Разложение на простые множители в структурах с умножением

Е. Г. Шульгейфер

Введение

Вопрос о необходимых и достаточных условиях для однозначного разложения идеалов коммутативной области целостности в произведение степеней простых идеалов был решен Э. Нетер (см. Ван дер Варден [1], гл. 14). Эта „мультипликативная теория идеалов" в дальнейшем подвергалась многочисленным обобщениям. В частности, в работах Мория и Кобаяси [2, 3] соответствующие условия указаны для произвольных коммутативных колец.

С другой стороны, перенесению теории Нетер на случай некоммутативных колец с единицей посвящены работы Узкова [4] и Асано [5]. В этих работах рассматриваются как двусторонние, так и односторонние идеалы, причем получаются совсем различные теории; нас в дальнейшем будут интересовать лишь двусторонние идеалы.

В работе Узкова рассматриваются при этом лишь такие двусторонние идеалы, которые имеют непустое пересечение с множеством регулярных элементов, принадлежащих к фиксированному подкольцу центра рассматриваемого кольца. В работе же Асано рассматриваются лишь двусторонние идеалы, имеющие непустое пересечение с множеством всех регулярных элементов кольца, причем дополнительно требуется, чтобы рассматриваемое кольцо обладало кольцом отношений. Отметим, что эти параллельные теории были объединены в неопубликованной работе Б. С. Виленской.

Целью настоящей работы является разыскание необходимых и достаточных условий для хорошей арифметики двусторонних идеалов в произвольном некоммутативном кольце. Оказалось, что эти условия, обобщающие условия Мория и Кобаяси, используют лишь свойства структуры двусторонних идеалов и свойства умножения двусторонних идеалов. Это позволило строить всю теорию не для колец, а сразу для структур с умножением (см. определение в § 1). Этим, в частности, учитываются и те ограничения на рассматриваемые двусторонние идеалы, которые накладывались в работах Узкова и Асано. Вместе с тем полученные результаты применимы и к двусторонним присоединенным идеалам некоммутативного кольца (см. § 6), то есть ими обобщаются и ре-

зультаты работы автора [6], относящиеся к вопросу о хорошей арифметике для присоединенных идеалов коммутативного кольца.

Само понятие структуры с умножением не является новым — см. работы Крулля [7] и Уорда и Дилуорса [8], в основном посвященные перенесению на структуры с умножением вопроса о разложении идеала в пересечение примарных идеалов; см. также Биркгоф [9], гл. 13.

В заключение выражаю глубокую благодарность А. Г. Курошу, под руководством которого была выполнена настоящая работа.

§ 1

Определение. Множество S с элементами $a, b, c, \ldots$ называется *структурой с умножением*, если оно является структурой с наибольшим элементом e относительно операций сложения $a \cup b$ и пересечения $a \cap b$ и если для его элементов определена также операция умножения ab, которая удовлетворяет закону ассоциативности

$$(ab)c = a(bc) = abc,$$

со сложением связана законом дистрибутивности

$$a(b \cup c) = ab \cup ac, \quad (b \cup c)a = ba \cup ca,$$

с пересечением — условием

$$ab \leqslant a \cap b.$$

Из определения структуры с умножением следует:

1. Если $a \leqslant b$, то $ac \leqslant bc$ и $ca \leqslant cb$.

Действительно, если $a \leqslant b$, то $bc = (a \cup b)c = ac \cup bc$, то есть $ac \leqslant bc$. Аналогично доказывается, что $ca \leqslant cb$.

2. $(a \cap b)(a \cup b) \leqslant ab \cup ba$; $(a \cup b)(a \cap b) \leqslant ab \cup ba$.

3. Из $bc \leqslant a$ следует $(b \cup a)(c \cup a) \leqslant a$.

4. Если в структуре с умножением S существует наименьший элемент, который мы будем называть *нулем* и обозначать через 0, то он удовлетворяет условию $a0 = 0a = 0$, где a — произвольный элемент из S. Обратно, если элемент z удовлетворяет условию $za = az = z$, где a — произвольный элемент из S, то $z = 0$.

В дальнейшем изложении, если в определении (утверждении, оговорке) фигурирует нуль структуры с умножением S, то мы условимся, чтобы каждый раз не оговаривать: „если нуль в структуре с умножением S существует“, что это определение (утверждение, оговорка) имеет смысл, если в S существует 0.

Элемент $g \in S$, отличный от e, называется *максимальным элементом*, если в S не существует элемента, отличного от e и строго большего g.

Элемент $p \in S$, отличный от e, называется *простым элементом*, если из того, что $ab \leqslant p$ следует, что или $a \leqslant p$, или $b \leqslant p$.

Элемент $q \in S$ называется *примарным элементом,* если из того, что $ab \leqslant q$ и один из сомножителей не меньше q следует, что некоторая степень второго сомножителя меньше или равна q.

Элемент $z \in S$ называется *нильпотентным элементом,* если $z^k = 0$ для некоторого натурального числа k.

Элемент $e_1 \in S$ называется *единицей,* если для любого элемента a из S справедливо равенство: $ae_1 = e_1 a = a$; в этом случае $e_1 = e$.

