Глава 15

Группы

15.1. Алгебраическая операция

Пусть A — непустое множество. Отображение

$$\circ : \ A^r \to A,$$

называется *r-арной алгебраической операцией на множестве A* (или *над A*). Таким образом, алгебраическая операция каждому упорядоченному набору $a_1, a_2, \ldots, a_r$ элементов из A ставит в соответствие элемент c из A, который обозначим

$$\circ\,(a_1, a_2, \ldots, a_r). \tag{15.1}$$

Элементы $a_1, a_2, \ldots, a_r$ называются *операндами* или *аргументами*, а $c = \circ\,(a_1, a_2, \ldots, a_r)$ — *результатом* операции. Число r называется *арностью* операции. Если $r = 1$, то операция называется *унарной* или *одноместной*. В этом случае скобки в (15.1) часто опускают. Если $r = 2$, то операция называется *бинарной* или *двуместной*. Если $r = 3$, то операция называется *тернарной* или *трехместной*.

В конкретных случаях операции имеют специальные названия и обозначения, например, сложение «$+$», умножение «$\cdot$», операция обращения «$^{-1}$» и т. п. Для обозначения результата бинарной операции вместо *префиксной* формы записи (15.1) часто используют *инфиксную* форму, помещая символ операции между операндами: $a \circ b$. Иногда используется *постфиксная* форма записи, когда символ операции следует за операндами. Например, a^{-1} — результат применения унарной операции «$^{-1}$» к элементу a.

Бинарная операция $\circ$ называется *ассоциативной*, если для любых a, b, c из A

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Скобки, как всегда, указывают на порядок выполнения операций. Бинарная операция $\circ$ называется *коммутативной*, если для любых a, b из A

$$a \circ b = b \circ a.$$

Элемент e из A называется *нейтральным* относительно бинарной операции $\circ$, если для любого a из A

$$a \circ e = e \circ a = a.$$

Элемент b из A называется *симметричным* к a относительно бинарной операции $\circ$, если

$$a \circ b = b \circ a = e.$$

Иногда полезно рассмотрение 0-арных алгебраических операций, т. е. операций с арностью 0. Такая операция не имеет операндов и поэтому ее результат — фиксированный элемент множества A. Чтобы не иметь дела с «непривычными» отображениями $A^0 \to A$, можно считать, что 0-арная операция на самом деле имеет арность $r > 0$, например, 1, но ее единственный операнд *фиктивен*, т. е. результат не зависит от его значения. С помощью 0-арной операции можно зафиксировать некоторые выделенные элементы алгебры, например, нейтральный относительно другой операции.

Если $B \subseteq A$ и для любых $a_1, a_2, \ldots, a_r$ из B элемент $\circ\,(a_1, a_2, \ldots, a_r)$ также принадлежит B, то говорят, что B *замкнуто относительно операции* $\circ$. Очевидно, A замкнуто относительно любой алгебраической операции, заданной над A.

Пример 15.1. Рассмотрим любое числовое кольцо K. Сложение, вычитание и умножение, очевидно, являются алгебраическими бинарными операциями над K. Переход от a к противоположному элементу $-a$, является алгебраической унарной операцией над K.

Пусть F — произвольное числовое поле, а F^* — множество его ненулевых элементов. Операции умножения и деления, очевидно, являются алгебраическими бинарными операциями на множестве F^*. Операция обращения, числу a ставящая в соответствие a^{-1}, является алгебраической унарной операцией над F^*.

На множестве $K^{n\times n}$ квадратных матриц заданного порядка n с элементами из некоторого числового кольца K матричные сложение, вычитание и умножение являются алгебраическими бинарными операциями, а операция нахождения противоположной матрицы является алгебраической унарной операцией.

Аналогично для множества многочленов $K[x]$ с элементами из некоторого числового кольца K. На нем сложение, вычитание и умножение являются алгебраическими бинарными операциями, а операция нахождения противоположного многочлена — алгебраической унарной операцией.

Пусть V — линейное пространство над полем F. Сложение векторов является алгебраической бинарной операцией над V. Операция нахождения противоположного вектора является алгебраической унарной операцией над V. Умножение вектора на скаляр нельзя рассматривать как бинарную операцию на V (конечно, если только $V \neq F$), так как оно есть отображение $F \times V \to V$, а не $V \times V \to V$. Однако умножение на *фиксированный* скаляр α можно рассмотреть как унарную алгебраическую операцию, вектору a ставящую в соответствие вектор αa. Скалярное произведение векторов евклидова или унитарного пространства V алгебраической операцией не является (если $V \neq F$), так как оно каждой паре векторов ставит в соответствие число, а не вектор.

На множестве $\mathbf{V}_3$ радиус-векторов сложение и векторное произведение являются алгебраическими бинарными операциями. Двойное векторное произведение является алгебраической тернарной операцией. Ни скалярное, ни смешанное произведения алгебраическими операциями не являются.

Непустое множество A с одной бинарной операцией называется *группоидом*. Группоид с ассоциативной операцией называется *полугруппой*. Если операция к тому же коммутативна, то полугруппа называется *коммутативной полугруппой*.

Пример 15.2. Примеры коммутативных полугрупп: $\mathbb{N}$ относительно сложения, $\mathbb{N}$ относительно умножения, $\mathbb{Z}$ относительно сложения, $\mathbb{Z}$ относительно умножения, $\mathbb{Z}_-$ (множество отрицательных целых чисел) относительно сложения.

Полугруппами *не* являются, например, $\mathbb{N}$ относительно вычитания (не алгебраическая операция), $\mathbb{N}$ относительно деления (не алгебраическая операция), $\mathbb{Z}$ относительно вычитания (отсутствие ассоциативности), $\mathbb{Z}$ относительно деления (не алгебраическая операция).

Пример 15.3. Приведем пример некоммутативной полугруппы. Пусть X — некоторое множество. Рассмотрим множество Φ_X всех отображений $X \to X$. Определим операцию *умножения* отображений (также используются названия «*композиция*» и «*суперпозиция*» отображений). Пусть $\varphi \in \Phi_X$, $\psi \in \Phi_X$. Под произведением отображений φ и ψ понимается отображение, обозначаемое $\varphi\psi$ и определенное по следующей формуле:

$$(\varphi\,\psi)\,x = \varphi\,(\psi x) \tag{15.2}$$

для любого $x \in X$. Таким образом, отображение $\varphi\psi$ получается в результате последовательного применения сначала отображения ψ, а затем — отображения φ. Обратите внимание, что, таким образом, результирующее преобразование вычисляется «справа налево». Очевидно, что операция умножения является алгебраической на множестве Φ_X. Так как для любого $x \in X$

$$\big(\varphi(\psi\vartheta)\big)x = \varphi\big((\psi\vartheta)x\big) = \varphi\big(\psi(\vartheta x)\big) = (\varphi\psi)(\vartheta x) = \big((\varphi\psi)\vartheta\big)x,$$

то $\varphi\,(\psi\,\vartheta) = (\varphi\,\psi)\,\vartheta$, следовательно, эта операция ассоциативна, поэтому Φ_X — полугруппа. При $|X| \geq 2$, эта полугруппа некоммутативная.

