Ткачев С.Б.

каф. Математического моделирования
МГТУ им. Н.Э. Баумана

ДИСКРЕТНАЯ МАТЕМАТИКА

ИУ5 — 4 семестр, 2015 г.

Лекция 9. ГРУППЫ, КОЛЬЦА, ПОЛЯ

Существует две формы записи бинарной операции группы. В **аддитивной записи** операцию обозначают знаком $+$, нейтральный элемент — знаком $\mathbf{0}$, элемент, обратный к a относительно операции $+$, записывают в виде $-a$ и называют **противоположным** к a.
Бинарную операцию группы в этом случае называют **сложением**

В **мультипликативной записи** операцию обозначают знаком $\cdot$, нейтральный элемент — знаком $\mathbf{1}$, элемент, обратный к a, записывают в виде a^{-1}.
В этом случае бинарную операцию группы называют **умножением** (также **умножением группы** или **групповым умножением**), элемент $a \cdot b$ —**произведением** элементов a и b, и записывают в виде ab.

Пример 9.1. Алгебра $(\mathbb{Z}, +)$ — коммутативная группа.
На множестве целых чисел операция сложения ассоциативна и коммутативна.
Число 0 есть нейтральный элемент.
Для каждого целого числа n существует обратный по сложению элемент, число $-n$, противоположное n.
Рассматриваемую группу называют **аддитивной группой целых чисел**.

Пример 9.2. Множество всех *биекций* некоторого множества A на себя с операцией композиции отображений есть группа.

Композиция двух биекций есть биекция.

Операция композиции ассоциативна.

Нейтральный элемент — тождественное отображение id_A — есть биекция.

Для всякой биекции $f\colon A \to A$ отображение f^{-1}, обратное биекции f, определено, является биекцией и выполнены равенства $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_A$.

Эту группу называют **симметрической группой множества** A.

Если множество A конечно, — **группой подстановок** множества A.

Пример 9.3.
Алгебры $(\mathbb{Q} \setminus \{0\}, \cdot)$ и $(\mathbb{R} \setminus \{0\}, \cdot)$ есть коммутативные группы.
Их называют
мультипликативной группой рациональных чисел
и **мультипликативной группой действительных чисел** соответственно.

В каждой из них число 1 есть нейтральный элемент (единица) группы.
Обратный к числу x по операции умножения элемент x^{-1} есть число $x^{-1} = 1/x$.

Пример 9.4.
Рассмотрим алгебру $\mathbb{Z}_k^+ = (\{0,\ 1,\ \ldots,\ k-1\},\ \oplus_k)$. Операция $\oplus_k$ (**сложения по модулю k**) определяется следующим образом:
для любых двух m и n число $m \oplus_k n$, называемое **суммой** чисел m и n **по модулю** k, равно остатку от деления арифметической суммы $m+n$ на k.

Эта алгебра является коммутативной группой. Ее называют **аддитивной группой вычетов по модулю** k.

Нейтральным элементом служит число 0.

Обратным к числу n будет $k-n$, т.к. $n \oplus_k (k-n) = 0$.

Пример 9.5. Множество всех невырожденных (т.е. имеющих ненулевой определитель) числовых квадратных матриц порядка n с операцией умножения матриц является группой.

Произведение двух невырожденных матриц снова есть невырожденная матрица.

Единичная матрица порядка n невырожденная.

Матрица, обратная к невырожденной, также является невырожденной.

При использовании аддитивной записи операции для коммутативной группы $\mathcal{G} = (G, +, \mathbf{0})$ уравнения $a + x = b$, $x + a = b$ сводятся к одному:

$$a + x = b,$$

Решение уравнения есть $x = b + (-a)$.

Правую часть этого равенства в коммутативной группе называют **разностью** элементов b и a и обзначают $b - a$.

Операцию, сопоставляющую упорядоченной паре (a, b) разность $b - a$, называют операцией **вычитания**.

С учетом введенных обозначений решение уравнения в коммутативной группе можно записать так: $x = b - a$.

9.1. Группа подстановок

Рассмотрим взаимнооднозначное отображение n -элементного множества $\{1, 2, \dots, n\}$ в себя (биекцию). Такую биекцию называют *подстановкой* этого множества.

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}.$$

Образ 1 (при отображении σ) есть α_1 , образ 2 есть α_2 , $\dots$, образ n есть α_n .

Циклом длины k называют подстановку, которая отображает β_1 в β_2, β_2 в β_3, $\ldots$, β_{k-1} в β_k, а β_k в β_1, где $\beta_i \in \{1, \ldots, n\}$, $i = 1, \ldots, k$ и все β_i попарно различны, а все элементы, отличные от β_1, $\ldots$, β_k, отображаются сами в себя.
Цикл записывают ее в виде $(\beta_1 \; \beta_2 \; \ldots \; \beta_k)$.

Например, подстановку из группы S_4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

можно записать в виде $(1\;3\;4)$.

Цикл длины 2 называют *транспозицией*.

Обратная подстановка

Подстановка, обратная подстановке

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

есть подстановка, которая отображает α_1 в 1, α_2 в 2, ... α_n в n. Отметим, что при записи обратной подстановки элементы первой строки тем не менее записываются в обычном порядке: $1, \ldots, n$.