Лемма. *Если в S наибольший элемент e является единицей, то*

1) *если $a \cup b = e$ и $a \cup c = e$, то $a \cup (b \cap c) = e$ и $a \cup bc = e$,*

2) *если $a \cup b = e$, то $a \cap b = ab \cup ba$.*

Доказательство. 1. $e = e^2 = (a \cup b)(a \cup c) \leqslant a^2 \cup ac \cup ba \cup bc \leqslant a \cup bc$, следовательно, $a \cup bc = e$.

Так как $bc \leqslant b \cap c$, то $e = a \cup bc \leqslant a \cup (b \cap c)$. Тем самым показано, что и $a \cup (b \cap c) = e$.

2. Следует из свойства 2 структуры с умножением, приведенного на стр. 101.

Структура с умножением S называется *полукоммутативной,* если в ней каждая пара максимальных элементов a, b, если они вообще в S существуют, обладает свойством перестановочности: $ab = ba$.

§ 2

Будем говорить, что в структуре с умножением S имеет место *хорошая арифметика,* если

1) в S каждый элемент, отличный от e и 0, с точностью до перестановок сомножителей однозначно разлагается в произведение конечного числа простых элементов;

2) в S для любого элемента a и произвольного элемента b, строго большего элемента a, найдутся элементы c_1 и c_2 такие, что $a = bc_1$, $a = c_2 b$.

Основная теорема. *Для того чтобы в структуре с умножением S, содержащей хотя бы один элемент, отличный от e и 0, имела место хорошая арифметика, необходимо и достаточно, чтобы в S выполнялись следующие шесть условий:*

1. Наибольший элемент e является единицей.

2. Структура с умножением S полукоммутативна.

3. В S выполняется условие обрыва возрастающих цепочек элементов.

4. В S каждый отличный от 0 простой элемент является максимальным элементом.

5. Все отличные от 0 степени каждого максимального простого элемента из S различны.

6. Между n-ой и $n+1$-ой степенью каждого максимального простого элемента из S, если эти степени не совпадают, нет промежуточных элементов.

Доказательство необходимости условий 1—6. Пусть в структуре с умножением S, содержащей хотя бы один элемент, отличный от e и 0, имеет место хорошая арифметика. Тогда в S справедливы следующие леммы:

Лемма 1. *В S выполняется условие* 1.

Доказательство. Так как в S каждый элемент, отличный от e и 0, разлагается в произведение конечного числа простых элементов, а равенство $0e = e0 = 0$ всегда имеет место, то лемма 1 будет доказана, если мы покажем, что в S справедливо равенство

$$ae = ea = a, \tag{1}$$

где элемент a равен или произвольному отличному от нуля простому элементу p, или элементу e.

Пусть $a = e$. Если бы было $e^2 < e$, то, так как в S каждый элемент, отличный от e, меньше некоторого простого элемента, элемент e^2 также должен был бы быть меньше некоторого простого элемента, чего быть не может.

Пусть $a = p$, где p — произвольный отличный от 0 простой элемент из S. Элемент e строго больше простого элемента p, следовательно, используя второе условие хорошей арифметики, мы получаем, что в S существуют элементы q_1 и q_2 такие, что $p = q_1 e$ и $p = eq_2$. Так как элемент p — простой, то $q_1 \leqslant p$ и $q_2 \leqslant p$. Но элементы q_1 и q_2 не могут быть строго меньше элемента p, ибо произведения $q_1 e$ и eq_2 меньше или равны каждому из сомножителей.

Тем самым доказано, что $q_1 = q_2 = p$, то есть доказано, что в S для любого отличного от 0 простого элемента справедливо равенство (1).

Лемма 2. *В S выполняется условие* 4.

Доказательство. Если бы отличный от 0 простой элемент p из S был строго меньше отличного от e элемента q, то, в силу второго условия хорошей арифметики, в S нашелся бы элемент h такой, что $p = qh$. Повторяя рассуждение, приведенное в конце доказательства леммы 1, мы показали бы, что $h = p$. Таким образом, простой элемент p разлагался бы в произведение двух элементов, отличных от e, что противоречит первому условию хорошей арифметики.

Лемма 3. *Если в S существует нулевой элемент, то в S существует нильпотентный простой элемент.*

Доказательство. Если в S нуль является простым элементом, то лемма справедлива. Допустим поэтому, что 0 — непростой элемент. Тогда существуют такие элементы a и b, отличные от e и 0, что $ab = 0$.

Пусть $a = p'_1 \dots p'_n$ и $b = p''_1 \dots p''_m$ есть разложение элементов a и b на простые множители. Следовательно,

$$p'_1 \dots p'_n p''_1 \dots p''_m = 0.$$

Таким образом, 0 разлагается в произведение конечного числа простых элементов. Это разложение неоднозначно, и мы из всех таких разложений выберем такое, у которого число простых множителей наименьшее. Пусть

$$0=p_1\dots p_r \tag{1}$$

такое разложение. Покажем, что $p_1=p_2=\dots=p_r$. Предположим, что это не так. Тогда найдется такое натуральное число k, $1<k\leqslant r$, что в правой части равенства (1) все $p_i=p_1$, для $i=1,\dots,k-1$, а $p_k\neq p_1$. Таким образом, равенство (1) можно переписать в виде

$$0=p_1^{k-1}p_k\dots p_r.$$

В силу леммы 2, $p_1\cup p_k=e$. Отсюда, так как e является единицей, по лемме, доказанной в § 1, следует, что $p_1^{k-1}\cup p_k=e$. Откуда получаем

$$p_k\dots p_r=ep_k\dots p_r=(p_1^{k-1}\cup p_k)p_k\dots p_r=p_k^2\dots p_r. \tag{2}$$

Ввиду того, что в разложении (1) число простых множителей наименьшее, элемент $c=p_k\dots p_r\neq 0$. Следовательно, равенство (2) противоречит однозначности разложения элемента c на простые множители.

