Глава десятая

БЕСКОНЕЧНЫЕ РАСШИРЕНИЯ ПОЛЕЙ

Каждое поле получается из своего простого подполя с помощью конечного или бесконечного расширения. В главах 6 и 8 мы рассмотрели конечные расширения полей; в этой главе рассматриваются бесконечные расширения полей, сначала алгебраические, а затем — трансцендентные.

§ 72. Алгебраически замкнутые поля

Среди алгебраических расширений заданного поля важную роль играют, конечно, *максимальные* алгебраические расширения, т. е. такие, которые не допускают дальнейшего алгебраического расширения. Существование таких расширений будет доказано в настоящем параграфе.

Чтобы поле Ω было максимальным алгебраическим расширением, необходимо следующее условие: каждый многочлен кольца $\Omega[x]$ полностью разлагается на линейные множители (иначе можно было бы, в соответствии с § 39, расширить поле Ω с помощью присоединения корня какого-либо нелинейного неразложимого множителя). Это условие является и достаточным. Действительно, если каждый многочлен в $\Omega[x]$ разлагается на линейные множители, то все простые многочлены в $\Omega[x]$ линейны и каждый элемент любого алгебраического расширения Ω' поля Ω оказывается корнем некоторого линейного многочлена $x-a$ в $\Omega[x]$, т. е. совпадает с некоторым элементом a поля Ω.

Поэтому дадим следующее определение:

Поле Ω называется алгебраически замкнутым, если любой многочлен в $\Omega[x]$ разлагается на линейные множители.

Равнозначное с этим определение таково: *поле Ω алгебраически замкнуто, если каждый отличный от константы многочлен из $\Omega[x]$ обладает в Ω хоть одним корнем, т. е. хоть одним линейным множителем в $\Omega[x]$.*

Действительно, если такое условие выполнено и произвольно взятый многочлен $f(x)$ разлагается на неразложимые множители, то все они должны быть линейными.

«Основная теорема алгебры», к которой мы вернемся в § 80, утверждает, что поле комплексных чисел алгебраически замкнуто. Следующим примером алгебраически замкнутого поля может слу-

жить поле всех комплексных алгебраических чисел, т. е. множество тех комплексных чисел, которые удовлетворяют какому-либо уравнению с рациональными коэффициентами. Комплексные корни уравнения с алгебраическими коэффициентами являются и в самом деле алгебраическими не только над полем алгебраических чисел, но и над полем рациональных чисел, т. е. сами являются алгебраическими числами.

В этом параграфе мы покажем, как построить алгебраически замкнутое расширение произвольно заданного поля P и притом чисто алгебраическим путем. Штейницу принадлежит следующая

Основная теорема. *Для каждого поля* P *существует алгебраически замкнутое алгебраическое расширение* Ω. *С точностью до эквивалентности это расширение определено однозначно: любые два алгебраически замкнутых алгебраических расширения* Ω, Ω' *поля* P *эквивалентны.*

Доказательству этой теоремы мы должны предпослать несколько лемм:

Лемма 1. *Пусть* Ω — *алгебраическое расширение поля* P. *Достаточным условием для того, чтобы* Ω *было алгебраически замкнутым, является разложение на линейные множители любого многочлена из* $\mathsf{P}[x]$ *в кольце* $\Omega[x]$.

Доказательство. Пусть $f(x)$ — произвольный многочлен из $\Omega[x]$. Если он не разлагается на линейные множители, то можно присоединить некоторый его корень α и прийти к собственному надполю Ω'. Элемент α является алгебраическим над Ω, а Ω является алгебраическим расширением поля P; следовательно, элемент α алгебраичен и над P. Поэтому он является корнем некоторого многочлена $g(x)$ из $\mathsf{P}[x]$. Этот многочлен разлагается в $\Omega[x]$ на линейные множители. Следовательно, α — корень некоторого линейного множителя в $\Omega[x]$, т. е. принадлежит полю Ω, что противоречит предположению.

Лемма 2. *Если поле* P *вполне упорядочено, то кольцо многочленов* $\mathsf{P}[x]$ *может быть вполне упорядочено и притом так, что в этом упорядочении поле* P *будет отрезком.*

Доказательство. Определим отношение порядка между многочленами $f(x)$ из $\mathsf{P}[x]$ следующим образом: пусть $f(x) < g(x)$, когда выполнено одно из условий:

1) степень $f(x)$ меньше степени $g(x)$;
2) степень $f(x)$ равна степени $g(x)$ и равна n, т. е.

$$f(x) = a_0x^n + \ldots + a_n, \quad g(x) = b_0x^n + \ldots + b_n$$

и при некотором индексе k:

$$a_i = b_i \text{ для } i < k,$$

$$a_k < b_k \text{ в смысле упорядочения поля } \mathsf{P}.$$

При этом для многочлена 0 делается исключение: ему присваивается степень 0. Очевидно, что таким способом получается некоторое упорядочение, в смысле которого $\mathsf{P}[x]$ вполне упорядочено. Показывается это так: в каждом непустом множестве многочленов есть непустое подмножество многочленов наименьшей степени; пусть таковая равна n. В этом подмножестве есть непустое подмножество многочленов, коэффициент a_0 которых является первым в смысле имеющегося порядка среди свободных членов рассматриваемых многочленов; в указанном подмножестве есть в свою очередь подмножество многочленов с первым a_1 и т. д. Подмножество с первым a_n, которое в конце концов получится, может состоять лишь из одного-единственного многочлена (так как $a_0, \ldots, a_n$ определяются однозначно благодаря последовательно выполняемому условию минимальности в выборе); этот многочлен является первым элементом в заданном множестве.

Лемма 3. *Если поле* P *вполне упорядочено и заданы многочлен* $f(x)$ *степени* n *и* n *символов* $\alpha_1, \ldots, \alpha_n$, *то поле* $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$, *в котором* $f(x)$ *полностью разлагается на линейные множители* $\prod_1^n (x-\alpha_i)$, *строится единственным образом и является вполне упорядоченным. Поле* P *в смысле этого порядка является отрезком.*

Доказательство. Мы будем присоединять корни $\alpha_1, \ldots, \alpha_n$ последовательно, вследствие чего из $\mathsf{P}=\mathsf{P}_0$ последовательно будут возникать поля $\mathsf{P}_1, \ldots, \mathsf{P}_n$. Предположим, что $\mathsf{P}_{i-1}=\mathsf{P}(\alpha_1, \ldots, \alpha_{i-1})$ — уже построенное поле и что P — отрезок в P_{i-1}; тогда P_i будет строиться так.

