Н.Г. Чеботарев

Основы теории Галуа

Часть 2

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Н11

Н.Г. Чеботарев
Н11 Основы теории Галуа: Часть 2 / Н.Г. Чеботарев – М.: Книга по Требованию, 2019. – 161 с.

ISBN 978-5-458-25760-2

Настоящая книга является продолжением первой части "Основ теории Галуа". Она посвящена исследованию свойств алгебраических чисел в связи с теорией Галуа. Предлагаемый материал содержит элементы теории алгебраических чисел и идеалов, а также элементы аналитической теории идеалов, доведенные до определения плотности простых чисел, принадлежащих к отдельным классам подстановок (автоморфизмов поля). Предназначена для научных работников математиков, физиков-теоретиков, аспирантов и студентов естественных вузов.

ISBN 978-5-458-25760-2

ПРЕДИСЛОВИЕ

Настоящая вторая часть „Основ теории Галуа" должна была по замыслу содержать все главнейшие современные результаты, посвященные приложениям теории Галуа к алгебраическим числам, и поэтому должна была содержать теорию абелевых полей, в частности полей классов, а также теорию алгебр (или гиперкомплексных чисел) в приложении к полям классов. Однако оказалось, что методическая обработка имеющегося по этим вопросам журнального материала потребует много времени и повлечет за собой дальнейшую задержку выхода в свет этой части книги. В виду этого я решил опубликовать в виде отдельной книги эту часть, содержащую элементы теории алгебраических чисел и идеалов, но пронизанную связью с теорией Галуа, а также элементы аналитической теории идеалов, доведенные до определения плотности простых чисел, принадлежащих к отдельным классам подстановок (автоморфизмов поля).

Выход в свет теории алгебраических чисел отдельной книгой может быть оправдан особенно потому, что книг на русском языке по теории чисел почти нет. Существуют лишь: литографированный курс Д. А. Граве, Арифметическая теория алгебраических величин, ч. I — Квадратичная область, Вельмин, Теория алгебраических чисел, являющаяся почти библиографической редкостью, и недавно вышедший на украинском языке перевод книги Гекке (E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen).

Однако и во всей мировой литературе трудно указать книгу, которая по материалу была бы близка к этой книге. Почти все выходящие теперь книги по теории алгебраических чисел избегают ставить ее в связь с теорией групп и теорией Галуа; книга Гекке ограничивается случаем абелевых групп. Ближе всего материал настоящей книги лежит к материалу второго тома „Учебника алгебры" Вебера (H. Weber), но содержит много упрощений, выработанных после 1899 г., когда вышла книга Вебера (например несравненно проще доказана теорема Кронекера-Вебера; геометрическая теорема Минковского заменена простой алгебраической теоремой Гурвица), а также более поздние результаты, например о плотностях простых чисел (Фробениус), каковые у Вебера изложены только для случая абелевых полей (теорема Дирихле о простых числах в арифметической прогрессии).

Книга состоит из двух глав. Первая посвящена элементарной теории идеалов. Обычно все курсы теории идеалов принимают за основу или Кронекеровскую теорию функционалов (Вебер) или Дедекиндову теорию модулей (Дирихле-Дедекинд, Бахман, Ландау, Гекке); я выбрал теорию Золотарева, которая быстрее вводит читателя в курс дела и отличается большей наглядностью. В дальнейшем я доказал эквивалентность определений Золотарева и Дедекинда.

В § 5-я привожу новое доказательство теоремы Дедекинда о критических простых числах. Это простое по идее доказательство пользуется аппаратом теории Галуа, в частности теоремой Силова из теории групп.

В §§ 6—7 доказывается теорема Минковского при помощи леммы Гурвица, доказательство которой проводится более подробно, чем у самого Гурвица.

В § 8 вводится понятие группы инерции, при помощи которого из теоремы Минковского легко выводится так называемая теорема монодромин, с помощью которой многие формулировки и выводы значительно упрощаются.

