ACTUALITÉS SCIENTIFIQUES ET INDUSTRIELLES
1251

PUBLICATIONS DE L'INSTITUT DE MATHÉMATIQUE
DE L'UNIVERSITÉ DE NANCAGO

IRVING KAPLANSKY

An introduction to differential algebra

HERMANN, PARIS, 1957

БИБЛИОТЕКА СБОРНИКА
«МАТЕМАТИКА»

И. КАПЛАНСКИЙ

ВВЕДЕНИЕ В ДИФФЕРЕНЦИАЛЬНУЮ АЛГЕБРУ

Перевод с английского
Г. И. КЛЕЙНЕРМАНА

Под редакцией
М. М. ПОСТНИКОВА

ИЗДАТЕЛЬСТВО
ИНОСТРАННОЙ ЛИТЕРАТУРЫ
Москва, 1959

АННОТАЦИЯ

Дифференциальная алгебра — новая и несомненно обладающая большим будущим ветвь алгебры, устанавливающая своеобразную связь последней с теорией дифференциальных уравнений. Литература на русском языке по этой дисциплине отсутствует.

Брошюра И. Капланского знакомит читателя с основами современной дифференциальной алгебры и с возможными путями развития этой науки. В ней излагаются, в частности, основы теории Галуа для дифференциальных полей, т. е. теории Пикара — Вессио в ее современном виде.

Брошюра эта будет очень полезна для математиков самых различных специальностей, желающих познакомится с фундаментальными понятиями дифференциальной алгебры.

Она может быть также использована в качестве введения математиками, которые предполагают в дальнейшем глубже изучить эту теорию.

Редакция литературы по математическим наукам.

ИЗ ПРЕДИСЛОВИЯ АВТОРА

Дифференциальную алгебру легко описать: она состоит (на 99% или более) из работ Ритта и Колчина.

Я написал эту брошюру для того, чтобы дифференциальная алгебра стала более доступна математической общественности. Ритт был в душе аналитиком, сам же предмет по существу относится к алгебре. Вследствие этого Ритт писал в таком стиле, который часто затруднял путь в дифференциальную алгебру как аналитикам, так и алгебраистам.

Основная статья Колчина [2], посвященная теории Пикара — Вессио, написана удивительно ясно и элегантно. Однако ее невозможно полностью понять, не обращаясь к другим работам. В частности, она содержит существенные ссылки на более раннюю статью [1], в которой в свою очередь используется теория Ритта. Некоторые необходимые факты из алгебраической геометрии могут также затруднить многих читателей.

Я пытался сделать изложение по возможности замкнутым в себе и элементарным. Кроме стандартного курса алгебры (в объеме, скажем, книги Birkhoff and MacLane, Survey of Modern Algebra), предполагаемый читатель должен владеть лишь теоремой Гильберта о корнях, теоремой Гильберта о базисах, начатками теории степени трансцендентности и обладать хотя бы поверхностным знанием теоретико-множественной топологии. Более осведомленный читатель без труда обнаружит, что в отдельных местах доказательства можно было бы сократить, применяя более хитроумный аппарат (кронекеровы произведения, теорию линейной свободы полей, методы алгебраической геометрии и т. п.).

Книга содержит два основных новшества:

1) Теория Пикара — Вессио развита без использования теоремы Ритта — Роденбаша о базисах.

В результате этого книга, по существу, содержит два введения: главы I—VI являются введением к статьям Колчина, в то время как главы I и VII могут служить введением к обеим книгам Ритта и к его многочисленным статьям (главу VII можно читать непосредственно после главы I).

2) Необходимая теория алгебраических матричных групп развивается исключительно в рамках теоретико-множественной топологии. В главе IV, посвященной этим вопросам, излагается лишь тот минимум, который необходим для следующих двух глав. Естественному аналитическому продолжению этих идей посвящается приложенное к книге добавление (глава VIII).

Я хотел бы обратить внимание еще на два менее существенных момента.

3) В начале главы III дается краткий обзор классической теории Галуа. Я благодарен мистеру Джорджу Моргану за поправку, внесенную им в доказательство леммы 3.2.

4) В главе VI полностью разобран „конкретный“ пример уравнения $y''+xy=0$, не разрешимого в квадратурах. Исследования такого рода можно найти кое-где в более ранних работах, восходящих к Лиувиллю. Соответствующие ссылки могут быть найдены в обширной библиографии, приведенной Колчиным в статье [2].

Глава I

ОБЩИЕ СВЕДЕНИЯ О ДИФФЕРЕНЦИАЛЬНЫХ КОЛЬЦАХ

1. Дифференцирования. Дифференцированием кольца A называется аддитивное отображение $a \to a'$ кольца A в себя, удовлетворяющее соотношению

$$(ab)' = a'b + ab'.$$

Обозначая последовательные производные[1]) через a', a'', a''', ..., $a^{(n)}$, по индукции получаем следующее правило Лейбница:

$$(ab)^{(n)} = a^{(n)}b + \ldots + C_n^i a^{(n-i)} b^{(i)} + \ldots + ab^{(n)}.$$

Если элементы a и a' перестановочны, то $(a^n)' = na^{n-1}a'$. Элемент, производный от единицы (если она имеется в кольце A), равен нулю. Для любого регулярного элемента a (элемента, обладающего двусторонним обратным элементом a^{-1}), продифференцировав тождество $aa^{-1}=1$, мы получим

$$(a^{-1})' = -a^{-1}a'a^{-1}.$$

Теорема 1.1. *Любое дифференцирование в произвольной области целостности допускает единственное продолжение на соответствующее поле отношений.*

Доказательство. Единственность продолжения очевидна. Для доказательства существования определим дифференцирование в поле отношений, полагая

$$\left(\frac{a}{b}\right)' = \frac{ba' - ab'}{b^2}.$$

Легко видеть, что определение корректно, т. е. что результат не меняется при замене дроби a/b на ac/bc. Для

1) Элемент a' называется производным от элемента a, а элемент a называется интегралом элемента a'. — *Прим. перев.*

проверки аддитивности этого отображения следует дроби a/b и c/d привести к общему знаменателю bd и воспользоваться линейностью написанной формулы относительно a. Доказательство правила дифференцирования произведения вполне автоматично и сводится к более длинной выкладке.

2. Дифференциальные кольца. Дифференциальным кольцом называется коммутативное кольцо с единицей, в котором отмечено некоторое дифференцирование.

Примеры. 1. Любое коммутативное кольцо с единицей является дифференциальным кольцом относительно тривиального дифференцирования (т. е. дифференцирования, переводящего каждый элемент кольца в нуль). Таким образом, можно сказать, что теория обычных колец содержится в теории дифференциальных колец в качестве частного случая.

Заметим, что в кольце целых чисел и в поле рациональных чисел никакое дифференцирование, кроме тривиального, невозможно.

2. Кольцо всех бесконечно дифференцируемых функций на действительной прямой относительно обычного дифференцирования. (Мы рассматриваем лишь бесконечно дифференцируемые функции, для того чтобы иметь систему, замкнутую относительно дифференцирования.)

3. Кольцо целых функций относительно обычного дифференцирования. Заметим, что в отличие от предыдущего примера это кольцо не имеет делителей нуля и, следовательно, можно образовать его поле отношений (поле мероморфных функций). Более общий пример мы получим, рассматривая функции, аналитические в некоторой области комплексной плоскости.

4. Пусть A — произвольное дифференциальное кольцо. Через $A[x]$ мы будем, как обычно, обозначать кольцо всех многочленов с коэффициентами из A от одного (обыкновенного) неизвестного. В случае, когда A является полем, мы через $A(x)$ будем обозначать поле рациональных функций от x. Дифференцирование кольца A можно продолжить на кольцо $A[x]$, принимая за x' произвольный элемент, полагая $(x^n)' = nx^{n-1}x'$ и распространяя это отображение по линейности. Аналогичной свободой мы располагаем при превращении поля $A(x)$ в дифференциальное (см. теорему 1.1).

5. Пусть снова A — произвольное дифференциальное кольцо. Рассмотрим кольцо $A[x_i]$ многочленов от бесконечного числа обыкновенных неизвестных $x_0, x_1, x_2, \ldots$. Приняв элемент x_{i+1} за производный от элемента x_i, мы получим в кольце $A[x_i]$ некоторое однозначно определенное дифференцирование. В соответствии с этим целесообразно несколько изменить обозначения, полагая

$$x_0 = x, \qquad x_n = x^{(n)}.$$

Описанный процесс будем называть присоединением *дифференциального неизвестного*; получающееся дифференциальное кольцо будем обозначать через $A\{x\}$. Элементы кольца $A\{x\}$ называются *дифференциальными многочленами* от x (они являются обычными многочленами от x и его производных).

Если дифференциальное кольцо A является полем, то кольцо $A\{x\}$ представляет собой дифференциальную область целостности, и ее дифференцирование можно единственным образом продолжить на соответствующее поле отношений (теорема 1.1). Это поле отношений будем обозначать через $A\langle x\rangle$; его элементы (отношения дифференциальных многочленов) мы будем называть *дифференциальными рациональными функциями* от x.

Обозначения $\{\ \}$ и $\langle\ \rangle$ мы будем употреблять не только в случае присоединения дифференциального неизвестного, но и в случае присоединения элементов объемлющего дифференциального кольца или поля.

В любом дифференциальном кольце A элементы, производные которых равны нулю, образуют подкольцо C, называемое *кольцом констант*. Если A — поле, то и C — поле. Заметим, что C содержит подкольцо, порожденное единичным элементом кольца A.

Идеал I дифференциального кольца A называется дифференциальным идеалом, если из $a \in I$ следует, что $a' \in I$, или короче, если $I' \subset I$. В этом случае кольцо A/I можно определить как дифференциальное кольцо, считая производным от смежного класса $a+I$ класс $a'+I$; это определение не зависит от выбора представителей в смежных классах и действительно приводит к некоторому дифференцированию кольца A/I.

Гомоморфизм дифференциального кольца A в дифференциальное кольцо B (в обычном алгебраическом смысле) называется *дифференциальным гомоморфизмом*, если он перестановочен с дифференцированиями. Для любого дифференциального идеала I кольца A естественный гомоморфизм кольца A на кольцо A/I является дифференциальным гомоморфизмом. Понятия *дифференциального изоморфизма* и *дифференциального автоморфизма* определяются аналогично.

Теорема 1.2. *Ядро I произвольного дифференциального гомоморфизма, определенного в дифференциальном кольце A, является дифференциальным идеалом, и фактор-кольцо A/I дифференциально изоморфно образу кольца A.*

Доказательство очевидно, и мы его опустим.

3. Радикальные идеалы. Как и в обычной теории коммутативных колец, мы называем идеал I *радикальным*[1], если из $a^n \in I$ следует, что $a \in I$.

Лемма 1.3. *Если элемент ab принадлежит радикальному дифференциальному идеалу I, то $ab' \in I$ и $a'b \in I$.*

Доказательство. По условию $(ab)' = a'b + ab' \in I$. Отсюда, умножая на ab', получаем[2] $(ab')^2 \in I$ и, следовательно, $ab' \in I$.

Лемма 1.4. *Для любого радикального дифференциального идеала I и любого подмножества S дифференциального кольца A множество T всех элементов $x \in A$, для которых $xS \subseteq I$, является радикальным дифференциальным идеалом кольца A.*

Доказательство. Тот факт, что T является идеалом, доказывается в обычной теории колец. Далее, из леммы 1.3 следует, что T — дифференциальный идеал. Наконец, пусть $x^n \in T$. Тогда $x^n s^n \in I$ для любого элемента $s \in S$. Так как I — радикальный идеал, то отсюда вытекает, что $xs \in I$ и поэтому $x \in T$.

В произвольном коммутативном кольце пересечение любого множества радикальных идеалов является радикальным идеалом. В произвольном дифференциальном кольце пересечение любого множества дифференциальных идеалов является дифференциальным идеалом. Следовательно, пересечение любого множества радикальных дифференциальных идеалов является радикальным дифференциальным идеалом. Поэтому для любого подмножества S некоторого дифференциального кольца существует минимальный радикальный дифференциальный идеал, содержащий подмножество S; этот идеал мы будем обозначать через $\{S\}$ (не следует путать употребление скобок в этом случае с употреблением скобок в случае дифференциально-кольцевого присоединения).

[1] Идеалы с этими свойствами иногда называют совершенными. — *Прим. перев.*

[2] Напомним, что кольцо A предполагается коммутативным. — *Прим. ред.*

Лемма 1.5 *Для любого элемента a и любого подмножества S дифференциального кольца имеет место соотношение $a\{S\} \subset \{aS\}$.*

Доказательство. Множество всех элементов x, для которых $ax \in \{aS\}$ является, согласно лемме 1.4, радикальным дифференциальным идеалом. Этот идеал содержит подмножество S, а следовательно, и идеал $\{S\}$.

Лемма 1.6. *Для любых подмножеств S и T дифференциального кольца имеет место соотношение $\{S\}\{T\} \subset \subset \{ST\}$.*

Доказательство. Множество всех элементов x, для которых $x\{T\} \subset \{ST\}$ содержит, согласно лемме 1.5, подмножество S, а согласно лемме 1.4, является радикальным дифференциальным идеалом. Следовательно, это множество содержит идеал $\{S\}$.

4. Алгебры Ритта. Радикал произвольного идеала определяется, как множество всех элементов, некоторая степень которых принадлежит этому идеалу; радикал является, очевидно, радикальным идеалом. Для целей теории дифференциальных колец нужна была бы теорема о том, что радикал дифференциального идеала также является дифференциальным идеалом. Однако в общем случае это утверждение не верно.

Пример. Над полем характеристики 2 рассмотрим алгебру A ранга 2 с базисом 1, x, где $x^2 = 0$, а 1 — единица алгебры A. Полагая $1' = 0$, $x' = 1$, мы получили в A некоторое дифференцирование. Легко видеть, что радикал нулевого идеала совпадает с главным идеалом, порожденным элементом x, и, следовательно, не является дифференциальным идеалом.

Определение. *Алгеброй Ритта* называется дифференциальное кольцо, содержащее поле рациональных чисел (необходимо являющееся подполем кольца констант). Алгебра Ритта является алгеброй в обычном смысле над полем рациональных чисел (вообще говоря, бесконечного ранга).

Лемма. 1.7. *Пусть I — дифференциальный идеал алгебры Ритта, и пусть a — такой элемент, что $a^n \in I$. Тогда $(a')^{2n-1} \in I$.*

Доказательство. Докажем индукцией по k, что

$$a^{n-k}(a')^{2k-1} \in I.$$

Так как $(a^n)' = na^{n-1}a' \in I$ и идеал I выдерживает умножение на $\frac{1}{n}$, то $a^{n-1}a' \in I$, что доказывает справедливость нашего утверждения при $k=1$. Предположим теперь, что $a^{n-k}(a')^{2k-1} \in I$. Тогда

$$[a^{n-k}(a')^{2k-1}]' = (n-k)\,a^{n-k-1}(a')^{2k-1} + \\ + a^{n-k}(2k-1)(a')^{2k-2}a'' \in I.$$

Умножая это соотношение на a', мы получим, что второе слагаемое принадлежит идеалу I. Избавившись от множителя $n-k$ при первом слагаемом, мы получим, что $a^{n-k-1}(a')^{2k-1} \in I$. Тем самым общий шаг индукции проведен. При $k=n$ мы видим, что $(a')^{2n-1} \in I$.

Лемма. 1.8. *В алгебре Ритта радикал любого дифференциального идеала является дифференциальным идеалом.*

Это непосредственно следует из леммы 1.7.

Глава II

ПРОДОЛЖЕНИЕ ИЗОМОРФИЗМОВ

5. Теорема Крулля. В обычной теории коммутативных колец известна теорема о том, что любой радикальный идеал является пересечением простых идеалов. Оказывается, что слово „дифференциальный“ может быть включено и в посылку и в заключение этой теоремы. Доказательство этого факта основано на следующей лемме.

Лемма. *Пусть T — произвольное подмножество дифференциального кольца A, замкнутое относительно умножения, а Q — максимальный радикальный дифференциальный идеал, не содержащий ни одного элемента множества T. Тогда идеал Q прост.*

Доказательство. Пусть, вопреки утверждению, $ab \in Q$, $a \notin Q$, $b \notin Q$. Тогда идеалы $\{Q, a\}$ и $\{Q, b\}$ являются отличными от Q радикальными дифференциальными идеалами, включающими идеал Q и поэтому содержащими некоторые элементы множества T. Обозначая эти элементы через t_1 и t_2, в силу леммы 1.6, получим, что, вопреки условию,

$$t_1t_2 \in \{Q, a\}\{Q, b\} \subset Q.$$

Теорема 2.1. *Каждый радикальный дифференциальный идеал I дифференциального кольца A является пересечением простых дифференциальных идеалов.*

Доказательство. Достаточно для любого элемента x, не принадлежащего идеалу I, построить простой дифференциальный идеал, содержащий идеал I, но не содержащий элемент x. Пусть T — множество степеней элемента x. В силу леммы Цорна, существует максимальный радикальный дифференциальный идеал Q, включающий идеал I и не содержащий ни одного элемента множества T. Согласно только что доказанной лемме, идеал Q прост.

3 Зак. 267. И. Капланский

6. Расширение простых идеалов. Пусть A — дифференциальное кольцо, содержащееся в дифференциальном кольце B (предполагается, что единицы колец A и B совпадают), P — простой дифференциальный идеал кольца A и I — радикальный дифференциальный идеал кольца B, высекающий идеал P (т. е. $I \cap A = P$). Поставим следующие два вопроса:

1) Можно ли расширить идеал I до простого дифференциального идеала, тоже высекающего идеал P?

2) Является ли идеал I пересечением простых дифференциальных идеалов, высекающих идеал P?

Ответ на первый вопрос всегда оказывается утвердительным.

Теорема. 2.2. *Пусть A — некоторое дифференциальное подкольцо дифференциального кольца B и I — такой радикальный дифференциальный идеал кольца B, что пересечение $P = I \cap A$ является простым дифференциальным идеалом в A. Тогда идеал I может быть расширен до простого дифференциального идеала кольца B, тоже высекающего идеал P.*

Доказательство. Достаточно применить доказанную выше лемму, принимая за T дополнение к идеалу P в кольце A.

Для того чтобы ответ и на второй вопрос был утвердительным, надо дополнительно потребовать, чтобы из включений $ab \in I$, $a \in A$, $b \in B$ вытекало бы либо включение $a \in I$, либо включение $b \in I$. Это требование неизбежно, так как каждый идеал I, удовлетворяющий заключению теоремы, обладает этим свойством.

Теорема. 2.3. *Пусть A — некоторое дифференциальное подкольцо дифференциального кольца B, а I — такой радикальный дифференциальный идеал кольца B, что из включений $ab \in I$, $a \in A$, $b \in B$ вытекает либо включение $a \in I$, либо включение $b \in I$. (Для такого идеала пересечение $P = I \cap A$ является простым идеалом кольца A.) Тогда идеал I может быть представлен как пересечение простых дифференциальных идеалов кольца B, каждый из которых тоже высекает идеал P.*

Доказательство. Пусть x — произвольный элемент кольца B, не принадлежащий I. Мы должны построить простой дифференциальный идеал кольца B, содержащий идеал I, не содержащий элемент x и высекающий идеал P. Пусть T — множество всех элементов вида ax^n, где $a \in A$, $a \notin P$. Множество T замкнуто относительно умножения и, как вытекает из наших предположений, не пересекается с идеалом I. Следовательно, согласно доказанной выше лемме, существует простой дифференциальный идеал Q, содержащий идеал I и не содержащий ни одного элемента множества T. Очевидно, что $x \notin Q$, так как $x \in T$. Кроме того, $Q \cap A = P$. Действительно, если $a \in Q \cap A$, то $ax \in Q$, что невозможно при $a \notin P$. (Этим коротким доказательством теоремы 2.3 я обязан Роберту Макрею.)

