

состоящий из всех $a \in K$, бесконечно малых над F . Тогда \mathfrak{m} — единственный максимальный идеал в \mathfrak{o} , поскольку любой элемент из \mathfrak{o} , не лежащий в \mathfrak{m} , имеет обратный в \mathfrak{o} . Мы будем называть \mathfrak{o} кольцом нормирования, определенным упорядочением расширения K/F .

Предложение 1. Пусть K — упорядоченное поле, F — его подполе, \mathfrak{o} — кольцо нормирования, определенное упорядочением расширения K/F , и \mathfrak{m} — его максимальный идеал. Тогда $\mathfrak{o}/\mathfrak{m}$ — вещественное поле (см. § 2).

Доказательство. В противном случае мы имели бы равенство

$$-1 = \sum a_i^2 + a,$$

где $a_i \in \mathfrak{o}$ и $a \in \mathfrak{m}$. Но поскольку сумма $\sum a_i^2$ положительна, а элемент a бесконечно мал, это равенство, очевидно, невозможно.

§ 2. Вещественные поля

Поле K называется *вещественным*, если -1 не является суммой квадратов в K ¹⁾. Поле K называется *вещественно замкнутым*, если оно вещественное и любое его вещественное алгебраическое расширение совпадает с K . Другими словами, K является максимальным по отношению к свойству вещественности алгебраических замыканий.

Предложение 2. Пусть K — вещественное поле.

(i) Если $a \in K$, то либо $K(\sqrt{a})$, либо $K(\sqrt{-a})$ — вещественное поле. Если a — сумма квадратов в K , то поле $K(\sqrt{a})$ вещественное. Если поле $K(\sqrt{a})$ не является вещественным, то $-a$ есть сумма квадратов в K .

(ii) Если f — неприводимый многочлен нечетной степени n из $K[X]$ и a — корень f , то поле $K(a)$ вещественное.

Доказательство. Пусть $a \in K$. Если a — квадрат в K , то поле $K(\sqrt{a}) = K$ и, следовательно, является вещественным по условию. Предположим, что a не есть квадрат в K . Если поле $K(\sqrt{a})$ не вещественное, то существуют $b_i, c_i \in K$, такие, что

$$-1 = \sum (b_i + c_i \sqrt{a})^2 = \sum (b_i^2 + 2c_i b_i \sqrt{a} + c_i^2 a).$$

¹⁾ Принято говорить в таком случае о *формально вещественном* поле, но мы сохраним краткую терминологию автора, поскольку из контекста ясно, когда речь идет об обычном поле вещественных чисел. — Прим. ред.

Так как $1, \sqrt{a}$ линейно независимы над K , то отсюда вытекает, что

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Если a — сумма квадратов в K , то получаем противоречие. Во всяком случае,

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

есть частное сумм квадратов и, значит, в силу сделанного выше замечания $-a$ является суммой квадратов. Следовательно, поле $K(\sqrt{-a})$ вещественное, что доказывает наше первое утверждение.

Что касается второго, то предположим, что $K(a)$ не вещественное. Тогда мы можем записать

$$-1 = \sum g_i(a)^2,$$

где многочлены g_i из $K[X]$ имеют степени $\leq n - 1$. В $K[X]$ существует многочлен h , такой, что

$$-1 = \sum g_i(X)^2 + h(X)f(X).$$

Сумма $\sum g_i(X)^2$ имеет четную степень, и эта степень должна быть > 0 , так как иначе -1 была бы суммой квадратов в K . Степень эта $\leq 2n - 2$. Поскольку f имеет нечетную степень n , h имеет нечетную степень $\leq n - 2$. Мы видим, что если β — корень h , то -1 есть сумма квадратов в $K(\beta)$. Так как $\deg h < \deg f$, то доказательство завершается по индукции.

Пусть K — вещественное поле. Под *вещественным замыканием* поля K мы будем понимать вещественно замкнутое поле L , алгебраическое над K .

