§ 6. КВАЗИГРУППЫ И ЛУПЫ

Мы пришли к понятию полугруппы, заметив, что в некоторых из определений группы участвует бинарная ассоциативная операция. Первое определение группы из § 2 после удаления из него требования ассоциативности умножения приводит к другому важному понятию, также ставшему в последнее время предметом содержательной теории. Именно, группоид, в котором для любых элементов a, b однозначно разрешимы уравнения

$$ax = b, \quad ya = b,$$

называется *квазигруппой*. Как и в § 2, можно утверждать. что квазигруппы составляют многообразие относительно трех бинарных операций ab, $b \setminus a$, b / a, определяемое тождествами

$$x(y \setminus x) = y, \qquad (y / x)\, x = y,$$
$$xy \setminus x = y, \qquad yx / x = y.$$

Из определения квазигруппы нельзя вывести существование в ней единицы. Квазигруппа, обладающая единицей, называется *лупой*. Лупы также составляют многообразие, сигнатура которого состоит из трех бинарных и одной нульарной операции.

Нельзя рассчитывать на то, что для оправдания выбора квазигрупп в качестве объекта самостоятельного изучения можно будет использовать каким-либо способом преобразования или отображения. Для этой цели хорошо служат, однако, так называемые сети. По образцу геометрической сети, состоящей из всех точек плоскости и трех семейств прямых — все прямые, параллельные оси абсцисс, оси ординат и еще одной прямой,— введем следующее понятие. Рассмотрим систему из четырех непустых попарно непересекающихся множеств P, L^1, L^2, L^3; элементы первого множества назовем *точками*, остальных множеств — *прямыми*, причем нумерацию множеств (или, как мы будем говорить, семейств) прямых считаем фиксированной. Примем, что точки и прямые могут находиться в отношении *инцидентности*, выражаемом словами «точка лежит на прямой», «прямая проходит через точку» и т. д.

Назовем эту систему *сетью*, если выполняются следующие требования:

а) через каждую точку проходит одна и только одна прямая каждого из трех семейств;

б) две прямые, принадлежащие к различным семействам, пересекаются в одной и только одной точке.

Заметим, что ввиду а) прямые одного семейства не могут пересекаться. Заметим также, что семейства L^1, L^2, L^3 равномощны — мы получим взаимно однозначное соответствие между L^1 и L^2, если фиксируем некоторую прямую l^3 из L^3 и сопоставим друг другу те прямые из L^1 и L^2, которые пересекаются в точке, лежащей на l^3.

Если G — множество, равномощное с каждым из L^i, $i = 1, 2, 3$, то прямые каждого из этих трех семейств можно снабдить индексами, пробегающими множество G. Фиксировав эти индексации, притом совершенно произвольные, мы следующим образом определяем на G операцию умножения: $ab = c$, если через точку пересечения прямых $l_a^1 \in L^1$ и $l_b^2 \in L^2$ проходит прямая $l_c^3 \in L^3$. Относительно этой операции G будет квазигруппой: единственным решением уравнения $ax = b$, например, будет индекс той единственной прямой семейства L^2, которая проходит через точку пересечения прямых l_a^1 и l_c^3. Эта квазигруппа называется *координатной квазигруппой* исходной сети.

Всякая квазигруппа G является координатной квазигруппой некоторой сети. Построим эту сеть. Ее точками считаем упорядоченные пары (a, b) элементов из G, прямыми i-го семейства, $i = 1, 2, 3,$ — символы l_a^i для всех $a \in G$. Точка (a, b) считается инцидентной прямой l_a^1 первого семейства, прямой l_b^2 второго и прямой l_{ab}^3 третьего. Следовательно, требование а) выполняется. Выполняется и требование б): прямые l_a^1 и l_b^2 пересекаются в точке (a, b), прямые l_a^1 и l_c^3 — в точке $(a, c \setminus a)$, прямые l_b^2 и l_c^3 — в точке $(c / b, b)$. Очевидно, что при указанной индексации прямых построенной сети координатной квазигруппой служит как раз квазигруппа G.

Заметим, что применения квазигрупп, в частности, в теории алгебраических кривых, связаны обычно с указанным представлением квазигруппы в качестве координатной квазигруппы некоторой сети. Иногда, впрочем, берется понятие, двойственное к сети (прямые называются точками, а точки — прямыми).

Координатная квазигруппа сети зависит, очевидно, от выбранных индексаций прямых каждого семейства. Если эти индексации будут изменены (что равносильно применению к ним некоторых подстановок множества G), то на том же множестве G будет определена новая квазигруппа, в общем случае с первоначальной не изоморфная. Эти квазигруппы будут, однако, изотопными в соответствии со следующим общим определением.

Два группоида, с операциями $a \cdot b$ и $a \circ b$, определенные на одном и том же множестве G, называются *изотопными*, если существуют такие подстановки ρ, σ и τ множества G, что для любых a, $b \in G$

$$a \circ b = (a\rho \cdot b\sigma)\tau.$$

Легко проверяется, что отношение *изотопии* будет для бинарных операций на множестве G отношением эквивалентности.

