ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Ордена Трудового Красного Знамени федеральное государственное
бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

Кафедра Теории вероятностей и прикладной математики

Демин Д.Б.

Учебно-методическое пособие
по курсу

Дополнительные главы алгебры

Часть 1

для студентов 2 курса дневного обучения
направления 01.03.04 «Прикладная математика»

Москва 2017

План УМД на 2016/2017 уч. год

Учебно-методическое пособие
по курсу

Дополнительные главы алгебры

Часть 1

для направления 01.03.04 «Прикладная математика»

Составитель: Д.Б. Демин, к.ф.-м.н., доцент

Предлагаемое учебное пособие по курсу «Дополнительные главы алгебры» включает в себя специальные разделы алгебры, касающиеся теории групп, колец и полей. Этот курс изучается студентами направления 01.03.04 «Прикладная математика» на 2-м курсе в четвертом семестре и является логическим продолжением курса «Линейная алгебра и аналитическая геометрия», изучаемого на 1-м курсе в первом и втором семестрах. В пособии приведены: тематика лекционных и практических занятий, список рекомендуемой литературы, краткое изложение основ курса, список вопросов и задания для самостоятельного решения.

Издание утверждено на заседании кафедры ТВиПМ. Протокол № 7 от «14» марта 2017 г.

Рецензент: А.Г. Кюркчан, д.ф.-м.н., профессор

ВВЕДЕНИЕ

Предлагаемое учебное пособие по курсу «Дополнительные главы алгебры» включает в себя специальные разделы алгебры, касающиеся изучения основ теории групп, колец и полей. Этот курс изучается студентами направления 01.03.04 «Прикладная математика» на 2-м курсе в четвертом семестре и является логическим продолжением курса «Линейная алгебра и аналитическая геометрия», изучаемого на 1-м курсе в первом и втором семестрах. В пособии приведены: тематика лекционных и практических занятий, список рекомендуемой литературы, краткое изложение основ курса, список вопросов и задания для самостоятельного решения.

Содержание курса

1. Введение в абстрактную алгебру. Алгебраические операции, их свойства. Таблица Кэли. Алгебраические структуры. Отношения. Отношение эквивалентности. Виды отображений. Группоид, полугруппа, моноид.
2. Группы. Примеры групп. Подгруппы. Порядок элемента группы. Циклические группы. Симметрическая группа подстановок. Теорема Кэли. Характеристика группы.
3. Изоморфизмы групп. Гомоморфизмы групп. Теоремы о изоморфизме и гомоморфизме. Примеры. Ядро гомоморфизма.
4. Смежные классы. Примеры. Индекс подгруппы в группе. Теорема Лагранжа. Отношение сопряженности.
5. Нормальные делители. Факторгруппа. Прямое произведение (прямая сумма групп).
6. Кольца и алгебры. Примеры колец. Кольцо целых чисел. Кольцо многочленов. Кольца классов вычетов. Подкольцо. Обратимые элементы кольца, делители нуля.
7. Идеалы. Главные идеалы. Максимальные и простые идеалы. Идеалы в кольцах многочленов. Факторкольцо.
8. Деление с остатком в кольцах целых чисел и многочленов над кольцом целых чисел. Евклидовы кольца. Идеалы в евклидовых кольцах.
9. Поля. Примеры полей. Поле рациональных дробей. Конечные поля. Поле классов вычетов. Характеристика поля. Подполе. Конечные и алгебраические расширения полей.

Список литературы

Основная литература:

1. Курош А.Г. Курс высшей алгебры. СПб.: Лань, 2008.
2. Кострикин А.И. Введение в алгебру. Т.1, Т.3. М.: МЦНМО, 2012.
3. Сборник задач по алгебре. Под ред. А.И.Кострикина. М.: МЦНМО, 2012.
4. Сборник задач по математике для втузов. Ч. 1. Под ред. А.В. Ефимова и А.С. Поспелова. М.: Физматлит, 2014.

Дополнительная литература:

5. Ван дер Варден Б.Л. Алгебра. СПб.: Лань, 2004.
6. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.
7. М.М. Глухов, В.П. Елизаров, А.А. Нечаев. Алгебра. СПб.: Лань, 2015.
8. Э.Б. Винберг. Курс алгебры. М.: Изд-во «Факториал Пресс», 2001.

АЛГЕБРАИЧЕСКИЕ ОПЕРАЦИИ. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ. ОТНОШЕНИЯ

Предметом алгебры является изучение алгебраических операций, подобных сложению и умножению чисел, производимых над элементами, вообще говоря, произвольных множеств. Основной задачей алгебры является исследование алгебраических структур, т.е. множеств, наделенных некоторыми алгебраическими операциями.

n-арная операция ω в множестве A $(n \geq 1)$ сопоставляет всякой упорядоченной системе из n элементов $a_1, a_2, ..., a_n \in A$ однозначно определенный элемент $\omega(a_1, a_2, ..., a_n) \in A$. Другими словами, n-арной операцией на множестве A называется любое отображение прямого произведения $\underbrace{A \times A \times ... \times A}_{n} = A^n$ (n-ая декартова степень) в A: $\omega : A^n \to A$. n-арную операцию можно также называть n-местной операцией.

Правило, задаваемое операцией ω, воплощается в виде графика $\Gamma(\omega)$. График $\Gamma(\omega)$ состоит из пар вида $\langle (a_1, a_2, ..., a_n), b \rangle$, где $b = \omega(a_1, a_2, ..., a_n) \in A$. График однозначно определяет операцию, если множество A конечно. Его можно задать в виде таблицы из двух столбцов: в левом (входном) столбце выписываются все элементы множества A^n, а в правом (выходном) столбце – соответствующие элементы из A.

При $n=1$ получим унарную или одноместную операцию, т.е. это любое отображение множества A в себя.

При $n=0$ нульарная или нульместная операция фиксирует в множестве A некоторый определенный элемент.

Наиболее важной на практике (и достаточно хорошо изученной) является бинарная операция (случай $n=2$).

Под бинарной (или двуместной) операцией f на множестве A понимается любое отображение $f: A\times A\to A$, т.е. правило, по которому всяким двум элементам из множества A, взятым в определенном порядке, ставится в соответствие вполне определенный третий элемент, принадлежащий этому же множеству.

Каждой бинарной операции сопоставляется ее график, который удобно задать в виде таблицы, в первом столбце и первой строке которой выписываются все элементы множества A, а на пересечении строки, на входе которой стоит a_i, и столбца, на входе которого стоит a_j, помещается $f(a_i, a_j)\in A$. Такую таблицу принято называть таблицей Кэли.

НОД	4	6	12
4	4	2	4
6	2	6	6
12	4	6	12

Например, таблица Кэли для операции НОД(a,b) на множестве $A=\{4, 6, 12\}$ будет иметь вид, приведенный слева. НОД является бинарной операцией на множестве A, т.к. все результаты этой операции – числа из того же множества.

Для обозначения бинарной операции, помимо $f(a,b)$ более употребительна другая система обозначений – при помощи «инфикса» – специального символа, ставящегося между компонентами пары <a, b>, к которой применяется операция. Например: a+b, a*b, a∘b, a·b, a–b, A∪B, A∩B, A\B и др. Использование знака "∘" называется мультипликативной системой обозначений, а использование знака "+" – аддитивной.

Примеры бинарных операций.

1. Сложение и умножение являются бинарными операциями на множествах N, Z, Q, R, C (N – множество натуральных чисел, Z – множество целых чисел, Q – множество рациональных чисел, R – множество действительных чисел и C – множество комплексных чисел). Вычитание является бинарной операцией на Z, Q, R, но не на N. Деление не является бинарной операцией на множествах Q и R, т.к. деление на ноль невозможно, но является бинарной операцией на множествах Q\{0}, R\{0}. Для любого нечислового мно-

жества M объединение, пересечение и разность множеств являются бинарными операциями на M.

2. Используемые обозначения множеств: $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ – множество неотрицательных целых чисел. $\mathbb{R}_+$ – множество неотрицательных вещественных чисел. Сложение, умножение и операция возведения в степень являются бинарными операциями на множествах $\mathbb{Z}_+$ и $\mathbb{R}_+$.

3. На множестве матриц умножение вещественных квадратных матриц заданного порядка есть бинарная алгебраическая операция.

4. Операция векторного произведения на множестве векторов трехмерного вещественного векторного пространства R^3 есть бинарная операция.

5. Операция композиции геометрических преобразований есть бинарная операция.

6. Сложение и умножение функций действительного переменного (в том числе и многочленов) являются бинарными операциями.

7. Пусть M, N, P – некоторые множества, а f: $N \to M$, g: $P \to N$ – некоторые отображения (функции). Произведением или композицией отображений f и g называется отображение вида $f \circ g$: $P \to M$, т.е. $(f \circ g)(a) = f(g(a))$, $\forall a \in P$. Композиция отображений есть бинарная операция на множестве отображений.

Группоид, полугруппа, моноид

Пара объектов $<M, F>$, где M – множество, а F – операция (бинарная) на M, называется ***группоидом***. Множество M называется носителем группоида, а операция F – операцией группоида.

Группоид называется конечным, если его носитель конечен, бесконечным, если его носитель бесконечен, счетным, если его носитель счетен, и т.д. Элементы носителя группоида называются элементами самого группоида. Если группоид конечен, то число его элементов называется порядком группоида. Как и для всякого множества M, мощность, т.е. порядок группоида обозначается символами Card M, ord M или |M|.