Прежде всего в силу леммы 2 кольцо многочленов $\mathsf{P}_{i-1}[x]$ вполне упорядочивается. Многочлен f разлагается в этом кольце на неразложимые множители, среди которых на первом месте будут стоять $x-\alpha_1, \ldots, x-\alpha_{i-1}$; среди остальных множителей пусть $f_i(x)$ будет первым в смысле имеющегося порядка. Вместе с символом α_i, обозначающим корень многочлена $f_i(x)$, мы определяем на основе § 39 поле $\mathsf{P}_i=\mathsf{P}_{i-1}(\alpha_i)$ как совокупность всех сумм

$$\sum_0^{h-1} c_\lambda \alpha_i^\lambda,$$

где h — степень многочлена $f_i(x)$. Если $f_i(x)$ линеен, то, конечно, мы полагаем $\mathsf{P}_i=\mathsf{P}_{i-1}$; символ α_i в этом случае не нужен. Построенное поле вполне упорядочивается с помощью следующего условия: каждому элементу поля $\sum_0^{h-1} c_\lambda \alpha_i^\lambda$ сопоставим многочлен $\sum_0^{h-1} c_\lambda x^\lambda$ и элементы поля упорядочим точно так же, как упорядочены соответствующие им многочлены.

Очевидно, тогда P_{i-1} является отрезком в P_i, а потому и P — отрезок в P_i.

Тем самым поля $\mathsf{P}_1, \ldots, \mathsf{P}_n$ построены и вполне упорядочены. Поле P_n является искомым однозначно определенным полем $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$.

Лемма 4. *Если в упорядоченном множестве полей каждое предшествующее поле является подполем последующего, то объединение этих полей является полем.*

Доказательство. Для любых двух элементов α, β объединения существуют два поля Σ_α, Σ_β, которые содержат α и β и из которых одно предшествует другому. В объемлющем поле определены элементы $\alpha+\beta$ и $\alpha\cdot\beta$ и именно так определяются эти элементы в каждом из полей, содержащих α и β, потому что из любых двух таких полей одно предшествует другому и является его подполем. Например, чтобы доказать закон ассоциативности

$$\alpha\beta\cdot\gamma=\alpha\cdot\beta\gamma,$$

найдем среди полей Σ_α, Σ_β, Σ_γ то, которое содержит два других поля (наибольшее); в этом поле содержатся α, β и γ и в нем закон ассоциативности выполнен. Тем же способом проверяются все остальные правила вычислений с элементами объединения.

Доказательство основной теоремы распадается на две части: построение поля Ω и доказательство единственности. Построение поля и доказательство единственности проводятся с помощью трансфинитной индукции в смысле § 71.

Построение поля Ω. Лемма 1 свидетельствует о том, что для построения алгебраически замкнутого расширения Ω поля P достаточно построить такое алгебраическое расширение поля P, чтобы каждый многочлен из $\mathsf{P}[x]$ разлагался над этим расширением на линейные множители.

Будем считать, что поле P, а потому и кольцо многочленов $\mathsf{P}[x]$, вполне упорядочены. Каждому многочлену $f(x)$ сопоставим столько новых символов $\alpha_1, \ldots, \alpha_n$, какова его степень.

Далее, каждому многочлену $f(x)$ сопоставим два вполне упорядоченных поля P_f, Σ_f, которые определяются следующим рекуррентным способом.

1. Поле P_f является объединением поля P и всех полей Σ_g для $g<f$.

2. Поле P_f вполне упорядочивается так, чтобы P и все поля Σ_g при $g<f$ были отрезками в P_f.

3. Поле Σ_f получается из P_f присоединением всех корней многочлена f с помощью символов $\alpha_1, \ldots, \alpha_n$ в соответствии с леммой 3.

Нужно доказать, что таким способом действительно однозначно определяются вполне упорядоченные поля P_f, Σ_f, если

только уже определены все предыдущие P_g, Σ_g, удовлетворяющие перечисленным выше требованиям.

Если выполнено требование 3, то прежде всего P_f — отрезок в Σ_f. Из этого и из требования 2 следует, что поле P и каждое поле $\Sigma_g\,(g<f)$ являются отрезками в Σ_f. Предположим, что рассматриваемые требования выполнены для всех предыдущих индексов f, так что

$$\mathsf{P} \text{ — отрезок в } \Sigma_h \text{ при } \quad h<f,$$
$$\Sigma_g \text{ — отрезок в } \Sigma_h \text{ при } g<h<f.$$

Отсюда следует, что поле P и поля $\Sigma_h\,(h<f)$ составляют множество того типа, о котором говорит лемма 4. Следовательно, объединение этих полей снова является полем, которое в соответствии с требованием 1 мы должны обозначить через P_f. Структура вполне упорядоченного поля на P_f однозначно определяется требованием 2, потому что любые два элемента a, b из P_f принадлежат одному из полей P или Σ_g и поэтому связаны отношением $a<b$ или $a>b$, которое должно сохраняться в P_f. Это отношение порядка является одним и тем же во всех полях P или Σ_g, которые содержат как a, так и b, потому что все эти поля являются отрезками друг друга. Итак, отношение порядка определено. То, что оно определяет вполне упорядоченное множество, очевидно, так как каждое непустое множество $\mathfrak{M}$ в P_f содержит по меньшей мере один элемент из P или из некоторого поля Σ_g, а потому и первый элемент из $\mathfrak{M}\cap\mathsf{P}$ или из $\mathfrak{M}\cap\Sigma_g$. Этот элемент одновременно является и первым элементом в $\mathfrak{M}$.

Таким образом, поле P_f вполне упорядочивается с помощью требований 1 и 2. Так как поле Σ_f однозначно определяется требованием 3, поля P_f и Σ_f построены.

В силу условия 3 многочлен $f(x)$ полностью разлагается на линейные множители в поле Σ_f. Далее, с помощью трансфинитной индукции показывается, что Σ_f является алгебраическим над P. Действительно, предположим, что все поля $\Sigma_g\,(g<f)$ уже алгебраические. Тогда и их объединение с полем P, т. е. поле P_f, алгебраическое. Далее, поле Σ_f в силу условия 3 алгебраично над P_f, а потому алгебраично и над P.

Составим теперь объединение Ω всех полей Σ_f; согласно лемме 4 оно является полем. Это поле алгебраично над P и над ним разлагаются все многочлены f (так как каждый многочлен f разлагается уже над Σ_f). Следовательно, поле Ω алгебраически замкнуто (лемма 1).

Единственность поля Ω. Пусть Ω и Ω' — два поля, являющиеся алгебраическими и алгебраически замкнутыми расширениями поля P. Докажем эквивалентность этих полей. Для этого будем считать, что оба поля вполне упорядочены. Построим

для каждого отрезка $\mathfrak{A}$ из Ω (само поле Ω также считается одним из таких отрезков) подмножество $\mathfrak{A}'$ в Ω' и некоторый изоморфизм

$$\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}').$$

Последний должен удовлетворять следующим рекуррентным соотношениям.

1. Изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ должен оставлять каждый элемент поля P на месте.

2. Изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ при $\mathfrak{B} \subset \mathfrak{A}$ должен быть продолжением изоморфизма $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$.

3. Если $\mathfrak{A}$ обладает последним элементом a, так что $\mathfrak{A} = \mathfrak{B} \cup \{a\}$, и если a — корень неразложимого в $\mathsf{P}(\mathfrak{B})$ многочлена $f(x)$, то элемент a' должен быть первым корнем соответствующего в силу $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ многочлена $f'(x)$ во вполне упорядоченном поле Ω'.

