М. М. ПОСТНИКОВ

# ОСНОВЫ ТЕОРИИ ГАЛУА

ФИЗМАТГИЗ 1960

М. М. ПОСТНИ

# ОСНОВЫ ТЕОРИИ ГАЛУА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1960

## АННОТАЦИЯ

Книга содержит краткое изложение теории Галуа. Она рассчитана на студентов II—III курсов университетов, прослушавших первую часть курса высшей алгебры, и может быть использована также студентами педагогических институтов, а также лицами, не имеющими специальной математической подготовки и желающими самостоятельно ознакомиться с теорией Галуа.

Изложение автора несколько отличается от общепринятого и дает возможность разобраться в основных идеях теории Галуа без применения ряда более трудных разделов современной алгебры.

---

*Михаил Михайлович Постников.*

Основы теории Галуа.

Редактор *Х. М. Коган.*

Техн. редактор *Е. А. Ермакова.* Корректор *С. А. Шорыгин.*

Сдано в набор 26/XI 1959 г. Подписано к печати 30/I 1960 г. Бумага 84×108/32.
Физ. печ. л. 3,88. Условн. печ. л. 6,35. Уч.-изд. л. 5,75.
Тираж 9000 экз. Т-01019. Цена книги 2 р. 90 к. Заказ 915.

Государственное издательство физико-математической литературы.
Москва, В-71, Ленинский проспект, 15.

Типография № 2 им. Евг. Соколовой УПП Ленсовнархоза.
Ленинград, Измайловский пр., 29.

# ОГЛАВЛЕНИЕ

## ПРЕДИСЛОВИЕ

Эта книга в первую очередь предназначена для студентов второго и третьего курсов университетов, приступающих к изучению теории Галуа. Ввиду этого от читателя предполагается владение лишь основами высшей алгебры в объеме программы первого курса университетов. С другой стороны, теоретический материал, излагаемый в книге, примерами не сопровождается, поскольку предполагается, что это должно быть сделано на лекциях или семинарских занятиях. Задачи, включенные в текст книги, имеют совершенно тривиальный характер и предназначены исключительно для самоконтроля читателя. Следует отметить, что принятый в книге порядок изложения отличается от порядка, в котором теория Галуа должна излагаться на лекциях (например, группы подстановок в лекционном курсе должны появиться значительно ранее).

Теория Галуа излагается в книге для полей, принадлежащих некоторому единому «универсальному», алгебраически замкнутому полю характеристики 0 (для определенности — полю комплексных чисел). Это позволяет избежать трудной для начинающего абстрактной теоремы о существовании и единственности (с точностью до изоморфизма) поля разложения данного многочлена. С другой стороны, при таком изложении фактической потери общности не происходит, поскольку, как известно, любое поле можно включить в алгебраически замкнутое.

Другая, не столь существенная особенность принятого в этой книге изложения состоит в том, что мы тщательно избегаем использования теоремы о продолжении изоморфизма, заменяя ее, быть может, более кустарными, но зато более доступными соображениями теории симметрических функций. Далее, мы более педантично, чем это обыкновенно делается, исследуем соотношения между различными определениями конечного расширения, а изложение теоретико-группового

материала основываем на понятии гомоморфизма (заметим кстати, что для гомоморфизмов «на» и изоморфизмов «в» мы употребляем специальные термины, недавно появившиеся в литературе и быстро завоевывающие права гражданства).

Так как теория групп играет в теории Галуа лишь вспомогательную роль, она изложена лишь постольку, поскольку это необходимо для развития общей теории Галуа и ее применений к задаче о решении уравнений в радикалах. Например, хотя мы и излагаем понятия нормального ряда и его уплотнения, но никаких теорем типа теорем Шрейера или Жордана — Гёльдера в книге нет.

При изложении теории подстановок подробно доказывается теорема о разложении подстановок в произведение независимых циклов, а понятие четности подстановки вводится на основе рассмотрения разложения подстановки в произведение транспозиций. Не настаивая решительным образом на преимуществе такого способа введения понятия четности подстановки (по сравнению со стандартным, основанным на рассмотрении инверсий в перестановках), мы все же считаем, что и этот способ заслуживает внимания. Простоту знакопеременной группы мы доказываем следуя недавно появившейся работе Редеи. Доказательство Редеи, как нам представляется, проще общепринятого доказательства Бауера.

