МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. П. Г. ДЕМИДОВА

Кафедра компьютерной безопасности и
математических методов обработки информации

В. Г. Дурнев, О. В. Зеткина

МЕТОДЫ КОМБИНАТОРНОЙ ТЕОРИИ ГРУПП В СОВРЕМЕННОЙ КРИПТОГРАФИИ

Учебно-методическое пособие

ЯРОСЛАВЛЬ
ЯрГУ
2017

УДК 519.1:003.26(072)
ББК 3973.2-018.2я73
Д 84

Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2017 года

Рецензент
кафедра компьютерной безопасности
и математических методов обработки информации

Дурнев, Валерий Георгиевич

Д 84 Методы комбинаторной теории групп в современной криптографии : учеб.-метод. пособие / В. Г. Дурнев, О. В. Зеткина ; Яросл. гос. ун-т. им. П. Г. Демидова. – Ярославль : ЯрГУ, 2017. – 52 с.

В пособии излагаются основные понятия комбинаторной теории групп, необходимые для реализации криптопротоколов, базирующихся на группах.

Пособие предназначено для студентов, обучающихся по специальности “Компьютерная безопасность”. Оно может быть использовано при изучении дисциплин “Криптографические методы защиты информации”, “Модели безопасности компьютерных систем” и “Криптографические протоколы”, а также специальных дисциплин.

Библиогр.: 29 назв.

УДК 519.1:003.26(072)
ББК 3973.2-018.2я73

Оглавление

1. Предисловие

Предлагаемое вниманию читателя пособие – введение в одно из современных направлений математико-криптографических исследований – криптография, базирующаяся на группах (в английской терминологии – *group-based cryptography*) – доступно для студентов, обучающихся по специальности "Компьютерная безопасность".

При написании пособия автор использовал прежде всего классическую монографию по комбинаторной теории групп В. Магнуса, А. Карраса и Д. Солитэра "Комбинаторная теория групп" [8] и монографию Р. Линдона и П. Шуппа "Комбинаторная теория групп" [7].

Описания приводимых в пособии криптографических протоколов базируется на монографии В. А. Романькова "Алгебраическая криптография" [18] и монографиях А. Мясникова, В. Шпильрайна и А. Ушакова (Myasnikov A., Shpilrain V., Ushakov A.) "Non-commutative cryptography and complexity of group-theoretic problems" [28] и "Group-based cryptography. Advances courses in Math" [27].

Кроме того, в той или иной мере использовались включенные в список литературы работы различных авторов. Всем им, как и тем, чьи работы не вошли в список литературы, однако оказали идейное влияние на формирование взглядов автора на предмет, мы выражаем искреннюю благодарность и признательность. Входящий в пособие материал по комбинаторной теории групп можно считать, в основном, уже достаточно устоявшимся, ставшим общематематическим достоянием, хотя время от времени и появляются как новые работы, так и оригинальные доказательства известных в этой области теорем.

О содержании пособия можно понять по его оглавлению. Приведем лишь его краткий обзор.

В начальных параграфах излагается базовый материал по комбинаторной теории групп – задание групп образующими и определяющими соотношениями. Описывается построение фундаментальной группы топологического пространства. Рассматриваются важные для дальнейшего группы – группы узлов и кос. Обсуждается вопрос о нахождении задания подгрупп и факторгрупп по заданиям групп. Завершается начальная часть пособия обсуждением фундаментальной теоремы топологии и комбинаторной теории групп – классической теореме Зейферта – ван Кампена.

Представлены некоторые основные современные криптографические протоколы, базирующиеся на группах и групповых кольцах.

Продолжение пособия будет посвящено доказательству фундаментальных теорем комбинаторной теории групп – классической теоремы П. С. Новикова об алгоритмической неразрешимости "Проблемы равенства в теории групп" ("Проблемы эквивалентности слов", "Проблемы тождества") и классической теоремы С. И. Адяна – М. Рабина об алгоритмической неразрешимости "Проблемы распознаваемости свойств в теории групп".

“Килиманджаро – покрытый вечными снегами
горный масив высотой в 19710 футов, как
говорят, высшая точка Африки. Племя масаи
называет его западный пик “Нгайэ-Нгайя”,
что значит “Дом бога”.
Почти у самой вершины западного пика лежит
иссохший мерзлый труп леопарда.
Что понадобилось леопарду на такой высоте,
никто объяснить не может”.
Э. Хемингуэй. “Снега Килиманджаро”.

“ Фактор Мэлори”. “Отвечая на вопрос
“Нью-Йорк таймс”, почему ему так хочется
забраться на Эверест, Джордж Мэлори ответил:
“ Потому, что она есть””

“Обучение редко приносит плоды кому-либо, кроме тех,
кто предрасположен к нему, но им оно почти не нужно”.
Гиббонс.

2. Задание групп образующими и определяющими соотношениями

В 1882–1883 гг. Вальтером фон Диком был предложен “конструктивный” способ задания групп – *задание групп образующими элементами и определяющими соотношениями*. Такое задание групп естественным образом возникает в топологии как способ задания фундаментальных групп некоторых топологических пространств.

Но начнем мы с более общего понятия – понятия ***полусистемы Туэ***, введенного норвежским математиком Акселем Туэ в 1914 году.

Пусть $\mathcal{A} = \{a_1, \ldots, a_n\}$ – произвольный конечный алфавит. Зафиксируем некоторый конечный набор упорядоченных пар слов $\langle A_1, B_1\rangle$, ..., $\langle A_m, B_m\rangle$ в этом алфавите. С каждой парой $\langle A_i, B_i\rangle$ свяжем *элементарное преобразование* слов в алфавите $\mathcal{A}$ – переход вида

$$UA_iV \longrightarrow UB_iV,$$

где U и V – произвольные слова в алфавите $\mathcal{A}$. Саму упорядоченную пару слов $\langle A_i, B_i\rangle$ традиционно обозначают в виде $A_i \to B_i$. Полученный объект обозначается в виде

$$\langle\, a_1, \ldots, a_n \,|\, A_1 \to B_1, \ldots, A_m \to B_m \,\rangle$$

и называется ***полусистемой Туэ***, или *системой полу-Туэ*, и будет обозначаться через SST. При этом $\mathcal{A} = \{a_1, \ldots, a_n\}$ называется *алфавитом полусистемы* SST, а $A_1 \to B_1$, ..., $A_m \to B_m$ – ее *системой подстановок*.

Основным понятием для полусистем Туэ является ***понятие выводимости***.

Пусть W и U – слова в алфавите полусистемы Туэ

$$SST = \langle\, a_1, \ldots, a_n \,|\, A_1 \to B_1, \ldots, A_m \to B_m \,\rangle.$$

Слово U называется ***выводимым*** из слова W, если существует последовательность элементарных преобразований

$$W = W_0 \to W_1 \to \ldots \to W_k \to W_{k+1} \to \ldots \to W_s = U,$$

переводящая слово U в слово W.

В ***проблеме выводимости для полусистем Туэ***, сформулированной А. Туэ в 1914 году, требуется разработать общий метод, позволяющий по любым двум словам W и U в алфавите полусистемы Туэ SST определить, выводимо ли слово U из слова W.

Аксель Туэ (19.02.1863 – 7.03.1922) – норвежский математик. Ему принадлежат важные результаты в теории чисел, диофантовом анализе и разработке метода тригонометрических сумм. Широкую известность получили метод Туэ в теории диофантовых приближений, теорема Туэ – Зигеля – Рота, теорема Туэ о конечности числа целочисленных решений однородного диофантова уравнения с двумя неизвестными и системы Туэ.

Рассмотрим введенный Вальтером фон Диком в 1882–1883 гг. способ *задания групп образующими элементами и определяющими соотношениями*. Как уже отмечалось выше, такой способ задания групп возникает естественным образом в топологии как способ задания фундаментальных групп некоторых топологических пространств. Более подробно мы это рассмотрим позже.

Пусть $\mathcal{A} = \{a_1, \ldots, a_n\}$ – произвольный конечный алфавит. Введем алфавит букв-двойников $\mathcal{A}^{-1} = \{a_1^{-1}, \ldots, a_n^{-1}\}$. Объединение $\mathcal{A} \cup \mathcal{A}^{-1}$ этих алфавитов будем называть *групповым алфавитом*.

Зафиксируем некоторый конечный набор упорядоченных пар слов $\langle A_1, B_1\rangle$, ..., $\langle A_m, B_m\rangle$ в этом групповом алфавите. С каждой парой $\langle A_i, B_i\rangle$ свяжем два *элементарных преобразования* слов в групповом алфавите $\mathcal{A} \cup \mathcal{A}^{-1}$ – переходы вида

$$UA_iV \longrightarrow UB_iV, \quad UB_iV \longrightarrow UA_iV,$$

где U и V – произвольные слова в групповом алфавите.

К этим элементарным преобразованиям добавим так называемые *тривиальные элементарные преобразования* слов в групповом алфавите $\mathcal{A} \cup \mathcal{A}^{-1}$ – переходы вида

$$Ua_i^{\varepsilon}a_i^{-\varepsilon}V \longrightarrow UV, \quad UV \longrightarrow Ua_i^{\varepsilon}a_i^{-\varepsilon}V,$$

где U и V – произвольные слова в групповом алфавите, а $\varepsilon \in \{-1, 1\}$. Преобразования первого вида называются *сокращениями*, а второго – *вставками*.

Саму упорядоченную пару слов $\langle A_i, B_i \rangle$ традиционно обозначают в виде $A_i = B_i$. Полученный объект обозначается в виде

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle,$$

и он будет служить заданием некоторой группы, которая будет обозначаться тем же способом. При этом a_1, ..., a_n называются *образующими элементами* этой группы, а $A_1 = B_1$, ..., $A_m = B_m$ – ее *определяющими соотношениями*.

Для построения этой группы используем отношение выводимости слов.

Как и в случае полусистем Туэ, слово U называется *выводимым* из слова W (обозначается $W \vdash^* U$), если существует последовательность элементарных преобразований

$$W = W_0 \to W_1 \to \ldots \to W_k \to W_{k+1} \to \ldots \to W_s = U,$$

переводящая слово U в слово W.

Нетрудно показать, что отношение выводимости $\vdash^*$ в рассматриваемом случае является отношением эквивалентности, т. е. оно рефлексивно, транзитивно и симметрично. Соответствующие классы эквивалентности будем обозначать через $[W]$.

На множестве классов эквивалентности естественным образом определяется умножение равенством

$$[W] \cdot [U] = [WU],$$

где WU – обычное произведение (сочленение, конкатенация) слов W и U.

Нетрудно проверить, что множество классов эквивалентности относительно введенной операции умножения является группой. При этом роль нейтрального элемента выполняет класс $[1]$, где через 1 обозначено пустое слово, а элементом, обратным к $[W]$, является $[\overline{W}]$, где

$$\overline{a_{i_1}^{\varepsilon_1} \ldots a_{i_t}^{\varepsilon_t}} = a_{i_t}^{-\varepsilon_t} \ldots a_{i_1}^{-\varepsilon_1}.$$

Построенная группа обозначается через

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle$$

и называется *группой, заданной образующими элементами* a_1, ..., a_n и *определяющими соотношениями* $A_1 = B_1$, ..., $A_m = B_m$.

Если некоторая группа G изоморфна построенной группе, то говорят, что *группа G имеет задание (генетический код, копредставление)*

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle.$$

Например, симметрическая группа S_3 имеет задание

$$\langle\langle\, a, b \,|\, a^3 = 1,\, b^2 = 1, ba = a^2 b \,\rangle\rangle,$$

Группа $SL(2,Z)$ целочисленных матриц второго порядка с определителем, равным единице, имеет задание

$$\langle\langle\, a, b \,|\, a^6 = 1,\, b^4 = 1, a^3 = b^2 \,\rangle\rangle,$$

а ее факторгруппа по центру $PSL(2,Z)$ (проективная специальная целочисленная группа матриц второго порядка) имеет задание

$$\langle\langle\, a, b \,|\, a^3 = 1,\, b^2 = 1 \,\rangle\rangle.$$

Заметим, что группа кос на трех нитях и группа узла клеверный лист (трилистник) имеют одно и то же задание:

$$\langle\langle\, a, b \,|\, a^3 = b^2 \,\rangle\rangle.$$

В связи с рассмотренным способом задания групп М. Дэн в работе 1911 года [21] сформулировал три алгоритмические проблемы, получившие название *фундаментальные проблемы М. Дэна –* ***проблему тождества***, ***проблему сопряженности*** и ***проблему изоморфизма***.

Проблема тождества. *Требуется разработать общий метод (алгоритм), позволяющий по любому заданию группы*

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle$$

и по любым двум (групповым) словам W и U в этих образующих определить, равны ли элементы $[W]$ и $[U]$, т. е. можно ли из слова W вывести слово U, пользуясь указанными определяющими соотношениями и тривиальными соотношениями.

Проблема сопряженности. *Требуется разработать общий метод (алгоритм), позволяющий по любому заданию группы*

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle$$

и по любым двум (групповым) словам W и U в этих образующих определить, сопряжены ли элементы $[W]$ и $[U]$, т. е. найдется ли такое слово Z, что $[Z]^{-1}[W][Z] = [U]$ (можно ли из слова $\overline{Z}WZ$ вывести слово U, пользуясь указанными определяющими соотношениями и тривиальными соотношениями).

Проблема изоморфизма. *Требуется разработать общий метод (алгоритм), позволяющий по любым двум заданиям*

$$\langle\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle\rangle$$

и

$$\langle\langle\, b_1, \ldots, b_p \,|\, C_1 = D_1, \ldots, C_q = D_q \,\rangle\rangle$$

определить, будут ли изоморфны соответствующие группы.

Первые две проблемы были сформулированы М. Дэном в предыдущей работе 1910 года, а третью проблему можно обнаружить в работе Х. Титце 1908 года, но не выделенную там специально. Однако особое внимание этим проблемам было уделено именно в работе М. Дэна 1911 года, которая начинается с формулировки этих трех проблем.

Заметим, что в проблемах М. Дэна речь фактически шла о построении соответствующих разрешающих алгоритмов. Вопрос же о существовании самих алгоритмов в те годы еще не возникал. Позже было установлено, что для аналогичных алгоритмических проблем соответствующие алгоритмы не существуют, поэтому *фундаментальные проблемы М. Дэна* - – ***проблема тождества***, ***проблема сопряженности*** и ***проблема изоморфизма*** - могут быть переформулированы следующим образом.

Проблема тождества. *По любому заданию группы*

$$\langle\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle\rangle$$

и по любым двум (групповым) словам W и U в этих образующих определить, равны ли элементы $[W]$ и $[U]$, т. е. можно ли из слова W вывести слово U, пользуясь указанными определяющими соотношениями и тривиальными соотношениями.

