§ 3. ПОЛУГРУППЫ

В двух первых определениях группы из предыдущего параграфа участвует бинарное ассоциативное умножение. Множество с одной бинарной ассоциативной операцией называется *полугруппой*. Это не просто термин, введенный для сокращения речи,— класс полугрупп, являющийся, очевидно, многообразием, уже стал носителем богатой теории, а применения полугрупп в математике и смежных науках все умножаются.

Нужно сказать, что и логические оправдания для понятия полугруппы как предмета самостоятельного изучения могут быть приведены столь же убедительные, как и для понятия группы. Покажем это. Правда, это будет скорее относиться к *полугруппам с единицей*, которые составляют многообразие алгебр с сигнатурой, состоящей из бинарного умножения и нульарной операции, отмечающей элемент 1, причем умножение ассоциативно и, кроме того, выполняются тождества

$$x \cdot 1 = 1 \cdot x = x. \tag{1}$$

Впрочем, *любую полугруппу G добавлением одного единственного элемента* 1 *можно вложить в полугруппу с единицей*. При этом умножение, заданное в G, сохраняется, а произведение, хотя бы один из сомножителей которого есть 1, определяется в соответствии с (1). Ассоциативность так определенного умножения проверяется без затруднений.

Как известно, *преобразованием* множества M называется любое отображение этого множества в себя (т. е. на некоторое подмножество). В частности, *подстановкой* множества M называется любое взаимно однозначное отображение этого множества на себя.

С другой стороны, если даны множества M, N, P и отображения φ: $M \to N$ и ψ: $N \to P$, то последовательное выполнение этих отображений дает отображение $\varphi\psi$: $M \to P$, называемое их *произведением*. Таким образом, для всех $a \in M$

$$a(\varphi\psi) = (a\varphi)\psi.$$

Это умножение отображений ассоциативно: если даны отображения

$$\varphi\colon M \to N,\ \psi\colon N \to P,\ \chi\colon P \to Q,$$

то

$$(\varphi\psi)\chi = \varphi(\psi\chi),$$

так как для любого $a \in M$

$$a[(\varphi\psi)\chi] = [a(\varphi\psi)]\chi = [(a\varphi)\psi]\chi = (a\varphi)(\psi\chi) = \\ = a[\varphi(\psi\chi)].$$

Умножение отображений не является, понятно, алгебраической операцией в смысле § 1. Она будет, однако, таковой в случае преобразований одного множества. При этом множество всех преобразований данного множества M оказывается полугруппой; это *симметрическая полугруппа* на множестве M.

Симметрическая полугруппа на M оказывается полугруппой с единицей. Роль единицы играет *тождественная подстановка* ε_M,

$$a\varepsilon_M = a \text{ для всех } a \in M.$$

Больше того, для любых отображений $\varphi\colon M \to N$ и $\psi\colon L \to M$ будет, очевидно,

$$\varepsilon_M\varphi = \varphi, \quad \psi\varepsilon_M = \psi,$$

т. е. тождественная подстановка ε_M играет роль единицы по отношению к умножению любых отображений, если, понятно, соответствующее произведение имеет смысл.

Подстановки множества M выделяются в симметрической полугруппе на M как такие ее элементы φ, для которых существуют обратные элементы φ^{-1}, удовлетворяющие условиям

$$\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon_M.$$

Обратное преобразование φ^{-1} само будет подстановкой, переводящей для всякого $a \in M$ элемент $a\varphi$ в элемент a. Так как произведение подстановок само будет подстановкой и это умножение ассоциативно, то мы

получаем, что множество всех подстановок данного множества M будет группой; это *симметрическая группа* на множестве M.

Мы видим, что симметрическая группа на M выделяется в симметрической полугруппе на M как содержащаяся в ней однозначно определенная максимальная группа с тем же умножением и той же единицей.

