ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЭЛЕМЕНТЫ

Развитие теории идеалов имеет с исторической точки зрения два источника: теорию алгебраических чисел и теорию идеалов в кольцах многочленов. Обе эти теории, однако, возникли из совершенно различных по своей постановке задач. В то время как основной задачей теории идеалов в кольцах многочленов является определение корней и установление необходимых и достаточных условий для принадлежности некоторого многочлена заданному идеалу, в теории целых алгебраических чисел исходным является вопрос о разложении на множители. К этому вопросу можно прийти, например, в следующих рассмотрениях.

В кольце чисел $a+b\sqrt{-5}$, где a и b — целые рациональные числа, не имеет места теорема об однозначности разложения элементов на множители. Например, число 9 обладает двумя существенно различными разложениями на простые [1]) множители:

$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5}).$$

Это обстоятельство побудило Дедекинда расширить область рассматриваемых элементов до области идеалов (так им впервые были названы эти объекты; Дедекинд следовал за Куммером, который добился однозначности разложения на простые множители в полях деления круга с помощью введения некоторых «идеальных чисел»). Ему удалось показать, что в этой области каждый идеал равен однозначно определенному произведению простых идеалов. Действительно, если в указанном выше примере ввести простые идеалы

$$\mathfrak{p}_1=(3,\ 2+\sqrt{-5}),\ \mathfrak{p}_2=(3,\ 2-\sqrt{-5}),$$

---

[1]) Числа 3 и $2\pm\sqrt{-5}$ неразложимы: это следует из того, что их норма (ср. § 47) равна 9. Если бы они были разложимы, то либо оба сомножителя имели бы норму ± 3, либо один из них норму ± 1. Но чисел вида $a+b\sqrt{-5}$ с нормой ± 3 не существует, так как иначе было бы

$$a^2+5b^2=\pm 3,$$

что в области целых чисел невозможно. Числом же с нормой ± 1 обязательно является один из обратимых элементов ± 1, так как

$$a^2+5b^2=\pm 1$$

может выполняться лишь при $a=\pm 1$, $b=0$.

то, как легко подсчитать,

$$(3)=\mathfrak{p}_1\mathfrak{p}_2;\quad (2+\sqrt{-5})=\mathfrak{p}_1^2;\quad (2-\sqrt{-5})=\mathfrak{p}_2^2,$$

откуда для главного идеала (9) получается (единственное) разложение

$$(9)=\mathfrak{p}_1^2\mathfrak{p}_2^2.$$

В этой главе будет изложена классическая (дедекиндова) теория идеалов целых элементов в модернизованной аксиоматической форме, предложенной Э. Нётер [1]).

§ 134. Конечные $\mathfrak{R}$-модули

Мы рассматриваем здесь модули над некоторым (не обязательно коммутативным) кольцом $\mathfrak{R}$, т. е. модули, для которых кольцо $\mathfrak{R}$ является областью левых мультипликаторов. В большинстве рассматриваемых случаев модули содержатся либо в $\mathfrak{R}$ (и, таким образом, являются левыми идеалами в $\mathfrak{R}$), либо в некотором кольце $\mathfrak{S}$, содержащем данную область мультипликаторов $\mathfrak{R}$.

Под *конечным* $\mathfrak{R}$-*модулем* подразумевается такой модуль $\mathfrak{M}$, который порождается конечным *базисом* $(a_1, \ldots, a_h)$, или, иначе, элементы которого могут быть выражены как линейные комбинации фиксированных элементов $a_1, \ldots, a_h$ с целочисленными коэффициентами и коэффициентами из $\mathfrak{R}$:

$$m=r_1a_1+\ldots+r_ha_h+n_1a_1+\ldots+n_ha_h,$$
$$(r_\nu\in\mathfrak{R},\quad n_\nu-\text{целые числа}). \qquad (1)$$

В этом случае пишут $\mathfrak{M}=(a_1, \ldots, a_h)$.

Говорят, что для модуля $\mathfrak{M}$ выполнена *теорема о цепях делителей*, если каждая цепь подмодулей $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ в $\mathfrak{M}$, где каждый предыдущий член является собственным подмодулем следующего члена (т. е. последующий является «делителем» предыдущего):

$$\mathfrak{M}_1\subset\mathfrak{M}_2\subset\ldots,$$

обрывается после конечного числа шагов.

Теорема. *Если в модуле $\mathfrak{M}$ выполнена теорема о цепях делителей, то каждый подмодуль в $\mathfrak{M}$ имеет конечный базис и наоборот.*

Эта теорема является обобщением теоремы из § 115 о базисе идеала и теоремы о цепях делителей. Доказательство в данном случае совершенно аналогично. Чтобы найти базис для произвольно выбранного подмодуля $\mathfrak{N}$, нужно взять в $\mathfrak{R}$ какой-нибудь элемент a_1. Если $(a_1)=\mathfrak{N}$, то больше доказывать нечего; в про-

---

[1]) Noether E. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.—Math. Ann., 1926, 96, S. 26—61.

тивном случае выберем в $\mathfrak{N}$ элемент a_2, не принадлежащий подмодулю (a_1). Если $(a_1, a_2) = \mathfrak{N}$, то опять-таки больше доказывать нечего; в противном случае выберем следующий элемент a_3 и т. д. Если известно, что цепь модулей

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

обрывается, то $\mathfrak{N}$ обладает конечным базисом.

Обратно, если каждый подмодуль в $\mathfrak{M}$ обладает конечным базисом и

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \ldots$$

— цепь подмодулей в $\mathfrak{M}$, то объединение $\mathfrak{B}$ всех $\mathfrak{M}_\nu$ — тоже подмодуль, обладающий по условию конечным базисом:

$$\mathfrak{B} = (a_1, \ldots, a_r).$$

Все a_ν, однако, содержатся уже в некотором $\mathfrak{M}_\omega$, участвующем в данной цепи; следовательно, $\mathfrak{B} \subseteq \mathfrak{M}_\omega$, откуда $\mathfrak{B} = \mathfrak{M}_\omega$. Таким образом, цепь обрывается на $\mathfrak{M}_\omega$.

О том, при каких условиях в модуле $\mathfrak{M}$ выполняется теорема о цепях делителей, говорит следующая

Теорема. *Если в кольце $\mathfrak{R}$ имеет место теорема о цепях делителей для левых идеалов и $\mathfrak{M}$ — произвольный конечный $\mathfrak{R}$-модуль, то в $\mathfrak{M}$ имеет место теорема о цепях делителей для $\mathfrak{R}$-модулей.*

Вот утверждение, равносильное этому (в силу предыдущей теоремы):

Если в $\mathfrak{R}$ каждый левый идеал обладает конечным базисом и модуль $\mathfrak{M}$ обладает конечным базисом над $\mathfrak{R}$, то каждый подмодуль в $\mathfrak{M}$ имеет конечный базис над $\mathfrak{R}$.

Доказательство совершенно аналогично доказательству теоремы Гильберта о базисе (§ 115). Пусть $\mathfrak{M} = (a_1, \ldots, a_h)$ и $\mathfrak{N}$ — произвольный подмодуль в $\mathfrak{M}$. Каждый элемент из $\mathfrak{N}$ можно записать в виде (1). Если в выражении (1) среди $2h$ коэффициентов $r_1, \ldots, n_h$ последнее $2h - l$ (т. е. начиная с $(l+1)$-го и заканчивая $2h$-м) равны нулю, то мы говорим о *выражении длины* $\leqslant l$. Рассмотрим все входящие в $\mathfrak{N}$ выражения длины $\leqslant l$. Коэффициенты при l-м слагаемом в них составляют, как легко видеть, некоторый левый идеал в $\mathfrak{N}$ или в кольце $\mathbb{Z}$ целых чисел. Этот идеал обладает конечным базисом

$$(b_{l1}, \ldots, b_{ls_l}).$$

Каждый из $b_{l\nu}$ является последним (l-м) коэффициентом (r_l или n_{l-h}) некоторого выражения (1), которое мы обозначим через $B_{l\nu}$:

$$B_{l\nu} = r_1 a_1 + \ldots + b_{l\nu} a_l \quad \text{или} \quad B_{l\nu} = r_1 a_1 + \ldots + b_{l\nu} a_{l-h}.$$

Мы утверждаем теперь, что все выражения $B_{l\nu}$ ($l=1, \ldots, 2k$; $\nu=1, \ldots, s_l$) составляют базис в $\mathfrak{R}$. Действительно, каждый элемент (1) из $\mathfrak{R}$ длины l может быть освобожден от l-го коэффициента с помощью вычитания некоторой линейной комбинации элементов $B_{l1}, \ldots, B_{ls_l}$ (с коэффициентами из $\mathfrak{R}$ или $\mathbb{Z}$ — в зависимости от значения l), т. е. данное выражение (1) можно свести к выражению меньшей длины. Тем же способом полученное выражение можно изменить и еще уменьшить длину; продолжая таким образом, мы в конце концов придем к нулю. Значит, каждый элемент из $\mathfrak{R}$ может быть представлен в виде линейной комбинации элементов $B_{l\nu}$, что и требовалось доказать. Если один из идеалов $(b_{l1}, \ldots, b_{ls_l})$ окажется равным нулю, то соответствующие элементы $B_{l\nu}$ не надо включать в базис.

§ 135. Элементы, целые над кольцом

Пусть $\mathfrak{R}$ — подкольцо кольца $\mathfrak{T}$.

Элемент t из $\mathfrak{T}$ называется *целым над* $\mathfrak{R}$, если все степени[1]) t принадлежат конечному $\mathfrak{R}$-модулю вида $(a_1, \ldots, a_m)$ или если все степени t линейно выражаются через конечное множество элементов $a_1, \ldots, a_m$ кольца $\mathfrak{T}$ в виде

$$t^\rho = r_1a_1 + \ldots + r_ma_m + n_1a_1 + \ldots + n_ma_m$$
$$(r_\nu \in \mathfrak{R}, \quad n_\nu \text{ — целые числа}). \quad (1)$$

В частности, каждый элемент r из $\mathfrak{R}$ является целым над $\mathfrak{R}$, так как $r, r^2, r^3, \ldots$ принадлежат $\mathfrak{R}$-модулю (r). Конечно, и единичный элемент из $\mathfrak{T}$, если он существует, является целым над $\mathfrak{R}$.

Если $\mathfrak{T}$ — поле, которое, следовательно, содержит поле частных P кольца $\mathfrak{R}$, то степени любого целого элемента t линейно зависят от конечного множества величин $a_1, \ldots, a_m$ с коэффициентами из P, потому что P содержит не только кольцо $\mathfrak{R}$, но и единицу. Тем самым среди степеней элемента t есть лишь конечное множество линейно независимых над P; поэтому элемент t является алгебраическим над P, и вместо «целый элемент» часто говорят «*целый алгебраический элемент*».

Если $\mathfrak{R}$ — кольцо, в котором имеет место теорема о цепях делителей для левых идеалов, то, согласно § 134, она имеет место и в подмодулях конечного $\mathfrak{R}$-модуля $(a_1, \ldots, a_m)$. В частности, цепь модулей

$$(t) \subseteq (t, t^2) \subseteq \ldots$$

стабилизируется и, значит, некоторая степень элемента t линейно

[1]) Под степенями в этом параграфе подразумеваются только системы с положительными показателями.