Лемма 4. *Если в S существует непростой нулевой элемент, то в S существует единственный простой элемент, который является нильпотентным элементом и каждый элемент из S равен некоторой степени этого простого элемента.*

Доказательство. Существование в S нильпотентного простого элемента следует из леммы 3. Так как по лемме 2 каждый простой элемент из S является максимальным элементом, то нильпотентный простой элемент является единственным простым элементом в S.

Вторая часть леммы следует из того, что в S имеет место разложение каждого элемента, отличного от e и 0, на простые множители, а элементы e и 0 можно представить в виде: $e=p^0$, $0=p^k$, где k — показатель нильпотентности элемента p.

Лемма 5. *В S выполняется условие* 2.

Доказательство. Прежде всего покажем, что в S каждый максимальный элемент является простым элементом. В самом деле, если бы в S существовал непростой максимальный элемент g, то в S существовали бы элементы a и b такие, что $ab\leqslant g$, $a\not\leqslant g$, $b\not\leqslant g$. Откуда следовало бы: $e^2=(g\cup a)(g\cup b)\leqslant g$, что противоречит тому, что в S, по лемме 1, элемент e является единицей.

Пусть p_1 и p_2 — произвольная пара максимальных элементов из S. Если $p_1=p_2$, то равенство $p_1p_2=p_2p_1$ всегда имеет место. Поэтому можно предположить, что $p_1\neq p_2$. Тогда элемент $q=p_1\cap p_2$ будет строго меньше элемента p_1. В силу второго условия хорошей арифметики в S существует элементы h_1 и h_2 такие, что $q=h_1p_1$, $q=p_1h_2$. Но $q=h_1p_1=p_1h_2<p_2$ и так как элемент p_2 — простой, а элемент

$p_1 \nleqslant p_2$, то $h_1 \leqslant p_2$ и $h_2 \leqslant p_2$. Следовательно, $q \leqslant p_1 p_2$, $q \leqslant p_2 p_1$. Так как обратные включения всегда имеют место, то $q = p_1 p_2 = p_2 p_1$. Тем самым лемма 5 доказана.

Из леммы 5 следует, что в структуре с умножением S каждый элемент, отличный от e и 0, с точностью до перестановок сомножителей однозначно разлагается в произведение конечного числа степеней различных простых элементов.

Лемма 6. *Пусть в S элемент b, отличный от e, больше элемента a, отличного от 0. Тогда, если разложение элемента a в произведение степеней различных простых элементов имеет вид: $a = p_1^{n_1} \dots p_k^{n_k}$, то разложение элемента b в произведение степеней различных простых элементов имеет вид: $b = p_1^{m_1} \dots p_k^{m_k}$, причем $0 \leqslant m_i \leqslant n_i$, $i = 1, \dots, k$; нулевая степень максимального простого элемента полагается равной e.*

После доказательства леммы 5 лемма 6 непосредственно следует из того, что в S имеет место хорошая арифметика.

Из леммы 6 следует, что в S выполняется условие 3.

Из леммы 4 и 6 следует, что в S выполняется условие 6.

Действительно, если $p^{n+1} \neq 0$, то условие 6 следует из леммы 6. Если же $p^{n+1} = 0$, то условие 6 следует из леммы 4.

Условие 5 следует из однозначности разложения элементов из S, отличных от e и 0, на простые множители.

Таким образом, необходимость выполнения в структуре с умножением S, содержащей хотя бы один элемент, отличный от e и 0, условий 1—6 для того, чтобы в ней имела место хорошая арифметика, полностью доказана.

§ 3

Доказательство достаточности условий 1—6. Пусть в структуре с умножением S выполняются условия 1—6. Тогда в S справедливы следующие леммы:

Лемма 7. *В S каждый максимальный элемент является простым элементом.*

Так как в S выполняется условие 1, то доказательство леммы 7 проводится дословно так, как было проведено доказательство первой части леммы 5.

В силу того, что в S выполняется условие 1, мы можем нулевую степень любого максимального простого элемента из S считать равной e; при этом условия 5 и 6 останутся справедливы и для нулевой степени максимального простого элемента.