7. Лемма о кольцах многочленов. Для удобства мы выделим следующую элементарную (не относящуюся к дифференциальным кольцам) лемму.

Лемма. 2.4. *Пусть L — произвольное поле, K — некоторое его подполе, B — кольцо многочленов над полем K от некоторого (быть может, бесконечного) множества неизвестных, и A — его подкольцо, состоящее из многочленов с коэффициентами из поля K. Пусть, далее, P — произвольный идеал кольца A, J — идеал кольца B, порожденный идеалом P, и I — радикал идеала J. Тогда* a) *если P — радикальный идеал, то $I \cap A = P$;* b) *если P — простой идеал, то из включения $ab \in I$, где $a \in A$, $b \in B$ вытекает либо включение $a \in P$, либо включение $b \in I$;* c) *если характеристика поля L равна нулю и $P \neq A$ (идеал P может не быть радикальным), то для любого неизвестного y и любого элемента s поля L, не принадлежащего подполю K, разность $y - s$ не принадлежит идеалу I.*

Доказательство. Рассмотрим поле L как векторное пространство над полем K. Пусть u_α, где α пробегает некоторое множество индексов, — произвольный базис векторного пространства L. Отдельные элементы этого базиса мы будем обозначать через u_1, u_2 и т. д. (хотя мы и не предполагаем множество индексов счетным или даже вполне упорядоченным). В частности, мы будем считать, что $u_1 = 1$. Каждый элемент кольца B единственным образом представляется в виде $\sum a_\alpha u_\alpha$, где $a_\alpha \in A$; этот элемент принадлежит кольцу A только тогда, когда все коэффициенты, за исключением коэффициента a_1, равны нулю. Кроме того, идеал J состоит из всех элементов вида $\sum p_\alpha u_\alpha$, где $p_\alpha \in P$. Следовательно, $J \cap A = P$ (каков бы ни был идеал P).

a) Пусть P — радикальный идеал. Для любого элемента $b \in I \cap A$ некоторая его степень b^n принадлежит, по определению, идеалу $J \cap A = P$. Так как идеал P радикален, то отсюда вытекает, что $b \in P$. Таким образом, $I \cap A = P$.

b) Пусть теперь P — простой идеал, и пусть $ab \in I$, где $a \in A$, $b \in B$. Тогда $a^n b^n \in J$. Пусть $b^n = \sum a_\alpha u_\alpha$. Тогда $\sum (a^n a_\alpha) u_\alpha \in J$ и, следовательно, $a^n a_\alpha \in P$ для любого α. Но это возможно только тогда, когда $a \in P$ или когда $a_\alpha \in P$ для всех α, в последнем случае $b^n \in J$ и $b \in I$.

c) Предполагая, что разность $y - s$ принадлежит идеалу I, мы придем сейчас к противоречию. Действительно, при этом предположении некоторая степень $(y-s)^m$ элемента $(y-s)$ принадлежит идеалу J. Пусть I_0 — множество всех многочленов от y (с коэффициентами из поля L), принадлежащих идеалу J. Множество I_0 является главным идеалом [1], который порождается некоторым элементом, делящим элемент $(y-s)^m$. Этот элемент не может быть константой (т. е. отличным от нуля элементом поля L), так как в этом случае идеал J совпал бы с кольцом B, а идеал $P = J \cap A$ — с кольцом A, что, согласно условию, невозможно. Следовательно, рассматриваемый элемент имеет вид $(y-s)^r$, где $r \geqslant 1$. Пусть теперь базис u_α выбран так, что $u_1 = 1$ и $u_2 = s$. В разложении элемента $(y-s)^r$ по элементам базиса каждый коэффициент должен принадлежать идеалу P, а следовательно, и идеалу J. Это относится, в частности, к коэффициенту при u_1, который представляет собой многочлен, начинающийся с члена y^r и не содержащий члена с y^{r-1}. Этот многочлен должен совпадать [2] с многочленом $(y-s)^r = y^r - rsy^{r-1} + \ldots$. Так как характеристика поля L равна нулю, то это невозможно.

Замечание. Можно доказать следующее утверждение, более сильное, чем (c): для полей нулевой характеристики

[1] В кольце многочленов над полем L от одного переменного y. — *Прим. ред.*

[2] Так как он делится на многочлен $(y-s)^r$. — *Прим. ред.*

идеал I радикален, если радикален идеал P; однако в дальнейшем мы пользоваться этим усиленным результатом не будем.

8. Допустимые изоморфизмы. Изоморфизм между полями K и L мы будем называть *допустимым*, если существует поле M, содержащее оба поля K и L.

Допустимые изоморфизмы будут на первых порах играть роль заменителей автоморфизмов; в соответствующем месте мы докажем, что допустимые изоморфизмы на самом деле являются автоморфизмами. Классическая теория Галуа основывается на том, что конечное сепарабельное расширение N поля K тогда и только тогда нормально над K, когда каждый допустимый изоморфизм поля N, оставляющий неподвижными все элементы поля K, является автоморфизмом. В современном изложении теории Галуа допустимые изоморфизмы вовсе не упоминаются, но они, по-видимому, совершенно необходимы для теории Галуа дифференциальных полей. Мы сейчас докажем две основные теоремы относительно продолжения и существования допустимых изоморфизмов. Читателю будет полезно сравнить эти теоремы с их (более простыми) аналогами в обычной теории полей.

Теорема 2.5. *Пусть M — дифференциальное поле характеристики нуль, а K и L — его дифференциальные подполя. Тогда любое дифференциальное изоморфное отображение S поля K на поле L может быть продолжено до допустимого дифференциального изоморфизма поля M.*

Доказательство. Согласно принципу трансфинитной индукции, достаточно доказать следующее утверждение: для любого элемента u поля M, не принадлежащего полю K, существует продолжение изоморфизма S, определенное на элементе u и переводящее этот элемент в некоторый элемент соответствующим образом подобранного расширения поля M. Пусть $K\{u\}$ — дифференциальная область целостности, полученная присоединением элемента u к полю K, а $K\{y\}$ — дифференциальная область целостности, полученная присоединением дифференциального неизвестного y. Пусть, далее, P_1 — ядро дифференциального гомоморфного отображения кольца $K\{y\}$ на кольцо $K\{u\}$, оставляющего неподвижными все элементы поля K и переводящего элемент y в элемент u; этот идеал является простым дифференциальным идеалом кольца $K\{y\}$ (он служит дифференциальным аналогом неприводимого многочлена с корнем u, который используется в соответствующем рассуждении в обычной теории полей). Изоморфизм S переводит идеал P_1 в некоторый простой дифференциальный идеал P кольца $L\{y\}$. Пусть J — идеал кольца $M\{y\}$, порожденный идеалом P. Этот идеал состоит из всех конечных сумм вида $\sum p_i m_i$, где $p_i \in P$, $m_i \in M\{y\}$, и поэтому является дифференциальным идеалом. Пусть I — его радикал. Согласно лемме 1.8, радикал I является (радикальным) дифференциальным идеалом кольца $M\{y\}$. Кроме того, $I \cap L\{y\} = P$, согласно утверждению (а) леммы 2.4. (Роль участвующих в лемме полей K и L здесь играют поля L и M. Заметим, что с точки зрения обычной алгебры кольцо $M\{y\}$ получается приседининением к полю M счетного множества обычных неизвестных.) Наконец, согласно теореме 2.2, идеал I можно расширить до такого простого дифференциального идеала Q кольца $M\{y\}$, что $Q \cap L\{y\} = P$.

Пусть v — образ элемента y при естественном гомоморфном отображении кольца $M\{y\}$ на кольцо $M\{y\}/Q$. Определим дифференциальный гомоморфизм кольца $K\{y\}$ на кольцо $L\{v\}$, отобразив сначала кольцо $K\{y\}$ на кольцо $L\{y\}$ посредством изоморфизма S, а затем кольцо $L\{y\}$ на кольцо $L\{v\}$ посредством отображения, переводящего элемент y в элемент v. Так как ядром последнего отображения является пересечение $Q \cap L\{y\} = P$, то ядром результирующего дифференциального гомоморфизма служит идеал P_1. Следовательно, этот гомоморфизм определяет некоторый дифференциальный изоморфизм между областями целостности $K\{u\}$ и $L\{v\}$, продолжающий изоморфизм S. В силу теоремы 1.1, этот изоморфизм может быть единственным образом продолжен до дифференциального изоморфизма между соответствующими полями отношений.

Теорема 2.6. *Пусть K — дифференциальное подполе дифференциального поля L, имеющее характеристику нуль, и s — некоторый элемент поля L, не принадлежащий полю K. Тогда существует допустимый дифференциальный изоморфизм поля L, для которого s не является неподвижным элементом, а поле K тождественно отображается на себя.*

Доказательство. По существу доказательство совпадает с доказательством теоремы 2.5. Пусть y — дифференциаль-

ное неизвестное и P — ядро естественного гомоморфного отображения кольца $K\{y\}$ на кольцо $K\{s\}$. Очевидно, что $P \neq K\{y\}$ для $s \neq 0$. Пусть J — идеал кольца $L\{y\}$, порожденный идеалом P. Будем пока считать, что $L = K\langle s\rangle$. Радикал I идеала J тогда является радикальным дифференциальным идеалом кольца $L\{y\}$, высекающим в кольце $K\{y\}$ идеал P. Расширим идеал I до простого дифференциального идеала Q кольца $L\{y\}$, тоже высекающего идеал P. Пусть t — образ элемента y при естественном гомоморфном отображении кольца $L\{y\}$ на кольцо $L\{y\}/Q$. Сопоставляя элементу s элемент t, мы получим допустимый дифференциальный изоморфизм между полями $K\langle s\rangle$ и $K\langle t\rangle$. Очевидно, что элементы s и t совпадают только тогда, когда $y - s \in Q$.

Согласно утверждению (b) леммы 2.4, условия теоремы 2.3 выполнены (роль колец A и B играют кольца $K\{y\}$ и $L\{y\}$ соответственно). Следовательно, пересечение всевозможных идеалов Q построенного выше типа совпадает с идеалом I. Поэтому если $y - s \in Q$ для всех идеалов Q, то $y - s \in I$. Но это противоречит утверждению (с) леммы 2.4.

Переходя к полям отношений, мы получим дифференциальный изоморфизм между полями $K\langle s\rangle$ и $L\langle t\rangle$, при котором образ элемента s отличен от s. Остается заметить, что, согласно теореме 2.5, этот изоморфизм можно продолжить до допустимого дифференциального изоморфизма, определенного на всем поле L.

Глава III

ЭЛЕМЕНТЫ ТЕОРИИ ГАЛУА

9. Дифференциальная группа Галуа. Пусть M — произвольное дифференциальное поле и K — его дифференциальное подполе. Дифференциальной группой Галуа G поля M относительно поля K мы будем называть группу всех дифференциальных автоморфизмов поля M, оставляющих все элементы K неподвижными. Для любого „промежуточного“ дифференциального поля L мы будем через L' обозначать подгруппу группы G, состоящую из всех автоморфизмов, оставляющих все элементы поля L неподвижными (иными словами, L' есть дифференциальная группа Галуа поля M над полем L). Для любой подгруппы H группы G мы будем обозначать через H' множество всех элементов поля M, остающихся неподвижными при всех автоморфизмах из группы H; множество H' автоматически является дифференциальным полем, заключенным между полями K и M. Очевидно, что $L'' \supset L$ и $L_1' \subset L_2'$, если $L_1 \subset L_2$. Аналогичные включения имеют место и для подгрупп. Отсюда, в частности, следует, что $H''' = H'$ и $L''' = L'$. Поле L мы будем называть *замкнутым*, если $L'' = L$. Аналогично группу H мы будем называть *замкнутой*, если $H'' = H$. Таким образом, *каждый штрихованный объект замкнут, и штрихование устанавливает взаимно однозначное соответствие между замкнутыми подгруппами и замкнутыми промежуточными дифференциальными полями*. При этом, конечно, остается открытым основной вопрос: какие подгруппы и подполя замкнуты?

Классическая теория Галуа может быть несколько дополнена доказательством того, что свойство полей или групп быть замкнутыми сохраняется при „конечных расширениях“. Мы не будем пользоваться этими соображениями в полном объеме и докажем только то, что подгруппа, соответствующая конечному расширению, имеет конечный индекс.

Лемма 3.1. *Пусть N — произвольное дифференциальное поле, K — его дифференциальное подполе, а L и M — такие промежуточные дифференциальные подполя, что $M \supset L$ и $[M:L] = n$. Пусть, далее, L' и M' — соответствующие подгруппы дифференциальной группы Галуа поля N над полем K. Тогда индекс подгруппы M' в группе L' не превосходит n.*

Доказательство. Поскольку относительные степени полей, как и индексы подгрупп, мультипликативны, достаточно доказать лемму для случая простого расширения. Пусть $M = L(u)$. Тогда правые смежные классы группы L' по подгруппе M' в точности соответствуют всевозможным образам элемента u (при автоморфизмах, оставляющих все элементы поля L неподвижными). Существует не более n таких образов, ибо каждый из них является корнем неприводимого над полем L многочлена, имеющего своим корнем элемент u.

Лемма 3.2. *Пусть G — дифференциальная группа Галуа дифференциального поля M над полем K, а H и J — такие ее подгруппы, что $H \supset J$ и индекс подгруппы J в подгруппе H равен n. Пусть, далее, H' и J' — соответствующие промежуточные дифференциальные поля. Тогда $[J':H'] \leqslant n$.*

Доказательство. Пусть, вопреки заключению, в поле J' существует $n+1$ элементов $u_1, \ldots, u_{n+1}$, линейно независимых над полем H'. Рассмотрим произвольные представители $S_1, S_2, \ldots, S_n$ правых смежных классов группы H по подгруппе J. Для удобства можно считать, что $S_1 = E$. Составим следующую систему уравнений:

$$\sum_{i=1}^{n+1} a_i (u_i S_j) = 0 \qquad (j = 1, \ldots, n). \tag{*}$$

Так как эта система состоит из n линейных однородных уравнений с $n+1$ неизвестными, то она имеет нетривиальные решения в поле M. Среди всех таких решений выберем одно из самых „коротких“ решений, т. е. решение, содержащее наибольшее количество нулей. Пусть это решение состоит из отличных от нуля элементов $a_1, a_2, \ldots, a_r$ и соответствующего числа нулей. Можно считать, что $a_1 = 1$. Все элементы a_i не могут принадлежать полю H', так как в противном случае первое из уравнений системы (*)

противоречило бы линейной независимости элементов $u_1, \ldots, u_{n+1}$. Предположим для определенности, что полю H не принадлежит элемент a_r. Тогда некоторый автоморфизм из группы H не оставляет элемент a_r неподвижным. Пусть этот автоморфизм принадлежит смежному классу JS_k. Так как все элементы u_i инвариантны относительно группы J, то, не меняя уравнений (*), можно как угодно изменить выбор представителей в смежных классах. В частности, можно считать, что $a_r S_k \neq a_r$. Поэтому, применив к равенствам (*) автоморфизм S_k, мы получим другое решение системы (*). Вычтя одно решение из другого, мы придем к более короткому решению [1]), что по условию невозможно.

Комбинируя эти две леммы, мы получим следующую лемму.

Лемма 3.3. *Любое конечное расширение замкнутого промежуточного дифференциального поля замкнуто. Аналогично, любая подгруппа дифференциальной группы Галуа, обладающая замкнутой подгруппой конечного индекса, замкнута.*

Кое-что о значении нормальных делителей может быть доказано даже и в рассматриваемом чрезвычайно общем контексте.

Теорема 3.4. *Пусть M — произвольное дифференциальное поле, K — его дифференциальное подполе, G — дифференциальная группа Галуа поля M над полем K. Тогда* a) *для любого нормального делителя H группы G каждый дифференциальный автоморфизм поля M над полем K отображает поле H' само на себя;* b) *если L — такое промежуточное дифференциальное поле, что каждый дифференциальный автоморфизм поля M над полем K отображает поле L само на себя, то подгруппа L' является нормальным делителем группы G, а факторгруппа G/L' — группой всех дифференциальных автоморфизмов поля L над полем K, продолжающихся на поле M.*

Доказательство. a) Пусть S — произвольный дифференциальный автоморфизм поля M над полем K. Оказывается, что $xS \in H'$ для любого элемента $x \in H'$, т. е. что $xST = xS$

[1]) Действительно, первые координаты обоих решений совпадают. — *Прим. ред.*

для любого автоморфизма $T \in H$. Действительно, $STS^{-1} \in H$ и, следовательно, $xSTS^{-1} = x$. Тем самым доказано, что S отображает поле H' само на себя. Но то же самое имеет место и для автоморфизма S^{-1}. Поэтому автоморфизм S отображает поле H' само на себя.

b) Чтобы доказать, что подгруппа L' — нормальный делитель, достаточно повторить в обратном порядке рассуждения, проведенные в пункте (a). Рассмотрим, далее, естественный гомоморфизм группы G в дифференциальную группу Галуа поля L над полем K, получающийся ограничением области действия автоморфизмов полем L. Ядром этого гомоморфизма является нормальный делитель L', а его образ состоит из всех дифференциальных автоморфизмов поля L над полем K, продолжающихся на все поле M.

Стоит отметить следующее следствие теоремы 3.4: *замыкание нормального делителя является нормальным делителем.*

Будем говорить, что поле M нормально над полем K, если для каждого элемента поля M, не принадлежащего полю K, существует дифференциальный автоморфизм поля M над полем K, для которого этот элемент не является неподвижным. В терминах, введенных выше, нормальность означает, что $K'' = K$, т. е. что поле K замкнуто.

Легко видеть, что подполе L, соответствующее нормальному делителю, нормально над K. Обратное утверждение, вообще говоря, неверно. Условия, достаточные для того, чтобы обратное утверждение было справедливо, указываются ниже, в лемме 3.6.

Лемма 3.5. *Для любого замкнутого подполя L нормализатор соответствующей подгруппы H (т. е. множество всех автоморфизмов $S \in G$, для которых $SHS^{-1} = H$) совпадает с множеством всех автоморфизмов $S \in G$, отображающих поле L само на себя.*

Доказательство аналогично доказательству теоремы 3.4.

Лемма 3.6. *Пусть L — замкнутое подполе поля M, нормальное над полем K, и H — соответствующая подгруппа. Если нормализатор H_1 подгруппы H замкнут и каждый дифференциальный автоморфизм поля L над полем K продолжается на поле M, то подгруппа H является нормальным делителем, а факторгруппа G/H —*

полной дифференциальной группой Галуа поля L над полем K.

Доказательство. Тот факт, что подгруппа H является нормальным делителем, означает, что $H_1 = G$, т. е. что $L_1 = K$, где L_1 — поле, соответствующее подгруппе H_1 (напомним, что подгруппа H_1 замкнута). Согласно лемме 3.5, подгруппа H_1 состоит из всех автоморфизмов $S \in G$, отображающих поле L само на себя. Совокупность всех автоморфизмов поля L, индуцированных автоморфизмами группы H_1, совпадает с совокупностью всех автоморфизмов поля L над полем K, так как любой такой автоморфизм по условию продолжается на поле M. Так как поле L нормально над полем K, то отсюда следует, что никакой элемент поля L, не принадлежащий полю K, не остается неподвижным при всех автоморфизмах из группы H_1. Но это и означает, что $L_1 = K$. Второе утверждение леммы вытекает из последнего утверждения теоремы 3.4.

