ЛЕКЦИЯ 17

ПОЛЯ

РАСШИРЕНИЕ ПОЛЕЙ

СУЩЕСТВОВАНИЕ ПОЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

ПРИМЕРЫ ПОЛЕЙ

Пример 1. Числовые поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ являются основными примерами полей для нас.

Пример 2. Для каждого простого числа p мы имеем поле вычетов $\mathbb{Z}_p$ из p элементов.

Пример 3. Поля из 4, 8, 9, 27 элементов легко строятся как

$$\mathbb{Z}_2[x]/(x^2+x+1), \quad \mathbb{Z}_2[x]/(x^3+x+1), \quad \mathbb{Z}_3[x]/(x^2+1), \quad \mathbb{Z}_3[x]/(x^3+x^2+x-1).$$

Пример 4. Для любого натурального числа n, свободного от квадратов, существует поле $\mathbb{Q}[\sqrt{n}]$, которое получается как

$$\mathbb{Q}[x]/(x^2-n).$$

Пример 5. Для любого поля $\mathbb{F}$ можно рассмотреть поле $\mathbb{F}(x)$ рациональных дробей над $\mathbb{F}$. Оно состоит из дробей

$$\frac{f(x)}{g(x)}, \quad f(x), g(x) \in \mathbb{F}[x], \quad g(x) \neq 0.$$

ХАРАКТЕРИСТИКА ПОЛЯ

В поле всегда есть единица, не равная нулю. В аддитивной группе поля единица порождает циклическую подгруппу $\langle 1 \rangle = \{1, 1+1, 1+1+1, \dots\}$. Если данная группа конечна и содержит n элементов, то говорят, что характеристика поля равна n. Если циклическая группа $\langle 1 \rangle$ бесконечна, то говорят, что характеристика поля - нулевая.

Замечание 1. Если у поля $\mathbb{F}$ характеристика равна $n > 0$, то n — простое число.

Действительно, если $n = mk$, то в поле $\mathbb{F}$ сумма m единиц (не равная нулю), умноженная на сумму k единиц (не равную нулю) равна нулю. Значит, в поле имеются делители нуля, что невозможно. Таким образом, положительная характеристика всегда является простым числом.

Если единица в поле имеет порядок p или бесконечный порядок, то такой же порядок имеет и любой ненулевой элемент:

$$a+a+\dots+a+a = a\cdot 1+a\cdot 1+\dots+a\cdot 1 = a(1+1+\dots+1).$$

Лемма 1. *Если поле* $\mathbb{F}$ *имеет характеристику* 0*, то в него естественно вложено подполе* $\mathbb{Q}$ *рациональных чисел. Если поле* $\mathbb{F}$ *имеет характеристику* p*, то в него естественно вложено подполе* $\mathbb{Z}_p$*.*

Доказательство. Действительно, пусть характеристика поля $\mathbb{F}$ равна нулю. Тогда целые числа можно вложить в поле $\mathbb{F}$ следующим образом: если $n > 0$, то $n = 1 + 1 + \cdots + 1$ (сумма n единиц), отображаем ее в сумму того же числа единиц; ноль отображаем в ноль, а противополжное к n — в противоположное к его образу.

Такое отображение, очевидно, будет гомоморфизмом. Если бы какой-то ненулевой элемент принадлежал ядру этого гомоморфизма, то сумма конечного числа единиц была бы равно нулю в поле $\mathbb{F}$, что невозможно. Значит, это вложение.

Таким образом, можно считать, что целые числа лежат в поле $\mathbb{F}$. Рациональные числа тогда лежат в нем как отношения целых к натуральным.

Если у поля $\mathbb{F}$ характеристика равна p, то то же самое отображение имеет ядро — все целые числа, кратные p. ТАким образом, образ $\mathbb{Z}$ — это $\mathbb{Z}_p$, которое является полем. □

Лемма 2. *Конечное поле может содержать только p^n элементов, где p — простое, n — натуральное число.*

Доказательство. Любое поле является линейным пространством над своим подполем (прямая проверка). В конечном поле характеристики p (ясно, что конечное поле не может иметь характеристику ноль) содержится подполе $\mathbb{Z}_p$. Также ясно, что конечное поле конечномерно. Пусть его размерность над $\mathbb{Z}_p$ равна n. Тогда в нем ровно p^n элементов. □

Упражнение 1. Существует ли бесконечное поле положительной характеристики?

Лемма 3. *Если поле $\mathbb{F}$ характеристики p конечно, то отображение $x \mapsto x^p$ является его автоморфизмом.*

Доказательство. Действительно, это отображение, очевидно, мультипликативно. Оно аддитивно, так как

$$(x+y)^p = x^p + C_p^1 x^{p-1} y + C_p^2 x^{p-2} y^2 + \cdots + C_p^{p-1} x y^{p-1} + y^p,$$

а так как C_p^i для $i = 1, \ldots, p-1$ делится на p, то эта сумма равна $x^p + y^p$ в поле $\mathbb{F}$.

Отображение инъективно, так как из $x^p = y^p$ следует $x^p - y^p = 0 \Longrightarrow (x-y)^p = 0 \Longrightarrow x - y = 0$.

Благодаря конечности поля оно оказывается биективным. $\square$

РАСШИРЕНИЯ ПОЛЕЙ

Определение 1. Поле L называется *расширением* поля K, если K является подполем в L. Расширение L поля K называется *конечным*, если $\dim_K L < \infty$. Число $\dim_K L <$ в этом случае называется *степенью* расширения L.

Элемент $x \in L$ называется *алгебраическим* над K, если он удовлетворяет некоторому нетривиальному алгебраическому уравнению с коэффициентами из K, и *трансцендентным* в противном случае. Расширение L поля K называется *алгебраическим*, если всякий его элемент алгебраичен над K.