Решение уравнений в группе подстановок

В группе S_3 решим следующее уравнение:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ X = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Умножив обе части уравнения слева на

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

получим

$$X = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Окончательно получим

$$X = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

9.2. Кольца, тела, поля

Определение 9.1. **Кольцом** называют **алгебру**

$$\mathcal{R} = (R,\ +,\ \cdot,\ \mathbf{0},\ \mathbf{1}),$$

сигнатура которой состоит из двух бинарных и двух нульарных операций, причем для любых $a,\ b,\ c \in R$ выполняются равенства:

1) $a + (b + c) = (a + b) + c\,;$
2) $a + b = b + a\,;$
3) $a + \mathbf{0} = a\,;$
4) для каждого $a \in R$ существует элемент a', такой, что $a + a' = \mathbf{0}\,;$
5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c\,;$
6) $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a\,;$
7) $a \cdot (b + c) = a \cdot b + a \cdot c\,,\ (b + c) \cdot a = b \cdot a + c \cdot a\,.$

Операцию $+$ называют **сложением кольца**.
Операцию $\cdot$ — **умножением кольца**.
Элемент $\mathbf{0}$ — **нулем кольца**.
элемент $\mathbf{1}$ — **единицей кольца**.

Равенства 1–7, указанные в определении, называют **аксиомами кольца**.

Аксиомы кольца 1–4 означают, что алгебра $(R, +, \mathbf{0})$, сигнатура которой состоит только из операций сложения кольца $+$ и нуля кольца $\mathbf{0}$, является **абелевой группой**. Эту группу называют **аддитивной группой кольца** $\mathcal{R}$

Аксиомы кольца 5 и 6 показывают, что алгебра $(R, \cdot, \mathbf{1})$, сигнатура которой включает только умножение кольца $\cdot$ и единицу кольца $\mathbf{1}$, есть моноид. Этот моноид называют **мультипликативным моноидом кольца** $\mathcal{R}$

Аксиома 7 устанавливает связь между сложением кольца и умножением кольца. Операция умножения дистрибутивна относительно операции сложения.

Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями $\mathcal{R} = (R, +, \cdot, \mathbf{0}, \mathbf{1})$, такая, что:

1) алгебра $(R, +, \mathbf{0})$ — коммутативная группа;

2) алгебра $(R, \cdot, \mathbf{1})$ — моноид;

3) операция $\cdot$ (умножения кольца) дистрибутивна относительно операции $+$ (сложения кольца).

Определение 9.2. Кольцо называют **коммутативным**, если его операция умножения коммутативна.

Пример 9.6.
а. Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо. Отметим, что алгебра $(\mathbb{N}, +, \cdot)$ кольцом не будет, поскольку $(\mathbb{N}, +)$ — коммутативная полугруппа, но не группа.

б. Рассмотрим алгебру

$$\mathbb{Z}_k = (\{0, 1, \ldots, k-1\}, \oplus_k, \odot_k, 0, 1)$$

($k \geq 1$) с операцией $\oplus_k$ сложения по модулю k и $\odot_k$ (умножения по модулю k).
Операция умножения по модулю k аналогична операции сложения по модулю k: $m \odot_k n$ равно остатку от деления на k числа $m \cdot n$.
Эта алгебра есть коммутативное кольцо, которое называют **кольцом вычетов по модулю** k .

Пример 9.7. **а.** Алгебра $(2^A, \triangle, \cap, \varnothing, A)$ — коммутативное кольцо. Это следует из свойств *пересечения* и *симметрической разности множеств*.

б. Множество всех квадратных матриц фиксированного порядка с операциями сложения и умножения матриц — некоммутативное кольцо.
Единицей этого кольца является единичная матрица, а нулем — нулевая.

Теорема 1. В любом кольце выполняются следующие тождества:

1 $\mathbf{0} \cdot a = a \cdot \mathbf{0} = \mathbf{0}$;

2 $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$;

3 $(a - b) \cdot c = a \cdot c - b \cdot c \,, \quad c \cdot (a - b) = c \cdot a - c \cdot b \,.$

◀ Докажем тождество $\mathbf{0} \cdot a = \mathbf{0} \quad (1)$.

$$\forall\, a\ (a + \mathbf{0} \cdot a = \mathbf{1} \cdot a + \mathbf{0} \cdot a =$$
$$(\mathbf{1} + \mathbf{0}) \cdot a = \mathbf{1} \cdot a = a).$$

В аддитивной группе кольца получили уравнение

$$a + \mathbf{0} \cdot a = a$$

относительно неизвестного элемента $\mathbf{0} \cdot a$.
В аддитивной группе любое уравнение вида $a + x = b$ имеет единственное решение $x = b - a$.
$\mathbf{0} \cdot a = a - a = \mathbf{0}$.

Тождество $a \cdot \mathbf{0} = \mathbf{0}$ доказывается аналогично.

Докажем тождество $-(a \cdot b) = a \cdot (-b) \quad (2)$. Имеем

$$a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot \mathbf{0} = \mathbf{0} \Rightarrow$$
$$\Rightarrow \; a \cdot (-b) = -(a \cdot b)$$

$(-a) \cdot b = -(a \cdot b)$ можно доказать точно так же.

Докажем тождества (3).
Рассмотрим $(a - b) \cdot c = a \cdot c - b \cdot c$.
С учетом доказанного выше имеем

$$a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b - a \cdot c,$$

т.е. тождество справедливо.
Тождество $c \cdot (a - b) = c \cdot a - c \cdot b$ доказывается аналогично. ►

Следствие 9.1. В любом кольце справедливо тождество

$$(-\mathbf{1}) \cdot x = x \cdot (-\mathbf{1}) = -x.$$

◀ Указанное следствие вытекает из второго тождества теоремы 1 при $a = \mathbf{1}$ и $b = x$. ▶

Первые два тождества в теореме выражают свойство, называемое **аннулирующим свойством нуля** в кольце.