10. Вронскиан. *Вронскианом* n элементов $y_1, \ldots, y_n$ произвольного дифференциального кольца называется определитель

$$W(y_1, \ldots, y_n) = \begin{vmatrix} y_1 & y_2 & \ldots & y_n \\ y_1' & y_2' & \ldots & y_n' \\ \cdot & \cdot & \ldots & \cdot \\ y_1^{(n-1)} & y_2^{(n-1)} & \ldots & y_n^{(n-1)} \end{vmatrix}.$$

Теорема 3.7. *Элементы некоторого дифференциального поля F с полем констант C тогда и только тогда линейно зависимы над C, когда их вронскиан равен нулю.*

Доказательство. Пусть элементы $y_1, \ldots, y_n$ линейно зависимы над C, т. е. $\sum c_i y_i = 0$. Дифференцируя это уравнение $n-1$ раз, мы получаем n линейных однородных уравнений относительно $c_1, c_2, \ldots, c_n$. Так как не все c_i равны нулю, то определитель системы равен нулю.

Обратно, пусть вронскиан элементов $y_1, \ldots, y_n$ равен нулю. Тогда в поле F можно найти нетривиальное решение $c_1, \ldots, c_n$ системы уравнений $\sum c_i y_i^{(j)} = 0$; $j = 0, \ldots, n-1$. Можно считать, что $c_1 = 1$ и что вронскиан элементов $y_2, \ldots, y_n$ не равен нулю. Продифференцировав каждое из первых $n-1$ уравнений и учтя соответствующие уравнения исходной системы, мы получим систему $n-1$ линейных однородных уравнений относительно $c_2', \ldots, c_n'$, определитель которой является вронскианом элементов $y_2, \ldots, y_n$. Поэтому $c_2' = \ldots = c_n' = 0$, т. е. все c_i являются константами.

Благодаря теореме 3.7 высказывание „данные элементы линейно зависимы над полем констант“ имеет смысл, не зависящий от поля, в котором рассматриваются эти элементы. Действительно, обращение в нуль вронскиана не зависит от выбора поля.

11. Расширения Пикара — Вессио. Рассмотрим линейное однородное дифференциальное уравнение

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + \ldots + a_{n-1} y' + a_n y = 0 \qquad (*)$$

с коэффициентами в некотором дифференциальном поле K. Пусть $u_1, \ldots, u_{n+1}$ — произвольные решения этого уравнения, принадлежащие некоторому (возможно, большему) дифференциальному полю. Легко видеть, что элементы $u_1, \ldots, u_{n+1}$ линейно зависимы над полем констант. Действительно, равенства $L(u_i) = 0$ $(i = 1, \ldots, n+1)$ показывают, что последняя строка вронскиана, состоящая из элементов $u_1, \ldots, u_{n+1}$, является линейной комбинацией предыдущих строк.

Определение. Дифференциальное поле M, содержащее поле K, называется *расширением Пикара — Вессио* поля K (соответствующим уравнению (*)), если

1) $$M = K\langle u_1, \ldots, u_n \rangle,$$

где $u_1, \ldots, u_n$ — n решений уравнения (*), линейно независимых над полем констант;

2) поле M имеет то же самое поле констант, что и поле K.

Если характеристика поля K равна нулю и поле констант алгебраически замкнуто, то основной вопрос о существовании решается положительно: для любого однородного линейного дифференциального уравнения над полем K существует соответствующее ему расширение Пикара — Вессио. Самая трудная часть доказательства связана с условием сохранения поля констант (см. [3]). Те же соображения могут быть использованы (по сообщению Колчина) и для доказательства единственности (с точностью до дифференциального изоморфизма) расширения Пикара — Вессио, соответствующего данному уравнению.

Примеры расширений Пикара — Вессио. 1. Два простых примера (присоединение интеграла и присоединение экспоненты интеграла) будут рассмотрены в следующем пункте.

2. В случае, когда K является полем всех мероморфных функций в некоторой области комплексной плоскости, классические теоремы существования показывают, что расширения Пикара — Вессио существуют для любого линейного однородного дифференциального уравнения над полем K.

3. Если мы свободны в выборе основного поля и его надполя, то легко показать, что существует расширение Пикара — Вессио, дифференциальная группа Галуа которого является полной линейной группой. Действительно, пусть K_0 — произвольное дифференциальное поле, а $M = K_0\langle x_1, \ldots, x_n\rangle$ — поле, полученное присоединением к полю K_0 дифференциальных неизвестных $x_1, \ldots, x_n$. Пусть, далее, T — произвольное невырожденное линейное преобразование неизвестных $x_1, \ldots, x_n$ с коэффициентами из поля констант C поля K_0:

$$x_iT = \sum c_{ij}x_j, \qquad c_{ij} \in C.$$

Распространим преобразование T на все поле M, полагая для производных

$$x_i^{(m)}T = \sum_j c_{ij}x_j^{(m)}.$$

В результате мы получим некоторый дифференциальный автоморфизм поля M. Пусть K — поле, состоящее из всех элементов поля M, неподвижных при любом преобразовании T, и пусть

$$L(y) = \frac{W(y, x_1, \ldots, x_n)}{W(x_1, \ldots, x_n)},$$

где W — вронскиан. Равенство $L(y) = 0$ является линейным однородным дифференциальным уравнением относительно y с коэффициентами из поля K; элементы $x_1, \ldots, x_n$ — линейно независимые решения этого уравнения; поле M — расширение Пикара — Вессио поля K, соответствующее уравнению $L(y) = 0$; дифференциальная группа Галуа этого расширения совпадает с полной линейной группой.

В главе V, где завершается изложение теории Галуа, мы сможем существенно обобщить этот результат: рассматривая M над соответствующим промежуточным дифференциальным полем, мы представим произвольную алгебраическую матричную группу как группу Галуа.

Пусть M — произвольное расширение Пикара — Вессио поля K и S — некоторый дифференциальный автоморфизм поля M над полем K. Элементы u_iS линейно выражаются через элементы u_j с коэффициентами из поля констант C. Пусть $u_iS = \sum c_{ij}u_j$. Матрица (c_{ij}) — невырожденная, так как обратному автоморфизму соответствует обратная матрица. Таким образом, дифференциальная группа Галуа изоморфна некоторой мультипликативной группе невырожденных матриц над полем C. Вопрос о том, какие матричные группы могут при этом появиться, представляет собой один из основных вопросов, которые мы будем рассматривать.

Лемма 3.8. *Пусть $K \subset L \subset M$ — дифференциальные поля. Если поле L является расширением Пикара — Вессио поля K, а поле M имеет то же поле констант, что и поле K, то при любом дифференциальном автоморфизме поля M над полем K поле L переходит в себя.*

Доказательство очевидно.

12. Два специальных случая.

12. Два специальных случая. Рассмотрим теперь два важнейших типа расширений, которые послужат нам основой для дальнейших построений. Первый тип расширений получается посредством присоединения интеграла от элемента, не имеющего интеграла в данном поле. Последнее ограничение вызвано тем, что в противном случае расширение сводится к присоединению некоторой новой константы.

Лемма 3.9. *Пусть K — произвольное дифференциальное поле характеристики нуль и u — такой элемент некоторого большего дифференциального поля, что $u' = a \in K$. Тогда, если элемент a не является производным ни от какого элемента поля K, то элемент u трансцендентен над полем K, а поле $K\langle u\rangle$ является расширением Пикара — Вессио поля K, дифференциальная группа Галуа которого изоморфна аддитивной группе поля констант поля K.*

Доказательство. Предполагая, что элемент u алгебраичен над полем K, рассмотрим неприводимое уравнение, которому удовлетворяет этот элемент:

$$u^n + bu^{n-1} + \ldots = 0.$$

Продифференцировав это уравнение, мы получим, что элемент u удовлетворяет уравнению

$$nu^{n-1}a+b'u^{n-1}+\ldots=0.$$

Отсюда вытекает, что $na+b'=0$, так что элемент a является производным от элемента $-\frac{b}{n}\in K$. Полученное противоречие доказывает трансцендентность элемента u.

Докажем теперь, что поле $K\langle u\rangle$ не содержит новых констант. Пусть некоторый многочлен $b_1u^n+b_2u^{n-1}+\ldots$ является константой. Продифференцировав этот многочлен, мы получим уравнение

$$b_1'u^n+(nb_1a+b_2')\,u^{n-1}+\ldots=0.$$

Так как элемент u трансцендентен, то $b_1'=nb_1a+b_2'=0$ и, следовательно, элемент a является производным от элемента $-b_2/nb_1$, что противоречит условию. Пусть, далее, некоторая рациональная функция $f(u)/g(u)$ является константой. Мы можем считать, что эта дробь несократима, степень многочлена $g(u)$ больше нуля и его старший коэффициент равен единице. Продифференцировав эту функцию, мы получим, что $f/g=f'/g'$, где g' — отличный от нуля многочлен, степень которого меньше степени многочлена g. В силу несократимости дроби f/g это равенство невозможно.

Заметив, что элементы 1 и u — решения уравнения $y''-(a'/a)\,y'=0$, линейно независимые над полем констант, мы убеждаемся в том, что поле $K\langle u\rangle$ действительно является расширением Пикара — Вессио поля K.

При любом автоморфизме поля $K\langle u\rangle$ над полем K элемент u должен перейти в элемент с тем же производным элементом a, т. е. в элемент $u+c$, где c принадлежит полю констант C. Обратно, любое отображение $u\to u+c$ порождает некоторый автоморфизм поля $K\langle u\rangle$ над полем K по крайней мере в чисто алгебраическом смысле. Убедимся прямым подсчетом, что этот автоморфизм является дифференциальным автоморфизмом. Проверку достаточно провести лишь для элементов, являющихся многочленами от u. Любой такой многочлен $\sum\lambda_iu^i$ переходит в многочлен $\sum\lambda_i(u+c)^i$, производная от которого имеет вид

$$\sum\left[i\lambda_i(u+c)^{i-1}a+\lambda_i'(u+c)^i\right]$$

и является, очевидно, образом производного многочлена $\sum\left[i\lambda_iu^{i-1}+\lambda_i'u^i\right]$.

Второй тип расширений получается посредством присоединения *экспоненты интеграла*. Для этого случая мы докажем следующий несколько более слабый результат.

Лемма 3.10. *Пусть K — произвольное дифференциальное поле и u — такой элемент, удовлетворяющий уравнению $y'-ay=0\,(a\in K)$, что расширение $K\langle u\rangle$ имеет то же поле констант, что и поле K. Тогда поле $K\langle u\rangle$ является расширением Пикара — Вессио поля K, и его дифференциальная группа Галуа изоморфна некоторой подгруппе мультипликативной группы отличных от нуля констант поля K.*

Доказательство. Тот факт, что поле $K\langle u\rangle$ является расширением Пикара — Вессио поля K непосредственно вытекает из определения. Пусть v — произвольное решение уравнения $y'-ay=0$. Тогда $(v/u)'=0$, так что $v=cu$, где c — некоторая константа. Таким образом, каждый дифференциальный автоморфизм порождается некоторым соответствием $u\to cu$.

13. Расширения Лиувилля. Поле M называется *расширением Лиувилля* поля K, если существует такая цепочка промежуточных дифференциальных полей $K=K_1\subset K_2\subset\ldots$ $\ldots\subset K_n=M$, что для любого i поле K_{i+1} является расширением поля K_i с помощью интеграла или экспоненты интеграла.

Теорема 3.11. *Если расширение Лиувилля M дифференциального поля K имеет то же поле констант, что и поле K, то его дифференциальная группа Галуа G разрешима.*

Доказательство. Из лемм 3.9, 3.10 и 3.8 следует, что каждый дифференциальный автоморфизм поля M над полем K отображает поле K_2 само на себя. Пусть H_2 — подгруппа группы G, соответствующая подполю K_2, в смысле теории Галуа. Согласно теореме 3.4, подгруппа H_2 является нормальным делителем группы G. Так как факторгруппа G/H_2 является подгруппой дифференциальной группы Галуа поля K_2 над полем K (теорема 3.4), а эта последняя абелева, то и факторгруппа G/H_2 абелева. Продолжая рассуждение, мы убедимся в том, что группа G разрешима.

Этот результат обладает двумя недостатками. Во-первых, было бы желательно доказать аналогичную теорему для по-

5 Зак. 267. И. Капланский

лей, *вложенных* в расширения Лиувилля. Во-вторых, следовало бы допустить алгебраические расширения как дополнительный тип „строительных кирпичей". Для того чтобы достичь такого рода усовершенствований, требуется существенно более глубокая теория.

14. Треугольные автоморфизмы. Следующая теорема 3.12 является первым шагом на пути к обращению теоремы 3.11. Мы помещаем ее в этом параграфе с целью подчеркнуть, что ее доказательство не требует ничего из той более глубокой теории, которую мы еще будем развивать.

Теорема 3.12. *Пусть дифференциальное поле M нормально над своим дифференциальным подполем K, и пусть $u_1, \ldots, u_n$ — такие элементы поля M, что для каждого дифференциального автоморфизма σ поля M имеет место равенство*

$$u_i\sigma = a_{i,i}u_i + a_{i,i+1}u_{i+1} + \ldots + a_{i,n}u_n \quad (i = 1, \ldots, n), \quad (*)$$

где $a_{i,j}$ — константы поля M (зависящие от автоморфизма σ). Тогда поле $K\langle u_1, \ldots, u_n\rangle$ является расширением Лиувилля поля K.

Доказательство. Последнее из уравнений (*) имеет вид $u_n\sigma = a_{n,n}u_n$. Дифференцируя и деля получающееся уравнение на исходное, мы получим, что элемент u'_n/u_n инвариантен относительно σ (можно считать, что $u_n \neq 0$, так как в противном случае элемент u_n можно было бы просто опустить). Отсюда и из того, что поле M нормально над полем K, вытекает, что $u'_n/u_n \in K$. Следовательно, присоединение элемента u_n к полю K представляет собой присоединение экспоненты интеграла. Разделив теперь каждое из предыдущих $n-1$ уравнений на $u_n\sigma = a_{nn}u_n$ и продифференцировав, мы получим следующую систему уравнений:

$$\left(\frac{u_i}{u_n}\right)'\sigma = \frac{a_{i,i}}{a_{n,n}}\left(\frac{u_i}{u_n}\right)' + \ldots + \frac{a_{i,n-1}}{a_{n,n}}\left(\frac{u_{n-1}}{u_n}\right)'.$$

Эта система является системой уравнений для элементов $(u_i/u_n)'$ $(i = 1, \ldots, n-1)$, имеющей то же строение, что и исходная система. Рассуждая по индукции, мы получаем отсюда, что присоединение к полю K элементов $(u_i/u_n)'$ представляет собой расширение Лиувилля. Присоединение же самих элементов u_i/u_n означает присоединение интегралов.

Глава IV

АЛГЕБРАИЧЕСКИЕ МАТРИЧНЫЕ ГРУППЫ И ТОПОЛОГИЯ ЗАРИСКОГО

15. Z-пространства. Пусть F — произвольное поле, V — n-мерное векторное пространство над полем F и $F[x_1, \ldots, x_n]$ — кольцо многочленов от n неизвестных над полем F. Под *алгебраическим многообразием* пространства V мы понимаем множество всех корней некоторой системы многочленов из кольца $F[x_1, \ldots, x_n]$. Иначе алгебраическое многообразие можно определить как множество всех корней произвольного идеала кольца $F[x_1, \ldots, x_n]$. По теореме Гильберта о базисах идеалы кольца $F[x_1, \ldots, x_n]$ удовлетворяют условию обрыва возрастающих цепей. Следовательно, алгебраические многообразия пространства V удовлетворяют условию обрыва убывающих цепей.

Известно, что объединение конечного числа или пересечение любого числа алгебраических многообразий является алгебраическим многообразием. Поэтому мы можем использовать алгебраические многообразия в качестве замкнутых множеств некоторой T_1-топологии пространства V. Эту топологию мы будем называть *топологией Зариского*.

Переходя на абстрактную точку зрения, мы будем рассматривать T_1-пространства, удовлетворяющие условию обрыва убывающих цепей замкнутых множеств (или, что то же, условию обрыва возрастающих цепей открытых множеств). Такие пространства мы будем называть *Z-пространствами*.

Лемма 4.1. а) *Каждое подпространство Z-пространства является Z-пространством.* b) *Каждое T_1-пространство, являющееся непрерывным образом Z-пространства, является Z-пространством,* с) *каждое хаусдорфово Z-пространство конечно.*

Первые два утверждения леммы очевидны; третье следует из известного результата о том, что бесконечное хаусдорфово пространство содержит бесконечно много непересекающихся открытых множеств.

Лемма 4.2. *Любое Z-пространство является объединением конечного числа непересекающихся, связных, одновременно замкнутых и открытых подмножеств.*

Доказательство. Пусть X — произвольное Z-пространство. Если это пространство несвязно, то оно является объединением двух непересекающихся множеств, замкнутых и открытых одновременно. Если хотя бы одно из этих множеств несвязно, то его также можно расщепить на два множества, замкнутые и открытые одновременно. Ввиду условия обрыва убывающих цепей замкнутых множеств этот процесс остановится после конечного числа шагов, и мы придем к связной, открытой и одновременно замкнутой компоненте пространства X. В дополнении этой компоненты можно найти по аналогичным соображениям другую такую компоненту и т. д. Условие обрыва возрастающих цепей открытых множеств обеспечивает окончание этого построения в конечное число шагов.

16. T_1-группы и Z-группы.

Группа G всех неособых матриц порядка n над произвольным полем F является подмножеством n^2-мерного пространства, и потому на ней определена топология Зариского. Ниже мы покажем, что в этой „топологической группе" операция взятия обратного элемента непрерывна, а операция умножения непрерывна по каждому переменному. Однако по совокупности переменных умножение не непрерывно (если группа G бесконечна). Действительно известно, что если умножение непрерывно по совокупности переменных, то пространство группы G — хаусдорфово (и даже вполне регулярно), тогда как, согласно утверждению (с) леммы 4.1, хаусдорфово Z-пространство конечно.

Группа $G \times G$ является подмножеством $2n^2$-мерного пространства и потому в ней также определена топология Зариского. Эта топология сильнее произведения самой на себя топологии Зариского, определенной в группе G, и в ней умножение, заданное в группе G, непрерывно по совокупности обоих переменных. Однако рассмотрение последней топологии не соответствует нашему намерению изучать группу G по возможности в духе абстрактной теории топологических групп.

Лемма 4.3. *Пусть V и W — векторные пространства размерности m и n соответственно над полем F с топологией Зариского, $r_1, \ldots, r_n$ — некоторые рациональные функции от m переменных $x_1, \ldots, x_m$, S — множество всех точек пространства V, в которых знаменатели функций $r_1, \ldots, r_n$ обращаются в нуль, и T — дополнение к множеству S в пространстве V. Тогда отображение множества T в пространство W, определенное соответствием $(x_1, \ldots, x_m) \to (y_1, \ldots, y_n)$, где $y_i = r_i(x_1, \ldots, x_m)$ непрерывно.*

Доказательство. Нужно показать, что прообраз любого замкнутого множества замкнут. Произвольное замкнутое множество пространства W состоит по определению из всех корней некоторой системы многочленов $g_j(y_1, \ldots, y_n)$. Его прообраз состоит из всех корней (в V) системы рациональных функций $g_j(r_1, \ldots, r_n)$, или, что то же, из всех корней их числителей. Это множество замкнуто в топологии Зариского множества T.

Пример матричной группы с топологией Зариского оправдывает следующее

Определение. Будем говорить, что G есть *T_1-группа*, если G является группой и T_1-пространством, причем операция взятия обратного элемента непрерывна, а умножение непрерывно по каждому из сомножителей. Другими словами, требуется, чтобы левое умножение, правое умножение и взятие обратного элемента были бы гомеоморфными отображениями группы G на себя. T_1-группу, пространство которой является Z-пространством, мы будем называть Z-группой.