Проблема сопряженности. *По любому заданию группы*

$$\langle\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle\rangle$$

и по любым двум (групповым) словам W и U в этих образующих определить, сопряжены ли элементы $[W]$ и $[U]$, т. е. найдется ли такое слово Z, что $[Z]^{-1}[W][Z] = [U]$ (можно ли из слова $\overline{Z}WZ$ вывести слово U, пользуясь указанными определяющими соотношениями и тривиальными соотношениями).

Проблема изоморфизма. *По любым двум заданиям*

$$\langle\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle\rangle$$

и

$$\langle\langle\, b_1,\, \ldots,\, b_p \,|\, C_1 \,=\, D_1,\, \ldots,\, C_q \,=\, D_q \,\rangle\rangle$$

определить, будут ли изоморфны соответствующие группы.

По современным представлениям каждая из сформулированных *фундаментальных проблем М. Дэна* может иметь ***решение*** как ***в положительном***, так и ***в отрицательном смысле***. ***Решением*** *фундаментальной проблемы М. Дэна* ***в положительном смысле*** считается соответствующий ***алгоритм*** (***общий метод***), о котором шла речь в первоначальной формулировке проблемы, а ***решением*** *фундаментальной проблемы М. Дэна* ***в отрицательном смысле – доказательство теоремы о невозможности построить соответствующий алгоритм***.

Почти полвека проблемы М. Дэна не поддавались решению и только в начале 1950-х годов Петр Сергеевич Новиков доказал, что *искомые алгоритмы построить невозможно.*

Так как проблемы М. Дэна долгое время решить не удавалось, то естественно возникло желание рассмотреть более общую ситуацию – аналогичные алгоритмические проблемы для полугрупп, заданных образующими элементами и определяющими соотношениями, и установить их неразрешимость.

В 40-е годы XX века А. А. Марков и Э. Пост независимо и практически одновременно установили алгоритмическую неразрешимость проблемы равенства (эквивалентности) слов для полугрупп, заданных конечным числом образующих элементов и конечным числом определяющих соотношений. Это понятие вводится аналогично введенному выше понятию группы, заданной образующими элементами и определяющими соотношениями.

Пусть $\mathcal{A} = \{a_1, \ldots, a_n\}$ – произвольный конечный алфавит.

Зафиксируем некоторый конечный набор упорядоченных пар слов $\langle A_1, B_1\rangle$, ..., $\langle A_m, B_m\rangle$ в этом алфавите. С каждой парой $\langle A_i, B_i\rangle$ свяжем два *элементарных преобразования* слов в алфавите $\mathcal{A}$ – переходы вида

$$UA_iV \longrightarrow UB_iV, \quad UB_iV \longrightarrow UA_iV,$$

где U и V – произвольные слова в этом алфавите.

Саму упорядоченную пару слов $\langle A_i, B_i\rangle$ традиционно обозначают в виде $A_i = B_i$. Полученный объект обозначается в виде

$$\langle\, a_1, \ldots, a_n \,|\, A_1 = B_1, \ldots, A_m = B_m \,\rangle,$$

и он будет служить заданием некоторой полугруппы, которая будет обозначаться тем же способом. При этом a_1, ..., a_n называются *образующими элементами* этой полугруппы, а $A_1 = B_1$, ..., $A_m = B_m$ – ее *определяющими соотношениями.*

Для построения этой полугруппы, как и в случае группы, используем отношение выводимости слов.

Слово U называется *выводимым* из слова W (обозначается $W \vdash^* U$), если либо оно ему графически равно (выводимо за 0 шагов), либо существует последовательность элементарных преобразований

$$W = W_0 \to W_1 \to \ldots \to W_k \to W_{k+1} \to \ldots \to W_s = U,$$

переводящая слово U в слово W.

Нетрудно показать, что отношение выводимости $\vdash^*$ в рассматриваемом случае является отношением эквивалентности, т. е. оно рефлексивно, транзитивно и симметрично. Соответствующие классы эквивалентности будем обозначать через $[W]$.

На множестве классов эквивалентности естественным образом определяется умножение равенством

$$[W] \cdot [U] = [WU],$$

где WU – обычное произведение (сочленение, конкатенация) слов W и U.

Нетрудно проверить, что множество классов эквивалентности относительно введенной операции умножения является полугруппой с единицей (моноидом). При этом роль нейтрального элемента выполняет класс [1], где через 1 обозначено пустое слово. Построенная полугруппа обозначается через

$$\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle$$

и называется *полугруппой, заданной образующими элементами* a_1, ..., a_n и *определяющими соотношениями* $A_1 = B_1$, ..., $A_m = B_m$.

Если некоторая полугруппа S изоморфна построенной полугруппе, то говорят, что *полугруппа* S *имеет задание (генетический код, копредставление)*

$$\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle.$$

В связи с рассмотренным способом задания полугрупп естественно возникают алгоритмические проблемы, аналогичные проблемам М. Дэна, – ***проблема равенства (эквивалентности) слов для полугрупп*** и ***проблема изоморфизма для полугрупп***.

Проблема равенства (эквивалентности) слов для полугрупп. *По любому заданию полугруппы*

$$\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle$$

и по любым двум словам W *и* U *в этих образующих определить, равны ли элементы* $[W]$ *и* $[U]$, *т. е. можно ли из слова* W *вывести слово* U, *пользуясь указанными определяющими соотношениями.*

Проблема изоморфизма для полугрупп. *По любым двум заданиям*

$$\langle\, a_1,\, \ldots,\, a_n \,|\, A_1 \,=\, B_1,\, \ldots,\, A_m \,=\, B_m \,\rangle$$

и

$$\langle\, b_1,\, \ldots,\, b_p \,|\, C_1 \,=\, D_1,\, \ldots,\, C_q \,=\, D_q \,\rangle$$

определить, будут ли изоморфны соответствующие полугруппы.

Как было сказано выше, в 40-е годы XX века А. А. Марков и Э. Пост независимо и практически одновременно установили алгоритмическую неразрешимость проблемы равенства (эквивалентности) слов для полугрупп, заданных конечным числом образующих элементов и конечным числом определяющих соотношений. Неразрешимость проблемы изоморфизма для полугрупп легко следует из неразрешимости для них проблемы равенства слов.

Появление точного понятия алгоритма позволило установить неразрешимость многих алгоритмических проблем. Сначала неразрешимые алгоритмические проблемы были найдены в самой теории алгоритмов, затем в математической логике. Позже было установлено их существование и в других разделах математики – алгебре, топологии, теории чисел, анализе, теории обыкновенных дифференциальных уравнений. Было доказано, что они есть и среди

известных задач, поставленных в математике ранее, до создания теории алгоритмов, и долгие годы не поддававшихся решению. Таковыми оказались в математической логике – ***проблема выводимости для полусистем Туэ***, ***проблема выводимости для Исчисления Предикатов***, в алгебре – ***фундаментальные проблемы М. Дэна для конечно определенных групп*** и аналогичные проблемы для конечно определенных полугрупп, в топологии – ***проблема гомеоморфизма для полиэдров*** (многообразий, являющихся "правильными"объединениями со склейкой стандартных симплексов), в теории чисел – ***проблема разрешимости в целых или натуральных числах полиномиальных уравнений*** $F(x_1, \ldots, x_n) = 0$ (10-я проблема Д. Гильберта). Был найден ряд алгоритмически не разрешимых проблем, связанных с вопросом о существовании решения для систем обыкновенных дифференциальных уравнений, с вопросом о сходимости несобственных интегралов и наличием первообразных из некоторого фиксированного класса для функций определенного класса [11], [12].

В первой половине XX века исследователей прежде всего интересовало, существует ли алгоритм для решения рассматриваемой задачи. Во второй половине XX века особый интерес стал представлять вопрос о сложности соответствующего алгоритма, т. е. об используемых им ресурсах – времени и памяти. В определенной мере это было связано с компьютерной реализацией алгоритмов. Наиболее интересными представляются вопросы, связанные с получением нетривиальных нижних оценок сложности алгоритмов, решающих заданную задачу. Однако эта тема выходит за рамки нашего пособия.

Вопросы для самопроверки

1. Любую ли счетную группу можно задать образующими и определяющими соотношениями?

2. Приведите примеры задания известных групп образующими и определяющими соотношениями.

3. Сформулируйте фундаментальные проблемы Дэна.

3. Фундаментальные группы

В большой работе 1895 года "Analysis Situs" А. Пуанкаре ввел понятие фундаментальной группы, а в столь же большой работе 1908 года Х. Титце установил, что фундаментальные группы некоторых многообразий, заданных клеточными комплексами, имеют конечные задания. Начиная с работ Ж. Листинга 1848 года, интенсивно изучаемый класс наглядных топологических объектов составляли узлы. В докладе 1905 года В. Виртингер изложил метод нахождения группы узла по его проекции на евклидову плоскость. Ранее М. Дэн предложил несколько иной способ нахождения задания группы узла, однако впоследствии метод В. Виртингера стал более распространенным. М. Дэн доказал, что узел

изотопически эквивалентен окружности тогда и только тогда, когда его группа абелева, а значит, циклическая.

Напомним, что *топологическое пространство* – это произвольное непустое множество U вместе с непустым подмножеством τ множества $P(U)$ всех подмножеств множества U, для которых выполняются следующие условия, называемые аксиомами *топологического пространства*:

1) $\emptyset \in \tau$, $U \in \tau$;

2) пересечение любых двух множеств из τ само принадлежит τ;

3) объединение любого семейства множеств из τ само принадлежит τ.

В дальнейшем, чтобы избежать некоторой тавтологичности, мы про множества, элементы которого сами являются множествами или подмножествами, вместо "множество множеств" или "множество подмножеств" будем говорить "семейство множеств" или "семейство подмножеств". Элементы τ являются подмножествами множества U, т. е. τ – это некоторое множество подмножеств множества U, но мы часто будем говорить, что τ – это некоторое семейство подмножеств множества U.

Подмножества множества U, входящие в τ, называются *открытыми* множествами в U, а их дополнения – *замкнутыми* множествами в U. Само τ называется *топологией*.

Таким образом, *топологическое пространство* - это набор $\langle U,\ \tau \rangle$, при этом само множество U называется *основным множеством* или *носителем* топологического пространства, а τ – его топологией. Но мы будем придерживаться устоявшейся практики и обозначать через U как само топологическое пространство, т. е. набор, состоящий из множества (носитель) и топологии, так и сам носитель. Это не приведет к путанице, так как мы не будем рассматривать различные топологии, заданные на одном и том же множестве.

Хорошо известными примерами топологических пространств являются $\langle R^n,\ \tau_o \rangle$, где топология τ_o состоит из всех открытых подмножеств множества R^n, т. е. таких подмножеств, которые вместе с принадлежащей ему точкой содержат и весь открытый шар подходящего радиуса с центром в этой точке.

На произвольном подмножестве V множества U носителя топологического пространства $\langle U,\ \tau \rangle$ естественным образом вводится индуцированная топология $\tau_{U\ ind\ V}$

$$\tau_{U\ ind\ V} = \{\, V \cap W \,|\, W \in \tau \,\}.$$

Непрерывное отображение топологического пространства $\langle U_1,\ \tau_1 \rangle$ в топологическое пространство $\langle U_2,\ \tau_2 \rangle$ – это любое отображение f основного множества U_1 в основное множество U_2 такое, что для любого подмножества Y множества U_2 его полный прообраз

$$f^{-1}(Y) = \{\, x \,|\, x \in U_1 \,\&\, f(x) \in Y \,\}$$

является открытым, т. е. принадлежит τ_1.

Гомеоморфизм топологического пространства $\langle U_1,\ \tau_1 \rangle$ на топологическое пространство $\langle U_2,\ \tau_2 \rangle$ – это любое биективное отображение f основного множества U_1 на основное множество U_2 такое, что как само отображение f, так и обратное ему отображение f^{-1} непрерывны.

Два топологических пространства называются *гомеоморфными*, если существуют гомеоморфизм одного из них на другое.

Так же, как в алгебре полугруппы, группы, кольца, поля и другие алгебраические системы рассматриваются с "с точностью до изоморфности", так и в топологии топологические пространства рассматриваются "с точностью до гомеоморфности".

Путь в топологическом пространстве $\langle U,\ \tau \rangle$ – это любое непрерывное отображение f отрезка $[0,1]$ во множество U. При этом $f(0)$ называется начальной точкой пути f, а $f(1)$ – его конечной точкой.

Для любых двух путей f и g в топологическом пространстве $\langle U,\ \tau \rangle$ таких, что $f(1) = g(0)$, т. е. конечная точка пути f совпадает с начальной точкой пути g (путь g начинается там, где заканчивается путь f), определено их произведение $f * g$:

$$(f * g)(t) = \begin{cases} f(2t) & \text{при } 0 \le t \le 1/2; \\ g(2t-1) & \text{при } 1/2 \le t \le 1. \end{cases}$$

Для любых двух путей f и g в топологическом пространстве $\langle U,\ \tau \rangle$ таких, что $f(0) = g(0)$ и $f(1) = g(1)$, определено понятие *гомотопической эквивалентности.*

Пути f и g в топологическом пространстве $\langle U,\ \tau \rangle$ такие, что $f(0) = g(0)$ и $f(1) = g(1)$, называются *гомотопически эквивалентными*, если существует такое непрерывное отображение $F(t,s)$ единичного квадрата $I^2 = \{(t,s) \,|\, 0 \le t,s \le 1\}$ во множество U, для которого выполняются следующие условия:

$$1)(\forall t)_{0\le t\le 1}(F(t,0) = f(t),\ F(t,1) = g(t)),$$
$$2)(\forall s)_{0\le s\le 1}(F(0,s) = f(0),\ F(1,s) = f(1)).$$

При этом отображение $F(t,s)$ называется *гомотопией* путей f и g. Это утверждение мы будем записывать в виде

$$f \overset{F}{\sim} g$$

и говорить, что гомотопия F *переводит путь* f *в путь* g. Отметим, что $F(t,s)$ – это непрерывная функция от двух переменных, определенная на единичном квадрате и принимающая значения во множестве U.

Запись

$$f \sim g$$

будет служить сокращением для утверждения: *существует гомотопия* F*, переводящая путь* f *в путь* g.

Путь f называется *замкнутым* или *петлей* (в точке $p = f(0)$), если его начальная и конечная точки совпадают, т. е. $f(0) = f(1)$.

Зафиксируем во множестве U произвольную точку p и рассмотрим множество $L(U,p)$ всех петель в этой точке, т. е. непрерывных путей, начинающихся и заканчивающихся в этой точке p. Нетрудно проверить, что отношение гомотопической эквивалентности $\sim$ является отношением эквивалентности на множестве $L(U,p)$.

$$f \overset{Id(f,s)}{\sim} f,$$

где $(\forall s)_{0\le s\le 1}(\forall t)_{0\le t\le 1} Id(f,s)(t,s) = f(t)$.

Если $f \overset{F}{\sim} g$, то $f \overset{\overline{F}_s}{\sim} g$, где $(\forall s)_{0\le s\le 1}(\forall t)_{0\le t\le 1}\overline{F}_s(t,s) = F(t,1-s)$.