Тождества (3) теоремы 1 выражает свойство дистрибутивности операции умножения кольца относительно операции вычитания.

В любом кольце производя вычисления , можно раскрывать скобки и менять знаки так же, как и при сложении, вычитании и умножении действительных чисел.

Определение 9.3. Ненулевые элементы a и b кольца $\mathcal{R}$ называют **делителями нуля**, если $a \cdot b = \mathbf{0}$ или $b \cdot a = \mathbf{0}$.

Пример 9.8. Кольцо вычетов по модулю k, если k — составное число.
В этом случае произведение по модулю k любых m и n, дающих при обычном перемножении число, кратное k, будет равно нулю.
В кольце вычетов по модулю 6 элементы 2 и 3 являются делителями нуля, поскольку $2 \odot_6 3 = 0$.

Пример 9.9. Кольцо квадратных матриц фиксированного порядка (не меньшего двух).
Например, для матриц второго порядка имеем

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

При отличных от нуля a и b приведенные матрицы являются делителями нуля.

Определение 9.4. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Определение 9.5. Коммутативное тело называют **полем**, а группу ненулевых элементов тела (поля) по умножению —**мультипликативной группой** этого **тела(поля)**.

Поле есть частный случай кольца, в котором операции обладают дополнительными свойствами.

Аксиомы поля

Поле есть алгебра $\mathcal{F} = (F, +, \cdot, \mathbf{0}, \mathbf{1})$, сигнатура которой состоит из двух бинарных и двух нульарных операций, причем справедливы тождества:

1) $a + (b + c) = (a + b) + c$;
2) $a + b = b + a$;
3) $a + \mathbf{0} = a$;
4) для каждого $a \in F$ существует элемент $-a$, такой, что $a + (-a) = \mathbf{0}$;
5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6) $a \cdot b = b \cdot a$;
7) $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$;
8) для каждого $a \in F$, отличного от $\mathbf{0}$, существует элемент a^{-1}, такой, что $a \cdot a^{-1} = \mathbf{1}$;
9) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Пример 9.10.

а. Алгебра $(\mathbb{Q}, \, , +, \cdot, 0, 1)$ есть поле, называемое **полем рациональных чисел**.

б. Алгебры $(\mathbb{R}, +, \cdot, 0, 1)$ и $(\mathbb{C}, +, \cdot, 0, 1)$ есть поля, называемые **полями действительных** и **комплексных чисел** соответственно.

9.3. Области целостности

Областью целостности называют **коммутативное кольцо** без **делителей нуля**.

Так, кольцо целых чисел есть область целостности.

Утверждение 9.1. Если A — конечное множество и $f : A \to A$ — инъекция, то она является сюръекцией и следовательно биекцией

Теорема 2. Конечная область целостности является **полем**.

◀ Поле — это кольцо, умножение которого **коммутативно**, каждый ненулевой элемент a имеет **обратный элемент** относительно **умножения**.
Область целостности является **коммутативным** кольцом без делителей нуля.
Докажем, что для конечной области целостности любой ненулевой элемент обратим, т.е.

$$\forall\ (a \neq \mathbf{0})\exists x\ (\text{единственный})\ |\ a \cdot x = \mathbf{1}.$$

Фиксируем произвольный элемент $a \neq \mathbf{0}$.
Определим отображение f_a множества всех ненулевых элементов в себя по формуле $f_a(x) = a \cdot x$
($a \cdot x \neq \mathbf{0}$ в области целостности при $a \neq \mathbf{0}$ и $x \neq \mathbf{0}$).
Докажем, что отображение f_a — инъекция (каждый элемент из области значений имеет единственный прообраз).

$$a \cdot x = a \cdot y \;\Rightarrow\; a \cdot (x - y) = \mathbf{0} \Rightarrow$$
$$\Rightarrow x - y = \mathbf{0} \;(\text{т.к. делители нуля отсутствуют}) \Rightarrow\; x = y$$

Множество носитель по условию теоремы конечено, следовательно, f_a — биекция (утверждение 9.1).
Поэтому $\forall(y)\, \exists(\text{ единственный } x)|\; y = a \cdot x$.
В частности, при $y = \mathbf{1}$ равенство $a \cdot x = \mathbf{1}$ выполнено для некоторого однозначно определенного x , т.е. $x = a^{-1}$. ▶

Следствия теоремы 2.

Следствие 9.2. Кольцо $\mathbb{Z}_p$ вычетов по модулю p является полем тогда и только тогда, когда p — простое число.

◀ Пусть $\mathbb{Z}_p$ является полем. Покажем, что p — простое число.
Предположим — p составное.
Тогда найдутся такие k и l, $0 < k \leq p-1; 0 < l \leq p-1$, что $p = k \cdot l \Rightarrow$
$k \cdot l = 0 \,(\mathrm{mod\,p}) \Rightarrow$ k и l — делители нуля в кольце $\mathbb{Z}_p$.
Следовательно, $\mathbb{Z}_p$ — не поле.
Число p не может быть составным.

Пусть p — простое число.