Известные свойства компоненты единицы сохраняются в любой T_1-группе:

Лемма 4.4. *Компонента единицы T_1-группы является замкнутым нормальным делителем.*

Доказательство. Пусть C — компонента единицы T_1-группы G. Множество C^{-1} связно (как непрерывный образ связного множества) и содержит единицу, следовательно, $C^{-1} \subset C$. Для любого элемента $c \in C$ множество cC связно и имеет с C общий элемент c, следовательно, $cC \subset C$. Таким образом, C является подгруппой. Так как для любого элемента x группы G множество $x^{-1}Cx$ связно и содержит единицу, то $x^{-1}Cx \subset C$, следовательно, C является нормальным делителем.

Сопоставляя леммы 4.2 и 4.4, мы видим, что имеет место следующая

Лемма 4.5. *Компонента единицы Z-группы является замкнутым нормальным делителем конечного индекса.*

17. C-группы. В T_1-группе и даже в Z-группе центр не обязан быть замкнутым. Аналогично замыкание абелевой подгруппы может не быть абелевой группой. Наиболее печальным для нас является тот факт, что коммутант связной группы может оказаться несвязным. Соответствующие примеры можно строить, например, на основании следующих соображений. Пусть G — произвольная группа. Введем в нее топологию, объявив замкнутыми только конечные множества и всю группу. (Это наиболее слабая из всех возможных T_1-топологий на группе G; мы будем ее называть минимальной T_1-топологией.) Относительно этой топологии G является T_1-группой. Чтобы получить пример, скажем, группы с незамкнутым центром, достаточно взять абстрактную группу G, центр которой бесконечен, но не совпадает с G (примеров таких групп достаточно много).

Для наших целей все же нет необходимости сужать класс рассматриваемых групп до топологических групп. Достаточно следующей более слабой аксиомы.

Определение. C-группой называется Z-группа, в которой для любого фиксированного элемента x отображение $a \to a^{-1}xa$ непрерывно.

Матричная группа в топологии Зариского является C-группой. Действительно, пусть X — произвольная фиксированная матрица. Так как элементы матрицы $A^{-1}XA$ являются рациональными функциями элементов матрицы A, то, в силу леммы 4.3, отображение $A \to A^{-1}XA$ непрерывно. Аналогично можно показать, что отображение, переводящее матрицу A в некоторое „слово“, состоящее из A и любых фиксированных матриц, непрерывно. Однако никакими словами, кроме $A^{-1}XA$, мы пользоваться не будем.

Лемма 4.6. *Если компонента единицы C-группы G имеет конечный индекс k, то каждый конечный класс сопряженных элементов группы G содержит не более k элементов.*

Доказательство. Пусть существует элемент x, имеющий конечное, но превосходящее k число сопряженных. При

непрерывном отображении $a \to a^{-1}xa$ прообраз каждого сопряженного элемента открыт и замкнут одновременно. Тем самым группа G разлагается в более, чем k открытых и одновременно замкнутых множеств. Полученное противоречие доказывает лемму.

Отметим следующий специальный случай леммы 4.6:

Лемма 4.7. *В связной C-группе каждый нецентральный элемент имеет бесконечно много сопряженных.*

Теорема 4.8. *Коммутант G' связной C-группы G связен.*

Доказательство. Пусть D_k — множество всех произведений по k коммутаторов в группе G. Тогда $D_1 \subset D_2 \subset \ldots$ и объединение всех множеств D_k совпадает с коммутантом G'. Достаточно доказать, что каждое множество D_k связно. Рассмотрим отображение

$$a_1 \to a_1^{-1}b_1^{-1}a_1b_1a_2^{-1}b_2^{-1}a_2b_2 \ldots a_k^{-1}b_k^{-1}a_kb_k,$$

где все элементы, кроме элемента a_1, фиксированы. Это отображение непрерывно и потому переводит группу G в связное множество. Последнее имеет элемент, общий с множеством D_{k-1}, получающийся при $a_1 = b_1$. Меняя элемент a_1, мы представим, следовательно, множество D_k в виде объединения связных множеств, каждое из которых имеет общую точку с множеством D_{k-1}, которое мы по индуктивному предположению считаем связным. Поэтому множество D_k связно.

Приведем в заключение еще два результата, которые будут нужны нам в главе V.

Лемма 4.9. *Пусть G — произвольная C-группа и H — такая ее замкнутая подгруппа, что либо 1) индекс подгруппы H в группе G конечен, либо 2) H является нормальным делителем с абелевой факторгруппой подгруппы, G/H. Тогда, если компонента единицы подгруппы H разрешима, то компонента единицы группы G также разрешима.*

Доказательство. В случае (1) обе компоненты единицы совпадают.

Случай (2). Пусть K и K_1 — компоненты единицы групп G и H, а G', K' — коммутанты групп G и K соответственно. По условию, нормальный делитель H содержит коммутант G', а потому и коммутант K'. Но по теореме 4.8 коммутант K'

связен. Следовательно, $K' \subset K_1$. По предположению, группа K_1 разрешима. Поэтому ее подгруппа K', а следовательно, и группа K разрешимы.

Лемма 4.10. *Нормализатор замкнутой подгруппы C-группы замкнут.*

Доказательство. Пусть S — замкнутая подгруппа. Рассмотрим отображение $a \to asa^{-1}$, где $s \in S$. Прообраз подгруппы S при этом отображении замкнут и состоит из всех элементов a, для которых $asa^{-1} \in S$. Пересечение этих замкнутых множеств для всех элементов $s \in S$ состоит из всех элементов a, для которых $aSa^{-1} \subset S$ и является замкнутым множеством. Аналогично множество всех элементов a, для которых $a^{-1}Sa \subset S$ также является замкнутым множеством. Пересечение этих двух замкнутых множеств и представляет собой нормализатор подгруппы S.

18. Разрешимые связные матричные группы. Докажем теперь следующую теорему, играющую основную роль в теории Пикара — Вессио.

Теорема 4.11. *Если разрешимая мультипликативная группа G неособых матриц над алгебраически замкнутым полем связна в топологии Зариского, то все ее матрицы можно одновременно привести к треугольному виду.*

Замечания. 1. Теорема Ли в теории групп Ли утверждает то же самое; отличие состоит в том, что в теореме Ли матрицы рассматриваются над полем комплексных чисел, а связность понимается в смысле эвклидовой топологии. Но топология Зариского слабее эвклидовой, так что из эвклидовой связности вытекает связность в смысле топологии Зариского. Таким образом, теорема 4.11 сильнее теоремы Ли и является ее обобщением на любое алгебраически замкнутое поле.

2. Иногда под теоремой Ли подразумевают следующий ее инфинитезимальный аналог: матрицы разрешимой матричной алгебры Ли над алгебраически замкнутым полем могут быть одновременно приведены к треугольному виду. Эта теорема верна для полей характеристики нуль и ложна, если характеристика равна p. Вот яркий пример того, что группы иногда ведут себя лучше, чем алгебры Ли.

3. По известной теореме любое коммутативное множество матриц (не обязательно группа) над алгебраически замкнутым полем может быть одновременно приведено к треугольному виду; связность при этом несущественна. Этот факт мы используем в соответствующем месте доказательства теоремы 4.11.

4. Однако исключить из посылки теоремы 4.11 условие связности, вообще говоря, нельзя. Действительно, любая конечная разрешимая группа может быть точно представлена унитарными матрицами, а множество унитарных матриц одновременно приводится к треугольному виду только тогда, когда оно коммутативно.

5. Появление в теореме 4.11 условия связности является некоторым ее недостатком, поскольку эта теорема имеет, по существу, чисто алгебраический характер. Ввиду этого стоит отметить ее чисто алгебраическое следствие: любая разрешимая мультипликативная группа матриц обладает нормальным делителем конечного индекса, матрицы которого одновременно приводятся к треугольному виду. Если мы захотим избавиться от предположения алгебраической замкнутости основного поля, то останется справедливым следующее утверждение: разрешимая группа матриц над произвольным полем содержит нормальный делитель конечного индекса, коммутант которого нильпотентен.

Доказательство теоремы 4.11. Разделим доказательство на шесть этапов.

1) Пусть группа G приводима, т. е. соответствующее векторное пространство (обозначим его через V) имеет нетривиальное инвариантное подпространство W. Выбрав базис подпространства W, дополним его до базиса всего пространства V. В полученном базисе матрицы A_i группы G имеют следующий вид:

$$A_i = \begin{pmatrix} B_i & 0 \\ * & C_i \end{pmatrix}.$$

Отображение $A_i \to B_i$ является гомоморфизмом, в силу леммы 4.3 непрерывным. Поэтому матрицы B_i образуют связную разрешимую группу. Доказывая теорему индукцией по порядку матриц, мы можем предполагать, что матрицы B_i могут быть одновременно приведены к треугольному виду. Аналогичные соображения применимы к матрицам C_i. Следовательно, матрицы группы G одновременно приводятся к треугольному виду. Таким образом, группу G можно считать неприводимой.

2) Согласно теореме 4.8, коммутант G' группы G связен. Доказывая теорему индукцией по длине убывающего ряда коммутантов, будем считать, что матрицы коммутанта G' уже имеют треугольный вид.

3) Пусть W — подпространство пространства V, порожденное всеми общими для всех матриц группы G' собственными векторами. Это подпространство отлично от нуля, так как треугольный вид матриц группы G' обеспечивает существование по крайней мере одного общего собственного вектора. Кроме того, это подпространство инвариантно относительно группы G. Действительно, пусть α — общий собственный вектор: $\alpha T = c(T)\alpha$ для всех матриц $T \in G'$. Тогда, так как $STS^{-1} \in G'$ для любой матрицы $S \in G$, то $\alpha STS^{-1} = c(STS^{-1})\alpha$. Таким образом, вектор αST отличается от вектора αS лишь скалярным множителем, так что вектор αS является общим собственным вектором для всех матриц группы G'. Так как группа G по условию неприводима, то отсюда следует, что $W = V$. Другими словами, мы можем считать, что все матрицы группы G' диагональны.

4) Итак, пусть элемент группы G' является диагональной матрицей. Матрицы, сопряженные в G с матрицами группы G' принадлежат группе G' и потому также диагональны. Другими словами, все матрицы, сопряженные с данной, получаются перестановками ее диагональных элементов. Следовательно, каждый элемент группы G' имеет в группе G конечное число сопряженных. В силу леммы 4.7, отсюда вытекает, что подгруппа G' принадлежит центру группы G.

5) Предположим, что группа G' содержит нескалярную матрицу T. Пусть c — один из характеристических корней матрицы T. Рассмотрим множество W всех векторов α пространства V, для которых $\alpha T = c\alpha$. Так как матрица T перестановочна с группой G, то подпространство W инвариантно относительно группы G. Следовательно, $W = V$ и $T = cE$. Это противоречие доказывает, что все матрицы группы G' скалярны.

6) Так как группа G' является коммутантом группы G, то все ее матрицы унимодулярны и потому их диагональные элементы являются корнями n-й степени из единицы. Поскольку таких корней конечное число, то коммутант G'

конечен. Так как в силу теоремы 4.8 коммутант G' связен, то $G' = E$, т. е. группа G коммутативна. Но для коммутативной группы теорема известна. Тем самым теорема 4.11 полностью доказана.

19. Один специальный результат. В главе VI нам понадобится следующая теорема относительно разрешимых матричных групп.

Теорема 4.12. *Если группа G унимодулярных матриц второго порядка над алгебраически замкнутым полем является алгебраической группой, т. е. замкнута в топологии Зариского, а ее компонента единицы K разрешима, то имеет место хотя бы одно из следующих утверждений:*

1) *группа G конечна;*

2) *матрицы группы K могут быть одновременно приведены к диагональному виду и $[G:K] = 2$;*

3) *матрицы группы G могут быть одновременно приведены к треугольному виду.*

Доказательство. Рассмотрим сначала случай, когда матрицы группы K могут быть одновременно приведены к диагональному виду. В этом случае группа K состоит из матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Так как группа K замкнута в группе G, то она является алгебраической группой. Другими словами, группа K состоит из всех матриц указанного выше вида, для которых элемент a удовлетворяет некоторому полиномиальному уравнению. Поэтому либо группа K конечна (тогда и группа G конечна), либо группа K содержит все матрицы рассматриваемого вида. Как и в этапе (3) доказательства теоремы 4.11, легко показать, что общий собственный вектор матриц группы K переводится матрицами группы G снова в общий собственный вектор. Следовательно, каждый элемент группы G либо оставляет на месте, либо переставляет одномерные подпространства, определяемые базисными векторами. Следовательно, индекс подгруппы K в группе G равен либо единице, либо двум.

Рассмотрим теперь случай, когда матрицы группы K не приводятся одновременно к диагональному виду. Так как, согласно теореме 4.11, матрицы группы K могут быть одновременно приведены к треугольному виду, то в этом случае матрицы группы K имеют один и только один общий собственный вектор. Этот вектор необходимо инвариантен относительно группы G, т. е. матрицы группы G одновременно приводятся к треугольному виду.

Глава V

ТЕОРИЯ ГАЛУА

20. Три леммы. В этом вводном пункте излагаются три нужные для дальнейшего леммы.

Лемма 5.1. *Пусть K — произвольное дифференциальное поле с алгебраически замкнутым полем констант C, L — дифференциальное расширение поля K, и D — его поле констант. Пусть, далее, f_α и g — многочлены от конечного числа обычных неизвестных над полем K, где α пробегает некоторое (быть может, бесконечное) множество индексов. Тогда если уравнения $f_\alpha = 0$ и неравенство $g \neq 0$ имеют совместное решение в поле D, то они имеют совместное решение и в поле C.*

Доказательство. Пусть u_β — некоторый базис поля K, рассматриваемого как векторное пространство над полем C. Каждый многочлен f_α допускает единственное представление в виде $f_\alpha = \sum h_{\alpha\beta} u_\beta$, где $h_{\alpha\beta}$ — многочлены с коэффициентами из поля C. Так как независимость элементов u_β над полем констант сохраняется[1]) в поле L, то каждое решение уравнений $f_\alpha = 0$, принадлежащее полю D, обращает в нуль все многочлены $h_{\alpha\beta}$. С другой стороны, если уравнения $h_{\alpha\beta} = 0$ разрешимы в поле D, то по теореме Гильберта о корнях они имеют решение и в поле C.

Остается показать, что в поле C существует решение, не обращающее многочлен g в нуль. Пусть $\sum t_\gamma u_\gamma$ — разложение многочлена g по базису u_β. Если каждое решение[2]) уравнений $h_{\alpha\beta} = 0$ является в то же время корнем многочлена g (а потому и корнем каждого многочлена t_γ), то, согласно той же теореме о корнях, существуют такие целые числа r_γ, что $t_\gamma^{r_\gamma} \in I$, где I — идеал, порожденный многочле-

[1]) См. последний абзац пункта 10. — *Прим. перев.*
[2]) Принадлежащее полю C. — *Прим. ред.*

нами $h_{\alpha\beta}$. Но тогда каждое решение уравнений $f_\alpha = 0$, принадлежащее полю D, также обращает многочлен g в нуль, что противоречит условию.

Аналогичные рассуждения позволяют доказать следующую лемму.

Лемма 5.2. *Пусть K — произвольное дифференциальное поле с полем констант C. Если константы $k_1, \ldots, k_r$ некоторого дифференциального расширения поля K алгебраически зависимы над K, то они алгебраически зависимы и над C.*

Доказательство. Пусть имеет место полиномиальное соотношение $f(k_1, \ldots, k_r) = 0$ с коэффициентами из поля K. Рассматривая снова некоторый базис u_β поля K над полем C, положим $f = \sum h_\beta u_\beta$, где h_β — некоторые многочлены над полем C. Тогда $h_\beta(k_1, \ldots, k_r) = 0$, т. е. элементы $k_1, \ldots, k_r$ алгебраически зависимы над полем C.

Лемма 5.3. *Пусть F — произвольное поле, I — область целостности над F конечной степени трансцендентности (над F), и P — такой простой идеал области целостности I, что $P \neq 0$ и $P \neq I$. Тогда степень трансцендентности (над F) факторкольца $I/P = K$ строго меньше степени трансцендентности кольца I.*

Доказательство[1]). Пусть $\xi_1, \ldots, \xi_s$ — максимальная система алгебраически независимых (над полем F) элементов кольца K, и пусть $x_1, \ldots, x_s$ — произвольные прообразы элементов $\xi_1, \ldots, \xi_s$ в кольце I. Ясно, что элементы $x_1, \ldots, x_s$ алгебраически независимы и, более того, никакой отличный от нуля элемент кольца $F[x_1, \ldots, x_s]$ не принадлежит идеалу P.

Пусть y — любой отличный от нуля элемент идеала P. Для доказательства леммы достаточно показать, что система $x_1, \ldots, x_s, y$ алгебраически независима. Предположим, что эта система алгебраически зависима. Тогда элемент y является корнем некоторого многочлена, коэффициенты которого принадлежат кольцу $F[x_1, \ldots, x_s]$. Пусть f — многочлен наименьшей степени, обладающий этим свойством. Тогда его свободный член отличен от нуля. С другой стороны,

[1]) Это доказательство принадлежит переводчику. Доказательство, приведенное в английском тексте, недостаточно строго. — *Прим. перев.*

этот свободный член должен принадлежать идеалу P. Полученное противоречие доказывает, что система $x_1, \ldots, x_s, y$ алгебраически независима.

21. Нормальность расширений Пикара — Вессио. Пусть $M = K\langle u_1, u_2, \ldots, u_n\rangle$ — расширение Пикара — Вессио поля K и σ — допустимый дифференциальный изоморфизм поля M над полем K, т. е. дифференциальный изоморфизм поля M на некоторое подполе заданного объемлющего дифференциального поля N, оставляющий элементы поля K неподвижными. Каждый элемент $u_i\sigma$ является (вместе с u_i) решением дифференциального уравнения, определяющего данное расширение, и потому имеет вид $\sum k_{ij}u_j$, где k_{ij} — некоторые константы поля N. Таким образом, каждый изоморфизм σ порождает некоторую неособую матрицу, состоящую из констант. Докажем, что получающиеся таким образом матрицы определяются системой полиномиальных уравнений.

Лемма 5.4. *Для любого расширения Пикара — Вессио $M = K\langle u_1, \ldots, u_n\rangle$ произвольного дифференциального поля K существует такая система S многочленов (от n^2 обычных неизвестных) с коэффициентами из поля констант C, что*

1) *элементы матриц, соответствующих допустимым дифференциальным изоморфизмам поля M над полем K, обращают в нуль все многочлены системы S;*

2) *для любого дифференциального расширения N поля M и любой неособой матрицы (k_{ij}), состоящей из констант поля N, обращающих в нуль все многочлены системы S, существует допустимый дифференциальный изоморфизм поля M над полем K в поле N, переводящий элементы u_i в элементы $\sum k_{ij}u_j$.*

Доказательство. Пусть $y_1, \ldots, y_n$ — дифференциальные неизвестные над полем K. Определим дифференциальный гомоморфизм кольца $K\{y_1, \ldots, y_n\}$ в поле M, оставив все элементы поля K неподвижными и отобразив y_i в u_i. Ядро Γ этого гомоморфизма является, очевидно, простым дифференциальным идеалом кольца $K\{y_1, \ldots, y_n\}$.

Пусть c_{ij} $(i, j = 1, \ldots, n)$ — система n^2 обычных неизвестных над полем M. Соответствие $y_i \to \sum c_{ij}u_j$ определяет тогда некоторый дифференциальный гомоморфизм кольца $K\{y_1, \ldots, y_n\}$ в кольцо $M[c_{ij}]$. Пусть Δ — образ идеала Γ при этом гомоморфизме. Этот образ является идеалом кольца (обыкновенных) многочленов с коэффициентами из поля M. Пусть w_α — базис поля M как векторного пространства над полем C. Запишем каждый многочлен идеала Δ в виде линейной комбинации элементов w_α с коэффициентами, являющимися многочленами над полем C. Множество S всех этих многочленов удовлетворяет, как мы докажем, всем требованиям нашей леммы.