Нужно показать, что этими тремя требованиями действительно определяется изоморфизм $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$, если только он уже определен для всех предыдущих отрезков $\mathfrak{B} \subset \mathfrak{A}$. Здесь необходимо различать два случая.

Первый случай. Множество $\mathfrak{A}$ не имеет последнего элемента. Тогда каждый элемент a принадлежит некоторому предыдущему отрезку $\mathfrak{B}$; поэтому $\mathfrak{A}$ является объединением отрезков $\mathfrak{B}$, а потому $\mathsf{P}(\mathfrak{A})$ — объединением полей $\mathsf{P}(\mathfrak{B})$ для $\mathfrak{B} \subset \mathfrak{A}$. Так как каждый из изоморфизмов $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ является продолжением всех предыдущих, то каждому элементу α при всех этих изоморфизмах сопоставляется лишь один элемент α'. Поэтому существует одно и только одно отображение $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$, продолжающее все предыдущие изоморфизмы $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$, а именно — отображение $\alpha \longmapsto \alpha'$. Очевидно, оно является изоморфизмом и удовлетворяет требованиям 1 и 2.

Второй случай. Множество $\mathfrak{A}$ имеет последний элемент a; следовательно, $\mathfrak{A} = \mathfrak{B} \cup \{a\}$. Вследствие требования 3 элемент a', сопоставляемый элементу a, однозначно определен. Так как a' над полем $\mathsf{P}(\mathfrak{B}')$ (в смысле рассматриваемого изоморфизма) удовлетворяет «тому же» неразложимому уравнению, что и a над $\mathsf{P}(\mathfrak{B})$, то изоморфизм $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$ (и в том случае, когда $\mathfrak{B}$ пусто, т. е. тождественный изоморфизм $\mathsf{P} \to \mathsf{P}$) продолжается до изоморфизма $\mathsf{P}(\mathfrak{B}, a) \to \mathsf{P}(\mathfrak{B}', a')$, при котором a переходит в a' (§ 41). Каждым из приведенных выше требований этот изоморфизм определен однозначно, потому что каждая рациональная функция $\varphi(a)$ с коэффициентами из $\mathfrak{A}$ обязательно переходит в функцию $\varphi'(a')$ с соответствующими коэффициентами из $\mathfrak{B}'$. То, что так определенный изоморфизм $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ удовлетворяет требованиям 1 и 2, очевидно.

Тем самым построение изоморфизма $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ завершено. Обозначим через Ω'' объединение всех полей $\mathsf{P}(\mathfrak{A}')$; тогда существует

изоморфизм $\mathsf{P}(\Omega) \to \Omega''$ или $\Omega \to \Omega''$, оставляющий на месте каждый элемент поля P. Так как поле Ω алгебраически замкнуто, таким же должно быть и Ω'', а потому Ω'' совпадает со всем полем Ω'. Отсюда следует эквивалентность полей Ω и Ω'.

Значение алгебраически замкнутого расширения данного поля состоит в том, что с точностью до эквивалентности оно содержит все возможные алгебраические расширения этого поля. Точнее:

Если Ω — алгебраически замкнутое алгебраическое расширение поля P и Σ — произвольное алгебраическое расширение поля P, то внутри Ω существует расширение Σ_0, эквивалентное расширению Σ.

Доказательство. Продолжим Σ до некоторого алгебраически замкнутого алгебраического расширения Ω'. Оно будет алгебраическим и над P, а потому эквивалентным расширению Ω. При каком-то изоморфизме, переводящем Ω' в Ω и сохраняющем неподвижным каждый элемент из P, поле Σ переходит в некоторое эквивалентное ему подполе Σ_0 в Ω.

Задача. Доказать существование и единственность расширения поля P, которое получается присоединением всех корней заданного множества многочленов из $\mathsf{P}[x]$.

Замечание. Вместо трансфинитной индукции в таком доказательстве, как приведенное в этом параграфе, можно использовать лемму Цорна. См. Цорн (Zorn M.). — Bull. Amer. Math. Soc., 1935, **41**, p. 667.

§ 73. Простые трансцендентные расширения

Каждое простое трансцендентное расширение поля Δ, как мы знаем, эквивалентно полю частных $\Delta(x)$ кольца многочленов $\Delta[x]$. Поэтому мы изучим это поле частных

$$\Omega = \Delta(x).$$

Элементами поля Ω служат рациональные функции

$$\eta = \frac{f(x)}{g(x)}.$$

Это представление можно считать несократимым (f и g взаимно просты). Наибольшая из степеней многочленов $f(x)$ и $g(x)$ называется *степенью* функции η.

Теорема. *Каждый отличный от константы элемент η степени n трансцендентен над Δ и поле $\Delta(x)$ — алгебраическое расширение поля $\Delta(\eta)$ степени n.*

Доказательство. Представление $\eta = f(x)/g(x)$ будем считать несократимым. Тогда элемент x удовлетворяет уравнению

$$g(x) \cdot \eta - f(x) = 0$$

с коэффициентами из $\Delta(\eta)$. Эти коэффициенты не могут быть все равны нулю. Действительно, если бы все они равнялись нулю и a_k был бы при той же степени x любым ненулевым коэффициен-

том многочлена $g(x)$, а b_k — ненулевым коэффициентом многочлена $f(x)$, то должно было бы иметь место равенство

$$a_k\eta - b_k = 0,$$

откуда $\eta = b_k/a_k = \text{const}$, что противоречит предположению. Следовательно, элемент x алгебраичен над $\Delta(\eta)$.

Если бы элемент η был алгебраическим над Δ, то и x был бы алгебраическим над Δ, что, однако, не так. Следовательно, элемент η трансцендентен над Δ.

Элемент x является корнем многочлена степени n

$$g(z)\eta - f(z)$$

в кольце $\Delta(\eta)(z)$. Этот многочлен неразложим в $\Delta(\eta)[z]$, потому что иначе он был бы разложим и в кольце $\Delta[\eta, z]$, и, так как он линеен по η, один из множителей должен был бы зависеть не от η, а лишь от z. Но такого множителя не может быть, потому что $g(z)$ и $f(z)$ взаимно просты.

Следовательно, элемент x является алгебраическим степени n над полем $\Delta(\eta)$. Отсюда следует утверждение о том, что $(\Delta(x) : \Delta(\eta)) = n$.

Для дальнейшего отметим, что многочлен

$$g(z)\eta - f(z)$$

не имеет множителей, зависящих только от z (т. е. лежащих в $\Delta[z]$). Это утверждение остается верным, когда η заменяется своим значением $f(x)/g(x)$ и умножается на знаменатель $g(x)$; тем самым многочлен

$$g(z)f(x) - f(z)g(x)$$

кольца $\Delta[x, z]$ не имеет множителей, зависящих только от z.

Из доказанной теоремы вытекают три следствия.

