Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 9

Примеры полей. Характеристика поля. Расширения полей, алгебраические и трансцендентные элементы. Минимальные многочлен. Конечное расширение и его степень. Присоединение корня многочлена. Поле разложения многочлена: существование и единственность.

Мы знаем не так много примеров полей. Это бесконечные поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и конечные поля $\mathbb{Z}_p$, где p — простое число. Конструкция поля отношений позволяет строить новые поля из уже имеющихся. А именно, если K — произвольное поле, то можно рассмотреть поле отношений $K(x)$ кольца многочленов $K[x]$ (это поле называется *полем рациональных дробей* над K). Элементами поля $K(x)$ являются дроби $f(x)/g(x)$, где $f(x), g(x) \in K[x]$ и $g(x) \neq 0$.

Несколько других примеров полей:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, \quad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}, \quad \mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}.$$

Определение 1. Пусть K — произвольное поле. *Характеристикой* поля K называется такое наименьшее натуральное число p, что $\underbrace{1 + \ldots + 1}_{p} = 0$. Если такого натурального p не существует, говорят, что характеристика поля равна нулю. Обозначение: $\operatorname{char} K$.

Например, $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$ и $\operatorname{char} \mathbb{Z}_p = \operatorname{char} \mathbb{Z}_p(x) = p$.

Из определения следует, что всякое поле характеристики нуль бесконечно. Примером бесконечного поля характеристики $p > 0$ является поле $\mathbb{Z}_p(x)$.

Предложение 1. *Характеристика произвольного поля K либо равна нулю, либо является простым числом.*

Доказательство. Положим $p = \operatorname{char} K$ и предположим, что $p > 0$. Так как $0 \neq 1$ в K, то $p \geqslant 2$. Если число p не является простым, то $p = mk$ для некоторых $m, k \in \mathbb{N}$, $1 < m, k < p$. Тогда в K верно равенство

$$0 = \underbrace{1 + \ldots + 1}_{mk} = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{k}).$$

В силу минимальности числа p в последнем выражении обе скобки отличны от нуля, но такое невозможно, так как в поле нет делителей нуля. □

Упражнение 1. Пересечение любого семейства подполей фиксированного поля K является подполем в K. В частности, для всякого подмножества $S \subseteq K$ существует наименьшее по включению подполе в K, содержащее S. Это подполе совпадает с пересечением всех подполей в K, содержащих S.

Из приведённого выше упражнения следует, что в каждом поле существует наименьшее по включению подполе, оно называется *простым подполем*.

Предложение 2. *Пусть K — поле и K_0 — его простое подполе. Тогда:*

(1) *если* $\operatorname{char} K = p > 0$, *то* $K_0 \cong \mathbb{Z}_p$;

(2) *если* $\operatorname{char} K = 0$, *то* $K_0 \cong \mathbb{Q}$.

Доказательство. Пусть $\langle 1 \rangle \subseteq K$ — циклическая подгруппа по сложению, порождённая единицей. Заметим, что $\langle 1 \rangle$ — подкольцо в K. Поскольку всякое подполе поля K содержит единицу, оно содержит и множество $\langle 1 \rangle$. Следовательно, $\langle 1 \rangle \subseteq K_0$.

Если $\operatorname{char} K = p > 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \simeq \mathbb{Z}_p$. Но, как мы уже знаем из лекции 6, кольцо $\mathbb{Z}_p$ является полем, поэтому $K_0 = \langle 1 \rangle \simeq \mathbb{Z}_p$.

Если же $\operatorname{char} K = 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \cong \mathbb{Z}$. Тогда K_0 содержит все дроби вида a/b, где $a, b \in \langle 1 \rangle$ и $b \neq 0$. Ясно, что все такие дроби образуют поле, изоморфное полю $\mathbb{Q}$. □

Определение 2. Если K — подполе поля F, то говорят, что F — *расширение* поля K.

Например, всякое поле есть расширение своего простого подполя.

Определение 3. *Степенью* расширения полей $K \subseteq F$ называется размерность поля F как векторного пространства над полем K. Обозначение $[F : K]$.

Например, $[\mathbb{C} : \mathbb{R}] = 2$ и $[\mathbb{R} : \mathbb{Q}] = \infty$.