выражается через более низкие степени:

$$t^h = r_1 t + \ldots + r_{h-1} t^{h-1} + n_1 t + \ldots + n_{h-1} t^{h-1}. \qquad (2)$$

Обратно, если t — элемент из $\mathfrak{T}$, который при выбранном подходящим образом числе h представляется в виде (2) с коэффициентами из $\mathfrak{R}$, соответственно из $\mathbb{Z}$, то с помощью (2) можно и более высокие степени элемента t выразить через конечное множество элементов t, t^2, ..., t^{h-1} и тем самым установить, что в соответствии с нашим определением элемент t является целым. Мы доказали следующее предложение:

Если в кольце $\mathfrak{R}$ имеет место теорема о цепях делителей для левых идеалов, то для того, чтобы элемент t был целым над $\mathfrak{R}$, необходимо и достаточно, чтобы выполнялось равенство вида (2).

Если $\mathfrak{T}$ — поле, то равенство (2) доставляет новое выражение того факта, что t алгебраичен над полем P. Если в $\mathfrak{R}$ есть единица, то к множеству степеней элемента t можно добавить и $t^0 = 1$, а в равенстве (2) удалить группу слагаемых $n_1 t + \ldots + n_{h-1} t^{h-1}$. Вместо (2), таким образом, получается более простое равенство:

$$t^h - r_{h-1} t^{h-1} - \ldots - r_0 = 0,$$

характерной особенностью которого является то, что коэффициент при высшей степени элемента t равен единице.

Примеры. *Целые алгебраические числа* — это алгебраические числа, являющиеся целыми над кольцом $\mathbb{Z}$ обычных целых чисел, т. е. удовлетворяющие некоторому целочисленному уравнению со старшим коэффициентом 1. *Целые алгебраические функции от x_1, ..., x_n* — это функции из некоторого алгебраического расширения поля $\mathsf{K}(x_1, \ldots, x_n)$, которые являются целыми над кольцом многочленов $\mathsf{K}[x_1, \ldots, x_n]$; при этом K является заранее фиксированным основным полем. *Абсолютно целые алгебраические функции от x_1, ..., x_n* — это функции, которые являются целыми над кольцом целочисленных многочленов $\mathbb{Z}[x_1, \ldots, x_n]$.

В любом кольце $\mathfrak{T}$ сумма, разность и произведение двух целых над $\mathfrak{R}$ элементов являются целыми. Иначе говоря, целые над $\mathfrak{R}$ элементы из $\mathfrak{T}$ составляют некоторое кольцо $\mathfrak{S}$.

Доказательство. Если все степени элемента s выражаются через a_1, ..., a_m, а все степени элемента t выражаются через b_1, ..., b_n линейно, то все степени элементов $s+t$, $s-t$ и $s \cdot t$ линейно выражаются через a_1, ..., a_m, b_1, ..., b_n, $a_1 b_1$, $a_1 b_2$, ..., $a_m b_n$.

Если предположить выполненной теорему о цепях делителей для идеалов кольца $\mathfrak{S}$, то можно доказать транзитивность свойства быть целым элементом.

Если $\mathfrak{S}$ — кольцо целых элементов коммутативного кольца $\mathfrak{T}$ (над подкольцом $\mathfrak{R}$) и t — элемент из $\mathfrak{T}$, целый над $\mathfrak{S}$, то этот элемент t является целым и над $\mathfrak{R}$ (т. е. содержится в $\mathfrak{S}$). Или, иначе: *если элемент t удовлетворяет равенству* (2) *с коэффициентами r_ν, целыми над $\mathfrak{R}$, то сам t является целым над $\mathfrak{R}$.*

Доказательство. С помощью многократного применения равенства (2) все степени $t^{h+\lambda}$ элемента t можно выразить линейно через $t, t^2, \ldots, t^{h-1}$ с коэффициентами, которые являются либо целыми числами, либо целыми рациональными функциями от произведений степеней коэффициентов r_ν. Для каждого r_ν существует конечное множество элементов из $\mathfrak{T}$, через которые r_ν линейно выражается с коэффициентами из $\mathfrak{R}$ и $\mathbb{Z}$, следовательно, все произведения степеней элементов r_ν выражаются через конечное множество произведений элементов из указанных выше конечных множеств. Умножим эти произведения, которых всего конечное число, на $t, t^2, \ldots, t^{h-1}$ и добавим к полученному множеству еще $t, t^2, \ldots, t^{h-1}$; тогда получится конечное множество элементов, через которые уже все степени элемента t линейно выражаются с коэффициентами из $\mathfrak{R}$ и целочисленными коэффициентами.

Кольцо $\mathfrak{S}$ называется *целозамкнутым в некотором объемлющем кольце* $\mathfrak{T}$, если каждый целый над $\mathfrak{S}$ элемент из $\mathfrak{T}$ принадлежит уже $\mathfrak{S}$. В частности, целостное кольцо $\mathfrak{S}$ называется просто *целозамкнутым*, если оно целозамкнуто в своем поле частных Σ. Как легко видеть, это означает, что каждый элемент t из Σ, степени t^ρ которого выражаются как дроби с некоторым фиксированным знаменателем из $\mathfrak{S}$, принадлежит кольцу $\mathfrak{S}$. Действительно, конечное множество элементов, через которые могут быть выражены все степени некоторого целого числа t, может быть приведено к общему знаменателю и, обратно, если все степени элемента t представляются в виде дробей со знаменателем s, то они линейно выражаются через элемент s^{-1}.

Из предыдущей теоремы следует, что в случае коммутативного кольца $\mathfrak{T}$ *кольцо $\mathfrak{S}$ всех целых над $\mathfrak{R}$ элементов из $\mathfrak{T}$ является целозамкнутым в $\mathfrak{T}$, если идеалы из $\mathfrak{S}$ удовлетворяют теореме о цепях делителей.*

Такая же теорема может быть доказана и без предположения о справедливости теоремы о цепях делителей, если считать, что кольцо $\mathfrak{R}$ целозамкнуто в своем поле частных P, а $\mathfrak{T}$ является конечным расширением поля P. Для доказательства поле $\mathfrak{T}$ расширяется до некоторого расширения Галуа $\mathfrak{T}'$ поля P, а $\mathfrak{S}$ — до кольца $\mathfrak{S}'$ целых элементов поля $\mathfrak{T}'$. Если некоторый элемент t является целым над $\mathfrak{S}$, а потому и над $\mathfrak{S}'$, то таковыми будут и элементы, сопряженные с t над P, а также элементарные симметрические функции этих сопряженных элементов, т. е. коэффициенты уравнения, определяющего элемент t. В силу

целозамкнутости кольца $\mathfrak{R}$ эти коэффициенты принадлежат кольцу $\mathfrak{R}$, так что t оказывается целым над $\mathfrak{R}$ и, следовательно, $t \in \mathfrak{S}$.

Одно достаточное, но не необходимое условие для целозамкнутости целостного кольца дает следующая

Теорема. *Целостное кольцо с единицей, в котором имеет место теорема об однозначности разложения на простые множители, целозамкнуто в своем поле частных.*

Доказательство. Каждый элемент поля частных можно представить дробью a/b, в которой a и b не имеют общих простых множителей. Тогда, если все степени дроби a/b можно освободить от знаменателей умножением на некоторый элемент c, то ca^n, а потому и c, должны делиться на b^n при каждом натуральном n, что, однако, возможно лишь тогда, когда b — некоторый обратимый элемент, и поэтому $a/b = ab^{-1}$ — элемент из данного целостного кольца.

Из этой теоремы следует, что всякое кольцо главных идеалов (в частности, кольцо целых чисел $\mathbb{Z}$), всякое кольцо целочисленных многочленов и всякое кольцо многочленов над каким-либо полем K являются целозамкнутыми.

Задача 1. Корни из единицы в любом поле являются целыми над любым подкольцом.

Задача 2. Какие числа из поля гауссовых чисел $\mathbb{Q}(i)$ являются целыми над $\mathbb{Z}$? Решить аналогичный вопрос для поля $\mathbb{Q}(\rho)$, где $\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Задача 3. Если целостное кольцо $\mathfrak{R}$ целозамкнуто, то и кольцо многочленов $\mathfrak{R}[x]$ целозамкнуто.

§ 136. Целые элементы в поле

Пусть $\mathfrak{R}$ — целостное кольцо, P — его поле частных, Σ — конечное коммутативное расширение поля P и $\mathfrak{S}$ — кольцо целых над $\mathfrak{R}$ элементов из Σ. Очевидно, что $\mathfrak{S}$ является кольцом, содержащим кольцо $\mathfrak{R}$. Связь между кольцами $\mathfrak{R}$, $\mathfrak{S}$ и полями P, Σ схематически можно изобразить так:

$$\begin{array}{ccc} \mathfrak{R} & \subseteq & \mathfrak{S} \\ \cap & & \cap \\ \mathsf{P} & \subseteq & \Sigma. \end{array}$$

Такие соотношения будут считаться выполненными всюду в данном параграфе. Под словом «целый» здесь постоянно подразумевается «целый над $\mathfrak{R}$».

Примеры. Если $\mathfrak{R}$ — кольцо обычных целых чисел, то P — поле обычных рациональных чисел; поле Σ является некоторым числовым полем (конечным над P), а $\mathfrak{S}$ — кольцом целых алгебраических чисел поля Σ.

Если $\mathfrak{R}$ — кольцо многочленов: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, то P — поле рациональных функций; в этом случае Σ получается присоединением конечного множества алгебраических функций, а $\mathfrak{S}$ оказывается составленным из целых алгебраических функций поля Σ.

Наша цель состоит в изучении теории идеалов в кольце $\mathfrak{S}$. Как мы знаем, для этого в первую очередь нужно выяснить, справедлива ли в $\mathfrak{S}$ теорема о цепях делителей для идеалов. Точнее, нужно выяснить, переносится ли на $\mathfrak{S}$ теорема о цепях делителей при условии, что она выполнена в $\mathfrak{R}$. В соответствии с теоремами из § 134 это возможно, если существует базис для $\mathfrak{S}$ как для $\mathfrak{R}$-модуля. Этим рассуждением определяется наша ближайшая цель.

Прежде всего, одна подготовительная

Теорема. *Если σ — некоторый элемент поля Σ, то $\sigma = s/r$, где $s \in \mathfrak{S}$, $r \in \mathfrak{R}$.*

Доказательство. Элемент σ удовлетворяет некоторому уравнению с коэффициентами из P. Эти коэффициенты являются дробями, числители и знаменатели которых принадлежат кольцу $\mathfrak{R}$. С помощью умножения на произведение всех этих знаменателей упомянутые дроби становятся элементами из $\mathfrak{R}$ и получается уравнение

$$r_0\sigma^m + r_1\sigma^{m-1} + \ldots + r_m = 0.$$

Положим $r_0 = r$ и умножим это на r^{m-1}:

$$(r\sigma)^m + r_1(r\sigma)^{m-1} + r_2 r(r\sigma)^{m-2} + \ldots + r_m r^{m-1} = 0.$$

Следовательно, $r\sigma$ — целый элемент над $\mathfrak{R}$. Положим $r\sigma = s$ и тем самым получим требуемое.

Из этой теоремы следует, что Σ — поле частных кольца $\mathfrak{S}$.

Если некоторый элемент ξ является целым над основным кольцом, то и все сопряженные с ним элементы (в некотором расширении Галуа поля P, содержащем Σ) являются целыми.

Доказательство. Конечное множество элементов из Σ, через которые по условию линейно выражаются все степени элемента ξ, при любом изоморфизме поля Σ переходит снова в конечное множество элементов, через которые линейно выражаются все степени того или иного сопряженного с ξ элемента.