Если $f \overset{F}{\sim} g$, $g \overset{G}{\sim} h$,то $f \overset{(F*G)_s}{\sim} h$, где $(\forall s)_{0\le s\le 1}(\forall t)_{0\le t\le 1}(F*G)_s(t,s) = (F(*,s)*G(*,s))(t)$. При этом при фиксированном s через $F(*,s)$ $(G(*,s))$ обозначен путь, заданный равенством $F(*,s)(t) = F(t,s)$ $(G(*,s)(t) = G(t,s))$.

Более того, отношение гомотопической эквивалентности $\sim$ согласовано с операцией умножения путей, т. е. если $f \sim f'$ и $g \sim g'$, то $f*g \sim f'*g'$:

если $f \overset{F}{\sim} f'$, $g \overset{G}{\sim} g'$, то $f*g \overset{(F*G)_s}{\sim} f'*g'$.

Это дает возможность на фактормножестве $L(U,p)/\sim$, состоящем из классов $[f]_\sim$ гомотопически эквивалентных петель в точке p

$$[f]_\sim = \{\, g \,|\, g - \text{петля в точке } \ p \ u \ \ f \sim g\}$$

и обозначаемым в дальнейшем через $\pi(U,p)$, естественным образом определить операцию $\cdot$ умножения классов равенством

$$[f]_\sim \cdot [g]_\sim \ = \ [f*g]_\sim.$$

Определение не зависит от выбора представителей в классах эквивалентности. Поэтому $\langle \pi(U,p), \cdot \rangle$ – *группоид*. Покажем, что этот группоид является *группой*.

Для любых трех путей f, g и h таких, что $f(1) = g(0)$ и $g(1) = h(0)$, справедлива эквивалентность

$$f*(g*h) \sim (f*g)*h.$$

Нетрудно понять, что следующая гомотопия задает требуемую гомотопическую эквивалентность:

$$F(t,s) \ = \ \begin{cases} f(\frac{4}{s+1}t) & \text{при } 0 \le t \le \frac{s+1}{4}; \\ g(4t-1-s) & \text{при } \frac{s+1}{4} \le t \le \frac{s+2}{4}; \\ h(\frac{4t-2-s}{2-s}) & \text{при } \frac{s+2}{4} \le t \le 1. \end{cases}$$

Поэтому умножение классов эквивалентных путей ассоциативно. Значит, группоид $\langle \pi(U,p), \cdot \rangle$ является полугруппой.

Для произвольной точки $a \in U$ обозначим через e_a *постоянный путь в точке* a, т. е. для любого $0 \leq t \leq 1$ $e_a(t) = a$.

Для произвольного пути f и точек $q = f(0)$, $p = f(1)$ справедливы эквивалентности $f * e_p \sim f$ и $e_q * f \sim f$.

Нетрудно проверить, что первую эквивалентность задает гомотопия

$$F_p(t,s) = \begin{cases} f(\frac{2}{s+1}t) & \text{при } 0 \leq t \leq \frac{s+1}{2}; \\ p & \text{при } \frac{s+1}{2} \leq t \leq 1, \end{cases}$$

а вторую – гомотопия

$$F_q(t,s) = \begin{cases} q & \text{при } 0 \leq t \leq \frac{s}{2}; \\ f(\frac{2t-s}{2-s}) & \text{при } \frac{s}{2} \leq t \leq 1. \end{cases}$$

Поэтому роль нейтрального элемента в полугруппе $\langle \pi(U,p), \cdot \rangle$ выполняет класс $[e_p]_\sim$. Значит, полугруппа $\langle \pi(U,p), \cdot \rangle$ является полугруппой с единицей или моноидом.

Для установления обратимости произвольного элемента этого моноида достаточно заметить, что для любого пути f и точек $q = f(0)$, $p = f(1)$ справедливы эквивалентности $f * \bar{f} \sim e_p$ и $\bar{f} * f \sim e_q$.

Нетрудно проверить, что первую эквивалентность задает гомотопия

$$F(t,s) = \begin{cases} f(2t) & \text{при } 0 \leq t \leq \frac{1-s}{2}; \\ f(1-s) = \bar{f}(s) & \text{при } \frac{1-s}{2} \leq t \leq \frac{1+s}{2}; \\ \bar{f}(2t-1) = f(2(1-t)) & \text{при } \frac{1+s}{2} \leq t \leq 1. \end{cases}$$

а вторую – гомотопия

$$F(t,s) = \begin{cases} \bar{f}(2t) = f(1-2t) & \text{при } 0 \leq t \leq \frac{s}{2}; \\ f(1-s) = \bar{f}(s) & \text{при } \frac{s}{2} \leq t \leq \frac{2-s}{2}; \\ f(2t-1) = f(2(1-t)) & \text{при } \frac{2-s}{2} \leq t \leq 1. \end{cases}$$

Таким образом, группоид $\langle \pi(U,p), \cdot \rangle$ является группой и называется *фундаментальной группой* или *группой Пуанкаре* топологического пространства U в точке p. Эта группа обычно обозначается через $\pi(U,p)$. Фундаментальная группа топологического пространства U в точке p также обозначается через $\pi_1(U,p)$ и называется первой гомотопической группой топологического пространства U в точке p. Для произвольного натурального числа n определяется n-я гомотопическая группа $\pi_n(U,p)$. Но такие группы по целому ряду причин находятся вне зоны нашего интереса.

В определении фундаментальной группы $\pi(U,p)$ участвует точка p. Но для достаточно широкого класса топологических пространств фундаментальные группы, отвечающие различным точкам, оказываются изоморфными.

Топологическое пространство U называется *линейно связным*, если любые две его точки могут быть соединены непрерывным путем.

Покажем, что если топологическое пространство U *линейно связно*, то для любых двух его точек p и q фундаментальные группы $\pi(U,p)$ и $\pi(U,q)$ изоморфны. Для построения изоморфизма группы $\pi(U,p)$ на $\pi(U,q)$ обозначим через α, непрерывный путь в пространстве U из точки q в точку p, т. е. $\alpha(0) = q$ и $\alpha(1) = p$. Если f – петля в точке p, то $\alpha * f * \bar{\alpha}$ – петля в точке q.

Рассмотрим отображение α_*, переводящее класс $[f]_\sim$ петель в точке p в класс $[\alpha * f * \bar{\alpha}]_\sim$ петель в точке q, т. е.

$$\alpha_*([f]_\sim) \;=\; [\alpha * f * \bar{\alpha}]_\sim.$$

Покажем, что α_* – *изоморфизм* группы $\pi(U,p)$ на группу $\pi(U,q)$.

Для установления независимости определения отображения α_* от выбора представителя в классе эквивалентности предположим, что $f \sim f'$ и $F(t,s)$ – гомотопия, переводящая путь f в путь f'. При каждом фиксированном s функция от t, равная $F(t,s)$, задает путь, который мы будем обозначать через $F(*,s)$. Тогда гомотопия $F_\alpha(t,s) \;=\; (\alpha * F(*,s) * \bar{\alpha}(t)$ устанавливает эквивалентность путей $\alpha * f * \bar{\alpha}$ и $\alpha * f' * \bar{\alpha}$. Значит, определение корректно.

Отображение α_* обратимо – обратным ему служит отображение β_*, заданное равенством

$$\beta_*([h]_\sim) \;=\; [\bar{\alpha} * h * \alpha]_\sim.$$

Наконец, равенство

$$\alpha_*([f]_\sim \cdot [g]_\sim) \;=\; \alpha_*([f]_\sim) \cdot \alpha_*([g]_\sim)$$

следует из эквивалентности

$$\alpha * (f * g) * \bar{\alpha} \;\sim\; (\alpha * f * \bar{\alpha}) * (\alpha * g * \bar{\alpha}),$$

которая легко получается из ранее установленных эквивалентностей.

Вопросы для самопроверки

1. Что такое *путь в топологическом пространстве*?

2. Какие пути в топологическом пространстве называются *гомотопически эквивалентными*?

3. Что является элементом фундаментальной группы топологического пространства?

4. Как определяется произведение двух элементов фундаментальной группы топологического пространства?

4. Непрерывные отображения топологических пространств и гомоморфизмы фундаментальных групп

Непрерывные отображения топологических пространств играют важную роль в общей топологии. Они иногда для краткости называются *морфизмами* топологических пространств. Топологические пространства вместе с их непрерывными отображениями (морфизмами) образуют *категорию топологических пространств*, но рассмотрение этой темы выходит за рамки пособия. Группы вместе с их гомоморфизмами (морфизмами групп) образуют *категорию групп*. Между этими двумя категориями имеется тесная связь.

С каждым непрерывным отображением φ топологического пространства U с фиксированной (отмеченной) точкой p в топологическое пространство V естественным образом связывается гомоморфизм φ_* фундаментальной группы $\pi(U,p)$ в фундаментальную группу $\pi(V,\varphi(p))$. Если f – путь (петля) в топологическом пространстве U, то суперпозиция $\varphi\circ f$ - путь (петля) в топологическом пространстве V. При этом: если гомотопия F устанавливает эквивалентность путей f и f', то гомотопия $\varphi\circ F$ устанавливает эквивалентность путей $\varphi\circ f$ и $\varphi\circ f'$. Кроме того, для любых двух путей f и g таких, что $f(1)=g(0)$, выполняется равенство $\varphi\circ(f*g) = (\varphi\circ f)*(\varphi\circ g)$. Поэтому равенство

$$\varphi_*([f]_\sim = [\varphi\circ f]_\sim)$$

задает гомоморфизм φ_* фундаментальной группы $\pi(U,p)$ в фундаментальную группу $\pi(V,\varphi(p))$.

Если φ – непрерывное отображение топологического пространства U с фиксированной (отмеченной) точкой p в топологическое пространство V, а ψ – непрерывное отображение топологического пространства V с фиксированной (отмеченной) точкой $\varphi(p)$ в топологическое пространство W, то для соответствующих гомоморфизмов фундаментальных групп выполняется равенство

$$(\psi\circ\varphi)_* = \psi_*\circ\varphi_*.$$

Кроме того, если Id_U – тождественное отображение множества U на себя, т.е. для любого элемента u множества U выполняется равенство $Id_U(u)=u$, то $(Id_U)_*$ – тождественный гомоморфизм фундаментальной группы $\pi(U,p)$ на себя.

Поэтому, *если φ – гомеоморфизм топологических пространств U и V, т. е. биективное отображение множества U на V и при этом как φ, так и ему обратное отображение φ^{-1} непрерывны, то φ_* – изоморфизм фундаментальной группы $\pi(U,p)$ на фундаментальную группу $\pi(V,\varphi(p))$.*

Значит, *если топологические пространства U и V гомеоморфны, то их фундаментальные группы $\pi(U,p)$ и $\pi(V,\varphi(p))$ изоморфны.*

Обычно это утверждение применяется в обратном направлении: *если фундаментальные группы топологических пространств неизоморфны, то сами топологические пространства негомеоморфны.*

Вопросы для самопроверки

1. Дайте определение непрерывного отображения одного топологического пространства в другое.

2. Что такое гомоморфизм фундаментальных групп топологических пространств, индуцированный непрерывным отображением?

3. Какие два топологических пространства называются гомеоморфными?

5. Узлы и косы

Многие из нас умеют завязывать *узлы* на не слишком короткой веревке, но не все – у некоторых, в том числе и у автора, – шнурки на ботинках постоянно развязываются. Простейший узел изображен на рис.1.1.

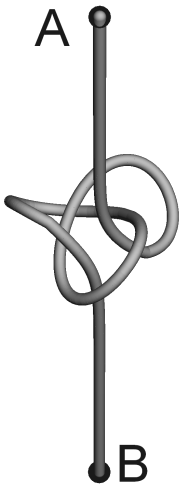

Рис. 1.1

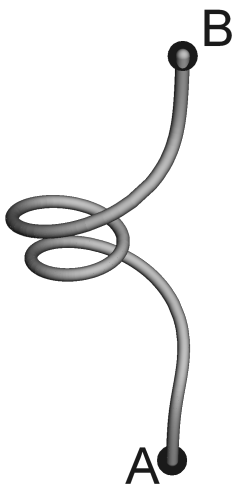

Рис. 1.2

Интуитивно ясно, что если закрепить концы веревки A и B, то этот узел, не разрывая веревку, нельзя развязать, т. е. преобразовать в *тривиальный* узел, изображенный на рис.1.2.

Вместо закрепления концов веревки A и B их можно просто склеить, и тогда узел с рис.1.1 превратится в узел на рис. 2.1, называемый *клеверным листом*, или *трилистником*, а "незаузленный" узел с рис. 1.2 превратится в окружность с рис. 2.2.

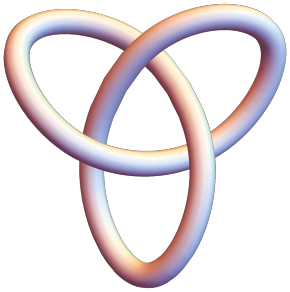

Рис. 2.1

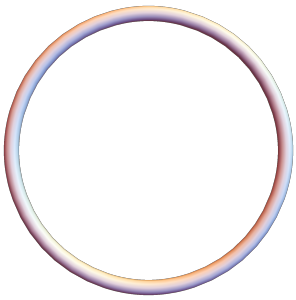

Рис. 2.2

Если обычную окружность рис. 2.2 назвать “незаузленной” окружностью, то узел с Рис. 2.1 можно назвать “заузленной окружностью”: если на узлы с рис. 2.1 и рис. 2.2 посмотреть как на ходы, которые проел червяк в яблоке, то “червяк их не сможет различить”, т. е. “сами по себе” и узел с рис.2.1 и узел с рис. 2.2 – это просто окружности, но они по-разному расположены в пространстве R^3. Чтобы сделать узел объектом математического изучения, требуется ввести адекватную математическую замену рассмотренных “физических” объектов. Узел в R^3 – это замкнутая кривая без самопересечений.

Мы приходим к следующему определению узла в R^3:

узел в R^3 – это образ $f(S)$ – единичной окружности S относительно инъективного, непрерывного отображения f этой окружности в R^3.

Однако это слишком общее определение, как и определение непрерывной кривой, под которое подходит кривая Пеано, заполняющая весь единичный квадрат. Поэтому понятие непрерывной кривой обычно сужается до понятия гладкой кривой. Так и в случае узлов обычно ограничиваются изучением так называемых *полигональных узлов* – узлов, образованных замкнутыми ломаными линиями в R^3 без самопересечений.

Математическая теория узлов начала интенсивно развиваться, начиная с работы Листинга 1848 года. Большой вклад в теорию узлов в первой половине XX века внесли Виртингер, Дэн, Александер, Рейдемейстер и Зейферт. Узлы относятся к так называемой “топологии малой размерности”.