Теорема 1. Всякое вещественное поле K обладает вещественным замыканием. Вещественно замкнутое поле R имеет единственное упорядочение (а именно, положительные элементы в R — это суммы квадратов). Всякий положительный элемент в R является квадратом, и всякий многочлен нечетной степени из $R[X]$ имеет корень в R . Имеет место равенство $\bar{R} = R(\sqrt{-1})$

Доказательство. В силу леммы Цорна наше поле K содержится в некотором вещественно замкнутом поле, алгебраическом над K . Пусть теперь \bar{R} — вещественно замкнутое поле и P — множество не-нулевых элементов из \bar{R} , являющихся суммами квадратов. Тогда P замкнуто относительно сложения и умножения. В силу предложения 2 всякий элемент из P есть квадрат в \bar{R} и для данного элемента $a \in P$, $a \neq 0$, будет либо $a \in R$, либо $-a \in R$. Таким образом, P определяет упорядочение. Опять-таки в силу предложения 2 всякий многочлен нечетной степени над R имеет корень в R . Наше последнее утверждение вытекает из примера 5 гл VIII, § 2.

Следствие. Пусть K — вещественное поле и a — элемент из K , не являющийся суммой квадратов. Тогда существует упорядочение поля K , при котором элемент a отрицателен.

Доказательство. В силу предложения 2 поле $K(\sqrt{-a})$ вещественно и, следовательно, имеет упорядочение как подполе своего вещественного замыкания. Относительно этого упорядочения $-a > 0$ и, значит, a отрицателен.

Предложение 3. Пусть R — поле, такое, что $R \neq \bar{R}$ и $\bar{R} = R(\sqrt{-1})$. Тогда R вещественно и, следовательно, вещественно замкнуто.

Доказательство. Пусть P — множество элементов из R , которые являются квадратами и $\neq 0$. Мы утверждаем, что P есть упорядочение поля R . Действительно, пусть $a \in R$, $a \neq 0$. Предположим, что a не является квадратом в R . Пусть a — корень уравнения $X^2 - a = 0$. Тогда $R(a) = R(\sqrt{-1})$ и, следовательно, существуют $c, d \in R$, для которых $a = c + d\sqrt{-1}$. В таком случае

$$a^2 = c^2 + 2cd\sqrt{-1} - d^2.$$

Так как $1, \sqrt{-1}$ линейно независимы над R , то $c = 0$ (поскольку $a \notin R^2$) и, следовательно, $-a$ есть квадрат.

Теперь докажем, что сумма квадратов будет квадратом. Для простоты положим $i = \sqrt{-1}$. Поскольку поле $R(i)$ алгебраически замкнуто, для данных $a, b \in R$ мы можем найти $c, d \in R$, такие, что $(c + di)^2 = a + bi$. Тогда $a = c^2 - d^2$ и $b = 2cd$. Следовательно, $a^2 + b^2 = (c^2 + d^2)^2$.

Если $a \in R$, $a \neq 0$, то одновременно a и $-a$ не могут быть квадратами в R . Таким образом, P — упорядочение, и наше предложение доказано.

Теорема 2. Пусть R — вещественно замкнутое поле, $a, b \in R$ и $f(X)$ — многочлен из $R[X]$, причем $f(a) < 0$ и $f(b) > 0$. Тогда существует элемент с между a и b , для которого $f(c) = 0$.

Доказательство. Так как поле $R(\sqrt{-1})$ алгебраически замкнуто, то f разлагается над R в произведение неприводимых множителей степеней 1 и 2. Если многочлен $X^2 + aX + \beta$ неприводим ($a, \beta \in R$), то он является суммой квадратов, а именно

$$\left(X + \frac{a}{2}\right)^2 + \left(\beta - \frac{a^2}{4}\right),$$

так что $4\beta > a^2$. Следовательно, изменение знака f происходит за счет изменения знака какого-то линейного множителя, который, как тривиально проверяется, должен иметь корень, лежащий между a и b .

Лемма. Пусть K — подполе упорядоченного поля E и $a \in E$ — алгебраический элемент над K , являющийся корнем многочлена

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$$

с коэффициентами в K . Тогда $|a| \leq 1 + |a_{n-1}| + \dots + |a_0|$.

Доказательство. Если $|a| \leq 1$, то утверждение очевидно. Если $|a| > 1$, то выражаем $|a|^n$ через члены меньшей степени, делим на $|a|^{n-1}$ и получаем доказательство нашей леммы.

