§ 9. АССОЦИАТИВНЫЕ КОЛЬЦА

Настало время вспомнить, что в курсе высшей алгебры наряду с понятием группы значительное место занимают понятия ассоциативного кольца и модуля. Начнем с первого из них. Напомним, что *ассоциативное кольцо* можно определить как множество, являющееся абелевой группой по сложению и полугруппой по умножению (они называются соответственно аддитивной группой и мультипликативной полугруппой кольца), причем эти операции связаны законами дистрибутивности

$$x(y+z) = xy + xz,$$
$$(x+y)z = xz + yz.$$

Ассоциативные кольца составляют, следовательно, многообразие.

Любая абелева группа G может служить аддитивной группой некоторого ассоциативного кольца — достаточно взять на G нулевое умножение, т. е. положить $ab = 0$ для всех a, $b \in G$, где 0 — нуль аддитивной группы. С другой стороны, не всякая полугруппа служит мультипликативной полугруппой некоторого ассоциативного кольца. Действительно, известно, что во всяком кольце R для любого его элемента a выполняются равенства

$$a \cdot 0 = 0 \cdot a = 0, \tag{1}$$

т. е. мультипликативная полугруппа ассоциативного кольца всегда является *полугруппой с нулем* (нуль полугруппы определяется равенствами (1)).

Всякая полугруппа G изоморфно вкладывается в мультипликативную полугруппу некоторого ассоциативного кольца.

Предположим сперва, что G уже является подполугруппой мультипликативной полугруппы кольца R. Тогда подкольцо, порожденное множеством G, будет состоять из тех элементов кольца R, которые хотя бы одним способом записываются в виде суммы

$$\sum_{a\in G}{}' k_a a, \tag{2}$$

где a пробегает все элементы из G, а коэффициенты являются целыми числами, причем не более конечного числа этих коэффициентов отлично от нуля; это условие на коэффициенты отмечено штрихом у знака суммы. Ясно, что элемент $b \in G$ допускает запись вида (2), а именно, с $k_b = 1$ и $k_a = 0$ для всех $a \neq b$. В соответствии со свойствами операций в кольце элементы этого вида составляют подкольцо, так как

$$\sum_{a\in G}{}' k_a a + \sum_{a\in G}{}' l_a a = \sum_{a\in G}{}' (k_a + l_a)\, a, \tag{3}$$

$$0 = \sum_{a\in G}{}' 0\cdot a, \tag{4}$$

$$-\Big(\sum_{a\in G}{}' k_a a\Big) = \sum_{a\in G}{}' (-k_a)\, a, \tag{5}$$

$$\sum_{a\in G}{}' k_a a \cdot \sum_{b\in G}{}' l_b b = \sum_{c\in G}{}' m_c c, \tag{6}$$

где m_c является суммой всех отличных от нуля произведений $k_a l_b$ для таких a и b, что $ab = c$. Ясно, что правые части равенств (3) — (6) имеют вид (2) с конечным числом ненулевых коэффициентов. В частности, равенство (6) означает, что конечные суммы, стоящие множителями в левой части этого равенства, перемножаются почленно, затем применяются равенства вида

$$k_a a \cdot l_b b = (k_a l_b)(ab),$$

произведения ab заменяются равными им элементами c полугруппы G и, наконец, выполняется приведение подобных членов. Полученное подкольцо порождается, очевидно, множеством G.

Пусть теперь G — произвольная полугруппа. Рассмотрим множество всевозможных формальных сумм вида (2) и определим в этом множестве операции в соответствии с равенствами (3) — (6). Мы получим ассоциативное кольцо. В самом деле, по сложению это будет абелева группа, как без всяких затруднений следует из (3) — (5). Проверка ассоциативности умножения и законов дистрибутивности уже несколько громоздка, но не представляет никаких принципиальных трудностей, и мы ее опускаем. Отметим, что умножение в соответствии с (6) слов вида (2), имеющих лишь один ненулевой коэффициент, притом равный единице, сводится к умножению элементов полугруппы G. Этим определяется изоморфное вложение заданной полугруппы G в мультипликативную полугруппу построенного нами кольца. Это самое свободное из возможных вложений нашей полугруппы в том смысле, что всякий элемент кольца записывается через элементы полугруппы в виде (2) однозначно.

Построенное нами кольцо называется *целочислeнным полугрупповым кольцом* полугруппы G, а если G — группа, то *целочисленным групповым кольцом* этой группы.