В § 9 доказана теорема Кронекера-Вебера об абелевых полях и полях деления круга. В общем доказательство построено по Гильберту. Для наиболее трудного случая иррегулярных критических чисел доказательство заменено новым, идея которого принадлежит Фуэтеру (R. Fueter).

§§ 10—12 посвящены группе разложения с приложением к выводу теоремы Штикельбергера-Вороного, а также к выводу квадратичного закона взаимности по Мириманову и Гензелю (K. Hensel).

Глава вторая, посвященная аналитической теории идеалов, имеет целью получение результатов аналитической теории, которые имеют важные приложения в общей теории идеалов. Руководствуясь этим принципом выбора, я избегал помещения результатов, касающихся тонкостей оценки остаточных членов, и не поместил весьма важной формулы Гекке, как не имеющей непосредственного приложения к излагаемым вопросам приложения теории Галуа к алгебраическим числам.

В § 1 доказывается конечность числа идеальных классов и излагается связь эквивалентности идеалов с подобием соответствующих матриц (см. Шур).

§ 2 посвящен теории единиц алгебраического поля, изложенной по ван-дер-Вардену (B. L. van der Waerden). Здесь в виде примера изложена связь единиц вещественного квадратичного поля с непрерывными дробями.

В § 3 изложена теория Дирихле о простых числах в арифметической прогрессии. Вместо доказательства необращения в нуль выражений h (1) я, руководствуясь примером Вебера, отсылаю читателей к следующему параграфу, в котором тот же результат получается при помощи рассмотрения высших полей деления круга.

§ 4 посвящен рассмотрению Дедекиндовой ζ-функции и содержит доказательство результата Кронекера о существовании бесчисленного множества простых идеалов первой степени.

В § 5 выводится результат Фробениуса относительно простых чисел, принадлежащих к отделам подстановок группы Галуа поля.

В § 6 результат Фробениуса обобщается на классы подстановок. Изложение значительно отличается от изложения первоначальной журнальной статьи. Внесены упрощения, предложенные М. Ф. Кравчуком и Шрейером (O. Schreier).

Характер изложения второй части отличается от такового в первой большей сжатостью, неизбежно связанной с обилием материала и с тем, что вторая часть предназначена для более высокого уровня читателей, главным образом для специалистов по алгебре и теории чисел и для аспирантов, пишущих диссертации в этой области.

Н. Чеботарев.

ВВЕДЕНИЕ

Как мы видели в первой части, теория Галуа дает возможность привести изучение ряда свойств полей алгебраических чисел, в первую очередь перечисление всевозможных делителей этих полей, к изучению структуры групп этих полей, состоящих из конечного числа элементов. Но, как известно, структура группы Галуа не определяет всех его свойств: имеется немалое число арифметических свойств этих полей, не определяемых вполне их группами, но тем не менее стоящих в тесной связи с последними. Я позволю себе привести в виде примера такой связи замечательную теорему, впервые высказанную Кронекером (Kronecker) и доказанную Вебером (H. Weber):

> Всякое поле, группа Галуа которого абелева (будет говорить: *абелево поле*), если область рациональности есть поле рациональных чисел, является *полем деления* круга, т. е. его величины рационально выражаются через некоторые корни из единиц).

Эта часть „Основ теории Галуа" как раз имеет в виду изложить эту связь. Для этого необходимо глубокое знакомство с арифметикой алгебраических полей, каковой и посвящается главным образом настоящая книга.

Глава I

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ИДЕАЛОВ

§ 1. Целые алгебраические числа

1. *Целым алгебраическим* числом называется число, удовлетворяющее неприводимому уравнению с целыми рациональными коэфициентами, причем коэфициент при старшем члене равен единице.

2. Докажем, что число, являющееся корнем какого бы то ни было уравнения с целыми рациональными коэфициентами и единицей при старшем члене, есть целое алгебраическое число, т. е. что то неприводимое уравнение, корнем которого является это число, будет того же типа. Для этого достаточно доказать следующую теорему Гаусса:

Теорема 1. Если полином $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$ с целыми рациональными коэфициентами разлагается на два множителя с рациональными коэфициентами: $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n = (b_0 + b_1 x + \ldots + b_{u-1} x^{u-1} + x^u)(c_0 + c_1 x + \ldots + c_{v-1} x^{v-1} + x^v)$; $(u + v = n)$, то коэфициенты b_i, c_j этих множителей суть тоже целые рациональные числа.