1) Предположим, что допустимый дифференциальный изоморфизм σ поля M над полем K переводит элемент u_i в линейную комбинацию $\sum k_{ij}u_j$. Рассмотрим композицию естественного гомоморфного отображения кольца $K\{y_1, \ldots, y_n\}$ в кольцо $K\{u_1, \ldots, u_n\}$ и автоморфизма σ. Эта композиция отображает идеал Γ в нуль. С другой стороны, рассмотрим композицию гомоморфизмов, определенных соответствиями $y_i \to \sum c_{ij}u_j$ и $c_{ij} \to k_{ij}$. При этом отображении идеал Γ переходит в множество значений, которые принимают многочлены идеала Δ при $c_{ij} = k_{ij}$. Однако оба составных отображения, очевидно, совпадают, следовательно, все многочлены идеала Δ обращаются в нуль при $c_{ij} = k_{ij}$. Выразив каждый многочлен этого идеала через базис w_α, мы немедленно получим, что все многочлены системы S обращаются в нуль при $c_{ij} = k_{ij}$.

2) Пусть теперь заданы поле N и неособая матрица (k_{ij}), состоящая из констант поля N, обращающих в нуль все многочлены системы S. Рассмотрим гомоморфное отображение кольца $K\{y_1, \ldots, y_n\}$ в поле N, определенное соответствиями $y_i \to \sum c_{ij}u_j$ и $c_{ij} \to k_{ij}$. Ядро этого отображения содержит идеал Γ и поэтому определяет некоторое гомоморфное отображение σ кольца $K\{u_1, \ldots, u_n\}$ на кольцо $K\{u_1\sigma, \ldots, u_n\sigma\}$, где $u_i\sigma = \sum k_{ij}u_j$. Если бы мы знали, что отображение σ взаимно однозначно, то мы могли бы его продолжить на поля отношений, и доказательство было бы закончено. С помощью леммы 5.3 мы теперь и докажем, что отображение σ взаимно однозначно. Действительно, предположив противное, мы получим, что

$$\partial K\langle u_1, \ldots, u_n\rangle/K > \partial K\langle u_1\sigma, \ldots, u_n\sigma\rangle/K; \qquad (*)$$

знак ∂ мы используем для обозначения степени трансцендентности; все рассматриваемые степени трансцендентности конечны, так как элементы u_i удовлетворяют соответствующим дифференциальным уравнениям. Для краткости мы будем писать $K\langle u\rangle$ вместо $K\langle u_1, \ldots, u_n\rangle$ и т. п. Из неравенства (*) ввиду аддитивности степени трансцендентности вытекает, что

$$\partial K\langle u, u\sigma\rangle/K\langle u\rangle < \partial K\langle u, u\sigma\rangle/K\langle u\sigma\rangle. \qquad (**)$$

Но

$$\partial K\langle u, u\sigma\rangle/K\langle u\rangle = \partial K\langle u, k\rangle/K\langle u\rangle = \partial C(k)/C;$$

последнее — в силу леммы 5.2. Аналогично

$$\partial K\langle u, u\sigma\rangle/K\langle u\sigma\rangle = \partial C'(k)/C',$$

где C' — поле констант поля $K\langle u\sigma\rangle$. С другой стороны, как легко видеть, $\partial C'(k)/C' \leqslant \partial C(k)/C$, что противоречит неравенству (**). Тем самым лемма 5.4 полностью доказана.

Основные теоремы теории Галуа теперь уже легко выводятся из полученных нами результатов. Первая из этих теорем представляет собой непосредственное следствие леммы 5.4.

Теорема 5.5. *Дифференциальная группа Галуа расширения Пикара — Вессио является алгебраической матричной группой над полем констант.*

Лемма 5.6. *Пусть K — произвольное дифференциальное поле с алгебраически замкнутым полем констант и M — некоторое его расширение Пикара — Вессио. Если для некоторого элемента $z \in M$ и двух семейств x_α и y_α элементов поля M, где α пробегает некоторое (быть может, бесконечное) множество индексов, существует допустимый дифференциальный изоморфизм поля M над полем K, при котором образ элемента z отличен от z, а каждый элемент x_α переходит в соответствующий элемент y_α, то существует дифференциальный автоморфизм поля M над полем K, обладающий теми же свойствами.*

Доказательство. Обозначая данный дифференцильный изоморфизм через σ, положим

$$u_i\sigma = \sum k_{ij}u_j,$$

где k_{ij} — константы некоторого объемлющего поля. Пусть x

и y — произвольные элементы поля M. Каждый из этих элементов является отношением двух дифференциальных многочленов от u; пусть, например, $x=P(u)/Q(u)$, $y=R(u)/S(u)$. Соотношение $y=x\sigma$ равносильно равенству

$$S(u)P(u\sigma)=R(u)Q(u\sigma).$$

Подставив сюда $u_i\sigma=\sum k_{ij}u_j$, мы получим полиномиальное соотношение для элементов k_{ij} с коэффициентами из поля M. Каждое соотношение $x_\alpha\sigma=y_\alpha$ приводит таким образом к некоторому уравнению для элементов k_{ij}. Присоединим все эти уравнения к уравнениям, указанным в лемме 5.4. Кроме того, объединим неравенство, получающееся из условия $z\sigma\neq z$, с неравенством $|k_{ij}|\neq 0$ в одно неравенство. В поле констант объемлющего поля система, состоящая из полученных уравнений и неравенства, имеет решение; в силу леммы 5.1, эта система имеет решение и в поле C, которое и определяет требуемый автоморфизм.

Теорема 5.7. *Каждое расширение Пикара — Вессио дифференциального поля K характеристики нуль с алгебраически замкнутым полем констант является его нормальным расширением.*

Доказательство. Мы должны доказать, что для любого элемента z поля M, не принадлежащего полю K, существует дифференциальный автоморфизм поля M над полем K, для которого элемент z не является неподвижным элементом. Но, в силу теорем 2.6 и 2.5, существует обладающий этим свойством допустимый дифференциальный изоморфизм поля M над полем K. Таким образом, для доказательства теоремы 5.7 достаточно применить лемму 5.6.

Теорема 5.8. *Пусть K — произвольное дифференциальное поле характеристики нуль с алгебраически замкнутым полем констант и M — некоторое его расширение Пикара — Вессио. Тогда каждый дифференциальный изоморфизм (над полем K) произвольной пары промежуточных дифференциальных полей может быть продолжен до дифференциального автоморфизма поля M. В частности, каждый дифференциальный автоморфизм над K любого промежуточного дифференциального поля может быть продолжен до дифференциального автоморфизма поля M.*

Доказательство. Сначала с помощью теоремы 2.5 продолжаем данный дифференциальный изоморфизм до допустимого дифференциального изоморфизма, определенного на всем поле M, а затем применяем лемму 5.6.

22. Завершение теории Галуа. Подведем некоторые итоги. Пусть M — расширение Пикара — Вессио поля K (характеристики нуль с алгебраически замкнутым полем констант). Поле M является также расширением Пикара — Вессио любого промежуточного дифференциального поля L. Согласно теореме 5.7, расширение M нормально над L. На языке теории Галуа, введенном в главе III, это означает, что все промежуточные дифференциальные поля замкнуты.

С другой стороны, пусть H — произвольный нормальный делитель дифференциальной группы Галуа G, и пусть $L=H'$ — соответствующее дифференциальное подполе. Предположим, что нормальный делитель H замкнут в смысле теории Галуа. По теореме 5.8 все дифференциальные автоморфизмы поля L над полем K могут быть продолжены на все поле M. Из теоремы 3.4 вытекает поэтому, что факторгруппа G/H является полной дифференциальной группой Галуа поля L над полем K. Кроме того (см. леммы 3.6 и 4.10), если поле L замкнуто и нормально над полем K, то соответствующая подгруппа является нормальным делителем.

В силу теоремы 5.6, группа G является алгебраической матричной группой, так же как и все ее подгруппы, соответствующие промежуточным дифференциальным полям. Таким образом, для завершения теории остается только установить, что все алгебраические подгруппы группы G замкнуты в смысле теории Галуа.

Для этого в свою очередь достаточно показать, что любая подгруппа H группы G плотна в группе H'' в смысле топологии Зариского. Если это не так, то существует многочлен f (от n^2 переменных с коэффициентами из поля C), обращающийся в нуль всюду на группе H и отличный от нуля на группе H''. Для упрощения обозначений мы ограничимся случаем $n=2$, хотя все дальнейшие рассуждения полностью применимы и для любого n. Таким образом, мы будем считать, что $M=K\langle u, v\rangle$. Так как матрица

$$\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$$

не вырождена, то для нее существует обратная к ней матрица

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Пусть y и z — дифференциальные неизвестные над полем M. Определим дифференциальный многочлен F формулой

$$F(y, z) = f(Ay + By', \ Az + Bz', \ Cy + Dy', \ Cz + Dz').$$

Сделаем в многочлене F подстановку $y = u\sigma$, $z = v\sigma$, где σ — произвольный элемент группы H. Так как

$$\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} u & v \\ u' & v' \end{pmatrix} \begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix},$$

где (k_{ij}) — матрица, соответствующая автоморфизму σ, то

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}.$$

Следовательно, $F(u\sigma, v\sigma) = 0$ для всех элементов σ группы H, но не для всех элементов σ группы H''. Среди всех дифференциальных многочленов из кольца $M\{y, z\}$, обладающих этим свойством, выберем один с наименьшим числом членов (в записи многочлена как суммы одночленов). Обозначим этот многочлен через E. Можно считать, что один из коэффициентов многочлена E равен единице. Для любого элемента τ группы H обозначим через E_τ многочлен, получающийся из многочлена E заменой всех его коэффициентов их образами при автоморфизме τ. Тогда многочлен

$$E_\tau(u\sigma, v\sigma) = [E(u\sigma\tau^{-1}, v\sigma\tau^{-1})]\tau$$

равен нулю для всех элементов σ группы H. Многочлен $E - E_\tau$ имеет меньше членов, чем многочлен E, и потому обращается в нуль на всех элементах вида $u\sigma$, $v\sigma$, где $\sigma \in H''$. Если многочлен $E - E_\tau$ не равен тождественно нулю, то в поле M существует такой элемент γ, что многочлен $E - \gamma[E - E_\tau]$ имеет меньше членов, чем многочлен E. Но многочлен $E - \gamma[E - E_\tau]$, как и многочлен E обращается в нуль на элементах вида $u\sigma$, $v\sigma$ при всех $\sigma \in H$, но не при всех $\sigma \in H''$, что противоречит выбору многочлена E. Таким образом, $E - E_\tau \equiv 0$, т. е. все коэффициенты многочлена E

лежат в дифференциальном поле H', соответствующем подгруппе H. Другими словами, эти коэффициенты инвариантны относительно группы H'', и поэтому $E(u\sigma, v\sigma) = 0$ для всех элементов σ группы H''. Мы пришли к противоречию.

Резюмируем наши результаты в следующей теореме.

Теорема 5.9. *Пусть M — произвольное расширение Пикара — Вессио дифференциального поля K характеристики нуль с алгебраически замкнутым полем констант. Теория Галуа устанавлизает взаимно однозначное соответствие между промежуточными дифференциальными полями и алгебраическими подгруппами дифференциальной группы Галуа G. Замкнутая подгруппа H группы G тогда и только тогда является нормальным делителем, когда соответствующее поле L нормально над K; в этом случае факторгруппа G/H является полной дифференциальной группой Галуа поля L над полем K.*

23. Расширения Лиувилля. Как и в обычной теории Галуа, важно изучить влияние расширения основного поля на дифференциальную группу Галуа.

Лемма 5.10. *Пусть M — расширение Пикара — Вессио поля K (характеристики нуль с алгебраически замкнутым полем констант). Тогда любое его расширение $N = M\langle z\rangle$, не содержащее новых констант, является расширением Пикара — Вессио поля $L = K\langle z\rangle$. Дифференциальная группа Галуа этого расширения изоморфна некоторой алгебраической подгруппе дифференциальной группы Галуа поля M над полем K, а именно подгруппе, состоящей из автоморфизмов, тождественных на поле $M \cap L$.*

Доказательство. Непосредственно ясно, что поле N является расширением Пикара — Вессио поля L. Действительно, оба поля имеют одно и то же поле констант и поле N порождается над полем L теми же решениями (исходного дифференциального уравнения), которые порождают поле M над полем K. Каждый дифференциальный автоморфизм поля N над полем K автоматически отображает поле M само на себя (см. лемму 3.8). Благодаря этому возникает некоторое гомоморфное отображение дифференциальной группы Галуа поля N над полем L на некоторую подгруппу (например, G_1) дифференциальной группы Галуа поля M

над полем K. Каждый автоморфизм из ядра этого гомоморфизма оставляет неподвижными все элементы как поля M, так и поля L, а потому и все элементы поля N. Следовательно, рассматриваемый гомоморфизм является изоморфизмом, а его образ G_1 — алгебраической группой матриц (теорема 5.5). Поле, соответствующее этой подгруппе, очевидно, совпадает с пересечением $M \cap L$. Остается заметить, что по теореме 5.9 группа G_1 содержит все дифференциальные автоморфизмы поля M, тождественные на поле $M \cap L$.

Получим теперь два основных результата относительно разрешимости дифференциальных уравнений в квадратурах.

Теорема 5.11. *Пусть M — расширение Пикара — Вессио поля K (характеристики нуль с алгебраически замкнутым полем констант). Если компонента единицы дифференциальной группы Галуа этого расширения разрешима, то оно является расширением Лиувилля некоторого конечного нормального расширения поля K.*

Доказательство. Пусть G — дифференциальная группа Галуа данного расширения, C — компонента единицы группы G и L — промежуточное дифференциальное поле, соответствующее подгруппе C. Тогда L является конечным нормальным расширением поля K[1]), а C — дифференциальной группой Галуа расширения M над полем L. Тот факт, что поле M является расширением Лиувилля поля L, теперь непосредственно вытекает из теорем 4.11 и 3.12.

Дифференциальное поле N мы будем называть *обобщенным расширением Лиувилля* поля K, если его можно получить из поля K конечным числом шагов, каждый из которых является либо конечным алгебраическим расширением, либо присоединением интеграла или экспоненты интеграла.

Теорема 5.12. *Пусть M — произвольное расширение Пикара — Вессио поля K (характеристики нуль с алгебраически замкнутым полем констант). Если поле M можно вложить в не содержащее новых констант дифференциальное поле N, являющееся обобщенным расширением Лиувилля поля K, то компонента единицы дифференциальной группы Галуа G расширения M над полем K разрешима (откуда, согласно теореме 5.11, следует, что поле M является расширением Лиувилля некоторого конечного расширения поля K).*

[1]) В силу леммы 4.5, 3.2 и теоремы 5.9. — *Прим. перев.*

Доказательство. Проведем индукцию по числу шагов, ведущих от K к N. Пусть $K\langle z\rangle$ будет первым шагом. Тогда, по индуктивному предположению, компонента единицы дифференциальной группы Галуа поля $M\langle z\rangle$ над полем $K\langle z\rangle$ разрешима. В силу леммы 5.10, эта группа изоморфна некоторой подгруппе H группы G, соответствующей полю $M \cap K\langle z\rangle$. Если элемент z алгебраичен над полем K, то подгруппа H имеет в группе G конечный индекс (см. лемму 3.1). С другой стороны, если z является интегралом или экспонентой интеграла, то, в силу лемм 3.9 и и 3.10, поле $K\langle z\rangle$ является расширением Пикара — Вессио поля K с абелевой группой Галуа, и поэтому все дифференциальные поля между полями K и $K\langle z\rangle$ нормальны над полем K. В частности, поле $M \cap K\langle z\rangle$ нормально над полем K, и его дифференциальная группа Галуа абелева. Следовательно, подгруппа H является нормальным делителем группы G, и факторгруппа G/H абелева. В обоих случаях из леммы 4.9 вытекает, что компонента единицы группы G разрешима.

В заключение этой главы мы изложим (с соответствующими ссылками на статьи Колчина) некоторые более тонкие результаты Галуа.

1. Группа Галуа позволяет узнать, когда линейное однородное дифференциальное уравнение может быть решено с помощью одних только интегралов или одних только экспонент интегралов. Если мы отвлечемся от осложнений, обусловленных тем, что группа Галуа может быть несвязной, то имеют место следующие факты: разрешимость при помощи одних только интегралов соответствует тому, что все матрицы группы Галуа приводятся одновременно к специальному треугольному виду (единицы из диагонали и нули под ней); разрешимость при помощи одних только экспонент интегралов соответствует тому, что все матрицы группы Галуа приводятся одновременно к диагональному виду (см. [2]).

2. Приводимость группы Галуа (или, вернее, векторного пространства, в котором она действует) равносильна своего рода разложимости дифференциального уравнения (см. [2], § 22).

3. Если группа Галуа уравнения неразрешима, то уравнение не может быть решено в квадратурах, даже если допустить введение новых констант [3].

4. Изложенная теория может быть распространена на дифференциальные поля с несколькими перестановочными между собой дифференцированиями [5].

5. К теореме 5.9 можно добавить последний мазок: всякое нормальное промежуточное поле также является расширением Пикара — Вессио основного поля (см. [7], стр. 891).

6. По существу, вся теория может быть перенесена на некоторый класс более общих расширений, которые Колчин назвал *сильно нормальными* (см. [6], [7]). Это обобщение точно соответствует замене алгебраических матричных групп групповыми алгебраическими многообразиями.

Глава VI

УРАВНЕНИЯ ВТОРОГО ПОРЯДКА

24. Вронскиан. Пусть $M = K\langle u_1, \ldots, u_n\rangle$ — расширение Пикара — Вессио и W — вронскиан элементов $u_1, \ldots, u_n$.

Лемма 6.1. *Для любого дифференциального автоморфизма σ поля M над полем K имеет место соотношение $W\sigma = |c_{ij}|W$, где (c_{ij}) — матрица, соответствующая автоморфизму σ.*

Доказательство. Так как $u_i\sigma = \sum c_{ij}u_j$, то матрица Вронского для элементов u после умножения на матрицу (c_{ij}) переходит в матрицу Вронского для элементов $u\sigma$. Переходя к определителям, получаем требуемое соотношение.

Лемма 6.2. *Поле $K\langle W\rangle$ соответствует унимодулярной подгруппе дифференциальной группы Галуа.*

Доказательство. В силу леммы 6.1, автоморфизм σ тогда и только тогда не меняет вронскиана W, когда $|c_{ij}| = 1$.

Лемма 6.3. *Если дифференциальное уравнение, соответствующее рассматриваемому расширению, имеет вид*

$$y^{(n)} + ay^{(n-1)} + \ldots = 0,$$

то $W' = -aW$.

Доказательство. Операция дифференцирования определителя W по строкам сводится к дифференцированию его последней строки. Заменив получающиеся в этой строке элементы $u_1^{(n)}, \ldots, u_n^{(n)}$ их выражениями через низшие производные (в силу данного дифференциального уравнения), мы придем к равенству $W' = -aW$.

Следствие. *Если $a = 0$, то W является константой, и поэтому дифференциальная группа Галуа состоит из унимодулярных матриц.*

В связи с последним результатом напомним классический способ уничтожения члена $ay^{(n-1)}$ путем введения экспоненты некоторого интеграла. Пусть w — решение уравнения $nw'+aw=0$. Полагая $y=wz$, мы получим уравнение относительно z, не содержащее члена с $z^{(n-1)}$.

