполнено для любого коатома t' решётки $D(n)$, то это неравенство выполнено и для любого коатома τ решётки $\lceil L \rceil_1$, так как по утверждению 2.10,в) $|I_g|(t') = |I_g|(\upsilon(t', L))$.

С другой стороны, если t — коатом решётки $D(n)$ и $\upsilon(t, L) = \tau$, то в $\lceil L \rceil_1$ имеется коатом τ' такой, что τ делит τ'. Если при этом $|I_g|(\tau') < r$, то в силу антимонотонности функции $|I_g|(t)$ выполнено и неравенство $|I_g|(\tau) < r$. Так как по утверждению 2.10,в) $|I_g|(t) = |I_g|(\tau)$, то отсюда следует, что $|I_g|(t) < r$. Следовательно, если неравенство $|I_g|(\tau') < r$ выполнено для любого коатома τ' решётки $\lceil L \rceil_1$, то оно выполнено и для любого коатома t решётки $D(n)$.

Таким образом, неравенство $|I_g|(t) < r$ выполнено для любого коатома t решётки $\lceil L \rceil_1$ тогда и только тогда, когда это неравенство выполнено для любого коатома t решётки $D(n)$. Так как $|I_g|(n) = |X| \geqslant r$, $r = 1, \ldots, |X|$, и функция $|I(g)|$ антимонотонна, то по следствию 1 теоремы 1.8 отсюда получаем требуемый критерий тривиальности $\Phi(|I| \geqslant r)$-признака в циклической группе $\langle g \rangle$. □

Уточним полученные утверждения для $\Phi(|I| \geqslant 1)$-признака.

Следствие 1. $\Pi(\Phi(|I| \geqslant 1), g) = \mathrm{prm}\, L$, *вследствие этого:*

1) $\mathrm{pok}_g\, \Phi(|I| \geqslant 1) = l_1$;

2) $\Phi(|I| \geqslant 1)$*-признак в циклической группе* $\langle g \rangle$ *является квазиполным тогда и только тогда, когда множество* $\mathrm{prm}\, L$ *совпадает со множеством атомов решётки* $D(n)$.

Доказательство. По теореме 2.8,а)

$$\Pi(\Phi(|I| \geqslant 1), g) = \mathrm{prm}\{t \in \lceil L \rceil \colon |I_g|(t) \geqslant 1\}.$$

Так как $|I_g|(t) \geqslant 1$ для любого $t \in \lceil L \rceil$, то отсюда получаем, что

$$\Pi(\Phi(|I| \geqslant 1), g) = \mathrm{prm} \lceil L \rceil.$$

Множество $\lceil L \rceil$ состоит из всех чисел вида $HOK(l_{i_1}, \ldots, l_{i_s})$, где $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, m\}$, $1 \leqslant s \leqslant m$, поэтому $\mathrm{prm} \lceil L \rceil = \mathrm{prm}\, L$. Значит,

$$\Pi(\Phi(|I| \geqslant 1), g) = \mathrm{prm}\, L.$$

По следствию 1 теоремы 1.5 $\mathrm{pok}_g\, \Phi(|I| \geqslant 1)$ есть наименьшее из чисел множества $\Pi(\Phi(|I| \geqslant 1), g)$. Значит, $\mathrm{pok}_g\, \Phi(|I| \geqslant 1)$ есть наименьшее из

чисел множества $\operatorname{prm} L$. По условию это число равно l_1. Используя полученное выражение для множества $\Pi(\Phi(|I| \geqslant 1), g)$, получаем по утверждению 1.11,б) критерий квазиполноты $\Phi(|I| \geqslant 1)$-признака в циклической группе $\langle g \rangle$. □

Следствие 2. *Подгруппа $\Phi(|I| \geqslant 1)$-тривиальности циклической группы $\langle g \rangle$ есть $\langle g^t \rangle$, где $t = HOK(\operatorname{mp}_n(l_1), \ldots, \operatorname{mp}_n(l_m))$.*

Доказательство. По следствию 1 теоремы 2.8

$$\Pi(\Phi(|I| \geqslant 1), g) = \operatorname{prm} L = \{l_{j_1}, \ldots, l_{j_r}\},$$

где $\{j_1, \ldots, j_r\} \subseteq \{1, \ldots, m\}$ и $1 \leqslant r \leqslant m$. Тогда по следствию теоремы 1.7 подгруппа $\Phi(|I| \geqslant 1)$-тривиальности группы $\langle g \rangle$ есть $\langle g^t \rangle$, где

$$t = HOK(\operatorname{mp}_n(l_{j_1}), \ldots, \operatorname{mp}_n(l_{j_r})).$$

Если l_i / l_j, где $i, j \in \{1, \ldots, m\}$, то из определения 1.21 следует, что $\operatorname{mp}_n(l_j)$ делит $\operatorname{mp}_n(l_i)$. Так как любое число набора L делится на одно из чисел множества $\operatorname{prm} L$, то

$$HOK(\operatorname{mp}_n(l_{j_1}), \ldots, \operatorname{mp}_n(l_{j_r})) = HOK(\operatorname{mp}_n(l_1), \ldots, \operatorname{mp}_n(l_m)).\square$$

Следствие 3. *$\Phi(|I| \geqslant 1)$-признак тривиален в циклической группе $\langle g \rangle$ тогда и только тогда, когда g — равноцикловая подстановка.*

Доказательство. Тривиальность любого наследственного H-признака в циклической группе $\langle g \rangle$ означает, что $\operatorname{pok}_g H = n$. Значит, в силу следствия 1 теоремы 2.8 тривиальность $\Phi(|I| \geqslant 1)$-признака в группе $\langle g \rangle$ равносильна тому, что $l_1 = n$. Так как по условию $n = HOK(l_1, \ldots, l_m)$, где m — натуральное и $l_1 < \ldots < l_m$, то равенство $l_1 = n$ возможно лишь в том случае, когда $m = 1$, т. е. g — равноцикловая подстановка. □

Теорема 2.9. *Пусть $S = \{s_1, \ldots, s_p\} \subseteq \Phi(X)$ и $G = \langle S \rangle$. Тогда:*

а) *$\Phi(|I| \geqslant 1)$-показатель группы G равен обхвату графа $\Gamma_{S(X)}$ группы G, построенному по системе образующих S, и справедлива оценка:*

$$\operatorname{pok}_S \Phi(|I| \geqslant 1) \leqslant \min\{l_{11}, \ldots, l_{p1}\},$$

где l_{j1} — наименьшая из длин циклов подстановки s_j, $j = 1, \ldots, p$;

б) *тривиальность $\Phi(|I| \geqslant 1)$-признака в группе подстановок G равносильна каждому из следующих предложений:*

б1) *группа G состоит из равноцикловых подстановок;*

б2) *имеется c-базис группы G, состоящий из равноцикловых подстановок.*

Доказательство. а) По определению $\operatorname{pok}_S \Phi(|I| \geqslant 1)$ есть наименьшая из длин элементов g группы G (в системе образующих S), для которых $I(g) \neq \varnothing$.

Если $g(x) = x$ для некоторого $x \in X$ и кратчайшее слово в алфавите S, представляющее преобразование g, есть $s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_t}$, то это равносильно тому, что в графе $\Gamma_{S(X)}$ кратчайший цикл, содержащий элемент x, имеет длину t. Следовательно, $\operatorname{pok}_S \Phi(|I| \geqslant 1)$ есть обхват графа $\Gamma_{S(X)}$.

По следствию 4 теоремы 1.5 $\operatorname{pok}_S \Phi(|I| \geqslant 1)$ не превышает наименьшего из чисел множества $\Pi(\Phi(|I| \geqslant 1), s_1) \cup \ldots \cup \Pi(\Phi(|I| \geqslant 1), s_p)$, где по следствию 1 теоремы 2.8 наименьшее из чисел множества $\Pi(\Phi(|I| \geqslant 1), s_j)$ равно l_{j1}, $j = 1, \ldots, p$.

б) Рассмотрим c-покрытие группы G с произвольной системой R c-образующих (см. равенство (1.2) при $Q = G$).

По утверждению 1.8,в) $\Phi(|I| \geqslant 1)$-признак тривиален в группе G тогда и только тогда, когда $\Phi(|I| \geqslant 1)$-признак тривиален в циклической группе $\langle g \rangle$ для любого $g \in R$.

Это утверждение верно, в частности, если $R = G$ или если R есть c-базис группы G. Отсюда и из следствия 3 теоремы 2.8 получаем, что тривиальность $\Phi(|I| \geqslant 1)$-признака в группе подстановок G равносильна как предложению б1) (при $R = G$), так и предложению б2) (при системе R, являющейся c-базисом группы G). □

Пример 2.15. Пусть $X = V_r$ — пространство двоичных r-мерных векторов и Σ_r — группа сдвигов пространства V_r, т. е. если $x \in V_r$ и $g_\alpha \in \Sigma_r$, то $g_\alpha(x) = x \oplus \alpha$.

Группа сдвигов Σ_r пространства V_r имеет тривиальный $\Phi(|I| \geqslant 1)$-признак. Все нетождественные подстановки группы Σ_r состоят из 2^{r-1} циклов длины 2, т. е. являются равноцикловыми. ◇

Пример 2.16. Определим при некоторых r характеристики наследственного $\Phi(|I| \geqslant r)$-признака в циклической группе $\langle g \rangle$, порождаемой подстановкой g степени 84 с цикловой структурой $C(g) = (1^7, 6, 15, 21, 35)$.

Порядок подстановки g равен 210, $L(g) = (1, 6, 15, 21, 35)$, $K = (7, 1, 1, 1, 1)$.

а) Рассмотрим $\Phi(|I| \geqslant 1)$-признак. В данном случае $\Phi(|I| \geqslant 1)$-признак нетривиален в силу того, что подстановка g не является равноцикловой (следствие 3 теоремы 2.8).

1) По следствию 1 теоремы 2.8

$$\Pi(\Phi(|I| \geqslant 1), g) = \operatorname{prm} L = \operatorname{prm}\{1, 6, 15, 21, 35\} = \{1\} \text{ и } \operatorname{pok}_g \Phi(|I| \geqslant 1) = 1.$$

Следовательно, $\langle g \rangle \subseteq \Phi(|I| \geqslant 1)$.

2) Подгруппа $\Phi(|I| \geqslant 1)$-тривиальности группы $\langle g \rangle$ тривиальна, так как по следствию 2 теоремы 2.8 совпадает с группой $\langle g^t \rangle$, где $t = \operatorname{mp}_{210}(1) = 210$.

б) Рассмотрим $\Phi(|I| \geqslant 17)$-признак.

1) По теореме 2.8,а)

$$\Pi(\Phi(|I| \geqslant 17), g) = \operatorname{prm}\{t \in \lceil L \rceil : |I(g^t)| \geqslant 17\},$$

отсюда и из вычислений примера 2.14 (см. табл. 2.1) следует, что

$$\Phi(|I| \geqslant 17) \cap \langle g \rangle = \langle g^{15} \rangle \cup \langle g^{21} \rangle \cup \langle g^{35} \rangle,$$

так как

$$\Pi(\Phi(|I| \geqslant 17), g) = \operatorname{prm}\{15, 21, 35, 30, 42, 105, 210\} = \{15, 21, 35\}.$$

Отсюда по следствию 1 теоремы 1.5 получаем, что $\operatorname{pok}_g \Phi(|I| \geqslant 17) = 15$, и по следствию 2 теоремы 1.5 получаем, что $\Phi(|I| \geqslant 17)$-признак в группе $\langle g \rangle$ нетривиален.

2) Подгруппа $\Phi(|I| \geqslant 17)$-тривиальности группы $\langle g \rangle$ тривиальна, так как следствию теоремы 1.7 совпадает с группой $\langle g^t \rangle$, где

$$t = HOK(\operatorname{mp}_{210}(15), \operatorname{mp}_{210}(21), \operatorname{mp}_{210}(35)) = HOK(14, 10, 6) = 210. \diamond$$

§ 2.4. Исследование в группах подстановок наследственных признаков, определяемых свойством нормальной неподвижности

2.4.1. Свойство делимости порядков неподвижных подмножеств подстановок циклической группы. Определим на множестве $N_n \times N_n$ функцию $\eta_g(t, \tau)$ от переменных t и τ, принимающую неотрицательные рациональные значения:

$$\eta_g(t, \tau) = \begin{cases} \dfrac{|I_g|(t)}{|I_g|(\tau)}, & |I_g|(\tau) \neq 0, \\ 0, & |I_g|(\tau) = 0. \end{cases} \tag{2.19}$$

Из равенств (2.14) следует, что для всех $t, \tau \in N_n$

$$\eta_g(t, \tau) = \begin{cases} \dfrac{\lambda(\alpha^t, L, K)}{\lambda(\alpha^\tau, L, K)}, & \alpha^\tau \text{ — ненулевой вектор}, \\ 0, & \alpha^\tau \text{ — нулевой вектор},. \end{cases} \tag{2.20}$$

где векторы α^t и α^τ определены равенствами (2.15).

Пусть w и w' — упорядоченные наборы чисел из множества N_n, где $w = (\tau_0, \tau_1, \ldots, \tau_k)$, $w' = (\tau'_0, \tau'_1, \ldots, \tau'_k)$, $k \geqslant 0$. Число элементов набора w обозначим символом $|w|$. Следовательно, $|w| = |w'| = k+1$.

Определение 2.16. Пусть $|w| = |w'| > 1$, тогда *наборы* w и w' назовём η_g*-эквивалентными*, если

$$\eta_g(\tau_{i-1}, \tau_i) = \eta_g(\tau'_{i-1}, \tau'_i), \quad i = 1, \ldots, k. \diamondsuit$$

Если $|w| > 1$, то через $R_g^\eta(w)$ обозначим множество значений функции $\eta_g(t, \tau)$ на всех k соседних парах набора w:

$$R_g^\eta(w) = \{\eta_g(\tau_0, \tau_1), \eta_g(\tau_1, \tau_2), \ldots, \eta_g(\tau_{k-1}, \tau_k)\}^*. \tag{2.21}$$

Определение 2.17. Пусть $|w| > 1$, тогда набор w назовём *нормальным* (p*-нормальным*), если $R_g^\eta(w) \subseteq N$ ($R_g^\eta(w) \subseteq N^{[p]}$). $\diamondsuit$

Замечание 1. Пара чисел (t, τ) из множества N_n является нормальной (p-нормальной), если $\eta_g(t, \tau) \in N$ ($\eta_g(t, \tau) \in N^{[p]}$).

Замечание 2. Если набор w является нормальным (p-нормальным), то $|I_g|(t) > 0$ для любого $t \in \{\tau_0, \tau_1, \ldots, \tau_k\}$.

Замечание 3. Если наборы w и w' η_g-эквивалентны, то $R_g^\eta(w) = R_g^\eta(w')$.

Замечание 4. Если набор w является нормальным (p-нормальным), то и η_g-эквивалентный ему набор w' является нормальным (p-нормальным).

Определение 2.18. Если $|w| > 1$ и в наборе w имеются совпадающие соседние числа, т. е. $\tau_i = \tau_{i-1}$ при некотором $i \in \{1, \ldots, k\}$, то *редукцией набора* w назовём упорядоченный набор w', полученный удалением из набора w всех чисел, совпадающих с предыдущим числом: элемент τ_i удаляется тогда и только тогда, когда $\tau_i = \tau_{i-1}$, $i = 1, \ldots, k$. Если $\tau_i \neq \tau_{i-1}$ при любом $i = 1, \ldots, k$, то редукцией набора w является сам набор w. $\diamondsuit$

Замечание. Редукция набора w есть единственное число τ_0 тогда и только тогда, когда $\tau_0 = \tau_1 = \ldots = \tau_k$. $\diamondsuit$

Эпиморфизм $\upsilon(t, L)$, определённый равенством (2.18), индуцирует отображение $\bar{\upsilon}(w, L)$ наборов натуральных чисел в упорядоченные наборы элементов решётки $\lceil L \rceil_1$:

$$\bar{\upsilon}(w, L) = (\upsilon(\tau_0, L), \upsilon(\tau_1, L), \ldots, \upsilon(\tau_k, L)).$$

Утверждение 2.11. *Пусть* $w=(\tau_0, \tau_1, \ldots, \tau_k)$ *и* $|w|>1$. *Тогда:*
а) *наборы* w *и* $\bar{v}(w, L)$ η_g*-эквивалентны;*
б) *если* $|I_g|(\tau_i)>0$ *при* $i=1, \ldots, k$, *то*

$$\eta_g(\tau_0, \tau_k)=\eta_g(\tau_0, \tau_1)\cdot\eta_g(\tau_1, \tau_2)\cdot\ldots\cdot\eta_g(\tau_{k-1}, \tau_k).$$

в) *если* w' *— редукция набора* w *и* $|w'|>1$, *то*

$$R_g^\eta(w')\subseteq R_g^\eta(w)\subseteq\{1\}\cup R_g^\eta(w'). \tag{2.22}$$

Доказательство. а) Если $|I_g|(\tau_i)>0$, то из равенства (2.19) и утверждения 2.10,в) следует, $i=1, \ldots, k$:

$$\eta_g(\tau_{i-1}, \tau_i)=\frac{|I_g|(\tau_{i-1})}{|I_g|(\tau_i)}=\frac{|I_g|(v(\tau_{i-1}, L))}{|I_g|(v(\tau_i, L))}=\eta_g(v(\tau_{i-1}, L), v(\tau_i, L)).$$

Если $|I_g|(\tau_i)=0$, то $\eta_g(\tau_{i-1}, \tau_i)=0$ и, следовательно, по утверждению 2.10,в) $|I_g|(v(\tau_i, L))=0$, поэтому из равенства (2.19) получаем, что

$$\eta_g(\tau_{i-1}, \tau_i)=0=\eta_g(v(\tau_{i-1}, L), v(\tau_i, L)), \quad i=1, \ldots, k.$$

Значит, в любом случае наборы w и $\bar{v}(w, L)$ η_g-эквивалентны.
Утверждение б) следует из равенства (2.19).
в) Пусть $\tau_i=\tau_{i-1}$ при некотором $i\in\{1, \ldots, k\}$, тогда $|I_g|(\tau_i)=|I_g|(\tau_{i-1})$.
Достаточно доказать, что если набор w' получен удалением единственного числа τ_i из набора w, то выполнены включения (2.22).
Если набор w' получен удалением числа τ_i из набора w, то множество $R_g^\eta(w')$ получается из множества $R_g^\eta(w)$ либо удалением числа $\eta_g(\tau_{k-1}, \tau_k)$, если $i=k$, либо удалением чисел $\eta_g(\tau_{i-1}, \tau_i)$, $\eta_g(\tau_i, \tau_{i+1})$ и добавлением числа $\eta_g(\tau_{i-1}, \tau_{i+1})$, если $i<k$.
Если $|I_g|(\tau_i)=0$, то $|I_g|(\tau_{i-1})=0$ и из равенства (2.19) следует, что при $i<k$

$$\eta_g(\tau_{i-1}, \tau_i)=\eta_g(\tau_i, \tau_{i+1})=\eta_g(\tau_{i-1}, \tau_{i+1})=0$$

и при $i=k$

$$\eta_g(\tau_{k-1}, \tau_k)=\eta_g(\tau_{k-2}, \tau_{k-1})=0.$$

Значит, $R_g^\eta(w')=R_g^\eta(w)$ в случае $|I_g|(\tau_i)=0$.
Если $|I_g|(\tau_i)>0$, то $|I_g|(\tau_{i-1})>0$ и из равенства (2.19) следует, что если $i=k$, то

$$\eta_g(\tau_{k-1}, \tau_k)=1,$$

и если $i<k$, то

$$\eta_g(\tau_{i-1}, \tau_i)=1, \quad \eta_g(\tau_i, \tau_{i+1})=\eta_g(\tau_{i-1}, \tau_{i+1}).$$

Следовательно, в любом случае при удалении числа τ_i из набора w, $i=1, \ldots, k$, множество $R_g^\eta(w')$ «беднее» множества $R_g^\eta(w)$ не более чем на одно число, равное 1, т. е. включения (2.22) выполнены. □

Следствие 1 из утверждения 2.11,а) и определений 2.16, 2.17. *Набор* w *является нормальным (*p*-нормальным) тогда и только тогда, когда является нормальным (*p*-нормальным) набор* $\bar{v}(w, L)$. ◇

Следствие 2. *Если все пары соседних чисел набора w являются нормальными (p-нормальными), то $\eta_g(\tau_0, \tau_k) \in N$ ($\eta_g(\tau_0, \tau_k) \in N^{[p]}$).*

Доказательство. Из утверждения 2.11,б) следует, что если $\eta_g(\tau_{i-1}, \tau_i) \in N$ ($\eta_g(\tau_{i-1}, \tau_i) \in N^{[p]}$), $i = 1, \ldots, k$, то и их произведение $\eta_g(\tau_0, \tau_k) \in N$ ($\eta_g(\tau_0, \tau_k) \in N^{[p]}$). □

Следствие 3. *Набор w, где $|w| > 1$, является нормальным (p-нормальным) тогда и только тогда, когда его редукция w' либо является нормальной (p-нормальной), либо состоит из единственного числа τ_0 и при этом $|I_g|(\tau_0) > 0$.*

Доказательство. Если набор w состоит из одинаковых чисел, т. е. $w = (\tau, \tau, \ldots, \tau)$, то $|w'| = 1$ и из равенства (2.19) следует, что набор w является нормальным (p-нормальным) тогда и только тогда, когда $|I_g|(\tau) > 0$.