Рассматривая решение уравнений в радикалах, мы ограничиваемся задачей о решении уравнений в произвольных (быть может, приводимых) радикалах. Тем самым уравнения деления круга по определению считаются разрешимыми в радикалах, что, конечно, существенно упрощает теорию.

Хотя при таком подходе к решению уравнений в радикалах получающиеся результаты нельзя, например, применить к задаче о построении правильных многоугольников с помощью циркуля и линейки (поскольку теория гауссовых периодов остается целиком вне рамок нашего изложения), все же достигаемое на этом пути упрощение теории столь значительно, что для первоначального ознакомления с основными идеями, на которых основывается применение теории Галуа к задаче о разрешении в радикалах, рассмотрение лишь неприводимых радикалов представляется нецелесообразным.

В последней главе книги рассматриваются общие (т. е. имеющие буквенные коэффициенты) уравнения. Так как полем коэффициентов этих уравнений является поле рациональных

функций, то, оставаясь на указанной выше точке зрения, мы вынуждены специально доказывать, что это поле можно включить в алгебраически замкнутое поле (именно, в поле дробно-степенных рядов). Алгебраическая замкнутость поля дробно-степенных рядов доказывается по Островскому с помощью леммы Гензеля. Это доказательство, хотя и не эффективно, но значительно проще конструктивного доказательства, основанного на многоугольнике Ньютона и не раз излагавшегося на русском языке.

Для ссылки на материал первого курса мы используем книгу А. Г. Куроша «Курс высшей алгебры», которая в тексте называется просто «Курс». При этом страницы указываются по четвертому или пятому изданиям.

Автор пользуется случаем поблагодарить В. Г. Болтянского и Д. К. Фаддеева, прочитавших книгу в рукописи и сделавших много ценных замечаний.

*Автор*

ГЛАВА I

# ЭЛЕМЕНТЫ ТЕОРИИ ПОЛЕЙ

## 1. Предварительные замечания

*Полем* мы называем непустое множество $P$ комплексных чисел, обладающее следующими свойствами:

1) если $a \in P$ и $b \in P$, то $a+b \in P$ и $ab \in P$;

2) если $a \in P$, то $-a \in P$ и $a^{-1} \in P$ (при $a \neq 0$).

Полями являются, например, поле рациональных чисел $R$, поле действительных чисел $D$ и поле комплексных чисел $C$.

Поле $P$ называется *подполем* поля $K$, а поле $K$ — *расширением* поля $P$, если любой элемент поля $P$ принадлежит полю $K$, т. е. если[1]) $P \subset K$. Любое поле (в нашем смысле) является подполем поля комплексных чисел.

Легко видеть, что каждое поле содержит единицу, а следовательно и все поле рациональных чисел $R$, т. е. любое поле является расширением поля рациональных чисел.

В современной алгебре принято абстрактное определение поля как множества с двумя алгебраическими операциями, удовлетворяющим определенным аксиомам (см. Курс, стр. 28). В отличие от таких «абстрактных» полей, поля в нашем смысле называются *числовыми*. Излагаемую в этой книге теорию можно без большого труда перенести и на случай нечисловых полей. Переход от числовых полей к произвольным влечет в основном лишь чисто технические трудности. Эти трудности связаны с тем, что в нечисловом поле некоторое кратное единицы может оказаться равным нулю, а неприводимый многочлен — обладать кратными корнями.

[1]) Обозначение $P \subset K$ не исключает случая, когда $P$ совпадает с $K$.