Суммы и произведения целых элементов снова являются целыми; поэтому являются целыми и элементарные симметрические функции от ξ и сопряженных с ним элементов. Мы получили следующее предложение:

Если в некотором неразложимом над полем P уравнении, которому удовлетворяет целый элемент ξ, старший коэффициент равен единице, то и все остальные коэффициенты этого уравнения

являются целыми над $\mathfrak{R}$. *В частности, если кольцо* $\mathfrak{R}$ *целозамкнуто в* P, *то все эти коэффициенты принадлежат* $\mathfrak{R}$.

В случае целозамкнутого кольца $\mathfrak{R}$ это предложение дает удобное средство для выяснения, является ли тот или иной элемент ξ целым: для этого не нужно строить все уравнения, которым удовлетворяет ξ, и среди них отыскивать уравнения с целыми коэффициентами, а достаточно найти неразложимое уравнение для ξ со старшим коэффициентом 1. Если все его коэффициенты целые, то и ξ — целый элемент, если же не все коэффициенты целые, то и ξ не является целым.

Сделаем теперь три следующих предположения:

I. *Кольцо* $\mathfrak{R}$ *целозамкнуто в своем поле частных* P.

II. *В кольце* $\mathfrak{R}$ *имеет место теорема о цепях делителей для идеалов.*

III. *Поле* Σ *является сепарабельным расширением поля* P. Из III, в соответствии с § 46, следует, что поле Σ порождается некоторым «примитивным элементом» σ: $\Sigma = \mathsf{P}(\sigma)$. Согласно последней теореме $\sigma = s/r$ $(r \in \mathfrak{S},\ r \in \mathfrak{R})$; следовательно, это поле порождается и целым элементом s. Элемент s удовлетворяет некоторому уравнению n-й степени, где n — степень расширения Σ/P. Каждый элемент ξ из Σ можно представить в виде

$$\xi = \sum_{0}^{n-1} \rho_k s^k \qquad (\rho_k \in \mathsf{P}). \tag{1}$$

Если в (1) заменить s на сопряженные с ним элементы s_ν (в каком-либо расширении Галуа поля Σ, содержащем P), каковых, согласно § 44, существует ровно n, то для элементов ξ_ν, сопряженных с ξ, получатся равенства

$$\xi_\nu = \sum_{0}^{n-1} \rho_k s_\nu^k \qquad (\nu = 1,\ 2,\ \ldots,\ n). \tag{2}$$

Определитель этой системы уравнений равен[1])

$$D = |s_\nu^k| = \prod_{\lambda < \mu} (s_\lambda - s_\mu).$$

Квадрат этого определителя является симметрической функцией от s_ν, а потому содержится в P. Так как сопряженные элементы s_ν все различны, $D \neq 0$. Следовательно, систему уравнений (2) можно решить:

$$\rho_k = \frac{\sum S_{k\nu}\xi_\nu}{D},$$

[1]) См. задачу 2 из § 28. — *Прим. ред.*

где $S_{k\nu}$ и D — многочлены от s_ν, т. е. элементы, целые над $\mathfrak{R}$. Умножение этого равенства на D^2 дает

$$D^2\rho_k = \sum_\nu DS_{k\nu}\xi_\nu. \tag{3}$$

Если теперь предположить, что ξ является элементом из $\mathfrak{S}$, т. е. целым элементом, то окажется, что элементы ξ_ν, а с ними и левая часть в (3) целые. Вместе с тем левая часть является элементом из P. Так как кольцо $\mathfrak{R}$ целозамкнуто в P, то элемент $D^2\rho_k$ принадлежит $\mathfrak{R}$. Положим $D^2\rho_k = r_k$; тогда $\rho_k = r_k D^{-2}$ и, согласно (1),

$$\xi = \sum_0^{n-1} r_k D^{-2} s^k.$$

Следовательно, каждое ξ из $\mathfrak{S}$ может быть линейно выражено через $D^{-2}s^0$, $D^{-2}s^1$, ..., $D^{-2}s^{n-1}$ с коэффициентами из $\mathfrak{R}$. Другими словами, кольцо $\mathfrak{S}$ содержится в конечном $\mathfrak{R}$-модуле:

$$\mathfrak{M} = (D^{-2}s^0,\ D^{-2}s^1,\ \ldots,\ D^{-2}s^{n-1}).$$

Отсюда, согласно теоремам из § 134, следует, что $\mathfrak{S}$, *как и всякий подмодуль в* $\mathfrak{S}$ *и, в частности, всякий идеал в* $\mathfrak{S}$, *обладает конечным базисом над* $\mathfrak{R}$ *как модуль, или, что то же самое, для* $\mathfrak{R}$*-модулей и, в частности, для идеалов в* $\mathfrak{S}$, *выполняется теорема о цепях делителей.* Если, например, $\mathfrak{R}$ — кольцо главных идеалов, то даже $\mathfrak{S}$ и каждый подмодуль в $\mathfrak{S}$ обладают линейно независимыми базисами как модули над $\mathfrak{R}$.

Под $\mathfrak{R}$-*порядком* в Σ подразумевается всякое кольцо в Σ, которое содержит $\mathfrak{R}$ и является конечным $\mathfrak{R}$-модулем. В соответствии со сказанным выше кольцо $\mathfrak{S}$ является $\mathfrak{R}$-порядком, как и любое кольцо, заключенное между $\mathfrak{R}$ и $\mathfrak{S}$. Обратно, из определения целостности следует, что каждый $\mathfrak{R}$-порядок $\mathfrak{T}$ в Σ состоит исключительно из целых элементов, т. е. принадлежит кольцу $\mathfrak{S}$. Тем самым кольцо $\mathfrak{S}$ можно охарактеризовать как $\mathfrak{R}$-порядок в Σ, содержащий все остальные $\mathfrak{R}$-порядки. Кольцо $\mathfrak{S}$ называют также *главным порядком* поля Σ. Если пойдет речь об «идеалах поля», «единицах поля» и т. д., то всегда будут иметься в виду идеалы из $\mathfrak{S}$, единицы из $\mathfrak{S}$ и т. д. В соответствии с § 135 кольцо $\mathfrak{S}$ целозамкнуто в поле Σ.

Результаты этого параграфа не остаются справедливыми в некоммутативных алгебрах над P; препятствие состоит в том, что сумма двух целых элементов уже не обязана быть целой. Поэтому совокупность всех целых элементов не является порядком. Несмотря на то, что каждый порядок по-прежнему состоит из целых элементов, в некоммутативном случае не существует наибольшего, главного порядка, содержащего все остальные. При подходящих предположениях относительно поля Σ появляются различные максимальные $\mathfrak{R}$-порядки, так что каждый $\mathfrak{R}$-порядок, а также каждый целый элемент содержатся по

крайней мере в одном максимальном $\mathfrak{R}$-порядке. По поводу теории идеалов в таких максимальных $\mathfrak{R}$-порядках см. Дойринг (Deuring M.). Algebren. — Ergebn. Math., 1935, **4**, Heft 1.

Во всех $\mathfrak{R}$-порядках поля Σ, в соответствии с доказанным выше, выполняется теорема о цепях делителей. Поэтому для таких порядков выполнены теоремы о существовании и единственности разложения на простые множители из §§ 118 и 119 (представление всех идеалов в виде пересечения примарных идеалов).

Согласно § 122 значительное упрощение теории идеалов оказывается возможным тогда, когда каждый отличный от нуля простой идеал $\mathfrak{R}$-порядка $\mathfrak{o}$ не имеет делителей. Следующая теорема устанавливает условия, при которых имеет место этот случай:

Если в кольце $\mathfrak{R}$ каждый простой идеал, отличный от нуля, не имеет делителей, то и в каждом $\mathfrak{R}$-порядке $\mathfrak{o}$ каждый ненулевой идеал не имеет делителей.

Доказательство. Пусть $\mathfrak{p}$ — произвольный простой идеал из $\mathfrak{o}$, содержащий отличный от нуля элемент t. Элемент t удовлетворяет некоторому уравнению с коэффициентами из $\mathfrak{R}$:

$$t^h + a_1 t^{h-1} + \ldots + a_h = 0,$$

которое мы будем считать выбранным наименьшей возможной степени и со старшим коэффициентом 1; в этом уравнении $a_h \neq 0$, так как иначе можно было бы сократить на t. Следовательно, $a_h \equiv 0\,(t) \equiv 0\,(\mathfrak{p})$, а потому a_h принадлежит пересечению $\mathfrak{p} \cap \mathfrak{R}$. Это пересечение является простым идеалом в $\mathfrak{R}$, потому что если произведение каких-нибудь двух элементов из $\mathfrak{R}$ принадлежит $\mathfrak{R} \cap \mathfrak{p}$, а потому и $\mathfrak{p}$, то один из сомножителей должен принадлежать $\mathfrak{p}$, а потому и $\mathfrak{R} \cap \mathfrak{p}$. Так как a_h принадлежит простому идеалу $\mathfrak{R} \cap \mathfrak{p}$, этот простой идеал отличен от нулевого, а потому не имеет делителей.

Если теперь $\mathfrak{a}$ — произвольный собственный делитель идеала $\mathfrak{p}$ и u — некоторый элемент из $\mathfrak{a}$, не принадлежащий $\mathfrak{p}$, то u удовлетворяет уравнению вида

$$u^l + b_1 u^{l-1} + \ldots + b_l = 0,$$

а потому и сравнению с наименьшей возможной степенью

$$u^k + c_1 u^{k-1} + \ldots + c_k \equiv 0\,(\mathfrak{p}),$$

в котором вновь $c_k \not\equiv 0\,(\mathfrak{p})$, так как иначе возможно было бы сокращение на u. Следовательно, $c_k \equiv 0\,(u) \equiv 0\,(\mathfrak{a})$, а потому элемент c_k принадлежит пересечению $\mathfrak{a} \cap \mathfrak{R}$ и не принадлежит пересечению $\mathfrak{p} \cap \mathfrak{R}$. Таким образом, это пересечение $\mathfrak{a} \cap \mathfrak{R}$ является собственным делителем идеала $\mathfrak{p} \cap \mathfrak{R}$ и по этой причине совпадает с $\mathfrak{R}$. Следовательно, идеал $\mathfrak{a}$ содержит единичный элемент, так что $\mathfrak{a} = \mathfrak{o}$. Теорема доказана.

Предположения этой теоремы выполнены, в частности, тогда, когда $\mathfrak{R}$ является кольцом главных идеалов (кольцом целых чисел, кольцом многочленов от одной переменной). Таким образом, в этом случае в $\mathfrak{o}$ выполнена теорема о том, что каждый идеал, отличный от нуля и единичного идеала, однозначно представляется в виде произведения взаимно простых и отличных от $\mathfrak{o}$ примарных идеалов.

Однако, как мы увидим, для главного порядка $\mathfrak{S}$ выполняется нечто большее: примарные идеалы равны степеням простых идеалов, а потому в этом случае *каждый идеал равен произведению степеней простых идеалов*. Ввиду значительности этого главного результата «классической» дедекиндовой теории идеалов для теории числовых и функциональных полей мы докажем его, не используя понятия примарного идеала и общей теории идеалов. Это будет сделано в следующем параграфе с помощью метода, предложенного Круллем[1]).

Задача 1. Если $\mathfrak{R}$ — кольцо главных идеалов, $(\omega_1, \ldots, \omega_n)$ — всегда существующий в этом случае линейно независимый базис $\mathfrak{R}$-порядка $\mathfrak{o}$ и $\left(\omega_1^{(i)}, \ldots, \omega_n^{(i)}\right)$ — сопряженные базисы в некотором расширении Галуа поля P, то «дискриминант поля»

$$D = \begin{vmatrix} \omega_1^{(1)} \ldots \omega_n^{(1)} \\ \cdots\cdots \\ \omega_1^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}^2$$

является целым, рациональным и отличным от нуля.