Пусть набор w состоит не из одинаковых чисел, тогда $|w'| > 1$. По утверждению 2.11,а) $R_g^\eta(w') \subseteq R_g^\eta(w)$, значит, если $R_g^\eta(w) \subseteq N$ ($R_g^\eta(w) \subseteq N^{[p]}$), то и $R_g^\eta(w') \subseteq N$ ($R_g^\eta(w') \subseteq N^{[p]}$).

Вместе с тем, по утверждению 2.11,а) $R_g^\eta(w) \subseteq \{1\} \cup R_g^\eta(w')$. Поэтому если $R_g^\eta(w') \subseteq N$ ($R_g^\eta(w') \subseteq N^{[p]}$), то и $R_g^\eta(w) \subseteq N$ ($R_g^\eta(w) \subseteq N^{[p]}$). □

2.4.2. Нормально неподвижные подстановки и их свойства. Рассмотрим D-диаграмму и $\lceil L \rceil_1$-диаграмму g-подфункции $|I_g|(t)$ функции $|I(g)|$. По утверждению 2.8,а) и следствию 3 утверждения 2.10 соответственно эти диаграммы являются простыми. Следовательно, в соответствующих графах $\Gamma_D(|I_g|)$ и $\Gamma_L(|I_g|)$ (см. определения 1.26, 1.27) каждая вершина τ помечена единственным символом $|I_g|(\tau)$.

Дуги и пути этих графов являются упорядоченными наборами чисел из множества $\{1, \ldots, n\}$, в которых любые соседние числа различны, так как смежные вершины пути различны. Поэтому из определений 2.17 и 2.16 и из следствий утверждения 2.11 вытекают следующие свойства любого пути w в графе $\Gamma_D(|I_g|)$ или графе $\Gamma_L(|I_g|)$:

1) последовательность вершин пути w является редуцированным набором чисел;

2) путь w является нормальным (p-нормальным) тогда и только тогда, когда он состоит из нормальных (p-нормальных) дуг;

3) путь w является нормальным (p-нормальным) тогда и только тогда, когда является нормальным (p-нормальным) набор $\bar{v}(w, L)$;

4) путь w из t в τ является нормальным (p-нормальным) тогда и только тогда, когда редукция набора $\bar{v}(w, L)$ либо является нормальной (p-нормальной), либо состоит из единственного числа t и при этом $|I_g|(t) > 0$.

Обозначим через $W_D(t, \tau)$ (через $W_L(t, \tau)$) множество всех путей из t в τ в графе $\Gamma_D(|I_g|)$ (в графе $\Gamma_L(|I_g|)$), где $t \neq \tau$.

Определение 2.19. *Вершина τ графа $\Gamma_D(|I_g|)$ или графа $\Gamma_L(|I_g|)$* называется *нормальной (p-нормальной)*, если либо $\tau = n$, либо при $\tau \neq n$ является нормальным (p-нормальным) любой путь $w \in W_D(n, \tau)$ или соответственно любой путь $w \in W_L(n, \tau)$. ◇

Множество всех нормальных (p-нормальных) вершин графов $\Gamma_D(|I_g|)$ и $\Gamma_L(|I_g|)$ обозначим соответственно $D^\nu(g)$ и $L^\nu(g)$ ($D^{p\nu}(g)$ и $L^{p\nu}(g)$).

Определение 2.20. Подстановка g называется *нормально (p-нормально) неподвижной*, если функция $|I_g|(t)$ является антинормальной (p-антинормальной). ◇

Из определения 1.24 следует, что если подстановка g нормально (p-нормально) неподвижна, то $I(g) \neq \varnothing$.

Пример 2.17. а) Подстановка e является нормально неподвижной и p-нормально неподвижной при любом натуральном p.

В этом случае $n=1$ и $\eta_g(1,1)=1\in N^{[p]}$ при любом натуральном p.

б) Полноцикловая подстановка g множества X не является нормально неподвижной, так как $I(g)=\varnothing$.

в) Подстановка g множества X, где $|X|>2$, с цикловой структурой, заданной множествами $L=(1,|X|-1)$ и $K=(1,1)$, является нормально неподвижной и $|X|$-нормально неподвижной.

В этом случае $n=|X|-1$, $|I_g|(n)=|X|$ и $|I_g|(t)=1$ при $t=1,\ldots,n-1$. Следовательно, из равенства (2.19) получаем:

$$\eta_g(t,\tau)=\begin{cases}|X|, & t=n,\quad \tau\in\{1,\ldots,n-1\},\\ 1, & \text{в противном случае.}\end{cases}\ \diamondsuit$$

Множество всех подстановок группы $\Phi(X)$, являющихся нормально (p-нормально) неподвижными, обозначим $\Lambda^{[\nu]}(X)$ или кратко $\Lambda^{[\nu]}$ ($\Lambda^{[p\nu]}(X)$ или кратко $\Lambda^{[p\nu]}$).

Отсюда и из определения 2.20 следует, что при любом натуральном p:

$$\Lambda^{[p\nu]}\subseteq\Lambda^{[\nu]}\subseteq\Phi(|I|\geqslant 1), \tag{2.23}$$

где $\Lambda^{[p\nu]}\neq\varnothing$ при любом натуральном p (см. пример 2.17).

Далее доказательства некоторых теорем и утверждений, помечены символом *. Это означает, что во избежание перегруженности в помеченных доказательствах рассмотрены только свойства, связанные с нормальностью дуг и вершин графов $\Gamma_D(|I_g|)$ и $\Gamma_L(|I_g|)$. Доказательства, связанные со свойством p-нормальности дуг и вершин этих графов, проводятся аналогично.

Утверждение 2.12. *Следующие предложения равносильны:*

1) $g\in\Lambda^{[\nu]}$ ($g\in\Lambda^{[p\nu]}$);

2) $\eta_g(t,\tau)\in N$ ($\eta_g(t,\tau)\in N^{[p]}$) *для всех* $\tau, t\in N_n$ *таких, что* (τ,n) *делит* (t,n);

3) $\eta_g(t,\tau)\in N$ ($\eta_g(t,\tau)\in N^{[p]}$) *для всех* $\tau, t\in N_n$ *таких, что* τ/t;

4) $\eta_g(t,\tau)\in N$ ($\eta_g(t,\tau)\in N^{[p]}$) *для всех* $\tau, t\in D(n)$ *таких, что* τ/t;

5) $\eta_g(t,\tau)\in N$ ($\eta_g(t,\tau)\in N^{[p]}$) *для всех* $\tau, t\in\lceil L\rceil_1$ *таких, что* τ/t;

6) *все дуги графа* $\Gamma_D(|I_g|)$ *являются нормальными* (p-*нормальными*);

7) *все вершины графа* $\Gamma_D(|I_g|)$ *являются нормальными* (p-*нормальными*);

8) *вершина* 1 *графа* $\Gamma_D(|I_g|)$ *является нормальной* (p-*нормальной*);

9) *все дуги графа* $\Gamma_L(|I_g|)$ *являются нормальными* (p-*нормальными*);

10) *все вершины графа* $\Gamma_L(|I_g|)$ *являются нормальными* (p-*нормальными*);

11) *вершина* 1 *графа* $\Gamma_L(|I_g|)$ *является нормальной* (p-*нормальной*).

Доказательство *. Нормальная неподвижность подстановки g равносильна предложению 2,в) силу определений 2.20 и 1.24.

Используем далее схему доказательства:

$$2\to3\to4\to5\to2,\quad 4\to6\to4,\ 6\to7\to8\to6,\quad 5\to9\to5,\quad 9\to10\to11\to9,$$

где переход $i\to j$ означает следование предложения i из предложения j для $i,j\in\{2,3,\ldots,11\}$.

Если $\tau, t\in N_n$ и τ/t, то (τ,n) делит (t,n). Поэтому из второго предложения следует третье.

Так как $\lceil L \rceil_1 \subseteq D(n) \subseteq \{1, \ldots, n\}$, то из третьего предложения следует четвёртое и из четвёртого предложения следует пятое.

Докажем, что из пятого предложения следует второе.

Пусть $\tau, t \in N_n$ и (τ, n) делит (t, n). По утверждению 2.10 $\upsilon(\tau, L)$ есть нормальный эпиморфизм, поэтому $\upsilon(\tau, L)$ делит $\upsilon(t, L)$. Значит, по условию предложения 5 упорядоченная пара $(\upsilon(t, L), \upsilon(\tau, L))$ вершин из $\lceil L \rceil_1$ является нормальной. Отсюда по следствию 1 утверждения 2.11 получаем, что упорядоченная пара (t, τ) вершин из $D(n)$ также является нормальной. Цепочка $2 \to 3 \to 4 \to 5 \to 2$ доказана.

Если пара (t, τ) есть дуга графа $\Gamma_D(|I_g|)$, то $t, \tau \in D(n)$ и τ / t. Значит, из предложения 4 следует предложение 6.

Если выполнено предложение 6 и τ / t, то путь w из $W_D(t, \tau)$ состоит из нормальных дуг. Отсюда по следствию 2 утверждения 2.11 получаем, что $\eta_g(t, \tau) \in N$. Значит, выполнено предложение 4 и цепочка $4 \to 6 \to 4$ доказана.

Из предложения 6 следует предложение 7 по определению 2.19.

Из предложения 7 следует предложение 8 очевидным образом.

Так как для любой дуги (t, τ) графа $\Gamma_D(|I_g|)$ найдётся путь из n в 1, проходящий через эту дугу, то из предложения 8 следует предложение 6 по определению 2.19. Цепочка $6 \to 7 \to 8 \to 6$ доказана.

Если пара (t, τ) есть дуга графа $\Gamma_L(|I_g|)$, то $t, \tau \in \lceil L \rceil_1$ и τ / t. Значит, из предложения 5 следует предложение 9.

Если выполнено предложение 9 и τ / t, то путь w из $W_L(t, \tau)$ состоит из нормальных дуг. Отсюда по следствию 2 утверждения 2.11 получаем, что $\eta_g(t, \tau) \in N$. Значит, выполнено предложение 5 и цепочка $5 \to 9 \to 5$ доказана.

Из предложения 9 следует предложение 10 по определению 2.19.

Из предложения 10 следует предложение 11 очевидным образом.

Так как для любой дуги (t, τ) графа $\Gamma_L(|I_g|)$ найдётся путь из n в 1, проходящий через эту дугу, то из предложения 11 следует предложение 9 по определению 2.19. Цепочка $9 \to 10 \to 11 \to 9$ доказана. □

Пример 2.18. Подстановка g множества X, где $|X| = 2l$ и $l > 2$, с цикловой структурой, заданной наборами $L = (1, l-1, l)$ и $K = (1, 1, 1)$, не является нормально неподвижной.

Для этой подстановки $\bar{L} = (l-1, L)$. Используя следствие 1,а) утверждения 2.10, вычисляем:

$$\lceil L \rceil_1 = \{1\} \cup \lceil \bar{L} \rceil = (1, l-1, l, l \cdot (l-1)).$$

Используя следствие 1,б) утверждения 2.10, получаем:

$$N_{I(g)} = \{1, l, l+1, 2l\}^* = \{1, l, l+1, 2l\}.$$

По предложению 5 утверждения 2.12 достаточно проверить включения $\eta_g(t, \tau) \in N$ ($\eta_g(t, \tau) \in N^{[p]}$) для всех $\tau, t \in \lceil L \rceil_1$ таких, что τ / t.

Исходя из вычисленных множеств $\lceil L \rceil_1$ и $N_{I(g)}$ получаем, что

$$\eta_g(l-1, 1) = l, \eta_g(l, 1) = l+1, \eta_g(l \cdot (l-1), l-1) = 2, \eta_g(l \cdot (l-1), l) = \frac{2l}{l+1},$$

где $\frac{2l}{l+1} \notin N$ при любом $l > 2$. ◇

При распознавании подстановок, не являющихся нормально (p-нормально) неподвижными, может быть использовано следующее утверждение.

Утверждение 2.13. *Если хотя бы одно из чисел* $\frac{|X|}{k_1}$, $\frac{|X|}{|I_g|(t)}$, $\frac{|I_g|(t)}{k_1}$ *) не принадлежит* N *(не принадлежит* $N^{[p]}$*),* $t = 1, \ldots, n$, *то* $g \notin N^{[\nu]}$ *(*$g \notin N^{[p\nu]}$*).*

Доказательство *. При $t=n$ и $\tau=1,\ldots,n$ число (τ, n) делит число (t, n). Поэтому из предложения 2 утверждения 2.12 следует, что $\eta_g(n, \tau)\in N$, если $g\in\Lambda^{[\nu]}$. Так как $|I_g|(n)=|X|$, то из равенства (2.19) имеем:

$$\eta_g(n, \tau)=\frac{|X|}{|I_g|(\tau)}.$$

При $\tau=1$ и $t=1,\ldots,n$ число (τ, n) делит число (t, n). Поэтому из предложения 2 утверждения 2.12 следует, что $\eta_g(t, 1)\in N$, если $g\in\Lambda^{[\nu]}$. Так как $|I(g)|=k_1$, то из равенства (2.19) имеем: $\eta_g(t, 1)=\frac{|I_g|(t)}{k_1}$.

Отсюда следует, в частности, что если $g\in\Lambda^{[\nu]}$, то $\eta_g(n, 1)\in N$, где $\eta_g(n, 1)=\frac{|X|}{k_1}$. □

Следствие. *Если $g\in\Lambda^{[\nu]}$ и $|X|=p^r$, где p — простое, r — натуральное, то $g\in\Lambda^{[p\nu]}$ и $|I(g^t)|\in N^{[p]}$, $t=1,\ldots,n$.*

Доказательство. По утверждению 2.13 $|I_g|(t)$ делит $|X|$, $t=1,\ldots,n$. Поэтому если $|X|=p^r$, то $|I_g|(t)\in N^{[p]}$. □

Пример 2.19. Определим, является ли нормально (p-нормально) неподвижной подстановка g степени 84, у которой цикловая структура определяется числами:

$$C(g)=(1^7, 6, 15, 21, 35).$$

Для этой подстановки $|X|=84$, $\operatorname{ord} g=210$.

В примере 2.14 посчитано (табл. 2.1), что $|I(g^{42})|=34$. Так как $|I(g^{42})|$ не делит $|X|$, то по утверждению 2.13 подстановка $g\notin\Lambda^{[\nu]}$ и $g\notin\Lambda^{[p\nu]}$ при любом натуральном p. ◇

2.4.3. Исследование в группах подстановок наследственных признаков, связанных с нормальной и p-нормальной неподвижностью подстановок. Из примера 2.17,а) следует, что всякая группа подстановок G имеет $\Lambda^{[\nu]}$-признак ($\Lambda^{[p\nu]}$-признак). Убедимся, что этот признак в группе G является наследственным, и определим множество $(\Lambda^{[\nu]}, g)$-пороговых ($(\Lambda^{[p\nu]}, g)$-пороговых) чисел для произвольной подстановки $g\in G$.

Утверждение 2.14. *Пусть каждое из последующих чисел набора (n, τ'', τ', τ) делит предыдущее число, где $n\neq\tau$. Тогда:*

а) *если $\tau\in D^{\nu}(g)$ $(\tau\in D^{p\nu}(g))$, то $\tau'\in D^{\nu}(g)$ и $\eta_g(\tau'', \tau')\in N$ $(\tau'\in D^{p\nu}(g)$ и $\eta_g(\tau'', \tau')\in N^{[p]})$;*

б) *если $\tau'', \tau'\in\lceil L\rceil_1$ и $\tau\in L^{\nu}(g)$ $(\tau\in L^{p\nu}(g))$, то $\tau'\in L^{\nu}(g)$ и $\eta_g(\tau'', \tau')\in N$ $(\tau'\in L^{p\nu}(g)$ и $\eta_g(\tau'', \tau')\in N^{[p]})$.*

Доказательство *. Рассмотрим любой путь $w\in W_D(n, \tau)$ $(w\in W_L(n, \tau))$, проходящий через вершину τ', и любой путь $w'\in W_D(n, \tau)$ $(w'\in W_L(n, \tau))$, проходящий последовательно через вершины τ'' и τ'; такие пути имеются, так как по условию каждая из последующих вершин набора (n, τ', τ'', τ) делит предыдущую вершину.

Путь w можно составить из путей w_{12} и w_3, а путь w' можно составить из трёх путей w_1, w_2 и w_3, где w_{12} (w_1, w_2, w_3) есть произвольный путь из n в τ' (из n в τ'', из τ'' в τ', из τ' в τ).

Если $\tau'=n$, то по определению 2.19 вершина τ' является нормальной как в графе $\Gamma_D(|I_g|)$, так и в графе $\Gamma_L(|I_g|)$.

Пусть $\tau'\neq n$. Так как $\tau\in D^{\nu}(g)$ $(\tau\in L^{\nu}(g))$, то по определению 2.19 любой путь $w\in W_D(n, \tau)$ $(w\in W_L(n, \tau))$ состоит из нормальных дуг, в том числе, пути w и w'.

Отсюда следует, во-первых, что путь w_{12} в графе $\Gamma_D(|I_g|)$ (в графе $\Gamma_L(|I_g|)$) тоже составлен из нормальных дуг. Значит, по определению 2.19 вершина τ' является нормальной как в графе $\Gamma_D(|I_g|)$, так и в графе $\Gamma_L(|I_g|)$.

Во-вторых, если $\tau'' \neq \tau'$, то путь w_2 в графе $\Gamma_D(|I_g|)$ (в графе $\Gamma_L(|I_g|)$) тоже составлен тоже из нормальных дуг. Значит, по следствию 2 утверждения 2.11 $\eta_g(\tau'', \tau') \in N$.