Определение 4. Расширение полей $K \subseteq F$ называется *конечным*, если $[F : K] < \infty$.

Предложение 3. *Пусть $K \subseteq F$ и $F \subseteq L$ — конечные расширения полей. Тогда расширение $F \subseteq L$ также конечно и $[L : K] = [L : F][F : K]$.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис F над K и $f_1, \ldots, f_m$ — базис L над F. Достаточно доказать, что множество

$$\{e_i f_j \mid i = 1, \ldots, n;\ j = 1, \ldots, m\} \tag{1}$$

является базисом L над K. Для этого сначала покажем, что произвольный элемент $a \in L$ представим в виде линейной комбинации элементов (1) с коэффициентами из K. Поскольку $f_1, \ldots, f_m$ — базис L над F, имеем $a = \sum\limits_{j=1}^{m} \alpha_j f_j$ для некоторых $\alpha_j \in F$. Далее, поскольку $e_1, \ldots, e_n$ — базис F над K, для каждого $j = 1, \ldots, m$ имеем $\alpha_j = \sum\limits_{i=1}^{n} \beta_{ij} e_i$ для некоторых $\beta_{ij} \in K$. Отсюда получаем, что $a = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \beta_{ij}(e_i f_j)$.

Теперь проверим линейную независимость элементов (1). Пусть $\sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \gamma_{ij}(e_j f_i) = 0$, где $\gamma_{ij} \in K$. Переписав это равенство в виде $\sum\limits_{j=1}^{m} (\sum\limits_{i=1}^{n} \gamma_{ij} e_i) f_j = 0$ и воспользовавшись тем, что элементы $f_1, \ldots, f_m$ линейно независимы над F, мы получим $\sum\limits_{i=1}^{n} \gamma_{ij} e_i = 0$ для каждого $j = 1, \ldots, m$. Теперь из линейной независимости элементов $e_1, \ldots, e_n$ над K вытекает, что $\gamma_{ij} = 0$ при всех i, j. Таким образом, элементы (1) линейно независимы. □

Пусть $K \subseteq F$ — расширение полей.

Определение 5. Элемент $\alpha \in F$ называется *алгебраическим* над подполем K, если существует ненулевой многочлен $f(x) \in K[x]$, для которого $f(\alpha) = 0$. В противном случае α называется *трансцендентным* элементом над K.

Определение 6. *Минимальным многочленом* алгебраического элемента $\alpha \in F$ над подполем K называется ненулевой многочлен $h_\alpha(x)$ наименьшей степени, для которого $h_\alpha(\alpha) = 0$.

Лемма 1. *Пусть $\alpha \in F$ — алгебраический элемент над K и $h_\alpha(x)$ — его минимальный многочлен. Тогда:*

(а) *$h_\alpha(x)$ определён однозначно с точностью до пропорциональности;*

(б) *$h_\alpha(x)$ является неприводимым многочленом над полем K;*

(в) *для произвольного многочлена $f(x) \in K[x]$ равенство $f(\alpha) = 0$ имеет место тогда и только тогда, когда $h_\alpha(x)$ делит $f(x)$.*

Доказательство. (а) Пусть $h'_\alpha(x)$ — ещё один минимальный многочлен элемента α над K. Тогда $\deg h_\alpha(x) = \deg h'_\alpha(x)$. Умножив многочлены $h_\alpha(x)$ и $h'_\alpha(x)$ на подходящие константы, добьёмся того, чтобы их старшие коэффициенты стали равны единице. После этого положим $g(x) = h_\alpha(x) - h'_\alpha(x)$. Тогда $g(\alpha) = 0$ и $\deg g(x) < \deg h_\alpha(x)$. Учитывая определение минимального многочлена, мы получаем $g(x) = 0$.

(б) Пусть $h_\alpha(x) = h_1(x)h_2(x)$ для некоторых $h_1(x), h_2(x) \in K[x]$, причём $0 < \deg h_i(x) < \deg h_\alpha(x)$ при $i = 1, 2$. Так как $h_\alpha(\alpha) = 0$, то либо $h_1(\alpha) = 0$, либо $h_2(\alpha) = 0$, что противоречит минимальности $h_\alpha(x)$.