Задача 2. Пусть $\Sigma = \mathsf{P}(\sqrt{d})$ и $\mathfrak{R}$ — кольцо, целозамкнутое в P. Доказать, что те и только те элементы $\xi = a + b\sqrt{d}$ являются целыми над $\mathfrak{R}$, у которых следы и нормы

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

принадлежат кольцу $\mathfrak{R}$.

Задача 3. Если в задаче 2 $\mathfrak{R} = \mathsf{K}[x]$ — кольцо многочленов от одной переменной и d — некоторый многочлен, не имеющий кратных множителей, то $\xi = a + b\sqrt{d}$ является целым элементом тогда и только тогда, когда a и b принадлежат $\mathfrak{R}$.

Задача 4. Если в задаче 2 $\mathfrak{R} = \mathbb{Z}$ — кольцо целых чисел и d — некоторое число, свободное от квадратов[2]), то один из базисов главного порядка в случае $d \not\equiv 1\ (4)$ состоит из чисел $1, \sqrt{d}$, а в случае $d \equiv 1\ (4)$ — из чисел $1, \dfrac{1+\sqrt{d}}{2}$.

---

[1]) Krull W. Zur Theorie der allgemeinen Zahlringe. — Math. Ann., 1928, 99, S. 51—70.

[2]) То есть не делится на квадрат простого числа. — *Прим. ред.*

§ 137. Аксиоматическое обоснование классической теории идеалов

Пусть $\mathfrak{o}$ — произвольное целостное кольцо (коммутативное кольцо без делителей нуля), в котором выполнены следующие три аксиомы:

I. Теорема о цепях делителей для идеалов.

II. Все отличные от нуля простые идеалы не имеют делителей.

III. Кольцо $\mathfrak{o}$ целозамкнуто в своем поле частных Σ.

Примерами таких колец могут служить: 1) кольца главных идеалов; 2) главные порядки, которые получаются при конечных расширениях поля частных по схеме из § 136 из колец главных идеалов (в частности, главные порядки в числовых полях и полях функций от одной переменной).

Элементы поля Σ, являющиеся целыми над $\mathfrak{o}$, а потому, согласно III, принадлежащие кольцу $\mathfrak{o}$, будут называться просто *целыми*. В частности, единичный элемент из Σ является целым, так что $\mathfrak{o}$ — целостное кольцо с единицей.

Наряду с идеалами из $\mathfrak{o}$ (или $\mathfrak{o}$-модулями внутри $\mathfrak{o}$) мы будем рассматривать и $\mathfrak{o}$-модули внутри Σ, т. е. подмножества поля Σ, которые вместе с a и b содержат также $a-b$, а вместе с a — элементы ra, где r — любое целое число. Если такой $\mathfrak{o}$-модуль $\mathfrak{a}$ обладает конечным базисом, то $\mathfrak{a}$ называют *дробным идеалом*. Если $\mathfrak{o}$-модуль $\mathfrak{a}$ состоит только из целых элементов ($\mathfrak{a} \subseteq \mathfrak{o}$), то он является идеалом в обычном смысле или, как мы будем теперь говорить, *целым идеалом*.

Под *суммой* или *наибольшим общим делителем* $(\mathfrak{a}, \mathfrak{b})$ двух $\mathfrak{o}$-модулей $\mathfrak{a}$ и $\mathfrak{b}$ мы подразумеваем (как и в случае идеалов) модуль всевозможных сумм $a+b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$; равным образом под произведением $\mathfrak{a}\mathfrak{b}$ подразумевается модуль, порожденный всевозможными произведениями ab или совокупностью всех сумм $\sum a_\nu b_\nu$.

Суммы и произведения $\mathfrak{o}$-модулей с конечными базисами снова являются $\mathfrak{o}$-модулями с конечными базисами.

В последующих теоремах мы обозначаем готическими буквами лишь ненулевые целые идеалы в кольце $\mathfrak{o}$, а буквой $\mathfrak{p}$ — с индексами или без — постоянно обозначается какой-нибудь ненулевой простой идеал.

Лемма 1. *Для каждого идеала $\mathfrak{a}$ существует произведение простых идеалов $\mathfrak{p}_i$, делящих $\mathfrak{a}$, кратное идеалу $\mathfrak{a}$:*

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(\mathfrak{a}).$$

Доказательство. Если идеал $\mathfrak{a}$ простой, то лемма верна. Если же $\mathfrak{a}$ не является простым, то существует произведение двух главных идеалов $\mathfrak{b}\mathfrak{c}$ такое, что

$$\mathfrak{b}\mathfrak{c} \equiv 0\,(\mathfrak{a}), \quad \mathfrak{b} \not\equiv 0\,(\mathfrak{a}), \quad \mathfrak{c} \not\equiv 0\,(\mathfrak{a}).$$

Идеалы $\mathfrak{b}' = (\mathfrak{b}, \mathfrak{a})$, $\mathfrak{c}' = (\mathfrak{c}, \mathfrak{a})$ являются собственными делителями идеала $\mathfrak{a}$ и

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{b}, \mathfrak{a}) \cdot (\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}\mathfrak{c}, \mathfrak{b}\mathfrak{a}, \mathfrak{a}\mathfrak{c}, \mathfrak{a}^2) \equiv 0\,(\mathfrak{a}).$$

Если считать данную лемму выполненной для идеалов $\mathfrak{b}'$ и $\mathfrak{c}'$, то существуют некоторое произведение $\mathfrak{p}_1 \ldots \mathfrak{p}_s \equiv 0\,(\mathfrak{b}')$ и некоторое произведение $\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r \equiv 0\,(\mathfrak{c}')$. В этом случае произведение $\mathfrak{p}_1 \ldots \mathfrak{p}_s \mathfrak{p}_{s+1} \ldots \mathfrak{p}_r$ делится на $\mathfrak{b}' \cdot \mathfrak{c}'$, а потому и на $\mathfrak{a}$, и лемма оказывается выполненной для $\mathfrak{a}$. Но если бы лемма была неверна для идеала $\mathfrak{a}$, то она была бы неверна и для одного из делителей $\mathfrak{b}'$ или $\mathfrak{c}'$; этот делитель в свою очередь обладал бы делителем (собственным), для которого данная лемма не выполнена, и т. д. Таким способом мы получили бы бесконечную цепь собственных делителей, что, согласно аксиоме I, невозможно. Следовательно, лемма верна для каждого идеала $\mathfrak{a}$.

Лемма 2. *Если идеал* $\mathfrak{p}$ *простой, то из* $\mathfrak{a}\mathfrak{b} \equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{a} \equiv 0\,(\mathfrak{p})$ *или* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Доказательство. Если $\mathfrak{a} \not\equiv 0\,(\mathfrak{p})$ и $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$, то существуют такой элемент a из $\mathfrak{a}$ и такой элемент b из $\mathfrak{b}$, что оба они не принадлежат $\mathfrak{p}$. Но их произведение ab, находясь в $\mathfrak{a}\mathfrak{b}$, должно было бы принадлежать $\mathfrak{p}$, а это противоречит тому, что идеал $\mathfrak{p}$ прост.

Символом $\mathfrak{p}^{-1}$ мы будем обозначать совокупность (целых или дробных) элементов a, для которых $a\mathfrak{p}$ — целый идеал. Очевидно, $\mathfrak{p}^{-1}$ — некоторый $\mathfrak{o}$-модуль.

Лемма 3. *Если* $\mathfrak{p} \neq \mathfrak{o}$, *то в* $\mathfrak{p}^{-1}$ *существует нецелый элемент.*

Доказательство. Пусть c — произвольный отличный от нуля элемент из $\mathfrak{p}$. Согласно лемме 1 существует произведение простых идеалов со свойством:

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(c).$$

Мы можем предположить, что это произведение несократимо, т. е. его нельзя заменить никаким частичным произведением типа $\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(c)$. Так как произведение $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ делится на $\mathfrak{p}$, то один из его сомножителей, скажем, $\mathfrak{p}_1$, должен делиться на $\mathfrak{p}$, а потому совпадает с $\mathfrak{p}$.

Тем самым

$$\mathfrak{p}\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0\,(c),$$
$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\equiv 0\,(c).$$

Следовательно, существует не принадлежащий идеалу (c) элемент b из произведения $\mathfrak{p}_2 \ldots \mathfrak{p}_r$. Для него справедливы соотношения

$$\mathfrak{p}b \equiv 0\,(\mathfrak{p}\mathfrak{p}_2 \ldots \mathfrak{p}_r) \equiv 0\,(c).$$

Следовательно, идеал $\mathfrak{p}b/c$ целый, а потому b/c принадлежит идеалу $\mathfrak{p}^{-1}$. Но так как $b \not\equiv 0\,(c)$, то элемент b/c не является целым, что и требовалось доказать.

Теорема 1. *Если* $\mathfrak{p}=\mathfrak{o}$, *то*

$$\mathfrak{p}\cdot\mathfrak{p}^{-1}=\mathfrak{o}.$$

Доказательство. Согласно определению идеала $\mathfrak{p}^{-1}$ имеет место включение $\mathfrak{o}\subseteq\mathfrak{p}^{-1}$, так что $\mathfrak{p}=\mathfrak{o}\mathfrak{p}\subset\mathfrak{p}^{-1}\mathfrak{p}$. Следовательно, целый идеал $\mathfrak{p}\mathfrak{p}^{-1}$ является делителем идеала $\mathfrak{p}$, а потому он равен либо $\mathfrak{p}$, либо $\mathfrak{o}$. Предположим, что

$$\mathfrak{p}\cdot\mathfrak{p}^{-1}=\mathfrak{p}.$$

Тогда $\mathfrak{p}\cdot(\mathfrak{p}^{-1})^2=(\mathfrak{p}\mathfrak{p}^{-1})\,\mathfrak{p}^{-1}=\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{p}$, $\mathfrak{p}\,(\mathfrak{p}^{-1})^3=\mathfrak{p}$ и т. д. Следовательно, если $a\neq 0$ — произвольный элемент из $\mathfrak{p}$ и b — произвольный элемент из $\mathfrak{p}^{-1}$, то элемент $ab^e\in\mathfrak{p}\,(\mathfrak{p}^{-1})^e$ является целым, в силу чего все степени элемента b представляются как дроби с одним и тем же фиксированным знаменателем a. Поэтому элемент b целый. Это оказывается выполненным для произвольного элемента b из $\mathfrak{p}^{-1}$, что противоречит лемме 3.