Лемма 8. *Если в S элемент q больше какой-либо степени максимального простого элемента p, то есть $p^n \leqslant q$, то элемент q равен некоторой степени элемента p.*

Доказательство. Элемент $q \leqslant e = p^0$. Пусть k — наибольшее число, при котором $q \leqslant p^k$, $k \geqslant 0$, и пусть m — наименьшее число, при котором $p^m \leqslant q$, $m \leqslant n$. Для доказательства леммы нужно пока-

зать, что $m=k$. Допустим противное, то есть допустим, что $k<m$. Тогда мы будем иметь: $p^m<q<p^k$. В силу условия 6, $m\neq k+1$. Из специального выбора чисел k и m следует, что $p^{k+1}\not\leqslant q$ и $q\not\leqslant p^{k+1}$. Отсюда, используя 6, получаем $p^{k+1}\cup q=p^k$. Умножив обе части последнего равенства на элемент p^{m-k-1}, мы получим, что

$$p^m\cup p^{m-k-1}q=p^{m-1}.$$

Так как $p^m<q$, то и элемент $p^{m-1}=p^m\cup p^{m-k-1}q\leqslant p$, что противоречит выбору числа m.

Лемма 9. *В S каждая степень простого элемента является примарным элементом.*

Доказательство. Если элемент q равен простому нулевому элементу или нулевой степени максимального простого элемента, то он, очевидно, будет примарным элементом. Поэтому предположим, что $q=p^n$, где p — отличный от 0 простой элемент, $n\neq 0$. В силу условия 4, элемент p — максимальный простой элемент. Пусть произведение $a'b'\leqslant p^n$ и один из множителей, например элемент b', не меньше элемента p^n, то есть $b'\not\leqslant p^n$. Тогда для элементов $a=a'\cup p^n$ и $b=b'\cup p^n$ также имеет место включение: $ab\leqslant p^n$. По условию элемент $b>p^n$, а элемент $a\geqslant p^n$. Из леммы 8 следует, что $a=p^m$ и $b=p^k$, причем $m\leqslant n$, $k<n$. Элемент p^m не может равняться e, ибо из условия $p^m=e$ следовало бы $p^mp^k=p^k>p^n$, что противоречило бы тому, что $p^mp^k\leqslant p^n$. Следовательно, некоторая степень элемента p^m меньше или равна элементу p^n. Тем более некоторая степень элемента a' меньше или равна элементу p^n. Лемма доказана.

Лемма 10. *В S каждый элемент, отличный от e и 0, с точностью до перестановок сомножителей однозначно разлагается в произведение конечного числа простых элементов.*

Доказательство. В силу того, что в S выполняется условие обрыва возрастающих цепочек элементов, доказательство леммы можно вести по индукции сверху.

Из леммы 7 и условия 5 следует, что лемма справедлива для максимальных элементов. Поэтому предположим, что лемма верна для всех элементов, строго больших элемента c, отличного от 0, и докажем, что лемма верна и для элемента c. По условию 4 элемент c — непростой. Следовательно, найдутся элементы a' и b' такие, что $a'\not\leqslant c$, $b'\not\leqslant c$, а $a'b'\leqslant c$. Тогда для элементов $a=a'\cup c$ и $b=b'\cup c$ также выполняется включение: $ab\leqslant c$.

В S выполняется условие 1. Следовательно, элементы a и b, строго большие элемента c, не равны e. По предположению элементы a и b можно однозначно разложить в произведение конечного числа простых элементов, которые, в силу условия 4, являются максимальными элементами. Пусть $a=p_1\dots p_n$, $b=p'_1\dots p'_m$ такое разложение. Тогда

$$p_1\dots p_np'_1\dots p'_m\leqslant c. \qquad (1)$$

В силу полукоммутативности S левая часть включения (1) равняется произведению степеней различных простых элементов. Таким образом, включение (1) можно записать в виде

$$p_1^{n_1} \dots p_r^{n_r} \leqslant c. \tag{2}$$

По лемме 8 элементы $p_i^{n_i} \cup c \geqslant p_i^{n_i}$ равны $p_i^{m_i}$, где $m_i \leqslant n_i$. Из включения (2) следует включение

$$p_1^{m_1} \dots p_r^{m_r} \leqslant c. \tag{3}$$

Некоторые из элементов $p_i^{m_i}$ могут равняться e. В силу полукоммутативности S мы можем предположить, что первые $k \geqslant 1$ элементов $p_i^{n_i}$ не равны e, а остальные равны e. Так как e является единицей, то из включения (3) следует включение:

$$p_1^{m_1} \dots p_k^{m_k} \leqslant c. \tag{4}$$

Каждый элемент $p_i^{m_i}$, $i=1, \dots, k$, больше или равен элементу c, поэтому

$$c \leqslant p_1^{m_1} \cap \dots \cap p_k^{m_k}. \tag{5}$$

Так как в S сумма любой пары различных простых элементов, отличных от 0, в силу условия 4, равна единице e и в S выполняется условие 2, то из леммы, доказанной в § 1, следует, что в S произведение конечного числа степеней различных простых элементов равно их пересечению.

Таким образом, левая часть включения (4) равна правой части включения (5). Следовательно,

$$c = p_1^{m_1} \dots p_k^{m_k}. \tag{6}$$

Тем самым доказано, что элемент c разлагается в произведение конечного числа простых элементов.