Если мультипликативная полугруппа ассоциативного кольца R обладает единицей (см. § 3), то R называется *кольцом с единицей*. Ассоциативные кольца с единицей составляют, очевидно, многообразие.

Всякое ассоциативное кольцо R изоморфно вкладывается в ассоциативное кольцо с единицей.

Предположим сперва, что кольцо R уже содержится в ассоциативном кольце $\bar{R}$ с единицей e. Тогда подкольцо, порожденное в $\bar{R}$ множеством $R \cup e$, будет состоять из тех элементов, которые хотя бы одним способом записываются в виде

$$a + ke, \tag{7}$$

где $a \in R$, k — целое число; обозначим выражение (7) символом (a, k). Из свойств операций в кольце $\bar{R}$ следует:

$$(a, k) + (b, l) = (a + b, k + l), \tag{8}$$

$$0 = (0, 0), \tag{9}$$

$$-(a, k) = (-a, -k), \tag{10}$$

$$(a, k)(b, l) = (ab + la + kb, kl). \tag{11}$$

Пусть теперь R — произвольное ассоциативное кольцо. Рассмотрим множество всевозможных пар вида

(a, k), где $a \in R$, k — целое число, и определим в нем операции в соответствии с равенствами (8) — (11). Мы получим ассоциативное кольцо — очевидно, что это будет абелева группа по сложению, а проверка ассоциативности умножения и законов дистрибутивности хотя и громоздка, но не представляет никаких принципиальных трудностей. Единицей этого кольца служит пара $(0, 1)$, как немедленно следует из (11). Наконец, из (8) и (11) следует

$$(a, 0) + (b, 0) = (a + b, 0),$$
$$(a, 0)(b, 0) = (ab, 0),$$

т. е. пары вида $(a, 0)$ составляют в построенном нами кольце подкольцо, изоморфное исходному кольцу R. Мы получили самое свободное вложение кольца R в кольцо с единицей в том смысле, что запись элементов кольца $\bar{R}$ в виде (7) — ввиду (8) — (11) будет

$$(a, k) = (a, 0) + k(0, 1)$$

— оказывается однозначной.

Ассоциативно-коммутативные кольца (умножение не только ассоциативно, но и коммутативно) были подсказаны, понятно, кольцами чисел, кольцами многочленов и кольцами функций. Покажем, чем оправдывается большой интерес к произвольным ассоциативным кольцам.

Рассмотрим гомоморфизмы некоторой группы G, записанной мультипликативно, в абелеву группу G', записанную аддитивно. Если φ и ψ — два таких гомоморфизма, то отображение $\varphi + \psi$, определяемое равенством

$$a(\varphi + \psi) = a\varphi + a\psi, \quad a \in G, \tag{12}$$

также будет гомоморфизмом G в G'. Действительно, ввиду коммутативности сложения в G' получаем для любых $a, b \in G$

$$(ab)(\varphi + \psi) = (ab)\varphi + (ab)\psi =$$
$$= a\varphi + b\varphi + a\psi + b\psi = (a\varphi + a\psi) + (b\varphi + b\psi) =$$
$$= a(\varphi + \psi) + b(\varphi + \psi).$$

Ясно, что это сложение гомоморфизмов коммутативно и ассоциативно. Роль нуля играет *нулевой гомоморфизм*, отображающий всю группу G в нуль группы G'. С другой стороны, для любого гомоморфизма $\varphi\colon G \to G'$ отображение $-\varphi$, определяемое равенством

$$a(-\varphi) = -a\varphi, \quad a \in G,$$

будет гомоморфизмом, так как для любых $a, b \in G$

$$(ab)(-\varphi) = -(ab)\varphi = -(a\varphi + b\varphi) = \\ = (-a\varphi) + (-b\varphi) = a(-\varphi) + b(-\varphi).$$

Этот гомоморфизм будет *противоположным* для φ, так как для $a \in G$

$$a[\varphi + (-\varphi)] = a\varphi + a(-\varphi) = a\varphi - a\varphi = 0,$$

т. е. $\varphi + (-\varphi)$ равно нулевому гомоморфизму.