Может быть, самый известный узел – это *гордиев узел*, с которым связана легенда и известное выражение “разрубить гордиев узел”. Легенда гласит, что фригийский царь Гордий завязал весьма сложный узел, а жрецы Фригийского храма Зевса предсказали, что первый, кто развяжет этот узел, будет самым выдающимся царем, ему покорится весь мир, он создаст империю, охватывающую всю Азию. По мнению некоторых авторов, легенда гласит (в изложении легенды некоторыми авторами), что покоривший столицу Фригии великий полководец древности Александр Македонский, войдя в древний храм без долгих размышлений выхватил меч и рассек одним ударом гордиев узел (таким виделся излагавшим этот вариант древней легенды идеал правителя). Это решительное, но необдуманное действие истолковали жрецы: “Он завоюет мир! Но мечом, а не дипломатией”. Однако другие авторы утверждают (в изложении легенды другими авторами), что Александр Македонский не разрубил узел мечом, а решил

задачу (проблему): он вынул закреплявший яремный ремень крюк – “гестор”, – и узел развязался! (таким виделся излагавшим в таком варианте легенду идеал правителя) На этом историческом примере можно было бы порассуждать о взаимоотношениях в истории “метода грубой силы” и “интеллектуального метода” – “прыгать” или “думать”, что можно было бы увязать и с вопросом обеспечения информационной безопасности, но, может быть, сделаем это в другое время и в другом месте.

Рассмотрим еще один достаточно интересный объект “топологии малой размерности” – *косу*. В наш “век коротких стрижек” может быть многие и забыли о косах, некогда украшавших женские головы. Пример косы на двух нитях приведен на рис. 3.

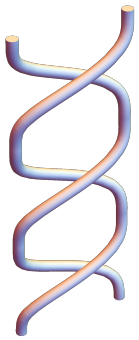

Рис. 3

Этот пример косы не случайный: коса с рис. 3 тесно связана с узлом трилистник с рис. 2.1, но об этом позже.

Как и в случае узлов, для математического изучения кос нам потребуется заменить “реальные” косы на математические косы, которые мы будем попрежнему называть просто *косами*.

Для построения *кос* на n нитях фиксируем в пространстве R^3 два набора из n точек каждый:

$$P_1 = (1,0,1), P_2 = (2,0,1), \ldots, P_n = (n,0,1) \quad \text{и}$$
$$Q_1 = (1,0,0), Q_2 = (2,0,0), \ldots, Q_n = (n,0,0).$$

Тогда коса – это набор из n непрерывных инъективных отображений $f_1(t)$, $f_2(t)$, ..., $f_n(t)$ единичного отрезка $[0,1]$ в пространство R^3 таких, что при любом i $(1 \le i \le n)$:

$f_i(0) = P_i$ и существует такое j_i, что $f_i(1) = Q_{j_i}$, причем числа j_1, ..., j_n образуют перестановку чисел 1, ..., n. Кроме того,

если $f_i(t) = (f_i^{(1)}(t), f_i^{(2)}(t), f_i^{(3)}(t))$, то $f_i^{(3)}(t))$ – монотонно убывающая функция и при $i \neq j$

$f_i([0,1]) \cap f_j([0,1]) = \emptyset$.

Т.е. функция $f_i(t)$– это "непрерывная нить, идущая монотонно сверху вниз из точки P_i в точку Q_{j_i}, а последнее условие означает, что нити попарно не пересекаются". Второе условие гарантирует монотонное спускание нити вниз.

На самом деле коса определяется с точностью до некоторой эквивалентности: две косы B и B_1 на n нитях называются эквивалентными (не различаются, считаются одной и той же косой), если существует гомеоморфизм f пространства R^3, т.е. такое биективное отображение этого пространства на себя, что f и f^{-1} непрерывны, ограничения f на подпространства $\{(x,y,z)|x \geq 1\}$ и $\{(x,y,z)|x \leq -1\}$ оставляет на месте точки этих подпространств (индуцирует тождественные отображения на этих подпространствах) и $f(B) = B_1$. Но нам не потребуется это математическое уточнение этого интуитивно ясного понятия "нити косы можно непрерывно и без склейки деформировать".

Более интересным является то, что косы можно умножать. Как это происходит легко понять из рис. 4: чтобы косу σ умножить на косу τ, надо просто к σ "приклеить, прикрепить" косу τ.

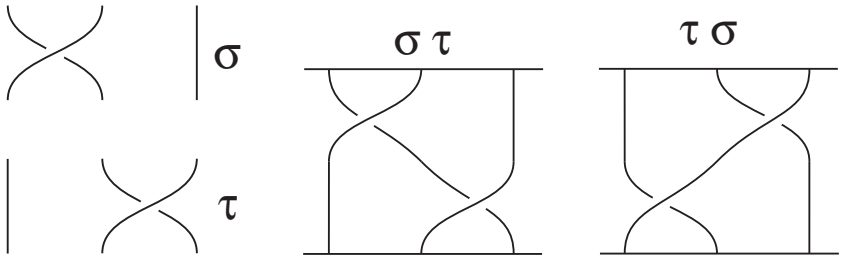

Рис. 4

Аналогично на множестве всех кос на n нитях можно достаточно естественным образом ввести операцию умножения кос ("склейку" кос), относительно которой получим весьма интересную и важную группу $B(n)$, которая изучается уже более 60 лет – с середины XX века, является источником все новых задач и обобщений, а в начале XXI века нашла применения в криптографии [25]. Для узлов тоже можно определить бинарную алгебраическую операцию, состоящую в "привязывании" одного узла к другому, но относительно нее группы не получим, а получим лишь коммутативную полугруппу, если примем, что существует "множество всех узлов в пространстве R^3". Но и в таком случае, придется рассматривать в качестве элементов полуруппы не узлы, а классы эквивалентных узлов.

Если коса σ – это набор непрерывных инъективных отображений $f_1(t)$, $f_2(t)$, ..., $f_n(t)$ единичного отрезка $[0,1]$ в пространство R^3 таких, что при любом i $(1 \leq i \leq n)$: $f_i(0) = P_i$ и $f_i(1) = Q_{j_i}$, а коса τ – это набор непрерывных инъективных отображений $g_1(t)$, $g_2(t)$, ..., $g_n(t)$ единичного отрезка $[0,1]$ в пространство R^3 таких, что при любом i $(1 \leq i \leq n)$: $g_i(0) = P_i$ и $g_i(1) = Q_{t_i}$, то коса $\sigma\tau$, равная произведению этих кос σ и τ – это набор непрерывных инъективных

отображений $h_1(t)$, $h_2(t)$, ..., $h_n(t)$ единичного отрезка $[0,1]$ в пространство R^3 таких, что при любом i $(1 \le i \le n)$: $h_i(0) = P_i$ и

$$h(t) = \begin{cases} f_i(2t), & \text{если } 0 \le t \le 1/2; \\ g_{j_i}(2t-1), & \text{если } 1/2 \le t \le 1. \end{cases}$$

Относительно введенной операции умножения косы на n нитях образуют группу $B(n)$, которая может быть весьма несложно задана ***образующими элементами и определяющими соотношениями***, но об этом будет сказано ниже. Косы можно рассматривать как геометрические (топологические) объекты, но можно на них смотреть и как на алгебраические объекты. Алгебраическая теория кос ведет свое начало с работ Артина [20] и А.А. Маркова [10].

Узлы и косы – простейшие объекты изучения 3-мерной топологии или, как теперь принято говорить, топологии малой размерности. Известно, что ряд проблем на сегодняшний день решен для топологии достаточно большой размерности, однако для размерностей 3 и 4 при решении аналогичных вопросов нередко возникают немалые трудности. Например, проблема гомеоморфности отрицательно решена А.А. Марковым для 4-мерных многообразий [9]. А для 3-мерных многообразий лишь в 1994 году положительно решена алгоритмическая проблема распознавания стандартной 3-мерной сферы и совсем недавно доказана гипотеза Пуанкаре. С.П. Новиков доказал [2] алгоритмическую неразрешимость проблемы распознавания стандартной 5-мерной сферы, а для 4-мерной сферы вопрос остается открытым.

Узлы $K_1 \subseteq R^3$ и $K_2 \subseteq R^3$ называются ***эквивалентными***, *если существует гомеоморфизм* f *пространства* R^3 *такой, что* $f(K_1) = K_2$. Мы не интересуемся вопросом, сохраняет ли гомеоморфизм f ориентацию пространства R^3. Так как $f(R^3 \setminus K_1) = R^3 \setminus K_2$, то f_* – изоморфизм фундаментальных групп $\pi(R^3 \setminus K_1)$ и $\pi(R^3 \setminus K_2)$. Поэтому *если группы двух узлов неизоморфны, то сами узлы неэквивалентны.* Это открывает путь доказательства неэквивалентности узлов и делает естественным связать с узлом $K \subseteq R^3$ группу $G(K) = \pi(R^3 \setminus K)$, называемую *группой узла* K.

Виртингер установил, что если узел K допускает "достаточно хорошую" проекцию на плоскость, то можно найти достаточно простое задание его группы $G(K)$ ***образующими элементами и определяющими соотношениями*** и попытаться применить алгебраические методы для доказательства неэквивалентности узлов K_1 и K_2 – через доказательство неизоморфности их групп $G(K_1)$ и $G(K_2)$.

Группа тривиального узла является бесконечной циклической, т.е. имеет задание

$$\langle\langle\, a \,|\, \emptyset \,\rangle\rangle,$$

а группа трилистника имеет задание

$$\langle\langle\, a, b \,|\, a^3 = b^2 \,\rangle\rangle.$$

Но как доказать, что эти группы не изоморфны?

Среди гомоморфных образов группы трилистника есть симметрическая группа $S(3)$ степени 3, имеющая задание

$$\langle\langle\, a, b \,|\, a^3 = 1,\, b^2 = 1, ba^2 = ab \,\rangle\rangle.$$

А симметрическая группа $S(3)$ нециклическая, значит нециклическая и группа трилистника (гомоморфный образ циклической группы сам является циклической группой). Поэтому группа трилистника не изоморфна группе тривиального узла. Значит ***трилистник нельзя развязать***!

Вопросы для самопроверки

1. Дайте определение узла.
2. Какие два узла называются эквивалентными?
3. Дайте определение группы узла.
4. Как умножаются косы?
5. Дайте определение группы кос.

6. Задания подгрупп и факторгрупп

Для произвольной группы G и произвольного ее подмножества $U \subseteq G$ через $gr(U)$ обозначается *пересечение всех подгрупп H группы G, содержащих множество U*. Так как пересечение любого семейства подгрупп само является подгруппой, то $gr(U)$ – подгруппа группы G, содержащая U ($U \subseteq gr(U) \leq G$). Кроме того, *она является минимальной относительно включения подгруппой группы G, содержащей U*, т. е. если H – подгруппа группы G, содержащая U ($U \subseteq H \leq G$), то $gr(U) \subseteq H$.

Подгруппа $gr(U)$ называется *подгруппой группы G, порожденной множеством ее элементов U* . При этом само множество U называется *множеством порождающих или образующих элементов* (для) подгруппы $gr(U)$. Если $G = gr(U)$, то множество U называется *множеством порождающих или образующих элементов* (для) группы $gr(G)$.

Нетрудно показать, что справедливо равенство

$$gr(U) \,=\, \{\, u_1^{\varepsilon_1} \cdots u_n^{\varepsilon_n} \,|\, n \in \mathbb{N},\; u_1, \ldots, u_n \,\in\, U,\; \varepsilon_1, \ldots, \varepsilon_n \,\in\, \{\, -1,\, 1 \,\}\,\}.$$

Рассмотрим близкое понятие. Для произвольной группы G и произвольного ее подмножества $U \subseteq G$ через $ngr(U)$ обозначается *пересечение всех нормальных подгрупп N группы G, содержащих множество U*. Так как пересечение любого семейства нормальных подгрупп само является нормальной подгруппой, то $ngr(U)$ – нормальная подгруппа группы G, содержащая U ($U \subseteq ngr(U) \trianglelefteq G$). Кроме того, *она является минимальной относительно включения нормальной подгруппой группы G, содержащей U*, т. е. если N – нормальная подгруппа группы G, содержащая U ($U \subseteq N \trianglelefteq G$), то $ngr(U) \subseteq N$.

Нормальная подгруппа $ngr(U)$ называется *нормальной подгруппой группы G, порожденной множеством ее элементов U* . При этом само множество U называется *множеством нормальных порождающих элементов* нормальной подгруппы $ngr(U)$.

Нетрудно показать, что справедливо равенство

$$ngr(U) = \{\, (v_1 u_1^{\varepsilon_1} v_1^{-1}) \cdots (v_n u_n^{\varepsilon_n} v_n^{-1}) \,|\, n \in \mathbb{N},\ u_1, \ldots, u_n \in U, \\ \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\},\ v_1, \ldots, v_n \in G \,\}.$$

Рассмотрим группу G, заданную образующими и определяющими соотношениями

$$G = \langle\langle\, \mathcal{A} \,|\, \mathcal{R} \,\rangle\rangle.$$

Пусть $H \leq G$ – ее подгруппа, а $N \trianglelefteq G$ – нормальная подгруппа. Естественно возникает вопрос о нахождении заданий образующими и определяющими соотношениями для подгруппы H и для факторгруппы G/N.

Предположим, что N является нормальным замыканием множества

$$\{\, [W_i] \,|\, i \in I \,\}$$

элементов группы G, где W_i – слова в групповом алфавите $\mathcal{A}$.

Нетрудно показать, что факторгруппа G/N имеет задание образующими и определяющими соотношениями

$$G/N = \langle\langle\, \mathcal{A} \,|\, \mathcal{R} \cup \{\, W_i = 1 \,|\, i \in I \,\} \,\rangle\rangle.$$

Сложнее решается вопрос о нахождении задания для подгруппы по заданию группы.

Рассмотрим группу G, заданную образующими и определяющими соотношениями

$$G = \langle\langle\, \mathcal{A} \,|\, \mathcal{R} \,\rangle\rangle.$$

Пусть $H \leq G$ – ее подгруппа, порожденная множеством

$$\{\, [W_i] \,|\, i \in I \,\}$$

элементов группы G, где W_i – слова в групповом алфавите $\mathcal{A}$. В дальнейшем, как обычно, будем работать как с элементами $[W]$ группы G, так и с их представителями W, где W – слово в групповом алфавите $\mathcal{A}$. Чтобы подчеркнуть последний факт, часто вместо записи W будем использовать "более выразительную" запись $W(a_j)$, считая, что

$$\mathcal{A} = \{\, a_j \,|\, j \in J \,\}.$$

Введем новый алфавит

$$\mathcal{S} = \{\, s_i \,|\, i \in I \,\},$$

взаимно однозначно сопоставив каждому образующему элементу $[W_i]$ новую букву s_i.

Введем основное для дальнейшего понятие – понятие *переписывающего процесса* τ для подгруппы H.