Таким образом, при изучении вопроса о разрешимости дифференциальных уравнений в квадратурах мы можем без ограничения общности предполагать, что коэффициент при $y^{(n-1)}$ равен нулю. В частности, при изучении уравнений второго порядка мы можем ограничиться уравнениями вида $y''+ay=0$.

25. Связь с уравнениями Риккати.

Теорема 6.4. *Пусть K — произвольное дифференциальное поле характеристики нуль с алгебраически замкнутым полем констант и M — расширение Пикара — Вессио поля K, соответствующее уравнению $y''+ay=0$, где $a\in K$. Если M представляет собой обобщенное расширение Лиувилля поля K, но не является его конечным расширением, то уравнение $t'=t^2+a$ имеет решение в некотором квадратичном расширении поля K.*

Доказательство. Согласно следствию из леммы 6.3, дифференциальная группа Галуа G поля M над полем K является алгебраической группой унимодулярных матриц второго порядка. По теореме 5.12 компонента единицы группы G разрешима, так что к группе G применима теорема 4.12. Случай, когда группа G конечна, по условию исключен. В каждом из остальных двух случаев мы можем утверждать, что существует такое квадратичное расширение L поля K, что все матрицы дифференциальной группы Галуа поля M над полем L одновременно приводятся к треугольному виду, т. е. существует отличное от нуля решение u уравнения $y''+ay=0$, которое под действием каждого дифференциального автоморфизма поля M над полем L приобретает постоянный множитель. Следовательно, $u'/u\in L$. Положим $t=-u'/u$. Тогда $u'=-ut$, $u''=-u't-ut'=u(t^2-t')$; в то же время $u''=-au$. Таким образом, $t'=t^2+a$.

Продолжим наши вычисления еще на один шаг вперед.

Лемма 6.5. *Пусть K — произвольное дифференциальное поле и t — некоторый элемент его расширения, удовлетворяющий соотношению $t'=t^2+a$, где $a\in K$. Пусть, далее, неприводимое над полем K уравнение, корнем которого является элемент t, имеет вид $t^2+rt+s=0$. Тогда*

$$r''+3rr'+r^3+4ar+2a'=0.$$

Доказательство. Дифференцируя равенство $t^2+rt+s=0$ и учитывая, что $t'=t^2+a$, мы получим соотношение

$$2t^3+rt^2+(2a+r')t+ar+s'=0.$$

Вычитая из этого соотношения равенство $t^2+rt+s=0$, умноженное на $2t$, мы получим

$$rt^2+(2s-2a-r')t-ar-s'=0.$$

Отсюда вытекает, что $2s-2a-r'=r^2$ и $-ar-s'=rs$. Следовательно, $2s'=2a'+r''+2rr'$. Подставляя в равенство $2rs+2s'+2ar=0$ выражения для $2s$ и $2s'$, мы получим требуемый результат.

26. Пример. Разберем уравнение $y''+xy=0$, рассматривая его в классическом стиле, т. е. принимая поле рациональных функций переменной x с комплексными коэффициентами за основное поле. Решения этого уравнения являются целыми функциями, и соответствующее расширение Пикара — Вессио M представляет собой вполне определенное подполе поля функций, мероморфных на всей плоскости. Степень $[M:K]$ обязательно бесконечна, так как в противном случае решения были бы алгебраическими функциями, а целая алгебраическая функция является многочленом и, следовательно, не может быть решением уравнения

$$y''+xy=0.$$

Исследуем возможность того, что уравнение $t'=t^2+x$ обладает решениями в поле K. Пусть $t=f/g$, где f и g — взаимно простые многочлены. Тогда

$$gf'-fg'-f^2=g^2x.$$

Если степень многочлена f больше степени многочлена g, то f^2 является единственным старшим членом этого уравнения и не может сократиться с другими членами. Если степень многочлена f не превосходит степени многочлена g, то единственным старшим членом является многочлен g^2x. Таким образом, уравнение $t' = t^2 + x$ в поле K решений не имеет.

Предположим теперь, что уравнение $t' = t^2 + x$ имеет решение в некотором квадратичном расширении поля K. Согласно утверждению, доказанному выше, это решение не принадлежит полю K. В этом случае применима лемма 6.5. Пусть $\sum_{i=1}^{n} c_i (x-a)^{-i}$ — часть разложения функции r на элементарные дроби, соответствующая линейному множителю $x-a$. Для того чтобы имело место равенство

$$r'' + 3rr' + r^3 + 4xr + 2 = 0,$$

два максимальных среди чисел $n+2$, $2n+1$ и $3n$ должны совпадать, что выполняется только при $n=1$. Таким образом, знаменатель рациональной функции r не может иметь кратных линейных множителей. Члену $c/(x-a)$ в функциях r'', $3rr'$ и r^3 соответствуют слагаемые $2c/(x-a)^3$, $-3c^2/(x-a)^3$ и $c^3/(x-a)^3$. Следовательно, $2c - 3c^2 + c^3 = 0$, т. е. $c=1$ или $c=2$.

Установив это, рассмотрим вновь представление $r = f/g$. После приведения рассматриваемого соотношения к общему знаменателю g^4 мы получим в числителе следующие члены:

$$g^3f'',\ fg^2g'',\ g^2f'g',\ fg(g')^2,\ ff'g^2,\ f^2gg',\ f^3g,\ xfg^3,\ g^4.$$

Если многочлены f и g имеют одинаковую степень, то член xfg^3 не может сократиться. Если степень многочлена f больше степени многочлена g, то не может сократиться член f^3g. Однако если степень многочлена g больше степени многочлена f, то старшие члены xfg^3 и g^4 могут взаимно уничтожиться; при этом степень многочлена f должна быть меньше степени многочлена g ровно на единицу.

Возвращаясь к разложению на элементарные дроби, мы видим таким образом, что функция r не имеет полиномиальной части, т. е. имеет вид $\sum \frac{c_i}{(x-a_i)}$, где $c_i = 1$ или $c_i = 2$. Следовательно, если $g(x) = x^k + \ldots$, то $f(x) = \alpha x^{k-1} + \ldots$, где α — некоторое положительное целое число. Но тогда члены xfg^3 и g^4, возникающие за счет членов $4xr$ и 2, не могут взаимно уничтожиться, ибо $4\alpha + 2 \neq 0$.

Резюмируя, мы получаем следующую теорему:

Теорема 6.6. *Уравнение $y'' + xy = 0$ не имеет решений ни в каком из полей, которые можно получить из поля рациональных функций переменной x последовательностью конечных алгебраических расширений, присоединений интегралов и присоединений экспонент интегралов.*

Дополнительными рассуждениями можно показать, что группа Гуала этого уравнения совпадает с полной унимодулярной группой матриц второго порядка. Это следует, например, из того факта, что в каждой ее собственной алгебраической подгруппе компонента единицы связна.

Глава VII

ТЕОРЕМА О БАЗИСАХ И ПРИЛОЖЕНИЯ

27. Теорема о базисах. Теорема Гильберта о базисах утверждает, что если в коммутативном кольце R с единицей выполняется условие обрыва возрастающих цепей идеалов, то это условие выполняется также и в кольце $R[x]$, получающемся в результате присоединения одного неизвестного.

Если пытаться отыскать аналогичную теорему для дифференциальных колец, то первым побуждением, вероятно, было бы подчинить кольцо R условию обрыва возрастающих цепей и постараться доказать, что это условие выполняется и в кольце $R\{x\}$, полученном в результате присоединения одного дифференциального неизвестного. Однако в такой формулировке предполагаемая теорема не верна даже тогда, когда кольцо R является полем. Действительно, дифференциальные идеалы, порожденные соответственно элементами x^2; x^2 и $(x')^2$; x^2, $(x')^2$ и $(x'')^2$; и т. д., образуют необрывающуюся возрастающую цепь.

Истинным аналогом теоремы Гильберта, играющим ту же роль в приложениях, является следующая

Теорема 7.1. (Теорема Ритта — Роденбаша о базисах.) *Если алгебра Ритта R удовлетворяет условию обрыва возрастающих цепей для радикальных дифференциальных идеалов, то результат $R\{x\}$ присоединения к этой алгебре одного дифференциального неизвестного также удовлетворяет этому условию.*

Замечание. Имеется два источника трудностей, возникающих при доказательстве теоремы. Во-первых, имеются „дифференциальные“ трудности, которые заставили нас, в частности, предположить, что R является алгеброй Ритта, а не просто дифференциальным кольцом. Во-вторых, основные трудности возникают из того факта, что и в посылке и в заключении теоремы появляются радикальные идеалы.

Читателю было бы полезно проанализировать второй источник трудностей, извлекая из приводимого ниже доказательства доказательство следующей теоремы: если в коммутативном кольце R с единицей выполнено условие обрыва возрастающих цепей для радикальных идеалов, то тому же условию удовлетворяет и кольцо $R[x]$.

Доказательство теоремы 7.1 требует некоторых подготовительных замечаний и лемм. В первую очередь нам понадобится следующее.

Определение. Радикальный дифференциальный идеал I дифференциального кольца называется идеалом *конечного типа*, если существует такая конечная система элементов $a_1, \ldots, a_n$ идеала I, что $I = \{a_1, \ldots, a_n\}$, т. е. такая, что I является минимальным радикальным дифференциальным идеалом, содержащим элементы $a_1, \ldots, a_n$.

Лемма 7.2. *Если для подмножества S алгебры Ритта A существует такой элемент $a \in A$, что $\{a, S\}$ является идеалом конечного типа, то в S найдутся такие элементы $b_1, \ldots, b_r$, что*

$$\{a, S\} = \{a, b_1, \ldots, b_r\}.$$

Доказательство. Пусть J — радикал дифференциального идеала I, порожденного множеством S и элементом a. Согласно лемме 1.8, идеал J радикален и потому совпадает с идеалом $\{a, S\}$. Пусть $\{a, S\} = \{c_1, \ldots, c_q\}$. Некоторая степень каждого элемента c_i выражается в виде линейной комбинации (с коэффициентами из алгебры A) элемента a, элементов множества S и их производных. Очевидно, что в качестве элементов $b_1, \ldots, b_r$ можно взять элементы подмножества S, которые при этом появляются.

Элементы кольца $R\{x\}$ мы будем называть *дифференциальными многочленами* относительно неизвестного x. Для любого такого дифференциального многочлена A существует наивысшая производная $x^{(r)}$, действительно содержащаяся в A. Ее порядок r мы назовем *порядком* дифференциального многочлена A. *Степенью* многочлена A назовем его степень относительно производной $x^{(r)}$. Мы будем говорить, что дифференциальный многочлен A_1 *ниже* дифференциального многочлена A, если его порядок меньше порядка многочлена A, а в случае совпадения порядков, если его степень меньше степени многочлена A.

Дифференциальный многочлен A порядка r и степени d можно записать в виде

$$A = B[x^{(r)}]^d + C,$$

где многочлен B не содержит производной $x^{(r)}$, а степень многочлена C относительно производной $x^{(r)}$ меньше степени многочлена A. Многочлен B мы будем называть *старшим коэффициентом* дифференциального многочлена A.

Частную производную $S = \partial A/\partial x^{(r)}$ назовем *сепарантой* многочлена A. (При отыскании этой частной производной мы считаем константами как элементы кольца R, так и низшие производные от x, включая и сам элемент x, если $r > 0$.)

Заметим, что и сепаранта и старший коэффициент многочлена A ниже, чем A.

Лемма 7.3. *Пусть A — дифференциальный многочлен относительно неизвестного x над алгеброй Ритта R, со старшим коэффициентом B и сепарантой S, и I — порожденный им дифференциальный идеал алгебры $R\{x\}$. Тогда для любого дифференциального многочлена F относительно неизвестного x существуют такие целые числа m и n и такой дифференциальный многочлен G, который ниже многочлена A, что*

$$B^m S^n F \equiv G \quad (\mathrm{mod}\, I).$$

Доказательство. Продифференцировав многочлен A, мы получим, что $A' = Sx^{(r+1)} + T_1$, где порядок многочлена T_1 строго меньше $r+1$; после k последовательных дифференцирований соответственно получим, что

$$A^{(k)} = Sx^{(r+k)} + T_k,$$

где порядок многочлена T_k строго меньше $r+k$.

Отсюда вытекает, что если порядок многочлена F больше r (скажем равен $r+k$), то соответствующая степень сепаранты S, умноженная на F, обладает тем свойством, что после вычитания из этого произведения некоторого выражения, кратного $A^{(k)}$, мы получим разность, порядок которой меньше $r+k$ [1]). Повторяя этот процесс, мы можем понизить порядок

[1]) Если многочлен F имеет степень e, т. е. $F = C(x^{(r+k)})^e + \ldots$, то многочлен $S^e F - C(A^{(k)})^e$ имеет степень меньше e. Повторяя этот процесс снижения степени, мы в результате действительно получим многочлен порядка меньше $r+k$. — *Прим. перев.*

до r. Далее, если степень многочлена F [1]) не меньше d (где d — степень многочлена A), то, применяя к данному дифференциальному многочлену A и к произведению многочлена F на соответствующую степень старшего коэффициента B известный алгоритм деления с остатком, мы можем понизить степень A до числа меньшего d.

Доказательство теоремы 7.1. Вместо теоремы 7.1 мы докажем равносильное утверждение о том, что каждый радикальный дифференциальный идеал кольца $R\{x\}$ имеет конечный тип. Если это не так, то, используя лемму Цорна, мы можем среди радикальных дифференциальных идеалов, не имеющих конечного типа, выбрать максимальный идеал I. Покажем, что этот максимальный идеал является простым идеалом. Пусть $ab \in I$, где $a \notin I$ и $b \notin I$. Тогда бо́льшие радикальные дифференциальные идеалы $\{I, a\}$ и $\{I, b\}$ содержат идеал I, но не совпадают с ним. Поэтому эти идеалы конечного типа. По лемме 7.2

$$\{I, a\} = \{a, c_1, \ldots, c_r\},$$
$$\{I, b\} = \{b, d_1, \ldots, d_s\},$$

где все элементы c_i и d_j принадлежат идеалу I. В силу леммы 1.6,

$$\{I, a\}\{I, b\} \subset \{ab, \ldots, c_r d_s\} \subset I.$$

Для любого элемента z идеала I элемент z^2 принадлежит идеалу $\{I, a\}\{I, b\}$, т. е. идеалу $\{ab, \ldots, c_r d_s\}$. Следовательно, элемент z тоже принадлежит идеалу $\{ab, \ldots, c_r d_s\}$, так что идеал I совпадает с идеалом $\{ab, \ldots, c_r d_s\}$. Таким образом, идеал I имеет конечный тип, что невозможно. Полученное противоречие доказывает, что идеал I является простым идеалом.

Пересечение $I \cap R$ является радикальным дифференциальным идеалом кольца R и имеет по условию конечный тип. Пусть J — радикальный дифференциальный идеал кольца $R\{x\}$, порожденный идеалом $I \cap R$. Так как этот идеал также имеет конечный тип, то он не может совпадать с идеалом I. Таким образом, идеал J является собственным подмножеством идеала I. Выберем в идеале I дифференциальный многочлен A,

[1]) Имеется в виду не исходный многочлен F, а многочлен порядка r, полученный описанным выше способом. — *Прим. ред.*

не принадлежащий идеалу J, так, чтобы у него был возможно меньший порядок и среди дифференциальных многочленов этого порядка он имел наименьшую степень. Пусть B — старший коэффициент многочлена A:

$$A = B[x^{(r)}]^d + C.$$

Он не может принадлежать идеалу I. Действительно, если $B \in I$, то $B \in J$, так как многочлен B ниже многочлена A, и поэтому $C \in I$. Следовательно, так как многочлен C также ниже многочлена A, то $C \in J$, что невозможно. Пусть S — сепаранта дифференциального многочлена A. Она не может принадлежать идеалу I. Действительно, если $S \in I$, то $S \in J$, так как сепаранта S ниже многочлена A, и, следовательно, многочлен

$$A - \frac{1}{d} x^{(r)} S$$

принадлежит идеалу I, но не идеалу J, что невозможно, так как этот многочлен ниже многочлена A. (Отметим, что предположение о том, что R является алгеброй Ритта, используется здесь по существу.) Так как идеал I прост, то из сказанного следует, что многочлен BS ему не принадлежит, и поэтому идеал $\{BS, I\}$ является радикальным дифференциальным идеалом, содержащим идеал I, но не совпадающим с ним. Следовательно, этот идеал имеет конечный тип. В силу леммы 7.2, $\{BS, I\} = \{BS, C_1, \ldots, C_q\}$, где все многочлены C_i принадлежат идеалу I.

Пусть F — произвольный элемент идеала I. Согласно лемме 7.3, существуют такие целые числа m и n и такой дифференциальный многочлен G, который ниже многочлена A, что разность $B^m S^n F - G$ принадлежит дифференциальному идеалу, порожденному элементом A, и, следовательно, тем более принадлежит идеалу I. Таким образом, многочлен G принадлежит идеалу I. Так как этот многочлен ниже многочлена A, то $G \in J$. Отсюда следует, что многочлен BSF принадлежит идеалу $\{J, A\}$. Так как это справедливо для всех многочленов $F \in I$, то $BSI \subset \{J, A\}$. Поэтому

$$I^2 \subset I\{BS, I\} \subset \{BSI, IC_1, \ldots, IC_q\} \subset$$

(согласно лемме 1.6)

$$\subset \{J, A, C_1, \ldots, C_q\} \subset I.$$

Отсюда следует (как и выше в аналогичном случае), что

$$I = \{J, A, C_1, \ldots, C_q\}.$$

Мы пришли к противоречию, так как идеал I не имеет конечного типа.

Следствие. *Для любой алгебры Ритта R, удовлетворяющей условию обрыва возрастающих цепей радикальных дифференциальных идеалов, результат $R\{x_1, \ldots, x_n\}$ присоединения к R конечного числа дифференциальных неизвестных также обладает этим свойством.*

Для приложений наиболее важен случай, когда алгебра R является дифференциальным полем характеристики нуль.

28. Системы дифференциальных уравнений. Любое алгебраическое дифференциальное уравнение (над некоторым дифференциальным полем F) является результатом приравнивания к нулю какого-нибудь дифференциального многочлена с коэффициентами из F. Решением является система элементов (возможно, некоторого дифференциального расширения поля F), удовлетворяющих этому уравнению. Следующая теорема является красивым непосредственным следствием теоремы 7.1.

Теорема 7.4. *Для произвольной бесконечной системы алгебраических дифференциальных уравнений над дифференциальным полем характеристики нуль относительно конечного числа дифференциальных неизвестных существует конечная подсистема, решения которой совпадают с решениями всей системы.*

29. Теорема разложения. Следующую теорему уместно сравнить с теоремой 2.1. За счет более сильной предпосылки в ней получено лучшее заключение.

Теорема 7.5. *В любом дифференциальном кольце, удовлетворяющем условию обрыва возрастающих цепей для радикальных дифференциальных идеалов, каждый радикальный дифференциальный идеал можно представить как пересечение конечного числа простых дифференциальных идеалов. В частности, это имеет место в кольце $F\{x_1, \ldots, x_n\}$, полученном присоединением конечного числа дифференциальных неизвестных к произвольному дифференциальному полю характеристики нуль.*

Доказательство. Предположим противное. Тогда (в силу условия обрыва возрастающих цепей, а не в силу леммы Цорна!) существует радикальный дифференциальный идеал I, максимальный среди идеалов, не являющихся пересечением конечного числа простых дифференциальных идеалов. Очевидно, что сам идеал I не является простым. Следовательно, существуют такие элементы a и b, что $ab \in I$, причем $a \notin I$, $b \notin I$. Радикальные дифференциальные идеалы $\{I, a\}$ и $\{I, b\}$ содержат идеал I как собственную часть и поэтому представимы в виде пересечения конечного числа простых дифференциальных идеалов.