Теперь мы можем доказать основную теорему о разложении:

Теорема 2. *Каждый идеал* $\mathfrak{a}$ *является произведением простых идеалов.*

Доказательство. Можно считать, что $\mathfrak{a}\neq\mathfrak{o}$. Пусть в соответствии с леммой 1

$$\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r\equiv 0\,(\mathfrak{a}) \tag{1}$$

и число r выбрано наименьшим; тогда ни одно из укороченных произведений не сравнимо с нулем по модулю $\mathfrak{a}$. Пусть далее $\mathfrak{p}$ — произвольный отличный от $\mathfrak{o}$ простой идеал, являющийся делителем идеала $\mathfrak{a}$ (таковой обязательно существует согласно лемме 1). Но тогда произведение $\mathfrak{p}_1\ldots\mathfrak{p}_r$ делится на $\mathfrak{p}$ и, следовательно (в силу леммы 2), одно из $\mathfrak{p}_i$ делится на $\mathfrak{p}$, а потому совпадает с $\mathfrak{p}$, поскольку идеалы $\mathfrak{p}_i$ не имеют делителей. Мы можем считать, что $\mathfrak{p}_1=\mathfrak{p}$. Умножим (1) на $\mathfrak{p}^{-1}$, тогда получится

$$\mathfrak{p}_2\ldots\mathfrak{p}_r\equiv 0\,(\mathfrak{p}^{-1}\mathfrak{a})\equiv 0\,(\mathfrak{o});$$

следовательно, $\mathfrak{p}^{-1}\mathfrak{a}$ — целый идеал, который включается в произведение менее чем r простых идеалов. Проведем теперь индукцию по r. Предположим, что для идеалов, которые включаются в произведение менее чем r простых идеалов, отличных от нуля, теорема уже доказана (для идеалов, включающихся лишь в один простой идеал, отличный от нуля, теорема очевидна). Тогда, в частности, теорема верна для $\mathfrak{p}^{-1}\mathfrak{a}$, т. е.

$$\mathfrak{p}^{-1}\mathfrak{a}=\mathfrak{p}_2'\ldots\mathfrak{p}_s'.$$

Умножение с обеих сторон на $\mathfrak{p}$ дает нужное представление для $\mathfrak{a}$.

Единственность такого представления гарантирует

Теорема 3. *Если* $\mathfrak{a}\equiv 0\,(\mathfrak{b})$ *и* $\mathfrak{a}=\mathfrak{p}_1\ldots\mathfrak{p}_r$, $\mathfrak{b}=\mathfrak{p}_1'\ldots\mathfrak{p}_s'$, *то каждый отличный от* $\mathfrak{o}$ *простой идеал, входящий в разложение идеала*

$\mathfrak{b}$, *входит и в разложение идеала* $\mathfrak{a}$ *и по крайней мере столько же раз.*

Доказательство. Пусть $\mathfrak{p}_1' \neq \mathfrak{o}$. Так как $\mathfrak{p}_1'$ — делитель идеала $\mathfrak{a}$, то, как и выше, мы приходим к выводу о том, что $\mathfrak{p}_1'$ — это один из идеалов $\mathfrak{p}_\nu$. Пусть, например, $\mathfrak{p}_1 = \mathfrak{p}_1'$. Тогда

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0\,(\mathfrak{p}_1^{-1}\mathfrak{b}),$$
$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$
$$\mathfrak{p}_1^{-1}\mathfrak{b} \equiv \mathfrak{p}'_2 \ldots \mathfrak{p}'_s.$$

Предположим, что наше утверждение уже доказано для меньших значений s (для $s=0$, $\mathfrak{b}=\mathfrak{o}$ утверждение тривиально); тогда каждый отличный от $\mathfrak{o}$ идеал из списка $\mathfrak{p}'_2, \ldots, \mathfrak{p}'_s$ входит в список $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ по крайней мере столько же раз. Отсюда следует требуемое.

Следствие 1. *Представление идеала* $\mathfrak{a}$ *в виде произведения простых идеалов единственно с точностью до порядка следования сомножителей и с точностью до числа сомножителей, равных* $\mathfrak{o}$.

Следствие 2. *Из делимости следует представление в виде произведения: если* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$, *то* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ *при некотором целом идеале* $\mathfrak{c}$.

Действительно, в качестве $\mathfrak{c}$ нужно взять произведение простых сомножителей, входящих в разложение идеала $\mathfrak{a}$, которые остаются свободными после составления произведения, равного $\mathfrak{b}$.

Задача. Разложить на простые множители-идеалы главные идеалы (2) и (3) в главном порядке числового поля $\mathbb{Q}(\sqrt{-5})$.

§ 138. Обращение и дополнение полученных результатов

Мы видели, что из аксиом I — III (§ 137) следуют теоремы 2 и 3, гарантирующие однозначное разложение идеалов на простые сомножители. Это положение обратимо:

Пусть $\mathfrak{o}$ — *целостное кольцо с единицей. Пусть в* $\mathfrak{o}$ *каждый целый идеал* $\mathfrak{a}$ *представим в виде произведения простых идеалов:* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$, *и пусть, если* $\mathfrak{a}$ *делится на* $\mathfrak{b}$, *то в каждом разложении для* $\mathfrak{a}$ *каждый отличный от* $\mathfrak{o}$ *множитель из разложения для* $\mathfrak{b}$ *участвует по крайней мере столько же раз. Тогда в кольце* $\mathfrak{o}$ *выполняются аксиомы* I — III.

Доказательство. Теорема о цепях (аксиома I) немедленно следует из того, что каждый целый идеал $\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \ldots \mathfrak{p}_s^{\rho_r}$ обладает лишь конечным числом делителей $\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r}$ $(\sigma_i \leqslant \rho_i)$. В частности, простой идеал $\mathfrak{p}$ делится только на $\mathfrak{p}$ и на $\mathfrak{o}$, так что выполнена и аксиома II.

Аксиома III (целозамкнутость кольца $\mathfrak{o}$ в поле частных Σ) доказывается так. Предположим, что λ — произвольный элемент поля Σ, целый над $\mathfrak{o}$; тогда некоторая его степень, скажем λ^m,

линейно выражается через $\lambda^0, \ldots, \lambda^{m-1}$, или, иначе говоря, принадлежит $\mathfrak{o}$-модулю $\mathfrak{l} = (\lambda^0, \lambda^1, \ldots, \lambda^{m-1})$. Если $\lambda = a/b$, то модуль $\mathfrak{l}$ с помощью умножения всех его элементов на идеал $\mathfrak{b} = (b^{m-1})$ становится целым идеалом. Очевидно, что $\mathfrak{l}$ удовлетворяет равенству $\mathfrak{l}^2 = \mathfrak{l}$. Умножение на $\mathfrak{b}^2$ дает

$$(\mathfrak{l}\mathfrak{b})^2 = (\mathfrak{l}\mathfrak{b})\mathfrak{b}.$$

В силу единственности отсюда следует, что

$$\mathfrak{l}\mathfrak{b} = \mathfrak{b},$$

и, таким образом, если обе части умножить еще на $b^{-(m-1)}$,

$$\mathfrak{l} = \mathfrak{o}.$$

Следовательно, элемент λ принадлежит кольцу $\mathfrak{o}$, что и требовалось доказать.

Обратимся теперь к обобщениям теорем 2 и 3, тоже относящимся к классической теории идеалов.

Тот факт, что из делимости следует возможность представлять элементы в виде произведения, позволяет ввести наибольший общий делитель и наименьшее общее кратное точно так же, как это делается в случае целых чисел с помощью разложения на простые множители.

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — два целых идеала:

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \ldots \mathfrak{p}_r^{\rho_r},$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r}$$

(здесь в обоих случаях указаны простые множители, входящие в $\mathfrak{a}$ и $\mathfrak{b}$, возможно, с нулевым показателем степени). Каждый общий делитель содержит лишь простые множители $\mathfrak{p}_i$ из перечисленных и при этом с показателем степени $\leqslant \tau_i$, где τ_i — наименьшее из чисел ρ_i, σ_i. Наибольший общий делитель $(\mathfrak{a}, \mathfrak{b})$ должен делиться на каждый общий делитель и, в частности, на $\mathfrak{p}_i^{\tau_i}$. Следовательно, он может иметь лишь следующий вид:

$$\mathfrak{p}_1^{\tau_1} \ldots \mathfrak{p}_r^{\tau_r}.$$

Точно так же устанавливается, что наименьшее общее кратное (пересечение) $\mathfrak{a} \cap \mathfrak{b}$ идеалов $\mathfrak{a}$ и $\mathfrak{b}$ является идеалом

$$\mathfrak{p}_1^{\mu_1} \ldots \mathfrak{p}_r^{\mu_r},$$

где μ_i — наибольшее из чисел ρ_i, σ_i.

Теорема 4. *Если* $\mathfrak{a} \equiv 0\ (\mathfrak{d})$, *то в* $\mathfrak{d}$ *существует элемент* d, *для которого*

$$(\mathfrak{a}, d) = \mathfrak{d},$$

Доказательство. Пусть

$$\mathfrak{a} = \mathfrak{p}_1^{\rho_1} \ldots \mathfrak{p}_r^{\rho_r},$$

$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r} \quad (0 \leqslant \sigma_i \leqslant \rho_i).$$

Мы должны выбрать элемент d так, чтобы d делился на $\mathfrak{b}$, но не имел общих с $\mathfrak{a}$ делителей, отличных от делителей идеала $\mathfrak{b}$. Положим

$$\mathfrak{c} = \mathfrak{p}_1^{\sigma_1+1} \ldots \mathfrak{p}_r^{\sigma_r+1},$$

$$\mathfrak{c}_i = \mathfrak{c} : \mathfrak{p}_i = \mathfrak{p}_1^{\sigma_1+1} \ldots \mathfrak{p}_i^{\sigma_i} \ldots \mathfrak{p}_r^{\sigma_r+1}.$$

Тогда $\mathfrak{c}_i \not\equiv 0\,(\mathfrak{c})$. Следовательно, существует элемент d_i, принадлежащий идеалу $\mathfrak{c}_i$, но не принадлежащий идеалу $\mathfrak{c}$. Тогда

$$d_i \equiv 0\,(\mathfrak{p}_j^{\sigma_j+1}) \text{ для } j \neq i,$$

$$d_i \not\equiv 0\,(\mathfrak{p}_i^{\sigma_i+1}).$$

Сумма

$$d = d_1 + \ldots + d_r$$

делится на $\mathfrak{b}$ (так как этим свойством обладают все d_i). Но вместе с тем

$$d \equiv d_i \not\equiv 0\,(\mathfrak{p}_i^{\sigma_i+1});$$

следовательно, элемент d не имеет с $\mathfrak{a}$ общих множителей, отличных от множителей идеала $\mathfrak{b}$.

Следствие 1. *В кольце классов вычетов $\mathfrak{o}/\mathfrak{a}$ каждый идеал $\mathfrak{b}/\mathfrak{a}$ является главным.*

Действительно, идеал $\mathfrak{b}/\mathfrak{a}$ порождается классом вычетов $\mathfrak{a} + d$.

Следствие 2. *Каждый идеал $\mathfrak{b}$ обладает базисом из двух элементов (a, d), где $a \neq 0$ — произвольно выбранный элемент из $\mathfrak{b}$.*

Действительно, пусть a — произвольный ненулевой элемент из $\mathfrak{b}$ и $\mathfrak{a} = (a)$. В соответствии с теоремой, приведенной выше, $(a, d) = \mathfrak{b}$.

Следствие 3. *Каждый идеал $\mathfrak{b}$ с помощью умножения на некоторый идеал $\mathfrak{d}$, взаимно простой с заданным идеалом $\mathfrak{c}$, может быть превращен в главный идеал.*

Доказательство. Положим $\mathfrak{a} = \mathfrak{c}\mathfrak{d}$. В соответствии с вышеприведенной теоремой имеем

$$(\mathfrak{a}, d) = \mathfrak{b}. \tag{1}$$

Так как d делится на $\mathfrak{d}$, мы можем считать, что

$$(d) = \mathfrak{b}\mathfrak{d}.$$

Ввиду (1)

$$(\mathfrak{c}\mathfrak{d}, \mathfrak{b}\mathfrak{d}) = \mathfrak{b}.$$

Следовательно, $\mathfrak{c}$ и $\mathfrak{b}$ должны быть взаимно простыми.