Переписывающий процесс для подгруппы H (относительно ее системы образующих $\{ W_i(a_j) \mid i \in I \}$) есть отображение

$$\tau : W(a_j) \mapsto V(s_i)$$

слов $W(a_j)$ в групповом алфавите $\mathcal{A}$, определяющих (задающих, представляющих) элементы из подгруппы H, в слова $V(s_i)$ в новом алфавите S при условии, что слова $W(a_j)$ и $V(W_i(a_j))$ определяют (задают, представляют) один и тот же элемент из подгруппы H.

Предположим, что в задании группы G образующими и определяющими соотношениями $G = \langle\langle \mathcal{A} \mid \mathcal{R} \rangle\rangle$ все соотношения из множества $\mathcal{R}$ имеют стандартизованный вид $R = 1$.

Пусть $H \leq G$ – ее подгруппа, порожденная множеством элементов

$$\{ [W_i] \mid i \in I \},$$

а τ – переписывающий процесс для подгруппы H относительно этой системы образующих.

Справедлива следующая теорема, доказательство которой можно изучить по монографии [8].

Теорема 1. *Подгруппа H допускает следующее задание образующими и определяющими соотношениями*

$$\langle\langle \mathcal{S} \mid \mathcal{R}_H \rangle\rangle,$$

где $\mathcal{S}$ – это введенный выше новый алфавит, а множество $\mathcal{R}_H$ определяющих соотношений состоит из следующих соотношений:

1) $\{ s_i = \tau(W_i(a_j)) \mid i \in I \}$,

2) $\tau(U(a_j)) = \tau(U^*(a_j))$ для каждой пары свободно равных слов $U(a_j)$ и $U^*(a_j)$, определяющих элементы из подгруппы H,

3) $\tau(U_1(a_j)U_2(a_j)) = \tau(U_1(a_j))\tau(U_2(a_j))$ для каждой пары слов $U_1(a_j)$ и $U_2(a_j)$, определяющих элементы из подгруппы H,

4) $\tau(V(a_j)RV^{-1}(a_j)) = 1$ для каждого соотношения $R = 1$ из множества $\mathcal{R}$ определяющих соотношений для группы G.

Упрощение этого множества определяющих соотношений производится за счет выбора специальной системы образующих. Для произвольной подгруппы H группы G рассматривается *система представителей $\overline{W}$ правых смежных классов HW* группы G по подгруппе H, причем представитель класса H – пустое слово. Отметим, что $W(\overline{W})^{-1} \in H$ и $HW = H\overline{W}$.

С доказательством следующей теоремы также можно ознакомиться по монографии [8].

Теорема 2. *Подгруппа H порождается множеством слов*

$$\{\,(Ka_j)(\overline{Ka_j})^{-1}\,|\,j\in J,\ K-\text{произвольный представитель правого смежного класса}\ \}.$$

Если каждому порождающему элементу $(Ka_j)(\overline{Ka_j})^{-1}$ для подгруппы H сопоставить новый символ (новую букву) s_{K,a_j}, то получим переписывающий процесс Рейдемейстера (Райдемайстера) τ_R, который слово

$$U \;=\; a_{t_1}^{\varepsilon_1}a_{t_2}^{\varepsilon_2}\dots a_{t_n}^{\varepsilon_n},$$

задающее элемент подгруппы H, преобразует в слово

$$\tau_R(U) \;=\; s_{K_1,a_{t_1}}^{\varepsilon_1}s_{K_2,a_{t_2}}^{\varepsilon_2}\dots s_{K_n,a_{t_n}}^{\varepsilon_n},$$

где K_j – представитель $j-1$-го начала слова U, если $\varepsilon_j=1$, и K_j – представитель j-го начала слова U, если $\varepsilon_j=-1$.

С доказательством следующей теоремы также можно ознакомиться по монографии [8].

Теорема 3. *Подгруппа H имеет следующее задание образующими и определяющими соотношениями*

$$\begin{gathered}\langle\langle\{\,s_{K,a_j}\,|\,j\in J,\ K-\text{произвольный представитель правого смежного класса}\ \}\,|\\ \{\,s_{K,a_j}=\tau_R((Ka_j)(\overline{Ka_j})^{-1})\,|\,j\in J,\\ K-\text{произвольный представитель правого смежного класса}\ \}\cup\\ \{\,\tau_R(KRK^{-1})=1\,|\,R=1\ -\ \text{произвольное соотношение из множества}\,\mathcal{R}\\ \text{определяющих соотношений для группы}\ G,\\ K-\text{произвольный представитель правого смежного класса}\ \}\rangle\rangle.\end{gathered}$$

Система представителей правых смежных классов называется *шрейеровской* (*шрайеровской*), если начало каждого представителя само является представителем. Переписывающий процесс Рейдемейстера (Райдемайстера) на основе шрейеровской (шрайеровской) системы представителей правых смежных классов называется *переписывающим процессом Рейдемейстера – Шрейера* (*переписывающим процессом Райдемайстера – Шрайера*) и обозначается через $\tau_{R,S}$.

Использование шрейеровской системы представителей правых смежных классов и переписывающего процесса Рейдемейстера – Шрейера приводят к следующей теореме, с доказательством которой также можно ознакомиться по монографии [8].

Теорема 4. *Подгруппа H имеет следующее задание образующими и определя-*

ющими соотношениями

$$\langle\langle \{\, s_{K,a_j} \,|\, j \in J,$$
$$K - \textit{произвольный шрейеровский представитель правого смежного класса } \} \,|$$
$$\{\, s_{M,a_j} = 1 \,|\, j \in J,$$
$$M - \textit{произвольный шрейеровский представитель правого смежного класса и слова}$$
$$\overline{Ma_j} \textit{ и } Ma_j \textit{ свободно равны } \} \cup$$
$$\{\, \tau_{R,S}(KRK^{-1}) = 1 \,|\, R = 1 - \textit{ произвольное соотношение из множества } \mathcal{R}$$
$$\textit{определяющих соотношений для группы } G,$$
$$K - \textit{произвольный шрейеровский представитель правого смежного класса } \} \rangle\rangle.$$

Следствие 1. *Любая подгруппа любой свободной группы сама является свободной группой.*

Вопросы для самопроверки

1. Как по заданию группы образующими и определяющими соотношениями можно найти задание ее подгруппы и факторгруппы?
2. Что такое система представителей правых смежных классов группы по ее подгруппе?
3. Что такое переписывающий процесс?
4. Что такое шрейеровская система представителей правых смежных классов группы по ее подгруппе?

7. Теорема Зейферта – ван Кампена

Предположим, что топологическое пространство U является объединением двух открытых линейно связных множеств U_1 и U_2 с непустым линейно связным пересечением $U_1 \cap U_2$. Рассмотрим диаграмму вложений

$$\begin{array}{ccccc} & & U_1 & & \\ & \overset{\varphi_1}{\nearrow} & & \overset{\psi_1}{\searrow} & \\ U_1 \cap U_2 & & & & U. \\ & \underset{\varphi_2}{\searrow} & & \underset{\psi_2}{\nearrow} & \\ & & U_2 & & \end{array}$$

Если в качестве отмеченной точки выбрать точку $p \in U_1 \cap U_2$, то из предыдущей коммутативной диаграммы непрерывных отображений получим следу-

ющую коммутативную диаграмму гомоморфизмов фундаментальных групп

$$\begin{array}{ccccc} & & \pi(U_1,p) & & \\ & \overset{\varphi_1^*}{\nearrow} & & \overset{\psi_1^*}{\searrow} & \\ \pi(U_1\cap U_2,p) & & & & \pi(U,p). \\ & \underset{\varphi_2^*}{\searrow} & & \underset{\psi_2^*}{\nearrow} & \\ & & \pi(U_2,p) & & \end{array}$$

Рассмотрим задания фундаментальных групп образующими и определяющими соотношениями

$$\pi(U_1\cap U_2,p) \,=\, \langle\langle\, \mathcal{A}_0 \,|\, \mathcal{R}_0 \,\rangle\rangle, \quad \pi(U_1,p) \,=\, \langle\langle\, \mathcal{A}_1 \,|\, \mathcal{R}_1 \,\rangle\rangle, \quad \pi(U_2,p) \,=\, \langle\langle\, \mathcal{A}_2 \,|\, \mathcal{R}_2 \,\rangle\rangle.$$

При этом считаем, что $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$.

Обозначим через $\mathcal{R}_3$ следующее множество соотношений в групповом алфавите $\mathcal{A}_1 \cup \mathcal{A}_2$

$$\mathcal{R}_3 \,=\, \{\, \varphi_1^*(a) \,=\, \varphi_2^*(a) \,|\, a \in \mathcal{A}_0 \,\},$$

где для каждого образующего $a \in \mathcal{A}_0$ через $\varphi_1^*(a)$ (соответственно $\varphi_2^*(a)$) обозначено соответствующее слово в групповом алфавите $\mathcal{A}_1$ (соответственно $\mathcal{A}_2$).

Теорема 5 (Зейферт – ван Кампен)**.** *Фундаментальная группа $\pi(U,p)$ имеет следующее задание образующими и определяющими соотношениями*

$$\pi(U,p) \,=\, \langle\langle\, \mathcal{A}_1 \cup \mathcal{A}_2 \,|\, \mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3 \,\rangle\rangle.$$

Рассмотрим применение фундаментальных групп для доказательства важной теоремы топологии – ***теоремы Брауэра о неподвижной точке***.

Обозначим через $B_n(r)$ *стандартный шар* радиуса r в n-мерном пространстве $\mathbb{R}^n$, т. е.

$$B_n(r) \,=\, \{\, (x_1,\ldots,x_n) \,|\, (x_1,\ldots,x_n) \in \mathbb{R}^n \,\&\, x_1^2 \,+\, \cdots \,+\, x_n^2 \,\leq\, r^2 \,\},$$

а через $S_n(r)$ – *стандартную сферу* радиуса r в n-мерном пространстве $\mathbb{R}^n$, т. е.

$$S_n(r) \,=\, \{\, (x_1,\ldots,x_n) \,|\, (x_1,\ldots,x_n) \in \mathbb{R}^n \,\&\, x_1^2 \,+\, \cdots \,+\, x_n^2 \,=\, r^2 \,\}.$$

Сфера $S_n(r)$ как *граница шара* $B_n(r)$ часто обозначается через $\partial B_n(r)$.

Теорема 6 (Брауэр)**.** *Для любого непрерывного отображения f шара $B_n(r)$ в себя найдется такая точка $a \in B_n(r)$, для которой выполнено равенство $f(a) = a$, т. е. точка a отображением f оставляется на месте (неподвижная точка отображения f).*

Доказательство. проведем методом от противного. Предположим, что для любой точки $x \in B_n(r)$ выполняется неравенство $f(x) \neq x$. Построим непрерывное отображение φ шара $B_n(r)$ на его границу $S_n(r)$, при котором все точки сферы $S_n(r)$ неподвижны. Для этого рассмотрим луч, идущий из точки $f(x)$ в точку x и через $\varphi(x)$ обозначим точку пересечения этого луча со сферой $S_n(r)$. Нетрудно проверить, что φ – непрерывное отображение шара $B_n(r)$ на его границу $S_n(r)$ и при этом все точки сферы $S_n(r)$ неподвижны. (Пояснения. Уравнение луча $y = f(x)+t(x-f(x))$, $t \geq 0$. Для нахождения точки пересечения луча с граничной сферой получаем уравнение $t^2||x-f(x)||^2+2t(f(x),x-f(x))+||f||^2-r^2 = 0$, где как обычно $||u||^2 = (u,u)$. Поэтому

$$t_0 = \frac{-(f(x),x-f(x)) + \sqrt{(f(x),x-f(x))^2 + (r^2-||f||^2)||x-f(x)||^2}}{||x-f(x)||^2},$$

$$\varphi(x) = f(x) + t_0(x-f(x)).$$

Обозначим через E естественное вложение сферы $S_n(r)$ в шар $B_n(r)$, а через I – тождественное отображение сферы $S_n(r)$ на себя. Получаем равенство $\varphi \circ E = I$. Выбрав $p \in S_n(r)$, получим гомоморфизмы групп

$$\pi(S_n(r),p) \stackrel{E_*}{\to} \pi(B_n(r),p) \stackrel{\varphi_*}{\to} \pi(S_n(r),p)$$

и равенства

$$\varphi_* \circ E_* = (\varphi \circ E)_* = I_* = Id,$$

из которого следует, что φ_* – сюръекция, а E_* – инъекция.

Легко показать, что *группа* $\pi(B_n(r),p)$ *тривиальна.*

Можно показать, хотя это и не так просто, что при $n = 2$ группа $\pi(S_2(r),p)$ отображением *бесконечная циклическая*, хотя для получения противоречия достаточно использовать нетривиальность этой группы.

Итак, при $n = 2$ теорема доказана. При $n > 2$ вместо фундаментальной группы (первой гомотопической группы) необходимо использовать, например, высшие гомотопические группы, так как в этом случае группа $\pi(S_n(r),p)$ тоже тривиальна. Этот случай мы оставляем без доказательства. □

Напомним, что узлы $K_1 \subseteq \mathbb{R}^3$ и $K_2 \subseteq \mathbb{R}^3$ называются *эквивалентными*, если существует такой гомеоморфизм φ пространства $\mathbb{R}^3$, что

$$\varphi(K_1) = K_2.$$

Узлы $K_1 \subseteq \mathbb{R}^3$ и $K_2 \subseteq \mathbb{R}^3$ называются *строго эквивалентными*, если существует такой гомеоморфизм ψ пространства $\mathbb{R}^3$, что ψ сохраняет ориентацию этого пространства и

$$\psi(K_1) = K_2.$$

Справедлива следующая теорема, доказательство которой требует привлечения достаточно сложного материала из топологии.

Теорема 7. *Узлы $K_1 \subseteq \mathbb{R}^3$ и $K_2 \subseteq \mathbb{R}^3$ строго эквивалентны тогда и только тогда, когда существует такое положительное число C и такой гомеоморфизм φ пространства $\mathbb{R}^3$, что*

$$\varphi(K_1) = K_2$$

и для любого $u \in \mathbb{R}^3$: если $||u|| \geq C$, то $\varphi(u) = u$.

Ручные узлы – это замкнутые ломаные линии без самопересечений в $\mathbb{R}^3$.

$K \subseteq \mathbb{R}^3$ – узел в $\mathbb{R}^3$. Пусть $p \in \mathbb{R}^3 \setminus K$. Тогда фундаментальная группа $\pi(\mathbb{R}^3 \setminus K, p)$ называется *группой узла* K и обозначается через $G(K)$.

Справедлива следующая теорема, доказательство которой базируется на теореме Зейферта – ван Кампена и требует привлечения достаточно сложного материала из топологии.

Теорема 8. *Группа $G(K)$ ручного узла K имеет задание вида*

$$G(K) = \langle\langle\, a_1, \ldots, a_n \,|\, a_1 = a_{i_1}^{\varepsilon_1} a_2 a_{i_1}^{-\varepsilon_1},\ a_2 = a_{i_2}^{\varepsilon_2} a_3 a_{i_2}^{-\varepsilon_2},\ \ldots,$$
$$a_{n-1} = a_{i_{n-1}}^{\varepsilon_{n-1}} a_n a_{i_{n-1}}^{-\varepsilon_{n-1}},\ a_n = a_{i_n}^{\varepsilon_n} a_1 a_{i_n}^{-\varepsilon_n} \,\rangle\rangle,$$

где $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$, а $i_1, \ldots, i_n \in \{1, 2, \ldots, n\}$.

