ЛЕКЦИЯ 18

РАСШИРЕНИЯ ПОЛЕЙ

СУЩЕСТВОВАНИЕ ПОЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

СУЩЕСТВОВАНИЕ ПОЛЯ ИЗ p^n ЭЛЕМЕНТОВ

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

Замечание 1. 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 (о башне полей). *Если L — конечное расширение поля K, а M — конечное расширение поля L, то M — конечное расширение поля K, причем*

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

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 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.

Пусть расширение M над K конечно, а 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 выше, 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. $\square$

Теорема 3. *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 заметим, 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. $\square$

Теорема 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. Во-первых, мы хотим доказать, что $\overline{K}$ является полем.

Для этого требуется показать, что сумма, разность, произведение и частное двух алгебраических над K — алгебраические над K.

Возьмем эти два алгебраических над K элемента: $a, b \in \overline{K}$ и рассмотрим поле $K(a, b)$. По предыдущей теореме оно конечно над K, по теореме 1 оно алгебраическое над K, то есть все его элементы (в том числе, $a+b, a-b, ab$ и a/b) — алгебраические над K. Значит, $\overline{K}$ — поле.

Далее нам нужно доказать, что любой элемент $a \in L$, алгебраический над $\overline{K}$, является алгебраическим над исходным полем K.

Пусть a является корнем многочлена

$$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n, \qquad \alpha_0, \ldots, \alpha_n \in \overline{K}.$$

Рассмотрим тогда поле $K_1 := K(\alpha_0, \ldots, \alpha_n)$, которое по предыдущей теореме является конечным расширением поля K. По условию элемент a — алгебраический над K_1, то есть расширение $K_1(a)$ — конечное над K_1, откуда оно является конечным расширением поля K, а по теореме 1 — алгебраическим. Таким образом, a — алгебраический над K, что и требовалось.

□

Следствие 1. *Поле $\overline{\mathbb{Q}}$ алгебраических чисел (всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами) алгебраически замкнуто.*

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 5. *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. $\square$

Теорема 6. *Для любого простого p и натурального n существует поле из p^n элементов.*

Доказательство. Рассмотрим поле L разложения многочлена $x^{p^n} - x$ над полем $\mathbb{Z}_p$.

У данного многочлена нет кратных корней (так как его производная равна -1 и взаимно проста с самим многочленом), поэтому все корни многочлена $x^{p^n} - x$, лежащие в L, различны.

Количество таких корней равно ровно $q = p^n$.

Докажем, что множество этих корней образует поле.

Действительно, если $a^q = a$ и $b^q = b$, то $(ab)^q = ab$, $(a/b)^q = a/b$, поэтому данное множество замкнуто относительно умножения и деления на ненулевые элементы.

Если $a^q = a$ и $b^q = b$, то $(a + b)^q = (a + b)^{p^n} = a^q + b^q = a + b$, то есть множество корней замкнуто относительно сложения и (аналогично) вычитания.

Таким образом, мы нашли искомое поле из p^n элементов.

□

РАСШИРЕНИЕ ГОМОМОРФИЗМА

Предложение 1. *Пусть $K(\alpha)$ — расширение поля K, полученное присоединением корня α неприводимого многочлена $h \in K[x]$, и φ — гомоморфизм поля K в некоторое поле $\mathbb{F}$. Гомоморфизм φ продолжается до гомоморфизма $\widetilde{\varphi} : K(\alpha) \to \mathbb{F}$ ровно столькими способами, сколько различных корней имеет в $\mathbb{F}$ многочлен $\varphi(h)$, полученный из h применением к его коэффициентам гомоморфизма φ.*

Доказательство. Искомое продолжение $\widetilde{\varphi}$, если оно существует, задается формулой

$$\widetilde{\varphi}(a_0 + a_1\alpha + \cdots + a_m\alpha^m) = \\ = \varphi(a_0)+\varphi(a_1)\beta+\cdots+\varphi(a_m)\beta^m, \quad (a_0, a_1, \ldots, a_m \in K),$$

где $\beta = \widetilde{\varphi}(\alpha)$ — некоторый элемент поля $\mathbb{F}$.

Применяя эту формулу к равенству $h(\alpha) = 0$, получаем, что $\varphi(h)(\beta) = 0$.

Обратно, если $\beta \in \mathbb{F}$ — корень многочлена $\varphi(h)$, то данная формула корректно определяет гомоморфизм $\widetilde{\varphi} : K(\alpha) \to \mathbb{F}$. □