Пусть $X = \{x_1, x_2, \ldots, x_n\}$ конечно. Тогда отображение φ удобно задавать в виде таблицы

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \varphi x_1 & \varphi x_2 & \ldots & \varphi x_n \end{pmatrix}.$$

Пример 15.4. Пусть $X = \{1, 2\}$. Построим множество Φ_X. Всего имеется 4 отображения:

$$\varepsilon = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Вычислим, например, произведения[1]:

$$ab = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ \downarrow & \downarrow \\ 1 & 1 \\ \downarrow & \downarrow \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = c,$$

$$ba = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ \downarrow & \downarrow \\ 2 & 1 \\ \downarrow & \downarrow \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = b.$$

Обратите внимание, что $ab \neq ba$, значит полугруппа некоммутативная. В следующей таблице (*таблице умножения* или *таблицы Кэли*) сведены воедино результаты применения операции умножения к каждой паре элементов из Φ_X. Результат операции, примененной, например, к элементам a и b, нужно найти на пересечении строки с меткой a (первый операнд) и столбца с меткой b (второй операнд). Проверьте правильность таблицы.

	ε	a	b	c
ε	ε	a	b	c
a	a	ε	c	b
b	b	b	b	b
c	c	c	c	c

Пример 15.5. Рассмотрим множество линейных функций $\varphi : \mathbb{R} \to \mathbb{R}$, т. е. отображений вида $\varphi x = ax + b$, где a, b — произвольные числа из $\mathbb{R}$. Легко видеть, что это множество образует подполугруппу в $\Phi_{\mathbb{R}}$.

Пусть M — группоид относительно операции $\circ$. Элемент $e' \in M$ называется *левым нейтральным*, если для любого $a \in M$

$$e' \circ a = a.$$

Элемент $e'' \in M$ называется *правым нейтральным*, если для любого $a \in M$

$$a \circ e'' = a.$$

Элемент $e \in M$ называется (*двусторонним*) *нейтральным*, если он одновременно и левый нейтральный, и правый нейтральный.

[1] Вычисления далее следует не путать с матричными произведениями.

Утверждение 15.6. *Если группоид M обладает левым нейтральным элементом e_1 и правым нейтральным элементом e_2, то $e = e_1 = e_2$ — двусторонний нейтральный элемент и других нейтральных (ни левых, ни правых, ни двусторонних) в группоиде нет.*

Доказательство. Пусть e_1 и e_2 — нейтральные элементы в M. Тогда

$$e_1 = e_1 \circ e_2 = e_2,$$

т. е. $e_1 = e_2$ ∎

Следствие 15.7. *Если в группоиде есть два разных левых нейтральных элемента, то нет правого нейтрального. И, наоборот, если в группоиде есть два разных правых нейтральных элемента, то нет левого нейтрального.*

Пусть группоид M содержит нейтральный элемент e. Элемент $b' \in M$ называется *левым симметричным* к $a \in M$, если $b' \circ a = e$. Элемент $b'' \in M$ называется *правым симметричным* к $a \in M$, если $a \circ b'' = e$. Элемент $b \in M$ называется (*двусторонним*) *симметричным* к $a \in M$, если b является одновременно левым симметричным и правым симметричным к a.

Утверждение 15.8. *Пусть полугруппа M содержит нейтральный элемент e. Если элемент a имеет левый симметричный элемент b' и правый симметричный элемент b'', то $b' = b''$ — двусторонний симметричный к a элемент и других симметричных к a (ни левых, ни правых, ни двусторонних) в M нет.*

Доказательство. Имеем

$$b' = b' \circ e = b' \circ (a \circ b'') = (b' \circ a) \circ b'' = e \circ b'' = b'',$$

т. е. $b' = b''$ — двусторонний симметричный к a элемент. Если бы нашелся еще один, скажем, левый, симметричный к a элемент b, то аналогично получаем, что $b = b''$. ∎

Упражнение 15.9. В полугруппах $\mathbb{N}$ с операцией $+$, $\mathbb{N}$ с операцией $\times$, $\mathbb{Z}$ с операцией $+$, $\mathbb{Z}$ с операцией $\times$ и полугруппе Φ_X из примера 15.4 найти все нейтральные элементы (левые/правые/двусторонние), и для каждого элемента указать (если есть) симметричный (левый/правый/двусторонний).

15.2. Группа

Полугруппа G с нейтральным элементом, в которой для каждого элемента существует симметричный, называется *группой*. Если операция $\circ$ коммутативна, то группа называется *коммутативной* или *абелевой*. Можно считать, что вместе с операцией $\circ$ в группе определены тесно связанные с ней нульарная операция нахождения нейтрального элемента и унарная операция обращения (нахождения симметричного элементы к заданному). Сама операция $\circ$ в группе G называется *групповой*.

Согласно утверждению 15.6 нейтральный элемент группы единственен. Согласно утверждению 15.8 для любого элемента группы симметричный элемент единственен.

Если групповая операция называется сложением (и обозначается $+$), то группа называется *аддитивной*. В этом случае нейтральный элемент называют *нулем* (или *нулевым элементом*) и обозначают 0. Элемент b, симметричный к a, называют *противоположным* и обозначают $-a$. Если групповая операция называется умножением (и обозначается $\times$ или $\cdot$), то группа называется *мультипликативной*. В этом случае нейтральный элемент называют *единицей*

(или *единичным элементом*) и обозначают e или 1. Элемент b, симметричный к a, называют *обратным* и обозначают a^{-1}. Часто значок операции в мультипликативных группах опускается, т. е. вместо $a \cdot b$ или $a \times b$ пишут ab.

Обратим внимание, что термины «аддитивный», «мультипликативный» говорят не о каких-то дополнительных свойствах групповой операции, а только о способе ее обозначения и названии. Пожалуй, единственным исключением является следующее: сложением называют всегда коммутативную операцию, поэтому аддитивные группы абелевы.

Далее, говоря об абстрактных группах мы будем использовать мультипликативные обозначения, а именно, групповую операцию будем называть умножением и обозначать $\cdot$ (а чаще опускать значок операции), нейтральный элемент будем называть единичным и обозначать e, симметричный к a элемент называть обратным и обозначать a^{-1}. Рассматривая конкретные примеры групп, мы разумеется будем оставлять принятые для этих групп обозначения[2].

Пример 15.10. Примеры абелевых групп:

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ относительно сложения;
2) $\mathbb{Q}^*$, $\mathbb{R}^*$ относительно умножения, где через F^* обозначено множество ненулевых элементов поля F;
3) множество $K^{m\times n}$ всех матриц размера $m \times n$ с элементами из кольца K;
4) $\mathbf{V}_2$, $\mathbf{V}_3$ относительно сложения;
5) если V — линейное пространство, то V образует группу относительно сложения.

Пример 15.11. Группами не являются, например, $\mathbb{N}$ относительно сложения, $\mathbb{Z}$ относительно вычитания, Φ_X при $|X| \geq 2$.

Пример 15.12. Рассмотрим еще некоторые примеры групп. Пусть F — некоторое поле.