Задача 1. Пусть $\mathfrak{O}$ — кольцо всех частных a/b, где a и b — целые и b не делится на некоторые наперед заданные простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Тогда каждому идеалу $\mathfrak{a}$ из $\mathfrak{o}$ соответствует некоторый идеал $\mathfrak{A}$ из $\mathfrak{O}$, состоящий из дробей a/b, где $a \in \mathfrak{a}$. Идеалам $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ соответствуют простые идеалы $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, а всем остальным простым идеалам из $\mathfrak{o}$ соответствует единичный идеал $\mathfrak{O}$. Каждый идеал в $\mathfrak{O}$ однозначно представляется в виде произведения степеней идеалов $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. Кроме того, в кольце $\mathfrak{O}$ каждый идеал является главным.

§ 139. Дробные идеалы

В § 137 $\mathfrak{o}$-модуль в поле частных Σ был назван *дробным идеалом*, если он обладает конечным базисом. Таким образом, идеалы в $\mathfrak{o}$, или «целые идеалы», являются частным случаем дробных идеалов.

Если $(\sigma_1 \ldots, \sigma_r)$ — базис некоторого дробного идеала, то с помощью умножения на подходящий знаменатель можно сделать все элементы базиса — а с ними и весь идеал — целыми.

Обратно, если некоторый $\mathfrak{o}$-модуль $\mathfrak{a}$ при умножении на какой-то целый элемент $b \neq 0$ становится целым идеалом, то в целом идеале $b\mathfrak{a}$ имеется конечный базис

$$b\mathfrak{a} = (a_1, \ldots, a_r),$$

а потому

$$\mathfrak{a} = \left(\frac{a_1}{b}, \ldots, \frac{a_r}{b}\right).$$

Тем самым мы доказали следующее предложение:

Произвольный $\mathfrak{o}$-модуль в поле Σ является дробным идеалом тогда и только тогда, когда он может быть сделан целым идеалом с помощью умножения на некоторый целый элемент $b \neq 0$.

Мы уже видели, что вместе с $\mathfrak{a}$ и $\mathfrak{b}$ идеалы $\mathfrak{a} \cdot \mathfrak{b}$ и $(\mathfrak{a}, \mathfrak{b})$ имеют конечные базисы, а потому они одновременно являются и дробными идеалами. То же самое остается верным и для частного модулей $\mathfrak{a} : \mathfrak{b}$, где $\mathfrak{a}$ и $\mathfrak{b}$ — целые идеалы и $\mathfrak{b} \neq 0$ [1]). Действительно, если $b \neq 0$ — произвольный элемент из $\mathfrak{b}$, то

$$b \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{b} \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a} \subseteq \mathfrak{o},$$

так что $\mathfrak{a} : \mathfrak{b}$ с помощью умножения на b становится целым идеалом.

В частности, $\mathfrak{o} : \mathfrak{p} = \mathfrak{p}^{-1}$ — дробный идеал.

Каждый целый или дробный ненулевой идеал обладает обратным.

Доказательство. Пусть $\mathfrak{c}$ — целый или дробный ненулевой идеал и элемент $b \neq 0$ выбран так, что идеал $b\mathfrak{c}$ целый:

$$b\mathfrak{c} = \mathfrak{a}. \tag{1}$$

---

[1]) Под *частным модулей* $\mathfrak{a} : \mathfrak{b}$ (в поле Σ) мы подразумеваем совокупность элементов λ из Σ, для которых $\lambda\mathfrak{b} \subseteq \mathfrak{a}$.

Если теперь $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r$, то умножение равенства (1) на $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\ldots\ldots\mathfrak{p}_r^{-1}$ дает в соответствии с теоремой 1 (§ 137)

$$(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\ldots\mathfrak{p}_r^{-1}\mathfrak{b})\,\mathfrak{c}=\mathfrak{o},$$

чем и доказано существование обратного идеала

$$\mathfrak{c}^{-1}=\mathfrak{p}_1^{-1}\ldots\mathfrak{p}_r^{-1}\mathfrak{b}.$$

Из этого предложения следует: *целые и дробные ненулевые идеалы образуют абелеву группу.*

Уравнение $\mathfrak{a}\mathfrak{c}=\mathfrak{b}$ однозначно решается относительно неизвестного $\mathfrak{c}$. Решением будет $\mathfrak{a}^{-1}\mathfrak{b}$, в других обозначениях, $\mathfrak{b}/\mathfrak{a}$.

Из доказанных ранее теорем теперь следует:

Каждый дробный идеал является отношением двух целых идеалов, т. е. представляется в виде

$$\frac{\mathfrak{p}_1'\ldots\mathfrak{p}_s'}{\mathfrak{p}_1''\ldots\mathfrak{p}_t''}.$$

При этом можно сокращать каждый идеал, участвующий одновременно как в числителе, так и в знаменателе.

Каждый дробный главный идеал (λ) *допускает представление в виде частного двух целых главных идеалов, в котором ни один из* r *любых наперед заданных простых идеалов не входит одновременно в числитель и знаменатель.*

Доказательство. Пусть после сокращения

$$(\lambda)=\frac{\mathfrak{p}_1'\ldots\mathfrak{p}_s'}{\mathfrak{p}_1''\ldots\mathfrak{p}_t''}$$

и $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ — наперед заданные r простых идеалов. С помощью умножения на некоторый идеал $\mathfrak{b}$, взаимно простой с произведением $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r$, мы получим в знаменателе некоторый главный идеал (d):

$$(\lambda)=\frac{\mathfrak{b}\mathfrak{p}_1'\ldots\mathfrak{p}_s'}{\mathfrak{b}\mathfrak{p}_1''\ldots\mathfrak{p}_t''}=\frac{\mathfrak{b}\mathfrak{p}_1'\ldots\mathfrak{p}_s'}{(d)},$$

следовательно,

$$\mathfrak{b}\mathfrak{p}_1'\ldots\mathfrak{p}_s'=(\lambda d).$$

Таким образом, и числитель оказался главным идеалом. При этом ни один из идеалов $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ не входит в числитель и знаменатель.

Задача. Дробь-идеал $\mathfrak{a}^{-1}\mathfrak{b}$ есть частное модулей $\mathfrak{b}:\mathfrak{a}$.

По поводу дальнейших сведений из теории идеалов в числовых полях мы отсылаем читателя к книге: Гекке Э. Лекции по теории алгебраических чисел. — М.: Гостехиздат, 1939. По поводу теории идеалов в функциональных полях и ее приложений отсылаем читателя к фундаментальной работе Дедекинда и Вебера (Dedekind R., Weber H.). — Crelle's J., 1882, 92, S. 181.

§ 140. Теория идеалов в произвольных целозамкнутых целостных кольцах

Существуют важные целостные кольца, удовлетворяющие аксиомам I и III, но не удовлетворяющие аксиоме II из § 137. Обратимся, например, к кольцу многочленов $K[x_1, \ldots, x_n]$ более чем от одной переменной или к кольцу целочисленных многочленов и их конечным целозамкнутым расширениям (главным порядкам). Во всех этих кольцах есть простые идеалы, отличные от нулевого и единичного, обладающие собственными делителями — простыми идеалами с этим же свойством. В таких кольцах нельзя, следовательно, применять теорию идеалов из § 137. Покажем, что, несмотря на это, основные результаты развитой теории остаются верными, если заменить отношение равенства идеалов отношением «квазиравенства», определяемым ниже [1]).

Итак, пусть $\mathfrak{o}$ — целостное кольцо, целозамкнутое в своем поле частных Σ. Готические буквы в дальнейшем будут обозначать ненулевые дробные идеалы, т. е. $\mathfrak{o}$-модули в Σ, которые становятся целыми идеалами при умножении на подходящий ненулевой элемент из $\mathfrak{o}$. Под обратным идеалом $\mathfrak{a}^{-1}$ опять будет подразумеваться совокупность тех элементов r из Σ, для которых идеал $r\mathfrak{a}$ является целым.

Определим: идеал $\mathfrak{a}$ *квазиравен* идеалу $\mathfrak{b}$, если $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$. Обозначение: $\mathfrak{a} \sim \mathfrak{b}$. Отношение $\sim$, очевидно, рефлексивно, симметрично и транзитивно.

Равным образом идеал $\mathfrak{a}$ называется *квазиделителем* идеала $\mathfrak{b}$, а $\mathfrak{b}$ — *квазикратным* идеала $\mathfrak{a}$, если $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$ или, что то же самое, если $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал. Обозначение: $\mathfrak{a} \leqslant \mathfrak{b}$ или $\mathfrak{b} \geqslant \mathfrak{a}$.

Простейшие свойства символов $\leqslant$ и $\sim$ таковы:

1. Из $\mathfrak{a} \supseteq \mathfrak{b}$ следует $\mathfrak{a} \leqslant \mathfrak{b}$. (Доказательство очевидно.)

2. Если $\mathfrak{a}$ — главный идеал: $\mathfrak{a} = (a)$, то, обратно, из $\mathfrak{a} \leqslant \mathfrak{b}$ следует $\mathfrak{a} \supseteq \mathfrak{b}$. Действительно, тогда $\mathfrak{a}^{-1} = (a^{-1})$; из предположения о том, что $\mathfrak{a}^{-1}\mathfrak{b}$ — целый идеал, следует, что $a^{-1}\mathfrak{b}$ — целый идеал, т. е. все элементы из $\mathfrak{b}$ делятся на a.

3. Если $\mathfrak{a} \leqslant \mathfrak{b}$ и одновременно $\mathfrak{a} \geqslant \mathfrak{b}$, то $\mathfrak{a} \sim \mathfrak{b}$.

4. Все квазикратные $\mathfrak{b}$ идеала $\mathfrak{a}$ и, в частности, все квазиравные идеалу $\mathfrak{a}$ идеалы $\mathfrak{b}$ обладают свойством: $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. (Немедленное следствие из целостности идеала $\mathfrak{b}\mathfrak{a}^{-1}$.)

Таким образом, в частности, $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. Согласно 1 отсюда следует, что $\mathfrak{a} \geqslant (\mathfrak{a}^{-1})^{-1}$. С другой стороны, идеал $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ целый, так что $\mathfrak{a} \leqslant (\mathfrak{a}^{-1})^{-1}$, и мы получили свойство

5. $\mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}$.

---

[1]) Теория, опубликованная автором в Math. Ann., 1929, **101**, была впоследствии приведена Артином в более стройный вид и публикуется здесь именно в таком виде.

Согласно 4 и 5 идеал $(\mathfrak{a}^{-1})^{-1}$ является *наибольшим из содержащих* $\mathfrak{a}$ *и квазиравных ему*. Мы будем обозначать идеал $(\mathfrak{a}^{-1})^{-1}$ через $\mathfrak{a}^*$.

6. Если $\mathfrak{a} \leqslant \mathfrak{b}$, то $\mathfrak{a}\mathfrak{c} \leqslant \mathfrak{b}\mathfrak{c}$. Действительно, $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{a}$ является целым, так что $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$ и $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{b}$ — целый идеал; следовательно, $\mathfrak{c}\mathfrak{a} \leqslant \mathfrak{c}\mathfrak{b}$.

7. Если $\mathfrak{a} \sim \mathfrak{b}$, то $\mathfrak{a}\mathfrak{c} \sim \mathfrak{c}\mathfrak{b}$. (Следствие из 6.)

8. Если $\mathfrak{a} \sim \mathfrak{b}$ и $\mathfrak{c} \sim \mathfrak{d}$, то $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$. (Потому что в соответствии с 7 имеем $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$.)