(в) Очевидно, что если $h_\alpha(x)$ делит $f(x)$, то $f(\alpha) = 0$. Докажем обратное утверждение. Разделим $f(x)$ на $h_\alpha(x)$ с остатком: $f(x) = q(x)h_\alpha(x) + r(x)$, где $q(x), r(x) \in K[x]$ и $\deg r(x) < \deg h_\alpha(x)$. Тогда условие $f(\alpha) = 0$ влечёт $r(\alpha) = 0$. Из минимальности многочлена $h_\alpha(x)$ получаем $r(x) = 0$. □

Для каждого элемента $\alpha \in F$ обозначим через $K(\alpha)$ наименьшее подполе в F, содержащее K и α.

Предложение 4. *Пусть $\alpha \in F$ — алгебраический элемент над K и n — степень его минимального многочлена над K. Тогда*

$$K(\alpha) = \{\beta_0 + \beta_1\alpha + \ldots + \beta_{n-1}\alpha^{n-1} \mid \beta_0, \ldots, \beta_{n-1} \in K\}.$$

Кроме того, элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ линейно независимы над K. В частности, $[K(\alpha) : K] = n$.

Доказательство. Легко видеть, что

$$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in K[x], f(\alpha) \neq 0\}.$$

Действительно, такие элементы лежат в любом подполе поля F, содержащем K и α, и сами образуют поле. Теперь возьмём произвольный элемент $\frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$ и покажем, что он представим в виде, указанном в условии. Пусть $h_\alpha(x) \in K[x]$ — минимальный многочлен элемента α над K. Поскольку $g(\alpha) \neq 0$, в силу леммы 1(в) многочлен $h_\alpha(x)$ не делит $g(x)$. Но $h_\alpha(x)$ неприводим по лемме 1(б), поэтому $(g(x), h_\alpha(x)) = 1$. Значит, существуют такие многочлены $u(x), v(x) \in K[x]$, что $u(x)g(x) + v(x)h_\alpha(x) = 1$. Подставляя в последнее равенство $x = \alpha$, мы получаем $u(\alpha)g(\alpha) = 1$. Отсюда $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)u(\alpha)$, и мы избавились от знаменателя. Теперь уменьшим степень числителя. Пусть $r(x)$ — остаток от деления $f(x)u(x)$ на $h_\alpha(x)$. Тогда $f(\alpha)u(\alpha) = r(\alpha)$ и, значит, $\frac{f(\alpha)}{g(\alpha)} = r(\alpha)$, что показывает представимость элемента $\frac{f\alpha)}{g(\alpha)}$ в требуемом виде.

Остаётся показать, что элементы $1, \alpha, \ldots, \alpha^{n-1}$ поля F линейно независимы над K. Если

$$\gamma_0 + \gamma_1\alpha + \ldots + \gamma_{n-1}\alpha^{n-1} = 0$$

для некоторых $\gamma_0, \gamma_1, \ldots, \gamma_{n-1} \in K$, то для многочлена $w(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{n-1}x^{n-1} \in K[x]$ получаем $w(\alpha) = 0$. Тогда из леммы 1(в) и условия $\deg w(x) < \deg h_\alpha(x)$ вытекает, что $w(x) = 0$, то есть $\gamma_0 = \gamma_1 = \ldots = \gamma_{n-1} = 0$. □

Теорема 1. *Пусть K — произвольное поле и $f(x) \in K[x]$ — многочлен положительной степени. Тогда существует конечное расширение $K \subseteq F$, в котором многочлен $f(x)$ имеет корень.*

Доказательство. Достаточно построить конечное расширение, в котором имеет корень один из неприводимых делителей $p(x)$ многочлена $f(x)$.

Покажем сначала, что факторкольцо $K[x]/(p(x))$ является полем. В самом деле, если многочлен $g(x) \in K[x]$ не делится на $p(x)$, то $(g(x), p(x)) = 1$, и тогда существуют многочлены $u(x), v(x) \in K[x]$, для которых $u(x)g(x) + v(x)p(x) = 1$. Взяв образ последнего равенства в факторкольце $K[x]/(p(x))$, мы получим

$$(u(x) + (p(x)))(g(x) + (p(x))) = 1 + (p(x)),$$

т. е. элемент $u(x) + (p(x))$ является обратным к $g(x) + (p(x))$. Значит, $K[x]/(p(x))$ — поле, и мы возьмём его в качестве F.