1) Множество всех невырожденных матриц порядка n относительно умножения образуют группу. Эта группа называется *полной линейной группой* и обозначается $\mathrm{GL}(F, n)$. При $n \geq 2$ эта группа не является абелевой.
2) Множество всех матриц порядка n с определителем, равным 1, относительно умножения образуют группу. Эта группа называется *специальной линейной группой* и обозначается $\mathrm{SL}(F, n)$. При $n \geq 2$ эта группа не является абелевой.
3) Множество всех ортогональных вещественных матриц порядка n относительно операции умножения образуют группу. Эта группа называется *полной ортогональной группой* и обозначается $\mathrm{GO}(n)$. Она является подгруппой группы вещественных матриц порядка n с определителем ± 1
4) Множество всех ортогональных матриц порядка n с определителем, равным 1, относительно операции умножения образуют группу. Эта группа называется *специальной ортогональной группой* и обозначается $\mathrm{SO}(n)$.
5) Множество всех унитарных комплексных матриц порядка n относительно умножения образуют группу. Эта группа называется *полной унитарной группой* и обозначается $\mathrm{GU}(n)$. Она является подгруппой группы комплексных матриц порядка n с определителем, по модулю равным 1.
6) Множество всех унитарных матриц порядка n с определителем, равным 1, относительно умножения образуют группу. Эта группа называется *специальной унитарной группой* и обозначается $\mathrm{SU}(n)$.
7) Множество всех ортогональных преобразований вещественного пространства размерности n образует группу, изоморфную $\mathrm{GO}(n)$.
8) Множество всех унитарных преобразований комплексного пространства размерности n образует группу, изоморфную $\mathrm{GU}(n)$.

[2]Термины «аддитивный» и «мультипликативный» применяются также к полугруппам, группоидам и т. д.

15.3. Симметрическая группа

Во множестве Φ_X всех преобразований некоторого множества X рассмотрим подмножество S_X всех биекций. Легко видеть, что операция умножения преобразований замкнута на Φ_X и ассоциативна, следовательно, S_X — полугруппа. Далее, S_X обладает нейтральным элементом: его роль выполняет тождественное преобразование ε. Для любого элемента φ в S_X существует симметричный элемент — обратное преобразование ε^{-1}. Следовательно, S_X — группа. Эта группа при $|X| \geq 3$ абелевой не является. Если $X = \{1, 2, \ldots, n\}$, то S_X называется *симметрической группой* или *группой подстановок* степени n и обозначается S_n. Порядок этой группы, очевидно, равен $n!$. Для подстановки

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

обратной, легко видеть, является

$$\varphi^{-1} = \begin{pmatrix} j_1 & j_2 & \ldots & j_n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Пример 15.13. Рассмотрим группу S_3. В ней содержится 6 подстановок:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Таблица Кэли для S_3 выглядит следующим образом:

	ε	a	b	c	d	f
ε	ε	a	b	c	d	f
a	a	ε	f	d	c	d
b	b	d	ε	f	a	c
c	c	f	d	ε	b	a
d	d	b	c	a	f	ε
f	f	c	a	b	ε	d

Подстановка

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_{k-1} & i_k & i_{k+1} & \ldots & i_n \\ i_2 & i_3 & \ldots & i_k & i_1 & i_{k+1} & \ldots & i_n \end{pmatrix} \tag{15.3}$$

называется *циклом*, причем k называется *длиной* цикла. Цикл длины 2 называется транспозицией. Кратко цикл (15.3) записывается так: $(i_1\ i_2\ \ldots\ i_{k-1}\ i_k)$. Разумеется, тот же цикл можно обозначить как $(i_2\ i_3\ \ldots\ i_k\ i_1)$ или $(i_k\ i_1\ i_2\ \ldots\ i_{k-2}\ i_{k-1})$ и т. п. Будем говорить, что этот цикл *составлен* из элементов $i_1, i_2, \ldots, i_k$). Для примера рассмотрим циклы

$$(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 \end{pmatrix},$$

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

Циклы $(i_1\ i_2\ \ldots\ i_{k-1}\ i_k)$ и $(j_1\ j_2\ \ldots\ j_{k-1}\ j_m)$ называются *независимыми*, если они составлены из разных наборов элементов, т. е. $i_p \neq j_q$ при $p \neq q$. Легко видеть, что независимые циклы коммутируют, т. е. если φ, ψ — независимые циклы, то $\varphi\psi = \psi\varphi$.

Почти очевидным является следующее

Утверждение 15.14. *Любая подстановка раскладывается в произведение независимых циклов. Такое представление единственно с точностью до порядка сомножителей.*

Пример 15.15. Разложим в произведение независимых циклов подстановку

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

Для «полноты» к произведению $(1\ 3\ 4)\,(2\ 6)$ мы можем дописать циклы длины 1: $\varphi = (1\ 3\ 4)\,(2\ 6)\,(5)\,(7)$.

Утверждение 15.16. *Любую подстановку можно представить в виде произведения транспозиций.*

Доказательство. В силу утверждения 15.14 достаточно представить в виде произведения транспозиций произвольный цикл. Легко проверить, что

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

∎

Пусть φ — подстановка. Говорят, что пара $\varphi(i)$, $\varphi(j)$, где $i < j$, образует *инверсию* в подстановке φ, если $\varphi(i) > \varphi(j)$. Обозначим $\sigma(\varphi)$ общее число инверсий в подстановке φ. Если $\sigma(\varphi)$ четно, то подстановка называется *четной*. Если $\sigma(\varphi)$ нечетно, то подстановка называется *нечетной*.

Пример 15.17. Подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 5 & 2 & 7 \end{pmatrix}$$

содержит 9 инверсий: (3, 1), (3, 2), (6, 4), (6, 1), (6, 5), (6, 2), (4, 1), (4, 2), (5, 2). Подстановка нечетная.

Подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 7 & 4 & 6 \end{pmatrix}$$

содержит 4 инверсии: (2, 1), (5, 4), (7, 4), (7, 6). Подстановка четная.

Утверждение 15.18. *Пусть $\varphi = (i\,j)\psi$, где φ, ψ — подстановки, а $(i\,j)$ — транспозиция $(i \neq j)$. Тогда четности подстановок φ, ψ различны (т. е. одна из них четная, а другая — нечетная).*

Утверждение 15.19. *Четность подстановки равна четности числа транспозиций, входящих в ее представление.*

Теорема 15.20. *Множество всех четных подстановок образуют подгруппу в S_n порядка $n!/2$ (при $n \geq 2$).*

Группа всех четных подстановок степени n называется *знакопеременной группой* и обозначается A_n.

15.4. Простейшие уравнения в группе

Простейшими уравнениями в группе называют уравнения вида

$$ax = b, \qquad ya = b,$$

где a, b — заданные элементы группы G, x, y — неизвестные элементы группы G.

Утверждение 15.21. *В группе G каждое из уравнений $ax = b$, $ya = b$ имеет, причем единственное, решение.*

Доказательство. Рассмотрим уравнение $ax = b$. Положим $x = a^{-1}b$. Проверим, что x является решением:

$$ax = a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Для доказательства единственности решения, предположим, что нашлось два решения: x и x'. Тогда $ax = b$, $ax' = b$, откуда

$$ax = ax'.$$

Умножая слева обе части этого тождества на a^{-1}, получаем

$$a^{-1}(ax) = a^{-1}(ax'),$$

пользуясь ассоциативностью, получаем

$$(a^{-1}a)x = (a^{-1}a)x',$$

откуда $ex = ex'$, т. е. $x = x'$.