Таким образом, *гомоморфизмы любой группы* G (легко проверить, что в качестве G здесь можно было бы взять не группу, а любую алгебру, однотипную с группой) *в абелеву группу* G' *составляет по сложению абелеву группу*. В частности, эндоморфизмы абелевой группы G составляют по сложению, определяемому равенством (12), абелеву группу. Вместе с тем, в соответствии с § 3 они составляют полугруппу с единицей по умножению в смысле умножения преобразований.

Покажем, что эти операции связаны законами дистрибутивности. Именно, для любого $a \in G$ и любых эндоморфизмов φ, ψ и χ

$$a[\varphi(\psi + \chi)] = (a\varphi)(\psi + \chi) = (a\varphi)\psi + (a\varphi)\chi = \\ = a(\varphi\psi) + a(\varphi\chi) = a(\varphi\psi + \varphi\chi),$$

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

Для дальнейшего отметим, что в доказательстве первого закона дистрибутивности не использовалось то, что преобразования φ, ψ, χ являются эндоморфизмами.

Таким образом, эндоморфизмы абелевой группы G составляют относительно операций сложения и умножения эндоморфизмов ассоциативное кольцо с единицей. Оно называется *кольцом эндоморфизмов* абелевой группы G.

Всякое ассоциативное кольцо изоморфно вкладывается в кольцо эндоморфизмов некоторой абелевой группы.

Так как всякое ассоциативное кольцо изоморфно вкладывается в ассоциативное кольцо с единицей, то мы будем доказывать следующую теорему:

Всякое ассоциативное кольцо R с единицей 1 *изоморфно вкладывается в кольцо эндоморфизмов своей аддитивной группы.*

В самом деле, сопоставим всякому $a \in R$ преобразование, переводящее всякий элемент $x \in R$ в элемент xa. Это эндоморфизм аддитивной группы кольца R, так как

$$(x + y)\, a = xa + ya.$$

Сумме и произведению элементов из R соответствуют сумма и произведение соответствующих эндоморфизмов, как показывают равенства

$$x\,(a + b) = xa + xb, \quad x\,(ab) = (xa)\, b.$$

Наконец, различным элементам из R соответствуют различные эндоморфизмы, так как из $a \neq b$ следует $1 \cdot a \neq 1 \cdot b$.

В теории ассоциативных колец, ныне весьма широко разработанной, большую роль играют следующие классы колец, не являющиеся, впрочем, многообразиями: кольца без делителей нуля и тела. Именно, кольцо R называется *кольцом без делителей нуля*, если его элементы, отличные от нуля, составляют подполугруппу мультипликативной полугруппы кольца, иными словами, если произведение любых двух элементов из R, отличных от нуля, само отлично от нуля. Если же указанная подполугруппа отличных от нуля элементов является по умножению даже группой, то кольцо называется *телом*, а в ассоциативно-коммутативном случае — *полем*.

Ясно, что всякое подкольцо кольца без делителей нуля, в частности, тела, само будет кольцом без делителей нуля. Возникает естественный вопрос, всякое ли ассоциативное кольцо без делителей нуля можно вложить в тело? Этот вопрос оказался тесно связанным с вопросом об условиях, при которых полугруппа может быть вложена в группу. Из свойств группы немедленно следует, что если полугруппа G является подполугруппой группы, то G будет *полугруппой с сокращениями*, т. е. для любых a, b, $c \in G$ из $ac = bc$, а также из $ca = cb$ следует $a = b$. Полугруппа ненулевых элементов всякого ассоциативного кольца без делителей нуля будет полугруппой с сокращениями: если в кольце без делителей нуля $ac = bc$ и $c \neq 0$, то $(a - b)c = 0$, откуда $a - b = 0$, т. е. $a = b$.

Можно доказать, что всякая коммутативная полугруппа с сокращениями изоморфно вкладывается в абелеву группу, а всякое ассоциативно-коммутативное кольцо без делителей нуля (т. е. область целостности) изоморфно вкладывается в тело. С другой стороны, А. И. Мальцев (Math. Ann. **113** (1937)) построил пример ассоциативного (но не коммутативного) кольца без делителей нуля, которое не вкладывается в тело, причем полугруппа ненулевых элементов этого кольца (являющаяся, как мы знаем, полугруппой с сокращениями) не вкладывается в группу. В самое последнее время несколько авторов, в частности, Л. А. Бокуть (ДАН СССР **165** (1965), 555—558), построили примеры ассоциативных колец без делителей нуля, которые не вкладываются в тело, хотя полугруппы их ненулевых элементов вкладываются в группу.