1. Степень функции $\eta = f(x)/g(x)$ зависит лишь от полей $\Delta(\eta)$ и $\Delta(x)$, а не от того или иного выбора порождающего элемента x.

2. Равенство $\Delta(\eta) = \Delta(x)$ имеет место тогда и только тогда, когда η имеет степень 1, т. е. является дробно-линейной функцией. Это означает: *порождающим элементом поля, кроме элемента x, может служить любая дробно-линейная функция от x и только такая функция.*

3. Любой автоморфизм поля $\Delta(x)$, оставляющий на месте каждый элемент поля Δ, должен переводить элемент x в какой-либо порождающий элемент поля. Обратно, если x переводится в какой-либо порождающий элемент $\bar{x} = \frac{ax+b}{cx+d}$ и каждая функция $\varphi(x)$ — в функцию $\varphi(\bar{x})$, то получается автоморфизм, при котором все элементы из Δ остаются на месте. Следовательно,

Все автоморфизмы поля $\Delta(x)$ над полем Δ являются дробно-линейными подстановками

$$\bar{x}=\frac{ax+b}{cx+d}, \quad ad-bc\neq 0.$$

Важной для некоторых геометрических исследований является

Теорема Люрота. *Каждое промежуточное поле Σ, для которого $\Delta\subset\Sigma\subseteq\Delta(x)$, является простым трансцендентным расширением*: $\Sigma=\Delta(\theta)$.

Доказательство. Элемент x должен быть алгебраическим над Σ, потому что если η — любой элемент из Σ, не принадлежащий полю Δ, то, как было показано, элемент x является алгебраическим над $\Delta(\eta)$ и тем более алгебраическим над Σ. Пусть неразложимый в кольце многочленов $\Sigma[z]$ многочлен со старшим коэффициентом 1 и корнем x имеет вид

$$f_0(z)=z^n+a_1z^{n-1}+\ldots+a_n. \tag{1}$$

Выясним строение этого многочлена.

Элементы a_i являются рациональными функциями от x. С помощью умножения на общий знаменатель их можно сделать целыми рациональными функциями и, кроме того, получить многочлен относительно x с содержанием 1 (ср. § 30):

$$f(x, z)=b_0(x)z^n+b_1(x)z^{n-1}+\ldots+b_n(x).$$

Степень этого многочлена по x обозначим через m, а по z — через n.

Коэффициенты $a_i=b_i/b_0$ из (1) не могут все быть независимыми от x, так как иначе x оказался бы алгебраическим элементом над Δ; поэтому один из них, скажем,

$$\theta=a_i=\frac{b_i(x)}{b_0(x)},$$

должен фактически зависеть от x; запишем его в несократимом виде:

$$\theta=\frac{g(x)}{h(x)}.$$

Степени многочленов $g(x)$ и $h(x)$ не превосходят m. Многочлен

$$g(z)-\theta h(z)=g(z)-\frac{g(x)}{h(x)}h(z)$$

(не являющийся тождественным нулем) имеет корень $z=x$, а потому он делится на $f_0(z)$ в кольце $\Sigma[z]$. Согласно § 30, если перейти от этих рациональных по x многочленов к целым по x многочленам с содержанием 1, то отношение делимости сохранится, и мы получим

$$h(x)g(z)-g(x)h(z)=q(x, z)f(x, z).$$

Левая часть в этом равенстве имеет степень по x, не превосходящую m. Но справа уже многочлен f имеет степень m; следовательно, степень левой части в точности равна m и $q(x, z)$ не зависит от x. Однако зависящий лишь от z множитель не может делить левую часть (см. выше); поэтому $q(x, z)$ является константой:

$$h(x)g(z) - g(x)h(z) = q \cdot f(x, z).$$

Так как присутствие константы q роли не играет, строение многочлена $f(x, z)$ описано полностью. Степень многочлена $f(x, z)$ по x равна m; следовательно (по соображениям симметрии), и степень по z равна m, так что $m = n$. По меньшей мере одна из степеней многочленов $g(x)$ и $h(x)$ должна фактически достигать значения m; следовательно, и функция θ должна иметь степень m по x.

Тем самым, так как с одной стороны установлено равенство

$$(\Delta(x) : \Delta(\theta)) = m,$$

а с другой — равенство

$$(\Delta(x) : \Sigma) = m;$$

то, поскольку Σ содержит $\Delta(\theta)$,

$$(\Sigma : \Delta(\theta)) = 1,$$
$$\Sigma = \Delta(\theta).$$

Теорема Люрота имеет следующее значение для геометрии.

Плоская (неприводимая) алгебраическая кривая $F(\xi, \eta) = 0$ называется *рациональной*, если ее точки, за исключением некоторого конечного числа из них, представляются рациональными параметрическими уравнениями

$$\xi = f(t),$$
$$\eta = g(t).$$

Может оказаться так, что каждая точка кривой (за исключением конечного числа) получается при нескольких значениях параметра t. (Например:

$$\xi = t^2,$$
$$\eta = t^2 + 1;$$

для t и $-t$ получается одна и та же точка.) В силу теоремы Люрота с помощью удачного выбора параметра это явление всегда можно обойти. Действительно, пусть Δ — поле, которое содержит коэффициенты функций f, g, и t — какая-нибудь переменная. Тогда $\Sigma = \Delta(f, g)$ является подполем поля $\Delta(t)$. Если t' — примитивный элемент поля Σ, то

$$f(t) = f_1(t') \text{ (рациональная функция)},$$
$$g(t) = g_1(t') \text{ (рациональная функция)},$$
$$t' = \varphi(f, g) = \varphi(\xi, \eta),$$

и легко проверить, что новое параметрическое представление

$$\xi = f_1(t'),$$
$$\eta = g_1(t')$$

Основная теорема 3. *Если элемент w алгебраически зависит от $v_1, \ldots, v_s$ и каждый v_j $(j=1, \ldots, s)$ алгебраически зависит от $u_1, \ldots, u_n$, то w алгебраически зависит от $u_1, \ldots, u_n$.*

Доказательство. Если w — алгебраический элемент над полем $\mathsf{P}(v_1, \ldots, v_s)$, то он будет алгебраическим и над $\mathsf{P}(u_1, \ldots, u_n, v_1, \ldots, v_s)$, а это поле алгебраично над $\mathsf{P}(u_1, \ldots, u_n)$. Поэтому в силу § 41 элемент w алгебраичен над $\mathsf{P}(u_1, \ldots, u_n)$, что и требовалось доказать.

В силу этих основных теорем об алгебраической зависимости справедливы и следствия из них, аналогичные сформулированным в § 20; в частности, справедлива теорема о замене.

Аналогом понятия линейной независимости может служить понятие алгебраической независимости: элементы $u_1, \ldots, u_n$ называются *алгебраически независимыми* над основным полем P, если ни один из них не является алгебраически зависимым от остальных. Имеет место

Теорема. *Элементы $u_1, \ldots, u_r$ алгебраически независимы тогда и только тогда, когда из*

$$f(u_1, \ldots, u_r)=0,$$

где f — многочлен с коэффициентами из P, следует равенство нулю всех коэффициентов многочлена f.