Если $\tau'' = \tau'$, то $\eta_g(\tau'', \tau') \in N$, так как $\eta_g(\tau', \tau') = 1$. □

Следствие 1. а) *Если* $M \subseteq D(n)$ *и* $\operatorname{dom} M$ *не содержит нормальных (*p*-нормальных) вершин графа* $\Gamma_D(|I_g|)$, *то* $M \cap D^{\nu}(g) = \varnothing$ $(M \cap D^{p\nu}(g) = \varnothing)$.

б) *Если* $M \subseteq \lceil L \rceil_1$ *и* $\operatorname{dom} M$ *не содержит нормальных (*p*-нормальных) вершин графа* $\Gamma_L(|I_g|)$, *то* $M \cap L^{\nu}(g) = \varnothing$ $(M \cap L^{p\nu}(g) = \varnothing)$.

Доказательство *. Любая вершина τ из M либо принадлежит $\operatorname{dom} M$, либо делит некоторую вершину τ' из $\operatorname{dom} M$.

В первом случае $\tau \notin D^{\nu}(g)$ $(\tau \notin L^{\nu}(g))$ по условию.

Во втором случае, если $\tau \in D^{\nu}(g)$ $(\tau \in L^{\nu}(g))$, то по утверждению 2.14 $\tau' \in D^{\nu}(g)$ $(\tau' \in L^{\nu}(g))$, что противоречит условию.

Значит, $M \cap D^{\nu}(g) = \varnothing$ $(M \cap L^{\nu}(g) = \varnothing)$. □

Из утверждения 2.14 и его следствия 1 непосредственно получаем.

Следствие 2. а) *Любой путь* $w \in W_D(n, \tau)$ *либо проходит только через нормальные (*p*-нормальные) вершины, если* $\tau \in D^{\nu}(g)$ *(если* $\tau \in D^{p\nu}(g)$*), либо разбивается на два отрезка соответственно нормальных и не нормальных (*p*-нормальных и не* p*-нормальных) вершин, если* $\tau \notin D^{\nu}(g)$ $(\tau \notin D^{p\nu}(g))$.

б) *Любой путь* $w \in W_L(n, \tau)$ *либо проходит только через нормальные (*p*-нормальные) вершины, если* $\tau \in L^{\nu}(g)$ *(если* $\tau \in L^{p\nu}(g)$*), либо разбивается на два отрезка соответственно нормальных и не нормальных (*p*-нормальных и не* p*-нормальных) вершин, если* $\tau \notin L^{\nu}(g)$ $(\tau \notin L^{p\nu}(g))$. ◇

Замечание. Из утверждения 2.14,а) следует, что множество подстановок $\{g^{\tau}\colon \tau \in D^{\nu}(g)\}$ (множество подстановок $\{g^{\tau}\colon \tau \in D^{p\nu}(g)\}$) является наследственным. Вместе с тем, из утверждения 2.14,б) не следует, что множество подстановок $\{g^{\tau}\colon \tau \in L^{\nu}(g)\}$ (множество подстановок $\{g^{\tau}\colon \tau \in L^{p\nu}(g)\}$) является наследственным, так как из включения $\tau \in \lceil L \rceil_1$ не следует, что всякое число, кратное числу τ, принадлежит $\lceil L \rceil_1$.

Теорема 2.10. *Подстановка* $g^{\tau} \in \Lambda^{[\nu]}$ $(g^{\tau} \in \Lambda^{[p\nu]})$ *при* $\tau \in D(n)$ *тогда и только тогда, когда* $\tau \in D^{\nu}(g)$ $(\tau \in D^{p\nu}(g))$.

Доказательство *. Обозначим $h = g^{\tau}$. Если $\tau \in D^{\nu}(g)$, то τ / n и $\operatorname{ord} h = \frac{n}{\tau}$.

Пусть $t, \mu \in D\left(\frac{n}{\tau}\right)$ и μ / t. Тогда $\tau \cdot \mu$ делит $\tau \cdot t$, при этом $\tau \cdot t, \tau \cdot \mu \in D(n)$. Так как τ делит $\tau \cdot \mu$, то по утверждению 2.14,а) $\tau \cdot t, \tau \cdot \mu \in D^{\nu}(g)$ и выполнено включение $\eta_g(\tau \cdot t, \tau \cdot \mu) \in N$. При сделанных обозначениях это включение равносильно включению $\eta_h(t, \mu) \in N$.

В силу произвольности рассмотренных делителей t и μ числа $\frac{n}{\tau}$ для подстановки H выполнено предложение 4 утверждения 2.12, т. е. $h \in \Lambda^{[\nu]}$. Значит, $g^{\tau} \in \Lambda^{[\nu]}$.

Докажем в обратную сторону. Пусть $\tau \in D(n) \setminus D^{\nu}(g)$. Тогда по определению 2.19 $\tau \neq n$ и имеется путь $(\tau_0, \tau_1, \ldots, \tau_k) \in W_D(n, \tau)$, содержащий дугу, не являющуюся нормальной. Значит, $\eta_g(\tau_{j-1}, \tau_j) \notin N$ при некотором $j \in \{1, \ldots, k\}$.

Так как τ/τ_{j-1} и τ/τ_j, где $\tau_{j-1}, \tau_j \in D(n)$, то $\frac{\tau_{j-1}}{\tau}, \frac{\tau_j}{\tau} \in D\left(\frac{n}{\tau}\right)$. Следовательно, при сделанных обозначениях $\eta_h\left(\frac{\tau_{j-1}}{\tau}, \frac{\tau_j}{\tau}\right) \notin N$, где $\frac{\tau_j}{\tau}$ делит $\frac{\tau_{j-1}}{\tau}$, так как τ_j/τ_{j-1}. Значит, для подстановки h предложение 4 утверждения 2.12 не выполнено, и $g^\tau \notin \mathfrak{N}^{[\nu]}$. □

Обозначим через $\psi_\Lambda^{[\nu]}$ (через $\psi_\Lambda^{[p\nu]}$) характеристическую функцию $\mathfrak{N}^{[\nu]}$-признака ($\mathfrak{N}^{[p\nu]}$-признака) в группе подстановок $\Phi(X)$ и через $\psi_{\Lambda,g}^{[\nu]}(t)$ (через $\psi_{\Lambda,g}^{[p\nu]}(t)$) обозначим g-подфункцию этой характеристической функции.

Следствие 1. *Всякая подгруппа G группы подстановок $\Phi(X)$ имеет наследственный $\mathfrak{N}^{[\nu]}$-признак ($\mathfrak{N}^{[p\nu]}$-признак), при этом*

$$\Pi(\mathfrak{N}^{[\nu]}, g) = \operatorname{prm} D^\nu(g)$$

$$(\Pi(\mathfrak{N}^{[p\nu]}, g) = \operatorname{prm} D^{p\nu}(g)).$$

Доказательство *. Из утверждения 2.2 следует, что цикловая структура подстановки g однозначно определяет множество цикловых структур всех подстановок циклической группы $\langle g\rangle$. Следовательно, цикловая структура подстановки g однозначно определяет наличие или отсутствие у подстановки g свойства нормальной неподвижности. Значит, функция $\psi_\Lambda^{[\nu]}$ является характеристикой цикловых структур подстановок группы $\Phi(X)$.

Вместе с тем, если $g \in \mathfrak{N}^{[\nu]}$ то по предложению 7 утверждения 2.12 $D^\nu(g) = D(n)$, и, следовательно, по теореме 2.10 $g^\tau \in \mathfrak{N}^{[\nu]}$ при любом $\tau \in D(n)$. Отсюда по следствию утверждения 2.8 получаем, что $\mathfrak{N}^{[\nu]}$-признак в группе G является наследственным.

Так как по теореме 2.10 множество $\{t \in D(n)\colon g^t \in \mathfrak{N}^{[\nu]}\}$ совпадает со множеством $D^\nu(g)$, то по теореме 1.5,в) получаем выражение для множества $\Pi(\mathfrak{N}^{[\nu]}, g)$. □

Следствие 2. $\operatorname{pok}_g \mathfrak{N}^{[\nu]} = \min D^\nu(g)$ $(\operatorname{pok}_g \mathfrak{N}^{[p\nu]} = \min D^{p\nu}(g))$.

Доказательство *. По следствию 1 теоремы 1.5 $\operatorname{pok}_g \mathfrak{N}^{[\nu]}$ есть наименьшее из чисел множества $\operatorname{prm} D^\nu(g)$, это число совпадает с наименьшим из чисел множества $D^\nu(g)$. □

Следствие 3. *$\mathfrak{N}^{[\nu]}$-признак ($\mathfrak{N}^{[p\nu]}$-признак) тривиален в циклической группе $\langle g\rangle$ тогда и только тогда, когда в графе $\Gamma_D(|I_g|)$ все дуги, инцидентные вершине n, не являются нормальными (p-нормальными).*

Доказательство *. Так как $e \in \mathfrak{N}^{[\nu]}$, то $\psi_{\Lambda,g}^{[\nu]}(n) = 1$. Значит, по следствию 2 теоремы 1.8 $\mathfrak{N}^{[\nu]}$-признак тривиален в группе $\langle g\rangle$, если $\psi_{\Lambda,g}^{[\nu]}(t) = 0$ для любого коатома t решётки $D(n)$.

Последнее условие по теореме 2.10 равносильно тому, что каждый коатом t решётки $D(n)$ не является нормальной вершиной графа $\Gamma_D(|I_g|)$. Из определения 2.19 следует, что каждый коатом t решётки $D(n)$ не является нормальной вершиной графа $\Gamma_D(|I_g|)$ тогда и только тогда, когда не являются нормальными все дуги, инцидентные вершине n. □

Следствие 4. *$\mathfrak{N}^{[\nu]}$-признак ($\mathfrak{N}^{[p\nu]}$-признак) в циклической группе $\langle g\rangle$ является квазиполным тогда и только тогда, когда множество* $\operatorname{prm} D^\nu(g)$ *(множество* $\operatorname{prm} D^{p\nu}(g)$*) совпадает со множеством атомов решётки $D(n)$.*

Доказательство *. Используя выражение для множества $\Pi(\mathfrak{N}^{[\nu]}, g)$, полученное в следствии 1 теоремы 2.10, получаем по утверждению 1.11,б) критерий квазиполноты $\mathfrak{N}^{[\nu]}$-признака в циклической группе $\langle g\rangle$. □

2.4.4. О сложности определения в циклической группе подмножества нормально неподвижных подстановок. Вершины графа $\Gamma_D(|I_g|)$ (графа $\Gamma_L(|I_g|)$) можно разбить на ярусы (занумеруем их числами от 0 до r_D (до r_L)) последующему правилу: нулевой ярус состоит из вершины n; r_D-й ярус (r_L-й ярус) состоит из вершины 1; к i-му ярусу отнесем все вершины, которые покрываются хотя бы одной вершиной $(i-1)$-го яруса, $i=1, 2, \ldots, r_D$ $(i=1, 2, \ldots, r_L)$.

Из определения 2.19 вытекает следующий критерий нормальности (p-нормальности) вершины τ графа $\Gamma_D(|I_g|)$ или графа $\Gamma_L(|I_g|)$.

Утверждение 2.15. *Вершина τ i-го яруса графа $\Gamma_D(|I_g|)$ или графа $\Gamma_L(|I_g|)$ является нормальной (p-нормальной) тогда и только тогда, когда нормальны (p-нормальны) все дуги, входящие в вершину τ, и нормальны (p-нормальны) все вершины $(i-1)$-го яруса соответственно графа $\Gamma_D(|I_g|)$ или графа $\Gamma_L(|I_g|)$, покрывающие вершину τ, $i=1, 2, \ldots, r_D$ $(i=1, 2, \ldots, r_L)$.* $\diamondsuit$

Из следствия 1 теоремы 2.10 следует, что определение (Λ, g)-пороговых ($(\Lambda^{[p]}, g)$-пороговых) чисел, и, следовательно, порождающего элемента подгруппы $\Lambda^{[\nu]}$-тривиальности ($\Lambda^{[p\nu]}$-тривиальности) группы $\langle g\rangle$, связано с вычислениями на графе $\Gamma_D(|I_g|)$.

Опишем основанный на утверждении 2.15 способ вычисления множества $\Pi(\Lambda^{[\nu]}, g)$ (множества $\Pi(\Lambda^{[p\nu]}, g)$), а заодно и множества $\operatorname{prm} L^{\nu}(g)$ ($\operatorname{prm} L^{p\nu}(g)$).

В качестве исходных данных алгоритм использует вершины и дуги графа $\Gamma_D(|I_g|)$ (графа $\Gamma_L(|I_g|)$).

Алгоритм 2.1.

1. Определение множества $D^{\nu}(g)$ (множества $L^{\nu}(g)$).

Последовательно просматриваем ярусы графа $\Gamma_D(|I_g|)$ (графа $\Gamma_L(|I_g|)$), начиная с 1-го, и разделяем множество вершин данного яруса на нормальные и не нормальные вершины, руководствуясь правилами:

1) если вершина покрывается хотя бы одной из ненормальных вершин предыдущего яруса, то она не нормальна;

2) если вершина покрывается только нормальными вершинами предыдущего яруса, то она является нормальной тогда и только тогда, когда нормальны все дуги, входящие в данную вершину.

2. Определение множества $\operatorname{prm} D^{\nu}(g)$ (множества $\operatorname{prm} L^{\nu}(g)$).

Просматриваем ярусы графа $\Gamma_D(|I_g|)$ (графа $\Gamma_L(|I_g|)$) в обратном порядке, начиная с яруса с наибольшим номером μ_D (номером μ_L), который содержит непустое множество нормальных вершин. При этом руководствуемся правилами:

1) все нормальные вершины μ_D-го яруса (μ_L-го яруса) принадлежат множеству $\operatorname{prm} D^{\nu}(g)$ (множеству $\operatorname{prm} L^{\nu}(g)$)

2) если $\mu_D > 0$ ($\mu_L > 0$), то нормальная вершина $(i-1)$-го яруса принадлежит множеству $\operatorname{prm} D^{\nu}(g)$ (множеству $\operatorname{prm} L^{\nu}(g)$) тогда и только тогда, когда она не покрывает ни одну нормальную вершину i-го яруса, $i=\mu_D, \mu_D-1, \ldots, 2$ $(i=\mu_L, \mu_L-1, \ldots, 2)$. $\square$

Корректность данного алгоритма следует из утверждения 2.15 и теоремы 2.10.

Алгоритм 2.1 требует в худшем случае двукратного просмотра всех дуг графа $\Gamma_D(|I_g|)$ (графа $\Gamma_L(|I_g|)$), поэтому сложность вычислений имеет порядок числа дуг графа.

Вместе с тем, возникает вопрос, нельзя ли вычислительно проще определить множество $\Pi(\Lambda^{[\nu]}, g)$ (множество $\Pi(\Lambda^{[p\nu]}, g)$), используя вычисления

на графе $\Gamma_L(|I_g|)$, которые, как можно ожидать, являются менее сложными в силу того, что $\lceil L \rceil_1 \subseteq D(n)$?

В случае $g \in \Lambda^{[\nu]}$ ($g \in \Lambda^{[p\nu]}$) положительный ответ следует из утверждения 2.12. Например, согласно предложению 9 для распознавания нормальной (p-нормальной) неподвижности подстановки g достаточно проверить нормальность (p-нормальность) всех дуг графа $\Gamma_L(|I_g|)$.

Для исследования этого вопроса в случае, когда $g \notin \Lambda^{[\nu]}$ ($g \notin \Lambda^{[p\nu]}$) установим связи между некоторыми характеристиками графов $\Gamma_D(|I_g|)$ и $\Gamma_L(|I_g|)$. Далее считаем, что $g \notin \Lambda^{[\nu]}$ ($g \notin \Lambda^{[p\nu]}$).

Утверждение 2.16. *Включение* $\tau \in \lceil L \rceil_1 \cap D^\nu(g)$ ($\tau \in \lceil L \rceil_1 \cap D^{p\nu}(g)$) *верно тогда и только тогда, когда верно включение* $\tau \in L^\nu(g)$ ($\tau \in L^{p\nu}(g)$).

Доказательство *. Рассмотрим путь $(t_0, t_1, \ldots, t_l) \in W_L(n, \tau)$ и путь $w = (\tau_0, \tau_1, \ldots, \tau_k)$, где $w \in W_D(n, \tau)$ и w проходит последовательно через вершины $t_0, t_1, \ldots, t_l$. Такой путь w имеется, так как $\lceil L \rceil_1 \subseteq D(n)$ и, следовательно, каждая из вершин $t_0, t_1, \ldots, t_l$ принадлежит $D(n)$.

Пусть $\tau \in \lceil L \rceil_1 \cap D^\nu(g)$. Так как каждая из последующих вершин пути $(t_0, t_1, \ldots, t_l)$ делит предыдущую вершину, то $\eta_g(t_{i-1}, t_i) \in N$ по утверждению 2.14,а), $i = 1, \ldots, l$. Значит, путь $(t_0, t_1, \ldots, t_l)$ составлен из нормальных дуг графа $\Gamma_L(|I_g|)$. В силу произвольности рассмотренного пути $(t_0, t_1, \ldots, t_l)$ из $W_L(n, \tau)$ получаем по определению 2.19, что $\tau \in L^\nu(g)$.

Пусть $\tau \in \lceil L \rceil_1 \setminus D^\nu(g)$. Тогда $\tau \in D(n) \setminus D^\nu(g)$ и по определению 2.19 некоторый путь w из $W_D(n, \tau)$ не является нормальным. Отсюда, по следствию 1 утверждения 2.11 не является нормальным и набор $\bar{\upsilon}(w, L)$. Значит, если $w = (\tau_0, \tau_1, \ldots, \tau_k)$, то $\eta_g(\upsilon(\tau_{i-1}, L), \upsilon(\tau_i, L)) \notin N$ при некотором $i \in \{1, \ldots, k\}$.

Предположим, что $\tau \in L^\nu(g)$. Тогда любой путь из $W_L(n, \tau)$ состоит из нормальных дуг, в частности, путь u, проходящий последовательно, через вершины $\upsilon(\tau_{i-1}, L)$ и $\upsilon(\tau_i, L)$. Такой путь имеется, так как каждое из последующих чисел набора $(n, \upsilon(\tau_{i-1}, L), \upsilon(\tau_i, L), \tau)$ делит предыдущее число.

Действительно, $\upsilon(\tau_{i-1}, L)$ делит n, так как любое число из $\lceil L \rceil_1$ делит n. Число $\upsilon(\tau_i, L)$ делит $\upsilon(\tau_{i-1}, L)$ и число $\upsilon(\tau, L)$ делит $\upsilon(\tau_i, L)$ по свойству нормального эпиморфизма $\upsilon(t, L)$ (см. утверждение 2.10), так как соответственно τ_i / τ_{i-1} и τ / τ_i. При этом по утверждению 2.10,б) $\upsilon(\tau, L) = \tau$, так как $\tau \in \lceil L \rceil_1$.