Используя аналогичные рассуждения, легко проверить, что единственным решением уравнения $ya = b$ является $y = ba^{-1}$. ∎

Операция $\backslash$, определяемая формулой $a\backslash b = a^{-1}b$ называется *левым делением* (b *слева* делится на a). Операция $/$, определяемая формулой $b/a = ba^{-1}$ называется *правым делением* (b *справа* делится на a). Если группа G абелева, то это одна и та же операция (называемая просто *делением*).

Теорема 15.22. *Если в полугруппе G для любых a и b из G каждое из уравнений $ax = b$, $ya = b$ имеет решение, то G — группа.*

Доказательство. Докажем, что в условиях теоремы в G найдется единица и для любого элемента существует обратный.

Возьмем произвольный $a \in G$. Рассмотрим уравнение $ax = a$. Пусть x — некоторое его решение. Докажем, что x является правым единичным (нейтральным) элементом в G. Действительно, для любого $b \in G$ по условию теоремы найдется решение y уравнения $ya = b$, тогда

$$bx = (ya)x = y(ax) = ya = b,$$

т. е. x — правый единичный элемент. Аналогично доказывается, что в G найдется левый единичный. Следовательно, согласно утверждению 15.6 в G есть (двусторонний) единичный элемент e.

Теперь докажем, что для любого элемента a в G найдется обратный. Для этого рассмотрим уравнения $ax = e$ и $ya = e$. Решением x первого уравнения является правый обратный к a. Решением y второго уравнения является левый обратный к a. По утверждению 15.8 $x = y$ есть (единственный) обратный к a элемент. ∎

Теорема 15.23. *Если полугруппа G конечна и для любых a, b из G каждое из уравнений $ax = b$, $ya = b$ имеет не более одного решения, то G — группа.*

Доказательство. Пусть

$$G = \{a_1, a_2, \ldots, a_n\}.$$

Рассмотрим произвольный элемент $a = a_k$ из G. Умножая каждый элемент группы G на a, получаем

$$aG = \{aa_1, aa_2, \ldots, aa_n\},$$

причем при $i \neq j$ имеем $aa_i \neq aa_j$. Действительно, в противном случае мы получили бы, что уравнение $ax = b$, где $b = aa_i = aa_j$, имеет по крайней мере два решения: a_i и a_j. Таким образом, все элементы в списке $aa_1, aa_2, \ldots, aa_n$ попарно различны. Итак, $|G| = |aG| = n$ и $aG \subseteq G$, поэтому $aG = G$.

Покажем теперь, что из равенства $aG = G$ следует, что для любого b из G уравнение $ax = b$ имеет решение. Действительно, для некоторого i имеем $aa_i = b$, т. е. $x = a_i$ есть решение уравнения $ax = b$.

Аналогично показываем, что для любых a, b из G уравнение $ya = b$ имеет решение.

По теореме 15.22 получаем, что G — группа. ∎

Свойство, заключающееся в том, что для любых a, b из G каждое из уравнений $ax = b$, $ya = b$ имеет не более одного решения, означает возможность *сокращения* (слева и справа соответственно), т. е. означает, что

- из $ax = ax'$ следует $x = x'$ (сокращение слева);
- из $xa = x'a$ следует $x = x'$ (сокращение справа).

Таким образом, теорему 15.23 можно переформулировать следующим образом:

Следствие 15.24. *Конечная полугруппа с сокращением есть группа.*

Условие конечности полугруппы в теореме 15.23 и следствии 15.24 является существенным. Действительно, рассмотрим, например, полугруппу $\mathbb{N}$ относительно операции умножения (или сложения). Это полугруппа с сокращением, однако она не является группой.

Из теоремы 15.23 вытекает следующее свойство таблиц Кэли для конечной группы.

Следствие 15.25. *Для конечной группы все элементы любой строки ее таблицы Кэли различны. Аналогичное утверждение верно и для столбцов таблицы.*

Пример 15.26. Построим все неизоморфные группы 4-го порядка. Пусть $G = \{e, a, b, c\}$, причем e — единица. Сделаем заготовку таблицы Кэли и начнем ее заполнять, пользуясь свойством из следствия 15.25. Первые строка и столбец заполняются очевидным образом:

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

В клетке $(2,2)$ может стоять e, b, c, но не a, так как a уже встречается во второй строке (и во втором столбце). Вначале попробуем там разместить e. Чтобы показать произвольность этого выбора, подчеркнем ее:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$		
b	b			
c	c			

Теперь посмотрим, что можно разместить в клетке $(2,3)$. Там не могут стоять a и e (они уже есть во второй строке), и не может стоять b (он уже есть в третьем столбце). Приходим к выводу, что там может быть только c:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	
b	b			
c	c			

Теперь приходим к выводу, что в клетке $(2,4)$ может стоять только b:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	b
b	b			
c	c			

Аналогично заполняется второй столбец:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	b
b	b	c		
c	c	b		

В клетку $(3,3)$ можно поместить e или a (но не b и не c). Вначале попробуем e, причем ввиду произвольности этого выбора опять подчеркнем букву:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	b
b	b	c	$\underline{e}$	
c	c	b		

Оставшиеся клетки $(3,4)$, $(4,3)$ и $(4,4)$ заполняются однозначно:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	b
b	b	c	$\underline{e}$	a
c	c	b	a	e

(15.4)

Мы получили одну из таблиц Кэли. Операция получилась коммутативной, однако ассоциативность нужно как-то доказывать. Если основываться только на определении, потребовалось бы перебрать все упорядоченные тройки из четырех элементов, которых $4^3 = 256$ вариантов (коммутативность уменьшает число вариантов в два раза).

Вместо этого построим группу подстановок, изоморфную данной алгебраической системе. Положим

$$\varphi e = \varepsilon, \quad \varphi a = (1\,2)(3\,4), \quad \varphi b = (1\,3)(2\,4), \quad \varphi c = (1\,4)(2\,3).$$

Перемножая эти подстановки по обычным правилам, мы воспроизведем нашу таблицу Кэли. Умножение подстановок ассоциативно, тем самым доказана ассоциативность операции, заданной таблицей 15.4. То, что мы построили именно группу (это четверная группа Клейна), теперь следует из теоремы 15.22.

Итак, мы построили одну группу 4-го порядка. Чтобы получить другие, применим метод перебора с возвратом. Последний произвольный выбор был сделан для клетки $(3,3)$, изменим его и вместо e поместим в эту клетку a (теперь уже выбор однозначен). Клетки $(3,4)$, $(4,3)$ и $(4,4)$ заполним по-новому (также однозначно). Получим новую таблицу:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{e}$	c	b
b	b	c	a	e
c	c	b	e	a

(15.5)

Построим группу подстановок, изоморфную данной алгебраической системе. Положим

$$\varphi e = \varepsilon, \quad \varphi a = (1\,2)(3\,4), \quad \varphi b = (1\,3\,2\,4), \quad \varphi c = (1\,4\,2\,3).$$

Вспомним условие задачи: группы должны быть неизоморфными. Рассмотрим квадраты элементов новой группы. Имеем $e^2 = e$, $a^2 = e$, но $b^2 = a \neq e$, $c^2 = a \neq e$. В группе Клейна, построенной раньше, квадраты всех элементов были равны e. Ясно, что группы неизоморфны.