Основные свойства бинарных операций

1. Бинарная алгебраическая операция на множестве M называется идемпотентной, если $\forall x \in M$: $x \circ x = x$. Это означает, что диагональ таблицы Кэли имеет тот же вид, что и входная строка или входной столбец.
2. Бинарная алгебраическая операция $\circ$ на множестве M называется коммутативной, если для любых двух элементов x и y из M выполняется

условие: $x \circ y = y \circ x$. В этом случае таблица Кэли операции симметрична относительной диагонали.

3. Бинарная алгебраическая операция ◦ на множестве *M* называется обратимой слева, если для любых *a* и *b* существует такой *x* из *M*, что: $x \circ a = b$ (или *xa*= *b*). Операция обратима слева, если в каждом столбце таблицы операции нет пропущенных элементов.
4. Бинарная алгебраическая операция ◦ на множестве *M* называется обратимой справа, если для любых *a* и *b* существует такой *x* из *M*, что: $a \circ x = b$ (или *ax*= *b*). Операция обратима справа, если в каждой строке таблицы операции нет пропущенных элементов.
5. Операция ◦ на множестве *M* называется сократимой слева, если для любых *x*, *y*, *z* из *M*: $x \circ y = x \circ z \Rightarrow y = z$. Операция сократима слева, если в каждой строке таблицы нет одинаковых элементов.
6. Операция ◦ на множестве *M* называется сократимой справа, если для любых *x*, *y*, *z* из *M* выполняется условие: $y \circ x = z \circ x \Rightarrow y = z$. Аналогично, операция сократима справа тогда и только тогда, когда в каждом столбце таблицы операции нет одинаковых элементов.
7. Операция ◦ на множестве *M* называется ассоциативной (сочетательный закон), если для любых трех элементов *x*, *y*, *z* из *M* выполняется условие: (*x*◦ *y*) ◦ *z*= *x*◦(*y*◦ *z*).

Группоид <*M*, ◦> называется ***идемпотентным*** (обратимым, коммутативным и т.д.), если его операция идемпотентна (соответственно обратима, коммутативна и т.д.).

Из характеристик свойств обратимости и сократимости следует, что:

– конечный группоид обратим слева, если он сократим справа;

– конечный группоид обратим справа, если он сократим слева.

Итак, группоид обратим слева (справа), если любое уравнение $xa = b$ ($ax = b$) имеет решение.

Группоид сократим слева (справа), если любое уравнение $ax = b$ ($xa = b$) имеет не более одного решения.

Пример: группоид <ℕ,+> не идемпотентен (4+4≠4), коммутативен, не обратим ни слева, ни справа, сократим и слева, и справа, ассоциативен. Такие же характеристики имеет и группоид <ℕ, ∗>.

Единичные и обратные элементы

Пусть <*M*, ◦> – группоид. Элемент $e \in M$ называется левой единицей (левым нейтральным элементом), если $ex = x$ для любых $x \in M$. Элемент

$e \in M$ называется правой единицей (правым нейтральным элементом), если $xe = x$ для $x \in M$.

Если в M имеется левая единица e_1 и правая единица e_2, то они совпадают, и элемент $e = e_1 = e_2$ называется (двусторонней) единицей (или просто нейтральным элекментом).

Таким образом, в группоиде M может существовать однозначно определенный элемент $e \in M$, удовлетворяющий условиям: $ex = x$, $xe = x$ для любых $x \in M$.

Пусть <M, ∘> – группоид с двухсторонней единицей e. Элемент b называется правым обратным для a, если $a \circ b = e$; левым обратным для a, если $b \circ a = e$; (двухсторонним) обратным для a, если он является как правым, так и левым обратным для а, т.е. если $a \circ b = b \circ a = e$.

В аддитивном случае вместо «единиц» говорят о «нулях», вместо «обратных» – о «противоположных».

Алгеброй называется упорядоченная пара $A = (A, \Omega)$, где A – непустое множество, Ω - множество операций на А. (|A|=A, элементы A – это элементы алгебры А). А есть алгебра относительно операций Ω.

Группоид <M, ∘> называется ***полугруппой***, если его основная бинарная операция ассоциативна, т.е. полугруппа – это множество, на котором задана ассоциативная операция.

Группоиды <ℕ, +>, <ℕ, *>, <ℤ, +>, <ℤ, *>, <ℚ, +>, <ℚ\{0}, *>, <ℝ, +>, <ℝ\{0}, *>, <ℂ, +>, <$\mathbb{Q}^+$, *>, <$\mathbb{R}^+$, *> являются полугруппами. Любой одноэлементный группоид всегда является полугруппой. Группоид <ℤ, –> полугруппой не является.

Полугруппа с единичным (нейтральным) элементом называется ***моноидом*** (или полугруппой с единицей).

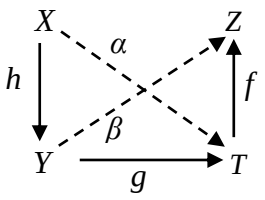
Например, множество всех целых чисел, кратных n, которое обозначается как $n\mathbb{Z}$, есть коммутативный моноид относительно операции сложения и коммутативная полугруппа без единицы относительно операции умножения (при $n > 1$).

Можно показать, что множество A всех отображений является моноидом относительно операции композиции.

Пусть $h: X \to Y$, $g: Y \to Z$, $f: Z \to T$ – три отображения. Их композиция всегда ассоциативна, т.е.

$$f \circ (g \circ h) = (f \circ g) \circ h,$$

что следует из наглядной диаграммы (см. рисунок). Из рисунка видно, что $f \circ \alpha = \beta \circ h$, где $\alpha = g \circ h$,



$\beta = f \circ g$.

В множестве отображений A существует тождественное отображение (т.е. нейтральный элемент), которое можно обозначить так:

$e_x : X \to X$, где $e_x(x) = x, \forall x \in X$.

Тогда композиции $f \circ e_x = f$ и $e_y \circ f = f$ для любого отображения $f : X \to Y$ ($e_y : Y \to Y, e_y(y) = y, \forall y \in Y$).

Бинарные отношения

Декартовым (или прямым) произведением двух множеств X и Y называется множество всех упорядоченных пар (x, y):

$X \times Y = \{(x, y) | x \in X, y \in Y\}$.

Например, если R – множество действительных чисел, то $\mathsf{R} \times \mathsf{R} = \mathsf{R}^2$ – декартов квадрат, т.е. это множество всех декартовых координат точек на плоскости относительно заданных координатных осей.

Если $X_1, ..., X_n$ – любой конечный набор множеств, то назовем последовательностью, или строкой, или кортежем длины n символ $(x_1, ..., x_n)$, где $x_i \in X_i$. Множество всех таких последовательностей называется ***прямым (декартовым) произведением*** множеств $X_1, ..., X_n$ и обозначается как $X_1 \times ... \times X_n$ или $\prod_{i=1}^{n} X_i$. При $X_1 = ... = X_n = X$ пишут сокращенно $X^n = X \times X \times ... \times X$ и говорят о n-ной декартовой степени множества X.

Очевидно, что мощность $|X \times Y| = n \cdot m$. если $n = |X|$, $m = |Y|$.

Любое подмножество R множества (декартова произведения) $A \times B$ называется ***бинарным отношением*** (или соответствием) между множествами A и B.

Если $(a, b) \in R$, то пишут aRb и говорят, что элемент a находится в отношении R с элементом b.

Бинарным отношением R на множестве A называется подмножество декартова квадрата $A^2 = A \times A$ ($R \subseteq A \times A$).

Пример: каждой функции $f : X \to Y$ сопоставляется ее график, т.е. подмножество вида: $\Gamma(f) = \{(x, y) | x \in X, y \in f(x)\} \subseteq X \times Y$, являющееся бинарным отношением между X и Y.

Бинарное отношение $R \subseteq A \times A$ называется ***рефлексивным***, если aRa, $\forall a \in A$.

Пример: отношения "=" и "≤" – рефлексивные на множестве N.

Бинарное отношение $R \subseteq A \times A$ называется ***симметричным*** если aRb влечет ($\Rightarrow$) bRa.

Пример: отношение "=" является симметричным, а отношения "<" и "≤" – нет.

Бинарное отношение $R \subseteq A \times A$ называется ***транзитивным***, если aRb и $bRc \Rightarrow aRc$ для $\forall a, b, c \in A$.

Пример: отношения "<", "≤" и "=" являются транзитивными.

Рефлексивное, симметричное и транзитивное отношение R называется ***отношением эквивалентности***, и обозначается как ~ (или $\cong$).

Бинарное отношение называется антисимметричным на множестве A, если aRb и bRa влечет $a = b$.

Например, отношение "≤" на $\mathbb{N}$ является антисимметричным (отношение $\subset$ также антисимметрично).

Бинарное отношение $R \subseteq A \times A$ называется отношением порядка на A, если оно транзитивно и антисимметрично.

Бинарное отношение $R \subseteq A \times A$ называется отношением строгого порядка на A, если оно транзитивно и антирефлексивно. Например, отношение "<" является отношением строгого порядка, а отношение "≤" – нестрогого порядка.

Рефлексивное, антисимметричное и транзитивное отношение называется отношением частичного порядка. Множество с таким отношением на нем называется частично упорядоченным множеством. Частичный порядок называется линейным порядком, если для любых элементов a и b выполнено либо aRb, либо bRa (или оба, тогда они равны по свойству антисимметричности).