Предположим, что $m \cdot n = 0 \,(\mathrm{mod\,p})$, т.е. элементы m и n кольца $\mathbb{Z}_p$ будут делителями нуля (кольцо не область целостности).

p — простое число и $(m \cdot n = 0 \,(\mathrm{mod\,p})) \Rightarrow$
$\left((m = 0 \,(\mathrm{mod\,p})) \vee (n = 0 \,(\mathrm{mod\,p})) \right)$

Т.к. $((0 \leq m \leq p-1) \wedge (0 \leq n \leq p-1)) \Rightarrow (m = 0) \vee (n = 0)$. Следовательно, при простом p делителей нуля нет.

Кольцо $\mathbb{Z}_p$ является конечной областью целостности и по теореме 2 — полем. ▶

Материал для самостоятельного изучения

9.4. Циклическая полугруппа

В свободном моноиде, порожденном некоторым конечным множеством, оба закона сокращения справедливы, но никаких обратных элементов не существует.
В полугруппе можно умножать любой элемент a сам на себя, причем в силу ассоциативности операции полугруппы элемент $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ раз}}$ определен однозначно.

Этот элемент называют n-й **степенью элемента** a и обозначают a^n.
При этом $a^1 = a$, $a^n = a \cdot a^{n-1}$, $n = 2, 3, \ldots$

В моноиде вводят также нулевую степень элемента, полагая $a^0 = \mathbf{1}$.
Если $(A, \cdot, \mathbf{1})$ — группа, то можно ввести и отрицательные степени элемента согласно равенству $a^{-n} = (a^{-1})^n$, $n = 1, 2, \ldots$

Сформулируем утверждения о свойствах степеней (без доказательства).

Утверждение 9.2. Для любой полугруппы $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (m, $n \in \mathbb{N}$).

Утверждение 9.3. Для любой группы $a^{-n} = (a^n)^{-1}$ $(n \in \mathbb{N})$, $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (m, $n \in \mathbb{Z}$).

Определение 9.6. Полугруппу (в частности, группу) $(A, \cdot)$ называют **циклической**, если существует такой элемент a, что любой элемент x полугруппы является некоторой (целой) степенью элемента a.
Элемент a называют **образующим элементом полугруппы (группы)**.

Пример 9.11. а. Полугруппа $(\mathbb{N}, +)$ циклическая, с образующим элементом 1. При аддитивной записи бинарной операции возведение элемента a в положительную степень n есть сумма n этих элементов, и это записывают $n \cdot a$ (или na, без знака умножения).

б. Группа $(\mathbb{Z}, +, 0)$ также циклическая. Для нее образующими элементами могут быть 1 и -1.
Рассмотрим элемент 1. Тогда $0 \cdot 1 = 0$, $n \cdot 1 = \underbrace{1 + \ldots + 1}_{n \text{ раз}} = n$ ($n > 0$) и $(-1) \cdot 1 = -1$, $(-n) \cdot 1 = n \cdot (-1) = \underbrace{(-1) + \ldots + (-1)}_{n \text{ раз}} = -n$ ($n > 0$).
Если в качестве образующего взять элемент -1, то $0 \cdot (-1) = 0$, отрицательные целые числа получаются как положительные „степени“ -1, а положительные — как отрицательные „степени“ -1. Например, $(-2) \cdot (-1) = 2$, $4 \cdot (-1) = -4$.

в. Группа $(\mathbb{Z}_3,\ \oplus_3,\ 0)$ вычетов по модулю 3 циклическая, причем любой ее ненулевой элемент является образующим. Действительно, для 1 имеем $1 \oplus_3 1 = 2$, $1 \oplus_3 1 \oplus_3 1 = 0$, а для 2 получим $2^2 = 2 \oplus_3 2 = 1$, $2 \oplus_3 2 \oplus_3 2 = 0$. #

Рассмотрим подробнее строение конечных циклических групп, используя мультипликативную запись бинарной операции.

Вспомним, *конечная алгебра* (**конечная группа**, в частности) — это алгебра, носитель которой — конечное множество.

Порядком конечной группы называют количество элементов в этой группе.

Например, аддитивная группа вычетов по модулю k имеет порядок k.

Симметрическая группа степени n, т.е. группа подстановок S_n, имеет порядок $n!$.

Мультипликативная группа вычетов по модулю p, где p — простое число, имеет порядок $p-1$.

Порядок элемента a циклической группы — это наименьшее положительное n, такое, что $a^n = \mathbf{1}$.

Теорема 3. Порядок образующего элемента конечной циклической группы равен порядку самой группы.

◀ Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — конечная циклическая группа с образующим элементом a и $n > 0$ — порядок этого элемента.
Тогда все степени $a^0 = \mathbf{1}$, $a^1 = a$, …, a^{n-1} попарно различны.
Действительно, если $a^k = a^l$, $0 < l < k < n$, то $a^{k-l} = a^{k+(-l)} = a^k a^{-l} = a^l a^{-l} = a^{l-l} = \mathbf{1}$.
Получено противоречие с выбором n как порядка элемента a, поскольку $k - l < n$ (найдена степень, меньшая n, при возведении в которую элемента a получится единица).

Докажем, что любая степень элемента a принадлежит множеству $\{\mathbf{1},\ a,\ \ldots,\ a^{n-1}\}$.