Заметим теперь, что расширение $K \subseteq F$ является конечным. Действительно, для всякого многочлена $g(x) \in K[x]$ в поле $F = K[x]/(p(x))$ имеем $g(x) + (p(x)) = r(x) + (p(x))$, где $r(x)$ — остаток от деления $g(x)$ на $p(x)$. Отсюда следует, что F порождается как векторное пространство над K элементами

$$1 + (p(x)), x + (p(x)), \ldots, x^{n-1} + (p(x)),$$

где $n = \deg p(x)$. (Так же легко показать, что эти элементы образуют базис в F над K.)

Остаётся показать, что в поле F многочлен $p(x)$ имеет корень. Это похоже на обман, но корнем будет... $x + (p(x))$. Действительно, пусть $p(x) = a_n x^n + a_{n-1}x^{n-1} + a_1 x + a_0$, где $a_0, a_1, \ldots, a_n \in K$. Тогда

$$p(x + (p(x))) = a_n(x + (p(x)))^n + a_{n-1}(x + (p(x)))^{n-1} + \ldots + a_1(x + (p(x)) + a_0 =$$
$$= (a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0) + (p(x)) = p(x) + (p(x)) = (p(x)),$$

а $(p(x))$ есть не что иное, как нуль в F. □

Говорят, что поле $K[x]/(p(x))$ получено из поля K *присоединением корня* неприводимого многочлена $p(x)$. Нетрудно проверить, что если α — некоторый корень многочлена $p(x)$ в $K[x]/(p(x))$, то поле $K[x]/(p(x))$ совпадает с подполем $K(\alpha)$.

Определение 7. Пусть K — некоторое поле и $f(x) \in K[x]$ — многочлен положительной степени. *Полем разложения* многочлена $f(x)$ называется такое расширение F поля K, что

(1) многочлен $f(x)$ разлагается над F на линейные множители;

(2) корни многочлена $f(x)$ не лежат ни в каком собственном подполе поля F, содержащем K.

Пример 1. Рассмотрим многочлен $f(x) = x^4 + x^3 + x^2 + x + 1$ над $\mathbb{Q}$. Так как $(x-1)f(x) = x^5 - 1$, корнями многочлена $f(x)$ являются все корни степени 5 из единицы, отличные от единицы. Если присоединить к $\mathbb{Q}$ один из корней ϵ многочлена f, то его остальные корни можно получить, возводя число ϵ в натуральные степени. Таким образом, присоединение одного корня сразу приводит к полю разложения многочлена.

Пример 2. Многочлен $f(x) = x^3 - 2$ неприводим над полем $\mathbb{Q}$. Присоединение к полю $\mathbb{Q}$ корня этого многочлена приводит к полю $\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$. Данное поле не является полем разложения многочлена $f(x)$, поскольку в нём $f(x)$ имеет только один корень и не имеет двух других корней. Поскольку корнями данного многочлена являются числа

$$\sqrt[3]{2}, \quad \sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{-3}}{2}), \quad \sqrt[3]{2}(-\frac{1}{2} - \frac{\sqrt{-3}}{2}),$$

полем разложения многочлена $f(x)$ является поле

$$F = \{\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2\sqrt[3]{4} + \alpha_3\sqrt{-3} + \alpha_4\sqrt[3]{2}\sqrt{-3} + \alpha_5\sqrt[3]{4}\sqrt{-3} \mid \alpha_i \in \mathbb{Q}\},$$

которое имеет над $\mathbb{Q}$ степень 6.

Пусть F и F' — два расширения поля K. Говорят, что изоморфизм $F \xrightarrow{\sim} F'$ является *тождественным на* K, если при этом изоморфизме каждый элемент поля K переходит в себя.

Теорема 2. *Поле разложения любого многочлена $f(x) \in K[x]$ существует и единственно с точностью до изоморфизма, тождественного на K.*

Доказательство этой теоремы можно найти, например, в книге Э. Б. Винберга «Курс алгебры». Мы не включаем это доказательство в программу нашего курса.

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 1, §§ 3–6 и глава 9, § 5)
[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 4, § 3)
[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 5, § 1)
[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 14, §§ 66-67)