Например, отношение "≤" на $\mathbb{N}$ является линейным порядком. На множестве M мощности n можно ввести $n!$ различных линейных порядков.

Задания для самостоятельного решения

1. Сколько различных бинарных операций можно ввести на множестве мощности n?
2. На множестве $M = \{1, 2, 4, 8\}$ введена операция $x * y = x$, $\forall x, y \in M$. Построить таблицу Кэли данной операции и найти все левые (правые) единицы.
3. Укажите все отношения линейного порядка на множестве $M = \{1, 2, 3\}$. Сколько таких отношений будет на множестве из n элементов?
4. Образует ли множество квадратных матриц $M_n(R)$ с операцией умножения моноид?
5. Какими свойствами обладают отношения параллельности и перпендикулярности, определенные на множестве прямых на плоскости?

ГРУППА

Группа – это множество $G \neq \varnothing$ с определенной на ней бинарной операцией, которая двум элементам $a,b \in G$ ставит в соответствие третий элемент $c \in G$ такой, что $a \circ b = c$. Эта операция удовлетворяет следующим условиям (свойствам, аксиомам):

1. ассоциативность: $(a \circ b) \circ c = a \circ (b \circ c)$;
2. условие существования нейтрального элемента: среди элементов G имеется некоторый определенный элемент, называемый нейтральным и обозначаемый символом e (либо «0» в аддитивном случае, либо «1» – в мультипликативном), такой, что:
   $a \circ e = e \circ a = a, \ \forall a \in G$;
3. условие существования обратного элемента: для любого элемента $a \in G$ найдется такой элемент b того же множества G, что
   $a \circ b = b \circ a = e$.

   Элемент b называется обратным к a и обозначается a^{-1}.

Группу с введенной на ней операцией ("$\circ$") будем обозначать как $(G,\circ)$ или $\langle G,\circ \rangle$. Если "$\circ$"="$\cdot$" (умножение), то группа $(G,\cdot)$ называется мультипликативной, а группа $(G,+)$ – аддитивной.

Группа является алгебраической структурой с одной бинарной операцией. Моноид, в котором каждый элемент обратим, является группой.

В дальнейшем, если не будет оговорено особо, группы по умножению $(G,\cdot)$ будем обозначать просто через G, а аддитивные группы через G^+.

Если в группе G кроме указанных выше аксиом выполняется еще условие коммутативности, т.е.

$a \circ b = b \circ a, \ \forall a,b \in G,$

то группа G называется коммутативной или абелевой группой.

Группа G, содержащая n элементов, называется конечной, а число n называется порядком группы и обозначается так: $|G| = ordG = n$.

Примеры групп

1) $(\mathbb{Z}, +)$ – группа целых чисел (групповая операция – обычное сложение целых чисел). Также $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ – группы рациональных, действительных и комплексных чисел.
2) $(\mathbb{Q}\backslash\{0\}, \cdot) = \mathbb{Q}^*$ - группа рациональных чисел (без нуля) по умножению. Также $(\mathbb{R}\backslash\{0\}, \cdot) = \mathbb{R}^*$ и $(\mathbb{C}\backslash\{0\}, \cdot) = \mathbb{C}^*$ – мультипликативные группы действительных и комплексных чисел (без нуля).
3) Множество матриц $M_{m\times n}$ (где M есть одно из множеств $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) с операцией сложения образует группу. Нейтральным элементом в этой

группе является нулевая матрица, а обратным элементом является противоположная матрица.

4) Все квадратные матрицы порядка n с элементами из некоторого поля A (например, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) с отличным от нуля определителем образуют группу по умножению, нейтральным элементом в которой является единичная матрица. Такая группа обозначается как $(GL(n,A),\cdot)$ или $GL_n(A)$. $SL_n(A)$ – это подгруппа $GL_n(A)$, обозначающая мультипликативную группу невырожденных матриц порядка n с определителем, равным единице.
5) Множество $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ остатков от деления целых чисел из $\mathbb{Z}$ на число $n \in \mathbb{N}$ с операцией сложения по модулю n образует аддитивную коммутативную группу (вычетов) порядка n.
6) Множества многочленов произвольной степени с основной операцией сложения с коэффициентами из $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ или $\mathbb{Z}_n$ образуют группы по сложению, которые обозначаются как $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_n[x]$.
7) Множество геометрических векторов с обычной операцией сложения векторов образуют аддитивную группу.
8) Множество биективных преобразований (отображений) с операцией композиции образуют группу.

Теоремы о группах

1. В произвольной группе произведение любого числа элементов не зависит от расстановки скобок.
2. Если для любого элемента g группы G найдется элемент e' такой, что $g \cdot e' = g$ или $e' \cdot g = g$, то $e' = e$ есть нейтральный элемент группы G.
3. Для любого элемента g группы G существует и при том единственный обратный (в аддитивном случае – противоположный) элемент g^{-1} такой, что $g \cdot g^{-1} = g^{-1} \cdot g = e$.
4. Пусть $a, b \in G$. Рассмотрим в группе G уравнение $xa = b$. Очевидно, что это уравнение имеет единственное решение $x = ba^{-1}$. Точно также уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$. Следствием из этого будет утверждение, что если $ab = ac$ и $ba = ca$, то $b = c$.
5. Для любых $a, b \in G$ выполняется следующее равенство: $(ab)^{-1} = b^{-1}a^{-1}$.

Подгруппы

Подмножество H группы G ($H \subset G$) называется подгруппой в G, если 1) $e \in H$; 2) для $\forall h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$; 3) $\forall h \in H \Rightarrow h^{-1} \in H$. Обозначение: $H < G$.

Подгруппа H называется собственной, если $H \neq \{e\}$ и $H \neq G$.

***Теорема*:** подмножество H группы G является подгруппой этой группы тогда и только тогда, когда для $\forall a,b \in H$ следует, что $ab^{-1} \in H$.

Подгруппа H группы G также является группой.

Циклические группы

Пусть G – мультипликативная группа и $a \in G$. Если любой элемент $g \in G$ записывается в виде $g = a^n$ для некоторого $n \in \mathbb{Z}$, то группа $G = \langle a \rangle =$ $= \{\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots\}$ называется ***циклической группой*** с образующим элементом a (или циклической группой, порожденной элементом a).

Для всех групп G (не только циклических) справедливо:

$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m, \ \forall m,n \in \mathbb{Z}.$

Из этого равенства следует, что все циклические группы коммутативны. Обратное вообще говоря не верно.

Если в циклической группе $G = \langle a \rangle$ все степени a^n различны, то она бесконечна. В противном случае она конечна. Действительно, если в циклической группе $a^k = a^l$ (для некоторых k и l $(k > l)$), то $a^{k-l} = a^0 = e$. Фиксировав наименьший такой показатель, при котором $a^n = e$, приходим к выводу, что группа G исчерпывается элементами $a^0 = e$, a^1, a^2, a^3, … , a^{n-1} (в аддитивном случае $0 = 0a$, a, $2a$, … , $(n-1)a$). Причем все эти элементы различны между собой.

Наименьший целый положительный показатель n, для которого $a^n = e$, называют ***порядком элемента*** a, а сам элемент a называют ***элементом конечного порядка*** n (обозначение: $n = ord\, a = |a|$). Очевидно, что в конечной группе G все элементы являются элементами конечного порядка. Справедливы следующие утверждения.

Утверждение 1. Если в группе G порядка n есть элемент порядка n, то эта группа циклическая.

Утверждение 2. Порядок любого элемента a группы G равен порядку циклической группы $\langle a \rangle$, порожденной этим элементом.

Утверждение 4. Всякая группа простого порядка – циклическая.

Утверждение 5. Всякая подгруппа циклической группы есть снова циклическая группа.

Утверждение 6. Если $ord\, a = n$, то $ord\, a^k = \dfrac{n}{(n,k)}$,

где (n,k) = НОД(n,k).

Следствие из утверждения 6. Элемент a^k является порождающим элементом циклической группы $\langle a \rangle$ порядка n, если $(n,k)=1$.

Утверждение 7. Если $ord\,a = n$, $ord\,b = m$ и при этом $(n,m)=1$, $ab = ba$, то $ord(ab) = nm$.

Если в группе G все элементы (кроме нейтрального) являются элементами бесконечного порядка, то группа G называется ***группой без кручения***. Если же порядки всех элементов конечны, то группа называется ***периодической***. В общем случае группа называется ***смешанной***.

Если все элементы группы G (кроме нейтрального, порядок которого равен 1), имеют одинаковый конечный порядок n, то говорят, что группа G имеет ***характеристику*** n. Группа G имеет характеристику 0, если все ее элементы, отличные от нейтрального, имеют бесконечный порядок. Если в группе G имеются элементы различного порядка, то такая группа характеристики не имеет. Очевидно, что собственная подгруппа группы характеристики n также имеет характеристику n.

Утверждение 8. Если группа G имеет характеристику n, то n – простое число (докажите все эти утверждения самостоятельно).

Примеры циклических групп.