Таким образом, дуга $(\upsilon(\tau_{i-1}, L), \upsilon(\tau_i, L))$ пути u является нормальной. Имеем противоречие. Следовательно, $\tau \in \lceil L \rceil_1 \setminus L^\nu(g)$. □

Обозначим через $Z(g)$ (через $Z^p(g)$) множество всех делителей числа n, которые не кратны ни одному из чисел множества $L^\nu(g)$ (множества $L^{p\nu}(g)$) и одновременно не делят ни одно из чисел множества $\lceil L \rceil_1 \setminus L^\nu(g)$ (множества $\lceil L \rceil_1 \setminus L^{p\nu}(g)$). Положим также

$$Z^\nu(g) = Z(g) \cap D^\nu(g), \quad Z^{p\nu}(g) = Z^p(g) \cap D^{p\nu}(g).$$

Теорема 2.11. *Если* $g \notin \Lambda^{[\nu]}$ ($g \notin \Lambda^{[p\nu]}$), *то*

$$\Pi(\Lambda^{[\nu]}, g) = \mathrm{prm}(L^\nu(g) \cup Z^\nu(g))$$
$$(\Pi(\Lambda^{[p\nu]}, g) = \mathrm{prm}(L^{p\nu}(g) \cup Z^{p\nu}(g)).$$

Доказательство *. Если $g \notin \Lambda^{[\nu]}$, то в силу предложения 10 утверждения 2.12 $\lceil L \rceil_1 \setminus L^\nu(g) \neq \varnothing$, поэтому множество вершин графа $\Gamma_D(|I_g|)$ разбивается на 3 подмножества:

1) непустое множество $R_1(g)$ всех чисел, которые делят хотя бы одно из чисел множества $\lceil L\rceil_1 \setminus L^\nu(g)$,

2) непустое множество $R_2(g)$ всех чисел, которые кратны хотя бы одному из чисел множества $L^\nu(g)$,

3) множество остальных чисел, которое обозначено $Z(g)$.

По утверждению 2.16

$$\lceil L\rceil_1 \cap D^\nu(g) = L^\nu(g), \quad \lceil L\rceil_1 \cap (D(n) \setminus D^\nu(g)) = \lceil L\rceil_1 \setminus L^\nu(g).$$

Поэтому $D^\nu(g) \cap (\lceil L\rceil_1 \setminus L^\nu(g)) = \varnothing$. Отсюда по утверждению 2.14 получаем, что $D^\nu(g) \cap R_1(g) = \varnothing$. Следовательно,

$$D^\nu(g) \subseteq R_2(g) \cup Z(g).$$

Так как множество $D^\nu(g)$ содержит только нормальные вершины графа $\Gamma_D(|I_g|)$, то

$$D^\nu(g) \subseteq R_2(g) \cup Z^\nu(g).$$

Вместе с тем, выполнено и обратное включение, так как $Z^\nu(g) \subseteq D^\nu(g)$ по определению множества $Z^\nu(g)$ и по утверждению 2.14 $R_2(g) \subseteq D^\nu(g)$. Следовательно,

$$D^\nu(g) = R_2(g) \cup Z^\nu(g).$$

Отсюда получаем, что

$$\operatorname{prm} D^\nu(g) = \operatorname{prm}(R_2(g) \cup Z^\nu(g)).$$

Каждое из чисел множества $R_2(g) \setminus L^\nu(g)$ кратно некоторому числу множества $L^\nu(g)$, поэтому

$$\operatorname{prm}(R_2(g) \cup Z^\nu(g)) = \operatorname{prm}(L^\nu(g) \cup Z^\nu(g)),$$

следовательно, равенство для множества $\operatorname{prm} D^\nu(g)$ принимает вид:

$$\operatorname{prm} D^\nu(g) = \operatorname{prm}(L^\nu(g) \cup Z^\nu(g)).$$

Отсюда по следствию 1 теоремы 2.10 получаем теорему 2.11. □

Опишем теперь алгоритм определения множества $\Pi(\Lambda^{[\nu]}, g)$ (множества $\Pi(\Lambda^{[p^\nu]}, g)$), использующий в качестве исходных данных вершины и дуги графов $\Gamma_L(|I_g|)$ и $\Gamma_D(|I_g|)$.

Обозначим через $L_i^\nu(g)$ (через $Z_i(g)$) множество всех вершин из $L^\nu(g)$ (из $Z(g)$), принадлежащих i-му ярусу графа $\Gamma_D(|I_g|)$, и через A_i и B_i — множества всех соответственно нормальных и не нормальных вершин множества $Z_i(g)$, $i = 1, 2, \ldots, r_D$.

Пусть μ и δ — соответственно наименьший и наибольший номера ярусов графа $\Gamma_D(|I_g|)$, которые содержат хотя бы одну вершину множества $Z(g)$, $0 < \mu \leqslant \delta$. Тогда $A_{\mu-1} = B_{\mu-1} = \varnothing$ и

$$Z^\nu(g) = \bigcup_{i=\mu}^{\delta} A_i \tag{2.24}$$

Алгоритм 2.2*.

1. По графу $\Gamma_L(|I_g|)$ определяем с помощью п. 1 алгоритма 2.1 множество $L^\nu(g)$ и определяем множества $L_i^\nu(g)$, $i = 1, 2, \ldots, r_D$.

2. Определяем множество $Z(g)$ и множества $Z_i(g)$, $i = 1, 2, \ldots, r_D$.

3. Разбиваем множество $Z_i(g)$ на подмножества A_i и B_i, $i = \mu, \mu + 1, \ldots, \delta$, руководствуясь правилами:

1) если вершина τ из $Z_i(g)$ покрывается хотя бы одной из вершин множества B_{i-1}, то $\tau \in B_i$;

2) если вершина τ из $Z_i(g)$ не покрывается ни одной из вершин множества B_{i-1}, то $\tau \in A_i$ тогда и только тогда, когда является нормальной упорядоченная пара $(v(t, L), v(\tau, L))$ вершин множества $\lceil L \rceil_1$ при любой вершине $t \in A_{i-1} \cup L^{\nu}_{i-1}(g)$ такой, что t покрывает вершину τ.

4. Определяем множество $\mathrm{prm}(L^{\nu}(g) \cup Z^{\nu}(g))$, используя разбиение множества $L^{\nu}(g) \cup Z^{\nu}(g)$ по ярусам (см. п. 2 алгоритма 2.1). □

Корректность алгоритма 2.2 следует из утверждений 2.15, 2.16 и теорем 2.10, 2.11.

Пример 2.20. Определим множество $\Pi(\Lambda^{[\nu]}, g)$ для подстановки g степени 84, имеющей цикловую структуру $C(g) = (1^7, 6, 15, 21, 35)$.

Подстановка g не является нормально неподвижной (см. пример 2.19).

Порядок подстановки g равен 210. В примере 2.14 посчитано:

$$L = (1, 6, 15, 21, 35),$$
$$\lceil L \rceil_1 = \{1, 6, 15, 21, 35, 30, 42, 105, 210\}.$$

Множество всех делителей числа 210 есть

$$D(210) = \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}.$$

Расположим по ярусам вершины графов $\Gamma_L(|I_g|)$ и $\Gamma_D(|I_g|)$ (табл. 2.2 и 2.3) и укажем для каждой вершины t через знак / величину $|I_g|(t)$ из табл. 2.1 примера 2.14.

Таблица 2.2

Характеристики $\lceil L \rceil_1$-диаграммы функции $|I_g|(t)$

Номер яруса	вершина $t/\lvert I_g\rvert(t)$			
0	210/84			
1	105/78	42/34	30/28	
2	35/42	21/28	15/22	6/13
3	1/7			

Таблица 2.3

Характеристики D-диаграммы функции $|I_g|(t)$

Номер яруса	вершина $t/\lvert I_g\rvert(t)$					
0	210/84					
1	105/78	70/42	42/34	30/28		
2	35/42	21/28	15/22	14/7	10/7	6/13
3	7/7	5/7	3/7	2/7		
4	1/7					

Применяя алгоритм 2.1, определяем по табл. 2.2:

$$L^{\nu}(g) = \{210, 30\}.$$

Значит,

$$\operatorname{prm} L^{\nu}(g) = \{30\},$$
$$\lceil L \rceil_1 \setminus L^{\nu}(g) = \{1, 6, 15, 21, 35, 42, 105\}.$$

Отсюда определяем по табл. 2.3:

$$Z(g) = \{70, 10\} = Z^{\nu}(g).$$

Следовательно, по теореме 2.11

$$\Pi(\mathfrak{N}^{\nu}, g) = \operatorname{prm} D^{\nu}(g) = \operatorname{prm}(L^{\nu}(g) \cup Z^{\nu}(g)) = \{10\}.$$

Таким образом, циклическая группа $\langle g \rangle$ имеет подгруппу $\langle g^{10} \rangle$ нормально неподвижных подстановок.

Из приведённых расчётов следует также, что циклическая группа $\langle g \rangle$ имеет подгруппу $\langle g^{30} \rangle$ 3-нормально неподвижных подстановок и подгруппу $\langle g^{70} \rangle$ 2-нормально неподвижных подстановок. ◇

Укажем класс подстановок g, для которых определение множества $\Pi(\mathfrak{N}^{\nu}, g)$ (множества $\Pi(\mathfrak{N}^{p\nu}, g)$) не требует трудоёмких вычислений.

У т в е р ж д е н и е 2.17. *Пусть $g \notin \mathfrak{N}^{\nu}$ и подстановка g состоит из циклов длины $l_i = q^{n_i}$, $i = 1, \ldots, m$, где q — простое и $0 \leqslant n_1 < \ldots < n_m$. Тогда единственное $(\mathfrak{N}^{\nu}, g)$-пороговое ($(\mathfrak{N}^{p\nu}, g)$-пороговое) число t равно:*

$$t = \begin{cases} l_m, & \text{если } \eta_g(l_m, l_{m-1}) \notin N; \\ l_j, & \text{если } \eta_g(l_i, l_{i-1}) \in N,\ i = j+1, \ldots, m,\ \eta_g(l_j, l_{j-1}) \notin N,\ 1 < j < m; \\ l_1, & \text{если } \eta_g(l_i, l_{i-1}) \in N,\ i = 2, \ldots, m. \end{cases}$$

Д о к а з а т е л ь с т в о. При данных условиях множество $D(n)$ (множество $\lceil L \rceil_1$) есть цепь длины n (длины m), $n = l_m$ и

$$\lceil L \rceil_1 = \begin{cases} L \cup \{1\}, & n_1 > 0 \\ L, & n_1 = 0. \end{cases}$$

В графе $\Gamma_L(|I_g|)$ имеется единственный путь w_j из n в l_j, состоящий из дуг $(l_m, l_{m-1}), \ldots, (l_{j+1}, l_j)$, $j = 0, 1, \ldots, m-1$, где $l_0 = 1$.

Из определения 2.19 следует, что вершина l_j графа $\Gamma_L(|I_g|)$ является нормальной тогда и только тогда, когда нормальны все дуги пути w_j.

Отсюда l_j есть число из множества $\operatorname{prm} L^{\nu}(g)$, притом единственное, тогда и только тогда, когда являются нормальными все дуги пути w_j и дуга (l_j, l_{j-1}) не является нормальной, если $j > 0$. Заметим, что в случае $n_1 > 0$ дуга (l_1, l_0) не является нормальной, так как $g \notin \mathfrak{N}^{\nu}$ и, значит, $|I_g|(1) = 0$. Следовательно, множество $\operatorname{prm} L^{\nu}(g)$ состоит из числа t, определённого утверждением 2.17.

Пусть $\operatorname{prm} L^{\nu}(g) = \{l_j\}$ для некоторого $j \in \{1, \ldots, m\}$. Докажем, что $\Pi(\mathfrak{N}^{\nu}, g) = \{l_j\}$.

Если $l_1 = 1$ (т. е. $n_1 = 0$), то $j > 1$, в противном случае по предложению 11 утверждения 2.12 подстановка $g \in \mathfrak{N}^{\nu}$, что противоречит условиям утверждения.

Пусть $j=1$ и $l_1>1$ (т. е. $n_1>0$). Тогда $\lceil L\rceil_1 \setminus L^\nu(g)=\{1\}$ и множество $Z(g)$ состоит из чисел q^i, где $0<i<n_1$. Следовательно, по утверждению 2.10,в)

$$|I_g|(q^i)=|I_g|(\upsilon(q^i, L))=|I_g|(1)=0,$$

откуда получаем, что $\eta_g(l_1, q^i)=0$ для чисел i, удовлетворяющих неравенствам $0<i<n_1$. Следовательно, в этом случае $Z^\nu(g)=\varnothing$.

Пусть $j>1$, тогда $\lceil L\rceil_1 \setminus L^\nu(g)=\{1, l_1, \ldots, l_{j-1}\}$. Значит:

1) если $n_j-n_{j-1}>1$, то множество $Z(g)$ состоит из чисел q^i, где $n_{j-1}<i<n_j$;

2) если $n_j-n_{j-1}=1$, то $Z(g)=\varnothing$.

Пусть $n_j-n_{j-1}>1$, тогда по утверждению 2.10,в)

$$|I_g|(q^i)=|I_g|(\upsilon(q^i, L))=|I_g|(l_{j-1}),$$

откуда получаем, что $\eta_g(l_j, q^i)=\eta_g(l_j, l_{j-1})$ для чисел i, удовлетворяющих неравенствам $0\leqslant i<n_1$. Следовательно, $\eta_g(l_j, q^i)\notin N$, так как $\eta_g(l_j, l_{j-1})\notin N$.

Значит, в любом случае $Z^\nu(g)=\varnothing$, отсюда по теореме 2.11 получаем, что

$$\Pi(\mathfrak{N}^{[\nu]}, g)=\mathrm{prm}(L^\nu(g))=\{l_j\}.\square$$

Замечание. Определение множества $\Pi(\mathfrak{N}^{[\nu]}, g)$ для класса подстановок g, рассмотренного в утверждении 2.17, с помощью вычислений на графе $\Gamma_D(|I_g|)$ имеет сложность порядка n, в то время как с помощью вычислений на графе $\Gamma_L(|I_g|)$ эта задача имеет сложность порядка m.

§ 2.5. Исследование в группах подстановок наследственных признаков, определяемых разбиениями основного множества

2.5.1. Определяющие свойства разбиений конечного множества; характеристики g-разбиений. Обозначим через $\mathrm{Part}(X)$ решётку всех разбиений множества X на непустые подмножества. Пусть $\pi\in\mathrm{Part}(X)$ и $\pi=(X_1, \ldots, X_k)$, тогда подмножества $X_1, \ldots, X_k$ множества X называют *блоками разбиения* π и

$$X=\bigcup_{i=1}^{k} X_i.$$

Одноэлементный блок разбиения π называют *тривиальным блоком* этого разбиения.

Между множеством всех отношений эквивалентности на множестве X и множеством $\mathrm{Part}(X)$ имеется биекция [7, гл. IV, § 4], задаваемая правилом: для $x, x'\in X$ выполнено отношение $x\overset{\pi}{\cong}x'$ тогда и только тогда, когда элементы x и x' принадлежат одному блоку разбиения π.

Множество $\mathrm{Part}(X)$ образует решётку по отношению $\leqslant$, определённому следующим образом: $\pi\leqslant\pi'$ тогда и только тогда, когда разбиение π является *продолжением разбиения* π', т. е. каждый блок разбиения π' есть либо блок разбиения π, либо объединение нескольких блоков разбиения π.

Атомы, коатомы и отношение покрытия в решётке $\mathrm{Part}(X)$ описаны в лемме 1 [7, гл. IV, § 4]. Атомами решётки $\mathrm{Part}(X)$ являются разбиения,

имеющие только один нетривиальный блок, состоящий из двух элементов. Коатомами решётки $\mathrm{Part}(X)$ являются разбиения, имеющие ровно 2 блока. Отношение $\pi' > -\pi$ выполнено тогда и только тогда, когда разбиение π' получено из разбиения π заменой каких-либо двух блоков их объединением.

Произвольная подстановка $g \in \Phi(X)$ однозначно определяет разбиение (обозначим его $\pi(g)$) множества X на блоки, из элементов которых составлены циклы подстановки g. Разбиение $\pi(g)$ назовём *g-разбиением* множества X. Следовательно, любой группе подстановок G соответствует множество Π_G g-разбиений этих подстановок:

$$\Pi_G = \{\pi(g)\colon\ g \in G\}.$$

Рассмотрим $\pi(g)$ как функцию из класса $F(\Phi(X), \mathrm{Part}(X))$. Через $\pi_g(t)$ обозначим g-подфункцию функции $\pi(g)$.

Утверждение 2.18. *Для любой подстановки $g \in \Phi(X)$ порядка n:*

а) $\pi_g(t) \leqslant \pi_g(1)$, $t = 1, \ldots, n$;

б) $\pi_g(t) = \pi_g(d)$, *где* $d = (t, n)$, *и* $\pi_g(\tau) \neq \pi_g(d)$, *если* $\tau, d \in D(n)$ *и* $\tau \neq d$, *вследствие этого множество g-разбиений $\Pi_{\langle g\rangle}$ есть решётка, антиизоморфная решётке $D(n)$;*

в) *если B_G есть c-базис группы подстановок G, то*

$$\Pi_G = \bigcup_{g \in B_G} \Pi_{\langle g\rangle},$$

вследствие этого подмножество Π_G решётки $\mathrm{Part}(X)$ образует нижнюю полурешётку.

Доказательство. Утверждения а) и б) вытекают из утверждения 2.3.

Выражение для множества Π_G в утверждении в) следует из определения множества Π_G и представления (1.3) при $Q = G$. Заметим, что в силу утверждения 2.18,б) множество $\Pi_{\langle g\rangle}$ не зависит от выбора порождающего элемента группы $\langle g\rangle$. Следовательно, в силу единственности канонического c-покрытия группы G множество Π_G не зависит от выбора c-базиса группы G.

Множество Π_G образует нижнюю полурешётку, так как оно содержит наименьшее разбиение $\pi(e)$ решётки $\mathrm{Part}(X)$. □

Определение 2.21. Функцию f из $F(\Phi(X), Y)$ назовём *характеристикой g-разбиений*, если из равенства $\pi(g) = \pi(g')$ для $g, g' \in \Phi(X)$ следует равенство $f(g) = f(g')$. ◇

Замечание. Характеристики g-разбиений определены, по существу, на множестве $\mathrm{Part}(X)$, т. е. принадлежат классу функций $F(\mathrm{Part}(X), Y)$. Отсюда и из утверждения 2.18,б) следует, что D-диаграмма g-подфункции любой характеристики g-разбиений является простой. ◇

Пример 2.21. а) Множество $I(g)$ всех неподвижных относительно подстановки g элементов множества X совпадает с множеством всех тривиальных блоков разбиения $\pi(g)$. Следовательно, $I(g) \in F(\mathrm{Part}(X), 2^X)$, т. е. множество $I(g)$ можно рассматривать как характеристику g-разбиений.

б) Пусть определена функция $f\colon 2^X \to X$, тогда для подстановки $g \in \Phi(X)$, где $\pi(g) = (X_1, \ldots, X_k)$, определим множество $\bar{f}(g)$:

$$\bar{f}(g) = (f(X_1), \ldots, f(X_k))^*.$$

Если для любого $Y \subseteq X$ величина $f(Y)$ инвариантна относительно любой перестановки элементов множества Y, то множество $\bar{f}(g)$ можно рассматривать как характеристику g-разбиений, т. е. $\bar{f}(g)\colon \mathrm{Part}(X) \to 2^X$.