Также обратим внимание, что группа, определяемая таблицей 15.5 циклическая: все ее элементы являются степенью одного элемента, называемого порождающим. В качестве порождающего можно взять b или c. Например, для b: $b = b^1$, $a = b^2$, $c = b^3$, $e = b^4 = b^0$.

Вернемся к клетке $(2,2)$. Вместо e в нее можно поместить b. Этот выбор опять произволен, поэтому букву подчеркнем. Заполнение остальных клеток второй строки и второго столбца однозначно. В клетку $(3,3)$ можно поместить только e, так как если туда поместить a, то в клетку $(3,4)$ придется поместить e, что недопустимо. Мы получили еще одну таблицу Кэли:

	e	a	b	c
e	e	a	b	c
a	a	$\underline{b}$	c	e
b	b	c	e	a
c	c	e	a	b

(15.6)

На самом деле, группы, представленные таблицами 15.5 и 15.6 изоморфны. Изоморфизм следует из того, что обе группы циклические. Можно задать его явно (предполагается, что φ — отображение первой группы на вторую):

$$\varphi e = e, \quad \varphi a = b, \quad \varphi b = a, \quad \varphi c = c.$$

Еще одна (последняя) таблица получается, если мы поставим в клетку $(2,2)$ элемент c и далее заполним всю таблицу:

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	a	c
c	c	b	c	e

(15.7)

Построенная группа также изморфна группам, представленным таблицами 15.5 и 15.6. Поэтому делаем вывод: поставленная задача решена, неизоморфных групп 4-го порядка существует всего две: одна группа Клейна, другая — циклическая.

15.5. Подгруппа

Подмножество M группы G называется *подгруппой* группы G, если оно само является группой относительно той же групповой операции[3]. Легко видеть, что любая группа G обладает по карйней мере двумя, тривиальными, подгруппами: единичной подгуппой $\{e\}$ и подгруппой G.

Теорема 15.27 (Критерии подгруппы)**.** *Пусть G — группа, $M \subset G$, $M \neq \emptyset$. Для того, чтобы M являлось подгруппой необходимо и достаточно, чтобы выполнялось любое из следующих 3 эквивалентных условий:*

1) *для любых $a, b \in M$ выполнено $ab \in M$ (замкнутость относительно групповой операции), $a^{-1} \in M$ (замкнутость относительно операции обращения);*

2) *для любых $a, b \in M$ выполнено $a/b \in M$ (замкнутость относительно правого деления);*

3) *для любых $a, b \in M$ выполнено $a\backslash b \in M$ (замкнутость относительно левого деления).*

Если M конечно, то чтобы M являлось подгруппой необходимо и достаточно, чтобы

4) *для любых $a, b \in M$ выполнено $ab \in M$, $a^{-1} \in M$.*

Доказательство. Необходимость всех условий (т. е. необходимость замкнутости относительно указанных операций) очевидна. Поэтому докажем достаточность.

1) M замкнуто относительно групповой операции и операции обращения. Остается проверить, что $e \in M$. Действительно, e можно представить как $e = aa^{-1}$, для любого $a \in M$ (такой a существует, так как $M \neq \emptyset$). Но в силу замкнутости относительно групповой операции и операции обращения $aa^{-1} \in M$, т. е. $e \in M$.

2) Для любого a имеем $e = a/a \in M$. Далее, $a^{-1} = e/a \in M$.

3) Доказывается аналогично п. 2).

4) По утверждению 15.21 каждое из уравнений $ax = b$ и $ya = b$, где a, b — произвольные элементы из M, имеет в G единственное решение[4]. Так как $M \subseteq G$ каждое из этих уравнений имеет в M не более одного решения. По теореме 15.23 получаем, что M — группа.

∎

[3] С формальной точки зрения данное определение не совсем корректно и требует уточнения. Дело в том, что r-арная алгебраическая операция $\circ$ в G не является алгебраической для $M \subset G$: операция $\circ$ есть отображение из G^r в G, а не из M^r в M. Пусть G — группа относительно операции $\circ$: $G \times G \to G$. Пусть $M \subseteq G$ и $M \neq \emptyset$. Рассмотрим *сужение* $\circ_M$ операции $\circ$ на множество M. Сужение $\circ_M$ определено формулой $a \circ_M b = a \circ b$ для всех a и b из M. Тогда M называется *подгруппой* группы G, если M является группой относительно $\circ_M$.

[4] Т. е. для любых a, b из M найдутся единственные x и y из G, такие, что $ax = b$ и $ya = b$.

15.6. Теорема Кэли

Симметрическая группа S_n играет важную роль в теории конечных групп. Дело в том, что подгруппами групп S_n исчерпываются все (с точностью до изоморфизма) конечные группы.

Теорема 15.28 (Кэли)**.** *Для любой группы G порядка n существует подгруппа M группы S_n, изоморфная G.*

Доказательство. Пусть $G = \{a_1, a_2, \ldots, a_n\}$. Для удобства вместо S_n возьмем $S(G)$. Рассмотрим отображение $\varphi:\ G \to S(G)$, заданное формулой

$$\varphi a_j = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_j a_1 & a_j a_2 & \ldots & a_j a_n \end{pmatrix}.$$

Легко проверить, что $\varphi(a_j a_i) = \varphi a_j \cdot \varphi a_i$. Таким образом, φ — гомоморфизм из G в $S(G)$. Его полный образ φG является подгруппой в $S(G)$. Для завершения доказательства теоремы осталось положить $M = S(G)$. ∎

Пример 15.29. Для группы G 3-го порядка, заданной таблицей Кэли

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

,

построим в $S(G)$ подгруппу, изоморфную G.

$$\varphi e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}, \qquad \varphi a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}, \qquad \varphi b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}.$$

Обратите внимание, что нижние строки записанных здесь подстановок — это соответствующие строки таблицы Кэли. Заменяя $e \mapsto 1$, $a \mapsto 2$, $b \mapsto 3$, получаем

$$\varphi e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon, \qquad \varphi a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3), \qquad \varphi b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2).$$

Обобщение теоремы Кэли справедливо и для бесконечных групп:

Теорема 15.30. *Для любой (не обязательно конечной) группы G существует подгруппа M группы $S(G)$, изоморфная G.*

15.7. Циклические группы

Пусть A — некоторое непустое подмножество элементов группы G. *Подгруппой, порожденной множеством A*, называется минимальная (по включению) подгруппа H, содержащая A, т. е. такая подгруппа H, содержащая A, что любая подгруппа, содержащая A, содержит также H.

Теорема 15.31. *Подгруппа H группы G, порожденная множеством A, существует и единственна. Более того,*

1) *H есть пересечение (возможно бесконечное) всех подгрупп в G, содержащих A;*

2) *H состоит из всех произведений вида $a_1 a_2 \dots a_t$ из произвольного конечного числа t множителей, где $a_i \in A$ или $a_i^{-1} \in A$ $(i = 1, 2, \dots, t)$; в частности, подгруппа (a), порождаемая одним элементом a, содержит все степени a^k, где $k \in \mathbb{Z}$.*

Подгруппа H, порожденная множеством A, обозначается (A). Множество A называется *образующим* или *порождающим* для подгруппы H. Если $A = \{a_1, a_2, \dots, a_m\}$, то подгруппа (A) обозначается $(a_1, \dots, a_m)$. *Порядком* $|a|$ элемента a называется порядок порождаемой этим элементом подгруппы (a).