Существование симметрических групп и симметрических полугрупп в равной мере оправдывает выбор групп и полугрупп в качестве объектов изучения. Правда, для групп известна следующая теорема Кэли:

Теорема 1. *Всякая группа G изоморфно вкладывается в симметрическую группу на множестве G.*

Параллельная теорема справедлива, однако, и для полугрупп:

Теорема 1′. *Всякая полугруппа с единицей G изоморфно вкладывается в симметрическую полугруппу на множестве G.*

Из последней теоремы немедленно следует, ввиду сказанного выше, что всякая полугруппа G изоморфно вкладывается в некоторую симметрическую полугруппу, хотя в общем случае последняя берется на некотором большем, чем G, множестве.

Покажем, что теоремы 1 и 1′ являются непосредственными следствиями двух других теорем, представляющих и самостоятельный интерес. Отметим сперва, что *произведение гомоморфизмов универсальных алгебр* (в смысле умножения отображений) *само будет гомоморфизмом*. Действительно, если даны однотипные алгебры G, G', G'' с системой операций Ω и гомоморфизмы $\varphi\colon G \to G'$, $\psi\colon G' \to G''$, то для любого $\omega \in \Omega_n$, $n \geqslant 1$, и любых элементов $a_1, a_2, \ldots, a_n \in G$ будет

$$\begin{aligned}(a_1a_2\ldots a_n\omega)(\varphi\psi) &= [(a_1a_2\ldots a_n\omega)\varphi]\psi = \\ &= [(a_1\varphi)(a_2\varphi)\ldots(a_n\varphi)\omega]\psi = \\ &= [(a_1\varphi)\psi][(a_2\varphi)\psi]\ldots[(a_n\varphi)\psi]\omega = \\ &= [a_1(\varphi\psi)][a_2(\varphi\psi)]\ldots[a_n(\varphi\psi)]\omega.\end{aligned}$$

С другой стороны, если операция $\omega \in \Omega_0$ отмечает в

алгебрах G, G', G'' соответственно элементы 0_ω, $0'_\omega$, $0''_\omega$, то

$$0_\omega(\varphi\psi) = (0_\omega\varphi)\psi = 0'_\omega\psi = 0''_\omega.$$

Отсюда следует, что множество всех эндоморфизмов данной алгебры G составляет подполугруппу в симметрической полугруппе на множестве G, притом содержащую единицу этой полугруппы,— тождественная подстановка является, очевидно, даже автоморфизмом. Полученная полугруппа с единицей называется *полугруппой (всех) эндоморфизмов* алгебры G.

Аналогично всякий автоморфизм алгебры G является подстановкой в множестве G. Произведение двух автоморфизмов этой алгебры будет и подстановкой, и эндоморфизмом, а поэтому само будет автоморфизмом. Обратная подстановка φ^{-1} для автоморфизма φ сама будет автоморфизмом: если $\omega \in \Omega_n$, $n \geqslant 1$, и $a_1, a_2, \ldots, a_n \in G$, то существуют такие $b_1, b_2, \ldots, b_n \in G$, что $a_i = b_i\varphi$, $i = 1, 2, \ldots, n$, а поэтому

$$\begin{aligned}(a_1a_2\ldots a_n\omega)\varphi^{-1} &= [(b_1\varphi)(b_2\varphi)\ldots(b_n\varphi)\omega]\varphi^{-1} = \\ &= (b_1b_2\ldots b_n\omega)(\varphi\varphi^{-1}) = b_1b_2\ldots b_n\omega = \\ &= (a_1\varphi^{-1})(a_2\varphi^{-1})\ldots(a_n\varphi^{-1})\omega.\end{aligned}$$

Если же $\omega \in \Omega_0$ отмечает в G элемент 0_ω, то из $0_\omega\varphi = 0_\omega$ следует $0_\omega\varphi^{-1} = 0_\omega$. Таким образом, все автоморфизмы данной алгебры G составляют подгруппу в симметрической группе на множестве G; это *группа (всех) автоморфизмов* алгебры G. Очевидно, что эта группа выделяется в полугруппе всех эндоморфизмов алгебры G как содержащаяся в ней однозначно определенная максимальная группа с тем же умножением и той же единицей. Можно сказать также, что группа автоморфизмов есть группа всех обратимых элементов полугруппы эндоморфизмов.