Докажем, что разложение (6) с точностью до перестановок сомножителей определяется однозначно. Пусть имеется два разложения элемента c на простые множители: $c = p_1^{m_1} \dots p_k^{m_k}$ и $c = p_1'^{n_1} \dots p_t'^{n_t}$. Следовательно,

$$p_1^{m_1} \dots p_k^{m_k} = p_1'^{n_1} \dots p_t'^{n_t}. \tag{7}$$

В силу полукоммутативности S мы можем предположить, что левая и правая часть равенства (7) есть произведение степеней различных простых элементов.

Из условия 4 следует, что каждый простой множитель из одной части равенства (7) равен одному из простых множителей из другой части равенства (7). Следовательно, $k=t$ и, не нарушая общности, мы можем предположить, что $p_i = p_i'$, $i=1, \dots, k$.

Предположим теперь, что для некоторого i простой множитель p_i входит в одну из частей равенства (7) в меньшей степени, чем

в другую, например для $i=1$, $m_1 < n_1$. Тогда, в силу условия 5, элемент $p_1^{n_1}$ должен быть строго меньше элемента $p_1^{m_1}$. Но из равенства (7) следует, что элемент $p_1^{n_1}$ больше произведения $p_1^{m_1} \dots p_k^{m_k}$ и так как, по условию 4, элемент $p_1^{n_1}$ не может быть больше никакой степени элемента $p_2^{m_2} \dots p_k^{m_k}$, то предположение о том, что $p_1^{n_1} < p_1^{m_1}$ противоречит тому, что элемент $p_1^{n_1}$, по лемме 9, является примарным элементом.

Таким образом, лемма 10 доказана. Тем самым доказано, что в S выполняется первое условие хорошей арифметики.

Аналогично тому, как мы доказывали в лемме 10 единственность разложения каждого элемента, отличного от e и 0, на простые множители, можно показать, что в S справедлива лемма 6.

Из первого условия хорошей арифметики, леммы 6, условий 1 и 2 следует, что в S выполняется и второе условие хорошей арифметики.

Таким образом, основная теорема полностью доказана.

Следствие. *Если в структуре с умножением S имеет место хорошая арифметика, то в ней выполняется закон дистрибутивности*

$$(a \cup b) \cap c = (a \cap c) \cup (b \cap c).$$

Это следствие легко вытекает из леммы 6 и условия 2.

§ 4

В этом параграфе будут построены примеры, показывающие независимость всех шести условий основной теоремы.

1. S является структурой с умножением идеалов алгебры с тремя образующими e, a и b над простым полем характеристики 2 и с таблицей умножения:

	e	a	b
e	e	a	b
a	a	0	0
b	b	0	0

В S выполняются условия 1—5 и не выполняется условие 6.

2. S является структурой с умножением идеалов алгебры с двумя образующими e и a над простым полем характеристики 2 и с таблицей умножения:

	e	a
e	e	a
a	a	a

В S выполняются условия 1—4 и 6 и не выполняется условие 5.

3. S является структурой с умножением идеалов двусторонней прямой суммы двух колец целых чисел.

В S выполняются условия 1—3, 5 и 6 и не выполняется условие 4.

4. На вполне упорядоченном счетном бесконечном множестве с последним элементом

$$0 = x_0 < x_1 < \ldots < x_n < \ldots < e$$

определим умножение: $e^2 = e$, $ex_i = x_i e = x_i$, $x_i x_j = 0$, для любых i и j.

В полученной структуре с умножением S выполняются условия 1, 2, 4—6, так как в S нет ни простых, ни максимальных элементов, и не выполняется условие 3.

5. Пусть S будет свободная ассоциативная полугруппа с двумя образующими p_1 и p_2 и с единицей $e = p_1^0 = p_2^0$. Таким образом, произвольный элемент a из S имеет вид

$$a = p_1^{\alpha_1} p_2^{\beta_1} p_1^{\alpha_2} p_2^{\beta_2} \ldots p_1^{\alpha_n} p_2^{\beta_n},$$

где α_i, $i = 2, \ldots n$, β_j, $j = 1, \ldots n-1$, — натуральные числа, а целые положительные числа α_1 и β_n могут равняться нулю.

В S следующим образом введем отношение порядка:

Единица e больше любого элемента a из S.

Элемент b мы будем называть *уменьшением* элемента a, а элемент a будем называть *увеличением* элемента b, если существует хотя бы одна конечная цепочка элементов

$$a = c_0, c_1, \ldots, c_k = b$$

такая, что элемент c_i получается из элемента c_{i-1} заменой в нем множителя $p_1 p_2$ на $p_2 p_1$, то есть если $c_{i-1} = p_1^{\alpha_1} p_2^{\beta_1} \ldots p_1^{\alpha_j} p_2^{\beta_j} \ldots p_1^{\alpha_n} p_2^{\beta_n}$, то элемент

$$c_i = p_1^{\alpha_1} p_2^{\beta_1} \ldots p_1^{\alpha_j - 1} p_2 p_1 p_2^{\beta_j - 1} \ldots p_1^{\alpha_n} p_2^{\beta_n}.$$

Элемент a больше элемента b, если существует такой элемент a', являющийся уменьшением элемента a, что $b = b_1 a' b_2$, где элементы b_1 и b_2 могут равняться e.