$\forall(m \in \mathbb{Z})\ \exists(n, k \in \mathbb{Z}) |\ (m = kn+q)$, где $(q \in \mathbb{Z}\ \wedge 0 \leq q < n$

Тогда

$$a^m = a^{kn+q} = a^{kn} \cdot a^q = (a^n)^k \cdot a^q = \mathbf{1} \cdot a^q = a^q \in \{\mathbf{1},\ a,\ \ldots,\ a^{n-1}$$

Поскольку каждый элемент группы $\mathcal{G}$ есть некоторая степень элемента a, то $G = \{\mathbf{1},\ a,\ \ldots,\ a^{n-1}\}$ и порядок группы равен n. ►

Из доказанной теоремы следует, что в бесконечной циклической группе не существует такого $n > 0$, что для образующего элемента a группы выполняется равенство $a^n = \mathbf{1}$.

9.5. Подгруппы.

Пусть $\mathcal{G} = (G, *)$ — произвольный группоид и $H \subseteq G$ — некоторое подмножество множества G.
Рассмотрим свойства бинарной операции $*$ группоида $\mathcal{G}$ на подмножестве H.

Определение 9.7. Множество $H \subseteq G$ **замкнуто относительно операции** $*$, если $x * y \in H$ для любых x, $y \in H$.

В этом случае подмножество H с операцией $*$ будет группоидом $\mathcal{H} = (H, *)$. Его называют **подгруппоидом** группоида $\mathcal{G}$.

Если подмножество H замкнуто относительно бинарной операции $*$ и эта *бинарная операция ассоциативна* на множестве G, то операция останется ассоциативной и при ее ограничении на подмножество H.
Если группоид $\mathcal{G}$ является полугруппой, то и всякий его подгруппоид будет полугруппой, называемой подполугруппой полугруппы $\mathcal{G}$.

Однако в случае, когда группоид является *моноидом* (*группой*), уже нельзя утверждать, что любой подгруппоид является также моноидом (группой).

Пример 9.12. Рассмотрим группоид —**аддитивную группу целых чисел** $(\mathbb{Z}, +)$.
Выделим в множестве целых чисел подмножество $\mathbb{N}$ натуральных чисел. Это подмножество замкнуто относительно операциии сложения $+$, группоид $(\mathbb{N}, +)$ будет подгруппоидом группоида $(\mathbb{Z}, +)$.
Так как операция сложения чисел ассоциативна, $(\mathbb{N}, +)$ будет подполугруппой. Однако в множестве $\mathbb{N}$ отсутствует **нейтральный элемент** 0 относительно операции сложения. Следовательно, $(\mathbb{N}, +)$ не является группой (не является даже моноидом).

Пусть $\mathcal{M} = (M, \cdot, \mathbf{1})$ — моноид.
Если P есть подмножество M, замкнутое относительно бинарной операции $\cdot$ моноида $\mathcal{M}$ и содержащее нейтральный элемент **(единицу)** $\mathbf{1}$ этого моноида, то $\mathcal{P} = (P, \cdot, \mathbf{1})$ также есть моноид.
Его называют **подмоноидом** моноида $\mathcal{M}$.
Замкнутость подмножества $B \subseteq A$ относительно нульарной операции a на A равносильна соотношению $a \in B$.

Определение 9.8. Моноид $\mathcal{P} = (P, \cdot, \mathbf{1})$ есть подмоноид моноида $\mathcal{M} = (M, \cdot, \mathbf{1})$ тогда и только тогда, когда множество P замкнуто относительно бинарной операции $\cdot$ моноида $\mathcal{M}$, а также относительно его нульарной операции $\mathbf{1}$.

Определение 9.9. Пусть $\mathcal{G} = (G, \cdot, {}^{-1}, \mathbf{1})$ — группа, а H есть подмножество G, замкнутое относительно операции $\cdot$ группы $\mathcal{G}$, содержащее нейтральный элемент **(единицу)** $\mathbf{1}$ этой группы и вместе с каждым элементом $x \in H$ содержащее **элемент** x^{-1}, **обратный** к x, т.е. замкнутое относительно унарной операции ${}^{-1}$ взятия обратного, которая здесь включена в сигнатуру группы.

Тогда $\mathcal{H} = (H, \cdot, {}^{-1}, \mathbf{1})$ также есть группа, которую называют **подгруппой** группы $\mathcal{G}$.

Пусть ω — унарная операция на множестве G моноида $\mathcal{G}$, $\mathcal{H}$ — некоторый его подмоноид.
Подмоноид $\mathcal{H}$ моноида $\mathcal{G}$ называется замкнутым относительно унарной операции ω , если для каждого $x \in H$ имеет место $\omega(x) \in H$.
Группа $\mathcal{H} = (H, \cdot, ^{-1}, \mathbf{1})$ есть подгруппа группы $\mathcal{G} = (G, \cdot, ^{-1}, \mathbf{1})$ в том и только в том случае, когда множество H замкнуто относительно всех операций $\cdot$, $^{-1}$, $\mathbf{1}$ сигнатуры группы $\mathcal{G}$.
Единица моноида (группы) служит одновременно единицей любого его подмоноида (любой подгруппы).

Пример 9.13.

а. Подмножество всех натуральных четных чисел есть подполугруппа полугруппы $(\mathbb{N}, +)$ (подмножество всех натуральных четных чисел замкнуто относительно сложения, операция сложения ассоциативна).

б. Аддитивная полугруппа натуральных чисел с нулем $(\mathbb{N} \cup \{0\}, +)$ — моноид с нейтральным элементом 0.