Таким образом, для того чтобы прийти к противоречию, достаточно показать, что $I = \{I, a\} \cap \{I, b\}$. Так как, согласно лемме 1.6,

$$\{I, a\}\,\{I, b\} \subset \{ab, I\} \subset I,$$

то для любого элемента c идеала $\{I, a\} \cap \{I, b\}$ имеет место включение $c^2 \in \{I, a\}\,\{I, b\} \subset I$ и потому — включение $c \in I$. Таким образом, $\{I, a\} \cap \{I, b\} \subset I$. Обратное включение очевидно.

Единственность указанного в теореме 7.5 разложения не относится к дифференциальной алгебре. Назовем представление идеала I в виде пересечения некоторых идеалов *несократимым*, если ни один из этих идеалов не может быть опущен.

Теорема 7.6. *Если идеал I коммутативного кольца с единицей может быть представлен двумя способами как несократимое пересечение простых идеалов*

$$I = P_1 \cap \ldots \cap P_r = Q_1 \cap \ldots \cap Q_s,$$

то $r = s$ и при соответствующей нумерации $P_i = Q_i$.

Доказательство. Так как $P_1 \cap P_2 \cap \ldots \cap P_r \subset Q_1$, то $P_1 \cdot \ldots \cdot P_r \subset Q_1$ и, следовательно, один из идеалов P_i содержится в идеале Q_1. Можно считать, что $P_1 \subset Q_1$. Аналогично один из идеалов Q_i содержится в идеале P_1. Из несократимости представления следует, что этим идеалом необходимо является идеал Q_1, так что $P_1 = Q_1$. Аналогично каждый идеал Q_i совпадает с некоторым идеалом P_i, и обратно.

30. Изучение отдельного дифференциального многочлена. В этом пункте мы проанализируем, как теория, изложенная в предыдущих пунктах, применяется в том частном случае, когда рассматриваемый радикальный дифференциальный идеал порождается одним многочленом.

Рассмотрим произвольный дифференциальный многочлен A от одного дифференциального неизвестного y. Пусть r — его порядок, а S — его сепаранта: $S = \partial A/\partial y^{(r)}$. Обозначим через J множество всех многочленов B, для которых $BS \subset \{A\}$. Согласно лемме 1.4, J является радикальным дифференциальным идеалом. Мы будем придерживаться этих обозначений во всем дальнейшем изложении.

Лемма 7.7. $\{A\} = \{A, S\} \cap J$.

Доказательство. Тот факт, что идеал $\{A\}$ содержится и в идеале $\{A, S\}$ и в идеале J, очевиден. Обратно, если $C \in J \cap \{A, S\}$, то

$$C^2 \in C\{A, S\} \subset \{CA, CS\} \subset \{A\}$$

и, следовательно, $C \in \{A\}$.

Начиная с этого места мы должны предположить, что основное дифференциальное поле имеет характеристику нуль.

Лемма 7.8. *Если многочлен A неприводим (в обычном алгебраическом смысле — как многочлен от бесконечного числа неизвестных $y, y', y'', \ldots$), то любой дифференциальный многочлен G, принадлежащий дифференциальному идеалу, порожденному многочленом A, и имеющий порядок не больший порядка многочлена A, делится на A.*

Доказательство. По условию имеет место равенство вида

$$G = C_0A + C_1A' + \ldots + C_kA^{(k)}. \qquad (*)$$

Кроме того, $A^{(i)} = Sy^{(r+i)} + T_{r+i}$ $(i = 1, 2, 3, \ldots)$, причем порядок многочлена T_{r+i} меньше $r+i$. Будем рассматривать соотношение (*) как тождество относительно неизвестных $y, y', y'', \ldots$. Элемент $y^{(r+k)}$ может входить в многочлен C_i, но не должен входить в многочлен G. Заменив в (*) элемент $y^{(r+k)}$ выражением $\left(A^{(k)} - T_{k+r}\right)/S$ (заметим, что $S \neq 0$, так как характеристика поля равна нулю), мы снова получим тождество. После умножения на соответствующую степень сепаранты S мы придем, следовательно, к соотношению вида

$$S^jG = D_0A + D_1A' + \ldots + D_{k-1}A^{(k-1)}.$$

Повторяя это построение, мы получим, что многочлен A делит многочлен вида S^jG. Но многочлен A не делит сепаранту S (ибо S ниже A). Следовательно, A делит G. (Отметим, что с точки зрения обычной алгебры мы оперируем в области целостности, полученной присоединением счетного числа неизвестных к некоторому полю; в этой области целостности имеет место однозначность разложения на множители.)

Лемма 7.9. *Для неприводимого многочлена A идеал J прост.*

Доказательство. Предположим, что $FG \in J$. Мы должны доказать, что по крайней мере один из многочленов F и G принадлежит идеалу J. Пусть I — дифференциальный идеал, порожденный многочленом A. Легко видеть, что существуют такие целые числа m и n и такие дифференциальные многочлены F_1 и G_1, порядки которых не превосходят порядка многочлена A, что

$$S^mF \equiv F_1, \quad S^nG \equiv G_1 \qquad (\mathrm{mod}\ I)$$

(доказательство этого утверждения неявно содержится в доказательстве леммы 7.3). Так как $SFG \in \{A\}$ (по определению идеала J), а, согласно лемме 1.8, идеал $\{A\}$ является радикалом идеала I, то существует такое число k, что $(SFG)^k \in I$. После умножения на $S^{mk+nk-k}$ мы получим отсюда, что $(S^mF)^k(S^nG)^k \in I$. Следовательно, $(F_1G_1)^k \in I$. Поэтому, в силу леммы 7.8, многочлен A делит многочлен $(F_1G_1)^k$. Так как многочлен A неприводим, то он делит либо многочлен F_1, либо многочлен G_1. Допустим, что A делит F_1. Это означает, что $S^mF \in I$, $S^mF^m \in I$, $SF \in \{A\}$, $F \in J$.

Теорема 7.10. *Пусть F — произвольное дифференциальное поле характеристики нуль, A — произвольный неприводимый дифференциальный многочлен от одного неизвестного над полем F, и S — его сепаранта. Тогда множество J всех дифференциальных многочленов B, для которых $BS \in \{A\}$ является простым дифференциальным идеалом. Пусть $\{A, S\} = P_1 \cap \ldots \cap P_r$ несократимое представление идеала $\{A, S\}$ в виде пересечения простых дифференциальных идеалов. Тогда в несократимом представлении идеала $\{A\}$ участвуют идеал J и некоторые из идеалов P_i.*

Доказательство. Доказательства требует только последнее утверждение. Согласно лемме 7.7 имеет место представление $\{A\} = J \cap P_1 \cap \ldots \cap P_r$. Если бы из него можно было выбросить идеал J, то мы получили бы, что

$$J \cap P_1 \cap \ldots \cap P_r = P_1 \cap \ldots \cap P_r,$$

т. е. что $J \supset \{S, A\}$, $S \in J$ и $S^2 \in \{A\}$. Таким образом, некоторая степень сепаранты S принадлежала бы идеалу, порожденному многочленом A, и потому, в силу леммы 7.8, сепаранта S делилась бы на многочлен A, что невозможно.

Компонента J в представлении идеала $\{A\}$ называется ***идеалом общего решения***, а остальные компоненты — ***идеалами особых решений***.

31. Примеры. а) $A = (y')^2 - 4y$. Здесь $S = 2y'$, так что $\{S, A\}$ является идеалом, порожденным элементом y и всеми его производными. Этот идеал максимален. Легко видеть, что элемент y' не принадлежит идеалу J. Действительно, если $y' \in J$, то $y' \in \{A\}$, так как $y' \in \{S, A\}$, и поэтому некоторая степень элемента y' принадлежит дифференциальному идеалу, порожденному многочленом A, и, согласно лемме 7.8, делится на A. Но многочлен A не может быть делителем никакой степени элемента y'. Таким образом, $y' \notin J$. Но $A' = 2y'(y''-2)$, так что, ввиду простоты идеала J, $y''-2 \in J$. Следовательно, идеал J содержит идеал $K = \{(y')^2 - 4y, y''-2\}$. Обычный идеал, порожденный элементами $(y')^2-4y, y''-2, y''', \ldots$, уже сам является дифференциальным идеалом. Более того, этот идеал прост; действительно, переходя к вычетам по модулю этого идеала, мы можем вначале „отбросить“ переменные $y'', y''', \ldots$, а затем перейти к вычетам по модулю неприводимого многочлена $(y')^2 - 4y$. Итак, идеал K прост. Очевидно, что $\{A\} = J \cap \{S, A\} \cap K$. Если бы идеал J содержал идеал K как собственную часть, то мы могли бы удалить J из этого соотношения, что противоречит теореме 7.10. Следовательно, $J = K$. Таким образом, мы получили точное описание разложения радикального дифференциального идеала $\{A\}$.

Будем теперь искать решения уравнения $(y')^2 - 4y = 0$. Если t является решением, то $t'(t''-2) = 0$. Поэтому или $t' = 0$, или $t'' = 2$.

В первом случае $t=0$. Во втором — $(t'/2)'=1$, и, следовательно, обозначая через x некоторый фиксированный элемент, для которого $x'=1$, мы получаем $t'/2=x+c$ и $t=(t'/2)^2=(x+c)^2$, где c — произвольная константа. Классическая интерпретация: множество решений распадается на семейство парабол (решения, принадлежащие идеалу J) и огибающую этого семейства — прямую $y=0$, которая является особым решением.

b) $A=(y')^2-4y^3$. Снова $S=2y'$, и $\{A, S\}$ является идеалом, порожденным элементом y и его производными. Как и выше, мы получаем, что идеал J порождается элементом $(y')^2-4y^3$ и элементом $y''-6y^2$ и его производными. Следовательно, $J\subset\{A, S\}$, т. е. $\{A\}=J$ и потому прост уже сам идеал $\{A\}$.

Решения имеют вид $y=0$, $y=(x+c)^{-2}$.

Частное решение уравнения $A=0$ называется *особым*, если оно обращает в нуль сепаранту S дифференциального многочлена A. В примере (b) мы столкнулись с таким случаем, когда общее решение содержит особое решение.

Глава VIII

ДОБАВЛЕНИЕ. МАТРИЧНЫЕ ГРУППЫ И ИХ ОБОБЩЕНИЯ

32. Разрешимость. Начнем с доказательства следующего результата, справедливого для любых T_1-групп:

Теорема 8.1. *В произвольной T_1-группе замыкание подгруппы является подгруппой; замыкание нормального делителя является нормальным делителем.*

Доказательство. Пусть G — произвольная группа, S — любая ее подгруппа и S_1 — замыкание подгруппы S. Для любого элемента $s\in S$ отображение $x\to sx$ является гомеоморфным отображением группы G самой на себя. Поэтому прообраз множества S_1 при этом отображении замкнут. Так как этот прообраз содержит подгруппу S, то он содержит и ее замыкание S_1. Таким образом, $sS_1\subset S_1$. Аналогично, рассмотрев отображение $x\to xt$, где $t\in S_1$, мы получим, что $S_1S_1\subset S_1$. Так как $S_1^{-1}=S_1$ ввиду непрерывности операции взятия обратного элемента, S_1 действительно является подгруппой.

Для любого элемента $a\in G$ отображение $x\to axa^{-1}$ является гомеоморфным отображением группы G на себя. Поэтому множество aS_1a^{-1} замкнуто. Если теперь подгруппа S является нормальным делителем, то множество aS_1a^{-1} содержит подгруппу S, а следовательно, и ее замыкание S_1. Таким образом, $a^{-1}S_1a\subset S_1$, так что S_1 является нормальным делителем.

Для произвольной T_1-группы утверждение о том, что замыкание абелевой подгруппы абелево, вообще говоря, неверно (построение соответствующего примера см. п. 17). Однако оно справедливо для любой C-группы. Мы докажем следующий, несколько более общий результат.

Теорема 8.2. *Пусть G — произвольная C-группа, а S и T — такие ее подгруппы, что $S\supset T$, причем подгруппа T содержит коммутант подгруппы S. Тогда замыкание T_1*

подгруппы T содержит коммутант замыкания S_1 подгруппы S.

Доказательство. Для любого фиксированного элемента b подгруппы S отображение $a \to aba^{-1}b^{-1}$ непрерывно. Прообраз подгруппы T_1 при этом отображении содержит подгруппу S, а следовательно, и подгруппу S_1. Аналогично для любого элемента a подгруппы S_1 отображение $b \to aba^{-1}b^{-1}$ непрерывно и прообраз подгруппы T_1 при этом отображении содержит подгруппу S, а потому и подгруппу S_1. Таким образом, подгруппа T_1 содержит все коммутаторы элементов подгруппы S_1.

Следствие 1. *В любой C-группе замыкание абелевой подгруппы является абелевой подгруппой.*

Доказательство. Применим теорему 8.2 к случаю, когда $T = E$.

Следствие 2. *В любой C-группе замыкание разрешимой подгруппы является разрешимой подгруппой.*

Доказательство. Пусть H — разрешимая подгруппа некоторой C-группы, K — ее замыкание, $H = H_1 \supset \ldots \supset H_n = E$ — убывающий ряд коммутантов подгруппы H, и K_i — замыкание подгруппы H_i. По теореме 8.2 подгруппа K_{i+1} содержит коммутант подгруппы K_i. Следовательно, каждая факторгруппа K_i/K_{i+1} абелева, так что группа K разрешима.

В заключение этого пункта приведем один результат, доказанный Колчиным [4] для матричных групп в топологии Зариского

Назовем T_1-группу G *топологически разрешимой*, если существует такая цепь $G = G_1 \supset G_2 \supset \ldots \supset G_n = E$ замкнутых подгрупп, каждая из которых является нормальным делителем предыдущей, что все факторгруппы G_i/G_{i+1} абелевы. Разумеется, каждая топологически разрешимая группа разрешима. Оказывается, что для C-групп имеет место и обратное утверждение.

Теорема. 8.3. *Любая разрешимая C-группа G топологически разрешима.*

Доказательство. Проведем индукцию по длине убывающего ряда коммутантов группы G. Предположим, что он кончается членом $G_k = E$. Тогда G_{k-1} является абелевым нормальным делителем группы G. Его замыкание H является, в силу теоремы 8.1 и следствия 1 из теоремы 8.2, абелевым нормальным делителем. Группа G/H тоже является C-группой, и ее убывающий ряд коммутантов короче ряда группы G. По индуктивному предположению группа G/H топологически разрешима. Следовательно, и группа G топологически разрешима.

33. CZ-группы. Любая группа может быть превращена в C-группу: достаточно взять ее в дискретной топологии. Любую группу можно превратить и в Z-группу: достаточно взять ее в минимальной T_1-топологии. Однако не каждую группу можно превратить в CZ-группу. Действительно, из лемм 4.5 и 4.6 вытекает.

Теорема 8.4. *Для любой CZ-группы и, в частности, для любой мультипликативной группы матриц существует конечная верхняя граница для числа элементов в конечных классах сопряженных.*

Более полезный результат можно вывести из условия обрыва убывающих цепей замкнутых множеств, если вспомнить, что централизаторы в C-группах замкнуты [1]).

Теорема 8.5. *В любой CZ-группе и, в частности, в любой мультипликативной группе матриц централизаторы подмножеств удовлетворяют условию обрыва убывающих цепей.*

Группа конечных четных перестановок над бесконечным множеством элементов, очевидно, не удовлетворяет условию обрыва убывающих цепей централизаторов. Кроме того, она проста, поэтому каждое ее нетривильное матричное представление должно быть точным. Следовательно, имеет место

Теорема 8.6. *Группа конечных четных перестановок над бесконечным множеством элементов не допускает никакого матричного представления (при любом поле и любом порядке матриц), кроме представления, при котором каждому элементу группы соответствует единичная матрица.*

Существование группы с этим свойством, по-видимому, в литературе еще не отмечалось.

---

[1]) Достаточно заметить, что централизатор элемента b можно определить как его прообраз при отображении $a \to aba^{-1}$, а централизатор подмножества — как пересечение централизаторов всех его элементов. — *Прим. перев.*

34. Неприводимые множества; условие обрыва возрастающих цепей. В теории, развитой в главе IV, большую роль играло понятие связности. Но в алгебраической геометрии важна скорее не связность, а неприводимость.

Определение. Топологическое пространство X называется *неприводимым*, если оно не может быть представлено как объединение двух собственных замкнутых подмножеств. Подмножество пространства X называется неприводимым, если в индуцированной топологии оно является неприводимым топологическим пространством.

Замечание. Легко видеть, что неприводимое хаусдорфово пространство содержит не более одной точки.

В следующей лемме собраны некоторые нужные нам факты; ее доказательство несложно, и мы его опустим (подробное изложение см. [10]).

Лемма 8.7. 1) *Непрерывный образ неприводимого пространства является неприводимым пространством.* 2) *Замыкание неприводимого множества является неприводимым множеством.* 3) *Любое Z-пространство может быть представлено в виде объединения $S_1 \cup S_2 \cup \ldots \cup S_r$ конечного числа замкнутых неприводимых подмножеств. Если это представление несократимо (т. е. ни одно из подмножеств S_i не может быть опущено), то оно единственно.*

В главе IV мы ограничивались рассмотрением связных множеств, так как для групп понятия связности и неприводимости совпадают.

Лемма 8.8. *Единственным несократимым разложением Z-группы G на замкнутые неприводимые множества является ее разбиение на смежные классы по компоненте единицы C.*

Доказательство. Пусть $G = S_1 \cup S_2 \cup \ldots \cup S_r$ — разложение группы G на замкнутые неприводимые множества. В первую очередь мы докажем, что множества S_i попарно не пересекаются. Пусть $a \in S_1 \cap S_2$. Каждый гомеоморфизм группы G только переставляет множества S_i между собой (ввиду единственности разложения). Так как для любого элемента b группы G существует гомеоморфизм (например, соответствующее правое умножение), переводящий элемент a в элемент b, то элемент b также принадлежит двум различным множествам S_i. В частности, любой элемент множества S_1

принадлежит по крайней мере еще одному множеству S_i (где $i > 1$). Таким образом,

$$S_1 = (S_1 \cap S_2) \cup \ldots \cup (S_1 \cap S_r).$$

Так как каждое пересечение $S_1 \cap S_i$ замкнуто и является собственным подмножеством множества S_1, то это соотношение противоречит неприводимости множества S_1. Таким образом, все множества S_i попарно не пересекаются.

Пусть S_1 является тем множеством рассматриваемого разложения, которое содержит единицу группы G. Для любого элемента $a \in S_1$ множество $S_1 a$ пересекает множество S_1 и является одним из множеств S_i, следовательно, $S_1 a = S_1$. Равным образом, $S_1^{-1} = S_1$, так что S_1 является подгруппой. Эта подгруппа, естественно, связна; она является компонентой единицы, а остальные множества S_i представляют собой смежные классы по подгруппе S_1.

Следствие. *Связная Z-группа неприводима.*

Пусть теперь F — произвольное поле. Легко видеть, что в n-мерном векторном пространстве V над полем F, рассматриваемом в топологии Зариского, выполняется условие обрыва возрастающих цепей неприводимых замкнутых подмножеств. Действительно, каждое неприводимое замкнутое подмножество имеет размерность, не превосходящую n, а, с другой стороны, размерность является строго возрастающей функцией. Отсюда вытекает, что любая матричная группа в топологии Зариского удовлетворяет условию обрыва возрастающих цепей замкнутых неприводимых подмножеств и, в частности (следствие из леммы 8.8), замкнутых связных подгрупп. Пользуясь этим фактом, мы получим ряд интересных следствий.