Отметим, что из этой леммы вытекает, что элемент, алгебраический над некоторым упорядоченным полем, не может быть бесконечно большим относительно этого поля.

Пусть $f(X)$ — многочлен с коэффициентами в вещественно замкнутом поле R , не имеющий кратных корней, и $u < v$ — элементы из R . Под последовательностью Штурма для f на интервале $[u, v]$ мы будем понимать упорядоченную систему многочленов

$$S = \{f = f_0, f' = f_1, \dots, f_m\},$$

обладающую следующими свойствами:

ШТ 1. Последний многочлен f_m является отличной от нуля константой.

ШТ 2. Ни для какого $0 \leq j \leq m-1$ не существует точки $x \in [u, v]$, такой, что $f_j(x) = f_{j+1}(x) = 0$.

ШТ 3. Если $x \in [u, v]$ и $f_j(x) = 0$ для некоторого $j = 1, \dots, m-1$, то $f_{j-1}(x)$ и $f_{j+1}(x)$ имеют противоположные знаки.

ШТ 4. Имеем $f_j(u) \neq 0$ и $f_j(v) \neq 0$ для всех $j = 0, \dots, m^1$.

Для любого элемента $x \in [u, v]$, не являющегося корнем ни для какого из многочленов f_j , мы будем обозначать через $W_S(x)$ число перемен знаков в последовательности

$$\{f(x), f_1(x), \dots, f_m(x)\}$$

и будем называть $W_S(x)$ вариацией знаков в этой последовательности.

Теорема Штурма. Число корней многочлена f , заключенных между u и v , равно разности $W_S(u) - W_S(v)$ для любой последовательности Штурма S .

Доказательство. Заметим, что если $a_1 < a_2 < \dots < a_r$ — упорядоченная последовательность корней многочленов f_j в $[u, v]$

¹⁾ Читатель заметит, что без специального выбора интервала $[u, v]$ выполнение этого условия при $j \neq 0$ не обеспечивается конструкцией системы. На самом деле его можно заменить условием возрастания произведения $f_0(x)f_1(x)$ при возрастании x в малой окрестности (относительно интервальной топологии) нуля a многочлена $f = f_0$. В определении вариации $W_S(\beta)$ нужно тогда потребовать $f(\beta) \neq 0$ и выбросить из последовательности $\{f_0(\beta), \dots, f_m(\beta)\}$ нулевые члены. — Прим. ред.

($j = 0, \dots, m - 1$), то вариация $W_S(x)$ постоянна в открытых интервалах между этими корнями (в силу теоремы 2). Следовательно, достаточно доказать, что если имеется точно один элемент a , такой, что $u < a < v$ и a есть корень некоторого f_j , то разность $W_S(u) - W_S(v)$ равна 1, когда a — корень f , и 0 в противном случае. Предположим сначала, что a — корень некоторого f_j для $1 \leq j \leq m - 1$. Тогда согласно ШТ З элементы $f_{j-1}(a), f_{j+1}(a)$ имеют противоположные знаки и эти знаки не изменяются при замене a на u или v . Следовательно, вариация знаков в последовательностях

$$\{f_{j-1}(u), f_j(u), f_{j+1}(u)\} \text{ и } \{f_{j-1}(v), f_j(v), f_{j+1}(v)\}$$

одна и та же, а именно равна 1. Таким образом, если a не является корнем f , то $W_S(u) = W_S(v)$. Если теперь a — корень f , то $f(u)$ и $f(v)$ имеют противоположные знаки, но $f'(u)$ и $f'(v)$ имеют один и тот же знак, а именно знак, совпадающий со знаком $f(v)$. Следовательно, в этом случае $W_S(u) = W_S(v) + 1$. Это доказывает нашу теорему.

Для многочлена без кратных корней последовательность Штурма строится без труда. Применяя алгоритм Евклида, получаем

$$\begin{aligned} f &= g_1 f' - f_2, \\ f_1 &= g_2 f_2 - f_3, \\ &\quad \cdot \cdot \cdot \cdot \cdot \cdot \\ f_{m-2} &= g_{m-1} f_{m-1} - f_m, \end{aligned}$$

где $f' = f_1$. Так как f, f' не имеют общих множителей, то последний член в этой последовательности будет отличной от нуля константой. Тривиально проверяются и другие свойства последовательности Штурма. Если бы, например, два последовательных многочлена в этой последовательности имели общий нуль, то он был бы нулем и для всех остальных многочленов, вопреки тому факту, что последний из них в 0 не обращается.