Доказательство. Если $f(u_1, \ldots, u_r)=0$ имеет своим следствием равенство нулю многочлена f, то, очевидно, ни один из элементов u_i не может быть алгебраически зависимым от остальных u_j. Пусть, наоборот, элементы $u_1, \ldots, u_r$ алгебраически независимы. Если

$$f(u_1, \ldots, u_r)=0$$

и если многочлен f расположен по степеням элемента u_r, то коэффициенты $f_i(u_1, \ldots, u_{r-1})$ этого многочлена оказываются тождественно равными нулю. Расположим эти коэффициенты-многочлены по степеням элемента u_{r-1} и точно так же установим, что и их коэффициенты тождественно равны нулю; продолжая таким образом, мы в конце концов установим, что коэффициенты многочлена f равны нулю.

Согласно этой теореме элементы $u_1, \ldots, u_r$ при условии, что они алгебраически независимы, не связываются никаким алгебраическим уравнением. По этой причине их называют *независимыми трансцендентными элементами*.

Если $u_1, \ldots, u_r$ алгебраически независимы и $z_1, \ldots, z_r$ — переменные над полем P, то каждому многочлену $f(z_1, \ldots, z_r)$ с коэффициентами из P можно взаимно однозначно сопоставить многочлен $f(u_1, \ldots, u_r)$. Поэтому $\mathsf{P}[z_1, \ldots, z_r] \cong \mathsf{P}[u_1, \ldots, u_r]$. Из существования этого изоморфизма колец многочленов следует

существование изоморфизма полей частных:

$$\mathsf{P}(z_1, \ldots, z_r) \cong \mathsf{P}(u_1, \ldots, u_r).$$

Таким образом, независимые трансцендентные элементы $u_1, \ldots, u_r$ совпадают в смысле алгебраических свойств с обычными независимыми переменными.

Понятия алгебраической зависимости и независимости могут быть введены и для бесконечных множеств. Элемент v называется (*алгебраически*) *зависимым от множества* $\mathfrak{M}$ (*над основным полем* P), если он алгебраичен над полем $\mathsf{P}(\mathfrak{M})$, т. е. удовлетворяет некоторому уравнению, коэффициентами которого являются рациональные функции от элементов множества $\mathfrak{M}$ с коэффициентами из поля P [1]). В этом случае упомянутое уравнение с помощью умножения на произведение знаменателей коэффициентов можно сделать целым рациональным уравнением с элементами из $\mathfrak{M}$. В такое уравнение входит лишь конечное число элементов $u_1, \ldots, u_n$ множества $\mathfrak{M}$, поэтому:

Если элемент v зависит от $\mathfrak{M}$, то v зависит от конечного числа элементов $u_1, \ldots, u_n$ из $\mathfrak{M}$.

Выберем конечное множество $\{u_1, \ldots, u_n\}$ так, чтобы ни один из его элементов не был лишним; тогда в силу основной теоремы 2 каждый элемент u_i зависит от v и от остальных u_j.

Основная теорема 3 без оговорок переносится на случай бесконечных множеств:

Если u зависит от $\mathfrak{M}$ и каждый элемент из $\mathfrak{M}$ зависит от $\mathfrak{N}$, то u зависит от $\mathfrak{N}$.

Множество $\mathfrak{N}$ называется (*алгебраически*) *зависимым* от множества $\mathfrak{M}$, если все элементы из $\mathfrak{N}$ зависят от $\mathfrak{M}$. Если $\mathfrak{N}$ зависит от $\mathfrak{M}$, а $\mathfrak{M}$ зависит от $\mathfrak{L}$, то $\mathfrak{N}$ зависит от $\mathfrak{L}$.

Если два множества $\mathfrak{M}$ и $\mathfrak{N}$ зависят друг от друга, то они называются *эквивалентными* (над P). Отношение эквивалентности, введенное таким путем, является рефлексивным, симметричным и транзитивным.

Множество $\mathfrak{M}$ называется *алгебраически независимым* (над P), если ни один из его элементов не зависит алгебраически от остальных. В этом случае говорят также, что множество $\mathfrak{M}$ «состоит из независимых трансцендентных элементов».

Если множество $\mathfrak{M}$ алгебраически независимо, то соотношение между элементами $\mathfrak{M}$ вида

$$f(u_1, \ldots, u_r) = 0,$$

где f — многочлен с коэффициентами из P, может выполняться лишь тогда, когда f тождественно равен нулю:

$$f(x_1, \ldots, x_r) = 0 \text{ (для переменных } x_i).$$

---

[1]) Элемент зависит от пустого множества, если он алгебраичен над P.

Если построить кольцо многочленов $\mathsf{P}[\mathfrak{X}]$ от стольких переменных x_i, сколько элементов в $\mathfrak{M}$ (неважно, конечно или бесконечно это множество) и каждому многочлену $f(x_1, \ldots, x_r)$ сопоставить элемент поля $f(u_1, \ldots, u_r)$, то, очевидно, получится некоторый гомоморфизм кольца многочленов на кольцо $\mathsf{P}[\mathfrak{M}]$ элементов поля $f(u_1, \ldots, u_r)$. Если $\mathfrak{M}$ алгебраически независимо, то различные многочлены переходят в различные элементы поля; следовательно, в этом случае получается изоморфизм

$$\mathsf{P}[\mathfrak{X}] \cong \mathsf{P}[\mathfrak{M}].$$

Из изоморфизма колец многочленов вновь следует изоморфизм полей частных. Тем самым доказана теорема:

Поле $\mathsf{P}(\mathfrak{M})$, *получающееся присоединением алгебраически независимого множества* $\mathfrak{M}$ *к полю* P, *изоморфно полю рациональных функций от множества переменных* $\mathfrak{X}$, *равномощного множеству* $\mathfrak{M}$, *т. е. полю частных кольца многочленов* $\mathsf{P}[\mathfrak{X}]$.

Каждое поле $\mathsf{P}(\mathfrak{M})$, которое получается присоединением алгебраически независимого множества $\mathfrak{M}$ к P, называется *чисто трансцендентным расширением поля* P. Строение чисто трансцендентных расширений полностью описывается предыдущей теоремой: каждое такое расширение изоморфно полю частных некоторого кольца многочленов. Таким образом, строение поля $\mathsf{P}(\mathfrak{M})$ зависит лишь от мощности множества $\mathfrak{M}$: эта мощность называется *степенью трансцендентности*; ей посвящен следующий параграф.