В частности, пусть X — аддитивная группа и для любого $Y \subseteq X$

$$\sigma(Y) = \sum_{x \in Y} x.$$

Тогда для подстановки $g \in \Phi(X)$ определим функцию $\bar{\sigma}(g)$:

$$\bar{\sigma}(g) = \{\sigma(X_1), \ldots, \sigma(X_k)\}^*. \tag{2.25}$$

Функция $\bar{\sigma}(g)$ является характеристикой g-разбиений, так как функция $\sigma(Y)$ инвариантна относительно любой перестановки элементов множества Y. ◇

2.5.2. Исследование групповых признаков, определяемых разбиениями основного множества. Обозначим через $\Phi(\pi)$, где $\pi \in \mathrm{Part}(X)$, множество подстановок g из группы $\Phi(X)$, для которых $\pi(g) \leqslant \pi$.

Теорема 2.12. *Любая группа подстановок G имеет групповой $\Phi(\pi)$-признак при любом разбиении $\pi \in \mathrm{Part}(X)$. Если $G = \langle S \rangle$, то*

$$\mathrm{pok}_S\, \Phi(\pi) \leqslant |G\colon (G \cap \Phi(\pi))|.$$

Доказательство. Множество подстановок $\Phi(\pi)$ замкнуто относительно произведения, следовательно, $\Phi(\pi) < \Phi(X)$ и любая группа подстановок G имеет групповой $\Phi(\pi)$-признак. Отсюда по теореме 1.1 получаем оценку для величины $\mathrm{pok}_S\, \Phi(\pi)$. □

Напомним некоторые определения и утверждения [6, гл. XI, § 7], необходимые для рассмотрения свойств неподвижных подмножеств подстановок.

Пусть $G < \Phi(X)$ и $g \in G$.

Определение 2.22. *Стабилизатором элемента x (подмножества Y) множества X в группе подстановок G* называется множество подстановок g группы G, относительно которых элемент x (каждый элемент x подмножества Y) является неподвижным. ◇

Стабилизатор элемента x (подмножества Y) в группе подстановок G обозначим через G_x (через G_Y).

Замечание. По лемме Бернсайда для всякого $x \in X$ стабилизатор G_x есть подгруппа группы G и

$$|G| = |G_x| \cdot |G(x)|,$$

где $G(x)$ — орбита элемента x относительно группы G.

В силу этого равенства условие тривиальности стабилизатора G_x в группе подстановок G равносильно условию $|G| = |G(x)|$. ◇

Очевидно, $G_Y < G$ при любом $Y \subseteq X$, так как $G_Y = \bigcap\limits_{x \in Y} G_x$. Следовательно, всякая группа G подстановок множества X имеет при любом $Y \subseteq X$ групповой G_Y-признак.

Подмножеству Y поставим в соответствие разбиение $\pi_Y \in \mathrm{Part}(X)$, в котором каждый элемент $y \in Y$ образует тривиальный блок и все элементы $x \in X \setminus Y$ образуют единый блок. В силу указанного соответствия $\Phi_Y = \Phi(\pi_Y)$. Следовательно, Φ_Y-признак есть частный случай $\Phi(\pi)$-признака, рассмотренного в пункте 2.5.1.

Исследуем в группах подстановок характеристики групповых признаков: Φ_x-признака и Φ_Y-признака, $x \in X$, $Y \subseteq X$.

Обозначим через $l_x(g)$ длину цикла в графе Γ_g, которому принадлежит элемент x, т. е. $l_x(g) \in L(g)$.

Теорема 2.13. *Для любого* $x \in X$

а) $\mathrm{pok}_g \Phi_x = l_x(g)$;

б) *подгруппа* Φ_x*-тривиальности группы* $\langle g \rangle$ *есть* $\langle g^t \rangle$, *где* $t = \mathrm{mp}_n(l_x(g))$;

в) Φ_x*-признак в циклической группе* $\langle g \rangle$ *тривиален тогда и только тогда, когда* g *— унидоминантная подстановка и число* $l_x(g)$ *доминирует во множестве* $L(g)$;

г) Φ_x*-признак является квазиполным в циклической группе* $\langle g \rangle$ *тогда и только тогда, когда* n *есть степень простого числа* p *и* $l_x(g) = p$.

Доказательство. а) Так как Φ_x — группа, то по следствию 2 теоремы 1.5 имеется единственное (Φ_x, g)-пороговое число, которое по следствию 1 теоремы 1.5 совпадает с $\mathrm{pok}_g \Phi_x$.

По определению $\mathrm{pok}_g \Phi_x$ есть наименьшее натуральное число t такое, что $g^t(x) = x$. Следовательно, $\mathrm{pok}_g \Phi_x = l_x(g)$.

б) Единственное (Φ_x, g)-пороговое число равно $l_x(g)$. Значит, по следствию теоремы 1.7 подгруппа Φ_x-тривиальности группы $\langle g \rangle$ порождается элементом g^t, где $t = \mathrm{mp}_n(l_x(g))$.

в) Так как единственное (Φ_x, g)-пороговое число равно $l_x(g)$, то по следствию 2 теоремы 1.5 тривиальность Φ_x-признака в группе $\langle g \rangle$ равносильна тому, что $l_x(g) = n$, где $n = HOK\{l_1, \ldots, l_m\}$ и $l_x(g) \in \{l_1, \ldots, l_m\}$. Значит, $l_x(g)$ — единственное доминирующее число множества $L(g)$.

Утверждение г) вытекает из следствия утверждения 1.11 и теоремы 2.13,а). □

Теорема 2.14. *Для любого* $Y \subseteq X$

а) $\mathrm{pok}_g \Phi_Y = HOK\{l_x(g)\colon x \in Y\}$;

б) *подгруппа* Φ_Y*-тривиальности группы* $\langle g \rangle$ *есть* $\langle g^t \rangle$, *где*

$$t = \mathrm{mp}_n(HOK\{l_x(g)\colon x \in Y\});$$

в) Φ_Y*-признак в циклической группе* $\langle g \rangle$ *тривиален тогда и только тогда, когда* $HOK\{l_x(g)\colon x \in Y\} = n$; *в частности, если* $\mathrm{dom}\, L \subseteq \{l_x(g)\colon x \in Y\}^*$, *то группа* $\langle g \rangle$ *имеет тривиальный* Φ_Y*-признак;*

г) Φ_Y*-признак является квазиполным в циклической группе* $\langle g \rangle$ *тогда и только тогда, когда* n *есть степень простого числа* p *и* $HOK\{l_x(g)\colon x \in Y\} = p$.

Доказательство. а) Φ_Y-признак совпадает с групповым $\bigcap_{x \in Y} \Phi_x$-признаком в группе G подстановок множества X. При этом из следствия 2 теоремы 1.6 вытекает, что

$$\mathrm{pok}_g \Phi_Y = HOK\{\mathrm{pok}_g \Phi_x\colon x \in Y\}.$$

Отсюда и из теоремы 2.13,а) получаем выражение для $\mathrm{pok}_g \Phi_Y$.

б) Единственное (Φ_Y, g)-пороговое число равно $HOK\{l_x(g)\colon x \in Y\}$. Значит, по следствию теоремы 1.7 подгруппа Φ_Y-тривиальности группы $\langle g \rangle$ порождается элементом g^t, где $t = \mathrm{mp}_n(HOK\{l_x(g)\colon x \in Y\})$.

в) Так как единственное (Φ_Y, g)-пороговое число равно $HOK\{l_x(g)\colon x \in Y\}$, то по следствию 2 теоремы 1.5 тривиальность Φ_x-признака в группе $\langle g \rangle$ равносильна тому, что $HOK\{l_x(g)\colon x \in Y\} = n$.

Пусть $\mathrm{dom}\, L = \{l_1, \ldots, l_d\}$, где $1 \leqslant d \leqslant m$, тогда $n = HOK\{l_1, \ldots, l_d\}$. Если $\{l_1, \ldots, l_d\} \subseteq \{l_x(g)\colon x \in Y\}^*$, то выполнена цепочка соотношений:

$$n = HOK\{l_1, \ldots, l_d\} \leqslant HOK\{l_x(g)\colon x \in Y\} \leqslant n.$$

Значит, $HOK\{l_x(g)\colon x \in Y\} = n$ и Φ_Y-признак в группе $\langle g \rangle$ тривиален.

Утверждение г) вытекает из следствия утверждения 1.11 и теоремы 2.14,а). □

Теорема 2.15. *Пусть* $S=\{s_1,\ldots,s_p\}\subseteq\Phi(X)$ *и* $G=\langle S\rangle$. *Тогда:*

а) *для любого* $x\in X$ Φ_x*-показатель группы* G *равен длине* $\omega_x(\Gamma_{S(X)})$ *кратчайшего цикла в графе* $\Gamma_{S(X)}$, *содержащего вершину* x, *и выполнено:*

$$\operatorname{pok}_S\Phi_x\leqslant\min\{l_x(s_1),\ldots,l_x(s_p)\};$$

б) *для любого* $Y\subseteq X$

$$\operatorname{pok}_S\Phi_Y\leqslant\min\{\operatorname{pok}_{s_1}\Phi_Y,\ldots,\operatorname{pok}_{s_p}\Phi_Y\};$$

в) *тривиальность* Φ_x*-признака в группе подстановок* G *равносильна каждому из следующих предложений:*

в1) *любая подстановка* g *группы* G *является унидоминантной и число* $l_x(g)$ *доминирует во множестве* $L(g)$;

в2) *каждый элемент* g *некоторого* c*-базиса* B_G *группы* G *является унидоминантной подстановкой и число* $l_x(g)$ *доминирует во множестве* $L(g)$;

г) *тривиальность* Φ_Y*-признака в группе подстановок* G *равносильна каждому из следующих предложений:*

г1) *для любой подстановки* g *группы* G *выполнено равенство* $НОК\{l_x(g)\colon x\in Y\}=\operatorname{ord}g$;

г2) *для любого элемента* g *некоторого* c*-базиса* B_G *группы* G *выполнено равенство* $НОК\{l_x(g)\colon x\in Y\}=\operatorname{ord}g$.

Доказательство. а) По определению $\operatorname{pok}_S\Phi_x$ есть наименьшее натуральное t такое, что при некоторых $i_1,\ldots,i_t\in\{1,\ldots,p\}$ для преобразования $g=s_{i_1}\cdot\ldots\cdot s_{i_t}$ выполнено равенство $g(x)=x$. Из определения графа $\Gamma_{S(X)}$ следует, что число t совпадает с длиной кратчайшего цикла в графе $\Gamma_{S(X)}$, содержащего вершину x.

По утверждению 1.2

$$\operatorname{pok}_S\Phi_x\leqslant\min_{j\in\{1,\ldots,p\}}\{\operatorname{pok}_{s_j}\Phi_x\},$$

где по теореме 2.13,а) $\operatorname{pok}_{s_j}\Phi_x=l_x(s_j)$, $j=1,\ldots,p$.

б) Применяя утверждение 1.2 к Φ_Y-признаку в группе G, получаем требуемое неравенство для $\operatorname{pok}_S\Phi_Y$.

в) Рассмотрим тривиальное c-покрытие группы G, т. е. в равенстве (1.2) положим $Q=R=G$.

По утверждению 1.8,в) Φ_x-признак тривиален в группе G тогда и только тогда, когда он тривиален в циклической группе $\langle g\rangle$ для любого $g\in R$ (в нашем случае для любого $g\in G$). Отсюда и из теоремы 2.13,в) получаем, что тривиальность Φ_x-признака в группе подстановок G равносильна предложению в1).

Предложение в2) следует из в1) очевидным образом. Покажем, что из предложения в2) следует предложение в1).

Если подстановка g — унидоминантная, то в силу наследственности U-признака подстановка g^t — также унидоминантная. Кроме того, если число $l_x(g)$ доминирует в наборе $L(g)$, то по утверждению 2.4,а) число $l_x(g^t)$ доминирует во множестве $L(g^t)$, $t=1,\ldots,n$.

Значит, если каждый элемент g некоторого c-базиса B_G группы G является унидоминантной подстановкой и число $l_x(g)$ доминирует в наборе $L(g)$, то группа G состоит из унидоминантных подстановок g таких, что число $l_x(g)$ доминирует во множестве $L(g)$.

г) Доказывается аналогично теореме 2.15,в) с использованием теоремы 2.14,в). □

Пример 2.22. Группа сдвигов Σ_r пространства V_r двоичных r-мерных векторов имеет при любом векторе $x \in V_r$ тривиальный Φ_x-признак, так как любая нетождественная подстановка g группы Σ_r состоит из 2^{r-1} циклов длины 2, т. е. является унидоминантной, где число 2 доминирует в наборе $L(g)$. ◇

Пример 2.23. Пусть подстановка g множества $\{1, 2, \ldots, 84\}$ (см. примеры 2.6, 2.9, 2.11) имеет цикловую структуру $C(g) = (1^7, 6, 15, 21, 35)$, и, в частности, циклы длины 1, 6 и 15 образованы соответственно подмножествами элементов:

$$(1), (2), (3), (4), (5), (6), (7), (8, 9, \ldots, 13), (14, 15, \ldots, 28).$$

Порядок подстановки g равен 210 и

$$L = (1, 6, 15, 21, 35), K = (7, 1, 1, 1, 1), \operatorname{dom} L = (6, 15, 21, 35).$$

Определим при некоторых $x \in \{1, 2, \ldots, 84\}$ характеристики группового Φ_x-признака в циклической группе $\langle g \rangle$.

По теореме 2.13,в) Φ_x-признак в группе $\langle g \rangle$ нетривиален при любом $x \in \{1, 2, \ldots, 84\}$, так как g есть 4-доминантная подстановка.

По теореме 2.13,г) Φ_x-признак в группе $\langle g \rangle$ не является квазиполным при любом $x \in \{1, 2, \ldots, 84\}$, так как решётка $D(210)$ содержит более одного атома.

а) Рассмотрим групповой Φ_9-признак в группе $\langle g \rangle$.

1) $\Pi(\Phi_9, g) = \{l_9(g)\} = \{6\}$, отсюда по теореме 2.13,а) $\operatorname{pok}_g \Phi_9 = 6$;

2) по теореме 2.13,б) подгруппа Φ_9-тривиальности группы $\langle g \rangle$ совпадает с группой $\langle g^{35} \rangle$, так как $\operatorname{mp}_{210}(6) = 35$.

б) Рассмотрим групповой Φ_{16}-признак в группе $\langle g \rangle$.

1) $\Pi(\Phi_{16}, g) = \{l_{16}(g)\} = \{15\}$, отсюда по теореме 2.13,а) $\operatorname{pok}_g \Phi_{16} = 15$;

2) по теореме 2.13,б) подгруппа Φ_{16}-тривиальности группы $\langle g \rangle$ совпадает с группой $\langle g^{14} \rangle$, так как $\operatorname{mp}_{210}(15) = 14$. ◇

Пример 2.24. Для подстановки g множества $\{1, 2, \ldots, 84\}$ из примера 2.23 определим при некоторых $Y \subseteq \{1, 2, \ldots, 84\}$ характеристики группового Φ_Y-признака в группе $\langle g \rangle$.

По теореме 2.14,г) Φ_Y-признак в группе $\langle g \rangle$ не является квазиполным при любом $Y \subseteq \{1, 2, \ldots, 84\}$, так как решётка $D(210)$ содержит более одного атома.

а) Пусть $Y = \{9, 16\}$. По теореме 2.14,а)

$$\operatorname{pok}_g \Phi_Y = HOK(l_9(g), l_{16}(g)) = HOK(6, 15) = 30.$$

По теореме 2.14,в) Φ_Y-признак в группе $\langle g \rangle$ нетривиален, так как $\operatorname{pok}_g \Phi_Y \neq 210$.

По теореме 2.14,б) подгруппа Φ_Y-тривиальности группы $\langle g \rangle$ совпадает с группой $\langle g^7 \rangle$, так как $\operatorname{mp}_{210}(30) = 7$.

б) Пусть $Y = \{1, 9, 11\}$. По теореме 2.14,а)

$$\operatorname{pok}_g \Phi_Y = HOK(l_1(g), l_9(g), l_{11}(g)) = HOK(1, 6, 6) = 6.$$

По теореме 2.14,в) Φ_Y-признак в группе $\langle g \rangle$ нетривиален, так как $\operatorname{pok}_g \Phi_Y \neq 210$.

По теореме 2.14,б) подгруппа Φ_Y-тривиальности группы $\langle g \rangle$ совпадает с группой $\langle g^{35} \rangle$, так как $\operatorname{mp}_{210}(6) = 35$. ◇

§ 2.6. Исследование наследственных признаков в группах подстановок аддитивной группы

2.6.1. Наследственные признаки сравнения функций. Пусть $f, f' \in F(\Phi(X), Y)$, где Y — линейно или частично упорядоченное множество. Обозначим через $\Phi(f \leqslant f')$ множество подстановок:

$$\Phi(f \leqslant f') = \{g \in \Phi(X): f(g) \leqslant f'(g)\}.$$

Определение 2.23. H-признак в группе подстановок G назовём *признаком сравнения функций* f и f', если $G \cap H \subseteq \Phi(f \leqslant f')$.

Утверждение 2.19. *Если функции f и f' являются характеристиками g-разбиений, то $\Phi(f \leqslant f')$-признак сравнения функций f и f' в группе подстановок G является наследственным тогда и только тогда, когда из включения $g \in G \cap \Phi(f \leqslant f')$ следует, что $g^t \in G \cap \Phi(f \leqslant f')$ при любом $t \in D(n)$, при этом $f(e) \leqslant f'(e)$.*

Доказательство. Из определения 1.8 следует, что $\Phi(f \leqslant f')$-признак сравнения функций f и f' в группе подстановок G является наследственным, если из включения $g \in G \cap \Phi(f \leqslant f')$ следует, что $\langle g \rangle \subseteq G \cap \Phi(f \leqslant f')$. Иначе говоря, если для $g \in G$ из неравенства $f(g) \leqslant f'(g)$ следуют неравенства $f(g^t) \leqslant f'(g^t)$, $t = 1, \ldots, n$.

Если функции f и f' являются характеристиками g-разбиений, то из утверждения 2.18,б) следует, что последняя система неравенств равносильна собственной подсистеме неравенств при всех $t \in D(n)$. В частности, при $t = n$ получаем: $f(e) \leqslant f'(e)$. □

Следствие. *Если $\Phi(f \leqslant f')$-признак сравнения функций f и f' в группе подстановок $\langle g \rangle$ является наследственным, то по теореме* 1.5, в)

$$\Pi(\Phi(f \leqslant f'), g) = \operatorname{prm}\{t \in D(n): \langle g^t \rangle \subseteq (\Phi(f \leqslant f')\}. \diamondsuit$$

Пусть основное множество X образует аддитивную группу. Рассмотрим признак сравнения характеристик g-разбиений $\bar{\sigma}(g)$ и $I(g)$ (см. пример 2.21). Для этого определим:

$$\Phi(\bar{\sigma} \subseteq I) = \{g \in \Phi(X): \bar{\sigma}(g) \subseteq I(g)\}.$$

Из равенства (2.25) следует, что $g \in \Phi(\bar{\sigma} \subseteq I)$ тогда и только тогда, когда $\sigma(X_i) \in I(g)$, $i = 1, \ldots, k$, где $\pi(g) = (X_1, \ldots, X_k)$.

Тождественная подстановка $e \in \Phi(\bar{\sigma} \subseteq I)$, так как $\bar{\sigma}(e) = X = I(e)$.

Определение 2.24. *Подстановку g* аддитивной группы X назовём *$\bar{\sigma}$-стабильной*, если $g^t \in \Phi(\bar{\sigma} \subseteq I)$, $t = 1, \ldots, n$. $\diamondsuit$

Класс всех $\bar{\sigma}$-стабильных подстановок группы $\Phi(X)$ обозначим $\Sigma(X)$ или кратко Σ.