Поля, в которых это затруднение не возникает, называются полями характеристики 0 (см. Курс, стр. 32 и 213). К ним, кроме числовых полей, принадлежат, например, поля рациональных функций. Другая, более существенная трудность, возникающая при переходе от числовых к нечисловым полям, проявляется, в частности, в том, что различные нечисловые поля, вообще говоря, никак не связаны между собой: например, нельзя говорить о сумме элементов двух различных полей. Эту трудность удобнее всего преодолеть, ограничив класс рассматриваемых полей подполями некоторого достаточно широкого «универсального» поля. Именно на этом пути, выбирая за универсальное поле поле комплексных чисел, мы и приходим к числовым полям. В общем случае от универсального поля достаточно потребовать алгебраической замкнутости, т. е. потребовать, чтобы любой многочлен над этим полем разлагался в нем на линейные множители. Легко проверяется, что *вся излагаемая ниже теория остается справедливой без каких-либо изменений, если под полями понимать подполя некоторого фиксированного, но в остальном произвольного алгебраически замкнутого поля характеристики* 0.

## 2. Некоторые важные типы расширений

Расширение $K$ поля $P$ называется *конечным*, если в поле $K$ существуют такие элементы $\alpha_1, \ldots, \alpha_n$, что любой элемент $\beta \in K$ единственным образом записывается в виде линейной комбинации этих элементов с коэффициентами из поля $P$:

$$\beta = b_1\alpha_1 + \ldots + b_n\alpha_n, \quad b_1, \ldots, b_n \in P.$$

Обладающая этим свойством система элементов $\alpha_1, \ldots, \alpha_n$ называется *базисом* поля $K$ над полем $P$.

К понятию конечного расширения можно подойти и с другой стороны, заметив, что любое расширение $K$ поля $P$ можно рассматривать как линейное пространство над полем $P$. Действительно, элементы поля $K$ можно складывать и умножать на элементы поля $P$, причем обе операции (сложение и умножение на элементы поля $P$), очевидно, обладают всеми необходимыми свойствами. С этой точки зрения, расширение $K$ тогда и только тогда конечно, когда оно имеет конечную размерность (как линейное пространство над полем $P$), а си-

стема элементов тогда и только тогда является его базисом (в только что определенном смысле), когда она является его базисом в смысле теории линейных пространств. Так как все базисы конечномерного линейного пространства состоят из одного и того же числа векторов, то, в частности, все базисы поля $K$ над полем $P$ состоят из одного и того же числа элементов. Это число называется *степенью* поля $K$ над полем $P$ и обозначается через $[K:P]$ (с точки зрения теории линейных пространств, степень поля $K$ это его размерность как линейного пространства над полем $P$).

Задача. Доказать, что степень $[K:P]$ тогда и только тогда равна единице, когда $K=P$.

Пусть $P$ — произвольное поле (числовое) и $\alpha_1, \ldots, \alpha_n$ — произвольные числа (т. е. элементы поля $C$). Рассмотрим всевозможные поля, являющиеся расширениями поля $P$ и содержащие числа $\alpha_1, \ldots, \alpha_n$. Такие поля существуют, ибо, например, к их числу принадлежит поле $C$ всех комплексных чисел. Легко видеть, что пересечение всех этих полей также является полем (вообще, без труда доказывается, что пересечение любой системы полей само является полем). Это пересечение является, очевидно, минимальным расширением поля $P$, содержащим числа $\alpha_1, \ldots, \alpha_n$ (минимальность означает, что это пересечение является подполем любого другого, содержащего числа $\alpha_1, \ldots, \alpha_n$ расширения поля $P$). Это минимальное расширение обозначается через $P(\alpha_1, \ldots, \alpha_n)$ и называется расширением, *порожденным* числами $\alpha_1, \ldots, \alpha_n$.

Очевидно, что $P(\alpha_1, \ldots, \alpha_n)=P$ тогда и только тогда, когда $\alpha_1, \ldots, \alpha_n \in P$.

Задача. Доказать, что поле $P(\alpha_1, \ldots, \alpha_n)$ можно определить как совокупность всех чисел, получающихся в результате применения к числам поля $P$ и числам $\alpha_1, \ldots, \alpha_n$ всевозможных комбинаций четырех арифметических действий.