§ 75. Степень трансцендентности

Мы покажем, что каждое расширение данного поля может быть разложено на некоторое чисто трансцендентное расширение и следующее за ним алгебраическое расширение. В основе рассуждений лежит теорема:

Пусть Ω — *произвольное расширение поля* P. *Тогда каждое подмножество* $\mathfrak{M}$ *поля* Ω *эквивалентно в смысле алгебраической зависимости некоторому своему подмножеству* $\mathfrak{M}'$, *являющемуся алгебраически независимым.*

Доказательство. Пусть $\mathfrak{M}$ вполне упорядочено. Подмножество $\mathfrak{M}'$ определим следующим образом: элемент a из $\mathfrak{M}$ принадлежит $\mathfrak{M}'$, если a не зависит алгебраически от предшествующего ему отрезка $\mathfrak{A}$. Тогда о множестве $\mathfrak{M}'$ можно высказать и доказать следующие утверждения:

1. Множество $\mathfrak{M}'$ алгебраически независимо. Действительно, если бы некоторый его элемент a_1 зависел от элементов $a_2, \ldots, a_k$, то множество $\{a_2, \ldots, a_k\}$ можно было бы выбрать минимальным и тогда каждый элемент a_i зависел бы от всех остальных. В частности, последний в смысле имеющегося порядка элемент a_i зависел

бы от остальных элементов. Но тогда этот последний a_i (в силу определения множества $\mathfrak{M}'$) не мог бы принадлежать множеству $\mathfrak{M}'$.

2. Множество $\mathfrak{M}$ зависит от $\mathfrak{M}'$. Действительно, в противном случае в $\mathfrak{M}$ существовал бы первый элемент a, не зависящий от $\mathfrak{M}'$. Элемент a не принадлежит множеству $\mathfrak{M}'$, а потому зависит от предшествующего отрезка $\mathfrak{A}$, который в свою очередь (ведь a — первый не зависящий от $\mathfrak{M}'$ элемент) зависит от $\mathfrak{M}'$. Тем самым элемент a зависит от $\mathfrak{M}'$, что противоречит предположению.

Дополнение. *Если $\mathfrak{M} \subset \mathfrak{N}$, то каждая эквивалентная множеству $\mathfrak{M}$ алгебраически независимая подсистема $\mathfrak{M}'$ в $\mathfrak{M}$ может быть дополнена до алгебраически независимой подсистемы в $\mathfrak{N}$, эквивалентной множеству $\mathfrak{N}$.*

Доказательство. Сделаем множество $\mathfrak{N}$ вполне упорядоченным так, чтобы элементы множества $\mathfrak{M}$ оказались предшествующими остальным элементам объемлющего множества, и построим систему $\mathfrak{N}'$ из $\mathfrak{N}$ аналогично тому, как строилась система $\mathfrak{M}'$ из множества $\mathfrak{M}$ в предыдущей теореме. Очевидно, $\mathfrak{N}'$ содержит среди прочих и элементы из $\mathfrak{M}'$.

Система $\mathfrak{M}'$ называется *неприводимой*.

Задача 1. Провести доказательство этой теоремы с помощью леммы Цорна, примененной к замкнутому множеству A всех алгебраически независимых подмножеств из $\mathfrak{M}$.

Согласно предыдущей теореме каждое расширение Ω поля P можно рассматривать как некоторое алгебраическое расширение поля $\mathsf{P}(\mathfrak{S})$, где $\mathfrak{S}$ — неприводимая система, а потому $\mathsf{P}(\mathfrak{S})$ — чисто трансцендентное расширение поля P. Таким образом, это означает, что поле Ω получается из P с помощью некоторого чисто трансцендентного расширения и последующего чисто алгебраического расширения.

Построенная в предыдущих теоремах неприводимая система $\mathfrak{M}'$ является, конечно, не единственной; однако мощность этой системы (и тип чисто трансцендентного расширения $\mathsf{P}(\mathfrak{M})$) определена однозначно. Действительно, имеет место теорема:

Две эквивалентные алгебраически независимые системы $\mathfrak{M}$, $\mathfrak{N}$ равномощны.

По поводу общего доказательства этой теоремы можно указать оригинальную работу Штейница в J. reine angew. Math. **137**, а также книгу: Гаупт (Haupt O.). Einführung in die Algebra II, Kap. 23,6. Важнейший частный случай имеет место тогда, когда по крайней мере одна из систем $\mathfrak{M}$, $\mathfrak{N}$ конечна. Например, если $\mathfrak{M}$ состоит из r элементов $u_1, \ldots, u_r$, то согласно следствию 4 (§ 20) в $\mathfrak{N}$ имеется не более r элементов, так что и $\mathfrak{N}$ — конечное множество; поскольку на том же основании $\mathfrak{M}$ не может иметь больше элементов, чем $\mathfrak{N}$, множества $\mathfrak{M}$ и $\mathfrak{N}$ равномощны.

Однозначно определенная мощность алгебраически независимой системы $\mathfrak{M}$, эквивалентной полю Ω, называется *степенью трансцендентности* поля Ω над полем P.

Теорема. *Расширение, получающееся в результате двух последовательных расширений (конечных) степеней трансцендентности s и t, имеет степень трансцендентности $s+t$*[1].

Доказательство. Пусть $\mathsf{P} \subseteq \Sigma \subseteq \Omega$. Пусть $\mathfrak{S}$ — система, алгебраически независимая над P, эквивалентная полю Σ и принадлежащая Σ, и пусть $\mathfrak{T}$ — система, агебраически независимая над Σ, эквивалентная полю Ω и содержащаяся в Ω. Тогда $\mathfrak{S}$ имеет мощность s, $\mathfrak{T}$ имеет мощность t и множество $\mathfrak{S}$ не пересекается с $\mathfrak{T}$, так что объединение $\mathfrak{S} \cup \mathfrak{T}$ имеет мощность $s+t$. Если мы сможем установить, что система $\mathfrak{S} \cup \mathfrak{T}$ алгебраически независима над P и эквивалентна полю Ω, то требуемое будет доказано.

Поле Ω является алгебраическим над Σ ($\mathfrak{T}$), а Σ — алгебраическим над P ($\mathfrak{S}$); следовательно, Ω является алгебраическим над P ($\mathfrak{S}$, $\mathfrak{T}$), т. е. эквивалентным системе $\mathfrak{S} \cup \mathfrak{T}$.

Если бы существовало какое-либо алгебраическое соотношение между конечным множеством элементов из $\mathfrak{S} \cup \mathfrak{T}$ с коэффициентами из P, то в него прежде всего не могли бы входить элементы из $\mathfrak{T}$, потому что иначе существовало бы соотношение между этими элементами с коэффициентами из Σ, что противоречит алгебраической независимости множества $\mathfrak{T}$. Таким образом, алгебраическое соотношение оказалось бы соотношением лишь между элементами из $\mathfrak{S}$, что противоречит их алгебраической независимости. Следовательно, множество $\mathfrak{S} \cup \mathfrak{T}$ является алгебраически независимым над P, чем и завершается доказательство.

§ 76. Дифференцирование алгебраических функций

Введенное в § 27 определение производной многочлена $f(x)$ без каких-либо дополнений переносится на рациональные функции одной переменной

$$\varphi(x) = \frac{f(x)}{g(x)}$$

с коэффициентами из поля P. Действительно, составим выражение

$$\varphi(x+h) - \varphi(x) = \frac{f(x+h)\,g(x) - f(x)\,g(x+h)}{g(x)\,g(x+h)};$$

---

[1]) Эта теорема справедлива и для бесконечных степеней трансцендентности, но для этого надо ввести понятие сложения бесконечных мощностей, о котором мы не говорили.