Подмножество всех положительных (> 0) четных чисел с операцией сложения не будет подмоноидом моноида $(\mathbb{N} \cup \{0\}, +, 0)$, так как ее носитель не содержит нуля — единицы моноида.

Подмножество всех натуральных чисел вместе с нулем, делящихся на заданное число $k > 1$, замкнуто относительно операции сложения; на нем может быть определен подмоноид моноида $(\mathbb{N} \cup \{0\}, +, 0)$.

в. Группа рациональных чисел $\mathbb{Q}$ с операцией умножения, является подгруппой группы действительных чисел с операцией умножения $(\mathbb{R} \setminus \{0\}, \cdot, 1)$.
г. Алгебра $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ не является подгруппой группы $(\mathbb{R} \setminus \{0\}, \cdot, 1)$, т.к. не содержит вместе с каждым целым числом m обратного к нему числа $\dfrac{1}{m}$.
Данное множество будет моноидом т.к. оно замкнуто относительно операции умножения и содержит единицу.

9.6. Циклические подгруппы

Пусть $\mathcal{G} = (G, \cdot, ^{-1}, \mathbf{1})$ — группа.
Произведение любых **степеней элемента** a есть снова некоторая степень элемента a, нулевая степень дает единицу группы, а обратным к элементу a^k является элемент a^{-k}.
Таким образом, множество всех степеней фиксированного элемента a группы $\mathcal{G}$ является подгруппой группы $\mathcal{G}$.

Определение 9.10. Подгруппу группы $\mathcal{G}$, заданную на множестве всех степеней фиксированного элемента a, называют **циклической подгруппой** группы $\mathcal{G}$, **порожденной элементом** a.

Пример 9.14. В группе $\mathbb{Z}_{13}^*$ (мультипликативной группе вычетов по модулю 13) построим циклическую подгруппу, порожденную элементом 5.

Имеем: $5^0 = 1\,,\ 5^1 = 5\,,\ 5^2 = 5 \odot_{13} 5 = 12\,,\ 5^3 = 5 \odot_{13} 12 = 8\,,\ 5^4 = 5 \odot_{13} 8 = 1\,.$

Порядок этой циклической подгруппы равен 4.

Она состоит из элементов: 1, 5, 8 и 12.

9.7. Теорема Лагранжа

Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — группа, а $\mathcal{H} = (H, \cdot, \mathbf{1})$ — ее подгруппа.

Левым смежным классом подгруппы $\mathcal{H}$ **по элементу** $a \in G$ называют множество

$$aH = \{y\colon y = a \cdot h,\ h \in H\}\,.$$

Соответственно **правый смежный класс подгруппы** $\mathcal{H}$ **по элементу** $a \in G$ — это множество

$$Ha = \{y\colon y = h \cdot a,\ h \in H\}\,.$$

Очевидно, что в коммутативной группе $aH = Ha$.

Утверждение 9.4.

$$a \in H \Rightarrow aH = H$$

◀ Рассмотрим левые смежные классы.
Покажем методом двух включений, что если $a \in H$, то $aH = H$.
С одной стороны

$$(x \in aH) \wedge (a \in H) \Rightarrow \exists h \in H \quad x = ah.$$

Поскольку множество H замкнуто относительно умножения группы $\mathcal{G}$ $\Rightarrow$ $x \in H$.

Обратно,

$$x \in H \Rightarrow \ x = \mathbf{1} \cdot x = (aa^{-1})x = a(a^{-1}x) = ah$$

где $h = a^{-1}x \in H \Rightarrow \ x \in aH$.
Окончательно получим $aH = H$. ▶

Покажем, что с использованием смежных классов можно построить отношение эквивалентности.
Введем **бинарное отношение** $\sim_H$ на множестве G следующим образом: элементы a и b связаны отношением $\sim_H$ ($a \sim_H b$), если и только если левые смежные классы подгруппы $\mathcal{H}$ по элементам a и b совпадают ($aH = bH$).

Теорема 4. Бинарное отношение $\sim_H$ есть эквивалентность на G , причем класс эквивалентности произвольного элемента $a \in G$ совпадает с левым смежным классом aH .

◀ Докажем, что $\sim_H$ является эквивалентностью на G.

$\forall a \in G \ (aH = aH) \Rightarrow a \sim_H a \Rightarrow$ **рефлексивно**;

$a \sim_H b \Rightarrow (aH = bH) \Rightarrow (bH = aH) \Rightarrow (b \sim_H a) \Rightarrow$

$\Rightarrow$ **симметричность**;

$a \sim_H b \wedge b \sim_H c \Rightarrow (aH = bH) \wedge (bH = cH) \Rightarrow a \sim_H c \Rightarrow$

$\Rightarrow$ **транзитивность**

$\sim_H$ есть эквивалентность

Методом двух включений докажем , что класс эквивалентности произвольного элемента a равен aH $[a]_{\sim_H} = aH$.
Пусть

$$x \in [a]_{\sim_H} \Rightarrow x \sim_H a \Rightarrow xH = aH$$

Из равенства множеств $xH = \{xh_1 | h_1 \in H\}$ и $aH = \{ah | h \in H\}$ следует, что любой элемент вида $ah \in aH$, $h \in H$, может быть представлен в виде $xh_1 \in xH$, где $h_1 \in H$, т.е. $ah = xh_1$.
Отсюда $x = ahh_1^{-1} = ah_2$, где $h_2 = hh_1^{-1}$. $h_2 \in H$ в силу замкнутости подгруппы $\mathcal{H}$ относительно групповой операции, и $ah_2 \in aH$.
Следовательно, $[a]_{\sim_H} \subseteq aH$.