Число $\alpha$ называется *алгебраическим над полем* $P$, если оно является корнем некоторого (не равного тождественно нулю) многочлена с коэффициентами из поля $P$. Любой элемент поля $P$, очевидно, алгебраичен над этим полем (если верно и обратное, т. е. если любое алгебраическое над полем $P$ число принадлежит этому полю, то $P$ называется алгебраически замкнутым полем; ср. п. 1). Очевидно, далее, что любое число, алгебраическое над полем $P$, является алгебраическим числом и над любым расширением поля $P$,

Подчеркнем, что обратное утверждение, вообще говоря, неверно. Например, любое комплексное число является алгебраическим над полем $D$ действительных чисел (ибо оно является корнем квадратного трехчлена с действительными коэффициентами), тогда как существуют числа (даже действительные), не алгебраические над полем $R$ рациональных чисел. В качестве примера неалгебраических над полем $R$ чисел можно указать известные числа $e$ и $\pi$, неалгебраичность которых доказывается в полных курсах теории чисел.

*Расширение $K$ поля $P$ называется алгебраически порожденным*, если оно порождается некоторой конечной системой алгебраических над полем $P$ чисел, т. е. если существуют такие алгебраические над полем $P$ числа $\alpha_1, \ldots, \alpha_s$, что $K = P(\alpha_1, \ldots, \alpha_n)$. Если, в частности, $s = 1$, то поле $K = P(\alpha_1)$ называется *простым алгебраическим расширением поля $P$*.

Расширение $K$ поля $P$ называется *составным алгебраическим расширением*, если существует такая цепочка подполей

$$P = L_0 \subset L_1 \subset \ldots \subset L_{s-1} \subset L_s = K,$$

*начинающаяся с поля $P$ и кончающаяся полем $K$, что для* любого $i = 1, \ldots, s$ поле $L_i$ является простым алгебраическим расширением поля $L_{i-1}$. Если $L_i = L_{i-1}(\alpha_i)$, $i = 1, \ldots, s$, то поле $K$ обозначается через $P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$. Подчеркнем, *что алгебраичность чисел $\alpha_2, \ldots, \alpha_s$ под полем $P$* в этом определении не предполагается.

Наконец, расширение $K$ поля $P$ называется *алгебраическим*, если любой его элемент является числом алгебраическим над полем $P$.

Таким образом, мы ввели следующие пять типов расширения:

1) конечные расширения;
2) алгебраически порожденные расширения;
3) составные алгебраические расширения;
4) простые алгебраические расширения;
5) алгебраические расширения.

В этой главе мы изучим соотношения, имеющиеся между этими типами расширений, а также строение расширений каждого из этих типов (кроме, впрочем, последнего).

## 3. Минимальный многочлен. Строение простых алгебраических расширений

Пусть $P$ — произвольное поле и $\alpha$ — алгебраическое над полем $P$ число. По определению, число $\alpha$ является корнем некоторого многочлена над полем $P$. Многочлен $f(x)$, имеющий наименьшую степень среди всех многочленов с этим свойством, называется *минимальным многочленом* алгебраического числа $\alpha$. Этот многочлен неприводим, ибо в противном случае число $\alpha$ было бы корнем хотя бы одного его делителя меньшей степени, что по условию невозможно. Любой многочлен, корнем которого является число $\alpha$, не взаимно прост с минимальным многочленом $f(x)$ и, следовательно, делится на этот многочлен. В частности, неприводимый многочлен с корнем $\alpha$ может отличаться от минимального многочлена лишь постоянным множителем. Другими словами, неприводимый многочлен с корнем $\alpha$ определен однозначно (с точностью до постоянного множителя). Степень $n$ этого многочлена называется *степенью алгебраического числа* $\alpha$ над полем $P$. Степень $n$ равна единице тогда и только тогда, когда $\alpha \in P$.

Пусть $\alpha$ — алгебраическое над полем $P$ число, $f(x)$ — его минимальный многочлен и $n$ — его степень. Рассмотрим множество $K$ всех чисел $\beta$, для каждого из которых существует такой многочлен $g(x)$ над полем $P$, что $\beta = g(\alpha)$. Очевидно, что

$$K \subset P(\alpha).$$

Докажем, что $K$ является полем. Так как сумма, разность и произведение любых элементов из $K$, очевидно, снова принадлежат $K$, то нужно только доказать, что для любого отличного от нуля числа $\beta \in K$ число $\beta^{-1}$ также принадлежит $K$.