Справедливы следующие теоремы, из которых теоремы 1 и 1′ немедленно следуют:

Теорема 2. *Всякая группа G изоморфна группе всех автоморфизмов некоторой универсальной алгебры, определенной на множестве G.*

Теорема 2′. *Всякая полугруппа с единицей G изоморфна полугруппе всех эндоморфизмов некоторой универсальной алгебры, определенной на множестве G.*

Оказывается, что теорема 2 сама следует из теоремы 2′. Проведем сперва некоторые вспомогательные рассмотрения.

Пусть задано эпиморфное (в частности, изоморфное) отображение φ полугруппы G с единицей e на полугруппу G'. Тогда образ $e\varphi$ единицы будет единицей в G'. Если элемент a обратим в G, то образ $a^{-1}\varphi$ его обратного элемента a^{-1} будет в G' обратным для элемента $a\varphi$, т. е. $(a\varphi)^{-1} = a^{-1}\varphi$. Отсюда следует, что *полугруппа, изоморфная группе, сама будет группой.*

В самом деле, если b' — произвольный элемент из G', то существует такой элемент $b \in G$, что $b\varphi = b'$. Тогда

$$b'(e\varphi) = (b\varphi)(e\varphi) = (be)\varphi = b\varphi = b'$$

и аналогично $(e\varphi)b' = b'$. С другой стороны,

$$(a\varphi)(a^{-1}\varphi) = (aa^{-1})\varphi = e\varphi$$

и аналогично $(a^{-1}\varphi)(a\varphi) = e\varphi$.

Пусть теперь теорема 2′ уже доказана и пусть дана произвольная группа G. Являясь, в частности, полугруппой с единицей, G будет изоморфна полугруппе всех эндоморфизмов некоторой алгебры, определенной на множестве G. Эта последняя полугруппа будет, следовательно, группой. Отсюда вытекает, что все эндоморфизмы рассматриваемой алгебры обратимы, т. е. являются на самом деле ее автоморфизмами, что доказывает теорему 2.

Остается доказать теорему 2′. Если дана полугруппа G с единицей e, то для всякого $a \in G$ возьмем в множестве G унарную операцию ω_a, являющуюся в полугруппе G левым умножением на элемент a,

$$x\omega_a = ax \text{ для все х } x \in G.$$

Множество G со всеми операциями ω_a, $a \in G$, будет алгеброй, которую обозначим через $\overline{G}$. Правое умножение φ_b в полугруппе G на элемент b, $x\varphi_b = xb$ для всех $x \in G$, будет эндоморфизмом алгебры $\overline{G}$, так как

для любых x, $a \in G$

$$(x\omega_a)\varphi_b = (ax)b = a(xb) = (x\varphi_b)\omega_a.$$

При этом если $b \neq c$, то $\varphi_b \neq \varphi_c$, так как

$$e\varphi_b = eb = b, \quad e\varphi_c = ec = c.$$

Эндоморфизмами φ_b, $b \in G$, исчерпываются все эндоморфизмы алгебры $\bar{G}$, так как если φ — произвольный ее эндоморфизм и $e\varphi = c$, то для всех $x \in G$

$$x\varphi = (xe)\varphi = (e\omega_x)\varphi = (e\varphi)\omega_x = xc = x\varphi_c,$$

т. е. $\varphi = \varphi_c$. Мы получили взаимно однозначное соответствие между всеми эндоморфизмами алгебры $\bar{G}$ и всеми элементами полугруппы G, которое будет на самом деле изоморфизмом соответствующих полугрупп, так как для всех x, b, $c \in G$

$$x\varphi_{bc} = x(bc) = (xb)c = (x\varphi_b)\varphi_c = x(\varphi_b\varphi_c),$$

т. е. $\varphi_{bc} = \varphi_b\varphi_c$. При этом, как и должно быть, единице полугруппы G соответствует тождественный автоморфизм алгебры $\bar{G}$, так как для всех $x \in G$

$$x\varphi_e = xe = x.$$

Теорема 2′ доказана.