Теорема 8.9. *Связная CZ-группа G, удовлетворяющая условию обрыва возрастающих цепей для замкнутых связных нормальных делителей, обладает единственным максимальным связным разрешимым нормальным делителем M. Этот нормальный делитель автоматически замкнут. Центр Z/M группы G/M конечен, а его прообраз Z является единственным максимальным разрешимым нормальным делителем группы G.*

Доказательство. Вследствие условия обрыва возрастающих цепей в группе G существует хотя бы один максимальный связный замкнутый нормальный делитель M. Для любого связного разрешимого нормального делителя H подгруппа HM является разрешимым и связным нормальным делителем. Замыкание подгруппы HM разрешимо (следствие 2 из теоремы 8.2), связно и является нормальным делителем. Следовательно, $H \subset M$.

Группа G/M (она тоже является CZ-группой) не имеет связных разрешимых нормальных делителей. Следовательно, каждый ее разрешимый нормальный делитель конечен и, следовательно (лемма 4.7), централен. Таким образом, подгруппа Z/M конечна, и Z является единственным максимальным разрешимым нормальным делителем группы G.

Лемма 8.11. *Если нормальный делитель H некоторой группы G и соответствующая факторгруппа G/H обладают единственным максимальным нормальным делителем, то тем же свойством обладает и группа G.*

Доказательство этой леммы предоставляется читателю. Из теоремы 8.9 и леммы 8.11 вытекает.

Теорема 8.12. *Любая CZ-группа G, удовлетворяющая условию обрыва возрастающих цепей замкнутых связных нормальных делителей, в частности, любая матричная группа (в топологии Зариского) обладает единственным максимальным разрешимым нормальным делителем.*

Для матричных групп эта теорема была другим способом доказана Цассенхаузом [11].

35. Образы неприводимых множеств. Все, что было изложено в главе IV и до сих пор излагалось в главе VIII, применимо к любой матричной группе, не обязательно алгебраической. Естественно, что, оставаясь в том же круге понятий, нельзя доказать свойства матричных групп, по существу зависящие от условия алгебраичности. В этом заключительном пункте мы вводим некоторую дополнительную аксиому, позволяющую прийти к существенно более глубоким результатам.

Определение. Пусть X — произвольное топологическое пространство. Мы будем говорить, что подмножество S пространства X *полузамкнуто*, если S содержит подмножество T, плотное в S и относительно открытое в его замыкании S_1 (это определение заимствовано из алгебраической геометрии, где рассматриваются алгебраические многообразия, из которых удалены части многообразий меньших размерностей).

Лемма 8.13. *Пусть G — произвольная CZ-группа и U — ее полузамкнутое плотное подмножество. Тогда $UU = G$.*

Доказательство. По условию $U \supset V$, где V — некоторое открытое плотное подмножество группы G. Покажем, что $VV = G$. Для любого элемента $x \in G$ множества V и $V^{-1}x$ непусты и открыты. Так как группа G неприводима (следствие из леммы 8.8), то пересечение $V \cap V^{-1}x$ непусто. Следовательно, $x \in VV$.

Под *словом* в некоторой группе относительно переменных $x_1, \ldots, x_r$ мы понимаем произведение степеней (положительных или отрицательных) переменных x_i и, возможно, некоторых других фиксированных элементов группы.

Теперь сформулируем нужную нам аксиому, которую мы будем называть аксиомой (D).

(D) Мы будем говорить, что T_1-группа G удовлетворяет аксиоме (D), если для любых замкнутых неприводимых множеств $C_1, \ldots, C_r$ и любого слова $f(x_1, \ldots, x_r)$ совокупность значений слова f, когда каждое из переменных x_i пробегает соответствующее множество C_i ($i = 1, \ldots, r$), является полузамкнутым неприводимым множеством.

Тот факт, что алгебраические матричные группы в топологии Зариского (над произвольным алгебраически замкнутым полем) удовлетворяют аксиоме (D), по существу доказан в книге Шевалле по алгебраическим группам [12]. Прямое доказательство этого факта легко получается с помощью теории исключения.

Теорема 8.14. *Пусть $S_1, \ldots, S_r$ — замкнутые связные подгруппы Z-группы G, удовлетворяющей условию обрыва возрастающих цепей для замкнутых неприводимых множеств и аксиоме (D). Пусть, кроме того, $f_i(x_1, \ldots, x_r)$, $i = 1, \ldots, k$, — такие слова, что для каждого из них существуют значения переменных $x_j \in S_j$, при которых это слово принимает значение e [1]). Тогда подгруппа H, порожденная всеми элементами вида $f_1(x_1, \ldots, x_r), \ldots, f_k(x_1, \ldots, x_r)$, где $x_j \in S_j$, замкнута. Кроме того, существует такое целое число n, что каждый элемент этой*

[1]) Через e обозначается единица группы G. — *Прим. перев.*

подгруппы является произведением не более чем n элементов вида f_i и обратных к ним.

Доказательство. Без ограничения общности можно считать, что к данным словам f_i, присоединены „обратные“ слова $f_1^{-1}, \ldots, f_k^{-1}$. Если это уже сделано, то подгруппу H мы можем рассматривать как совокупность всех произведений значений слов f_i.

Пусть $m_1, \ldots, m_t$ — произвольная последовательность целых чисел, каждое из которых лежит в пределах от 1 до k, $C(m_1, \ldots, m_t)$ — множество всех элементов вида $f_{m_1} \ldots f_{m_t}$, где аргументы $x_1, \ldots, x_r$ пробегают подгруппы $S_1, \ldots, S_r$ соответственно [1]), и $D(m_1, \ldots, m_t)$ — замыкание множества $C(m_1, \ldots, m_t)$. Из аксиомы (D) вытекает [2]), что множество $D(m_1, \ldots, m_t)$ неприводимо. С другой стороны, из того, что при соответствующих значениях аргументов слова f_i принимают значение e, следует, что $C(m_1, \ldots, m_{t-1}) \subset C(m_1, \ldots, m_t)$; то же соотношение имеет место, конечно, для их замыканий.

Пусть H_1 — объединение всех этих замыканий. Из условия обрыва возрастающих цепей замкнутых неприводимых множеств с помощью простого комбинаторного рассуждения вытекает существование такого целого числа p, что H_1 является объединением уже только тех множеств $D(m_1, \ldots, m_t)$, для которых $t \leqslant p$. Следовательно, множество H_1 замкнуто. Так как подгруппа H плотна в H_1, то H_1 есть не что иное, как ее замыкание, и, следовательно, является подгруппой группы G. Пусть теперь H_0 — объединение всех множеств $C(m_1, \ldots, m_t)$, для которых $t \leqslant p$. В силу аксиомы (D), множество H_0 полузамкнуто; так как его замыканием является подгруппа H_1, то, согласно лемме 8.13, $H_0H_0 = H_1$. Это доказывает, что $H = H_1$ и, следовательно, подгруппа H замкнута. Тем самым первое утверждение теоремы полностью доказано. Второе утверждение также непосредственно вытекает отсюда (достаточно за n принять число $2p$).

[1]) Предполагается, что в различных словах f_{m_i} аргументы $x_1, \ldots, x_r$ принимают, вообще говоря, различные значения. — *Прим. перев.*

[2]) Аксиому (D) следует применить к слову $f\left(x_1^{(1)}, \ldots, x_r^{(1)}, x_1^{(2)}, \ldots \ldots, x_r^{(t)}\right) = f_{m_1}\left(x_1^{(1)}, \ldots, x_r^{(1)}\right) \ldots f_{m_t}\left(x_1^{(t)}, \ldots, x_r^{(t)}\right)$ и к замкнутым связным подгруппам $S_1^{(1)}, \ldots, S_r^{(1)}, S_1^{(2)}, \ldots, S_r^{(t)}$, где $S_i^{(k)} = S_i$. — *Прим. перев.*

В заключение отметим следующие четыре частных случая теоремы 8.14.

Теорема 8.15. *Подгруппа, порожденная замкнутыми связными подгруппами $S_1, \ldots, S_r$ произвольной Z-группы G, удовлетворяющей условию обрыва возрастающих цепей замкнутых неприводимых подмножеств и аксиоме (D), замкнута. Любой ее элемент является произведением не более чем n элементов данных подгрупп, где n — некоторое целое число.*

Доказательство. Достаточно применить теорему 8.14 к многочлену $x_1x_2 \ldots x_r$.

Простые примеры показывают, что в теореме 8.15 нельзя отбросить предположение о связности подгрупп S_i. Однако это ограничение можно снять, если все подгруппы, кроме одной, являются нормальными делителями.

Теорема 8.16. *Пусть G — произвольная Z-группа, удовлетворяющая условию обрыва возрастающих цепей для замкнутых неприводимых подмножеств и аксиоме (D). Пусть, далее, S и T — замкнутые подгруппы группы G. Тогда если подгруппа S является нормальным делителем, то подгруппа ST замкнута.*

Доказательство. Пусть S_0 и T_0 — компоненты единиц подгрупп S и T соответственно. Согласно теореме 8.15, подгруппа S_0T_0 замкнута. Так как она в подгруппе ST имеет конечный индекс, то последняя также замкнута.

Теорема 8.17. *Для любой Z-группы G, удовлетворяющей условию обрыва возрастающих цепей замкнутых неприводимых подмножеств и аксиоме (D), подгруппа G_r, порожденная r-ми степенями элементов группы G, замкнута. Любой ее элемент является произведением не более чем n r-ых степеней, где n — некоторое целое число.*

Доказательство. Достаточно применить теорему 8.14 к многочлену x^r.

Я не знаю, существенно ли для справедливости теоремы 8.17 предположение о связности группы G. Что же касается следующей теоремы, то для нее связность несущественна. (Для связных алгебраических матричных групп эта теорема доказана Шевалле [12]; излагаемое ниже доказательство принадлежит Розенлихту.)

Теорема 8.18. *Коммутант G' произвольной Z-группы G, удовлетворяющей условию обрыва возрастающих цепей замкнутых неприводимых подмножеств и аксиоме (D), замкнут. Любой его элемент является произведением не более чем n коммутаторов, где n — некоторое целое число.*

Доказательство. Пусть $z_1, z_2, \ldots, z_h$ — представители смежных классов группы G по ее компоненте единицы C. Обозначим через $f_i(x, y)$ коммутатор элементов $z_i x$ и y. Так как $f_i = e$ при $x = y = e$, то к этим h многочленам применима теорема 8.14 (предполагается, что переменные x и y пробегают подгруппу C). Получающаяся подгруппа H замкнута; кроме того, ее элементы являются произведениями ограниченного числа коммутаторов. Так как факторгруппа C/H лежит в центре факторгруппы G/H, доказательство теоремы сводится к следующей чисто теоретико-групповой теореме, установленной независимо друг от друга Бэром, Нейманом и Виттом.

Теорема 8.19. *Если центр группы G имеет конечный индекс, то коммутант группы G конечен.*

Приведем здесь доказательство теоремы 8.19, принадлежащее Дональду Орнштейну. Пусть $a_1, \ldots, a_m$ — представители смежных классов группы G по ее центру. Любой коммутатор группы G имеет вид $a_i^{-1} a_j^{-1} a_i a_j$, так что коммутаторов не более чем m^2. Наша задача — найти границы для длин произведений коммутаторов. В достаточно длинном произведении хотя бы один коммутатор повторяется m раз. Мы можем так переставить множители, чтобы эти m элементов оказались соседними. При этом некоторые коммутаторы заменятся на сопряженные, что не повлияет на дальнейшие рассуждения. Для завершения доказательства остается воспользоваться следующей леммой.

Лемма 8.20. *Если элемент $(ab)^m$ принадлежит центру группы, то элемент $(a^{-1}b^{-1}ab)^m$ является произведением $(m-1)$ коммутаторов.*

Докажем, что для любого r элемент $(a^{-1}b^{-1}ab)^r$ может быть записан в виде произведения элемента $(a^{-1}b^{-1})^r (ab)^r$ и $r-1$, коммутаторов. Предположив, что это верно для $r-1$; мы получаем

$$(a^{-1}b^{-1}ab)^r = a^{-1}b^{-1}ab\,(a^{-1}b^{-1})^{r-1}(ab)^{r-1} c_{r-2} \ldots c_1,$$

где c_i — коммутаторы. Переставим элементы ab и $(a^{-1}b^{-1})^{r-1}$; тогда появится новый коммутатор, который можно, заменив его на сопряженный, поместить непосредственно перед коммутатором c_{r-2}. Тем самым наше утверждение доказано и для r. Применим его при $r = m$. Так как элементы $(ab)^m$ и $(ba)^m$ сопряжены, они равны. Следовательно, $(a^{-1}b^{-1})^m (ab)^m = e$. Тем самым лемма полностью доказана.

ГЛОССАРИЙ

Ниже следует перечень важнейших определений в порядке, более или менее соответствующем порядку их появления в тексте.

Дифференцирование. Аддитивное отображение, подчиняющееся закону дифференцирования произведения.

Дифференциальное кольцо. Коммутативное кольцо с единицей, в котором выделено дифференцирование.

Дифференциальный идеал. Идеал, замкнутый относительно дифференцирования.

Дифференциальный гомоморфизм (*изоморфизм, автоморфизм*). Гомоморфное (изоморфное, автоморфное) отображение, перестановочное с дифференцированием.

Константа. Элемент, производная которого равна нулю.

Радикал идеала. Множество всех элементов, некоторая степень которых принадлежит идеалу.

Радикальный идеал. Идеал, совпадающий со своим радикалом.

Алгебра Ритта. Дифференциальное кольцо, содержащее поле рациональных чисел.

Допустимый изоморфизм. Изоморфизм между двумя полями, содержащимися в одном общем надполе.

Дифференциальная группа Галуа. Группа всех дифференциальных автоморфизмов данного поля, оставляющих все элементы основного поля неподвижными.

Вронскиан n элементов. Определитель n-го порядка, в i-ой строке которого стоят производные $i-1$-го порядка данных элементов.

Расширение Пикара—Вессио. Не содержащее новых констант расширение, порожденное линейно независимыми решениями линейного однородного уравнения n-го порядка.

Присоединение интеграла. Присоединение элемента u, производная u' которого принадлежит основному полю.

Присоединение экспоненты интеграла. Присоединение элемента u, логарифмическая производная u'/u которого принадлежит основному полю.

Расширение Лиувилля. Результат конечного числа расширений, каждое из которых состоит либо в присоединении интеграла, либо в присоединении экспоненты интеграла.

Обобщенное расширение Лиувилля. Результат конечного числа расширений, каждое из которых состоит либо в присоединении интеграла или экспоненты интеграла, либо является конечным алгебраическим расширением.

Топология Зариского. Топология, замкнутыми множествами которой служат алгебраические многообразия.

Алгебраическая матричная группа. Группа, состоящая из всех неособых матриц, удовлетворяющих некоторому множеству полиномиальных соотношений (т. е. замкнутая подгруппа полной линейной группы в топологии Зариского).

Z-пространство. T_1-пространство, удовлетворяющее условию обрыва убывающих цепей замкнутых множеств.

T_1-группа. Группа с T_1-топологией, в которой переход к обратному элементу непрерывен, а умножение непрерывно по каждому переменному.

Z-группа. T_1-группа, являющаяся Z-пространством.

C-группа. T_1-группа, в которой отображение $a \to a^{-1}xa$ (элемент x фиксирован) непрерывно.

CZ-группа. T_1-группа, одновременно являющаяся C- и Z-группой.

Дифференциальный многочлен. Многочлен от некоторого элемента (скажем y) и его производных. Его *порядок* — порядок высшей производной $y^{(r)}$, действительно содержащейся в многочлене. Его *степень* d — степень относительно производной $y^{(r)}$. Его *старший коэффициент* — коэффициент при $[y^{(r)}]^d$. Его *сепаранта* — частная производная по $y^{(r)}$.

Неприводимое топологическое пространство. Пространство, которое не может быть представлено в виде объединения двух замкнутых собственных подмножеств.

Обозначения для присоединений. Мы рассматриваем четыре рода присоединений; каждое имеет свои обозначения. Скобки [ ] употребляются для присоединений в смысле обычной теории колец, скобки ( ) — для присоединений в смысле обычной теории полей, скобки { } — для присоединений в смысле теории дифференциальных колец и, наконец, скобки ⟨ ⟩ — для присоединений в смысле теории дифференциальных полей. Скобки { } употребляются также для обозначения минимального радикального дифференциального идеала, содержащего данное множество.

ЛИТЕРАТУРА

Колчин Е. Р. (Kolchin E. R.)

[1] Extensions of differential fields I, Ann. of Math., **43** (1942), 724—729.

[2] Algebraic matric groups and the Picard — Vessiot theory of homogeneous linear ordinary differential equations, Ann. of Math., **49** (1948), 1—42.

[3] Existence theorems connected with the Picard—Vessiot theory of homogeneous linear ordinary differential equations, Bull. Amer. Math. Soc., **54** (1948), 927—932.

[4] On certain concepts in the theory of algebraic matric groups, Ann. of Math., **49** (1948), 774—789.

[5] Picard—Vessiot theory of partial differential fields, Proc. Amer. Math. Soc., **3** (1952), 596—603.

[6] Galois theory of differential fields, Amer. J. of Math., **75** (1953), 753—824.

[7] On the Galois theory of differential fields, Amer. J. of Math., **77** (1955), 868—894.

Ритт Ж. Ф. (Ritt J. F.)

[8] Differential equations from the algebraic standpoint, Amer. Math. Soc. Coll. Pub., № 14, New York, 1932.

[9] Differential algebra, Amer. Math. Soc. Coll. Pub., № 33, New York, 1950.

Серр Ж.—П. (Serre J.—P.)

[10] Faisceaux algébriques cohérents, Ann. of Math., **61** (1955), 197—278.

Цассенхауз Г. (Zassenhaus H.)

[11] Beweis eines Satzes über diskrete Gruppen, Hamb. Abh., **12** (1938), 289—312.

Шевалле К. (Chevalley C.)

[12] Теория групп Ли, т. II (Алгебраические группы. Общая теория алгебр Ли), ИЛ, М., 1958.

ОГЛАВЛЕНИЕ

Из предисловия автора 5

Глава I. Общие сведения о дифференциальных кольцах 7

1. Дифференцирования 7
2. Дифференциальные кольца 8
3. Радикальные идеалы 10
4. Алгебры Ритта 11

Глава II. Продолжение изоморфизмов 13

5. Теорема Крулля 13
6. Расширение простых идеалов 14
7. Лемма о кольцах многочленов 15
8. Допустимые изоморфизмы 17

Глава III. Элементы теории Галуа 20

9. Дифференциальная группа Галуа 20
10. Вронскиан 24
11. Расширения Пикара—Вессио 25
12. Два специальных случая 27
13. Расширения Лиувилля 29
14. Треугольные автоморфизмы 30

Глава IV. Алгебраические матричные группы и топология Зариского 31

15. Z-пространства 31
16. T_1-группы и Z-группы 32
17. C-группы 34
18. Разрешимые связные матричные группы . . 36
19. Один специальный результат 39

Глава V. Теория Галуа 41

20. Три леммы 41
21. Нормальность расширений Пикара—Вессио 43
22. Завершение теории Галуа 47
23. Расширения Лиувилля 49

Глава VI. Уравнения второго порядка 53

24. Вронскиан 53
25. Связь с уравнениями Риккати 54
26. Пример 55

Глава VII. Теорема о базисах и приложения 58

27. Теорема о базисах 58
28. Системы дифференциальных уравнений . . . 63
29. Теорема разложения 63
30. Изучение отдельного дифференциального многочлена 65
31. Примеры 67

Глава VIII. Добавление. Матричные группы и их обобщения 69

32. Разрешимость 69
33. CZ-группы 71
34. Неприводимые множества; условие обрыва возрастающих цепей 72
35. Образы неприводимых множеств 74

Глоссарий 80

Литература 83