Докажем, что $aH \subseteq [a]_{\sim_H}$ (второе включение).
Пусть

$$x \in aH, \text{ тогда } \exists h \in H \mid x = ah \Rightarrow xH = ahH.$$

$$ahH = \{(ah)h_3 | h_3 \in H\} = \{a(hh_3) | h_3 \in H\} = \\ = \{ah_4 | h_4 \in H\} = aH$$

$$\Rightarrow xH = aH \Rightarrow (x \sim_H a) \Rightarrow x \in [a]_{\sim_H} \Rightarrow aH \subseteq [a]_{\sim_H}$$

►

Определение 9.11. Множества A и B называются **равномощными** $(|A| = |B|)$, если существует взаимнооднозначное отображение (биекция) f множества A на множество B.

Теорема 5. Всякий левый смежный класс подгруппы H **равномощен** H.

◀ Для произвольного фиксированного $a \in G$ зададим отображение $\varphi_a \colon H \to aH$ следующим образом:

$$\varphi_a(h) = ah.$$

1. Отображение φ_a есть сюръекция, так как если $y \in aH$, то $y = ah$ для некоторого $h \in H$, откуда $y = \varphi_a(h)$.
2. φ_a — инъекция, поскольку из равенства $ah_1 = ah_2$ в силу законов сокращения в группе $\mathcal{G}$ следует $h_1 = h_2$.
Следовательно, φ_a — биекция и $|aH| = |H|$. ▶

Определение 9.12. Порядком конечной группы называется количество элементов этой группы.

Теорема 6 (теорема Лагранжа). Порядок конечной группы делится на порядок любой ее подгруппы.

◀ Во введенном выше отношении эквивалентности $\sim_H$ классом эквивалентности элемента a является множество aH (левый смежный класс подгруппы H по элементу a). Согласно теореме 4, все левые смежные классы образуют разбиение множества G на подмножества, равномощные в силу теоремы 5 подгруппе H.
Так как группа $\mathcal{G}$ конечна, то число элементов разбиения конечно. Обозначив это число через k, заключаем, что $|G| = k|H|$. Следовательно, порядок группы $|G|$ делится на порядок группы $|H|$. ▶

Следствия теоремы Лагранжа.

Следствие 9.3. Любая группа простого порядка является циклической.

◄ Возьмем в группе, порядок которой есть простое число, какую-то ее циклическую подгруппу, образующий элемент которой отличен от единицы (нейтрального элемента) группы.
Тогда эта подгруппа содержит не менее двух элементов и ее порядок, согласно теореме Лагранжа, должен быть делителем порядка группы.
Поскольку порядок всей группы — простое число, а порядок подгруппы не меньше 2, то он совпадет с порядком всей группы. ►

Рассмотрим моноид (группу) $(M, \cdot)$.

Подмоноид $(P, \cdot)$ (подгруппу) называют **тривиальным подмоноидом (тривиальной подгруппой)**, если **носитель** содержит только единицу исходного моноида ($P = \{\mathbf{1}\}$) или совпадает с носителем исходного моноида (группы) ($P = M$).

Группу называют **неразложимой**, если она не имеет **нетривиальных подгрупп**.

Следствие 9.4. Конечная группа неразложима тогда и только тогда, когда она является циклической группой, порядок которой есть простое число.

◄ Пусть группа циклическая и ее порядок — простое число. Согласно теореме Лагранжа, каждая ее подгруппа имеет порядок, равный либо единице, либо порядку всей группы, следовательно, группа неразложима.

Обратно. Пусть конечная группа $\mathcal{G} = (G, \cdot, \mathbf{1})$ неразложима.
Покажем, что $|G|$ — простое число.
Выберем элемент $a \neq \mathbf{1}$.
Тогда циклическая подгруппа с образующим элементом a совпадает с $\mathcal{G}$.
Допустим, что $|G|$ — составное число, т.е.

$$\exists(k, l \in \mathbb{N}, k \neq 1, l \neq 1, k \neq |G|, l \neq |G|) \mid |G| = kl$$

Тогда циклическая подгруппа с образующим элементом $b = a^k$ не совпадает с $\mathcal{G}$, так как $b^l = a^{kl} = a^{|G|} = \mathbf{1}$ и в этой подгруппе не более l элементов, что противоречит неразложимости группы $\mathcal{G}$.
Следовательно, порядок группы $\mathcal{G}$ есть простое число. ▶

Следствие 9.5. В конечной группе $\mathcal{G}$ для любого элемента $b \in G$ имеет место равенство $b^{|G|} = 1$.

◀ Если группа $\mathcal{G}$ циклическая и элемент b — ее образующий элемент, утверждение очевидно.
Если же элемент b является образующим элементом некоторой циклической подгруппы группы $\mathcal{G}$ порядка $k < |G|$, то в силу теоремы Лагранжа $|G| = kl$ для некоторого натурального l.
Отсюда получаем $b^{|G|} = b^{kl} = \left(b^k\right)^l = \mathbf{1}^l = \mathbf{1}$. ▶

Подмоноид, **носитель** которого содержит только единицу исходного моноида ($P = \{\mathbf{1}\}$), а также подмоноид, носитель которого совпадает с носителем исходного моноида ($P = M$), называют **тривиальным подмоноидом** (в частности, **тривиальной подгруппой**).