Следствие. Пусть K — упорядоченное поле, f — неприводимый многочлен над K степени ≥ 1 . Число корней f в двух вещественных замыканиях поля K , индуцирующих заданное упорядочение на K , одинаково.

Доказательство. Используя лемму, мы можем взять в качестве v достаточно большой положительный и в качестве u достаточно большой отрицательный элементы в K , так чтобы все корни f и все корни многочленов в последовательности Штурма лежали между u и v . Тогда $W_S(u) - W_S(v)$ будет равно общему числу корней f в любом вещественном замыкании поля K , индуцирующем заданное упорядочение.

Теорема 3. Пусть K — упорядоченное поле и R, R' — его вещественные замыкания, индуцирующие заданное упорядочение на K . Тогда существует однозначно определенный изоморфизм $\sigma: R \rightarrow R'$ над K , и этот изоморфизм сохраняет порядок.

Доказательство. Мы покажем сперва, что для данного конечного подрасширения E в R над K существует вложение E в R' над K . Пусть $E = K(a)$, и пусть $f(X) = \text{Irr}(a, K, X)$. Тогда $f(a) = 0$ и следствие теоремы Штурма показывает, что f имеет некоторый корень β в R' . Таким образом, существует изоморфизм $K(a)$ на $K(\beta)$ над K , отображающий a в β .

Пусть $\alpha_1, \dots, \alpha_n$ — различные корни f в R и β_1, \dots, β_n — различные корни f в R' , причем

$$\begin{aligned} \alpha_1 &< \dots < \alpha_n \text{ в упорядочении поля } R, \\ \beta_1 &< \dots < \beta_n \text{ в упорядочении поля } R'. \end{aligned}$$

Мы утверждаем, что можно выбрать вложение σ поля $K(a_1, \dots, a_n)$ в R' таким образом, что $\sigma\alpha_i = \beta_i$ для $i = 1, \dots, n$. Действительно, пусть γ_i — такой элемент из R , что

$$\gamma_i^2 = a_{i+1} - a_i \text{ при } i = 1, \dots, n-1,$$

и пусть $E_1 = K(a_1, \dots, a_n, \gamma_1, \dots, \gamma_{n-1})$. В силу только что доказанного существует вложение σ поля E_1 в R' , а тогда $\sigma\alpha_{i+1} - \sigma\alpha_i$ есть квадрат в R' . Следовательно,

$$\sigma\alpha_1 < \dots < \sigma\alpha_n.$$

Это доказывает, что $\sigma\alpha_i = \beta_i$ для $i = 1, \dots, n$. Кроме того, последнее условие полностью определяет действие σ на $K(a_1, \dots, a_n)$. Мы утверждаем, что σ сохраняет порядок. Действительно, пусть $y \in K(a_1, \dots, a_n)$, $0 < y$ и элемент $\gamma \in R$ таков, что $\gamma^2 = y$. Тогда существует вложение поля $K(a_1, \dots, a_n, \gamma_1, \dots, \gamma_{n-1}, \gamma)$ в R' над K , которое индуцирует σ на $K(a_1, \dots, a_n)$ и для которого σy есть квадрат, а, значит, как и утверждалось, $\sigma y > 0$.

Используя теперь лемму Цорна, мы, очевидно, получим изоморфизм R на R' над K . Этот изоморфизм сохраняет порядок, поскольку он отображает квадраты на квадраты. Тем самым теорема доказана.

Предложение 4. Пусть K — упорядоченное поле, K' — его расширение, в котором нет соотношений вида

$$-1 = \sum_{i=1}^n a_i a_i^2$$

с $a_i \in K$, $a_i > 0$, и $a_i \in K'$. Пусть L — поле, получающее из K' присоединением квадратных корней из всех положительных элементов поля K . Тогда L вещественно.