тогда числитель этой дроби обращается в нуль при $h=0$; следовательно, у него есть множитель h. Разделим обе части на h; получится

$$\frac{\varphi(x+h)-\varphi(x)}{h}=\frac{q(x,h)}{g(x)\,g(x+h)}. \tag{1}$$

Правая часть является рациональной функцией по h, которая при $h=0$ принимает вполне определенное значение, так как знаменатель при $h=0$ не обращается в нуль. Это значение рациональной функции мы называем *дифференциальным отношением* или *производной* $\varphi'(x)$ рациональной функции $\varphi(x)$:

$$\varphi'(x)=\frac{d\varphi(x)}{dx}=\frac{q(x,0)}{g(x)^2}. \tag{2}$$

Чтобы фактически вычислить $q(x, 0)$, разложим числитель правой части в (1) по возрастающим степеням h, разделим на h и положим $h=0$; тогда

$$q(x,0)=f'(x)\,g(x)-f(x)\,g'(x);$$

при подстановке этого выражения в (2) получается известная формула для производной частного:

$$\frac{d}{dx}\frac{f(x)}{g(x)}=\frac{f'(x)\,g(x)-f(x)\,g'(x)}{g(x)^2}.$$

Пусть $R(u_1, \ldots, u_n)$ — произвольная рациональная функция; пусть $R'_1, \ldots, R'_n$ — ее частные производные по переменным $u_1, \ldots, u_n$ и пусть $\varphi_1, \ldots, \varphi_n$ — рациональные функции от x.

Выведем *формулу для полной производной*:

$$\frac{d}{dx}R(\varphi_1, \ldots, \varphi_n)=\sum_1^n R'_\nu(\varphi_1, \ldots, \varphi_n)\,\frac{d\varphi_\nu}{dx}. \tag{3}$$

Для этой цели в соответствии с определением производной положим

$$\varphi_\nu(x+h)-\varphi_\nu(x)=h\psi_\nu(x, h), \qquad \psi_\nu(x, 0)=\varphi'_\nu(x),$$

и

$$\begin{aligned}R(u_1+h_1, \ldots, u_n+h_n)-R(u_1, \ldots, u_n)&=\\ =\sum_{\nu=1}^n \{R(u_1+h_1, \ldots, u_\nu+h_\nu, u_{\nu+1}, \ldots, u_n)&-\\ -R(u_1+h_1, \ldots, u_\nu, u_{\nu+1}, \ldots, u_n)\}&=\\ =\sum_{\nu=1}^n h_\nu S_\nu(u_1+h_1, \ldots, u_\nu, h_\nu, u_{\nu+1}, \ldots, u_n)&,\end{aligned} \tag{4}$$

где

$$S_\nu(u_1, \ldots, u_\nu, 0, u_{\nu+1}, \ldots, u_n)=R'_\nu(u_1, \ldots, u_n).$$

Положим в тождестве (4)

$$u_\nu = \varphi_\nu(x),\ h_\nu = \varphi_\nu(x+h) - \varphi_\nu(x) = h\psi_\nu(x,\ h)$$

и разделим полученное выражение на h:

$$\frac{R(\varphi_1(x+h),\ \ldots,\ \varphi_n(x+h)) - R(\varphi_1(x),\ \ldots,\ \varphi_n(x))}{h} =$$

$$= \sum_{\nu=1}^{n} \psi_\nu(x,\ h)\, S_\nu(\varphi_1 + h\psi_1,\ \ldots,\ \varphi_\nu,\ h\psi_\nu,\ \varphi_{\nu+1},\ \ldots,\ \varphi_n).$$

Положим справа $h=0$; тогда

$$\frac{d}{dx} R(\varphi_1,\ \ldots,\ \varphi_n) = \sum \varphi'_\nu(x)\, R'_\nu(\varphi_1,\ \ldots,\ \varphi_n),$$

чем и доказывается (3).

Попытаемся распространить теорию дифференцирования на алгебраические функции одной переменной x. Под *алгебраической функцией одной переменной* x мы понимаем произвольный элемент η алгебраического расширения поля $\mathsf{P}(x)$.

Мы будем считать, что элемент η сепарабелен над $\mathsf{P}(x)$. Таким образом, алгебраическая функция η является корнем некоторого неразложимого над $\mathsf{P}(x)$ сепарабельного многочлена $F(x,\ y)$:

$$F(x,\ \eta) = 0.$$

Производные многочлена $F(x,\ y)$ по x и y обозначим соответственно через F'_x и F'_y. В силу сепарабельности многочлен $F'_y(x,\ y)$ не имеет общих корней с $F(x,\ y)$; следовательно,

$$F'_y(x,\ \eta) \neq 0.$$

Для разумного определения производной $d\eta/dx$ нужно потребовать, чтобы многочлен $F(x,\ y)$ удовлетворял формуле полной производной

$$F'_x(x,\ \eta) + \frac{d\eta}{dx} F'_y(x,\ y) = 0.$$

Положим по определению

$$\frac{d\eta}{dx} = -\frac{F'_x(x,\ \eta)}{F'_y(x,\ \eta)}. \tag{5}$$

Сразу усматривается, что это определение не зависит от выбора многочлена $F(x,\ y)$, потому что если $F(x,\ y)$ заменить на $F(x,\ y)\cdot\psi(x)$, где $\psi(x)$ — произвольная рациональная функция от x, то $F'_x(x,\ \eta)$ и $F'_y(x,\ \eta)$ в (5) заменятся на

$$F'_x(x,\ \eta)\ \psi(x) + F(x,\ \eta)\cdot\psi'(x) = F'_x(x,\ \eta)\ \psi(x)$$

и на

$$F'_y(x, \eta)\cdot\psi(x),$$

что не изменит соотношения (5).

В частности, если $\eta = c$ — константа из P, то x не входит в уравнение, определяющее элемент η, поэтому $\frac{dc}{dx} = 0$.