Из теоремы следует

Утверждение 15.32. *Порядок элемента a группы G равен минимальному натуральному n, при котором $a^n = e$.*

Если $G = (a)$, то группа G называется *циклической*.

Из теоремы 15.7 получаем, что (a) состоит из всех степеней элемента a:

$$(a) = \left\{\dots, a^{-2}, a^{-1}, e = a^0, a, a^2, a^3, \dots\right\}.$$

Такая запись, разумеется, не означает, что (a) содержит бесконечное множество элементов: в этом «бесконечном перечне» элементы могут повторяться. Легко проверить, что для любых целых k и l

$$a^k a^l = a^{k+l}, \qquad (a^k)^l = a^{kl},$$

откуда, в частности, имеем $a^k a^l = a^l a^k$, т. е. циклическая группа абелева. Отсюда, например, следует, что симметрическая группа S_n при $n \geq 3$ не циклическая, так как не является абелевой.

Пример 15.33. Примеры циклических групп:

1) аддитивная группа целых чисел $\mathbb{Z}$; порождающие элементы: 1 и -1;

2) мультипликативная группа U_n корней n-й степени из единицы.

Утверждение 15.34. *Любая циклическая группа изомофна аддитивной группе целых чисел $\mathbb{Z}$, или мультипликативной группе U_n корней n-й степени из единицы.*

Доказательство. Рассмотрим циклическую группу (a). Рассмотрим каждый из двух взаимоисключающих случаев:

1) $a^k \neq a^l$ для всех целых k, l, таких, что $k \neq l$;

2) найдутся целые k, l, такие, что $k \neq l$, $a^k = a^l$.

В первом случае докажем, что (a) изоморфна аддитивной группе целых чисел. Действительно, изоморфизм φ легко определяется следующим правилом: $\varphi(a^k) = k$.

Во втором случае докажем, что (a) изоморфна мультипликативной группе U_n, где $n = \min\{m > 0 : a^m = e\}$. Вначале проверим, что множество $M = \{m > 0 : a^m = e\}$ не пусто. Действительно, по условию имеем $a^k = a^l$ для некоторых неравных k и l. Для определенности положим $k > l$ и обозначим $m = k - l > 0$. Из равенства $a^k = a^l$ следует $a^m = a^{k-l} = e$, т. е. $m \in M$, значит, $M \neq \emptyset$.

Теперь покажем, что $(a) = \{e = a^0, a, a^2, \ldots, a^{n-1}\}$ Рассмотрим a^m для любого целого m. Поделим m на n с остатком. Получаем $m = qn + r$, где $0 \leq r \leq n-1$. Откуда $a^m = a^{qn+r} = (a^n)^q a^r = e\, a^r = a^r$. Итак, a^m совпадает с одним из элементов $e, a, a^2, \ldots, a^{n-1}$.

Теперь покажем что среди элементов $e, a, a^2, \ldots, a^{n-1}$ нет двух одинаковых. Действительно, если $a^k = a^l$, где $k > l$, то $a^{k-l} = e$, что противоречит минимальности m.

Изоморфизм φ группы (a) мультипликативной группе U_n задается формулой

$$\varphi a^k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n},$$

что проверяется непосредственно. ∎

Утверждение 15.35. *Любая подгруппа циклической группы — циклическая.*

Доказательство. Пусть H — подгруппа группы $G = (a)$. Утверждение тривиально, когда $H = \{e\}$. В противном случае множество $M = \{m > 0 :\ a^m \in H\}$ не пусто, и, следовательно, существует $m = \min M$.

Докажем, что $H = (a^m)$. Включение $(a^m) \subseteq H$ очевидно. Докажем обратное включение. Пусть $a^l \in H$. Разделим l с остатком на m. Получаем $l = qm + r$, где $0 \leq r \leq m-1$. Докажем, что $r = 0$. Действительно, $a^r = a^{l-qm} = a^l\,(a^m)^{-q} \in H$ и условие $r > 0$ противоречило бы минимальности m. Итак, $r = 0$, откуда $a^l = a^{qm} = (a^m)^q \in H$. ∎

Утверждение 15.36. *Для любых $k, n \in \mathbb{Z}$ существуют $u, v \in \mathbb{Z}$, такие, что $uk + vn = \delta$, где $\delta = \text{НОД}(k, n)$.*

Доказательство. В аддитивной группе $\mathbb{Z}$ рассмотрим подгруппу $H = \{uk + vn :\ u, n \in \mathbb{Z}\}$, порожденную элементами k, n. Согласно утверждению 15.35 эта подгруппа циклическая. Обозначим через δ порождающий элемент этой подгруппы. Докажем, что $\delta = \text{НОД}(k, n)$, что приводит к требуемому.

Так как δ — порождающий элемент подгруппы H, то $k \vdots \delta$, $n \vdots \delta$, т. е. δ — общий делитель k и n. С другой стороны, так как $\delta \in H$, то найдутся целые u, v, такие, что $uk + vn = \delta$. Из этого равенства получаем, что если d — какой-то общий делитель k и n, то он будет делителем и для δ. Таким образом, $\delta = \text{НОД}(k, n)$. ∎

Утверждение 15.37. *Пусть $G = (a)$, $|G| = n$, $k \in \mathbb{Z}$, $\delta = \text{НОД}(n, k)$, тогда $(a^k) = (a^\delta)$ и $|a^k| = |a^\delta| = n/\delta$. В частности, $G = (a^k)$ тогда и только тогда, когда $\text{НОД}(n, k) = 1$.*

Доказательство. Обозначим $\delta = \text{НОД}(n, k)$. Пусть $k = \delta k'$, $n = \delta n'$ и $uk + vn = \delta$.

Вначале покажем, что $(a^k) = (a^\delta)$. Так как $a^k = (a^\delta)^{k'} \in (a^\delta)$, то $(a^k) \subseteq (a^\delta)$. С другой стороны, $a^\delta = a^{uk+vn} = (a^k)^u (a^n)^v = (a^k)^u \in (a^k)$, откуда $(a^\delta) \subseteq (a^k)$.

Итак, $(a^k) = (a^\delta)$, однако легко видеть, что

$$(a^\delta) = \left\{e, a^\delta, a^{2\delta}, \ldots, a^{(n'-1)\delta}\right\},$$

причем в правой части этого равенства нет повторяющихся элементов. Таким образом, $|a^k| = |a^\delta| = n' = n/\delta$. ∎

Утверждение 15.38. *Пусть G — циклическая группа порядка n. Для любого делителя d числа n в G существует единственная подгруппа порядка d и других подгрупп нет.*

Доказательство. По утверждению 15.35 все подгруппы группы $G = (a)$ циклические. Поэтому чтобы перебрать их все, достаточно рассмотреть каждый элемент a^k группы G и вместе с ним рассмотреть подгруппу, которую он порождает. Но по утверждению 15.37 $(a^k) = (a^\delta)$, где $\delta = \text{НОД}(n, k)$, поэтому, чтобы перебрать все подгруппы группы G, достаточно рассматривать только элементы a^δ, где δ — делитель n. ∎

Порождающий элемент группы U_n называется *примитивным* или *первообразным* корнем n-й степени из 1. В силу утверждения 15.32 можно дать следующее эквивадентное определение первообразного корня: число ω называется первообразным корнем n-й степени из 1, если $\omega^n = 1$ и $\omega^m \neq 1$ для всякого натурального $m < n$ (т. е. ω является корнем n-й степени из 1, но не является корнем из 1 никакой меньшей степени).