Замечание 1. Так как функции $\bar{\sigma}(g)$ и $I(g)$ являются характеристиками g-разбиений, то по утверждению 2.19 подстановка g аддитивной группы X является $\bar{\sigma}$-стабильной тогда и только тогда, когда $g^t \in \Phi(\bar{\sigma} \subseteq I)$ при любом $t \in D(n)$.

Замечание 2. Для любой подстановки $g \in \Phi(X)$ множество $\bar{\sigma}(g)$ не пусто, поэтому если подстановка g является $\bar{\sigma}$-стабильной, то $I(g) \neq \varnothing$. Следовательно,

$$\Sigma(X) \subseteq \Phi(|I| \geqslant 1).$$

Замечание 3. В любой группе подстановок Σ-признак является наследственным признаком сравнения функций $\bar{\sigma}(g)$ и $I(g)$, что следует

из определения 2.24. Множество $\Pi(\Sigma, g)$ определяется в соответствии с теоремой 1.5,в) выражением:

$$\Pi(\Sigma, g) = \mathrm{prm}\{t \in D(n)\colon \langle g^t\rangle \subseteq \Phi(\bar{\sigma} \subseteq I)\}.\diamondsuit$$

2.6.2. Наследственный признак $\bar{\sigma}$-смещения в группах подстановок. Для подстановок циклической группы $\langle g\rangle$ определим наборы элементов множества X. Пусть $\pi(g^t) = (X_{1,t}, \ldots, X_{k_t,t})$, тогда

$$\Delta(\bar{\sigma}, g^t) = \{\delta_{1,t}, \ldots, \delta_{k_t,t}\},$$

где для $i = 1, \ldots, k_t$ и $t = 1, \ldots, n$

$$\delta_{i,t} = g^t(\sigma(X_{i,t})) - \sigma(X_{i,t}).$$

Например, тождественной подстановке e соответствует набор $\Delta(\bar{\sigma}, e)$, состоящий из $|X|$ элементов равных θ, где θ — нейтральный элемент аддитивной группы X.

Определение 2.25. *Подстановку g* аддитивной группы X назовём *$\bar{\sigma}$-смещённой*, если для $i = 1, \ldots, k_t$ и $t = 1, \ldots, n$

$$\delta_{i,t} = (1 - |X_{i,t}|) \cdot g^t(\theta).\diamondsuit$$

Множество всех $\bar{\sigma}$-смещённых подстановок группы X обозначим $\Sigma^{\downarrow}(X)$ (кратко $\Sigma^{\downarrow}$).

Замечание 1. Если $g(\theta) = \theta$, то из определений 2.24 и 2.25 следует, что $\bar{\sigma}$-смещённость подстановки g равносильна $\bar{\sigma}$-стабильности всех подстановок циклической группы $\langle g\rangle$.

Следовательно, $\Sigma^{\downarrow}(X) \cap \Phi_\theta(X) = \Sigma(X) \cap \Phi_\theta(X)$, где $\Phi_\theta(X)$ — стабилизатор элемента θ в группе подстановок $\Phi(X)$.

Замечание 2. $\Sigma^{\downarrow}$-признак в любой группе подстановок G является наследственным признаком, что вытекает из определения 2.25. При этом из теоремы 1.5,в) следует, что

$$\Pi(\Sigma^{\downarrow}, g) = \mathrm{prm}\{t \in D(n)\colon g^t \in \Sigma^{\downarrow}\}.$$

Замечание 3. В частности, подстановка g пространства V_n двоичных n-мерных векторов является $\bar{\sigma}$-смещённой, если $\delta_{i,t} = \theta$ для каждого цикла $X_{i,t}$ нечётной длины подстановки g^t, и $\delta_{i,t} = g^t(\theta)$ для каждого цикла $X_{i,t}$ чётной длины подстановки g^t, $t = 1, \ldots, n$.

2.6.3. Наследственные признаки квазиаффинности в группах подстановок. Рассмотрим функцию f, определённую на циклической подгруппе $\langle g\rangle$ конечной группы Φ и принимающую значения в частично упорядоченном множестве Y.

Определение 2.26. *Функцию f* назовём *регулярной индекса z* (на циклической подгруппе $\langle g\rangle$), где z/n, если наименьший период последовательности $\{f(g), f(g^2), \ldots, f(g^n)\}$ равен $\frac{n}{z}$. $\diamondsuit$

Замечание 1. Всякая функция, определённая на циклической подгруппе $\langle g\rangle$, является регулярной некоторого индекса z, где z/n. В частности, регулярность индекса 1 для функции f равносильна тому, что наименьший период последовательности $\{f(g), f(g^2), \ldots, f(g^n)\}$ равен n.

Замечание 2. Функция f является регулярной индекса n тогда и только тогда, когда f является константой. $\diamondsuit$

Рассмотрим функцию $f \in F(\langle g \rangle, N)$.

Определение 2.27. *Функцию f* назовём псевдонормальной (*псевдоантинормальной, p-псевдонормальной, p-псевдоантинормальной*) индекса z, где p, z — натуральные и z/n, если ограничение функции f на множество $\{g, \ldots, g^{\frac{n}{z}}\}$ есть нормальная (антинормальная, p-нормальная, p-антинормальная) функция. ◇

Замечание 1. Для функции f свойство псевдонормальности (псевдоантинормальности, p-псевдонормальности, p-псевдоантинормальности) индекса 1 и свойство нормальности (антинормальности, p-нормальности, p-антинормальности) являются тождественными.

Замечание 2. Всякая функция f из $F(\langle g \rangle, N)$ является псевдонормальной (псевдоантинормальной, p-псевдонормальной, p-псевдоантинормальной) индекса n. ◇

Для подстановки g порядка n и $\alpha \in X$ определим множество:

$$\Delta_\alpha(g) = \{x \in X\colon g(x) - x = \alpha\}.$$

Отсюда следует, что g есть подстановка сдвига на элемент α, т. е. $g(x) = x + \alpha$, тогда и только тогда, когда $\Delta_\alpha(g) = X$.

Подстановке g и набору $\bar{\alpha} \in X^n$, где $\bar{\alpha} = (\alpha(1), \ldots, \alpha(n))$, поставим в соответствие набор, состоящий из n натуральных чисел:

$$\bar{\rho}_{g,\bar{\alpha}} = (\bar{\rho}_{g,\bar{\alpha}}(1), \ldots, \bar{\rho}_{g,\bar{\alpha}}(n)),$$

где для $t = 1, \ldots, n$

$$\bar{\rho}_{g,\bar{\alpha}}(t) = |\Delta_{\alpha(t)}(g^t)|.$$

Набор $\bar{\rho}_{g,\bar{\alpha}}$ при фиксированном наборе $\bar{\alpha}$ можно рассматривать как табличное задание функции (обозначим её также $\bar{\rho}_{g,\bar{\alpha}}$), определённой на подстановках циклической группы $\langle g \rangle$ порядка n. При $\bar{\alpha} = (g(\theta), \ldots, g^n(\theta))$ функцию $\bar{\rho}_{g,\bar{\alpha}}$ обозначим кратко через $\bar{\rho}_g$.

Определение 2.28. *Подстановку g* аддитивной группы X назовём *псевдоаффинной* (*p-псевдоаффинной*) *индекса z*, где z/n, если функция $\bar{\rho}_g$ одновременно является регулярной индекса z и псевдоантинормальной (p-псевдоантинормальной) индекса z.

Подстановку g назовём *псевдоаффинной* (*p-псевдоаффинной*), если функция $\bar{\rho}_g$ одновременно является регулярной индекса z и псевдоантинормальной (p-псевдоантинормальной) индекса z при некотором $z \in D(\operatorname{ord} g)$. ◇

Множество всех псевдоаффинных (p-псевдоаффинных, псевдоаффинных индекса z, p-псевдоаффинных индекса z) подстановок из $\Phi(X)$ обозначим $PA(\mathrm{X})$ или кратко PA ($PA^p(\mathrm{X})$ или кратко PA^p, $PA_z(\mathrm{X})$ или кратко PA_z, $PA_z^p(X)$ или кратко PA_z^p).

Множества $PA(X)$ и $PA^p(X)$ не пусты, так как содержат подстановку e.

Замечание. Из определения 2.28 следует, что $PA_z^p \subseteq PA_z$ при любом $z \in D(n)$ и, следовательно, $PA^p(X) \subseteq PA(X)$.

Утверждение 2.20.

$$PA_1(X) \cap \Phi_\theta(X) = \Lambda^{[\nu]}(X) \cap \Phi_\theta(X)$$
$$(PA_1^p(X) \cap \Phi_\theta(X) = \Lambda^{[p\nu]}(X) \cap \Phi_\theta(X)).$$

Доказательство *. Заметим, что $\Delta_\theta(g) = I(g)$ и если $g(\theta) = \theta$, то $(g(\theta), \ldots, g^n(\theta)) = (\theta, \ldots, \theta)$. Поэтому если $g(\theta) = \theta$, то таблица функции $\bar{\rho}_g$ имеет вид:

$$\bar{\rho}_g = (|I(g)|, \ldots, |I(g^n)|).$$

Следовательно, если $g(\theta)=\theta$, то из определений 2.27 и 2.20 следует, что для функции $\bar{\rho}_g$ псевдоантинормальность индекса 1 равносильна нормальной неподвижности подстановки g.

Вместе с тем, функция $\bar{\rho}_g$ является регулярной индекса 1, так как из формул (2.14), (2.15) следует, что $|I(g^t)|=|X|$ тогда и только тогда, когда $t=n$. Следовательно, если $g(\theta)=\theta$, то для функции $\bar{\rho}_g$ псевдоаффинность индекса 1 равносильна нормальной неподвижности подстановки g. Отсюда получаем требуемое равенство. □

Определение 2.29. *Подстановку* g аддитивной группы X назовём *квазиаффинной* (*p-квазиаффинной*), если $\langle g\rangle \subseteq PA(X)$ ($\langle g\rangle \subseteq PA^p(X)$). ◇

Множество всех квазиаффинных (p-квазиаффинных) подстановок аддитивной группы X обозначим $QA(X)$ или кратко QA (обозначим $QA^p(X)$ или кратко QA^p).

Из определения 2.29 следует, что

$$QA(X)\subseteq PA(X)\quad (QA^p(X)\subseteq PA^p(X)),$$
$$QA^p(X)\subseteq QA(X).$$

При этом QA-признак (QA^p-признак) в любой группе подстановок G является наследственным признаком.

Множество $\Pi(QA, g)$ (множество $\Pi(QA^p, g)$) определяется теоремой 1.5,в):

$$\Pi(QA, g)=\mathrm{prm}\{t\in D(n)\colon g^t\in QA\}$$
$$(\Pi(QA^p, g)=\mathrm{prm}\{t\in D(n)\colon g^t\in QA^p\}).$$

§ 2.7. Соотношения между классами наследственных признаков

Многообразие рассмотренных признаков в группе $\Phi(X)$ и её подгруппах приводит к естественной задаче описания различных классов признаков и соотношений между ними.

Множество всех признаков в группе подстановок $\Phi(X)$ в соответствии с определением 1.4 можно рассматривать как булеан $2^{\Phi(X)}$ группы $\Phi(X)$.

Наибольший интерес с точки зрения приложений представляет систематизация множества наследственных признаков в группе подстановок $\Phi(X)$ (обозначим это множество $\mathrm{A}H_{\Phi(X)}$).

По утверждению 1.7,б) $\mathrm{A}H_{\Phi(X)}$ есть кольцо всех наследственных подмножеств группы $\Phi(X)$, рассматриваемой как частично упорядоченное множество. Следовательно, множество $\mathrm{A}H_{\Phi(X)}$ образует решётку относительно теоретико-множественного включения.

Любые два признака из $\mathrm{A}H_{\Phi(X)}$ имеют непустое пересечение, содержащее как минимум тождественную подстановку e (см. утверждение 1.5,а)). Наибольшим и наименьшим элементами решётки $\mathrm{A}H_{\Phi(X)}$ являются соответственно группа $\Phi(X)$ и одноэлементное множество, состоящее из подстановки e.

Рассмотрим теоретико-множественные соотношения между рассмотренными ранее классами наследственных признаков. Обозначим $|X|=q$.

1. Пусть $\mu(g)$ — число различных длин циклов в цикловой структуре $C(g)$ подстановки g множества X и $\Phi(\mu\leqslant r)$ есть множество подстановок g из группы $\Phi(X)$, для которых $\mu(g)\leqslant r$. Если $L(g)=(l_1,\ldots,l_m)$, то $\mu(g)=m$, при этом $l_1+\ldots+l_m\leqslant q$.

Следовательно, при фиксированном q функция $\mu(g)$ принимает наибольшее значение для тех подстановок g, у которых $K(g)=(1,\ldots,1)$ и множество $L(g)$ состоит из наименьших различных чисел $l_1,\ldots,l_m$ таких, что $l_1+\ldots+l_m=q$. Значит, наибольшее значение m функции $\mu(g)$ определяется из неравенств:

$$1+2+\ldots+m\leqslant q<1+2+\ldots+m+(m+1).$$

При $m<2q^{1/2}$ эти неравенства удовлетворяются. Следовательно, $\Phi(\mu\leqslant r)$-признак достаточно рассматривать лишь при натуральных $r\leqslant 2q^{1/2}$, так как $\Phi(\mu\leqslant r)=\Phi(X)$ при $r\geqslant 2q^{1/2}$.

Из определения множества $\Phi(\mu\leqslant r)$ следует, что

$$\Phi(\mu\leqslant[2q^{1/2}])\supseteq\Phi(\mu\leqslant[2q^{1/2}]-1)\supseteq\ldots\supseteq\Phi(\mu\leqslant 1). \tag{2.26}$$

2. Функция $|\operatorname{dom}L(g)|$ принимает наибольшее значение при фиксированном q для тех подстановок g, у которых $K(g)=(1,\ldots,1)$ и множество $L(g)$ состоит из возможно большего числа m попарно несравнимых чисел $l_1,\ldots,l_m$ таких, что $l_1+\ldots+l_m\leqslant q$. Отсюда следует, что m не превышает наибольшего числа простых чисел, сумма которых не превосходит q. Значит, при фиксированном q число $m-1$ оценивается сверху числом членов арифметической прогрессии, составленной из нечётных чисел, начиная с 3, сумма которой не превышает $q-2$:

$$3+5+\ldots+(2m-1)\leqslant q-2.$$

При $m<q^{1/2}$ эти неравенства удовлетворяются. Следовательно, $\Phi(\operatorname{dom}\leqslant r)$-признак достаточно рассматривать лишь при натуральных $r\leqslant q^{1/2}$, так как $\Phi(\operatorname{dom}\leqslant r)=\Phi(X)$ при $r\geqslant q^{1/2}$.

Из определения множеств $\Phi(\mu\leqslant r)$ и $\Phi(\operatorname{dom}\leqslant r)$ следует, что при $r\leqslant q^{1/2}$

$$\Phi(\mu\leqslant r)\subseteq\Phi(\operatorname{dom}\leqslant r), \tag{2.27}$$

кроме того, из определения множеств $\Phi(\operatorname{dom}\leqslant r)$, U и $\bar{C}$ следует цепочка включений:

$$\Phi(\operatorname{dom}\leqslant[q^{1/2}])\supseteq\Phi(\operatorname{dom}\leqslant[q^{1/2}]-1)\supseteq\ldots\supseteq\Phi(\operatorname{dom}\leqslant 1)=U\supseteq\bar{C}. \tag{2.28}$$

3. При фиксированном q наибольшее значение функции $|\operatorname{opn}L^2|$ есть C_m^2, где m можно оценить сверху так же, как в п. 2. Значит, $\Phi(\operatorname{opn}\leqslant r)$-признак достаточно рассматривать лишь при натуральных $r\leqslant\frac{1}{2}(q-q^{1/2})$, так как $\Phi(\operatorname{opn}\leqslant r)=\Phi(X)$ при $r\geqslant\frac{1}{2}(q-q^{1/2})$.

Из определения множеств $\Phi(\operatorname{opn}\leqslant r)$, $\bar{C}$ и CH следует что

$$\Phi(\operatorname{opn}\leqslant[\tfrac{1}{2}(q-q^{1/2})])\supseteq\Phi(\operatorname{opn}\leqslant[\tfrac{1}{2}(q-q^{1/2})]-1)\supseteq\ldots\supseteq\Phi(\operatorname{opn}\leqslant 0)=$$
$$=\bar{C}\supseteq CH. \tag{2.29}$$

4. Если множество $L(g)$ образует цепь, то при фиксированном q наибольшая из длин цепей оценивается числом членов геометрической прогрессии со знаменателем 2 и суммой, не превышающей q. Следовательно, длина m цепи $L(g)$ не превышает $\log_2 q$ и $CH(r)$-признак достаточно рассматривать лишь при натуральных $r\leqslant\log_2 q$.

Из определения множеств CH и $CH(r)$ следует, что

$$CH=CH([\log_2 q])\supseteq CH([\log_2 q]-1)\supseteq\ldots\supseteq CH(1)=\Phi(\mu\leqslant 1). \tag{2.30}$$

5. Наибольшие значения функций $\varkappa(g)$, $\varkappa^l(g)$ и $\xi^l(g)$ не превышают q, отсюда в соответствии с определениями множеств $\Phi(\varkappa \geqslant r)$, $\Phi(\varkappa^l \geqslant r)$ и $\Phi(\xi^l \geqslant r)$ выполнены следующие цепочки включений:

$$\Phi(X) = \Phi(\varkappa \geqslant 1) \supseteq \Phi(\varkappa \geqslant 2) \supseteq \ldots \supseteq \Phi(\varkappa \geqslant q); \tag{2.31}$$

$$\Phi(X) = \Phi(\varkappa^l \geqslant 0) \supseteq \Phi(\varkappa^l \geqslant 1) \supseteq \ldots \supseteq \Phi(\varkappa^l \geqslant q), \quad l = 1, \ldots, q; \tag{2.32}$$

$$\Phi(X) = \Phi(\xi^l \geqslant 0) \supseteq \Phi(\xi^l \geqslant 1) \supseteq \ldots \supseteq \Phi(\xi^l \geqslant q), \quad l = 1, \ldots, q; \tag{2.33}$$

$$\Phi(\varkappa^l \geqslant \left[\tfrac{r}{l}\right]) \supseteq \Phi(\xi^l \geqslant r) \supseteq \Phi(\varkappa^l \geqslant r), \quad l, r \in \{1, \ldots, q\}; \tag{2.34}$$

$$\Phi(\varkappa \geqslant r) \supseteq \Phi(\varkappa^l \geqslant r), \quad l, r \in \{1, \ldots, q\}. \tag{2.35}$$

6. С учётом определения множества $\Phi(|I| \geqslant r)$ верны цепочки включений, $r = 1, \ldots, q$:

$$\Phi(\varkappa \geqslant r) = \Phi(\varkappa^q \geqslant r) \supseteq \Phi(\varkappa^{q-1} \geqslant r) \supseteq \ldots \supseteq \Phi(\varkappa^1 \geqslant r) = \Phi(|I| \geqslant r); \tag{2.36}$$

$$\Phi(X) = \Phi(\xi^q \geqslant r) \supseteq \Phi(\xi^{q-1} \geqslant r) \supseteq \ldots \supseteq \Phi(\xi^1 \geqslant r) = \Phi(|I| \geqslant r); \tag{2.37}$$

$$\Phi(X) = \Phi(|I| \geqslant 0) \supseteq \Phi(|I| \geqslant 1) \supseteq \ldots \supseteq \Phi(|I| \geqslant q). \tag{2.38}$$

7. Из определения 2.20 нормально (p-нормально) неподвижных подстановок следует, что при любом простом p выполнены включения:

$$\Phi(|I| \geqslant 1) \supseteq \Lambda^{[\nu]} \supseteq \Lambda^{[p\nu]}. \tag{2.39}$$

8. Для любой цепи разбиений $\pi_1 \geqslant \ldots \geqslant \pi_r$ множества X, содержащейся в решётке $\mathrm{Part}(X)$, выполнена цепь включений:

$$\Phi(\pi_1) \supseteq \ldots \supseteq \Phi(\pi_r). \tag{2.40}$$

9. Для любой цепи подмножеств $\varnothing \subseteq Y_1 \subseteq \ldots \subseteq Y_r \subseteq X$ множества X, содержащейся в решётке 2^X, выполнена цепь включений:

$$\Phi(X) = \Phi_{\varnothing} \supseteq \Phi_{Y_1} \supseteq \ldots \supseteq \Phi_{Y_r} \supseteq \Phi_X = \langle e \rangle. \tag{2.41}$$

Пусть далее множество X образует аддитивную группу.