Пусть ζ — произвольный элемент поля $\mathsf{P}(x, \eta)$, т. е. некоторая рациональная функция от x и η, целая рациональная по η:

$$\zeta = \varphi(x, \eta).$$

Для этой функции мы докажем следующую формулу полной производной:

$$\frac{d\zeta}{dx} = \varphi'_x(x, \eta) + \varphi'_y(x, \eta)\frac{d\eta}{dx}, \tag{6}$$

где φ'_x и φ'_y — производные от $\varphi(x, y)$ по x и по y. С этой целью составим уравнение, определяющее ζ, которое можно считать целым рациональным по x и ζ:

$$G(x, \zeta) = 0;$$

подставим в него выражение $\varphi(x, \eta)$ для ζ и затем заменим η на переменную y. Полученный многочлен от y имеет корнем η и потому делится на $F(x, y)$:

$$G(x, \varphi(x, y)) = Q(x, y)F(x, y).$$

Если продифференцировать это тождество по x и y с помощью формулы полной производной (3), то получится

$$\left.\begin{aligned} G'_x(x, \varphi(x, y)) + G'_z(x, \varphi(x, y))\varphi'_x(x, y) &= QF'_x + Q'_xF(x, y), \\ G'_z(x, \varphi(x, y))\varphi'_y(x, y) &= QF'_y + Q'_yF(x, y). \end{aligned}\right\}$$

Заменим теперь y опять на η, благодаря чему члены с $F(x, y)$ обратятся в нуль; в соответствии с определением (5), далее,

$$F'_x(x, \eta) = -F'_y(x, \eta)\frac{d\eta}{dx},$$

$$G'_x(x, \zeta) = -G'_z(x, \zeta)\frac{d\zeta}{dx}.$$

Отсюда получается, что

$$\left.\begin{aligned} -G'_z(x, \zeta)\frac{d\zeta}{dx} + G'_z(x, \zeta)\varphi'_x(x, \eta) &= -Q(x, \eta)F'_y(x, \eta)\frac{d\eta}{dx}, \\ G'_z(x, \zeta)\varphi'_y(x, \eta) &= Q(x, \eta)F'_y(x, \eta). \end{aligned}\right\}$$

Умножим второе равенство на $\frac{d\eta}{dx}$, прибавим к первому, и раз-

делим полученное равенство на G'_z; получим

$$-\frac{d\zeta}{dx}+\varphi'_x(x,\ \eta)+\varphi'_y(x,\ \eta)\frac{d\eta}{dx}=0,$$

что и доказывает (6).

После того как с помощью проведенного вычисления установлен частный случай (6), не представляет труда доказательство общей *формулы полной производной*. Соответствующее правило таково: *если* $\eta_1, \ldots, \eta_n$ — *сепарабельные алгебраические функции от* x *из некоторого поля и* $R(u_1, \ldots, u_n)$ — *многочлен с производными* R'_ν, *то*

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=\sum_1^n R'_\nu(\eta_1, \ldots, \eta_n)\frac{d\eta_\nu}{dx}. \tag{7}$$

Доказательство. Пусть θ — примитивный элемент сепарабельного расширения $\mathsf{P}(x, \eta_1, \ldots, \eta_n)$ поля $\mathsf{P}(x)$. Тогда все η_ν являются рациональными функциями от x и θ:

$$\eta_\nu=\varphi_\nu(x,\ \theta).$$

Согласно (6), если $\varphi'_{\nu x}$ и $\varphi'_{\nu t}$ — производные от $\varphi_\nu(x,\ t)$ по x и по t, то

$$\frac{d\eta_\nu}{dx}=\varphi'_{\nu x}(x,\ \theta)+\varphi'_{\nu t}(x,\ \theta)\frac{d\theta}{dx},$$

и, равным образом, если R'_x и R'_t — производные функции

$$R(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t)),$$

то

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=\frac{d}{dx}R(\varphi_1(x,\ \theta), \ldots, \varphi_n(x,\ \theta))=$$
$$=R'_x(x,\ \theta)+R'_t(x,\ \theta)\frac{d\theta}{dx}.$$

Но в силу (3)

$$R'_x(x,\ t)=\sum_1^n R'_\nu(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t))\varphi'_{\nu x}(x,\ t),$$

$$R'_t(x,\ t)=\sum_1^n R'_\nu(\varphi_1(x,\ t), \ldots, \varphi_n(x,\ t))\varphi'_{\nu t}(x,\ t);$$

следовательно,

$$\frac{d}{dx}R(\eta_1, \ldots, \eta_n)=$$
$$=\sum_1^n R'_\nu(\varphi_1(x,\ \theta), \ldots, \varphi_n(x,\ \theta))\left\{\varphi'_{\nu x}(x,\ \theta)+\varphi'_{\nu t}(x,\ \theta)\cdot\frac{d\theta}{dx}\right\}=$$
$$=\sum_1^n R'_\nu(\eta_1, \ldots, \eta_n)\frac{d\eta_\nu}{dx}.$$

Вот важнейшие частные случаи общей формулы (7):

$$\frac{d}{dx}(\eta+\zeta)=\frac{d\eta}{dx}+\frac{d\zeta}{dx}; \tag{8}$$

$$\frac{d}{dx}\eta\zeta=\eta\frac{d\zeta}{dx}+\frac{d\eta}{dx}\zeta; \tag{9}$$

$$\frac{d}{dx}\frac{\eta}{\zeta}=\frac{1}{\zeta^2}\left(\zeta\frac{d\eta}{dx}-\eta\frac{d\zeta}{dx}\right); \tag{10}$$

$$\frac{d}{dx}\eta^r=r\eta^{r-1}\frac{d\eta}{dx}. \tag{11}$$

Определение производных (5) применимо, конечно, не только тогда, когда x — переменная, но и тогда, когда x — любой трансцендентный относительно P элемент, а η — алгебраический сепарабельный элемент над $\mathsf{P}(x)$. В этом случае элемент x предпочтительнее обозначать через ξ. Таким образом, в любом поле степени трансцендентности 1 над P все элементы η, сепарабельные над $\mathsf{P}(\xi)$, можно дифференцировать по трансцендентному элементу ξ.

Если η и ζ алгебраически зависят от ξ, то поле $\mathsf{P}(\xi, \eta, \zeta)$ имеет степень трансцендентности 1 над P. Если теперь η трансцендентен над P, то ζ алгебраически зависит от η. Предположим, что ζ сепарабелен над $\mathsf{P}(\eta)$; тогда можно построить $d\zeta/d\eta$. Если

$$G(\eta, \zeta)=0 \tag{12}$$

— определяющее уравнение элемента ζ над $\mathsf{P}(\eta)$ и если G'_y и G'_z — частные производные многочлена $G(y, z)$, то

$$G'_y(\eta, \zeta)+G'_z(\eta, \zeta)\frac{d\zeta}{d\eta}=0. \tag{13}$$

С другой стороны, если продифференцировать (12) по ξ, то в соответствии с формулой полной производной получится равенство

$$G'_y(\eta, \zeta)\frac{d\eta}{d\xi}+G'_z(\eta, \zeta)\frac{d\zeta}{d\xi}=0. \tag{14}$$

Если (13) умножить на $\frac{d\eta}{d\xi}$ и вычесть из (14), то получится формула производной сложной функции

$$\frac{d\zeta}{d\xi}=\frac{d\zeta}{d\eta}\cdot\frac{d\eta}{d\xi}. \tag{15}$$

В частности, при $\zeta=\xi$ она дает

$$\frac{d\xi}{d\eta}\cdot\frac{d\eta}{d\xi}=1. \tag{16}$$

Таким образом, мы получили чисто алгебраически, не прибегая к понятию предела, все обычные правила дифференциального исчисления для алгебраических функций одной переменной.