Пример 15.39. Циклическая группа $U_{10} = \{1, \omega, \omega^2, \ldots, \omega^9\}$, где $\omega = \cos\frac{\pi}{5} + i\sin\frac{\pi}{5}$. обладает 4 подгруппами:

$$(\omega) = (\omega^3) = (\omega^7) = (\omega^9) = U_{10};$$

$$(\omega^2) = (\omega^4) = (\omega^6) = (\omega^8) = \{1, \omega^2, \omega^4, \omega^6, \omega^8\};$$

$$(\omega^5) = \{1, \omega^5\};$$

$$(1) = \{1\}.$$

ω, ω^3, ω^7, ω^9 — первообразные корни 10-й степени из 1.

Пример 15.40. Циклическая группа $U_{12} = \{1, \omega, \omega^2, \ldots, \omega^{11}\}$, где $\omega = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6}$. обладает 6 подгруппами:

$$(\omega) = (\omega^5) = (\omega^7) = (\omega^{11}) = U_{12};$$

$$(\omega^2) = (\omega^{10}) = \{1, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{10}\};$$

$$(\omega^3) = (\omega^9) = \{1, \omega^3, \omega^6, \omega^9\};$$

$$(\omega^4) = (\omega^8) = \{1, \omega^4, \omega^8\};$$

$$(\omega^6) = \{1, \omega^6\};$$

$$(1) = \{1\}.$$

ω, ω^5, ω^7, ω^{11} — первообразные корни 12-й степени из 1.

15.8. Смежные классы

Пусть A, B — некоторые непустые подмножества группы G. Определим операцию умножения таких подмножеств по правилу «каждый с каждым»[5]:

$$A \cdot B = \{ab : \ a \in A, \ b \in B\}.$$

Легко видеть[6], что введенная операция умножения на множестве всех подмножеств группы G обладает ассоциативностью, т. е. $A(BC) = (AB)C$ для любых подмножеств A, B, C группы G. Таким образом, относительно этой операции множество $2^G \setminus \emptyset$ всех непустых подмножеств группы G образует полугруппу с единицей (в качестве единицы выступает множество $\{e\}$).

Вместо $\{a\} \cdot B$ часто будем писать aB, а вместо $A \cdot \{b\}$ будем писать Ab.

[5]Каждый элемент множества A умножается на каждый элемент множества B. Множество всех таких произведений и составляет $A \cdot B$.

[6]Введенную операция умножения следует отличать от декартового произведения $A \times B$.

Утверждение 15.41. *Если H — подгруппа группы G и $h \in H$, то*[7]

$$hH = Hh = HH = H.$$

Доказательство. Включения $hH \subseteq HH$, $Hh \subseteq HH$ тривиальны. Включение $HH \subseteq H$ следует из замкнутости подгруппы H. Включения $H \subseteq hH$, $H \subseteq Hh$ следуют из разрешимости в H уравнений $a = hx$ и $a = yh$ для любого $a \in H$. ∎

Пусть H — подгруппа в G и $a \in G$. Множество $aH = \{ah : h \in H\}$ называется *левым смежным классом по подгруппе H, порожденным элементом a*. Множество $Ha = \{ha : h \in H\}$ называется *правым смежным классом по подгруппе H, порожденным элементом a*.

Нижеследующие утверждения 15.42–15.45 будут сформулированы и доказаны для левых смежных классов, однако их нетрудно переформулировать и для правых смежных классов.

Утверждение 15.42. *Пусть H — подгруппа группы G и $a, b \in G$. Тогда $|aH| = |bH| = |H|$.*

Доказательство. Достаточно доказать, что $|aH| = |H|$. Для этого определим отображение $\varphi : H \to aH$ по формуле $\varphi h = ah$. Легко видеть, что φ — биекция. ∎

Утверждение 15.43. *Пусть H — подгруппа группы G и $a, b \in G$. Следующие условия эквивалентны:*

1) $aH = bH$;

2) $b \in aH$;

3) $a \backslash b = a^{-1}b \in H$.

Доказательство. Импликация (1) ⇒ (2) очевидна. Докажем (2) ⇒ (1). Так как $b \in aH$, то $b = ah$ для некоторого $h \in H$. Поэтому $bH = (ah)H = a(hH) = aH$.

Теперь докажем эквивалентность условий (2) и (3):

$$b \in aH \iff \exists\, h \in H : b = ah \iff \exists\, h \in H : a^{-1}b = h,$$

что завершает доказательство. ∎

Эквивалентность условий (1) и (2) в утверждении 15.43 означает, что левый смежный класс порождается любым своим представителем и только ими. Эквивалентность условий (1) и (3) дает удобный критерий совпадения двух смежных классов.

Утверждение 15.44. *Левые смежные классы по одной подгруппе либо совпадают либо не пересекаются, т. е. если H — подгруппа группы G и $a, b \in G$, то*

$$aH = bH \quad \text{или} \quad aH \cap bH = \emptyset.$$

Доказательство. Если $aH \cap bH \neq \emptyset$, то найдется $x \in aH \cap bH$, откуда следует, что существуют $h_1, h_2 \in H$, такие, что $ah_1 = bH_2$. Следовательно, $a^{-1}b = h_1 h_2^{-1} \in H$. По утверждению 15.43 $aH = bH$. ∎

[7] Вместо $H \cdot H$ или, что то же, HH мы не пишем H^2, чтобы не спутать HH с декартовым квадратом $H \times H$.

Будем говорить, что элементы a и b группы G *конгруэнтны* (по подгруппе H при разбиении G на левые смежные классы), если выполнено любое из эквивалентных условий утверждения 15.43. Согласно утверждению 15.44 введенное отношение конгруэнтности является отношением эквивалентности.

Итак, мы получили разбиение группы G на левые смежные классы:

$$G = \bigcup_{a \in G} aH, \quad \text{где} \quad aH = bH \quad \text{или} \quad aH \cap bH = \emptyset.$$

Количество различных левых смежных классов (если их множество конечно) назовем *индексом группы G по подгруппе H* и обозначим $I(G/H)$. Теперь, используя утверждение 15.42, получаем следующий важный результат.

Теорема 15.45 (Лагранж)**.** *Пусть H — подгруппа конечной группы G, тогда*

$$|G| = |H| \cdot I(G/H).$$

Следствие 15.46. *Порядок подгруппы конечной группы есть делитель прорядка группы, т. е. если H — подгруппа конечной группы G, то $|G| \vdots |H|$.*

Заметим, что если $|G| = n$, $n \vdots d$, то группа G может как содержать несколько подгрупп порядка d, так и не содержать ни одной подгруппы такого порядка. Например, четверная группа Клейна V_4 содержит 3 подгруппы порядка 2. В знакопеременной группе A_4 (ее порядок 12) нет подгрупп порядка 6. Напомним, что если G — циклическая, то, согласно утверждению 15.38, для любого делителя d числа n в G существует единственная подгруппа порядка d (и других подгрупп нет).