Такое определение отношения порядка, очевидно, эквивалентно следующему:

Элемент a больше элемента b, если существует такой элемент b', являющийся увеличением элемента b, что $b' = b_1' a b_2'$, где элементы b_1' и b_2' могут равняться e.

Легко проверить, что множество S, с введенным отношением порядка, является частично упорядоченным множеством.

Можно показать, что частично упорядоченное множество S, с имеющейся в нем операцией умножения, является структурой с умножением, в которой выполняются условия 1, 3—6 и не выполняется условие 2.

6. S является структурой с умножением идеалов двусторонней прямой суммы произвольного поля P и кольца R с нулевым умножением, построенного на аддитивной группе простого порядка.

В S выполняются условия 2—6 и не выполняется условие 1.

§ 5

Подструктура S структуры двусторонних идеалов некоторого кольца называется *замкнутой подструктурой,* если

1) в S вместе с двусторонними идеалами A и B содержится их произведение AB.

2) в S вместе с двусторонним идеалом A содержатся все двусторонние идеалы, содержащие A.

Замкнутая подструктура структуры двусторонних идеалов ассоциативного кольца, очевидно, является структурой с умножением. Таким образом, условия 1—6 основной теоремы являются необходимыми и достаточными условиями для того, чтобы в ассоциативном кольце, содержащем хотя бы один собственный двусторонний идеал, имела место хорошая арифметика для двусторонних идеалов из определенной замкнутой подструктуры; в частности, для того, чтобы в кольце имела место хорошая арифметика для *всех* двусторонних идеалов.

Двусторонние идеалы, рассматривавшиеся в работах А. И. Узкова [4] и К. Асано [5], составляют замкнутые подструктуры. Правда, в общем случае определение хорошей арифметики, данное в нашей работе, является более узким, чем то, которым пользовались Узков и Асано — пример 5 предыдущего параграфа обладает, как можно проверить, хорошей арифметикой в смысле Узкова, но не обладает хорошей арифметикой в нашем смысле. Однако в тех случаях, которые рассматривались в работах Узкова и Асано, полукоммутативность изучавшихся замкнутых подструктур двусторонних идеалов была доказана, а поэтому условия 1—6 основной теоремы настоящей работы могут и в этих случаях служить в качестве необходимых и достаточных условий.

Если кольцо коммутативное, то из наших условий 1—6 легко выводятся условия, указанные в работах Мория и Кобаяси [2], и обратно.

§ 6

Аналогично тому, как в § 8 работы Андрунакиевича [10], было определено понятие присоединенного идеала коммутативного кольца, можно в случае произвольного кольца ввести понятие *двустороннего присоединенного идеала.*

Почти дословно повторяя доказательство, приведенное в § 8 работы (10), можно показать, что множество двусторонних присоединенных идеалов ассоциативного кольца является структурой с умножением. Так как для двусторонних присоединенных идеалов, как легко проверить, справедлива теорема 8 работы [10], то для произвольного кольца верна теорема 2, сформулированная в нашей работе [6]: *Множество всех двусторонних присоединенных идеалов и множество всех отмеченных идеалов кольца R составляют изоморфные структуры;* определение отмеченного идеала см. в работе [6].

Из результатов работы Фостера [11] следует, что если кольцо R обладает единицей, то в нем структура с умножением двусторонних идеалов изоморфна как структура с умножением структуре с умножением двусторонних присоединенных идеалов.

Простой пример показывает, что в кольцах без единицы последнее утверждение вообще не верно.

Действительно, в кольце четных чисел идеал (6) является, как легко проверить, отмеченным идеалом, а его квадрат, идеал (36), не является отмеченным идеалом. Таким образом, в кольце четных чисел, структура отмеченных идеалов не является даже структурой с умножением.

Однако справедлива следующая теорема:

Теорема 1. *Если в кольце R структура отмеченных идеалов S является структурой с умножением, то она изоморфна, как структура с умножением, структуре с умножением двусторонних присоединенных идеалов S этого кольца.*

Доказательство. В силу теоремы 2 работы [6] структура S изоморфна структуре S^*. Поэтому нам остается показать, что если отмеченным идеалам A и B соответствуют двусторонние присоединенные идеалы A^* и B^*, то отмеченному идеалу AB соответствует двусторонний присоединенный идеал $A^* \circ B^*$.

В самом деле, пусть отмеченному идеалу AB соответствует двусторонний присоединенный идеал $(AB)^*$, а двустороннему присоединенному идеалу $A^* \circ B^*$ соответствует отмеченный идеал C. Рассмотрим фактор-кольцо кольца R по отмеченному идеалу ABC. Кольцо $\bar{R} = \frac{R}{ABC}$ обладает единицей. Поэтому в кольце $\bar{R}$ структура с умножением двусторонних присоединенных идеалов изоморфна как структура с умножением, структуре двусторонних идеалов. Следовательно, в $\bar{R}$ гомоморфные образы $\overline{AB}$ и $\bar{C}$ отмеченных идеалов AB и C совпадают. Так как $ABC \subset C$ и $ABC \subset AB$, то из равенства $\overline{AB} = \bar{C}$ следует равенство $AB = C$. Откуда, в силу взаимно-однозначного соответствия между двусторонними присоединенными идеалами и отмеченными идеалами кольца R, $A^* \circ B^* = (AB)^*$.