По определению,

$$\beta = g(\alpha),$$

где $g(x)$ — некоторый многочлен над полем $P$. Поскольку $g(\alpha) \neq 0$, то многочлен $g(x)$ не делится на многочлен $f(x)$ и, следовательно (в силу неприводимости многочлена $f(x)$), многочлены $g(x)$ и $f(x)$ взаимно просты. Поэтому, согласно известной теореме (см. Курс, стр. 197), над полем $P$

существуют такие многочлены $u(x)$ и $v(x)$, что

$$f(x)\,u(x)+g(x)\,v(x)=1.$$

Полагая в этом равенстве $x=\alpha$, мы получим:

$$\beta v(\alpha)=1,$$

т. е. $\beta^{-1}=v(\alpha)$, так что $\beta^{-1}\in K$.

Таким образом, множество $K$ действительно является полем. Так как, по определению, $P\subset K$ и $\alpha\in K$, то $K$ является расширением поля $P$, содержащим число $\alpha$. Поэтому в силу минимальности поля $P(\alpha)$:

$$P(\alpha)\subset K.$$

Сопоставляя это включение с включением $K\subset P(\alpha)$, мы получаем, что

$$K=P(\alpha).$$

Тем самым мы доказали, что *для любого элемента* $\beta$ *поля* $P(\alpha)$ *найдется такой многочлен* $g(x)$ *над полем* $P$, *что* $\beta=g(\alpha)$. Этот многочлен определен неоднозначно, ибо к нему можно прибавить любой многочлен, делящийся на многочлен $f(x)$. Другими словами, если разность $g(x)-g_1(x)$ делится на многочлен $f(x)$, то $g(\alpha)=g_1(\alpha)$. Обратно, если $g(\alpha)=g_1(\alpha)$, то многочлены $g(x)-g_1(x)$ и $f(x)$ не взаимно просты (ибо они имеют общий корень $\alpha$) и, следовательно, многочлен $g(x)-g_1(x)$ делится на многочлен $f(x)$. Таким образом,

$$g(\alpha)=g_1(\alpha)$$

*тогда и только тогда, когда разность* $g(x)-g_1(x)$ *делится на многочлен* $f(x)$.

В частности, если $r(x)$ — остаток от деления многочлена $g(x)$ на многочлен $f(x)$, то $g(\alpha)=r(\alpha)$. Следовательно, любой элемент поля $P(\alpha)$ можно представить в виде $r(\alpha)$, где степень многочлена $r(x)$ меньше $n$ (т. е. меньше степени многочлена $f(x)$). Другими словами, для любого элемента $\beta\in P(\alpha)$ существуют такие элементы $b_0, b_1, \ldots, b_{n-1}\in P$ (коэффициенты многочлена $r(x)$), что

$$\beta=b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}. \qquad (1)$$

Так как разность $r(x)-r_1(x)$, где $r(x)$ и $r_1(x)$ — многочлены степени, меньшей $n$, делится на многочлен $f(x)$ сте-

пени $n$ только тогда, когда $r(x)=r_1(x)$, то это представление однозначно. Таким образом, любой элемент $\beta$ поля $P(\alpha)$ однозначно записывается в виде (1). Другими словами, *элементы*

$$1, \alpha, \ldots, \alpha^{n-1}$$

*образуют базис поля* $P(\alpha)$ над полем $P$. Следовательно, *простое алгебраическое расширение* $P(\alpha)$ *является конечным расширением и его степень* $[P(\alpha):P]$ *равна степени числа* $\alpha$. Иначе говоря, класс расширений типа 4) содержится в классе расширений типа 1).