1) Аддитивная группа целых чисел $\mathbb{Z}$ является циклической группой бесконечного порядка, т.е. группой без кручения. Эта группа порождается элементами 1 или –1.
2) Аддитивная группа вычетов по модулю n: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, состоящая из остатков от деления целых чисел из $\mathbb{Z}$ на число $n \in \mathbb{N}$, является конечной циклической группой порядка n. Образующим элементом группы $\mathbb{Z}_n$ является число 1 и любое число k $(k < n)$, взаимно простое с n (т.е. $(n,k)=1$).
3) Группа корней из единицы U_n также является конечной циклической группой, изоморфной группе $\mathbb{Z}_n$. Эта группа состоит из всех решений (корней) уравнения $z^n = 1$. Из теории комплексных чисел известно, что решениями этого уравнения являются числа вида:

   $z_k = e^{i\frac{2\pi k}{n}}$, $k = 0,1,\ldots,n-1$ (или $z_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$).

   Здесь $z_0 = 1$, $z_1 = e^{i\frac{2\pi}{n}}$, $z_2 = e^{i\frac{2\pi}{n}2} = z_1^2$, $z_3 = z_1^3$, … , $z_1^n = 1 = z_0$. Таким образом, $U_n = \{z_0, z_1, \ldots, z_{n-1}\}$, где z_0 – единичный, а z_1 – образующий элементы группы U_n.

4) Группа $k\mathbb{Z}_n$ $(k < n)$, состоящая из элементов группы $\mathbb{Z}_n$, делящихся на k по модулю n.

Изоморфизмы и гомоморфизмы групп

Группы $(G_1, \circ)$ и $(G_2, *)$ называются ***изоморфными***, если существует биективное (взаимно однозначное) отображение $f: G_1 \to G_2$, которое сохраняет групповую операцию, т.е. $f(a \circ b) = f(a) * f(b)$, $\forall a, b \in G_1$.

Обозначение изоморфизма: $G_1 \cong G_2$.

Изоморфизм f обладает следующими свойствами:

1. отношение изоморфизма является отношением эквивалентности на множестве всех групп;
2. в изоморфных группах образ и прообраз единицы (нейтрального элемента) является единицей (нейтральным элементом);
3. $f(a^{-1}) = f(a)^{-1}$;
4. Обратное отображение $f^{-1}: G_2 \to G_1$ тоже является изоморфизмом.

В качестве изоморфного отображения f мультипликативной группы $(\mathbb{R}_+, \cdot)$ положительных действительных чисел на аддитивную группу $(\mathbb{R}, +)$ всех действительных чисел может служить $f: x \to \ln x$, так как $\ln(ab) = \ln a + \ln b$. Обратным к f служит отображение $f^{-1}: x \to e^x$.

Изоморфное отображение группы G на себя называется ***автоморфизмом***. Автоморфизмы группы характеризуют ее симметрию. Множество всех автоморфизмов группы G образует группу относительно композиции, которую обозначают как $\mathrm{Aut}\, G$. Единичным элементом $\mathrm{Aut}\, G$ является тождественный автоморфизм $e_G: g \to g$, $\forall g \in G$.

Пример: группой автоморфизмов циклической группы $\mathbb{Z}$ является группа $\mathbb{Z}_2$. Действительно при отображении образующего элемента 1 в любое целое число $t \in \mathbb{Z}$, отличное от 1 и –1, получим изоморфное отображение $\mathbb{Z}$ на группу $t\mathbb{Z}$, что не является автоморфизмом. Поэтому здесь возможны только два автоморфизма: $f_1: n \to n$ (тождественный автоморфизм) и $f_2: n \to -n$, $\forall n \in \mathbb{Z}$, причем очевидно, что $f_2 \circ f_2 = f_1$. Это изоморфно группе из двух элементов, т.е. группе $\mathbb{Z}_2$.

Теорема. Всякая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$, а всякая конечная циклическая группа порядка n изоморфна $\mathbb{Z}_n$.

Связи между разными алгебраическими структурами одного типа устанавливаются при помощи гомоморфизмов.

Гомоморфизмом группы $(G,\circ)$ в группу $(H,*)$ называется такое отображение $f:G\to H$, которое удовлетворяет условию:

$f(a\circ b)=f(a)*f(b),\ \forall a,b\in G$.

Понятие гомоморфизма отличается от понятия изоморфизма тем, что оно не требует биективности отображения f.

Ядром гомоморфизма f называется множество $\operatorname{Ker} f=\{g\in G:$ $f(g)=e'$ – нейтральный элемент группы $H\}$. Если $\operatorname{Ker} f=\{e\}$, то $f:G\to \operatorname{Im} f$ – изоморфизм. $\operatorname{Ker} f$ является подгруппой в G. $\operatorname{Im} f$ – это образ гомоморфизма: $\operatorname{Im} f=\{f(g): g\in G\}=f(G)$.

Гомоморфное отображение группы в себя называется ее эндоморфизмом, а сюръективное отображение группы G на группу H – эпиморфизмом (гомоморфизм «на»). Гомоморфизм с единичным ядром называется мономорфизмом. Поэтому изоморфизм – это эпиморфизм и мономорфизм одновременно.

Укажем свойства гомоморфизма $f:G\to H$.

1) Единица e группы G переходит в единицу e' группы H.

2) $f(a^{-1})=f(a)^{-1},\ \forall a\in G$.

3) Гомоморфный образ группы является подгруппой, т.е. $\operatorname{Im} f<H$.

Пример: Найти все гомоморфизмы из $\mathbb{Z}_n$ в $\mathbb{Z}_m$.

Пусть $f:\ \mathbb{Z}_n\to\mathbb{Z}_m$ – гомоморфизм. Возьмем любой образующий элемент в группе $\mathbb{Z}_n$, например, 1: $f(1)=t\in\mathbb{Z}_m$. Тогда $f(k)=k\,f(1)=kt$, $\forall k\in\mathbb{Z}_n$. Поэтому для задания гомоморфизма f достаточно указать образ 1, т.е. t. Так как порядок 1 в $\mathbb{Z}_n$ равен n, то порядок $f(1)$ делит n $(t|n)$. Так как $ord(t)=\dfrac{m}{(m,t)}$ (см. утверждение 6), то $\dfrac{m}{(m,t)}\Big| n$. Это условие является достаточным, чтобы отображение $f:\ \mathbb{Z}_n\to\mathbb{Z}_m$, заданное правилом $f(k)=kt$, было гомоморфизмом.

Например, найдем все гомоморфизмы из $\mathbb{Z}_3$ в $\mathbb{Z}_{36}$. Если $f(1)=t$, то $\dfrac{36}{(36,t)}\Big| 3$, тогда либо $(36,t)=36$, либо $(36,t)=12$. Так как $t\in\mathbb{Z}_{36}$, то $t=\{0,12,24\}$. Значит существует всего 3 гомоморфизма из $\mathbb{Z}_3$ в $\mathbb{Z}_{36}$, а именно: f_1, f_2, f_3 таких, что: $f_1(a)\equiv 0$, $\forall k\in\ \mathbb{Z}_3$; $f_2(0)=0$, $f_2(1)=12$, $f_2(2)=24$ и $f_3(0)=0$, $f_3(1)=24$, $f_3(2)=12$.

Для того, чтобы понять все многообразие конечных групп, а также то, как вычисляются порядки элементов в циклических группах, рассмотрим несколько специальных видов групп.

Симметрическая группа подстановок

Рассмотрим конечное множество X, состоящее из n элементов. Поскольку для нас природа этих элементов не важна, занумеруем эти элементы натуральным рядом чисел 1, 2, 3, …, n и будем считать, что $X = \{1, 2, 3, \ldots, n\}$.

Перестановкой φ степени n называется биективное отображение множества X на себя, т.е. $\varphi: X \to X$ и $i \to \varphi(i)$, $i = 1, 2, \ldots, n$.

Множество всех перестановок обозначается символом S_n и $\forall \varphi \in S_n$ используется двустрочная запись:

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{pmatrix} \text{ или } \varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Здесь первая строка обозначает множество элементов из X, а вторая строка – в какие элементы из X эти элементы отобразились.

В комбинаторике под перестановкой некоторых элементов понимают всевозможные способы, которыми эти элементы выстраиваются в ряд. Так, перестановка n предметов сводится нумерацией к перестановке чисел от 1 до n. Результат перестановки записывается строкой (i_1, i_2, … , i_n).

Подстановка – это операция, изменяющая порядок элементов в перестановке. Часто перестановку $\varphi \in S_n$ называют подстановкой.

Как известно из комбинаторики, общее число перестановок n предметов равно $n!$, поэтому $|S_n| = n!$.

На множестве S_n можно ввести операцию умножения подстановок φ и ψ, которую можно понимать как композицию φ и ψ, т.е.

$\varphi \circ \psi = \varphi(\psi(i))$, $i = 1, 2, \ldots, n$.

В соответствии с правилом композиции, произведение подстановок φ и ψ понимается как последовательное применение сначала ψ, потом φ.

Множество всех подстановок (перестановок) S_n с композицией в качестве групповой операции является ***группой*** и называется ***симметрической группой подстановок степени*** n, $Ord\, S_n = |S_n| = n!$

Покажем, что S_n – группа. Очевидно, что композиция (произведение) подстановок тоже является подстановкой. Действительно, пусть

$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ и $\psi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$, тогда

$$\varphi \circ \psi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(j_1) & \varphi(j_2) & \dots & \varphi(j_n) \end{pmatrix}.$$

Умножим, например, $\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ на $\psi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Тогда

$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. В силу правила композиции сначала выполняется подстановка ψ. Например, $\psi(1) = 3$, а затем, взяв $\varphi(\psi(1)) = \varphi(3)$, получим 3 и т.д. Но $\psi\varphi == \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, т.е. произведение подстановок не коммутативно.

