

Э. АРТИН

Теория
Галуа

Э. АРТИН

ТЕОРИЯ ГАЛУА

Перевод с английского А. В. Самохина

Москва
Издательство МЦНМО
2004

УДК 512
ББК 22.14
А86

*Издание осуществлено при поддержке РФФИ
(издательский проект № 02-01-14082).*



Серия КЛАССИЧЕСКИЕ МОНОГРАФИИ: МАТЕМАТИКА

Артин Э.

А86 Теория Галуа / Пер. с англ. А. В. Самохина. — М.: МЦНМО, 2004. — 66 с. — (Классические монографии: математика).

ISBN 5-94057-062-3

В книге изложены основы теории Галуа. Она написана ясным языком, материал тщательно подобран, ее автор — известный математик. Впервые она была опубликована в 1944 г. и затем неоднократно переиздавалась. Отдельная глава посвящена вопросу о разрешимости алгебраических уравнений в радикалах и построению правильных многогранников с помощью циркуля и линейки.

Для студентов и аспирантов физико-математических специальностей.

ББК 22.14

ISBN 5-94057-062-3

© МЦНМО, перев. на русск. яз., 2004.

Предисловие к русскому изданию

Эмиль Артин (1898—1962) родился в Вене. В возрасте 18 лет он поступил в Венский университет, но проучившись там меньше года, попал в армию. После войны закончил Лейпцигский университет под руководством Герглотца и защитил диссертацию о квадратичных функциональных полях. Наиболее творческие годы он провел, преподавая в Гамбургском университете. Нацизм заставил его, как и множество других замечательных математиков, эмигрировать в 1937 году в Америку, где он создал еще большую научную школу, чем в Германии, особенно за годы преподавания в Принстоне. В 1958 году он вернулся в Гамбург.

Артин не был математиком-мономаном. Кроме математики он интересовался механикой, теорией относительности, химией, биологией, астрономией (он показывал ученикам телескоп, сделанный своими руками), хорошо знал и любил музыку (играл на флейте, фортепиано и клавесине).

Его вклад в алгебру, теорию чисел и топологию огромен. Он решил семнадцатую проблему Гильберта, открыл расширения Артина—Шрайера, закон взаимности Артина в теории полей классов, создал теорию кос, ввел артиновы кольца и разрешимые группы, предложил функциональный аналог гипотезы Римана (теперь теорема Хассе—Вейля), гипотезу Артина о примитивных корнях, гипотезу Артина о голоморфности L -рядов и многое другое.

Артин писал: «Математика — это искусство» и относил это в полной мере к книгам по математике. Он автор по меньшей мере шести классических книг: «Теория Галуа», «Кольца с условиями минимальности» (с Несбитом и Траллом), «Геометрическая алгебра» (имеется русский перевод), «Алгебраические числа и алгебраические функции», «Гамма-функция» и «Теория полей классов» (с Тейтом). Мне представляется, что самые замечательные из них — первая и последняя. Первая — перед вами.

М. А. Цфасман

Линейная алгебра

1.1. Тела

Телом¹⁾ называется множество, в котором заданы две операции — умножение и сложение, аналогичные умножению и сложению в множестве действительных чисел (которое является частным случаем тела). В любом теле F существуют однозначно определенные элементы — так называемые 0 и 1, которые взаимодействуют с другими элементами тела относительно операций умножения и сложения так же, как их аналоги в системе действительных чисел. Эта аналогия с действительными числами неполна в двух отношениях: 1) умножение не всегда предполагается коммутативным, 2) тело может иметь конечное число элементов.

Точнее говоря, тело — это множество, которое является аддитивной абелевой группой относительно вышеупомянутой операции сложения, а ненулевые элементы этого множества образуют группу по умножению. Наконец, эти две групповые операции связаны между собой законом дистрибутивности. Кроме того, произведение нуля с любым элементом тела полагается равным нулю.

Если умножение в теле коммутативно, то тело называется полем.

1.2. Векторные пространства

Аддитивная абелева группа V , элементы которой обозначаются через $A, B, \dots$, называется (*левым*) *векторным пространством* над телом F , элементы которого обозначаются $a, b, \dots$, если для каждой пары $a \in F$ и $A \in V$ определен элемент $a \cdot A$, принадлежащий группе V , и выполняются следующие условия:

$$\begin{aligned} 1) \quad a \cdot (A + B) &= a \cdot A + a \cdot B, & 3) \quad a \cdot (b \cdot A) &= (a \cdot b) \cdot A, \\ 2) \quad (a + b) \cdot A &= a \cdot A + b \cdot A, & 4) \quad 1 \cdot A &= A. \end{aligned}$$

Читатель без труда проверит, что если V — векторное пространство над F , то $0 \cdot A = 0$ и $a \cdot 0 = 0$. Например, первое соотношение следует из

¹⁾ В иностранной литературе кольцо, в котором всякий ненулевой элемент обратим, часто называется полем. Если же умножение в таком кольце коммутативно, то оно называется коммутативным полем. В русской же литературе поля принято называть телами, а коммутативные поля — полями. — *Прим. ред.*

уравнений

$$a \cdot A = (a + 0) \cdot A = a \cdot A + 0 \cdot A.$$

Иногда произведения элементов тела F с элементами пространства V записываются в виде $A \cdot a$. В этом случае мы называем V *правым векторным* пространством над F , чтобы подчеркнуть разницу с предыдущим случаем, когда элементы тела F действуют слева. В дальнейшем если левые и правые векторные пространства не встречаются одновременно, то мы будем просто использовать термин «векторное пространство».