Любое одно из определяющих соотношений можно опустить.

Следствие 2. *Факторгруппа $G(K)/[G(K), G(K)]$ группы $G(K)$ ручного узла K по ее коммутанту $[G(K), G(K)]$ является бесконечной циклической группой.*

Вопросы для самопроверки

1. Дайте определение неподвижной точки отображения.
2. Сформулируйте теорему Брауэра о неподвижной точке.
3. Приведите примеры применения теоремы Брауэра о неподвижной точке.
4. Докажите, что факторгруппа ручного узла по ее коммутанту является бесконечной циклической.

8. Преобразования Тице

Рассмотрим некоторые преобразования заданий групп образующими и определяющими соотношениями. Зафиксируем произвольное задание группы образующими и определяющими соотношениями

$$\langle\langle\, \mathcal{A} \,|\, \mathcal{S} \,\rangle\rangle. \tag{I}$$

Напомним, что

$$\mathcal{A}^{-1} = \{\, a^{-1} \,|\, a \in \mathcal{A} \,\},$$

$\mathcal{A}^{-1}$ называется *алфавитом букв-двойников*, а $\mathcal{A}\cup\mathcal{A}^{-1}$ – *групповым алфавитом*. Каждое *формальное равенство* вида $A = B$, где A и B – слова в групповом алфавите, называется *соотношением*. Если $A \overset{\mathcal{S}}{\sim} B$, то говорят, что *соотношение $A = B$ является следствием множества соотношений $\mathcal{S}$* или что *соотношение $A = B$ следует (выводимо) из множества соотношений $\mathcal{S}$*, и обозначают это утверждение через $\mathcal{S} \vdash A = B$.

Если $\mathcal{R}$ – некоторое множество соотношений, каждое из которых следует (выводимо) из множества соотношений $\mathcal{S}$, то рассмотрим новое задание группы образующими и определяющими соотношениями

$$\langle\langle\, \mathcal{A} \,|\, \mathcal{S} \cup \mathcal{R} \,\rangle\rangle. \tag{II}$$

Нетрудно проверить, что для любых двух слов C и D в групповом алфавите справедлива эквивалентность

$$C \overset{\mathcal{S}}{\sim} D \quad\Longleftrightarrow\quad C \overset{\mathcal{S}\cup\mathcal{R}}{\sim} D.$$

Поэтому для любого слова C в групповом алфавите справедливо равенство

$$[C]_{\underset{\sim}{\mathcal{S}}} = [C]_{\underset{\sim}{\mathcal{S}\cup\mathcal{R}}}.$$

Значит, группы с заданиями (I) и (II) совпадают.

Переход от задания (I) к заданию (II) называется *преобразованием Тице первого типа*, а обратный переход от задания (II) к заданию (I) называется *преобразованием Тице второго типа*.

Рассмотрим еще два типа преобразований Тице. Буквы алфавита $\mathcal{R}$ будем обозначать через a_i.

Выбираем произвольное конечное или счетное множество слов $\{\, W_j(a_i) \,|\, j \in J \,\}$. Для каждого из этих слов $W_j(a_i)$ выберем *новую букву* b_j и рассмотрим новое задание группы образующими и определяющими соотношениями

$$\langle\langle\, \mathcal{A} \cup \{\, b_j \,|\, j \in J \,\} \,|\, \mathcal{S} \cup \{\, b_j = W_j(a_i) \,|\, j \in J \,\} \,\rangle\rangle. \tag{III}$$

Переход от задания (I) к заданию (III) называется *преобразованием Тице третьего типа*, а обратный переход от задания (III) к заданию (I) называется *преобразованием Тице четвертого типа*.

Для краткости обозначим через $\mathcal{S}_1$ множество $\{\, b_j = W_j(a_i) \,|\, j \in J \,\}$ *новых соотношений*.

Нетрудно проверить, что для любых двух слов C и D в групповом алфавите $\mathcal{A}$ справедлива эквивалентность

$$C \overset{\mathcal{S}}{\sim} D \quad\Longleftrightarrow\quad C \overset{\mathcal{S}\cup\mathcal{S}_1}{\sim} D.$$

Значит, отображение

$$\varphi : [C]_{\underset{\sim}{\mathcal{S}}} \quad\to\quad [C]_{\underset{\sim}{\mathcal{S}\cup\mathcal{S}_1}}$$

задает изоморфизм группы с заданием (I) на группу с заданием (III).

Поэтому если от одного задания образующими и определяющими соотношениями можно перейти к другому заданию образующими и определяющими соотношениями, то соответствующие группы изоморфны. Справедливо и обратное утверждение, на доказательстве которого мы не будем останавливаться, а сформулируем лишь итоговую важную теорему.

Теорема 9. *Два задания образующими и определяющими соотношениями задают изоморфные группы тогда и только тогда, когда от одного из них можно перейти к другому с помощью конечного числа преобразований Тице.*

Вопросы для самопроверки

1. Докажите, что преобразования Тице приводят к изоморфным группам.
2. Верно ли, что любое преобразование Тице можно заменить на конечную последовательность простых (элементарных) преобразований Тице?
3. Приведите примеры упрощения представлений групп с помощью преобразований Тице.

9. Свободное дифференциальное исчисление

Для произвольной группы G через $\mathbb{Z}[G]$, как обычно, обозначаем ее *целочисленное групповое кольцо*, элементами которого являются "формальные суммы" вида

$$\sum_{g\in G} m_g g,$$

где m_g – целые числа и лишь конечное число из них отлично от нуля. Операции сложения и умножения определяются естественным образом:

$$\sum_{g\in G} m_g g + \sum_{g\in G} n_g g = \sum_{g\in G} (m_g + n_g)g, \quad \sum_{g\in G} m_g g \cdot \sum_{g\in G} n_g g = \sum_{g\in G} \Big(\sum_{uv=g} m_u n_v\Big)\, g.$$

$\mathbb{Z}[G]$ – *ассоциативное кольцо с единицей*. Оно будет коммутативным тогда и только тогда, когда G – абелева группа.

Каждый групповой гомоморфизм $\varphi : G \to H$ естественным образом продолжается до гомоморфизма колец:

$$\varphi^* : \mathbb{Z}[G] \to \mathbb{Z}[H], \quad \varphi^*\Big(\sum_{g\in G} m_g g\Big) = \sum_{g\in G} m_g \varphi(g).$$

Через tr обозначается гомоморфизм (отображение) *тривиализации*, задаваемый равенством

$$tr\Big(\sum_{g\in G} m_g g\Big) = \Big(\sum_{g\in G} m_g\Big)e,$$

где e – нейтральный элемент группы G, т. е. tr – это продолжение на $\mathbb{Z}[G]$ тривиального гомоморфизма группы G.

Мы отождествляем элемент me группового кольца $\mathbb{Z}[G]$, где m – целое число, а e – нейтральный (единичный) элемент группы G с целым числом m, а элемент $1g$ группового кольца $\mathbb{Z}[G]$, где g – элемент группы G, отождествляем с элементом g. Это дает нам возможность считать, что

$$\mathbb{Z} \subseteq \mathbb{Z}[G], \quad G \subseteq \mathbb{Z}[G].$$

Дифференцирование D группового кольца $\mathbb{Z}[G]$ – это произвольное отображение

$$D : \mathbb{Z}[G] \to \mathbb{Z}[G],$$

удовлетворяющее условию: для любых двух элементов u и v кольца $\mathbb{Z}[G]$ выполняются равенства

$$D(u + v) = D(u) + D(v), \quad D(u \cdot v) = D(u) \cdot tr(v) + u \cdot D(v).$$

Легко проверить, что сумма $D_1 + D_2$ двух дифференцирований D_1 и D_2, заданная естественным образом

$$(D_1 + D_2)(u) = D_1(u) + D_2(u), \quad u \in \mathbb{Z}[G],$$

является дифференцированием. Кроме того, можно определить произведение дифференцирования D на элемент $v \in \mathbb{Z}[G]$ группового кольца (справа) равенством

$$(D \cdot v)(u) = D(u) \cdot v, \quad u \in \mathbb{Z}[G].$$

Легко проверить, что $D \cdot v$ является дифференцированием.

Обозначим через F_n свободную группу ранга n, свободные образующие которой по чисто техническим причинам нам будет удобно обозначать через x_1, ..., x_n.

Каждой свободной образующей x_i соответствует дифференцирование $\partial/\partial x_i$ – *частная производная по переменной* x_i, удовлетворяющее равенству

$$\frac{\partial x_j}{\partial x_i} = \delta_{ij},$$

где δ_{ij} – символ Кронекера. Тогда все дифференцирования целочисленного группового кольца $\mathbb{Z}[F_n]$ свободной группы F_n задаются равенством

$$D(u) = \sum_{i=1}^{n} \frac{\partial u}{\partial x_i} u_i(x_1, \ldots, x_n),$$

где $u_1(x_1, \ldots, x_n)$, ... , $u_n(x_1, \ldots, x_n)$ – элементы группового кольца $\mathbb{Z}[F_n]$. Так как

$$u_i(x_1, \ldots, x_n) = D(x_i),$$

то получаем равенство

$$D(u) = \sum_{i=1}^{n} \frac{\partial u}{\partial x_i} D(x_i).$$

Так как отображение

$$u \mapsto u - tr(u)$$

является дифференцированием, то справедливо равенство

$$u - tr(u) = \sum_{i=1}^{n} \frac{\partial u}{\partial x_i}(x_i - 1).$$

Пусть $w(x_1, \ldots, x_n)$, $u_1(x_1, \ldots, x_n)$, ..., $u_n(x_1, \ldots, x_n)$ – произвольные элементы свободной группы F_n и

$$W(x_1, \ldots, x_n) = w(u_1(x_1, \ldots, x_n), \ldots, u_n(x_1, \ldots, x_n)).$$

Тогда справедливо следующее равенство, которое называется *цепным правилом*, или правилом дифференцирования сложной функции

$$\frac{\partial W(x_1, \ldots, x_n)}{\partial x_i} = \sum_{j=1}^{n} \frac{\partial w(x_1, \ldots, x_n)}{\partial x_j} \cdot \frac{\partial u_j(x_1, \ldots, x_n)}{\partial x_i}.$$

Любое отображение

$$\begin{array}{ccc} x_1 & \mapsto & u_1(x_1, \ldots, x_n) \\ \ldots & \ldots & \ldots \\ x_n & \mapsto & u_n(x_1, \ldots, x_n) \end{array}$$

однозначно продолжается до эндоморфизма φ свободной группы F_n. При этом справедливы эквивалентности:

φ – автоморфизм свободной группы $F_n \iff$
$u_1(x_1, \ldots, x_n), \ldots, u_n(x_1, \ldots, x_n)$ – образующие свободной группы $F_n \iff$
$u_1(x_1, \ldots, x_n), \ldots, u_n(x_1, \ldots, x_n)$ – свободные образующие свободной группы F_n.

В связи с этим представляет интерес следующая теорема.

Теорема 10 (Birman J.S.). *Элементы $u_1(x_1, \ldots, x_n)$, ..., $u_n(x_1, \ldots, x_n)$ свободной группы F_n являются ее свободными образующими тогда и только тогда, когда в целочисленном групповом кольце $\mathbb{Z}[F_n]$ матрица из частных производных*

$$\begin{pmatrix} \frac{\partial u_1}{\partial x_1} & \frac{\partial u_1}{\partial x_2} & \ldots & \frac{\partial u_1}{\partial x_n} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{\partial u_n}{\partial x_1} & \frac{\partial u_n}{\partial x_2} & \ldots & \frac{\partial u_n}{\partial x_n} \end{pmatrix}$$

имеет левую обратную матрицу.

А.Ф. Красников получил интересное, далеко идущее обобщение этой теоремы.

Для произвольной группы G и ее нормальной подгруппы N естественный гомоморфизм

$$\varphi : G/[N, N] \to G/N$$

однозначно продолжается до гомоморфизма групповых колец

$$\varphi : \mathbb{Z}[G/[N,N]] \to \mathbb{Z}[G/N].$$

Это дает возможность рассматривать дифференцирования группового кольца $\mathbb{Z}[G/[N,N]]$ со значениями в групповом кольце $\mathbb{Z}[G/N]$: любому дифференцированию

$$D : \mathbb{Z}[G/[N,N]]] \to \mathbb{Z}[G/[N,N]]$$

группового кольца $\mathbb{Z}[G/[N,N]]$ со значениями в нем самом можно сопоставить дифференцирование

$$\varphi \circ D : \mathbb{Z}[G/[N,N]] \to \mathbb{Z}[G/N]$$

группового кольца $\mathbb{Z}[G/[N,N]]$ со значениями в групповом кольце $\mathbb{Z}[G/N]$. Можно рассматривать частные дифференцирования $\varphi \circ \partial/\partial x_i$ группового кольца $\mathbb{Z}[F_n/[N,N]]$ со значениями в групповом кольце $\mathbb{Z}[F_n/N]$, где F_n – свободная группа ранга n со свободными образующими x_1, ..., x_n.

Теорема 11 (А.Ф. Красников)**.** *Элементы $u_1(x_1,\ldots,x_n)$, ..., $u_n(x_1,\ldots,x_n)$ группы $F_n/[N,N]$ являются ее образующими тогда и только тогда, когда в целочисленном групповом кольце $\mathbb{Z}[F_n/N]$ матрица из частных производных*

$$\begin{pmatrix} \varphi \circ \frac{\partial u_1}{\partial x_1} & \varphi \circ \frac{\partial u_1}{\partial x_2} & \ldots & \varphi \circ \frac{\partial u_1}{\partial x_n} \\ \ldots & \ldots & \ldots & \ldots \\ \varphi \circ \frac{\partial u_n}{\partial x_1} & \varphi \circ \frac{\partial u_n}{\partial x_2} & \ldots & \varphi \circ \frac{\partial u_n}{\partial x_n} \end{pmatrix}$$

имеет левую обратную матрицу.

Хорошо известна эквивалентность

$$w(x_1,\ldots,x_n) \in [N,N] \iff \mathop{\&}_{i=1}^{n} \varphi \circ \frac{\partial w}{\partial x_i} = 0 \text{ в групповом кольце } \mathbb{Z}[F_n/N],$$

на основе которой легко построить алгоритм, решающий проблему вхождения в коммутанты $F_n^{(k)}$ свободной группы F_n.

Вопросы для самопроверки

1. Что такое свободное дифференциальное исчисление Фокса?

2. Определите понятие частной производной для элемента свободной группы с использованием представителей классов эквивалентных слов.

3. Докажите независимость предыдущего определения от выбора представителя класса.