Доказательство. Допустим противное: пусть коэфициенты, представленные в виде несократимых дробей, содержат в знаменателях простой множитель p самое большее в s-ой степени $(s > 0)$, и пусть b_k будет первый из этих коэфициентов, содержащих в знаменателях точно p^s. Пусть также коэфициенты c_j содержат в своих знаменателях p самое большее в t-ой степени $(t \geqq 0)$ и пусть c_r будет первый из этих коэфициентов, содержащих в своих знаменателях точно p^t. Рассмотрим коэфициент a_{k+r}:

$$a_{k+r} = b_k c_r + b_{k+1} c_{r-1} + \ldots + b_{k-1} c_{r+1} + \ldots$$

В этом выражении слагаемое $b_k c_r$ будет содержать в знаменателе точно p^{s+t}, в то время как остальные слагаемые должны содержать в знаменателях меньшие, чем $(s+t)$-ая степени. В самом деле, слагаемые первой строки суть произведения чисел b_{k+t}, содержащих в знаменателях p в степенях $\leqq s$,

и чисел c_{r-i}, содержащих в знаменателях p в степенях $<t$ (в случае $t=0$ мы должны полагать $r=0$, так что этих слагаемых вовсе не будет). Слагаемые же второй строки суть произведения чисел b_{k-i}, содержащих в знаменателях p в степенях $<s$, и чисел c_{r+i}, содержащих в знаменателях p в степенях $\leqq t$. Таким образом, дробная часть слагаемого $b_k c_r$ не может быть уничтожена прибавлением остальных слагаемых, и сумма a_{k+r} должна быть равна дробному числу, что противоречит условию. Таким образом, коэфициенты b_i, c_j должны быть целыми числами, что и требовалось доказать.

Следствие. Рациональное целое алгебраическое число есть целое рациональное число.

3. Имеет место

Теорема 2. Сумма и произведение двух или нескольких целых алгебраических чисел есть целое алгебраическое число.

Доказательство. Докажем более общую теорему: если α, β — целые алгебраические числа, удовлетворяющие соответственно уравнениям

$$x^m + a_1 x^{m-1} + \quad . + a_{m-1} x + a_m = 0 \qquad (1.1)$$

$$y^n + b_1 y^{n-1} + \quad . + b_{n-1} y + b_n = 0 \qquad (1.2)$$

с целыми рациональными коэфициентами, то $\varphi(\alpha, \beta)$, где $\varphi(x, y)$ есть произвольный целочисленный полином, есть целое алгебраическое число. Очевидно, что теорема легко распространяется на случай большего числа целых алгебраических чисел.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_m$ и $\beta_1, \beta_2, \ldots, \beta_n$ будут полные системы корней соответственно уравнений (1.1) и (1.2). Из свойств этих уравнений следует, что элементарно-симметрические функции от этих систем суть целые алгебраические числа. Но $\varphi(\alpha, \beta)$ является корнем уравнения

$$F(u) = \prod_{i=1}^{m} \prod_{j=1}^{n} \{u - \varphi(\alpha_i, \beta_j)\} = 0. \qquad (1.3)$$

Вместе с тем в части I, стр. 63,3° мы убедились, что всякий целочисленный симметрический полином от корней выражается целочисленным полиномом от их элементарно-симметрических функций. Поэтому все коэфициенты при различных степенях u полинома $F(u)$ являются целыми рациональными числами, а коэфициент при u^{mn} равен единице. Из теоремы 1 следует, что $\varepsilon(\alpha, \beta)$ есть целое алгебраическое число, ч. и т. д.

4. Отметим еще одну теорему:

Теорема 3. Если ω есть корень уравнения $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$, коэфициенты которого суть целые алгебраические числа, то ω есть целое алгебраическое число.