1.3. Однородные линейные уравнения

Если в теле F заданы $m \cdot n$ элементов a_{ij} , $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$, то часто бывает необходимо знать условия, гарантирующие существование таких элементов тела F , что выполнены следующие равенства:

[illegible]

Читатель, возможно, помнит, что такие уравнения называются *линейными однородными*, а множество элементов $x_1, x_2, \dots, x_n$ тела F , для которых эти равенства верны, называется решением системы уравнений. Если не все элементы $x_1, x_2, \dots, x_n$ равны нулю, то решение называется *нетривиальным*; иначе оно называется *тривиальным*.

Теорема 1. Система линейных однородных уравнений всегда имеет нетривиальное решение, если число неизвестных превосходит число уравнений.

Доказательство этой теоремы проводится методом, знакомым большинству школьников старших классов, а именно, методом последовательного исключения неизвестных.

Если имеется пустое множество уравнений для n неизвестных, то на эти неизвестные нет никаких ограничений и мы полагаем их равными 1.

Далее будем действовать по полной индукции.

Предположим, что любая система из k уравнений с более чем k неизвестными имеет нетривиальное решение при $k < m$. Допустим, что для системы уравнений (3.1) выполняется неравенство $n > m$, и обозначим выражение $a_{i1}x_1 + \dots + a_{in}x_n$ через L_i , $i = 1, 2, \dots, m$. Мы ищем такие элементы $x_1, \dots, x_n$, не все равные нулю, что $L_1 = L_2 = \dots = L_m = 0$. Если $a_{ij} = 0$ для всех i и j , то любой набор $x_1, \dots, x_n$ будет решением. Если же не все a_{ij} равны нулю, то можно считать, что $a_{11} \neq 0$, перепорядочив переменные и уравнения подходящим образом. Существование нетривиального решения исходной системы уравнений равносильно

существованию нетривиального решения следующей системы:

$$\begin{aligned} L_1 &= 0, \\ L_2 - a_{21}a_{11}^{-1}L_1 &= 0, \\ &\dots\dots\dots \\ L_m - a_{m1}a_{11}^{-1}L_1 &= 0. \end{aligned}$$

Действительно если $x_1, \dots, x_n$ — решение последней системы уравнений, то, поскольку $L_1 = 0$, второй член каждого из оставшихся уравнений равен нулю, и тем самым $L_2 = L_3 = \dots = L_m = 0$. Обратно, если выполнено (3.1), то, очевидно, новая система имеет решение. Читатель может заметить, что новая система была подобрана таким образом, что переменная x_1 исключается из последних $m - 1$ уравнений. Кроме того, если существует нетривиальное решение последних $m - 1$ уравнений, рассматриваемых как система от переменных $x_2, \dots, x_n$, то, полагая $x_1 = -a_{11}^{-1}(a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n)$, мы получим решение исходной системы. Однако система из последних $m - 1$ уравнений имеет решение по индуктивному предположению, откуда и следует утверждение теоремы.

Замечание. Если бы мы записали линейные однородные уравнения в форме $\sum x_j a_{ij} = 0$, $j = 1, 2, \dots, n$, то теорема по-прежнему осталась бы верной и ее доказательство проходило бы без изменений.

1.4. Зависимость и независимость векторов

Векторы $A_1, \dots, A_n$ векторного пространства V над телом F называются *линейно зависимыми*, если существуют такие элементы этого тела $x_1, \dots, x_n$, не все равные нулю, что $x_1A_1 + x_2A_2 + \dots + x_nA_n = 0$. В противном случае векторы называются (*линейно*) *независимыми*.

Размерностью векторного пространства V над телом F называют максимальное число линейно независимых векторов в V . Так, размерность пространства V равна n , если в V есть n линейно независимых векторов, но любое множество из $(n + 1)$ векторов линейно зависимо.

Система векторов $A_1, \dots, A_m$ в V называется *системой образующих*, если любой вектор A из V может быть линейно выражен через $A_1, \dots, A_m$, т.е. $A = \sum_{i=1}^m a_i A_i$ для подходящих a_i , $i = 1, \dots, m$, $a_i \in F$.

Теорема 2. В любой системе образующих максимальное число линейно независимых векторов равно размерности векторного пространства.