Ассоциативность умножения подстановок следует из ассоциативности операции композиции над отображениями.

Укажем в S_n нейтральный элемент. Подстановка $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ называется тождественной подстановкой и является единицей в S_n, так как

$$e\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \varphi$$

Очевидно, что под действием подстановки φ 1 переходит в i_1. а потом подстановка e переводит i_1 в i_1 и т.д. Точно также $\varphi e = \varphi$.

Так как подстановка является биективным отображением множества X в X, то обязательно существует обратное отображение, т.е. у любой подстановки существует обратная подстановка. Найдем ее. Пусть

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Очевидно, что обратная подстановка $\psi = \varphi^{-1}$ должна «уничтожать» действие подстановки φ, т.е., например, если $\varphi(1) = i_1$, то $\psi(i_1)$ должно равняться 1 и т.д. В результате придем к следующей подстановке:

$$\psi = \varphi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Далее, упорядочивая первую строку подстановки ψ по возрастанию, получим требуемую обратную подстановку. Итак, S_n – группа.

Например, группа S_2 состоит из подстановок $e=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ и $\varphi=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$.

Так как здесь $\varphi^2=e$, то эта группа циклическая и изоморфна группе $\mathbb{Z}_2$.

Рассмотрим группу S_3. Она состоит из подстановок $e=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $\varphi_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$, $\varphi_2=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$, $\varphi_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$, $\varphi_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, $\varphi_5=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$. Эта группа не коммутативна, соответственно и не циклична и все последующие группы S_n уже не коммутативны. Но она содержит внутри себя циклические подгруппы. Например, $\varphi_3^2=e$ и так как подстановка φ_3 оставляет на месте число 3, то циклическая подгруппа $\langle\varphi_3\rangle$ группы S_3 изоморфна S_2. Вообще, любые группы подстановок являются подгруппами S_n. Так, например, S_n внутри себя содержит S_{n-1} и т.д. вплоть до S_2. Вместо S_n иногда говорят об изоморфной группе отображений $Sym(G)=S(G)$, $ordG=n$, элементами которой являются перестановки элементов группы G, а изоморфизм достигается нумерацией элементов группы G. Здесь справедлива следующая теорема.

Теорема Кэли. Всякая конечная группа изоморфна некоторой подгруппе группы подстановок S_n.

Эта теорема играет большую роль в теории групп. Ее важность состоит в том, что она выделяет универсальный объект – симметрическую группу S_n как вместилище всех конечных групп, рассматриваемых с точностью до изоморфизма.

Покажем как вычислять порядки элементов группы S_n. Для этого введем понятие цикла или цикловой подстановки.

Подстановка $\varphi\in S_n$ называется ***циклом*** длины s и обозначается как $(i_1\ i_2\ \dots\ i_s)$, если она циклически переставляет i_1 в i_2, i_2 в i_3 и т.д., а i_s в i_1, т.е. $\varphi(i_1)=i_2$, $\varphi(i_2)=i_3$, … , $\varphi(i_s)=i_1$, а остальные числа остаются на месте.

Итак, цикл $\varphi=(i_1\ i_2\ \dots\ i_s)$ можно представить как

$$\varphi=\begin{pmatrix}i_1 & i_2 & \dots & i_{s-1} & i_s & j_1 & \dots & j_{n-s}\\ i_2 & i_3 & \dots & i_s & i_1 & j_1 & \dots & j_{n-s}\end{pmatrix}.$$

Например, подстановка $\varphi = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} = (1\,2\,\dots\,n)$ – это цикл длины n. Эта подстановка является полным циклом в S_n. Таким образом, для циклов определена однострочная запись.

Пусть, например, $(5\,1\,4) \in S_5$, тогда $(5\,1\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$. Здесь очевидно, что $(5\,1\,4) = (1\,4\,5) = (4\,5\,1)$, т.е. цикл $\varphi = (i_1\ i_2\ \dots\ i_s)$ можно начинать с любого i_k $(k = 1,\dots,s)$.

Циклы длины два принято называть ***транспозициями*** (общий вид транспозиции: $\varphi = (i_1\ i_2)$). Очевидно, что цикл длины один есть тождественная подстановка.

Циклы σ_1 и σ_2 называются ***независимыми***, если среди фактически переставляемых ими чисел нет общих, при этом $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Например, $\sigma = (1\,3)(2\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (2\,4)(3\,1)$.

Теорема. Любая подстановка $\varphi \neq e$ в S_n раскладывается в произведение независимых циклов длины ≥ 2. Это разложение определено однозначно с точностью до порядка следования циклов, т.е.

$\varphi = \sigma_1\sigma_2 \dots \sigma_m$,

где σ_i $(i = 1,\dots,m)$ – попарно независимые циклы.

Например, $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 5 & 7 \end{pmatrix} = (1\,2\,4)(3\,6\,5)(7) = (1\,2\,4)(3\,6\,5)$.

Следствием указанной выше теоремы является следующее утверждение: любая подстановка $\varphi \in S_n$ является произведением транспозиций. Так как подстановка может быть записана в виде произведения циклов, то достаточно записать цикл в виде произведения транспозиций. Это можно сделать, например, так:

$(1\,2 \dots\, k-1\,k) = (1\,k)(1\,k-1) \dots (1\,3)(1\,2)$.

При этом из теоремы не следует единственность записи подстановки через транспозиции. Например:

$\sigma = (i_1\ i_2\ i_3 \dots i_{k-1}\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \dots (i_1\ i_3)(i_1\ i_2)$,

$\sigma = (i_1\ i_2\ i_3 \dots i_{k-1}\ i_k) = (i_2\ i_3 \dots i_{k-1}\ i_k\ i_1) = (i_2\ i_1)(i_2\ i_k)\ (i_2\ i_{k-1}) \dots (i_2\ i_3)$ и т.д.

Эти две записи цикла σ содержат одинаковое число $k-1$ совершенно различных транспозиций. Более того, транспозиции, вообще говоря, не пе-

рестановочны, а их число не является инвариантом подстановки. Например, в S_4 имеем:

$$(1\,2\,3)=(1\,3)(1\,2)=(2\,3)(1\,3)=(1\,3)(2\,4)(1\,2)(1\,4).$$

Определим теперь порядок цикла.

Пусть $\sigma=(i_1\ i_2\ \ldots\ i_k)$ есть цикл длины k $(2\le k\le n)$ группы S_n. Этот цикл всякое число переводит в соседнее справа, кроме последнего, которое переходит в первое, т.е. циклическая подстановка σ осуществляет «циклический сдвиг» чисел $i_1\ i_2\ \ldots\ i_k$ на одну позицию влево. Тогда σ^s будет осуществлять циклический сдвиг чисел $i_1\ i_2\ \ldots\ i_k$ на s единиц влево. Но тогда при $s=k$ все числа останутся неподвижными, т.е. $\sigma^k=e$ и $\sigma^s\ne e$ при $s=\overline{1,k-1}$. Таким образом, ***порядок цикла*** длины k равен k: $ord\,\sigma=k$.

Число циклов $(i_1\ i_2\ \ldots\ i_k)$ длины k в S_n равно $C_n^k(k-1)!$

Порядок перестановки φ в S_n, заданной своим разложением на независимые циклы, равен наименьшему общему кратному длин этих циклов:

$$ord\,\varphi=\text{НОК}(s_1,s_2,\ldots,s_m,\ \text{где}\ \varphi=(i_1\ldots i_{s_1})(j_1\ldots j_{s_2})\ldots(k_1\ldots k_{s_m}).$$

Пример: Вычислить порядок подстановки

$$\varphi=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&9&5&8&1&2&4&6\end{pmatrix}.$$

Так как $\varphi=(1\,3\,9\,6)(2\,7)(4\,5\,8)$, то $ord\,\varphi=\text{НОК}(4,2,3)=12$, т.е. $\varphi^{12}=e$.

Порядок подстановки используется при возведении ее в степень.

Пример: Возведем подстановку φ из предыдущего примера в степень –1001. Так как: –1001 = 12·(–84)+7, то $\varphi^{-1001}=\varphi^7$. Но

$$\varphi^7=(1\,3\,9\,6)^7(2\,7)^7(4\,5\,8)^7=(1\,3\,9\,6)^3(2\,7)^1(4\,5\,8)^1=(1\,6\,9\,3)(2\,7)(4\,5\,8).$$

Таким образом, $\varphi^{-1001}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&7&1&5&8&9&2&4&3\end{pmatrix}$.

Далее, введем понятие знака перестановки.

Знак перестановки φ – это число $\text{sgn}(\varphi)(=\varepsilon_\varphi)=(-1)^p$, где p – количество транспозиций в разложении $\varphi=\sigma_1\sigma_2\ldots\sigma_p$ (здесь σ_i $(i=1,\ldots,p)$ – попарно независимые циклы), при этом четность целого числа p всегда одна и та же и не зависит от способа разложения циклов на транспозиции. Кроме того, знак перестановки обладает следующим свойством:

$\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$, для $\forall\ \alpha,\beta\in S_n$.

Если $\varepsilon_\varphi = 1$, то подстановка φ называется ***четной***, если же $\varepsilon_\varphi = -1$, то ***нечетной***. Существует другое определение четности подстановки.