Если все идеалы, квазиравные некоторому фиксированному идеалу, объединить в один класс, то класс произведения $\mathfrak{a}\mathfrak{c}$ будет, в соответствии с 8, зависеть лишь от класса идеала $\mathfrak{a}$ и класса идеала $\mathfrak{c}$. Следовательно, мы можем определить *произведение* двух последних классов как класс произведения $\mathfrak{a}\mathfrak{c}$.

9. Единичным классом относительно умножения классов является класс идеалов, квазиравных единичному идеалу $\mathfrak{o}$, потому что для каждого $\mathfrak{a}$ имеет место равенство $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$.

10. Все квазикратные кольца $\mathfrak{o}$ и, в частности, все идеалы единичного класса являются целыми. (Частный случай свойства 2: нужно положить $a = 1$.) Следствие: все идеалы, квазиравные некоторому целому идеалу, являются целыми.

Мы докажем теперь важнейшее свойство обращения:

11. $\mathfrak{a}\mathfrak{a}^{-1} \sim \mathfrak{o}$.

То, что $\mathfrak{a}\mathfrak{a}^{-1} \geqslant \mathfrak{o}$, очевидно, потому что $\mathfrak{a}\mathfrak{a}^{-1}$ — целый идеал. Остается доказать, что $\mathfrak{a}\mathfrak{a}^{-1} \leqslant \mathfrak{o}$ или $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteq \mathfrak{o}$. Если λ принадлежит $(\mathfrak{a}\mathfrak{a}^{-1})^{-1}$, то идеал $\lambda\mathfrak{a}\mathfrak{a}^{-1}$ является целым, а потому $\lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, откуда $\lambda^2\mathfrak{a}^{-1} \subseteq \lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ и т. д., и вообще $\lambda^n\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, так что $\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ — целый идеал. Если μ — произвольный элемент из $\mathfrak{a}^{-1}\mathfrak{a}$, то все степени элемента λ после умножения на μ становятся целыми. С помощью условия целозамкнутости кольца $\mathfrak{o}$, аналогично тому, как это было при доказательстве теоремы 1 из § 137, получается, что сам элемент λ является целым.

Из 11 следует, что при определенном выше умножении классов класс идеала $\mathfrak{a}^{-1}$ является обратным по отношению к классу идеала $\mathfrak{a}$: произведение классов идеалов $\mathfrak{a}$ и $\mathfrak{a}^{-1}$ есть единичный класс. Отсюда получается

Теорема 1. *Классы квазиравных идеалов образуют группу.*

Следующие два утверждения позволяют рассматривать квазиделимость и квазиравенство как делимость и соответственно равенство с точностью до множителей из единичного класса:

12. Из $\mathfrak{a} \geqslant \mathfrak{b}$ следует, что $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$, где $\mathfrak{c} \sim \mathfrak{o}$ и идеал $\mathfrak{d}$ целый. В частности, $\mathfrak{a} \sim \mathfrak{b}\mathfrak{d}$.

13. Из $\mathfrak{a} \sim \mathfrak{b}$ следует, что $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$, где $\mathfrak{c} \sim \mathfrak{o}$ и $\mathfrak{d} \sim \mathfrak{o}$.

Действительно, в обоих случаях $\mathfrak{a}(\mathfrak{b}\mathfrak{b}^{-1}) = \mathfrak{b}(\mathfrak{a}\mathfrak{b}^{-1})$.

Наибольший общий делитель $(\mathfrak{a}, \mathfrak{b})$ является, конечно, квазиделителем как идеала $\mathfrak{a}$, так и идеала $\mathfrak{b}$. Покажем теперь, что:

14. Каждый общий квазиделитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$ является квазиделителем и идеала $(\mathfrak{a}, \mathfrak{b})$. Действительно, если $\mathfrak{c}$ — один из таких делителей, то $\mathfrak{c}^*$ — общий делитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$, а потому и идеала $(\mathfrak{a}, \mathfrak{b})$.

Два целых идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *квазивзаимно простыми*, если $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$, или, что то же, если каждый целый общий квазиделитель идеалов $\mathfrak{a}$ и $\mathfrak{b}$ квазиравен кольцу $\mathfrak{o}$.

15. Если идеал $\mathfrak{a}$ является квазивзаимно простым с идеалами $\mathfrak{b}$ и $\mathfrak{c}$, то он является таковым и по отношению к произведению $\mathfrak{bc}$. Действительно, в этом случае

$$(\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{ac}, \mathfrak{ba}, \mathfrak{bc}) \subseteq (\mathfrak{a}, \mathfrak{bc}).$$

Левая часть квазиравна кольцу $\mathfrak{o}$, а потому и правая часть должна быть такой же.

Следуя Артину, докажем теперь такое предложение:

Теорема 2 (теорема о продолжении). *Если даны два разложения некоторого целого идеала* $\mathfrak{a}$:

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2 \ldots \mathfrak{c}_n, \tag{1}$$

то оба произведения можно дальше разложить так, чтобы они совпадали с точностью до порядка следования сомножителей и квазиравенства:

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu}, \quad \mathfrak{c}_\mu \sim \prod_\lambda \mathfrak{b}_{\lambda\mu}. \tag{2}$$

Доказательство. Положим $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$. В силу 12 имеем $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$ и $\mathfrak{c}_1 \sim \mathfrak{b}_{11}\mathfrak{c}_1'$. Следовательно, $\mathfrak{b}_{11} = (\mathfrak{b}_1, \mathfrak{c}_1) \sim (\mathfrak{b}_{11}\mathfrak{b}_1', \mathfrak{b}_{11}\mathfrak{c}_1') = \mathfrak{b}_{11}(\mathfrak{b}_1', \mathfrak{c}_1')$, так что $(\mathfrak{b}_1', \mathfrak{c}_1') \sim \mathfrak{o}$. Положим далее $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$. В силу 12 имеем $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1''$ и $\mathfrak{c}_2 = \mathfrak{b}_{12}\mathfrak{c}_2'$, откуда вновь следует, что $(\mathfrak{b}_1'', \mathfrak{c}_2') \sim \mathfrak{o}$. Продолжая таким образом, мы в конце концов получим, что $\mathfrak{b}_1 = \mathfrak{b}_{11}\mathfrak{b}_{12} \ldots \mathfrak{b}_{1n}\mathfrak{d}$ и $\mathfrak{c}_\mu = \mathfrak{b}_{1\mu}\mathfrak{c}_\mu'$ $(\mu = 1, 2, \ldots, n)$. Подставим это в (1); тогда окажется, что

$$\mathfrak{b}_{11}\mathfrak{b}_{12} \ldots \mathfrak{b}_{1n}\mathfrak{d}\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{b}_{11}\mathfrak{c}_1'\mathfrak{b}_{12}\mathfrak{c}_2' \ldots \mathfrak{b}_{1n}\mathfrak{c}_n'.$$

В силу группового свойства (теорема 1) можно сократить на $\mathfrak{b}_{11} \ldots \mathfrak{b}_{1n}$:

$$\mathfrak{d}\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \ldots \mathfrak{c}_n'.$$

Идеал $\mathfrak{d}$ квазивзаимно прост со всеми $\mathfrak{c}_\mu'$ и, значит, с произведением $\mathfrak{c}_1'\mathfrak{c}_2' \ldots \mathfrak{c}_n'$. Однако $\mathfrak{d}$ входит в качестве множителя в левую часть соотношения, а потому является делителем произведения $\mathfrak{c}_1'\mathfrak{c}_2' \ldots \mathfrak{c}_n'$. Значит, должно иметь место квазиравенство $\mathfrak{d} \sim \mathfrak{o}$ и можно отбросить множитель $\mathfrak{d}$ тоже:

$$\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \ldots \mathfrak{c}_n'.$$

Эти рассуждения теперь можно повторить для $\mathfrak{b}_2, \ldots, \mathfrak{b}_m$ и получить в конце концов требуемые разложения (2).

Начиная с этого места, все готические буквы будут обозначать целые ненулевые идеалы. Такой идеал $\mathfrak{p}$ мы будем называть *неразложимым*, если он не является квазиравным идеалу $\mathfrak{o}$ и если в каждом представлении в виде произведения $\mathfrak{p} \sim \mathfrak{a}\mathfrak{b}$ один из сомножителей обязательно принадлежит единичному классу, или, что в силу 12 то же самое, если идеал $\mathfrak{p}$, не являясь квазиравным идеалу $\mathfrak{o}$, не имеет множителей, отличных от $\mathfrak{p}$ и от $\mathfrak{o}$ в смысле отношения квазиравенства.

Если заменить неразложимый идеал $\mathfrak{p}$ на максимальный содержащий его идеал $\mathfrak{p}^*$, то каждый собственный делитель идеала $\mathfrak{p}^*$ не будет квазиравен идеалу $\mathfrak{p}$, а потому обязан быть квазиравным идеалу $\mathfrak{o}$. Каждый идеал, квазикратный идеалу $\mathfrak{p}$ или идеалу $\mathfrak{p}^*$, является в силу 4 кратным идеала $\mathfrak{p}^*$. Отсюда получается

16. Идеал $\mathfrak{p}^*$ является простым.

Действительно, если некоторое произведение $\mathfrak{b}\mathfrak{c}$ двух главных идеалов $\mathfrak{b}$ и $\mathfrak{c}$ делится на $\mathfrak{p}^*$, но $\mathfrak{b}$ не делится на $\mathfrak{p}^*$, то идеал $(\mathfrak{b}, \mathfrak{p}^*)$ является собственным делителем идеала $\mathfrak{p}^*$, а потому он квазиравен $\mathfrak{o}$, откуда

$$\mathfrak{c} = \mathfrak{o}\mathfrak{c} \sim (\mathfrak{b}, \mathfrak{p}^*)\mathfrak{c} = (\mathfrak{b}\mathfrak{c}, \mathfrak{p}^*\mathfrak{c}) \geqslant (\mathfrak{p}^*, \mathfrak{p}^*) = \mathfrak{p}^*,$$

следовательно, идеал $\mathfrak{c}$ является квазикратным идеала $\mathfrak{p}^*$, а потому он делится на $\mathfrak{p}^*$.

Если предположить, что в $\mathfrak{o}$ выполнена теорема о цепях делителей, то окажется справедливым следующее:

17. Цепь целых идеалов $\mathfrak{a}_1 > \mathfrak{a}_2 > \ldots$, в которой каждый последующий идеал является собственным квазиделителем предыдущего (т. е. квазиделителем, не являющимся квазиравным), обрывается после конечного числа шагов.

Действительно, если заменить идеалы $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ наибольшими квазиравными идеалами $\mathfrak{a}_1^*, \mathfrak{a}_2^*, \ldots$, то получится цепь из целых идеалов $\mathfrak{a}_1^* \subset \mathfrak{a}_2^* \subset \ldots$, которая, в соответствии с теоремой о цепях делителей, должна оборваться.