## 4. Алгебраичность конечных расширений

Пусть $\beta$ — произвольный элемент конечного расширения $K$ поля $P$ и пусть $[K:P]=n$. Так как в $n$-мерном линейном пространстве любые $n+1$ векторов линейно зависимы, то, в частности, элементы

$$1, \beta, \ldots, \beta^n$$

линейно зависимы над полем $P$, т. е. в $P$ существуют такие числа $c_0, c_1, \ldots, c_n$, среди которых хотя бы одно не равно нулю, что

$$c_0+c_1\beta+\ldots+c_n\beta^n=0.$$

Это означает, что число $\beta$ служит корнем многочлена

$$c_0+c_1x+\ldots+c_nx^n$$

и, следовательно, является алгебраическим (над полем $P$) числом. Тем самым доказано, что *любое конечное расширение алгебраично*, т. е. класс расширений типа 1) содержится в классе расширений типа 5).

Кроме того, мы получаем, что степень (над $P$) любого элемента конечного расширения $K$ поля $P$ не превосходит степени $n$ этого расширения.

Пусть теперь $\alpha_1, \ldots, \alpha_n$ — базис поля $K$ над полем $P$. Так как числа $\alpha_1, \ldots, \alpha_n$ являются, по доказанному, алгебраическими числами (над $P$), то порожденное ими расширение $P(\alpha_1, \ldots, \alpha_n)$ является алгебраически порожденным расширением. В силу минимальности этого расширения оно содержится в поле $K$:

$$P(\alpha_1, \ldots, \alpha_n)\subset K.$$

С другой стороны, так как из $\alpha_1, \ldots, \alpha_n \in P(\alpha_1, \ldots, \alpha_n)$ следует, что $b_1\alpha_1 + \ldots + b_n\alpha_n \in P(\alpha_1, \ldots, \alpha_n)$ для любых чисел $b_1, \ldots, b_n \in P$, то любой элемент поля $K$ содержится в поле $P(\alpha_1, \ldots, \alpha_n)$, т. е.

$$K \subset P(\alpha_1, \ldots, \alpha_n).$$

Следовательно,

$$K = P(\alpha_1, \ldots, \alpha_n).$$

Таким образом, доказано, что *любое конечное расширение является алгебраически порожденным*, т. е. класс расширений типа 1) содержится в классе расширений типа 2).

## 5. Строение составных алгебраических расширений

Пусть $K = P(\alpha_1)(\alpha_2)\ldots(\alpha_s)$ — составное алгебраическое расширение поля $P$. Оказывается, что любой элемент поля $K$ выражается в виде многочлена (над $P$) от $\alpha_1, \alpha_2, \ldots, \alpha_s$, т. е. что *для любого элемента* $\beta \in K$ *существует над полем* $P$ *такой многочлен* $g(x_1, \ldots, x_s)$ (*от* $s$ *неизвестных*), что

$$\beta = g(\alpha_1, \ldots, \alpha_s).$$

Мы докажем это утверждение индукцией по $s$. Если $s = 1$, то $K = P(\alpha_1)$, и, следовательно, в этом случае теорема справедлива (см. п. 3). Предполагая теперь, что теорема уже доказана для поля $L = P(\alpha_1)\ldots(\alpha_{s-1})$, рассмотрим произвольный элемент $\beta \in K$. Так как $K = L(\alpha_s)$, то над полем $L$ существует такой многочлен $h(x)$, что $\beta = h(\alpha_s)$. Пусть

$$h(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_n x^n, \quad \text{где } \gamma_0, \gamma_1, \ldots, \gamma_n \in L.$$

По предположению индукции для любого $i = 0, 1, \ldots, n$ найдется такой многочлен $h_i(x_1, \ldots, x_{s-1})$ (от $s-1$ неизвестных), что

$$\gamma_i = h_i(\alpha_1, \ldots, \alpha_{s-1}).$$

Следовательно, полагая

$$g(x_1, \ldots, x_s) = h_0(x_1, \ldots, x_{s-1}) + h_1(x_1, \ldots, x_{s-1})x_s + \ldots$$
$$\ldots + h_n(x_1, \ldots, x_{s-1})\,x_s^n,$$

мы получим, что

$$\beta = g(\alpha_1, \ldots, \alpha_s).$$

Тем самым наше утверждение полностью доказано.