Пусть $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \in S_n$. Возьмем любые два числа i и k из первой строки представления φ. Скажем, что пара чисел (i,k) образует ***инверсию***, если либо $i < k$ и $a_i > a_k$, либо $i > k$ и $a_i < a_k$. Тогда подстановка φ, содержащая четное число инверсий, является ***четной подстановкой***, в противном случае – нечетной. Это определение не дает конструктивного способа выяснения четности любой подстановки. Поэтому рассмотрим другой способ определения четности. Так цикл σ_k длины s_k является четной подстановкой, если число s_k нечетно. Это следует из того, что цикл длины s_k можно представить в виде произведения как минимум $s_k - 1$ транспозиций, а любая транспозиция является нечетной подстановкой, .т.е. ее знак равен –1. Используя свойство знака перестановки, получим, что знак произведения транспозиций определяется четностью их количества. Так, цикл длины 3 является четной подстановкой, цикли длины 4 – нечетной и т.д. Тогда, если подстановку φ представить в виде разложения независимых циклов $\sigma_1\sigma_2...\sigma_p$ длин s_1, …, s_p, то знак подстановки

$$\varepsilon_\varphi = (-1)^{\delta(\varphi)},$$

где $\delta(\varphi)$ – декремент подстановки, и

$$\delta(\varphi) = \sum_{k=1}^{p} (s_k - 1).$$

Например, подстановка $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 7 & 1 & 4 & 6 \end{pmatrix}$ раскладывается как $\varphi = (1\,2\,3\,5)(4\,7\,6)$, тогда $\delta(\varphi) = (4-1) + (3-1) = 5$,т.е. $\varepsilon_\varphi = (-1)^5 = -1$, это означает, что подстановка φ – нечетная.

Из свойства знака подстановки следует, что при перемножении четных подстановок всегда получается четная подстановка, т.е. множество четных подстановок замкнуто относительно операции умножения, при этом обратной к четной подстановке также всегда будет четная подстановка, так как их произведение равно тождественной подстановке, которая является четной. Отсюда следует, что множество четных подстановок образует подгруппу группы S_n и обозначается как A_n. Порядок группы A_n ра-

вен $n!/2$ (так количество четных и нечетных подстановок в S_n всегда одинаково). При этом множество нечетных подстановок группу не образует.

Симметрические группы S_n и циклические группы тесно связаны с группами движений геометрических фигур на плоскости и в пространстве.

Простейшие группы движений

К группам движений относятся как конечные, так и бесконечные группы самосовмещений (симметрий) геометрических фигур. Под самосовмещением данной фигуры F понимают такое движение фигуры F, которое переводит F в саму себя, .т.е. совмещает F с самой собой. Все движения подразделяются на: повороты, отражения, переносы и композиции отражений и переносов.

Так, группа самосовмещений (симметрий) правильного n-угольника образуется при помощи n поворотов на плоскости на углы $2k\pi/n$, $k=0,...,n-1$ и n отражений относительно осей симметрии, проходящих через центр n-угольника и составляющих друг с другом равные углы. Группу симметрий правильного n-угольника принято называть группой диэдра и обозначать через D_n. Эта группа некоммутативна. Очевидно, что мощность D_n равна $2n$. Группа вращений C_n правильного n-угольника на плоскости является подгруппой D_n и изоморфна циклической группе $\mathbb{Z}_n$ и циклической подгруппе подстановок $\langle(1\,2\,...\,n)\rangle$.

В качестве конкретного примера рассмотрим группу симметрий правильного треугольника D_3. Занумеруем вершины треугольника числами 1, 2 и 3. Группа D_3 состоит из 6 элементов, а именно: из поворотов на углы 0, $\varphi_1=2\pi/3$ и $\varphi_2=4\pi/3$ на плоскости и трех отражений (поворотов) ψ_1, ψ_2 и ψ_3 вокруг осей симметрии в пространстве, соединяющих вершины 1, 2 и 3 с серединами противоположных сторон треугольника. Видно, что $\varphi_1^2=\varphi_2$, $\varphi_1^3=e$, $\psi_1^2=\psi_2^2=\psi_3^2=e$ (e – тождественный поворот). При этом, повороты ψ_1, ψ_2 и ψ_3 не могут быть получены из композиции (произведения) поворотов φ_1 и φ_2, но $\varphi_1\circ\psi_1=\psi_3$, $\psi_1\circ\varphi_1=\psi_2$ и т.д. Отождествим повороты треугольника с элементами группы S_3. Тогда $\varphi_1=(1\,2\,3)$, $\varphi_1^2=\varphi_2=(1\,3\,2)$, $\psi_1=(2\,3)$, $\psi_2=(1\,3)$, $\psi_3=(1\,2)$. Таким образом, группа симметрий правильного треугольника D_3 является изоморфной группе S_3.

Если перейти к рассмотрению групп симметрий пространственных фигур, то оказывается, что группа симметрий правильной n-угольной пирамиды (в ее основании лежит правильный n-угольник) полностью изо-

морфна группе вращений C_n правильного n-угольника. Рассмотрим двойную пирамиду (диэдр), состоящую из двух правильных n-угольных пирамид, чьи основания совмещены, а вершины находятся по разные стороны от основания. Ее группа вращений будет изоморфна группе симметрий правильного n-угольника, т.е. группе диэдра D_n.

Если рассматривать правильную треугольную пирамиду с равными сторонами (тетраэдр), то ее группа симметрий образуется при помощи 2 нетождественных вращений вокруг четырех осей, соединяющих вершины тетраэдра с серединами противоположных граней и вращений вокруг трех осей, соединяющих середины противоположных ребер тетраэдра. Добавляя сюда тождественное вращение, получаем группу из 12 элементов. Можно легко показать, что группа вращений тетраэдра (если занумеровать его вершины числами 1, 2, 3, 4) будет изоморфна подгруппе четных подстановок A_4 группы S_4.

Смежные классы

Пусть H_1 и H_2 – произвольные подмножества группы G.

Произведением подмножеств H_1 и H_2 называется подмножество H_3, состоящее из всех элементов вида h_1h_2, где $h_1 \in H_1$, $h_2 \in H_2$. Для произведения подмножеств используется обозначение: $H_3 = H_1H_2$. Эта операция ассоциативна. Очевидно, что $H_1\varnothing = \varnothing H_1 = \varnothing$, $H_1\{e\} = \{e\}H_1 = H_1$. Таким образом, множество всех подмножеств группы G является полугруппой с двусторонней единицей и обозначается как 2^H (H – любое подмножество в группе G). Отметим, что если H_1 и H_2 являются подгруппами группы G, то H_1H_2 вообще говоря подгруппой не является, при этом $H_1H_2 \subseteq \{H_1 \cup H_2\}$. Если H – подгруппа, то $HH = H$ (идемпотентность).

Множество H_1H_2 (где H_1 и H_2 – подгруппы группы G) тогда и только тогда является подгруппой G, когда $H_1H_2 = \{H_1 \cup H_2\}$.

Рассмотрим далее тот случай, когда одно из подмножеств, например H_1, состоит только из одного элемента. Пусть $g \in G$ и H – подгруппа группы G. Если $g \notin H$, то подмножество $gH = \{gh : h \in H\}$ не пересекается с H. Подмножество gH группы G называется ***левым смежным классом*** группы G по подгруппе H. Аналогично, подмножество Hg группы G называется ***правым смежным классом*** группы G по подгруппе H. При выборе различных элементов $g \in G$, правые и левые смежные классы подгруппы H в G изменяются. Так, если были выбраны смежные классы

g_1H и g_2H, причем $g_1, g_2 \in G$, $g_1, g_2 \notin H$, то смежные классы g_1H и g_2H состоят из разных элементов и не пересекаются.

Приведем основные свойства смежных классов на примере левых смежных классов (для правых смежных классов эти свойства аналогичны):

1) Если $g \in H$, то $gH \equiv H$.
2) $g \in gH$. Это следует из того, что H содержит нейтральный элемент e, а значит gH содержит элемент $ge = g$.
3) Два левых смежных класса группы G по подгруппе H или совпадают или не имеют общих элементов. Это следует из того, что если два смежных класса g_1H и g_2H имеют общий элемент $a = g_1h_1 = g_2h_2$ $(g_1, g_2 \in G, h_1, h_2 \in H)$, то $g_2 = g_1h_1h_2^{-1}$. Отсюда $g_2h = g_1h_1h_2^{-1}h = g_1h'$, где $h' = h_1h_2^{-1}h \in H$. Тогда $g_2H \subset g_1H$. Аналогично доказывается, что $g_1H \subset g_2H$, т.е. $g_1H = g_2H$.
4) $g_1H = g_2H$, если $g_1^{-1}g_2 \in H$. Это следует из свойства 3).
5) Разбиение группы G на левые смежные классы по подгруппе H определяет на G отношение эквивалентности. Действительно, любой элемент $g \in G$ содержится в смежном классе gH, это означает, что группу G можно представить в виде объединения непересекающихся смежных классов по подгруппе H вида:
   $G = \bigcup_i g_iH$, $g_i \in G$, $g_i \notin H$.

   Это вводит на группе G отношение эквивалентности, которое означает, что если два элемента a и b группы G эквивалентны, т.е. $a \sim b$, то значит они принадлежат одному и тому же смежному классу, например aH. При этом, если $a \sim b$, то $a^{-1}b \in H$ (см. свойство 4). Самостоятельно докажите, что это отношение, рефлексивно, симметрично и транзитивно.