10. Из замечания 2 к определению 2.24 следует, что

$$\Sigma(X) \subseteq \Phi(|I| \geqslant 1). \tag{2.42}$$

11. Из замечания 1 к определению 2.25 следует, что

$$\Sigma^{\downarrow}(X) \cap \Phi_\theta(X) = \Sigma(X) \cap \Phi_\theta(X), \tag{2.43}$$

где $\Phi_\theta(X)$ — стабилизатор элемента θ в группе подстановок $\Phi(X)$.

12. По утверждению 2.20

$$PA_1(X) \cap \Phi_\theta(X) = \Lambda^{[\nu]}(X) \cap \Phi_\theta(X) \tag{2.44}$$

$$(PA_1^p(X) \cap \Phi_\theta(X) = \Lambda^{[p\nu]}(X) \cap \Phi_\theta(X)). \tag{2.45}$$

13. Из определений 2.28 и 2.29 следует, что

$$QA^p(X) \subseteq PA^p(X) \subseteq PA(X), \tag{2.46}$$

$$QA^p(X) \subseteq QA(X) \subseteq PA(X). \tag{2.47}$$

Некоторые из полученных соотношений можно использовать для определения линейных и аффинных подгрупп в группах подстановок векторного пространства.

ГЛАВА III

ИССЛЕДОВАНИЕ ГРУППОВЫХ ПРИЗНАКОВ ЛИНЕЙНОСТИ И АФФИННОСТИ В ГРУППАХ ПОДСТАНОВОК ВЕКТОРНОГО ПРОСТРАНСТВА

Пусть P^r — векторное пространство размерности r над конечным полем P характеристики p, $|P^r| = q$, $\Phi(P^r)$ — группа всех подстановок пространства P^r и $G < \Phi(P^r)$.

Обозначим через $GL(r, P)$ и $AGL(r, P)$ соответственно полную линейную и полную аффинную группы подстановок пространства P^r. Группу $G \cap GL(r, P)$ обычно называют линейной подгруппой группы G, и группу $G \cap AGL(r, P)$ называют аффинной подгруппой группы G.

Во многих приложениях важной задачей является определение линейной и аффинной подгрупп заданной группы G подстановок пространства P^r. Например, в криптологии шифрование с помощью линейной подстановки считается слабым, так как элементы ключа (или открытого текста) могут быть определены с небольшой вычислительной трудоемкостью при помощи решения системы линейных уравнений.

С целью предотвращения подобной угрозы семейство шифрующих подстановок конструируют таким образом, чтобы либо исключить использование линейных подстановок, либо использовать их настолько редко, чтобы это было не опасно. Такой эффект достигается, как правило, с помощью использования композиций линейных и нелинейных отображений.

Здесь предлагается подход к решению данного класса задач, основанный на определении ряда наследственных подмножеств группы G, каждое из которых содержит линейную (аффинную) подгруппу. Таким образом, линейная (аффинная) подгруппа содержится в пересечении указанных наследственных подмножеств группы G, что позволяет существенно сузить область поиска линейных (аффинных) подстановок группы G, а в ряде случаев — доказать тривиальность линейной (аффинной) подгруппы подстановок.

Некоторые из рассмотренных примеров показывают, что преимуществом такого подхода является относительная простота вычисления наследственных подмножеств по сравнению с тотальной проверкой линейности всех подстановок группы G.

§ 3.1. Об определении линейного признака в группах подстановок векторного пространства

Определение 3.1. Групповой $GL(r, P)$-признак (в группе G) назовём *линейным признаком* (в группе G).

Если $G = \langle S \rangle$, то *показателем линейности группы G в системе образующих S* назовём $\mathrm{pok}_S\, GL(r, P)$; *показателем линейности подстановки g* пространства P^r назовём $\mathrm{pok}_g\, GL(r, P)$. ◇

Теорема 3.1. *Для линейной подгруппы $GL(r, P)$ группы $\Phi(P^r)$ справедливо:*

$$GL(r, P) \subseteq \Phi_\theta \cap U(P^r) \cap \Lambda^{[p\nu]}(P^r) \cap \Sigma(P^r),$$

где θ — ноль пространства P^r и Φ_θ — стабилизатор элемента θ в группе $\Phi(P^r)$, множества $U(P^r)$, $\Lambda^{[p\nu]}(P^r)$ и $\Sigma(P^r)$ суть множества соответственно всех унидоминантных, p-нормально неподвижных и $\bar{\sigma}$-стабильных подстановок пространства P^r.

Доказательство. 1. Так как свойство $g(\theta)=\theta$ выполнено для всякого линейного преобразования g пространства P^r, то

$$GL(r, P) < \Phi_\theta. \tag{3.1}$$

2. По теореме 2 [4] для всякого линейного преобразования g пространства P^r можно указать вектор $\beta \in P^r$, минимальный многочлен которого совпадает с минимальным многочленом преобразования g. Следовательно, период вектора β относительно линейной подстановки g равен порядку n линейной подстановки g, т. е. $l_\beta(g)=n$.

По теореме 18 [6, гл. XI] для подстановки g

$$n = HOK\{l_x(g)\colon x \in P^r\},$$

следовательно, $l_x(g)$ делит $l_\beta(g)$ при любом $x \in P^r$. Это означает, что число $l_\beta(g)$ доминирует во множестве $L(g)$. Следовательно, g — унидоминантная подстановка и

$$GL(r, P) \subseteq U(P^r). \tag{3.2}$$

3. Для любой линейной подстановки g множество $I(g^t)$ непусто (так как содержит элемент θ) и образует подпространство пространства P^r, $t=1, \ldots, n$. Следовательно, $|I_g|(t) \in N^{[p]}$.

Если $\tau, t \in \{1, \ldots, n\}$ и τ/t, то по утверждению 2.9 $I(g^\tau) \subseteq I(g^t)$. Отсюда и из включений $|I(g^t)| \in N^{[p]}$ и $|I(g^\tau)| \in N^{[p]}$ следует, что для функции $\eta_g(t, \tau)$, определённой равенством (2.19), выполнено включение $\eta_g(t, \tau) \in N^{[p]}$ при любых $\tau, t \in \{1, \ldots, n\}$ таких, что τ/t. Следовательно, по предложению 3 утверждения 2.12 $g \in \Lambda^{[p\nu]}(P^r)$. Отсюда получаем:

$$GL(r, P) \subseteq \Lambda^{[p\nu]}(P^r). \tag{3.3}$$

4. Пусть g — линейная подстановка пространства P^r и $\pi(g)=(X_1, \ldots, X_k)$. Рассмотрим произвольный вектор x пространства P^r, без ограничения общности можно считать, что $x \in X_1$, где $|X_1|=l$. Тогда

$$\sigma(X_1) = x + g(x) + \ldots + g^{l-1}(x),$$

и из линейности подстановки φ получаем:

$$g(\sigma(X_1)) = g(x) + g^2(x) + \ldots + g^l(x).$$

По условию $g^l(x)=x$, значит, $g(\sigma(X_1))=\sigma(X_1)$. Следовательно, $\sigma(X_1) \in I(g)$. В силу произвольности рассмотренного вектора x отсюда получаем, что $\bar{\sigma}(g) \subseteq I(g)$ для любой линейной подстановки g. Так как циклическая группа $\langle g \rangle$ состоит из линейных подстановок, то для любой линейной подстановки g выполнено включение:

$$\langle g \rangle \subseteq \Phi(\bar{\sigma} \subseteq I).$$

Отсюда по определению 2.24 получаем, что любая линейная подстановка является $\bar{\sigma}$-стабильной. Следовательно,

$$GL(r, P) \subseteq \Sigma(P^r). \tag{3.4}$$

Таким образом, из включений (3.1)–(3.4) следует теорема 3.1. □

Следствие 1. *Линейная подгруппа $G\cap GL(r, P)$ группы подстановок G содержится в пересечении трёх наследственных подмножеств стабилизатора G_θ элемента θ в группе G, обладающих соответственно U-признаком, $\Lambda^{[p\nu]}$-признаком и Σ-признаком:*

$$G\cap GL(r, P)\subseteq G_\theta\cap(G\cap U(P^r))\cap(G\cap\Lambda^{[p\nu]}(P^r))\cap(G\cap\Sigma(P^r)). \quad (3.5)$$

Доказательство. Из теоремы 3.1 следует, что

$$G\cap GL(r, P)\subseteq(G\cap\Phi_\theta)\cap(G\cap U(P^r))\cap(G\cap\Lambda^{[p\nu]}(P^r))\cap(G\cap\Sigma(P^r)),$$

при этом $G\cap\Phi_\theta=G_\theta$. □

Следствие 2. *Если в нетривиальной группе G тривиален хотя бы один из трёх признаков: G_θ-признак, $\Lambda^{[p\nu]}(P^r)$-признак, $\Sigma(P^r)$-признак, или пересечение любых m признаков из множества $\{G_\theta, \Lambda^{[p\nu]}(P^r), \Sigma(P^r)\}$, где $2\leqslant m\leqslant 4$, то тривиален и линейный признак в группе G.*

Доказательство. Из равенства (3.5) следует, что если тривиально хотя бы одно из трёх множеств: G_θ, $G\cap\Lambda^{[p\nu]}(P^r)$, $G\cap\Sigma(P^r)$, то и линейная группа $G\cap GL(r, P)$ является тривиальной. Заметим, что в силу нетривиальности группы G наследственное множество $G\cap U(P^r)$ не является тривиальным по следствию 1 теоремы 2.3.

Кроме того, из равенства (3.5) следует тривиальность линейной группы $G\cap GL(r, P)$ в случае, если пересечение любых m множеств системы $\{G_\theta, \Lambda^{[p\nu]}(P^r), \Sigma(P^r)\}$, где $2\leqslant m\leqslant 4$, содержит лишь тождественную подстановку. □

Замечание. Если B есть c-базис группы G, то по утверждению 1.8,в) группа G имеет тривиальный линейный признак в том и только в том случае, если для любого $g\in B$ циклическая группа $\langle g\rangle$ имеет тривиальный линейный признак. ◇

Теорема 3.2. *Пусть элемент θ пространства P^r принадлежит циклу длины l подстановки g, и $g'=g^l$. Тогда линейная подгруппа циклической группы $\langle g\rangle$ порождается элементом $(g')^t$, где t есть делитель числа $\frac{n}{l}$, кратный хотя бы одному из чисел множества* $\mathrm{prm}\{HOK(\tau_1, \tau_2, \tau_3)\}^*$, *где $\tau_1\in\Pi(U, g')$, $\tau_2\in\Pi(\Lambda^{[p\nu]}, g')$, $\tau_3\in\Pi(\Sigma, g')$.*

Доказательство. По следствию 1 теоремы 3.1

$$\langle g\rangle\cap GL(r, P)\subseteq\langle g\rangle_\theta\cap U(P^r)\cap\Lambda^{[p\nu]}(P^r)\cap\Sigma(P^r), \quad (3.6)$$

где по теореме 2.13,а) $\langle g\rangle_\theta=\langle g^l\rangle=\langle g'\rangle$. Значит, линейная подгруппа циклической группы $\langle g\rangle$ есть подгруппа стабилизатора $\langle g\rangle_\theta$, содержащаяся в его наследственном подмножестве $\langle g\rangle_\theta\cap H$ при $H=U(P^r)\cap\Lambda^{[p\nu]}(P^r)\cap\Sigma(P^r)$.

Следовательно, группа $\langle g\rangle\cap GL(r, P)$ порождается элементом $(g')^t$, где по теореме 1.5,а) число t делит $\mathrm{ord}(\langle g\rangle_\theta)$, равный $\frac{n}{l}$, и из равенства (1.6) следует, что число t кратно хотя бы одному из (H, g')-пороговых чисел.

По следствию 2 теоремы 1.6 множество $\Pi(H, g')$ определено выражением:

$$\Pi(H, g')=\mathrm{prm}\{HOK(\tau_1, \tau_2, \tau_3)\}^*,$$

где $\tau_1\in\Pi(U, g')$, $\tau_2\in\Pi(\Lambda^{[p\nu]}, g')$, $\tau_3\in\Pi(\Sigma, g')$. □

Следствие 1. *В условиях теоремы 3.2 циклическая группа $\langle g\rangle$ имеет тривиальный линейный признак, если выполнено любое из двух условий:*

а) $l=\mathrm{ord}\, g$;

б) $l < \operatorname{ord} g$ *и* $HOK(\tau_1, \tau_2, \tau_3) = \operatorname{ord} g'$ *для любых чисел* $\tau_1 \in \Pi(U, g')$, $\tau_2 \in \Pi(\Lambda^{[p^\nu]}, g')$, $\tau_3 \in \Pi(\Sigma, g')$.

Доказательство. Из равенства (3.6) следует, что для тривиальности линейного признака в циклической группе $\langle g \rangle$ достаточно, чтобы либо был тривиален стабилизатор $\langle g \rangle_\theta$, либо нетривиальный стабилизатор $\langle g \rangle_\theta$ имел бы тривиальный H-признак, где $H = U(P^r) \cap \Lambda^{[p^\nu]}(P^r) \cap \Sigma(P^r)$.

Из замечания к определению 2.22 следует, что тривиальность стабилизатора $\langle g \rangle_\theta$ в группе $\langle g \rangle$ равносильна совпадению порядка группы $\langle g \rangle$ с порядком орбиты элемента θ в группе $\langle g \rangle$, т. е. равенству $l = \operatorname{ord} g$. Следовательно, при условии а) линейный признак в циклической группе $\langle g \rangle$ является тривиальным.

В силу наследственности H-признака его тривиальность в стабилизаторе $\langle g \rangle_\theta$ равносильна (см. следствие 2 теоремы 1.5) равенству $\Pi(H, g') = \{\operatorname{ord} g'\}$. Из следствия 2 теоремы 1.6 получаем, что это равенство выполнено тогда и только тогда, когда $HOK(\tau_1, \tau_2, \tau_3) = \operatorname{ord} g'$ для любых чисел $\tau_1 \in \Pi(U, g')$, $\tau_2 \in \Pi(\Lambda^{[p^\nu]}, g')$, $\tau_3 \in \Pi(\Sigma, g')$. Следовательно, при условии б) линейный признак в группе $\langle g \rangle$ тривиален. □

Следствие 2. *Если* $g \notin GL(r, P)$, *то циклическая группа* $\langle g \rangle$ *имеет квазиполный линейный признак тогда и только тогда, когда группа* $\langle g \rangle$ *примарна (*n *есть степень простого числа* v*) и* $g^v \in GL(r, P)$.

Доказательство вытекает непосредственно из следствия утверждения 1.11.

Пример 3.1. Циклическая группа $\langle g \rangle$ имеет тривиальный линейный признак, если:

а) g — нелинейная подстановка и $\operatorname{ord} g$ — простое число;

б) g — полноцикловая подстановка;

в) g — нелинейная подстановка с редукцией цикловой структуры $L(g) = \{1, q-1\}$, где $g(\theta) \neq \theta$.

Тривиальность линейного признака в циклической группе $\langle g \rangle$ следует:

– в случае а) — из следствия теоремы 1.2;

– в случаях б) и в) — из тривиальности стабилизатора $\langle g \rangle_\theta$ по следствию 1,а) теоремы 3.2.

В случае в) порядок циклической группы $\langle g \rangle$ равен $q-1$. Такая группа порождается нелинейной подстановкой g, подобной линейной подстановке g' максимального периода (равного $q-1$). Для построения порождающей подстановки g достаточно взять нелинейную подстановку δ со свойством $\delta(\theta) \neq \theta$ и положить: $g = \delta^{-1} \cdot g' \cdot \delta$. ◇

Пример 3.2. Определим линейную подгруппу циклической группы $\langle g \rangle$, где g — подстановка пространства V_7 двоичных векторов, для которой $g(\theta) = \theta$ и цикловая структура имеет вид: $C(g) = (1^{51}, 6, 15, 21, 35)$.

В этом случае $L(g) = (1, 6, 15, 21, 35)$, $\operatorname{ord} g = 210$ и стабилизатор $\langle g \rangle_\theta = \langle g \rangle$. Следовательно, $U(V_7) \cap \Lambda^{[2\nu]}(V_7) \cap \Sigma(V_7)$-признак в группе $\langle g \rangle_\theta$ совпадает с $U(V_7) \cap \Lambda^{[2\nu]}(V_7) \cap \Sigma(V_7)$-признаком в группе $\langle g \rangle$. Для определения множества $\Pi(\Lambda^{[p^\nu]}, g)$ вычислим для данной подстановки таблицу, аналогичную табл. 2.3.

Таблица 3.1

Характеристики D-диаграммы функции $|I_g|(t)$

Номер яруса	вершина $t/\lvert I_g\rvert(t)$					
0	210/128					
1	105/122	70/86	42/78	30/72		
2	35/86	21/72	15/66	14/51	10/51	6/57
3	7/51	5/51	3/51	2/51		
4	1/51					

Из данной таблицы определяем, что все дуги D-диаграммы, инцидентные вершине 210, не являются 2-нормальными. Значит, по следствию 3 теоремы 2.10 циклическая группа $\langle g\rangle$ имеет тривиальный $\Lambda^{[2\nu]}$-признак.

Отсюда получаем по следствию 2 теоремы 3.1, что циклическая группа $\langle g\rangle$ имеет тривиальную линейную подгруппу. ◇

§ 3.2. Об определении аффинного признака в группах подстановок векторного пространства

Определение 3.2. Групповой $AGL(r, P)$-признак (в группе G) назовём *аффинным признаком* (в группе G).

Если $G = \langle S\rangle$, то *показателем аффинности группы G в системе образующих S* назовём $\mathrm{pok}_S\, AGL(r, P)$; *показателем аффинности подстановки g* пространства P^r назовём $\mathrm{pok}_g\, AGL(r, P)$. ◇

Лемма 3.1. *Пусть аффинная подстановка g пространства P^r, где* $\mathrm{ord}\, g = n$, *имеет вид*

$$g(x) = \varphi(x) + \alpha, \tag{3.7}$$

где φ есть линейная подстановка порядка m и вектор α принадлежит циклу длины l подстановки g. Тогда m есть делитель числа n, кратный $\mathrm{mp}_n(l)$, *и подстановка g является псевдоаффинной индекса* $\frac{n}{m}$.