Следствие 15.47. *Группа простого порядка — циклическая.*

Утверждения 15.42–15.45 были сформулированы и доказаны применительно к разбиению группы на левые смежные классы, однако их нетрудно переформулировать и для правых смежных классов. Например, утверждение 15.43 нужно заменить на следующее (обратите внимание, что вместо левого деления $a\backslash b = a^{-1}b$ в условии (3) мы имеем правое деление $a/b = ab^{-1}$)

Утверждение 15.48. *Пусть H — подгруппа группы G и $a, b \in G$. Следующие условия эквивалентны:*

1) $Ha = Hb$;

2) $b \in Ha$;

3) $a/b = ab^{-1} \in H$.

Аналогично мы приходим к понятию «правого» индекса конечной группы по подгруппе. Из теоремы Лагранжа тогда следует, что эта величина совпадает с «левым» индексом:

Следствие 15.49. *Количество левых смежных классов конечной группы G по подгруппе H равно количеству правых смежных классов группы G по подгруппе H.*

Заметим, что несмотря на то, что количества левых и правых смежных классов по одной и той же подгруппе совпадают, само разбиение группы на правые смежные классы может отличаться от разбиения на левые смежные классы.

15.9. Фактор–группа

Большой интерес представляет случай, когда разбиение группы G по подгруппе H на левые смежные классы совпадает с разбиением G по H на правые смежные классы, т. е. когда

$$aH = Ha \quad \text{для любого } a \in G.$$

В этом случае подгруппу H называют *нормальной подгруппой* или *нормальным делителем* группы G. Разумеется, любая подгруппа абелевой группы является номальной.

Следующее утверждение дает удобный критерий нормальности подгруппы.

Утверждение 15.50. *Пусть H — подгруппа группы G. Следующие условия эквивалентны:*

1) *$aH = Ha$ для любого $a \in G$, т. е. H — нормальная подгруппа;*

2) *$a^{-1}Ha = H$ для любого $a \in G$;*

3) *$a^{-1}Ha \subseteq H$ для любого $a \in G$.*

Доказательство. Равносильность условий (1) и (2) очевидна. Импликация (2) $\Rightarrow$ (3) тривиальна. Докажем справедливость импликации (3) $\Rightarrow$ (2). Домножая обе части включения

$$a^{-1}Ha \subseteq H \tag{15.8}$$

на a слева и на a^{-1} справа, получаем $H \subseteq aHa^{-1}$. Так как (15.8) справедливо для любого $a \in G$, то, заменяя a на a^{-1}, получаем $aHa^{-1} \subseteq H$. Итак, $H \subseteq aHa^{-1} \subseteq H$, откуда $H = aHa^{-1}$, поэтому $aH = Ha$. ∎

Утверждение 15.51. *Пересечение нормальных делителей является нормальным делителем*

Доказательство. Использовать условие (3) из утверждения 15.50. ∎

Имея группу G и любую ее нормальную группу H, мы можем построить новую группу G/H, называемую *фактор-группой*. Множество ее элементов есть множество всех смежных классов группы G по подгруппе H (левых или, что эквивалентно в силу нормальности подгруппы H, правых). В качестве операции рассматривается умножение по правилу «каждый с каждым»:

$$aH \cdot bH = \{ah_1 \cdot bh_2 : \ h_1, h_2 \in H\}$$

или умножение «по представителям»:

$$aH \cdot bH = (ab)H. \tag{15.9}$$

Оказывается, эти правила эквивалентны. Действительно,

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H.$$

Также обратим внимание, что при умножении смежных классов получается смежный класс. Таким образом, операция умножения смежных классов введена корректно: она замкнута на множестве G/H.

Ассоциативность операции следует из ассоциативности групповой операции.

В качестве единицы выступает смежный класс H. Действительно, для любого $a \in G$, используя (15.9), получаем

$$aH \cdot H = aH \cdot eH = (ae)H = aH.$$

Обратным элементом к aH является $a^{-1}H$. Действительно, используя (15.9), получаем

$$aH \cdot a^{-1}H = (aa^{-1})H = H = (a^{-1}a)H = a^{-1}H \cdot aH.$$

15.10. Гомоморфизмы групп

Утверждение 15.52. *Пусть H — нормальная подгруппа группы G, тогда отображение $\eta : G \to G/H$, заданное формулой $\eta a = aH$, где $a \in G$, является сюръективным гомоморфизмом из G в G/H.*

Доказательство. Сюръективность отображения η очевидна. Для любых a, b из G имеем

$$\eta(ab) = (ab)H = aH \cdot bH = \eta a \cdot \eta b,$$

это доказывает, что η — гомоморфизм. ∎

Пусть $\varphi : G \to G'$ — гомоморфизм из группы G в группу G'. Ядром гомоморфизма φ называется множество всех элементов из G, отображающихся в единицу e' группы G':

$$\operatorname{Ker}\varphi = \{x \in G : \varphi x = e'\}.$$

Утверждение 15.53. *Ядро $\operatorname{Ker}\varphi$ гомоморфизма $\varphi : G \to G'$ является нормальной подгруппой группы G.*

Доказательство. Легко проверить, что $\operatorname{Ker}\varphi$ — подгруппа в G. Для любого $a \in G$ имеем

$$\varphi(a^{-1} \operatorname{Ker}\varphi\, a) = \varphi(a^{-1})\,\varphi(\operatorname{Ker}\varphi)\,\varphi(a) = \varphi(a^{-1})\,\varphi(\operatorname{Ker}\varphi)\,\varphi(a) = e',$$

откуда $a^{-1} \operatorname{Ker}\varphi\, a \subseteq \operatorname{Ker}\varphi$. Теперь из утверждения 15.50 получаем, что $\operatorname{Ker}\varphi$ — нормальный делитель. ∎

Утверждение 15.54. *Пусть $\varphi : G \to G'$ — гомоморфизм из группы G в группу G'. Тогда образ φG изоморфен фактор-группе $G/\operatorname{Ker}\varphi$:*

$$\varphi G \cong G/\operatorname{Ker}\varphi,$$

а именно отображение $\psi : G/\operatorname{Ker}\varphi \to \varphi G$, определяемое формулой $\psi(a \operatorname{Ker}\varphi) = \varphi a$, является изоморфизмом.

Доказательство. Покажем, что ψ — изоморфизм. Сначала проверим, что отображение ψ является биекцией. Действительно, для любых a, b из G

$$\varphi a = \varphi b \;\Leftrightarrow\; e' = (\varphi a)^{-1}\varphi b = \varphi(a^{-1}b) \;\Leftrightarrow\; a^{-1}b \in \operatorname{Ker}\varphi \;\Leftrightarrow\; a \operatorname{Ker}\varphi = b \operatorname{Ker}\varphi.$$

G φG

$G/\operatorname{Ker}\varphi$

Теперь докажем, что φ — гомоморфизм. Для любых a, b из G имеем

$$\psi(a \operatorname{Ker}\varphi \cdot b \operatorname{Ker}\varphi) = \psi(ab \operatorname{Ker}\varphi) = \varphi(ab) = \varphi a \cdot \varphi b = \psi(a \operatorname{Ker}\varphi) \cdot \psi(b \operatorname{Ker}\varphi),$$

что завершает доказательство. ∎