В то время как в коммутативном случае наличие единицы является необходимым условием для того, чтобы в кольце имела место хорошая арифметика для идеалов [см. работу (2)], в некоммутативном случае существуют кольца с хорошей арифметикой для двусторонних идеалов, не имеющие единицы.

Пример: Кольцо R равно полупрямой сумме

$$R = R_1 + R_2,$$

где R_1 — простое кольцо без единицы, а R_2 — кольцо с нулевым умножением, построенное на аддитивной группе кольца R_1. Элементы кольца R_1 будем обозначать через $a, b, \ldots$, а соответствующие элементы

кольца R_2 — через $\bar{a}, \bar{b}, \ldots$. Умножение элементов кольца R_1 на элементы кольца R_2 определим следующим образом: $a\bar{b}=\overline{ab}$; $\bar{b}a=\overline{ba}$. Кольцо R имеет единственный собственный двусторонний идеал R_2, квадрат которого равен нулю. В R выполняются равенства:

$$R^2=R; \quad RR_2=R_2R=R_2.$$

Таким образом, в кольце R имеет место хорошая арифметика для двусторонних идеалов. Заметим, что кольцо R не имеет ни одного собственного двустороннего присоединенного идеала.

Тем не менее справедлива следующая теорема:

Теорема 2. *Если в ассоциативном кольце R, содержащем хотя бы один собственный двусторонний идеал, имеет место хорошая арифметика для двусторонних идеалов, то структура отмеченных идеалов кольца R является замкнутой подструктурой структуры двусторонних идеалов этого кольца.*

Доказательство. Очевидно, что если двусторонний идеал J является отмеченным идеалом, то все двусторонние идеалы, содержащие J, также будут отмеченными идеалами.

Теперь докажем, что если в кольце R двусторонние идеалы A и B являются отмеченными идеалами, то и их произведение AB будет отмеченным идеалом.

Если отмеченные идеалы A и B равны отмеченному идеалу R, который, в силу условия 1 основной теоремы, удовлетворяет равенству $R^2 = R$, то наше утверждение справедливо. Отсюда следует, что если структура отмеченных идеалов кольца R состоит из одного элемента R, то теорема 2 верна. Поэтому можно предположить, что в кольце R существуют отличные от R отмеченные идеалы. Тогда в R существуют отмеченные простые идеалы, отличные от R. Для доказательства нашего утверждения для отмеченных идеалов, отличных от R, покажем прежде всего, что все степени простого отмеченного идеала P из R будут отмеченными идеалами.

Доказательство этого утверждения будем вести по индукции. По предположению, простой идеал P является отмеченным идеалом. Допустим, что уже доказано, что двусторонний идеал P^n является отмеченным идеалом и докажем, что тогда двусторонний идеал P^{n+1} также будет отмеченным идеалом.

Рассмотрим фактор-кольцо $\bar{R} = \frac{R}{P^{n+1}}$. Так как в R имеет место хорошая арифметика для двусторонних идеалов, то в нем выполняется равенство $RJ=JR=J$, где J — произвольный двусторонний идеал из R, следовательно в $\bar{R}$ для любого двустороннего идеала $\bar{J}$ справедливо равенство

$$\bar{R}\bar{J}=\bar{J}\bar{R}=\bar{J}. \tag{1}$$

Двусторонний идеал $\overline{P}^n$, по предположению, является отмеченным идеалом, следовательно, фактор-кольцо $\frac{\overline{R}}{\overline{P}^n}$ обладает единицей. Полным прообразом этой единицы в кольце R будет двусторонний присоединенный идеал $(\overline{P}^n)^*$. Покажем, что в $(\overline{P}^n)^*$ существует идемпотентный элемент.

Действительно, пусть $\overline{e}_1$ — произвольный элемент из $(\overline{P}^n)^*$. Элемент $\overline{e}_1$ отображается на единицу кольца $\frac{\overline{R}}{\overline{P}^n}$, следовательно, $\overline{e}_1^2=\overline{e}_1+\overline{u}$, где $\overline{u}$ — элемент из $\overline{P}^n$. Очевидно, что $\overline{e}_1\overline{u}=\overline{u}\overline{e}_1$. Оттуда, как легко проверить, учитывая, что $(\overline{P}^n)^2=0$, так как $P^{2n}\subseteq P^{n+1}$, элемент $\overline{e}=\overline{e}_1-2\overline{e}_1\overline{u}+\overline{u}$ является идемпотентным элементом, содержащимся в $(\overline{P}^n)^*$.

Элемент $\overline{e}$ отображается на единицу кольца, $\overline{R}/\overline{P}^n$, следовательно для любого элемента $\overline{x}$ из $\overline{R}$ имеют место равенства:

$$\overline{e}\,\overline{x}=\overline{x}+\overline{z}_1 \tag{2}$$

$$\overline{x}\,\overline{e}=\overline{x}+\overline{z}_2, \tag{3}$$

где $\overline{z}_1$ и $\overline{z}_2$ — элементы из $\overline{P}^n$. Покажем, что $\overline{z}_1=\overline{0}$. Умножив обе части равенства (2) на элемент $\overline{e}$, мы получим

$$\overline{e}^2\overline{x}=\overline{e}\,\overline{x}=\overline{e}\overline{x}+\overline{e}\overline{z}_1,$$

то есть $\overline{e}\overline{z}_1=\overline{0}$.