Доказательство. Будем называть сопряженным с $f(x)$ полиномом такой полином $f^{(k)}(x)$, в котором хотя бы один коэфициент полинома $f(x)$ заменен сопряженной с ним величиной, т. е. другим корнем того неприводимого уравнения с рациональными коэфициентами, которому удовлетворяет этот полином. Тогда произведение

$$\Phi(x)=\prod_k f^{(k)}(x)$$

является полиномом с рациональными коэфициентами. Рассуждая так же, как при доказательстве теоремы 2, мы убедимся, что они должны быть целыми числами. Так как старший коэфициент в $\Phi(x)$ есть единица, то величина ω, являющаяся корнем уравнения $\Phi(x)=0$, есть в силу теоремы 1 целое алгебраическое число, ч. и т. д.

5. Из теоремы 2 следует, что совокупность целых (алгебраических) чисел рассматриваемого поля воспроизводится при сложении, вычитании и умножении, т. е. что сумма, разность и произведение двух чисел этой совокупности тоже принадлежат к совокупности. Такого рода совокупности называются *кольцами*. В дальнейшем мы познакомимся с другими примерами колец.

6. Пусть величина α удовлетворяет неприводимому уравнению

$$x^n+a_1x^{n-1}+\quad\quad+a_{n-1}x+a_n=0.$$

Все корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ этого уравнения образуют систему *сопряженных с* α величин. Среди их элементарно-симметрических функций особо важное значение имеют две, для которых введены специальные наименования и обозначения. *Следом* величины α называется сумма

$$S(\alpha)=\alpha_1+\alpha_2+\ldots+\alpha_n. \tag{1.4}$$

Нормой величины α называется произведение

$$N(\alpha)=\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_n. \tag{1.5}$$

Рассмотрим поле $K(\alpha)$, образованное рациональными функциями с рациональными коэфициентами от α. Известно (см. часть 1, стр. 73, теорема 46, и стр. 74, теорема 48), что полином

$$g(t)=[t-R(\alpha_1)]\,[t-R(\alpha_2)]\ldots[t-R(\alpha_n)],$$

где $R(\alpha)$ — произвольная рациональная функция от α — есть степень неприводимого полинома от t, которая просто равна неприводимому полиному в том и только в том случае, если $\Theta=R(\alpha)$ есть *примитивная величина* поля, т. е. если α, а с нею любая величина поля $K(\alpha)$, рационально выражается через Θ. Если мы теперь условимся под следом и нормой величины $\Theta=R(\alpha)$ внутри $K(\alpha)$ разуметь соответственно величины

$$\begin{aligned} S[R(\alpha)]&=R(\alpha_1)+R(\alpha_2)+\ \ldots+R(\alpha_n)\\ N[R(\alpha)]&=R(\alpha_1)\ \ R(\alpha_2)\qquad\cdot R(\alpha_n)\end{aligned}$$

(так что, например, для рациональной величины a мы имеем $S(a)=n\cdot a$, $N(a)=a^n$), то имеют место следующие формулы

$$S(\alpha+\beta)=S(\alpha)+S(\beta) \tag{1.6}$$
$$N(\alpha\cdot\beta)=N(\alpha)\cdot N(\beta). \tag{1.7}$$

7. В заключение отметим одну полезную для дальнейшего формулу. Пусть примитивная величина α поля удовлетворяет неприводимому уравнению $f(x)=0$. Имеет место тождество

$$f(t)=(t-\alpha_1)(t-\alpha_2)\ldots(t-\alpha_n)=N(t-\alpha), \tag{1.8}$$

где t — произвольная (переменная) величина, которой можно придавать любые численные значения, если мы только условимся, что при переходе к сопряженным величинам в выражении $t-\alpha$ значение t будет оставаться неизменным.