10. Некоторые криптографические протоколы на группах

В описываемых ниже протоколах используются общепринятые в алгебре обозначения: $g^a = aga^{-1}$ – *элемент, сопряженный с элементом* g *посредством элемента* a и $[a,b] = aba^{-1}b^{-1}$ – *коммутатор элементов* a и b. Хорошо известны равенства $(g^a)^b = g^{ba}$ и $[a,b]^{-1} = [b,a]$.

Протокол Anschel-Anschel-Goldfeld

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) группу G – *платформу протокола.*

В первоначальном варианте протокола в качестве группы G выбиралась группа $B(n)$ кос на n нитях. Некоторое обоснование такого выбора будет приведено ниже.

Для выработки общего *сеансового ключа* Алиса выбирает (открыто) набор элементов

$$a_1,\, a_2,\, \ldots,\, a_p \in G.$$

Боб выбирает (открыто) набор элементов

$$b_1,\, b_2,\, \ldots,\, b_q \in G.$$

Группа G и указанные наборы элементов – *открытый ключ (public key).*

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретный (private)* элемент

$$u = u(a_1, a_2, \ldots, a_p),$$

вычисляет элементы

$$b_1' = ub_1u^{-1},\, b_2' = ub_2u^{-1},\, \ldots\, b_q' = ub_qu^{-1}$$

(набор элементов группы G, сопряженных с открытым (public) набором Боба посредством ее секретного элемента) и по открытому каналу пересылает этот набор Бобу.

Боб "*случайным образом*" выбирает *секретный (private)* элемент

$$v = v(b_1, b_2, \ldots, b_q),$$

вычисляет элементы

$$a_1' = va_1v^{-1},\, a_2' = va_2v^{-1},\, \ldots\, a_p' = va_pv^{-1}$$

(набор элементов группы G, сопряженных с открытым (public) набором Алисы посредством его секретного элемента) и по открытому каналу пересылает этот набор Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент

$$W_A = uu(a'_1, a'_2, \ldots, a'_p)^{-1} = uvu^{-1}v^{-1} = [u, v].$$

Боб вычисляет элемент

$$W_B = vv(b'_1, b'_2, \ldots, b'_q)^{-1} = vuv^{-1}u^{-1} = [v, u] = [u, v]^{-1}.$$

Общий секретный ключ

Элемент $K = [u, v]$ – общий секретный ключ Алисы и Боба.

Мы не будем подробно обсуждать криптостойкость описанного протокола, сделаем лишь отдельные замечания. Ясно, что базу протокола составляет работа с наборами сопряженных элементов группы G. Поэтому в качестве подходящих для реализации протокола групп G естественно выбирать группы, в которых проблема сопряженности "*трудно разрешима*", а возможно даже и алгоритмически неразрешима. Кроме того, возникает проблема работы с элементами группы G и проблема "*конструктивного*" задания самой группы G. На сегодняшний день в качестве "достаточно удобного конструктивного задания" бесконечных некоммутативных групп может рассматриваться задание групп конечным числом образующих и конечным (рекурсивным) множеством определяющих соотношений. В этом случае элементы группы G заменяются представителями – словами в групповом алфавите образующих, но тогда возникает *проблема однозначности*, которая может быть решена с использованием *канонических форм записи элементов*, т. е. в каждом классе эквивалентных слов выделяется единственное слово. Оно называется *канонической формой* и переход от произвольного слова, задающего данный элемент, к канонической форме должен быть "достаточно простым". Именно по этим причинам в первоначальном варианте протокола в качестве группы G выбиралась группа $B(n)$ кос на n нитях. Известно, что проблема сопряженности в группах кос является "достаточно трудной", хотя и разрешимой. Группы кос имеют простое задание образующими и определяющими соотношениями, для них существуют весьма удобные канонические формы записи элементов.

Протокол Ko – Lee – Cheon – Han – Kang – Park

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) группу G – *платформу протокола*, два конечных подмножества U_A и U_B попарно коммутирующих элементов и элемент $g \in G$. Тогда попарно коммутируют и элементы подгрупп $A = gr(U_A)$ и $B = gr(U_B)$ группы G.

В первоначальном варианте протокола в качестве группы G выбиралась группа $B(n)$ кос на $n = 2k+1 \geq 5$ нитях. $U_A = \{\sigma_1, \ldots, \sigma_k\}$ $U_B = \{\sigma_{k+2}, \ldots, \sigma_{2k+1}\}$. В этом случае подгруппы A и B изоморфны группе $B(k)$ кос на k нитях.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретный (private)* элемент a, вычисляет элемент g^a и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретный (private)* элемент b, вычисляет элемент g^b и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = (g^b)^a = g^{ab}$.

Боб вычисляет элемент $K_B = (g^a)^b = g^{ba}$.

Общий секретный ключ

$K = K_A = K_B$.

Протокол Wang – Cao – Okamoto – Shao

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) некоммутативный моноид G – *платформу протокола*, элемент $g \in G$ и *обратимый* элемент $x \in G$.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретное (private)* натуральное число $\alpha \in N$, вычисляет элемент g^{x^α} и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретное (private)* натуральное число $\beta \in N$, вычисляет элемент g^{x^β} и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = (g^{x^\beta})^{x^\alpha} = g^{x^{\alpha+\beta}}$.

Боб вычисляет элемент $K_B = (g^{x^\alpha})^{x^\beta} = g^{x^{\beta+\alpha}}$.

Общий секретный ключ

$K = K_A = K_B$.

Криптографическая стойкость рассмотренных криптоалгоритмов (криптопротоколов) обосновывается сложностью задачи *нахождения сопрягающего элемента*. Но в отличие от "*классической*" постановки *проблемы сопряженности*, восходящей к фундаментальной работе М. Дэна и состоящей в определении, имеет ли уравнение $h = xgx^{-1}$ решение в группе G, в формулировке задачи *нахождения сопрягающего элемента* известно, что это уравнение имеет решение и требуется его найти. Сложность последней задачи в настоящее время мало изучена.

Однако В. А. Романьков получил достаточно неожиданный результат: он предложил "обходной" путь "взлома" описанных выше и многих других криптопротоколов, в той или иной мере использующих сопряженные элементы, без нахождения самих сопрягающих элементов. В. А. Романьков показал, что если группа G линейна, т. е. изоморфна при некотором n и "конструктивном" поле F подгруппе полной линейной группы $GF(n, F)$, то описанные протоколы "взламываются" за полиномиальное время разработанным им общим методом.

Следующие протоколы базируются на полугрупповом или групповом умножении

Протокол Сидельников В. М. – Черепнев М. А. – Ященко В. Ю.

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) полугруппу (моноид, группу) G – *платформу протокола*, два конечных подмножества U_A и U_B по-

парно коммутирующих элементов и элемент $g \in G$. Тогда попарно коммутируют элементы подполугрупп $A = subsemigroup(U_A)$ и $B = subsemigroup(U_B)$ полугруппы G.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретные (private)* элементы $a, a' \in A$, вычисляет элемент aga' и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретные (private)* элементы $b, b' \in B$, вычисляет элемент bgb' и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = a(bgb')a' = (ab)g(b'a')$.

Боб вычисляет элемент $K_B = b(aga')a' = (ba)g(a'b')$.

Общий секретный ключ

$K = K_A = K_B = abgb'a'$.

Основную идею этого протокола Сидельникова В. М. – Черепнева М. А. – Ященко В. Ю. 1994 года можно обнаружить в целом ряде более поздних протоколов других авторов, отличительной особенностью которых является указание конкретных полугрупп и групп, впрочем, как правило, линейных, а как показал В. А. Романьков в этом случае протокол не может считаться криптографически стойким.

Протокол Stickel

Начальная установка

G – неабелева конечная группа, а f и g – два ее коммутирующих элемента, $l_0 = ordf$ и $k_0 = ordg$ – порядки этих элементов.

G, f, g, l_0 и g_0 – *открытые данные.*

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретные (private)* натуральные числа $1 < k < k_0$ $1 < l < l_0$, вычисляет элемент $g^k f^l$ и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретные (private)* натуральные числа $1 < r < k_0$ $1 < s < l_0$, вычисляет элемент $g^r f^s$ и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = g^k(g^r f^s)f^l = g^{k+r} f^{s+l}$.

Боб вычисляет элемент $K_B = g^r(g^k f^l)f^s = g^{r+k} f^{l+s}$.

Общий секретный ключ

$K = K_A = K_B$.

Описанный протокол очевидным образом переносится на случай произвольной группы G. При этом, как показал В. А. Романьков, для криптостойкости протокола следует прежде всего потребовать, чтобы группа G не была линейной.

Следующие протоколы базируются на групповых автоморфизмах и эндоморфизмах.

Для произвольной алгебраической системы G (полугруппа, моноид, группа, кольцо и т. д.) через $End(G)$ (соответственно $Aut(G)$) как обычно обозначаем

ее полугруппу эндоморфизмов, т. е. гомоморфизмов системы G в себя (соответственно группу автоморфизмов, т.е. биективных гомоморфизмов системы G на себя). Для произвольного эндоморфизма $\alpha \in End(G)$ и произвольного элемента $g \in G$ через g^α будем обозначать образ $\alpha(g)$ элемента g относительно эндоморфизма α.

Протокол Mahalanobis

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) группу G – *платформу протокола*, два конечных подмножества U_A и U_B попарно коммутирующих элементов группы автоморфизмов $Aut(G)$ и элемент $g \in G$. Тогда попарно коммутируют элементы подгрупп $A = gr(U_A)$ и $B = gr(U_B)$ группы автоморфизмов $Aut(G)$.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретный (private)* автоморфизм $\alpha \in A$, вычисляет элемент g^α и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретный (private)* автоморфизм $\beta \in B$, вычисляет элемент g^β и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = (g^\beta)^\alpha = g^{\alpha\cdot\beta}$.

Боб вычисляет элемент $K_B = (g^\alpha)^\beta = g^{\beta\cdot\alpha}$.

Общий секретный ключ

$K = K_A = g^{\alpha\cdot\beta} = g^{\beta\cdot\alpha} = K_B$.

Протокол Mahalanobis

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) группу G – платформу протокола, два конечных подмножества U_A и U_B попарно коммутирующих элементов группы автоморфизмов $Aut(G)$ и элемент $g \in G$. Тогда попарно коммутируют элементы подгрупп $A = gr(U_A)$ и $B = gr(U_B)$ группы автоморфизмов $Aut(G)$.

Выработка материалов для создания общего секретного ключа

Алиса "случайным образом" выбирает секретный (private) автоморфизм $\alpha \in A$, вычисляет элемент g^α и пересылает его Бобу.

Боб "случайным образом" выбирает секретный (private) автоморфизм $\beta \in B$, вычисляет элемент $(g^\alpha)^\beta$ и пересылает его Алисе.

Алиса вычисляет элемент $((g^\alpha)^\beta)^{\alpha^{-1}=g^\beta}$.

Алиса "случайным образом" выбирает еще один секретный (private) автоморфизм $\gamma \in A$, вычисляет элемент $(g^\beta)^\gamma$ и пересылает его Бобу.

Выработка общего секретного ключа

Алиса вычисляет элемент $K_A = g^\gamma$.

Боб вычисляет элемент $K_B = ((g^\beta)^\gamma)^{\beta^{-1}}$.

Общий секретный ключ

$K = K_A = g^\gamma = K_B$.

Протокол Habeeb – Kahrobaei – Koupparis – Shpilrain

В этом протоколе используется понятие *голоморфа* $Hol(G)$ полугруппы (группы) G. Через $Hol(G)$ обозначается множество $Aut(G) \times G$, на котором операция умножения задается следующим равенством:

$$(\alpha, g) \cdot (\beta, h) \;=\; (\alpha\beta, \beta(g)h).$$

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) полугруппу или группу G – *платформу протокола*, автоморфизм $\alpha \in Aut(G)$ и элемент $g \in G$.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретное (private)* натуральное число $m \in N$, вычисляет элемент голоморфа $Hol(G)$

$$(\alpha, g)^m \;=\; (\alpha^m, \alpha^{m-1}(g) \cdot \alpha^{m-2}(g) \cdot \ldots \cdot \alpha^2(g) \cdot \alpha(g) \cdot g)$$

и пересылает Бобу только вторую компоненту

$$a_m \;=\; \alpha^{m-1}(g) \cdot \alpha^{m-2}(g) \cdot \ldots \cdot \alpha^2(g) \cdot \alpha(g) \cdot g.$$

Боб "*случайным образом*" выбирает *секретное (private)* натуральное число $n \in N$, вычисляет элемент голоморфа $Hol(G)$

$$(\alpha, g)^n \;=\; (\alpha^n, \alpha^{n-1}(g) \cdot \alpha^{n-2}(g) \cdot \ldots \cdot \alpha^2(g) \cdot \alpha(g) \cdot g)$$

и пересылает Алисе только вторую компоненту

$$a_n \;=\; \alpha^{n-1}(g) \cdot \alpha^{n-2}(g) \cdot \ldots \cdot \alpha^2(g) \cdot \alpha(g) \cdot g.$$

Выработка общего секретного ключа

Алиса вычисляет элемент

$$(*, a_n) \cdot (\alpha^m, a_m) \;=\; (* \cdot \alpha^m, \alpha^m(a_n) \cdot a_m) \;=\; (* \cdot \alpha^m, a_{n+m}).$$

$K_A \;=\; a_{n+m}$.

Боб вычисляет элемент

$$(**, a_m) \cdot (\alpha^n, a_n) \;=\; (** \cdot \alpha^n, \alpha^n(a_m) \cdot a_n) \;=\; (** \cdot \alpha^n, a_{m+n}).$$

$K_B \;=\; a_{m+n}$.

Общий секретный ключ

$K \;=\; K_A \;=\; a_{n+m} \;=\; a_{m+n} \;=\; K_B$.

Рассмотрим протоколы аутентификации, основанные на некоторых алгоритмических проблемах теории групп, которые по ряду причин можно отнести к *сложным алгоритмическим проблемам.*

Протокол Романькова – Григорьева – Шпильрайна

Криптографическая стойкость этого протокола базируется на сложности *проблемы эндоморфной сводимости* для групп.

Начальная установка

Открыто выбирается бесконечная "*эффективно заданная*", например, конечно определенная в некотором многообразии, группа G – платформа протокола с разрешимой проблемой равенства, но с *алгоритмически неразрешимой проблемой эндоморфной сводимости* или, по крайней мере, "*трудной*" *проблемой эндоморфной сводимости.* В случае *алгоритмически неразрешимой проблемы эндоморфной сводимостидля группы G доказано, что невозможно построить алгоритм, позволяющий по произвольным двум элементам g и f этой группы определить, существует ли такой эндоморфизм φ этой группы, для которого выполняется равенство $\varphi(g) = f$.* В случае '*трудной*" *проблемы эндоморфной сводимости* требуются уточнения, например в терминах машин Тьюринга.