Доказательство. Если—нет, то существует соотношение типа

$$-1 = \sum_{i=1}^n a_i a_i^2$$

с $a_i \in K$, $a_i > 0$, и $a_i \in L$. (Мы можем взять $a_i = 1$.) Пусть r — наименьшее целое число, для которого мы можем записать указанное выше соотношение с a_i , лежащими в подполе поля L , имеющем вид

$$K'(\sqrt{b_1}, \dots, \sqrt{b_r}),$$

где $b_j \in K$, $b_j > 0$. Если

$$a_i = x_i + y_i \sqrt{b_r},$$

где

$$x_i, y_i \in K'(\sqrt{b_1}, \dots, \sqrt{b_{r-1}}),$$

то

$$-1 = \sum a_i (x_i + y_i \sqrt{b_r})^2 = \sum a_i (x_i^2 + 2x_i y_i \sqrt{b_r} + y_i^2 b_r).$$

По предположению $\sqrt{b_r}$ не лежит в $K'(\sqrt{b_1}, \dots, \sqrt{b_{r-1}})$. Следовательно,

$$-1 = \sum a_i x_i^2 + \sum a_i b_r y_i^2,$$

вопреки минимальности r .

Теорема 4. У всякого упорядоченного поля K существует вещественное замыкание R , индуцирующее заданное упорядочение на K .

Доказательство. Возьмем $K' = K$ в предложении 4. Тогда L вещественно и содержится в некотором вещественном замыкании. Наше утверждение теперь очевидно.

Следствие. Пусть K — упорядоченное поле и K' — его расширение. Для того чтобы существовало упорядочение на K' , индуцирующее заданное упорядочение поля K , необходимо и достаточно, чтобы отсутствовали соотношения типа

$$-1 = \sum_{i=1}^n a_i a_i^2,$$

где $a_i \in K$, $a_i > 0$ и $a_i \in K'$.

Доказательство. Если нет таких соотношений, то, согласно предложению 4, L вещественно и, значит, содержится в некотором вещественном замыкании, упорядочение которого индуцирует некоторое упорядочение на K' и заданное упорядочение на K , что и требовалось. Обратное очевидно.

ПРИМЕР. Пусть $\bar{\mathbf{Q}}$ — поле алгебраических чисел. Непосредственно видно, что \mathbf{Q} допускает только одно упорядочение, а именно обычное. Следовательно, любые два вещественных замыкания поля \mathbf{Q} в $\bar{\mathbf{Q}}$ изоморфны, причем соответствующий изоморфизм однозначно определен. Вещественные замыкания поля \mathbf{Q} в $\bar{\mathbf{Q}}$ исчерпываются в точности подполями в $\bar{\mathbf{Q}}$, над которыми $\bar{\mathbf{Q}}$ имеет конечную степень. Пусть K — конечное вещественное расширение поля \mathbf{Q} , содержащееся в $\bar{\mathbf{Q}}$. Элемент a из K тогда и только тогда будет суммой квадратов в K , когда положителен всякий элемент, сопряженный с a в поле вещественных чисел, или, что эквивалентно, в одном из вещественных замыканий поля \mathbf{Q} в $\bar{\mathbf{Q}}$.

Замечание. Теория, развитая в этом и предыдущем параграфах, принадлежит Артину — Шрейеру.

§ 3. Вещественные нули и гомоморфизмы

Подобно тому как мы развили теорию продолжения гомоморфизмов в алгебраически замкнутое поле и получили теорему Гильберта о нулях в алгебраически замкнутом поле, мы хотим теперь развить теорию для случая, когда принимаемые значения лежат в вещественно замкнутом поле. Одной из основных теорем будет следующая:

Теорема 5. Пусть k — поле, $K = k(x_1, \dots, x_n)$ — конечно порожденное расширение. Предположим, что k упорядочено. Пусть R_k — вещественное замыкание поля k , индуцирующее то же самое упорядочение на k , что и K . Тогда существует гомоморфизм

$$\varphi: k[x_1, \dots, x_n] \rightarrow R_k$$

над k .

В качестве приложений теоремы 5 получаем

Следствие 1. Пусть обозначения те же, что и в теореме, и пусть $y_1, \dots, y_m \in k[x]$, причем

$$y_1 < y_2 < \dots < y_m$$

в заданном упорядочении поля K . Тогда гомоморфизм φ можно выбрать таким образом, что

$$\varphi y_1 < \dots < \varphi y_m.$$