Теорема 1. *Любое конечное расширение поля является алгебраическим.*

Доказательство. Действительно, если L — конечное расширение поля K, то L_K — конечномерно. Рассмотрим произвольный элемент $g \in L$. Все степени элемента g не могут быть линейно независимы, поэтому существует некоторая линейная комбинация

этих степеней

$$\alpha_0 + \alpha_1 g + \alpha_2 g^2 + \cdots + \alpha_n g^n = 0.$$

Это означает алгебраичность элемента g. $\square$

Упражнение 2. Является ли алгебраическим расширением $\mathbb{R}$ над $\mathbb{Q}$?

Замечание 2. Напомним, что если K — поле, $K[x]$ — кольцо многочленов, $f(x) \in K[x]$ — произвольный многочлен степени n, то факторкольцо $L = K[x]/(f(x))$ является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над K. В этом случае L является конечным расширением поля K степени n (*простое расширение*).

Теорема 2. *Если L — конечное расширение поля K, а M — конечное расширение поля L, то M — конечное расширение поля K, причем*

$$\dim_K M = \dim_K L \cdot \dim_L M.$$

Доказательство. Пусть базис M над L — $f_1, \ldots, f_k$, базис L над K — $e_1, \ldots, e_m$. Покажем, что базис M над K — $\{f_i e_j \mid i = 1, \ldots, k, j = 1, \ldots, m\}$.

То, что данное множество порождает все M над K, очевидно.

Докажем линейную независимость. Пусть

$$\sum_{i,j} \alpha_{ij} f_i e_j = 0,$$

где $\alpha_{ij} \in K$.

Тогда

$$\sum_i (\alpha_{i,1} e_1 + \cdots + \alpha_{i,m} e_m) f_i = 0.$$

Так как $f_1, \ldots, f_k$ — базис M над L, то все коэффициенты при $f_1, \ldots, f_k$ равны нулю, но каждый коэффициент — это линейная комбинация элементов базиса L над K, то все $\alpha_{i,j}$ равны нулю, что и требовалось. □

Теорема 3. *Если L — расширение поля K, M — расширение поля L, а M — конечное расширение поля K, то расширения L над K и M над L — конечны.*

Доказательство. Пусть одно из расширений L над K или M над L бесконечно. Это означает, что один из базисов $f_1, \ldots$ поля M над полем L или $e_1, \ldots$ поля L над K бесконечен.

Точно так же, как в предыдущем доказательстве, мы тогда можем показать, что элементы вида $f_i e_j$ линейно независимы.

Однако их число бесконечно, а по условию поле M над K — конечно. □

Теорема 4. *Если поле L порождается над K конечным числом алгебраических элементов $u_1, \ldots, u_n$, то оно является конечным расширением поля K.*

Доказательство. Для начала поймем, что достаточно доказать утверждение при условии, что мы добавляем только одну переменную, так как добавление n переменных эквивалентно последовательному добавлению по одной переменной к все более расширяющимся полям.

Если мы рассматриваем поле $K(u)$, и оно является бесконечным расширением поля K, то существует

сколько угодно линейно независимых над K дробей вида $f_i(u)/g_i(u)$. Линейная независимость дробей

$$f_1(u)/g_1(u), \ldots, f_n(u)/g_n(u)$$

равносильна линейной независимости многочленов

$$h(u)f_1(u)/g_1(u), \ldots, h(u)f_n(u)/g_n(u),$$

где

$$h(u) = \text{НОК}(g_1(u), \ldots, g_n(u)),$$

что для любого n не может выполняться. Противоречие. □

Лемма 4. *Пусть L — какое-либо расширение поля K. Совокупность $\overline{K}$ всех элементов поля L, алгебраических над K, является подполем, алгебраически замкнутым в L (в том смысле, что любой элемент поля L, алгебраический над $\overline{K}$, принадлежит $\overline{K}$).*

Доказательство. Нам нужно доказать только, что сумма, разность, произведение и частное двух алгебраических над K — алгебраические над K. Это практически прямое следствие предыдущей леммы,

так как все эти функции от пар алгебраических элементов входят в конечное расширение, которое является алгебраическим. □

Теорема 5. *Поле $\overline{Q}$ алгебраических чисел (всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами) алгебраически замкнуто.*

Доказательство. Рассмотрим какой-нибудь многочлен с алгебраическими коэффициентами. Подполе поля $\overline{Q}$, содержащее все коэффициенты этого многочлена, является конечным расширением поля Q. Так как два последовательных конечных расширения дают конечное расширение, то корень многочлена — алгебраический над Q. □

ПОЛЕ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

Определение 2. Расширение L поля K называется *полем разложения* многочлена $f \in K[x]$ (не обязательно неприводимого), если f разлагается в $L[x]$ на линейные множители и поле L порождается над K его корнями.

Гомоморфизмы (в частности, изоморфизмы) расширений поля K, тождественные на K, называются *гомоморфизмами* (*изоморфизмами*) *над* K.

Теорема 6. *Поле разложения любого многочлена* $f \in K[x]$ *существует.*

Доказательство. Разложим многочлен $f(x)$ на неприводимые множители над полем K. Рассмотрим один из неприводимых множителей — $h(x)$.

Рассмотрим поле $K_1 = K[x]/(h(x))$. Как мы знаем, это поле является расширением поля K, в котором у многочлена $h(x)$ появляется (хотя бы один) корень. Таким образом, многочлен $f(x)$ над полем K_1 разложится на большее число неприводимых сомножителей.

Последовательными расширениями мы можем добиться того, чтобы все сомножители стали линейными. □