Доказательство. Методом математической индукции несложно вывести из равенства (3.7) формулу для степеней подстановки g:

$$g^t(x) = \varphi^t(x) + g^t(\theta), \tag{3.8}$$

где $g^t(\theta) = \alpha + \varphi(\alpha) + \ldots + \varphi^{t-1}(\alpha)$, $t = 1, \ldots, n$. Отсюда следует, что $g^t = e$ тогда и только тогда, когда $\varphi^t = e$ и $g^t(\theta) = \theta$, т. е. t кратно длине l_θ цикла подстановки g, которому принадлежит вектор θ. Следовательно, $n = HOK(m, l_\theta)$.

Вместе с тем, $l_\theta = l$ в силу равенства $g(\theta) = \alpha$, вытекающего из (3.7) при $x = \theta$. Значит, $n = HOK(m, l)$. Отсюда получаем, что m есть делитель числа n, кратный $\mathrm{mp}_n(l)$.

Из определения множества $\Delta_\alpha(g)$ (см. п. 2.6.3) следует, что для аффинной подстановки g включение $x \in \Delta_\alpha(g)$ выполнено тогда и только тогда, когда $x \in I(\varphi)$. Следовательно, для аффинной подстановки g таблица функции $\bar{\rho}_g$ (см. формулу (2.26) и комментарий к ней) имеет вид:

$$\bar{\rho}_g = (|I_\varphi|(1), \ldots, |I_\varphi|(n)), \tag{3.9}$$

Отсюда получаем, что таблица функции $\bar{\rho}_g$ есть периодическая последовательность с наименьшим периодом m, так как $|I_\varphi|(t)=|P^r|$ тогда и только тогда, когда t кратно m. Следовательно, по определению 2.26 функция $\bar{\rho}_g$ является регулярной индекса $\frac{n}{m}$.

Из равенства (3.9) следует также, что ограничение функции $\bar{\rho}_g$ на множество подстановок $\{g, \ldots, g^m\}$ есть таблица функции $|I_\varphi|(t)$, которая, как показано в теореме 3.1 для любой линейной подстановки φ, является p-антинормальной. Значит, по определению 2.27 функция $\bar{\rho}_g$ является p-псевдоантинормальной индекса $\frac{n}{m}$. Следовательно, по определению 2.28 подстановка g пространства P^r является p-псевдоаффинной индекса индекса $\frac{n}{m}$. □

Теорема 3.3. *Для аффинной подгруппы $AGL(r, P)$ группы $\Phi(P^r)$ справедливо:*

$$AGL(r, P) \subseteq \Sigma^{\downarrow}(P^r) \cap QA^p(P^r),$$

где $\Sigma^{\downarrow}(P^r)$ и $QA^p(P^r)$ суть множества соответственно всех $\bar{\sigma}$-смещённых и всех p-квазиаффинных подстановок пространства P^r.

Доказательство. Пусть g — аффинная подстановка пространства P^r и $\pi(g)=(X_1, \ldots, X_k)$. Рассмотрим произвольный вектор x пространства P^r, без ограничения общности можно считать, что $x \in X_1$, где $|X_1|=l$. Тогда из равенства (3.6), используя линейность подстановки φ, получаем:

$$\begin{gathered} g(\sigma(X_1)) = \varphi(x + g(x) + \ldots + g^{l-1}(x)) + \alpha = \\ = \varphi(x) + \varphi(g(x)) + \ldots + \varphi(g^{l-1}(x)) + \alpha = \\ = (\varphi(x) + \alpha) + (\varphi(g(x)) + \alpha) + \ldots + (\varphi(g^{l-1}(x)) + \alpha) + (1-l)\cdot\alpha = \\ = g(x) + g^2(x) + \ldots + g^l(x)) + (1-l)\cdot\alpha. \end{gathered}$$

По условию $g^l(x)=x$, значит,

$$g(\sigma(X_1)) = \sigma(X_1) + (1 - |X_1|)\cdot\alpha.$$

В силу произвольности рассмотренного цикла отсюда получаем по определению 2.25, что любая аффинная подстановка g пространства P^r является $\bar{\sigma}$-смещённой. Следовательно,

$$AGL(r, P) \subseteq \Sigma^{\downarrow}(P^r). \tag{3.10}$$

Из леммы 3.1 следует, что любая аффинная подстановка $g \in PA^p(P^r)$. Отсюда получаем, что все подстановки циклической группы $\langle g \rangle$ принадлежат $PA^p(P^r)$. Следовательно, по определению 2.29 $g \in QA^p(P^r)$.

Отсюда в силу произвольности рассмотренной аффинной подстановки получаем:

$$AGL(r, P) \subseteq QA^p(P^r). \tag{3.11}$$

Из включений (3.10), (3.11) получаем теорему 3.3. □

Следствие 1. *Аффинная подгруппа $G \cap AGL(r, P)$ группы подстановок G содержится в пересечении двух наследственных подмножеств группы G, обладающих соответственно $\Sigma^{\downarrow}$-признаком и QA^p-признаком:*

$$G \cap AGL(r, P) \subseteq (G \cap \Sigma^{\downarrow}(P^r)) \cap (G \cap QA^p(P^r)).\diamondsuit$$

Следствие 2. *Если хотя бы один из двух признаков: $\Sigma^{\downarrow}$-признак, QA^p-признак — или их пересечение является тривиальным в группе G, то тривиален и аффинный признак в группе G.* $\diamondsuit$

Замечание. Если B есть c-базис группы G, то по утверждению 1.8,в) группа G имеет тривиальный аффинный признак в том и только в том случае, если для любого $g \in B$ циклическая группа $\langle g \rangle$ имеет тривиальный аффинный признак. ◇

Теорема 3.4. а) *Аффинная подгруппа циклической группы* $\langle g \rangle$ *порождается элементом* g^t, *где* t *есть делитель числа* n, *кратный хотя бы одному из чисел множества* $\mathrm{prm}\{HOK(\tau, \tau')\}^*$, *где* $\tau \in \Pi(\Sigma^{\downarrow}, g)$, $\tau' \in \Pi(QA^p, g)$.

б) *Пусть* $\mathrm{pok}_g\, GL(r, P) = v$, $\mathrm{pok}_g\, AGL(r, P) = w$ *и* l_θ — *длина цикла подстановки* g, *которому принадлежит вектор* θ. *Тогда* w *есть делитель числа* v, *кратный* $\mathrm{mp}_v(l_\theta)$.

Доказательство. а) По следствию 1 теоремы 3.3

$$\langle g \rangle \cap AGL(r, P) \subseteq (\langle g \rangle \cap \Sigma^{\downarrow}(P^r)) \cap (\langle g \rangle \cap QA^p(P^r)) \qquad (3.12)$$

Значит, аффинная подгруппа циклической группы $\langle g \rangle$ содержится в наследственном подмножестве $\langle g \rangle \cap H$ при $H = \Sigma^{\downarrow}(P^r) \cap QA^p(P^r)$.

Следовательно, группа $\langle g \rangle \cap AGL(r, P)$ порождается элементом g^t, где по теореме 1.5,а) число t делит n и кратно хотя бы одному из (H, g)-пороговых чисел. Осталось заметить, что по следствию 2 теоремы 1.6 множество $\Pi(H, g)$ определяется выражением:

$$\Pi(H, g) = \mathrm{prm}\{HOK(\tau, \tau')\}^*,$$

где $\tau \in \Pi(\Sigma^{\downarrow}, g)$, $\tau' \in \Pi(QA^p, g)$.

б) По теореме 1.2 v/n и w/n, при этом $\mathrm{ord}(\langle g \rangle \cap GL(r, P)) = \frac{n}{v}$ и $\mathrm{ord}(\langle g \rangle \cap AGL(r, P)) = \frac{n}{w}$. Так как выполнено теоретико-групповое включение $\langle g \rangle \cap GL(r, P) < \langle g \rangle \cap AGL(r, P)$, то по теореме Лагранжа получаем, что w/v.

Из равенства (3.7) следует, что t-я степень аффинной подстановки g является линейной подстановкой тогда и только тогда, когда t кратно l_θ. Следовательно, $v = HOK(w, l_\theta)$. Отсюда w есть делитель числа v, кратный $\mathrm{mp}_v(l_\theta)$. □

Следствие 1. а) *Если циклическая группа* $\langle g \rangle$ *имеет тривиальный аффинный признак, то она имеет и тривиальный линейный признак.*

б) *Если* $g(\theta) = \theta$, *то циклическая группа* $\langle g \rangle$ *имеет тривиальный линейный признак тогда и только тогда, когда она имеет тривиальный аффинный признак.*

в) *Если* $HOK(\tau, \tau') = n$ *для любых чисел* $\tau \in \Pi(\Sigma^{\downarrow}, g)$ *и* $\tau' \in \Pi(QA^p, g)$, *то циклическая группа* $\langle g \rangle$ *имеет тривиальный аффинный признак.*

Доказательство. а) Утверждение следует из теоретико-групповых включений: $\langle e \rangle < \langle g \rangle \cap GL(r, P) < \langle g \rangle \cap AGL(r, P)$.

б) Если $g(\theta) = \theta$, то из равенства (3.8) следует, что линейная и аффинная подгруппы группы $\langle g \rangle$ совпадают.

в) Из равенства (3.12) следует, что аффинный признак в циклической группе $\langle g \rangle$ тривиален, если тривиален H-признак, где $H = \Sigma^{\downarrow}(P^r) \cap QA^p(P^r)$. В силу наследственности H-признака его тривиальность в группе $\langle g \rangle$ равносильна (см. следствие 2 теоремы 1.5) равенству $\Pi(H, g) = \{n\}$. Из следствия 2 теоремы 1.6 получаем, что это равенство выполнено тогда и только тогда, когда $HOK(\tau, \tau') = n$ для любых чисел $\tau \in \Pi(\Sigma^{\downarrow}, g)$ и $\tau' \in \Pi(QA^p, g)$. □

Следствие 2. *Циклическая группа* $\langle g \rangle$, *порождённая нелинейной подстановкой* g, *имеет квазиполный аффинный признак тогда и*

только тогда, когда группа $\langle g\rangle$ *примарна* (n *есть степень простого числа* w) *и* $g^w \in AGL(r, P)$.

Доказательство вытекает непосредственно из следствия утверждения 1.11.

Замечание. Если g — нелинейная подстановка пространства P^r и $\operatorname{ord} g$ — простое число, то из следствия теоремы 1.2 получаем, что циклическая группа $\langle g\rangle$ имеет тривиальный аффинный признак. ◇

Заключение

Основные результаты работы состоят в следующем.

1. Предложен общий подход к дифференциации конечных групп и их элементов по подмножеству элементов конечной группы, обладающих тем или иным заданным признаком.

С использованием данного подхода можно изучать, в частности, многие типы слабостей криптографических отображений в различных криптосистемах. Многообразие возможных направлений развития предложенного подхода для решения задач криптологии выходит за рамки исследований слабостей криптографических отображений, связанных с различными свойствами их нелинейности [13].

2. Исследована величина $\operatorname{pok}_S H$, характеризующая сложность порождения в системе образующих S хотя бы одного элемента множества H (элемента с признаком H). Получены оценки $\operatorname{pok}_S H$ через характеристики графа Кэли группы $\langle S\rangle$ и матрицы смежности этого графа, а также через величины $\operatorname{pok}_g H$, где $g \in S$, и некоторые другие.

3. Исследованы наследственные признаки в конечных группах. Этот класс признаков интересен не только с теоретической, но и с практической точки зрения, так как нередко свойства элемента g группы наследуются всеми элементами циклической группы $\langle g\rangle$.

Для группового признака в группе $\langle S\rangle$, порождённой системой образующих S, уточнено выражение величины $\operatorname{pok}_S H$ через характеристики графа Кэли группы $\langle S\rangle$, получена верхняя оценка величины $\operatorname{pok}_S H$ через индекс $|G\colon (G \cap H)|$. Показано, что эта оценка достижима на классе циклических групп.

Для наследственного признака H в группе $\langle S\rangle$, являющейся прямым произведением нескольких групп, установлены связи величины $\operatorname{pok}_S H$ с аналогичными величинами, соответствующими перемножаемым группам.

Группа G единственным образом представляется в виде несократимого объединения максимальных циклических подгрупп (в виде канонического c-покрытия). С использованием этого свойства показана принципиальная возможность сведения задачи исследования характеристик наследственного признака H в группе G к нескольким менее сложным задачам исследования соответствующих характеристик этого признака в циклических подгруппах группы, образующих её каноническое c-покрытие.

Одной из характеристик сложности реализации такого подхода к изучению наследственного признака H в группе G является величина $h_c(G)$, т. е. c-ширина группы G, равная числу циклических подгрупп в каноническом c-покрытии группы G.

Установлена (и далее использована при исследованиях признаков в группах подстановок) связь между классом наследственных признаков в конечной группе и классом монотонных и антимонотонных функций, заданных на группе.

4. В результате исследования наследственного признака H в циклической группе $\langle g\rangle$ порядка n:

– описано подмножество элементов группы $\langle g\rangle$, обладающих свойством H, через множество (H, g)-пороговых чисел, состоящее из единственного делителя числа n в случае группового признака и в противном случае образующее антицепь в решётке $D(n)$;

– показано, что величина $\mathrm{pok}_g H$ совпадает с наименьшим из (H, g)-пороговых чисел;

– получены условия тривиальности и квазиполноты признака H, а также условия, при которых признак H является групповым;

– показано, что подмножество элементов циклической группы $\langle g\rangle$, порождающих подгруппы с тривиальным наследственным признаком H, образует подгруппу, эта подгруппа описана через множество (H, g)-пороговых чисел.

5. С использованием результатов исследования признаков в конечных группах исследован ряд наследственных признаков в группах подстановок множества X. Эти признаки определены с помощью монотонных и антимонотонных функций, заданных на группе подстановок.

Выделены 3 класса функций, значения которых однозначно определены соответственно:

1) разбиением $\pi(g)$ основного множества X на циклы подстановки g;

2) цикловой структурой $C(g)$ подстановки g;

3) редукцией $L(g)$ цикловой структуры подстановки g.

Таким образом, описание наследственных признаков в циклической группе подстановок $\langle g\rangle$, определяемых функциями первого класса, определяется разбиением $\pi(g)$. Признаки, соответствующие функциям второго класса, описываются с помощью цикловой структуры $C(g)$ подстановки g, и для описания наследственных признаков, определяемых функциями третьего класса, достаточно использовать редукцию $L(g)$ цикловой структуры подстановки g.

Для каждого наследственного признака H в циклической группе $\langle g\rangle$ подстановок описано множество (H, g)-пороговых чисел, получены, как правило, условия тривиальности и квазиполноты признака.

Исследованы наследственные признаки в группе подстановок аддитивной группы.

Установлены теоретико-множественные связи между всеми изученными наследственными признаками.

6. Важным аспектом исследования наследственного признака H в циклической группе $\langle g\rangle$ является вычислительная сложность определения множества (H, g)-пороговых чисел. Для наследственных признаков в циклической группе $\langle g\rangle$ подстановок получены формулы или предложены алгоритмы, с использованием которых вычисляются пороговые числа признаков. В случае $\Lambda^{[\nu]}$-признака ($\Lambda^{[p^\nu]}$-признаков) предложены два алгоритма вычисления $(\Lambda^{[\nu]}, g)$-пороговых ($(\Lambda^{[\nu]}, g)$-пороговых) чисел. Исходной информацией первого алгоритма является диаграмма решётки $D(n)$, вершина t которой помечена числом $|I(g^t)|$ неподвижных элементов подстановки g^t.

С целью сокращения трудоёмкости вычислений построен гомоморфизм решёток $D(n) \to \lceil L\rceil_1$, с использованием которого второй алгоритм существенную часть вычислений выполняет на более компактной диаграмме решётки $\lceil L\rceil_1$, вершина t которой также помечена числом $|I(g^t)|$. Указан класс подстановок, для которых построенный гомоморфизм решёток существенно упрощает вычисление $(\Lambda^{[\nu]}, g)$-пороговых ($(\Lambda^{[\nu]}, g)$-пороговых) чисел.

7. Результаты исследования наследственных признаков в группах подстановок использованы для исследования характеристик линейного и аффинного признаков в группе G подстановок r-мерного векторного пространства P^r над конечным полем P.

Доказано, что линейная подгруппа $G \cap GL(r, P)$ (аффинная подгруппа $G \cap AGL(r, P)$) группы G, где $GL(r, P)$ и $AGL(r, P)$ — соответственно группы всех линейных и аффинных подстановок пространства P^r, включена в пересечение четырёх (двух) подмножеств группы G, определяемых конкретными наследственными признаками в группе G. Вычисление характеристик этих признаков позволяет во многих случаях существенно упростить определение линейной и аффинной подгрупп группы G, а в ряде случаев — доказать их тривиальность.

Получены критерий квазиполноты и достаточные условия тривиальности линейного и аффинного признаков в циклической группе подстановок пространства P^r.

8. Из нерешённых проблем исследования признаков в конечных группах наиболее актуальными представляются следующие:

1) распространение предложенного подхода к исследованию признаков с конечных групп на конечные полугруппы;

2) оценка c-ширины для различных классов групп и полугрупп;

3) исследование свойств c-базисов групп (полугрупп), в частности, связи c-базисов с системой образующих элементов группы (полугруппы);

4) улучшение в различных частных случаях данной в утверждении 1.2 оценки $\mathrm{pok}_g H$ через какие-либо характеристики системы S образующих элементов группы, где S состоит из двух и более элементов;

5) исследование структур различных преобразований пространства над конечным полем с целью выявления и описания новых наследственных признаков в группах подстановок и в полугруппах преобразований;

6) исследование вычислительной сложности определения различных характеристик признаков в группе (полугруппе);

7) исследование характеристик признаков в группе неавтономного регистра сдвига.

СПИСОК ЛИТЕРАТУРЫ

1. Берж К. Теория графов и её применение. — М.: ИЛ, 1962.
2. Биркгоф Г. Теория решёток. — М.: Наука, 1984.
3. Виноградов И. М. Основы теории чисел. — М.: Наука, 1972.
4. Гантмахер Ф. Р. Теория матриц. — 4-е изд. — М.: Наука, 1988.
5. Глухов М. М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // «Труды по дискретной математике». — Т. 1. — М.: ТВП, 1997. — С. 43–66.
6. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. — Т. 1. — М.: Гелиос-АРВ, 2003.
7. Гретцер Г. Общая теория решёток. — М.: Мир, 1982.
8. Гроссман И., Магнус В. Группы и их графы. — М.: Мир, 1971.
9. Дискретная математика и математические вопросы кибернетики. — Т. 1. — М.: Наука, 1974.
10. Князев А. В. О диаметрах псевдосимметрических графов // Мат. заметки. — 1987. — Т. 41, № 6, — С. 829–843.
11. Кострикин А. И. Введение в алгебру. Ч.III. Основные структуры алгебры. — М.: Физматлит, 2000.
12. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.
13. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.
14. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. — М.: Наука, 1974.
15. Струнков С. П. Введение в теорию линейных представлений конечных групп. — М.: МИФИ, 1993.
16. Фомичёв В. М. Дискретная математика и криптология. — М.: ДИАЛОГ-МИФИ, 2003.
17. Харари Ф. Теория графов. — М.: Мир, 1973.
18. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003.

19. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: ТРИУМФ, 2002.
20. Konheim A. Cryptography: A Primer. — N. Y.: John Wiley & Sons, 1981.
21. Rueppel R. A. Analysis and design of stream ciphers. — Berlin: Springer Verlag, 1986.

Поступило в редакцию 7 VI 2005