§ 2. Базис и дискриминант поля

1. В части 1 (стр. 74, теорема 49) мы убедились, что всякую величину поля можно, и притом однозначно, представить в форме

$$c_0+c\alpha+\ldots+c_{n-1}\alpha^{n-1}, \tag{2.1}$$

где $c_0, c_1, \ldots, c_{n-1}$ — рациональные числа. Будем называть систему чисел $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ *базисом поля*, если всякая величина поля может быть представлена в форме

$$c_0\omega_0+c_1\omega_1+\ldots+c_{n-1}\omega_{n-1} \tag{2.2}$$

с рациональными *координатами* $c_0, c_1, \ldots, c_{n-1}$. Базис типа $[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$ будем называть *степенным базисом поля*.

2. Чтобы узнать, является ли заданная система чисел $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ базисом нашего поля, будем исходить из некоторого степенного базиса $[1, \alpha, \ldots, \alpha^{n-1}]$, где α — любая примитивная величина поля. Выразим элементы заданной системы при помощи степенного базиса:

$$\left.\begin{aligned}
\omega_0&=c_{00}+c_{01}\alpha+\ldots+c_{0,n-1}\alpha^{n-1},\\
\omega_1&=c_{10}+c_{11}\alpha+\ldots+c_{1,n-1}\alpha^{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\omega_{n-1}&=c_{n-1,0}+c_{n-1,1}\alpha+\ldots+c_{n-1,n-1}\alpha^{n-1}
\end{aligned}\right\} \tag{2.3}$$

Этот переход мы будем также записывать так:

$$[\omega_0, \omega_1, \ldots, \omega_{n-1}]=\begin{pmatrix} c_{0,0} & \ldots & c_{0,n-1}\\ \ldots & \ldots & \ldots\\ c_{n-1,0} & \ldots & c_{n-1,n-1}\end{pmatrix}[1, \alpha, \ldots, \alpha^{n-1}]. \tag{2.3'}$$

Теорема 4. Система $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ является базисом поля тогда и только тогда, если определитель $|c_{ik}|$ отличен от нуля.

Доказательство. 1. Условие достаточно. В самом деле, если $|c_{ik}| \neq 0$, то систему равенств можно разрешить относительно $1, \alpha, \ldots, \alpha^{n-1}$, и тогда каждая из этих величин будет линейно (с рациональными коэфициентами) выражаться через $\omega_0, \omega_1, \ldots, \omega_{n-1}$. В таком же виде сможет быть выражена и каждая их линейная комбинация (2.1), т. е. каждая величина нашего поля.

2. Условие необходимо. В самом деле, если $|c_{ik}| = 0$, то из равенств (2.3) следует, что величины $\omega_0, \omega_1, \ldots, \omega_{n-1}$ связаны зависимостью

$$b_0\omega_0 + b_1\omega_1 + \ldots + b_{n-1}\omega_{n-1} = 0 \qquad (2.4)$$

с рациональными коэфициентами, из которых хотя бы один, например b_{n-1}, не равен нулю. Предположим, что $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ есть базис. Тогда каждая из величин $1, \alpha, \ldots, \alpha^{n-1}$ линейно выразится через $\omega_0, \omega_1, \ldots, \omega_{n-1}$. В этих выражениях мы при помощи (2.4) можем в силу $b_{n-1} \neq 0$ освободиться от величины ω_{n-1}. Исключая из этих выражений $\omega_0, \omega_1, \ldots, \omega_{n-2}$ мы получим по крайней мере одну линейную зависимость между $1, \alpha, \ldots, \alpha^{n-1}$ с рациональными коэфициентами. Это, однако, противоречит неприводимости полинома n-ой степени, корнем которого является α.

Из приведенного рассуждения вытекает также следующий критерий для базиса:

Теорема 5. Для того чтобы система n чисел $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ была базисом поля n-ой степени, необходимо и достаточно, чтобы между $\omega_0, \omega_1, \ldots, \omega_{n-1}$ не имела места зависимость типа (2.4).