"***Система***" или "***Доказывающий***" выбирает элемент $g \in G$ и "публикует" его.

"*Секретный*" ключ "*Доказывающего*" – эндоморфизм $\varphi \in End(G)$.

"*Открытый*" ключ – элемент $f = \varphi(g)$ группы G.

Раунд аутентификации

"***Доказывающий***" выбирает "*случайным образом*" эндоморфизм $\psi \in End(G)$, вычисляет "***Обязательство***" – элемент $v = \psi(f)$ и отправляет его "***Проверяющему***".

"***Проверяющий***" генерирует "*случайным образом*" бит ε и отправляет его "***Доказывающему***".

Если $\varepsilon = 0$, то "***Доказывающий***" отправляет "***Проверяющему***" ψ, который должен проверить справедливость равенства

$$v = \psi(f).$$

Если $\varepsilon = 1$, то "***Доказывающий***" отправляет "***Проверяющему***" композицию эндоморфизмов $\chi = \psi \cdot \varphi$, который должен проверить справедливость равенства

$$v = \chi(g).$$

Открытые параметры: группа G, элемент $g \in G$ и *секретный параметр* – эндоморфизм $\varphi \in End(G)$ – выбираются таким образом, чтобы по элементу g и его образу относительно "*секретного*" эндоморфизма $\varphi \in End(G)$ $f = \varphi(g)$ было "*вычислительно трудно*" восстановить сам "*секретный*" эндоморфизм $\varphi \in End(G)$.

Протокол Шпильрайна – Ушакова

Криптографическая стойкость этого протокола базируется на сложности *проблемы скрученной сопряженности* для групп.

Начальная установка

Открыто выбирается группа G – *платформа протокола*, два ее эндоморфизма φ и ψ и элемент $w \in G$.

"*Секретный*" ключ "***Доказывающего***" – элемент $s \in G$.

"*Открытый*" ключ – элемент $t = \psi(s^{-1})w\varphi(s)$ группы G.

Раунд аутентификации

"***Доказывающий***" выбирает "*случайным образом*" элемент $r \in G$, вычисляет "***Обязательство***" – элемент $u = \psi(r^{-1})t\varphi(r)$ и отправляет его "***Проверяющему***".

"***Проверяющий***" генерирует "*случайным образом*" бит ε и отправляет его "***Доказывающему***".

Если $\varepsilon = 0$, то "***Доказывающий***" отправляет "***Проверяющему***" $v = r$, который должен проверить справедливость равенства

$$u = \psi(v^{-1})t\varphi(v).$$

Если $\varepsilon = 1$, то "***Доказывающий***" отправляет "***Проверяющему***" $v = sr$, который должен проверить справедливость равенства

$$u = \psi(v^{-1})w\varphi(v).$$

Корректность протокола базируется на равенстве

$$u = \psi((sr)^{-1})w\varphi(sr).$$

Протокол Мегрелишвили – Джинджихадзе

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) векторное пространство $V = F_2^n$ размерности n над полем F_2 – *платформу протокола*, квадратную матрицу A порядка n и вектор $v \in V$.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретное (private)* натуральное число k, вычисляет вектор $u = vA^k$ и пересылает его Бобу.

Боб "*случайным образом*" выбирает *секретное (private)* натуральное число l, вычисляет вектор $w = vA^l$ и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет вектор $K_A = wA^k$.

Боб вычисляет вектор $K_B = uA^l$.

Общий секретный ключ

$K = K_A = vA^{k+l} = K_B$.

В. А. Романьков показал, что в таком виде протокол не может считаться криптографически стойким. Ситуацию не спасает и переход к векторному пространству $V = GF(q)^n$ размерности n над произвольным конечным полем $GF(q)$. Возможно следующее обобщение протокола Мегрелишвили – Джинджихадзе.

Начальная установка

Корреспонденты Алиса и Боб выбирают (открыто) группу (полугруппу, моноид, кольцо) G – *платформу протокола*, эндоморфизм $\varphi \in End(G)$ и элемент $g \in G$.

Выработка материалов для создания общего секретного ключа

Алиса "*случайным образом*" выбирает *секретное (private)* натуральное число k, вычисляет элемент $u = \varphi^k(g)$ и пересылает его Бобу.

Боб "*случайным образом*" выбирает секретное (private) натуральное число l, вычисляет элемент $w = \varphi^l(g)$ и пересылает его Алисе.

Выработка общего секретного ключа

Алиса вычисляет вектор $K_A = \varphi^k(w)$.

Боб вычисляет вектор $K_B = \varphi^l(g)$.

Общий секретный ключ

$K = K_A = \varphi^{k+l}(g) = K_B$.

Так как в протоколе не используется алгебраическая структура на множестве G и тот факт, что φ – эндоморфизм (сохраняет алгебраическую структуру на G), то можно обобщить протокол до ситуации, когда G – непустое множество, а φ – отображение множества G в себя (необязательно подстановка). Но тогда возникают проблемы "компактного" задания элементов множества G и отображения φ. В случае когда G – конечно порожденная группа (полугруппа), элементы G задаются как слова от образующих, а гомоморфизм φ задается образами образующих.

В связи как с описанными протоколами, так и с другими протоколами, базирующимися на бесконечных неабелевых группах возникает ряд принципиальных вопросов, которые явно сформулированы и достаточно подробно обсуждались в ряде работ.

1) Прежде всего возникает вопрос об "*эффективном задании*" группы G – *платформы* криптоалгоритмов. Достаточно перспективным представляется рассмотрение групп, имеющих конечное задание в многообразиях нильпотентных, разрешимых и периодических групп, которые к настоящему времени достаточно хорошо изучены. При этом, наверное, следует предполагать, что для группы G разрешима проблема равенства слов, хотя можно привести примеры криптоалгоритмов на базе конечно определенных групп с алгоритмически неразрешимой проблемой равенства слов. Но в этом случае возникает проблема "компактного задания" группы G, так как известные в настоящее время группы с алгоритмически неразрешимой проблемой равенства слов имеют "достаточно сложное" задание.

2) В криптопротоколах, предназначенных для выработки общего ключа, возникает необходимость приведения "корреспондентами" результатов вычислений к *единому виду*. Поэтому обычно используются *группы с канонической формой записи элементов*.

3) Возникает следующий непростой вопрос: *какую алгоритмически неразрешимую или хотя бы "вычислительно трудную" проблему для групп поло-*

жить в основу криптоалгоритма?. В качестве таких проблем в большинстве случаев берется одна из следующих проблем: *проблема равенства слов*, *проблема сопряженности*, *проблема степеней*, *проблема вхождения в подгруппы*, *проблема степенной сопряженности* и некоторые их комбинации.

Система Росошека

Основные идеи.

Сообщения – элементы группового (полугруппового) кольца $K[G]$ группы (полугруппы) G с коэффициентами из кольца K.

Если $\sigma \in End(K)$ и $\tau \in End(G)$, то отображение φ, заданное равенством

$$\varphi(\sum_{g\in G} m_g g) = \sum_{g\in G} \sigma(m_g)\tau(g),$$

является эндоморфизмом группового (полугруппового) кольца $K[G]$.

Начальная установка

Алиса выбирает эндоморфизмы $\sigma \in End(K)$ и $\tau \in End(G)$ с таким расчетом, чтобы

$$C(\sigma) \neq gr(\sigma), \quad C(\tau) \neq gr(\tau).$$

Алиса выбирает эндоморфизмы $\overline{\sigma} \in End(K)$ и $\overline{\tau} \in End(G)$ с таким расчетом, чтобы

$$\overline{\sigma} \in (C(\sigma) \setminus gr(\sigma)), \quad \overline{\tau} \in (C(\tau) \setminus gr(\tau)),$$

и строит эндоморфизм φ

$$\varphi(\sum_{g\in G} m_g g) = \sum_{g\in G} \overline{\sigma}(m_g)\overline{\tau}(g).$$

Открытый ключ Алисы: эндоморфизмы σ и τ, обратимый элемент x группового кольца $K[G]$ и элемент $\varphi(x)$.

Для произвольной пары натуральных чисел (i, j) строится эндоморфизм

$$\psi_{i,j}(\sum_{g\in G} m_g g) = \sum_{g\in G} \sigma^i(m_g)\tau^j(g),$$

который коммутирует с эндоморфизмом φ, но "может не быть с ним просто связан".

Шифрование

Результат зашифрования сообщения m – это

$$c = ((x^{-1})^{\psi_{i,j}}, m \cdot (x^{\varphi})^{\psi_{i,j}}).$$

Расшифрование

Расшифрование определяется равенством

$$m = (m \cdot (x^{\varphi})^{\psi_{i,j}}) \cdot ((x^{-1})^{\psi_{i,j}})^{\varphi}.$$

Вопросы для самопроверки

1. Какие требования предъявляются к группам, выступающим в качестве платформы для криптоалгоритмов и криптопротоколов?

2. Приведите примеры криптпротоколов на групповой платформе.

Литература

[1] Адян, С. И. Алгоритмические проблемы для групп и полугрупп / С. И. Адян, В. Г. Дурнев // Успехи мат. наук. – 2000. – Т. 55, № 2. – С. 3–94.

[2] Володин, И. А. О проблеме алгоритмического распознавания стандартной трехмерной сферы / И. А. Володин, В. Е. Кузнецов, А. Т. Фоменко // Успехи мат. наук. – 1974. – Т. 29, № 5. – С. 71–168.

[3] Дурнев, В. Г. О системах уравнений на свободных нильпотентных группах / В. Г. Дурнев // Вопросы теории групп и гомолог. алгебры. – Ярославль : ЯрГУ, 1981. – С. 66–69.

[4] Каргаполов, М. И. Основы теории групп / М. И. Каргаполов, Ю. И. Мерзляков. – М. : Наука, 1982. – 288 с.

[5] Коксетер, Г. С. М. Порождающие элементы и определяющие соотношения дискретных групп / Г. С. М. Коксетер, У. О. Дж. Мозер. – М. : Наука, 1980. – 236 с.

[6] Курош, А. Г. Теория групп / А. Г. Курош. – М. : Наука, 1967. – 442 с.

[7] Линдон, Р. Комбинаторная теория групп / Р. Линдон, П. Шупп. – М. : Мир, 1980. – 447 с.

[8] Магнус, В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. – М. : Наука, 1974. – 456 с.

[9] Марков, А. А. Неразрешимость проблемы гомеоморфии / А. А. Марков // Докл. АН СССР. – 1958. – Т. 121, № 2. – С. 218–220.

[10] Марков, А. А. Основы алгебраической теория кос / А. А. Марков // Труды МИАН им. В. А. Стеклова. – 1945. – Т. 16. – 28 с.

[11] Матиясевич, Ю. В. Диофантовость перечислимых множеств / Ю. В. Матиясевич // ДАН СССР. – 1970. – Т. 130, № 3. – С. 495–498.

[12] Матиясевич, Ю. В. Десятая проблема Гильберта / Ю. В. Матиясевич. – М. : Наука, 1993. – 224 с.

[13] Новиков, П. С. Об алгоритмической неразрешимости проблемы тождества теории групп / П. С. Новиков // Докл. АН СССР. – 1952. – Т. 85, № 4. – С. 709–712.

[14] Новиков, П. С. Неразрешимость проблемы сопряженности в теории групп / П. С. Новиков // Изв. АН СССР. Сер. матем. – 1954. – Т. 18, – № 6. С. 485–524.

[15] Новиков, П. С. Об алгоритмической неразрешимости проблемы тождества слов в теории групп / П. С. Новиков // Труды МИАН. – 1955. – Т. 44. – С. 1–124.

[16] Романьков, В. А. О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах / В. А. Романьков // Алгебра и логика. – 1977. – Т. 16, № 4. – С. 457–471.

[17] Романьков, В. А. Об уравнениях в свободных метабелевых группах / В. А. Романьков // Сиб. мат. журн. – 1979. – Т. 20, № 3. С. 671–673.

[18] Романьков, В. А. Алгебраическая криптография / В. А. Романьков. – Омск : Изд-во. Ом. гос. ун-та., 2013. – 240 с.

[19] Сидельников, В. М. Системы открытого распределения ключей на основе некоммутативных полурупп / В. М. Сидельников, М. А. Черепнев, В. В. Ященко // Докл. РАН. – 1993. – Т. 332, № 5. – С. 566–567.

[20] Artin, E. Theory of braids / E. Artin // Ann. Math. – 1947. – V. 48. – P. 101–126.

[21] Dehn, M. Über unendliche diskontinuerliche Gruppen / M. Dehn // Math. Ann. – 1911. – Bd. 71. – S. 116–144.

[22] Diffie, W. New directions in cryptography / W. Diffie, M. E. Hellman // IEEE Transaction Information Theory. – 1976. – V. 22, № 6. – P. 644–654.

[23] van Kampen, E. R. On the connection between the fundamental groups of some related spaces / E. R. van Kampen // Amer. J. Math. – 1933. – V. 55. – P. 261–267.

[24] van Kampen, E.R. On some lemmas in the theory of groups of some related spaces / E. R. van Kampen // Amer. J. Math. – 1933. – V. 55. – P. 268–273.

[25] Ko, K. H. New public-key cryptosistem using braid groups / K. H. Ko, S. J. Lee, J. H. Cheon // Advances in cryptology – CRYPTO 2000 (Santa Barbara, CA). Lecture Notes in Comput. Sci. – 2000. – V. 1880. – P. 166–183.

[26] Magnus, W. Das Identitäts problem für Gruppen mit einer definierenden Relation / W. Magnus // Math. Ann. – 1932. – Bd. 106. – S. 295–307. Рус. пер. : Успехи мат. наук. – 1941. – Вып. 8. С. 365–376.

[27] Myasnikov, A. Group-based cryptography / A. Myasnikov, V. Shpilrain, A. Ushakov – Advances courses in Math. CRM, Barselona. Basel-Berlin-New York: Birkhäuser Verlag. – 2008. – 183 p.

[28] Myasnikov, A. Non-commutative cryptography and complexity of group-theoretic problems / A. Myasnikov, V. Shpilrain, A. Ushakov – Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc. – 2001. – 196 p.

[29] Rivest, R. L. A method for obtaining digital signatures and public-key cryptosistems / R. L. Rivest, A. Shamir, L. Adleman // Comm. ACM. – 1978. – V. 21, № 2. – P. 120–126.

Учебное издание

Дурнев Валерий Георгиевич
Зеткина Оксана Валерьевна

МЕТОДЫ КОМБИНАТОРНОЙ ТЕОРИИ ГРУПП
В СОВРЕМЕННОЙ КРИПТОГРАФИИ

Учебно-методическое пособие

Редактор, корректор Л. Н. Селиванова

Подписано в печать 28.09.2017. Формат 60 × 84 1/8.
Усл. печ. л. 6,04. Уч.-изд. л. 3,0. Тираж 4 экз.
Заказ .....

Оригинал-макет подготовлен
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет имени П. Г.Демидова.
150003, Ярославль, ул. Советская, 14.