Изоморфизм двух бинарных операций, заданных на одном и том же множестве, является частным случаем изотопии, а именно при $\rho = \sigma = \tau^{-1}$. С другой стороны, изотопия называется *главной* (соответственно говорят о *главном изотопе*), если τ является тождественной подстановкой, т. е.

$$a \circ b = a\rho \cdot b\sigma.$$

Всякий изотоп группоида изоморфен некоторому его главному изотопу. Действительно, если на множестве G заданы группоиды с операциями $a \cdot b$ и $a \circ b$, причем $a \circ b = (a\rho \cdot b\sigma)\tau$, то операция

$$a \times b = a\tau\rho \cdot b\tau\sigma$$

определяет на G главный изотоп первого группоида, изоморфный второму, так как

$$(a\tau^{-1} \times b\tau^{-1})\tau = [(a\tau^{-1})\tau\rho \cdot (b\tau^{-1})\tau\sigma]\tau = (a\rho \cdot b\sigma)\tau = a \circ b.$$

Две координатные квазигруппы одной и той же сети, определенные на одном и том же множестве G, на самом деле изотопны. Действительно, обозначим операцию в первой квазигруппе через $a \circ b$, т. е. $a \circ b = c$ означает, что прямые l_a^1, l_b^2 и l_c^3 пересекаются в одной точке. Меняем теперь индексации прямых каждого семейства, подвергая их подстановкам ρ, σ и τ. Теперь эти же три прямые будут обозначены через $l_{a\rho}^1$, $l_{b\sigma}^2$, $l_{c\tau}^3$, причем каждый из элементов $a\rho$, $b\sigma$, $c\tau$ пробегает все множество G, а поэтому во второй квазигруппе (с операцией $a \cdot b$) будет

$$a\rho \cdot b\sigma = c\tau,$$

т. е.

$$a\rho \cdot b\sigma = (a \circ b)\tau.$$

Так как подстановки ρ, σ, τ были произвольными, то ясно, что *все координатные квазигруппы данной сети составляют, с точностью до изоморфизма, полный класс изотопных квазигрупп, определенных на множестве G.* Отсюда сразу следует, что *всякий группоид, изотопный квазигруппе, сам будет квазигруппой.* Используя сети, легко доказать также следующую т е о р е м у А л б е р т а (Trans. Amer. Math. Soc. 54 (1943), 507—519):

Всякая квазигруппа изотопна некоторой лупе.

В самом деле, заданная квазигруппа G служит координатной квазигруппой для сети (P, L^1, L^2, L^3). Отметим теперь в G некоторый элемент e и следующим образом изменим индексацию прямых: индексацию семейства L^3 оставим без изменения, а некоторую прямую семейства L^1 обозначим через l_e^1, после чего прямую семейства L^2 обозначим через l_b^2, если она проходит через точку пересечения прямых l_e^1 и l_b^3 (этим определяется, в частности, прямая l_e^2), и, наконец, прямую семейства L^1 обозначим через l_a^1, если она проходит через точку пересечения прямых l_e^2 и l_a^3. При этом, как легко проверить, индекс прямой l_e^1 не изменится. Координатная квазигруппа, соответствующая этой новой индексации, имеет, очевидно, элемент e своей единицей, т. е. будет лупой.

Изотопные лупы могут не быть изоморфными. Справедлива, однако, вторая теорема Алберта:

Если лупа (в частности, группа) изотопна некоторой группе, то они изоморфны.

Эта теорема вытекает, впрочем, из следующей теоремы Брака — Хьюза (Trans. Amer. Math. Soc. **60** (1946), 245—354; J. London Math. Soc. **32** (1957), 510—511):

Если группоид с единицей изотопен полугруппе, то они изоморфны, т. е. оба являются полугруппами с единицей.

Действительно, пусть на множестве G заданы группоид с умножением $a \cdot b$ и единицей e и полугруппа с умножением $a \circ b$, причем они изотопны, т. е.

$$a \circ b = (a\rho \cdot b\sigma)\tau,$$

где ρ, σ, τ — подстановки в G. Так как для любых a, b, $c \in G$

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

то

$$[(a\rho \cdot b\sigma)\tau\rho \cdot c\sigma]\tau = [a\rho \cdot (b\rho \cdot c\sigma)\tau\sigma]\tau,$$

откуда

$$(a\rho \cdot b\sigma)\tau\rho \cdot c\sigma = a\rho \cdot (b\rho \cdot c\sigma)\tau\sigma. \tag{1}$$

Полагая здесь $a\rho = c\sigma = e$, получаем для всех $b \in G$

$$b\sigma\tau\rho = b\rho\tau\sigma. \tag{2}$$

Полагая, далее, в (1) $a\rho = e$ и используя (2), получаем

$$b\rho\tau\sigma \cdot c\sigma = (b\rho \cdot c\sigma)\tau\sigma$$

или, заменяя $b\rho$ на a и $c\sigma$ на b,

$$a\tau\sigma \cdot b = (a \cdot b)\tau\sigma \tag{3}$$

для всех a, $b \in G$. Аналогично, полагая в (1) $c\sigma = e$ и используя (2), получаем

$$(a\rho \cdot b\sigma)\tau\rho = a\rho \cdot b\sigma\tau\rho$$

или, заменяя $a\rho$ на a и $b\sigma$ на b,

$$(a \cdot b)\tau\rho = a \cdot b\tau\rho \tag{4}$$

для всех $a, b \in G$. Наконец, последовательно используя (3), (4) и (2), получаем, что для любых $a, b \in G$

$$(a \circ b)\sigma\tau\rho = (a\rho \cdot b\sigma)\tau\sigma\tau\rho = (a\rho\tau\sigma \cdot b\sigma)\tau\rho = a\rho\tau\sigma \cdot b\sigma\tau\rho = \\ = a\sigma\tau\rho \cdot b\sigma\tau\rho,$$

т. е. подстановка $\sigma\tau\rho$ оказывается изоморфизмом между заданными группоидом и полугруппой. Теорема доказана.