Подмоноид, не являющийся тривиальным, называют **нетривиальным подмоноидом** (в частности, **нетривиальной подгруппой**).

Подгруппоид (подполугруппу, подмоноид, подгруппу) $(G, *)$ называют **собственным подгруппоидом (подполугруппой**, **подмоноидом**, **подгруппой**) группоида (полугруппы, моноида, группы) $(K, *)$, если его носитель G есть *собственное подмножество* множества K .

С помощью теоремы Лагранжа (точнее, следствия 9.5) можно доказать, что если целое число n не делится на простое число p, то $n^{p-1}-1$ делится на p. В теории чисел это утверждение известно как **малая теорема Ферма**.

Действительно, пусть $n = rp + k$, где r — целое, а $0 < k < p$ (остаток от деления n на p). Тогда ясно, что $n^{p-1} = k^{p-1} \pmod{p}$ (достаточно разложить $(rp+k)^{p-1}$ по формуле *бинома Ньютона*). Рассмотрим группу $\mathbb{Z}_p^*$ (*мультипликативную группу вычетов по модулю* p) и в этой группе элемент k. Порядок группы $\mathbb{Z}_p^* = p - 1$. Если $k = 1$, то

$$n^{p-1} - 1 = (1^{p-1} - 1) \pmod{p} = 0 \pmod{p}$$

и утверждение очевидно. Согласно следствию 9.5, в группе $\mathbb{Z}_p^*$ справедливо равенство $k^{p-1} = 1$, т.е. $k^{p-1} = 1 \pmod{p}$, и, следовательно, $k^{p-1} - 1 = 0 \pmod{p}$, т.е. число k^{p-1} равно 1 по модулю p. Поэтому $n^{p-1} = k^{p-1} = 1 \pmod{p}$.

Малая теорема Ферма дает возможность доказывать утверждения о делимости очень больших чисел. Например, из нее следует, что при $p = 97$ число 97 является делителем $n^{96} - 1$ для любого n, не делящегося на 97. Подобного рода заключения важны при разработке алгоритмов защиты информации.

Кроме того, используя малую теорему Ферма, можно вычислять в *полях вычетов* по *модулю* p (p — простое число) элементы, обратные к заданным относительно умножения. Действительно, если $a \in \mathbb{Z}_p$, то, так как $a^{p-1} = 1$, умножая последнее равенство на a^{-1}, получим $a^{p-2} = a^{-1}$. Таким образом, для того чтобы вычислить элемент, обратный к a по умножению, достаточно возвести его в степень $p - 2$ или, что равносильно, в степень, равную остатку от деления числа $p - 2$ на порядок циклической подгруппы группы $\mathbb{Z}_p^*$, порожденной элементом a.

Пример 9.15. Рассмотрим, как вычислить элемент, обратный к a по умножению в поле $\mathbb{Z}_{17}$. Согласно полученному выше результату, для вычисления обратного к a элемента нужно найти $a^{17-2} = a^{15}$. Однако объем вычислений можно сократить, если порядок циклической подгруппы, порожденной элементом a, меньше порядка группы.

Порядок группы $\mathbb{Z}_{17}^*$ равен 16, следовательно, порядок циклической подгруппы, порожденной элементом a, может составлять, согласно теореме Лагранжа, 2, 4, 8, 16 (т.е. быть каким-то из делителей числа 16). Поэтому при поиске обратного элемента достаточно проверить следующие степени a (кроме 15-й): 1 (остаток от деления 15 на 2), 3 (остаток от деления 15 на 4) и 7 (остаток от деления 15 на 8).

Найдем элемент, обратный к 2. Очевидно, что $2^{-1} \neq 2$, так как $2 \odot_{17} 2 = 4 \neq 1$. Далее получим $2^3 = 4 \odot_{17} 2 = 8$. Поскольку $2 \odot_{17} 8 = 16 \neq 1$, то $2^3 = 8$ также не является обратным к 2. Вычислим $2^7 = 2^3 \odot_{17} 2^3 \odot_{17} 2 = 8 \odot_{17} 8 \odot_{17} 2 = 9$. Поскольку $9 \odot_{17} 2 = 1$, в итоге получаем $2^{-1} = 9$.

Найдем элемент, обратный к 14. Так как $14 \odot_{17} 14 = 9$, то $14^{-1} \neq 14$. Вычисляем $14^3 = 14 \odot_{17} 9 = 7$, но $14 \odot_{17} 7 = 13$, т.е. $14^3 \neq 14^{-1}$. Далее,

$$\begin{aligned} &14^7 = 14^3 \odot_{17} 14^4 = 7 \odot_{17} 13 = 6, \\ &14 \odot_{17} 6 = 16 = -1. \end{aligned}$$

Мы видим, что и $14^7 \neq 14^{-1}$. Следовательно, остается вычислить $14^{-1} = 14^{15}$. Однако в этом случае вычисления можно сократить, заметив, что $14 \odot_{17} 14^7 = 14 \odot_{17} 6 = -1$. Из последнего равенства получим

$$1 = 14 \odot_{17} (-6) = 14 \odot_{17} 11,$$

откуда $14^{-1} = 11$.
Отметим, что $14^{16} = 1$, т.е. порядок циклической подгруппы, порожденной элементом 14, совпадает с порядком всей группы $\mathbb{Z}_{17}^*$, и, следовательно, эта группа является циклической, порожденной элементом 14 (хотя и не только им).