Пусть $A_1, \dots, A_n$ — система образующих векторного пространства V размерности n . Обозначим через r максимальное число линейно независимых векторов в системе образующих. Переупорядочивая векторы

подходящим образом, мы можем считать, что $A_1, \dots, A_r$ линейно независимы. По определению размерности отсюда следует, что $r \leq n$. Для любого j векторы $A_1, \dots, A_r, A_{r+j}$ линейно зависимы и в равенстве

$$a_1 A_1 + a_2 A_2 + \dots + a_r A_r + a_{r+j} A_{r+j} = 0,$$

выражающем зависимость, коэффициент $a_{r+j} \neq 0$, ибо в противном случае мы получили бы противоречие с предположением о линейной независимости векторов $A_1, \dots, A_r$. Поэтому,

$$A_{r+j} = -a_{r+j}^{-1} [a_1 A_1 + a_2 A_2 + \dots + a_r A_r].$$

Следовательно, множество векторов $A_1, \dots, A_r$ также является системой образующих, так как в соотношении, представляющем любой вектор пространства V как линейную комбинацию векторов $A_1, \dots, A_n$, слагаемые, содержащие A_{r+j} , $j \neq 0$, можно заменить на линейные комбинации векторов $A_1, \dots, A_r$.

Пусть теперь $B_1, \dots, B_t$ — любой набор векторов пространства V , где $t > r$. Тогда существуют такие a_{ij} , что $B_j = \sum_{i=1}^r a_{ij} A_i$, $j = 1, 2, \dots, t$, поскольку A_i — система образующих. Если мы сможем показать, что $B_1, \dots, B_t$ линейно зависимы, то мы получим оценку $r \geq n$ и тем самым, учитывая неравенство $r \leq n$, доказанное выше, получим доказательство теоремы. Таким образом, мы должны предъявить нетривиальное решение уравнения

$$x_1 B_1 + x_2 B_2 + \dots + x_t B_t = 0,$$

где $x_i \in F$. С этой целью найдем значения x_i , которые удовлетворяют системе линейных уравнений $\sum_{j=1}^t x_j a_{ij} = 0$, $i = 1, 2, \dots, r$. Этого будет достаточно, потому что выражения в левой части уравнений суть коэффициенты при A_i в сумме $\sum_{j=1}^t x_j B_j$, где B_j заменены на $\sum_{i=1}^r a_{ij} A_i$ и приведены подобные слагаемые. Но нетривиальное решение системы $\sum_{j=1}^t x_j a_{ij} = 0$, $i = 1, 2, \dots, r$, всегда существует по теореме 1.

Замечание. Любые n независимых векторов $A_1, \dots, A_n$ в векторном пространстве размерности n являются системой образующих. Для любого вектора A векторы $A, A_1, \dots, A_n$ зависимы и коэффициент при A в линейном соотношении не может быть равен нулю. Выражая A через $A_1, \dots, A_n$, мы видим, что $A_1, \dots, A_n$ — система образующих.

Подмножество векторного пространства называется *подпространством*, если оно является подгруппой пространства, рассматриваемого

Предисловие к русскому изданию	3
Глава 1. Линейная алгебра	4
1.1. Тела	4
1.2. Векторные пространства	4
1.3. Однородные линейные уравнения	5
1.4. Зависимость и независимость векторов	6
1.5. Неоднородные линейные уравнения	10
1.6. Определители	11
Глава 2. Теория полей	19
2.1. Расширения полей	19
2.2. Многочлены	20
2.3. Алгебраические элементы	22
2.4. Поля разложения	25
2.5. Однозначное разложение многочленов на неприводимые со- множители	28
2.6. Характеры групп	28
2.7. Приложения и примеры к теореме 13	31
2.8. Нормальные расширения	34
2.9. Конечные поля	40
2.10. Корни из единицы	45
2.11. Уравнения Нётер	46
2.12. Куммеровы расширения	47
2.13. Простые расширения	51
2.14. Существование нормального базиса	52
2.15. Теорема о естественных иррациональностях	53
Глава 3. Приложения (А. Н. Мильграм)	55
3.1. Разрешимые группы	55
3.2. Группы перестановок	56
3.3. Разрешимость уравнений в радикалах	57
3.4. Общее уравнение степени n	58
3.5. Разрешимые уравнения простой степени	60
3.6. Построения с помощью циркуля и линейки	63

Эмиль Артин
ТЕОРИЯ ГАЛУА

Редакторы А. Г. Кузнецов, О. А. Васильева

Лицензия ИД № 01335 от 24.03.2000 г. Подписано в печать 5.04.2004 г.

Формат $60 \times 90 \frac{1}{16}$. Бумага офсетная № 1.

Печать офсетная. Печ. л. 4,25. Тираж 1000 экз. Заказ № .

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241–05–00.

Отпечатано с готовых диапозитивов во ФГУП «Полиграфические ресурсы».

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. 241–72–85. E-mail: biblio@mcsme.ru