Можно сформулировать «теорему о цепях квазиделителей» (утверждение 17) как «принцип индукции по делителям» (см. § 115, четвертая формулировка теоремы о цепях делителей). Из этого принципа без труда получается, что каждый целый идеал квазиравен некоторому произведению неразложимых идеалов. Однозначность разложения получается как частный случай теоремы о продолжении (теорема 2). Таким образом, имеет место

Теорема 3. *Каждый ненулевой целый идеал квазиравен произведению неразложимых идеалов* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *(в качестве которых, конечно, можно выбрать простые идеалы* $\mathfrak{p}_1^*, \mathfrak{p}_2^*, \ldots, \mathfrak{p}_r^*$*), определенному однозначно с точностью до порядка следования сомножителей и квазиравенства.*

Следствие. Идеал $\mathfrak{a} \sim \mathfrak{p}_1 \ldots \mathfrak{p}_r$ тогда и только тогда квазиделится на $\mathfrak{b} \sim \mathfrak{p}_1' \ldots \mathfrak{p}_s'$, когда каждый множитель $\mathfrak{p}_i'$, входящий в разложение идеала $\mathfrak{b}$, входит в разложение идеала $\mathfrak{a}$ в не меньшей степени. В частности, если $\mathfrak{b}$ — главный идеал, то, согласно 2, из квазиделимости следует обычная делимость. Если в качестве $\mathfrak{a}$ и $\mathfrak{b}$ взять главные идеалы (a) и (b), то получится критерий делимости элемента a на элемент b или того, что элемент ab^{-1} целый. При добавлении классов неглавных идеалов к главным идеалам получится область, в которой, согласно теореме 3, имеет место однозначность разложения на простые множители, а этим и достигается цель «классической теории идеалов».

Теорема 3 имеет место и для дробных идеалов $\mathfrak{a}b^{-1}$, но в этом случае нужно рассматривать и отрицательные степени

$$\mathfrak{p}^{-k} = (\mathfrak{p}^{-1})^k.$$

Действительно, если

$$\mathfrak{a} \sim \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_r^{a_r} \quad \text{и} \quad (b) \sim \mathfrak{p}_1^{b_1} \ldots \mathfrak{p}_r^{b_r},$$

то

$$\mathfrak{a}b^{-1} \sim \mathfrak{p}_1^{a_1-b_1} \ldots \mathfrak{p}_r^{a_r-b_r}, \tag{3}$$

и показатели $a_i - b_i$ определены однозначно.

Чтобы выяснить отношение построенной сейчас теории к общей теории идеалов и к конкретной теории идеалов, развитой в § 137, мы должны выяснить, какие же простые идеалы являются неразложимыми и какие идеалы квазиравны единичному идеалу $\mathfrak{o}$.

Мы уже видели, что для неразложимого идеала $\mathfrak{p}$ идеал $\mathfrak{p}^*$ является простым. Докажем теперь следующее утверждение:

18. Любое ненулевое собственное кратное такого идеала $\mathfrak{p}^*$ не является простым.

Действительно, если $\mathfrak{a}$ — такое кратное, то $\mathfrak{a} \geqslant \mathfrak{p}^*$; в силу 12 в этом случае $\mathfrak{a}\mathfrak{c} = \mathfrak{p}^*\mathfrak{b}$, где $\mathfrak{c} \sim \mathfrak{o}$. Так как в разложении идеала $\mathfrak{b}$ каждый простой множитель участвует меньшее число раз, чем в $\mathfrak{a}$, то $\mathfrak{b} \not\equiv 0\,(\mathfrak{a})$; точно так же $\mathfrak{p}^* \not\equiv 0\,(\mathfrak{a})$, но $\mathfrak{p}^*\mathfrak{b} \equiv 0\,(\mathfrak{a})$. Следовательно, идеал $\mathfrak{a}$ не является простым.

Рассмотрим разложение произвольного простого идеала $\mathfrak{p}$. Либо $\mathfrak{p} \sim \mathfrak{o}$, либо в разложении $\mathfrak{p} \sim \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ участвует некоторый неразложимый множитель $\mathfrak{p}_1$. Тогда $\mathfrak{p} \geqslant \mathfrak{p}_1$ и, следовательно, $\mathfrak{p} \subseteq \mathfrak{p}_1^*$; но так как собственное кратное идеала $\mathfrak{p}_1^*$ не может быть простым идеалом, то должно иметь место равенство $\mathfrak{p} = \mathfrak{p}_1^*$. Следовательно,

$$\mathfrak{p}^* = (\mathfrak{p}_1^*)^* = \mathfrak{p}_1^* = \mathfrak{p},$$

а потому имеет место

19. Каждый простой идеал $\mathfrak{p}$ либо квазиравен $\mathfrak{o}$, либо неразложим и равен соответствующему $\mathfrak{p}^*$.

Во втором случае идеал $\mathfrak{p}$ не имеет ненулевых собственных кратных, являющихся простыми идеалами. Напротив, в первом случае, как сейчас будет показано, такое кратное всегда существует:

20. Если $\mathfrak{p} \sim \mathfrak{o}$, то существует неразложимый простой идеал $\mathfrak{p}_\nu^*$, являющийся собственным кратным идеала $\mathfrak{p}$. Действительно, если $p \neq 0$ — произвольный элемент из $\mathfrak{p}$ и $(p) \sim \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \sim \mathfrak{p}_1^*\mathfrak{p}_2^* \ldots \mathfrak{p}_r^*$ — его разложение, то из 2 следует, что $\mathfrak{p}_1^*\mathfrak{p}_2^* \ldots \mathfrak{p}_r^* \equiv 0\,(p) \equiv 0(\mathfrak{p})$, откуда $\mathfrak{p}_\nu^* \equiv 0\,(\mathfrak{p})$ при некотором ν. Но вместе с тем $\mathfrak{p}_\nu^* \neq \mathfrak{p}$, так как иначе выполнялось бы соотношение $\mathfrak{p}_\nu^* \sim \mathfrak{o}$.

Если мы назовем простой идеал, не имеющий никакого простого собственного кратного, отличного от нулевого идеала, *высоким*, а простой идеал, обладающий таким кратным, напротив, *низким*, то свойства 18, 19 и 20 можно объединить в следующей теореме:

Теорема 4. *Каждый высокий простой идеал $\mathfrak{p}$ неразложим и равен своему $\mathfrak{p}^*$; каждый низкий простой идеал квазиравен $\mathfrak{o}$.*

Идеал, не принадлежащий единичному классу, согласно теореме 3 о разложении, делится по крайней мере на один высокий простой идеал $\mathfrak{p} = \mathfrak{p}^*$. Но любой идеал из единичного класса не делится ни на какой высокий простой идеал. Тем самым единичный класс получает характеристику исключительно в терминах теории идеалов (т. е. без обращения к нецелым идеалам).

В силу аксиомы II в кольцах, описанных в § 137, каждый ненулевой простой идеал делится только на себя и на $\mathfrak{o}$; следовательно, там нет низких простых идеалов, отличных от $\mathfrak{o}$. Так как каждый идеал $\mathfrak{a} \neq \mathfrak{o}$ делится на некоторый простой идеал, не равный $\mathfrak{o}$ (доказательство: найдем среди делителей идеала $\mathfrak{a}$, не равных $\mathfrak{o}$, наибольший; он будет свободен от делителей и, следовательно, простой), то $\mathfrak{a}$ не может быть квазиравным $\mathfrak{o}$. Тем самым единичный класс состоит из одного лишь единичного идеала $\mathfrak{o}$. Из свойства 12 далее следует, что квазиделимость и делимость равносильны, а отсюда или из свойства 13 — что равносильны квазиравенство и равенство. Таким образом, теория идеалов из § 137 содержится как частный случай в изложенной здесь теории.

Теперь легко установить связи и с общей теорией идеалов, изложенной в пятнадцатой главе. Прежде всего, легко видеть, что каждый примарный идеал, у которого соответствующий простой идеал является низким, должен быть квазиравен идеалу $\mathfrak{o}$. Назовем эти примарные идеалы *низкими*, а остальные — *высокими примарными идеалами*. Идеал $\mathfrak{a}$ тогда и только тогда квазиравен идеалу $\mathfrak{o}$, когда все его примарные компоненты являются низкими. Если у идеалов $\mathfrak{a}$ и $\mathfrak{b}$ высокие примарные компоненты одинаковые (а низкие могут быть и различными),

то эти идеалы квазиравны. Среди идеалов, квазиравных данному идеалу $\mathfrak{a}$, существует наибольший в смысле включения идеал $\mathfrak{a}^*$; он получается отбрасыванием всех низких примарных компонент из разложения $\mathfrak{a}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$. Теоремы о разложении и единственности из этого параграфа можно интерпретировать так, что при этом все низкие примарные компоненты последовательно опускаются, а принимаются во внимание лишь высокие. Каждый из высоких примарных идеалов делится только на один высокий простой идеал и, следовательно, при разложении, в соответствии с теоремой 2, он оказывается равным некоторой степени простого идеала; иными словами, *каждый высокий примарный идеал квазиравен степени простого идеала.*

Обратно, каждая степень высокого простого идеала квазиравна некоторому высокому примарному идеалу. Действительно, если $\mathfrak{a}=\mathfrak{p}^r$ — степень высокого простого идеала, то $\mathfrak{a}$ не может делиться больше ни на какой другой высокий простой идеал (а только на $\mathfrak{p}$); следовательно, в разложении

$$\mathfrak{a}=\mathfrak{p}^r=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

участвует только один высокий примарный идеал. Если им является, скажем, $\mathfrak{q}_1$, то $\mathfrak{a}^*=\mathfrak{q}_1$; следовательно, идеал $\mathfrak{a}=\mathfrak{p}^r$ квазиравен примарному идеалу $\mathfrak{q}_1$.

Впрочем, идеал $\mathfrak{q}_1$ — это в точности определенная в § 120 r-я символическая степень простого идеала $\mathfrak{p}$. *Тем самым высокие примарные идеалы — это в точности символические степени высоких простых идеалов.*

Идеалы $\mathfrak{a}$, для которых $\mathfrak{a}^*=\mathfrak{a}$, называются, в соответствии с терминологией Прюфера, *v-идеалами.* Целые v-идеалы — это идеалы, в примарном разложении которых участвуют только высокие примарные идеалы. Все главные идеалы являются v-идеалами. В каждом классе квазиравных идеалов существует один-единственный v-идеал $\mathfrak{a}_v=\mathfrak{a}^*$. Если, следуя Прюферу и Круллю, ограничиться лишь v-идеалами, то понятие квазиравенства окажется ненужным. Основная теорема (теорема 3) переформулируется так:

Каждый v-идеал представляется единственным образом в виде пересечения символических степеней $\mathfrak{p}^{(r)}$ высоких примарных идеалов.

Задача 1. Все результаты этого параграфа справедливы и в кольцах с делителями нуля, если только ограничиться идеалами, не делящими нулевой идеал, а вместо поля частных взять кольцо частных.

Задача 2. Из теоремы 1 следует целозамкнутость кольца (см. § 138).

Задача 3. Доказать, что $\mathfrak{a}:\mathfrak{b}\sim\mathfrak{a}\mathfrak{b}^{-1}$.

Дальнейшие обобщения результатов этого параграфа см. в работах: Прюфер (Prüfer H.). — J. reine angew. Math., 1932, **168**, S. 1—36; Лоренцен (Lorenzen P.). — Math. Z., 1939, **45**, S. 533—553.

Сводка результатов теории идеалов

Следующее сопоставление показывает значение для теории идеалов в целостных кольцах сформулированных в § 128 аксиомы I (теорема о цепях делителей), аксиомы II (каждый простой идеал не имеет делителей) и аксиомы III (целозамкнутости):

из I следует: каждый идеал является наименьшим общим кратным некоторых примарных идеалов; соответствующие простые идеалы определены однозначно;

из I и II: каждый идеал является произведением однократных примарных идеалов; представление единственно;

из I и III: каждый идеал квазиравен некоторому произведению степеней простых идеалов; имеет место единственность с точностью до квазиравенства;

из I, II и III: каждый идеал есть произведение степеней простых идеалов; имеет место единственность.