3. Чтобы получить критерий базиса, независимый от степенных базисов и эффективный, т. е. могущий быть примененным к примерам, введем понятие *дискриминанта* системы чисел $\omega_0, \omega_1, \ldots, \omega_{n-1}$. Обозначая числа, сопряженные с α, так: $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ [причем, если $\Theta = R(\alpha)$, то $R(\alpha^{(i)})$ мы будем обозначать через $\Theta^{(i)}$], рассмотрим определитель

$$\begin{vmatrix} \omega_0, & \omega_1, & \ldots, & \omega_{n-1} \\ \omega_0', & \omega_1', & \ldots, & \omega_{n-1}' \\ \cdot & \cdot & \cdot & \cdot \\ \omega_0^{(n-1)}, & \omega_1^{(n-1)}, & \ldots, & \omega_{n-1}^{(n-1)} \end{vmatrix}. \qquad (2.5)$$

Его квадрат мы и будем называть *дискриминантом системы* $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$. Помножив этот определитель сам на себя

(по колоннам), мы получим для дискриминанта следующее выражение:

$$\Delta[\omega_0, \omega_1, \ldots, \omega_{n-1}] = \begin{vmatrix} S(\omega_0\omega_0), & S(\omega_0\omega_1), & \ldots, S(\omega_0\omega_{n-1}) \\ S(\omega_1\omega_0), & S(\omega_1\omega_1), & \ldots, S(\omega_1\omega_{n-1}) \\ \cdots & \cdots & \cdots \\ S(\omega_{n-1}\omega_0), & S(\omega_{n-1}\omega_1), & \ldots, S(\omega_{n-1}\omega_{n-1}) \end{vmatrix}, \quad (2.6)$$

показывающее, что дискриминанты равны рациональным числам.

Нетрудно убедиться, что дискриминант степенного базиса $[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$ равен дискриминанту уравнения, корнем которого является α.

4. Даны базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ и система чисел $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$, выражаемых через базис так:

$$[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \begin{pmatrix} c_{00}, & \ldots, c_{0,n-1} \\ \cdots & \cdots \\ c_{n-1,0}, & \ldots, c_{n-1,n-1} \end{pmatrix} [\omega_0, \omega_1, \ldots, \omega_{n-1}].$$

Составляя для обеих систем определители (2.5), мы на основании теоремы об умножении определителей будем иметь:

$$\begin{vmatrix} 1 & \eta_0, & \ldots, \eta_{n-1} \\ \cdots & \cdots & \cdots \\ \eta_0^{(n-1)}, & \ldots, & \eta_{n-1}^{(n-1)} \end{vmatrix} =$$

$$= \begin{vmatrix} c_{00}, & \ldots, c_{0,n-1} \\ \cdots & \cdots \\ c_{n-1,0}, & \ldots, c_{n-1,n-1} \end{vmatrix} \cdot \begin{vmatrix} \omega_0, & \ldots, \omega_{n-1} \\ \cdots & \cdots \\ \omega_0^{(n-1)}, & \ldots, \omega_{n-1}^{(n-1)} \end{vmatrix}.$$

Возводя эту формулу в квадрат, мы приходим к следующей важной формуле:

$$\Delta[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \begin{vmatrix} c_{00}, & \ldots, c_{0,n-1} \\ \cdots & \cdots \\ c_{n-1,0}, & \ldots, c_{n-1,n-1} \end{vmatrix}^2 \cdot \Delta[\omega_0, \omega_1, \ldots, \omega_{n-1}]. \quad (2.7)$$

Беря в качестве $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ степенной базис $[1, \alpha, \ldots, \alpha^{n-1}]$ и принимая во внимание, что дискриминанты неприводимых уравнений, как не имеющих кратных корней, отличны от нуля, а также теорему 4, мы приходим к

Теореме 6. Система $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$ является базисом тогда и только тогда, если ее дискриминант отличен от нуля.

5. Если элементы базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ являются целыми алгебраическими числами, то в силу теоремы 2 все числа вида $c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$, где $c_0, c_1, \ldots, c_{n-1}$ — целые рациональные числа, суть целые алгебраические числа. Возникает вопрос, все ли целые алгебраические числа нашего поля мы