Разбиение на смежные классы возникает естественным образом в группах перестановок S_n. Пусть $G = S_n$, а H есть совокупность элементов $\varphi \in S_n$, таких, что $\varphi(n) = n$, т.е. H переставляет все числа 1, 2, …, $n-1$ в S_n, кроме n. Нетрудно заметить, что H есть подгруппа в S_n, которая совпадает с S_{n-1}. Пусть $\tau_0 = e$ (тождественная перестановка), $\tau_i = (i\ n)$ – транспозиция, переводящая n в i ($i = 1, 2, \ldots, n-1$), тогда

$$S_n = \bigcup_{k=0}^{n-1} \tau_k S_{n-1}.$$

Рассмотрим разложение группы S_3 на левые и правые смежные классы по подгруппе $H = \langle (1\,2) \rangle \cong S_2 = \{e, (1\,2)\}$. Тогда получим:

$S_3 = \{e, (1\,2)\} \cup \{(1\,3), (1\,2\,3)\} \cup \{(2\,3), (1\,3\,2)\}$ – разложение на левые смежные классы;

$S_3 = \{e, (1\,2)\} \cup \{(1\,3), (1\,3\,2)\} \cup \{(2\,3), (1\,2\,3)\}$ – разложение на правые смежные классы.

Из этого примера видно, что множества левых и правых смежных классов группы G по подгруппе H не обязаны совпадать. Но это всегда выполняется, если группа G коммутативна. Тем не менее между множествами всех левых и правых смежных классов $\{gH\}$ и $\{Hg\}$ группы G по подгруппе H всегда существует взаимно однозначное (биективное) соответствие, а именно, если $x = gh \in gH$, то $x^{-1} = (gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1}$, т.е. $(gH)^{-1} = Hg^{-1}$. Таким образом, если $\{e, x, y, z, ...\}$ – множество представителей левых (правых) смежных классов, то $\{e, x^{-1}, y^{-1}, z^{-1}, ...\}$ – множество представителей правых (левых) смежных классов G по H. Мощности этих множеств совпадают.

Множество всех левых смежных классов группы G по подгруппе H обозначается через $(G/H)_l$, а множество всех правых смежных классов через $(G/H)_r$. Мощность множества (G/H) называется ***индексом*** подгруппы H в G и обозначается как: $(G:H) = |G/H| = ord(G/H)$.

Так как отображение $H \to gH$ взаимно однозначно, то $ord(gH) =$
$= (H:e) = ordH$. Отсюда придем к следующей формуле:

$$(G:e) = (G:H)(H:e) \Rightarrow |G| = |G/H| \cdot |H| \Rightarrow |G/H| = \frac{|G|}{|H|}.$$

Из этой формулы вытекает ***теорема Лагранжа***: порядок любой конечной группы делится на порядок каждой своей подгруппы. Следствием этой теоремы является то, что порядок любого элемента группы является делителем порядка группы.

Рассмотрим разбиение аддитивной группы целых чисел $\mathbb{Z}$ по подгруппе $m\mathbb{Z}$ чисел, кратных m, на смежные классы. Так как $\mathbb{Z}$ коммутативна, то разбиение $(\mathbb{Z}/m\mathbb{Z})_l$ совпадает с $(\mathbb{Z}/m\mathbb{Z})_r$. Любые два числа a и b из $\mathbb{Z}$ принадлежат одному и тому же смежному классу, если $a^{-1} \circ b \in m\mathbb{Z}?$, т.е. $-a + b \in \{mk, k \in \mathbb{Z}\}$. Это означает, что $b - a$ кратно m. Тогда $a \sim b$ равносильно $a \equiv b (\mathrm{mod} m)$ (сравнение по модулю m). При делении любого a из $\mathbb{Z}$ могут получаться остатки от деления, равные 0, 1, 2, …, $m-1$. Эти числа

будут минимальными представителями всех смежных классов группы $\mathbb{Z}$ по $m\mathbb{Z}$, т.е. разложение $(\mathbb{Z}/m\mathbb{Z})$ совпадает с разбиением $\mathbb{Z}$ на классы вычетов по модулю m и имеет следующий вид:

$$(\mathbb{Z}/m\mathbb{Z}) = \{0+mk,\ k\in\mathbb{Z}\}\cup\{1+mk_1,\ k_1\in\mathbb{Z}\}\cup\{2+mk_2,\ k_2\in\mathbb{Z}\}\cup\ldots$$

$$\ldots\cup\{m-1+mk_{m-1},\ k_{m-1}\in\mathbb{Z}\} = m\mathbb{Z}\cup(1+m\mathbb{Z})\cup\ldots(m-1+m\mathbb{Z}).$$

Этот пример дает общее определение сравнимости по модулю.

Пусть H – подгруппа группы G. Говорят, что элементы $g_1, g_2 \in G$ ***сравнимы по модулю*** H и пишут: $g_1 \equiv g_2 (\mathrm{mod} H)$, если $g_1^{-1} g_2 \in H$. Отношение сравнимости по модулю H есть отношение эквивалентности.

Аналогично, правые смежные классы Hg также задаются при помощи отношения сравнимости: $g_1 \equiv g_2 (\mathrm{mod} H)$, если $g_2 g_1^{-1} \in H$, т.е. $Hg_1 = Hg_2$.

Нормальные делители и фактор-группы

Выделим в группе G такие подгруппы H, для которых разбиения G по H на левые и правые смежные классы совпадают.

Подгруппа H группы G называется ***нормальным делителем*** (***инвариантной подгруппой*** или ***нормальной подгруппой***) группы G, если $\forall g \in G,\ \forall h \in H:\ g^{-1}hg \in H \Rightarrow gH = Hg$. Обозначение: $H \lhd G$.

Таким образом, H является нормальным делителем, если левостороннее разложение G по H совпадает с правосторонним разложением.

Для того, чтобы подгруппа H была нормальной в G, достаточно (но не необходимо), чтобы каждый элемент группы G был перестановочен с каждым элементом из H. В частности, в коммутативных (абелевых) группах любая подгруппа нормальна.

Теорема. Отношение сравнимости по модулю подгруппы H согласовано с операцией умножения в группе G тогда и только тогда, когда подгруппа H нормальна в G.

Согласованность операции умножения означает, что произведение любых двух смежных классов есть смежный класс:

$$(g_1H)(g_2H) = (g_1g_2)H = H(g_1g_2).$$

Из теоремы следует, что операция умножения в группе G определяет и операцию умножения на множестве смежных классов G/H. Эта операция наследует ассоциативность операции в G.

Элемент $H \in G/H$ является нейтральным элементом в G/H, что следует из того, что: $gH \cdot H = gH \cdot eH = (ge)H = gH$. Аналогично: $H \cdot gH = gH$ и $Hg \cdot H = H(ge) = Hg = H \cdot Hg$.

Кроме того, каждый смежный класс gH имеет обратный:

$(gH)^{-1} = Hg^{-1} = g^{-1}H$.

Таким образом, множество G/H является группой, если H – нормальная подгруппа в G. Группу G/H принято называть ***фактор-группой*** группы G по подгруппе H. Порядок фактор-группы G/H равен индексу группы H в G: $ord(G/H) = |G|/|H|$.

Группа, не имеющая нетривиальных нормальных подгрупп (кроме единичной и самой группы), называется ***простой группой***. К таким группам относится конечная группа $\mathbb{Z}_p$, где p – простое число.

Примеры фактор-групп.

1) Выше было показано, что разложение группы $\mathbb{Z}$ по подгруппе $m\mathbb{Z}$, т.е. множество $\mathbb{Z}/m\mathbb{Z}$ изоморфно группе $\mathbb{Z}_m$. Очевидно, что $\mathbb{Z}/m\mathbb{Z}$ – это фактор-группа, причем она коммутативна. Вообще, если группа коммутативна, то любая ее фактор-группа также коммутативна.
2) Смежные классы группы $\mathbb{C}$ по подгруппе $\mathbb{R}$ есть прямые линии L_a = $=\{z: \operatorname{Im} z = a, a \in \mathbb{R}\}$. Операция сложения в множестве $\mathbb{C}/\mathbb{R}$ задается формулой: $L_a + L_b = \{z: \operatorname{Im} z = a + b\} = L_{a+b}$, так что фактор-группа $\mathbb{C}/\mathbb{R}$ изоморфна группе $\mathbb{R}$.
3) Смежные классы группы $\mathbb{C}^*$ по подгруппе $T = \{z \in \mathbb{C}^*: |z| = 1\}$ есть окружности с центром в начале координат, т.е. $C_r = \{z \in \mathbb{C}^*: |z| = r > 0\}$. Операция умножения в $(\mathbb{C}^*/T)$ задается следующим образом: $C_{r_1} C_{r_2} = C_{r_1 r_2}$, та что фактор-группа $\mathbb{C}^*/T$ изоморфна группе $\mathbb{R}_+^*$.
4) Разбиение группы $GL_n(K)$ по $SL_n(K)$, является фактор-группой, так как левые и правые смежные классы здесь совпадают. Это следует из того, что в каждый смежный класс входят невырожденные матрицы с одинаковым определителем. Поэтому отношение сравнимости по модулю $H = SL_n(K)$: $g_1 \equiv g_2 (\mathrm{mod} H)$ как для левых, так и для правых смежных классов означает, что $\det g_1 = \det g_2$. $GL_n(K)/SL_n(K) \cong K^*$.

Пример 1 показывает, что если даже группа G и ее нормальная подгруппа H бесконечны, их фактор-группа может быть конечной.