В силу равенства (3), произвольный элемент $a\in\overline{R}$ можно представить в виде: $\overline{a}=\overline{a}\overline{e}-\overline{z}$, где $\overline{z}$ — элемент из $\overline{P}^n$. Так как $\overline{e}\overline{z}_1=\overline{0}$ и $(\overline{P}^n)^2=\overline{0}$, то $\overline{a}\overline{z}_1=\overline{a}\,\overline{e}\overline{z}_1-\overline{z}\overline{z}_1=0$. Следовательно, элемент $\overline{z}_1$ является полным правым делителем нуля кольца $\overline{R}$. Если бы было $\overline{z}_1\neq\overline{0}$, то для двустороннего идеала $(\overline{z}_1)$ выполнялось бы равенство $\overline{R}(\overline{z}_1)=\overline{0}$, что противоречит равенству (1). Таким образом, $\overline{z}_1=\overline{0}$ и, следовательно, элемент $\overline{e}$ является левой единицей кольца $\overline{R}$.

Аналогично доказывается, что $\overline{e}$ является правой единицей кольца $\overline{R}$. Таким образом, доказано, что двусторонний идеал P^{n+1} является отмеченным идеалом.

Тем самым наше утверждение о том, что все степени простого отмеченного идеала являются отмеченными идеалами, доказано.

Пусть двусторонний идеал $C=AB$, причем двусторонние идеалы A и B — отмеченные идеалы. Так как в кольце R имеет место хорошая арифметика для двусторонних идеалов, то двусторонние идеалы A и B можно разложить в произведение степеней различных простых идеалов, которые будут, очевидно, отмеченными идеалами. Следовательно, двусторонний идеал C также можно разложить в произведение степеней различных простых отмеченных идеалов. Но, как было замечено при доказательстве леммы 10, § 3, в кольце R с хорошей арифметикой для двусторонних идеалов произведение степеней различных про-

стых идеалов равно их пересечению. Таким образом, двусторонний идеал C равен пересечению конечного числа отмеченных идеалов. Отсюда, используя теорему 2 работы [6], мы получим, что двусторонний идеал C является отмеченным идеалом. Теорема доказана.

С помощью теорем 1 и 2 можно легко доказать следующую теорему:

Теорема 3. *Если в ассоциативном кольце R имеет место хорошая арифметика для двусторонних идеалов, то в нем имеет место хорошая арифметика и для двусторонних присоединенных идеалов.*

Действительно, если в R нет ни одного собственного двустороннего присоединенного идеала, то теорема справедлива. Поэтому можно предположить, что в R существует собственный двусторонний присоединенный идеал. Тогда в R существует хотя бы один собственный отмеченный идеал. Отсюда, в силу теоремы 2, следует, что структура отмеченных идеалов кольца R является замкнутой подструктурой структуры двусторонних идеалов этого кольца, следовательно, является структурой с умножением.

Так как в R имеет место хорошая арифметика для двусторонних идеалов, то в замкнутой подструктуре отмеченных идеалов также имеет место хорошая арифметика. Откуда, в силу теоремы 1, следует, что в кольце R имеет место хорошая арифметика и для двусторонних присоединенных идеалов.

ЛИТЕРАТУРА

1. Б. Л. Ван дер Варден, Современная алгебра, Гостехиздат, 1947.

2. M. Moriya und Y. Kobayasi, Eine notwendige Bedingung für die eindeutige Primfactorzerlegung der Ideale in einem kommutativen Ring, Proc. Imp. Acad. Tokyo, 17 (1914), 129—133.

3. Y. Kobayasi und M. Moriya, Eine hinreichende Bedingung für die eindeutige Primfactorzerlegung der Ideale in einem kommutativen Ring, Proc. Imp. Acad. Tokyo, 17 (1941), 129—133.

4. А. И. Узков, Абстрактное обоснование брандтовой теории идеалов, Матем. сборник 6 (1939), 263—281.

5. K. Asano, Arithmetische Idealtheorie in nichtkommutativen Ringen, Jap. J. Math., 15 (1939), 1—36.

6. Е. Г. Шульгейфер, Мультипликативная теория присоединенных идеалов в коммутативных кольцах, ДАН СССР 54 (1949), 633—636.

7. W. Krull, Zur Theorie der zweiseitigen Ideale in nichtkommutativen Bereichen, Math. Zeitschrift, 28 (1928), 481—503.

8. M. Ward and R. Dilworth, Residuated lattices, Trans. Am. Math. Soc. 45 (1939), 335—354.

9. G. Birkhoff, Lattice theory, Revised ed., N. Y., 1948.

10. В. А. Андрунакиевич, Полурадикальные кольца, Изв. Ак. наук СССР (Сер. мат.), 12 (1948), 129—178).

11. A. L. Foster, The idempotent elements of a commutative ring form a boolean algebra, ring duality, and transformation theory, Duke Math. J. 12 (1945), 143—152.

Поступило 27. V 1950 г.