Выше было отмечено, что если H_1 и H_2 являются подгруппами группы G, то их произведение $H_1 H_2$ вообще говоря не обязано быть подгруппой. Оказывается, если одна из подгрупп H_1 или H_2 нормальна, то мно-

жество H_1H_2 есть подгруппа в G. Если же обе подгруппы H_1 и H_2 нормальны в G, то множество H_1H_2 является нормальной подгруппой в G. Пересечение нормальных подгрупп есть нормальная подгруппа.

Утверждение 1. Всякая подгруппа индекса 2 – нормальна.

Утверждение 2. Если H – нормальная подгруппа группы G индекса n, то $g^n \in H$, $\forall g \in G$.

Из утверждения 1 следует, что подгруппа четных подстановок A_n в симметрической группе подстановок S_n является нормальной, так как разложение S_n по A_n содержит только два смежных класса: это собственно сама подгруппа A_n и множество нечетных подстановок. Тогда S_n / A_n – это фактор-группа, которая изоморфна абелевой группе C_2.

Множество Z элементов группы G называется ***центром группы*** G, если все элементы из Z перестановочны с любыми элементами из G, т.е.

$Z = Z(G) = \{z \in G : zg = gz, \forall g \in G\}$.

Группа G является коммутативной тогда и только тогда, когда $Z(G) = G$. Если $Z(G) = \{e\}$, то группа G называется группой без центра. Центр группы $Z(G)$ является нормальной коммутативной подгруппой в G.

Если группа G имеет порядок $|G| = p^k$ (p – простое число), то она называется p-группой. Такая группа всегда обладает нетривиальным центром $Z(G) \neq e$. При этом она имеет нормальные подгруппы порядков p^r для любых $r \le k$.

Утверждение 3. Ядро гомоморфизма $f : G \to H$, т.е. подгруппа $\operatorname{Ker} f$ в G является ее нормальной подгруппой. Именно, если $h \in \operatorname{Ker} f$, то $f(g^{-1}hg) = f(g^{-1}) f(h) f(g) = f^{-1}(g) f(g) = e' \in H \Rightarrow g^{-1}hg \in \operatorname{Ker} f$, $\forall g \in G$. Из этого утверждения получаем основную теорему о гомоморфизме.

Теорема 1 (основная теорема о гомоморфизме). Если $f : G \to H$ – гомоморфизм групп G и H с ядром $K = \operatorname{Ker} f$, то $G / K \cong \operatorname{Im} f$, т.е. фактор-группа G / K изоморфна образу гомоморфизма f.

Из теоремы 1 следует, что отображение $\pi : G \to G / K$ есть эндоморфизм групп, который принято называть *естественным гомоморфизмом*.

Следствие. Если группа G конечна, то $|G| = |\operatorname{Im} f| \cdot |\operatorname{Ker} f|$.

Теорема 2 (теорема о соответствии). Пусть G – группа, H и K – ее подгруппы, причем K – нормальна в G и $K \subset H$. Тогда $\overline{H} = H / K$ есть нормальная подгруппа в $\overline{G} = G / K$, $H \lhd G$, при этом

$G/H \cong \overline{G}/\overline{H} = (G/K)(H/K)$.

В связи с теоремой о соответствии рассмотрим следующий пример. Пусть $n = dm$ – натуральное число, $d > 1$. Очевидно, что $n\mathbb{Z} \subset d\mathbb{Z}$ и отображение $f : x \to dx + n\mathbb{Z}$ является эпиморфизмом групп $\mathbb{Z} \to d\mathbb{Z}/n\mathbb{Z} =$ $= \{di + n\mathbb{Z},\ i = 0,1,...m-1\}$ с ядром $m\mathbb{Z}$. По теореме о гомоморфизме имеем: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$. По теореме о соответствии имеем: $\mathbb{Z}/d\mathbb{Z} \cong$ $\cong (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$, т.е. $\mathbb{Z}_d \cong \mathbb{Z}_n/\mathbb{Z}_m$.

Примеры на основную теорему о гомоморфизме.

1) Рассмотрим гомоморфизм $f:\ \mathbb{C} \to \mathbb{R},\ f(z) = \operatorname{Im} z$. Имеем: $\operatorname{Im} f = \mathbb{R}$, $\operatorname{Ker} f = \mathbb{R}$, так что $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.
2) Рассмотрим гомоморфизм $f:\ \mathbb{C}^* \to \mathbb{R}_+^*,\ f(z) = |z|$. Здесь: $\operatorname{Im} f = \mathbb{R}_+^*$, $\operatorname{Ker} f = T = \{z \in \mathbb{C}^* : |z| = 1\}$, тогда $\mathbb{C}^*/T \cong \mathbb{R}_+^*$.
3) Рассмотрим гомоморфизм $f:\ \mathbb{R} \to \mathbb{C}^*,\ x = e^{ix}$. Здесь: $\operatorname{Im} f = T$, $\operatorname{Ker} f = 2\pi\mathbb{Z}$. Поэтому $\mathbb{R}/2\pi\mathbb{Z} \cong T$. Аналогично, $\mathbb{R}/n\mathbb{Z} \cong T$, $\forall n \in \mathbb{N}$.
4) Рассмотрим гомоморфизм $f:\ \mathbb{C}^* \to \mathbb{C}^*,\ f(z) = z^n$. Имеем: $\operatorname{Im} f = \mathbb{C}^*$, $\operatorname{Ker} f = C_n = \left\{z_k = e^{i2\pi k/n}, k = 0,1,...n-1, n \in \mathbb{N}\right\}$, так что $\mathbb{C}^*/C_n \cong \mathbb{C}^*$.

Классы сопряженных элементов

Пусть x и y принадлежат группе G. Эти элементы называются сопряженными и пишут: $x \approx y$, если $y = gxg^{-1}$ для некоторого $g \in G$. Множество x^G всех элементов, сопряженных с x, называется классом сопряженных элементов (классом сопряженности): $x^G = \{gxg^{-1} :\ g \in G\}$.

Подгруппа H нормальна в группе G тогда и только тогда, когда она является объединением классов сопряженных элементов, т.е. когда вместе с каждым своим элементом x содержит все элементы, сопряженные с x.

Из соотношения $y = gxg^{-1}$ следует, что $x = g^{-1}yg$.

Можно показать, что сопряженность двух элементов является отношением эквивалентности. При помощи этого отношения любая группа G распадается на непересекающиеся классы попарно сопряженных между собой элементов. Отметим, что классы сопряженности не обязаны совпадать со смежными классами. Так, класс сопряженности нейтрального элемента e любой группы G состоит только из одного элемента e. В абелевой группе любой класс сопряженности состоит из одного элемента.

В симметрической группе подстановок S_n подстановки сопряжены, если они имеют одинаковую цикловую структуру. Например, подстановки $\sigma = (i_1\ i_2 \ldots)(j_1\ j_2 \ldots)\ldots$ и $\sigma' = (i_1'\ i_2' \ldots)(j_1'\ j_2' \ldots)\ldots$ с циклами одинаковой длины сопрягаются при помощи подстановки $\varphi = \begin{pmatrix} i_1 & i_2 & \ldots & j_1 & j_2 & \ldots \\ i_1' & i_2' & \ldots & j_1' & j_2' & \ldots \end{pmatrix}$. Что легко проверяется. Действительно, $\varphi^{-1}\sigma'\varphi$ будет равно:

$$\begin{pmatrix} i_1' & i_2' & \ldots & j_1' & j' & \ldots \\ i_1 & i_2 & \ldots & j_1 & j_2 & \ldots \end{pmatrix}(i_1'\ i_2' \ldots)(j_1'\ j_2' \ldots)\ldots\begin{pmatrix} i_1 & i_2 & \ldots & j_1 & j_2 & \ldots \\ i_1' & i_2' & \ldots & j_1' & j_2' & \ldots \end{pmatrix} =$$

$$= (i_1\ i_2 \ldots)(j_1\ j_2 \ldots)\ldots$$

Задания для самостоятельного решения

1. Является ли мультипликативная группа $\mathbb{Z}_p^*=\{1, 2, \ldots, p-1\}$, где p – простое число, циклической?
2. Найти порядки каждого элемента мультипликативной группы $\mathbb{Z}_{12}^*$.
3. Найти группы автоморфизмов групп $\mathbb{Z}_p$ (p – простое число), S_3, D_4.
4. Найти все гомоморфизмы из $\mathbb{Z}_5$ в $\mathbb{Z}_{40}$.
5. Вычислите $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}^{147}$,
6. Найдите группы симметрий прямоугольника, ромба и параллелограмма. Опишите их при помощи подгрупп группы подстановок S_4.
7. Покажите, что группы вращений куба и октаэдра (правильного четырехугольного диэдра с равными сторонами) изоморфны группе S_4.
8. Найти левое и правое разложения группы S_3 по подгруппе $\langle(1\,3\,2)\rangle$.
9. (малая теорема Ферма) Докажите, что если p – простое число, то для любого целого числа a имеет место сравнение $a^p \equiv a(\mathrm{mod}\, p)$.
10. (теорема Эйлера) Докажите, что если число $\varphi(n)$ – порядок группы $\mathbb{Z}_n^*$, то для любого целого числа a, взаимно простого с n, имеет место сравнение $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$.
11. Найти смежные классы группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^*$.
12. Найдите все нормальные подгруппы и центр группы S_4.
13. В группе S_4 найти все подстановки, сопряженные с $(1\,2)(3\,4)$.